

arcutronix

@ccess the Ethernet

USER GUIDE

SCX2



**arcutronix GmbH
Deutschland**

**Installation and
Operation Manual**

SCX - System Controller

USER GUIDE



Product Family:	SCX2
Enclosed Descriptions:	
Product Type Number: SCX2	0805-7020
SW-Version (≥):	V 4_1_10
Date of Issue:	2011-09-07

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
<http://www.arcutronix.com>

Copyright Note

© Copyright 2009, arcutronix GmbH. All rights reserved.

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

Document Contents

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

Trademarks

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

About this Book

Document Organization

This guide describes the hardware and software of the SCX - System Controller. It provides information on configuration, system installation and the technical data.

The intended audience of this document is anyone who is responsible for installing, maintaining or operating the SCX - System Controller. 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. Font attributes are used to identify single words or chapters with certain content, e.g. screen shots and listings are in Courier, like:

```
This is a line of a screen shot.
```

The information in this manual is divided in several object orientated universal chapters. View and compare to your device to find the individual information: take the information that fits. Ignore the information, which is not relevant in the current case.

Chapters

Chapter 0, **Safety, Instructions, Statements**, handling, precautions, warnings.

Chapter 1, **Introduction**, general description of the SCX2 devices and applications for use.

Chapter 2, **Getting Started**, short form about installation, mounting and configuration of SCX2-family.

Chapter 3, **Hardware**, description of hardware and front panel elements.

Chapter 4, **Installation and Test**, installation procedures.

Chapter 5, **Control Software SCX2**, control and configuration of the SCX2.

Chapter 6, **SNMP and MIBs**, provides the description of the MIB.

Appendix A, **Technical Data**, technical data of the SCX2.

Appendix B, **FTP-Access**, technical data of the SCX2.

Appendix EC, **EC Declaration of Conformity**, valid for the SCX2 product family.

Release History

- 2009-01-14 First issue of the SCX2 User Guide.
- 2009-03-26 Added and changed the following topics:
- Updated the order number and fixed minor spelling issues.
 - CE declaration added.
 - Chapter 6 (SNMP) changed towards ax-MIBS.
- 2009-09-29 Added and changed the following topics:
- Updated configuration storage. All changes have to be stored on device.
 - Frontpage and last page in new design.
- 2010-02-24 Added and changed the following topics:
- Detailed explanation on how to setup the ftp-access for SCX2.
 - SCX2 does not support auto-X-over, as before stated in Appendix A, but is always in DTE-mode. Some statements in the manual were added to avoid problems.
- 2011-03-18 Added and changed the following topics:
- Minor corrections in chapter 3.

List of Contents

About this Book

Document Organization	about-1
Chapters	about-1
.....	about-2
.....	about-2
Release History	about-2

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	0-3
Inspection	0-3
Commissioning	0-3
Cleaning	0-3
Quality	0-4
Repair	0-4
Disposal and Recycling	0-4
CE Conformity	0-4
Electromagnetic Immunity Statement	0-5
Instructions to User	0-5
Electromagnetic Emissions Statements	0-5

Chapter 1 Introduction

SCX2 Description	1-1
General	1-1
SCX2 Functions at a Glance	1-2
Alarm Conditions	1-2
IP-Port	1-2
VT100-Port	1-3
SLIP	1-3
PPP	1-3
Order Information	1-4
Accessories	1-4
Housings and Cables	1-4

Chapter 2 Getting Started

Delivered Parts	2-1
Preparing the Startup	2-1
Operating Conditions	2-1
Ambient Conditions	2-1
SCX2 Mounting	2-2
Startup of the SCX2	2-2
Switching on the Device	2-2
Configuration Methods	2-3

Chapter 3 Hardware

Main Board	3-1
SCX2 Front Panel	3-1
Indicators & Connectors	3-2
Local IP-Management Interface	3-3
RS232 Control Port Connector	3-3
RS232 Connection Cable	3-4
Configuration of the Control Port (RJ45)	3-4
RS232 Configuration by the DIP Switch ST2	3-5
Advanced Management Daisy Chain	3-6
More SCX2 Configuration Switches	3-6

Chapter 4 Installation and Test

Preparation	4-1
ESD Protection of Cards	4-1
Environmental Conditions	4-1
Installation Hints	4-2
Power Management	4-2
Rules of the Power Management	4-2
Field Installation of SCX2 Cards	4-3
Installation	4-3
Removal	4-3

Chapter 5 Control Software SCX2

General Information	5-1
Local RS-232 Interface	5-1
Local Ethernet Interface	5-1
Security Issues	5-2
Login Screen	5-3
Navigation	5-4
Select a menu entry	5-4
Overview to keys	5-4
Display and User Actions	5-5

Exit	5-5
Main Menu	5-6
AGENT CONFIGURATION	5-7
Administrator Setup	5-8
Date and Time	5-9
TCP/IP Address and Settings	5-10
TCP/IP Routing Table	5-11
TCP/IP Address Cache (View Only)	5-12
SNMP System Information	5-13
SNMP Access Settings	5-14
SNMP Trap Receivers	5-15
Login User Access Settings	5-16
Realtime Event Monitoring	5-17
Event History	5-17
Maintenance	5-18
Factory Information	5-19
Save Agent Config to Flash	5-19
Restore Agent Config from Flash	5-20
Update Agent Application via X/Y-Modem	5-20
Flash File Manager	5-22
Reset Agent	5-23
Reset System	5-23
Startup History	5-23
Clear Alarm	5-24
Change Login Password	5-24
Flash File System and File Transfer	5-25
The Flash File System	5-25
Tips for Terminal Emulation Programs	5-25
Send Dialog Box	5-26
Serial Port	5-26
Telnet Tips	5-26
XModem	5-26
YModem	5-26
The Software for the Agent	5-26
The Software for Modules	5-27
SYSTEM	5-28
RACK 1	5-29
Setup of SCX2s	5-29
MANAGEMENT MODULE ON SLOT x	5-30
GENERAL INFORMATION	5-31
SELF TEST	5-32
RUN TIME	5-32
POWER SUPPLY	5-33
FANS	5-34
TEMPERATURE	5-35

TRAPS & ALARMS.	5-36
UPDATE	5-37

Chapter 6 SNMP and MIBs

SNMP Access Generally	6-1
SNMPv1	6-2
SNMPv2c	6-2
Traps.....	6-2
Installation Prerequisites.....	6-2
Preparing the SNMP Management System	6-3
Management Information Bases (MIBS).....	6-3
SCX2 MIB List	6-5
axg2 MIB.....	6-5
axg2-agent MIB	6-6
axg2-scx-as MIB.....	6-9
axg2-chassis MIB.....	6-10
axg2-chassis MIB Traps	6-11
axg2-scx-cs MIB.....	6-11
axg2-scx-cs MIB Traps	6-13
axg2-device MIB.....	6-13
axg2-Device MIB Traps	6-15
axg2-scx-ds MIB.....	6-16
axg2-scx-ds MIB Traps.....	6-18

Appendix A Technical Data

Appendix B FTP-Access

Intro.....	B-1
Proper Setup.....	B-1
FTP-connection.....	B-2
Windows Explorer.....	B-2
1st Step.....	B-2
2nd Step	B-3
3rd Step	B-4
Mozilla Firefox.....	B-5
1st Step.....	B-5
2nd Step	B-6
3rd Step	B-7
4th Step.....	B-8
Which File to which Directory?	B-9
SCX2-Files (RTB-Files)	B-9
Device-Files (BIP-Files)	B-10
WebGUI-Files (www)	B-10
Where to get the Update-File(s)?.....	B-10

Appendix EC EC Declaration of Conformity

Declaration of Conformity EC-1

List of Figures

Figure 1-1	SCX2 10-slot Chassis SRX10	1-1
Figure 2-1	Slot for SCX2 in rail 63	2-2
Figure 3-1	Pin Assignment of the Ethernet-Port Connector (RJ-45), DTE	3-3
Figure 3-2	Pin Assignment of the Control Port Connector (RJ-45)	3-4
Figure 3-3	RS232 Connection cable	3-4
Figure 3-4	SCX2, Main Board 2002.17810001.xx	3-5
Figure 3-5	SCX2, Piggy-Board 566.00.xx	3-7
Figure 6-1	The SNMP Generation 2 MIB Tree	6-4

List of Tables

Table 0-1	Effects of Cleaning Liquids	0-3
Table 1-1	Order Matrix	1-4
Table 1-2	Accessories Housings & Cables	1-4
Table 2-1	Ambient Conditions.	2-1
Table 3-1	SCX2 Front View: Connectors, Indicators, and Controls	3-2
Table 3-2	Indicator Color Meanings	3-3
Table 3-3	SCX2, RS232 Configuration Switch ST2, Management Operation Mode	3-5
Table 3-4	Pin Assignment of the Management Port Connectors	3-6
Table 5-1	Overview to key-strokes	5-4
Table 5-2	SCX2 Main Menu Options	5-6
Table 5-3	Agent Configuration	5-7
Table 5-4	SCX2 Agent Management Settings	5-8
Table 5-5	Date and Time Settings Menu.	5-9
Table 5-6	IP Address and IP Settings	5-10
Table 5-7	IP Routing Table, Change Existing Entry	5-11
Table 5-8	IP Routing Table, New Entry.	5-11
Table 5-9	SNMP System Group Settings	5-13
Table 5-10	SNMP Access Settings.	5-14
Table 5-11	IP Trap Receiver Table Change	5-15
Table 5-12	Trap Receiver Table	5-15
Table 5-13	Login User Access Settings	5-16
Table 5-14	Event History Navigation Options	5-17
Table 5-15	SCX2 Agent Maintenance.	5-18
Table 5-16	Flash File Manager Command Line	5-22
Table 5-17	SCX2 Agent Login Password	5-24
Table 5-19	Fan Status and Fan Adjustment	5-34
Table 5-18	Power Supply Status and Value	5-34
Table 5-20	Temperature Display and Alarm Setup	5-35
Table 5-21	Update and System Boot	5-38
Table 6-1	axg2.mib Objects	6-5
Table 6-2	axg2-agent.mib Objects	6-6
Table 6-3	axg2-scx-as.mib Objects.	6-9
Table 6-4	axg2-Chassis.mib Objects	6-10
Table 6-5	axg2-Chassis.mib Traps	6-11

Table 6-6	axg2-scx-cs.mib Objects.	6-11
Table 6-7	axg2-scx-cs.mib Traps	6-13
Table 6-8	axg2-device.mib Objects.	6-13
Table 6-9	axg2-Device.mib Traps	6-15
Table 6-10	axg2-scx-ds.mib Objects.	6-16
Table 6-11	axg2-scx-ds.mib Traps	6-18
Table A-1	SCX2 Technical Data	A-1
Table A-2	Technical Data of the SCX2 Ethernet Ports	A-1
Table A-3	Technical Data of the SCX2 Serial Interface	A-2
Table A-4	Technical Data of the SCX2 Ethernet/IP Management Access	A-2
Table A-5	Environmental conditions	A-2
Table A-6	Real Time Clock	A-3

Chapter 0

Safety, Instructions, Statements

Safety Precautions

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

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

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

NOTE: Before installing the device find out if any local technical rules must be observed. These may be defined by ANSI, ITU, 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.
- Attach a wrist strap and follow ESD procedures, see next paragraph.

Preventing Damage From Electrostatic Discharge



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

Card Protection

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

Grounding Procedure

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

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

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

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

- Set down cards with their component sides face up.

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

Technical Instructions to User

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

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

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

Inspection

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

Commissioning

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

Cleaning



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

Table 0-1 Effects of Cleaning Liquids

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

Quality

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



This product is manufactured to the arcutronix GmbH quality standards.

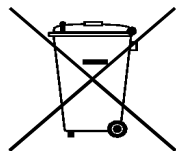
Repair

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 handled over to the applicable collection point for the recycling of electronic equipment.



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

CE Conformity



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

Electromagnetic Immunity Statement

This equipment has been tested and found to comply with the limits of EN 50082-2 (Electromagnetic Immunity for heavy industry).

Instructions to User

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

Electromagnetic Emissions Statements

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



WARNING: This is a Class A product. In a domestic environment, this product may cause interference in which case the user may be required to take adequate measure. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

United States Federal Communications Commission (FCC) Electromagnetic Emissions Statement

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

Canadian Department of Communications (DOC) Statement

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

European Communities

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

Chapter 1 Introduction

SCX2 Description

General

The System Controller SCX2 is used to control and configure all types of arcutronix connectivity devices. The SCX2 allows the administrator to control and monitor more than 250 local and corresponding remote devices via one single access point.

The System Controller provides access by using SNMP, Web-GUI, Telnet and local control terminal (e.g. VT100).



Figure 1-1 SCX2 10-slot Chassis SRX10

Web-GUI or local management (menu driven VT100 Terminal) assist a user friendly field installation and configuration. For SNMP management, several standard and product specific MIB files (Management Information Base) are provided.

SNMP management can be interconnected to any SNMP-compatible management software such as [HP Open View](#) and SNMPC ([Castle Rock](#)).

Remote SW-upload for SCX2 and each other component in the system rack is realized via FTP. After copying SW updates to SCX2 Flash File System updated files are loaded into agent and plugged modules during boot-up or on administrator request.

The in-band management capability, in combination with the System Controller SCX2 allow Carriers and ISPs to maintain and supervise all devices inside management system via single NMS access point (IP forwarding). Trap signaling helps to detect errors in case of any failure or status change at the local or remote site.

SCX2 Functions at a Glance

The SCX2 main agent allows the management of one main chassis and up to eight expansion chassis equipped with rack mounted line-cards (LCs) ¹. It provides access by using a control terminal (RS232 port) or any kind of management platform using SNMP, Telnet or a web-browser (10/100BaseTx port). The chassis and the installed rack mount cards can be monitored and configured locally and remotely.

The SCX2 control processor communicates with the arcutronix Multi Service System and installed rack mount cards and allows the following management features:

- Central management access device for system racks (SRX family)
- Up to 24 rack cards can be managed and supervised per system rack
 - Auto-detection of equipped cards
- Remote SW-upload for each component in a system rack via FTP
- Flash File System, for saving new and old SW files of all plugged cards
- Various management access options: SNMP, Web-GUI, Telnet, VT100
- Power and Fan control functionality
- SNMP trap-signalling in case of local or remote status changes
- Discovery of system rack types
- Acoustic alarm
- Alarm relay - Enhanced alarm threshold selectable in addition to autonomous alarm function via alarm relay contacts on fan module
- IP-forwarding, to afford IP management of all SCX2 cards in a network
- Compact 3RU rack card
- Power supply via system racks (SRX)

Alarm Conditions

Alarm conditions can be detected depending on the settings made in the control software. Each SCX2 card monitors all power supplies and rack mount cards of the chassis and the fan's function. If there is a failure recognized by an SCX2 card, an alarm will be set by the agent.

An acoustic alarm and additionally an alarm contact are used to execute an initiated alarm. The alarm contact is a part of the alarm output card or the fan module.

IP-Port

A RJ-45 Ethernet-Port is used to get IP-communication with the device and enable IP-based communication. The IP-address has to be configured before usage.

1. A special extension management card is required for this.

VT100-Port

A serial port is available on the front side of the unit to get RS232 communication. Either from a local PC with RS-232 I/F or via modem-link, the communication can be started.

If modem communication is used, the SCX2 supports SLIP and/or PPP to allow remote IP-based access via the modem.

SLIP

The Serial Line Internet Protocol (SLIP) is a mostly obsolete encapsulation of the Internet Protocol designed to work over serial ports and modem connections. It is documented in RFC 1055. On PCs, SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which is better engineered, has more features and does not require its IP address configuration to be set before it is established. On micro-controllers, however, SLIP is still the preferred way of encapsulating IP packets due to its very small overhead.

SLIP modifies a standard Internet datagram by appending a special "SLIP END" character to it, which allows datagrams to be distinguished as separate. SLIP requires a port configuration of 8 data bits, no parity, and either EIA hardware flow control, or CLOCAL mode (3-wire null-modem) UART operation settings.

SLIP does not provide error detection, being reliant on other higher-layer protocols for this. Therefore SLIP on its own is not satisfactory over a particularly error-prone dial-up connection. It is however still useful for testing OS' real-time capabilities under load (by looking at flood-ping statistics).

PPP

In networking, the Point-to-Point Protocol, or PPP, is a data link protocol commonly used to establish a direct connection between two networking nodes. It can provide connection authentication and can also provide transmission encryption privacy and compression.

PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, or fiber optic links such as SONET. Most Internet service providers (ISPs) use PPP for customer dial-up access to the Internet. Two encapsulated forms of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used by ISPs to connect Digital Subscriber Line (DSL) Internet service.

PPP is commonly used to act as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older, non-standard Serial Line Internet Protocol (SLIP), and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), Novell's Internetwork Packet Exchange (IPX), NBF and AppleTalk.

PPP is specified in RFC 1661.

Order Information

For the time being, the SCX2 is the sole member of SCX - System Controller family.

Table 1-1 Order Matrix

Art.- No.	Short Name	Description
0805-7020	SCX2	System Controller for connectivity system devices: <ul style="list-style-type: none">• SNMP• Web-GUI• Telnet• Terminal Management;• 3RU rack mount card.

Accessories

Housings and Cables

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

Table 1-2 Accessories Housings & Cables

Art.- No.	Short Name	Description
0805-9000	SRX10	Rack mount shelf: <ul style="list-style-type: none">• 19" chassis• Height: 3RU• 10 slots for line-cards• 1 slot for management• 2 slots for modular AC (115/230V) and/or DC (-48V) power supplies
0805-9500	SRX24	Rack mount shelf: <ul style="list-style-type: none">• 19" high density chassis• Height: 6RU• 24 slots for line-cards• 1 slot for management• 2 slots for modular AC (115/230V) and/or DC (-48V) power supplies
0717-9001	SHX3-7W	Stand-alone housing: <ul style="list-style-type: none">• 1 slot for 3RU line-card• VT100 Management port (D-Sub9)• Alarm contact• integrated wide range power supply; mains supply: 48VDC...110/230VAC

Table 1-2 *Accessories Housings & Cables*

Art.- No.	Short Name	Description
0500-001	PC-E	Power cord, European plug.
0500-002	PC-B	Power cord, Great Britain plug.
9500-0100	DCX-RJ45-D B9F	Digital Cable: RJ45 to D-Sub9 female; used for VT100-Management via an RS232 (RJ45 conn.) interface.

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

Chapter 2

Getting Started

For the startup of the SCX2 please follow the directions in this chapter. You must keep the operating conditions specified for the devices. In the following read about the startup preparation, the startup itself, and the possibility to automate the startup.



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:

- An SCX2 system
- optional: Digital Cable “RJ45 to D-Sub9 female” (9500-0100)

Preparing the Startup

Before you switch on the device you need to check the operating conditions and install the SCX2 into the chassis or the single-slot housing.

Operating Conditions

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

Ambient Conditions

The ambient conditions, which must be maintained for the SCX2, are shown in table 2-1.

Table 2-1 Ambient Conditions

Operating Temperature	5°C to 40°C
Max. Relative Humidity (non-condensing)	85% (30°C)

Table 2-1 Ambient Conditions

Input Voltage	+5V DC
Power Consumption	< 7 VA ⁱ

i. Depends on the given variant.

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.

SCX2 Mounting

To mount the SCX2 into the chassis please follow the subsequent step-by-step instructions.

1. Disconnect all cables from the SCX2 before mounting the device.
2. Place the SCX2 right way up on a table with the front panel looking in your direction.
3. Insert the SCX2 that way into the chassis as shown below. Use slot with the rail number 63!

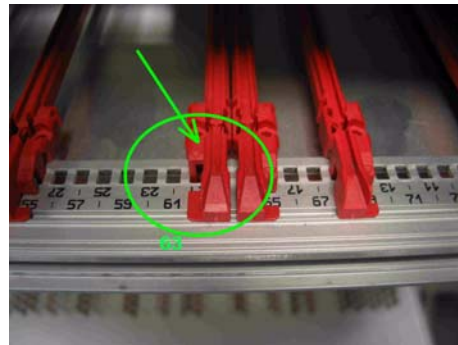
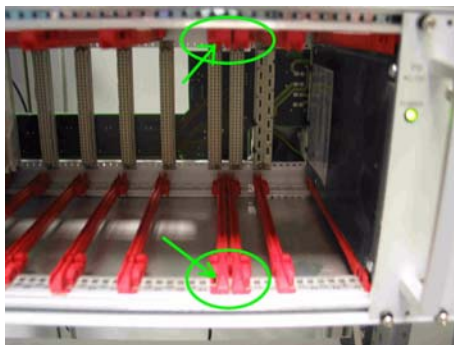


Figure 2-1 Slot for SCX2 in rail 63

4. Mount the SCX2 to the chassis using the provided screws.
5. Connect the interface cables to the SCX2.

Startup of the SCX2

Switching on the Device

Switching on the SCX2, please observe the following instructions:

1. Connect the mains cable to the chassis or single-slot housing containing the SCX2.
2. Plug the mains plug of the mains cable in a Home Office socket.

Configuration Methods

All configuration settings are made by using the management user I/F. For the system configuration you can choose one of the following configuration methods:

1. Local agent: To set up a connection to the system login using the telnet/SSH2 protocol or connect a serial terminal to the outband interface. A login screen will be presented to provide access to the local agent menus (Chapter 5, Control Software SCX2).
2. SNMP agent: You can use the SNMP protocol to manage the SCX2 (Chapter 6, SNMP and MIBs).
3. Web-based GUI. Connect with a standard internet browser (e.g. Firefox) to the IP-management I/F. A html-based GUI will allow easy configuration settings.

NOTE: There is no default (factory) IP-address given for the SCX2. The IP-address must be entered via the serial port during installation of the unit.



NOTE: You have to store any changes of configuration. Please see chap Chapter 5, **Save Agent Config to Flash**, on page page 5-19 for details.



NOTE: The TCP/IP-Port is wired like a PC in DTE pinning. Please use X-over cable, for direct link between PC and SCX2.

Chapter 3

Hardware

This chapter provides information on the main agent (SCX2) of the arcutronix Multi Service System with all the function indicators and external interfaces.

The SCX2 is a compact unit. All external connection points are accessible on the front panel. The indicator elements are also on the front panel.

Main Board

The SCX2 is a pure management card, which offers only management interfaces and connectors for optional chassis-chain.

LEDs and push-button for alarm-acknowledgement are presented on the front-side.

The SCX2 is build as a sandwich, composed of two PCBs.

SCX2 Front Panel

The SCX2 series offers on the front side the connectors for user and line interfaces plus a number of LEDs to show status of unit and interfaces.

Indicators & Connectors

Table 3-1 provides information on the connectors, indicators, and controls of the SCX2 main agent.

Table 3-1 SCX2 Front View: Connectors, Indicators, and Controls

Main Agent SCX2	Item	LED	Function	Normal Operation
	Control Port (RJ45)	-	Serial I/F for VT100 operation (RS-232D)	56700, 8, N, 1
	10/100BaseTx (RJ45)	-	Ethernet management I/F (DTE pinning)	IEEE Ethernet, auto-negotiation
	LED '100'	Green	100BaseTX transmission speed active. The interface works as 100BaseTX link.	Speed dependent
	LED 'LINK'	Green	10/100BaseTx link established at the Ethernet port	On, if a device is connected
	ACK	-	Alarm acknowledge key Pushing this button resets the acoustic alarm	N/A
	ALARM	Red	Indicates that an error has been detected.	Off
	WARNING	Yellow	Warning, malfunction is detected.	Off
	OK	Green	Normal operation.	On
	BUS 2	-	receptacle port #2 Management chain 2 to SCX2	Downstream to the sub chassis chain 2
	DOWNSTREAM 1	Green	Downstream receptacle port #1 enabled	On
	OVERCURRENT (upper)	Red	Overcurrent receptacle port #1 ⁱ Remove short cut or devices from bus 1	Off
	BUS 1	-	receptacle port #1 Management chain 1 to SCX2	Downstream to the sub chassis chain 1
	DOWNSTREAM 2	Green	Downstream receptacle port #2 enabled	On
	OVERCURRENT (lower)	Red	Overcurrent receptacle port #2 ⁱ Remove short cut or devices from bus 2.	Off

i. A potentially short circuit or a too high current will be indicated.

The SCX2 features several LEDs as indicators. The color of the LED indicator can help you to determine if there is a problem. Table 3-2 provides the meanings for the indicator colors.

Table 3-2 Indicator Color Meanings

Color	Meaning
Green	Signal level detection, mode display.
Yellow	Warnings that indicate unusual operation modes, loop, laser activity, etc.
Red	Indicates that errors and/or malfunctions have occurred.

Local IP-Management Interface

A separate RJ-45 jack on the front panel is foreseen to provide the local management access via a 10/100BaseTx port. CLI and SNMP are supported as user clients. You will find more configuration information in the section “Local Ethernet Interface” on page 5-1. The factory default IP address for initial configuration access is published in “TCP/IP Address and Settings” on page 5-10. The pin assignment is as follows:

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

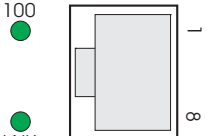
100	
LNK	

Figure 3-1 Pin Assignment of the Ethernet-Port Connector (RJ-45), DTE

- The green LED (top, ‘100’) indicates a 100BaseT link.
- The green LED (bottom, ‘LNK’) indicates, when the link is established and packets are transferred.



NOTE: The TCP/IP-Port is wired like a PC in DTE pinning. Please use X-over cable, for direct link between PC and SCX2.

RS232 Control Port Connector

The SCX2 card’s serial interface (RS232: 57600 or 9600 baud, 8 data bit, no parity, one stop bit) allows operator access via VT100 terminal emulation, to configure and monitor the local and remote rack mount cards. This information is displayed throughout various

menus. Status changes are detected and commands are transmitted to the cards and modules. Figure 3-2 provides the pin assignment of the control port connector.

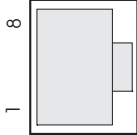
RJ45, Jack	Pin	Signal	Direction	Connect with DB9 on PC (DTE)
	1	DTR	Input	Pin4
	2	-	not connected	
	3	-	not connected	
	4	GND	Power	Pin5
	5	RXD	Input	Pin3
	6	TXD	Output	Pin2
	7	CTS	Input	Pin7
	8	RTS	Output	Pin8

Figure 3-2 Pin Assignment of the Control Port Connector (RJ-45)

RS232 Connection Cable

A connection cable is available to adapt the RJ-45 to a DB9 connector, if necessary. The connection cable acts as a “null modem cable” and you can connect your PC directly to the SCX2. Figure 3-3 displays the RS232 pin assignment for the serial management connection cable.

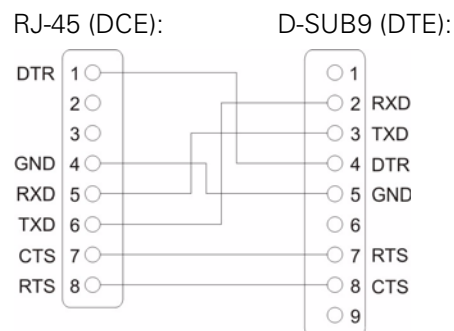


Figure 3-3 RS232 Connection cable

NOTE: The management connection cable can be ordered separately. For order information refer to Table 1-2.

Configuration of the Control Port (RJ45)

The default setting of the control port is: 57600 N 8 1. Use the DIP switch ST2 on the main board (2002.17810001.xx) to change the setting, e.g. to 9600 N 8 1.

You can also use the DIP switch ST2 to configure the SLIP/PPP operation mode.

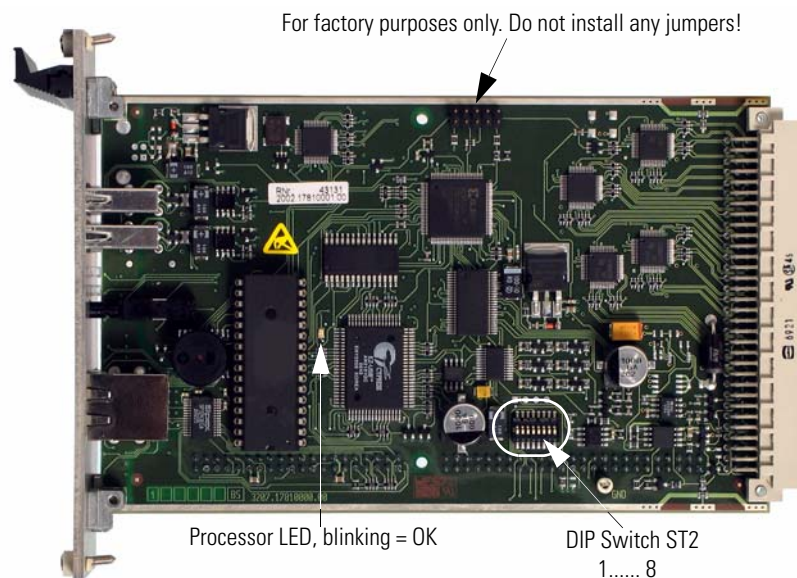


Figure 3-4 SCX2, Main Board 2002.17810001.xx

RS232 Configuration by the DIP Switch ST2

DIP switch ST2 is a 8-port switch. In factory default, all 8 switches are set to OFF:

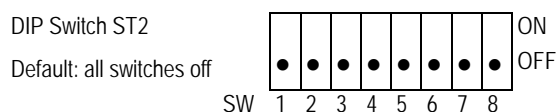


Table 3-3 gives an overview to the settings and meaning of the 8 switches.

Table 3-3 SCX2, RS232 Configuration Switch ST2, Management Operation Mode

Switch	Position	Function
SW1	Off	RS232 with 57600 bps (default setting)
	On	RS232 with 9600 bps
SW2	Off	VT100 operation at RS232 (default setting)
	On	PPP or SLIP operation at RS232
SW3	Off	PPP operation at RS232 (if SW2 = on)
	On	SLIP operation at RS232 (if SW2 = on)
SW4-SW7	Off	The setting of the DIP switches 4 to 8 is Off and must not be changed
	On	---- (no function)
SW5-SW8	Off	The control processor of the chassis boots from the EPROM or the on-board flash according to the software pre-definition
	On	The control processor of the chassis boots from the EPROM. This is an emergency function, which can be used after a failed in-system update for example.

Advanced Management Daisy Chain

Two receptacles allow to connect the SCX2 main agent to two chains of SCX2 sub-agents. Each of the downstream ports can handle up to four sub chassis.

Use USB A-B cables (DK-UAUB) to connect the DOWNSTREAM socket (connector type USB A) to the UPSTREAM socket (connector type USB B) of the sub-agent.

Table 3-4 Pin Assignment of the Management Port Connectors

Pin	Downstream Direction connector type A	Upstream Direction connector type B	Signal
1	POWER OUT	POWER IN	V__ USB-POWER
2	IN/OUT	IN/OUT	D-
3	IN/OUT	IN/OUT	D+
4	POWER GND	POWER GND	GND POWER
Shell	-	-	Shield

More SCX2 Configuration Switches

The SCX2 card consists of two boards. On the main board (2002.17810001.xx) the DIP-switch ST2 is located, which is important for serial interface usage (see Configuration of the Control Port (RJ45)). The piggy-board (566.00.03) does also host some switches.

CAUTION: These switches may not be changed! Otherwise the proper operation of the unit is not longer guaranteed! All DIP switches must remain in Off position.



Figure 3-5 SCX2, Piggy-Board 566.00.xx

Chapter 4

Installation and Test

This chapter provides the installation and removal procedures for the SCX2 rack mount cards in an arcutronix Multi Service System. It also provides hints for testing and troubleshooting.

Preparation

The installation of an arcutronix Multi Service System or a singleslot housing is described in the documentation of these parts. Care has to be taken to meet the requirements of power supply, air conditioning and proper environmental conditions.

4. Install the rack mount cards and other components.
Connect the cabling: Data cabling first, control cabling last. Do not connect any cables before the system has been mounted.
5. Configure the system.
Use a PC with VT100 emulation software at the singleslot housing's or agent card's RS-232 control port to configure the unit.

ESD Protection of Cards



CAUTION: Discharge of static electricity (ESD) can damage or degrade electronic components. Follow proper ESD procedures when working with the components of the arcutronix Multi Service System. For further information on ESD refer to the section "Preventing Damage From Electrostatic Discharge" on page 0-2.

NOTE: Always use an ESD wrist strap with a metal clip for grounding.

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.

Environmental Conditions

Environmental conditions must be met. The air condition must be capable of keeping the temperature inside the allowed ranges. Observe that the allowed temperature ranges during storage and operation are different. Furthermore, the air condition must keep the humidity within the allowed range. High air temperature and low system temperature can cause condensation. Condensation must be prevented under any circumstances. The maximum thermal load of the unit equals the maximum effective power dissipation of the system, as explained in the previous chapter.

Installation Hints

CAUTION: The air flow concept requires closed card slots. Always mount cover plates on empty slots to avoid local increase of temperature.

All arcutronix Multi Service System devices offer hot-swap capability and can be replaced while power is applied to the system.

Power Management

The intelligent arcutronix Multi Service System power management is a power share bus, indicating the available power which is left to feed the rack mount cards. This allows an effective utilization of the power supply capabilities.

NOTE: Read the following descriptions of the arcutronix Multi Service System power management and the management rules carefully, in order to prevent malfunctions.

Rules of the Power Management

- If the remaining power is not sufficient in the arcutronix Multi Service System, a rack card, e.g. agent or modem card, will not power up.
- The decision whether a unit will be powered up or not is taken, when a new card is inserted into the chassis (SHX) or if the whole system is powered up simultaneously. Once taken, this decision will not be revised. That means, if a rack mount card has been powered up once it stays operating, even if the whole power resources are used and an additional unit with priority status is inserted. This also means that if a rack mount card was rejected, it stays rejected, even if later the whole power resources are released.
- If the whole system is powered up simultaneously, e.g. by switching on the mains power, cards with priority will be started first. Then the agent and rack mount cards will begin to analyze the remaining power separately, beginning with the agent and then starting from slot 1. **Therefore, it is mandatory to remove a card which has been rejected by the power management. After changing the power consumption in the chassis, the card may be installed successfully.**

NOTE: Violation of the rules can cause overloads in the power management. Such a failure will be indicated by an acoustic alarm (1 kHz) activated by the main agent. Furthermore, the “PS” LED of the “Alarm Out” component Installation Procedure for an SCX2 Card, RC-S Sub-Card

Field Installation of SCX2 Cards

Installation

Procedure to install an SCX2 rack mount card in the arcutronix Multi Service System:



CAUTION: Prevent electrostatic discharge. Observe the ESD procedures and precautions below when you are handling the SCX2 hardware.

NOTE: Always use an ESD wrist strap with a metal clip for grounding. Ground the ESD wrist strap to the chassis.

Tools Required: A medium head Phillips (“Crosshead”) screwdriver is required. Use screwdrivers with the correct size.

1. Unscrew the cover plate of the slot you want to use and remove the cover plate.
2. Take the SCX2 card out of the anti-static bag.
3. Insert the card into the rails of the chassis (make sure that it slides in the rails).
4. Slide it in until you feel resistance and set the card into place.
5. Using the screwdriver secure the SCX2 card’s 2 self-retaining screws.
6. Connect the cabling to the user port and the line port.

After power-on the SCX2 rack mount card initializes itself.

Removal

Procedure to remove an SCX2 rack mount card from the arcutronix Multi Service System:



CAUTION: Prevent electrostatic discharge. Observe the ESD procedures and precautions below when you are handling the SCX2 hardware.

NOTE: Always use an ESD wrist strap with a metal clip for grounding. Ground the ESD wrist strap to the chassis.

Tools Required: A medium head Phillips (“Crosshead”) screwdriver is required. Use screwdrivers with the correct size.

1. Disconnect all cables from the SCX2.
2. Using the screwdriver loosen the SCX2 card’s 2 self-retaining screws, until you can feel that the screws have left the thread.
3. Pull out the card. Place it in an anti-static bag.
4. Close the gap of the card slot with a cover plate or with a spare rack card.
5. Fasten the fixing screws.

Chapter 5

Control Software SCX2

General Information

The control software of the SCX - System Controller allows you to configure the device and all attached line-cards via one single control terminal. There are different ways to get access to the unit:

- Serial Interface (VT100, RS232)
- Ethernet / IP

NOTE: You have to store any changes of configuration. Please see chap Chapter 5, **Save Agent Config to Flash**, on page 5-19 for details.

Local RS-232 Interface

Connect it to the control port of the singleslot housing or to agent's control port. The control port (designed as DCE) is an asynchronous RS232 interface with the following parameters:

- 57600 baud
- 8 data bit
- no parity
- 1 stop bit
- no flow control

Local Ethernet Interface

For the Telnet access you have to connect the Ethernet port of the Main Agent to your network.

NOTE: First, you must configure the IP parameters, at least the IP address and the IP subnet mask via the control port to get a valid ethernet access to your agent.



NOTE: You have to store any changes of configuration. Please see chap Chapter 5, **Save Agent Config to Flash**, on page 5-19 for details.



NOTE: The TCP/IP-Port is wired like a PC in DTE pinning. Please use X-over cable, for direct link between PC and SCX2.

Start the Telnet program on your PC with the IP address of the Main Agent. The telnet program nowadays is a component of the operating system (e.g. Windows).

You get access to the agent and start at the Login screen.

Under certain circumstances, when routing the terminal signals via a network, the following may occur: Hitting the Enter key results in an endless redraw of the menu. In this case disconnect and use CTRL-J instead.

NOTE: If you get access via the singleslot housing do not press the ESC key. Pressing the ESC key deactivates the input of numbers. When this occurs press any letter key on the keyboard to regain menu control.

When set to PPP or SLIP, the control port allows Telnet sessions. Additionally, management by Telnet can be done via the remote management channels which got assigned to certain time slots of the ports by the user. The menus will be identical, independently on the access method. The User and his Password has to be entered in the start page.

NOTE: The first access after delivery must be done with a terminal at the control port, because the IP setup must be performed before Telnet sessions are possible.

Security Issues

If only a few people shall be allowed to make changes in your system, it is possible to assign different access level and passwords. Refer to "Change Login Password" on page 5-24.

Any time you connect or reconnect to the initialized SCX2 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 unit.

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: Four different access-level are selectable with different access rights:

1. Monitor (only limited view)
2. Service (limited view plus limited modify)

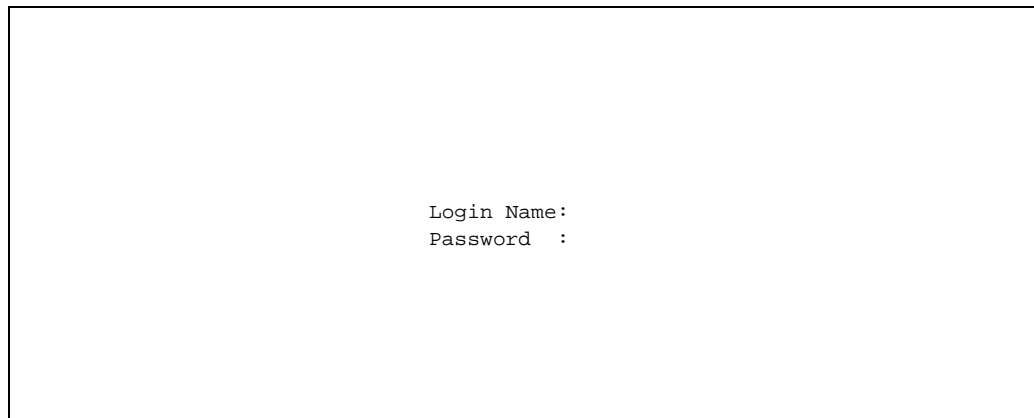
3. Standard (view and modify)
4. Admin (full access inclusive user administration)

If the device is started-up the very first time, only the user “admin” is defined. See in “Login User Access Settings” on page 5-16, how to define the other users and how to change the user password.

Login Screen

After a management connection has been established towards the SCX2 plugged in a chassis (SRX), the login screen will be displayed. The management software may be accessed by the user with different access levels. It is used to protect the access against unwanted access.

The Login screen is shown in the figure below. Please enter your Login Name and the adequate Password.



```

Login Name:
Password  :
```

This is the initial screen which is shown when a terminal gets connected. Here, you have to enter a defined user name and the corresponding password to gain access to the menu system. The bottom line displays the serial number of the agent, e.g.

```
AGENT No .xxx
```

The Login Name and the Password are set to “admin” at time of delivery. It should be changed immediately after the first login, otherwise full access to each screen is open to everybody. The entry is case sensitive. Take care to remember the exact writing of the login name and password!

If the given information has been entered correctly, the screen MAIN MENU will be displayed.

The text of **system Name** and **system Location** will be displayed in the login screen. If the login screen is not displayed, check the cabling and the terminal setup.

If cryptic text is displayed check the terminal data rate setting.

Users can be defined in the Administrator Setup menu.

The unit will fall back to this screen as soon as you leave the top level menu or disconnect the terminal or terminate the Telnet session.

CAUTION: Observe the section “Security Issues” above.

The password will not be displayed. Each character will be replaced by an asterisk (*). An error message will be displayed for any unsuccessful login. The application continues with the login screen. Depending on the access level, menu settings may not be accessible for the user.

Navigation

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

Select a menu entry

All menu lines with blue colored text, depict with italic letters in the screenshots, are accessible by the cursor². Black lines display only. Select any colored menu text of interest by cursor-up/ -down keys and press the Enter key. This will give access to the item of the line.

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

Overview to keys

Table 5-1 provides information on the menu options.

Table 5-1 Overview to key-strokes

Key	ASCII	Action	Remark
Enter (CR)	13	Selects the chosen entry.	Depending on the type of entry, different actions will happen: <ul style="list-style-type: none">• A new menu-page is opened• Open a pull-down menu and select one of the offered entries.• Enter a proper value or a string in a edit-line.
ESC	27	Leaves the current menu-page.	It make take a second after pressing the ESC key before the page is quit. To accelerate this, press 'space' after ESC. Use ESC to leave pull-down menus and/or edit-lines.
a	97	Change to the Alarm-log view.	

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

Table 5-1 Overview to key-strokes

Key	ASCII	Action	Remark
q	113	Leaves the current menu-page.	'q' can not be used to leave pull-down menus or edit-lines.
u	117	Update the current view.	
ArrowDown	258	Moves cursor down in the menu.	The cursor moves only from selectable to selectable entry. At the bottom entry of the menu, the cursor will be set to the top entry, after pressing ArrowDown.
ArrowUp	259	Moves cursor up in the menu.	The cursor moves only from selectable to selectable entry. At the top entry of the menu, the cursor will be set to the bottom entry, after pressing ArrowUp.

Display and User Actions

Values which can be read and/or changed by the user are marked with number followed by a single character. The characters distinguish the type of variable, please see table below. If you want to access the item, type the number and press the Enter key.

The meanings of the shortages are:

...	Sub-Menu
R	Read only
s	Select
t	Toggle
w	Writable

Exit

The selection 'Exit' always leads to the menu one level above.

Main Menu

After having logged into the main agent the following screen will be displayed:

```
MAIN MENU

AGENT
SYSTEM

EXIT

zzz i
```

i. This line provides a short message concerning the highlighted command.

From here, you have access to the other menus

With the text cursor chose the line, which contains the desired sub mask, and press <Enter> to select it. User with Read System access right only see **AGENT**.

Table 5-2 provides information on the menu options.

Table 5-2 SCX2 Main Menu Options

Parameter	Description	Format	Default
AGENT	all items for the agent, e.g. administration, see page 5-7.	Menu	
SYSTEM	all items for the components in the chassis, e.g. interface settings, see page 5-28.	Menu	
EXIT	Leave CLI and terminate the session.	Exit	

AGENT CONFIGURATION

Agent Configuration includes management settings like the TCP/IP address setting for SNMP access, maintenance, event monitoring and clear alarm.

AGENT CONFIGURATION
Administrator Setup
Realtime Event Monitoring
Event History
Maintenance
Clear Alarm
Change Login Password
Exit

Table 5-3 Agent Configuration

Selection	Description
Administrator Setup	Enters the menu MANAGEMENT SETTINGS for editing administrator tasks. See page 5-8
Realtime Event Monitoring	Shows the last events chronologically. Each event is fixed by date and time. See page 5-17
Event History	Scroll through the history of recent events, (no updating). See page 5-17
Maintenance	Enters the menu for maintenance tasks. See page 5-18
Clear Alarm ⁱ	Clears alarm and resets the alarm contact to off position. See page 5-24
Change Login Password ⁱⁱ	Enters the menu Change User Password for editing. See page 5-24
Exit	Leaves the menu system and terminates the session.

i. Not in the menu for users with Monitor access right.

ii. To change the password you must have the right to do this (set by the administrator in the mask Login User Access Settings).

Users with Read System access right see **system Information** and **Exit** instead of the other items in the screen AGENT CONFIGURATION.

Administrator Setup

Menu for MANAGEMENT SETTINGS by the administrator.

MANAGEMENT SETTINGS
Date and Time
TCP/IP Address and Settings
TCP/IP Routing Table
TCP/IP Address Cache (View Only)
SNMP System Information
SNMP Access Settings
SNMP Trap Receivers
Login User Access Settings
Exit

Table 5-4 SCX2 Agent Management Settings

Selection	Description
Date and Time	Enters the setup menu for date and time setup. See page 5-9
TCP/IP Address and Settings	Enters the setup menu for TCP/IP configuration. See page 5-10
TCP/IP Routing Table	Enters the setup menu for the TCP/IP routing table. See page 5-11
TCP/IP Address Cache (View Only)	Displays the current content of the ARP cache. See page 5-12
SNMP System Information	View and edit ⁱ the MIB II system group. See page 5-13
SNMP Access Settings ⁱ	View and edit the communities and trap settings. See page 5-14
SNMP Trap Receivers ⁱ	View and edit the trap receiver table. See page 5-15
Login User Access Settings ⁱ	Enters the setup menu for user administration. See page 5-16
Exit	Returns to the menu one level above.

i. Administrator only.

Date and Time

View and edit system date and time.

DATE AND TIME SETTINGS	
Current Date	12/11/2003
Current Time	14:15:01
Exit	
Back to the previous menu	

Table 5-5 *Date and Time Settings Menu*

Selection	Description
Current Date	Allows to modify the date of the system's clock, format MM/DD/YYYY.
Current time	Allows to modify the time of the system's clock, format HH:MM:SS.
Exit	Returns to the menu one level above.

TCP/IP Address and Settings

```
IP ADDRESS AND IP SETTINGS

IP SETTINGS FOR MANAGEMENT ACCESS

IP AND NETWORK ADDRESSING

IP Address          192.168.1.100
Subnet Mask         255.255.255.0

IP PERFORMANCE PARAMETERS

ARP Cache Timeout (secs)  20
Default TimeToLive (hops) 32
Reassemble Timeout (secs) 15

Exit
```

Table 5-6 IP Address and IP Settings

Selection	Description
IP Address	The IP address of the unit can be entered (decimal). This address is needed for any management access via network. Please note that global route addresses must be obtained from an Internet authority.
Subnet Mask	The appropriate subnet mask can be entered (decimal).
ARP Cache Time-out	Allows to modify the ARP response time-out (1... 255 seconds).
Default TimeToLive	Allows to modify the maximum hops value for outgoing management packets (1... 255 hops).
Reassemble Timeout	Allows to modify the IP frame reassembly time-out (1... 255 seconds) to complete a received IP frame.
Exit	Returns to the menu one level above.

NOTE: There is no default (factory) IP-address given for the SCX2. The IP-address must be entered via the serial port during installation of the unit.



NOTE: You have to store any changes of configuration. Please see chap Chapter 5, **Save Agent Config to Flash**, on page 5-19 for details.

TCP/IP Routing Table

To modify an existing route set cursor on the route to change or delete it.

IP ROUTING TABLE			
DESTINATION	ROUTE MASK	NEXT HOP	ROUTE PROTOCOL
192.168.100.1	255.255.255.0	192.168.1.1	local
(Add New Route)			
(Exit)			
Back Change Destination Change Route Mask Change Next Hop Delete Route			

Table 5-7 IP Routing Table, Change Existing Entry

Selection	Description
192.168.100.1	Allows to modify the routing entry. The selected line is displayed after pressing the enter key. Back is selected. Note: Use a sufficient large window (of terminal program) to see the selected line of the entry change screen.
Back	No change
Change Destination	Change the destination IP address of this route (a new management station).
Change Route Mask	Change the route mask of this route (the corresponding subnet mask).
Change Next Hop	Change the next hop of this route (the IP address of the router to be used).
Delete Route	Delete this route.
(Exit)	Returns to the menu one level above.

To add a new route set the cursor behind Add New Route and press the enter key. Up to 20 routes can be defined.

Table 5-8 IP Routing Table, New Entry

Selection	Description
Add New Route	Allows to generate a routing entry. The dialogue is started with the enter key: Enter new destination IP address: enter e.g. 11.22.33.44 (probably a management station) Corresponding next hop IP address: enter e.g. 11.22.1.1 (the address of the router to be used)
(Exit)	Returns to the menu one level above.

TCP/IP Address Cache (View Only)

The table displays the address cache contents (after TCP/IP actions).

INTERNAL ADDRESS RESOLUTION CACHE			
IP-ADDRESS	PHYSICAL ADDRESS	IF	TYPE
Press any key to leave ...			

SNMP System Information

This group contains the administrator information of the managed node (View and edit the MIB II system group.). The MIB II system group must be implemented for each agent.

```

SNMP SYSTEM GROUP SETTINGS

SNMP SYSTEM IDENTIFICATION

FIXED SYSTEM GROUP INFORMATION

System Description arcutronix G2 SNMP System
System ObjectID 1.3.6.1.4.1.760.2

VARIABLE SYSTEM GROUP INFORMATION

System Name      Mux #1
System Contact   Mr Manager
System Location  HQ, 1st floor
System Uptime    435759

Exit

```

User with Read System access right only see this screen.

The fixed system group information in this menu is displayed only.

System Description	Information about the device
System ObjectID	The vendor's authoritative identification of the network management subsystem contained in the entity

The variable system group information can be modified by the administrator user.

Table 5-9 *SNMP System Group Settings*

Selection	Description
System Name	Edit the system name (< 48 ASCII characters). Any name for the unit (e.g. name of the domain). This text is displayed in the start window.
System Contact	Edit the system contact (< 48 ASCII characters). Person who manages the unit.
System Location	Edit the system location (< 48 ASCII characters). Physical location of the unit. This text is displayed in the start window.
System Uptime	System uptime in 10ms units. Displays the time the unit is running since last power up in hundredth of seconds.
Exit	Returns to the menu one level above.

SNMP Access Settings

This menu allows to view and edit the communities and trap settings.

SNMP ACCESS SETTINGS	
COMMUNITY ACCESS LEVEL SETTINGS	
ACCESS LEVEL	PERMITTED WHEN COMMUNITY IS USED
Read System	public
Monitor	public
Service	public
Standard	public
Administrator	admin
OTHER SETTINGS	
Generate Authentication Traps	yes
Restrict Access to Trap Receivers	no
Exit	

Table 5-10 *SNMP Access Settings*

Selection	Description
Read System	Allows to see the system group information and nothing more.
Monitor	Allows to see all management objects, but not to change them (no set).
Service	Allows to see all management objects and set loops and BERT.
Standard	Allows to see and set all management objects, but not set the system group.
Administrator	Allows the complete administration, e.g. to modify the community to be used to perform all management tasks including the system group and user management and IP setup.
Generate Authentication Traps	Send authentication traps when access with an invalid community or a wrong IP address is restricted to trap receivers.
Restrict Access to Trap Receivers	Restrict SNMP access to members of the trap receiver list.
Exit	Returns to the menu one level above.

SNMP Trap Receivers

```

TRAP RECEIVER TABLE
TRAP RECEIVER  COMMUNITY TO USE FOR TRAPS
192.168.1.123  public
(Add New Trap Receiver)
(Exit)

Back  Change IP Address  Change Community  Delete Trap Receiver

```

To modify a trap receiver set cursor on that trap receiver to change or delete it.

Table 5-11 IP Trap Receiver Table Change

Selection	Description
192.168.1.123	Allows to change or delete the trap receiver entry. The selected line is displayed after pressing the enter key.
Back	No change
Change IP Address	Change the IP address of this trap receiver (management station).
Change Community	Change the community to be used (to access).
Delete Trap Receiver	Delete this trap receiver. Safety check by: 'Are you sure (y/n)?'
(Exit)	Returns to the menu one level above.

To add a new trap receiver set cursor behind Add New Trap Receiver. Up to 20 trap receiver can be defined.

Table 5-12 Trap Receiver Table

Selection	Description
(Add New Trap Receiver)	Allows to modify the trap receiver entry. Start the dialogue by the enter key: Enter new trap receiver IP address: Allows to enter several trap receiver entries. enter e.g. 192.168.1.123 (probably a management station) Community to use: The left most value is the trap receiver's IP address (probably a management station). The next value is the community to be sent with the trap.
<Enter>	Returns to the menu one level above back to the management settings menu.

Login User Access Settings

LOGIN NAME	ACCESS	ALTP	LAST CHANGE
admin	Administrator	Y	01/01/2003 02:47:33
operator	Monitor	N	10/14/2002 15:23:15
(Add New User)			
(Exit)			
Back Change Access Change Password Allow Password Alt. Delete User			

Table 5-13 Login User Access Settings

Selection	Description
<login name>	Allows to modify the settings for a user or to delete it. Press the enter key to see the possible operations on the screen. The meanings are explained below this table.
Add New User	Add a new user to the list. Enter the login name. Select the access level, see below.
Exit	Returns to the menu one level above.

Operations for each login name:

Back:	Do not modify anything; go back to the login name listing.
Change Access:	Change the access level. Select one of the access levels by using the 'up' or 'down' cursor:
Administrator	Complete configuration access and system critical management access topics.
Standard	Complete configuration access.
Service	Monitor access, use loops and BERT, but no permission to configure.
Monitor	Monitor access, but no permission to configure.
Read System	Displays only system relevant data.
Change Password:	Change the password the user has to type at login. Note: The default for a new user's password is the login name.
Allow Password Alt.:	Grant the user the right to modify his password. (Yes/No)
Delete User:	Delete login name from list. Safety check by: 'Are you sure (y/n)?' Note: Every user (also administrator) can be deleted. Caution: Without administrator a special password for the next login is needed!

Realtime Event Monitoring

This selection shows the stored events, < 20 lines, down to most recent events.

```

REALTIME EVENT MONITORING
01/14/2000 03:26:22 System startup
01/14/2000 03:26:39 New arcutronix Device has been attached
01/14/2000 03:26:45 MAIN MODUL: Registration successful
01/14/2000 03:26:46 Loss Of Signal
01/14/2000 03:26:46 Loss Of Frame
01/14/2000 03:26:56 New arcutronix Device has been attached
01/14/2000 03:26:59 LINE MODUL: Registration successful

```

The list will be appended on the screen as soon as new events happen. Hitting any key returns to the menu one level above.

Event History

Browse through the event history (no updating)

```

EVENT HISTORY
01/14/2000 03:26:22 System startup
01/14/2000 03:26:39 New arcutronix Device has been attached
01/14/2000 03:26:45 MAIN MODUL: Registration successful
01/14/2000 03:26:46 Loss Of Signal
01/14/2000 03:26:46 Loss Of Frame
01/14/2000 03:26:56 New arcutronix Device has been attached
01/14/2000 03:26:59 LINE MODUL: Registration successful

<<<      <<      <      EXIT      >      >>      >>>

```

Table 5-14 Event History Navigation Options

Selection	Description
<<<	Go to the first page of this listing.
<<	Scroll one page up
<	Scroll single events up
EXIT	Leave the Event History
>	Scroll single events down
>>	Scroll one page down
>>>	Go to the last page of this listing.

Maintenance

AGENT MAINTENANCE includes various maintenance functions - for authorized personnel only! It is used for Agent configuration, to save or restore configuration data.

AGENT MAINTENANCE - AUTHORIZED PERSONNEL ONLY	
	Factory Information
	Save Agent Config to Flash
	Restore Agent Config from Flash
	Update Agent Application via X/YModem
	Flash File Manager
	Reset Agent
	Reset System
	Startup History
	Exit
Leave to the main menu	

Table 5-15 SCX2 Agent Maintenance

Selection	Description
Factory Information	Shows the serial number and detailed information about the system. See page 5-19
Save Agent Config to Flash	Allows to store the present configuration as a file to the 'config' directory in the flash memory. The name can be chosen freely. But, although not mandatory, it is recommended to append the extension '.cfg'. See page 5-19
Restore Agent Config from Flash ⁱ	Restore a saved configuration from 'config' directory in the flash memory. A configuration file can be selected from a list. See page 5-20 Note: Loading a configuration file will reset the agent.
Update Agent Application via X/Y-Modem ⁱ	Allows to store a new application (operating system to be run) in the flash memory. You need a terminal program with X/YModem support. After confirmation the unit will attempt to establish the X- or YModem protocol. In case of failure a couple of retries will be performed until a final time-out will return to the menu. See page 5-20
Flash File Manager ⁱ	Enters the flash file manager menu. See page 5-22
Reset Agent ⁱ	Resets the agent to use new applications and/or restore configurations. The Agent will be rebooted without interruption of the data stream. See page 5-23
Reset System ⁱ	Allows to reset the whole system. The latest application (operating system) named 'agent*.rtb' will be loaded. See page 5-23 Note: A reset will cause a temporary interruption of the data transfer.
Startup History	Displays the history of resets and startups. See page 5-23
Exit	Returns to the menu one level above.

i. Administrator only.

Factory Information

Displays information about your SCX2.

```

                                FACTORY INFORMATION

Serial No.      :      xxxxxx

SW Version     :      1.13.000 DEBUG Apr 15 2005 10:18:54

MAC Address    :      FFFFFFFFFF

Exit

Back to the maintenance menu
```

Save Agent Config to Flash

Back up the agent configuration, store it to the 'config' directory in the flash memory.

NOTE: You have to store any changes of configuration to recall it after power down.

```

                                SAVE AGENT CONFIGURATION TO FLASH

IMPORTANT NOTES:

Only configurations whose names end up .cfg are valid.
If the configuration store is found to be corrupted at boot time, the system
will try to find a config file in the root directory.
If found any, it will load the newest one into the configuration store.

Saved configurations cannot be loaded manually into the configuration store
without rebooting the AGENT at the same time.

For renaming, moving or deleting of configuration files
please use the flash file manager.

There are 29649920 bytes file space free.
Save the current configuration now (y/n)?:
```

After confirmation with 'y' you will be asked for the file name (with extension '.cfg'):

```
Which file name shall be used for saving?: .cfg
```

Restore Agent Config from Flash

Restore the agent configuration from the 'config' directory in the flash memory. Select a configuration from this screen:

```
RESTORE AGENT CONFIGURATION FROM FLASH
IMPORTANT NOTE: Saved configurations cannot be loaded manually into
the configuration store without rebooting the AGENT at the same time!
CONFIGURATION          FILE DATE  FILE TIME
test2003.cfg           01/14/2000 05:03:06
fomux.cfg              03/20/2003 13:38:08
```

After selection of a configuration file you must confirm loading and rebooting:

```
Restore the agent configuration now (ATTENTION: This will reset the AGENT!) (y/n)?:
```

Update Agent Application via X/Y-Modem

Load new Agent application via XModem/YModem, using the serial interface. The terminal emulation software must be able to transfer files using XModem or YModem protocol. The new application (operating system to be run) is stored as file in the directory 'applicat' of the flash memory.

```
UPDATE AGENT APPLICATION VIA X/Y MODEM

IMPORTANT NOTES:

Only applications whose names begin with 'agent' and end up with '.rtb'
are startable.
Other application files must be renamed before they will be valid.
The newest application file in the root directory with a valid name
will be started at boot time.

For renaming, moving or deleting of application files
please use the flash file manager.

There are 7602176 bytes file space free.
Start getting the new application file now (y/n)?:
```


See Chapter 5, Flash File System and File Transfer on page 5-25 for the file transfer procedure.

Flash File Manager

The flash disk file manager shows the directories and files on the flash disk. The entries are generated with the naming conventions of the SCX2 main agent, but the user may create own entries additionally. Check for sufficient free space prior to any action.

```
C:\
(Leave)
service                <DIR> 01/02/2003 19:09:14
monitor                <DIR> 01/03/2003 28:13:14
applicat                <DIR> 01/04/2003 04:13:14
other                  <DIR> 01/05/2003 12:13:14
config                 <DIR> 01/06/2003 20:13:14
text                   <DIR> 01/07/2003 28:13:14
device                 <DIR> 01/08/2003 04:13:14
help                   <DIR> 01/09/2003 12:13:14
(Append new entry)

Flash size 8050688 bytes, 7602176 bytes free
```

The directories 'applicat' and 'config' include software and configuration of the agent. The directory 'device' includes the software of the modules. The directories 'service' and 'monitor' are properties of the administrator. The other directories are for special purposes and not user relevant.

To create a new directory or to load a file use (Append new entry).

Select one directory and press <enter> to see the flash file manager command line.

Flash File Manager Command Line

```
Back Rename Dir Move Dir Delete Dir Enter Dir
Flash size 8050688 bytes, 7602176 bytes free
Do not change anything
```

Table 5-16 Flash File Manager Command Line

Selection	Description
Back:	Do not change anything. Leave command menu / Go back one directory level.
Rename Dir:	Rename selected directory.
Move Dir:	Move selected directory to another location (path entry in Unix format).
Delete Dir:	Delete selected directory (directory must be empty).
Enter Dir:	Go to selected directory, enter into the directory.

Reset Agent

Reply 'y' to start Agent reboot.

```
RESET AGENT

IMPORTANT NOTES:

ATTENTION: Resetting will reboot only the AGENT
and will not cause temporary data traffic interruption!

Reset AGENT now (y/n)?:
```

Reset System

During a restart of the system the data transfer will be interrupted.

```
RESET SYSTEM

IMPORTANT NOTES:

ATTENTION: Resetting will reboot the whole system
and will cause temporary data traffic interruption!

Reset SYSTEM now (y/n)?:
```

Startup History

Display of the counter contents.

```
DISPLAY RESET HISTORY

Number of "Power Good"           starts: 152
Number of "Program Reset"        starts: 0
Number of "CPU shot down cycle"  starts: 0
Number of "Watchdog"             starts: 0
Number of "Agent resets by user" starts: 9
Number of "System resets by user" starts: 6
Number of "USB watchdog resets"  starts: 0

Press any key to continue ...
```

Clear Alarm

To clear the alarm generator select Clear Alarm in mask AGENT CONFIGURATION. This will reset the alarm contact to Off position.

Change Login Password

To change the password you must have the right to do this (set by the administrator in the mask Login User Access Settings). Select Change Login Password in mask AGENT CONFIGURATION. The dialogue allows to change the login password.³

Table 5-17 SCX2 Agent Login Password

Selection	Description
Change Login Password	Correct entry of your login name and current password is required to change the password. The new password must be entered twice to avoid typos. Note: The system administrator can allow or deny users to change their passwords.

After pressing <Enter> you will be prompted to enter the name:

```
Please enter your Login Name: _
```

and the password:

```
Please enter your Login Name: Administrator
Enter your current Password : *****

Please enter your new Password: *****
Enter your new Password again : *****
```

The last two lines allow to change the password. After the new password has been entered correctly twice you will be informed:

```
Your new Password has been saved. Your old Password is invalid now!
Press any key ...
```

You fall back to menu AGENT CONFIGURATION. The new password will be in use at the next login.

If you are logged in as an administrator, do the following to execute a firmware update:

- Save all existing firmware on the agent.
- Restart the Agent.
- Restore saved firmware to the modules.

3. The super password for a certain device with it's serial number is delivered in a closed envelope together with the device.

Flash File System and File Transfer

Agent software and module software updates normally resides on the flash (disk) store in the agent. From there the latest files are loaded into the agent or to the modules during boot-up or on request by the administrator.

The Flash File System

The flash file system is organized similar to the file system on a PC with a disk C:\ and some directories in the root. The entries (name.extension) for files or subdirectories are limited to 12 characters (8.3 notation). Directories and files follow the name convention for the Agent and all necessary entries are already installed. Full access to the flash disk (read and write) is possible via FTP after the IP-address of the Agent is set.

If you receive a software update on a PC readable medium, you must copy the files on it to the correct directories on the agent's flash disk. If there are '.bin' and '.bip' files you should load the '.bip' files, which are much shorter. The file transfer is realized by your terminal program with the protocol YModem or XModem. The YModem works much faster and transfers also the filename. Therefore YModem is the favorite protocol, if both are supported. It depends on the terminal program, how the file transfer works.

1. Start the Flash File Manager. Are there sufficient free bytes (else delete old files)?
2. Select the required directory and press the enter key.
3. Select and enter 'Enter Dir' in the command line.
4. Select and enter (Append new entry) to load the file.
5. Select and enter 'Load File' in the command line (use X/Y-Modem to load file).
6. On page 'X/Y-Modem File Load Page' select the kind of the file, i.e. 'Text File'
7. The available space is shown. Prepare loading by entering 'y'.
8. At 'Please start X/Y Mode transmission now...:' you start the transmission protocol at your terminal program. Within 1 minute you must start the file transfer, else the SCX2 main agent cancels by time-out. *In case you use Tera Term: open menu 'File - Transfer - XModem - Send' and select the new file on the distribution media. Leave the radio button on 'Checksum' and click on button 'Open'.* The file transfer starts immediately, you will be informed about proceedings in the file transfer window.
9. On success, you will see 'Reception finished with success!'. In case of XModem the name of the file has to be entered after this message. Enter the correct filename or rename the file later to the correct name. In case of YModem the file name was already transferred and now can be acknowledged or renamed.
10. Return to root directory and copy files to other directories in a similar way.

Tips for Terminal Emulation Programs

Do not activate *Send...* before you see 'Please start X/Y Mode transmission now...:'

Send Dialog Box

Enter or select the file name of the existing file to be sent.

Serial Port

Set the appropriate parameters in the [Setup] Serial port dialog box. Data must be 8 bit, and flow control must be set to hardware (CTS/RTS) or none.

Telnet Tips

If the file transfers fail, try connecting to the host with the binary option.

Binary File Transfer Option

If you want to send text files, don't select this option.

XModem

Transfers files between the PC and the host with the XModem protocol. XModem is rather slow but reliable and it transfers 128-byte packets with error detection. This allows the receiver to request retransmission of a corrupted packet. A one-second time-out during the reception of characters in the data block portion of a packet is used by XModem. The XModem option Checksum (Checksum/CRC/1K) will do it. The XModem file transfer protocol requires the communication lines to be transparent to all 8 bit characters, from \$00 to \$FF.

YModem

Transfers files between the PC and the host with the YModem protocol. YModem is a fast batch protocol, which can use 1 kilobyte packets. YModem can fall back to smaller packets when necessary. With large packets the YModem protocol transfers data up to four times faster than the XModem, i.e. transfer time for a 1 MB file is only 3:50 minutes for YModem instead of 16:30 minutes with XModem. File name and size are included in the YModem header. With YModem transferred files should preserve their exact length and file name, if this is supported by the receiving file system. File modification times may also be present in the YModem header.

The Software for the Agent

The software for the agent is stored in a file with the name 'agent***.RTB' (where *** means the release identification). To change the software in the agent the administrator must do one of:

- Load the new file with a terminal program by X/Y-Modem to the agent.
- Load the new file with a terminal program by the Flash File Manager to the agent. To load the new file with the Flash File Manager, do the following:
 - Open the directory 'applicat' by 'Enter Dir'.
 - Select (Append new entry) and 'Load File'.
 - Choose 'Application File'.

- Start loading by 'y'.
- See Chapter 5, Flash File System and File Transfer on 5-25 for the procedure.
- After the next restart the new file is in use in the agent.
- Load the new file with an FTP program into the agent directory 'applicat'.
 - The FTP program needs this entries:
 - IP-address of the agent
 - Administrator user name
 - Password for administrator
 - Binary file transfer
 - If the old software has the same filename as the new file, rename it to save the application.
 - Copy the new software file (agent***.RTB) to the directory 'applicat'.
 - After the next restart the new file will be used.

The Software for Modules

The software for modules is stored in the directory 'device' as file type *.hex, *.bin or *.bip. To update the software in a module copy the relevant file to 'device' by:

- Load the new file with a terminal program by the Flash File Manager to the agent. To load the new file with the Flash File Manager, do the following:
 - Open the directory 'device' by 'Enter Dir'.
 - Select (Append new entry) and 'Load File'.
 - Choose 'Device Load File'.
 - Start loading by 'y'.
 - See Chapter 5, Flash File System and File Transfer on 5-25 for the procedure.
 - The new file (e.g. 58810A12.BIN) is now in the directory 'device'.
- Load the new file with an FTP program into the modules directory 'device'.
 - The FTP program needs this entries:
 - IP-address of the agent
 - Administrator user name
 - Password for administrator
 - Binary file transfer
 - Copy the new software file (e.g. 58810A12.BIN) to the directory 'device'.
 - Leave this menu and continue the software update via the menu 'Software Update Modules' on the window 'Management Modules Page' in the Modules - tree. You must be logged in as administrator.

SYSTEM

The SYSTEM menu is intended to manage the setup of all local rack mount cards in a arcutronix Multi Service System via a terminal at the SCX2 main agent. It includes all installed chassis (racks).

```
SYSTEM
System Components
RACK 1
RACK 2

Exit

Back to higher Menu
```

Choose with the text cursor the line, which contains the desired sub mask, and press <Enter> to select it. Exit returns to the menu one level above. 'System Components' is the headline for the following list of chassis in the arcutronix Multi Service System.

The RACK 1 menu is similar to all other chassis menus and published in the following articles of this chapter.

RACK 1

The RACK 1 menu is similar to other RACK x menus and looks like:

```
SYSTEM
RACK 1
CSX4 ON SLOT 1
CSX4 ON SLOT 2
CFX2 ON SLOT 3
CFX2 ON SLOT 4
CEX2 ON SLOT 11
CEX2 ON SLOT 6
MANAGEMENT MODULE ON SLOT 11

Exit

Back to higher Menu
```

All manageable rack mount cards of RACK 1 are detected and displayed with their slot position. The rack control module has been detected in the example above in slot #5. Move the text cursor to the line, which contains the desired sub mask, and press <Enter> to select it. 'Exit' returns to the menu one level above. To manage the chassis and display information move the text cursor to the line 'MANAGEMENT MODULE ON SLOT 11', which contains the rack control module sub mask, and press <Enter> to open it.

Setup of SCX2s

To enter the setup menu for a rack mount card in the chassis move the cursor to the line of the rack mount card and press <Enter>. Please refer to the rack mount card's documentation for details of their control software.

MANAGEMENT MODULE ON SLOT x

The rack control module sub mask MANAGEMENT MODULE ON SLOT x allows access to various displays of information and is used to manage the chassis.

```
SYSTEM : RACK 1
MANAGEMENT MODULE ON SLOT 11

GENERAL INFORMATION
SELF TEST
RUN TIME
POWER SUPPLY
FANS
TEMPERATURE
TRAPS & ALARMS
Alarm Status          off
UPDATE

Exit

Back to higher Menu
```

Move the text cursor to the line and press the enter key to open and read the item. The screens are explained in the following paragraphs. The Alarm Status informs with “on” or “off” about the alarm LED.

GENERAL INFORMATION

This sub mask shows the SCX2 main agent details and consists of two screens. The first screen displays the SCX2 main agent serial number and the software revision.

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                GENERAL INFORMATION

Name                            MANAGEMENT MODULE
User Name                       ADMIN definable text
Device Description              USB Management Module
Equipment Variant               SCX2
Serial Number                   xxxxxx
Software Revision               1781009A01 (14.02.2008)
Article Number                  0805-7020
Article Release                 01
Order Information               SCX2
Manufacturer                     arcutronix GmbH
Rack Article Number             0805-9000
Rack Order Information          SRX10

Exit

Back to higher Menu
```

A user name up to 31 characters can be entered in this mask. Other information is factory-defined.

SELF TEST

In the sub mask Self Test you see status and result (never-started/wait-for-start/running/pass/failed) of the different tests, once they are started (set Test Action start/stop).

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                SELF TEST

RAM Test                        pass
ROM Test                        pass
FLASH Test                      pass
Test Action                     start

Exit

Back to higher Menu
```

RUN TIME

You see how long (in 'hours:minutes') the chassis and the fan modules have been running in the sub mask Run Time.

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                RUN TIME

Device Run Time                 000059:53
Fan 1 Run Time                  000001:43
Fan 2 Run Time                  000001:43

Exit

Back to higher Menu
```

POWER SUPPLY

The first part of the screen POWER SUPPLY shows the status of the power supplies.

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                POWER SUPPLY

Power Supply 1 Type              DC 12V
Power Supply 1 Status            ok
Power Supply 1 Value             5.40 V
Power Supply 2 Type              AC 230
Power Supply 2 Status            ok
Power Supply 2 Value             -5.38 V
Power Supply 4 Type
Power Supply 4 Status            not-plugged

Exit      Next

Show next page of this menu
```

The second screen of POWER SUPPLY looks like:

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                POWER SUPPLY

Power Supply 4 Value             0.00 V
Power Supply 5 Type
Power Supply 5 Status            not-plugged
Power Supply 5 Value             0.00 V

Exit      Previous

Back to higher Menu
```

Table 5-18 Power Supply Status and Value

Item	Status	Description
Power Supply x Status	ok	Power supply is working
	not-plugged	No power supply is inserted
	failed	Power supply is inserted but not correctly working
Power Supply x Value	5.xx V	Power supply is working and wired for positive polarity
	0.00 V	No power supply is inserted
	-5.xx V	Power supply is working and wired for negative polarity

FANS

In the sub mask FANS the status of the fans is displayed and you can make adjustments.

```

SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                FANS

Fan 1 Status                      ok
Fan 1 Speed                       2812
Fan 2 Status                      ok
Fan 2 Speed                       2876
Fan MinSpeed                      800

Exit

Back to higher Menu

```

Table 5-19 Fan Status and Fan Adjustment

Item	Selection	Description
Fan 1 Speed, Fan 2 Speed	display only	Shows the RPM speed of fan 1 or 2
Fan 1 Status, Fan 2 Status,	display only	Shows the status (not-plugged/underrun/ok) of fan 1 or 2
Fan 3 Speed	display only 0 ... 4000	Shows the RPM speed of Fan 3 (Rear-Fan-Module)
Fan 4 Speed	display only 0 ... 4000	Shows the RPM speed of Fan 4 (Rear-Fan-Module)
Fan MinSpeed ⁱ	500... 5000	Adjust of the minimum RPM speed of the fans

Table 5-19 Fan Status and Fan Adjustment

Item	Selection	Description
Fan MinSpeed Trap enable ⁱⁱ	disable, enable	Enable/disable the Trap when Speed of one fan sinks below the minimum RPM Speed.
Fan MinSpeed Alarm	disable, enable	Enable/disable the alarm when speed of one fan sinks below the minimum RPM speed.

i. The Fan MinSpeed factory set value is 1000

ii. The selection factory set value is disable

TEMPERATURE

The sub mask TEMPERATURE shows the temperature inside the device. You may configure the system to generate alarms in case of temperature over range.

```

SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                TEMPERATURE

Temperature SCX Card                43

Temperature Fan Module

Status                               ok

MinTemp                             5

MaxTemp                             50

Exit

Back to higher Menu

```

Table 5-20 Temperature Display and Alarm Setup

Item	Selection	Description
Temperature	-55 ... 125	Display of the temperature in °C within the device
Status	display only	(underrun/overrun/ok)
MinTemp ⁱ	0.. 5.. 20	Adjust the min. approved temperature in °C
MinTemp Trap enable ⁱⁱ	disable, enable	Enable/disable trap on a min. temperature condition
MinTemp Alarm	disable, enable	Enable/disable alarm on a min. temperature condition
MaxTemp ⁱⁱⁱ	30.. 60.. 70	Adjust the max. approved temperature in °C

Table 5-20 Temperature Display and Alarm Setup

Item	Selection	Description
MaxTemp Trap enable ⁱⁱ	disable, enable	Enable/disable trap on a max. temperature condition
MaxTemp Alarm	disable, enable	Enable/disable alarm on a max. temperature condition

i. Default value is 5

ii. The selection factory set value is disable

iii. Default value is 60

TRAPS & ALARMS

In this sub mask you can change (enabled/disabled) the settings for TRAPS & ALARMS.

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

                                TRAPS & ALARMS

MinTemp Alarm                    enabled
MaxTemp Alarm                    enabled
Power Fail Alarm                 enabled
Fan MinSpeed Alarm              enabled
MinTemp Trap                    disabled
MaxTemp Trap                    disabled
Power Fail Trap                 disabled
Fan MinSpeed Trap               disabled

Exit

Back to higher Menu
```


UPDATE

With the UPDATE mask the user ADMIN has the possibility to install software updates.

```
SYSTEM : RACK 1
MANAGEMENT MODULE ON SLOT 11

UPDATE

Exit      Previous
UPDATE
```

The sub mask UPDATE shows the boot selection and the software revision in the device. You may update the software and change the boot system.

```
SYSTEM : RACK 1 : MANAGEMENT MODULE ON SLOT 11

UPDATE

ReBoot is necessary      yes
Software Revision        58810A05 (1.03.2008)
Software Update
ReBoot                   no reboot

Exit
Back to higher Menu
```

Table 5-21 Update and System Boot

Item	Selection	Description
ReBoot is Necessary	display only	
	yes	Program from soldered flash runs => Execute a reboot to update.
	no	Program from plugged flash runs => Reboot not necessary to update.
Software Revision	display only	Latest software version, not inaccessibly the version, that is displayed in GENERAL INFORMATION.
Fan MinSpeed Trap enable ⁱ	disable, enable	Enable/disable the Trap when Speed of one fan sinks below the minimum RPM Speed.
Software Update	-	Start update, use the latest uploaded flash file with name 58810Axx.xxx (see "Maintenance" on page 5-18).
ReBoot	no reboot	No reboot will be executed.
	reboot from base flash	Reboot will be executed with program in the plugged flash.
	normal reboot	A normal reboot will be executed.
Fan 3 Speed	display only 0 ... 4000	Shows the RPM speed of Fan 3 (Rear-Fan-Module)
Fan 4 Speed	display only 0 ... 4000	Shows the RPM speed of Fan 4 (Rear-Fan-Module)

i. The selection factory set value is disable

Software Update

If you start a Software Update, the display will be: .

```

UPLOAD MODULES SOFTWARE PAGE - Software Update

Searching in directory C:\device
for the newest file starting with 58810A
and ending with: .hex .bin .bip

The newest File is: 58810A01.bip

Do you want to continue? (y/n):

```

If you want to load a new software, which is newer as indicated in the above screen, you may enter y. The load procedure may not be interrupted by a power-fail.

When the software update was successful, this screen is displayed:

```
UPLOAD MODULES SOFTWARE PAGE - Software Update

Update file: C:\device\58810A01.bip
Module has started the update process. Please wait.
Module is updating. Please wait.      Transferred bytes:   162490   100%
Module is processing the file. Please wait (ca. 40 sec).
Module is booting to complete update. Please wait.
Update succeed, To check that runs the updated software, see software revision.

                                Exit

Back to the higher Menu
```

Else you will get an error message, and the old software is still used.

Chapter 6

SNMP and MIBs

This chapter provides information on the SNMP and the management information bases (MIBs) used by the SCX2.

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: SNMPv1 (version 1) and SNMPv2c (version2, community-based).

SNMPv1

SNMPv1 first appeared in 1988 and is defined in IETF RFC1065, RFC1066 and RFC1067. It supports a basic set of commands (get, set and the possibility to send traps). Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in clear text.

SNMPv2c

Community-Based Simple Network Management Protocol version 2, or SNMP v2c, is defined in IETF RFC 1901-RFC1908. SNMP v2c revises version 1 and includes improvements in the areas of performance, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. SNMPv2c uses the same simple community-based security scheme as SNMP v1. While officially only a "Draft Standard", this is widely considered the de facto SNMP v2 standard.

Traps

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

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

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

Installation Prerequisites

This section provides the installation prerequisites for SNMP.

Prerequisites for SNMP management:

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

Preparing the SNMP Management System

Before managing the SCX2 by SNMP, one has to prepare the SNMP management system. First install the MIBs for the SCX2 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 recompile 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 an SNMP device or to retrieve operational data from the device. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. This model permits management across all layers of the OSI reference model.

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

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

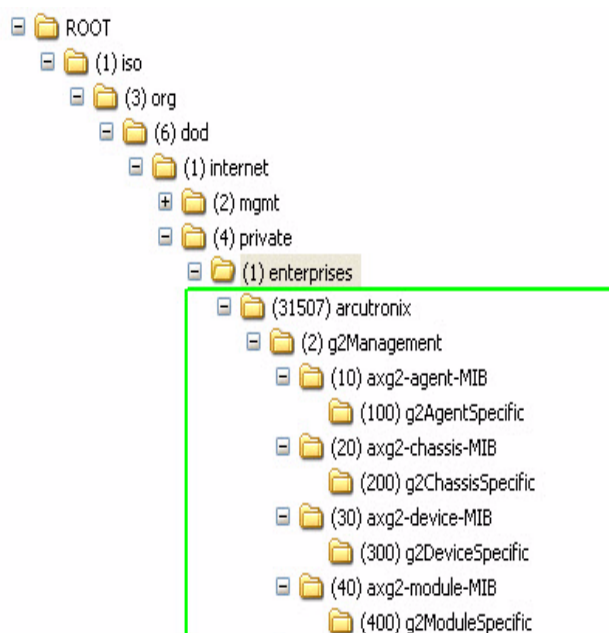


Figure 6-1 The SNMP Generation 2 MIB Tree

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

The global MIB sections contain variables which should be served by any SNMP agent. Each MIB object is assigned a name. These names are shown in the following MIB explanation. However, these names may show up somewhat extended or abbreviated on your screen, depending on the network management software you use. This is no malfunction but a feature of your software.

The following MIB explanations will provide a quick overview about the available features. However, you might find useful additional information when inspecting the MIBs themselves. The root ID includes the full path, i.e. a device-specific MIB for a rack mount card is based on: "arcutronix.g2Management.axg2-device-MIB.g2DeviceSpecific".

MIB imports for tables and traps: RFC1155-SMI, RFC1213-MIB, RFC-1212, RFC-1215. Trap numbers are derived from the main group, the MIB's OID and the trap sequence.

The MIB tables in this appendix contain the following information:

- MIB Name, or name of the MIB object
- Object Type of MIB:
 - group name = Group of variables or tables
 - table name = Table of MIB variables
 - table entry = Single MIB variable or index in a table
 - Variable type string or integer, rw = readable and writable

- /MIB-ID/ Description of the MIB object, variable contents
(ID notation: replace // by subsequent ID; /ID // is a sub tree of previous ID, followed by further IDs.)

SCX2 MIB List

The SCX2 MIB list provides access to the management variables, specific for the Multi Access Connectivity Systems. The g2Management MIB tables for SCX2 (next paragraphs) describes the chassis and devices and the traps for each module.

SCX2 MIBs are collected in files (tables) for the same number group (e.g. 760 2 10 //, where // is replaced by the next MIB-ID numbers). MIB lists and their traps for agent and chassis are explained in one of the next chapters. MIB lists and their traps for rack mount cards are in the user guide of the card. SCX2 MIBs are: axg2.mib, axg2-agent.mib, axg2-chassis.mib, axg2-cmg-ds.mib, axg2-device.mib, axg2-scx-as.mib, axg2-scx-cs.mib, axg2-scx-ds.mib.

axg2 MIB

The axg2.mib is explained in the Table 6-1. This MIB {arcutronix 2} specifies the general OIDs for arcutronix's g2Management.

Table 6-1 axg2.mib Objects

MIB Name	Object Type	Description
axg2	mib name	760 2 // arcutronix-axG2-MIB for g2Management.
axg2-agent-MIB		/10// {g2Management 10}
g2AgentSpecific		/100// Group of MIBs which contain informations about specific features of an agent. {axg2-agent-MIB 100}
axg2-chassis-MIB		/20// {g2Management 20}
g2ChassisSpecific		/200// Group of MIBs which contain informations about specific features of an unit. {axg2-chassis-MIB 200}
axg2-device-MIB		/30// {g2Management 30}
g2DeviceSpecific		/300// Group of MIBs which contain informations about specific features of an unit. {axg2-device-MIB 300}
chassispsTable	table name	Table with information about the power supply in the chassis.
chassispsEntry	table entry	The index of the table.
chassispsChassis		The index of the chassis.
chassispsPSIndex		The power supply index.
chassispsPSType		The textual description.
chassispsPSStatus		The status of the power supply.

Table 6-1 *axg2.mib Objects (continued)*

MIB Name	Object Type	Description
chassispsVoltageOutput		The voltage output of the power supply.
chassispsMinAllowedVoltage		This min allowed voltage of the power supply.
chassispsMaxAllowedVoltage		This max allowed voltage of the power supply.
chassispsAlarmEnabled		This enables or disables ALARMS of the power supply.
chassispsTrapEnabled		This enables or disables TRAPs of the power supply.

axg2-agent MIB

The axg2-agent.mib is explained in the Table 6-2. This MIB {g2Management 10} describes all (snmp-manageable entities) agents from arcutronix designed for the g2Management and is mandatory for those devices. For specific features of an agent see AgentSpecific-MIB {axg2-agent-MIB 100}.

Table 6-2 *axg2-agent.mib Objects*

MIB Name	Object Type	Description
axg2-agent	mib name	760 2 10 // THE axG2-AGENT MIB
agentSpeccificationGroup	group name	/1// AGENT SPECIFICATION GROUP
agentSerialNumber		1/ The serial number of the agent.
agentOrderInfo		2/ The order information of the agent.
agentArticleRev		3/ The article revision of the agent.
agentSoftwareRev		4/ The software revision of the agent.
agentHardwareRev		5/ Hardware revision of the agent.
agentMAC_Address		6/ The MAC Address of the agent.
agentGeneralConfigGroup	group name	/2// AGENT CONFIGURATION GROUP
agentAlarmStatus	rw	1/ This indicates the current status of the alarm generator. If an alarm is active, it can be reset here. If desired, the alarm can also be activated from here by writing 'active' to this object. INTEGER {active (1), inactive (2)}
agentSystemDate	rw	2/ This indicates the current system date as 'mm/dd/yyyy'. The date is used for telnet/console management purposes.
agentSystemTime	rw	3/ This indicates the current system time as 'hh:mm:ss'. The time is used for telnet/console management purposes.

Table 6-2 *axg2-agent.mib Objects (continued)*

MIB Name	Object Type	Description
agentResetAgent	rw	4/ This indicates the current status of the agent. If the agent shall be reset, it can be done here by writing 'reset' to this object. INTEGER {running (1), reset (2)}
agentResetSystem	rw	5/ This indicates the current status of the system the agent belongs to. If the whole system shall be reset, it can be done by setting 'reset' to this object. INTEGER {running (1), reset (2)}
agentGeneralConfigGroup	group name	
agentAlarmStatus	rw	This indicates the current status of the alarm generator. If an alarm is active, it can be reset here. If desired, the alarm can also be activated from here by writing 'active' to this object. SYNTAX INTEGER { active (1), inactive (2) }
agentSystemDate	rw	This indicates the current system date as 'mm/dd/yyyy'. The date is used for telnet/console management purposes.
agentSystemTime	rw	This indicates the current system time as 'hh:mm:ss'. The time used for telnet/console management purposes.
agentResetAgent	rw	This indicates the current status of the Agent. If the agent shall be reset, it can be done here by writing 'reset' to this object. SYNTAX INTEGER { running (1), reset (2) }
agentResetSystem	rw	This indicates the current status of the system the agent belongs to. If the whole system shall be reset, it can be done by setting 'reset' to this object. SYNTAX INTEGER { running (1), reset (2) }
agentTrapReceiverTable	table name	/3// This entity defines the Trap Receiver Table.
agentTrapReceiverEntry	table entry	1// One entry in this entity's trap receiver table, consisting of the trap receiver's IP address and the community string to be used with it. INDEX {trapReceiverNetAddress}
traprxNetAddress	rw	1/ The network (IP) address of a trap receiver.
traprxTrapCommunity	rw	2/ The community string used for traps being sent to a receiver.
traprxType	rw	3/ All entries return the value 1 (valid) for this object. Setting this object to the value 2 (invalid) deletes the entry from the trap receiver table. INTEGER {valid (1), invalid (2) address}
agentSecurityTable	table name	/4// This entity's Security Table.
agentSecurityEntry	table entry	1// One entry in this entity's security table, consisting of the security level and the community string to be used with it. INDEX {secLevel}
securityLevel		1/ The security level that is indicated by using the security community string. INTEGER {sysgroup-read-access (1), monitor-access (2), service-access (3), standard-mgmt-access (4), administrator-access (5)}

Table 6-2 *axg2-agent.mib Objects (continued)*

MIB Name	Object Type	Description
securityCommunity	rw	2/ The community string used for identification of the desired security level.
agentMngmtSecurityGroup	group name	/5// MANAGEMENT SECURITY GROUP
agentAuthenticationRestrictMode	rw	1/ Restricting management authorization means that only snmp requests from members of the trap receiver table will be accepted. Requests from other sources will instead cause an authentication trap, if enabled. When not restricted, snmp requests from any manager who uses a valid community will be accepted, although traps will be sent only to those destinations that are included in the trap receiver table. INTEGER {other (1), not-restricted (2), restricted (3)}
agentIPConfigGroup	group name	/6// AGENT IP CONFIG GROUP
agentNetAddress	rw	1/ The network address of this agent, e.g. the IP Address.
agentNetMask	rw	2/ The subnet mask of this agent.
agentARPCacheTimeout	rw	3/ The period of time (in seconds) until an entry disappears from the ARP cache. The allowed values are between 1 and 255.
agentTimeToLive	rw	4/ The time to live for an IP packet, respectively the number of hops an IP packet can pass until it is discarded. The allowed values are between 1 and 255.
agentReassembleTimeout	rw	5/ The reassemble time-out (in seconds) for an IP packet. The allowed values are between 1 and 255.
agentStatisticGroup	group name	
statisticPowerGood		Number of Power Good (i.e. number of agent's startups).
statisticProgReset		The number of program resets. This parameter is only of interest in case of troubleshooting.
statisticCPUShutdownCycles		The number of CPU shutdowns. This parameter is only of interest in case of troubleshooting.
statisticCPUWatchdogResets		The number of CPU watchdog resets, which were caused by software errors. This parameter is only of interest in case of troubleshooting.
statisticControllerWatchdogResets		The number of controller watchdog resets, which were caused by software or hardware errors. This parameter is only of interest in case of troubleshooting.
statisticAgentResetsByUser		The number of agent resets caused by user input.
statisticSystemResetsByUser		The number of system resets caused by user input.
agentEventMonitorTable	table name	/7// This entity's agent event monitoring table.

Table 6-2 *axg2-agent.mib Objects (continued)*

MIB Name	Object Type	Description
agentEventMonitorEntry	table entry	1// One entry in this table gives information about an event detected by the agent. Up to 25 events can be displayed in this table. INDEX {agentEventMonitorIndex}
eventIndex		1/ The Index of this Table.
eventDate		2/ The date an event occurred.
eventTime		3/ The point of time an event occurred.
eventMessage		4/ The message of an event.
agentTrapCounter	table name	/8// The number of sent enterprise traps.

axg2-scx-as MIB

The axg2-scx-as.mib is explained in the Table 6-3. This MIB {g2AgentSpecific 2} describes all (snmp-manageable entities) agents from arcutronix designed for the g2Management and is mandatory for those devices.

Table 6-3 *axg2-scx-as.mib Objects*

MIB Name	Object Type	Description
axg2-scx-as	mib name	760 2 10 100 3 // This MIB describes snmp-manageable entities
agentStatisticGroup	group name	/1// AGENT GENERAL STATISTIC GROUP
statisticPowerGood		1/ The number of power good events (i.e. number of agent's start-ups).
statisticProgReset		2/ The number of program resets. This parameter is only of interest in case of troubleshooting.
statisticCPUShutdownCycles		3/ The number of CPU shutdowns. This parameter is only of interest in case of troubleshooting.
statisticCPUShutdownCycles		3/ The number of CPU shutdowns. This parameter is only of interest in case of troubleshooting.
statisticCPUWatchdogResets		3/ The number of CPU watchdog resets, which were caused by software errors. This parameter is only of interest in case of troubleshooting.
statisticCPUWatchdogResets		3/ The number of controller watchdog resets, which were caused by software or hardware errors. This parameter is only of interest in case of troubleshooting.
statisticAgentResetsByUser		4/ The number of agent resets caused by user input.

Table 6-3 *axg2-scx-as.mib Objects (continued)*

MIB Name	Object Type	Description
statisticSystemResetsByUser		5/ The number of system resets caused by user input.
statisticControllerWatchdogResets		6/ The number of controller watchdog resets, which were caused by software or hardware errors. This parameter is only of interest in case of troubleshooting.

axg2-chassis MIB

The axg2-chassis.mib is explained in Table 6-4. This MIB {g2Management 20} describes and gives general information about all physical CHASSIS constructions that contain devices or modules from arcutronix designed for the g2Management and is mandatory for those. A chassis may be a stand-alone box as well as a cabinet consisting of several chassis (racks) and other components that contain lots of slots and modules. It may also contain one single device or various functional units. Also refer to g2ChassisSpecific-MIB {axg2-chassis 200}, for specific features of an unit see corresponding ChassisSpecific-MIB description.

Table 6-4 *axg2-Chassis.mib Objects*

MIB Name	Object Type	Description
axg2-chassis	mib name	760 2 20 // This MIB describes all g2Management CHASSIS
chassisGeneralInfoTable	table name	/1// Table which contains general information about the chassis.
chassisGeneralInfoEntry	table entry	1// The index of the table. INDEX {chassisIndex}
chassisIndex		1/ The index of a chassis managed via the corresponding agent.
chassisType		2/ The chassis type. INTEGER {modular-multiplexer (2), multiplexer (3), single-slot-housing (4), rack (5)}
chassisSpecificType		3/ The specific Type of the chassis. INTEGER {other (1), ra-g-45 (11), ra-g-65 (12), ra-g-125 (23) emux-m (40)}
chassisUserName	rw	4/ The user name of the chassis.
chassisSlots		5/ The number of slots (for modules, devices, ..) in the chassis.
chassisPowerSupplies		6/ The max. number of power supplies in the chassis.
chassisFans		7/ The max. number of fans in the chassis.
chassispsTable	table name	Table with information about the power supply in the chassis.
chassispsEntry	table entry	The index of the table.
chassispsChassis		The index of the chassis.
chassispsPSIndex		The power supply index.
chassispsPSType		The textual description.

Table 6-4 *axg2-Chassis.mib Objects (continued)*

MIB Name	Object Type	Description
chassispsPSSStatus		The status of the power supply.
chassispsVoltageOutput		The voltage output of the power supply.
chassispsMinAllowedVoltage		This min allowed voltage of the power supply.
chassispsMaxAllowedVoltage		This max allowed voltage of the power supply.
chassispsAlarmEnabled		This enables or disables ALARMS of the power supply.
chassispsTrapEnabled		This enables or disables TRAPs of the power supply.

axg2-chassis MIB Traps

The traps of axg2-chassis MIB are explained in the Table 6-5.

Table 6-5 *axg2-Chassis.mib Traps*

TRAP Name	Description
chassisChassisAdded	20001/ This trap will be sent when a chassis has been added to the list of chassis monitored by an agent. VARIABLES {trapCounter, chassisIndex, chassisSpecificType, chassisUserName}
chassisChassisRemoved	20002/ This trap will be sent when a chassis has been removed so that the agent is no longer able to monitor it. VARIABLES {trapCounter, chassisIndex, chassisSpecificType, chassisUserName}

axg2-scx-cs MIB

The axg2-scx-cs.mib is explained in the Table 6-6. This chassis specific {g2ChassisSpecific 2} MIB, content of MIB-TREE g2management, gives detailed information about the arcutronix Multi Service System chassis from arcutronix and attached components. Sub sections: rcPowerSupply {axg2-rc-cs 1}, rcPowerSupplyTable {rcPowerSupply 1}, rcPowerSupplyControlTable {rcPowerSupply 2}, rcFanControl {axg2-rc-cs 2}, rcFanControlTable {rcFanControl 1}, rcFansControlEntry {rcFanControl 2}, rcTemperatureTable {axg2-rc-cs 3}, rcStatusTable {axg2-rc-cs 4}, rcSelfTestTable {axg2-rc-cs 5}.

Table 6-6 *axg2-scx-cs.mib Objects*

MIB Name	Object Type	Description
axg2-scx-cs	mib name	760 2 20 200 3 // scx CHASSIS SPECIFIC MIB
scxPowerSupply	sub section	// SEQUENCE OF CHASSIS POWER SUPPLY Entries
scxPowerSupplyTable	table name	// Table with information about the power supplies in the chassis.

Table 6-6 *axg2-scx-cs.mib Objects (continued)*

MIB Name	Object Type	Description
scxPowerSupplyEntry	table entry	1// The index of the table. INDEX {powersupplyRack, powersupplyPSId}
powersupplyRack		1/ The id of the chassis.
powersupplyPSId		2/ The power supply id.
powersupplyPlugged		3/ The plugged-status of the power supply. INTEGER {yes (2), no (3)}
powersupplyPSType		4/ The textual description.
powersupplyStatus		5/ The status of the power supply. INTEGER {ok (2), failed (3), not-plugged (4), present (5), not-available (6)}
powersupplyVoltageOutput		6/ The voltage output of the power supply.
scxPowerSupplyControlTable	table name	2// Table with information about the power supplies in the chassis.
scxPowerSupplyControlEntry	table entry	1// The index of the table. INDEX {powersupplyCtrlRack}
powersupplyCtrlRack		1/ The id of the chassis.
powersupplyCtrlAlarmIndication	rw	2/ This enables or disables every alarm regarding power supplies supervised in the chassis by the agent. INTEGER {enabled (2), disabled (3)}
powersupplyCtrlTrapIndication	rw	3/ This enables or disables every trap regarding power supplies supervised in the chassis by the agent. INTEGER {enabled (2), disabled (3)}
scxFanControl	sub section	2// SEQUENCE OF CHASSIS FAN CONTROL Entry
scxFanControlTable	table name	1// Table which contains information about all fans.
scxFanControlEntry	table entry	1// The index of the table. INDEX {fanRack, fanId}
fanRack		1/ The id of the chassis.
fanId		2/ The fan id.
fanPlugged		3/ The plugged-status of the fan. INTEGER {yes (2), no (3)}
fanStatus		4/ Indicates the status of fan module 1 in chassis. INTEGER {not-plugged (2), underrun (3), ok (4), not-available (5)}
fanRPM		5/ The speed of fan in chassis.
fanRunTime		6/ Indicates the run time of fan module in chassis.
scxFansControlTable	table name	2// Table which contains information about all fans.
scxFansControlEntry	table entry	1// The index of the table. INDEX {fansRack}
fansRack		1/ The id of the chassis.
fansMinRPMLimit	rw	2/ The minimum speed of all fans in chassis.

Table 6-6 *axg2-scx-cs.mib* Objects (continued)

MIB Name	Object Type	Description
fansAlarmIndication	rw	3/ This enables or disables the alarm indication for all fans in the chassis. INTEGER {enabled (2), disabled (3)}
fansTrapIndication	rw	4/ This enables or disables the trap indication for all fans in the chassis. INTEGER {enabled (2), disabled (3)}

axg2-scx-cs MIB Traps

The traps of axg2-scx-cs MIB are explained in the Table 6-7.

Table 6-7 *axg2-scx-cs.mib* Traps

TRAP Name	Description
scxPowerSupplyAdded	20301/ This trap will be sent when a power supply has been added. VARIABLES {trapCounter, powersupplyRack, powersupplyPSId}
scxPowerSupplyRemoved	20302/ This trap will be sent when a power supply has been removed. VARIABLES {trapCounter, powersupplyRack, powersupplyPSId}
scxPowerSupplyFailed	20303/ This trap will be sent when a power supply has been failed. VARIABLES {trapCounter, powersupplyRack, powersupplyPSId, powersupplyVoltageOutput}
scxFanAdded	20304/ This trap will be sent when a fan has been added. VARIABLES {trapCounter, fanRack, fanId}
scxFanRemoved	20305/ This trap will be sent when a fan has been removed. VARIABLES {trapCounter, fanRack, fanId}
scxFanUnderrun	20306/ This trap will be sent when a fan status changed to underrun. VARIABLES {trapCounter, fanRack, fanId, fanRPM}

axg2-device MIB

The axg2-device.mib is explained in the Table 6-8. This MIB {g2Management 30} describes and gives general information about all devices from arcutronix designed for the g2Management and is mandatory for those. For specific features of devices see g2DeviceSpecific-MIB {300}.

Table 6-8 *axg2-device.mib* Objects

MIB Name	Object Type	Description
axg2-device	mib name	760 2 30 // THE DEVICE MIB (g2Management)
standardDeviceTable	table name	/1// Table which contains standard information about manageable (controllable) devices inserted into arcutronix equipment.

Table 6-8 *axg2-device.mib Objects (continued)*

MIB Name	Object Type	Description
standardDeviceEntry	table entry	1// The index of the table. INDEX {sdtRack, sdtSlot, sdtPort, sdtHop}
sdtRack		1/ The index of a chassis (rack) situated at the local side.
sdtSlot		2/ The index of a slot inside a chassis situated at the local side.
sdtPort		3/ This entry specifies the port at the local device, which is used to reach the remote device located at the specified hop (please refer also to the next entry sdtHop). For a local device this value is always set to '0'.
sdtHop		4/ In a chain of devices the hop number specifies the position of a device within the chain. The local device, which is located at the same site like the currently managed agent (ip-node) gets the number '0'. The first device, which is connected to the specified port (see sdtPort) of a local device gets the hop number '1'. The second device gets the number '2' and so on.
sdtDeviceType		5/ The type of a device.
sdtUserName	rw	6/ The user's defined name for a device.
sdtDescription		7/ The description of a device.
sdtSerialNumber		8/ The manufacturer's serial number of a device.
sdtSoftwareRev		9/ The software revision of a device.
sdtHardwareRev		10/ The hardware revision of a device.
sdtArticleRev		11/ The article revision of a device.
sdtOrderInfo		12/ The order information of a device.
sdtManufacturer		13/ The manufacturer of a device.
interDeviceCatenationTable	table name	/2// Table which contains information about the catenations between devices inserted into arcutronix equipment.
interDeviceCatenationEntry	table entry	1// The index of the table. INDEX {idctRack, idctSlot, idctPort, idctHop}
idctRack		1/ The index of a chassis (rack) situated at the local side.
idctSlot		2/ The index of a slot inside a chassis situated at the local side.
idctPort		3/ This entry specifies the port at a local device, which is used to reach the remote device located at the specified hop (please refer also to the next entry idctHop). For a local device this value is set to '0'.

Table 6-8 *axg2-device.mib* Objects (continued)

MIB Name	Object Type	Description
idctHop		4/ In a chain of devices the hop number specifies the position of a device within the chain. The local device, which is located at the same site like the currently managed agent (ip-node) gets the number '0'. The first device, which is connected to the specified port (see idctPort) of a local device gets the hop number '1'. The second device gets the number '2' and so on.
idctDeviceType		5/ The type of a device.
idctRemoteAgentIP		6/ The IP-Address of an agent situated at a remote location. If no remote agent is present the value is '0.0.0.0'.
idctRemoteRack		7/ The index of a chassis the remote device is built-in. '0' for unknown.
idctRemoteSlot		8/ The index of a slot inside a chassis the remote device is built-in. '0' for unknown.
idctRemotePort		9/ The port number of the remote device which is used for the communication with the local device. '0' for unknown.
localDeviceLinkTable	table name	/3// Table which contains data and management link information about all ports at local devices inserted into arcutronix equipment.
localDeviceLinkEntry	table entry	1// The index of the table. INDEX {ldltRack, ldltSlot, ldltPort}
ldltRack		1/ The index of a chassis (rack) where the device is installed.
ldltSlot		2/ The index of a slot inside a chassis where the device is installed.
ldltPort		3/ This entry specifies the port at a local device.
ldltLinkStatus		4/ Status of the data link between the local and the remote device. INTEGER {up (2), down (3)}
ldltMngmtAccess		5/ This entry is indicating the management access status to the corresponding remote device. INTEGER {active (2), not-active (3), not-supported (4)}

axg2-Device MIB Traps

The traps of axg2-Device MIB are explained in the Table 6-9.

Table 6-9 *axg2-Device.mib* Traps

TRAP Name	Description
devicesDeviceAdded	30001/ This trap will be sent when a device has been added to a chassis. VARIABLES {trapCounter, sdtRack, sdtSlot, sdtPort, sdtHop, sdtDeviceType}
devicesDeviceRemoved	30002/ This trap will be sent when a device has been removed from a chassis. VARIABLES {trapCounter, sdtRack, sdtSlot, sdtPort, sdtHop, sdtDeviceType}

axg2-scx-ds MIB

The axg2-scx-ds.mib is explained in the Table 6-10. This device specific {g2DeviceSpecific 20} MIB (content of MIB-TREE g2management) gives detailed information about the RC-588 Card from arcutronix and attached components. Sub sections: rcPowerSupply {axg2-rc-cs 1}, rcPowerSupplyTable {rcPowerSupply 1}, rcPowerSupplyControlTable {rcPowerSupply 2}, rcFanControl {axg2-rc-cs 2}, rcFanControlTable {rcFanControl 1}, rcFansControlEntry {rcFanControl 2}, rcTemperatureTable {axg2-rc-cs 3}, rcStatusTable {axg2-rc-cs 4}, rcSelfTestTable {axg2-rc-cs 5}

Table 6-10 axg2-scx-ds.mib Objects

MIB Name	Object Type	Description
axg2-scx-ds	mib name	760 2 20 200 20 // THE RC-588 DEVICE SPECIFIC MIB
rcPowerSupply	sub section	/1// SEQUENCE PowerSupplyEntry
scxTemperatureTable	table name	/1// Table which contains information about all fans.
scxTemperatureEntry	table entry	1// The index of the table. INDEX {tempRack}
tempRack		1/ The id of the chassis (rack).
tempBoard		2/ The current board temperature.
tempMin	rw	3/ The minimum allowed board temperature.
tempMax	rw	4/ The maximum allowed board temperature.
tempStatus		5/ Indicates the status of the board temperature. INTEGER {underrun (2), overrun (3), ok (4)}
tempMinAlarmIndication	rw	6/ This enables or disables the alarm indication in case of understepping of the minimum temperature limit. INTEGER {enabled (2), disabled (3)}
tempMaxAlarmIndication	rw	7/ This enables or disables the alarm indication in case of overstepping of the maximum temperature limit. INTEGER {enabled (2), disabled (3)}
tempMinTrapIndication	rw	8/ This enables or disables the trap indication in case of understepping of the minimum temperature limit. INTEGER {enabled (2), disabled (3)}
tempMaxTrapIndication	rw	9/ This enables or disables the alarm indication in case of overstepping of the maximum temperature limit. INTEGER {enabled (2), disabled (3)}
scxStatusTable	table name	/2// Table which contains information about the modules status in the chassis.
scxStatusEntry	table entry	1// The index of the table. INDEX {statRack}
statRack		1/ The id of the chassis (rack).
statRunTime		2/ The current run time of the rc card.

Table 6-10 *axg2-scx-ds.mib Objects (continued)*

MIB Name	Object Type	Description
statAlarm		3/ The current alarm status of the rc card. INTEGER {on (2), off (3)}
scxSelfTestTable	table name	/3// Table which contains information about all performable test.
scxSelfTestEntry	table entry	1// The index of the table. INDEX {selfRack}
selfRack		1/ The id of the chassis (rack).
selfRAMTest		2/ This entry shows the result status of the last card self test. After start, the status may change to 'running' before the first error that occurred is displayed. If no error was detected the status changes to 'pass'. INTEGER {other (1), never-started (2), wait-for-start (3), running (4), pass (5), failed (6)}
selfROMTest		3/ This entry shows the result status of the last card self test. After start, the status may change to 'running' before the first error that occurred is displayed. If no error was detected the status changes to 'pass'. INTEGER {other (1), never-started (2), wait-for-start (3), running (4), pass (5), failed (6)}
selfFLASHTest		4/ This entry shows the result status of the last card self test. After start, the status may change to 'running' before the first error that occurred is displayed. If no error was detected the status changes to 'pass'. INTEGER {other (1), never-started (2), wait-for-start (3), running (4), pass (5), failed (6)}
selfTestAction	rw	5/ This entry enables the execution of a selftest. Write requests with values other than 'start' or 'stop' will be rejected. INTEGER {start (2), stop (3)}
fomuxFansControlTable	table name	/2// Table which contains information about all fans.
fomuxFansControlEntry	table entry	1// The index of the table.
fansRack		1/ The id of the chassis.
fansMinRPMLimit	rw	2/ The minimum speed of all fans in chassis.
fansAlarmIndication	rw	3/ This enables or disables the alarm indication for all fans in the chassis. INTEGER { enabled (2), disabled (3) }
fansTrapIndication	rw	4/ This enables or disables the trap indication for all fans in the chassis. INTEGER { enabled (2), disabled (3) }

axg2-scx-ds MIB Traps

The traps of axg2-scx-ds MIB are explained in the Table 6-11.

Table 6-11 *axg2-scx-ds.mib Traps*

TRAP Name	Description
scxTemperatureUnderrun	32001/ This trap will be sent when the temperature status changed to underrun. VARIABLES { trapCounter, tempRack, tempBoard, tempMin } VARIABLES {tempRack, tempBoard, tempMin}
scxTemperatureOverrun	32002/ This trap will be sent when the temperature status changed to overrun. VARIABLES { trapCounter, tempRack, tempBoard, tempMax } VARIABLES {tempRack, tempBoard, tempMax}

Appendix A

Technical Data

Table A-1 provides the general technical data of the SCX - System Controller.

Table A-1 SCX2 Technical Data

Item	Type	Specification
Data transmission control port RS232/VT100	Data Rate	57.6 Kbps or 9.6 Kbps
	Protocol	8 data bits, no parity, one stop bit, no handshake
Data transmission SNMP port RJ45 10/100BaseTx	Ethernet Data Rate	10 Mbps or 100 Mbps
	Protocol	10BaseT or 100BaseTX
Data transmission advanced management chain	Downstream port	12 Mbps
	Upstream port	12 Mbps
Electrical specifications	Power Supply Voltage	+5 V DC \pm 5%
	Power Consumption	Pmax < 6.7 W (SCX2)
Mounting possibility	3 RU height, 8½ U width	Slot 11 in SRX10 or slot 25 in SRX24.
	Weight	300 g
Physical dimensions	Height	128 mm
	Width	43.18 mm (8.5 HP)
	Depth	187 mm

Table A-2 provides the technical data of the SCX2 Ethernet ports.

Table A-2 Technical Data of the SCX2 Ethernet Ports

Type	Description
Ethernet Port	
Connector:	RJ-45, 8-pin, DTE-mode, no(!) auto crossover
Data rate:	10/100BaseT acc. IEEE 802.3 (2002) with auto negotiation, full-/half-duplex detection
VLAN support:	IEEE 802.3 p,Q Q-in-Q capability (double VLAN tagging)
MAC addresses:	1k self-learning MAC address space

Table A-2 *Technical Data of the SCX2 Ethernet Ports (continued)*

Type	Description
Bandwidth limitation:	256k, 512k, 1M, 2M, 4M, 8M, 16M, 32M Broadcast and flooding limiter (16M)
References:	IEEE 802.3 (2002), 802.1 p,Q
Statistics:	SNMP RMON statistics

Table A-3 provides the technical data of the SCX2 serial interface.

Table A-3 *Technical Data of the SCX2 Serial Interface*

Type	Description
Serial Interface	
Connector	RJ-45, 8-pin
Data rate:	2.4, 9.6, 19.2, 38.4 (default), 57.6, 115.2 kbps
References:	EIA-232D (RS-232D)

Table A-4 provides the technical data of the SCX2 management access.

Table A-4 *Technical Data of the SCX2 Ethernet/IP Management Access*

Type	Description
Telnet	IETF RFC 854, RFC 855
SNMP	SNMPv1, SNMPv2c
SW-Download	via FTP, IETF RFC 959
Profile Store / Load	via TFTP, IETF RFC 1350
DHCP Client	IETF RFC 2131

Table A-5 provides the environmental conditions.

Table A-5 *Environmental conditions*

Item	Type	Specification
Environmental conditions	Temperature (operation)	+5... +40 °C
	Temperature (storage)	-30... +80 °C
	Humidity	10... 90%, non- cond.

Table A-6 provides the specification of the Real Time Clock.

Table A-6 *Real Time Clock*

Item	Type	Specification
Real Time Clock	Accuracy	10ppm (<1sec/day)
	Hold Time (without ext. power)	min. 11 days

Technical Data

Appendix B

FTP-Access

Intro

This appendix explain the FTP access for SCX2 units. As the file transfer for large files is very slow across a RS232-link, the best way to update device-SW (SW of the line-cards), SCX2-SW is to use FTP.

There are several FTP-clients available, which all can be used. This document does focus on Windows platform, using Windows Explorer or Mozilla Firefox with an extension.

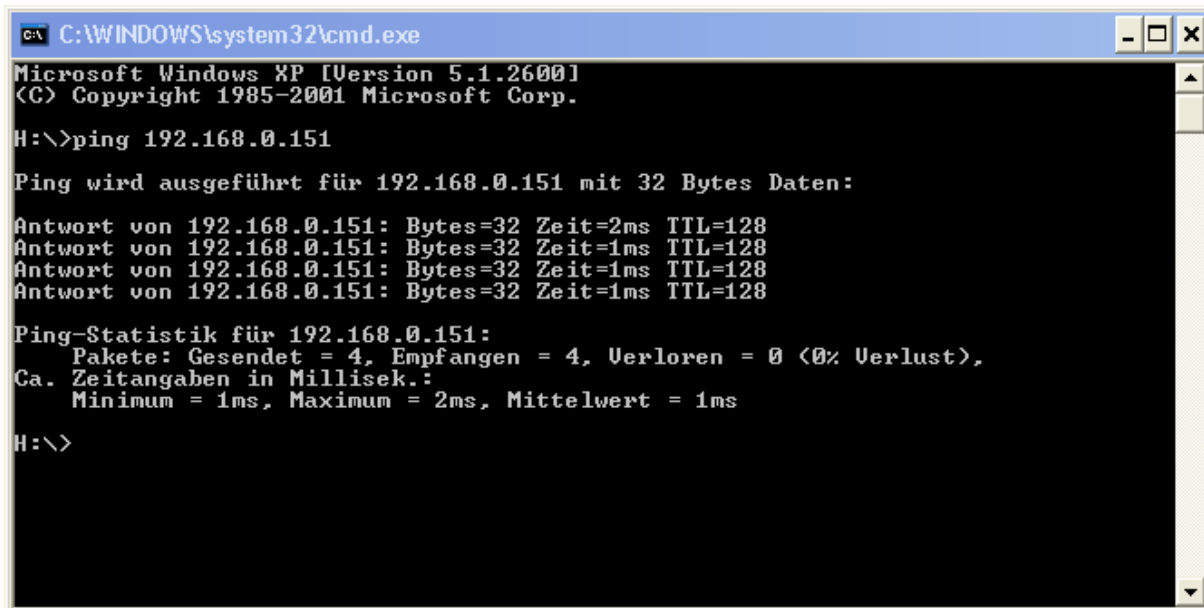
[FTP: File Transfer Protocol, RFC959.](#)

NOTE: The given document presents a lot of screen-shots to show, which windows and commands are required. The author is using a German version of Windows XP, so on your PC it might be different. At least the language.

Proper Setup

Using FTP for File Transfer requires a working IP-link from your PC to the SCX2:

1. Configure the IP-address of SCX2 in the right way and make sure your PC can reach the SCX2:
 - E.g. IP = 192.168.0.151
 - C:\ping 192.168.0.151



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>ping 192.168.0.151

Ping wird ausgeführt für 192.168.0.151 mit 32 Bytes Daten:

Antwort von 192.168.0.151: Bytes=32 Zeit=2ms TTL=128
Antwort von 192.168.0.151: Bytes=32 Zeit=1ms TTL=128
Antwort von 192.168.0.151: Bytes=32 Zeit=1ms TTL=128
Antwort von 192.168.0.151: Bytes=32 Zeit=1ms TTL=128

Ping-Statistik für 192.168.0.151:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 1ms, Maximum = 2ms, Mittelwert = 1ms

H:\>
```

Figure B-1 Ping SCX2

If the ping-command is successful, you can go on to the next step. Otherwise, you need to check cables, IP-address, Default-GW etc.

FTP-connection

Windows Explorer

1st Step

Open a new Windows-Explorer window and enter **ftp://admin@ip-address**

admin: This is the administrator username of the SCX2. By default, this is admin

ip-address: this is the configured IP-address of the SCX2. In our example 192.168.0.151:

ftp://admin@192.168.0.151

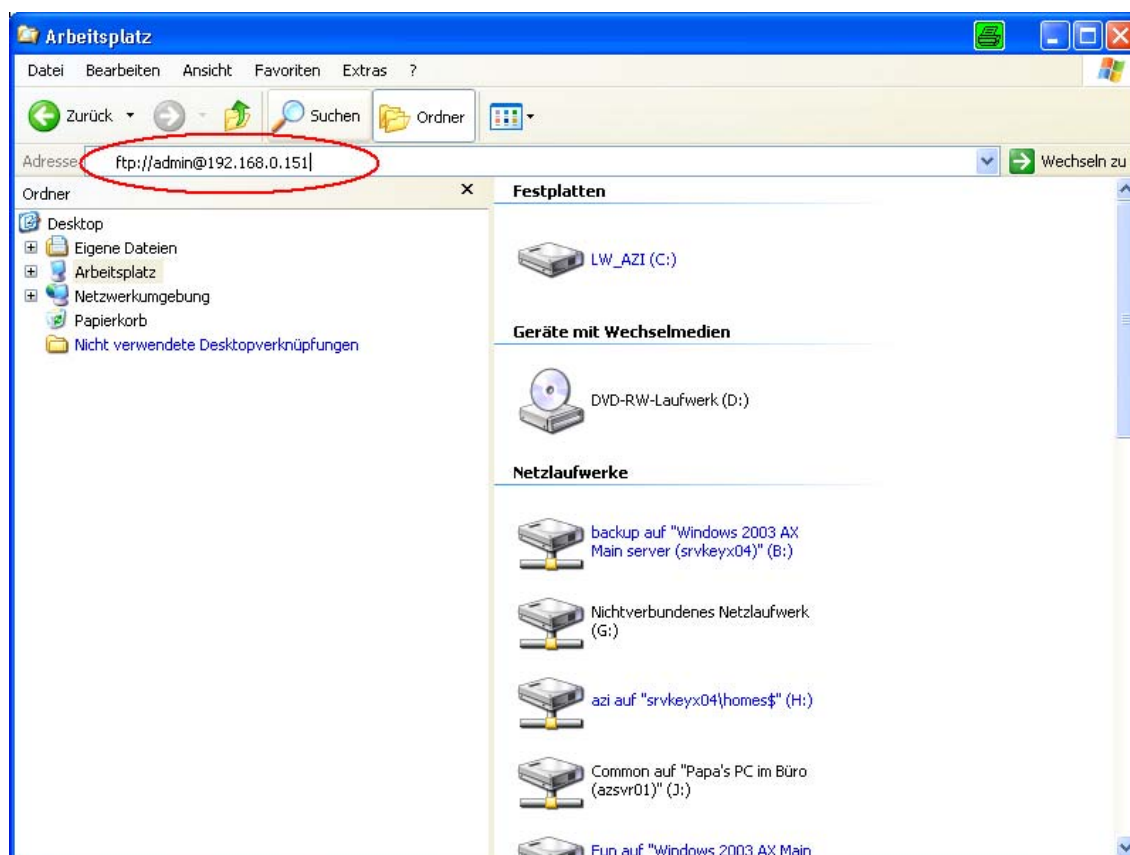


Figure B-2 ftp-access in MS-Internet Explorer

2nd Step

Press Enter and a new window will appear where username and password has to be entered. In default this is admin/admin. If you like, you can store the password to make it easier the next time:

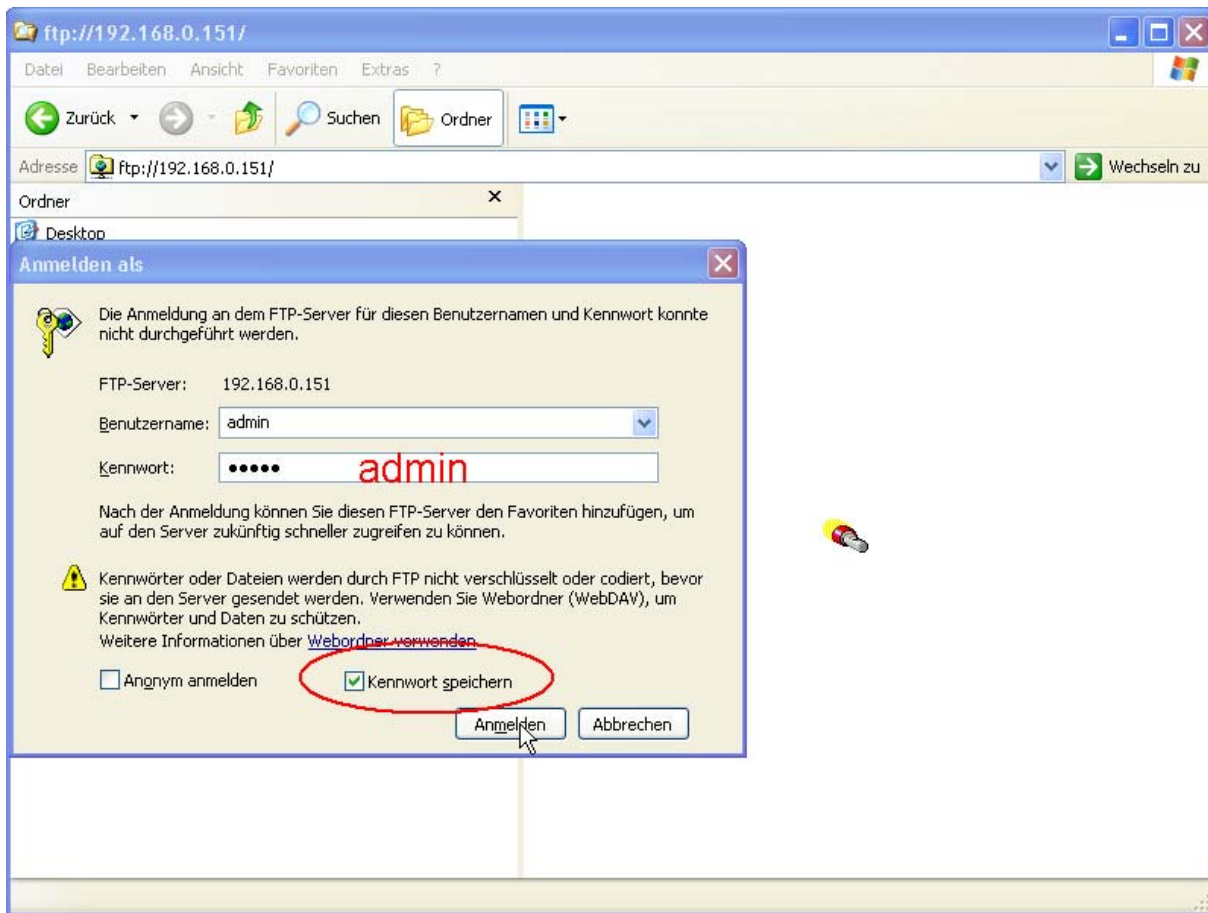


Figure B-3 ftp-access in MS-Internet Explorer

3rd Step

Now you will get FTP access to the SCX2 and see the following window:

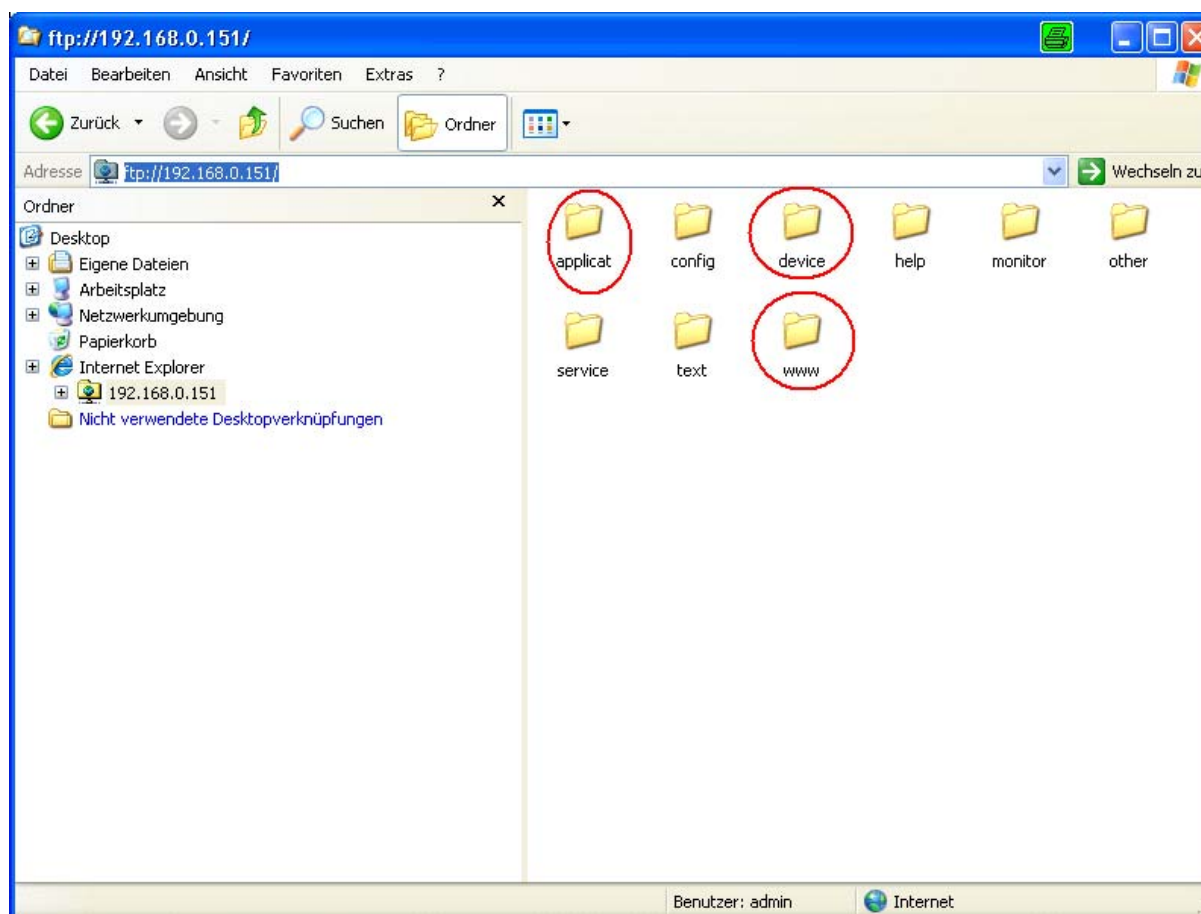


Figure B-4 Directories of SCX2

In this window, one can easily transfer the files to the correct folders:

- The SCX-SW to the "applicat" directory
- The FCX-SW (and all other device-SW) to the "device" directory
- The Web-GUI Update to the "www" directory. You can copy the www-directory in total. If it already exists, just confirm to overwrite the existing one.

Mozilla Firefox

1st Step

For Mozilla, we recommend to install FireFTP for Firefox. When FireFTP is installed, you get a new entry, to start the FTP-client:

FTP-Access FTP-connection

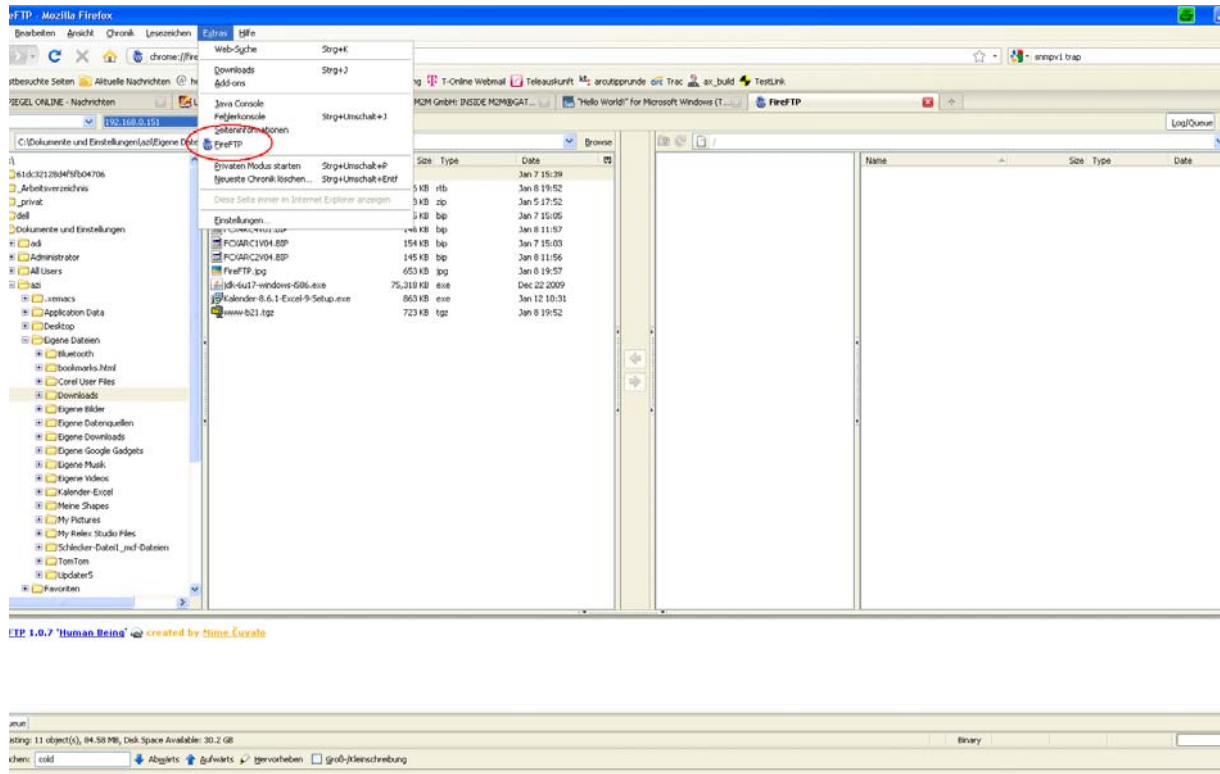


Figure B-5 ftp-access in Modzilla Firefox

2nd Step

Press "Edit" and a new window will appear where username and password has to be entered. In default this is admin/admin. The category can be free selected. We suggest to use enter SCX2 and use this category for all SCX2 FTP-sessions.

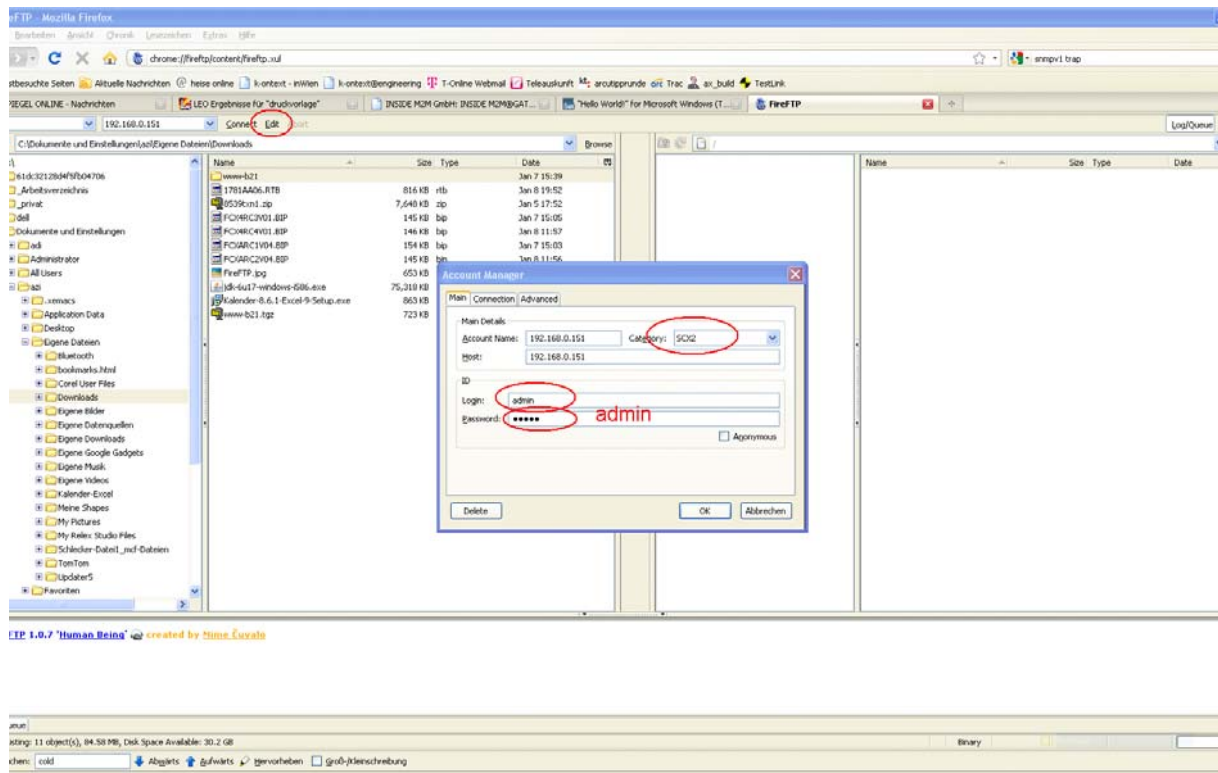


Figure B-6 ftp-access in Mozilla Firefox

3rd Step

The next time, you want to connect to an already defined SCX2, it is easy. Just select the right category and IP-address and press connect:

FTP-Access FTP-connection

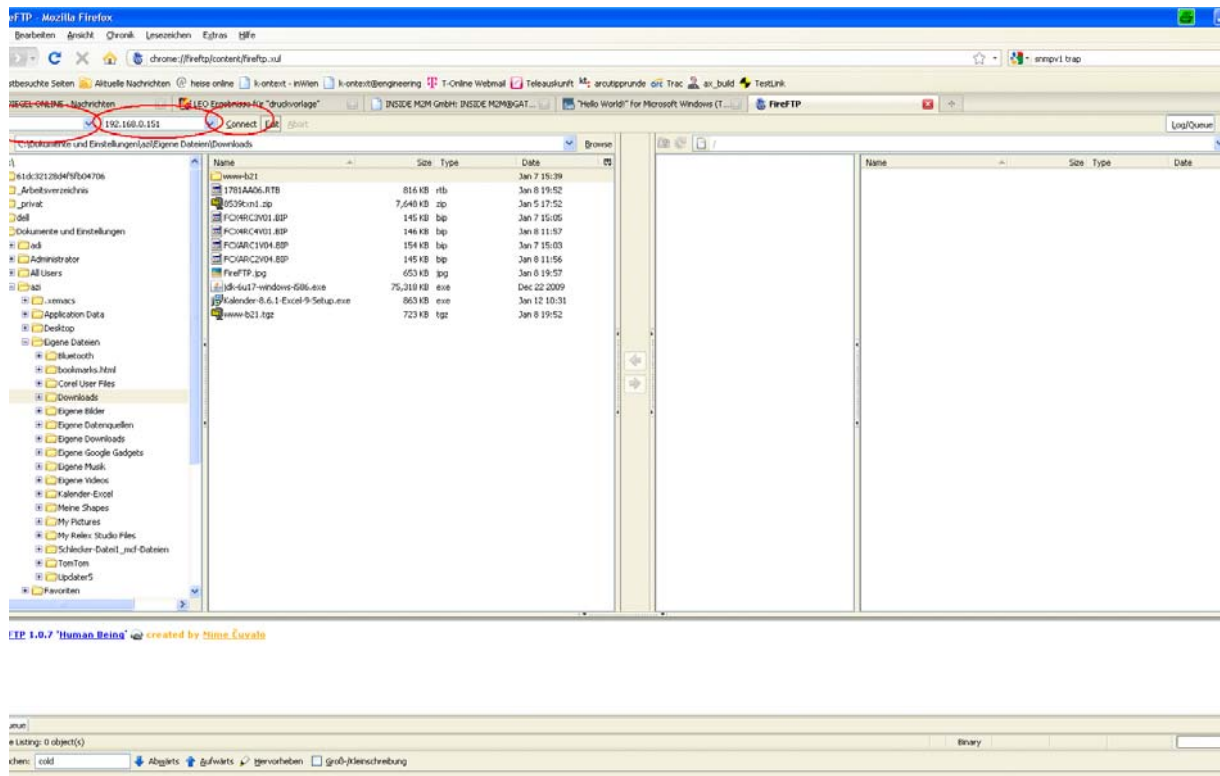


Figure B-7 ftp-access in Mozilla Firefox

4th Step

Now you will get FTP access to the SCX2 and see the following window:

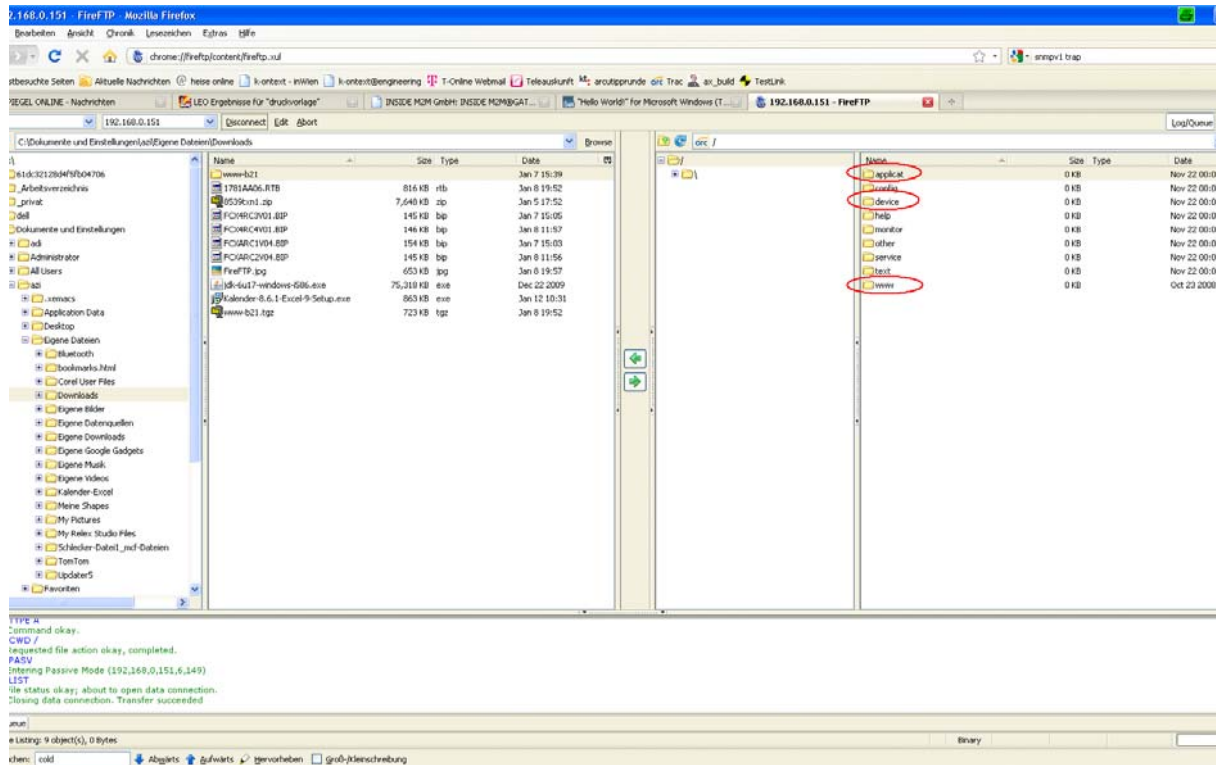


Figure B-8 Directories of SCX2

In this window, one can easily transfer the files to the correct folders:

- The SCX-SW to the "applicat" directory
- The FCX-SW (and all other device-SW) to the "device" directory
- The Web-GUI Update to the "www" directory. You can copy the www-directory in total. If it already exists, just confirm to overwrite the existing one.

Which File to which Directory?

SCX2-Files (RTB-Files)

The SCX2-update files do have the following name:

1781AAxx.RTB, where **AAxx** is the version of the file.

Copy **RTB**-files to the **applicat**-directory. Make sure, the latest file does have the newest date-code. Sometimes, the date-code gets lets with FTP. In case, delete older files!

FTP-Access

Where to get the Update-File(s)?

After the next reset, the SCX2 will start with the youngest RTB-file in the `applicat` directory.

Device-Files (BIP-Files)

The update files for all line-cards do have the following name:

`ZZZZA A_{xx} .BIP`, where `A A_{xx}` is the version of the file and `ZZZZ` is the device's name.

Copy `BIP`-files to the `device`-directory. When stored in the `device`-directory, you have access to them when you start SW-upgrade on a line-card. For security reasons, there is no automatic SW-upgrade available; each device has to be updated by its own.

WebGUI-Files (www)

If you want to update or initially install the WEBGUI, you have to install the `www`-directory at the root of the file-tree. You can copy the `www`-directory in total. If it already exists, just confirm to overwrite the existing one.

Where to get the Update-File(s)?

The update files are not available via Internet. Please contact your local arcutronix representative if you need additional features. He will provide you the correct file(s).

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: SCX – System Controller
Members: SCX2, SCX2e
Number: 0805-7020, 0903-3000

to which this declaration relates conforms to the following standards, which have been described in the CE-guideline:

89/336/EEC Electromagnetic compatibility
73/23/EEC Safety of low voltage equipment
1999/5/EC Radiocommunication & Telecommunication Terminal Equipment
93/68/EEC CE marking

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, 8.3.2010

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
www.arcutronix.com