RS2-4R Management Manual
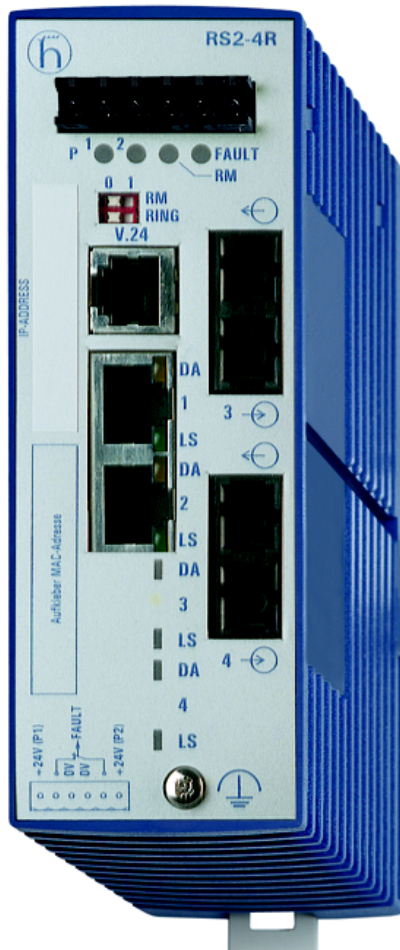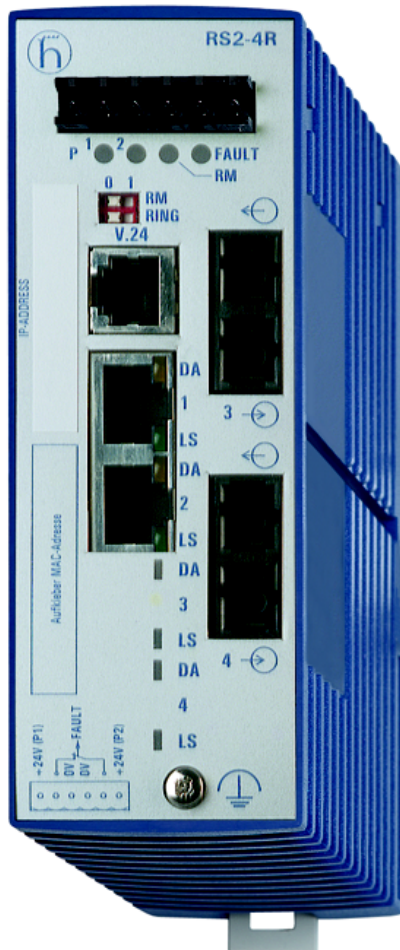
Industrial ETHERNET Rail Switch 2

RS2-4R Management Manual

Industrial ETHERNET Rail Switch 2

Hirschmann worldwide:

■ Germany

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Tel. ++49-7127-14-1480
Fax ++49-7127-14-1502
email: ans-hi-line@hirschmann.de
Internet: www.hirschmann.de

■ Switzerland

Hirschmann Electronics GmbH & Co. KG, Neckartenzlingen
Niederlassung Uster
Seestr. 16
CH-8610 Uster
Tel. ++41-1905-8282
Fax ++41-1905-8289
email: ans_ch@hirschmann.ch

■ France

Hirschmann Electronics S.A.S.
2, rue des Charpentiers
F-95330 Domont
Tel. ++33-1-39350100
Fax ++33-1-39350102
email: ans@hirschmann.fr

◼ Great Britain

Hirschmann Electronics Ltd.
4303 Waterside Centre
Solihull Parkway
Birmingham Business Park
Birmingham
West Midlands B37 7YN
Tel. ++44-121 329 5000
Fax ++44-121 329 5001
email: enquiry@hirschmann.co.uk

◼ Netherlands

Hirschmann Electronics B.V.
Pampuslaan 170
NL-1382 JS Weesp
Tel. ++31-294-462591
Fax ++31-294-462554
email: ans@hirschmann.nl

◼ Spain

Hirschmann Electronics S.A.
Calle Traspaderne, 29
Barrio del Aeropuerto
Edificio Barajas I, 2^a Planta
E-28042 Madrid
Tel. ++34-1-7461730
Fax ++34-1-7461735
email: hes@hirschmann.es

◼ Hungary

Hirschmann Electronics Kft.
Rokolya u. 1-13
H-1131 Budapest
Tel. ++36-1-3494199
Fax ++36-1-3298453
email: hirschmann.budapest@axelero.hu

■ **USA**

Hirschmann Electronics Inc.
20440 Century Boulevard, Suite 150
Germantown, MD 20874
Tel. ++1-240-686 2300
Fax ++1-240-686 3589
email: ans@hirschmann-usa.com

■ **Singapore**

Hirschmann Electronics Pte. Ltd.
2 International Business Park #11-02/03 Tower One
The Strategy Singapore 609930
Tel: ++65 6316 7797
Fax:++65 6316 7977
email: hirschmann.svi@pacific.net.sg

■ **China**

Hirschmann Electronics Pte Ltd Shanghai Office
Room 828, Summit Centre,
1088 West Yan An Road
Shanghai 200052
P.R. China
Tel: ++86-21 6207 6637
Fax: ++86-21 6207 6837
Mobile: ++86-1370 185 7382
E-Mail: hirschmann@sh163.net

For all other countries please dial Tel. +49-7127-14-16 20
Contact address see Hirschmann Germany.

Hirschmann Competence

In the longterm, product excellence alone is not an absolute guarantee of a successful project implementation. Comprehensive service makes a difference worldwide. In the current scenario of global competition, the Hirschmann Competence Center stands head and shoulders above the competition with its comprehensive spectrum of innovative services:

▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

▶ Training offers you an introduction to the technological fundamentals, product briefing and user training with certification.

▶ Support ranges from commissioning through the standby service to maintenance concepts.

With the Competence Center, you firmly rule out any compromise: the client-specific package leaves you free to choose the service components that you will use.

Internet:
http://www.hicomcenter.com

Contents

3 Installation and startup procedure 29

4 Functions

Contents

6 Management Information Base (MIB) 173

7 User Interface

A Appendix

1   Introduction

In 1984, Hirschmann implemented the world's first ever fiber optic based ETHERNET at the University of Stuttgart, Germany. Then in 1990, Hirschmann introduced the "ETHERNET Ring".

These innovations were followed in 1993 by the first media converters for fieldbus systems and rapid redundancy in the switched ETHERNET in 1998.

Today, the global specialist for enterprise-wide networks, from fiber INTERFACES for fieldbus systems through ETHERNET transceivers, hubs, switches and routers and fast ETHERNET switches to gigabit ETHERNET switches, offers a complete system family with unified management.

1.1 Industrial networking solutions with a future

Ethernet is the most widely used communication technology for IT systems. In the office environment, Ethernet has evolved into the standard technology. However, it is also gaining ground in the area of industrial automation. Apart from the advantages of being a standardized means of communication, it also offers a seamless infrastructure that extends from the office to the machine or to the sensor. This not only makes process and production data available on the field level but also provides this data directly to general data entry systems.

Although the Ethernet standard used in automation technology is the same as that used in offices, the requirements for network products are considerably different. In day-to-day industrial applications, networks are expected to work reliably under extreme conditions, such as electromagnetic interference, high operating temperatures and mechanical loads.

The Industrial ETHERNET Rail family was specifically designed for use in industrial automation applications, taking all these requirements into consideration. A result of these requirements is the redundant "ETHERNET Ring" developed by Hirschmann. This process enables continuous production operation, even when a reconfiguration of the network is necessary. The "ETHERNET Ring" also allows networks to be maintained and expanded while still in operation. Since the system is reconfigured in a matter of milliseconds, the "ETHERNET Ring" is considerably better suited to industrial use than the 'spanning tree' algorithm, which primarily meets the needs of office systems.

This process and other concepts from Hirschmann ensure ultimate network and production system reliability. The increased segmentation of the Industrial ETHERNET Rail products allow you to adapt your network to the specific geographical layout and security-related considerations in a more efficient matter. This scalability also ensures the network will meet all future requirements.

General features of the Industrial ETHERNET Rail products include:

► Durable construction for industrial use (IP 20, particularly EMC and vibration tests, 24 V supply voltage, without fan).

► Quick assembly (the sturdy devices are simply mounted on a standard DIN rail)

► Fast startup with Plug & Play technology (autonegotiation, autopolarity, autocrossing) and extensive diagnostic displays.

► Vollduplex switch technology is made possible by the store-and-foreward mode.

► High temperature range, permitting new fields of application

► The signal contact that is read as a binary signal and facilitates remote diagnostics.

1.2 The Industrial ETHERNET Rail Switches

Created from the start as mission-critical switches, Hirschmann's Industrial ETHERNET switches are distinguished by their high network reliability. The Hirschmann ring structure ensures that a single physical or logical error can not lead to system failure. The redundancy concepts incorporated into the switch enable the creation of a reliable, error-resistant communication network based on Ethernet.

Depending on how important the process application is, the level of resilience in the overall network can be scaled so as to meet future requirements as well. For example, where a controller has dual redundant network interface cards, each card could connect to separate switches on the same resilient fiber-optic ring. A second ring may also be integrated if double redundancy is required.

The Fast ETHERNET Rail Switch family RS2-4R allows you to configure medium to large sized deterministic ETHERNET / Fast ETHERNET networks easily and cost-effectively.

The small number of ports of this Rail Switch family allows you to economically install Industrial ETHERNET products in systems in which a low number of ports is required due to an efficient installation of redundant ring structures. For example, the compact Rail Switch RS2-4R for industrial use offers 4 ports:

▶ 2 twisted-pair ports (10/100 Mbit/s autonegotiation) and

▶ 2 uplink or HIPER Ring ports. Depending on the device model, both ports are available as a twisted-pair, multimode, singlemode or Longhaul interface.

An further important feature of the Rail Switches RS2-4R is the fast media redundancy. The failure of a transmission path will be recognized in less than 500 ms and the Rail Switch will divert data to a redundant path. You can activate this function via dip switches on any Rail Switch. This process developed by Hirschmann ensures ultimate network and system reliability. This function can also be used, for example, to expand existing networks while they are still in operation.

Rail Switches RS2-4R also contain an SNMP management agent and integrated Web-based management. This enables easy-to-handle configuration functions for a fast starting operation, and extensive network and device information also contributes to ultimate system reliability.

The 24 V operating voltage is supplied via a plug-in terminal block and can also be configured for redundancy. An additional contact in the terminal block allows you to read in device status messages directly. Integrated LED's allow fast on-site installation.

The Fast ETHERNET Rail Switches of the RS2-4R family have been developed consistenly according to industry standards which results in increased system productivity or cost savings for planning, startup and servicing operations.

2 Hardware

The Industrial ETHERNET Rail Switch RS2-4R family consists of 7 devices. These devices can be managed and have the same functionality, 2 twisted pair interfaces as well as two other model-dependent interfaces.

▶ RS2-4R
▶ RS2-4R 1MM SC
▶ RS2-4R 1SM SC
▶ RS2-4R 1LH SC
▶ RS2-4R 2MM SC
▶ RS2-4R 2SM SC
▶ RS2-4R 2LH SC

For the sake of simplicity, these 7 devices have been designated as RS2-4R in this manual.

The RS2-4R operates in store-and-forward mode. When a data packet is being received, the RS2-4R analyzes the source and destination addresses. It can store up to 1000 addresses with port allocations in its address table.
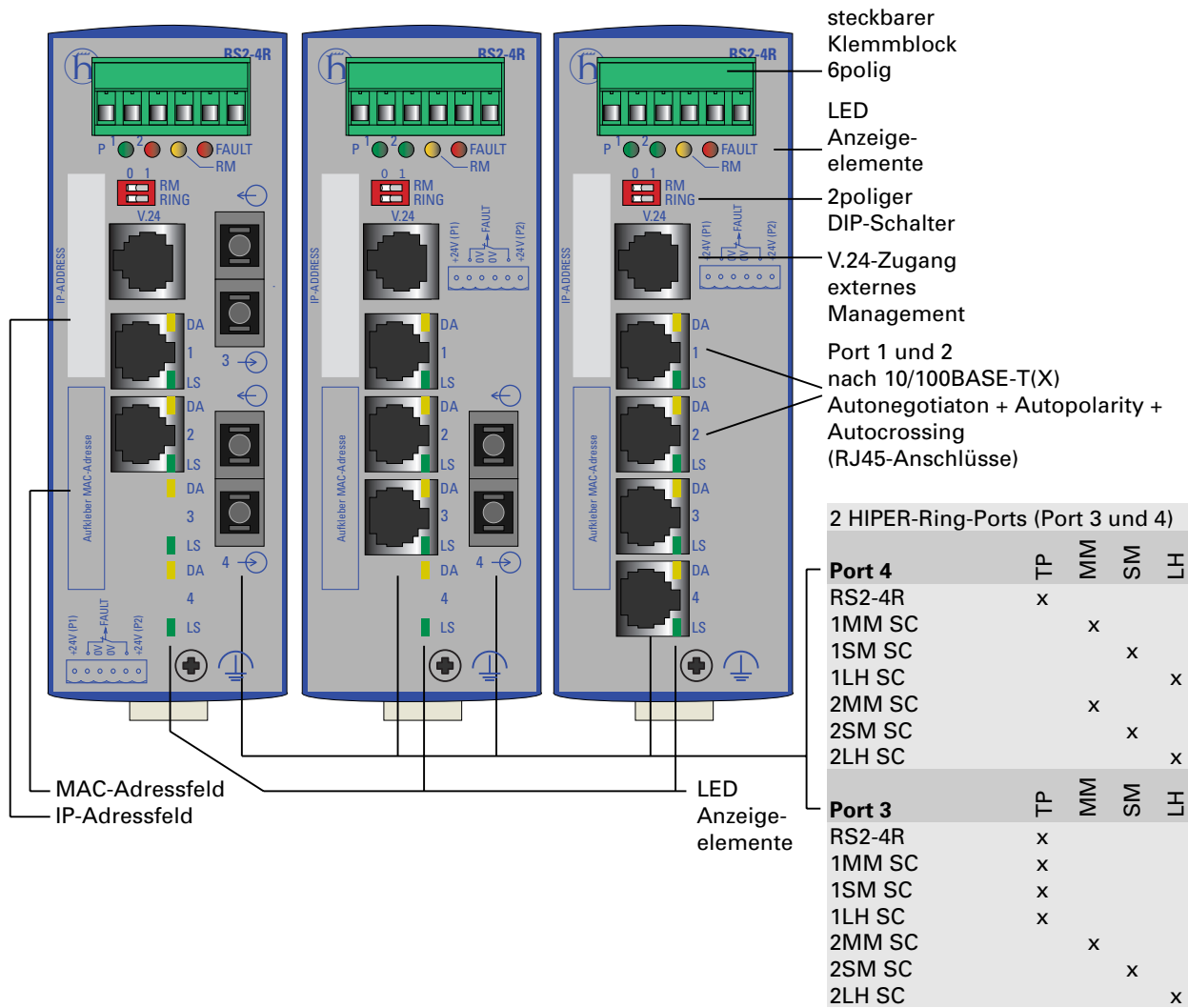
Fig. 1:   Front view of the RS2-4R

Labels (right side):

steckbarer Klemmblock 6polig

LED Anzeige-elemente

2poliger DIP-Schalter

V.24-Zugang externes Management

Port 1 und 2 nach 10/100BASE-T(X) Autonegotiaton + Autopolarity + Autocrossing (RJ45-Anschlüsse)

Labels (bottom):

MAC-Adressfeld

IP-Adressfeld

LED Anzeige-elemente

2 HIPER-Ring-Ports (Port 3 und 4)

Port 4	TP	MM	SM	LH
RS2-4R	x			
1MM SC		x		
1SM SC			x	
1LH SC				x
2MM SC		x		
2SM SC			x	
2LH SC				x

Port 3	TP	MM	SM	LH
RS2-4R	x			
1MM SC	x			
1SM SC	x			
1LH SC	x			
2MM SC		x		
2SM SC			x	
2LH SC				x

The LED's indicate data reception, connection status and processor status.

Device type	TP Ports 10/100	F/O Port multi mode 100 MBit/s	F/O Port single mode 1300 nm, 100 MBit/s	F/O Port single mode 1550 nm, 100 MBit/s
RS2-4R	1-4	–	–	–
RS2-4R 1MM SC	1-3	4	–	–
RS2-4R 1SM SC	1-3	–	4	–
RS2-4R 1LH SC	1-3	–	–	4
RS2-4R 2MM SC	1 + 2	3 + 4	–	–
RS2-4R 2SM SC	1 + 2	–	3 + 4	–
RS2-4R 2LH SC	1 + 2	–	–	3 + 4

Table 1: Device types, port assignment

The RS2-4R fulfills the testing requirements for electronic equipment in line with the Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1.

The Hirschmann "Basics Industrial ETHERNET and TCP/IP" (order no. 280 720-834) describes in detail
► how to set up a local network in compliance with ISO/IEC 8802-3 and
► provides instructions on network planning as well as on the installation of Ethernet networks.

3 Installation and startup procedure

The Industrial ETHERNET Rail Switch RS2-4R family has been developed for practical applications in a harsh industrial environment. Accordingly, the installation process has been kept simple.
The few configuration settings required for operation are described in this chapter.

3.1 Safety instructions

■ **Supply voltage**
The devices are designed for operation with a safety extra-low voltage. They may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.
The supply voltage is electrically isolated from the housing.
☐ Never start operation with damaged components!
☐ Relevant for North America:
   The subject unit is to be suppplied by a Class 2 power source complying with the requirements of the National Electrical Code, table 11(b). If power is redundant supplied (two individual power sources) the power sources together should comply with the requirements of the National Electrical Code, table 11 (b).
☐ Relevant for North America:
   Use 60/75°C or 75°C copper(CU)wire only.

■ **Shielding ground**
The shielding ground of the connectable twisted pair lines is connected to the front panel as a conductor.
☐ Beware of possible short circuits when connecting a cable section with conductive shielding braiding.

■ Housing

Only technicians authorized by Hirschmann are permitted to open the housing.

The device is grounded via the separated ground screw. It is located on the bottom of the front panel.

☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.

☐ The ventilation slits must not be covered to ensure free air circulation.

☐ The distance to the ventilation slots of the housing has to be a minimum of 10 cm.

☐ Never insert pointed objects (thin screwdrivers, wires, etc.) into the inside of the subrack! Failure to observe this point may result in injuries caused by electric shocks.

☐ The housing has to be mounted in upright position.

☐ If installed in a living area or office environment, the device must be operated exclusively in switch cabinets with fire protection characteristics according to EN 60950.

■ Environment

The device may only be operated in the listed maximum surrounding air temperature range at the listed relative air humidity range (non-condensing).

☐ The installation location is to be selected so as to ensure compliance with the climatic limits listed in the Technical Data.

☐ To be used in a Pollution Degree 2 environment only.

■ Qualification requirements for personnel

Qualified personnel as understood in this manual and the warning signs, are persons who are familiar with the setup, assembly, startup, and operation of this product and are appropriately qualified for their job. This includes, for example, those persons who have been:

▶ trained or directed or authorized to switch on and off, to ground and to label power circuits and devices or systems in accordance with current safety engineering standards;

▶ trained or directed in the care and use of appropriate safety equipment in accordance with the current standards of safety engineering;

▶ trained in providing first aid.

■ General Safety Instructions

This device is electrically operated. Adhere strictly to the safety requirements relating to voltages applied to the device as described in the operating instructions!

Failure to observe the information given in the warnings could result in serious injury and/or major damage.

☐ Only personnel that have received appropriate training should operate this device or work in its immediate vicinity. The personnel must be fully familiar with all of the warnings and maintenance measures in these operating instructions.

☐ Correct transport, storage, and assembly as well as careful operation and maintenance are essential in ensuring safe and reliable operation of this device.

☐ These products are only to be used in the manner indicated in this version of the manual.

☐ Any work that may have to be performed on the electrical installation should be performed by fully qualified technicians only.

Warning!
LED- or LASER components according to IEC 60825-1 (2001):
CLASS 1 LASER PRODUCT.
LIGHT EMITTING DIODE - CLASS 1 LED PRODUCT.

■ **National and international safety regulations**
   ☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.

■ **Note on the CE marking**
The devices comply with the regulations contained in the following European directives:

89/336/EEC
Directive of the council for standardizing the regulations of member states on electromagnetic compatibility (changed by RL 91/263/EEC, 92/31/EEC and 93/68/EEC).
In accordance with the above-named EU directives, the EU conformity declaration will be at the disposal of the relevant authorities at the following address:

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Germany
Phone ++49 7127 14 1480

The product can be used in living areas (living area, place of business, small business) and in industrial areas.

► Interference immunity: EN 61000-6-2:2001
► Emitted interference: EN 55022:1998 + A1 2000 Class A

Warning!
This is a class A device. This device can cause interference in living areas, and in this case the operator may be required to take appropriate measures.
The assembly guidelines provided in these instructions must be strictly adhered to in order to observe the EMC value limits.

■ FCC note:

Appropriate testing has established that this device fulfills the requirements of a class A digital device in line with part 15 of the FCC regulations.

These requirements are designed to provide sufficient protection against interference where the device is being used in a business environment. The device creates and uses high frequencies and can radiate same, and if it is not installed and used in accordance with this operating manual, it can cause radio transmission interference. The use of this device in a living area can also cause interference, and in this case the user is obliged to cover the costs of removing the interference.

■ Recycling note:

After usage, this product must be disposed of properly as electronic waste in accordance with the current disposal regulations of your county / state / country.

3.2 Device installation

3.2.1 Controls

■ **DIP switch**
  With the -pin DIP switch on the front panel of the RS2-4R

  ▶ the RM functionality (Redundancy Manager) can be switched on or off with the RM switch if the HIPER-Ring function is switched on. State on delivery: switch position 0 (Off), i.e. RM function not active (see "Redundant ring structure – HIPER-Ring" on page 114).

  ▶ the HIPER-Ring fuctionality can be switched on or off with the RING switch. State on delivery: switch position 0 (Off), i.e. HIPER-Ring function not active.

<div align="center">

0   1
RM   Redundanz Manager
RING HIPER-Ring

</div>
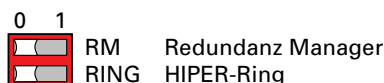
Fig. 2:   2-pin DIP switchr

RING	RM	Port 3 and Port 4	Redundancy Manager
0	-	TP port: Autonegotiation, FX port: 100 Mbit/s full duplex	off
1	0	Ring port: 100 Mbit/s full duplex	off
1	1	Ring port: 100 Mbit/s full duplex	on

Table 2: DIP switch function

☐ Check whether the switch default settings match your requirements.

3.2.2 6-pin terminal block

The supply voltage and the signal contact are connected via a 6-pin terminal block with Rast locking.

Warning!
The RS2-4R devices are designed for operation with safety extra-low voltage. Thus, they may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.

■ **Supply voltage**
The supply voltage can be connected redundantly. Both inputs are uncoupled. There is no distributed load. With redundant supply, the transformer supplies the RS2-4R alone with the higher output voltage. The supply voltage is electrically isolated from the housing.

■ **Signal contact:**
The signal contact monitors proper functioning of the RS2-4R, thus enabling remote diagnostics.
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit):

▶ The failure of at least one of the two supply voltages (supply voltage 1 or 2 < 18 V).

▶ A continuous malfunction in the RS2-4R (internal 3.3 VDC voltage).

▶ The defective link status of at least one port. With the RS2-4R, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.

▶ The loss of Redundancy guarantee.

▶ Error during self-test.

The following conditions are reported in RM mode:
▶ Ring monitoring is not possible, e.g. during software initialization.

Note: With non-redundant supply of the mains voltage, the RS2-4R reports a power failure. You can prevent this message by applying the supply voltage over the two inputs or by switching off the monitoring (see "Proper functioning" on page 139).

+24 V (P1)   0 V   0 V   +24 V (P2)

Fault
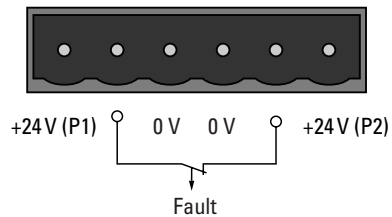
Fig. 3:   Pin assignment of the 6-pin terminal block

☐ Pull the terminal block off the RS2-4R and connect the power supply and signal lines.

3.2.3 Assembly

On delivery, the device is ready for operation.

☐ Slide the upper snap-in guide of the RS2-4R into the top-hat rail and press it down against the rail until it snaps into place.
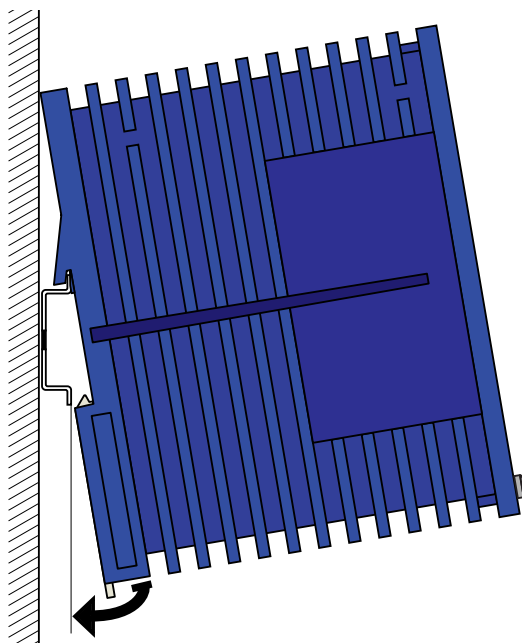
Fig. 4:   Assembly

Note: The front panel of the housing of the RS2-4R is grounded via a ground connection.

Note: The housing must not be opened.

Note: The shielding ground of the industrial connectable twisted pair lines is connected to the front panel as a conductor.

3.2.4 Interfaces

■ **10/100 Mbit/s connection**

10/100 Mbit/s ports (8-pin R45 socket) enable the connection of terminal devices or independent network segments in compliance with the IEEE 802.3 100BASE-TX / 10BASE-T standards. These ports support:
▶ autonegotiation
▶ autocrossing (when autonegotiation is switched off)
▶ autopolarity
▶ 100 Mbit/s half duplex mode
▶ 100 Mbit/s full duplex mode
▶ 10 Mbit/s half duplex mode
▶ 10 Mbit/s full duplex mode
State on delivery: autonegotiation is activated with exception of the HIPER-Ring ports: 100 Mbit/s full duplex.

The socket housings are electrically connected to the front panel.


```
n.c.   Pin 8
n.c.   Pin 7
TD-    Pin 6
n.c.   Pin 5
n.c.   Pin 4
TD+    Pin 3
RD-    Pin 2
RD+    Pin 1
```
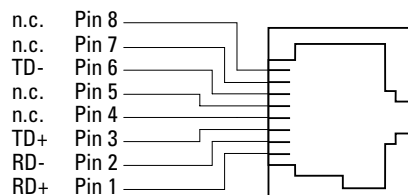
Fig. 5:   Pin assignment of a TP/TX interface, RJ45 socket

■ **100 Mbit/s F/O connection**

100 MBit/s F/O ports (DSC sockets) enable the connection of terminal devices or independent network segments in compliance with the IEEE 802.3 100BASE-FX standard. These ports support:
▶ full and half duplex mode
State on delivery: 100 Mbit/s full duplex

Note: Make sure, that you conncet LH ports only to LH ports, SM ports only to SM ports and MM ports only to MM ports.

■ V.24 interface (external management)

A serial interface is provided on the RJ11 socket (V.24 interface) for the local connection of

▶ an external management station (VT100 terminal or PC with appropriate terminal emulation). This makes it possible to establish a connection to the user interface UI (see "User Interface" on page 209).

▶ an ACA 11 AutoConfiguration Adapter.

VT-100 terminal settings:
- Speed: 9,600 baud
- Data: 8 bit
- Stopbit: 1 bit
- Handshake: off
- Parity: none

The V.24 interface can be activated with the baud rates 9,600 or 19,200. The setting at system start is 9,600 baud.
The transmission rate can be changed in the system monitor (see "3 Change Baudrate" on page 78).

The socket housing is electrically connected to the front panel of the device.
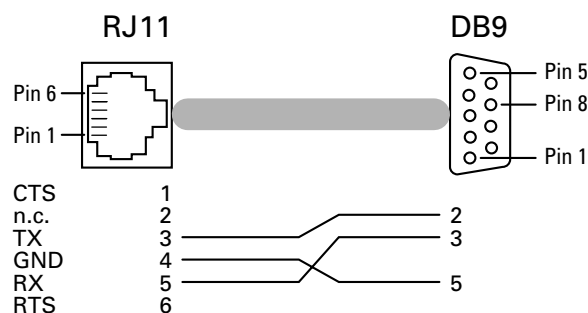
Fig. 6:   Pin assignment of the V24 interface

☐ Install the signal lines and, if necessary, the control line and terminal cable.
☐ Attach the ground cable to the ground screw.

3.2.5 Disassembly

☐ In order to remove the RS2-4R from the top-hat rail, move the screwdriver horizontally under the chassis in the locking gate, pull this down — without tilting the screwdriver — and fold the RS2-4R up.
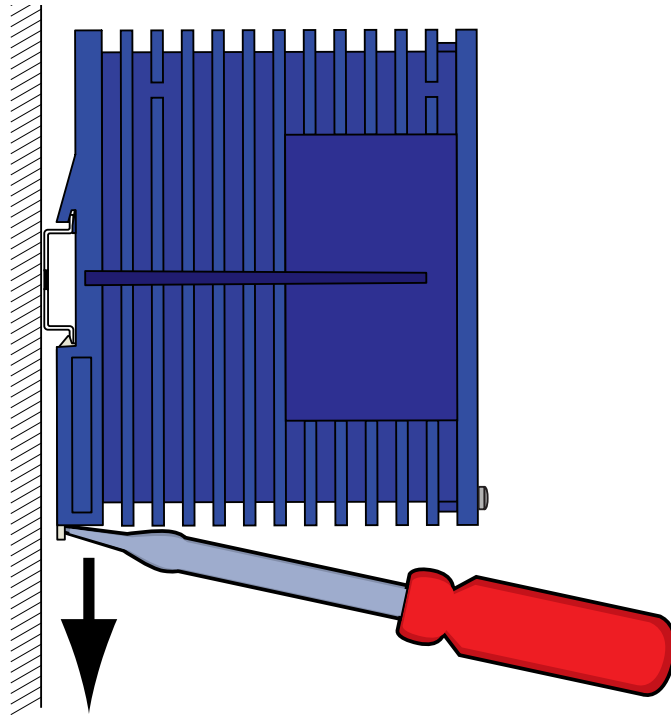
Fig. 7:   Disassembly

3.3 Startup operation

45

When the supply voltage is connected via the 6-pin terminal, start up the RS2-4R.

3.4 Basic settings

The RS2-4R is designed for ease of use and complies as far as possible with the "plug and play" principle. IP address(es) must be entered when the RS2-4R is installed for the first time.
The RS2-4R provides 6 options for configuring the IP addresses:

▶ Entry via the V.24 connection
▶ Entry by HiDiscovery protocol
▶ Configuration via BOOTP
▶ Configuration via DHCP
▶ Configuration via DHCP Option 82 and
▶ The AutoConfiguration Adapter

3.4.1 IP address (version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.
Since 1992, five classes of IP address have been defined in the RFC 1340.

Class	Network address	Host address	Address range
A	1 Byte	3 Bytes	1.0.0.0 to 126.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 to 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 3: IP address classification

The network address represents the fixed part of the IP address. The worldwide leading regulatory board for assigning Internet addresses is the IANA (Internet Assigned Numbers Authority). If you need an IP address block, contact your Internet-Service-Provider. Internet Service Providers should contact their local higher-level organization:

▶ APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region
▶ ARIN (American Registry for Internet Numbers) - Americas and Sub-Sahara Africa
▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
▶ RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

0	Net ID - 7 bits		Host ID - 24 bits	Klasse A
I	0	Net ID - 14 bits	Host ID - 16 bits	Klasse B
I I	0	Net ID - 21 bits	Host ID - 8 bit s	Klasse C
I I I	0	Multicast Group ID - 28 bits		Klasse D
I I I I		reserved for future use - 28 b its		Klasse E

Fig. 8:   Bit representation of the IP address

All IP addresses belong to class A when their first bit is a zero, i.e. the first decimal number is less than 128.
The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191.
The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

■ Network mask

Routers and gateways subdivide large networks into subnetworks. The network mask assigns the IP addresses of the individual devices to a particular subnetwork.

The division into subnetworks with the aid of the network mask is performed in much the same way as the division of the network addresses into classes A to C (net id).

In the part of the host address (host id) representing the mask, the bits are set to one. The remaining bits of the host address in the network mask are set to zero (see the following examples).
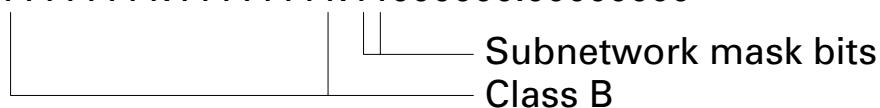
Example of a network mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000
└──────────────────────┤ └┴───── Subnetwork mask bits
                        └──────── Class B

Example of IP addresses with subnetworks assignment when the above subnet mask is applied:

Decimal notation
129.218.65.17

          └────────── 128 < 129 ≤ 191 → Class B

binary notation
10000001.11011010.01000001.00010001

                                      └── Subnetwork 1
                                          Network address

Decimal notation
129.218.129.17

          └────────── 128 < 129 ≤ 191 → Class B

binary notation
10000001.11011010.10000001.00010001

                                      └── Subnetwork 2
                                          Network address

■ **Example of how the network mask is used**

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?
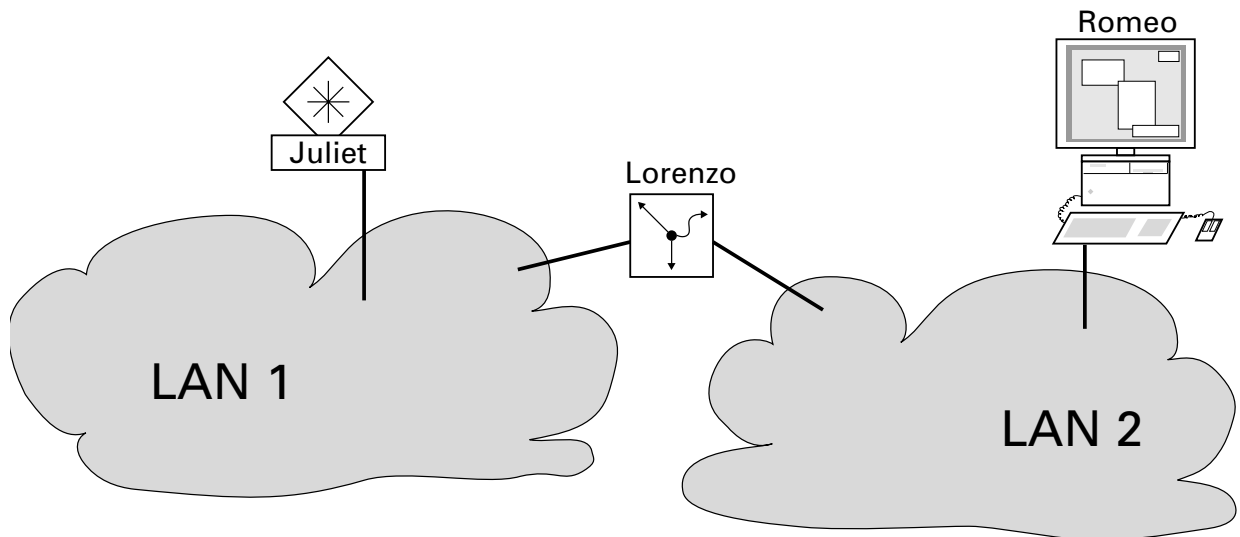
Fig. 9:   Management agent that is separated from its management station by a router

The management station "Romeo" wants to send data to the management agent "Juliet". Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable `hmNetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter then travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

3.4.2 System configuration via V.24 interface

If you do not configure the system via BOOTP, DHCP, Hidiscovery protocol or the ACA AutoConfiguration Adapter, then perform the configuration via the V.24 interface:
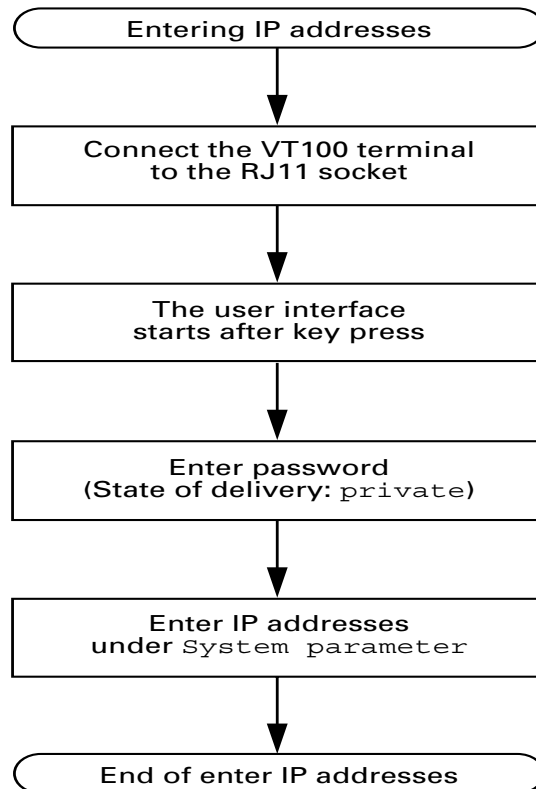
Fig. 10:   Flow chart for entering IP addresses

If there is no VT 100 terminal available in the vicinity of the installation location, the IP addresses can be entered prior to ultimate installation. A VT100 terminal or suitable emulation (e.g. MS Windows terminal) is required for this purpose.

Note: The installation of RS2-4R is easier if you enter the appropriate IP addresses for each RS2-4R at your workstation. Even if only one RS2-4R is to be installed, it may be more convenient to enter the IP addresses at your own workstation.

The RS2-4R should be labeled to prevent confusion during subsequent installation.

☐ Connect a VT 100 terminal or a PC with terminal emulation to the RJ11 socket (V.24).
  Data transfer parameters:
  Speed: 9,600 baud
  Data: 8 bit
  Parity: none
  Stopbit: 1 bit
  Handshake: off

Note: The transmission rate can be changed in the system monitor (see "3 Change Baudrate" on page 78).

☐ Once the RS2-4R has been installed, start it by connecting the power supply. The operating system is loaded.
  You start the user interface starts by pressing a key (see "Opening the user interface" on page 211).

☐ Enter the password you assigned (pay attention to lower and upper case letters) and press the enter key.

  Note: On delivery the password is set to private.

☐ Enter the IP addresses as described in "System parameters" on page 213 and in accordance with the following guidelines.

■ **Local IP address (**`local ip-address`**)**
  On delivery, the local IP address of the RS2-4R is 0.0.0.0.

■ **IP address of the gateway (**`gateway ip-address`**)**
  This entry is only needed if the and the management station/tftp server are located in different subnetworks (see "Example of how the network mask is used" on page 51).
  Enter the IP address of the gateway between the subnetwork with the and the path to the management station.
  The default setting of the IP address is 0.0.0.0.

■ **Network mask (**`netmask`**)**
   If your network has been divided up into subnetworks, and if these are
   identified with a network mask, then the network mask is to be entered
   here.
   The default setting of the network mask is 0.0.0.0.

The addresses are stored in a non-volatile memory.

After entering the IP address, you can easily configure the via the "Web-
based management" on page 119.

3.4.3 System configuration via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the switch
via the Ethernet.
You can easily configure additional parameters with the "Web-based
management" on page 119.

Install the HiDiscovery software on your PC. The software is on the CD
supplied with the switch.

☐ To install it, you start the installation program on the CD.

Note: The installation of HiDiscovery involves installing the WinPcap Version
3.0 software package.
If an earlier version of WinPcap is already installed on the PC, then you must
first uninstall it. A newer version remains intact when you install HiDiscovery.
However, this can not be guaranteed for all future versions of WinPcap. In
the event that the installation of HiDiscovery has overwritten a newer version
of WinPcap, then you uninstall WinPcap 3.0 and then re-install the new
version.

☐ Start the HiDiscovery program.
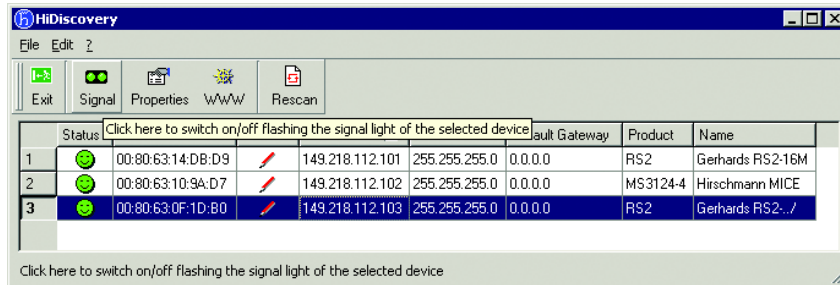
Fig. 11:   HiDiscovery

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.
HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.
☐ Select a device line.
☐ Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

By double-clicking a line, you open a window in which you can enter the device name and the IP parameter.
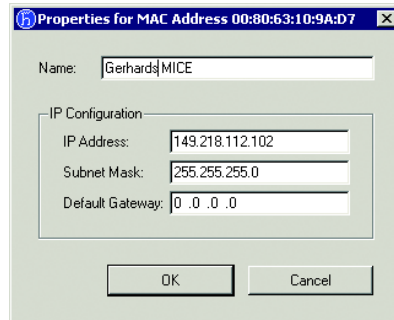
Fig. 12:   HiDiscovery - assigning IP parameters

Note: For security reasons, switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device.

3.4.4 System configuration via BOOTP (bootstrap protocol)

During startup operation the RS2-4R receives its configuration data according to the "BOOTP process" flowchart (see Fig. 13).

For the RS2-4R a BOOTP server should make available the following data:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateways
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
```

```
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:

rs2_01:ht=ethernet:ha=008063086501:ip=149.218.17.83:tc=
.global:
rs2_02:ht=ethernet:ha=008063086502:ip=149.218.17.84:tc=
.global:
.
.
```

Lines that start with a '#' character are comment lines.

The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:). The direct allocation of hardware address and IP address occurs in the device lines (rs2-0...).

☐ Enter one line for each device.
☐ After `ha=` enter the hardware address of the device.
☐ After `ip=` enter the IP address of the device.

The RS2-4R saves the configuration data received from the BOOTP server into its flash memory.

To enable/disable BOOTP, see and .

```
                        ┌──────────────────┐
                        │     Start-up     │
                        └──────────────────┘
                                 │
                                 ▼
                 ┌─────────────────────────────┐
                 │   Load boot configuration   │
                 └─────────────────────────────┘
              local │                    │ default
                    ▼                    │
         ┌──────────────────┐           │
         │ Load settings from│          │
         │   flash memory   │           │
         └──────────────────┘           │         │  Switch in initalization
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
                    │                    │
                    ▼                    │          │  Switch runs with
                    ○◄───────────────────┘          │  settings from
                    │                                   local flash
                    ▼
              ╱ DHCP  ╲      Yes    ┌──────────┐
             ╱   or    ╲──────────► │   Send   │
             ╲ BOOTP? ╱            │  DHCP/   │
              ╲      ╱             │  BOOTP   │
               No                  │ Requests │
                │                  └──────────┘
                │                        │
                │                        ▼
                │          No*   ╱ Reply from ╲  Yes   ┌──────────────────┐
                └──────────────► ╱ DHCP/BOOTP  ╲─────► │ Save IP parameter│
                          ╲  server?  ╱              │ and config file URL│
                           ╲        ╱                │     locally      │
                                │                    └──────────────────┘
                                ▼                            │
                                ○◄───────────────────────────┘
                                │
                                ▼
                 ┌─────────────────────────┐
                 │   initialize IP stack   │
                 │   with IP parameters    │
                 └─────────────────────────┘
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
                                │
                                ▼                    │  Switch is manageable
                               ( 2 )
```

Fig. 13:   Flow chart for the BOOTP/DHCP process, part 1
            * see note on page 135

```
                                    ( 2 )
                                      │
                                      ▼
          ┌───────────────────────────○───────────────────────────────┐
          │                           │                                │
          │                           ▼                                │
  ┌───────────────┐          ╱─────────────────╲                       │
  │ Start tftp    │   Yes   ╱  Load remote       ╲                      │
  │ process with  │◄────────  configuration from  │                    │
  │ config        │         ╲  URL of DHCP?       ╱                     │
  │ file URL of   │          ╲─────────────────╱                       │
  │ DHCP          │                   │ No                              │
  └───────────────┘                   │                                │
          │                           ▼                                │
          ▼                  ╱─────────────────╲       ┌───────────────────┐
  ╱───────────────╲          ╱  Load remote-    ╲  Yes │ Start tftp process│
  ╱     tftp       ╲         │  configuration?   ├─────►│ with config file  │
  ╲  successful?   ╱         ╲                   ╱      │ URL of            │
  ╲───────────────╱          ╲─────────────────╱       │ local configuration│
 No*        │                       │ No              └───────────────────┘
            │ Yes                    │                           │
            ▼                        │                           ▼
  ┌───────────────┐                  │                  ╱─────────────────╲
  │ Load transferred│                │                  ╱      tftp        ╲
  │ config file   │                  │                  ╲  successful?     ╱  No*
  └───────────────┘                  │                  ╲─────────────────╱
            │                        │                          │ Yes
            ▼                        │                          ▼
  ┌───────────────┐                  │                  ┌───────────────┐
  │ Save transferred│                │                  │ Load transferred│
  │ config file local│               │                  │ config file   │
  │ and set       │                  │                  └───────────────┘
  │ boot configuration│              │                          │
  │ to local      │                  │                          │
  └───────────────┘                  │                          │
          │                          ▼                          │
          └──────────────────────────○──────────────────────────┘
                                      │
                                      ▼
                             ╭─────────────────╮
                             │ Loading of      │
                             │ configurations data│
                             │ is complete     │
                             ╰─────────────────╯
```
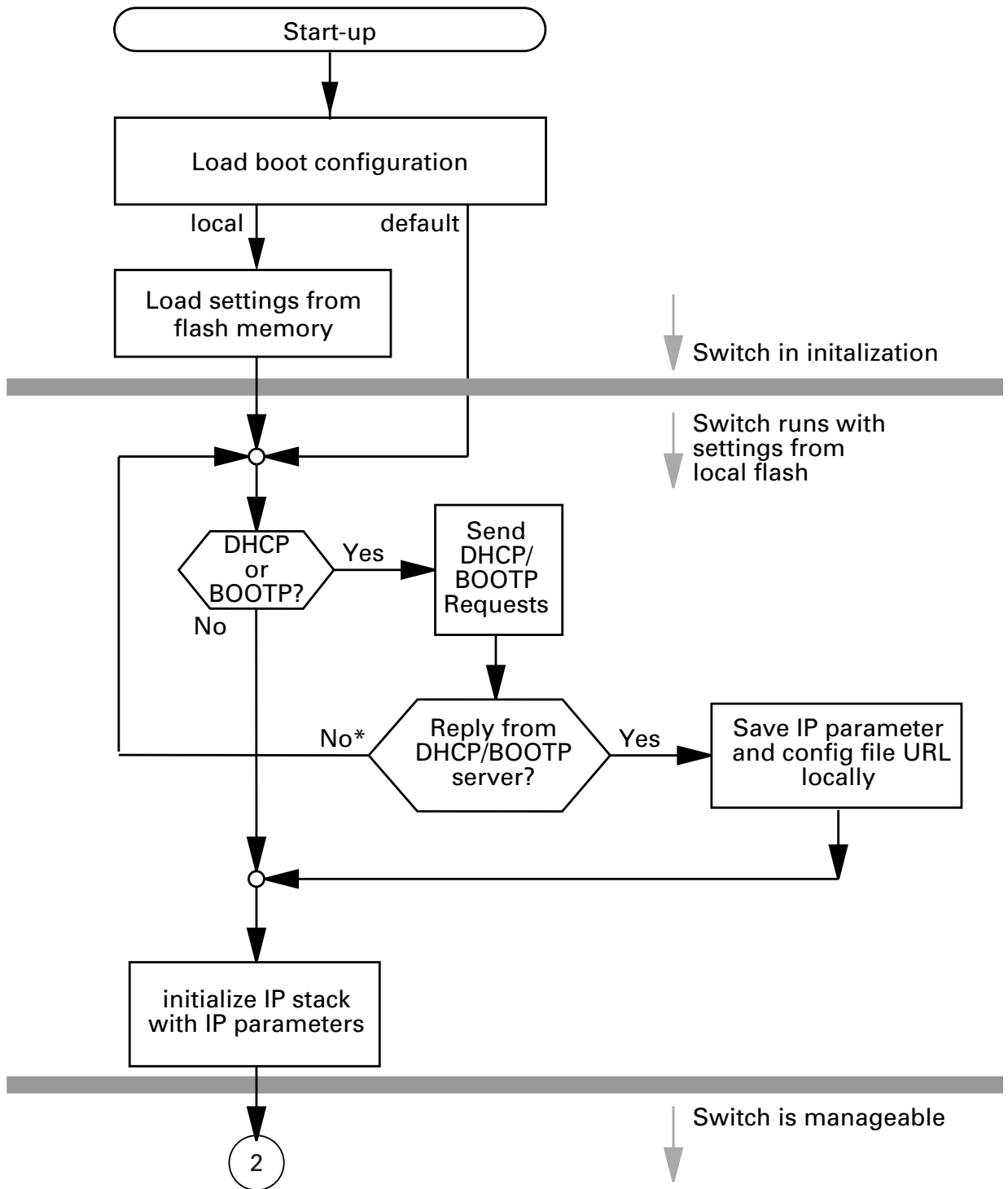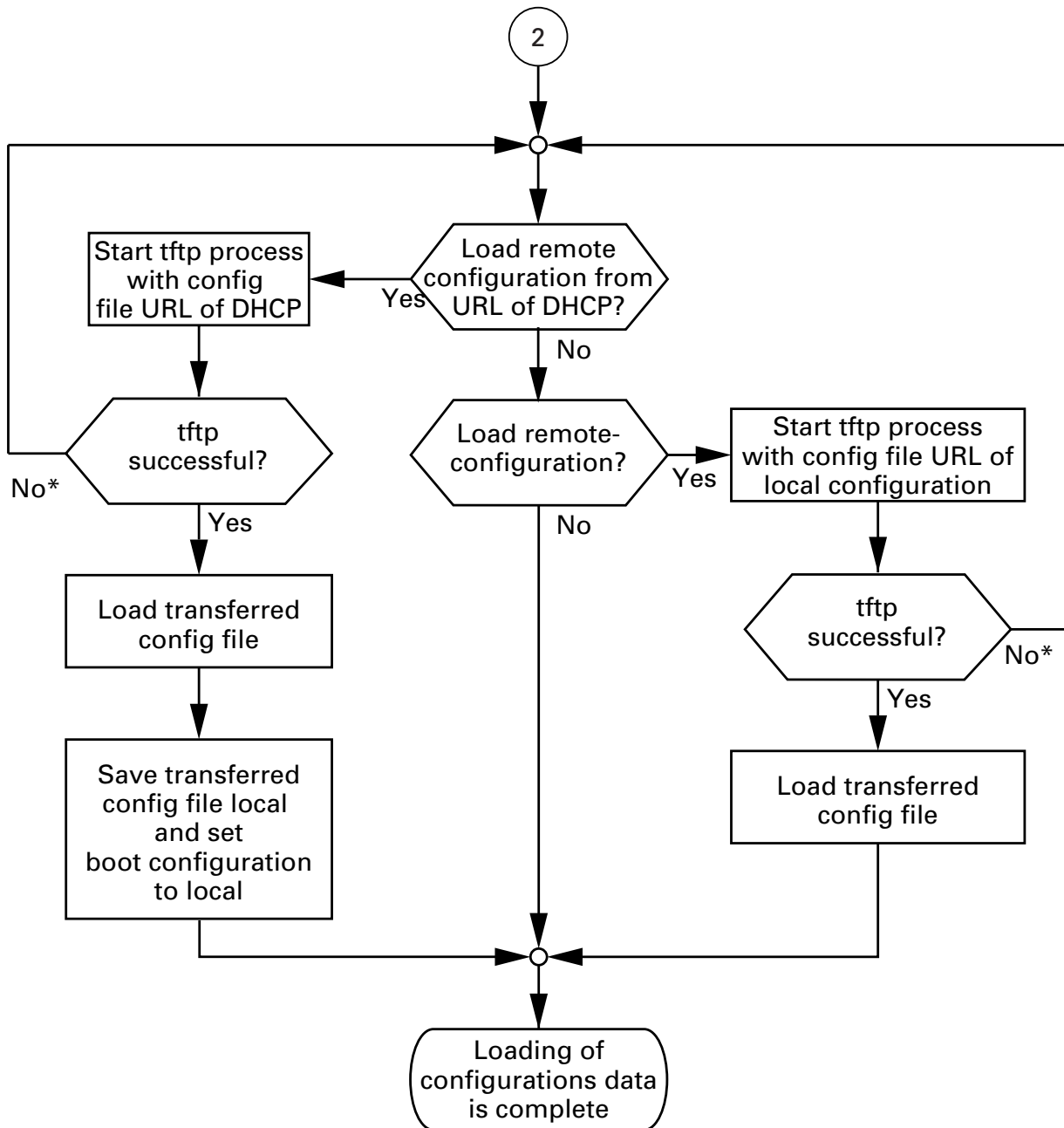
Fig. 14:   Flow chart for the BOOTP/DHCP process, part 2
*   * see note on page 135*

3.4.5 System configuration via DHCP (dynamic host configuration protocol)

The DHCP responds similarly to the BOOTP and offers in addition the configuration of a DHCP client with a name instead of the MAC address. For the DHCP, this name is known as the "client identifier" in accordance with rfc 2131.
The RS2-4R uses the name entered under `sysName` in the system group of the MIB II as the client identifier (see page 179). You can enter this system name directly via SNMP, the Web-based management (see "System data" on page 130), or the user interface (see "System parameters" on page 213).

On startup, an RS2-4R receives its configuration data according to the "BOOTP/DHCP process" flow chart (see Fig. 13).

The RS2-4R sends its system name to the DHCP server. The DHCP server can then assign an IP address as an alternative to the MAC address by using the system name.
In addition to the IP address, the DHCP server sends
– the tftp server name (if present),
– the name of the configuration file (if present).
The RS2-4R accepts this data as configuration parameters (see "Configure the network" on page 144).
If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
66	TFTP Server Name
67	Bootfile name

Table 4: DHCP options which the switch requests

The special feature of DHCP in contrast to BOOTP is that the server can only provide the configuration parameters for a certain period of time ("lease"). When this time period ("lease duration") expires, the DHCP client must attempt to renew the lease or negotiate a new one. A response similar to BOOTP can be set on the server (i.e. the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address – whichever one happens to be available – is assigned.

As long as DHCP is activated, the RS2-4R attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address. To activate/deactivate DHCP, see .

Note: When using HiVision network management, ensure that DHCP always assigns the original IP address to each RS2-4R.

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
  option subnet-mask 255.255.240.0;
  option routers 149.218.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
  hardware ethernet 00:80:63:08:65:42;
  fixed-address 149.218.112,82;
  }
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
# option dhcp-client-identifier "hugo";
  option dhcp-client-identifier 00:68:75:67:6f;
```

```
fixed-address 149.218.112.83;
server-name "149.218.112.11";
filename "/agent/config.dat";
}
```

Lines that start with a '#' character are comment lines.
The lines preceding the individually listed devices refer to settings that apply to all the following devices.
The `fixed-address` line assigns a permanent IP address to the device.
For further information, please refer to the DHCP server manual.

3.4.6 System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the "BOOTP/DHCP process" flow chart (see Fig. 13).

While the system configuration is based on the classic DHCP protocol on the device being configured (see "System configuration via DHCP (dynamic host configuration protocol)" on page 61), Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a switch) on the LAN.

The installation of a DHCP server is described in the chapter "Setting up DHCP Server Option 82" on page 233.
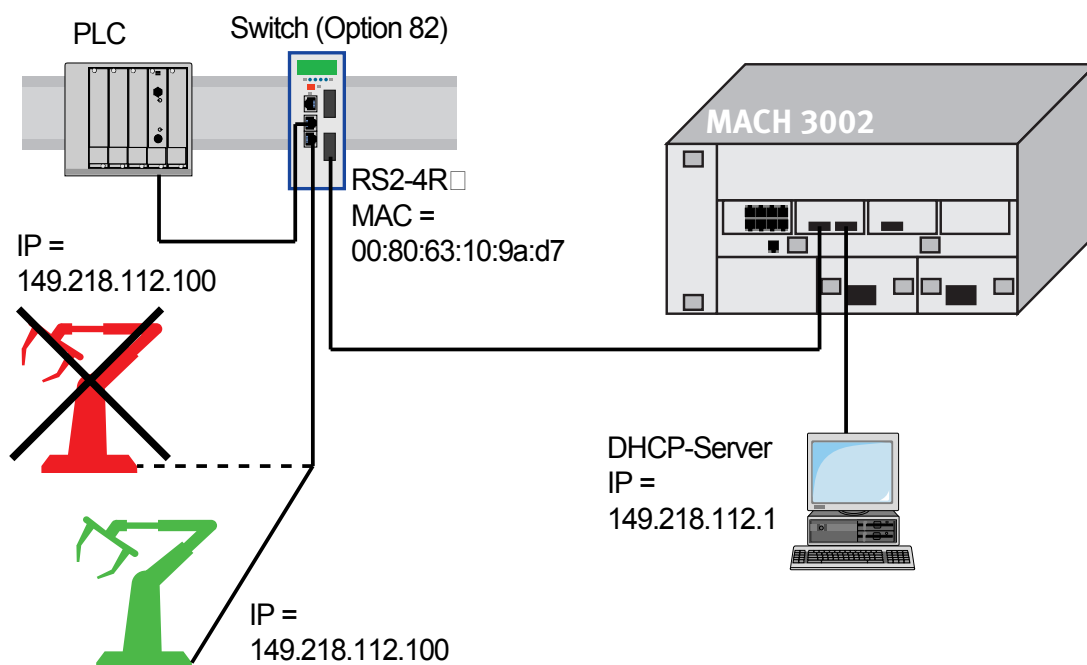
Fig. 15: Application example of using Option 82

3.4.7 ACA AutoConfiguration Adapter

The ACA is a device for storing the configuration data of a MICE, RS2-4R, RS2-16M, RS2-../.., or MACH 3000 switch. In the case of a switch failure, the ACA enables a very simple configuration data transfer by means of a substitute switch of the same type.

You can transfer the current switch configuration onto the ACA and the flash memory with "Save local configuration".

When you restart, the switch assumes the configuration data of the ACA and save them permanently into the flash memory. Which data the switch takes from the ACA depends on the setting in the restart configuration (see "Defining the start configuration" on page 135).

Setting	Result
Local	The switch takes all the data from the ACA
from URL	The switch takes the IP parameters from the ACA and the other data from the URL
defaults	The switch takes the IP parameters from the ACA and the other parameters from the default settings

Table 5: Data transfer from the ACA after restarting

You will find further information on operating the ACA in chapters "Update" on page 223 and "Defining the start configuration" on page 135.

3.5 tftp server for software updates

On delivery, the switch software is held in the flash memory. The RS2-4R boots the software from the flash memory.

Software updates can be realized via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

Note: An alternative to the tftp update is the http update. The http update saves you having to configure the tftp server.

The RS2-4R requires the following information to be able to make a software update from the tftp server:
▶ its own IP address (entered permanently),
▶ the IP address of the tftp server or gateway to the tftp server,
▶ the path in which the operating system of the tftp server is kept (see "Update" on page 223)

File transfer between RS2-4R and tftp server is handled by way of the **T**rivial **F**ile **T**ransfer **P**rotocol (tftp).

Management station and tftp server may be made up of one or more computers.

Preparation of the tftp server for the RS2-4R software involves the following steps:

▶ Setting-up the RS2-4R directories and copying the RS2-4R software

▶ Setting-up the tftp process

3.5.1 Setting up the tftp process

General prerequisites:

▶ The local address of the RS2-4R and the IP address of the tftp servers or the gateway are known to the RS2-4R.
▶ The TCP/IP stack with tftp is installed on tftp server.

The following sections contain information on setting up the tftp process, arranged according to operating system and application.

■ **SunOS and HP**
  ☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see fig. 16) and whether the status of this process is "IW":

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd
-s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not in the file, or if the related line is commented out (#), modify /etc/inetd.conf accordingly and then re-initialize the INET daemon. This is done with the command "kill -1 PID", where PID is the process ID of inetd.
This re-initialization can be executed automatically by inputting the following UNIX commands:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command "`man tftpd`".

Note: The command "`ps`" does not always show the tftp daemon, although it is actually running.

Special steps for HP workstations:
☐ During installation on an HP workstation, enter the user tftp in the `/etc/passwd` file.
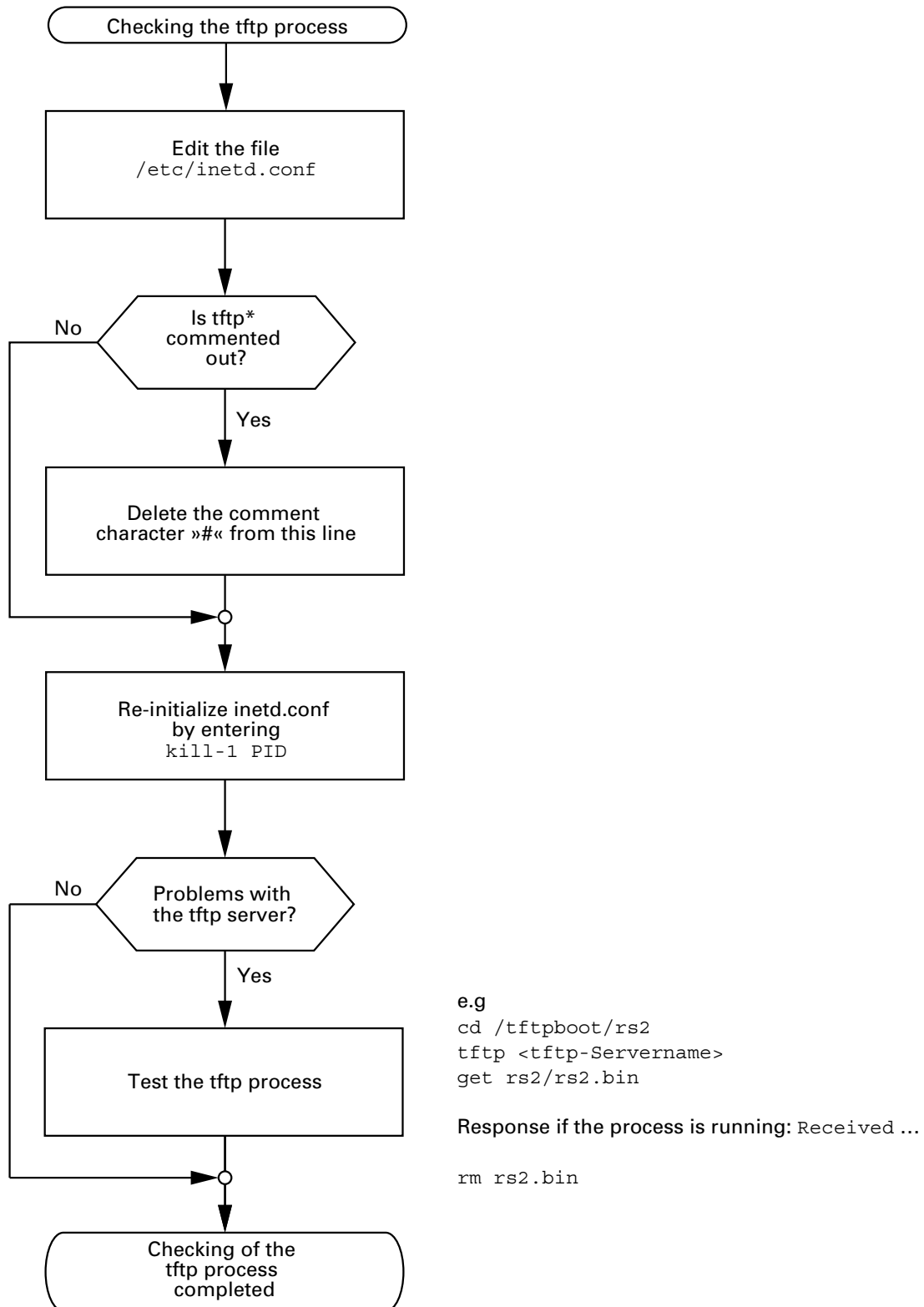
For example:

tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false

```
tftp        user ID,
*           is in the password field,
510         sample user ID,
20          sample group ID,
tftp serverfreely selectable designation,
/bin/falsemandatory entry (login shell)
```

☐ Test the tftp process with, for example:
```
cd /tftpboot/rs2
tftp <tftp-Servername>
get rs2/rs2.bin
rm .bin
```

```
e.g
cd /tftpboot/rs2
tftp <tftp-Servername>
get rs2/rs2.bin
```

Response if the process is running: `Received ...`

```
rm rs2.bin
```

* `tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot`

Fig. 16:   Flow chart for setting up tftp server with SunOS and HP

3.5.2 Software access rights

The agent needs read permission to the tftp directory with the RS2-4R software.

■ **Example of a UNIX tftp server**
  Once RS2-4R software has been installed, the tftp server should have the following directory structure with the stated access rights:

Filename	Access
rs2.bin	444-r--r--r--

Table 6: Directory structure of the software

  d = directory; r = read; w = write; x = execute
  1st position designates d (directory),
  2nd to 4th positions designate user access rights,
  5th to 7th positions designate access rights of user groups,
  8th to 10th positions designate access rights of all others.

3.6 System monitors

The system monitors facilitate the implementation of an

▶ update of the operating system

The software update can be implemented via V.24 or tftp.

The V.24 connection of the RS2-4R supports the baud rates 9,600 and 19,200.

3.6.1 Update of the operating system (system monitor 1)

System monitor 1 facilitates an update of the operating system of the RS2-4R via the V.24 connection.

The corresponding screen display shows the options

▶ 1   Update Operating System

▶ 2   Start Operating System

▶ 3   Change Baudrate

▶ 4   End

Note: Preferably use system monitor 2 to update the operating system.

If you boot RS2-4R with 9,600 baud, then the message "Press <1> to enter Monitor 1" appears on the terminal.

```
   8  MByte SDRAM detected.
   2  MByte FlashROM detected.


   Press <1> to enter Monitor                      1
```

Fig. 17: Screen display during the boot phase

Press the <1> key within one second to start system monitor 1.

```
    System-Monitor 1  V1.00  27.02.2002


   1  Update Operating System
   2  Start  Operating System
   3  Change Baudrate
   4  End








>
```

Fig. 18:   System monitor 1 screen display

■ 1 Update Operating System
This menu allows you to update the operating system.
The following window appears on the screen:

```
         Update Operating System with XMODEM


Maximal buffer size : 2031616 Bytes


 <RETURN> start the XMODEM
 <ESC> end
```

Fig. 19:   Update operating system screen display

To leave this screen and return to the main menu of system monitor 1, press the <ESC> key.

Press <RETURN>, to start the update with XMODEM. The following window appears on the screen:

```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second
```

Fig. 20:   Screen display when you start an update of the OS

Afterwards enter the name of the path in which the operating system to be loaded is located. Enter the path name via the terminal program, e.g. under Transmission: binary file. The transmission starts. When the transmission has finished the operating system is restarted.

■ 2 Start Operating System
Enter the number "2" to start the operating system.
System monitor 1 is shut down. The operating system will be started with 9,600 baud.

■ **3 Change Baudrate**
With this menu you can modify the baud rate.
The following window appears on the screen:

```
   Change Baudrate


   1     9600 baud
   2     19200 baud








 >
```

Fig. 21:   Screen display for changing baudrate

For an update of your operating system (see menu 1) you should choose
the maximum speed for the baud rate.
Afterwards adapt the speed of your terminal program to this baud rate.

■ 4 End

This menu shuts down system monitor 1.
The following window appears on the screen:

```
Systemreset !




















```
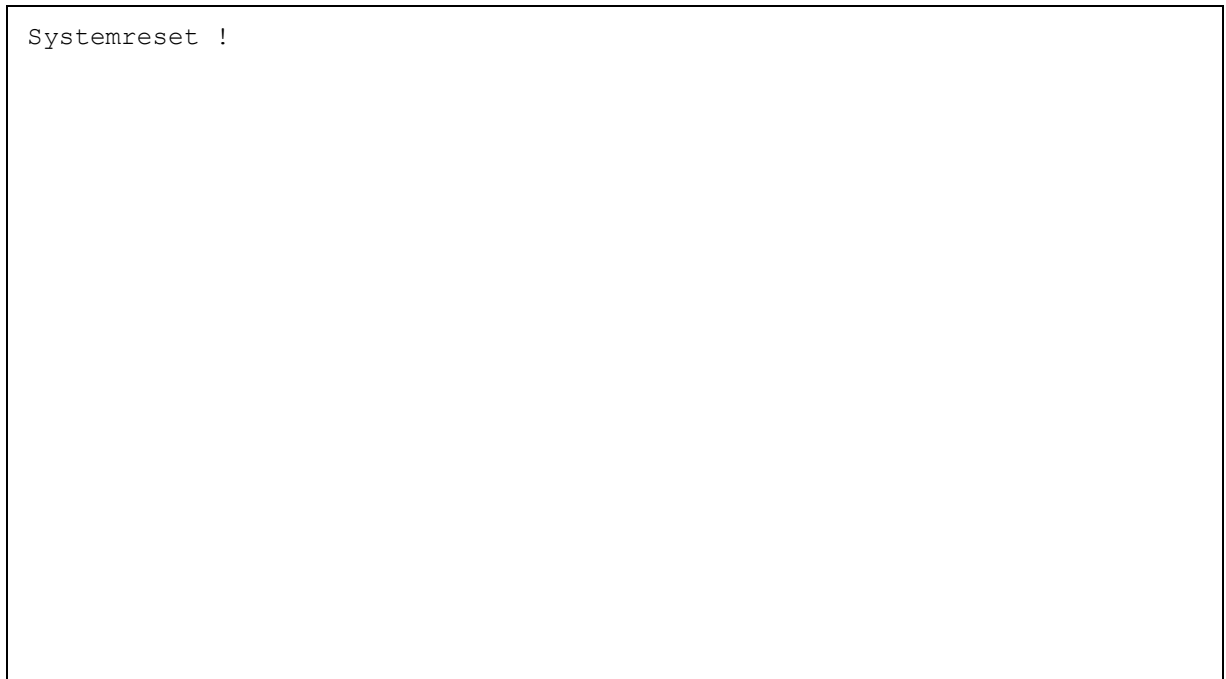
Fig. 22:   Screen display for shutting down system monitor 1

Afterwards execute hardware reset.

3.6.2 Software update (system monitor 2)

System monitor 2 facilitates an update of the RS2-4R operating system via V.24 as well as tftp.
The corresponding screen display shows the options

▶ 1   Software Update V24

▶ 2   Software Update tftp

▶ 3   Cancel Automatic Update

▶ 4   Change Baudrate

▶ 5   Set Factory Settings

▶ 6   Reset

▶ 7   End/Quit

If you boot the RS2-4R with 9,600 baud, then the following window appears on the screen:

```
     Press <2> to enter System-Monitor 2          2
```
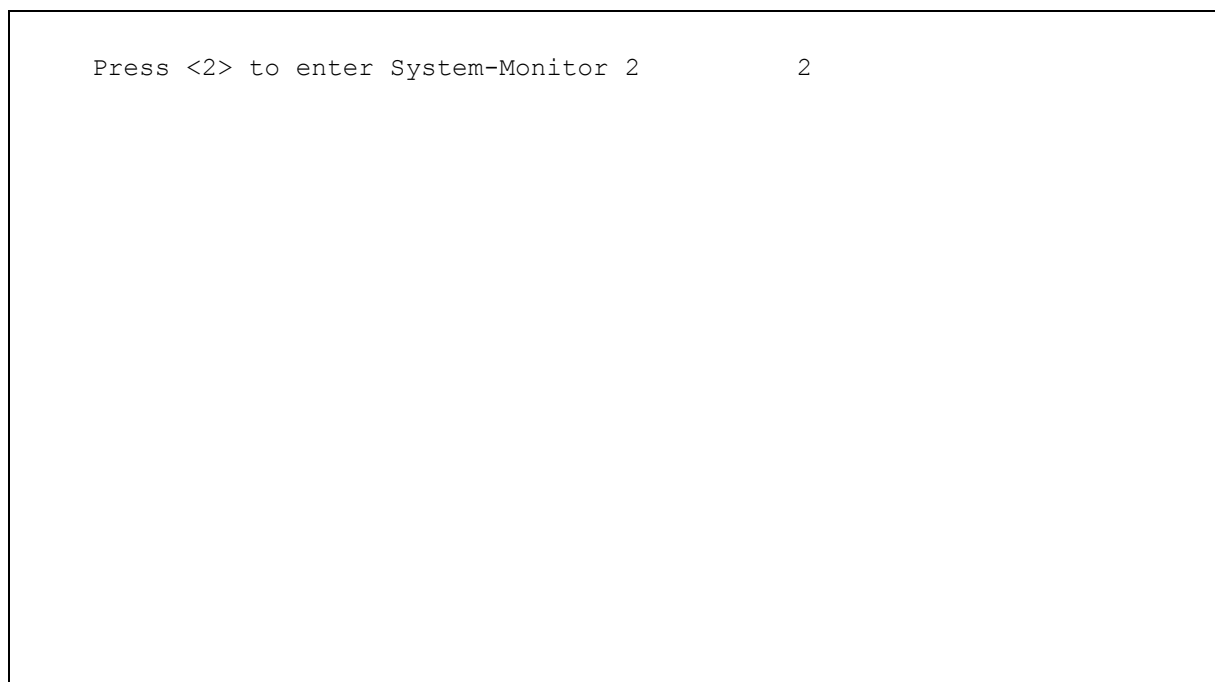
Fig. 23:   Screen display for starting system monitor 2

Press the <2> key within three seconds. System monitor 2 is started.

```
        System-Monitor 2  V1.00  27.02.2002


        1  Software Update V24
        2  Software Update TFTP
        3  Cancel automatic update
        4  Change Baudrate
        5  Set Factory Settings
        6  Reset
        7  End/Quit




        >
```

Fig. 24:   System monitor 2 screen display

■ **1 Software Update V24**
This menu executes an update of the operation system in the flash memory of the RS2-4R. The update runs via V.24.

Note: Preferably use tftp transfer to update the operation system (see "Update" on page 223). It is more than three times faster than the fastest V.24 transfer.

The following window appears on the screen:

```
            Update Operating System with XMODEM


 Maximal buffer size : 1616933 Bytes


  <RETURN> start the XMODEM
  <ESC> end
```

Fig. 25:   Update operating system screen display

To leave this screen and return to the main menu of system monitor 2, press the <ESC> key.

Press <RETURN> to start the update with XMODEM. The following window appears on the screen:

```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second
```

Fig. 26:   Screen display when you start an update of the OS

Afterwards enter the name of the path in which the operating system to be loaded is located. Enter the path name via the terminal program, e.g. under Transmission: binary file. The transmission starts. When the transmission has finished the operating system is restarted.

■ **2 Software Update tftp**
This menu executes an update of the operating system in the flash memory of the RS2-4R. The update runs via tftp.

■ **3 Cancel Automatic Update**
This menu terminates the automatic software update.

■ **4 Change Baudrate**
With this menu you can modify the baud rate.

■ **5 Set Factory Setting**
With this menu item you can restore the original settings.

■ **6 Reset**
The device performs a reset.

■ **7 End/Quit**
With this menu item you can terminate the system monitor 2.
The management software is started.

4 Functions

The devices of the Industrial ETHERNET Rail Switch RS2-4R series contain a wide variety of functions:

▶ Displays
▶ Hardware functions
▶ Frame switching
▶ Spanning Tree Algorithm
▶ Redundancy
▶ Management
▶ SNMP traps

There are three tools for operating these functions:

▶ User Interface (supplied with RS2-4R)
for setting basic functions (see "User Interface" on page 209).

▶ Web-based Management (supplied with RS2-4R)
for easy configuration of the agent (see "Web-based management" on page 119).

▶ HiVision Network Management
for easy configuration of all agents.

4.1 Displays

4.1.1 Device status

These LED's provide information about conditions which affect the operation of the whole RS2-4R.

■ P1 - Power 1 (green LED)

Display	Meaning
lit	supply voltage 1 is on
not lit	supply voltage 1 is less than 18 V

■ P2 - Power 2 (green LED)

Display	Meaning
lit	supply voltage 2 is on
not lit	supply voltage 2 is less than 18 V

■ RM - Redundancy Manager / ACA - AutoConfiguration Adapter (Green/yellow LED)

Display	Meaning
not lit	RM function inactive
lit green	RM function active, redundant port not active
lit yellow	RM function active, redundant port active
flashes green 2 times a second	loading configuration from the ACA.
flashes yellow 2 times a second	saving configuration from the ACA.
flashes green/yellow 2 times a second	error during save operation.
flashes 1 time a second	HIPER-Ring configuration error, i.e. no RM or several RMs active.

■ FAULT - Error (red LED)

Display	Meaning
lit	the signal contact is open, i.e. it reports an error.
not lit	the signal contact is closed, i.e. it does not report an error.

If the "Manual setting" on page 139 is active for the signal contact, the error display is then independent of the position of the signal contact.

4.1.2 Port status

These LED's display port-related information.

■ 1 to 4 - Data, DA (yellow LED)

Display	Meaning
not lit	no data traffic
flashes yellow	data traffic
flashing light in sequence	Initialization phase after restarting

■ 1 to 4 - Link status, LS (green/yellow LED)

Display	Meaning
not lit	no valid link
lit green	valid link
flashes green (once a period)	port is switched off by the RM (port 3 if the RM is active)
flashes green (three times a period)	port is switched off
flashing light in sequence	Initialization phase after restarting

4.2 Hardware functions

4.2.1 Diagnostics

When restarting, the RS2-4R performs a hardware self-diagnosis.
During operation, an integrated watchdog (monitoring unit) monitors the function of the software.

4.2.2 Autonegotiation

Autonegotiation is a procedure in which the switch automatically selects the operating mode of its 10/100 RJ-45 ports. When a connection is set up for the first time, the switch detects the speed (10 or 100 Mbit/s) and the transmission mode of the connected network (half duplex or full duplex). The automatic setting of the ports eliminates the need for manual intervention on the part of the user. The autonegotiation function is activated/deactivated by the web-based management, the user interface or SNMP.

Note: If the autonegotiation function is active for only one of both transmission partners, data transmission is halfduplex. The transmission partner determines the transmission rate without autonegotiation.

4.2.3 Autopolarity exchange

If the receive-line pair of a twisted pair cable is incorrectly connected (RD+ and RD- are reversed), polarity is reversed automatically.

4.2.4 Autocrossing

If the autonegotiation function is active, the RS2-4R detects the transmit and receive pairs (MDI, MDI-X). The RS2-4R automatically configures its port for the correct transmit and receive pins. Consequently it does not matter whether you connect devices using a cross-over or straight cable.

4.2.5 Line monitoring

■ **Twisted pair**
Using regular link-test pulses in accordance with the IEEE 802.3 10BASE-T/100BASE-TX standard, the RS2-4R monitors the connected TP line segments for short circuiting or interruptions. The RS2-4R does not send any data to a TP segment from which it does not receive a link-test pulse.

Note: An unassigned interface is interpreted as a line interruption. The TP line to a deactivated terminal device is also interpreted as a line interruption, since the connected device is unable to send link-test pulses.

■ **F/O**
   A RS2-4R monitors the connected fiber optic lines for breaks in accordance with the IEEE 802.3 100BASE-FX standard.

If a line interruption occurs the switch sends a trap to the management station. The sending of such a trap can be stopped by the management.

4.2.6 Reset

The RS2-4R is reset by the following events:

▶ Management
▶ Insufficient level of both input voltages
▶ internal supply voltage falls below the threshold value,
▶ Watchdog

The following actions are carried out after a reset:

▶ Self-diagnosis
▶ Initialization

4.3 Frame switching

4.3.1 Store-and-forward

All data received by a RS2-4R is stored, and its validity is checked. Invalid and defective data packets (> 1,522 Bytes or CRC errors) as well as fragments (< 64 Bytes) are discarded. Valid data packets are forwarded by a RS2-4R.

4.3.2 Multi-address capability

A RS2-4R learns all the source addresses for a port. Only packets with
- ▶ unknown addresses
- ▶ these addresses or
- ▶ a multi/broadcast address

in the destination address field are sent to this port.

An RS2-4R can learn up to 1000 addresses. This becomes necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to a RS2-4R.

4.3.3 Learning addresses

A RS2-4R monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time) are deleted by the RS2-4R from its address table.
The RS2-4R floods data packets with an unknown target address.
The RS2-4R transmits data pakets with known target addresses to specific destinations.

Note: A reboot deletes the learned address entries.

4.3.4 Prioritization

The RS2-4R supports two priority queues (traffic classes in compliance with IEEE 802.1D-1998). The received data packets are assigned to these classes by the priority of the data packet contained in the VLAN tag.

▶ Data packets with the priority field value 0-3 are forwarded with low priority.
▶ Data packets with the priority field value 4-7 are forwarded with high priority.
▶ All data packets with a VLAN tag are forwarded corresponding to the entered priority.

This function prevents high priority data traffic being disrupted by other traffic during busy periods. The lower priority traffic will be discarded when the memory or transmission channel is overloaded.

The RS2-4R offers for handling the priority classes:

▶ Strict priority.

■ **Strict priority**
  With Strict priority, the RS2-4R sends all data packets with a higher pri-
  ority level before it sends a data packet with the next lower priority level.
  Thus RS2-4R does not send a data packet with the next lower priority
  until there are no other data packets waiting in the queue.

4.3.5 Tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and prior-
itization functions in accordance with the IEEE 802.1 Q standard. The VLAN
tag consists of 4 Bytes. It is inserted between the source address field and
the type field.

With data packets with VLAN tag, the RS2-4R evaluates
▶   the priority information at all times, and
▶   the VLAN information, if VLANs have been set up.

Data packets whose VLAN tags contain priority information but no VLAN in-
formation (VLAN ID = 0) are known as "Priority Tagged Frames".
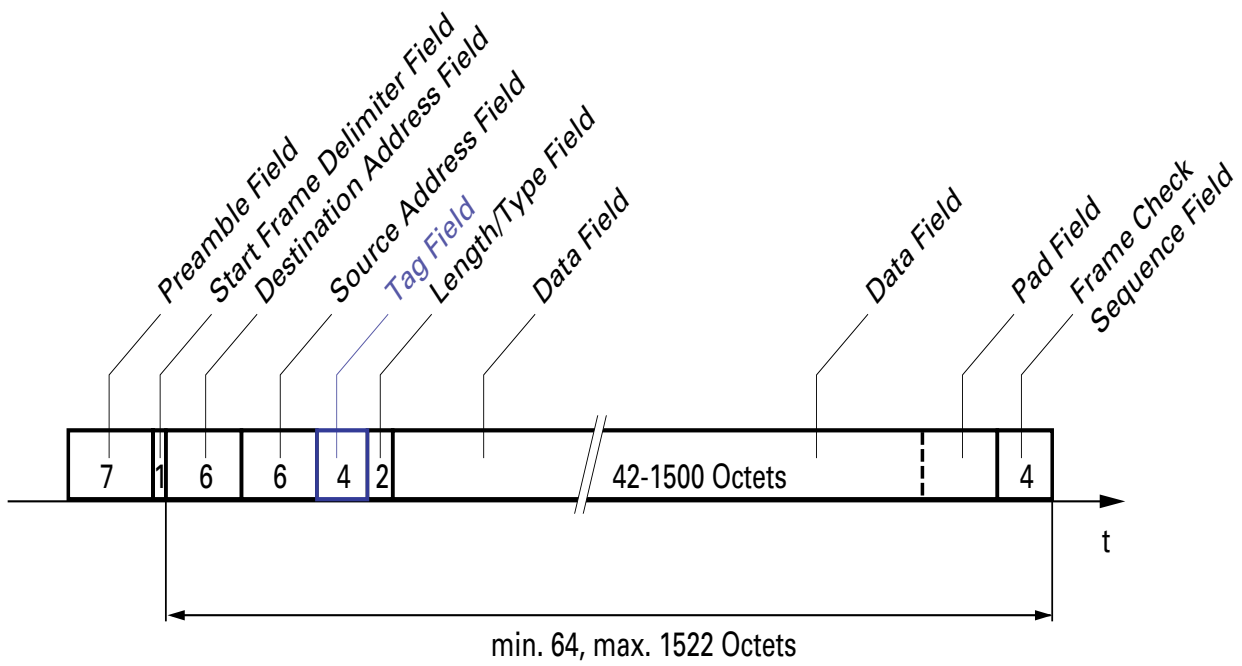
Fig. 27:   Ethernet data packet with tag
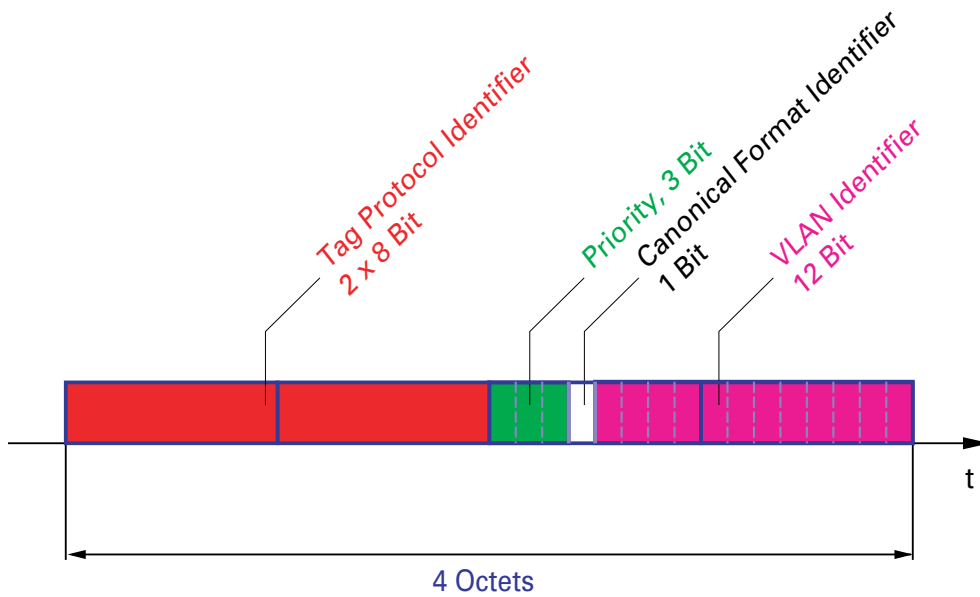
Fig. 28:   Tag-Format

4.3.6 Flow control

Flow control is a mechanism which acts as an overload protection. During periods of heavy traffic it holds off additional traffic.

In the example (see Fig. 29) the functioning of flow control is displayed graphically. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 is larger than the bandwidth of Workstation 4 to the switch. This leads to an overflow of the send queue of Port 4. The left-hand funnel symbolizes this status.

If the flow control function at Ports 1, 2 and 3 of the switch is turned on, the switch reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the conected devices that no data may be received at present.
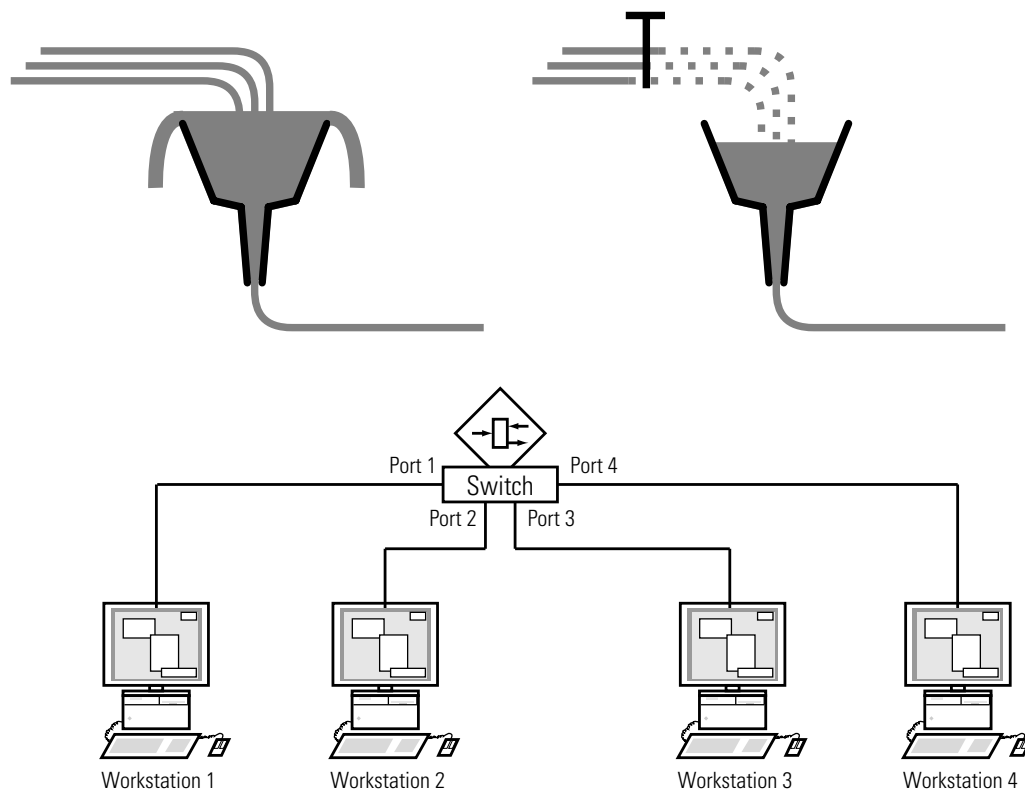
Fig. 29:   Example of flow control

■ **Flow control with a full duplex link**
In the example (see Fig. 29) there is a full duplex link between Work-station 2 and the switch.
Before the send queue of Port 4 overflows, the switch sends a request to Workstation 2 to include a small break in the sending transmission.

■ **Flow control with a half duplex link**
In the example (see Fig. 29) there is a half duplex link between Work-station 2 and the switch.
Before the send queue of Port 4 overflows, the switch sends data so that workstation 2 detects a collision and thus interrupts the transmission.

4.3.7 Port mirroring

In port mirroring, the data traffic related to a port, the source port, is copied
to another port, the destination port. Data traffic at the source port is not in-
fluenced by port mirroring (see "Setting port mirroring" auf Seite 170).
A management tool connected to the destination port, such as an RMON
probe, can thus observe the data traffic at the source port.
The destination port forwards data to be sent and blocks received data.
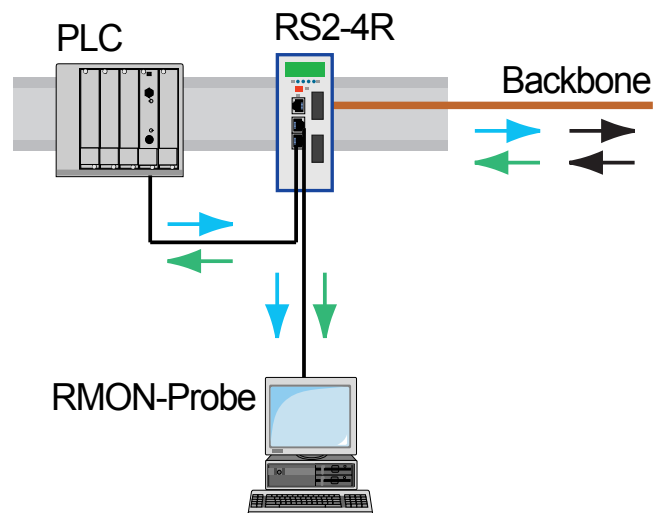
Fig. 30:   Portmirroring

4.3.8 Broadcast limiter

To guarantee reliable data exchange during high broadcast traffic, the switch can limit broadcast traffic.

By entering a number for each port, you can set the number of broadcasts that can be sent out of this port within a second.

If more than the maximum entered number of broadcasts are sent within a second, the switch rejects all subsequent broadcasts destined for this port.

A global setting activates/deactivates the broadcast limiter function at all ports.

4.4 Spanning Tree Algorithm

Local area networks are becoming ever larger. This is true both for their geographic size as well as for the number of stations they include. As the networks become larger, there are reasons why it often makes sense to implement several bridges:

▶ reduce network load in subnetworks
▶ create redundant connections and
▶ overcome distance limitations

Using many bridges with multiple connections between the subnetworks can lead to considerable problems, possibly even to total network failure if the bridges are configured incorrectly. The Spanning Tree Algorithm described in IEEE 802.1D was developed to prevent this.

Note: The standard demands that all bridges of a mesh have to work with the Spanning Tree Algorithm.

4.4.1 Tasks

The Spanning Tree Algorithm reduces the topology of any network that is connected using bridges to a single tree structure. The root bridge forms the origin of the tree structure. Any loops that could occur are broken according to pre-defined rules. If there should be a path failure, the algorithm will reverse the loop breakage in order to maintain the data traffic. It is thus possible to increase network reliability by redundant connections.

The following requirements must be met by the algorithm:

▶ It must automatically reconfigure the tree structure in case of a bridge failure or break in a data path.
▶ It must stabilize the tree structure for any size network.
▶ It must stabilize within a short, known time.

▶ It must produce a reproducible topology that can be pre-defined by management.
▶ It must be transparent to the terminal equipment.
▶ By creating a tree structure it must result in a low network load compared to the available transmission capacity.

4.4.2 Rules for creating the tree structure

Each bridge is uniquely described by the following parameters:

▶ Bridge identification
▶ Root path costs
▶ Port identification

◼ Bridge identification

The bridge identification is 8 bytes long. The 6 low-value bytes are formed by the 48-bit Ethernet address. This ensures that each bridge has a unique identification. The higher-value parts of the bridge identification are formed by the priority number which can be changed by the management administrator when configuring the network. The bridge with the numerically lowest-value bridge identification has the highest priority.

The MAC address and priority are kept in the Management Information Base (see "dot1dBridge (1.3.6.1.2.1.17)" on page 316):
- `dot1dBaseBridgeAddress` (1.3.6.1.2.1.17.1.1.0)
- `dot1dStpPriority` (1.3.6.1.2.1.17.2.2.0)
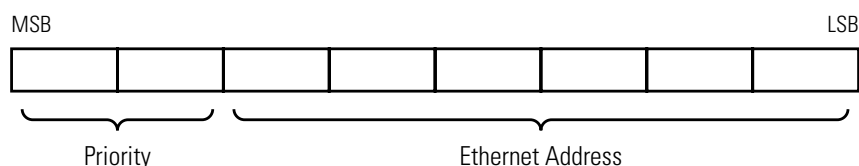
Fig. 31:   Bridge identification

■ **Root path costs**
Each path connecting two bridges has transmission costs assigned to it. The management administrator sets this value and specifies it for each path when configuring a bridge (see Table 7 on page 109).

Because the management administrator essentially has a free hand in specifying this value, he has a tool for ensuring that in case of redundant paths one path will be favored over the others.

The root path costs are calculated by adding up the individual path costs for the paths that a data packet must traverse between the port of a bridge and the root bridge.

The root path costs and individual path costs are stored in the Management Information Base (see "dot1dBridge (1.3.6.1.2.1.17)" on page 316):
- `dot1dStpRootCost` (1.3.6.1.2.1.17.2.6.0)
- `dot1dStpPortPathCost` (1.3.6.1.2.1.17.2.15.1.5.Index)
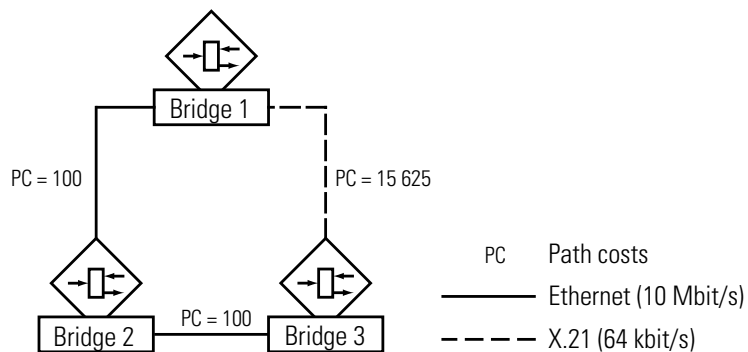
Fig. 32:   Path costs

■ **Port identification**
The port identification consists of two parts of 8 bits each. One part, the lower-value byte, reflects a fixed relationship to the physical port number. This part ensures that no port in a bridge receives the same designation as another port in the same bridge. The second part contains the priority number which is set by the management administrator. It is also true here that the port with the lowest numerical value for its port identifier is the one with the highest priority.

The port number and port priority number are stored in the Management Information Base (see "dot1dBridge (1.3.6.1.2.1.17)" on page 316):
- `dot1dStpPortPathCost` (1.3.6.1.2.1.17.2.15.10,1.Index)
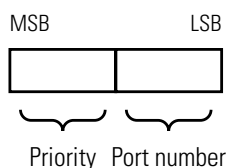- `dot1dStpPortPriority` (1.3.6.1.2.1.17.2.15.1.2.Index)

Fig. 33:   Port identification

In order to compute their tree structures, the bridges need information about other bridges that are present in the network. This information is obtained by each bridge sending a BPDU (Bridge Protocol Data Unit) to all other bridges.

Along with other information, the BPDU contains the

► bridge identification,
► root path costs, and
► port identification

(see IEEE 802.1D).

► The bridge with the numerically smallest bridge identification is made the root bridge. It forms the root of the tree structure.
► The structure of the tree depends upon the root path costs. The structure that is chosen is the one that provides the lowest path costs between each individual bridge and the root bridge.
► If there are multiple paths with the same root path costs, the priorities of the bridge identifications for the bridges connected to this path determine which bridge is blocked.
► If there are two paths leading away from a single bridge with the same root path costs, the port identification is used as the last criterion for determining which path is used (see Fig. 33). It decides which port is selected.
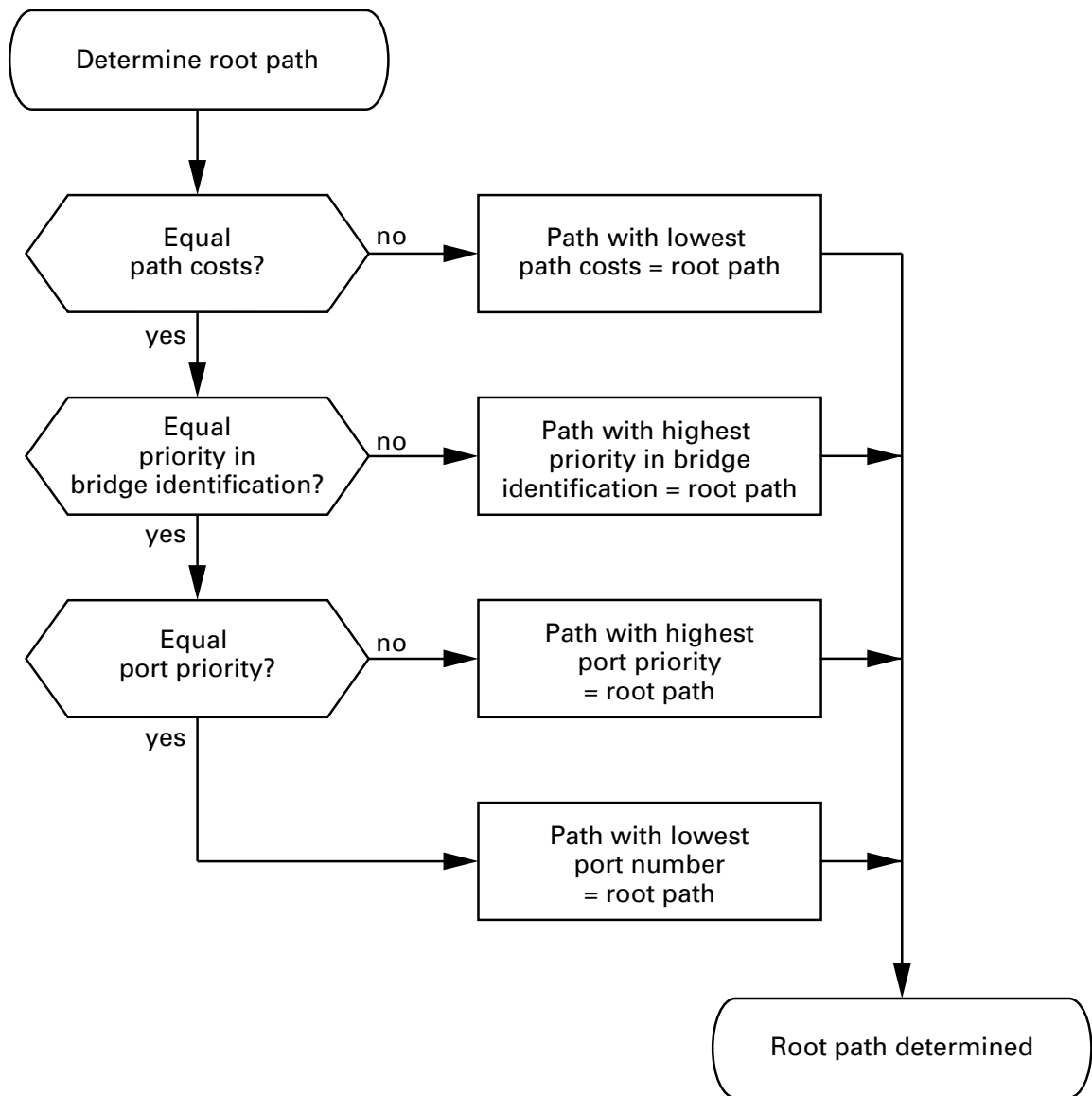
Fig. 34:   Flow chart for determining root path

Using the network diagram (see Fig. 35), it is possible to follow the logic in the flow chart (see Fig. 34) for determining the root path. The bridge with the numerically smallest bridge identification (in this case, bridge 1) is selected as the root bridge. In this example the partial paths all have the same path costs. The path between bridge 2 and bridge 3 is removed because a con-nection from bridge 3 to the root bridge via bridge 2 would result in twice the path costs.

The path from bridge 6 to the root bridge is interesting:

▶ The path via bridges 5 and 3 generates the same root path costs as the path via bridges 4 and 2.

▶ The path via bridge 4 is selected because the bridge identifier 40 is numerically less than 50.

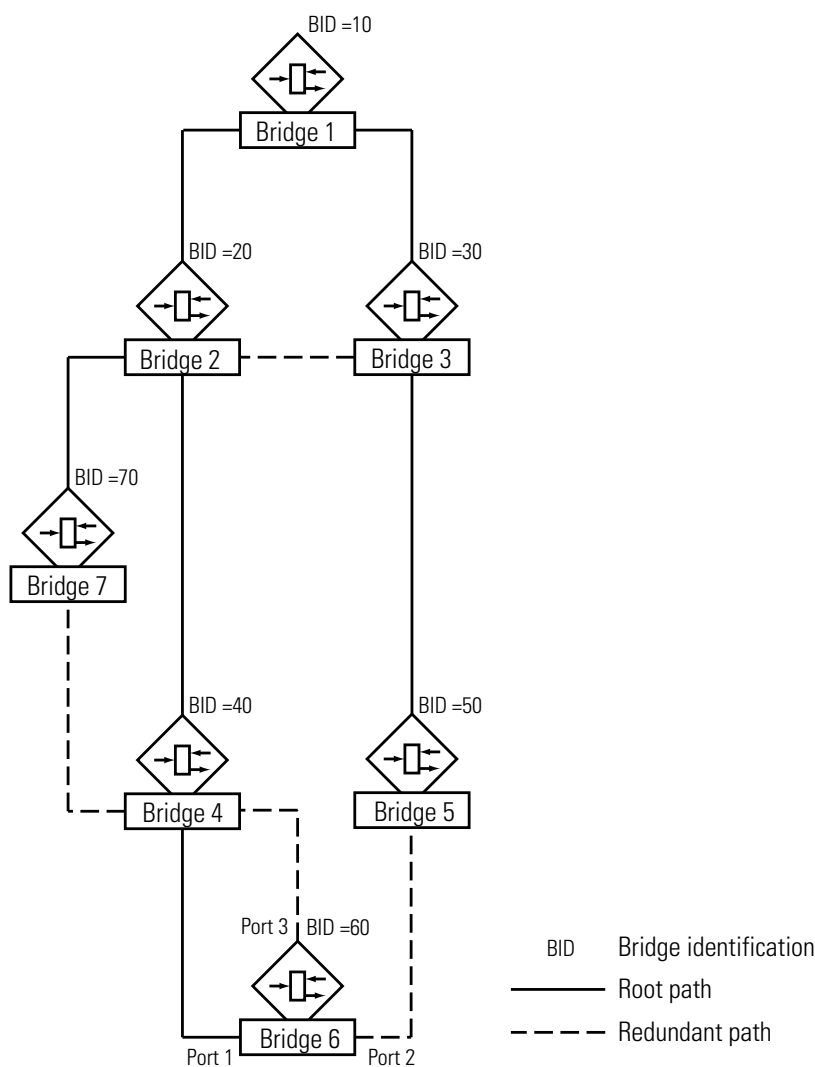▶ There are however two paths between bridge 6 and bridge 4. In this case, the larger port priority is decisive.

Fig. 35:   Root path determination example

4.4.3 Example: manipulation of a tree structure.

The management administrator of the network (see Fig. 35) soon discovers that this configuration, with bridge 1 as its root bridge, is unfavorable. The control packets that bridge 1 sends to the other bridges are concentrated on the paths between bridge 1 and bridge 2 and between bridge 1 and bridge 3. If the management administrator raises bridge 2 to the root bridge, the load caused by the control packets will be more evenly distributed among the sub-networks. This would result in the configuration shown (see Fig. 35). The paths between the individual bridges and the root bridge have become shorter.
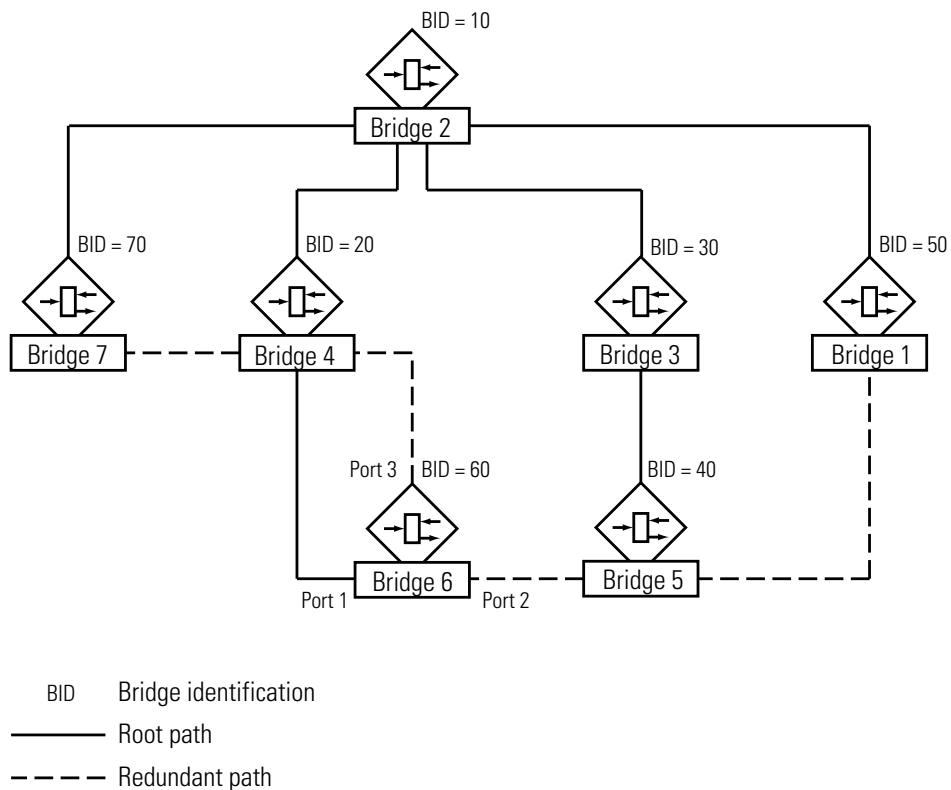
Fig. 36:   Example of a root path manipulation

4.4.4 Rapid Spanning Tree Protocol

The exponential increase in the use of LANs also in time-critical applications places new demands on the availability of the networks. Switch-over times in the high seconds range for reconfiguring the network when a subcomponent fails can no longer be tolerated. Thus it was inevitable that the once legendary Spanning Tree Protocol had to be revised in order to keep pace with our ever-changing world. The improvement from several seconds to less than one second, when compared with other technical changes, represents more an evolution or further development than a revolution.
This further development was adopted in June 2001 as IEEE 802.1w to supplement the existing IEEE 802.1D standard and dubbed Rapid Spanning Tree Algorithm and Protocol (RSTP).

RSTP is compatible to the traditional STP. If, however, both protocols are used simultaneously, there are no advantages to using the faster reconfiguration with RSTP.

RSTP does not change the tree structure calculation. RSTP only alters parameters, adds new parameters and mechanisms that accelerate the reconfiguration in the event of an error. The ports play a major role within this context.

■ **Port roles**
    RSTP assigns one of the following roles to each bridge port:

    ▶   (Root-Port),
        The port at which a bridge receives data packets with the lowest path costs from the root bridge.
        If there are several such ports, the bridge identification determines which port is the root port.
        If there is also more than one of these ports, the port identification determines which port is the root port (see Fig. 34).
        The root bridge does not have a root port itself.

Link speed	Recommended value	Recommended range	Range
<=100 Kb/s	200 000 000*	20 000 000-200 000 000	-200 000 000
1 Mb/s	20 000 000*	2 000 000-200 000 000	-200 000 000
10 Mb/s	2 000 000*	200 000-20 000 000	1-200 000 000
100 Mb/s	200 000*	20 000-2 000 000	1-200 000 000
1 Gb/s	20 000	2 000-200 000	1-200 000 000
10 Gb/s	2 000	200-20 000	1-200 000 000
100 Gb/s	200	20-2 000	1-200 000 000
1 Tb/s	20	2-200	1-200 000 000
10 Tb/s	2	1-20	1-200 000 000

*Table 7:   Recommended path costs according to the data rate
(see "Root path costs" on page 103)
* Bridges conformant to IEEE Std 802.1D, 1998 Edition, i.e., that support
only 16 bit values for Path Cost, should use 65 535 as the Path Cost for
these link speeds when used in conjunction with Bridges that support 32
bit Path Cost values.*

▶ Designated port
The port that connects the designated bridge to a network segment
that leads away from the root bridge.

Each network segment in which there is no further RSTP bridge is
connected to exactly one designated port. This designated port then
functions as an (edge port) at the same time. Characteristic of an edge
port is the fact that it does not receive any RST BPDUs (Rapid
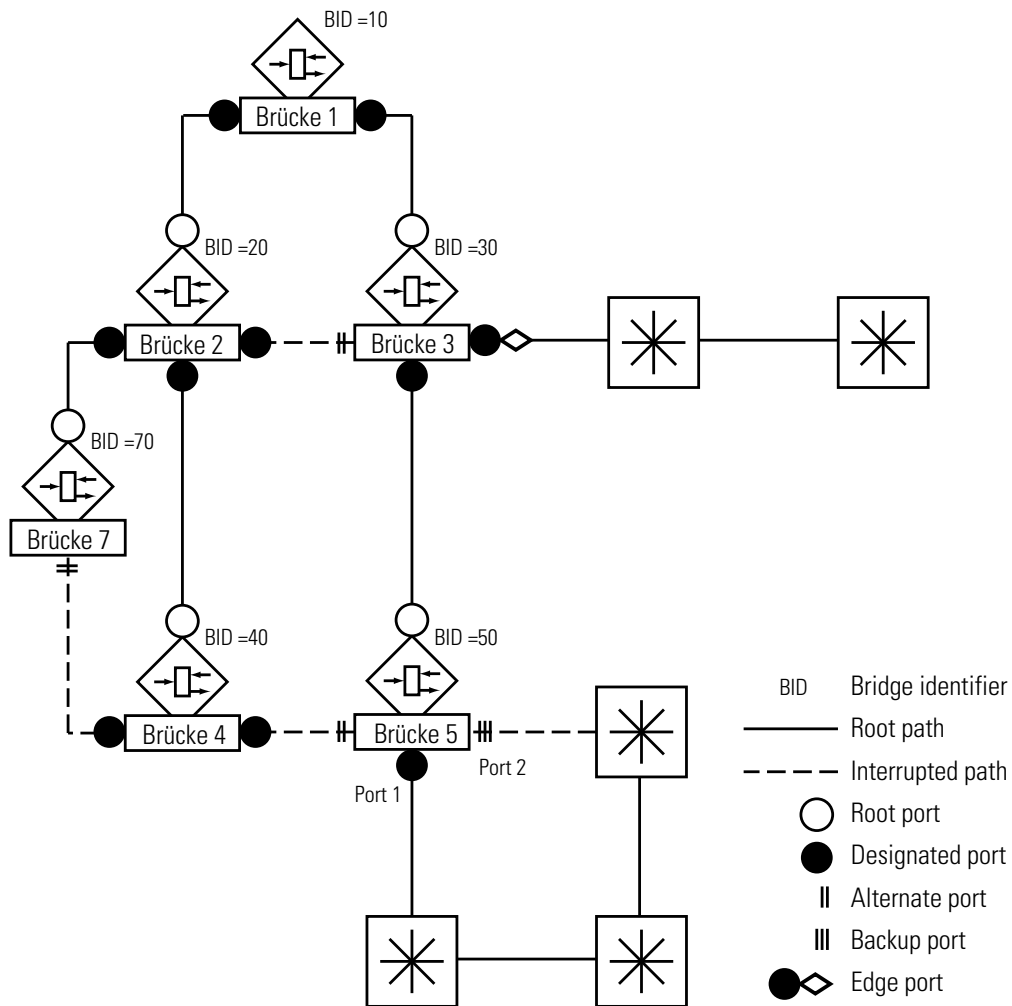Spanning Tree Bridge Protocol Data Unit).

Fig. 37:   Port role assignment

► Alternate port
The port that takes over the function of the root port if the connection to the root bridge fails. The alternative port re-establishes a reliable connection from the bridge to the root bridge.

► Backup port
A port that is available as a replacement in case the connection to the designated port of this network segment (without RSTP bridge) fails. The replacement port leads to the branches of the Spanning Tree.

► Disabled-Port,
Port that has no meaning within the Spanning Tree operation, so is disabled or has no link.

■ **Port statuses**
According to the tree structure and the status of the selected connection routes, RSTP assigns their statuses to the ports.

STP Port State	Administrative Bridge Port State	MAC Operational	RSTP Port State	Active Topology (Port Role)
DISABLED	Disabled	FALSE	Discarding*	Excluded (Disabled)
DISABLED	Enabled	FALSE	Discarding**	Excluded (Disabled)
BLOCKING	Enabled	TRUE	Discarding*	Excluded (Alternate, Backup)
LISTENING	Enabled	TRUE	Discarding*	Included (Root, Designated)
LEARNING	Enabled	TRUE	Learning	Included (Root, Designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (Root, Designated)

Table 8:   Relationship between the port-status values in the STP and RSTP
         * The dot1d-MIB displays "Disabled"

■ **Spanning Tree Priority Vector**
To assign roles to ports, the RSTP bridges exchange configuration information between themselves. This information is known as a "Spanning Tree Priority Vector". It contains the following elements:

▶ Bridge identification of the root bridge
▶ Root path costs of the transmitting bridge
▶ Bridge identification of the transmitting bridge
▶ Port identification of the port through which the message was sent
▶ Port identification of the port through which the message was received

Based on this information, the bridges involved in the RSTP are capable of calculating port roles by themselves and defining the port status of their own ports.

■ **Fast reconfiguration**
Why can RSTP react faster to an interruption of the root path?

▶ Introduction of edge ports
When reconfiguring RSTP switches to forwarding mode at the end of "Hello Time" immediately (see Table 12 on page 162). RSTP waits for the end of "Hello Time" to be sure, that no BPDU sending bridge is connected.
If the user is sure, that an DTE is connected to this port and still remains, he can switch off STP on this port. Thus there will be no latency at this port in the case of reconfiguration.

▶ Introduction of alternate ports
Since the port roles are already distributed in regular operation, a bridge can switch over immediately from the root port to the alternative port after having lost the connection to the root bridge.

▶ Communicating with neighboring bridges
The decentralized, direct communication between neighboring bridges permits immediate reaction to changes in state of the Spanning Tree architecture.

▶ Filter table
When STP is used, the age of the entries in the table determines what is to be updated. The RSTP deletes the entries of the ports immediately and specifically that are affected by reconfiguration.

▶ Reaction to an event
Without having to adhere to any time specifications, RSTP reacts immediately to events such as connection interruption, connection established, etc.

Note: The price for this fast reconfiguration is the risk that data packets may be duplicated or misplaced during the reconfiguration phase. If you cannot accept such a risk in your application, switch back to the slower Spanning Tree Protocol or select one of the other redundancy procedures described in this manual.

4.5 Redundancy

4.5.1 Line-type configuration

The RS2-4R enables you to set up backbones in line-type configurations. Cascading takes place via the HIPER-Ring ports.
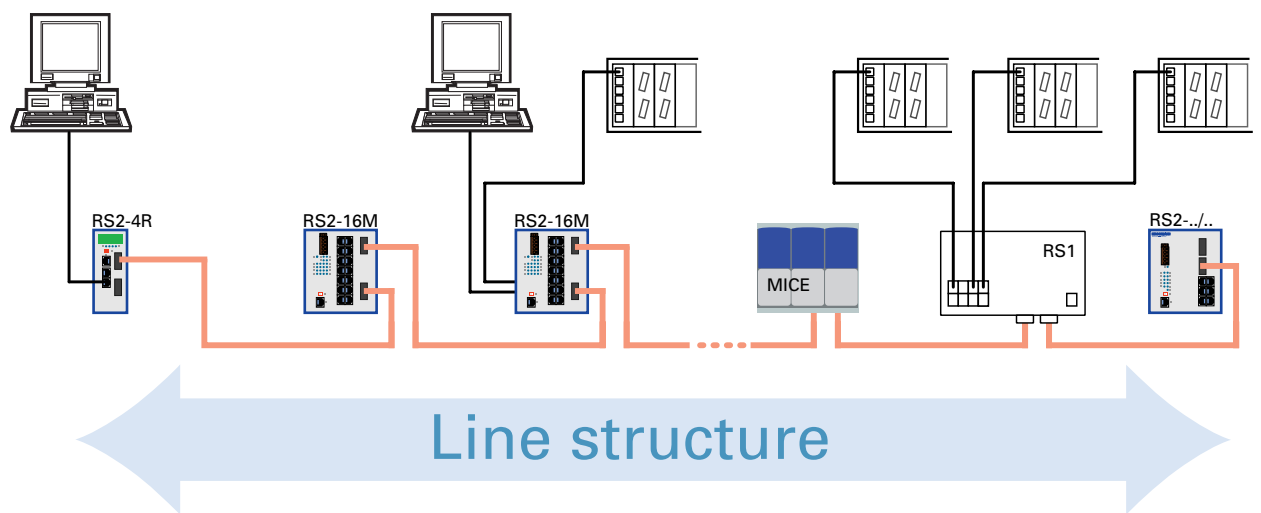

Fig. 38:   Line-type configuration

4.5.2 Redundant ring structure – HIPER-Ring

The two ends of a backbone in a line-type configuration can be closed to form
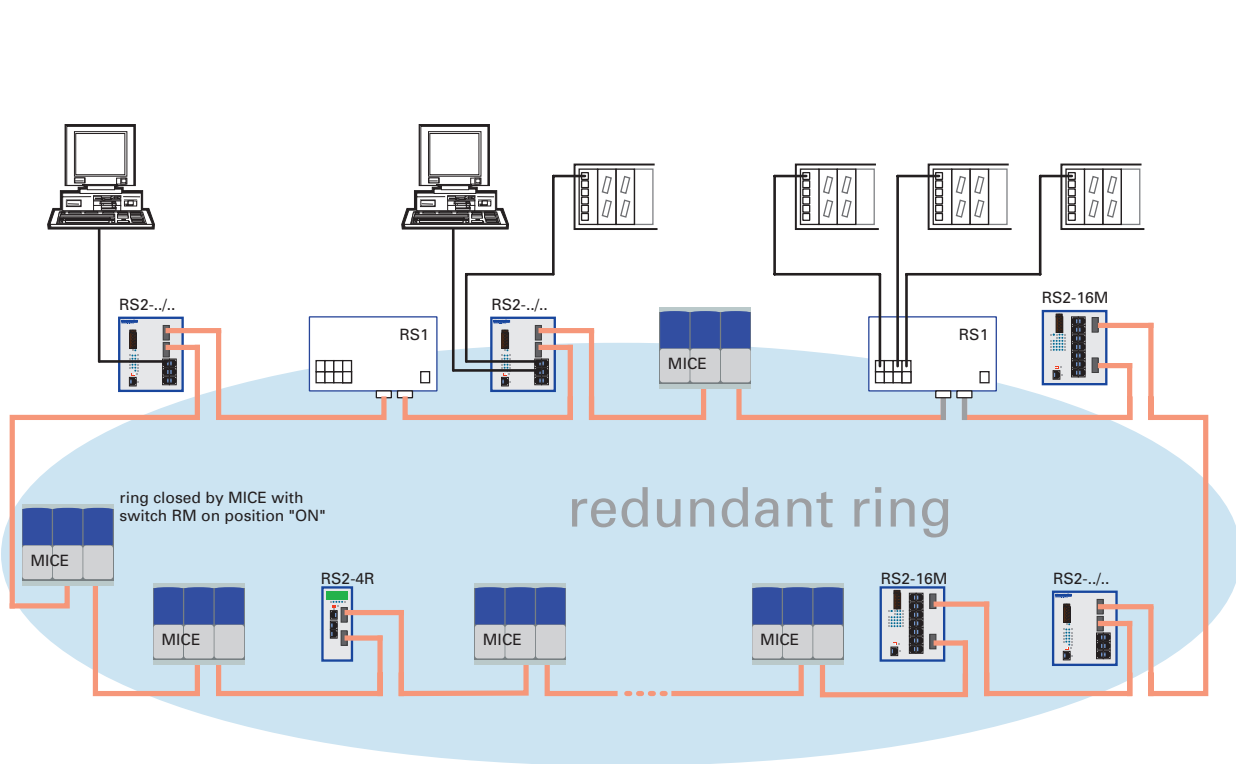a redundant ring by using the RM function (**R**edundancy **M**anager) of the
RS2-4R.

Fig. 39:   Redundant ring structure

The RS2-4R is integrated into the HIPER-Ring via the HIPER-Ring ports
(ports 3 and 4). It is possible to mix the RS1, RS2-16M, RS2-../.. , MACH
3000 and MICE in any combination within the HIPER-Ring. If a line section
fails, the ring structure of up to 50 Switches transforms back to a line-type
configuration within 0.5 seconds.

Note: The "HIPER-Ring" function requires the following setting for ports 15
and 16:
100 Mbit/s, full duplex and autonegotiation off (= settings on delivery).

4.6 Security

4.6.1 SNMP

The agent communicates with the network management station via the Simple Network Management Protocol. Therefore the network management station uses the *HiVision* network management software or the Web-based interface.
Every SNMP packet contains the IP address of the sending computer and the community under which the sender of the packet wants to access the switch MIB.

The switch receives the SNMP packet and compares the IP address of the sending computer and the community with the entries in the `hmAuthCommTable` and the `hmAuthHostTable` of its MIB. If the community has the appropriate access right, and if the IP address of the sending computer has been entered, then the switch will allow access.

In the delivery state, the switch is accessible via the "public" community (read only) and the "private" one (read and write) from every computer.

To protect your switch from unwanted access:

☐ First define a new community which you can access from your computer with all rights.

Note: Make a note of the community name and the associated index. For security reasons, the community name cannot be read later. Access to the community access, trap destination and trap configuration table is made via the community index.

☐ Treat this community **with discretion**. Because everyone who knows the community can access the switch MIB with the IP address of your computer.
☐ Limit the access rights of the known communities or delete their entries.

4.6.2 SNMP traps

If unusual events occur during normal operation of the RS2-4R, they are reported immediately to the management station. This is done by means of so-called **traps**- alarm messages - that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples of such events are:

▶ a hardware reset
▶ changing the basic device configuration
▶ segmentation of a port

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.
The management agent sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

■ **SNMP trap listing**
All the possible traps that can occur are listed in the following table.

authenticationFailure
is sent if a station attempts to access an agent without permission.

coldStart
is sent for a cold and warm start during the boot process after successful management initialization.

hmAutoconfigAdapterTrap
is sent when the ACA 11 AutoConfiguration Adapter is inserted or removed.

linkDown
is sent if the link to a port is interrupted.

linkUp
is sent if the link to a port is re-established.

hmPowerSupply
is sent if the status of the voltage supply changes.

hmSignallingRelay
is sent if the status of the signal contact changes.

newRoot
is sent if the sending agent becomes the new root of the spanning tree.

topologyChange
is sent if the transmission mode of a port changes.

risingAlarm
is sent if an RMON alarm input exceeds the upper threshold.

fallingAlarm
is sent if an RMON alarm input falls below the lower threshold.

hmRingRedReconfig
is sent if the configuration of the redundant ring changes.

hmSNTPTrap
is sent if errors occur in connection with the SNTP protocol (e.g. server not available).

hmRelayDuplicateTrap
is sent if a duplicate IP address is detected in connection with the DHCP Option 82.

4.6.3 SNMP traps when booting

The ColdStart trap is sent during every boot procedure.

5 Web-based management

The RS2-4R supports both SNMP management and Web-based management and can thus offer

► extensive diagnostic and configuration functions for fast startup and
► extensive network and device information.

The RS2-4R supports the TCP/IP protocol family.

The user-friendly Web-based interface gives you the option of managing the RS2-4R from any location in the network via a standard browser such as the Netscape Navigator/Communicator or the Microsoft Internet Explorer.
As a universal access tool, the Web browser uses an applet which communicates with the RS2-4R via the Simple Network Management Protocol (SNMP).
The Web-based interface allows you to graphically configure the RS2-4R.

5.1 Opening the Web-based interface

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Netscape Navigator/Communicator version 6.0 or higher or Microsoft Internet Explorer version 5.5 or higher.

Note: The Web-based interface uses the "Java™ Runtime Environment Version 1.3" plug-in. If it is not yet installed on your computer, it will be installed automatically via the Internet when you start the Web-based interface. This installation is very time-consuming.

For Windows NT users: cancel the installation. Install the plug-in from the enclosed CD-ROM. Proceed by starting the program file `j2re1_3_1_07-windows-i586-i.exe` in the Java directory on the CD-ROM.
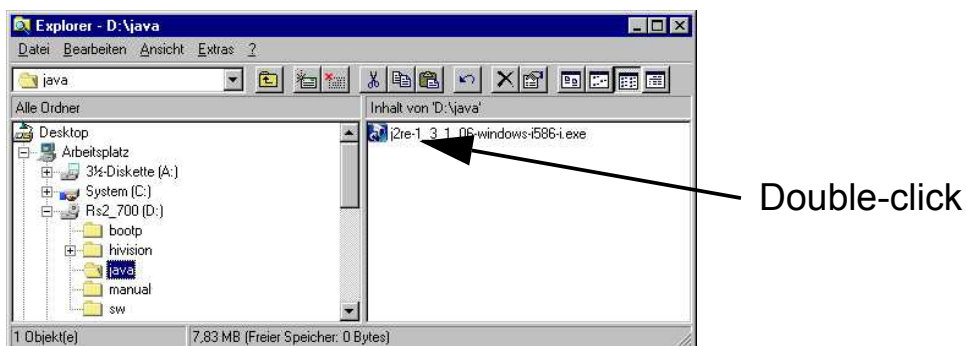
Fig. 40:   Install Java

☐ Start your Web browser.

☐ Make sure that you have activated JavaScript and Java in the security settings of your browser.

☐ Establish the connection by entering the IP address of the RS2-4R that you want to administer via the Web-based network management in the address field of the Web browser. Enter the address in the following form:

```
http://xxx.xxx.xxx.xxx
```

The login window will appear on the screen.

Fig. 41:   Login window

☐ Select the desired language.

☐ In the login fold-down menu, select
  – user, for read access or
  – admin, for read and write access
  to the switch.

☐ The password "public", with which you have read permission, appears in the password field. If you wish to access the RS2-4R with write permission, then highlight the contents of the password field and overwrite it with the password "private" (state on delivery).
Changing the password protects the RS2-4R against unauthorized access.

☐ Click on OK.

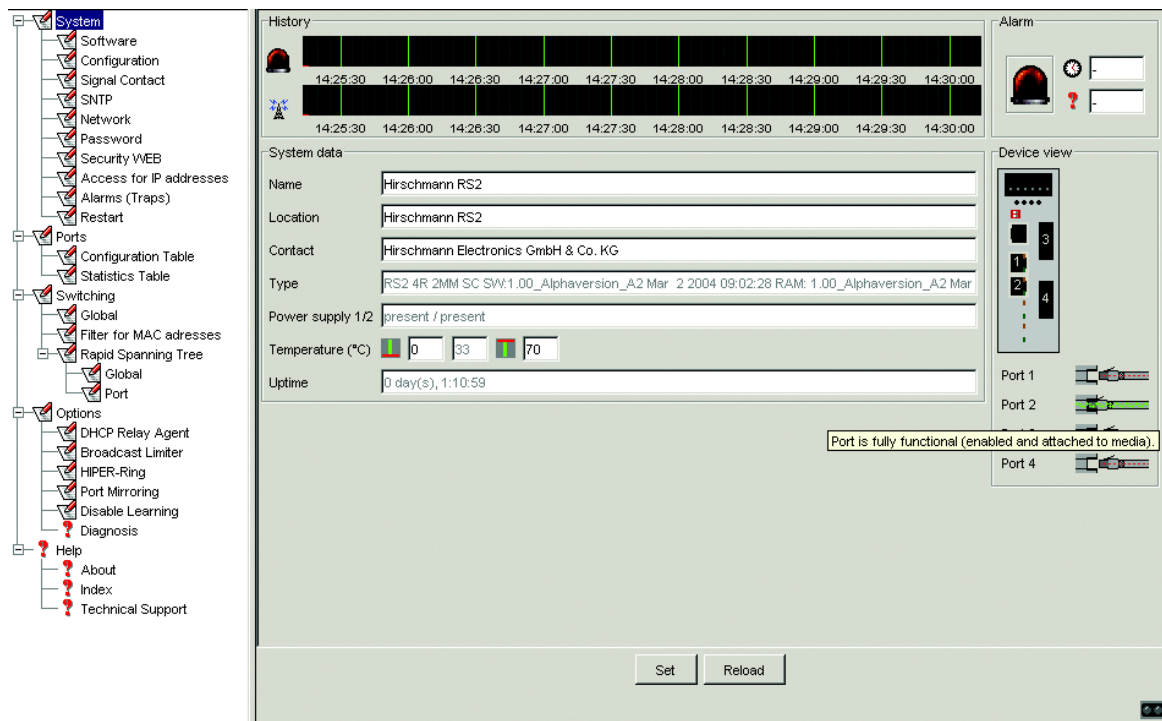The Website of the RS2-4R appears on the screen.

Fig. 42:   Website of the RS2-4R with bubble help

5.2 Menu tree

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the right mouse button you can use
"Expand all" to open up the whole menu tree and
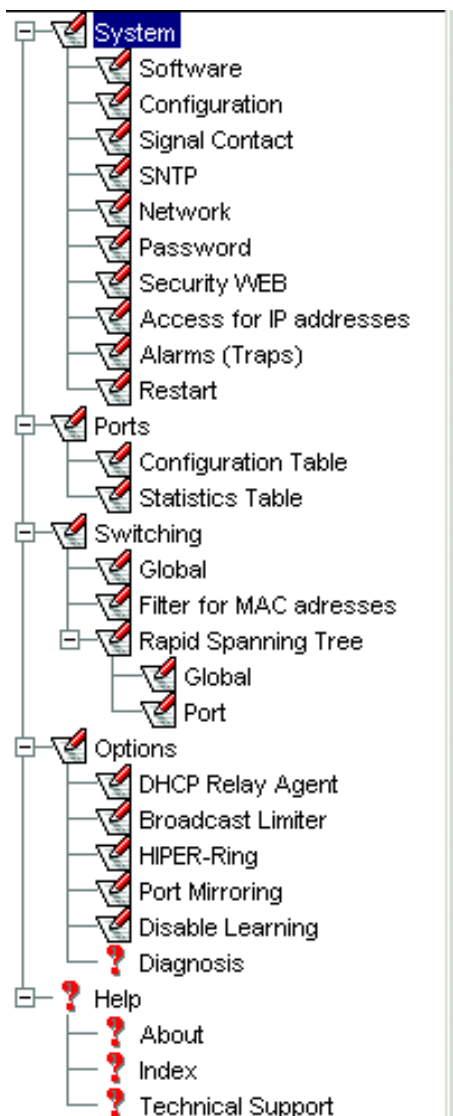"Collapse all" to close the menu tree up to the main menus.

```
System
    Software
    Configuration
    Signal Contact
    SNTP
    Network
    Password
    Security WEB
    Access for IP addresses
    Alarms (Traps)
    Restart
Ports
    Configuration Table
    Statistics Table
Switching
    Global
    Filter for MAC adresses
    Rapid Spanning Tree
        Global
        Port
Options
    DHCP Relay Agent
    Broadcast Limiter
    HIPER-Ring
    Port Mirroring
    Disable Learning
    Diagnosis
Help
    About
    Index
    Technical Support
```

Fig. 43:   Menu tree

5.3 System

The system menu contains the dialog boxes and tables used for system con-
figuration:

- ▶ Software update
- ▶ Set start configuration
- ▶ Set the network parameters
- ▶ Signal Contact
- ▶ SNTP
- ▶ Password
- ▶ WEB access
- ▶ Access for IP addresses
- ▶ Configuring traps
- ▶ Restart

The information section of the system menu is divided into:

► Recording
► Alarm
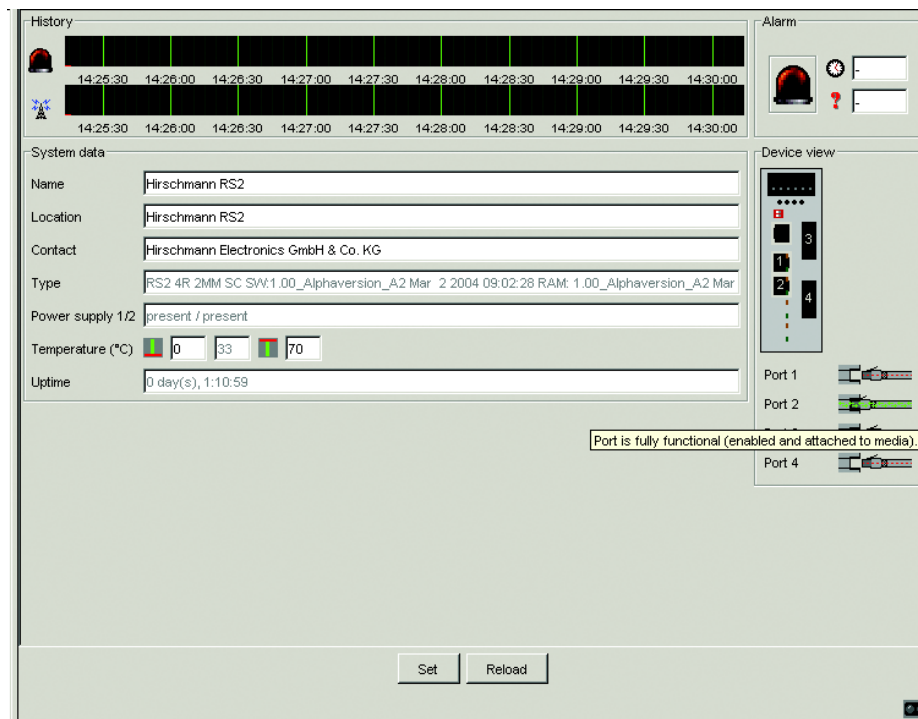► System data
► View of device
► Updating
► Port status

Fig. 44:   Information section in the system menu

■ **Recording**
This area of the Website shows the history of the RS2-4R.
Since the history is maintained by the Web browser applet, the history is available only while the applet is running. The time window extends up to 2 hours.

Records the alarm signal of the agent

Records the accessibility of the agent
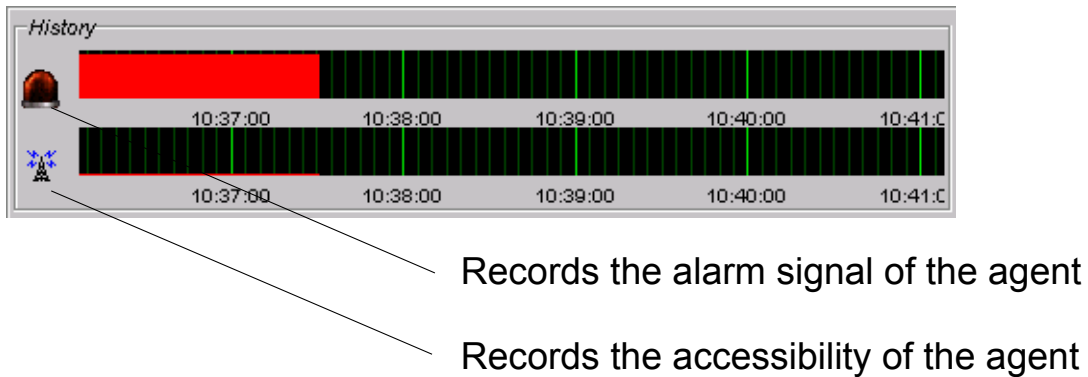
Fig. 45:   History display

■ **Alarm**
This section of the Website provides information on the alarm state of the RS2-4R.

Time of the oldest existing alarm

Cause of the oldest existing alarm

Activate/deactivate audible alarm siren (soundcard required)

The blinking lamp indicates an alarm
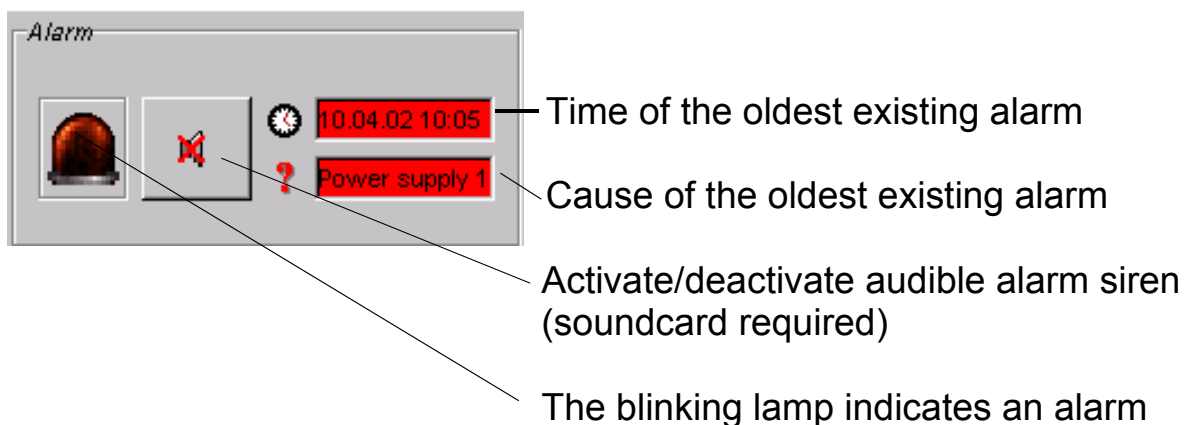
Fig. 46:   Alarm display

■ **System data**
This area of the Website displays the system history of the agent. Here you can change,
– the system name,
– the location description and
– the name of the contact person for this switch.

       – System name of the switch
       – Location of this switch
       – Contact person for this switch
       – Software and hardware version
       – Status of the power supply units
       – Temperature in switch, with alarm limits
       – Time that has elapsed since the switch was last restarted.

Fig. 47:   System parameter display

■ **View of device**
This area of the Website displays the image of the device. The symbols underneath the device view represent the status of the individual ports.
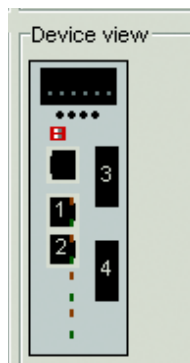

Fig. 48:   View of device

Meaning of the symbols:

The port is enabled and the connection is OK.

The port is locked by management.

The port is enabled and the connection is interrupted.

The RS2-4R cannot be reached.

■ **Updating**
This area of the Website at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the "Update" button requests the current data of the RS2-4R immediately. The applet polls the current data of the RS2-4R automatically every 100 seconds.

Reloading data in 40 sec

Fig. 49:   Time until update

5.3.1 Updating the software

With the software dialog you can carry out a software update of the RS2-4R via tftp or http.

■ **tftp Update**
For a tftp update you need a tftp server on which the software to be loaded is stored. The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/ path name/file name (e.g. `tftp://149.218.16.5/rs2/rs2.bin`). Click "tftp Update" to load the software from the tftp server to the RS2-4R.

■ **http Update**
For an http update you need access from your computer to the update software.
If you click "http Update" the RS2-4R opens a second browser window. Here you select the update software and click on "Update" to transfer the software to the RS2-4R.

http Update - 2nd browser window:
☐ Click on `Search` to select the software for the update.
☐ Click on "Update" to transfer the software to the switch.

http-Update

Click on "search" to select the software for the update.
Click on "Update" to transfer the software to the switch.
The end of the update is indicated by one of the following messages:

• Update completed successfully.
• Update failed. Reason: incorrect file.
• Update failed. Reason: file damaged.
• Update failed. Reason: flash error.

Close the second browser window with "File:close" to return to the dialog software.

Update file: [   ] [Durchsuchen...]

[Update]

Fig. 50:   Dialog software update via http

The end of the update is indicated by one of the following messages:

▶ Update completed successfully.
▶ Update failed. Reason: incorrect file.
▶ Update failed. Reason: file damaged.
▶ Update failed. Reason: flash error.
☐ Close this browser window with "`File: close`" to return to the dialog software.

To start the new software after loading, restart the RS2-4R (see dialog).

Note: You can define which configuration will be loaded by the switch during reboot by the settings in the dialogs and .
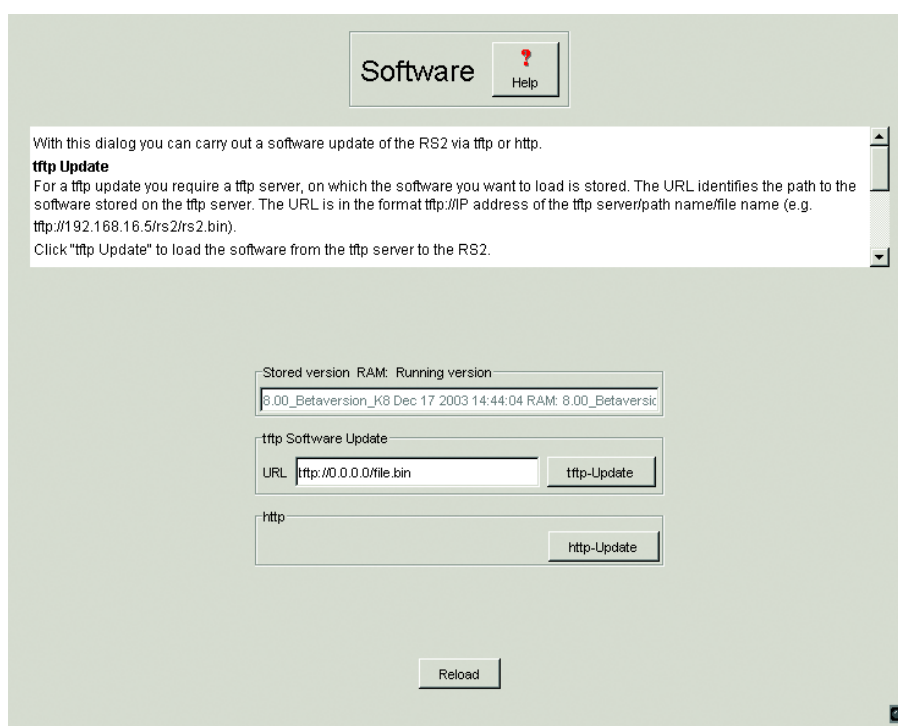

Fig. 51:   Dialog Update software

Delete the browser's cache contents after the software update. After a restart your browser is able to load the new release of the Web-based interface.

☐ – Netscape Navigator/Communicator:
    Close browser and reopen it.
    – Microsoft Internet Explorer:
    In `Extras: Internet options: Advanced`, select the topic "Delete
    temporary internet files when closing the browser".
    Close browser and reopen it.

5.3.2 Defining the start configuration

With this dialog you can:

▶ set a restart configuration,
▶ load a configuration,
▶ save a configuration,
▶ enter an URL,
▶ view the ACA status.

■ **Restart configuration**
In the "Load after reset" frame you can set the configuration with which the system is loaded when restarting.
If you select default, the parameters are reset to the original delivery state, with the exception of the settings you created in the Software, Configuration and Network dialogs.

■ **Load configuration**
In the "Load" frame you can
▶ load a local configuration,
▶ load a configuration from a file stored under the specified URL.
▶ load a configuration from a file stored under the specified URL and save it on the device.

■ **Save a configuration**
In the "Save" frame you can
▶ save the current configuration on the device.
▶ save the current configuration in a file under the specified URL.

Note: The status of the load, started by DHCP/BOOTP (see "Configure the network" on page 144), is displayed in the selected option "from URL & save local" in the "Load" frame. If you get an error message while saving the configuration, one reason may be that loading is not completed. DHCP/BOOTP does not finish loading until a valid configuration is loaded. If DHCP/BOOTP does not find any valid configuration you can stop the active loading by loading the local configuration in the "Load" frame.

■ **URL**
The URL identifies the path to the tftp server on which the configuration
file is to be stored. The URL is in the form
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://149.218.112.5/rs2/config.dat`).

Example to save on a tftp server
☐ Open a new file with any editor.
☐ Save the empty file to the appropriate path of the tftp server, including
   the file name, e.g. `RS2/RS2_01.cfg`
☐ In line "URL", enter the path of the tftp server, e.g.
   `tftp://149.218.112.214/RS2/RS2_01.cfg`.

Note: The configuration file includes all configuration data, including the
password. Therefore pay attention to the access rights on the tftp server.

■ Auto Configuration Adapter (ACA)

The ACA is a device for storing the configuration data of a MICE, RS2-../.., RS2-16M, RS2-4R or MACH 3000 switch. In the case of a switch failure, the ACA enables a very simple configuration data transfer by means of a substitute switch of the same type.

Storing the current configuration data in the ACA:
You can transfer the current switch configuration onto the ACA and the flash memory with "Save local configuration". First Select the "Local" setting in the "Save" field.

Transferring the configuration data from the ACA:
When you restart, the switch assumes the configuration data of the ACA and saves them permanently into the flash memory. Which data the switch takes from the ACA depends on the setting in the restart configuration (see Table 9 on page 137).
If the connected ACA does not contain any valid data, for example a new ACA, the switch then loads the data from the flash memory.

Setting	Result
Local	The switch takes all the data from the ACA
from URL	The switch takes the IP parameters from the ACA and the other data from the URL
defaults	The switch takes the IP parameters from the ACA and sets the other parameters to the default setting

Table 9: Data transfer from ACA after restart

Status	Meaning
notPresent	No ACA present.
ok	The configuration data from the ACA and the switch are consistent.
removed	The ACA has been removed after rebooting.
notInSync	The configuration data from the ACA and the switch are not consistent.
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA comes from another device type.
checksumErr	The configuration data is damaged.

Table 10: ACA status

Fig. 52:   Dialog Start configuration

5.3.3 Signal Contact

The signal contact is for

▶ manual setting the signal contact .
▶ monitoring proper functioning of the RS2-4R.

■ **Manual setting**
   This dialog gives you the option of remote switching the signal contact.
   ☐ Select "Opened" in the "Manual setting" field to open the contact.
   ☐ Select "Closed" in the "Manual setting" field to close the contact.
   Application options:
   ▶ Simulation of an error during SPS error monitoring.
   ▶ Remote control of a device via SNMP, such as switching on a camera.

■ **Proper functioning**
   The signal contact monitors the functions of the RS2-4R which makes it possible to perform remote diagnostics.
   A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit):
   ▶ the failure of at least one of the two supply voltages (power supply voltage 1 or 2 < 18 V). Select "Redundant power supply ignore", if you have not connected a redundant power supply.

   Note: With non-redundant supply of the mains voltage, the RS2-4R reports a power failure. You can prevent this message by applying the supply voltage over the two inputs.

   ▶ a continuous malfunction in the RS2-4R (internal 3.3 VDC voltage).
   ▶ the defective link status of at least one port. With the RS2-4R, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
   ▶ error during self-test.

   The following condition is reported in RM mode:
   ▶ Ring monitoring is not possible, e.g. during software initialization.
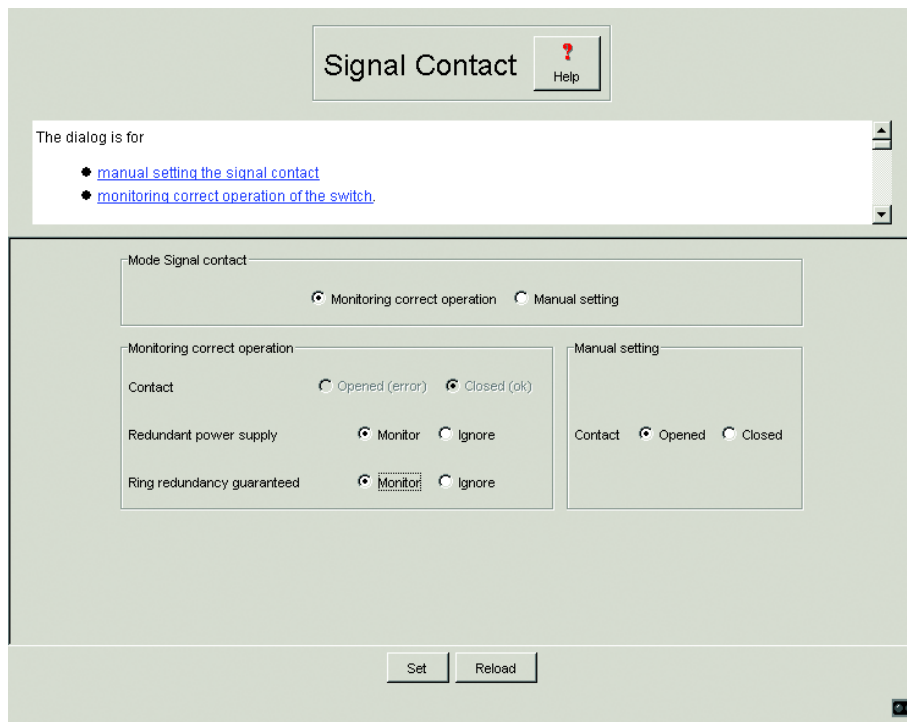
Fig. 53:   Dialog Signal contact

5.3.4 SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network. The switch supports the SNTP Server and SNTP Client functions. The SNTP Server places the UTC (Universal Time Coordinated) at disposal. The SNTP Client obtains the UTC.

■ **Configuration SNTP Client and Server**
  ☐ In this frame you switch the SNTP function on/off.
    When it is switched off,
    the SNTP server does not send any SNTP packages and does not reply to any SNTP requests.
    The SNTP client does not send any SNTP requests and does not interpret any broadcast/multicast packages.
  ☐ The "Local Offset" is for displaying/entering the time difference between the local time and the UTC.
    With "Set offset from PC", the agent determines the time zone on your PC and then calculates the local time difference.

  Note: When setting the time in zones with summer and winter times, make an adjustment for the local offset. The switch can also get the SNTP server IP address and the local offset from a DHCP server.

■ **SNTP-Status**
  ► The "SNTP time" displays the time with reference to Universal Time Coordinated (UTC).
    The display is the same worldwide. Local time differences are not taken into account.
  ► The "System time" uses UTC, allowing for the local time difference from UTC.
    "System time" = "SNTP time" + "Local offset"
  ☐ With "Set time from PC", the switch takes the PC time as the system time and calculates the SNTP time using the local time difference.
    "SNTP time" = "System time" - "Local offset"
  ► The "Status message" displays conditions such as "Server cannot be reached".

■ **Configuration SNTP Server**
   ☐ In "Anycast destination address" you enter the IP address to which the SNTP server on the switch sends the SNTP packages.

IP target address	Send SNTP packages periodically to
0.0.0.0	niemanden
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Table 11: Periodic sending of SNTP packages

   ☐ In "VLAN ID" you specify the VLAN to which the switch may periodically send SNTP packages.
   ☐ In "Anycast send interval" you specify the interval at which the switch sends SNTP packages (valid entries: 1 second to 3600 seconds, default: 120 seconds).

■ **Configuration SNTP Client**
   ☐ In "External Server Address" you enter the IP address of the SNTP server from which the switch periodically obtains the system time.
   ☐ In "Redundant Server Address" you enter the IP address of the SNTP server from which the switch periodically obtains the system time, if the switch does not receive an answer from the "external server address" 0.5 seconds after making a request.

Note: If you are receiving the system time from an external/redundant server address, you do not accept any SNTP broadcasts (see below). Otherwise you can never distinguish whether the switch is displaying the time from the server entered, or that of an SNTP broadcast package.

   ☐ In "Server request interval" you specify the interval at which the switch requests SNTP packages (valid entries: 1 second to 3600 seconds, default: 30 seconds).
   ☐ With "Accept SNTP Broadcasts" the switch takes the system time from SNTP broadcast/multicast packages which it receives.

Note: For the most accurate system time distribution possible, avoid having network components (routers, switches, hubs) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

Fig. 54:   Dialog SNTP

5.3.5 Configure the network

With this dialog you define the source from which the switch gets its network parameters after starting and assign network parameters.
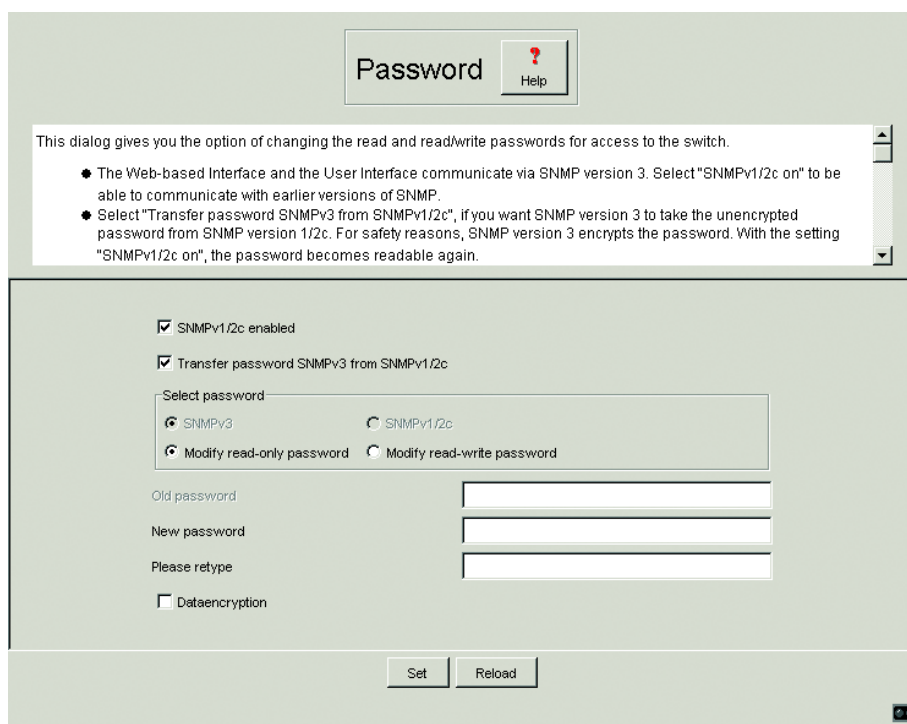

Fig. 55:   Dialog Network parameters

☐ Under "Modus" you enter where the RS2-4R is to obtain its IP parameters:

▶ In the BOOTP mode, the configuration comes from a BOOTP or DHCP server on the basis of the MAC address of the switch (see page 57).

▶ In the DHCP mode, the configuration comes from a DHCP server on the basis of the MAC address or the name of the switch (see page 61).

▶ In the local mode the net parameters in the switch memory are used.

☐ Enter the parameters according to the selected mode on the right.

☐ You enter the system name applicable to the DHCP protocol in the "System" on page 127 dialog, in the "Name" line.

☐ The HiDiscovery protocol (see "System configuration via HiDiscovery" on page 55) allows you to assign an IP address to the switch on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the switch from your PC with the HiDiscovery software delivered (setting on delivery: active).

5.3.6 Password

This dialog gives you the option of changing the read and read/write pass-words for access to the switch.

☐ The Web-based Interface and the User Interface communicate via SNMP version 3. Select "SNMPv1/2c on" to be able to communicate with earlier versions of SNMP.

☐ Select "Transfer password SNMPv3 from SNMPv1/2c", if you want SNMP version 3 to take the unencrypted password from SNMP version 1/2c. For safety reasons, SNMP version 3 encrypts the password. With the setting "SNMPv1/2c on", the password becomes readable again.

Fig. 56:   Dialog Password

Important: If you do not know a password with read/write access, you will not have write access to the switch!

Note: After changing the password for write access, restart the Web interface in order to access the switch.

Note: For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the switch without a valid password!

Note: In SNMP version 3, use more than 8 characters for the password, because many applications do not accept shorter passwords.

Access via a Web browser can be blocked with the dialog "WEB access" on page 148.
Access at IP address level is restricted via the dialog "Access for IP addresses" on page 149.

The Web-based Interface provides up to 4 different passwords:
▶ Read password SNMP version 3.
▶ Read/write password SNMP version 3. This is identical to the password in the User Interface.
▶ Read password SNMP version 1/2c.
▶ Read/write password SNMP version 1/2c.
For security reasons, the read password and the read/write password must not be identical.

☐ First select which password you want to change.

☐ Enter the old password in the line "Old password".

☐ Enter the new password in the line "New password".

☐ Repeat the new password in the line "Please re-enter".

Please note that passwords are case-sensitive.

☐ "Data encryption" encrypts the data of the Web-based management which is transferred between your PC and the switch with SNMP V3. You can set "Data encryption" differently for the access with read password and read/write password.

5.3.7 WEB access

This dialog allows you to switch off the Web server on the switch. After the Web server has been switched off, the switch can no longer be accessed via a Web browser.

Note: The Web server may be reactivated via the user interface.
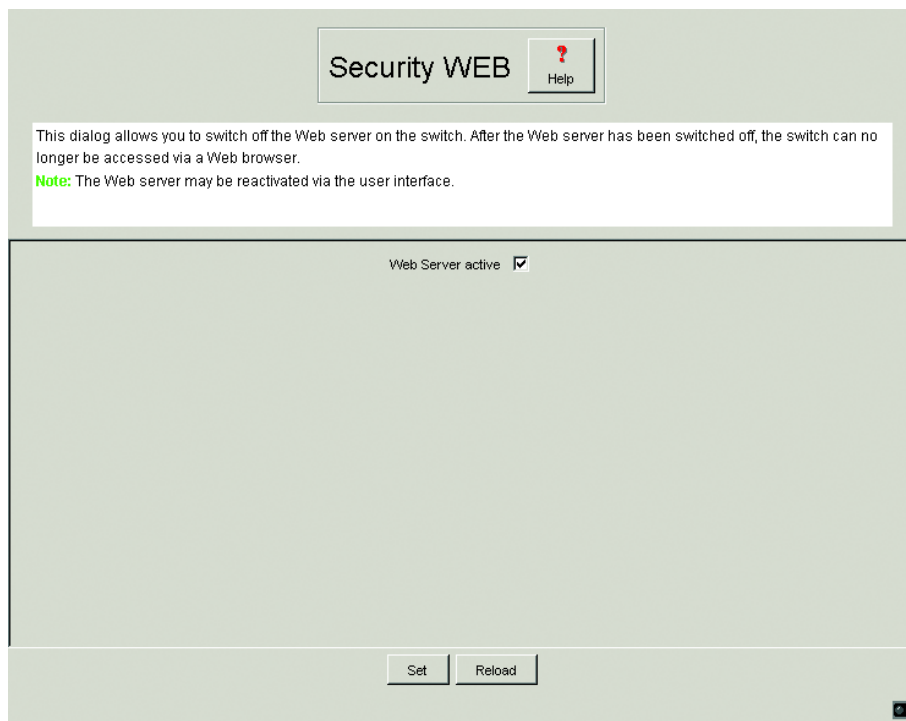
Fig. 57:   Dialog Security

5.3.8 Access for IP addresses

With this dialog you can specify via which IP addresses the switch may be accessed, and what kinds of passwords are to be used.

▶ In the "Index" column, you enter the current number to which the access restriction applies.
▶ In the "IP Address" column, you enter the IP address which may access the switch. No entry in this field, or the entry "0.0.0.0", enables access to the switch from computers with any IP address. In this case, the only access protection is the password.
▶ In the "Name" column, you can enter a name of your choice for the computer with this IP address.
▶ In the "Password" column, you specify whether this computer can access the switch with the read or with the read/write password.
▶ In the "State" column, you mark the entries to which access control applies.

Important: These settings apply to SNMPv1/2c. Because the Web-based interface communicates with SNMPv3, access to the Web-based interface occurs independently of the IP address.

Important: If no line is marked, then there are no access restrictions as regards the IP addresses!

Important: If you mark one or more lines, make sure that at least one of the lines has a read/write password. In this way you yourself keep the write access to the switch.

Note: Shaded table entries are those carried out by other management systems, such as HiVision, and cannot be changed with the Web-based management system.
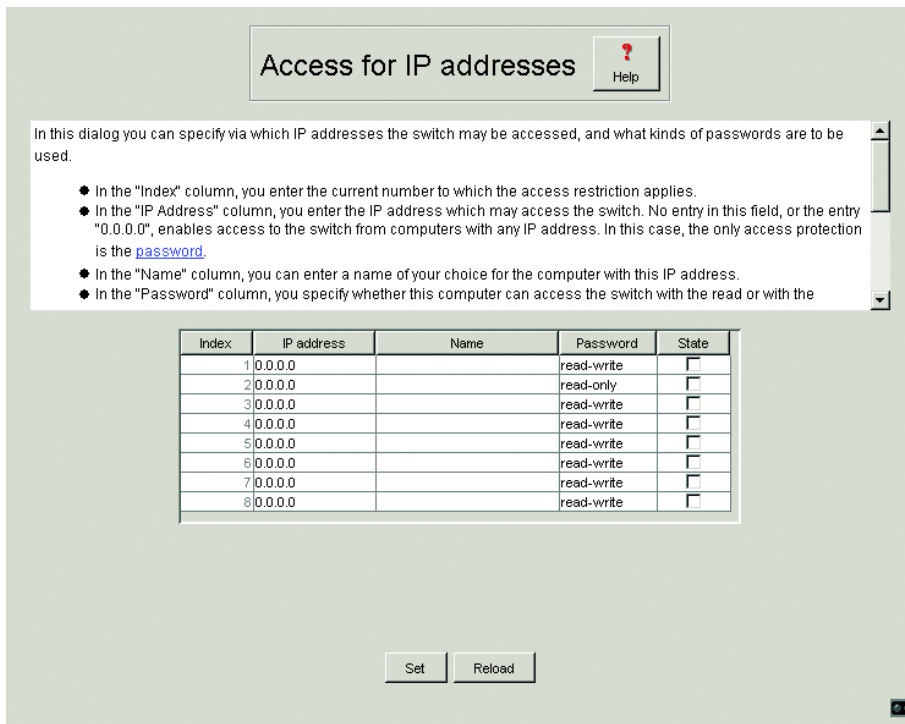
Fig. 58:   Dialog Access for IP addresses

5.3.9 Configuring traps

This dialog allows you to specify which events trigger an alarm (trap) and to whom these alarms should be sent.

▶ In the "IP Address" column, enter the IP address of a network management station to which the traps should be sent.
▶ In the "Name" column, you can enter a name for each recipient.
▶ In the "State" column, you mark the entries which should be taken into account when traps are being sent.

Note: Shaded table entries were carried out by other management systems, such as HiVision, and cannot be changed from here.

The events which can be selected are:

▶ Cold Start: The switch has been switched on.
▶ Link Down: At one port of the switch, the link to the device connected there has been interrupted.
▶ Link up: At one port of the switch, the link to a device connected there has been established.
▶ Authentication: The switch has rejected an unauthorized access attempt (see the Access for IP Addresses dialog).
▶ Chassis: encompasses the following events:
   – Power Supply: The status of a supply voltage has changed (see the System dialog).
   – Signaling Relay: The status of the signal contact has changed.
   – Stand-by: The status of the Redundancy Manager has changed (see the HIPER-Ring dialog "Configuring the HIPER-Ring function" on page 168).
   – AutoConfigAdapter: The AutoConfiguration Adapter, ACA, has been inserted or removed.
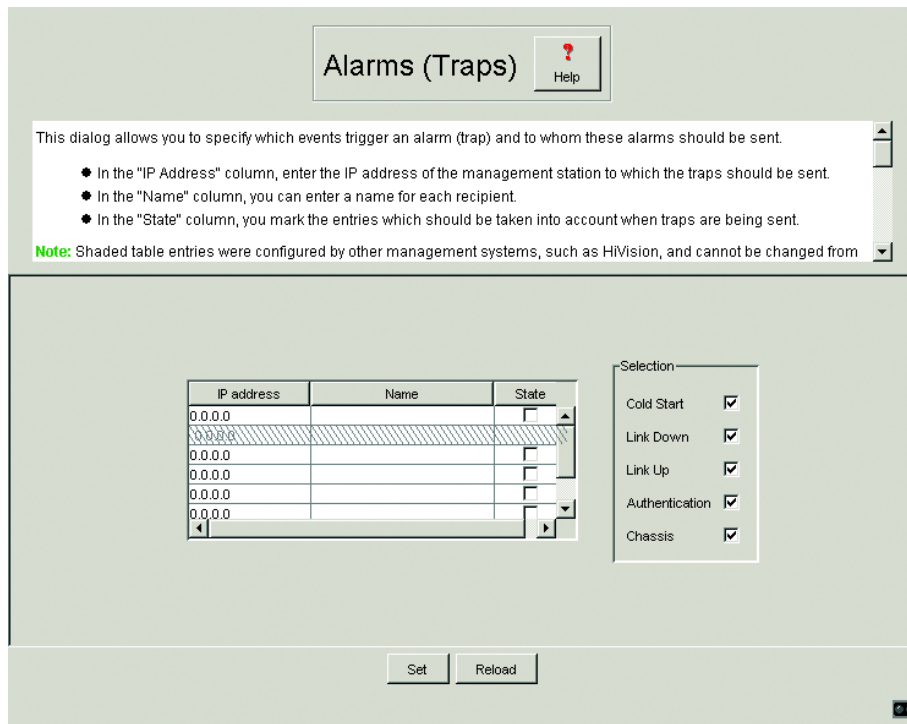
Fig. 59:   Dialog Alarms

5.3.10 Restarting the switch

This dialog allows you to

▶ restart the switch.
▶ reset the MAC address table
▶ reset the port counters
▶ reset the IP counters
▶ reset the protocol counters
▶ delete the log file.

Note: During the restart, the switch temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems such as HiVision.
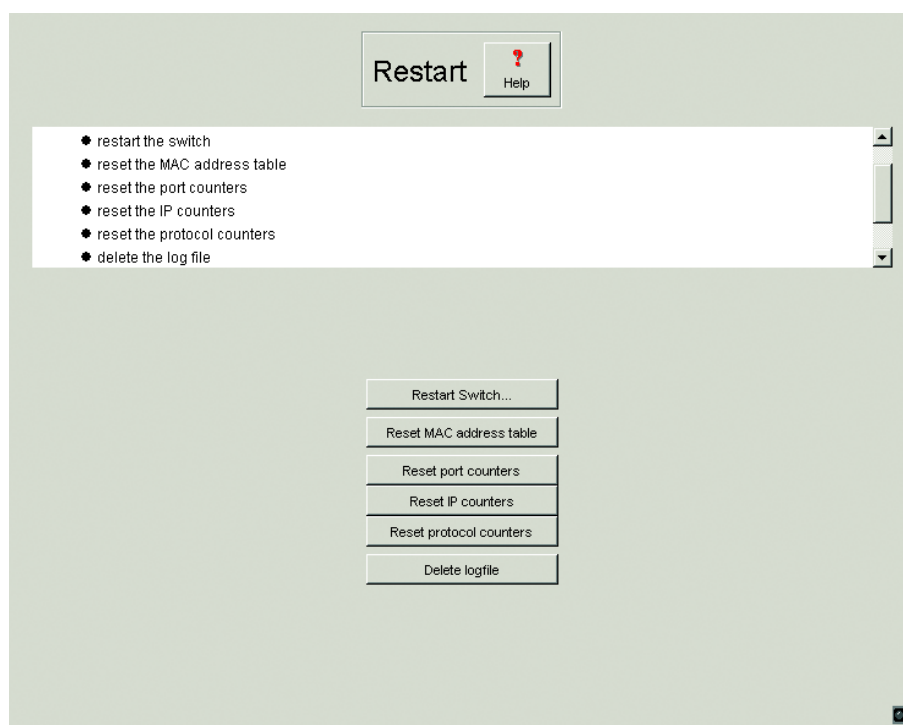
Fig. 60:   Dialog Restart

5.4 Ports

The Ports menu includes:

▶ The port configuration table
▶ The port statistics table

5.4.1 Port configuration table

This table allows you to configure every port of the switch.

▶ In the "Name" column, you can enter a name for every port.
▶ In the "Ports on" column, you can switch on the port by marking it here.
▶ In the "Flow Control" column, you mark this port to specify that flow control is active.
▶ In the "Signal Relay mask" column, you can specify that the signal contact is to be opened when a link alarm occurs.
▶ In the "Autonegotiation" column, you can activate the automatic selection of a port's operating mode by marking the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
▶ In the "Manual Configuration" column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  – 10 Mbit/s half duplex (HDX),
  – 10 Mbit/s full duplex (FDX),
  – 100 Mbit/s HDX and
  – 100 Mbit/s FDX.
▶ In the "Port Priority" column, you can specify the priority (in the range 0 to 7, default 0) with which the switch sends data packets which it receives without a VLAN tag at this port.

Note: The active automatic configuration has priority over the manual configuration.

Note: The following settings are required for the ring ports (see "Redundant ring structure – HIPER-Ring" on page 114):

– 100 MBit/s
– Full duplex
– Autonegotiation off
– Port on.

Fig. 61:   Dialog Port configuration table

5.4.2 Port statistics table

This table shows you the contents of various event counters. After a restart, all the event counters begin again at zero. The counters add up the events sent and the events received.

Fig. 62:   Dialog Port statistics table

5.5 Switching

The Switching menu includes:

▶ Basic Switch Data,
▶ Filtering Database
▶ GMRP / IGMP Configuration

5.5.1 Basic Switch Data

This dialog is used to display the basic switch data and for entering general settings. These settings include:

▶ The entry of the Aging Time for all dynamic entries in the range from 10 to 400 seconds (Unit: 1 second, default setting: 300).
In connection with the router redundancy (see MACH 3000), set the time greater/equal than 30 seconds.
▶ Switching off/permitting the flow control at all ports of the switch which are marked in the port configuration table.

5.5.2 Filtering Database

This table is used for displaying filters. Each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the switch (learned status). Data packets whose destination addresses are entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination addresses are not in the table are sent from the receiving port to all other ports. The following status settings are possible:

▶ learned: the filter was created automatically by the switch.

Fig. 63:   Dialog Filter table

Note: If the redundancy manager is active, it is not possible to make permanent unicast entries.

Note: In the filtering database you can create up to 56 filter for multicast addresses.

5.5.3 Rapid Spanning Tree

The Rapid Spanning Tree algorithm (RSTP) reduces the entire topology of a network connected by bridges to a single tree structure. The root bridge forms the basis of a tree structure. Ring structures are separated according to specified rules. If a path is interrupted, the algorithm cancels the division in order to maintain the data transmission. This enables redundant connections for increased data security (see "Spanning Tree Algorithm" on page 101).

The structure of the tree depends on the root path costs.

▶ The structure is selected so that the path costs between each individual bridge to the root bridge are kept to a minimum.
▶ In the case of a number of paths with the same root path costs, the priority of the bridge identification of the bridge connected to one of these paths decides which bridge should block.

Note: The lowest numerical value signifies the highest priority.

RSTP is compatible with the standard STP. However, the advantages of faster reconfiguration with the RSTP between two bridges are lost if one of the bridges only uses the STP protocol.

■ **Global settings**
These settings apply to the basis board. The administrator usually enters the values to be set for "Hello Time", "Forward Delay" and "Max. Age" in the root bridge. The root bridge then transfers this data to the other bridges. The dialog displays the data received from the root bridge in the left column. In the right column you enter the values which shall apply when this bridge becomes a root bridge.

Note: Because HIPER-Ring and STP use different redundancy concepts, the active RM function prevents enabling of STP

The time entries in the Global dialog are in units of 10 ms.
Example: Max Age = 2000 amounts to 20 seconds.

Variable	Meaning	Possible values	State on delivery
Priority	The priority and the MAC address go together to make up the bridge identification.	0 < n*4096 < 61440	32768
Hello Time	The bridge sends configuration messages (Configuration Bridge Protocol Data Units, CBPDU) if it is the root bridge, or when it is attempting to become the root bridge. Hello Time is the time in hundredths of a second between the sending of two configuration messages (Configuration Bridge Protocol Data Units, CBPDU). This is the current value being used by the bridge.	100 < n*100 < 1000	200
Max Age	Within the "Max Age" time period, the bridge expects to receive a BPDU. If the bridge does not receive a BPDU within this time period, this indicates that the root bridge has failed. The remaining bridges start the operation to specify the new root bridge.	600 - 4000	200
Forward Delay	The condition diagram of the Spanning Tree Protocol has four possible conditions: blocking, hearing, learning and normal. A certain amount of time passes when switching from one condition to another. This time is measured in hundredths of a second and checks how quickly the change is effected. This is the current value being used by the bridge. The condition change from normal to blocking occurs without a time lapse.	400 - 3000	1500

Table 12: Global STP/RSTP settings

■ **Port settings**
These settings apply to every individual port.

Variable	Meaning	Possible values	State on delivery
STP State	Switching STP/RSTP on/off at this port. Switch STP off when connecting a terminal device in order to avoid unnecessary waiting periods.	enable, disable	enable
Priority	The port priority is the first byte of the port identification.	16 < n*16< 240	128
Admin Pathcost	Enter the path costs to indicate preference for redundant paths. If the value is "0", the switch automatically calculates the path costs depending on the transmission rate.	0 - 200 000 000	0
Remove Tag	With the enable setting, the RS2-4R removes the VLAN tag from the frames which it sends at this port.	enable, disable	enable
Admin Edge Port	With Admin Edge Port you specify whether a terminal device (= true) or an (R)STP bridge (= false) shall be connected to this port. During reconfiguration, the Edge Port at a terminal device can switch to forwarding within 4 seconds. In any event, the bridge detects a connected (R)STP bridge and displays it under Ist Edge Port.	true, false	false
Admin Point-ToPointt	The point-to-point connection makes a direct connection between 2 RSTP bridges, serving to keep the reconfiguration time short. Select the forceTrue value if there is a half-duplex connection between 2 RSTP bridges.	auto, forceTrue, forceFalse	auto

Table 13: STP/RSTP port settings

5.6 Extras

The Ports menu includes:

▶ Configuring the DHCP Relay agent,
▶ Configuring the broadcast limiter,
▶ Configuring the HIPER-Ring function,
▶ Settting port mirroring
▶ Disable Learning

5.6.1 DHCP Relay Agent

This dialog allows you to configure the DHCP relay agent. The DHCP relay agent is a function which is integrated into this switch (see "System Configuration via DHCP Option 82" on page 64).

☐ Enter the DHCP server IP address.
If one DHCP server is not available, then you can enter up to three additional DHCP server IP addresses, so that the switch can change to another DHCP server.

☐ With Option 82, a DHCP relay agent which receives a DHCP request adds an "Option 82" field to the request, as long as the request received does not already have such a field.
When the function is switched off, the switch will forward attached "Option 82" fields, but it will not add any. In the "Type" frame, you specify the format in which the device recognition of this switch is entered in the "Option 82" field by the DHCP relay agent.
The options are:
– IP address
– MAC address (setting on delivery)
– System name (client ID).
– other (free definable ID, which you can enter in the following line)
"DHCP server RemoteID entry" shows you the value which you enter when configuring your DHCP server.
"Type display" shows the device recognition in the selected form.

▶ The "Circuit ID" column shows you the value which you enter when configuring your DHCP server. The "Circuit ID" contains the port number and the ID of the VLAN where the DHCP request has been received.

Example for the configuration of your DHCP server (see Fig. 87):
Type: `mac`
DHCP server RemoteID entry: `00 06 00 80 63 00 06 1E`
Circuit-ID: `B3 06 00 00 01 00 01 01`
It follows from this that the „Harwareadresse" in the DHCP server is:
`B306000001000101000600806300061E`

☐ In the "Relay function on/off" column, you can switch this function on/off for each port.

☐ In the "Hirschmann agent" column, you mark the ports to which a Hirschmann switch is connected.

5.6.2 Broadcast limiter

With the broadcast limiter you can define the maximum number of broadcasts allowed out of a port.

In the check box "Broadcast Limiter Mode", you turn the broadcast limiter on/off for all the ports.

Setting options per port:

▶ = 0, no limitation on the broadcasts allowed out of this port.
▶ > 0, maximum number of broadcasts per second that can be sent out of this port.

For further information on the broadcast delimiters, see "Broadcast limiter" on page 100.

5.6.3   Configuring the HIPER-Ring function

This dialog shows you the function of this switch in the HIPER-Ring. The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring.
The RS2-4R is integrated into the ring via the HIPER-Ring ports (Port 3 und 4). The Redundancy Manager is turned on and off by means of a dip switch on the housing . The status of the redundancy manager is active when the ring is open. This occurs when, for example, a data cable or a network component within the ring is down.

Note: The following settings are required for the ring ports (see "Port Configuration Table" on page 165):
– 100 Mbit/s
– full duplex
–   autonegotiation off
–   port on.

■ **Operation**
The HIPER-Ring function you switch on and of with the DIP-Switch in the front panel of the device. The "Operation frame" displays the DIP switch setting.

■ **Information**
"Redundancy guaranteed" tells you that if one of the lines affected by the function fails, a redundant line will take over the function of the failed line.

"Configuration failure" tells you whether the function is configured incompletely or incorrectly.
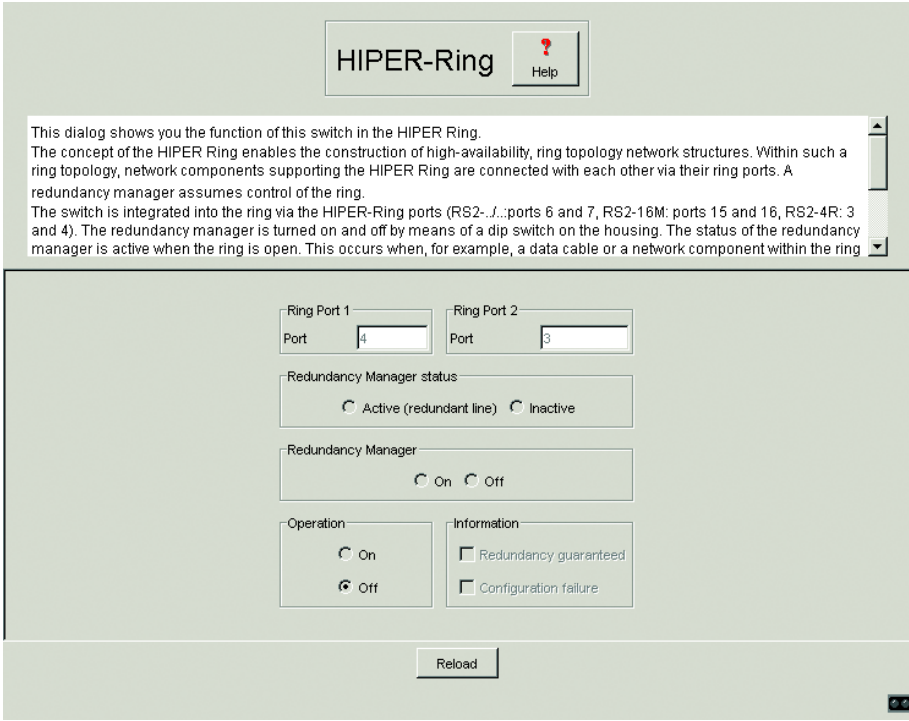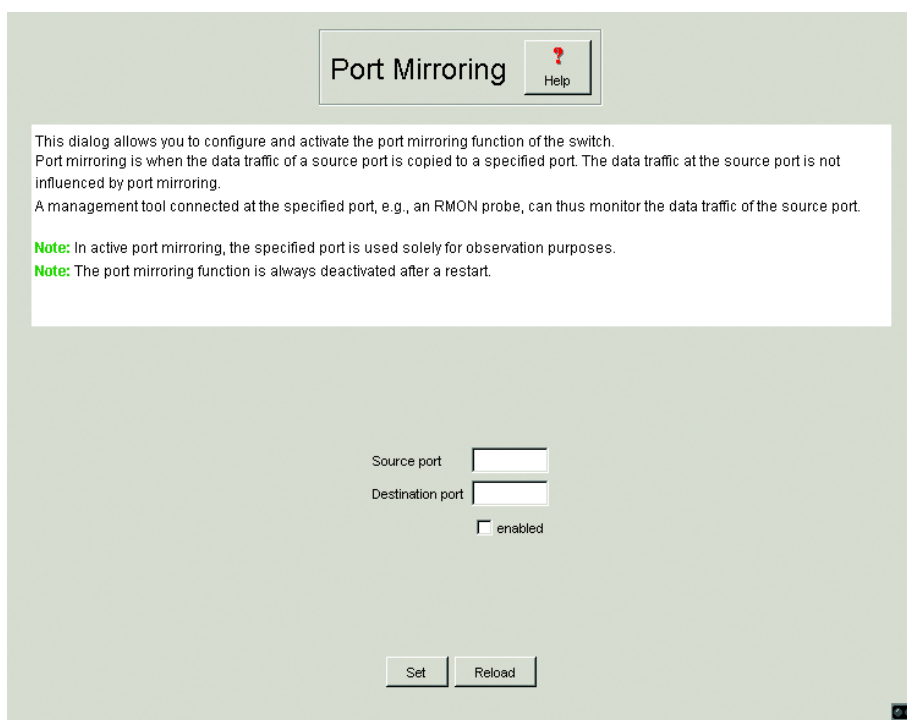
Fig. 64:   Dialog HIPER-Ring

5.6.4 Setting port mirroring

This dialog allows you to configure and activate the port mirroring function of the switch. Port mirroring is when the data traffic of a source port is copied to a specified port. The data traffic at the source port is not influenced by port mirroring. A management tool connected at the specified port, e.g., an RMON probe, can thus monitor the data traffic of the source port.

Note: In active port mirroring, the specified port is used solely for observation purposes.

Note: The port mirroring function is always deactivated after a restart.

Fig. 65:   Dialog Configure Port Mirroring

5.6.5 Switching the learning function on and off

This dialog allows you to monitor the data for all the ports. You mark the Disable Learning function to switch off the learning function of the RS2-4R. Then the RS2-4R will transfer all the data from each port to all the other ports.

Note: The learning function is always activated after a restart.
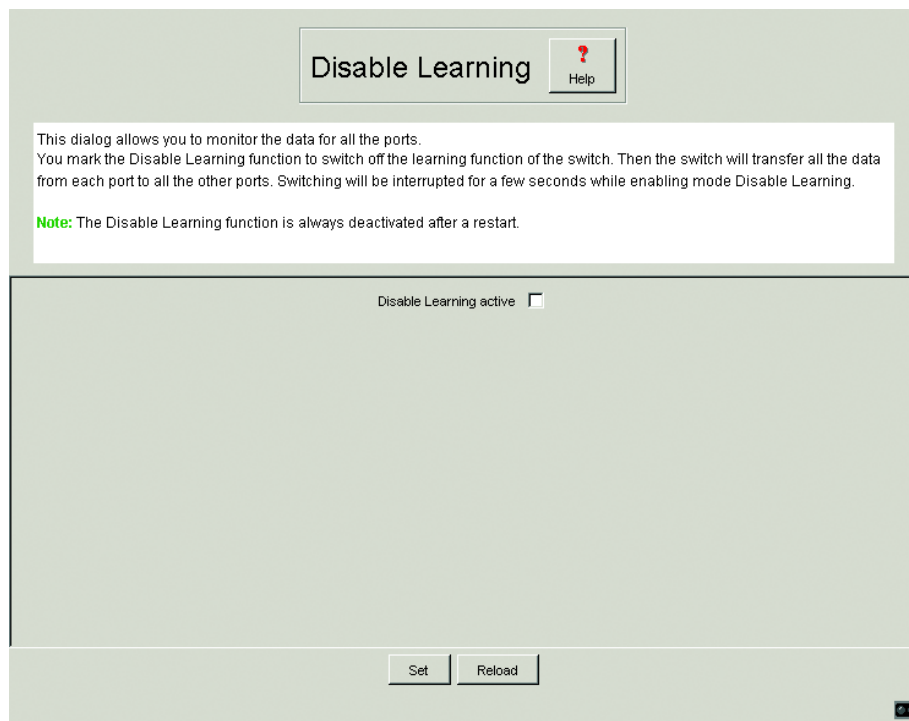
Fig. 66:   Dialog Disable learning

5.6.6 Diagnostics

The following reports are available for diagnostic purposes. In service situations, they pass the necessary information onto the technician.

► Watson
► Logfile

6 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the **object classes**. The "leaves" of the MIB are called **generic object classes**.

Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified.

The **object description** or the **object ID** (OID) identifies the object class.

The **subidentifier** (SID) is used for instantiation.

Example:
The generic object class

```
hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)
```

is the description of the abstract information "power supply state". However, it is not possible to read any information from this, as the system does not know which power supply is meant.

Specification of the subidentifier (2) images this abstract information onto reality (instantiates it), which means that it refers to power supply 2. A value is assigned to this instance and can then be read. The instance "get `1.3.6.1.4.1.248.14.1.2.1.3`2", for example, returns the response "1", which means that the power supply unit is ready for operation.

The following abbreviations are used in the MIB:

Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power

sys   System
UI   User Interface
Upr   Upper (e.g. threshold value)
ven   Vendor = manufacturer (Hirschmann)

Definition of the syntax terms used:

Integer	An integer in the range 0 - 2^{32}
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC address	12-digit hexadecimal number in accordance with ISO / IEC 8802-3
Object Identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)
Octet String	ASCII character string
PSID	Power Supply Identification (number of the power supply unit)
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in the range 0 - 2^{32}
Timeout	Time value in hundredths of a second Time value = integer in the range 0-2^{32}
Type field	4-digit hexadecimal number in accordance with ISO / IEC 8802-3
Counter	Integer (0 - 2^{32}) whose value is incremented by 1 when certain events occur.
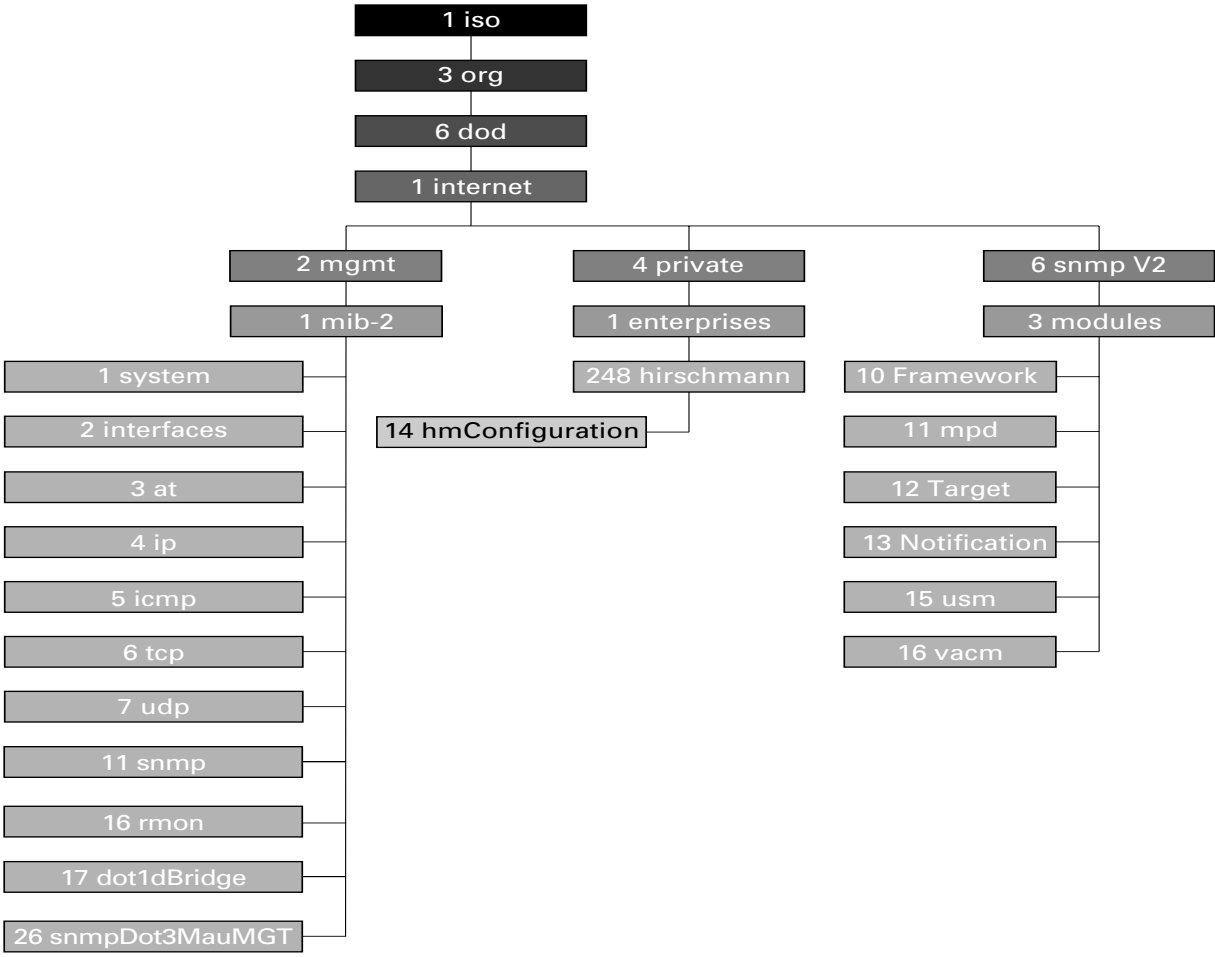
Fig. 67:   Tree structure of the Hirschmann MIB

6.1 MIB II

6.1.1 System Group (1.3.6.1.2.1.1)

The System Group is a required group for all systems. It contains system-related objects. If an agent has no value for a variable, then the response returned includes a string of length 0.

(1) system
```
|-- (1) sysDescr
|-- (2) sysObjectID
|-- (3) sysUpTime
|-- (4) sysContact
|-- (5) sysName
|-- (6) sysLocation
|-- (7) sysServices
|-- (8) sysORLastChange
|-- (9) sysORTable
|   |-- (1) sysOREntry
|   |   |-- (1) sysORIndex
|   |   |-- (2) sysORID
|   |   |-- (3) sysORDescr
|   |   |-- (4) sysORUpTime
```

sysDescr

OID   1.3.6.1.2.1.1.1.0

Syntax   Octet string (size: 0-255)

Access   Read

Description   A verbal description of the entry. This value should con-
               tain the full name and version number of
               - the type of system hardware
               - the operating system software, and
               - the network software.
               The description must consist only of printable ASCII char-
               acters.

sysObjectID

OID1.3.60,2.2.1.1.1.0

Syntax   Object identifier

Access   Read

Description   The authorization identification of the manufacturer of the
               network management system which is integrated into this
               device. This value is placed within the SMI enterprises
               subtree (1.3.6.1.4.1) and describes which type of device
               is being managed. For example: if the manufacturer "Hir-
               schmann GmbH" is assigned the subtree 1.3.6.1.4.1.248,
               then he can assign his bridge the identifier
               1.3.6.1.4.1.2.248.2.1.

sysUpTime

OID   1.3.6.1.2.1.1.3.0

Syntax   Time ticks

Access   Read

Description   The time in 1/100 seconds since the last reset of the network management unit.

sysContact

OID1.3.6.1.2.1.1.4.0

Syntax   Octet string (size: 0-255)

Access   Read and write

Description   The clear-text identification of the contact person for this managed node along with the information about how that person is to be contacted.

sysName

OID1.3.6.1.2.1.1.5.0

Syntax   Octet string (size: 0-255)

Access   Read and write

Description   A name for this node identifying it for administration. By convention, this is the fully qualified name in the domain.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet string (size: 0-255)
Access	Read and write
Description	The physical location of this node (e.g. "staircase, 3rd floor")

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0-127)
Access	Read
Description	This value designates the set of services offered by this device. It is the sum of several terms. For each layer of the OSI reference model there is one term in the form (2^{L-1}), where L identifies the layer. For example: For a node that primarily performs routing functions the value would be (2^{3-1}) = 4. For a node that is a host and which offers application services the value would be (2^{4-1}) + (2^{7-1}) = 72.

6.1.2 Interface group (1.3.6.1.2.1.2)

The interface group contains information about the device interfaces.

(2) `interfaces`

```
|-- (1) ifNumber
|-- (2) ifTable
|   |-- (1) ifEntry
|   |   |-- (1) ifIndex
|   |   |-- (2) ifDescr
|   |   |-- (3) ifType
|   |   |-- (4) ifMtu
|   |   |-- (5) ifSpeed
|   |   |-- (6) ifPhysAddress
|   |   |-- (7) ifAdminStatus
|   |   |-- (8) ifOperStatus
|   |   |-- (9) ifLastChange
|   |   |-- (10) ifInOctets
|   |   |-- (11) ifInUcastPkts
|   |   |-- (12) ifInNUcastPkts
|   |   |-- (13) ifInDiscards
|   |   |-- (14) ifInErrors
|   |   |-- (15) ifInUnknownProtos
|   |   |-- (16) ifOutOctets
|   |   |-- (17) ifOutUcastPkts
|   |   |-- (18) ifOutNUcastPkts
|   |   |-- (19) ifOutDiscards
|   |   |-- (20) ifOutErrors
|   |   |-- (21) ifOutQLen
|   |   |-- (22) ifSpecific
```

6.1.3 Address Translation Group (1.3.6.1.2.1.3)

The Address Translation Group is required for all systems. It contains infor-
mation about the assignment of addresses.

(3) `at`

```
|-- (1) atTable
|   |-- (1) atEntry
|   |   |-- (1) atIfIndex
|   |   |-- (2) atPhysAddress
|   |   |-- (3) atNetAddress
```

6.1.4 Internet Protocol Group (1.3.6.1.2.1.4)

The Internet Protocol Group is required for all systems. It contains informa-
tion affecting IP transmission.

(4) `ip`

```
|-- (1) ipForwarding
|-- (2) ipDefaultTTL
|-- (3) ipInReceives
|-- (4) ipInHdrErrors
|-- (5) ipInAddrErrors
|-- (6) ipForwDatagrams
|-- (7) ipInUnknownProtos
|-- (8) ipInDiscards
|-- (9) ipInDelivers
|-- (10) ipOutRequests
|-- (11) ipOutDiscards
|-- (12) ipOutNoRoutes
|-- (13) ipReasmTimeout
|-- (14) ipReasmReqds
|-- (15) ipReasmOKs
|-- (16) ipReasmFails
|-- (17) ipFragOKs
```

```
|
|-- (18) ipFragFails
|-- (19) ipFragCreates
|-- (20) ipAddrTable
|   |-- (1) ipAddrEntry
|   |   |-- (1) ipAdEntAddr
|   |   |-- (2) ipAdEntIfIndex
|   |   |-- (3) ipAdEntNetMask
|   |   |-- (4) ipAdEntBcastAddr
|   |   |-- (5) ipAdEntReasmMaxSize
|-- (21) ipRouteTable
|   |-- (1) ipRouteEntry
|   |   |-- (1) ipRouteDest
|   |   |-- (2) ipRouteIfIndex
|   |   |-- (3) ipRouteMetric1
|   |   |-- (4) ipRouteMetric2
|   |   |-- (5) ipRouteMetric3
|   |   |-- (6) ipRouteMetric4
|   |   |-- (7) ipRouteNextHop
|   |   |-- (8) ipRouteType
|   |   |-- (9) ipRouteProto
|   |   |-- (10) ipRouteAge
|   |   |-- (11) ipRouteMask
|   |   |-- (12) ipRouteMetric5
|   |   |-- (13) ipRouteInfo
|-- (22) ipNetToMediaTable
|   |-- (1) ipNetToMediaEntry
|   |   |-- (1) ipNetToMediaIfIndex
|   |   |-- (2) ipNetToMediaPhysAddress
|   |   |-- (3) ipNetToMediaNetAddress
|   |   |-- (4) ipNetToMediaType
|-- (23) ipRoutingDiscards
```

6.1.5 ICMP Group (1.3.6.1.2.1.5)

The Internet Control Message Protocol group is obligatory for all systems. It contains information on error handling and control for data exchange in the Internet.

(5) `icmp`

   -- (1) `icmpInMsgs`
   -- (2) `icmpInErrors`
   -- (3) `icmpInDestUnreachs`
   -- (4) `icmpInTimeExcds`
   -- (5) `icmpInParmProbs`
   -- (6) `icmpInSrcQuenchs`
   -- (7) `icmpInRedirects`
   -- (8) `icmpInEchos`
   -- (9) `icmpInEchoReps`
   -- (10) `icmpInTimestamps`
   -- (11) `icmpInTimestampReps`
   -- (12) `icmpInAddrMasks`
   -- (13) `icmpInAddrMaskReps`
   -- (14) `icmpOutMsgs`
   -- (15) `icmpOutErrors`
   -- (16) `icmpOutDestUnreachs`
   -- (17) `icmpOutTimeExcds`
   -- (18) `icmpOutParmProbs`
   -- (19) `icmpOutSrcQuenchs`
   -- (20) `icmpOutRedirects`
   -- (21) `icmpOutEchos`
   -- (22) `icmpOutEchoReps`
   -- (23) `icmpOutTimestamps`
   -- (24) `icmpOutTimestampReps`
   -- (25) `icmpOutAddrMasks`
   -- (26) `icmpOutAddrMaskReps`

6.1.6 Transfer Control Protocol Group (1.3.6.1.2.1.6)

The Transfer Control Protocol Group is required for all systems that have implemented TCP. Instances of objects that describe information about a particular TCP connection exist only as long as the connection exists.

(6) `tcp`

```
|-- (1) tcpRtoAlgorithm
|-- (2) tcpRtoMin
|-- (3) tcpRtoMax
|-- (4) tcpMaxConn
|-- (5) tcpActiveOpens
|-- (6) tcpPassiveOpens
|-- (7) tcpAttemptFails
|-- (8) tcpEstabResets
|-- (9) tcpCurrEstab
|-- (10) tcpInSegs
|-- (11) tcpOutSegs
|-- (12) tcpRetransSegs
|-- (13) tcpConnTable
|    |-- (1) tcpConnEntry
|    |    |-- (1) tcpConnState
|    |    |-- (2) tcpConnLocalAddress
|    |    |-- (3) tcpConnLocalPort
|    |    |-- (4) tcpConnRemAddress
|    |    |-- (5) tcpConnRemPort
|-- (14) tcpInErrs
|-- (15) tcpOutRsts
```

6.1.7 User Datagram Protocol Group (1.3.6.1.2.1.7)

The User Datagram Protocol Group is required for all systems that have implemented UDP.

(7) `udp`

```
|-- (1) udpInDatagrams
|-- (2) udpNoPorts
|-- (3) udpInErrors
|-- (4) udpOutDatagrams
|-- (5) udpTable
|   |-- (1) udpEntry
|   |   |-- (1) udpLocalAddress
|   |   |-- (2) udpLocalPort
```

6.1.8 Simple Network Management Protocol Group (1.3.6.1.2.1.11)

The Simple Network Management Protocol group is required for all systems. In SNMP installations that have been optimized to support either just one agent or one management station some of the listed objects will contain the value "0".

(11) `snmp`

```
-- (1) snmpInPkts
-- (2) snmpOutPkts
-- (3) snmpInBadVersions
-- (4) snmpInBadCommunityNames
-- (5) snmpInBadCommunityUses
-- (6) snmpInASNParseErrs
-- (7) not used
-- (8) snmpInTooBigs
-- (9) snmpInNoSuchNames
-- (10) snmpInBadValues
-- (11) snmpInReadOnlys
-- (12) snmpInGenErrs
-- (13) snmpInTotalReqVars
-- (14) snmpInTotalSetVars
-- (15) snmpInGetRequests
-- (16) snmpInGetNexts
-- (17) snmpInSetRequests
-- (18) snmpInGetResponses
-- (19) snmpInTraps
-- (20) snmpOutTooBigs
-- (21) snmpOutNoSuchNames
-- (22) snmpOutBadValues
-- (23) not used
-- (24) snmpOutGenErrs
-- (25) snmpOutGetRequests
-- (26) snmpOutGetNexts
-- (27) snmpOutSetRequests
-- (28) snmpOutGetResponses
-- (29) snmpOutTraps
-- (30) snmpEnableAuthenTraps
-- (31) snmpSilentDrops
-- (32) snmpProxyDrops
```

6.1.9 RMON Group (1.3.6.1.2.1.16)

This part of the MIB provides a continuous flow of current and historical network component data to the network management. The configuration of alarms and events controls the evaluation of network component counters. The agents inform the management station of the evaluation result by means of traps, depending on the configuration.

```
(16) rmon

   |--(1) statistics
   |   |--(1) etherStatsTable
   |   |   |--(1) etherStatsEntry
   |   |   |     |--(1) etherStatsIndex
   |   |   |     |--(2) etherStatsDataSource
   |   |   |     |--(3) etherStatsDropEvents
   |   |   |     |--(4) etherStatsOctets
   |   |   |     |--(5) etherStatsPkts
   |   |   |     |--(6) etherStatsBroadcastPkts
   |   |   |     |--(7) etherStatsMulticastPkts
   |   |   |     |--(8) etherStatsCRCAlignErrors
   |   |   |     |--(9) etherStatsUndersizePkts
   |   |   |     |--(10) etherStatsOversizePkts
   |   |   |     |--(11) etherStatsFragments
   |   |   |     |--(12) etherStatsJabbers
   |   |   |     |--(13) etherStatsCollisions
   |   |   |     |--(14) etherStatsPkts64Octets
   |   |   |     |--(15) etherStatsPkts65to127Octets
   |   |   |     |--(16) etherStatsPkts128to255Octets
   |   |   |     |--(17) etherStatsPkts256to511Octets
   |   |   |     |--(18) etherStatsPkts512to1023Octets
   |   |   |     |--(19) etherStatsPkts1024to1518Octets
   |   |   |     |--(20) etherStatsOwner
   |   |   |     |--(21) etherStatsStatus
   |--(2) history (2)
   |   |--(1) historyControlTable
   |   |   |--(1) historyControlEntry
   |   |   |     |--(1) historyControlIndex
   |   |   |     |--(2) historyControlDataSource
   |   |   |     |--(3) historyControlBucketsRequested
   |   |   |     |--(4) historyControlBucketsGranted
   |   |   |     |--(5) historyControlInterval
   |   |   |     |--(6) historyControlOwner
```

```
|  |  |  |--(7) historyControlStatus
|  |--(2) etherHistoryTable
|  |  |--(1) etherHistoryEntry
|  |  |  |--(1) etherHistoryIndex
|  |  |  |--(2) etherHistorySampleIndex
|  |  |  |--(3) etherHistoryIntervalStart
|  |  |  |--(4) etherHistoryDropEvents
|  |  |  |--(5) etherHistoryOctets
|  |  |  |--(6) etherHistoryPkts
|  |  |  |--(7) etherHistoryBroadcastPkts
|  |  |  |--(8) etherHistoryMulticastPkts
|  |  |  |--(9) etherHistoryCRCAlignErrors
|  |  |  |--(10) etherHistoryUndersizePkts
|  |  |  |--(11) etherHistoryOversizePkts
|  |  |  |--(12) etherHistoryFragments
|  |  |  |--(13) etherHistoryJabbers
|  |  |  |--(14) etherHistoryCollisions
|  |  |  |--(15) etherHistoryUtilization
|--(3) alarm
|  |--(1) alarmTable
|  |  |--(1) alarmEntry
|  |  |  |--(1) alarmIndex
|  |  |  |--(2) alarmInterval
|  |  |  |--(3) alarmVariable
|  |  |  |--(4) alarmSampleType
|  |  |  |--(5) alarmValue
|  |  |  |--(6) alarmStartupAlarm
|  |  |  |--(7) alarmRisingThreshold
|  |  |  |--(8) alarmFallingThreshold
|  |  |  |--(9) alarmRisingEventIndex
|  |  |  |--(10) alarmFallingEventIndex
|  |  |  |--(11) alarmOwner
|  |  |  |--(12) alarmStatus
|--(9) event
|  |--(1) eventTable
|  |  |--(1) eventEntry
|  |  |  |--(1) eventIndex
|  |  |  |--(2) eventDescription
|  |  |  |--(3) eventType
|  |  |  |--(4) eventCommunity
|  |  |  |--(5) eventLastTimeSent
|  |  |  |--(6) eventOwner
|  |  |  |--(7) eventStatus
```

```
|   |--(2) logTable
|   |   |--(1) logEntry
|   |   |   |--(1) logEventIndex
|   |   |   |--(2) logIndex
|   |   |   |--(3) logTime
|   |   |   |--(4) logDescription
|--(19) probeConfig
|   |--(15) smonCapabilities
|--(22) switchRMON
|   |--(1) smonMIBObjects
|   |   |--(1) dataSourceCaps
|   |   |   |--(1) dataSourceCapsTable
|   |   |   |   |--(1) dataSourceCapsEntry
|   |   |   |   |   |--(1) dataSourceCapsObject
|   |   |   |   |   |--(2) dataSourceRmonCaps
|   |   |   |   |   |--(3) dataSourceCopyCaps
|   |   |   |   |   |--(4) dataSourceCapsIfIndex
|   |   |--(3) portCopyConfig
|   |   |   |--(1) portCopyTable
|   |   |   |   |--(1) portCopyEntry
|   |   |   |   |   |--(1) portCopySource
|   |   |   |   |   |--(2) portCopyDest
|   |   |   |   |   |--(3) portCopyDestDropEvents
|   |   |   |   |   |--(4) portCopyDirection
|   |   |   |   |   |--(5) portCopyStatus
```

6.1.10 dot1dBridge (1.3.6.1.2.1.17)

This part of the MIB contains bridge-specific objects.

```
(17) dot1dBridge

   |--(1) dot1dBase
   |    |--(1) dot1dBaseBridgeAddress
   |    |--(2) dot1dBaseNumPorts
   |    |--(3) dot1dBaseType
   |    |--(4) dot1dBasePortTable
   |    |    |--(1) dot1dBasePortEntry
   |    |    |    |--(1) dot1dBasePort
   |    |    |    |--(2) dot1dBasePortIfIndex
   |    |    |    |--(3) dot1dBasePortCircuit
   |    |    |    |--(4) dot1dBasePortDelayExceededDiscards
   |    |    |    |--(5) dot1dBasePortMtuExceededDiscards
   |--(2) dot1dStp
   |    |--(1) dot1dStpProtocolSpecification
   |    |--(2) dot1dStpPriority
   |    |--(3) dot1dStpTimeSinceTopologyChange
   |    |--(4) dot1dStpTopChanges
   |    |--(5) dot1dStpDesignatedRoot
   |    |--(6) dot1dStpRootCost
   |    |--(7) dot1dStpRootPort
   |    |--(8) dot1dStpMaxAge
   |    |--(9) dot1dStpHelloTime
   |    |--(10) dot1dStpHoldTime
   |    |--(11) dot1dStpForwardDelay
   |    |--(12) dot1dStpBridgeMaxAge
   |    |--(13) dot1dStpBridgeHelloTime
   |    |--(14) dot1dStpBridgeForwardDelay
   |    |--(15) dot1dStpPortTable
   |    |    |--(1) dot1dStpPortEntry
   |    |    |    |--(1) dot1dStpPort
   |    |    |    |--(2) dot1dStpPortPriority
   |    |    |    |--(3) dot1dStpPortState
   |    |    |    |--(4) dot1dStpPortEnable
   |    |    |    |--(5) dot1dStpPortPathCost
   |    |    |    |--(6) dot1dStpPortDesignatedRoot
   |    |    |    |--(7) dot1dStpPortDesignatedCost
   |    |    |    |--(8) dot1dStpPortDesignatedBridge
   |    |    |    |--(9) dot1dStpPortDesignatedPort
```

```
|  |  |     |--(10) dot1dStpPortForwardTransitions
|  |  |     |--(11) dot1dStpPortPathCost32
|  |--(16) dot1dStpVersion
|  |--(17) dot1dStpTxHoldCount
|  |--(18) dot1dStpPathCostDefault
|  |--(19) dot1dStpExtPortTable
|  |     |--(1) dot1dStpExtPortEntry
|  |     |     |--(1) dot1dStpPortProtocolMigration
|  |     |     |--(2) dot1dStpPortAdminEdgePort
|  |     |     |--(3) dot1dStpPortOperEdgePort
|  |     |     |--(4) dot1dStpPortAdminPointToPoint
|  |     |     |--(5) dot1dStpPortOperPointToPoint
|  |     |     |--(6) dot1dStpPortAdminPathCost
|--(3) dot1dSr
|--(4) dot1dTp
|  |--(1) dot1dTpLearnedEntryDiscards
|  |--(2) dot1dTpAgingTime
|  |--(3) dot1dTpFdbTable
|  |     |--(1) dot1dTpFdbEntry
|  |     |     |--(1) dot1dTpFdbAddress
|  |     |     |--(2) dot1dTpFdbPort
|  |     |     |--(3) dot1dTpFdbStatus
|  |--(4) dot1dTpPortTable
|  |     |--(1) dot1dTpPortEntry
|  |     |     |--(1) dot1dTpPort
|  |     |     |--(2) dot1dTpPortMaxInfo
|  |     |     |--(3) dot1dTpPortInFrames
|  |     |     |--(4) dot1dTpPortOutFrames
|  |     |     |--(5) dot1dTpPortInDiscards
|--(6) pBridgeMIB
|  |--(1) pBridgeMIBObjects
|  |  |--(1) dot1dExtBase
|  |  |     |--(1) dot1dDeviceCapabilities
|  |  |     |--(2) dot1dTrafficClassesEnabled
|  |  |     |--(3) dot1dGmrpStatus
|  |  |     |--(4) dot1dPortCapabilitiesTable
|  |  |  |     |--(1) dot1dPortCapabilitiesEntry
|  |  |  |     |  |--(1) dot1dPortCapabilities
|  |  |--(2) dot1dPriority
|  |  |  |--(1) dot1dPortPriorityTable
|  |  |  |  |--(1) dot1dPortPriorityEntry
|  |  |  |  |  |--(1) dot1dPortDefaultUserPriority
|  |  |  |  |  |--(2) dot1dPortNumTrafficClasses
```

```
|  |  |   |--(3) dot1dTrafficClassTable
|  |  |   |  |--(1) dot1dPortPriorityEntry
|  |  |   |  |  |--(1) dot1dTrafficClassPriority
|  |  |   |  |  |--(2) dot1dTrafficClass
|--(7) qBridgeMIB
|  |--(1) qBridgeMIBObjects
|  |  |--(1) dot1qBase
|  |  |  |--(1) dot1qVlanVersionNumber
|  |  |  |--(2) dot1qMaxVlanId
|  |  |  |--(3) dot1qMaxSupportedVlans
|  |  |  |--(4) dot1qNumVlans
|  |  |  |--(5) dot1qGvrpStatus
|  |  |--(2) dot1qTp
|  |  |  |--(1) dot1qFdbTable
|  |  |  |  |--(1) dot1qFdbEntry
|  |  |  |  |  |--(1) dot1qFdbId
|  |  |  |  |  |--(2) dot1qFdbDynamicCount
|  |  |  |--(2) dot1qTpFdbTable
|  |  |  |  |--(1) dot1qTpFdbEntry
|  |  |  |  |  |--(1) dot1qTpFdbAddress
|  |  |  |  |  |--(2) dot1qTpFdbPort
|  |  |  |  |  |--(3) dot1qTpFdbStatus
```

6.1.11 MAU Management Group (1.3.6.1.2.1.26)

The MAU Management Group is responsible for setting the autonegotiation parameters.

```
(26) snmpDot3MauMgt
   |--(2) dot3IfMauBasicGroup
   |    |--(1) ifMauTable
   |    |    |--(1) ifMauEntry
   |    |    |    |-- (1) ifMauIfIndex
   |    |    |    |-- (2) ifMauIndex
   |    |    |    |-- (3) ifMauType
   |    |    |    |-- (4) ifMauStatus
   |    |    |    |-- (5) ifMauMediaAvailable
   |    |    |    |-- (6) ifMauMediaAvailableStateExits
   |    |    |    |-- (7) ifMauJabberState
   |    |    |    |-- (8) ifMauJabberingStateEnters
   |    |    |    |-- (9) ifMauFalseCarriers
   |    |    |    |-- (10)ifMauTypeList
   |    |    |    |-- (11)ifMauDefaultType
   |    |    |    |-- (12)ifMauAutoNegSupported
   |--(5) dot3IfMauAutoNegGroup
   |    |--(1) ifMauAutoNegTable
   |    |    |-- (1) ifMauAutoNegEntry
   |    |    |    |-- (1) ifMauAutoNegAdminStatus
   |    |    |    |-- (2) ifMauAutoNegRemoteSignaling
   |    |    |    |-- (4) ifMauAutoNegConfig
   |    |    |    |-- (5) ifMauAutoNegCapability
   |    |    |    |-- (6) ifMauAutoNegCapAdvertised
   |    |    |    |-- (7) ifMauAutoNegCapReceived
   |    |    |    |-- (8) ifMauAutoNegRestart
```

6.2 Private MIB

The private MIB is for configuring the device-specific properties of the RS2-4R.
The groups below are implemented in the RS2-4R from the private MIB hmConfiguration (OID = 1.3.6.1.4.1.248.14).

▶ hmChassis   (OID = 1.3.6.1.4.1.248.14.1)
▶ hmAgent   (OID = 1.3.6.1.4.1.248.14.2)
▶ hmUserGroup   (OID = 1.3.6.1.4.1.248.14.3)
▶ hmRingRedundancy   (OID = 1.3.6.1.4.1.248.14.5)

6.2.1 Device Group

The Device group contains information on the status of the hardware.

```
(14) hmConfiguration

   |--(1) hmChassis
   |   |--(1) hmSystemTable
   |   |   |--(1) hmSysProduct
   |   |   |--(2) hmSysVersion
   |   |   |--(3) hmSysGroupCapacity
   |   |   |--(4) hmSysGroupMap
   |   |   |--(5) hmSysMaxPowerSupply
   |   |   |--(6) hmSysMaxFan
   |   |   |--(7) hmSysGroupModuleCapacity
   |   |   |--(8) hmSysModulePortCapacity
   |   |   |--(9) hmSysGroupTable
   |   |   |   |--(1) hmSysGroupEntry
   |   |   |   |   |--(1) hmSysGroupID
   |   |   |   |   |--(2) hmSysGroupType
   |   |   |   |   |--(3) hmSysGroupDescription
   |   |   |   |   |--(4) hmSysGroupHwVersion
   |   |   |   |   |--(5)  hmSysGroupSwVersion
```

```
|   |   |   |     |--(6) hmSysGroupModuleMap
|   |   |   |     |--(7) hmSysGroupAction
|   |   |   |     |--(8) hmSysGroupActionResult
|   |   |--(11) hmInterfaceTable
|   |   |   |--(1) hmIfEntry
|   |   |   |     |--(1) hmIfaceGroupID
|   |   |   |     |--(2) hmIfaceID
|   |   |   |     |--(3) hmIfaceStpEnable
|   |   |   |     |--(4) hmIfaceLinkType
|   |   |   |     |--(5) hmIfaceAction
|   |   |   |     |--(6) hmIfaceNextHopMacAddress
|   |   |   |     |--(7) hmIfaceFlowControl
|   |   |   |     |--(8) hmIfacePriorityThreshold
|   |   |   |     |--(9) hmIfaceName
|   |   |   |     |--(10) hmIfaceTrunkID
|   |   |   |     |--(11) hmIfacePrioTOSEnable
|   |   |   |     |--(12) hmIfaceBcastLimit
|   |   |   |     |--(13) hmIfaceUtilization
|   |   |   |     |--(14) hmIfaceUtilizationControlInterval
|   |   |--(20) hmSysChassisName
|   |   |--(21) hmSysStpEnable
|   |   |--(22) hmSysFlowControl
|   |   |--(23) hmSysBOOTPEnable
|   |   |--(24) hmSysDHCPEnable
|   |   |--(25) hmSysTelnetEnable
|   |   |--(26) hmSysHTTPEnable
|   |   |--(27) hmSysPlugAndPlay
|   |   |--(29) hmBcastLimiterMode
|   |   |--(30) hmSystemTime
|   |--(2) hmPSTable
|   |   |--(1) hmPSEntry
|   |   |   |--(1) hmPSSysID
|   |   |   |--(2) hmPSID
|   |   |   |--(3) hmPSState
|   |--(5) hmCurrentAddressTable
|   |   |--(1) hmCurrentAddressEntry
|   |--(10) hmRS2ext
|   |   |--(1) hmRS2OperMode
|   |   |--(2) hmRS2ConfigError
|   |   |--(3) hmRS2SigRelayState
|   |   |--(4) hmSigLinkTable
|   |   |   |--(1) hmSigLinkEntry
|   |   |   |   |--(1) hmSigLinkID
```

```
|  |  |  |   |--(2) hmSigLinkAlarm
|  |  |--(5) hmSigTrapReason
|  |  |--(6) hmSigReasonIndex
|  |  |--(7) hmRS2TopologyGroup
|  |  |   |--(1) hmRS2PartnerIpAddress
|  |  |   |--(2) hmRS2TopologyTable
|  |  |   |   |--(1) hmRS2TopologyEntry
|  |  |   |   |   |--(1) hmRS2TopologyLinkID
|  |  |   |   |   |--(2) hmRS2TopologyIpAddress
|  |  |--(9) hmRS2DisableLearningGroup
|  |  |   |--(1) hmRS2DisableLearningStatus
|  |  |--(10) hmRS2SigRelayGroup
|  |  |   |--(1) hmRS2SigRelayMode
|  |  |   |--(2) hmRS2SigRelayManualState
|  |  |--(13) hmRS2PSGroup
|  |  |   |--(1) hmRS2PSAlarm
|--(13) hmRS2PSGroup
|   |--(1) hmRS2PSAlarm
|--(14) hmRS2RedundancyGroup
|   |--(1) hmRS2RedNotGuaranteedAlarm
|--(15) hmRS4RGroup
|   |--(1) hmRS4RVlanGroup
|   |   |--(1) hmRS4RVlanPortTable
|   |   |   |--(1) hmRS4RVlanPortEntry
|   |   |   |   |--(1) hmRS4RVlanPortID
|   |   |   |   |--(2) hmRS4RVlanPortTagFormatRstp
```

6.2.2 Management Group

The Management group contains parameters for configuring the management agent.

```
(14) hmConfiguration

    |--(2) hmAgent
    |    |--(1) hmAction
    |    |--(2) hmActionResult
    |    |--(3) hmNetwork
    |    |    |--(1) hmNetLocalIPAddr
    |    |    |--(2) hmNetLocalPhysAddr
    |    |    |--(3) hmNetGatewayIPAddr
    |    |    |--(4) hmNetMask
    |    |    |--(7) hmNetAction
    |    |    |--(8) hmNetVlanID
    |    |    |--(20) hmNetProfinetGroup
    |    |    |    |--(1) hmNetProfinetDiscoveryStatus
    |    |    |--(30) hmNetSNTPGroup
    |    |    |    |--(1) hmNetSNTPStatus
    |    |    |    |--(2) hmNetSNTPServer
    |    |    |    |--(3) hmNetSNTPTime
    |    |    |    |--(4) hmNetSNTPLocalOffset
    |    |    |    |--(5) hmNetSNTPServer2
    |    |    |    |--(6) hmNetSNTPSyncInterval
    |    |    |    |--(7) hmNetSNTPAcceptBroadcasts
    |    |    |    |--(8) hmNetSNTPAnycastAddr
    |    |    |    |--(9) hmNetSNTPAnycastVlan
    |    |    |    |--(10) hmNetSNTPAnycastInterval
    |    |    |    |--(11) hmNetSNTPOperStatus
    |    |    |--(50) hmNetSNMPGroup
    |    |    |    |--(1) hmNetSNMPv1Status
    |    |    |    |--(2) hmNetSNMPv2Status
    |    |    |    |--(3) hmNetSNMPv3Status
    |    |    |    |--(4) hmNetSNMPAccessStatus
    |    |--(4) hmFSTable
    |    |    |--(1) hmFSUpdFileName
    |    |    |--(2) hmFSConfFileName
    |    |    |--(3) hmFSLogFileName
    |    |    |--(4) hmFSUserName
    |    |    |--(5) hmFSTPPassword
    |    |    |--(6) hmFSAction
```

```
|   |   |--(8) hmFSActionResult
|   |   |--(9) hmFSBootConfiguration
|   |   |--(10) hmFSRunningConfiguration
|   |   |--(11) hmFSLastMessage
|   |   |--(200) hmAutoconfigGroup
|   |   |   |--(1) hmAutoconfigAdapterStatus
|   |--(5) hmTempTable
|   |   |--(1) hmTemperature
|   |   |--(2) hmTempUprLimit
|   |   |--(3) hmTempLwrLimit
|   |--(7) hmAuthGroup
|   |   |--(1) hmAuthHostTableEntriesMax
|   |   |--(2) hmAuthCommTableEntriesMax
|   |   |--(3) hmAuthCommTable
|   |   |   |--(1) hmAuthCommEntry
|   |   |   |   |--(1) hmAuthCommIndex
|   |   |   |   |--(2) hmAuthCommName
|   |   |   |   |--(3) hmAuthCommPerm
|   |   |   |   |--(4) hmAuthCommState
|   |   |--(4) hmAuthHostTable
|   |   |   |--(1) hmAuthHostEntry
|   |   |   |   |--(1) hmAuthHostIndex
|   |   |   |   |--(2) hmAuthHostName
|   |   |   |   |--(3) hmAuthHostCommIndex
|   |   |   |   |--(4) hmAuthHostIpAddress
|   |   |   |   |--(5) hmAuthHostIpMask
|   |   |   |   |--(6) hmAuthHostState
|   |--(8) hmTrapGroup
|   |   |--(1) hmTrapCommTableEntriesMax
|   |   |--(2) hmTrapDestTableEntriesMax
|   |   |--(3) hmTrapCommTable
|   |   |   |--(1) hmTrapCommEntry
|   |   |   |   |--(1) hmTrapCommIndex
|   |   |   |   |--(2) hmTrapCommCommIndex
|   |   |   |   |--(3) hmTrapCommColdStart
|   |   |   |   |--(4) hmTrapCommLinkDown
|   |   |   |   |--(5) hmTrapCommLinkUp
|   |   |   |   |--(6) hmTrapCommAuthentication
|   |   |   |   |--(7) hmTrapCommBridge
|   |   |   |   |--(8) hmTrapCommRMON
|   |   |   |   |--(9) hmTrapCommUsergroup
|   |   |   |   |--(10)hmTrapCommDualHoming
|   |   |   |   |--(11)hmTrapCommChassis
```

```
|   |   |   |   |--(12)hmTrapCommState
|   |   |   --(4) hmTrapDestTable
|   |   |       |--(1) hmTrapDestEntry
|   |   |       |   |--(1) hmTrapDestIndex
|   |   |       |   |--(2) hmTrapDestName
|   |   |       |   |--(3) hmTrapDestCommIndex
|   |   |       |   |--(4) hmTrapDestIpAddress
|   |   |       |   |--(5) hmTrapDestIpMask
|   |   |       |   |--(6) hmTrapDestState
|   |--(9) hmLastAccessGroup
|   |   |--(1) hmLastIpAddr
|   |   |--(2) hmLastPort
|   |   |--(3) hmLastCommunity
|   |--(11) hmRelayGroup
|   |   |--(1) hmRelayOption82Status
|   |   |--(2) hmRelayOptionRemoteIDType
|   |   |--(3) hmRelayOptionRemoteID
|   |   |--(10) hmRelayServerGroup
|   |   |   |--(1) hmRelayDHCPServerIpAddr
|   |   |   |--(2) hmRelayDHCPServer2IpAddr
|   |   |   |--(3) hmRelayDHCPServer3IpAddr
|   |   |   |--(4) hmRelayDHCPServer4IpAddr
|   |   |--(11) hmRelayInterfaceTable
|   |   |   |--(1) hmRelayIfEntry
|   |   |   |   |--(1) hmRelayIfaceGroupID
|   |   |   |   |--(2) hmRelayIfaceID
|   |   |   |   |--(3) hmRelayIfaceOption82Enable
|   |   |   |   |--(4) hmRelayIfaceBCRequestFwd
|   |   |--(20) hmRelayBCPktInCnt
|   |   |--(21) hmRelayMCPktInCnt
|   |   |--(22) hmRelayPktServerRelayCnt
|   |   |--(23) hmRelayPktClientRelayCnt
|   |   |--(24) hmRelayErrCnt
|   |   |--(25) hmRelayLastDuplicateIP
```

6.2.3 HIPER-Ring Redundancy Group

The HIPER-Ring Redundancy Group contains parameters for configuring the HIPER-Ring redundancy.

```
(14) hmConfiguration

   |--(5) hmRingRedundancy
   |   |--(1) hmRingRedTable
   |   |   |--(1) hmRingRedEntry
   |   |   |   |--(1) hmRingRedPrimGroupID
   |   |   |   |--(2) hmRingRedPrimIfIndex
   |   |   |   |--(3) hmRingRedPrimIfOpState
   |   |   |   |--(4) hmRingRedRedGroupID
   |   |   |   |--(5) hmRingRedRedIfIndex
   |   |   |   |--(6) hmRingRedRedIfOpState
   |   |   |   |--(7) hmRingRedOperState
   |   |   |   |--(8) hmRingRedMode
   |   |   |   |--(9) hmRingRedConfigOperState
```

6.3 SNMP V2 Module MIB

The SNMP V2 Module MIB is based on the SNMP-Mib "Simple Network Management Protocol Group (1.3.6.1.2.1.11)" on page 187.

6.3.1 Framework Group (1.3.6.1.6.3.10)

The framework group contains parameters for describing SNMP Management Frameworks

```
(3) snmpModules

   |-- (10) snmpFrameworkMIB
   |   |-- (2) snmpFrameworkMIBObjects
   |   |   |-- (1) snmpEngine
   |   |   |    |-- (1) snmpEngineID
   |   |   |    |-- (2) snmpEngineBoots
   |   |   |    |-- (3) snmpEngineTime
   |   |   |    |-- (4) snmpEngineMaxMessageSize
```

6.3.2 MPD Group (1.3.6.1.6.3.11)

The MPD group (Message Processing and Dispatching) contains
parameters for dispatching SNMP messages which are potentially in
different SNMP versions. It defines the procedures for dispatching potentially
multiple versions of SNMP messages

(3) `snmpModules`

```
|-- (11) snmpMPDMIB
|   |-- (2) snmpMPDMIBObjects
|   |   |-- (1) snmpUnknownSecurityModels
|   |   |-- (2) snmpInvalidMsgs
|   |   |-- (3) snmpUnknownPDUHandlers
```

6.3.3 Target Group (1.3.6.1.6.3.12)

The Target group contains parameters for specifying targets of SNMP management operations.

```
(3) snmpModules

   |-- (12) snmpTargetMIB
   |    |-- (2) snmpTargetObjects
   |    |    |-- (1) snmpTargetSpinLock
   |    |    |    |-- (2) snmpTargetAddrTable
   |    |    |    |    |-- (1) snmpTargetAddrEntry
   |    |    |    |    |    |-- (1) snmpTargetAddrName
   |    |    |    |    |    |-- (2) snmpTargetAddrTDomain
   |    |    |    |    |    |-- (3) snmpTargetAddrTAddress
   |    |    |    |    |    |-- (4) snmpTargetAddrTimeout
   |    |    |    |    |    |-- (5) snmpTargetAddrRetryCount
   |    |    |    |    |    |-- (6) snmpTargetAddrTagList |
   |    |    |    |    |    |-- (7) snmpTargetAddrParams
   |    |    |    |    |    |-- (8) snmpTargetAddrStorageType
   |    |    |    |    |    |-- (9) snmpTargetAddrRowStatus
   |    |    |    |-- (3) snmpTargetParamsTable
   |    |    |    |    |-- (1) snmpTargetParamsEntry
   |    |    |    |    |    |-- (1) snmpTargetParamsName
   |    |    |    |    |    |-- (2) snmpTargetParamsMPModel
   |    |    |    |    |    |-- (3) snmpTargetParamsSecurityModel
   |    |    |    |    |    |-- (4) snmpTargetParamsSecurityName
   |    |    |    |    |    |-- (5) snmpTargetParamsSecurityLevel
   |    |    |    |    |    |-- (6) snmpTargetParamsStorageType
   |    |    |    |    |    |-- (7) snmpTargetParamsRowStatus
   |    |    |-- (4) snmpUnavailableContexts
   |    |    |-- (5) snmpUnknownContexts
```

6.3.4 Notification Group (1.3.6.1.6.3.13)

The Notification group contains parameters for specifying targets for notification filtering.

```
(3) snmpModules

   |-- (13) snmpNotificationMIB
   |    |-- (1) snmpNotifyObjects
   |    |    |-- (1) snmpNotifyTable
   |    |    |    |-- (1) snmpNotifyEntry
   |    |    |    |    |-- (1) snmpNotifyName
   |    |    |    |    |-- (2) snmpNotifyTag
   |    |    |    |    |-- (3) snmpNotifyType
   |    |    |    |    |-- (4) snmpNotifyStorageType
   |    |    |    |    |-- (5) snmpNotifyRowStatus
   |    |    |-- (2) snmpNotifyFilterProfileTable
   |    |    |    |-- (1) snmpNotifyFilterProfileEntry
   |    |    |    |    |-- (1) snmpNotifyFilterProfileName
   |    |    |    |    |-- (2) snmpNotifyFilterProfileStorType
   |    |    |    |    |-- (3) snmpNotifyFilterProfileRowStatus
   |    |    |-- (3) snmpNotifyFilterTable
   |    |    |    |-- (1) snmpNotifyFilterEntry
   |    |    |    |    |-- (1) snmpNotifyFilterSubtree
   |    |    |    |    |-- (2) snmpNotifyFilterMask
   |    |    |    |    |-- (3) snmpNotifyFilterType
   |    |    |    |    |-- (4) snmpNotifyFilterStorageType
   |    |    |    |    |-- (5) snmpNotifyFilterRowStatus
```

6.3.5 USM Group (1.3.6.1.6.3.15)

The USM group (User-based Security Model) defines the elements of procedure for providing SNMP message level security

```
(3) snmpModules

   |-- (15) snmpUsmMIB
   |   |-- (1) usmMIBObjects
   |   |   |-- (1) usmStats
   |   |   |   |-- (1) usmStatsUnsupportedSecLevels
   |   |   |   |-- (2) usmStatsNotInTimeWindows
   |   |   |   |-- (3) usmStatsUnknownUserNames
   |   |   |   |-- (4) usmStatsUnknownEngineIDs
   |   |   |   |-- (5) usmStatsWrongDigests
   |   |   |   |-- (6) usmStatsDecryptionErrors
   |   |   |-- (2) usmUser
   |   |   |   |-- (1) usmUserSpinLock
   |   |   |   |   |-- (2) usmUserTable
   |   |   |   |   |   |-- (1) usmUserEntry
   |   |   |   |   |   |   |-- (1) usmUserEngineID
   |   |   |   |   |   |   |-- (2) usmUserName
   |   |   |   |   |   |   |-- (3) usmUserSecurityName
   |   |   |   |   |   |   |-- (4) usmUserCloneFrom
   |   |   |   |   |   |   |-- (5) usmUserAuthProtocol
   |   |   |   |   |   |   |-- (6) usmUserAuthKeyChange
   |   |   |   |   |   |   |-- (7) usmUserOwnAuthKeyChange
   |   |   |   |   |   |   |-- (8) usmUserPrivProtocol
   |   |   |   |   |   |   |-- (9) usmUserPrivKeyChange
   |   |   |   |   |   |   |-- (10) usmUserOwnPrivKeyChange
   |   |   |   |   |   |   |-- (11) usmUserPublic
   |   |   |   |   |   |   |-- (12) usmUserStorageType
   |   |   |   |   |   |   |-- (13) usmUserStatus
```

6.3.6 VACM Group (1.3.6.1.6.3.15)

The VACM group (View-based Access Control Model) defines the elements of procedure for controlling access to management information.

(3) `snmpModules`

```
|-- (16) snmpVacmMIB
|    |-- (1) vacmMIBObjects
|    |    |-- (1) vacmContextTable
|    |    |    |-- (1) vacmContextEntry
|    |    |    |    |-- (1) vacmContextName
|    |    |-- (2) vacmSecurityToGroupTable
|    |    |    |-- (1) vacmSecurityToGroupEntry
|    |    |    |    |-- (1) vacmSecurityModel
|    |    |    |    |-- (2) vacmSecurityName
|    |    |    |    |-- (3) vacmGroupName
|    |    |    |    |-- (4) vacmSecurityToGroupStorageType
|    |    |    |    |-- (5) vacmSecurityToGroupStatus
|    |    |-- (4) vacmAccessTable
|    |    |    |-- (1) vacmAccessEntry
|    |    |    |    |-- (1) vacmAccessContextPrefix
|    |    |    |    |-- (2) vacmAccessSecurityModel
|    |    |    |    |-- (3) vacmAccessSecurityLevel
|    |    |    |    |-- (4) vacmAccessContextMatch
|    |    |    |    |-- (5) vacmAccessReadViewName
|    |    |    |    |-- (6) vacmAccessWriteViewName
|    |    |    |    |-- (7) vacmAccessNotifyViewName
|    |    |    |    |-- (8) vacmAccessStorageType
|    |    |    |    |-- (9) vacmAccessStatus
|    |    |-- (5) vacmMIBViews
|    |    |    |-- (1) vacmViewSpinLock
|    |    |    |-- (2) vacmViewTreeFamilyTable
|    |    |    |    |-- (1) vacmViewTreeFamilyEntry
|    |    |    |    |    |-- (1) vacmViewTreeFamilyViewName
|    |    |    |    |    |-- (2) vacmViewTreeFamilySubtree
|    |    |    |    |    |-- (3) vacmViewTreeFamilyMask
|    |    |    |    |    |-- (4) vacmViewTreeFamilyType
|    |    |    |    |    |-- (5) vacmViewTreeFamilyStorageType
|    |    |    |    |    |-- (6) vacmViewTreeFamilyStatus
```

7 User Interface

The user interface offers users the option of choosing certain functions of the management RS2-4R in a menu-driven way.

The following menu items can be selected:
- ► System Parameter
- ► Switching General
- ► Switch Security
- ► Port Configuration / Statistics
- ► Port Mirroring / Disable Learning
- ► Configuration
- ► Update
- ► Password
- ► Ping
- ► System Reset

RS2-4R
Release 1.0 03/04

7.1 Opening the user interface

☐ After connecting the with a VT100 terminal via V.24, press a key. A window will appear on the screen for entering the password.
Only one user can access the user interface.

```
Login Screen                                                149.218.112.101
                                              Hirschmann ETHERNET Rail Switch 2



              Copyright (c) 2004 Hirschmann Electronics GmbH & Co. KG

                              All rights reserved.

                                RS2 Release 1.00

                        (Build date Mar 21 2004 08:51:29)




                        User:      [ admin            ]
                        Password:  [                  ]


```

Fig. 68:   Logging into the user interface program

☐ Enter the password. The default value for the password is **private**. You can change the password later in the user interface (see) or via the Web interface. Please note that passwords are case-sensitive.

The main menu screen appears.

```
┌──────────────────────────────────────────────────────────────────────┐
│ Main Menu                                               149.218.112.101│
│                                      Hirschmann ETHERNET Rail Switch 2  │
│                                                                        │
│                                                                        │
│                            System Parameter                            │
│                            Switching General                           │
│                            Switch Security                             │
│                            Port Configuration / Statistics             │
│                            Port Mirroring / Disable Learning           │
│                            Configuration                               │
│                            Update                                      │
│                            Password                                    │
│                                                                        │
│                            Ping                                        │
│                                                                        │
│                            System Reset                                │
│                                                                        │
│                                                                        │
│                                                                        │
│        LOGOUT                                                          │
│                                                                        │
│   Setup IP parameters                                                  │
│                                                                        │
└──────────────────────────────────────────────────────────────────────┘
```

Fig. 69:   Main menu

7.2 Operating the user interface

▶ Use the arrow keys or the tab key to move the cursor.

▶ To change the specified values in a selection field, press the space bar.

▶ The new settings are accepted if the cursor is in the APPLY field, and the enter key is pressed.

▶ The bottom line contains a help text for the selected item.

▶ To exit the user interface, select LOGOUT in the main menu and press the enter key.

The main menu consists of 7 submenus.

7.2.1 System parameters

This menu is for

▶ entering
  – IP addresses,
  – the subnet mask,
  – the gateway IP address.
▶ enabling/disabling the BOOTP/DHCP.
▶ displaying the MAC address of the RS2-4R.

```
System Parameter                                        149.218.112.101
                                    Hirschmann ETHERNET Rail Switch 2


                        IP Address       : [149.218.112.101]
                        Subnet Mask      : [255.255.255.0  ]
                        Default Gateway  : [0.0.0.0        ]

                        IP Configuration : < LOCAL >
                        HiDiscovery :      < Enable   >

                        MAC Address      : 00:80:63:00:02:77
                        System Name      : [Hirschmann RS2  ]

                        Note:

                     Set IP-Configuration <LOCAL> to use manual settings.
                    APPLY changes the state of the objects immediately and
                          saves the state to Non Volatile Memory.


    MAIN MENU  APPLY

Enter agent IP address in decimal dot format (e.g., 149.218.112.69)
```

Fig. 70:   Menu system parameters

■ **IP address**
Enter the IP address of this RS2-4R here. The default setting of the
address is 0.0.0.0.

■ **Subnet mask**
If you are working in a large network and are using network masks, you
can specify the mask of the subnet here. The default setting of the IP
address is 0.0.0.0.

■ **Gateway IP address**
Here you enter the IP address of the gateway through which the will
address other subnets. If there is no such gateway, you can omit this
entry. The default setting of the IP address is 0.0.0.0.

■ **IP configuration**
  □ Select the desired IP configuration mode. When you press the space bar, the following options become available:
    – Local
    – BOOTP
    – DHCP
    After selecting APPLY, the mode is activated (see "Basic settings" on page 47).

■ **HiDiscovery**
  The HiDiscovery protocol (see "System configuration via HiDiscovery" on page 55) allows you to assign an IP address to the switch on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the switch from your PC with the HiDiscovery software delivered (setting on delivery: Enable).

■ **MAC address**
  This field displays the MAC address of the device.

■ **System name**
  □ Assign your RS2-4R the name of your choice (see "System configuration via DHCP (dynamic host configuration protocol)" on page 61).

7.2.2 Switching General

The switch supports Rapid Spanning Tree.

☐ To activate it, select the line. Press the space bar to change the setting
    from `Disable` to `Enable`.
    Enter APPLY to activate the function immediately.

```
Switching General                                        149.218.112.101
                                      Hirschmann ETHERNET Rail Switch 2


   Rapid Spanning Tree : < Disable     >






   Note:

   APPLY changes the state of the object immediately.


   MAIN MENU   APPLY

Push space bar to Enable/Disable the {STP or RSTP} Protocol
```

Fig. 71:   Switching General

7.2.3 Switch security

The agent is accessible via:

► V.24
► Telnet
► the Web.

☐ To enable access via Telnet or the Web, select the Telnet or Web line.
   Press the space bar to change the setting from `Disable` to `Enable`.
   After APPLY is selected the new setting is immediately activated.

```
Switch Security                                         149.218.112.242
                                        Hirschmann ETHERNET Rail Switch 2


                        Web             : < Enable  >
                        SNMP            : < Enable  >


                        Note:

                      This settings are used to globally Enable or Disable
                       the loading of the Web Interface.
                      Set SNMP to ReadOnly if no writeaccess is required.


                       APPLY changes the state of the object immediately.


    MAIN MENU   APPLY

 Push space bar to Enable/Disable HTTP for entire switch
```

Fig. 72:   Access control

7.2.4 Port configuration / statistics

This menu is for port configuration and for displaying the port statistics.

☐ First enter the port number and press the return key.

☐ You can enter the name of your choice for this port after `Port Name`.

▶ State
  – `Disable` switches the port off
  – `Enable` switches the port on

▶ Transmission speed
  – `autonegotiate` activates the autonegotiation function
  – `10MHDX` 10 Mbit/s, half duplex
  – `10MFDX` 10 Mbit/s, full duplex
  – `100MHDX` 100 Mbit/s, half duplex
  – `100MFDX` 100 Mbit/s, full duplex

```
Port Configuration / Statistics                           149.218.112.101
                                      Hirschmann ETHERNET Rail Switch 2

  Port: 01             Port Name:  [                        ]

  State: <Enable  >  Set Speed:   <autonegotiate >
  Link:   Up         Actual Speed:  100MFDX          Type: 10/100 TP

  Port Statistics:

  Transmitted Packets:     27234
  Received    Packets:     1231027
  Received    Bytes:       154371683
  Received    Broadcasts:  917923
  Received    Multicasts:  183637
  Received    Fragments:   0
  Detected    CRCErrors:   0
  Detected    Collisions:  0



   MAIN MENU    APPLY    REFRESH

 Type in port number and press enter
```

Fig. 73:   Menu Port Configuration

7.2.5 Port Mirroring / Disable learning

This dialog gives you the option of viewing the data of all ports or of individual ports (monitoring).

▶ By selecting `Disable Learning`, you can disable the learning function. Consequently, the transmits all data from all ports to all ports.

▶ By selecting `Port Mirroring`, the mirrors all send/receive data of the "Source " to the "Destination Module.Port". The functions as a normal switch for the other ports.

▶ By selecting `Normal Switching`, you activate the learning function, and it functions as a normal switch.

Note: The setting `Normal Switching` is activated after a restart.

```
Port Mirroring / Disable Learning                           149.218.112.101
                                        Hirschmann ETHERNET Rail Switch 2


   Port Mirroring:    Source port: 0     Destination port: 0

   Mode  < Normal Switching >

   Note:
   Port Mirroring enables data packets from a source port to be copied to a
   specified destination port. This has no other effect on the data packets
   from the source port. When Port Mirroring is active, the specified
   destination port can only be used for observing data.
   Disable Learning allows you to capture all data packets received on every
   port. (Data packets with destination addresses for which filters are set
   manually or via the GMRP protocol will not be flooded)
   Switching will be interrupted for a few seconds while enabling
   mode Disable Learning.



   MAIN MENU  APPLY

 Type in port number and press enter
```

Fig. 74:   Menu Disable Learning

7.2.6 Configuration

The RS2-4R has two configuration settings:
- ▶ the default setting and
- ▶ the user-defined setting.

This submenu offers the option of storing a user-defined configuration.
This configuration can
- be loaded automatically when restarting or
- be loaded with the default configuration again after restarting.

With `Load after reset` you can determine which configuration setting
will be active after a restart:
- `default` loads the default configuration.
- `local` loads the user-defined configuration from the flash memory.
- `remote` loads the user-defined configuration from the configuration file on the tftp server.

With `Load` you determine which configuration is to be loaded:
- `local` loads the user-defined configuration from the flash memory.
- `remote` loads the user-defined configuration from the configuration file on the tftp server.

With `Save` you determine where the configuration setting is saved:
- `local` saves the user-defined configuration in the flash memory.
- `remote` saves the user-defined configuration as a configuration file on the tftp server.
- `configadapter` saves the user-defined configuration in the AutoConfig-uration Adapter and in the flash memory.

Any changes in this window are accepted by choosing `APPLY`.

The path for storing the configuration data on the tftp server is displayed in the line "URL".
tftp is not able to create a new file. Therefore create an empty file on the tftp server before you "Save to URL".

Example to save to a tftp server
☐ Open a new file with any editor.
☐ Save the empty file to the appropriate path of the tftp server, including the file name, e.g. /_01.cfg
☐ In the "URL" line, enter the path of the tftp server, e.g. tftp://149.218.112.214//_01.cfg.

Note: The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.

```
Save/Load Configuration                                      149.218.112.101
                                              Hirschmann ETHERNET Rail Switch 2


   Load after reset:  <  local configfile>

   Load:             <  local configfile>

   Save:             <  local configfile>


  URL of remote configuration file:  (e.g.: tftp://149.218.112.2/config.dat)
   [tftp://0.0.0.0/file.bin                                                  ]


   To load MIB-configuration after reset    APPLY Load after reset
   To load MIB-configuration                APPLY Load
   To save your current MIB-configuration   APPLY Save



    MAIN MENU   APPLY Load after reset   APPLY Load   APPLY Save

 Push space bar to select default, local or remote configuration file
```

Fig. 75:   Menu Save/Load Configuration

The selection of the AutoConfiguration Adapter (ACA) for a memory operation opens a new window - after you choose Apply - with the request:

☐ Pull the terminal block off the RS2-4R and connect the ACA to the V.24 connection of the .

Then the RS2-4R performs the memory operation. The RM LED shows the status of the memory operation (see "RM - Redundancy Manager / ACA - AutoConfiguration Adapter (Green/yellow LED)" on page 87).

The transition of the LED's from a flashing to a static state indicates the end of the memory operation.

☐ To go back to using the user interface, pull the ACA from the RS2-4R and connect the terminal block to the V.24 connection of the RS2-4R.

```
Save configuration                                     149.218.112.101
                                         Hirschmann ETHERNET Rail Switch 2



                    Please change terminalcable with adapter



        LED-Codes on LED RM and Standby:

        Alternate flash:         Adapterstatus not ok.
        Fast synchronous flash: Reading configuration from adapter
        Slow synchronous flash: Writing configuration to adapter


        Note:
        Adapter configuration is also saved to local configuration


```

Fig. 76:   Menu Memory Operation of AutoConfiguration Adapter

7.2.7 Update

Before you can update the software, you need to know the correct location (pathname) of the update file.

☐ Enter the correct pathname in the field `URL of update file` and then press the enter key.

In the line `Reset` you can decide whether the RS2-4R should be restarted immediately after loading an update or at a later time.

Choose `Apply` to load the update. It is active after a restart.

```
Update software                                        149.218.112.101
                                        Hirschmann ETHERNET Rail Switch 2


   URL of update file:
   [tftp://149.218.27.82/rs2wa/k2_pre2.bin                            ]

   A correct URL is for example:  (tftp://149.218.16.2/rs2/rs2.bin)


   Automatic Reset :  < Disable  >



   Note:

   APPLY saves the URL to Non Volatile Memory and starts the Update.



   MAIN MENU    APPLY

Enter URL of remote update file
```

Fig. 77:   Menu Update RS2-4R

7.2.8 Password

To protect your from unauthorized access, change the SNMPv3 read/write password and the SNMPv1/2c password in this submenu.

☐ The Web-based Interface and the User Interface communicate via SNMP version 3. Select "SNMPv1/2c YES" to be able to communicate with earlier versions of SNMP.

☐ Enter your old password in the field `Old SNMPv3 Password` and press the enter key.

☐ Enter your new password in the field `New SNMPv3 Password` and press the enter key.

☐ Repeat the entry of your new password in the field `Retype SNMPv3 password` and press the enter key.

☐ Enter your new password in the field `New SNMPv1/2c Password` and press the enter key.

☐ Repeat the entry of your new password in the field `Retype SNMPv1/2c password` and press the enter key.

☐ To accept the new passwords, choose `APPLY` and then press the enter key.

☐ To ensure that the new passwords are available after a restart, save this configuration .

```
Change Password                                           149.218.112.101
                                          Hirschmann ETHERNET Rail Switch 2

    User/WEB-Interface/SNMPv3 Password same as for SNMPv1/v2c: < Yes >

    SNMPv3 User:              admin
    Old SNMPv3 Password:     [                         ]
    New SNMPv3 Password:     [                         ]
    Re-type SNMPv3 Password: [                         ]

    SNMPv1/v2c Password (Community):          [                         ]
    Re-type SNMPv1/v2c Password (Community): [                         ]

    Note:
    To change the password/community type in the old and the new
    password/community and use APPLY to change.
    To save the password to non volatile memory,
    APPLY an overall configuration save.



   MAIN MENU  APPLY

Use 'Yes' to synchronize SNMPv1/2c community with SNMPv3 password
```

Fig. 78:   Menu Change Password

7.2.9 Ping

In the Ping menu you can test the accessibility of another network station.

☐ In the `IP Address of host` field, enter the IP address of the desired
    station and press the enter key.

Choose `Apply` to ping the desired station.

Depending on the accessibility of the station, you will receive the response:

`Host alive` or
`Host not alive.`

```
 Ping                                                149.218.112.101
                                      Hirschmann ETHERNET Rail Switch 2




                  IP Address of host  : [0.0.0.0        ]




                  Note:

                  Set valid IP Address and APPLY to ping.



    MAIN MENU    APPLY
 Enter IP Address in decimal dot format (e.g., 149.218.112.69)
```

Fig. 79:   Menu Ping

7.2.10 System reset

☐ To reset select the `Confirm Reset` line.
By pressing the space bar the setting changes from `No` to `Yes`. Choose
`APPLY` to reset the switch.

```
 Ping                                            149.218.112.101
                                 Hirschmann ETHERNET Rail Switch 2



                 IP Address of host  : [0.0.0.0        ]




                 Note:

                 Set valid IP Address and APPLY to ping.



    MAIN MENU    APPLY
 Enter IP Address in decimal dot format (e.g., 149.218.19.69)
```

Fig. 80:   Menu System Reset

A Appendix

FAQ

Answers to frequently asked questions can be found at the Hirschmann Website:

`www.hirschmann.com`

Under `Products/Support` inside `Automation and Network Solutions` is located on the pages `Products` the area `FAQ`.

For detailed information on all services offered by the Hirschmann Competence Center, please visit the Web site http://www.hicomcenter.com/.

Setting up DHCP Server Option 82

On the CDROM supplied with the switch you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP server on your PC
   insert the CD-ROM into the CD drive of your PC and
   under Additional Software, select "haneWIN DHCP-Server".
   To carry out the installation, follow the installation assistant.

☐ Start the `DHCP Server` program.
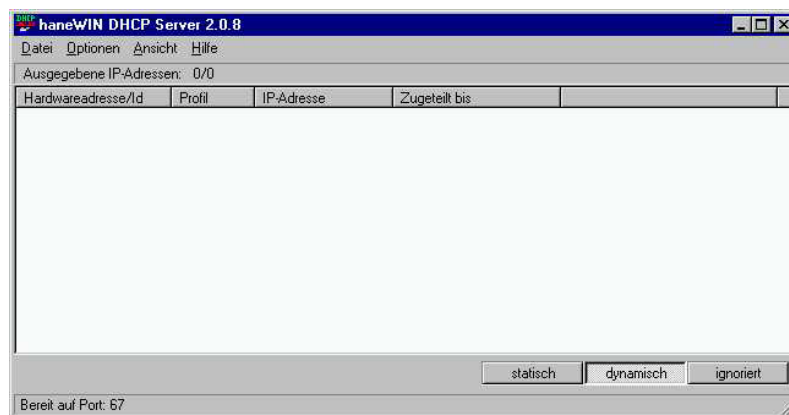
Fig. 81:   Start window of the DHCP server

☐ Select static.
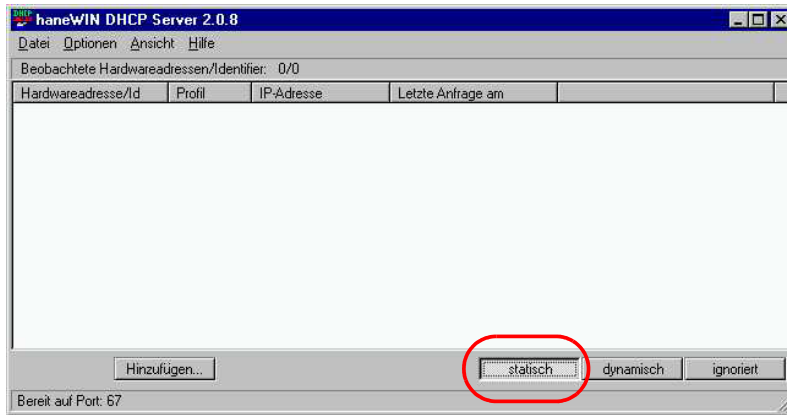
Fig. 82:   Static address input

☐ Open the window for the program settings in the menu bar:
    Options:Settings and select the DHCP tab page.
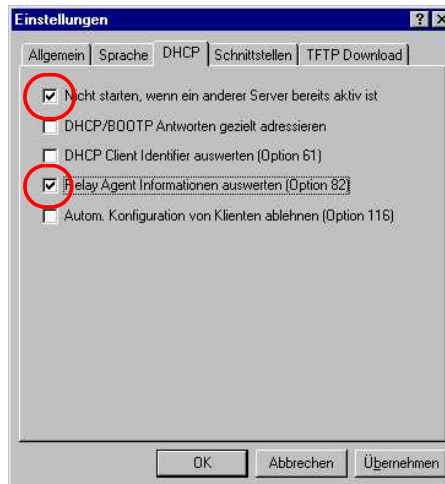
Fig. 83:   DHCP setting

☐ Select the DHCP tab page. Enter the settings shown in the illustration and click on OK.
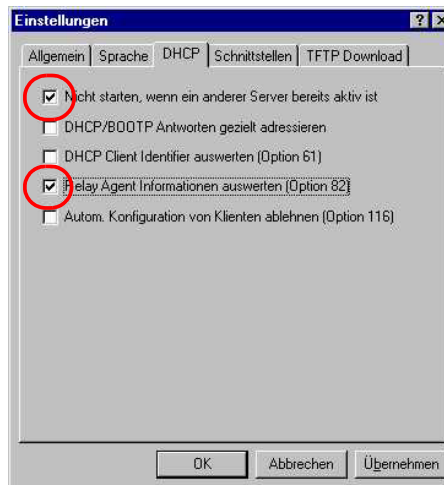
Fig. 84:   DHCP setting

☐ To enter the static addresses, click on Add.
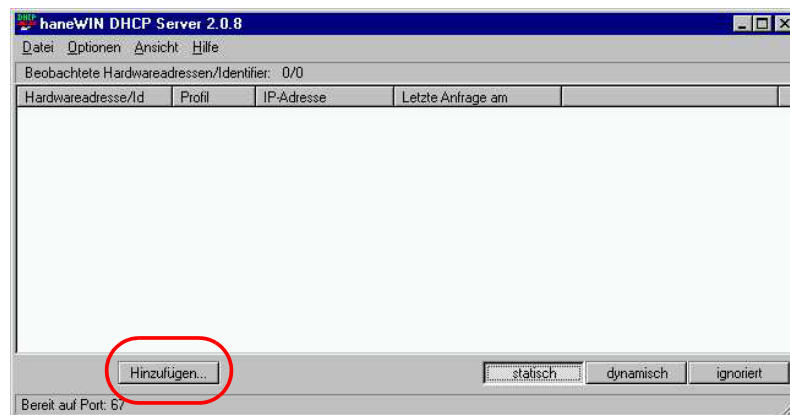
Fig. 85:   Adding static addresses

☐ Select `Circuit Identifier` and `Remote Identifier`.

Fig. 86:   Default setting for the fixed address assignment

☐ In the `Hardware address` field, you enter the `Circuit Identifier` and the `Remote Identifier`, see "DHCP Relay Agent" on page 166. With `Hardware address` you identify the switch and the port to which that device is connected, to which you want the assign the `IP address` in the line below it.

The hardware address is in the following form:

`ciclhhvvvvssmmpprirlxxxxxxxxxxxx`

  ▶ `ci`: sub-identifier for the type of the circuit ID
  ▶ `cl`: length of the circuit ID
  ▶ `hh`: Hirschmann identifier: `01` if a Hirschmann switch is connected to the port, otherwise `00`.
  ▶ `vvvv`: VLAN ID of the DHCP request (default: 0001 = VLAN 1)
  ▶ `ss`: socket of switch at which the module with that port is located to which the device is connected. Enter the value `00`.
  ▶ `mm`: module with the port to which the device is connected. Enter the value `00`.
  ▶ `pp`: port to which the device is connected.
  ▶ `ri`: sub-identifier for the type of the remote ID
  ▶ `rl`: length of the remote ID
  ▶ `xxxxxxxxxxxx`: remote ID of the switch (e.g. MAC address) to which a device is connected.
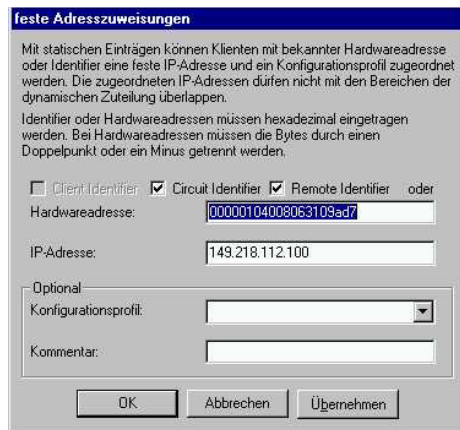
Fig. 87:   Entering the addresses
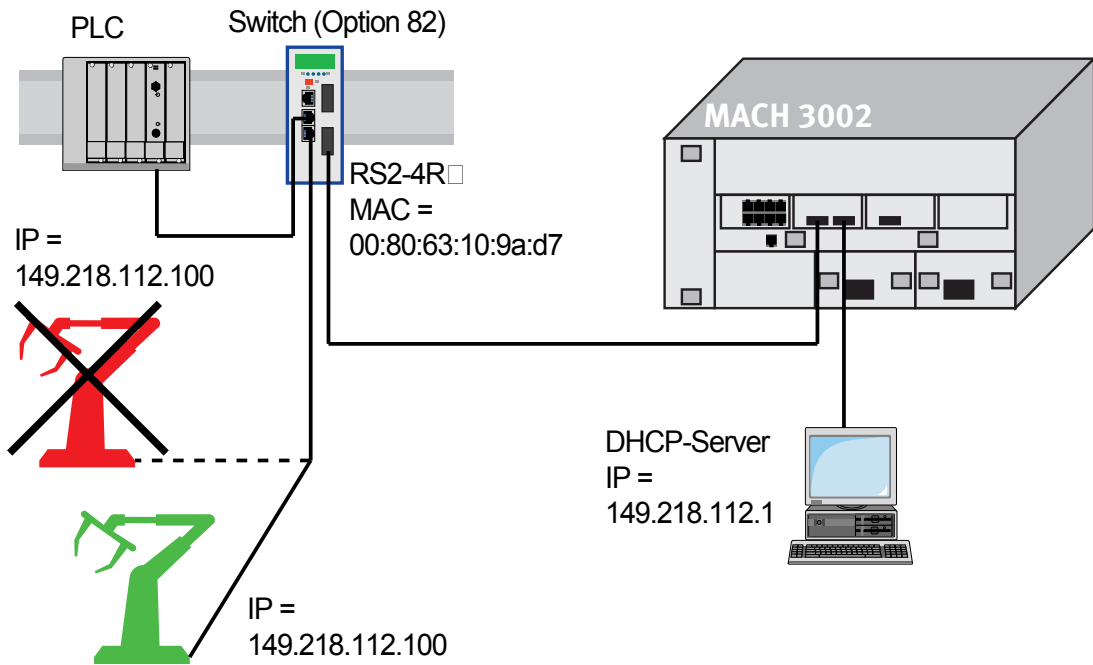
Fig. 88:   Application example of using Option 82

Based specifications and standards

■ List of norms and standards:

▶ EN 61000-6-2:2001 Basic standard - interference resistance in industry
▶ EN 55022:1998 + A1 2000 - Interference characteristics for IT systems
▶ EN 60950:1997 - Security in IT systems
▶ EN 61131-2:1994 + A12 2000 - Programmable Logic Controllers
▶ FCC 47 CFR Part 15:2000 – Code of Federal Regulations
▶ Germanischer Lloyd, Rules for Classification and Construction VI - 7 - 3 Part 1, Ed. 2001.
▶ cUL 508:1998 – Safety for Industrial Control Equipment
▶ cUL 1604 Electrical Equipment for Use in Class I and Class II, Div.2 and Class III Hazardous (Classified) Locations
▶ cUL 60950 Safety for Information Technoloy Equipment.

Certified devices are marked with a certification identifier.

■ List of RFC's

▶ RFC 768 (UDP)
▶ RFC 783 (TFTP)
▶ RFC 791 (IP)
▶ RFC 792 (ICMP)
▶ RFC 793 (TCP)
▶ RFC 826 (ARP)
▶ RFC 951 (BOOTP)
▶ RFC 1112 (IGMPv1)
▶ RFC 1157 (SNMPv1)
▶ RFC 1155 (SMIv1)
▶ RFC 1213 (MIB2)
▶ RFC 1493 (Dot1d)
▶ RFC 1542 (BOOTP-Extensions)
▶ RFC 1757 (RMON)
▶ RFC 1769 (SNTP)
▶ RFC 1907 (MIB2)

► RFC 1945 (HTTP/1.0)
► RFC 2131 (DHCP)
► RFC 2132 (DHCP-Options)
► RFC 2236 (IGMPv2)
► RFC 2239 (MAU-MIB)
► RFC 3411 (SNMP Framework)
► RFC3412 (SNMP MPD)
► RFC 3413 (SNMP Applications)
► RFC 3414 (SNMP USM)
► RFC 3415 (SNMP VACM)
► RFC 2613 (SMON)
► RFC 2674 (Dot1p/Q)

■ IEEE standards

IEEE 802.1 D	Switching, GARP, Spanning Tree
IEEE 802.1 D-1998	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP)
IEEE 802.1 Q	Tagging
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging)
IEEE 802.1 w.2001	Rapid Reconfiguration
IEEE 802.3-2002	Ethernet

Certifications

The following table indicates the certification status of the RS2-4R product family.

Standard	RS2-4R
EN 61131-2	complies with
CE	complies with
FCC 47 CFR Part 15	complies with
cUL 508 / CSA C22.2 No.142	pending
cUL 1604 / CSA C22.2 No.213	pending
Germanischer Lloyd	pending

Table 14: Certifications

Technical Data

RS2-4R

Dimensions W x H x D	47 x 131 x 111 mm
Weight	325 g, 0.7 lb
Top-hat rail fastener	in line with IEC 60715:1981 + A1:1995

Power supply

Operating voltage	24 V DC, -25% +33% Nec Class 2 power source, safety extra-low voltage (SELV/PELV) redundant inputs uncoupled
Power consumption / Power release	
with 4 TX ports	4.8 W maximum at 24 V DC 16.4 Btu (IT)/h
with 3 TX ports and 1 FX port	5.5 W maximum at 24 V DC 18.8 Btu (IT)/h
with 2 TX ports and 2 FX ports	6.8 W maximum at 24 V DC 23.2 Btu (IT)/h
Overload current protection at input	non-changeable thermal fuse

Environment

Ambient temperature	Surrouding air: -40 °C to +70 °C, -40 °F to +158 °F (RS2-4R 1LH SC and RS2-4R 2LH SC: 0 °C to 60 °C, 32 °F to 140 °F)
Storage temperature	Surrouding air: -40 °C to +85 °C (-4 °F to 176 °F)
Air humidity	10% to 95% (non-condensing)
Atmospheric pressure	Suitable for operation up to 2000 m (6561 ft), 795 hPa
Pollution Degree	2

Protection classes

Laser protection	Class 1 conforming to EN 60825-1 (2001)
Protection class	IP 20

EMC interference immunity

EN 61000-4-2	electrostatic discharge contact discharge: test level 3 (6 kV) air discharge: test level 3 (8 kV)
EN 61000-4-3	elektromagnetic field test level 3 (10 V/m; 80 - 2000 MHz)
EN 61000-4-4	fast transients (burst) test level 3 (2 kV power line, 1 kV data line)
EN 61000-4-5	surge voltage power line symmetrisch: test level 2 (1kV) unsymmetrisch: test level 3 (2kV); data Line: test level 2 (1kV)
EN 61000-4-6	cable-based RF faults: test level 3 10 V (150 kHz - 80 MHz)

EMC emitted immunity

EN 55022	Class A
FCC 47 CFR Part 15	Class A
Germanischer Lloyd	Rules for Classification and Construction VI - 7 - 3 Part 1, Ed. 2001

Stability

Vibration	IEC 60068-2-6 Test FC, testing level in line with IEC 61131-2 and Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1
Shock	IEC 60068-2-27 Test Ea, testing level in line with IEC 61131-2

Network size TX port 10BASE-T/100BASE-TX/1000BASE-TX

Length of a TP segment	100 m (328 ft) max.

Network size F/O ports 100BASE-FX
System attenuation

50/125 µm fiber, multimode	0-8 dB (MM)
62.5/125 µm fiber, multimode	0-11 dB (MM)
9/125 µm fiber, singlemode	0-16 dB (SM)
Wave length	1300 nm
9/125 µm fiber, singlemode	7-29 dB (LH)
Wave length	1550 nm

Example for F/O line length

50/125 µm fiber, multimode	5 km/16,400 ft max. (MM) data of fiber: 1 dB/km, 800 MHz*km
62,5/125 fiber, multimode	4 km/13,120 ft max. MM) 1 dB/km, 500 MHz*km
9/125 µm fiber, singlemode	30 km/98,420 ft max. (SM) data of fiber at 1300 nm, 0,4 dB/km 3,5 ps/(nm*km)
9/125 µm fiber, singlemode	24-86.6 km/78,740-284,121 ft (LH) data of fiber at 1550 nm, 0,3 dB/km 19 ps/(nm*km)

Software
Switch

Latency	6 µs
MAC address table	up to 1000 entries

Scope of delivery

Rail Switch RS2-4R incl.	terminal block for power supply
	RS2-4R manual on CDROM
	Description and operating instructions

Order number

RS2-4R	943 846-
RS2-4R 1MM SC	943 847-
RS2-4R 1SM SC	943 848-
RS2-4R 1LH SC	943 849-
RS2-4R 2MM SC	943 850-
RS2-4R 2SM SC	943 851-
RS2-4R 2LH SC	943 852-

Accessories

Manual: "Basics of Industrial ETHERNET and TCP/IP"	280720-834
AutoConfiguration Adapter ACA	943 751-001
Terminal cable	943 301-001
Rail Power Supply RPS 30	943 662-003
Rail Power Supply RPS 60	943 662-001
Rail Power Supply RPS 120	943 662-011
Network Management Software HiVision	943 471-100

Literature references

[1]   "Optische Übertragungstechnik
        in der Praxis"
        Christoph Wrobel
        Hüthig Buch Verlag Heidelberg
        ISBN 3-8266-5040-9

[2]   „TCP/IP Illustrated", Vol. 1
        W.R. Stevens
        Addison Wesley 1994
        ISBN 0-201-63346-9

[3]   Hirschmann Manual
        "Basics of Industrial ETHERNET and TCP/IP"
        280 720-834

[4]   Hirschmann Manual
        "MultiLAN Switch"
        943 309-001

[5]   Hirschmann Manual
        "ETHERNET"
        943 320-001

[6]   Hirschmann Manual
        „Network Managent HiVision"
        039 584-620

Copyright of integrated software

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the
successor of the GNU Library Public License, version 2, hence the version
number 2.1.]

■ Preamble

The licenses for most software are designed to take away your freedom
to share and change it. By contrast, the GNU General Public Licenses
are intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the Free
Software Foundation and other authors who decide to use it. You can
use it too, but we suggest you first think carefully about whether this
license or the ordinary General Public License is the better strategy to
use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish); that you receive source code or can get it if you
want it; that you can change the software and use pieces of it in new free
programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for you if you
distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages

are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

■ **Terms ans conditionas fpr copying, distribution and modification**
  ▶ 0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".
  A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

► 1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

► 2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a   table of
data to be supplied by an application program that uses   the facility,
other than as an argument passed when the facility   is invoked, then
you must make a good faith effort to ensure that,   in the event an
application does not supply such function or   table, the facility still
operates, and performs whatever part of   its purpose remains
meaningful.

(For example, a function in a library to compute square roots has a
purpose that is entirely well-defined independent of the application.
Therefore, Subsection 2d requires that any application-supplied
function or table used by this function must be optional: if the
application does not supply it, the square root function must still
compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library, and
can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote
it.

Thus, it is not the intent of this section to claim rights or contest your
rights to work written entirely by you; rather, the intent is to exercise
the right to control the distribution of derivative or collective works
based on the Library.

In addition, mere aggregation of another work not based on the
Library with the Library (or with a work based on the Library) on a
volume of a storage or distribution medium does not bring the other
work under the scope of this License.

► 3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

► 4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

► 5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked

without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

► 6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather

than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

► 7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

▶ 8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

▶ 9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

▶ 10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

▶ 11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

► 12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

► 13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

► 14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

► 15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

► 16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

■ How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the library's name and a brief idea of what it
does.> Copyright (C) <year>  <name of author>
```

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice
```

That's all there is to it!

The Legion Of The Bouncy Castle

Copyright (c) 2000 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Reader's comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your **assessment** of this manual:

	excellent	good	satisfactory	mediocre	poor
Accuracy	O	O	O	O	O
Readability	O	O	O	O	O
Comprehensibility	O	O	O	O	O
Examples	O	O	O	O	O
Structure/Layout	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover an error in the manual?
If so, on what page?

....

....

....

....

....

....

....

Suggestions for improvement and additional information:

....

....

....

....

General comments:

....

....

....

....

Company / Department   ....

Name / Telephone number   ....

Street   ....

Zip code / City   ....

Date / Signature   ....

Dear User,

Please fill out and return this page

– by fax to the number +49 (0)7127/14-1798 or
– by mail to
    Hirschmann Electronics GmbH & Co. KG
    Department AMM
    Stuttgarter Str. 45 - 51

    72654 Neckartenzlingen
    Germany

Index