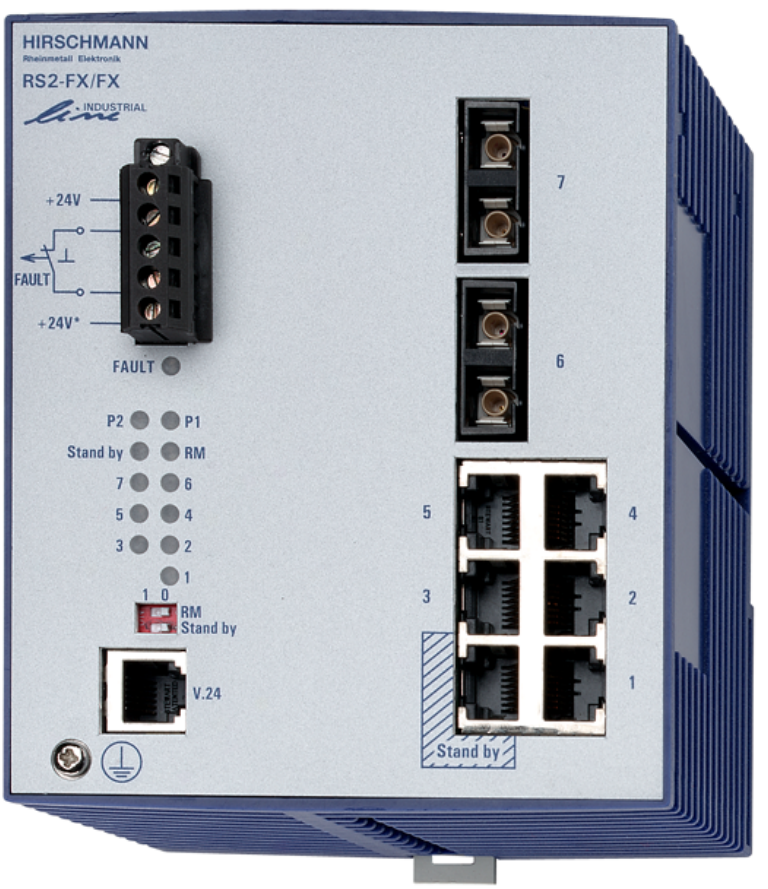
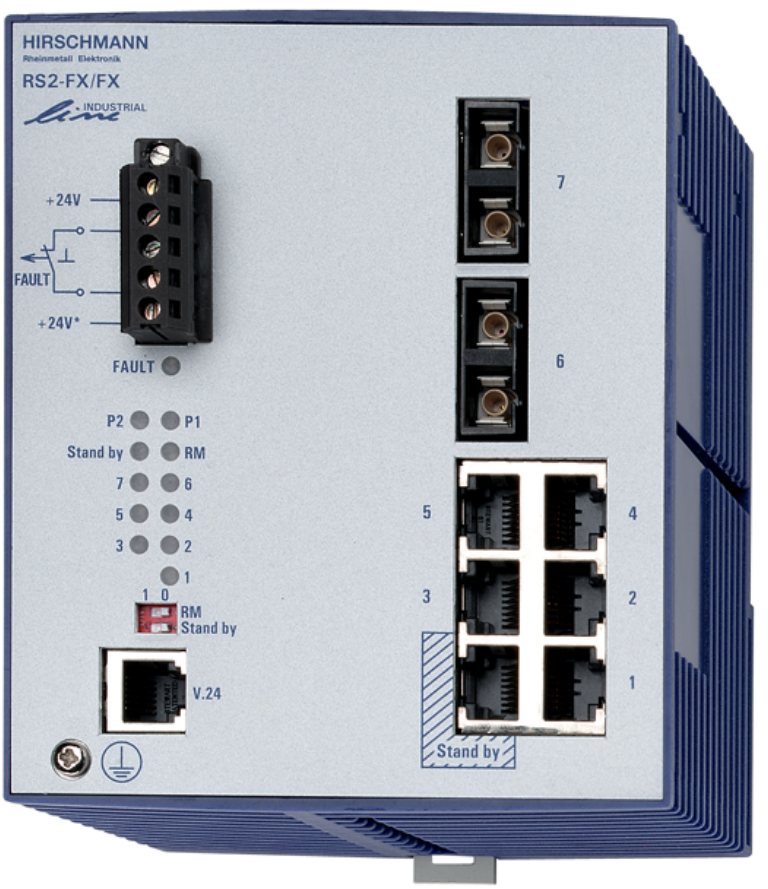
Handbuch RS2-../.. Management

Industrial ETHERNET Rail Switch 2



Handbuch RS2-../.. Management

Industrial ETHERNET Rail Switch 2



Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluß ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Electronics GmbH & Co. KG nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Printed in Germany

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Telefon +49 1805 141538

039 655-900-01-0904

Hirschmann weltweit:

Deutschland
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
E-Mail: ans-hi-line@hirschmann.de
Internet: www.hirschmann.de

Schweiz
Hirschmann Electronics GmbH & Co. KG, Neckartenzlingen
Niederlassung Uster
Seestr. 16
CH-8610 Uster
Tel. ++41-44905-8282
Fax ++41-44905-8289
E-Mail: ans_ch@hirschmann.ch

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

Großbritannien

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
E-Mail: enquiry@hirschmann.co.uk

Niederlande

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

Spanien

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
E-Mail: hes@hirschmann.es

Ungarn

Hirschmann Electronics Kft.
Rokolya u. 1-13
H-1131 Budapest
Tel. ++36-1-3494199
Fax ++36-1-3298453
E-Mail: info@hirschmann.hu

USA

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

Singapur

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
E-Mail: info@hirschmann.sh.cn

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

Für alle hier nicht aufgeführten Länder wählen Sie bitte
Tel. +49-7127-14-16 20
Kontaktadresse siehe Hirschmann Deutschland.

Hirschmann Competence

Langfristig garantieren hervorragende Produkte allein keine erfolgreiche Kundenbeziehung. Erst der umfassende Service macht weltweit den Unterschied. In dieser globalen Konkurrenz hat das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
- Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice bis zu den Wartungskonzepten.

Mit dem Competence Center entscheiden Sie sich in jedem Fall gegen jeden Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Servicekomponenten Sie in Anspruch nehmen.

Internet:
http://www.hicomcenter.com

Inhalt

3 Installation und Inbetriebnahme 27

4 Funktionen 83

1 Einführung

Hirschmann realisierte 1984 das weltweit erste ETHERNET auf Glasfaserbasis an der Universität in Stuttgart und erfand 1990 den „ETHERNET-Ring“.

Diesen Innovationen folgten 1993 die ersten Medienkonverter für Feldbusse und 1998 der HIPER-Ring für shared Ethernet-Netze.

Heute bietet der weltweit präsente Spezialist für unternehmensweite Netze von FiberINTERFACES für Feldbussysteme über ETHERNET-Transceiver, Hubs, Switches und Router sowie Fast-ETHERNET-Switches bis zu Gigabit-ETHERNET-Switches eine komplette Systemfamilie mit einheitlichem Management.

1.1 Industrielle Netzlösungen mit Zukunft

In der Automatisierungs- und Prozeßleittechnik geht der Trend eindeutig hin zu offenen und transparenten Systemlösungen, die immer häufiger auf PC-Steuerungen basieren und einen Intra- oder Internet-Zugang haben. Die wichtigsten Standards bilden dabei TCP/IP-Kommunikationsprotokolle und ETHERNET-Netzstrukturen. Sehr viele Controller, speicherprogrammierbare Steuerungen (SPS) und Distributed Controller Systems (DCS) verfügen heute bereits über eine ETHERNET-Schnittstelle. Derzeit arbeiten Organisationen und Unternehmen daran, bestehende Feldbusprotokolle auf TCP/IP abzubilden und Feldgeräte direkt mit einer ETHERNET-Schnittstelle auszurüsten.

Obwohl in der Automatisierungstechnik derselbe Ethernet-Standard wie im Office-Bereich eingesetzt wird, unterscheiden sich die Anforderungen an die Netzprodukte erheblich. Im industriellen Alltag müssen Netze unter extremen Bedingungen, wie elektromagnetischen Störfeldern, hohen Betriebstemperaturen und mechanischen Beanspruchungen, zuverlässig arbeiten.

Die Industrial ETHERNET Rail-Familie wurde unter Berücksichtigung dieser Anforderungen speziell für den Einsatz in der industriellen Automatisierung konzipiert. Ein Resultat der Anforderungen ist der von Hirschmann entwickelte redundante „HIPER-Ring“. Dieses Verfahren gewährleistet den kontinuierlichen Produktionsbetrieb auch dann, wenn eine Rekonfiguration des Netzes erforderlich ist. Außerdem bietet dieses Verfahren die Möglichkeit, Netze im laufenden Betrieb zu warten und zu erweitern. Da die Rekonfiguration innerhalb weniger Millisekunden erfolgt, ist der „HIPER-Ring“ wesentlich schneller als der Spanning Tree Algorithmus, der lediglich die Anforderungen aus dem Officebereich erfüllt.

Dieses Verfahren und weitere Hirschmann Konzepte sorgen für eine sehr hohe Verfügbarkeit des Netzes und der Produktionsanlagen. Durch dieaufeinander abgestimmten Industrial ETHERNET Rail-Produkte läßt sich das Netz jederzeit optimal an geographische und sicherheitsrelevante Belange der Anlagen anpassen und so skalieren, daß es auch zukünftigen Anforderungen gerecht wird.

Allgemeine Merkmale der Industrial ETHERNET Rail-Produkte sind:

- industriegerechter Aufbau (IP 20, besondere EMV- und Vibrationstests, 24 V-Versorgungsspannung, ohne Lüfter).
- die schnelle Montage, indem Sie die robusten Geräte einfach auf eine Hutschiene (Normprofilschiene) aufrasten.
- die zeitsparende Inbetriebnahme durch Plug & Play - Technik (Autonegotiation, Autopolarity, Autocrossing) und umfangreiche Diagnoseanzeigen.
- die Vollduplex-Switch-Technologie ermöglicht durch den Store and Foreward Modus.
- der hohe Temperaturbereich, der Ihnen neue Einsatzfelder ermöglicht.
- der Meldekontakt, der sich als binäres Signal erfassen lässt und eine einfache Ferndiagnose ermöglicht.

1.2 Die Industrial ETHERNET Rail Switches

Von Anfang an als mission-critical Switches konzipiert, zeichnen sich die Hirschmann Industrial ETHERNET Switches vor allem durch eine hohe Netzverfügbarkeit aus. Ein einzelner physischer oder logischer Fehler kann durch die Hirschmann Ringstruktur in keinem Fall zu einem Ausfall führen. Durch die in den Switches integrierten Redundanzkonzepte läßt sich ein ausfallsicheres, fehlertolerantes Kommunikationsnetz, auf Ethernet basierend, aufbauen.

Je nach Bedeutung der Prozeßanwendung, kann der Grad der Ausfallsicherheit für das gesamte Netz so skaliert werden, daß es auch zukünftigen Anforderungen gerecht wird. Verfügt beispielsweise ein Controller über zwei Netz-Interface-Karten, so kann jede dieser Karten an einen separaten Switch im gleichen redundanten Lichtwellenleiterring angeschlossen werden. Wird eine doppelte Absicherung gewünscht, besteht darüber hinaus die Möglichkeit, einen zweiten Ring zu integrieren.

Mit der Fast ETHERNET Rail Switch Familie RS2-../.. können Sie sich einfach und preiswert mittlere bis große deterministische ETHERNET/Fast ETHERNET-Netze aufbauen.

Ein Rail Switch RS2-../.. bietet Ihnen als kompaktes, industriegerechtes und auf einer Hutschiene aufrastbares Gerät fünf Twisted Pair Ports (10/100 Mbit/s autonegotiation) und zwei Ports (100 Mbit/s), die als Twisted Pair, Multimode oder Singlemode ausgeführt sind.

Ein weiteres wichtiges Merkmal der Rail Switches RS2-../.. ist die schnelle Medienredundanz. Dabei erkennt ein Rail Switch den Ausfall einer Übertragungsstrecke in weniger als 500 ms und leitet die Daten auf eine redundante Strecke um. Sie aktivieren diese Funktion indem Sie an einem beliebigen Rail Switch einfach einen Schalter betätigen. Dieses von Hirschmann entwickelte Verfahren gewährleistet eine hohe Verfügbarkeit des Netzes und der gesamten Anlage. Diese Funktion können Sie auch nutzen, um z.B. bestehende Netze im laufenden Betrieb zu erweitern.

Zusätzlich beinhalten die Rail Switches RS2-../.. einen SNMP-Management-Agenten und ein integriertes Web-based Management. Daraus resultieren einfach handhabbare Konfigurationsfunktionen für eine schnelle Inbetriebnahme und umfangreiche Netz- und Geräteinformationen, die zu einer hohen Anlagenverfügbarkeit beitragen.

Die 24 V-Spannungsversorgung können Sie über einen steckbaren Klemmblock redundant einspeisen. Ein zusätzlicher Kontakt im Klemmblock bietet Ihnen die Möglichkeit, Statusmeldungen der Geräte direkt einzulesen. LEDs unterstützen eine schnelle Inbetriebnahme vor Ort.

2 Hardware

Die Industrial ETHERNET Rail Switch RS2-../.. Familie besteht aus 6 Gerätevarianten. Diese Geräte sind managebar und verfügen über die gleichen Funktionen. Sie unterscheiden sich in den Schnittstellen zum Anschluß von Segmenten:

- RS2-TX/TX
- RS2-FX/FX
- RS2-FX/FX ST
- RS2-FX-SM/FX-SM
- RS2-FX-SM/FX-LH
- RS2-FX-LH/FX-LH

Der Einfachheit halber werden in diesem Buch diese 6 Geräte mit dem Namen RS2-../.. bezeichnet.

Der RS2-../.. arbeitet im store-and-forward-Modus. Während des Empfangs eines Datenpaketes analysiert der RS2-../.. die Quell-und Zieladresse. In seiner Adresstabelle speichert er bis zu 4000 Adressen mit Portzuweisungen.

Die LEDs zeigen unter anderem Datenempfang, Verbindungsstatus und Prozessorstatus an.

Gerätetyp	TP-Ports 10/100	LWL-Port multimode 100 MBit/s	LWL-Port singlemode 1300 nm, 100 MBit/s	LWL-Port singlemode 1550 nm, 100 MBit/s
RS2-TX/TX	1-7	–	–	–
RS2-FX/FX	1-5	6 + 7, SC-Buchse	–	–
RS2-FX/FX ST	1-5	6 + 7, ST-Buchse	–	–
RS2-FX-SM/FX-SM	1-5	–	6 + 7, SC-Buchse	–
RS2-FX-SM/FX-LH	1-5	–	6, SC-Buchse	7, SC-Buchse
RS2-FX-LH/FX-LH	1-5	–	–	6 + 7, SC-Buchse

Tab. 1: Gerätevarianten

Der RS2-../.. erfüllt die Prüfanforderungen für elektronische Betriebsmittel nach Germanischer Lloyd Richtlinien für die Durchführung von Baumusterprüfungen Teil 1.

Das Taschenbuch „Grundlagen Industrial ETHERNET und TCP/IP” von Hirschmann mit der Bestellnummer 280 710-834 beschreibt ausführlich unter anderem

- den Aufbau eines lokalen Netzes nach der Norm ISO/IEC 8802-3 und
- gibt Hinweise zur Netzplanung sowie Installation von Ethernet Netzen.

3 Installation und Inbetriebnahme

Die Industrial ETHERNET Rail Switch RS2-../.. Familie ist für die Praxis in der rauhen Industrie-Umgebung entwickelt. Dementsprechend einfach ist die Installation.
Die wenigen Konfigurationseinstellungen, die für den Betrieb notwendig sind, beschreibt dieses Kapitel.

Eine Liste vorweg gibt Ihnen einen raschen Überblick, welche Schritte Sie nacheinander durchführen, um den Switch in ein LAN zu integrieren:

☐ Installieren Sie den Switch, “Geräteinstallation” auf Seite 35.

☐ Weisen Sie dem Switch seine IP-Parameter zu, “Grundeinstellungen” auf Seite 45.
Falls notwendig, schalten Sie BOOTP/DHCP aus, “Netzparameter festlegen” auf Seite 170.

☐ Öffnen Sie das Web-based Interface, “Öffnen des Web-based Interfaces” auf Seite 145.

☐ Prüfen Sie, welche Software-Version auf Ihrem Switch instaliert ist, “Systemdaten” auf Seite 154.

☐ Falls erforderlich, laden Sie sich vom Hirschmann-Web-Server www.hirschmann.com die neueste Software-Version für den Switch herunter und installieren Sie die neue Software, “Software-Update durchführen” auf Seite 156.

☐ Legen Sie fest, mit welcher Konfiguration der Switch starten soll, “Start-Konfiguration festlegen” auf Seite 159.

☐ Schalten Sie die Ports aus, die sie nicht benutzen.
Falls erforderlich schalten Sie Autonegotiation an den betroffenen Ports aus.
Konfigurieren Sie den Link Alarm für die relevanten Ports und testen Sie die Einstellung,
“Port-Konfigurationstabelle” auf Seite 181.

☐ Geben Sie die Trap-Zieladresse Ihrer Netzmanagementstation ein, “Alarme (Traps) Konfiguration” auf Seite 177.

☐ Speichern Sie die getroffenen Einstellungen lokal und gegebenenfalls auf einen tftp-Server, “Start-Konfiguration festlegen” auf Seite 159.

☐ Ändern Sie das Paßwort, “Paßwort” auf Seite 172.

Die Netzmanagement Software HiVision bietet Ihnen diese und weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- Ereignislogbuch.
- Konfiguration von „System Location“ und „System Name“.
- Konfiguration des Netzadressbereichs und der SNMP-Parameter.
- Speichern der Konfiguration auf den Switch.
- Gleichzeitige Konfiguration mehrerer Switche.
- Konfiguration der Portanzeigefarbe Rot für einen Verbindungsfehler.

3.1 Sicherheitshinweise

Versorgungsspannung

Die Geräte sind für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsspannungsanschlüsse sowie an den Meldekontakt nur PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß IEC/EN 60950 angeschlossen werden.

Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

- ☐ Nehmen Sie nur unbeschädigte Teile in Betrieb!
- ☐ Relevant für Nordamerika:
  Das Gerät darf nur an eine Versorgungsspannung der Klasse 2 angeschlossen werden, die den Anforderungen des National Electrical Code, Table 11(b) entspricht. Wenn die Versorgung redundant erfolgt (zwei verschiedene Spannungsquellen), müssen die Versorgungsspannungen zusammen den Anforderungen des National Electrical Code, Table 11(b) entsprechen.
- ☐ Relevant für Nordamerika:
  Nur Kupferdraht/Leiter der Klasse 1 60/75°C oder 75°C verwenden.
- ☐ Relevant für Nordamerika:
  Die Verdrahtung der Spannungsversorgung und der Ein- und Ausgänge (E/A) muss den Verdrahtungsvorschriften Class 1, Division 2 [Artikel 501(b) des National Electrical Code (NEC-Vorschriften der USA), NFPA 70] und den geltenden gesetzlichen Vorschriften entsprechen.

Schirmungsmasse

Die Schirmungsmasse der anschließbaren Twisted-Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

- ☐ Achten Sie beim Anschließen eines Kabelsegmentes mit kontaktiertem Schirmungsgeflecht auf mögliche Erdschleifen.

Gehäuse

Das Öffnen des Gehäuses bleibt ausschließlich den von Hirschmann autorisierten Technikern vorbehalten.
Die Erdung erfolgt über die separate Erdungsschraube. Sie befindet sich links unten in der Frontblende.

- ☐ Achten Sie auf die Übereinstimmung der elektrischen Installation mit lokalen oder nationalen Sicherheitsvorschriften.
- ☐ Die Lüftungsschlitze dürfen nicht bedeckt werden, so daß die Luft frei zirkulieren kann.
- ☐ Der Abstand zu den Lüftungsschlitzen des Gehäuses muß mindestens 10 cm betragen.
- ☐ Stecken Sie niemals spitze Gegenstände (schmale Schraubendreher, Drähte oder Ähnliches) in das Innere des Produktes! Es besteht die Gefahr eines elektrischen Schlags.
- ☐ Das Gehäuse ist in aufrechter Lage zu montieren.
- ☐ Das Gerät darf bei Aufstellung in Wohn- oder Büroumgebung ausschließlich in Schaltschränken mit Brandschutzeigenschaften gemäß EN 60950 betrieben werden.

Umgebung

Das Gerät darf nur bei der angegebenen maximalen Umgebungslufttemperatur und bei der angegebenen relativen Luftfeuchtigkeit (nicht kondensierend) betrieben werden.

- ☐ Wählen Sie den Montageort so, daß die in den Technischen Daten angegebenen klimatischen Grenzwerte eingehalten werden.
- ☐ Verwendung nur in einer Umgebung mit Verschmutzungsgrad gemäß den Technischen Daten.

Anforderung an die Qualifikation des Personals

Qualifiziertes Personal im Sinne dieser Betriebsanleitung bzw. der Warnhinweise sind Personen, die mit Aufstellung, Montage, Inbetriebsetzung und Betrieb dieses Produktes vertraut sind und die über die ihrer Tätigkeit entsprechenden Qualifikationen verfügen, wie z.B.:

- Ausbildung oder Unterweisung bzw. Berechtigung, Stromkreise und Geräte bzw. Systeme gemäß den aktuellen Standards der Sicherheitstechnik ein- und auszuschalten, zu erden und zu kennzeichnen;
- Ausbildung oder Unterweisung gemäß den aktuellen Standards der Sicherheitstechnik in Pflege und Gebrauch angemessener Sicherheitsausrüstungen;
- Schulung in erster Hilfe.

Allgemeine Sicherheitsvorschriften

Dieses Gerät wird mit Elektrizität betrieben. Beachten Sie genauestens die in der Betriebsanleitung vorgeschriebenen Sicherheitsanforderungen an die anzulegenden Spannungen!

Bei Nichtbeachten der Warnhinweise können deshalb schwere Körperverletzungen und/oder Sachschäden auftreten.

- ☐ Nur entsprechend qualifiziertes Personal sollte an diesem Gerät oder in dessen Nähe arbeiten. Dieses Personal muß gründlich mit allen Warnungen und Instandhaltungsmaßnahmen gemäß dieser Betriebsanleitung vertraut sein.
- ☐ Der einwandfreie und sichere Betrieb dieses Gerätes setzt sachgemäßen Transport, fachgerechte Lagerung und Montage sowie sorgfältige Bedienung und Instandhaltung voraus.
- ☐ Verwenden Sie die Geräte nur wie im vorliegenden Handbuch vorgesehen. Beachten Sie insbesondere alle Warnungen und sicherheitsrelevanten Hinweise.
- ☐ Eventuell notwendige Arbeiten an der Elektroinstallation dürfen nur von einer hierfür ausgebildeten Fachkraft durchgeführt werden.

Warnung!
LED- oder LASER-Komponenten gemäß IEC 60825-1 (2001):
LASER KLASSE 1 - CLASS 1 LASER PRODUCT.
LICHT EMITTIERENDE DIODE KLASSE 1 - CLASS 1 LED PRODUCT.

Nationale und internationale Sicherheitsvorschriften

☐ Achten Sie auf die Übereinstimmung der elektrischen Installation mit lokalen oder nationalen Sicherheitsvorschriften.

Hinweis zur CE-Kennzeichnung

Die Geräte stimmen mit den Vorschriften der folgenden Europäischen Richtlinie überein:

89/336/EWG
Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (geändert durch RL 91/263/EWG, 92/31/EWG und 93/68/EWG).
Die EU-Konformitätserklärung wird gemäß der obengenannten EU-Richtlinien für die zuständigen Behörden zur Verfügung gehalten bei:

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Telefon 07127 14 1480

Das Produkt ist einsetzbar im Wohnbereich (Wohnbereich, Geschäfts- und Gewerbebereiche sowie Kleinbetriebe) sowie im Industriebereich.

- Störfestigkeit: EN 61000-6-2:2001
- Störaussendung: EN 55022:1998 + A1 2000 Class A

Warnung!
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.
Voraussetzung für die Einhaltung der EMV-Grenzwerte ist die strikte Einhaltung der in dieser Beschreibung und Betriebsanleitung angegebenen Aufbaurichtlinien.

FCC-Hinweis:

Es wurde nach entsprechender Prüfung festgestellt, daß dieses Gerät den Anforderungen an ein Digitalgerät der Klasse A gemäß Teil 15 der FCC-Vorschriften entspricht.
Diese Anforderungen sind darauf ausgelegt, einen angemessenen Schutz gegen Funkstörungen zu bieten, wenn das Gerät im gewerblichen Bereich eingesetzt wird. Das Gerät erzeugt und verwendet Hochfrequenzen und kann diese auch ausstrahlen, und wenn es nicht entsprechend dieser Betriebsanleitung installiert und benutzt wird, kann es Störungen des Funkverkehrs verursachen. Der Betrieb dieses Gerätes in einem Wohnbereich kann ebenfalls Funkstörungen verursachen; der Benutzer ist in diesem Fall verpflichtet, Funkstörungen auf seine Kosten zu beseitigen.

Recycling Hinweis:

Dieses Produkt ist nach seiner Verwendung entsprechend den aktuellen Entsorgungsvorschriften Ihres Landkreises / Landes / Staates als Elektronikschrott einer geordneten Entsorgung zuzuführen.

3.2 Geräteinstallation

3.2.1 Bedienelemente

DIP-Schalter

Mit dem 2poligen DIP-Schalter in der Frontblende des RS2-../..

- kann mit dem Schalter RM die RM-Funktion (Redundanz Manager) ein- bzw. ausgeschaltet werden. Im Lieferzustand (Stellung OFF) ist die RM-Funktion nicht aktiviert (siehe “Redundante Ringstruktur – HIPER-Ring” auf Seite 126).
- kann die Redundanz-Funktion ausgeschaltet werden. Hierzu bringen Sie beide Schalter in die Stellung 1 (On). Bei ausgeschalteter Redundanz-Funktion können Sie die Ring-Ports wie normale Ports benutzen.
- kann mit dem Schalter STAND-BY die Stand-by-Funktion ein- bzw. ausgeschaltet werden. Lieferzustand: Schalterstellung 0 (Off), d.h. Normalfunktion. Zur redundanten Kopplung von 10/100 Mbit/s Segmenten wird der RS2-../.. in der redundanten Strekke im Stand-by-Modus betrieben (siehe “Redundante Kopplung von HIPER-Ringen und Netzsegmenten” auf Seite 127).

Hinweis: Aktivieren Sie jeweils nur eine der beiden Funktionen STAND-BY oder RM. Das Aktivieren beider Funktionen gleichzeitig löst einen Reset des Gerätes aus.

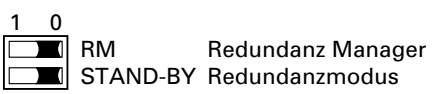


Abb. 1: 2poliger DIP-Schalter

☐ Überprüfen Sie, ob die Schaltervoreinstellung Ihren Anforderungen entspricht.

3.2.2 5poliger Klemmblock

Der Anschluß der Versorgungsspannung und des Meldekontaktes erfolgt über einen 6poligen Klemmblock mit Schraubverriegelung.

Warnung!
Die Geräte RS2-../.. sind für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsspannungsanschlüsse sowie an den Meldekontakt nur PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß IEC/EN 60950 angeschlossen werden.

- **Versorgungsspannung**
  Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den RS2-../.. alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

- **Meldekontakt:**
  Der Meldekontakt dient der Funktionsüberwachung des RS2-../.. und ermöglicht damit eine Ferndiagnose.
  Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung gemeldet:
  - der Ausfall mindestens einer der zwei Versorgungsspannungen (Versorgungsspannung 1 oder 2 < 18 V).
  - eine dauerhafte Störung im RS2-../.. (interne 3,3 VDC-Spannung).
  - der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Linkstatus kann beim RS2-../.. pro Port über das Management maskiert werden. Im Lieferzustand erfolgt keine Verbindungsüberwachung.
  - der Entfall der Redundanzgewährleistung
  - Fehler beim Selbsttest.

Im Stand-by-Modus werden folgende Zustände gemeldet:

- Steuerkabel unterbrochen
- Steuerkabel kurzgeschlossen
- Partnergerät ist im Stand-by-Modus

Im Normalmodus werden folgende Zustände gemeldet:

- Steuerkabel kurzgeschlossen
- Partnergerät ist im Normalmodus

Im RM-Betrieb wird zusätzlich folgender Zustand gemeldet:

- Ringredundanz gewährleistet. Im Lieferzustand erfolgt keine Überwachung der Ringredundanz

Hinweis: Bei nicht redundanter Zuführung der Versorgungsspannung meldet der RS2-../.. den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten (siehe “Funktionsüberwachung” auf Seite 163).

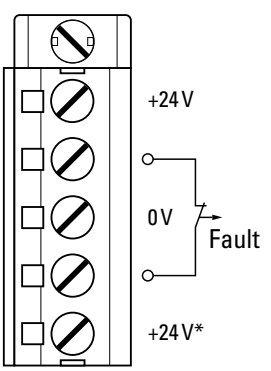


Abb. 2: Pinbelegung des 5poligen Klemmblocks

☐ Ziehen Sie den Klemmblock vom RS2-../.. ab und verdrahten Sie die Versorgungsspannungs- und Meldeleitungen.

3.2.3 Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert.

☐ Hängen Sie die obere Rastführung des RS2-../.. in die Hutschiene ein und drücken Sie es nach unten gegen die Hutschiene bis zum Einrasten.

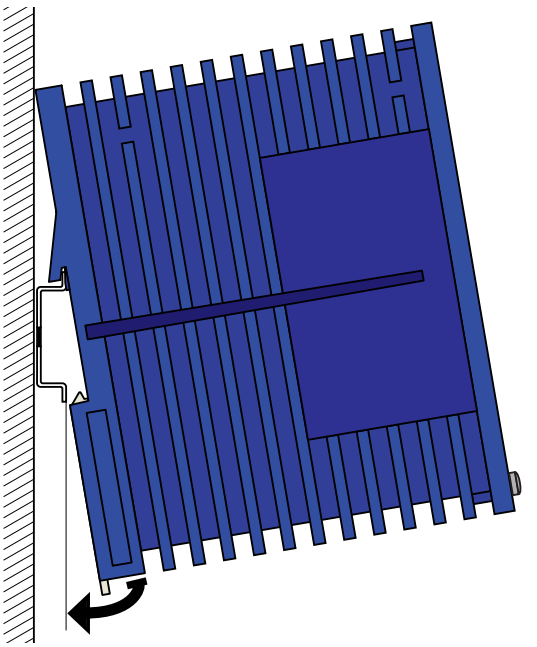


Abb. 3: Montage

Hinweis: Die Erdung der Frontblende des Gehäuses des RS2-../.. erfolgt über einen Erdungsanschluß.

Hinweis: Das Gehäuse darf nicht geöffnet werden.

Hinweis: Die Schirmungsmasse der anschließbaren Industrial Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

3.2.4 Schnittstellen

10/100 Mbit/s-Anschluß

10/100 Mbit Ports (8polige RJ45-Buchsen) ermöglichen den Anschluß von Endgeräten oder unabhängigen Netzsegmenten nach den Standards IEEE 802.3 100BASE-TX / 10BASE-T. Diese Ports unterstützen:

- Autonegotiation
- Autopolarity
- Autocrossing (bei eingeschaltetem Autonegotiation)
- 100 Mbit/s halbduplex,
- 100 Mbit/s vollduplex,
- 10 Mbit/s halbduplex,
- 10 Mbit/s vollduplex.

Lieferzustand: Autonegotiation aktiviert mit Ausnahme der HIPER-Ring-Ports (Port 6 und 7): 100 Mbit/s vollduplex.

Die Gehäuse der Buchsen sind galvanisch mit der Frontblende verbunden.

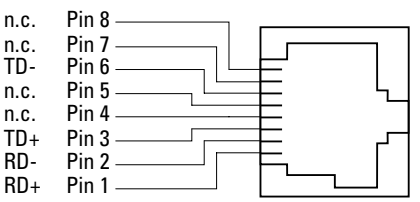


Abb. 4: Pinbelegung einer TP/TX-Schnittstelle im MDI-X-Modus, RJ45-Buchse

100 Mbit/s-LWL-Anschluß (HIPER-Ring Port)

100 MBit/s-LWL-Ports (DSC-Buchsen) ermöglichen den Anschluß von Endgeräten oder unabhängigen Netzsegmenten nach dem Standard IEEE 802.3 100BASE-FX. Diese Ports unterstützen:

- voll- und halbduplex Betrieb

Lieferzustand: vollduplex. Diese Konfiguration ist beim Aufbau redundanter Strukturen erforderlich.

Hinweis: Stellen Sie sicher, daß Sie LH-Ports nur mit LH-Ports, SM-Ports nur mit SM-Ports und MM-Ports nur mit MM-Ports verbinden.

Standby-Port

Eine 8polige RJ45-Buchse (Standby) dient zum Anschluß der Steuerleitung für die redundante Betriebsart zur redundanten Kopplung von redundanten Ringen (siehe “Redundante Kopplung von HIPER-Ringen und Netzsegmenten” auf Seite 127). Das Gehäuse der Buchse ist galvanisch mit der Frontblende des RS2-../.. verbunden. Die Ausgänge Stby_Out+ und Stby_Out- sind galvanisch von der Betriebsspannung und dem Gehäuse getrennt (Relaiskontakt).

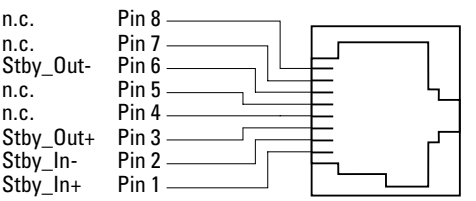


Abb. 5: Pinbelegung der Standby-Schnittstelle

Zur Bestimmung der maximalen Kabellänge des Steuerleitung messen Sie den Leitungswiderstand in Hin- und Rückrichtung. Der Gleichstromwiderstand darf bis zu 10 Ohm betragen.

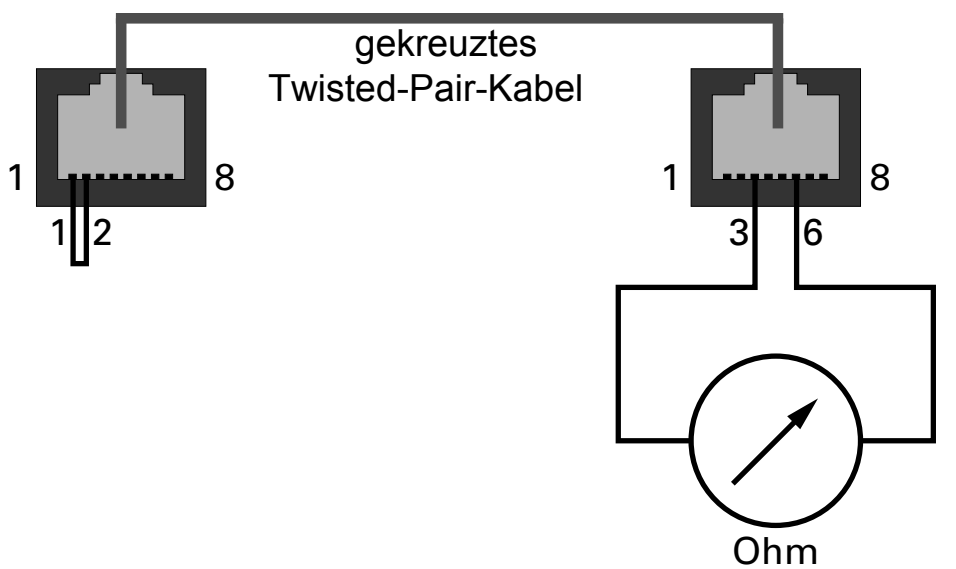


Abb. 6: Maximale Länge des Steuerungskabels

V.24-Schnittstelle (externes Management)

An der RJ11-Buchse (V.24-Schnittstelle) steht eine serielle Schnittstelle für den lokalen Anschluß

- einer externen Managementstation (VT100-Terminal oder PC mit entsprechender Terminalemulation) zur Verfügung. Damit kann eine Verbindung zum User Interface UI hergestellt werden (siehe “User Interface” auf Seite 273).
- eines AutoConfiguration Adapters ACA 11 zur Verfügung.

Einstellungen VT-100 Terminal:

- Speed:	9.600 Baud
- Data:	8 bit
- Stopbit:	1 bit
- Handshake:	off
- Parity:	none

Die V.24-Schnittstelle kann mit der Baudrate 9600 oder 19200 angesteuert werden. Die Einstellung nach Systemstart ist 9.600 Baud.
Die Übertragungsgeschwindigkeit können Sie im Systemmonitor (siehe “4 Change Baudrate” auf Seite 81) ändern.

Das Gehäuse der Anschlußbuchse ist galvanisch mit der Frontblende des Gerätes verbunden.
Die Signalleitungen sind galvanisch von der Versorgungsspannung (60 V Isolationsspannung) getrennt.

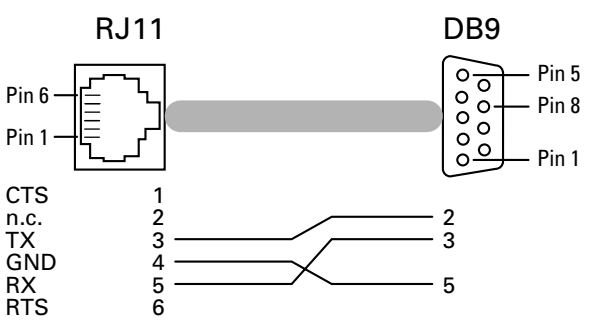


Abb. 7: Pinbelegung der V.24-Schnittstelle

☐ Montieren Sie die Signalleitungen und bei Bedarf die Steuerleitung und das Terminalkabel.

☐ Befestigen Sie das Erdungskabel an der Erdungsschraube.

3.2.5 Demontage

☐ Um den RS2-../.. von der Hutschiene zu demontieren, fahren Sie mit einem Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen - ohne den Schraubendreher zu kippen - nach unten und klappen den RS2-../.. nach oben.

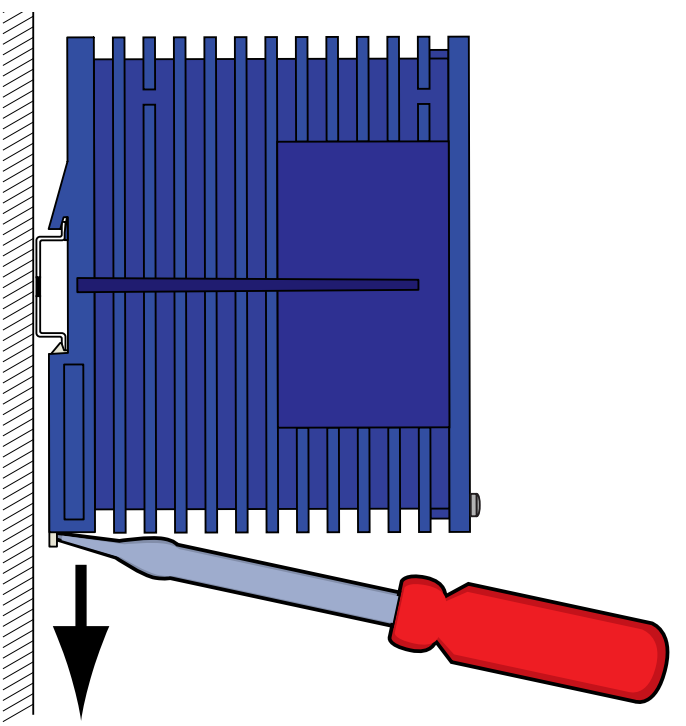


Abb. 8: Demontage

3.3 Inbetriebnahme

Mit dem Anschluß der Versorgungsspannung über den 5poligen Klemmblock nehmen Sie den RS2-../.. in Betrieb. Verriegeln Sie den Klemmblock mit der seitlichen Verriegelungsschraube.

3.4 Grundeinstellungen

Der RS2-../.. ist sehr anwenderfreundlich konzipiert und gehorcht soweit wie möglich dem Prinzip „Plug and Play“. Bei der Erstinstallation des RS2-../.. ist die Eingabe von IP-Adresse(n) notwendig.
Der RS2-../.. bietet 6 Möglichkeiten zur Konfiguration der IP-Adressen:

- Eingabe über den V.24-Anschluß,
- Eingabe mit Hilfe des HiDiscovery Protokolls
- Konfiguration über BOOTP,
- Konfiguration über DHCP,
- Konfiguration über DHCP Option 82 und
- AutoConfiguration Adapter.

3.4.1 IP-Adresse (Version 4)

Die IP-Adressen bestehen aus vier Bytes. Die vier Bytes werden durch einen Punkt getrennt, dezimal dargestellt.

Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Class	Netzadresse	Hostadresse	Adreßbereich
A	1 Byte	3 Bytes	1.0.0.0 bis 126.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Tab. 2: Klassen der IP-Adressen

Die Netzadresse stellt den festen Teil der IP-Adresse dar. Das weltweit oberste Organ für die Vergabe von Netzadressen ist die iana (Internet Assigned Numbers Authority). Wenn Sie einen IP-Adreßblock benötigen, dann kontaktieren Sie Ihren Internet-Service-Provider. Internet-Service-Provider wenden sich an ihre lokale übergeordnete Organisation:

- 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

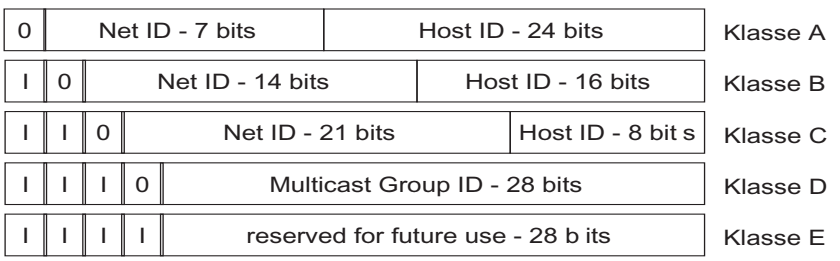


Abb. 9: Bitdarstellung der IP-Adresse

Alle IP-Adressen, deren erstes Bit eine Null ist, das heißt die erste Dezimalzahl kleiner als 128 ist, gehören der Klasse A an.
Ist das erste Bit einer IP-Adresse eine Eins und das zweite Bit eine Null, das heißt die erste Dezimalzahl liegt im Bereich von 128 bis 191, dann gehört die IP-Adresse der Klasse B an.
Sind die ersten beiden Bits einer IP-Adresse eine Eins, das heißt die erste Dezimalzahl ist größer als 191, dann handelt es sich um eine IP-Adresse der Klasse C.

Die Vergabe der Hostadresse (host id) obliegt dem Netzbetreiber. Er allein ist für die Einmaligkeit der IP-Adressen, die er vergibt, verantwortlich.

Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

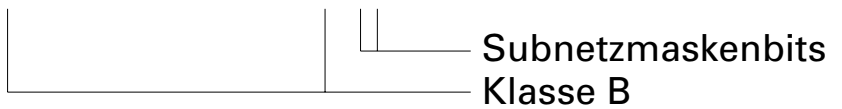
Die Einteilung in Subnetze mit Hilfe der Netzmaske geschieht analog zu der Einteilung in die Klassen A bis C der Netzadresse (net id).

Die Bits der Hostadresse (host id), die die Maske darstellen sollen, werden auf Eins gesetzt. Die restlichen Bits der Hostadresse in der Netzmaske werden auf Null gesetzt (vgl. folgende Beispiele).

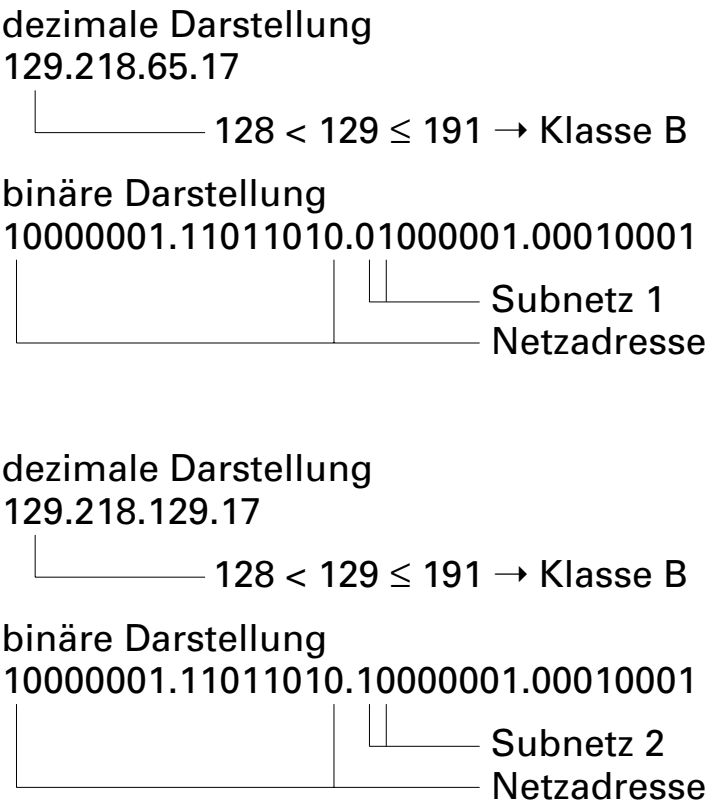
Beispiel für eine Netzmaske:

dezimale Darstellung
255.255.192.0

binäre Darstellung
11111111.11111111.11000000.00000000



Beispiel für IP-Adressen mit Subnetzzuordnung nach der Netzmaske aus dem obigen Beispiel:



Beispiel für die Anwendung der Netzmaske

In einem großen Netz ist es möglich, daß Gateways oder Router den Management-Agenten von ihrer Managementstation trennen. Wie erfolgt in einem solchen Fall die Adressierung?

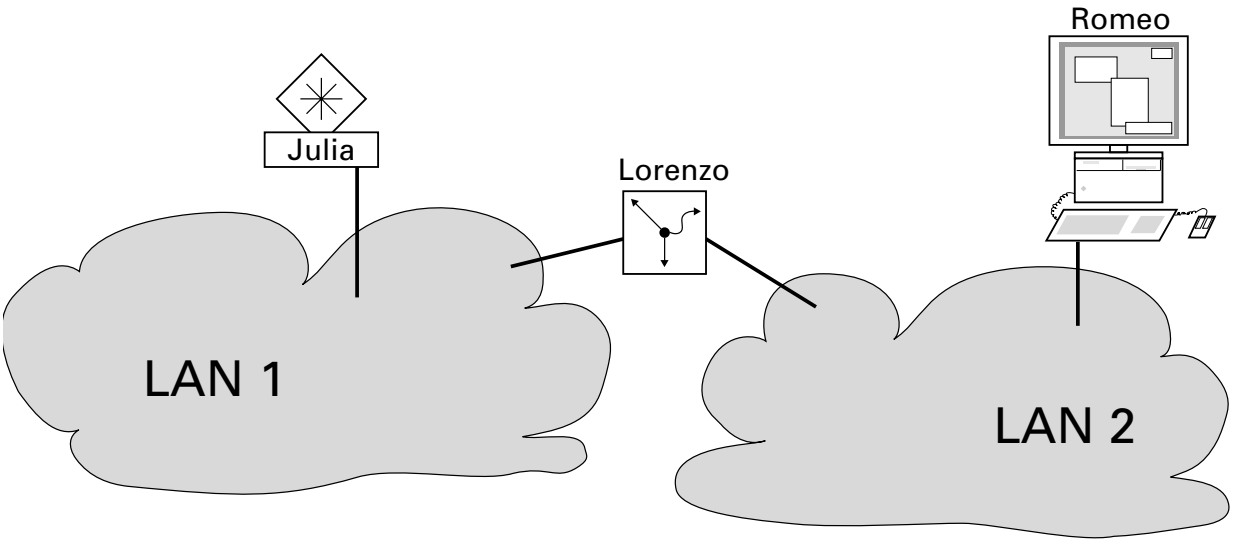


Abb. 10: Management-Agent durch Router von der Managementstation getrennt

Die Managementstation „Romeo” möchte Daten an den Management-Agenten „Julia” schicken. Romeo kennt die IP-Adresse von Julia und weiß, daß der Router „Lorenzo” den Weg zu Julia kennt.

Also packt Romeo seine Botschaft in einen Umschlag und schreibt als Zieladresse die IP-Adresse von Julia und als Quelladresse seine eigene IP-Adresse darauf.

Diesen Umschlag steckt Romeo in einen weiteren Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Quelladresse. Dieser Vorgang ist vergleichbar mit dem Übergang von der Ebene 3 zur Ebene 2 des ISO/OSI-Basis-Referenzmodells.

Nun steckt Romeo das gesamte Datenpaket in den Briefkasten, vergleichbar mit dem Übergang von der Ebene 2 zur Ebene 1, dem Senden des Datenpaketes in das Ethernet.

Lorenzo erhält den Brief, entfernt den äußeren Umschlag und erkennt auf dem inneren Umschlag, daß der Brief für Julia bestimmt ist. Er steckt den inneren Umschlag in einen neuen äußeren Umschlag, schaut in seiner Adreßliste, der ARP-Tabelle, nach der MAC-Adresse von Julia und schreibt diese auf den äußeren Umschlag als Zieladresse und seine eigene MAC-Adresse als Quelladresse. Das gesamte Datenpaket steckt er anschließend in den Briefkasten.

Julia empfängt den Brief, entfernt den äußeren Umschlag. Übrig bleibt der innere Umschlag mit Romeos IP-Adresse. Das Öffnen des inneren Umschlages und lesen der Botschaft entspricht einer Übergabe an höhere Protokollschichten des ISO/OSI-Schichtenmodells.

Julia möchte eine Antwort an Romeo zurücksenden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Quelladresse. Doch wohin soll Sie die Antwort schicken? Die MAC-Adresse von Romeo hat sie ja nicht erhalten. Die MAC-Adresse von Romeo blieb beim Wechseln des äußeren Umschlags bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen `hmNetGatewayIPAddr` Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

3.4.2 System-Konfiguration via V.24

Sollten Sie weder über BOOTP, DHCP, HiDiscovery Protokoll noch über den AutoConfiguration Adapter ACA das System konfigurieren, dann nehmen Sie die Konfiguration über den V.24-Schnittstelle vor:

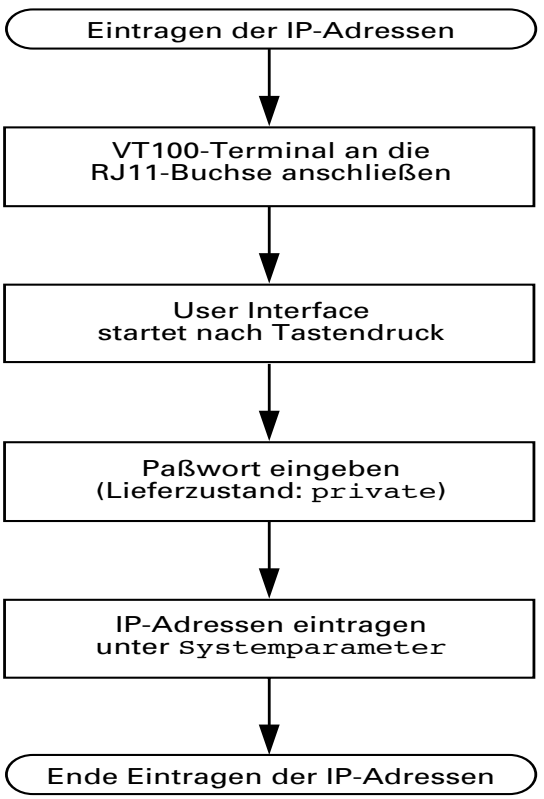


Abb. 11: Ablaufdiagramm Eintragen der IP-Adressen

Sollten Sie in der Nähe des Installationsortes kein VT100-Terminal zur Verfügung haben, dann können Sie vor der endgültigen Installation die IP-Adressen eingeben. Hierzu benötigen Sie ein VT100-Terminal oder eine entsprechende Emulation (z. B. MS Windows Terminal).

Hinweis: Bei der Installation mehrerer RS2-../.. ist es einfacher, wenn Sie an Ihrem Arbeitsplatz jedem RS2-../.. die jeweiligen IP-Adressen eingeben. Selbst bei der Installation von einem RS2-../.. kann es komfortabler sein, die IP-Adressen an Ihrem Arbeitsplatz einzugeben.

Das Kennzeichnen der RS2-../.. verhindert eine spätere Verwechslung bei der Installation.

☐ Schließen Sie an die RJ11-Buchse „V.24“ ein VT100-Terminal oder einen PC mit Terminal-Emulation an.
Übertragungsparameter:

Speed:	9.600 Baud
Data:	8 bit
Parity:	none
Stopbit:	1 bit
Handshake:	off

Hinweis: Die Übertragungsgeschwindigkeit können Sie im Systemmonitor (siehe “4 Change Baudrate” auf Seite 81) ändern.

☐ Nach der Installation des RS2-../.. starten Sie diesen durch Anlegen der Spannungsversorgung. Das Betriebssystem wird geladen.
Das User Interface startet nach einem Tastendruck (siehe “Öffnen des User Interfaces” auf Seite 275).

☐ Geben Sie das von Ihnen vergebene Paßwort ein (Großschreibung beachten) ein und drücken Sie anschließend die Eingabetaste.

Hinweis: Im Lieferzustand ist das Paßwort `private` eingestellt.

☐ Tragen Sie die IP-Adressen ein, wie in “System Parameter” auf Seite 277 beschrieben und gemäß den folgenden Erläuterungen.

- **Lokale IP-Adresse (`local ip-address`)**
  Im Lieferzustand besitzt der RS2-../.. die lokale IP-Adresse 0.0.0.0.

- **IP-Adresse des Gateways (`gateway ip-address`)**
  Diese Eingabe ist nur notwendig, wenn sich der RS2-../.. und die Managementstation bzw. der tftp-Server in unterschiedlichen Subnetzen befinden (siehe “Beispiel für die Anwendung der Netzmaske” auf Seite 49).
  Tragen Sie die IP-Adresse des Gateways ein, das das Subnetz mit dem RS2-../.. vom Pfad zur Managementstation trennt.
  Im Lieferzustand ist die IP-Adresse 0.0.0.0 eingetragen.

- **Netzmaske (`netmask`)**
  Haben Sie Ihr Netz in Subnetze aufgeteilt und identifizieren Sie diese mit einer Netzmaske, dann geben Sie an dieser Stelle die Netzmaske ein.
  Im Lieferzustand ist die Netzmaske 0.0.0.0 eingetragen.

Die Adressen werden in einem nichtflüchtigen Speicher abgelegt.

Nach der Eingabe der IP-Adresse können Sie den RS2-../.. über das “Web-based Management” auf Seite 143 komfortabel konfigurieren.

3.4.3 System-Konfiguration via HiDiscovery

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Switch über das Ethernet IP-Parameter zuzuweisen.
WeitereParameter können Sie mit dem “Web-based Management” auf Seite 143 komfortabel konfigurieren.

Installieren Sie die HiDiscovery-Software auf Ihrem PC. Die Software befindet sich auf der CD, die mit dem Switch ausgeliefert wurde.

☐ Zur Installation starten Sie das Installationsprogramm auf der CD.

Hinweis: Die Installation von HiDiscovery beinhaltet die Installation des Softwarepaketes WinPcap Version 3.0.
Sollte bereits eine frühere Version von WinPcap auf dem PC vorhanden sein, dann deinstallieren Sie diese zuvor. Eine neuere Version bleibt bei der Installation von HiDiscovery erhalten. Dies kann jedoch nicht für alle zukünftigen Versionen von WinPcap garantiert werden. Für den Fall, daß die Installation von HiDiscovery eine neuere Version von WinPCap überschrieben haben sollte, deinstallieren Sie WinPcap 3.0 und installieren Sie danach wieder die neue Version.

☐ Starten Sie das Programm HiDiscovery.

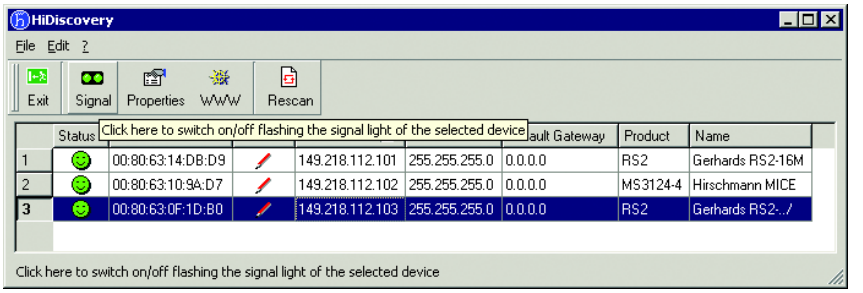


Abb. 12: HiDiscovery

Beim Start von HiDiscovery untersucht HiDiscovery automatisch das Netz nach Geräten, die das HiDiscovery-Protokoll unterstützen.
HiDiscovery benutzt die erste gefundene Netzwerkkarte des PCs. Sollte Ihr Rechner über mehrere Netzwerkkarten verfügen, können Sie diese in HiDiscovery in der Werkzeugleiste auswählen.

HiDiscovery zeigt für jedes Gerät, das auf das HiDiscovery Protokoll reagiert, eine Zeile an.

HiDiscovery ermöglicht das Identifizieren der angezeigten Geräte.
☐ Wählen Sie eine Gerätezeile aus.
☐ Klicken Sie auf das Symbol mit den zwei grünen Punkten in der Werkzeugleiste, um das Blinken der LEDs des ausgewählten Gerätes einzuschalten. Ein weiters Klicken auf das Symbol schaltet das Blinken aus.

Mit einem Doppelklick auf eine Zeile öffnen Sie ein Fenster, in dem Sie den Gerätename und die IP-Parameter eintragen können.

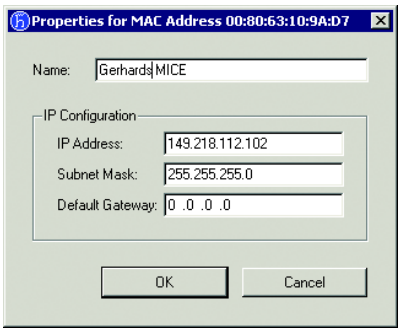


Abb. 13: HiDiscovery - IP-Parameter-Zuweisung

Hinweis: Schalten Sie aus Sicherheitsgründen im Web-based Interface die HiDiscovery-Funktion des Gerätes aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben.

3.4.4 System-Konfiguration via BOOTP (bootstrap protocol)

Bei der Inbetriebnahme erhält ein RS2-../.. gemäß dem Ablaufdiagramm "BOOTP-Prozeß" (siehe Abb. 14) seine Konfigurationsdaten.

Ein BOOTP-Server sollte folgende Daten für einen RS2-../.. bereitstellen:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# 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=ether-
net:ha=008063086501:ip=149.218.112.83:tc=.global:
rs2_02:ht=ether-
net:ha=008063086502:ip=149.218.112.84:tc=.global:
.
.
```

Zeilen mit vorangestelltem #-Zeichen sind Kommentarzeilen.

Die Zeilen unter ".global:" dienen der Arbeitserleichterung bei der Konfiguration mehrerer Geräte. Jedem Gerät weisen Sie mit dem Template (tc) die globalen Konfigurationsdaten (tc=.global:) zu.
In den Gerätezeilen (rs2-0...) erfolgt die direkte Zuordnung von Hardware- und IP-Adresse.

☐ Geben Sie für jedes Gerät eine Zeile ein.
☐ Geben Sie nach `ha=` die Hardware-Adresse des Gerätes ein.
☐ Geben Sie nach `ip=` die IP-Adresse des Gerätes ein.

Der RS2-../.. speichert die durch BOOTP gewonnenen Konfigurationsdaten permanent in seinen Flash-Speicher.

Zum Aktivieren/Deaktivieren von BOOTP siehe “IP-Konfiguration” auf Seite 279 und “Systemdaten” auf Seite 154.

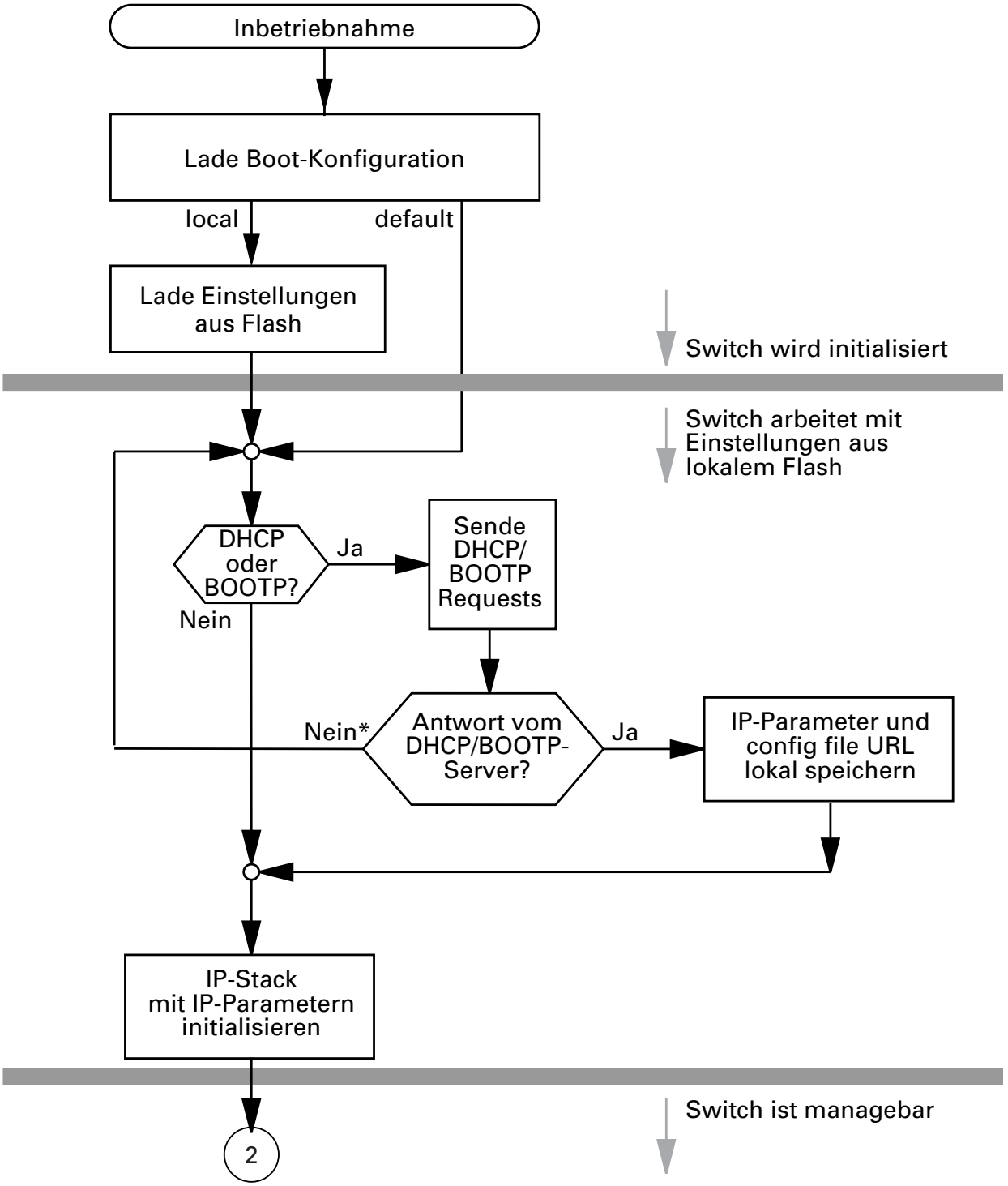


Abb. 14: Ablaufdiagramm BOOTP/DHCP-Prozeß, Teil 1
** siehe Hinweis auf Seite 160*

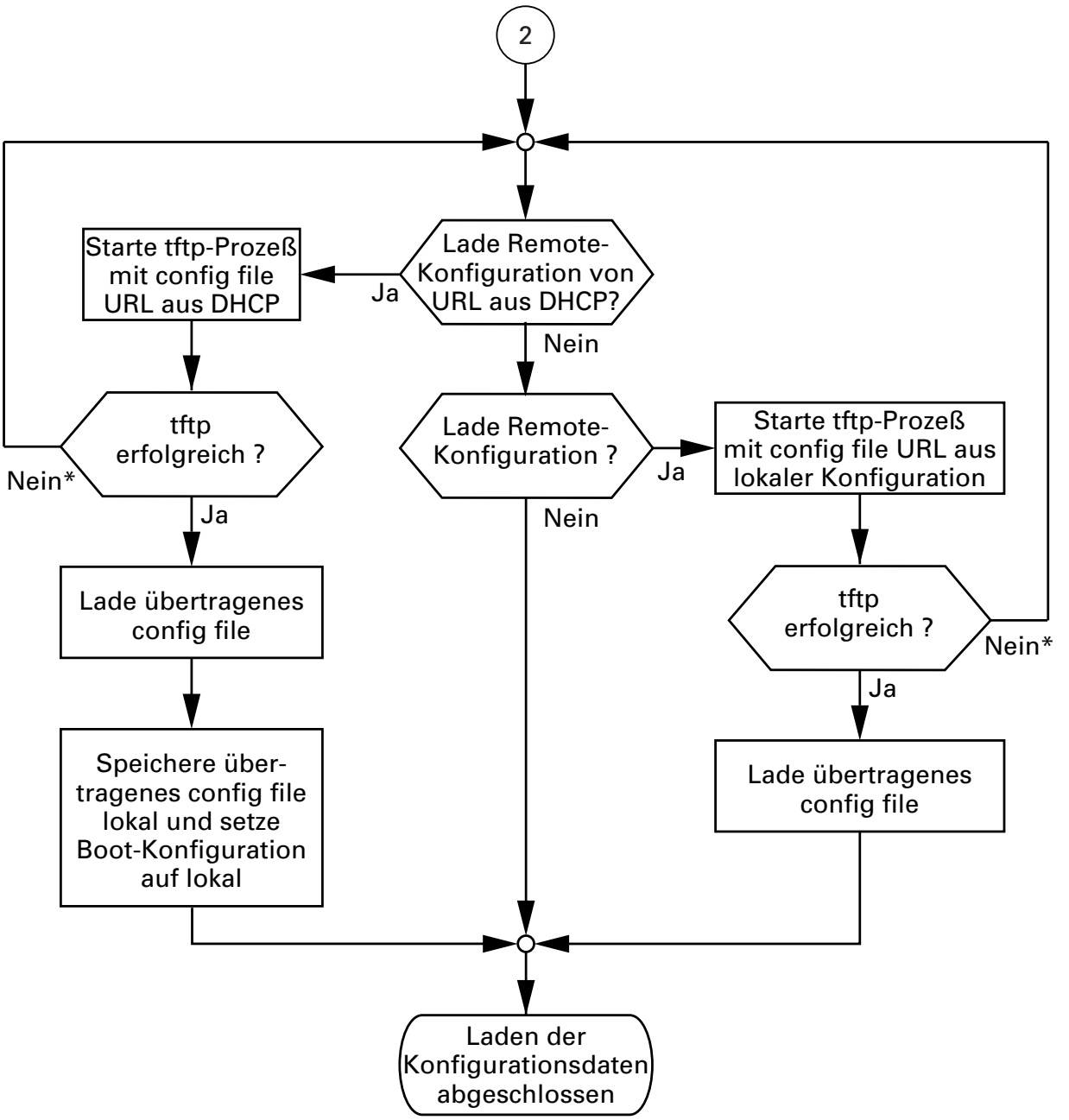


Abb. 15: Ablaufdiagramm BOOTP/DHCP-Prozeß, Teil 2
** siehe Hinweis auf Seite 160*

3.4.5 System-Konfiguration via DHCP (dynamic host configuration protocol)

Das DHCP verhält sich im Grunde wie das BOOTP und bietet zusätzlich die Konfiguration eines DHCP-Clients über einen Namen anstatt über die MAC-Adresse an. Dieser Name heißt bei DHCP nach rfc 2131 "client identifier". Der RS2-../.. verwendet den in der System-Gruppe der MIB II unter `sysName` eingetragenen Namen (siehe Seite 231) als client identifier. Die Eingabe dieses Systemnamens können Sie direkt vornehmen über SNMP, das Web-based Management (siehe “Systemdaten” auf Seite 154) oder das User Interface (siehe “System Parameter” auf Seite 277).

Bei der Inbetriebnahme erhält ein RS2-../.. gemäß dem Ablaufdiagramm "BOOTP/DHCP-Prozeß" (siehe Abb. 14) seine Konfigurationsdaten.

Der RS2-../.. übermittelt seinen Systemnamen dem DHCP-Server. Der DHCP-Server kann dann alternativ zur MAC-Adresse anhand des Systemnamens eine IP-Adresse vergeben.
Neben der IP-Adresse überträgt der DHCP-Server
– den tftp-Server-Namen (falls vorhanden),
– den Namen der Konfigurationsdatei (falls vorhanden).
Der RS2-../.. übernimmt diese Daten als Konfigurationsparameter (siehe “Netzparameter festlegen” auf Seite 170).
Wurde eine IP-Adresse von einem DHCP-Server zugeteilt, wird diese permanent lokal gespeichert.

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

Tab. 3: DHCP-Optionen, die der Switch anfordert

Das besondere von DHCP gegenüber BOOTP ist, daß der Server die Konfigurationsparameter (“lease”) nur für eine bestimmte Zeitspanne zur Verfügung stellen kann. Nach Ablauf dieser Zeitspanne (“lease duration”), muß der DHCP-Client versuchen dieses lease entweder zu erneuern oder ein neues lease aushandeln. Es kann zwar am Server ein BOOTP-ähnliches Verhalten eingestellt werden (d.h. einem bestimmten Client wird anhand der MAC-Adresse immer dieselbe IP-Adresse zugeordnet), aber dies setzt die explizite Konfiguration eines im Netz befindlichen DHCP-Servers voraus. Erfolgt diese Konfiguration nicht, wird irgendeine IP-Adresse – die gerade frei ist – zugewiesen.

Solange DHCP aktiviert ist, versucht der RS2-../.. eine IP-Adresse zu bekommen. Findet er nach einem Neustart keinen DHCP-Server, dann hat er keine IP-Adresse.
Zum Aktivieren/Deaktivieren von DHCP siehe “Netzparameter festlegen” auf Seite 170.

Hinweis: Achten Sie bei der Anwendung vom Netzmanagement HiVision darauf, daß DHCP jedem RS2-../.. immer die original IP-Adresse zuweist.

Beispiel für eine DHCP-Konfigurationsdatei:

```
# /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";
}
```

Zeilen mit vorangestelltem #-Zeichen sind Kommentarzeilen.
Die Zeilen vor den einzeln aufgeführten Geräten bezeichnen Einstellungen, die für alle folgenden Geräte gelten.
Die Zeile `fixed-address` weist dem Gerät eine feste IP-Adresse zu.
Weitere Informationen entnehmen Sie Ihren DHCP-Server-Handbuch.

3.4.6 System-Konfiguration via DHCP Option 82

Wie beim klassischen DHCP erhält bei der Inbetriebnahme ein Agent gemäß dem Ablaufdiagramm „BOOTP/DHCP-Prozeß“ (siehe Abb. 14) seine Konfigurationsdaten.

Während sich die System-Konfiguration über das klassische DHCP-Protokoll (siehe “System-Konfiguration via DHCP (dynamic host configuration protocol)” auf Seite 59) am zu konfigurierenden Gerät orientiert, orientiert sich die Option 82 an der Netztopologie. Dieses Verfahren bietet somit die Möglichkeit, einem beliebigen Gerät, das an einem bestimmten Ort (Port eines Switches) am LAN angeschlossen wird, immer die selbe IP-Adresse zuzuordnen.

Die Installation eines DHCP-Servers beschreibt das Kapitel “DHCP-Server Option 82 einrichten” auf Seite 299.

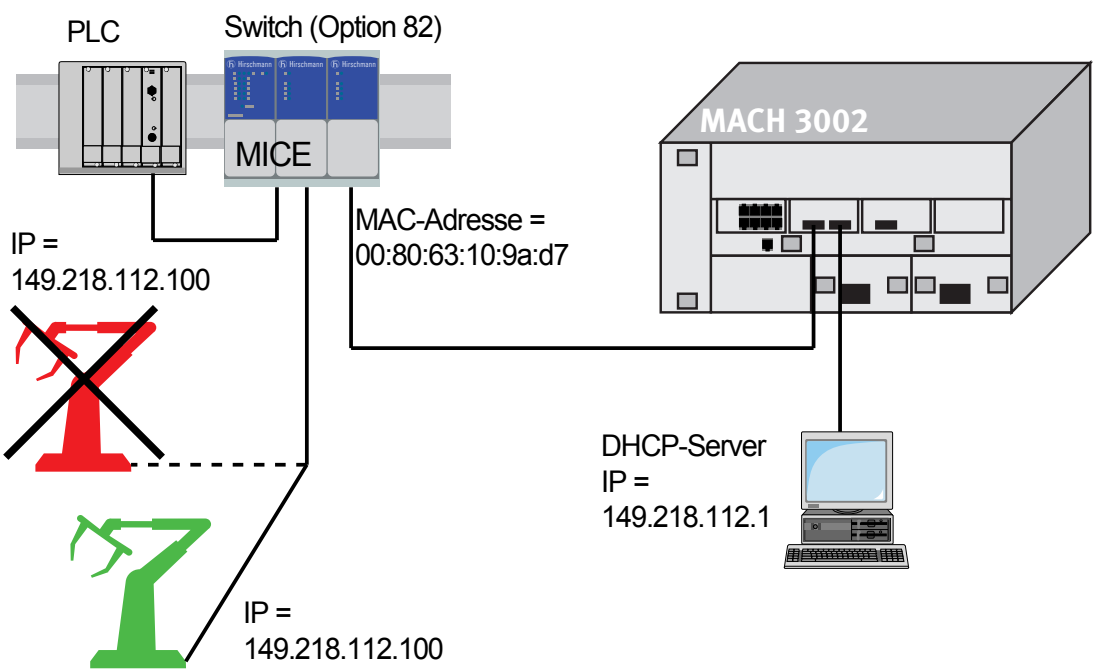


Abb. 16: Anwendungsbeispiel für den Einsatz von Option 82

3.4.7 AutoConfiguration Adapter ACA

Der ACA ist ein Gerät zum Speichern der Konfigurationsdaten eines Switches MICE, RS2-16M, RS2-../.. oder MACH 3000. Der ACA ermöglicht beim Ausfall eines Switches eine denkbar einfache Konfigurationdatenübernahme durch einen Ersatzswitch des gleichen Typs.

Mit „Lokal Konfiguration speichern“ können Sie die aktuelle Switch-Konfiguration auf den ACA 11 und in den Flash-Speicher übertragen.

Bei einem Neustart übernimmt der Switch die Konfigurationsdaten des ACAs und speichert Sie nicht flüchtig im Flash-Speicher. Welche Daten der Switch vom ACA übernimmt, hängt von der Einstellung der Neustartkonfiguration ab (siehe “Start-Konfiguration festlegen” auf Seite 159).

Einstellung	Auswirkung
Lokal	Der Switch übernimmt alle Daten aus dem ACA
vom URL	Der Switch übernimmt die IP-Parameter aus dem ACA und die anderen Daten vom URL
Voreinstellung	Der Switch übernimmt die IP-Parameter aus dem ACA und setzt die anderen Parameter auf den Lieferzustand

Tab. 4: Datenübernahme vom ACA nach Neustart

Weitere Informationen zur Bedienung des ACAs finden Sie im Kapitel “Update” auf Seite 289 und “Start-Konfiguration festlegen” auf Seite 159.

3.5 tftp-Server für SW-Updates

Im Lieferzustand steht die Switch-Software im Flash-Speicher. Der RS2-../.. bootet die Software vom Flash-Speicher.

Über einen tftp-Server können Software-Updates durchgeführt werden. Dies setzt voraus, daß im angeschlossenen Netz ein tftp-Server installiert und aktiv ist.

Hinweis: Eine Alternative zum tftp-Update bildet das http-Update. Das http-Update erspart die Konfiguration des tftp-Servers.

Um vom tftp-Server einen Software-Update durchführen zu können benötigt der RS2-../.. folgende Informationen:

- eigene IP-Adresse (fest eingetragen),
- IP-Adresse des tftp-Servers, bzw. des Gateways zum tftp-Server,
- Pfad, in dem das Betriebssystem des tftp-Servers liegt.
  (siehe “Update” auf Seite 289).

Der File-Transfer zwischen RS2-../.. und tftp-Server wird über das **T**rivial **F**ile **T**ransfer **P**rotocol (tftp) abgewickelt.

Managementstation und tftp-Server können sowohl aus einem als auch aus verschiedenen Rechnern bestehen.

Das Vorbereiten des tftp-Servers für die RS2-../..-Software beinhaltet die Schritte:

- Einrichten des RS2-../..-Verzeichnisses und kopieren der RS2-../..-Software
- Einrichten des tftp-Prozesses

3.5.1 tftp-Prozeß einrichten

Allgemeine Voraussetzungen:

- Die lokale IP-Adresse des RS2-../.. und die IP-Adresse des tftp-Servers bzw. des Gateways sind dem RS2-../.. bekannt.
- Der TCP/IP-Stack mit tftp ist auf dem tftp-Server installiert.

Die folgenden Abschnitte enthalten Hinweise zum Einrichten des tftp-Prozesses gegliedert nach Betriebssystemen und Anwendungen.

SunOS und HP

☐ Überprüfen Sie zunächst, ob der tftp-Dämon (Hintergrundprozeß) läuft, d. h. ob in der Datei /etc/inetd.conf folgende Zeile enthalten ist (siehe Abb. 17) und dessen Prozeßstatus „IW“ ist:

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
```

Falls dieser Prozeß nicht oder nur als Kommentarzeile (#) eingetragen ist, ändern Sie /etc/inetd.conf entsprechend und führen danach eine Neuinitialisierung des INET-Dämon durch. Dies geschieht mit dem Befehl „kill -1 PID“, wobei PID die Prozeßnummer von inetd ist. Durch Eingabe der folgenden UNIX-Befehlszeile wird diese Neuinitialisierung automatisch durchgeführt:

SunOS

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

HP

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

Eine zusätzliche Information zum tftp-Dämon tftpd können Sie mit dem UNIX-Kommando „man tftpd“ abrufen.

Hinweis: Der tftp-Dämon wird nicht immer mit dem Befehl „ps“ angezeigt, obwohl er läuft.

Besonderheit bei HP-Workstations:

☐ Tragen Sie bei der Installation auf einer HP-Workstation in die Datei /etc/passwd den Benutzer tftp ein.

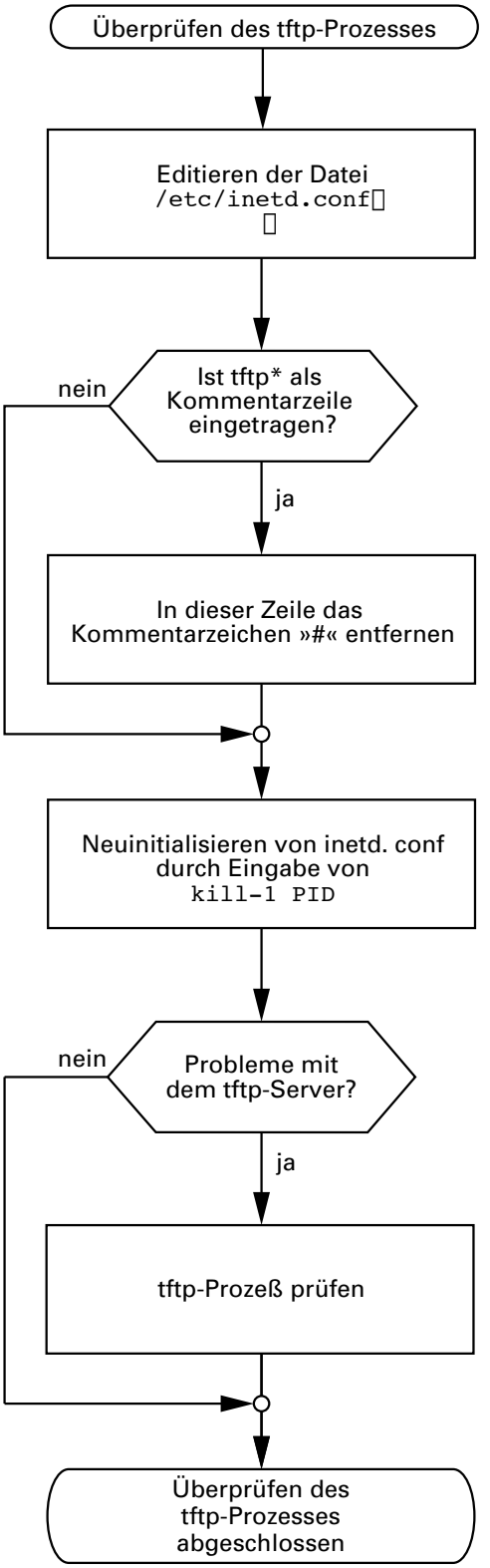
Zum Beispiel:

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

tftp	Benutzerkennung,
*	steht im Paßwortfeld,
510	Beispiel für die user-Nr.,
20	Beispiel für die group-Nr.,
tftp server	frei wählbare sinnvolle Bezeichnung,
/bin/false	obligatorischer Eintrag (login shell)

☐ Testen Sie den tftp-Prozeß mit z. B.:

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



z. B:

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

Antwort, wenn der Prozeß läuft: `Received ...`

```
rm rs2.bin
```

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

Abb. 17: Ablaufdiagramm tftp-Server einrichten bei SunOS und HP

3.5.2 Software-Zugriffsrechte

Der Agent benötigt Leserecht auf dem tftp-Verzeichnis, in das die RS2-../..-Software abgelegt ist.

Beispiel für einen tftp-Server unter UNIX

Nach der Installation der RS2-../..-Software sollte sich folgende Verzeichnis-Struktur mit den angegebenen Zugriffsrechten auf dem tftp-Server befinden:.

Dateiname	Rechte
rs2.bin	444-r--r--r--

Tab. 5: Verzeichnisstruktur der Software

`d` = Verzeichnis; `r` = lesen; `w` = schreiben; `x` = durchführen
1. Stelle bezeichnet `d` (Verzeichnis),
2. bis 4. Stelle bezeichnen die Zugriffsrechte vom Benutzer,
5. bis 7. Stelle bezeichnen die Zugriffsrechte von Benutzergruppen,
8. bis 10. Stelle bezeichnen die Zugriffsrechte aller anderen.

3.6 System-Monitore

Die System-Monitore ermöglichen die Durchführung eines

- Update des Betriebssystems

Das Software-Update kann über V.24 oder tftp erfolgen.

Der V.24-Anschluß des RS2-../.. unterstützt die Baudraten 9600, 19.200.

3.6.1 Betriebssystem-Update (System-Monitor 1)

System-Monitor 1 ermöglicht ein Update des Betriebssystems des RS2-../.. über den V.24-Anschluß.

Das dazugehörige Bildschirmfenster enthält die Auswahl zwischen

- 1 Update Operation System
- 2 Start Operation System
- 3 Change Baudrate
- 4 End

Hinweis: Benutzen Sie zum Update des Betriebssystems vorzugsweise den Systemmonitor 2.

Beim Booten des RS2-../.. mit 9600 Baud erscheint auf dem Terminal die Meldung „Press <1> to enter Monitor“.

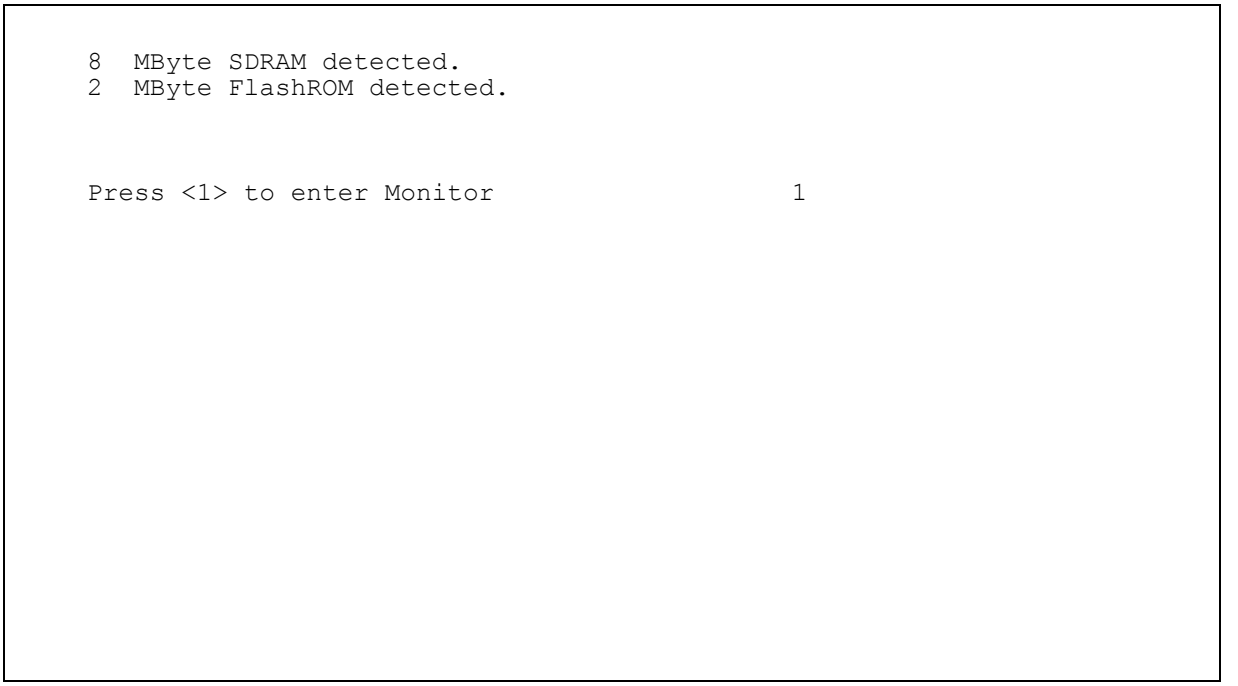


Abb. 18: Bildschirmansicht beim Bootvorgang

Drücken Sie innerhalb von einer Sekunde die <1>-Taste, um den System-Monitor 1 zu starten.

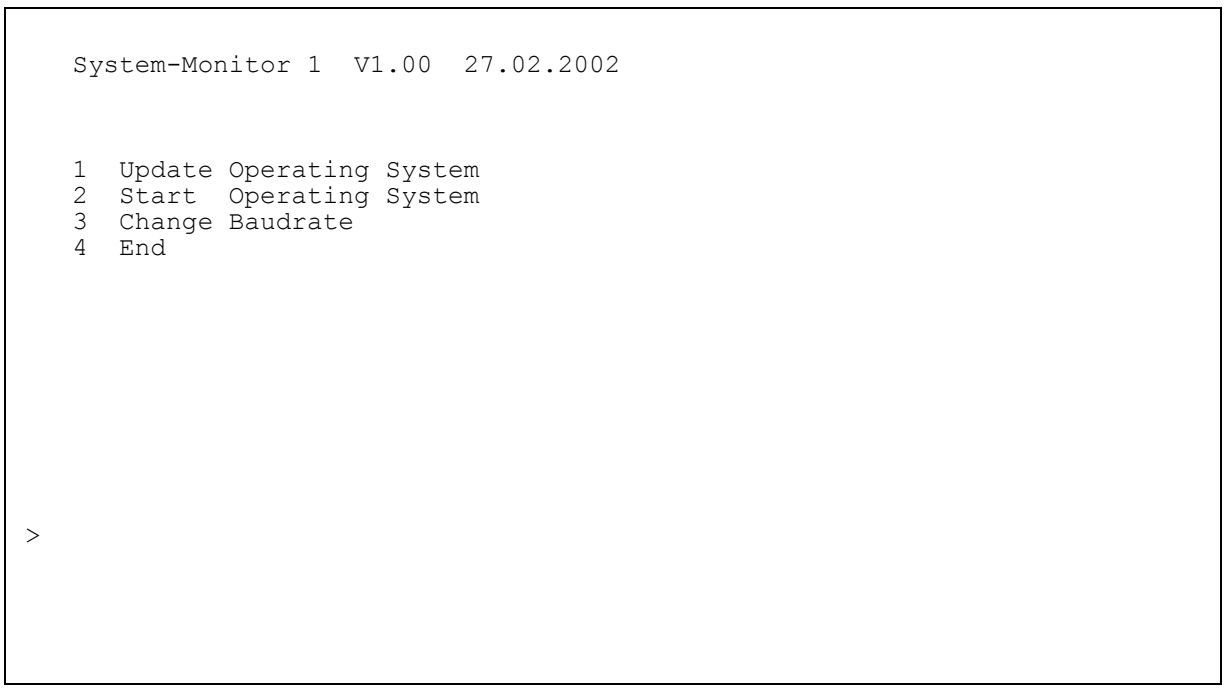


Abb. 19: Bildschirmansicht System-Monitor 1

1 Update Operation System

Mit diesem Menüpunkt führen Sie ein Update des Betriebssystems durch.
Am Bildschirm erscheint folgendes Fenster:

```
         Update Operating System with XMODEM

Maximal buffer size : 2031616 Bytes

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

Abb. 20: Bildschirmansicht Update Betriebssystem

Um den Bildschirm zu verlassen und zum Hauptmenü des System-Monitor 1 zurückzukehren, drücken Sie <ESC>.

Drücken Sie <RETURN>, um den Update mit XMODEM zu starten. Es erscheint folgendes Bildschirmfenster:

```
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 seconds
```

Abb. 21: Bildschirmansicht beim Start des Betriebssystem-Updates

Geben Sie anschließend den Pfad ein, in dem sich das aufzuspielende Betriebssystem befindet. Die Pfadeingabe erfolgt über das Terminalprogramm, z. B. unter Übertragung:Binärdatei. Die Übertragung beginnt. Nach dem Ende der Übertragung wird das Betriebssystem neu gestartet.

2 Start Operation System

Geben Sie die Ziffer „2“ ein, um das Betriebssystem zu starten.
Der System-Monitor 1 wird beendet. Das Betriebssystem wird mit 9.600 Baud gestartet.

3 Change Baudrate

Mit diesem Menüpunkt können Sie die Baudrate modifizieren.
Am Bildschirm erscheint folgendes Fenster:

```
   Change baudrate


   1    9600 baud
   2   19200 baud









>
```

Abb. 22: Bildschirmansicht beim Modifizieren der Baudrate

Für ein Betriebssystem-Update (vgl. Menüpunkt 1) sollten Sie die maximal mögliche Geschwindigkeit für die Baudrate wählen.
Passen Sie danach die Geschwindigkeit Ihres Terminal-Programms an diese Baudrate an.

4 End

Dieser Menüpunkt beendet den System-Monitor 1.
Am Bildschirm erscheint folgendes Fenster:

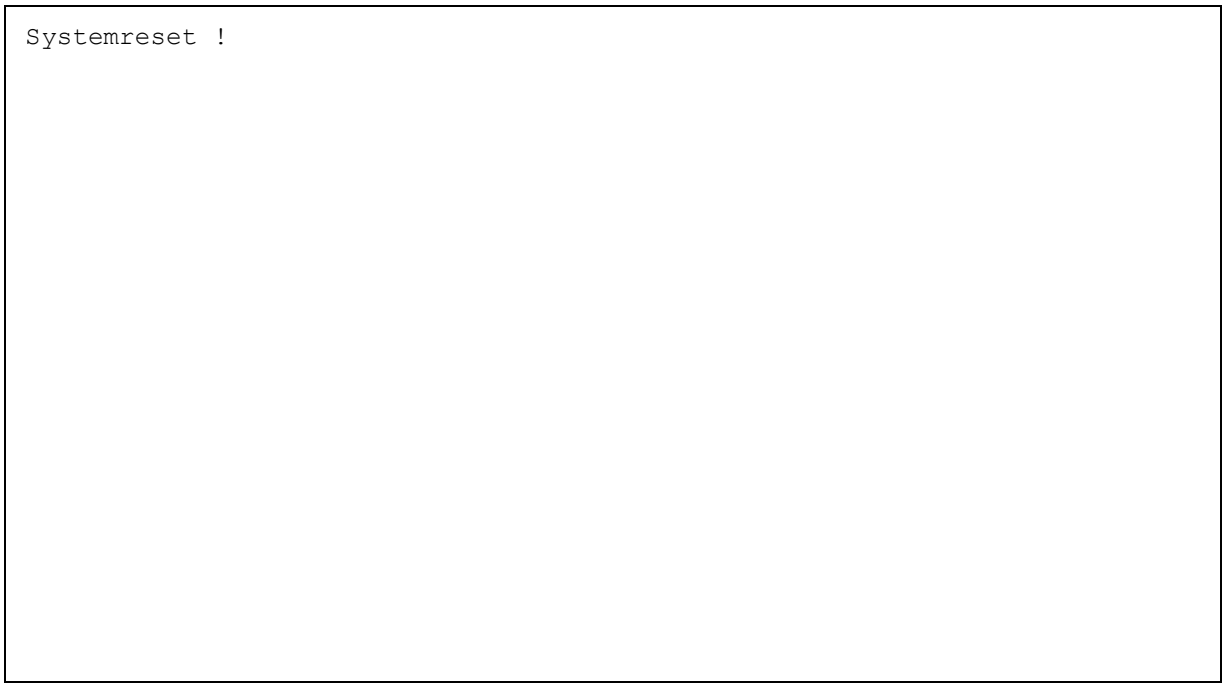


Abb. 23: Bildschirmansicht beim Beenden von System-Monitor 1

Führen Sie anschließend einen Hardware-Reset durch.

3.6.2 Software-Update (System-Monitor 2)

System-Monitor 2 ermöglicht ein Update des Betriebssystems des RS2-../.. sowohl über V.24 als auch über tftp.
Das dazugehörige Bildschirmfenster enthält die Auswahl zwischen

- 1 Software Update V24
- 2 Software Update tftp
- 3 Cancel Automatic Update
- 4 Change Baudrate
- 5 Set Factory Settings
- 6 Reset
- 7 End/Quit

Beim Booten des RS2-../.. mit 9.600 Baud erscheint am Bildschirm folgendes Fenster:

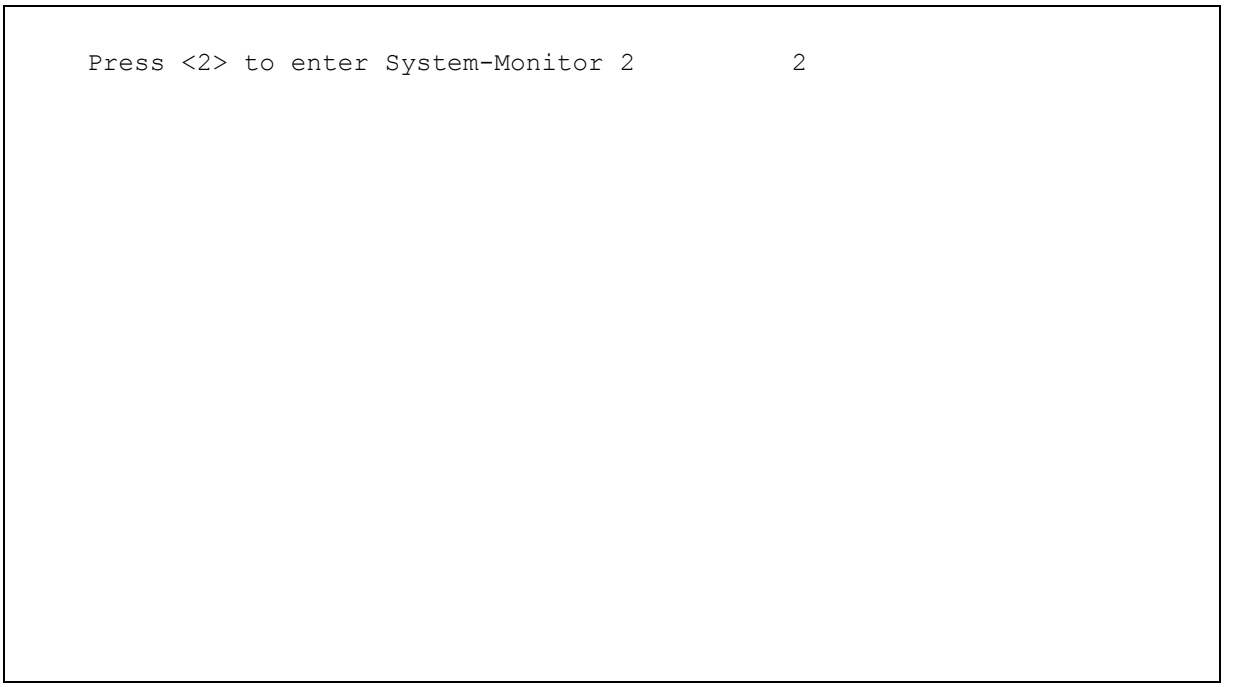


Abb. 24: Bildschirmansicht beim Starten von System-Monitor 2

Drücken Sie innerhalb von drei Sekunden die <2>-Taste. System-Monitor 2 wird gestartet.

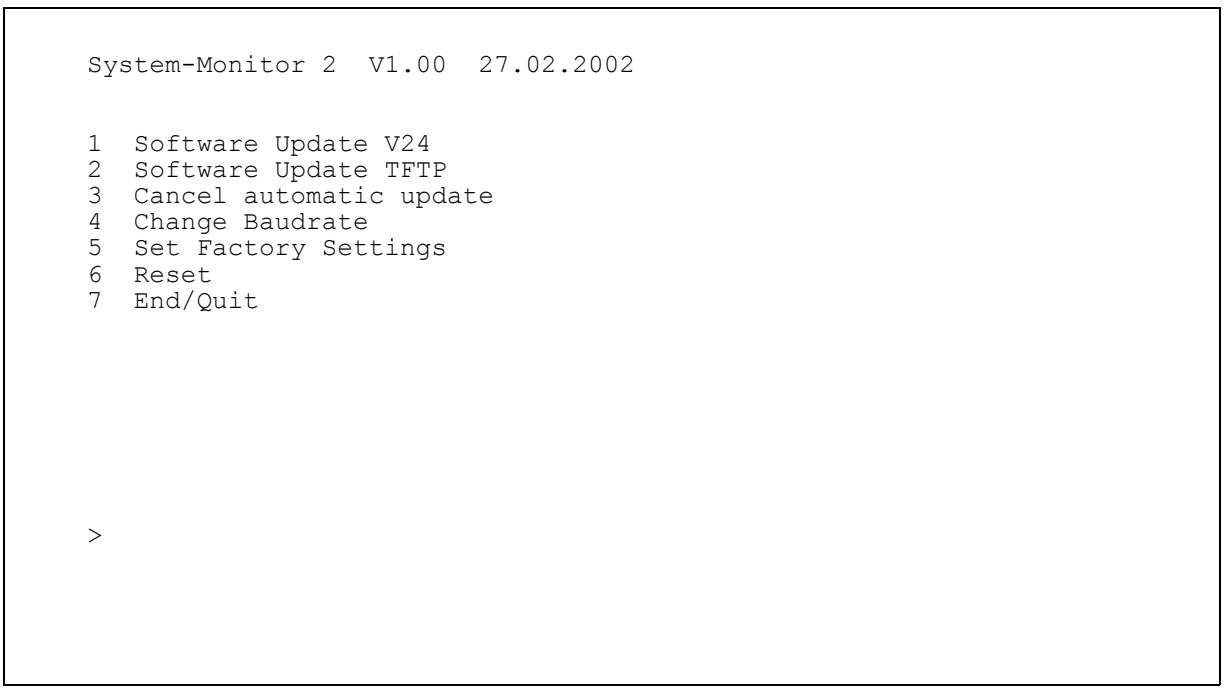


Abb. 25: Bildschirmansicht System-Monitor 2

1 Software Update V24

Dieser Menüpunkt führt ein Update des Betriebssystems im Flash-Speicher des RS2-../.. durch. Das Update erfolgt über V.24.

Hinweis: Benutzen Sie zum Update des Betriebssystems vorzugsweise die tftp-Übertragung (siehe “Update” auf Seite 289). Sie ist mehr als dreimal schneller als die schnellste V.24-Übertragung.

Am Bildschirm erscheint folgendes Fenster:

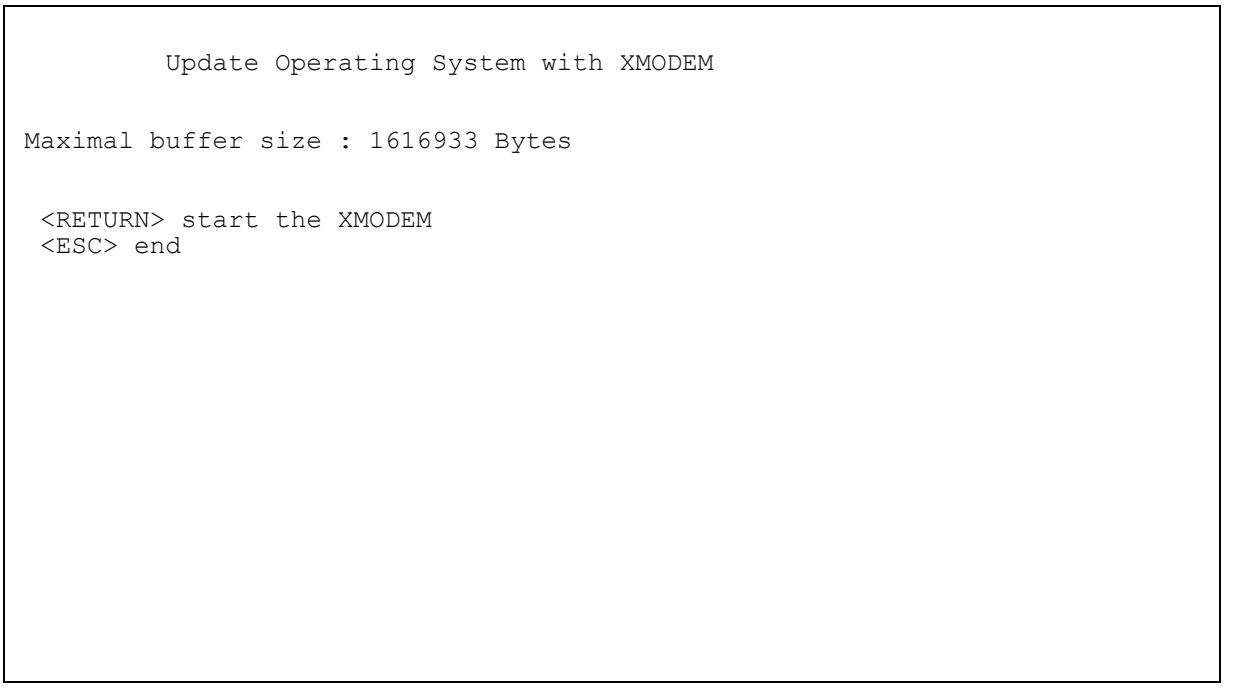


Abb. 26: Bildschirmansicht Update Betriebssystem

Um den Bildschirm zu verlassen und zum Hauptmenü des System-Monitor 2 zurückzukehren, drücken Sie <ESC>.

Drücken Sie <RETURN>, um den Update mit XMODEM zu starten. Es erscheint folgendes Bildschirmfenster:

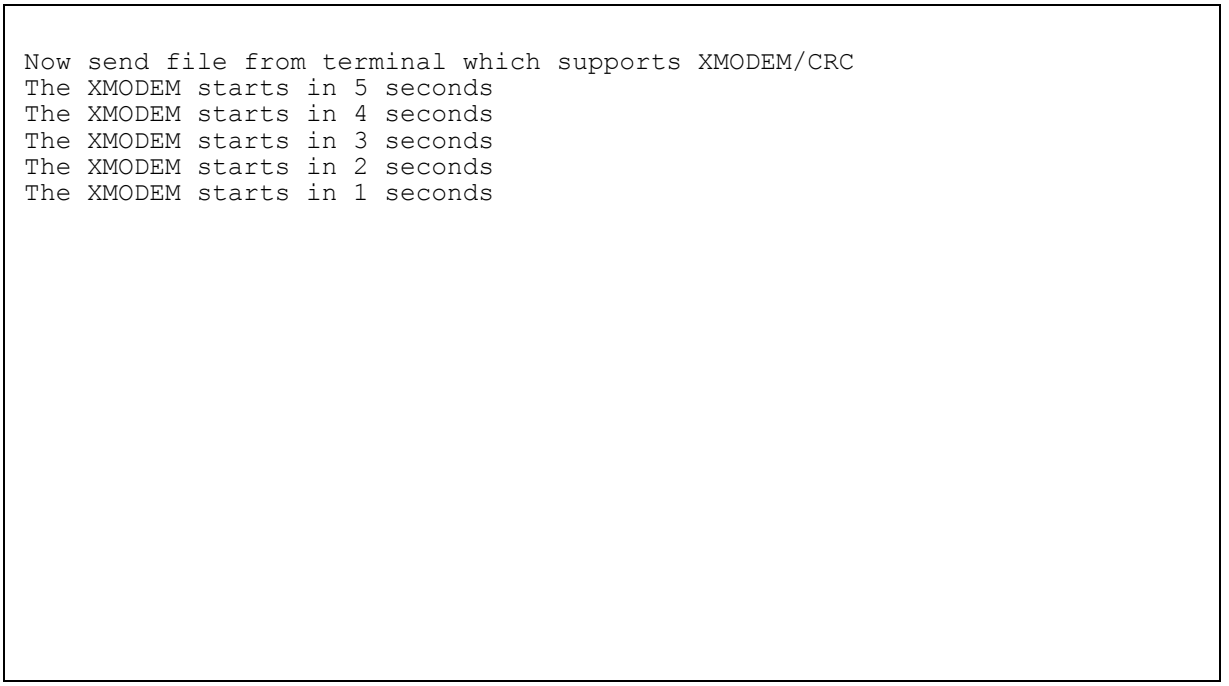


Abb. 27: Bildschirmansicht beim Start des Betriebssystem-Updates

Geben Sie anschließend den Pfad ein, in dem sich das aufzuspielende Betriebssystem befindet. Die Pfadeingabe erfolgt über das Terminalprogramm, z. B. unter Übertragung:Binärdatei. Die Übertragung beginnt. Nach dem Ende der Übertragung wird das Betriebssystem neu gestartet.

2 Software Update tftp

Dieser Menüpunkt führt ein Update des Betriebssystems im Flash-Speicher des RS2-../.. durch. Das Update erfolgt über tftp.

3 Cancel Automatic Update

Dieser Menüpunkt beendet ein gestartetes automatische Software Update.

4 Change Baudrate

Mit diesem Menüpunkt können Sie die Baudrate modifizieren.

5 Set Factory Setting

Mit diesem Menüpunkt setzten Sie die Einstellungen des Gerätes in den Auslieferungszustand zurück.

6 Reset

Das Gerät führt einen Reset durch.

7 End/Quit

Mit diesem Menüpunkt beenden Sie den System-Monitor 2.
Die Management-Software wird gestartet.

4 Funktionen

Die Geräte der Industrial ETHERNET Rail Switch RS2-../.. Familie enthalten eine Vielfalt von Funktionen:

- Anzeigen
- Hardware-Funktionen
- Frame-Switching
- Multicast
- Spanning Tree Algorithmus
- VLAN
- Redundanz
- Zeitsynchronisation
- Topologie-Erkennung
- Management
- SNMP-Traps

Zur Bedienung dieser Funktionen stehen drei Werkzeuge zur Verfügung:

- User Interface (im Lieferumfang des RS2-../.. enthalten)
  zur Einstellung elementarer Funktionen (siehe “User Interface” auf Seite 273).
- Web-based Management (im Lieferumfang des RS2-../.. enthalten)
  zur komfortablen Konfiguration des Agenten (siehe “Web-based Management” auf Seite 143).
- Netzmanagement HiVision
  zur komfortablen agentenübergreifenden Konfiguration.

4.1 Anzeigen

4.1.1 Gerätestatus

Diese LEDs geben Auskunft über Zustände, die Auswirkung auf die Funktion des gesamten RS2-../.. haben.

P1 - Power 1 (Grüne LED)

Anzeige	Bedeutung
leuchtet	Versorgungsspannung 1 liegt an
leuchtet nicht	Versorgungsspannung 1 ist ist kleiner 18 V

P2 - Power 2 (Grüne LED)

Anzeige	Bedeutung
leuchtet	Versorgungsspannung 2 liegt an
leuchtet nicht	Versorgungsspannung 2 ist ist kleiner 18 V

RM - Redundanz Manager (Grün/gelbe LED)

Anzeige	Bedeutung
leuchtet grün	RM-Funktion aktiv, redundanter Port nicht aktiv
leuchtet gelb	RM-Funktion aktiv, redundanter Port aktiv
leuchtet nicht	RM-Funktion nicht aktiv
blinkt grün	Fehlkonfiguration des HIPER-Rings (z.B. Ring nicht an Ringport angeschlossen.
blinkt gemeinsam mit STAND-BY	Speicheroperation in Zusammenhang mit dem AutoConfiguration Adapter ACA

FAULT - Fehler (Rote LED)

Anzeige	Bedeutung
leuchtet	Der Meldekontakt ist offen, d.h. er meldet einen Fehler.
leuchtet nicht	Der Meldekontakt ist geschlossen, d.h. er meldet keinen Fehler.

Ist beim Meldekontakt die “Manuelle Einstellung” auf Seite 163 aktiv, dann ist die Fehleranzeige unabhängig von der Stellung des Meldekontakts.

STAND-BY - (Grüne LED)

Anzeige	Bedeutung
leuchtet	Die Stand-by-Funktion ist eingeschaltet.
leuchtet nicht	Die Stand-by-Funktion ist ausgeschaltet.
blinkt	Speicheroperation in Zusammenhang mit dem AutoConfiguration Adapter ACA.

AutoConfiguration Adapter ACA

Die beiden LEDs STAND-BY und RM zeigen Speicheroperationen des ACA an.

Anzeige	Bedeutung
blinken alternativ:	Fehler bei der Speicheroperation.
LEDs blinken synchron; 2 mal pro Sekunde	Laden der Konfiguration vom ACA.
LEDs blinken synchron; 1 mal pro Sekunde	Speichern der Konfiguration in den ACA.

4.1.2 Portstatus

Diese LEDs zeigen portbezogene Informationen an.

1 bis 7 - Daten, Linkstatus (grün/gelbe LED)

Anzeige	Bedeutung
leuchtet nicht	keine gültige Verbindung
leuchtet grün	gültige Verbindung
blinkt grün (einmal pro Periode)	Port ist auf Stand-by geschaltet (Port 1)
blinkt grün (dreimal pro Periode)	Port ist ausgeschaltet
blitzt gelb	Datenempfang

4.2 Hardware-Funktionen

4.2.1 Diagnose

Beim Neustart führt der RS2-../.. einen Hardware-Selbsttest durch. Während des Betriebs überwacht ein integrierter Watchdog (Überwachungseinheit) die Funktion der Software.

4.2.2 Autonegotiation

Autonegotiation ist ein Verfahren, bei dem der Switch automatisch den Betriebsmodus seiner 10/100 RJ-45-Ports wählt. Beim ersten Verbindungsaufbau erkennt der Switch die Geschwindigkeit (10 oder 100 Mbit/s) und den Übertragungsmodus (halbduplex oder vollduplex) des verbundenen Netzes. Die automatische Einstellung der Ports macht manuelle Eingriffe durch den Anwender überflüssig. Die Aktivierung/Deaktivierung der Funktion Autonegotiation erfolgt über das Web-based Management, User Interface oder SNMP.

Hinweis: Ist nur bei einem der beiden Übertragungspartner die Autonegotiation-Funktion aktiv, dann erfolgt die Übertragung halbduplex. Die Übertragungsgeschwindigkeit gibt der Übertragungspartner ohne Autonegotiation vor.

4.2.3 Auto Polarity Exchange

Ist das Empfangsleitungspaar eines Twisted-Pair-Kabes falsch angeschlossen (RD+ und RD- vertauscht), dann erfolgt automatisch die Umkehrung der Polarität.

4.2.4 Autocrossing

Bei eingeschalteter Autonegotiation-Funktion erkennt der RS2-../.. das Sende- und Empfangsleitungspaar (MDI, MDI-X). Der RS2-../.. schaltet automatisch den Portausgang und -eingang auf die entsprechenden Leitungspaare. Somit spielt es keine Rolle, ob Sie zum Anschluß eines Gerätes ein gekreuztes (cross-over) oder ungekreuztes Kabel verwenden.

4.2.5 Leitungsüberwachung

- **Twisted Pair**
  Mit regelmäßigen Link-Test-Pulsen gemäß der Norm IEEE 802.3 10BASE-T/100BASE-TX überwacht der RS2-../.. die angeschlossenen TP-Leitungssegmente auf Kurzschluß oder Unterbrechung. Der RS2-../.. sendet keine Daten in ein TP-Segment, von dem es keinen Link-Test-Puls empfängt.

  Hinweis: Eine nicht belegte Schnittstelle wird als Leitungsunterbrechung bewertet. Ebenso wird die TP-Strecke zu einem ausgeschalteten Endgerät als Leitungsunterbrechung bewertet, da das stromlose, angeschlossene Gerät keine Link-Test-Pulse senden kann.

- **LWL**
  Gemäß der Norm IEEE 802.3 100BASE-FX überwacht ein RS2-../.. die angeschlossenen LWL-Leitungen auf Unterbrechung.

Beim Auftreten einer Leitungsunterbrechung sendet der Switch ein Trap an die Managementstation. Das Versenden dieses Traps kann durch das Management unterbunden werden.

4.2.6 Reset

Der RS2-../.. wird durch folgende Ereignisse zurückgesetzt:

- Management
- Unterschreiten beider Eingangsspannungsschwellen
- Watchdog

Nach einem Reset werden folgende Aktionen durchgeführt:

- Selbsttest
- Initialisierung

4.3 Frame-Switching

4.3.1 Store and Forward

Alle Daten, die ein RS2-../.. empfängt, werden gespeichert und auf ihre Gültigkeit geprüft. Ungültige und fehlerhafte Datenpakete (> 1.536 Byte oder CRC-Fehler) sowie Fragmente (< 64 Byte) werden verworfen. Gültige Datenpakete leitet ein RS2-../.. weiter.

4.3.2 Multiadress-Fähigkeit

Ein RS2-../.. lernt alle Quelladressen je Port. Nur Pakete mit
- unbekannten Adressen
- diesen Adressen oder
- einer Multi-/Broadcast-Adresse

im Zieladreßfeld werden an diesen Port gesendet.

Ein RS2-../.. kann bis zu 4000 Adressen lernen. Dies wird notwendig, wenn an einem oder mehreren Ports mehr als ein Endgerät angeschlossen ist. So können mehrere eigenständige Subnetze an ein RS2-../.. angeschlossen werden.

4.3.3 Adressen lernen

Ein RS2-../.. überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter (30 Sekunden, Aging Time) überschreiten, löscht der RS2-../.. aus seiner Adreßtabelle.
Datenpakete mit einer unbekannten Zieladresse flutet der RS2-../...
Datenpakete mit bekannter Zieladresse vermittelt der RS2-../.. gezielt.

Hinweis: Ein Neustart löscht die gelernten Adresseinträge.

4.3.4 Statische Adresseinträge

Zu den wichtigsten Funktionen eines Switch gehört unter anderen die Filterfunktion. Sie selektiert Datenpakete nach definierten Mustern, den Filtern. Diesen Mustern sind Vermittlungsvorschriften zugeordnet. Das heißt, ein Datenpaket, das ein Switch an einem Port empfängt, wird mit den Mustern verglichen. Besteht ein Muster, mit dem das Datenpaket übereinstimmt, dann sendet oder blockiert ein Switch dieses Datenpaket entsprechend den Vermittlungsvorschriften an den betroffenen Ports.

Als Filterkriterium können gelten:

- Zieladresse (Destination Address),
- Broadcast-Adresse,
- Gruppenadresse (Multicast).

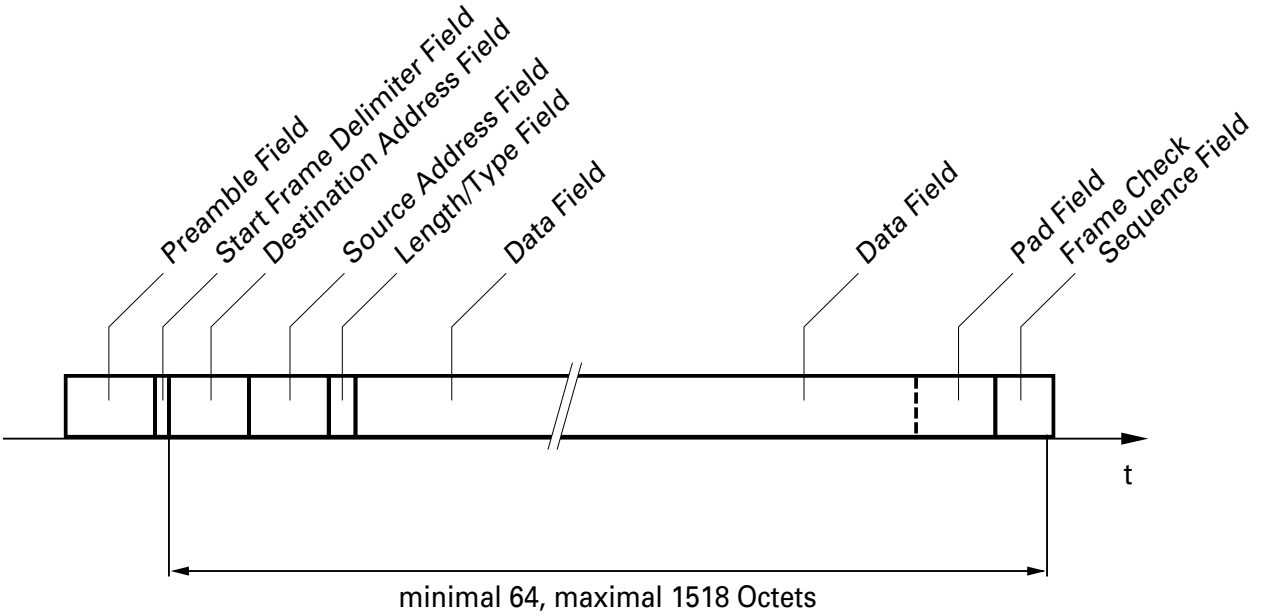


Abb. 28: Aufbau eines Ethernet-Datenpaketes

Zur Speicherung der einzelnen Filter dient die **Filtertabelle**. Sie ist unterteilt in drei Teile: einen statischen und zwei dynamische Teile. Der Management-Administrator beschreibt den statischen Teil der Filtertabelle (`dot1dStaticTable`). Ein Switch besitzt die Fähigkeit, während des Betriebes zu lernen, an welchem Port er Datenpakete mit welchen Quelladressen empfängt (siehe “Adressen lernen” auf Seite 94). Diese Information wird in einen dynamischen Teil (`dot1dTpFdbTable`) geschrieben. Von Nachbar-Agenten dynamisch gelernte und die per GMRP gelernte Adressen werden in den anderen dynamischen Teil geschrieben (siehe “Filtertabelle” auf Seite 186).
Adressen, die schon in der statischen Filtertabelle stehen, übernimmt ein Switch automatisch in den dynamischen Teil.
Eine statisch eingetragene Adresse kann nicht durch Lernen überschrieben werden.

4.3.5 Priorisierung

Der RS2-../.. unterstützt zwei Priority Queues (Traffic Classes nach IEEE 802.1D-1998). Die Zuordnung von empfangenen Datenpaketen zu diesen Klassen erfolgt durch die im VLAN-Tag enthaltene Priorität des Datenpaketes.

- Datenpakete mit dem Wert 0-3 im Prioritätsfeld werden mit niederer Priorität vermittelt.
- Datenpakete mit dem Wert 4-7 im Prioritätsfeld werden mit hoher Priorität vermittelt.
- Alle Datenpakete mit VLAN-Tag vermittelt der RS2-../.. entsprechend der eingetragenen Priorität.

Mit dieser Funktion wird verhindert, daß Datenverkehr höherer Priorität in Zeiten starker Verkehrslast durch anderen Verkehr gestört wird. Der Verkehr niedrigerer Priorität wird verworfen, wenn der Speicher oder Übertragungskanal überlastet ist.

Für die Handhabung der Prioritätsklassen bietet der RS2-../..:

- Strict Priority

Strict Priority
Bei Strict Priority vermittelt der RS2-../.. zuerst alle Datenpakete mit höherer Prioritätsstufe, bevor er ein Datenpaket mit der nächst niedrigeren Prioritätsstufe vermittelt. Ein Datenpaket mit der niedrigsten Prioritätsstufe vermittelt der RS2-../.. demnach erst, wenn keine anderen Datenpakete mehr in der Warteschlange stehen.

4.3.6 Tagging

Für die Funktionen VLAN und Priorisierung sieht der Standard IEEE 802.1 Q vor, daß in einen MAC-Datenrahmen das VLAN-Tag eingebunden wird. Das VLAN-Tag besteht aus 4 Bytes. Es steht zwischen dem Quelladreßfeld und dem Typfeld.

Der RS2-../.. wertet bei Datenpaketen mit VLAN-Tag
- die Prioritäts-Information immer und
- die VLAN-Information, wenn VLANs eingerichtet sind,

aus.

Datenpakete, deren VLAN-Tags eine Prioritäts-Information aber keine VLAN-Information (VLAN ID = 0) enthält, heißen „Priority Tagged Frames“.

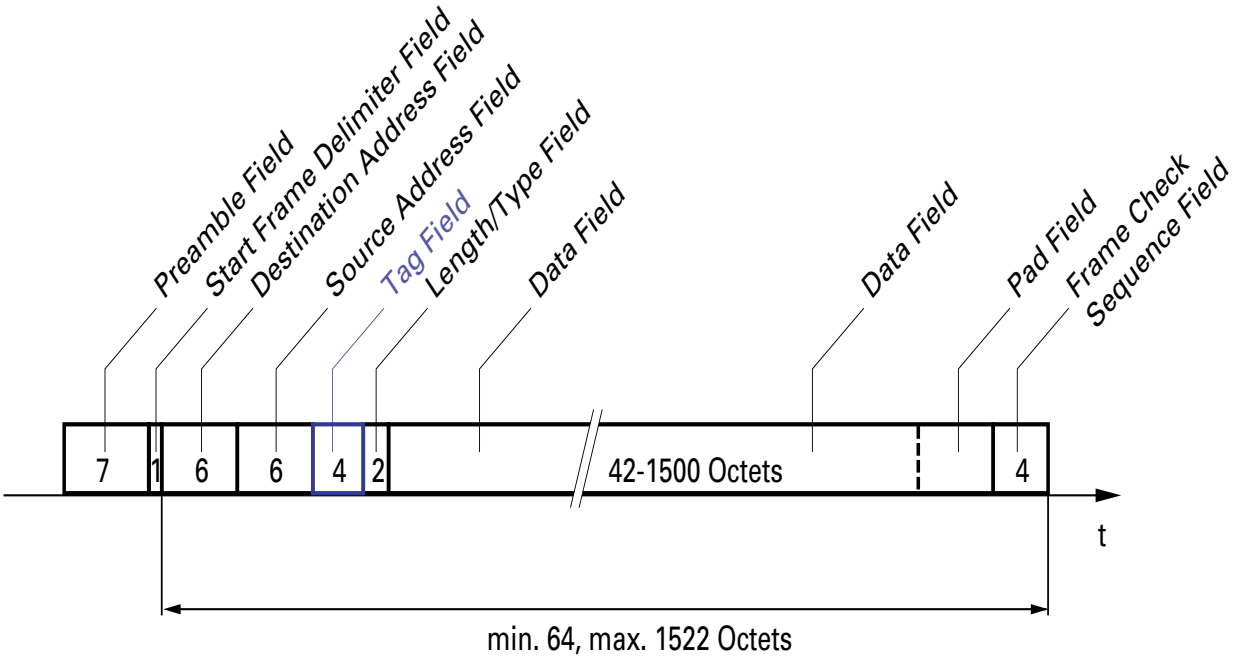


Abb. 29: Ethernet-Datenpaket mit Tag

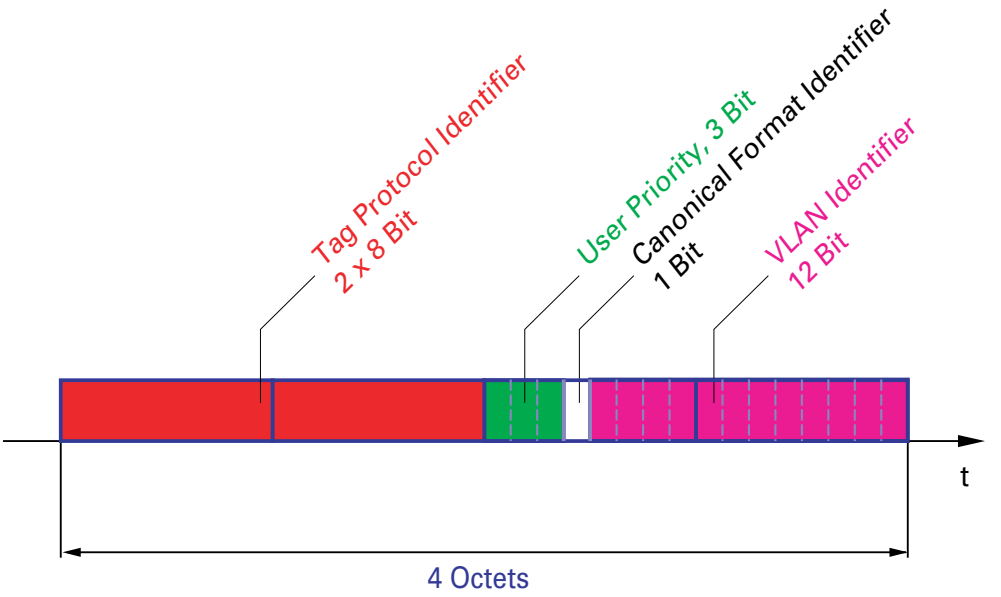


Abb. 30: Tag-Format

4.3.7 Flußkontrolle

Flußkontrolle ist ein Mechanismus, der als Überlastschutz für den Switch dient. Während verkehrsstarken Zeiten hält er zusätzlichen Verkehr vom Netz fern.

Im Beispiel (siehe Abb. 31) ist die Wirkungsweise der Flußkontrolle graphisch dargestellt. Die Workstations 1, 2 und 3 wollen zur gleichen Zeit viele Daten an die Workstation 4 übertragen. Die gemeinsame Bandbreite der Workstations 1, 2 und 3 zum Switch ist größer, als die Bandbreite von Workstation 4 zum Switch. So kommt es zum Überlaufen der Sende-Warteschlange von Port 4. Der linke Trichter symbolisiert diesen Zustand.

Wenn nun an den Ports 1, 2 und 3 des Switch die Funktion Flußkontrolle eingeschaltet ist, dann reagiert der Switch bevor der Trichter überläuft. Die Ports 1, 2 und 3 melden den angeschlossenen Geräten, daß im Moment keine Daten empfangen werden können.

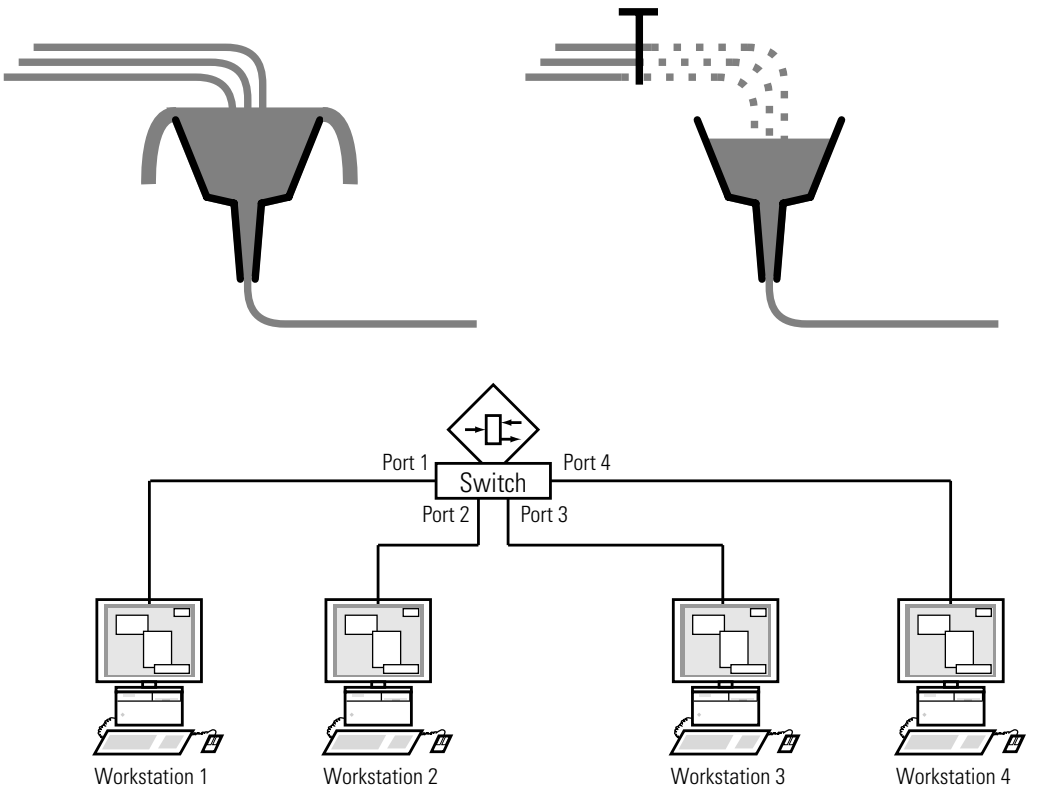


Abb. 31: Beispiel für Flußkontrolle

Flußkontrolle bei Vollduplex-Verbindung

Im Beispiel (siehe Abb. 31) sei zwischen der Workstation 2 und dem Switch eine Vollduplex-Verbindung.
Bevor die Sende-Warteschlange von Port 2 überläuft, sendet der Switch eine Aufforderung an Workstation 2, beim Senden eine kleine Pause einzulegen.

Flußkontrolle bei Halbduplex-Verbindung

Im Beispiel (siehe Abb. 31) sei zwischen der Workstation 2 und dem Switch eine Halbduplex-Verbindung.
Bevor die Sende-Warteschlange von Port 2 überläuft, sendet der Switch Daten zurück, damit die Workstation 2 eine Kollision erkennt und somit den Sendevorgang unterbricht.

4.3.8 Portmirroring (Portspiegelung)

Beim Portmirroring werden gültige Datenpakete eines Ports, dem Quellport, zu einem anderen Port, dem Zielport, kopiert. Der Datenverkehr am Quellport wird beim Portmirroring nicht beeinflußt (siehe “Einstellung des Portmirroring” auf Seite 218).
Ein am Zielport angeschlossenes Management-Werkzeug, wie z.B. ein RMON-Probe, kann so den Datenverkehr des Quellports beobachten.
Der Zielport leitet zu sendende Daten weiter und blockiert empfangene Daten.

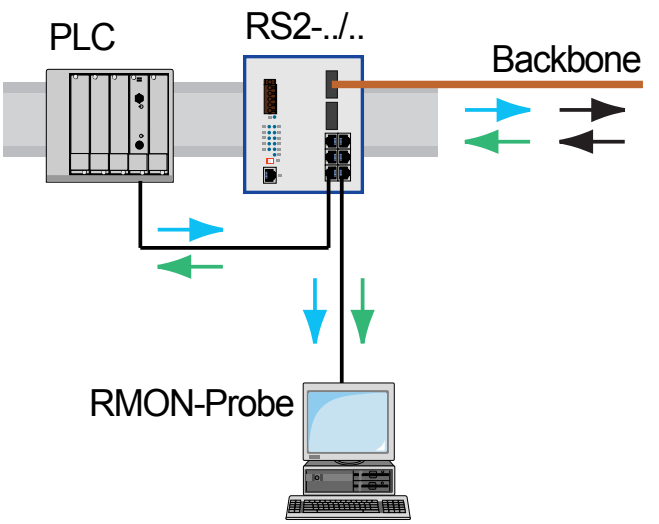


Abb. 32: Portmirroring

4.3.9 Broadcast Begrenzer

Um bei großer Broadcast-Belastung einen sicheren Datenaustausch zu gewährleisten, kann der Switch den Broadcast-Verkehr begrenzen.

Die Eingabe einer Zahl je Port legt fest, bis zu wieviele Broadcasts der Switch innerhalb einer Sekunde an diesem Port senden darf.

Werden an diesem Port mehr als die eingegebene maximale Anzahl von Broadcasts innerhalb einer Sekunde vermittelt, dann verwirft der Switch die folgenden Broadcasts an diesem Port.

Eine globale Einstellung aktiviert/deaktiviert die Broadcast-Begrenzer-Funktion an allen Ports.

4.4 Multicast-Anwendung

Die Datenverteilung im LAN unterscheidet drei Verteilungsklassen bezüglich der adressierten Empfänger:

- Unicast - ein Empfänger,
- Multicast - eine Gruppe von Empfängern,
- Broadcast - jeder erreichbare Empfänger.

Im Falle der Multicast-Adressierung leiten Switches alle Datenpakete mit einer Multicast-Adresse an allen Ports weiter. Dies führt zu einem erhöhten Bandbreitenbedarf.
Protokolle wie das GMRP und Verfahren wie IGMP-Snooping ermöglichen den Switches einen Informationsaustausch über die gezielte Vermittlung von Multicast-Datenpaketen. Das Vermitteln der Multicast-Datenpakete ausschließlich an den Ports, an denen Empfänger dieser Multicast-Datenpakete angeschlossenen sind, begrenzt den benötigten Bandbreitenbedarf.

IGMP-Multicast-Adressen erkennen Sie an dem Bereich, in dem eine Adresse liegt:

- MAC-Multicast-Adresse
  01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
- Klasse D IP-Multicast-Adresse
  224.0.0.0 - 239.255.255.255

Beispiel für eine Multicast-Anwendung

Die Kameras zur Maschinenüberwachung übertragen in der Regel ihre Bilder auf Monitore im Maschinenraum und in einen Überwachungsraum.
Bei einer IP-Übertragung sendet eine Kamera ihre Bilddaten mit einer Multicast-Adresse über das Netz.
Damit die vielen Bilddaten nicht unnötig das ganze Netz belasten, benutzt der RS2-../.. das GMRP zur Verteilung der Multicast-Adreß-Information. Dies hat zur Folge, daß die Bildaten mit einer Multicast-Adresse nur noch an jenen Ports vermittelt werden, an denen die zugehörigen Monitore zur Überwachung angeschlossen sind.

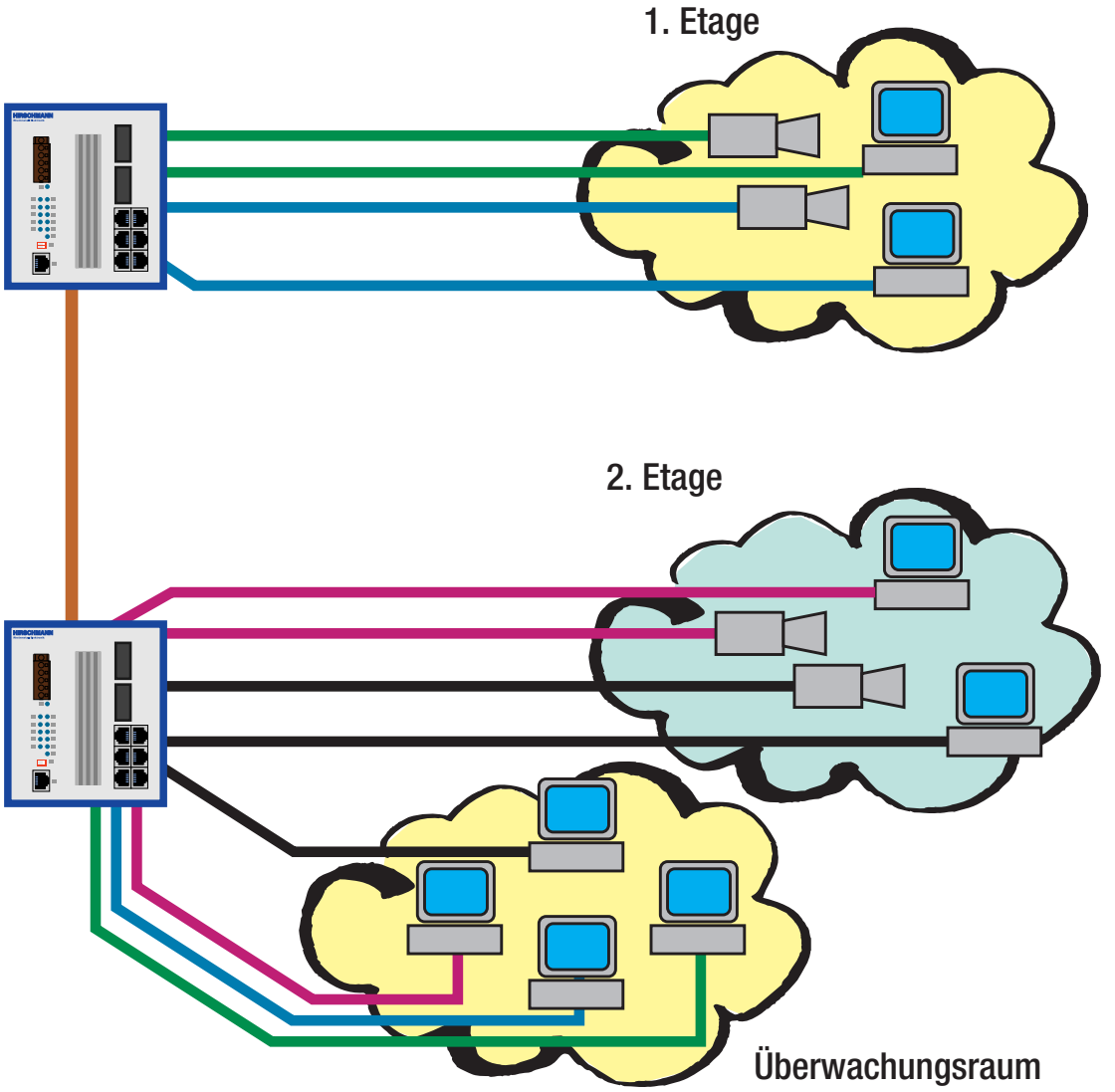


Abb. 33: Beispiel: Video-Überwachung in Maschinenräumen

4.4.1 GMRP

Das **G**ARP **M**ulticast **R**egistration **P**rotocol (GMRP) beschreibt die Verteilung von Multicast-Informationen zu anderen Switches auf Layer 2-Ebene. Dadurch können Switches Multicast-Adressen lernen. Beim Eintrag einer Multicast-Adresse in die statische Adreßtabelle, sendet der RS2-../.. diese Information an allen Ports. Angeschlossene Switches lernen dadurch, diese Muticast-Adresse an diesen RS2-../.. weiterzuleiten.

Hinweis: GMRP kann mit Hilfe des Web-based Interfaces (siehe “Multicast” auf Seite 188) oder des Netzmanagement HiVision (ab Release 5.1) aktiviert werden.
Hierzu wählen Sie in HiVison im Gerätefenster die Konfiguration des Agenten. Im Menü-Punkt `Switching Allgemein` ist die globale Einstellung für das GMRP.
Im Port-Fenster finden Sie unter `Konfiguration:GMRP` die Einstellung für diesen Port.

Im Lieferzustand ist GMRP bei allen Ports deaktiviert.

Geräte, die das GMRP nicht unterstützen, können durch einen statischen Filteradreß-Eintrag am Anschluß-Port in die Multicast-Adressierung mit eingebunden werden.

In einem Netz mit bis zu 20 RS2-../.. erfolgt innerhalb von 5 Sekunden (200 ms je Switch) der Aufbau des Multicast-Baums, nachdem die Multicast-Adresse zum ersten Mal an einem RS2-../..-Port eingetragen worden ist. Diese Zeit hängt ab von der eingestellten Join time (Voreinstellung 200 ms).

4.4.2 IGMP-Snooping

Das **IGMP I**nternet **G**roup **M**anagement **P**rotocol beschreibt die Verteilung von Multicast-Informationen zwischen Routern und Endgeräten auf Layer 3-Ebene.
Router mit aktiver IGMP-Funktion verschicken periodisch Anfragen (Query), um zu erfahren, welche IP-Multicast-Gruppen-Mitglieder im LAN angeschlossen sind. Multicast-Gruppen-Mitglieder antworten mit einer Report-Nachricht. Diese Report-Nachricht enthält alle für das IGMP notwendigen Parameter. Der Router trägt die IP-Multicast-Group-Adresse aus der Report-Nachricht in seine Routing-Tabelle ein. Dies bewirkt, daß er Frames mit dieser IP-Multicast-Group-Adresse im Zieladreßfeld ausschließlich gemäß der Routing-Tabelle vermittelt.
Geräte, die nicht mehr Mitglied einer Multicast-Gruppe sein wollen, melden sich mit einer Leave-Nachricht ab (ab IGMP Version 2) und versenden keine Report-Nachrichten mehr. Im IGMP Version 1 und 2 entfernt der Router den Routing-Tabelleneintrag, wenn er innerhalb einer bestimmten Zeit (Aging Time) keine Report-Nachricht empfängt.
Sind mehrere Router mit aktiver IGMP-Funktion im Netz, dann verhandeln diese bei IGMP Version 2 untereinander, welcher Router die Query-Funktion übernimmt. Ist kein Router im Netz, dann kann ein entsprechend ausgestatteter Switch die Query-Funktion übernehmen.

Ein Switch, der einen Multicast-Empfänger mit einem Router verbindet, kann mit Hilfe des IGMP-Snooping-Verfahrens die IGMP-Informationen auswerten.
IGMP-Snooping übersetzt IP-Multicast-Group-Adressen in MAC-Multicast-Adressen, so daß die IGMP-Funktion auch von Layer 2-Switches wahrgenommen werden können. Der Switch trägt die vom IGMP-Snooping aus den IP-Adressen gewonnenen MAC-Adressen der Multicast-Empfänger in die statische Adreßtabelle ein. Somit blockiert der Switch Multicast-Pakete an den Ports, an denen keine Multicast-Empfänger angeschlossen sind.

4.5 Spanning Tree Algorithmus

Lokale Netze werden immer größer. Dies gilt sowohl für die geographische Ausdehnung, als auch für die Anzahl der Netzteilnehmer. So ist es oft sinnvoll gleich mehrere Brücken einzusetzen, um z. B.:

- die Netzlast in Teilbereichen zu verringern,
- redundante Verbindungen aufzubauen und
- Entfernungseinschränkungen zu überwinden.

Der Einsatz mehrerer Brücken mit mehrfachen Verbindungen zwischen den Teilnetzen kann jedoch zu erheblichen Störungen, sogar zum Totalausfall des Netzes führen, wenn die Brücken falsch konfiguriert sind. Um dies zu verhindern, wurde der Spanning Tree Algorithmus entwickelt. Er ist im Standard IEEE 802.1D beschrieben.

Hinweis: Der Standard schreibt vor, daß alle Brücken innerhalb einer Vermaschung mit dem Spanning Tree Algorithmus arbeiten.

4.5.1 Aufgaben

Der Spanning Tree Algorithmus reduziert jegliche Topologie eines Netzes, das mit Brücken verbunden ist, auf eine einzige Baumstruktur. Die Wurzelbrücke bildet den Ursprung einer Baumstruktur. Eventuelle Ringstrukturen werden nach vorgegebenen Regeln aufgetrennt. Bei einer Pfadunterbrechung hebt der Algorithmus die Auftrennung zur Aufrechterhaltung des Datenverkehrs wieder auf. Dies erlaubt redundante Verbindungen zur Erhöhung der Datensicherheit.

Die Forderungen an den Algorithmus lauten:

- automatische Rekonfiguration der Baumstruktur bei Brückenfehler oder Unterbrechung eines Datenpfades,
- Stabilisierung der Baumstruktur bei jeglicher Netzgröße,
- Stabilisierung innerhalb einer kurzen bekannten Zeit,

- durch das Management vorbestimmbare und reproduzierter Topologie,
- Transparenz für die Endgeräte,
- geringe Netzlast gegenüber der verfügbaren Übertragungskapazität durch die Einrichtung der Baumstruktur.

4.5.2 Regeln für die Erstellung der Baumstruktur

Jede Brücke wird eindeutig durch Parameter beschrieben:

- Brückenidentifikation (Bridge Identifier),
- Wurzelpfadkosten,
- Portidentifikation (Port Identifier).

Brückenidentifikation

Die Brückenidentifikation besteht aus acht Byte. Die 48bit MAC-Adresse der Brücke stellt die sechs niederwertigen Bytes dar. Sie garantiert, daß jede Brücke eine andere Identifikation besitzt. Der höherwertigere Teil der Brückenidentifikation besteht aus der Prioritätszahl, die der Management-Administrator zur Konfiguration eines Netzes verändern kann. Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation besitzt die höchste Priorität.

Die MAC-Adresse und die Prioritätszahl sind in der Management Information Base (siehe “dot1dBridge (1.3.6.1.2.1.17)” auf Seite 243) abgelegt:
– `dot1dBaseBridgeAddress` (1.3.6.1.2.1.17.1.1.0)
– `dot1dStpPriority` (1.3.6.1.2.1.17.2.2.0)

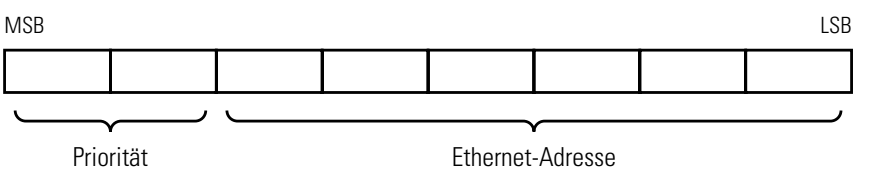


Abb. 34: Brückenidentifikation

Wurzelpfadkosten

Jedem Pfad, der zwei Brücken miteinander verbindet, sind Kosten für die Übertragung zugeordnet. Der Management-Administrator legt diesen Wert fest und gibt ihn bei der Konfiguration einer Brücke für jeden Pfad an (siehe Tab. 6 auf Seite 116).

Da der Management-Administrator diesen Wert letztendlich frei wählen kann, verfügt er hiermit über ein Werkzeug, bei redundanten Pfaden einem bestimmten Pfad den Vorzug zu geben.

Die Wurzelpfadkosten ist die Summe aller Einzelpfadkosten der Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Brücke und der Wurzelbrücke passiert.

Die Wurzelpfadkosten und die Einzelpfadkosten sind in der Management Information Base (siehe “dot1dBridge (1.3.6.1.2.1.17)” auf Seite 243) abgelegt:

– `dot1dStpRootCost` (1.3.6.1.2.1.17.2.6.0)
– `dot1dStpPortPathCost` (1.3.6.1.2.1.17.2.15.1.5.Index)

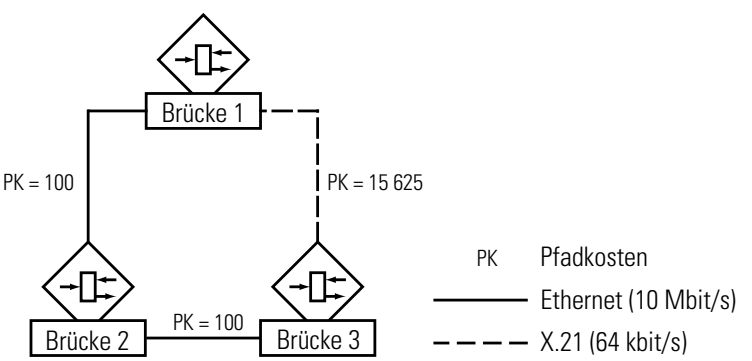


Abb. 35: Pfadkosten

Portidentifikation

Die Portidentifikation besteht aus zwei Teilen zu je acht Bit. Ein Teil, das niederwertigere Byte, gibt die feste Beziehung zur physikalischen Portnummer wieder. Dieser Teil gewährleistet, daß kein Port einer Brücke die gleiche Bezeichnung wie ein anderer Port dieser Brücke trägt. Der zweite Teil ist die Portprioritätszahl, die der Management-Administrator festlegt. Auch hier gilt: der Port mit dem kleinsten Zahlenwert für die Portidentifikation besitzt die höchste Priorität.

Die Portnummer und die Portprioritätszahl sind in der Management Information Base (siehe “dot1dBridge (1.3.6.1.2.1.17)” auf Seite 243) abgelegt:
– `dot1dStpPort` (1.3.6.1.2.1.17.2.15.1.1.Index)
– `dot1dStpPortPriority` (1.3.6.1.2.1.17.2.15.1.2.Index)

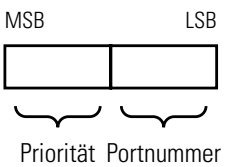


Abb. 36: Portidentifikation

Zur Berechnung der Baumstruktur benötigen die Brücken nähere Informationen über die anderen Brücken, die sich im Netz befinden. Um diese Informationen zu erhalten, sendet jede Brücke eine BPDU (Bridge Protocol Data Unit) an andere Brücken.

Bestandteil einer BPDU ist unter anderem die

- Brückenidentifikation,
- Wurzelpfadkosten und
- Portidentifikation

(siehe IEEE 802.1D).

- Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation wird zur Wurzelbrücke (Root Bridge). Sie ist die Wurzel der Baumstruktur.
- Der Aufbau des Baumes hängt von den Wurzelpfadkosten ab. Die Struktur wird so gewählt, daß die minimalen Pfadkosten zwischen jeder einzelnen Brücke zur Wurzelbrücke entstehen.

- Bei mehreren Pfaden mit gleichen Wurzelpfadkosten entscheidet die Priorität der Brückenidentifikation der Brücken, die an einen dieser Pfade angeschlossen ist, welche Brücke blockiert.
- Wenn von einer Brücke zwei Pfade mit den gleichen Wurzelpfadkosten wegführen, wird als letztes Kriterium die Portidentifikation herangezogen (siehe Abb. 36). Sie entscheidet, welcher Port gewählt wird.

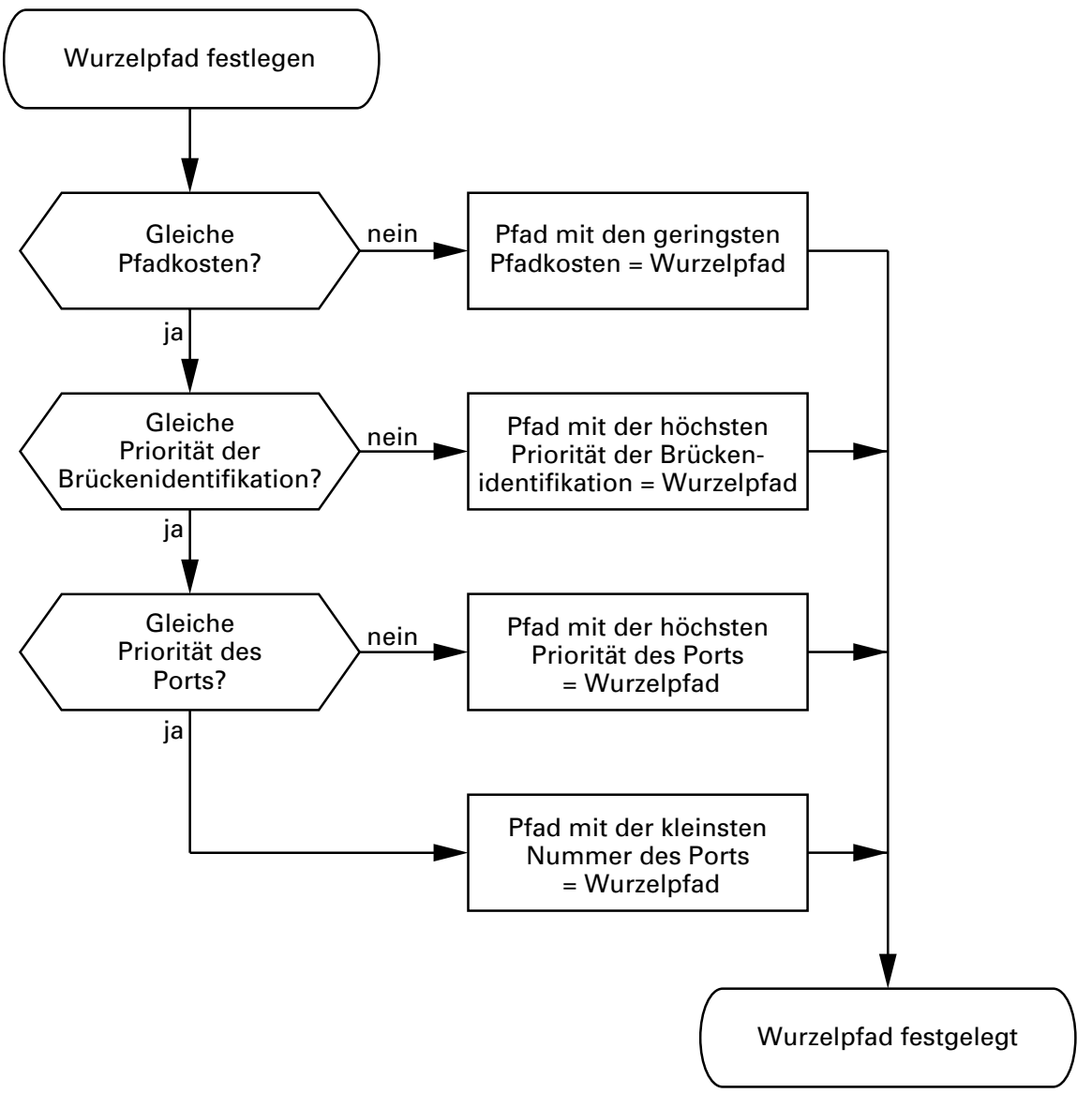


Abb. 37: Flußdiagramm Wurzelpfad festlegen

Anhand des Netzplanes (siehe Abb. 38) kann man das Flußdiagramm (siehe Abb. 37) zur Festlegung des Wurzelpfades (Root Path) nachvollziehen. Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation wird zur Wurzelbrücke, in diesem Fall die Brücke 1. Im Beispiel belasten alle Teilpfade die gleichen Pfadkosten. Der Pfad zwischen Brücke 2 und Brücke 3 wird unterbrochen, da eine Verbindung von Brücke 3 über Brücke 2 zur Wurzelbrücke die doppelten Pfadkosten verursachen würden.

Interessant ist der Pfad von der Brücke 6 zur Wurzelbrücke:

- Der Pfad über Brücke 5 und Brücke 3 verursacht die gleichen Wurzelpfadkosten wie der Pfad über Brücke 4 und Brücke 2.
- Gewählt wird der Pfad über Brücke 4, da der Zahlenwert 40 für die Brükkenidentifikation kleiner ist als der Zahlenwert 50.
- Zwischen Brücke 6 und Brücke 4 gibt es aber zwei Pfade. Hier entscheidet die höhere Portpriorität.

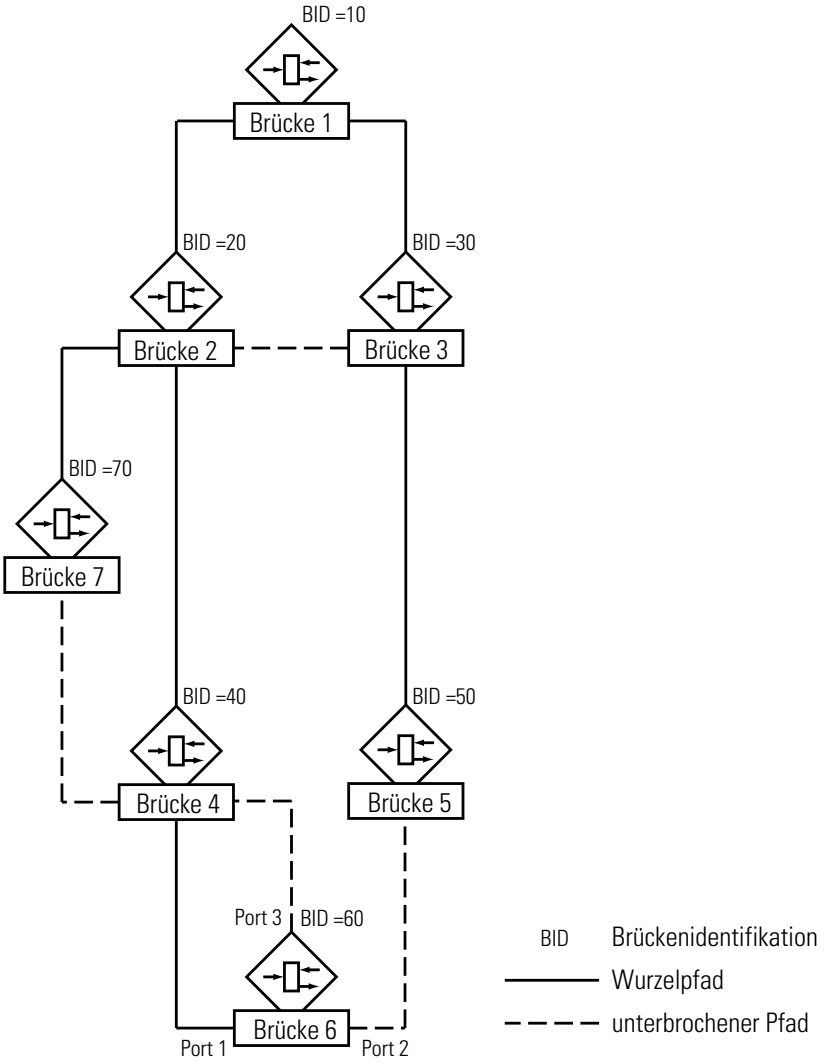


Abb. 38: Beispiel Wurzelpfad festlegen

4.5.3 Beispiel zur Manipulation der Baumstruktur.

Der Management-Administrator des Netzes (siehe Abb. 38) stellt bald fest, daß diese Konfiguration mit Brücke 1 als Wurzelbrücke ungünstig ist. Auf den Pfaden zwischen Brücke 1 zu Brücke 2 und Brücke 1 zu Brücke 3 summieren sich die Kontrollpakete, die die Wurzelbrücke zu allen anderen Brücken sendet.
Erhebt der Management-Administrator die Brücke 2 zur Wurzelbrücke, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Hieraus entsteht die (siehe Abb. 38) dargestellte Konfiguration. Die Wege zwischen den einzelnen Brücken zur Wurzelbrücke sind kürzer geworden.

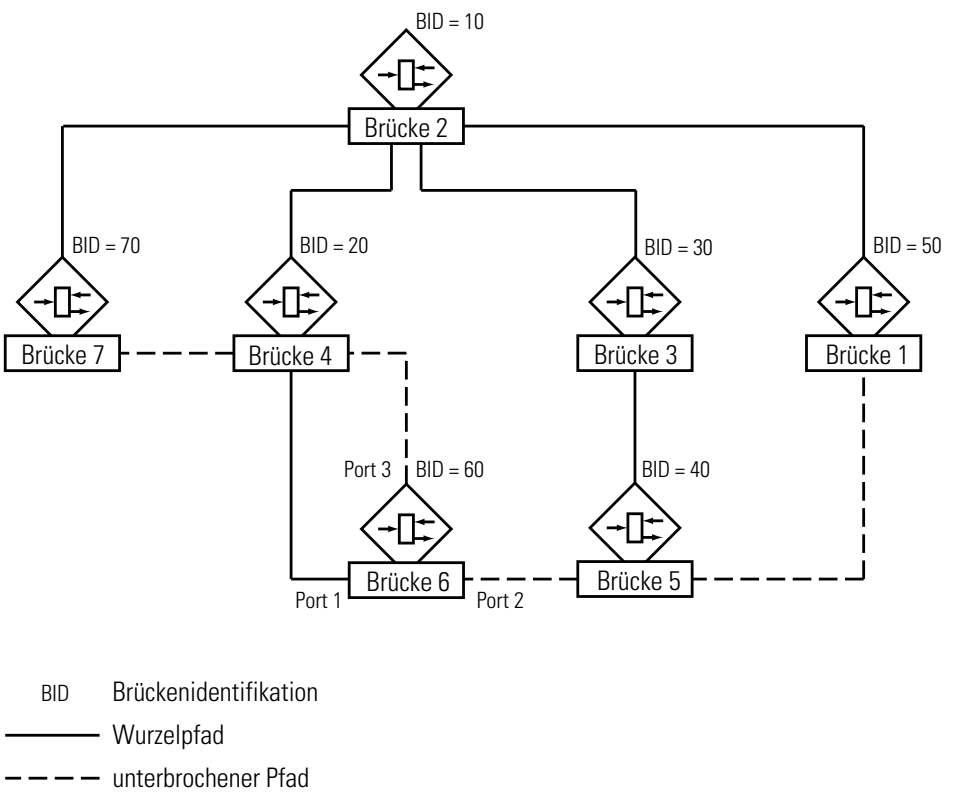


Abb. 39: Beispiel Wurzelpfad manipulieren

4.5.4 Rapid Spanning Tree Protocol

Das exponentielle Ansteigen der Nutzung von LANs auch in zeitkritischen Anwendungen stellt laufend neue Herausforderungen an die Verfügbarkeit des Netzes. Umschaltzeiten im hohen Sekundenbereich zur Rekonfiguration des Netzes beim Ausfall einer Teilkomponente sind nicht weiter tolerierbar. So war die Überarbeitung des in unsererer schnelllebigen Zeit schon als legendär zu bezeichnenden Spanning Tree Protokolls unumgänglich.
Die Verbesserung von mehreren Sekunden zu kleiner 1 Sekunde im Vergleich zu sonstigen Veränderungen unserer Zeit stellt eher eine Weiterentwicklung als eine Revolution dar.
Diese Weiterentwicklung wurde im Juni 2001 unter IEEE 802.1w zur Ergänzung der bestehenden Norm IEEE 802.1D mit der Bezeichnung Rapid Spanning Tree Algorithm and Protocol (RSTP) verabschiedet.

RSTP ist kompatibel zum herkömmlichen STP. Beim gleichzeitigen Einsatz beider Protokolle gehen jedoch die Vorteile der schnelleren Rekonfiguration beim RSTP verloren.

RSTP behält die Berechnung der Baumstruktur unverändert bei. RSTP ändert lediglich Parameter, fügt neue Parameter und Mechanismen hinzu, die die Rekonfiguration im Fehlerfall beschleunigen. Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

Port-Rollen

RSTP weist jedem Brückenport eine der folgenden Rollen zu:

- Wurzelport (Root-Port),
  der Port, an dem eine Brücke Datenpakete mit den niedrigsten Pfadkosten von der Wurzelbrücke empfängt.
  Existieren mehrere solche Ports, dann entscheidet die Brückenidentifikation, welcher Port Wurzelport ist.
  Existieren auch mehrere solche Ports, dann entscheidet die Portidentifikation, welcher Port Wurzelport ist (siehe Abb. 37).
  Die Wurzelbrücke selbst besitzt keinen Wurzelport.

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
<=100 KBit/s	200 000 000*	20 000 000-200 000 000	1-200 000 000
1 MBit/s	20 000 000*	2 000 000-200 000 000	1-200 000 000
10 MBit/s	2 000 000*	200 000-20 000 000	1-200 000 000
100 MBit/s	200 000*	20 000-2 000 000	1-200 000 000
1 GBit/s	20 000	2 000-200 000	1-200 000 000
10 GBit/s	2 000	200-20 000	1-200 000 000
100 GBit/s	200	20-2 000	1-200 000 000
1 TBit/s	20	2-200	1-200 000 000
10 TBit/s	2	1-20	1-200 000 000

Tab. 6: Empfohlene Pfadkosten in Abhängigkeit von der Datenrate
(siehe "Wurzelpfadkosten" auf Seite 109)
** IEEE 802.1D, 1998 Edition, konforme Brücken, die nur 16 Bit-Werte für die Pfadkosten unterstützen, sollten als Pfadkosten den Wert 65 535 anwenden, wenn Sie im Zusammenhang mit Brücken benutzt werden, die 32 Bit-Werte für die Pfadkosten unterstützen.*

- Designierter Port (Designated Port),
  der Port, der die designierte Brücke (Designated Bridge) mit einem Netzsegment verbindet, das von der Wurzelbrücke wegführt.

  Jedes Netzsegment, in dem sich keine weitere RSTP-Brücke befindet, ist mit genau einem designierten Port verbunden. Dieser designierte Port ist dann gleichzeitig ein Randport (Edge Port). Kennzeichen eines Randports ist die Tatsache, daß er keine RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Unit) empfängt.

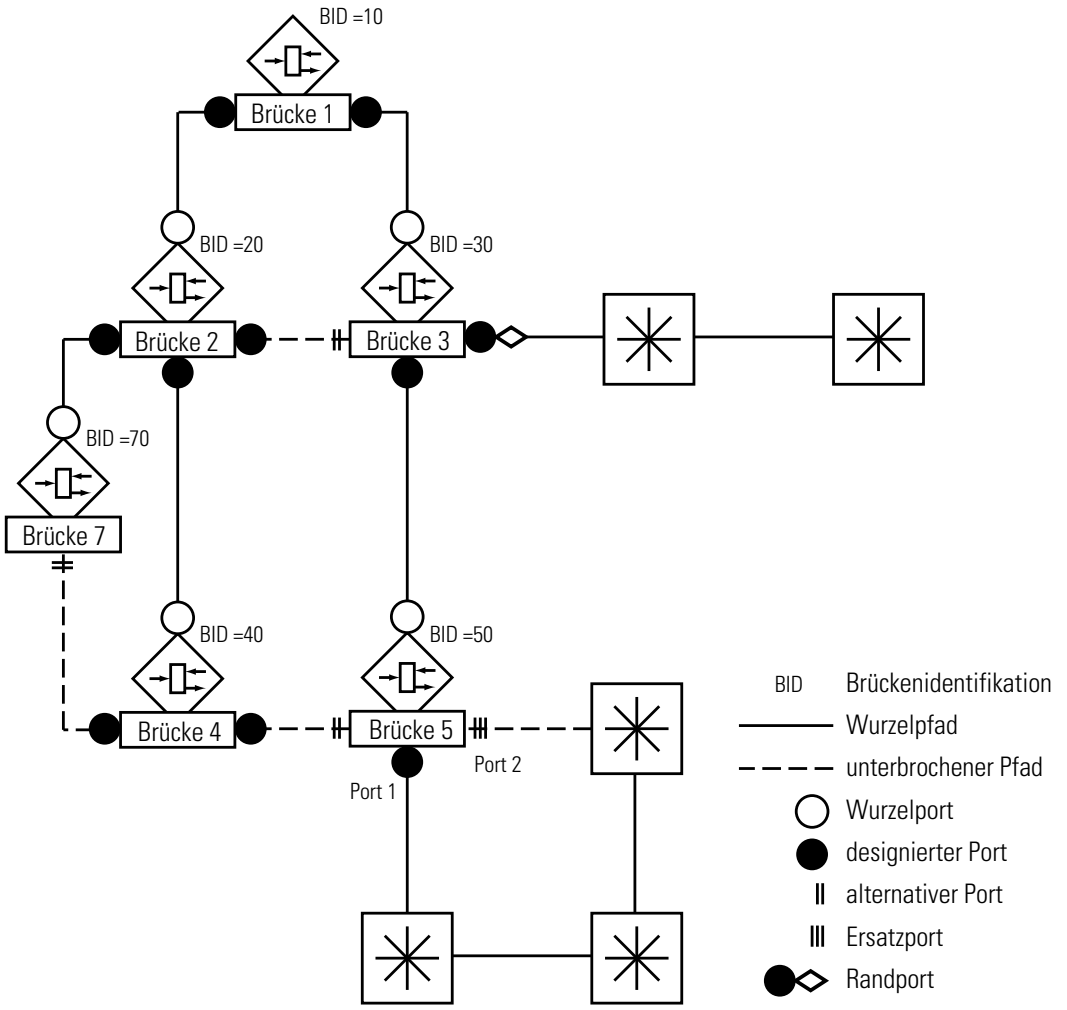


Abb. 40: Port-Rollen-Zuordnung

- Alternativer Port (Alternate port)
  der Port, der beim Ausfall der Verbindung zur Wurzelbrücke die Aufgabe des Wurzelports übernimmt. Der alternative Port stellt die Verbindung der Brücke zur Wurzelbrücke hin sicher.
- Ersatzport (Backup port)
  ein Port, der als Ersatz zur Verfügung steht, falls die Verbindung zum designierten Port dieses Netzsegmentes (ohne RSTP-Brücke) ausfällt. Der Ersatzport führt zu den Zweigen des Spanning Tree.
- Disabled-Port,
  Port, der innerhalb der Spanning Tree Operation keine Rolle spielt, also abgeschaltet ist, oder keine Verbindung hat.

Port-Stati

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topology (Port Rolle)
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)

Tab. 7: Beziehung zwischen Port-Status-Werten im STP und RSTP
** Die dot1d-MIB zeigt "Disabled" an.*

Spanning Tree Priority Vector

Um Ports Rollen zuzuteilen, tauschen die RSTP-Brücken Konfigurationsinformationen untereinander aus. Diese Informationen heißen "Spanning Tree Priority Vector". Sie sind Teil der RST BPDUs und enthalten folgende Informationen:

- Brückenidentifikation der Wurzelbrücke
- Wurzelpfadkosten der sendenden Brücke
- Brückenidentifikation der sendenden Brücke
- Portidentifikation des Ports, durch welchen die Nachricht gesendet wurde
- Portidentifikation des Ports, durch welchen die Nachricht empfangen wurde

Auf Basis dieser Informationen sind die am RSTP beteiligten Brücken in der Lage, selbst Port-Rollen berechnen zu können und den Portstatus der eigenen Ports zu definieren.

Schnelle Rekonfiguration

Warum kann RSTP schneller auf eine Unterbrechung des Wurzelpfades reagieren?

- Einführung von Randports
  Bei einer Rekonfiguration schaltet RSTP einen Randport sofort nach Ablauf von drei Sekunden in den Vermittlungsmodus. RSTP wartet "Hello Time" (siehe Tab. 13 auf Seite 193) ab, um sicher zu sein, daß keine BPDU sendende Brücke angeschlossen ist.
  Wenn der Anwender sicher ist, daß an diesem Port ein Endgerät angeschlossen ist und bleibt, dann kann er an diesem Port STP ausschalten. Dann entstehen im Rekonfigurationsfall an diesem Port keine Wartezeiten.
- Einführung von alternativen Ports
  Da schon im regulären Betrieb die Portrollen verteilt sind, kann eine Brücke sofort nach dem Verlust der Verbindung zur Wurzelbrücke vom Wurzel- zum alternativen Port umschalten.
- Kommunikation mit Nachbarbrücken (Punkt-zu-Punkt-Verbindungen)
  Die dezentrale, direkte Kommunikation zwischen benachbarten Brükken erlaubt eine unverzögerte Reaktion auf Zustandsänderungen der Spanning Tree Architektur.
- Filtertabelle
  Beim STP bestimmt das Alter der Einträge in der Filtertabelle über die Aktualisierung. Das RSTP löscht sofort und gezielt die Einträge der Ports, die von einer Umkonfiguration betroffen sind.
- Reaktion auf Ereignis
  Ohne Zeitvorgaben einhalten zu müssen, reagiert RSTP sofort auf Ereignisse wie Verbindungsunterbrechung, Verbindung vorhanden, u.a.

Hinweis: Der Preis für diese schnelle Rekonfiguration ist das Risiko, daß es während der Rekonfigurationsphase zur Duplizierung und zum Vertauschen von Datenpaketen kommen kann. Wenn Sie dies in Ihrer Anwendung nicht akzeptieren können, dann schalten Sie auf das langsamere Spanning Tree Protokoll um oder wählen Sie eines der anderen in diesem Buch beschriebenen, schnelleren Redundanzverfahren.

4.6 VLAN

Ein virtuelles LAN (VLAN) besteht aus einer Gruppe von Netzteilnehmern in einem oder mehreren Netzsegmenten, die so miteinander kommunizieren können, als gehörten sie demselben LAN an.

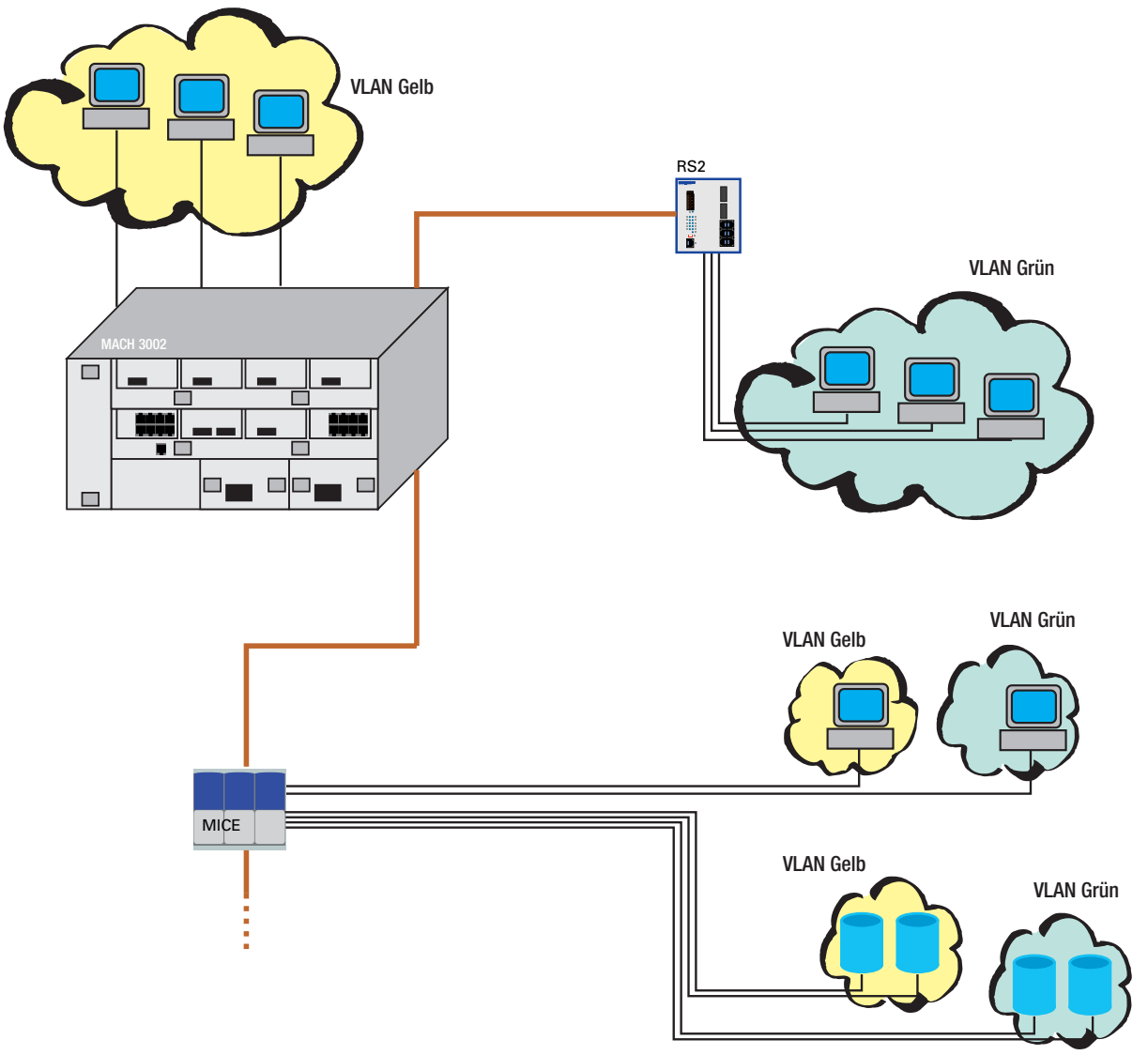


Abb. 41: Beispiel für VLAN

VLANs basieren auf logischen (statt physikalischen) Verbindungen und sind flexible Elemente der Netzgestaltung. Der wichtigste Vorteil der VLANs ist die Möglichkeit, daß man mit ihnen Anwender-Arbeitsgruppen bilden kann, die auf der Funktion der Teilnehmer basieren und nicht auf ihrem physikalischen Standort oder Medium.
Da Broad/Multicast-Datenpakete ausschließlich innerhalb eines virtuellen LANs vermittelt werden, bleibt das verbleibende Datennetz davon unbelastet.

Die VLAN-Funktion ist in der Norm IEEE 802.1Q definiert. Die maximale Anzahl von VLANs ist durch den Aufbau des VLAN-Tags (siehe Abb. 30) auf 4094 begrenzt.

Schlagworte, die oft im Zusammenhang mit VLANs benutzt werden sind:

- **Ingress Rule**
  Die Ingress Rules (= Eingangsregeln) legen fest, wie eingehende Daten vom Switch behandelt werden.

- **Egress Rule**
  Die Egress Rules (= Ausgangsregeln) legen fest, wie die ausgehenden Daten vom Switch behandelt werden.

- **VLAN Identifier**
  Die Zuordnung zu einem VLAN geschieht über eine VLAN Identifikation. Jedes in einem Netz existierende VLAN wird durch eine Identifikation gekennzeichnet. Diese Kennzeichnung muß eindeutig sein, d.h. jede Identifikation darf in einem Netz nur ein einziges Mal vergeben werden.

Port VLAN Identifier (PVID)

Das Management vergibt für jeden Port eine VLAN Identifikation. Deshalb heißt diese Identifikation Port VLAN Identifier.
Der Switch fügt beim Empfang jedem Datenpaket, das keinen Tag enthält, ein Tag ein. Dieses Tag enthält einen gültigen VLAN Identifier.
Beim Empfang eines Datenpaketes mit einen Prioritäts-Tag fügt der Switch den PortVLAN Identifier ein.

Member Set

Das Member Set ist eine Aufzählung der Ports, die zu einem VLAN gehören. Jedes VLAN besitzt ein Member Set.

Untagged Set

Das Untagged Set ist eine Aufzählung der Ports eines VLANs, die Datenpakete ohne Tag versenden. Jedes VLAN besitzt ein Untagged Set.

4.7 Redundanz

4.7.1 Linienstruktur

Die RS2-../.. ermöglichen den Aufbau von Backbones in Linienstrukturen. Die Kaskadierung erfolgt über die HIPER-Ring-Ports.

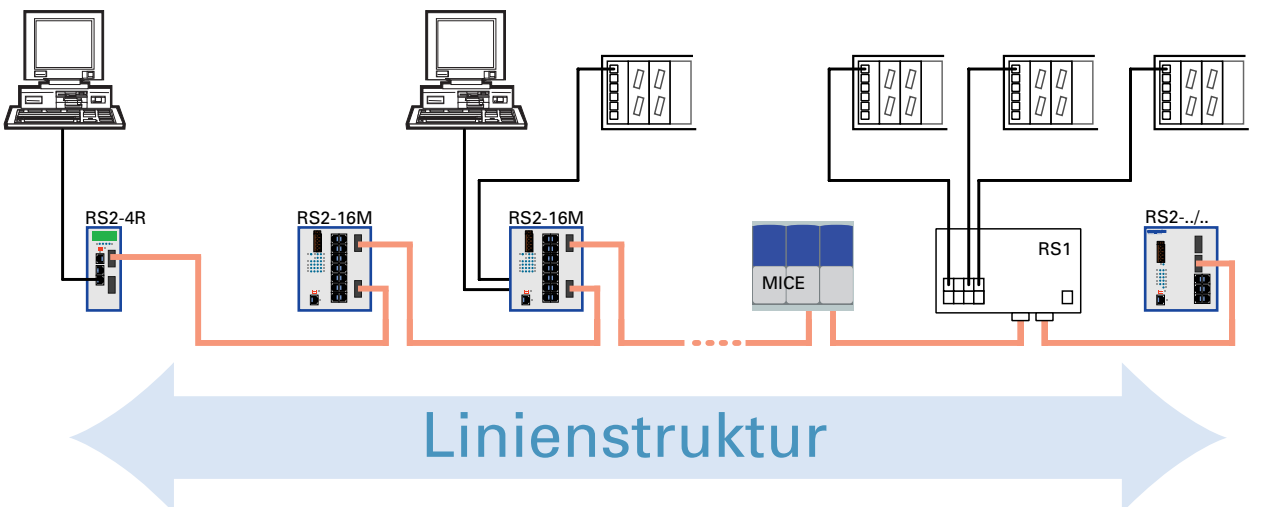


Abb. 42: Linienstruktur

4.7.2 Redundante Ringstruktur – HIPER-Ring

Mit Hilfe der RM-Funktion (**R**edundanz **M**anager) des RS2-../.. können die beiden Enden eines Backbones in Linienstruktur zu einem redundanten Ring, dem HIPER-Ring, geschlossen werden.

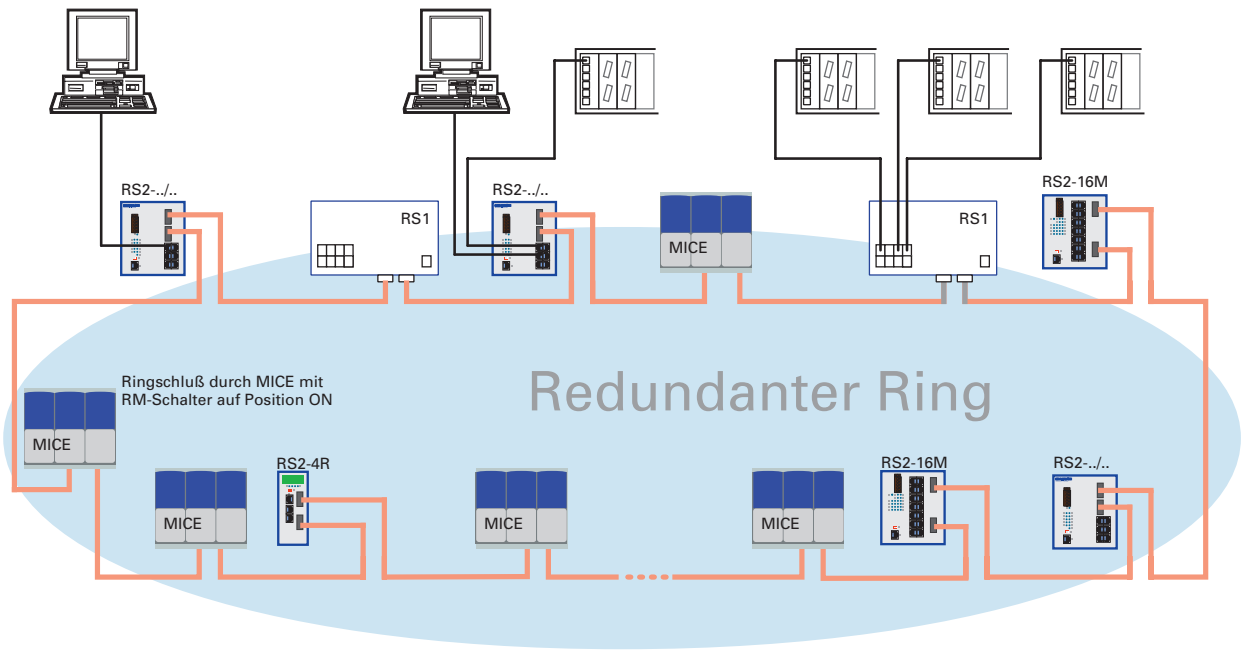


Abb. 43: Redundante Ringstruktur

Der RS2-../.. wird über die HIPER-Ring-Ports (Ports 6 und 7) in den HIPER-Ring integriert. Innerhalb eines HIPER-Ringes ist eine beliebige Mischung von RS1, RS2-../.., RS2-16M, RS2-4R, MACH3000 und MICE möglich. Beim Ausfall einer Teilstrecke wandelt sich die Ringstruktur bei bis zu 50 Switches innerhalb von 0,5 Sekunden wieder zurück in eine Linienstruktur.

Hinweis: Die Funktion „HIPER-Ring“ erfordert für die HIPER-Ring-Ports die Einstellung:
100 Mbit/s, Vollduplex und Autonegotiation aus (= Lieferzustand).

4.7.3 Redundante Kopplung von HIPER-Ringen und Netzsegmenten

Die im RS2-../.. eingebaute Steuerungsintelligenz erlaubt die redundante Kopplung von HIPER-Ringen und Netzsegmenten. Die Abbildung (siehe Abb. 44) zeigt die möglichen Konfigurationen.

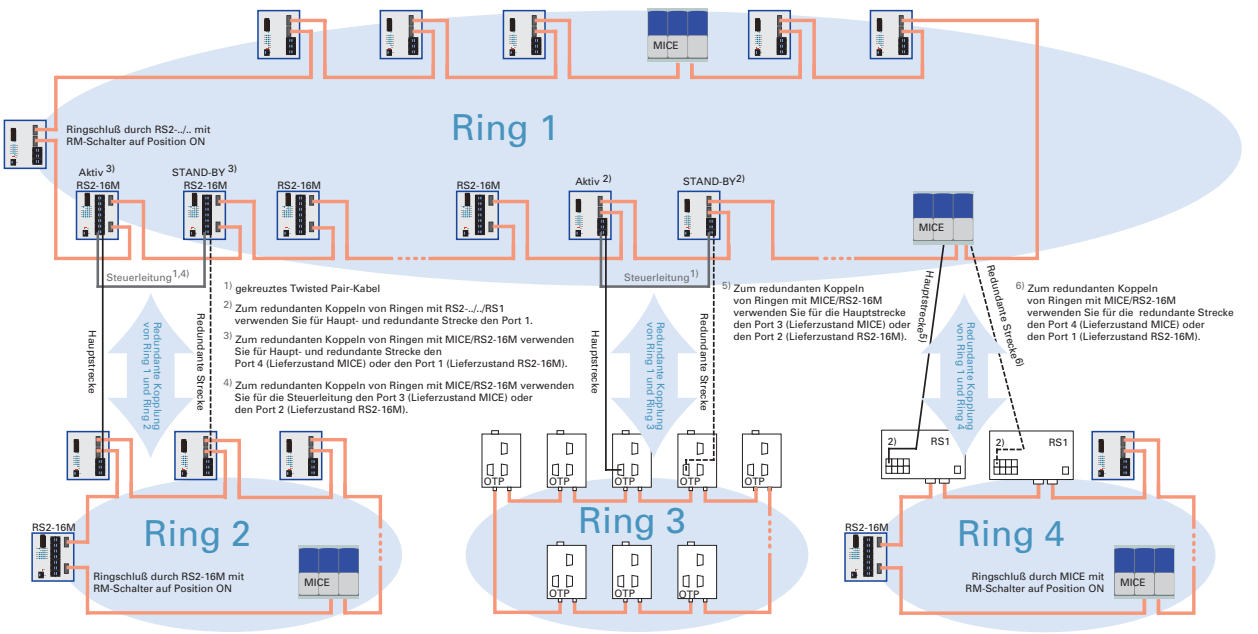


Abb. 44: Redundante Kopplung von Ringen

Die Verbindung zweier Netzsegmente erfolgt über zwei getrennte Pfade mit einem der folgenden Switches:

- RS2-16M,
- MICE (ab Rel. 3.0) oder
- MACH 3000 (ab Rel. 3.3).

Der Switch in der redundanten Strecke bekommt über die DIP-Schalter-Einstellung STAND-BY die Redundanzfunktion zugeordnet.
Der Switch in der redundanten Strecke und der Switch in der Hauptstrecke teilen sich über die Steuerleitung ihre Betriebszustände mit.

Unmittelbar nach dem Ausfall der Hauptstrecke gibt der redundante Switch die redundante Strecke frei. Ist die Hauptstrecke wieder in Ordnung, dann teilt dies der Switch in der Hauptstrecke dem redundanten Switch mit. Die Hauptstrecke wird freigegeben und die redundante Strecke wieder gesperrt. Ein Fehler wird innerhalb von 0,5 Sekunden erkannt und beseitigt.

4.8 Zeitsynchronisation

Was Echtzeit wirklich bedeutet, hängt von den Zeitanforderungen der Anwendung ab. Während SNTP im besten Fall eine Genauigkeit im Millisekunden-Bereich erzielen kann, erreicht IEEE 1588 mit dem Precision Time Protocol eine Genauigkeit im Submikrosekunden-Bereich.

4.8.1 SNTP

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren. SNTP ist hierarchisch aufgebaut. Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Der SNTP-Client bezieht die UTC vom SNTP-Server.

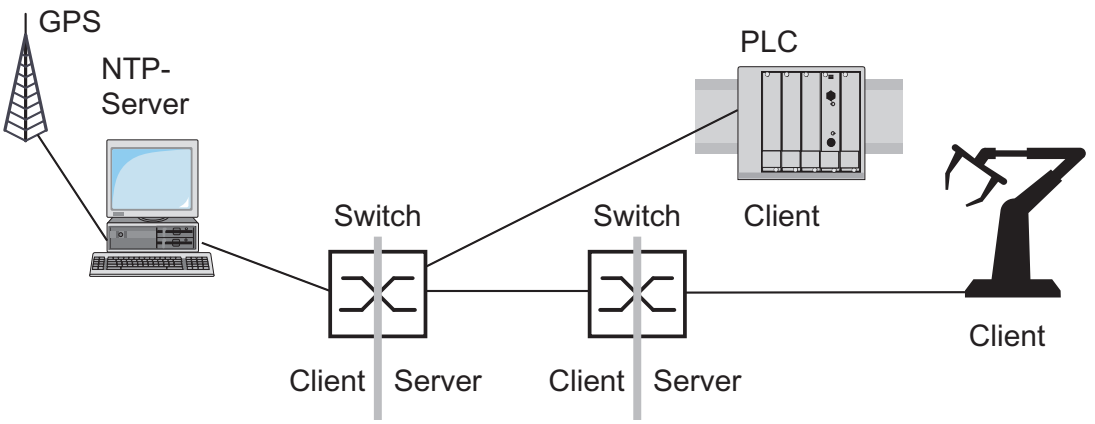


Abb. 45: SNTP-Kaskade

4.8.2 IEEE 1588 – Precison Time Protocol

Voraussetzung für zeitkritische, über ein LAN gesteuerte Anwendungen ist eine präzises Zeitmanagement. Der Standard IEEE 1588 beschreibt mit dem Precision Time Protocol (PTP) ein Verfahren, das ausgehend von einer genauesten Uhr die präzise Synchronisation aller Uhren in einem LAN ermöglicht.

Dieses Verfahren erlaubt eine Synchronisation der betroffenen Uhren mit einer Genauigkeit von bis zu wenigen 100 ns. Die Belastung des Netzes mit Synchronisationsnachrichten ist dabei verschwindend gering. PTP benutzt die Multicast-Kommunikation.

Einfluß auf die Präzision haben:

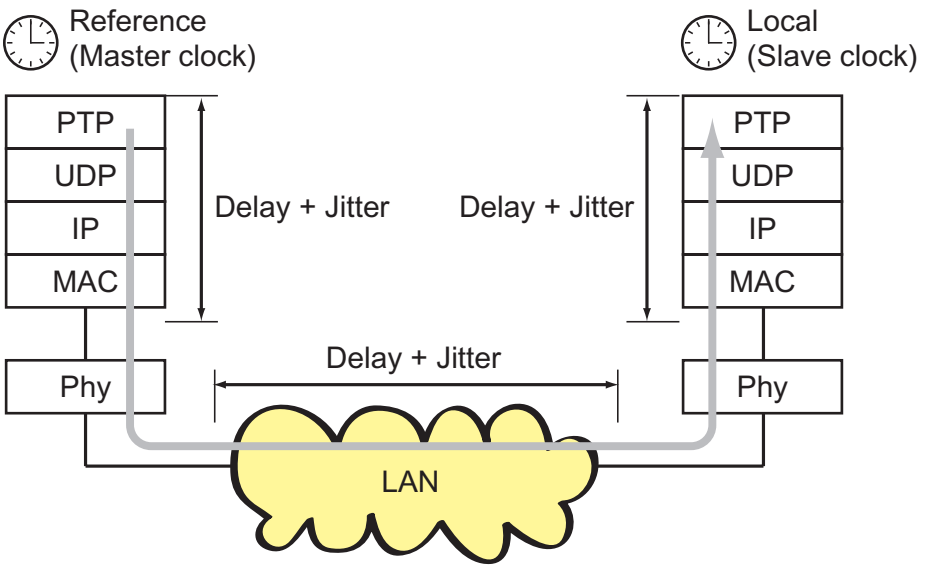
- Genauigkeit der Referenzuhr
  IEEE 1588 klassifiziert Uhren nach ihrer Genauigkeit. Ein Algorithmus, der die Genauigkeit der verfügbaren Uhren im Netz ermittelt, bestimmt die genaueste Uhr zur „Grandmaster"-Uhr.

Stratumnummer	Specifikation
0	Für zeitlich begrenzte, spezielle Zwecke, um einer Uhr einen besseren Wert zuzuordnen als allen anderen Uhren im Netz.
1	Bezeichnet die Uhr als Referenzuhr mit höchster Genauigkeit. Eine Stratum 1 Uhr kann sowohl Boundary als auch Ordenary Uhr sein. Zu Stratum 1 Uhren gehören GPS-Uhren und kalibrierte Atomuhren. Eine Stratum 1 Uhr kann nicht mittels PTP von einer anderen Uhr im PTP-System synchronisiert werden.
2	Bezeichnet die Uhr als Referenzuhr zweiter Wahl und kann nicht mittels PTP von einer anderen Uhr im PTP-System synchronisiert werden.
3	Bezeichnet die Uhr als Referenzuhr, die über eine externe Leitung andere Geräte synchronisieren kann.
4	Bezeichnet die Uhr als Referenzuhr.
5–254	Reserviert.
255	Voreinstellung. Eine solche Uhr sollte niemals beste Master-Uhr sein.

Tab. 8: Stratum – Klassifikation der Uhren

- Kabellaufzeiten; Gerätelaufzeiten (Delay)
  Das von IEEE 1588 vorgegebene Kommunikationsprotokoll ermöglicht die Ermittlung von Kabellaufzeiten. Formeln zur Berechnung der aktuellen Uhrzeit eliminieren Laufzeiten.

- Genauigkeit lokaler Uhren
  Das von IEEE 1588 vorgegebene Kommunikationsprotokoll berücksichtigt die Ungenauigkeit lokaler Uhren gegenüber der Referenzuhr. Berechnungsformeln erlauben die Synchronisation der lokalen Zeit unter Berücksichtigung der Ungenauigkeit der lokalen Uhr gegenüber der Referenzuhr.



PTP Precision Time Protocol (Application Layer)
UDP User Datagramm Protocol (Transport Layer)
IP Internet Protocol (Network Layer)
MAC Media Access Control
Phy Physical Layer

Abb. 46: Delay- und Jitterproblematik beim Uhrenabgleich

Um die Reduktion der Laufzeit und des Jitters im Protokollstapel zu umgehen, empfiehlt IEEE 1588, eine spezielle Hardware-Zeitstempeleinheit (Time Stamp Unit) zwischen MAC und Phy einzusetzen.

Die Laufzeit und der Jitter im LAN summiert sich in den Medien und Übertragungsgeräten entlang des Übertragungspfades.

Die Kabellaufzeiten sind relativ konstant. Änderungen treten sehr langsam auf. Diese Tatsache berücksichtigt IEEE 1588 durch regelmäßige Messungen und Neuberechnungen.

Die Ungenauigkeit durch Gerätelaufzeit und Geräte-Jitter umgeht IEEE 1588 durch die Definition von „Boundary Clocks“. Boundary Clocks sind Uhren, die in Geräte integriert sind. Diese Uhren werden auf der einen Seite im Signalpfad synchronisiert und auf der anderen Seite des Signalpfades dienen sie zur Synchronisation der folgenden Uhren (Ordinary Clocks).

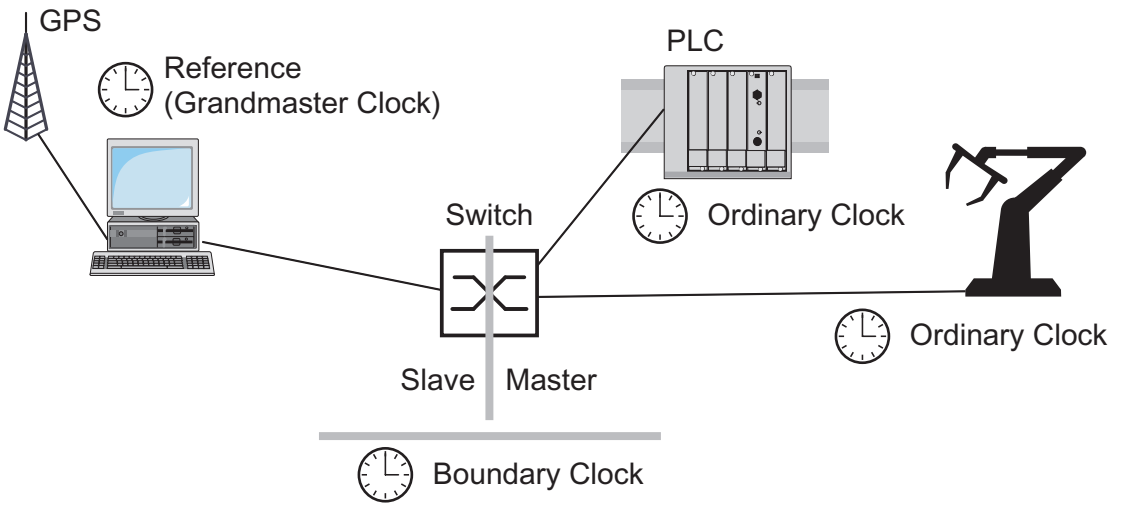


Abb. 47: Boundary Clock

Unabhängig von physikalischen Kommunikationspfaden sieht das PTP logische Kommunikationspfade vor, die Sie durch das Einrichten von PTP-Subdomänen definieren. Subdomänen haben den Zweck, Gruppen von Uhren, die zeitlich unabhängig vom Rest der Domäne sind, zu bilden. Typischerweise benutzen die Uhren einer Gruppe die gleichen Kommonikationspfade wie andere Uhren auch.

Die Einstellungen zum PTP nehmen Sie im Web-Interface vor (siehe Seite 169).

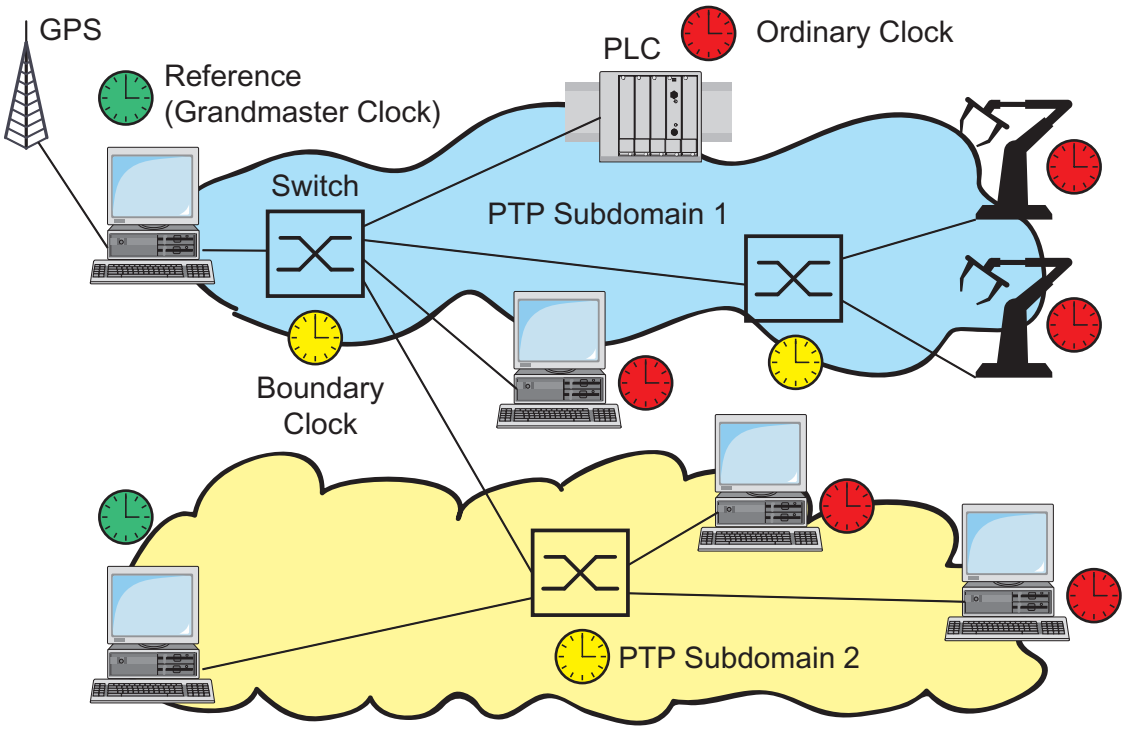


Abb. 48: PTP-Subdomänen

4.9 Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht dem Anwender eine automatische Topologie-Erkennung seines LANs.

Ein Gerät mit aktivem LLDP

- verbreitet eigene Verbindungs- und Management-Informationen an die angrenzenden Geräte des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben.
- empfängt Verbindungs- und Management-Informationen von angrenzenden Geräten des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben..
- errichtet ein Management-Informationsschema und Objektdefinitionen zum Speichern von Verbindungsinformationen benachbarter Geräte mit aktiviertem LLDP.

Als zentrales Element enthält die Verbindungsinformation die genaue, eindeutige Kennzeichnung eines Verbindungsendpunktes: MSAP (MAC Service Access Point). Diese setzt sich zusammen aus der MAC-Adresse des Gerätes und einer für dieses Gerät eindeutigen Portkennung.
Inhalt der Verbindungs- und Management-Informationen:

- Typ der Chassis-Kennung (z.B. macaddress)
- Chassis-Kennung (dessen MAC Adresse)
- Typ der Port-Kennung (z.B. macaddress)
- Port-Kennung (dessen Port-MAC Adresse)
- Beschreibung des Ports
- Systemname
- Systembeschreibung
- Unterstützte "System Capabilities" (z.B. Router = 14 oder Switch = 4)
- Momentan aktivierte "System Capabilities"
- Interface-Typ der Management Adresse
- Interface-Id der Management Adresse
- Object Identifier der Management Adresse (0.0 = nicht unterstützt!)
- VLAN-ID des Ports
- Fähigkeit des Ports, Autonegotiation zu unterstützen
- Zustand der Autonegotiation am Port

- Medium, Halb-/Vollduplexeinstellung und Geschwindigkeit-Einstellung des Ports
- Fehleranzeige

Diese Informationen sind von einer Netzmanagementstation abrufbar. Mit diesen Informationen ist die Netzmanagementstation in der Lage, die Topologie des Netzes darzustellen.

Zum Informationsaustausch benutzt LLDP eine IEEE-MAC-Adresse, die Switche normalerweise nicht vermitteln. Deshalb verwerfen Switches ohne LLDP-Unterstützung LLDP-Pakete. So verhindert ein nicht LLDP-fähiges Gerät zwischen zwei LLDP-fähigen Geräten den LLDP-Informationsaustausch zwischen diesen beiden Geräten. Um dies zu umgehen, versenden Hirschmann-Switche zusätzliche LLDP-Pakete an die Hirschmann-Multicast-MAC-Adresse 01:80:63:2F:FF:0B.

Die Einstellungen zur Topologie-Erkennung nehmen Sie im Web-Interface vor (siehe Seite 222).

4.10 Sicherheit

4.10.1 Portsicherheit

Der Switch schützt jeden Port vor unberechtigtem Zugriff.
Zur Sicherheitsüberwachung jedes einzelnen Ports stehen folgende Funktionen zur Verfügung:

- Wer hat Zugang zu diesem Port?
  Der Switch kennt 2 Klassen von Zugangskontrolle:
  - Jeder: keine Zugangsbeschränkung
  - Benutzer: ausschließlich ein zugewiesener Benutzer hat Zugang
- Welche Aktionen folgen auf einen unberechtigten Zugriff?
  Der Switch kann mit drei auswählbaren Aktionen auf einen unberechtigten Zugriff reagieren:
  - non: keine Reaktion
  - trapOnly: Meldung durch Verschicken eines Traps
  - portDisable: Meldung durch Verschicken eines Traps und Abschaltung des Ports

Die Einstellungen für die Port-Sicherheit erfolgen über das Web-based Management “Einstellung der Portsicherheit” auf Seite 220 oder das Netzmanagement HiVison. Hierzu wählen Sie im Gerätefenster mit der rechten Maustaste auf dem Agenten-Symbol `Sicherheit`. Im sich daraufhin öffnenden Agenten-Fenster finden Sie unter `Port Security` die Tabelle mit den entsprechenden MIB-Variablen.

4.10.2 SNMP

Der Agent kommuniziert über das Simple Network Management Protocol mit der Netzmanagement-Station. Diese benutzt hierzu die Netzmanagement-Software HiVision oder das Web-based Interface.
Jedes SNMP-Paket enthält die IP-Adresse des sendenden Rechners und die Community, unter welcher der Absender des Pakets auf die MIB des Switch zugreifen will.

Der Switch empfängt das SNMP-Paket und vergleicht die IP-Adresse des sendenden Rechners und die Community mit den Einträgen in der `hmAuth-CommTable` und der `hmAuthHostTable` ihrer MIB. Liegt die Community mit dem entsprechenden Zugriffsrecht vor und ist die IP-Adresse des sendenden Rechners eingetragen, dann gewährt der Switch den Zugriff.

Im Lieferzustand ist der Switch über die Community „public“ (nur lesen) und „private“ (lesen und schreiben) von jedem Rechner aus zugänglich.

Um ihren Switch vor unerwünschten Eingriffen zu schützen:

☐ Definieren Sie zuerst eine neue Community, unter welcher Sie mit allen Rechten von Ihrem Rechner aus zugreifen können .

Hinweis: Notieren Sie sich den Community-Namen und den dazu gehörigen Index. Aus Sicherheitsgründen kann der Community-Name später nicht mehr gelesen werden. Der Zugriff auf die Community-Access-, Trap-Destination- und Trap-Configuration-Table erfolgt über den Community-Index.

☐ Behandeln Sie diese Community **vertraulich**. Denn jeder, der die Community kennt, kann mit der IP-Adresse ihres Rechners auf die MIB des Switch zugreifen.
☐ Beschneiden Sie die Zugriffsrechte der bekannten Communities oder löschen Sie deren Einträge.

4.10.3 SNMP-Traps

Treten im Normalbetrieb des RS2-../.. außergewöhnliche Ereignisse auf, werden diese sofort der Managementstation mitgeteilt. Dies geschieht über sogenannte **Traps** - Alarmmeldungen - die das Polling-Verfahren umgehen. (Unter „Polling“ versteht man das zyklische Abfragen von Datenstationen). Traps ermöglichen eine schnelle Reaktion auf kritische Zustände.

Beispiele für solche Ereignisse sind:

- Hardware-Reset,
- Grundgeräte-Konfigurationsänderungen,
- Segmentierung eines Ports,

Zur Erhöhung der Übertragungssicherheit für die Meldungen können Traps an verschiedene Hosts verschickt werden. Eine Trap-Meldung besteht aus einem Paket, das nicht quittiert wird.
Der Management-Agent verschickt Traps an jene Hosts, die in der Zieltabelle (Trap Destination Table) eingetragen sind. Die Trap Destination Table kann mit der Managementstation über SNMP konfiguriert werden.

Auflistung der SNMP-Traps

Welche Traps im einzelnen auftreten können, ist in der folgenden Tabelle aufgelistet.

authenticationFailure
wird gesendet, falls eine Station versucht, unberechtigt auf einen Agenten zuzugreifen.

coldStart
wird sowohl bei Kalt- als auch bei Warmstart während des Bootens nach erfolgreicher Initialisierung des Managements gesendet.

hmAutoconfigAdapterTrap
wird gesendet, wenn der AutoConfiguration Adapter ACA 11 entfernt oder wieder aufgesteckt wird.

linkDown
wird gesendet, wenn die Verbindung zu einem Port unterbrochen wird.

linkUp
wird gesendet, sobald die Verbindung zu einem Port wieder hergestellt wird.

hmPowerSupply
wird gesendet, wenn sich der Status der Spannungsversorgung ändert.

hmSignallingRelay
wird gesendet, wenn sich der Zustand des Meldekontaktes ändert.

newRoot
wird gesendet, wenn der sendende Agent zur neuen Wurzel des Spanning Trees wird.

topologyChange
wird gesendet, wenn sich der Vermittlungsmodus eine Ports ändert.

hmStandby
wird gesendet, wenn sich der Betriebszustand des RS2-../.. ändert.

risingAlarm
wird gesendet, wenn ein RMON-Alarmeingang seine obere Schwelle überschreitet.

fallingAlarm
wird gesendet, wenn ein RMON-Alarmeingang seine untere Schwelle unterschreitet.

hmPortSecurityTrap
wird gesendet, wenn eine MAC/IP-Adressse an diesem Port erkannt wird, die nicht den aktuellen Einstellungen von

- `hmPortSecPermission` und
- `hmPorSecAction` entweder auf `trapOnly` (2) oder `portDisable` (3) gesetzt,

entspricht.

hmBPDUGuardTrap
wird gesendet, wenn an einem Port trotz aktivierter BPDU-Guard-Funktion eine BPDU empfangen wird.

hmRingRedReconfig
wird gesendet, sobald sich die Konfiguration des HIPER-Rings ändert.

hmRingRedCplReconfig
wird gesendet, sobald sich die Konfiguration der redundanten Ring-/ Netzkopplung ändert.

hmSNTPTrap
wird gesendet, wenn im Zusammenhang mit dem SNTP-Protokoll Fehler auftreten (z.B. Server nicht erreichbar).

hmRelayDuplicateTrap
wird gesendet, wenn im Zusammenhang mit der DHCP Option 82 eine doppelte IP-Adresse erkannt wird.

lldpRemTablesChangeTrap
wird gesendet, wenn sich ein Eintrag in der Topologie-Tabelle ändert.

4.10.4 SNMP-Traps beim Booten

Die Alarmmeldung ColdStart wird bei jedem Booten gesendet.

5 Web-based Management

Der Switch unterstützt sowohl SNMP-Management als auch Web-based Management und bietet dadurch

- umfangreiche Diagnose- und Konfigurationsfunktionen für eine schnelle Inbetriebnahme und
- umfangreiche Netz- und Geräteinformationen.

Der Switch unterstützt die TCP/IP Protokollfamilie.

Das komfortable Web-based Interface gibt Ihnen die Möglichkeit, den Switch von jedem beliebigen Ort im Netz über einen Standard- Browser wie Netscape Navigator/Communicator oder Microsoft Internet Explorer zu managen. Der Web Browser als universelles Zugriffstool zeigt ein Applett an, das mit dem Switch über das Simple Network Management Protokoll (SNMP) Daten austauscht.
Das Web-based Interface ermöglicht Ihnen eine grafische Konfiguration des Switch.

5.1 Öffnen des Web-based Interfaces

Zum Öffnen des Web-based Interface benötigen Sie einen Web Browser (Programm, das das Lesen von Hypertext ermöglicht), zum Beispiel den Netscape Navigator/Communicator ab der Version 6.0 oder den Microsoft Internet Explorer ab der Version 5.5.

Hinweis: Das Web-based Interface verwendet das Plugin "Java™ Runtime Environment Version 1.3". Ist dieses nicht auf Ihrem Rechner installiert, wird beim ersten Aufrufen des Web-based Interfaces automatisch eine Installation über das Internet aufgerufen. Diese Installation ist sehr zeitaufwendig.

Für Windows-Benutzer: Deshalb brechen Sie die Installation ab. Installieren Sie das Plugin von der beiliegenden CDROM. Hierzu starten Sie die Programmdatei `j2re1_3_1_07-windows-i586-i.exe` im Verzeichnis Java auf der CDROM.

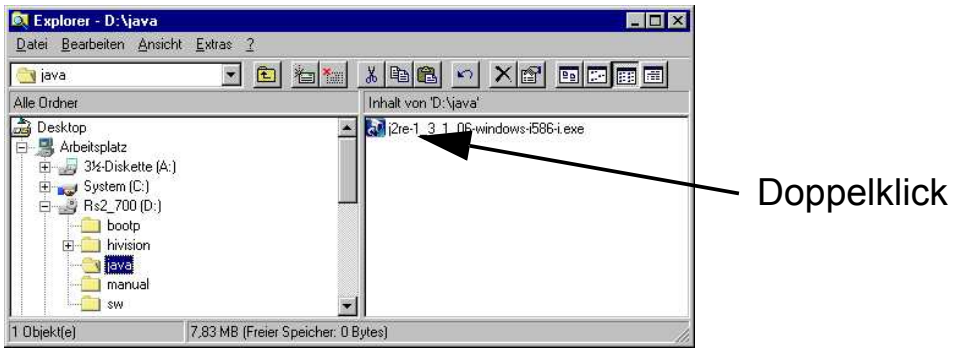


Abb. 49: Java installieren

☐ Starten Sie Ihren Web Browser.

☐ Stellen Sie sicher, daß in den Sicherheitseinstellungen Ihres Browsers Javascript und Java eingeschaltet ist.

☐ Zur Herstellung der Verbindung geben Sie im Adreßfeld des Web Browsers die IP-Adresse des RS2-../.., den Sie mit dem Web-based Management administrieren möchten, in der folgenden Form ein:

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

Auf dem Bildschirm erscheint das Login-Fenster.

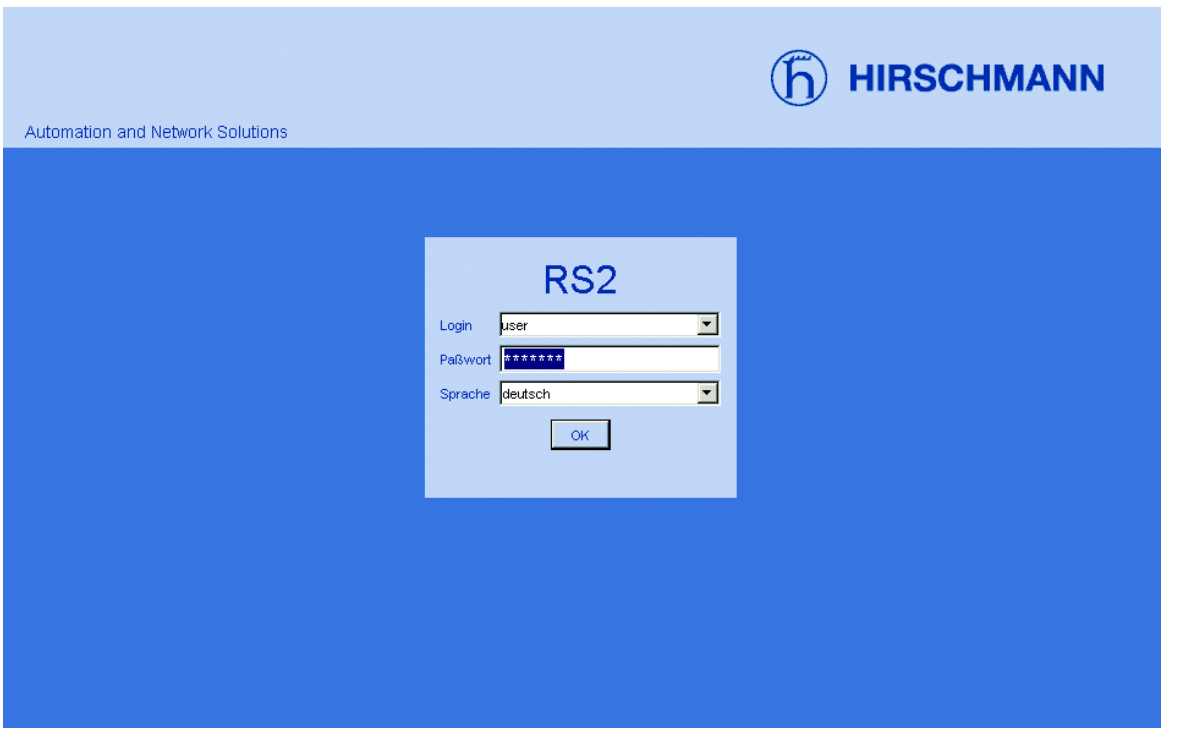


Abb. 50: Login-Fenster

☐ Wählen Sie die gewünschte Sprache aus.

☐ Wählen Sie im Login-Ausklappmenü
– user, um mit Leserecht oder
– admin, um mit Schreib- und Leserecht
auf den Switch zuzugreifen.

☐ Im Paßwort-Feld ist das Paßwort "public", mit dem Sie über Leserechte verfügen, vorgegeben. Wollen Sie mit Schreibrechten auf den RS2-../.. zugreifen, dann markieren Sie den Inhalt des Paßwortfeldes und überschreiben ihn mit dem Paßwort "private" (Lieferzustand).
Das Ändern des Paßwortes schützt den RS2-../.. vor unberechtigten Zugriffen.

☐ Klicken Sie auf OK.

Am Bildschirm erscheint die Web Site des RS2-../...

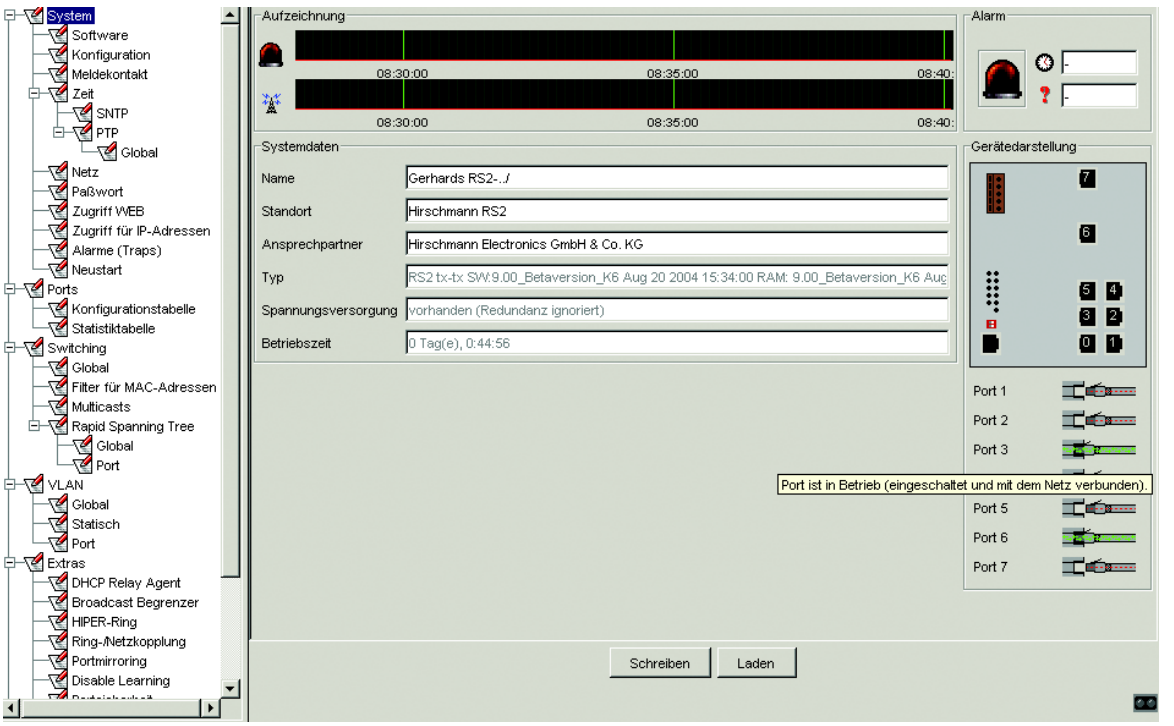


Abb. 51: Web-Site des RS2-../.. mit Sprechblasenhilfe

5.2 Menübaum

Der Menüteil zeigt die Menüpunkte. Durch Plazieren des Mauszeigers im Menüteil und Drücken der rechten Maustaste können Sie mit „Alle Einträge aufklappen“ den gesamten Menübaum aufklappen und mit „Alle Einträge einklappen“ den Menübaum bis auf die Hauptmenüs einklappen.

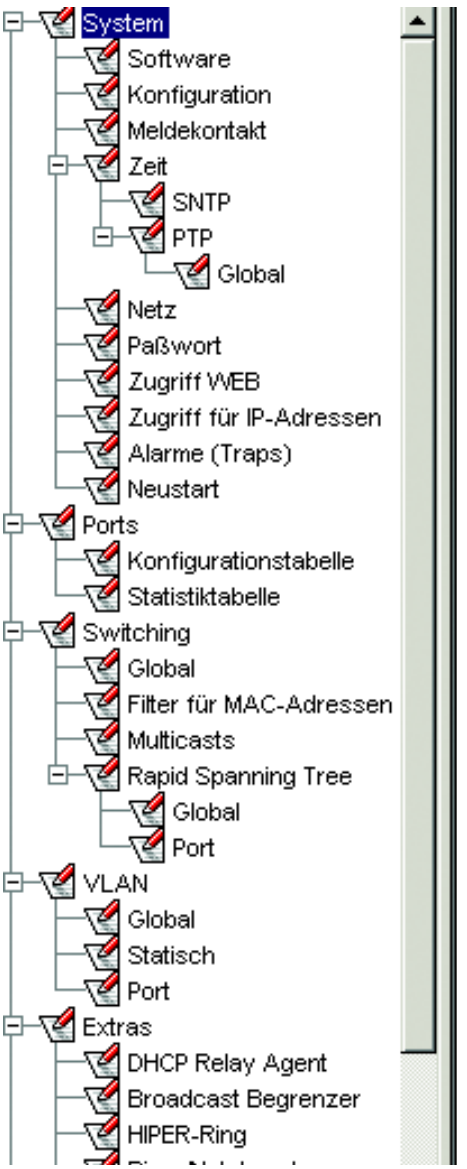


Abb. 52: Menübaum

5.3 System

Das Systemmenü enthält die Dialoge und Tabellen zur Systemkonfiguration:

- Software-Update
- Start-Konfiguration festlegen
- Netzparameter festlegen
- Meldekontakt
- SNTP
- Paßwort
- Zugriff WEB
- Zugriff für IP-Adressen
- Alarme (Traps) Konfiguration
- Neustart des Gerätes

Der Informationsteil im Systemmenü ist untergliedert in:

- Aufzeichnung
- Alarm
- Systemdaten
- Gerätedarstellung
- Aktualisierung
- Portstatus

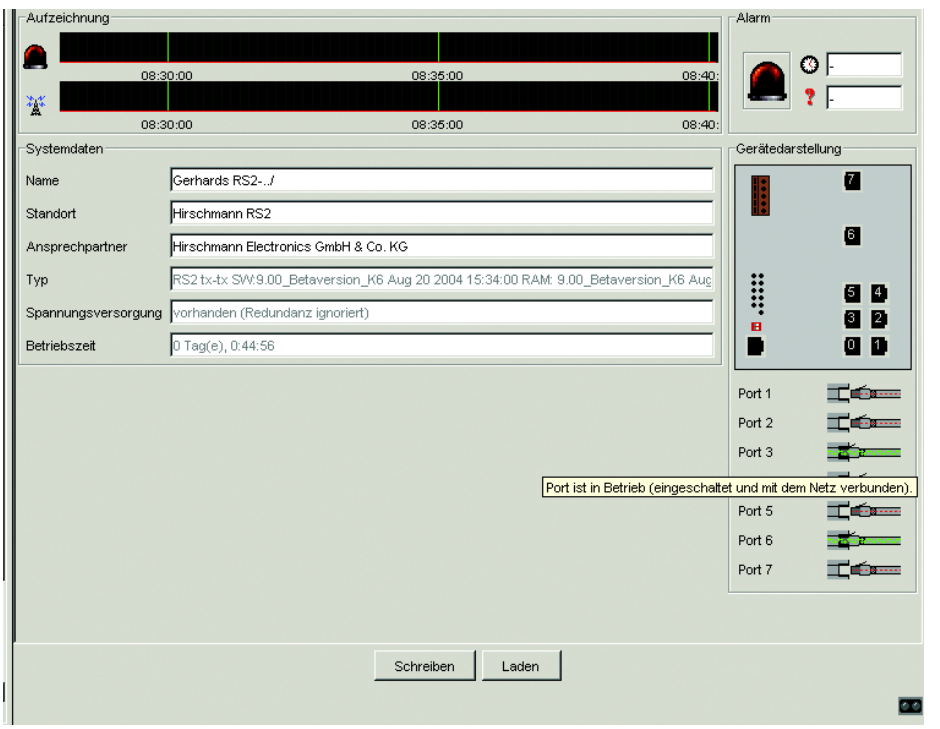


Abb. 53: Informationsteil im Systemmenü

Aufzeichnung

Dieser Bereich der Web-Site zeigt die Historie des RS2-../.. an.
Da die Historie vom Applet des Web-Browsers geführt wird, ist die Historie genau während der Laufzeit des Applets verfügbar. Das Zeitfenster umfaßt bis zu zwei Stunden.

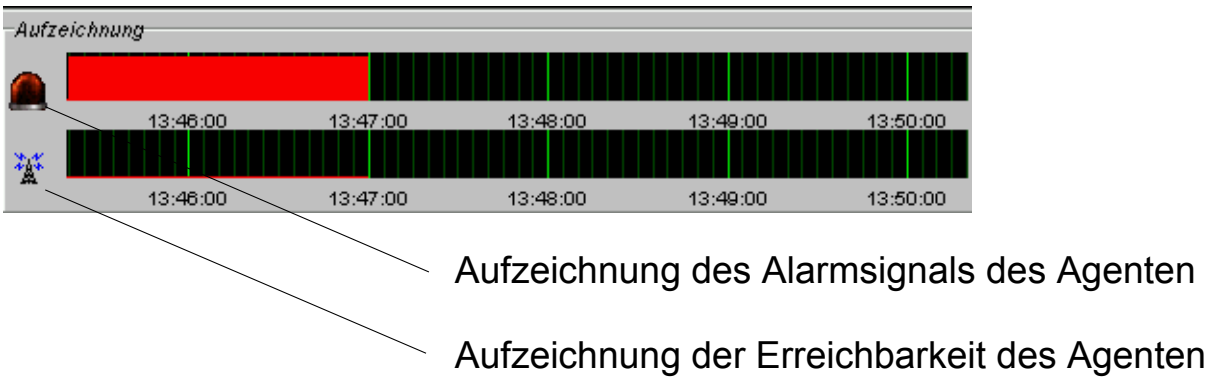


Abb. 54: Historien-Anzeige

Alarm

Dieser Bereich der Web-Site gibt Auskunft über den Alarmzustand des RS2-../...

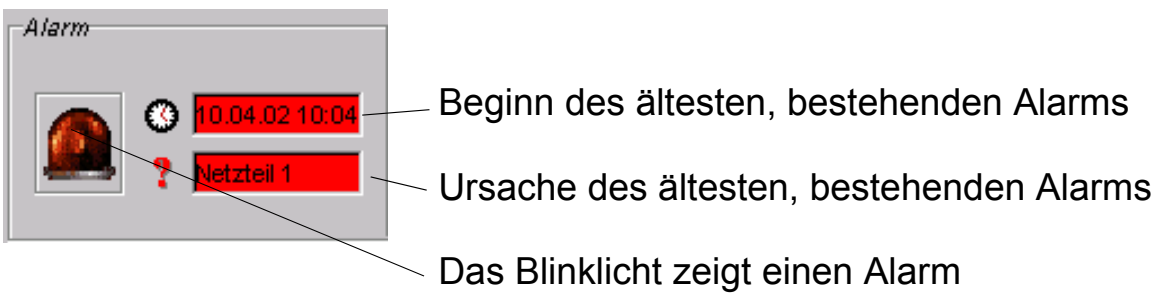


Abb. 55: Alarm-Anzeige

Systemdaten

Dieser Bereich der Web-Site zeigt die Systemparameter des Agenten an. Hier haben Sie die Möglichkeit,
– den Systemnamen,
– die Standortbezeichnung und
– den Namen des Ansprechpartner für diesen Switch
zu ändern.

– Systemname dieses Switches
– Standort dieses Switches
– Ansprechpartner für diesen Switch
– Soft- und Hardware-Version
– Status der Netzteile
– Zeit, die seit dem letzten Neustart dieses Switches vergangen ist.

Abb. 56: Systemparameter-Anzeige

Gerätedarstellung

Dieser Bereich der Web-Site zeigt das Bild des Gerätes. Unterhalb des Geräteabbildes stellen Symbole den Status der einzelnen Ports dar.

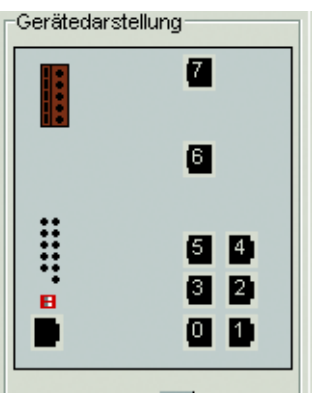


Abb. 57: Gerätedarstellung

Bedeutung der Symbole:

 Der Port ist freigegeben und die Verbindung ist in Ordnung.

 Der Port ist vom Management gesperrt.

 Der Port ist freigegeben und die Verbindung ist unterbrochen.

 Der RS2-../.. ist nicht erreichbar.

Aktualisierung

Dieser Bereich der Web-Site links unten zeigt an, nach welcher Zeit das Applet die aktuellen Daten dieses Dialogs wieder abruft. Das Klicken auf die „Laden“-Taste bewirkt ein sofortiges abrufen der aktuellen Daten des RS2-../... Das Applet ruft automatisch alle 100 Sekunden die aktuellen Daten des RS2-../.. ab.

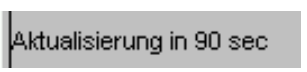


Abb. 58: Zeit bis zur Aktualisierung

5.3.1 Software-Update durchführen

Der Dialog Software bietet Ihnen die Möglichkeit, ein Software-Update des RS2-../.. via tftp oder http durchzuführen.

tftp-Update
Für ein tftp-Update benötigen Sie einen tftp-Server, auf dem die zu ladende Software abgelegt ist. Der URL kennzeichnet den Pfad zu der auf dem tftp-Server gespeicherten Software. Der URL hat die Form tftp:// IP-Adresse des tftp-Servers/Pfadname/Dateiname (z.B. `tftp://149.218.112.5/rs2/rs2.bin`).
Mit "tftp-Update" lädt der RS2-../.. die Software vom tftp-Server.

http-Update
Für ein http-Update benötigen Sie von Ihrem Rechner aus den Zugang zu der Update-Software.
Mit „http-Update“ öffnet der RS2-../.. ein zweites Browser-Fenster. Wählen Sie darin die Update-Software aus und klicken Sie auf „Update“, um die Software auf den RS2-../.. zu übertragen.

http-Update 2. Browser-Fenster:
- ☐ Klicken Sie auf `Durchsuchen`, um die Software für das Update auszuwählen.
- ☐ Klicken Sie auf „Update“, um die Software auf den Switch zu übertragen.

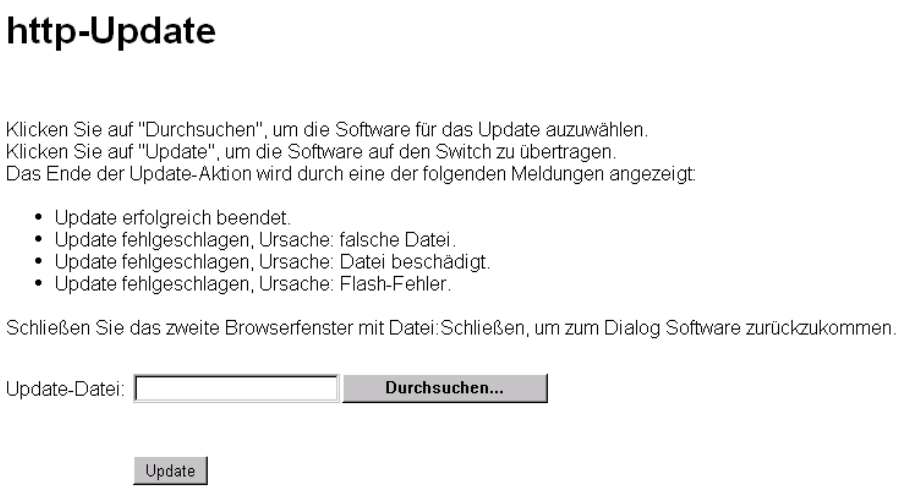


Abb. 59: Dialog Software-Update via http

Das Ende der Update-Aktion wird durch eine der folgenden Meldungen angezeigt:

- Update erfolgreich beendet.
- Update fehlgeschlagen, Ursache: falsche Datei.
- Update fehlgeschlagen, Ursache: Datei beschädigt.
- Update fehlgeschlagen, Ursache: Flash-Fehler.

☐ Schließen Sie das dieses Browser-Fenster mit `Datei:Schließen`, um zum Dialog Software zurückzukommen.

Um die neue Software nach dem Laden zu starten, führen Sie einen Neustart des RS2-../.. durch (siehe Dialog "Neustart des Switches" auf Seite 179).

Hinweis: Mit welcher Konfiguration der Switch nach einem Neustart geladen wird, legen Sie in den Dialogen "Start-Konfiguration festlegen" auf Seite 159 und "Netzparameter festlegen" auf Seite 170 fest.

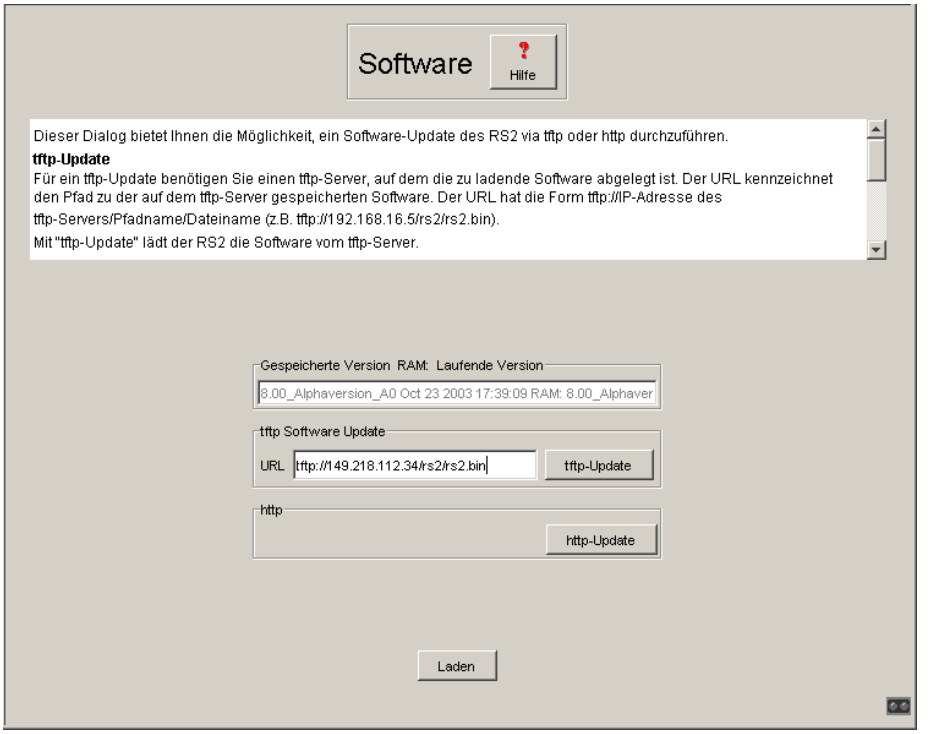


Abb. 60: Dialog Software-Update

Nach dem Software-Update löschen Sie den Inhalt des Zwischenspeichers Ihres Browsers. So kann Ihr Browser nach einem Neustart die neue Version des Web-based Interfaces laden.

☐ – Netscape Navigator/Communicator:
Browser schließen und neu öffnen.
– Microsoft Internet Explorer:
Unter `Extras:Internetoptionen:Erweitert` den Punkt „Leeren des Ordners Temporary Internet Files beim Schließen des Browser“ anwählen.
Browser schließen und neu öffnen.

5.3.2 Start-Konfiguration festlegen

Dieser Dialog bietet Ihnen die Möglichkeit,

- eine Neustartkonfiguration festzulegen,
- eine Konfiguration zu laden,
- eine Konfiguration zu speichern,
- einen URL einzugeben,
- den ACA-Status anzusehen.

Neustartkonfiguration

Im Rahmen „Konfiguration nach Neustart laden“ legen Sie die Konfiguration fest, mit der das System beim Neustart geladen wird.
Wenn Sie Voreinstellung wählen, werden die Parameter auf den Lieferzustand zurückgesetzt, mit Ausnahme der Einstellungen, die Sie in den Dialogen Software, Konfiguration und Netz vorgenommen haben

Konfiguration laden

Im Rahmen „Laden“ habe Sie die Möglichkeit,

- eine lokal gespeicherte Konfiguration zu laden.
- eine unter dem angegebenen URL gespeicherte Konfiguration zu laden.
- eine unter dem angegebenen URL gespeicherte Konfiguration zu laden und lokal zu speichern.

Konfiguration speichern

Im Rahmen „Speichern“ haben Sie die Möglichkeit,

- die aktuelle Konfiguration auf dem Gerät speichern.
- die aktuelle Konfiguration in einer Datei unter dem angegebenen URL zu speichern.

Hinweis: Den von DHCP/BOOTP (siehe "Netzparameter festlegen" auf Seite 170) gestarteten Ladevorgang zeigt die Selektion von "vom URL & lokal speichern" im Rahmen "Laden" an. Sollten Sie beim Speichern einer Konfiguration eine Fehlermeldung erhalten, dann kann eine Ursache ein aktiver Ladevorgang sein. DHCP/BOOTP beendet einen Ladevorgang erst, wenn eine gültige Konfiguration geladen ist. Findet DHCP/BOOTP keine gültige Konfiguration, dann beenden Sie den Ladevorgang durch laden der lokalen Konfiguration im Rahmen "Laden".

- **URL**

  Der URL kennzeichnet den Pfad zum tftp-Server auf dem die Konfigurationsdatei zu speichern ist. Der URL hat die Form tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname (z.B. `tftp://149.218.112.5/rs2/config.dat`).

  Beispiel zum Speichern auf einem tftp-Server
  - ☐ Öffnen Sie in einem Editor eine neue Datei.
  - ☐ Speichern Sie die leere Datei in den entsprechenden Pfad des tftp-Servers mit dem Dateinamen, z.B. `RS2/RS2_01.cfg`
  - ☐ Geben Sie in der Zeile „URL“ den Pfad des tftp-Servers ein, z.B. `tftp://149.218.112.214/RS2/RS22_01.cfg`.

  Hinweis: Die Konfigurationsdatei enthält alle Konfigurationsdaten, auch das Paßwort. Achten Sie deshalb auf die Zugriffsrechte auf dem tftp-Server.

AutoConfiguration Adapter (ACA)

Der ACA ist ein Gerät zum Speichern der Konfigurationsdaten eines Switches MICE, RS2../.., RS2-16M, RS2-4R oder MACH 3000. Der ACA ermöglicht beim Ausfall eines Switches eine denkbar einfache Konfigurationsdatenübernahme durch einen Ersatzswitch des gleichen Typs.

Aktuelle Konfigurationsdaten in den ACA speichern:
Sie haben die Möglichkeit, die aktuelle Switch-Konfiguration mit "Lokal Konfiguration speichern" auf den ACA und in den Flash-Speicher zu übertragen. Wählen Sie zuvor die Einstellung „Lokal“ im Feld „Speichern“.

Konfigurationsdaten vom ACA übernehmen:
Bei einem Neustart übernimmt der Switch die Konfigurationsdaten des ACAs und speichert Sie nicht flüchtig im Flash-Speicher. Welche Daten der Switch vom ACA übernimmt, hängt von der Einstellung der Neustartkonfiguration ab (siehe Tab. 9 auf Seite 161).
Enthält der angeschlossene ACA keine gültigen Daten, z.B. ein neuer ACA, dann lädt der Switch die Daten aus dem Flash-Speicher.

Einstellung	Auswirkung
Lokal	Der Switch übernimmt alle Daten aus dem ACA
vom URL	Der Switch übernimmt die IP-Parameter aus dem ACA und die anderen Daten vom URL
Voreinstellung	Der Switch übernimmt die IP-Parameter aus dem ACA und setzt die anderen Parameter auf den Lieferzustand

Tab. 9: Datenübernahme vom ACA nach Neustart

Status	Bedeutung
notPresent	Kein ACA vorhanden
ok	Konfigurationsdaten von ACA und Switch stimmen überein.
removed	Der ACA wurde nach dem Booten entfernt.
notInSync	Konfigurationsdaten von ACA und Switch stimmen nicht überein.
outOfMemory	Die lokalen Konfigurationsdaten sind zu umfangreich um sie auf dem ACA zu speichern.
wrongMachine	Die Konfigurationsdaten im ACA stammen von einem anderen Gerätetyp.
checksumErr	Die Konfigurationsdaten sind beschädigt.

Tab. 10: ACA-Status

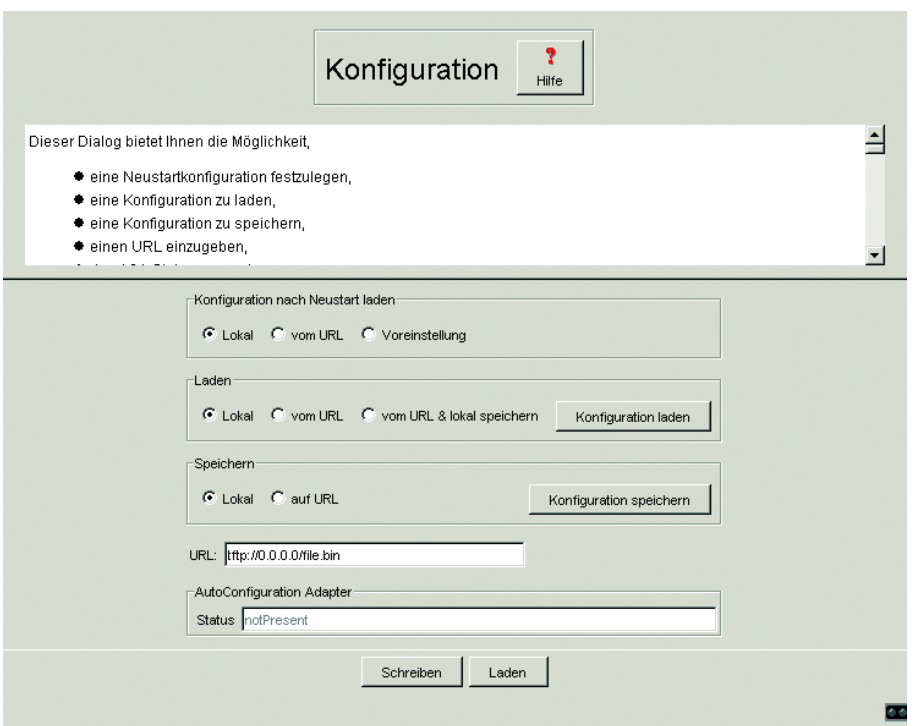


Abb. 61: Dialog Start-Konfiguration

5.3.3 Meldekontakt

Der Meldekontakt dient

- der manuelen Einstellung des Meldekontaktes.
- der Funktionsüberwachung des RS2-../.. und ermöglicht damit eine Ferndiagnose.

Manuelle Einstellung

Dieser Modus bietet Ihnen die Möglichkeit, den Meldekontakt fernzubedienen.

- ☐ Wählen Sie „Offen“ im Feld „Manuelle Einstellung“, um den Kontakt zu öffnen.
- ☐ Wählen Sie „Geschlossen“ im Feld „Manuelle Einstellung“, um den Kontakt zu schließen.

Anwendungsmöglichkeiten:

- Simulation eines Fehlers bei einer SPS-Fehlerüberwachung.
- Fernbedienung eines Gerätes über SNMP, wie z.B. das Einschalten einer Kamera.

Funktionsüberwachung

Der Meldekontakt dient der Funktionsüberwachung des RS2-../.. und ermöglicht damit eine Ferndiagnose.
Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung gemeldet:

- der Ausfall mindestens einer der zwei Versorgungsspannungen (Versorgungsspannung 1 oder 2 < 18 V). Wählen Sie „Redundante Stromversorgung ignorieren“, wenn Sie keine redundante Stromversorgung angeschlossen haben.

Hinweis: Bei nicht redundanter Zuführung der Versorgungsspannung meldet der RS2-../.. den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

- eine dauerhafte Störung im RS2-../.. (interne 3,3 VDC-Spannung).

- der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Linkstatus kann beim RS2-../.. pro Port über das Management maskiert werden. Im Lieferzustand erfolgt keine Verbindungsüberwachung.
- Fehler beim Selbsttest.
- der Entfall der Redundanzgewährleistung (siehe "Konfiguration der HIPER-Ring-Funktion" auf Seite 210 und/oder "Konfiguration der redundanten Kopplung von HIPER-Ringen und Netzsegmenten" auf Seite 211). Wählen Sie "Redundanzgewährleistung überwachen", wenn der Meldekontakt eine nicht mehr gewährleistete Redundanz melden soll.

Im Stand-by-Modus werden folgende Zustände gemeldet:
- Steuerkabel unterbrochen
- Partnergerät ist im Stand-by-Modus

Im RM-Betrieb wird zusätzlich folgender Zustand gemeldet:
- Ringredundanz gewährleistet. Im Lieferzustand erfolgt keine Überwachung der Ringredundanz.

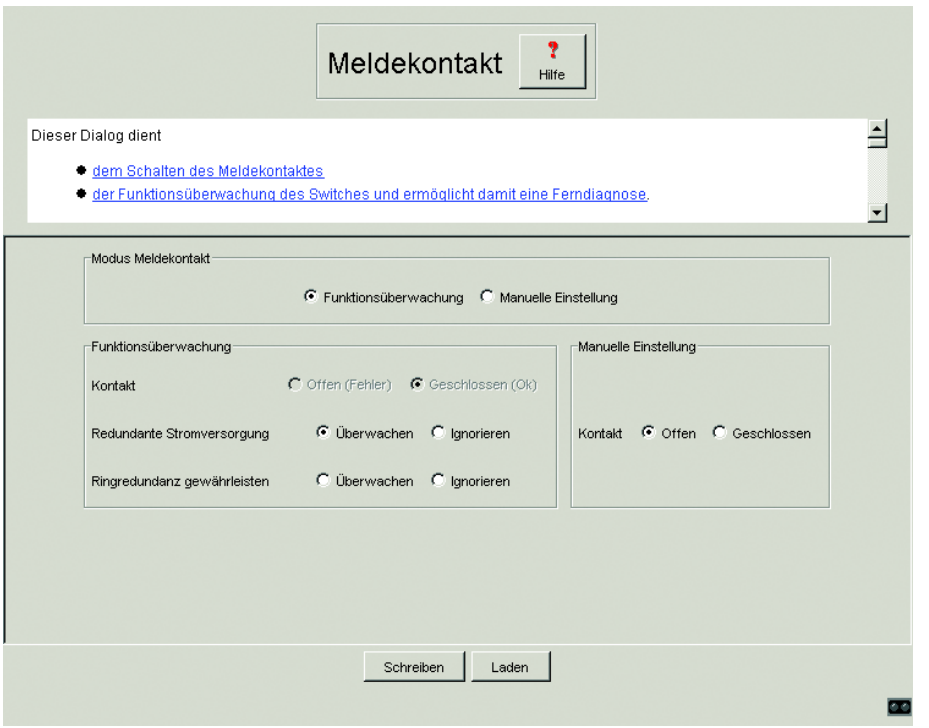


Abb. 62: Dialog Meldekontakt

5.3.4 Zeit

Dieser Dialog bietet Ihnen die Möglichkeit, unabhängig vom gewählten Zeitsynchronisationsprotokoll zeitbezogene Einstellungen vorzunehmen.

- Die „IEEE 1588-Zeit“ zeigt die mittels PTP empfangene Uhrzeit an.
  Die „SNTP-Zeit" zeigt die Uhrzeit bezogen auf die koordinierte Weltzeitmessung UTC an.
  Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.
- Die „Systemzeit" übernimmt die „IEEE 1588 / SNTP-Zeit" unter Berücksichtigung der lokalen Zeitdifferenz zur „IEEE 1588 / SNTP-Zeit".
  „Systemzeit" = „IEEE 1588 / SNTP-Zeit" + „Lokaler Offset"
- „Quelle der Zeit“ zeigt den Ursprung der folgenden Zeitangabe an. Der Switch wählt automatisch die Quelle mit der höchsten Genauigkeit.

☐ Mit „Setze Zeit vom PC“ übernimmt der Switch die Zeit des PCs als Systemzeit und berechnet mit der lokalen Zeitdifferenz die IEEE 1588 / SNTP-Zeit.
„IEEE 1588 / SNTP-Zeit" = „Systemzeit" - „Lokaler Offset"

☐ „Lokale Offset" dient zur Anzeige/Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der „IEEE 1588 / SNTP-Zeit".
Mit „Setze Offset vom PC" ermittelt der Agent die Zeitzone auf Ihrem PC und berechnet daraus die lokale Zeitdifferenz.

Hinweis: Passen Sie in Zeitzonen mit Sommer-/Winterzeit den lokalen Offset bei der Zeitumstellung an. Der Switch kann die SNTP-Server-IP-Adresse und den lokalen Offset auch von einem DHCP-Server beziehen.

Interaktion von PTP und SNTP

Laut PTP und SNTP können beide Protokolle parallel in einem Netz existieren. Da aber beide Protokolle die Systemzeit des Gerätes beeinflussen, können Situationen auftreten, in denen beide Protokolle konkurieren.

Hinweis: In einer SNTP-Kaskade (siehe Abb. 45) darf höchstens ein Gerät mit eingeschalteter PTP-Funktion und eingeschalteter SNTP-Funktion existieren.

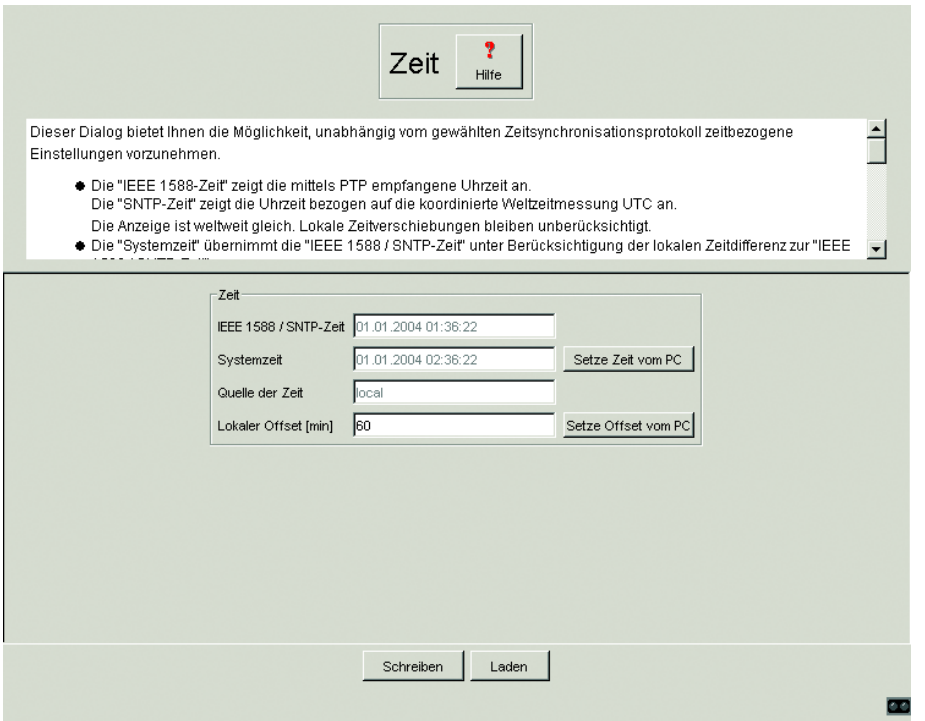


Abb. 63: Zeit

5.3.5 SNTP

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren. Der Switch unterstützt die SNTP-Server- und die SNTP-Client-Funktion. Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Der SNTP-Client bezieht die UTC.

Konfiguration SNTP-Client und -Server

☐ In diesem Rahmen schalten Sie die SNTP-Funktion ein/aus.
Im ausgeschalteten Zustand sendet der SNTP-Server keine SNTP-Pakete und beantwortet keine SNTP-Anfragen.
Der SNTP-Client sendet keine SNTP-Anforderungen und wertet keine SNTP-Broadcast-/Multicast-Pakete aus.

SNTP-Status

► Die „Statusmeldung“ zeigt Zustände an, wie z.B. „Server nicht erreichbar“.

Konfiguration SNTP-Server

☐ In „Ziel-Adresse“ geben Sie die IP-Adresse an, an welche der SNTP-Server auf dem Switch die SNTP-Pakete schickt.

IP-Zieladresse	zyklisch SNTP-Paket versenden an
0.0.0.0	niemanden
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Tab. 11: Zyklisches Versenden von SNTP-Paketen

☐ In „VLAN ID“ geben Sie das VLAN an, in welches der Switch zyklische SNTP-Pakete verschicken darf.

☐ In „Sendeintervall“ geben Sie den Zeitabstand an, in welchem der Switch SNTP-Pakete verschickt (gültige Werte: 1 Sekunde bis 3600 Sekunden, Lieferzustand: 120 Sekunden).

Konfiguration SNTP-Client

☐ In „Externe Server Adresse“ geben Sie die IP-Adresse des SNTP-Servers ein, von dem der Switch zyklisch die Systemzeit anfordert.

☐ In „Redundante Server Adresse“ geben Sie die IP-Adresse des SNTP-Servers ein, von dem der Switch zyklisch die Systemzeit anfordert, wenn er 0,5 Sekunden nach einer Anforderung keine Antwort vom „Externen Server Adresse“ erhält.

Hinweis: Wenn Sie von einer externen/redundanten Server-Adresse die Systemzeit beziehen, dann akzeptieren Sie keine SNTP-Broadcasts (siehe unten). Sonst können Sie nie unterscheiden, ob der Switch die Zeit des eingetragenen Servers oder die eines SNTP-Broadcast-Paketes anzeigt.

- ☐ In „Anforderungsintervall“ geben Sie den Zeitabstand ein, in dem der Switch SNTP-Pakete anfordert (gültige Werte: 1 Sekunde bis 3600 Sekunden, Lieferzustand: 30 Sekunden).
- ☐ Mit „SNTP Broadcasts akzeptieren“ übernimmt der Switch die Systemzeit aus SNTP-Broadcast-/Multicast-Paketen, die er empfängt.

Hinweis: Für eine möglichst genaue Systemzeitverteilung vermeiden Sie im Signalpfad zwischen SNTP-Server und SNTP-Client Netzwerkkomponenten (Router, Switches, Hubs), die kein SNTP unterstützen.

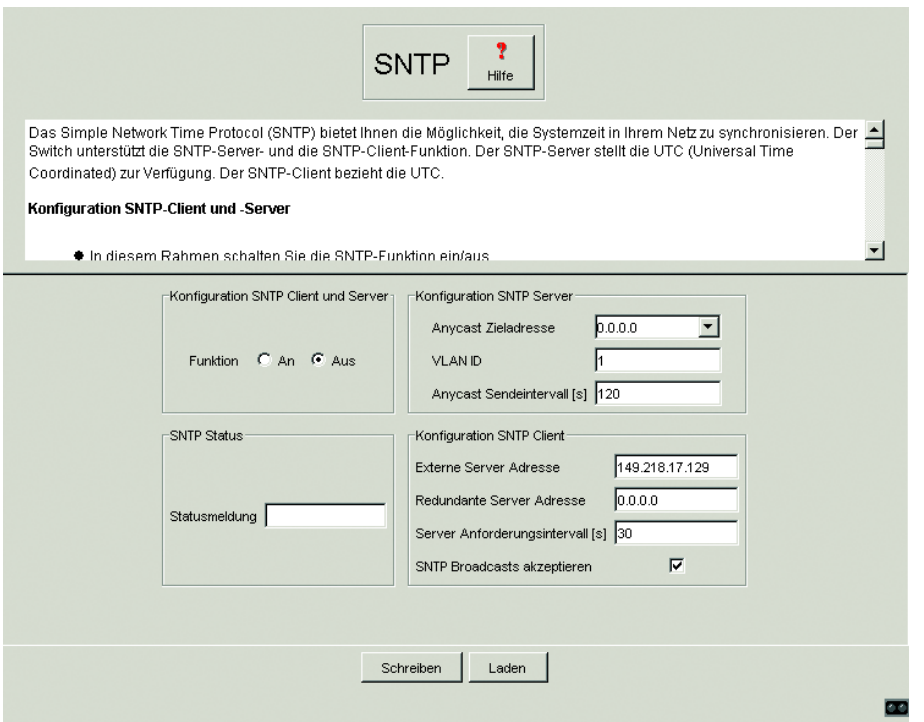


Abb. 64: Dialog SNTP

5.3.6 PTP

Der Standard IEEE 1588 beschreibt mit dem Precision Time Protocol (PTP) ein Verfahren, das ausgehend von einer genauesten Uhr die präzise Synchronisation aller Uhren in einem LAN ermöglicht (siehe "IEEE 1588 – Precison Time Protocol" auf Seite 130).

PTP Global

Dieser Dialog bietet Ihnen die Möglichkeit, Grundeinstellungen für das Precision Time Protocol vorzunehmen.

- Funktion
  In diesem Rahmen schalten Sie PTP ein/aus.

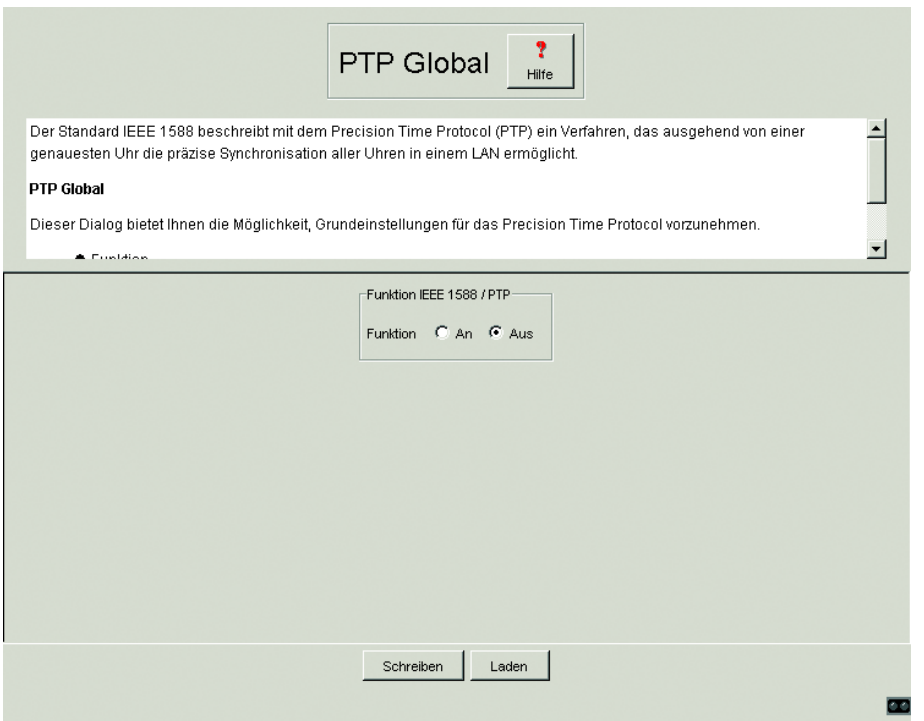


Abb. 65: PTP-Global

5.3.7 Netzparameter festlegen

Mit diesem Dialog legen Sie fest, aus welcher Quelle der Switch seine Netzparameter nach dem Start erhält, weisen Netzparameter und VLAN ID zu.

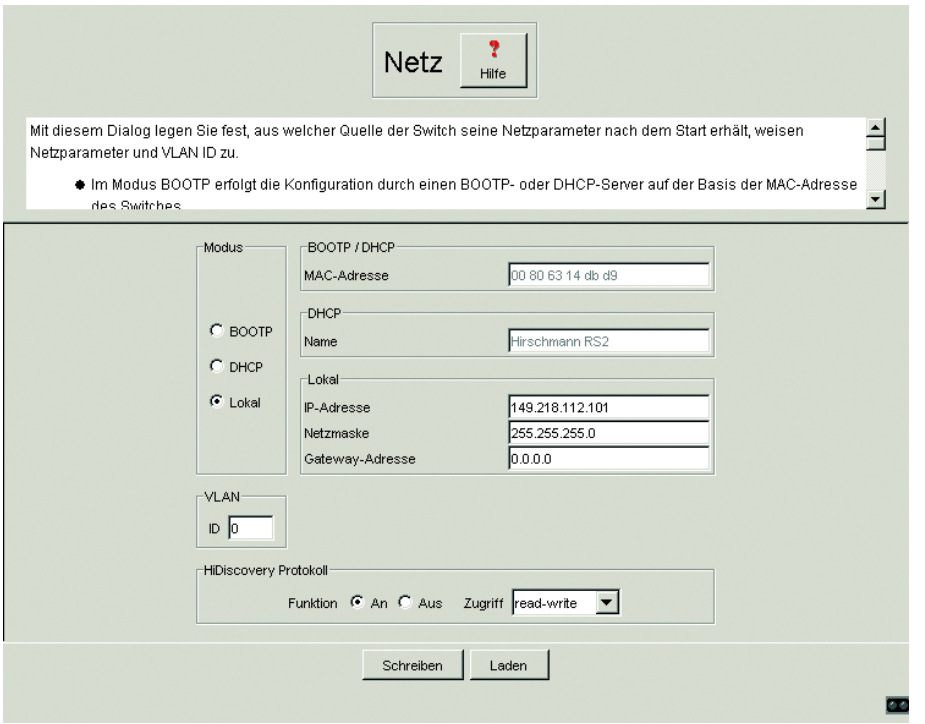


Abb. 66: Dialog Netzparameter

☐ Geben Sie unter „Modus“ ein, woher der RS2-../.. seine IP-Parameter bezieht:

- Im Modus BOOTP erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf der Basis der MAC-Adresse des Switches (siehe Seite 55).
- Im Modus DHCP erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Switches (siehe Seite 59).
- Im Modus lokal werden die Netzparameter aus dem Speicher des Switches verwendet.

- ☐ Geben Sie entsprechend des gewählten Modus rechts die Parameter ein.
- ☐ Den für das DHCP-Protokoll relevanten Namen geben Sie im Dialog "System" auf Seite 151 in der Zeile "Name" ein.
- ☐ Der Rahmen „VLAN ID“ bietet Ihnen die Möglichkeit, dem Agenten ein VLAN zuzuweisen. Mit dem Eintrag 0 ist der Agent aus jedem VLAN erreichbar.
- ☐ Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Switch an Hand seiner MAC-Adresse eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der mitgelieferten HiDiscovery-Software (siehe "System-Konfiguration via HiDiscovery" auf Seite 53) dem Switch eine IP-Adresse übertragen wollen (Lieferzustand: aktiv).

5.3.8 Paßwort

Dieser Dialog bietet Ihnen die Möglichkeit, das Lese- und das Schreib/Lese-Paßwort für den Zugriff auf den Switch zu ändern.

☐ Das Web-based Interface und das User Interface kommunizieren über SNMP Version 3. Wählen Sie „SNMPv1/2c ein“, um mit früheren Versionen von SNMP kommunizieren zu können.

☐ Wählen Sie „Paßwort SNMPv3 von SNMPv1/2c übernehmen“, wenn SNMP Version 3 das unverschlüsselte Paßwort von SNMP Version 1/2c übernehmen soll. Aus Sicherheitsgründen verschlüsselt SNMP Version 3 das Paßwort. Mit der Einstellung „SNMPv1/2c ein“ wird das Paßwort wieder lesbar!

Abb. 67: Dialog Paßwort

Wichtig: Wenn Sie kein Paßwort mit der Berechtigung „read-write“ kennen, haben Sie keine Möglichkeit auf den Switch schreibend zuzugreifen!

Hinweis: Um nach dem Ändern des Paßwortes für den Schreibzugriff auf den Switch zugreifen zu können, starten Sie das Web-Interface neu.

Hinweis: Aus Sicherheitsgründen werden die Paßwörter nicht angezeigt. Notieren Sie sich jede Änderung! Ohne gültiges Paßwort können Sie nicht auf den Switch zugreifen!

Hinweis: Verwenden Sie bei SNMP Version 3 mehr als 8 Zeichen für das Paßwort, da viele Anwendungen keine kürzeren Paßwörter akzeptieren.

Die Sperre des Zugriffs über einen Web-Browser erfolgt im Dialog "Zugriff WEB" auf Seite 174.
Die Beschränkung des Zugriffs auf IP-Adreßebene erfolgt im Dialog "Zugriff für IP-Adressen" auf Seite 175.

Das Web-based Interface bietet bis zu 4 unterschiedliche Paßwörter an:
- Lesepaßwort SNMP Version 3.
- Schreib-/Lesepaßwort SNMP Version 3. Dieses ist identisch mit dem Paßwort im User Interface (siehe "Password" auf Seite 290).
- Lesepaßwort SNMP Version 1/2c.
- Schreib-/Lesepaßwort SNMP Version 1/2c.

Aus Sicherheitsgründen können Lesepaßwort und Schreib-/Lesepaßwort nicht identisch sein.

☐ Wählen Sie zunächst, welches Paßwort Sie ändern wollen.

☐ Geben Sie in der Zeile „Altes Paßwort“ das alte Paßwort ein.

☐ Geben Sie in der Zeile „Neues Paßwort“ das neue Paßwort ein.

☐ Wiederholen Sie das neue Paßwort in der Zeile „bitte nochmals eingeben“.

Beachten Sie die Groß/Kleinschreibung.

☐ „Datenverschlüsselung“ sorgt für die Verschlüsselung der Daten des Web-based Managements, die zwischen Ihrem PC und dem Switch mit SNMP V3 übertragen werden. Sie können „Datenverschlüsselung“ für den Zugriff mit Lese- und Schreib-/Lesepaßwort unterschiedlich einstellen.

5.3.9 Zugriff WEB

Dieser Dialog bietet Ihnen die Möglichkeit, den Web-Server auf dem Switch abzuschalten. Nach dem Abschalten des Web-Servers ist ein Zugriff auf den Switch über einen Web-Browser nicht mehr möglich.

Hinweis: Über das User-Interface läßt sich der Web-Server wieder aktivieren.

Abb. 68: Dialog Zugriff WEB

5.3.10 Zugriff für IP-Adressen

Dieser Dialog bietet Ihnen die Möglichkeit, festzulegen, über welche IP-Adressen auf den Switch zugegriffen werden darf und welche Art von Paßwörtern dabei zu benutzen sind.

- In der Spalte „Index“ ist die laufende Nummer eingetragen, auf die sich die Zugriffsbeschränkung bezieht.
- In der Spalte „IP-address“ tragen Sie die IP-Adresse ein, die auf den Switch zugreifen darf. Kein Eintrag oder der Eintrag „0.0.0.0“ in diesem Feld erlaubt den Zugriff von Rechnern mit beliebigen IP-Adressen auf diesen Switch. In diesem Fall ist das Paßwort der einzige Zugriffsschutz.
- In der Spalte „Name“ können Sie für den Rechner mit dieser IP-Adresse einen beliebigen Namen eintragen.
- In der Spalte „Paßwort“ legen Sie fest, ob dieser Rechner mit dem Lese- oder mit dem Schreib/Lese-Paßwort zugreifen darf.
- In der Spalte „State“ kreuzen Sie die Einträge an, die bei der Zugriffskontrolle berücksichtigt werden sollen.

Wichtig: Diese Einstellungen gelten für SNMPv1/2c. Da das Web-based Interface mit SNMPv3 kommuniziert, erfolgt der Zugriff auf das Web-based Interface unabhängig von der IP-Adresse.

Wichtig: Ist keine Zeile angekreuzt, dann gibt es keine Zugriffsbeschränkung bezüglich der IP-Adressen!

Wichtig: Wenn Sie eine Zeile oder mehrere Zeilen ankreuzen, dann achten Sie darauf, daß mindestens eine Zeile mit Schreib/Lese-Paßwort angekreuzt ist. So erhalten Sie sich den Schreibzugriff auf den Switch.

Hinweis: Einträge in schraffierten Tabellenzeilen wurden durch andere Managementsysteme wie z.B. HiVision vorgenommen und können mit dem Web-based Management nicht verändert werden.

Abb. 69: Dialog Zugriff für IP-Adressen

5.3.11 Alarme (Traps) Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarme gesendet werden sollen.

- In der Spalte „IP-Adresse“ geben Sie die IP-Adresse des Empfängers an, an den die Traps geschickt werden sollen.
- In der Spalte „Name“ können Sie für jeden Empfänger einen beliebigen Namen eintragen.
- In der Spalte „Status“ kreuzen Sie die Einträge an, die beim Versenden von Traps berücksichtigt werden sollen.

Hinweis: Einträge in schraffierten Tabellenzeilen wurden durch andere Managementsysteme wie z.B. HiVision vorgenommen und können von hier aus nicht verändert werden.

Die auswählbaren Ereignisse haben folgende Bedeutung:

- Cold Start: Der Switch wurde eingeschaltet.
- Link Down: An einem Port des Switches wurde die Verbindung zu dem dort angeschlossenen Gerät unterbrochen.
- Link up: An einem Port des Switches wurde eine Verbindung mit einem dort angeschlossenen Gerät hergestellt.
- Authentication: Der Switch hat einen unerlaubten Zugriff zurückgewiesen (siehe Dialog Zugriff für IP-Adressen auf Seite 175 und Portsicherheit auf Seite 220).
- Bridge: Obwohl an einem Port die BPDU-Guard-Funktion aktiviert ist, wurde eine BPDU empfangen.
- Port Security: An einem Port wurde ein Datenpaket von einem nicht erlaubten Endgerät empfangen (siehe Dialog Portsicherheit auf Seite 220).
- Chassis: faßt die folgenden Ereignisse zusammen:
  - Power Supply: Der Status einer Versorgungsspannung hat sich geändert (siehe Dialog System).
  - Signalling Relay: Der Status des Meldekontakts hat sich geändert.
  - Stand-by: Der Status des Redundanz Managers hat sich geändert (siehe Dialog HIPER-Ring "Konfiguration der HIPER-Ring-Funktion" auf Seite 210).
  - AutoConfigAdapter: Der AutoConfiguration Adapter ACA wurde hinzugefügt oder entfernt.

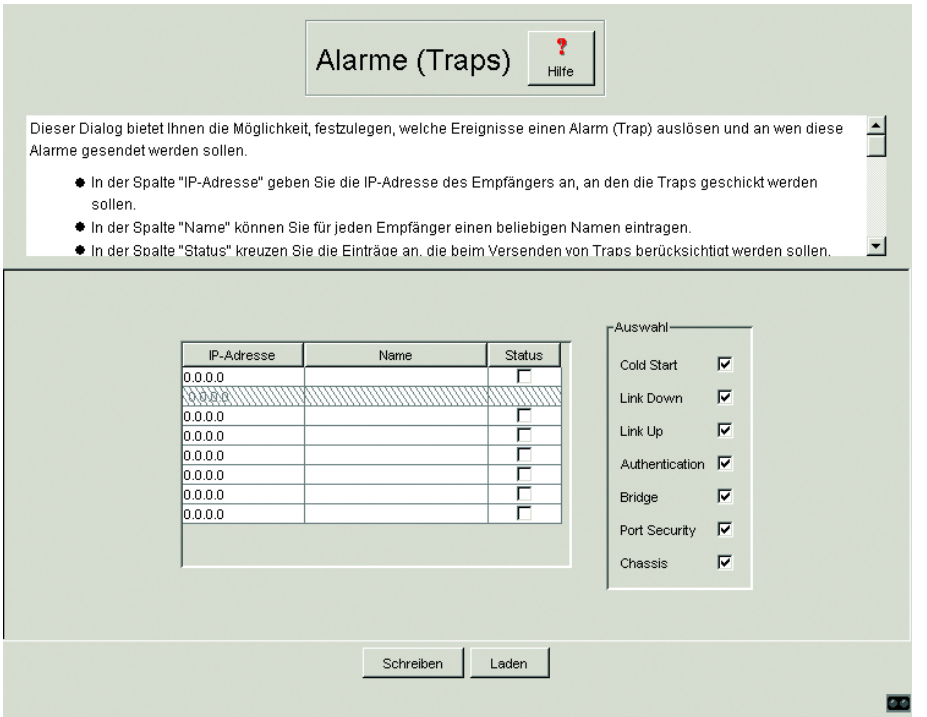


Abb. 70: Dialog Alarme

5.3.12 Neustart des Switches

Dieser Dialog bietet Ihnen die Möglichkeit,

- einen Neustart des Switches auszulösen,
- die MAC-Adreßtabelle zurückzusetzen,
- die Portzähler zurückzusetzen,
- die IP-Zähler zurückzusetzen,
- die Protokollzähler zurückzusetzen,
- die Logdatei zu löschen.

Hinweis: Während des Neustarts überträgt der Switch kurzfristig keine Daten und ist nicht durch das Web-based-Interface oder andere Managementsysteme wie z.B. HiVision erreichbar.

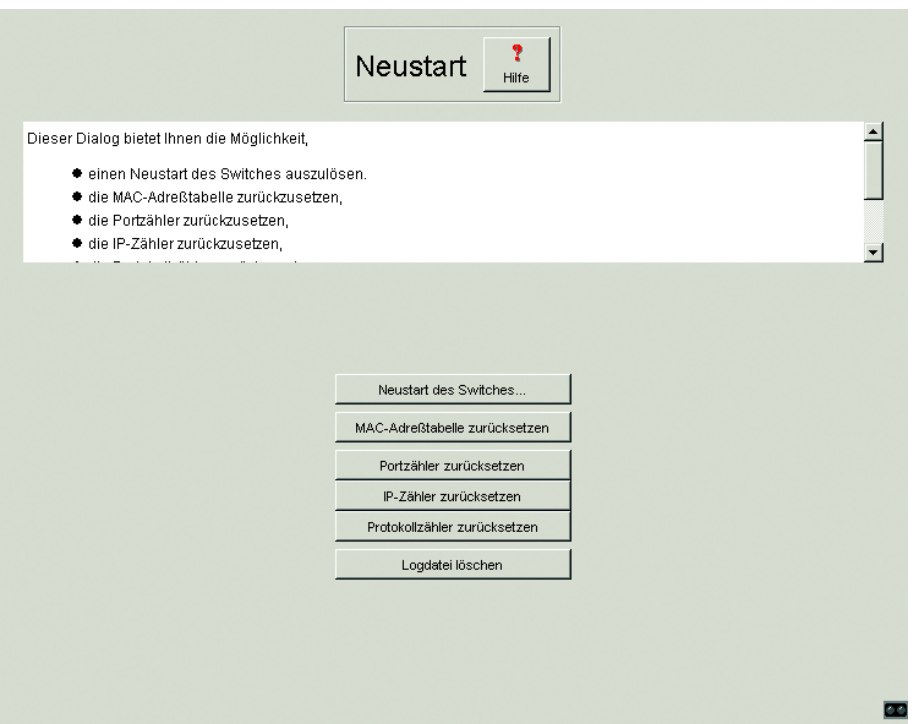


Abb. 71: Dialog Neustart

5.4 Ports

Das Menü Ports bietet die:

- Port-Konfigurationstabelle und die
- Port-Statistiktabelle.

5.4.1 Port-Konfigurationstabelle

Diese Tabelle bietet Ihnen die Möglichkeit, jeden Port des Switches zu konfigurieren.

- In der Spalte „Name“ haben Sie die Möglichkeit für jeden Port einen beliebigen Namen einzutragen.
- In der Spalte „Port an“ haben Sie die Möglichkeit, den Port durch ankreuzen einzuschalten.
- In der Spalte „Flußkontolle an“ legen Sie durch Ankreuzen fest, daß an diesem Port Flußkontrolle aktiv ist. Aktivieren Sie hierzu auch den globalen Schalter "Flußkontrolle" im Dialog "Switch-Grunddaten" auf Seite 185.
- In der Spalte „Link Alarm Meldekontakt“ legen Sie durch Ankreuzen fest, daß beim Auftreten eines Link Alarms der Meldekontakt geöffnet wird.
- In der Spalte „Automatische Konfiguration“ aktivieren Sie die automatische Auswahl der Betriebsart eines Ports, indem Sie das zugehörige Feld ankreuzen. Nach dem Einschalten der automatischen Konfiguration vergehen einige Sekunden, bis die Betriebsart eingestellt ist.
- In der Spalte „Manuelle Konfiguration“ stellen Sie die Betriebsart an diesem Port ein. Die möglichen Betriebsarten sind vom Medienmodul abhängig. Mögliche Betriebsarten sind:
  - 10 Mbit/s Halbduplex (HDX),
  - 10 Mbit/s Vollduplex (FDX),
  - 100 Mbit/s HDX und
  - 100 Mbit/s FDX.
- In der Spalte „Port Priorität“ haben Sie die Möglichkeit, die Priorität (im Bereich von 0 bis 7, Voreinstellung 0) festzulegen, mit welcher der Switch Datenpakete vermittelt, die er an diesem Port ohne VLAN-Tag empfängt.

Hinweis: Die aktive automatische Konfiguration hat Vorrang vor der manuellen Konfiguration.

Hinweis: Für die Ringports (siehe "Redundante Ringstruktur – HIPER-Ring" auf Seite 126) sind folgende Einstellungen erforderlich:
– 100 Mbit/s
– Vollduplex
– Autonegotiation aus
– Port an.

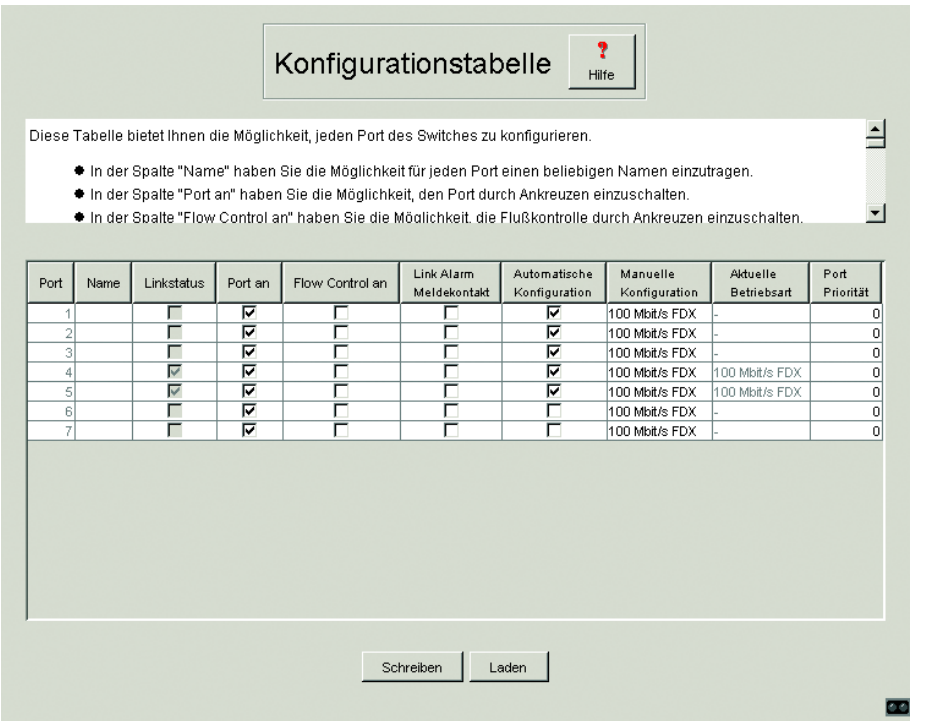


Abb. 72: Dialog Port-Konfigurationstabelle

5.4.2 Port-Statistiktabelle

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Nach einem Neustart beginnen sämtliche Ereigniszähler wieder bei Null. Die Zähler summieren die Ereignisse aus Sende- und Empfangsrichtung.

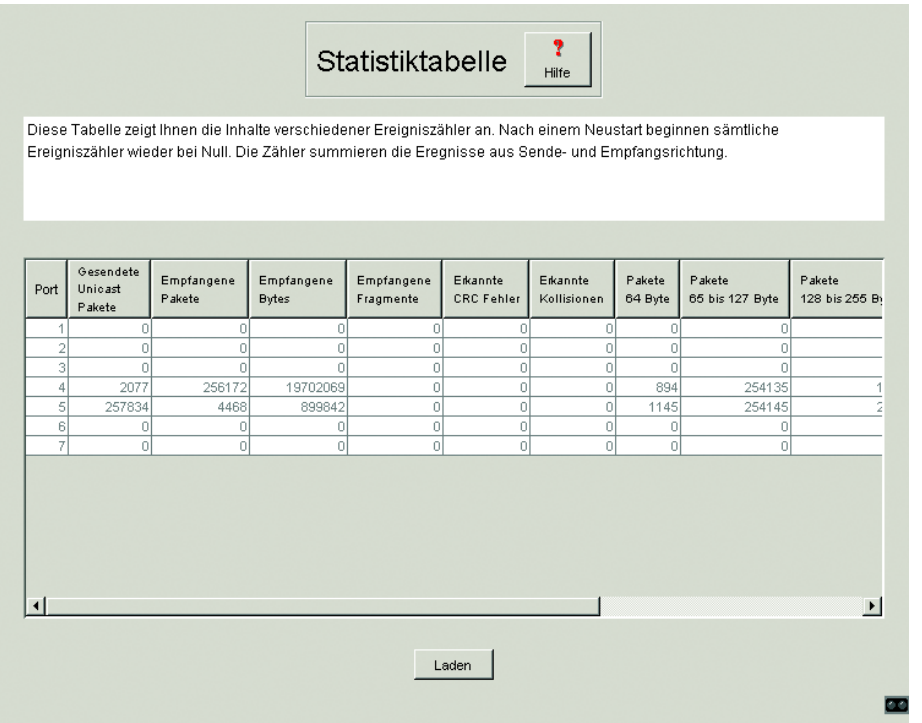


Abb. 73: Dialog Port-Statistiktabelle

5.5 Switching

Das Menü Switching bietet die:

- Switch-Grunddaten,
- Filtertabelle und die
- Konfiguration des GMRP / IGMP.

5.5.1 Switch-Grunddaten

Dieser Dialog dient zur Anzeige der Switch-Grunddaten und zur Eingabe übergreifender Einstellungen. Zu den übergreifenden Einstellungen zählen:

- Eingabe der Aging Time für alle dynamischen Einträge im Bereich von 10 bis 400 Sekunden (Einheit: 1 Sekunde, Voreinstellung: 30).
  Im Zusammenhang mit der Router-Redundanz (siehe MACH 3000) wählen Sie die Zeit größer/gleich 30 Sekunden.
- Ausschalten/Zulassen der Flußkontrolle an allen in der Portkonfigurationstabelle markierten Ports des Switches.

5.5.2 Filtertabelle

Die Filtertabelle dient zur Anzeige und Bearbeitung von Filtern. Jede Zeile stellt einen Filter dar. Filter legen die Vermittlungsweise von Datenpaketen fest. Sie werden entweder automatisch vom Switch (Status learned) oder manuell angelegt. Datenpakete deren Zieladresse in der Tabelle eingetragen ist, werden vom Empfangsport an die in der Tabelle markierten Ports vermittelt. Datenpakete, deren Zieladresse nicht in der Tabelle enthalten ist, werden vom Empfangsport an alle anderen Ports vermittelt. Im Dialog „Filter anlegen“ (siehe Bedientaste unten) haben Sie die Möglichkeit, neue Filter zu erzeugen. Folgende Stati sind möglich:

- `learned`: Das Filter wurde vom Switch automatisch angelegt.
- `Invalid`: Mit diesem Status löschen Sie ein manuell angelegtes Filter.
- `permanent`: Das Filter wird im Switch oder auf dem URL dauerhaft gespeichert (siehe "Start-Konfiguration festlegen" auf Seite 159).
- `deleteOnReset`: Das Filter wird bei einem Neustart des Switches gelöscht.
- `gmrp`: Das Filter wurde durch GMRP angelegt.
- `gmrp/permanent`: GMRP hat dem Filter, nachdem es durch den Administrator angelegt worden ist, weitere Portmarken hinzugefügt. Die durch das GMRP hinzugefügten Portmarken werden bei einem Neustart gelöscht.
- `gmrp/deleteOnReset`: Das Filter wurde vom Administrator angelegt und vom GMRP mit weiteren Portmarken ergänzt. Das Filter wird bei einem Neustart des Switches gelöscht.
- `igmp`: Das Filter wurde durch IGMP angelegt.

Im Dialog „Anlegen“ (siehe Bedientaste unten) haben Sie die Möglichkeit, neue Filter zu erzeugen.

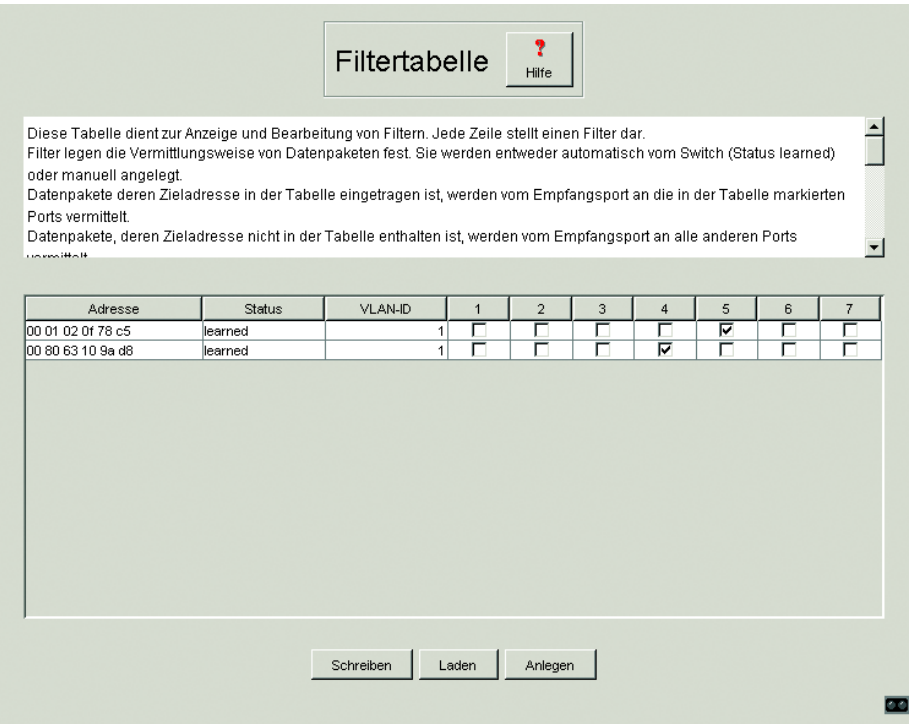


Abb. 74: Dialog Filtertabelle

Hinweis: Bei aktivem Redundanz Manager sind keine permanenten Unicast-Einträge möglich.

Hinweis: Die Filtertabelle bietet Ihnen die Möglichkeit, bis zu 56 Filter für Multicast-Adressen zu erzeugen.

5.5.3 Multicast

Das IGMP Internet Group Management Protocol beschreibt die Verteilung von Multicast-Informationen zwischen Routern und Endgeräten auf Layer 3-Ebene. Router mit aktiver IGMP-Funktion verschicken periodisch Anfragen (Query), um zu erfahren, welche IP-Multicast-Gruppen-Mitglieder im LAN angeschlossen sind (siehe "IGMP-Snooping" auf Seite 106).

Das GARP Multicast Registration Protocol (GMRP) beschreibt die Verteilung von Datenpaketen mit einer Multicast-Adresse als Zieladresse. Geräte, die Datenpakete mit einer Multicast-Adresse als Zieladresse empfangen wollen, veranlassen mit Hilfe des GMRPs die Registrierung der Multicast-Adresse. Registrieren heißt für einen Switch, die Multicast-Adresse in die Filtertabelle eintragen. Beim Eintrag einer Multicast-Adresse in die Filtertabelle, sendet der Switch diese Information in einem GMRP-Paket an allen Ports. Angeschlossene Switches lernen dadurch, diese Muticast-Adresse an diesen Switch weiterzuleiten. Das GMRP ermöglicht, daß Pakete mit einer Multicast-Adresse im Zieladreßfeld an den eingetragenen Ports vermittelt werden. Die anderen Ports bleiben von diesen Paketen unbelastet. Datenpakete mit nicht registrierten Multicast-Adressen sendet ein Switch an allen Ports.

Globales GMRP	aus
GMRP pro Port	ein
Vermittlung pro Port	selektiv

Tab. 12: Grundeinstellung des GMRP

Globale Einstellungen

„IGMP Snooping" bietet Ihnen die Möglichkeit, IGMP Snooping für den gesamten Switch global einzuschalten.
Ist IGMP Snooping ausgeschaltet, dann:

- wertet der Switch empfangene Query- und Report-Pakete nicht aus und
- sendet (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an allen Ports.

„GMRP“ bietet Ihnen die Möglichkeit, GMRP für den gesamten Switch global einzuschalten.
Ist GMRP ausgeschaltet, dann

- generiert der Switch keine GMRP-Pakete,
- wertet empfangene GMRP-Pakete nicht aus, verwirft sie und
- sendet (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an allen Ports.

Für empfangene GMRP-Pakete ist der Switch unabhängig von der GMRP-Einstellung transparent.

„inaktiv“ schaltet GMRP und IGMP Snooping aus.

IGMP-Querier

„IGMP Querier aktiv“ bietet Ihnen die Möglichkeit, die Query-Funktion ein-/auszuschalten.
Die Protokoll-Auswahlfelder bieten Ihnen die Möglichkeit, die IGMP-Version 1 oder 2 auszuwählen.

„Querier Transmit Interval“ bietet Ihnen die Möglichkeit, festzulegen, wie groß die Zeitabstände (in Sekunden) zwischen dem Versenden von IGMP-Query-Anfragen ist.

IGMP-Einstellungen

„Aging Intervall“ bietet Ihnen die Möglichkeit, festzulegen, nach welcher Zeit (in Sekunden) über IGMP Snooping gelernte Einträge in der Filtertabelle altern und dann gelöscht werden.

IGMP Forward all pro Port

Diese Tabellenspalte bietet Ihnen die Möglichkeit, bei eingeschaltetem globalem IGMP Snooping die IGMP Snooping-Funktion „Forward All“ ein-/auszuschalten. Mit der Einstellung "Forward All" vermittelt der Switch an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladreßfeld.

Hinweis: Sind mehrere Router an ein Subnetz angeschlossen, dann verwenden Sie IGMP Version 1, damit alle Router alle IGMP-Reports erhalten.

Hinweis: Wenn Sie IGMP Version 1 in einem Subnetz verwenden, dann verwenden Sie IGMP Version 1 auch im gesamten Netz.

Static Query Port

IGMP-Report-Nachrichten vermittelt ein Switch an die Ports, an denen er IGMP-Anfragen empfängt. Diese Tabellenspalte bietet Ihnen die Möglichkeit, IGMP-Report-Nachrichten auch an anderen ausgewählten Ports zu vermitteln.

GMRP pro Port

Diese Tabellenspalte bietet Ihnen die Möglichkeit, bei eingeschaltetem globalem GMRP das GMRP je Port ein-/auszuschalten. Das Ausschalten des GMRPs an einem Port verhindert Registrierungen für diesen Port und das Weiterleiten von GMRP-Paketen an diesem Port.

GMRP Service Requirements pro Port

Die GMRP Service Requirements des GMRP-Standards beschreiben die GMRP-Dienstanforderung durch das Endgerät an das gesamte Netz.

- Mit der Einstellung „selektiv“ (GMRP-Standard-Angabe: forward all unregistered groups) vermittelt der Switch an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladreßfeld,
  – die für diesen Port in der Filtertabelle eingetragen ist
  oder
  – für die kein Eintrag in der Filtertabelle existiert.
- Mit der Einstellung „alle“ (GMRP-Standard-Angabe: forward all groups) vermittelt der Switch an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladreßfeld.

Hinweis: Ist der Switch in einen HIPER-Ring eingebunden, dann gewähren Sie bei einer Ringunterbrechung eine schnelle Rekonfiguration des Netzes für Datenpakete mit registrierten Multicast-Zieladressen durch:

- Einschalten des GMRPs an den Ringports und global und
- Wahl der Vermittlungsart „alle“ pro Port an den Ringports.

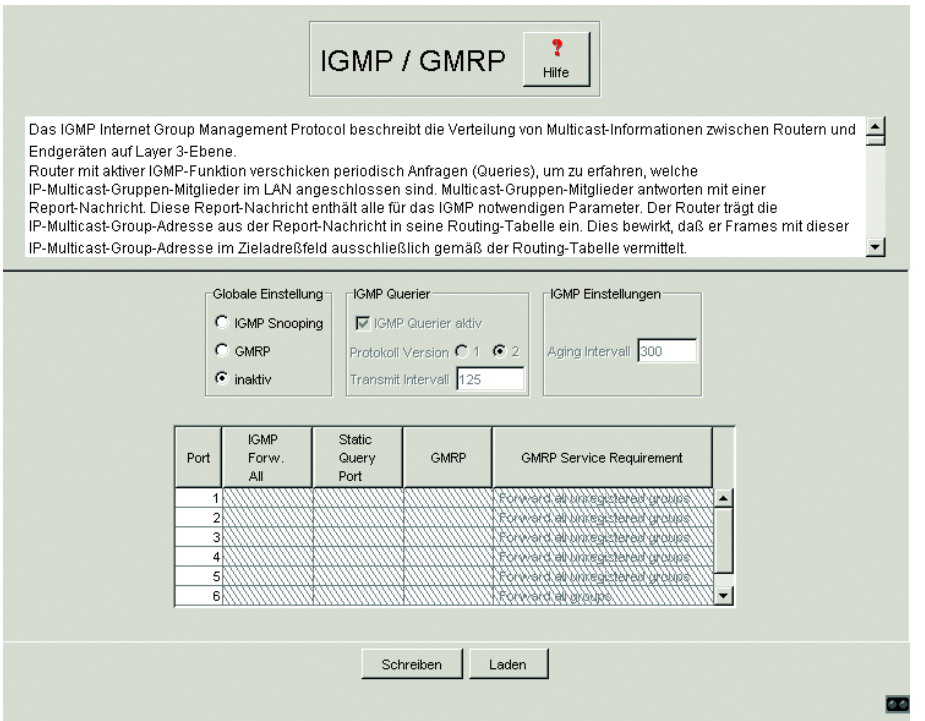


Abb. 75: Dialog IGMP/GMRP

5.5.4 Rapid Spanning Tree

Der Rapid Spanning Tree Algorithmus (RSTP) reduziert jegliche Topologie eines Netzes, das mit Brücken verbunden ist, auf eine einzige Baumstruktur. Die Wurzelbrücke bildet den Ursprung einer Baumstruktur. Eventuelle Ringstrukturen werden nach vorgegebenen Regeln aufgetrennt. Bei einer Pfadunterbrechung hebt der Algorithmus die Auftrennung zur Aufrechterhaltung des Datenverkehrs wieder auf. Dies erlaubt redundante Verbindungen zur Erhöhung der Datensicherheit (siehe "Spanning Tree Algorithmus" auf Seite 107).

Der Aufbau des Baumes hängt von den Wurzelpfadkosten ab.

- Die Struktur wird so gewählt, daß die minimalen Pfadkosten zwischen jeder einzelnen Brücke zur Wurzelbrücke entstehen.
- Bei mehreren Pfaden mit gleichen Wurzelpfadkosten entscheidet die Priorität der Brückenidentifikation der Brücken, die an einen dieser Pfade angeschlossen ist, welche Brücke blockiert.

Hinweis: Der niedrigste numerische Wert kennzeichnet die höchste Priorität.

RSTP ist kompatibel zum herkömmlichen STP. Die Vorteile der schnelleren Rekonfiguration beim RSTP zwischen zwei Brücken gehen jedoch verloren, wenn eine der beiden Brücke nur das STP-Protokoll einsetzt.

Globale Einstellungen

Diese Einstellungen beziehen sich auf den Switch.

Die BPDU-Guard-Funktion überwacht den Empfang von BPDUs.
Mit dem Einschalten dieser Funktion (Lieferzustand: Global ausgeschaltet) überwacht der Switch den Empfang von BPDUs an den Ports, an denen diese Funktion im RSTP-Portdialog aktiviert ist.BPDU-Gard ist wirksam an Edge-Ports, deren `Soll Edge Port` (siehe Tab. 14 auf Seite 194) gleich `true` ist (= Lieferzustand).
Beim Empfang einer BPDU schaltet die BPDU-Guard-Funktion den Port ab und kann eine Alarmmeldung (siehe "Auflistung der SNMP-Traps" auf Seite 139) senden.
Mit dem Ausschalten dieser Funktion überwacht der Switch an keinem Port den Empfang von BPDUs.

Diese Funktion bietet Ihnen eine einfache Möglichkeit eine Fehlkonfiguration an diesem Port zu erkennen.

In der Regel gibt der Administrator die einzustellenden Werte für „Hello Time“, „Forward Delay“ und „Max. Age“ in der Wurzelbrücke ein. Die Wurzelbrücke überträgt diese Daten dann an die anderen Brücken weiter. Die von der Wurzelbrücke erhaltenen Daten zeigt der Dialog in der linken Spalte an. In der rechten Spalte geben Sie die Werte ein, die gelten sollen, wenn diese Brücke zur Wurzelbrücke wird.

Hinweis: Da HIPER-Ring und STP unterschiedliche Redundanzkonzepte verfolgen, verhindert die aktive RM-Funktion das Einschalten des STP.

Die Zeiteingaben im Dialog Global haben die Einheit 10 ms.
Beispiel: Max Age = 2000 entspricht 20 Sekunden.

Variable	Bedeutung	Mögliche Werte	Lieferzustand
Priorität	Priorität und MAC-Adresse zusammen bilden die Brückenidentifikation.	0 < n*4096 < 61440	32768
Hello Time	Die Brücke sendet Konfigurationsmeldungen (Configuration Bridge Protocol Data Units, CBPDU), wenn sie die Wurzelbrücke ist, oder beim Versuch, Wurzelbrücke zu werden. HelloTime ist die Zeit in hundertstel Sekunden zwischen dem Senden zweier Konfigurationsmeldungen (Configuration Bridge Protocol Data Units, CBPDU). Dieses ist der aktuelle Wert, den die Brücke gerade benutzt.	100 < n*100 < 1000	200
Max Age	Nach Ablauf von Max. Age wird eine BPDU ungültig und verworfen.	600 - 4000	200
Forward Delay	Das Zustandsdiagramm des Spanning Tree Protokoll kennt vier Zustände: blockieren, hören, lernen und normal. Beim Wechsel von einem Zustand zum anderen vergeht eine gewisse Zeit. Diese Zeit wird in hundertstel Sekunden gemessen und kontrolliert wie schnell der Wechsel vonstatten geht. Dieses ist der aktuelle Wert, den die Brücke gerade benutzt. Der Zustandswechsel von normal nach blockieren erfolgt ohne Zeitverzögerung.	400 - 3000	1500

Tab. 13: Globale STP/RSTP-Einstellungen

Porteinstellungen

Diese Einstellungen beziehen sich auf jeden einzelnen Port.

Variable	Bedeutung	Mögliche Werte	Lieferzustand
STP Status	STP/RSTP an diesem Port ein-/ausschalten. Schalten Sie beim Anschluß eines Endgerätes STP aus, um unnötige Wartezeiten zu verhindern.	enable, disable	enable
Priorität	Die Portpriorität ist das erste Byte der Portidentifikation.	16 < n*16< 240	128
BPDU Guard an	Die BPDU-Guard-Funktion überwacht den Port auf den Empfang von BPDUs. Hinweis: Das Aktivieren der BPDU-Guard-Funktion ist nur wirksam, wenn diese Funktion auch global eingeschaltet ist (siehe "Globale Einstellungen" auf Seite 188)	enable, disable	disable
Soll Pfadkosten	Eingabe der Pfadkosten zur Bevorzugung redundanter Pfade. Beim Wert „0“ ermittelt der Switch automatisch die Pfadkosten in Abhängigkeit von der Übertragungsrate.	0 - 200 000 000	0
Soll Edge Port	Mit Soll Edge Port geben Sie an, ob an diesem Port ein Endgerät (= true) oder eine (R)STP-Brücket (= false) angeschlossen sein soll. Bei einer Rekonfiguration kann der Edge Port bei einem Endgerät innerhalb von 4 Sekunden auf Weiterleiten umschalten. In jedem Fall erkennt die Brücke eine angeschlossene (R)STP-Brücke und zeigt dies unter Ist Edge Port an.	true, false	false
Soll PointTo-Point	Die Punkt-zu-Punkt-Verbindung stellt eine direkte Verbindung zwischen 2 RSTP-Brücken dar und dient der schnellen Rekonfigurationszeit. Wählen Sie den Wert forceTrue, wenn zur Verbindung zwischen 2 RSTP-Brükken eine halbduplex Verbindung besteht.	auto, forceTrue, forceFalse	auto

Tab. 14: STP/RSTP-Port-Einstellungen

5.6 VLAN

Unter VLAN finden sich alle Tabellen und Attribute zur Konfiguration und Überwachung der VLAN-Funktion nach dem Standard IEEE 802.1Q.

Hinweis: Achten Sie bei der VLAN-Konfiguration darauf, daß der Port, an dem Ihre Managementstation angeschlossen ist, auch nach dem Speichern der VLAN-Konfiguration noch die Daten der Managementstation vermitteln kann. Die Zuweisung dieses Ports zu dem VLAN mit der ID 1 gewährleistet immer die Vermittlung der Daten der Managementstation.

Nach dem Ändern eines Eintrags:

`Schreiben`
Der Agent speichert den neuen Eintrag.
Die Änderung wird sofort wirksam.

`Laden`
Zeigt die aktuellen Konfigurationsdaten an.

Hinweis: Die VLAN-IDs der bis zu 40 VLANs liegen im Bereich zwischen 1 und 1024.

Hinweis: Betreiben sie in einem HIPER-Ring mit VLANs auschließlich Geräte mit der Software, die diese Funktion unterstützen:

- MICE Rel. 3.0 und höher,
- RS2-../.. Rel. 7.0 und höher,
- RS2-16M Rel. 7.1 und höher.

Hinweis: Bei der HIPER-Ring-Konfiguration wählen Sie die VLAN ID 1 für die Ringports.

5.6.1 VLAN einrichten

Zum Einrichten von VLANs legen Sie als erstes in der VLAN Statisch Tabelle (Static) die gewünschten VLANs an:

☐ Geben Sie nach einem Klick auf „Erzeugen“ den entsprechenden VLAN-Index ein. Eine neue Zeile erscheint in der Tabelle.

☐ Geben Sie einen beliebigen Namen für dieses VLAN ein.

☐ Definieren Sie die Zugehörigkeit der gewünschten Ports.
- – kein Mitglied im VLAN.
- M Mitglied im VLAN, Datenpakete mit Tag versenden.
- F Kein Mitglied im VLAN, auch nicht dynamisch über GVRP.
- U Mitglied im VLAN, Datenpakete ohne Tag versenden.

☐ Nach dem Anlegen der VLANs legen Sie in der Port-Tabelle (Port) die Regeln für empfangene Daten fest:

- ▶ VLAN ID
  legt fest, welchem VLAN ein empfangenes ungetaggtes Datenpaket zugeordnet wird.
- ▶ Ingress Filter
  legt fest, ob die empfangenen Tags ausgewertet werden.

☐ Markieren Sie VLAN Mode, um die VLAN-Funktion zu aktivieren. Bei aktiver VLAN-Funktion ist das VLAN-Status-Feld markiert.

☐ Speichern Sie die Konfiguration.

☐ Führen Sie einen Neustart des Switches durch.

Hinweis: Sollten Sie bei aktiver VLAN-Funktion die Portzugehörigkeit oder die Ingress-Filter-Einstellung ändern, dann speichern Sie die Konfiguration und führen Sie einen Neustart des Switches durch. So stellen Sie sicher, daß der Switch diese Einstellung auf alle Einträge in der Tabelle „Filter für MAC-Adressen“ anwendet.

5.6.2 Beispiel für ein einfaches VLAN

Das folgende Beispiel vermittelt einen schnellen Einstieg in die Konfiguration eines VLANs, wie es in der Praxis häufig zu finden ist.
Schritt für Schritt erfolgt die Konfiguration.

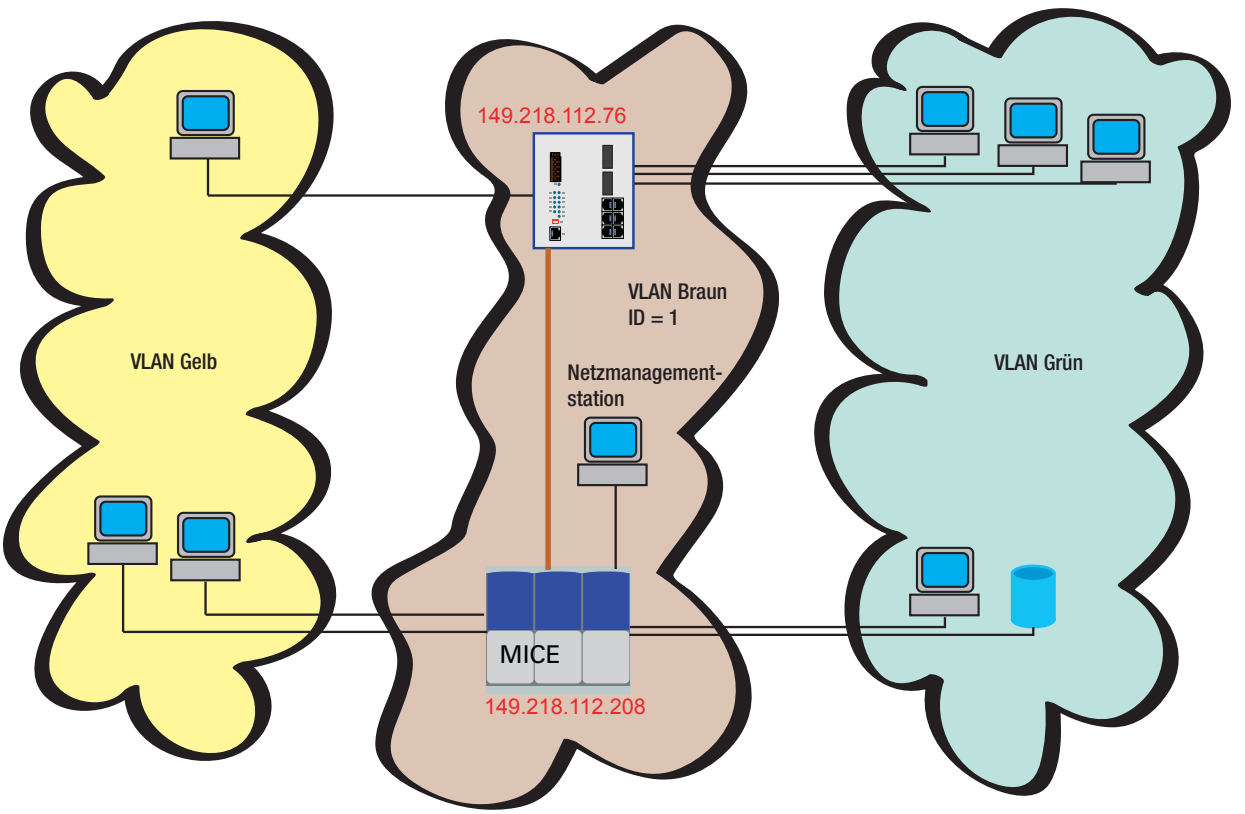


Abb. 76: Beispiel für ein VLAN

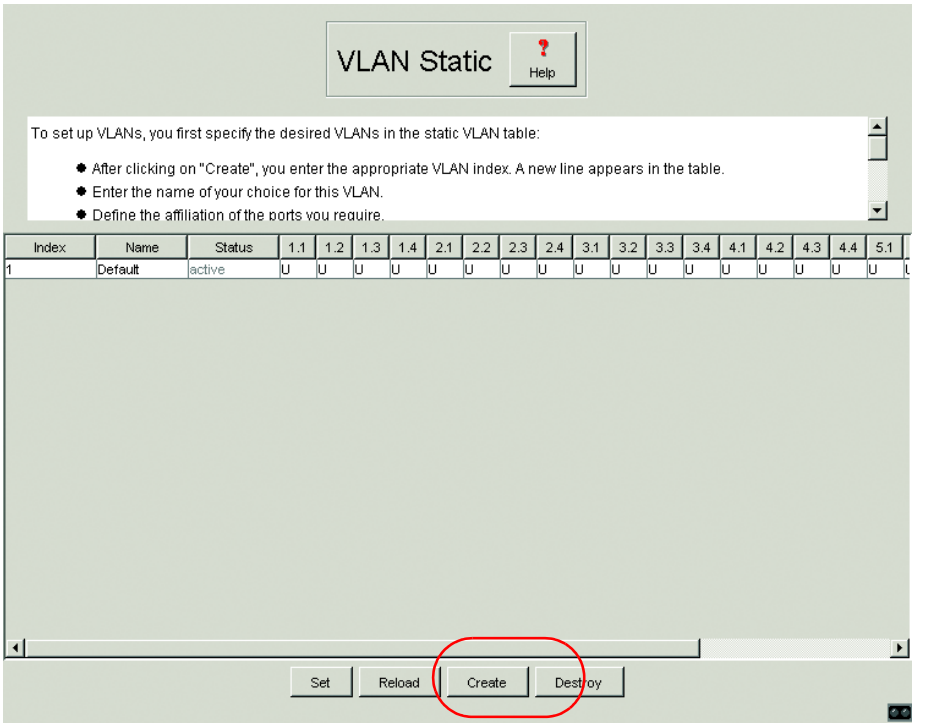


Abb. 77: VLAN erzeugen

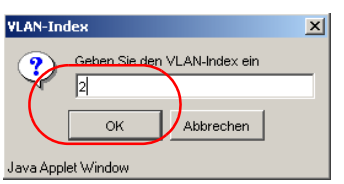


Abb. 78: VLAN ID eingeben

☐ Wiederholen Sie die Schritte VLAN erzeugen und VLAN ID eingeben für alle VLANs.

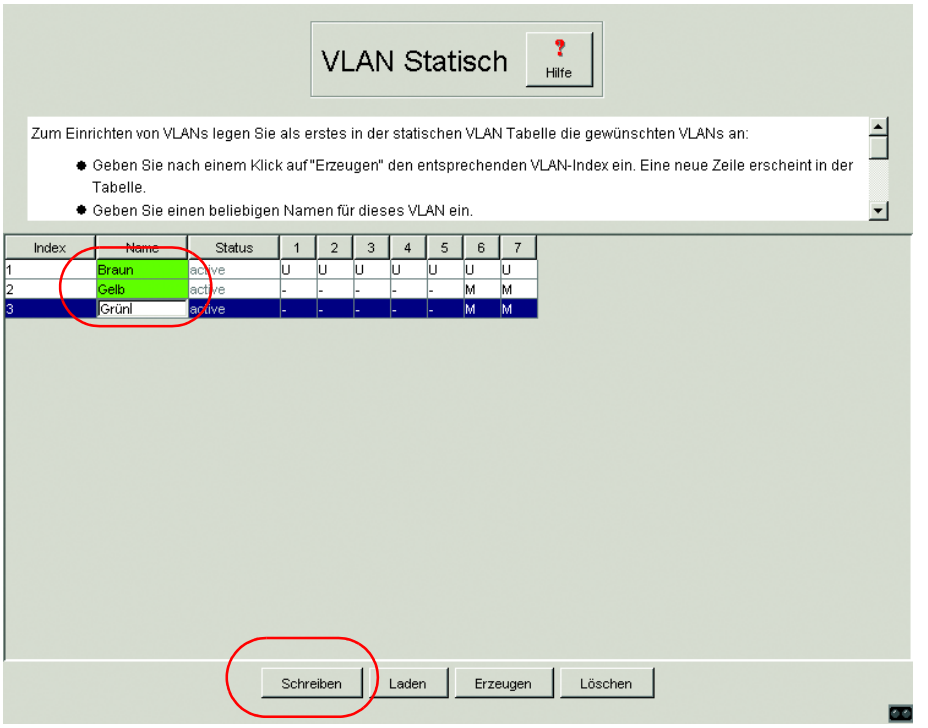


Abb. 79: VLANs mit beliebigen Namen benennen und speichern

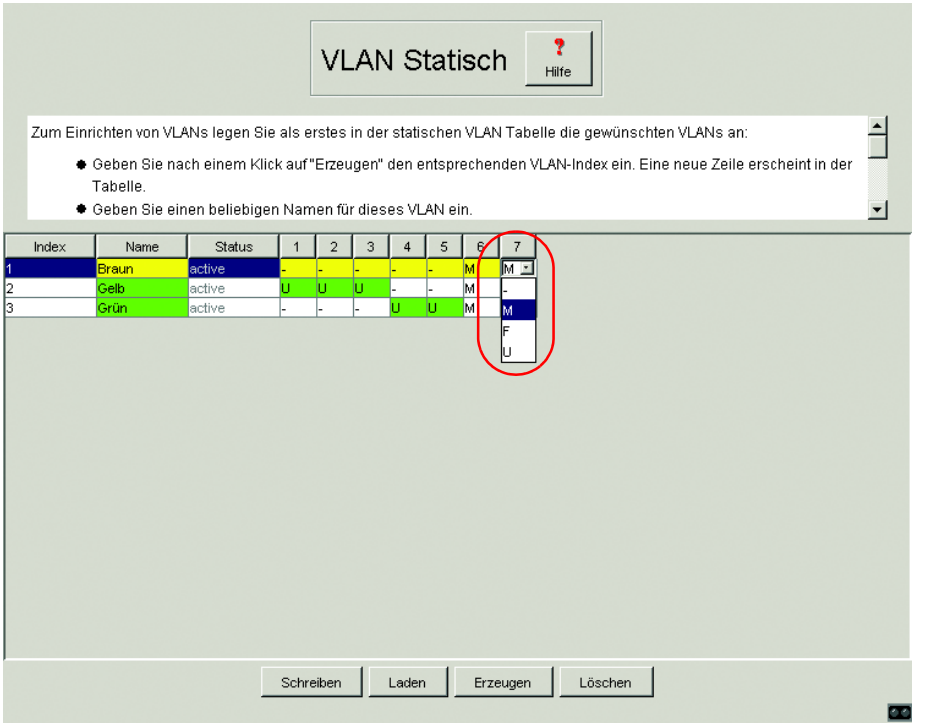


Abb. 80: VLAN-Zugehörigkeit der Ports definieren.

Die Ports 1 bis 3 sind den Endgeräten des VLANs Gelb und die Ports 4 bis 5 sind Endgeräten des VLANs Grün zugeordnet. Da Endgeräte in der Regel keine Datenpakete mit Tag senden, ist hier die Einstellung `U` zu wählen.

Der Port 6 dient als Uplink-Port zum nächsten Switch. Er erhält die Einstellung `M`. Somit kann er VLAN-Informationen weitergeben.

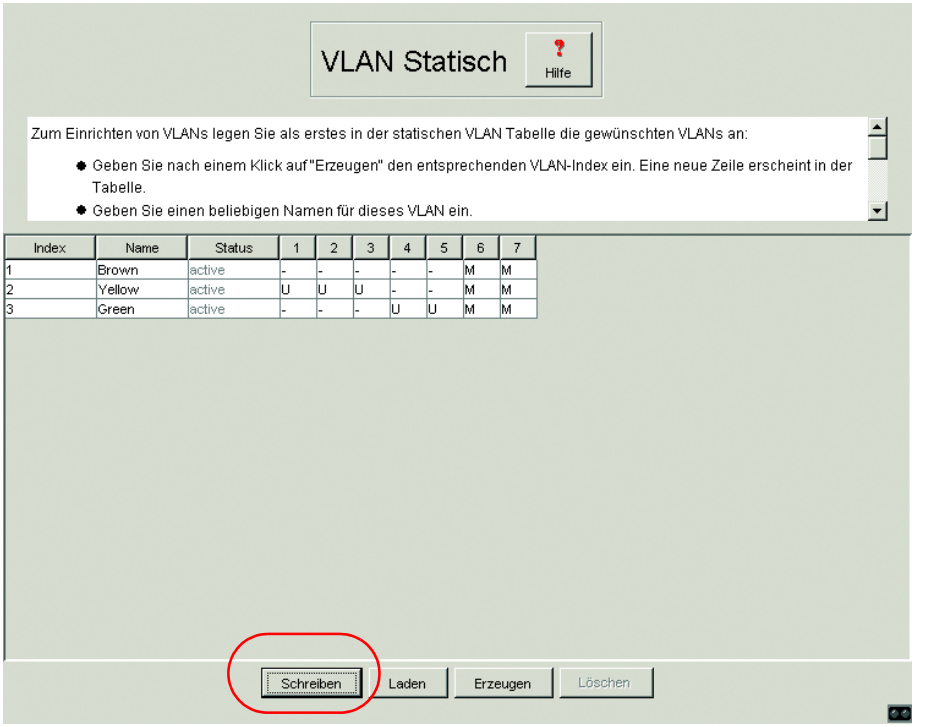


Abb. 81: VLAN-Konfiguration speichern

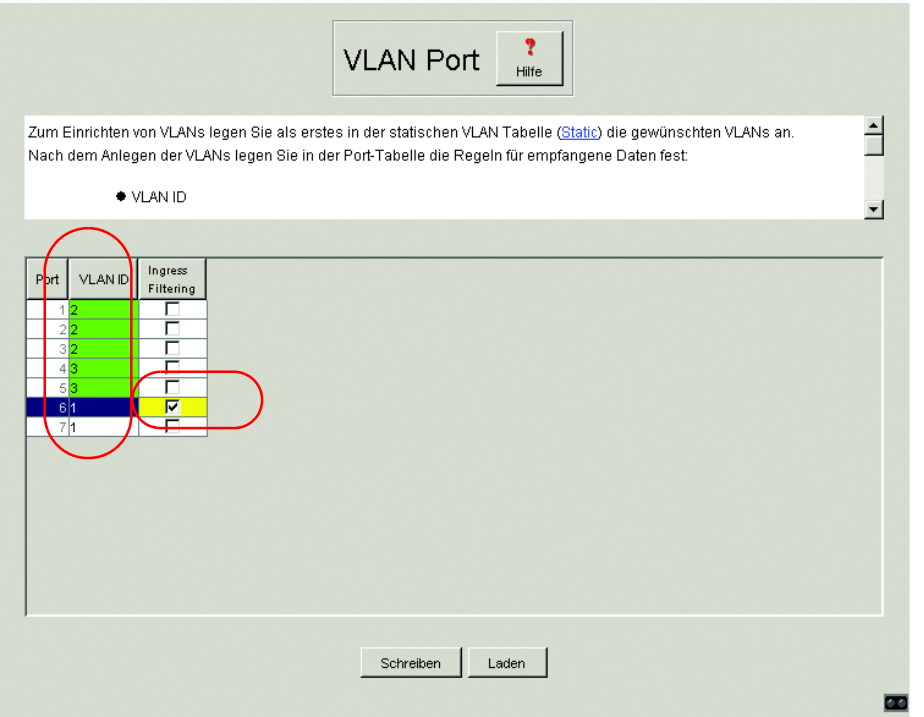


Abb. 82: VLAN-Identifikation den Ports zuweisen und speichern

Die Ports 1 bis 3 sind den Endgeräten des VLANs Gelb und somit der VLAN ID 2 und die Ports 4 und 5 sind Endgeräten des VLANS Grün und somit der VLAN ID 3 zugeordnet.
Der Port 6 dient als Uplink-Port zum nächsten Switch. Er gehört dem VLAN Braun an und erhält somit die VLAN ID 1. Die Aktivierung von `Ingress Filter` gewährleistet die Auswertung der empfangenen Tags an diesem Port.

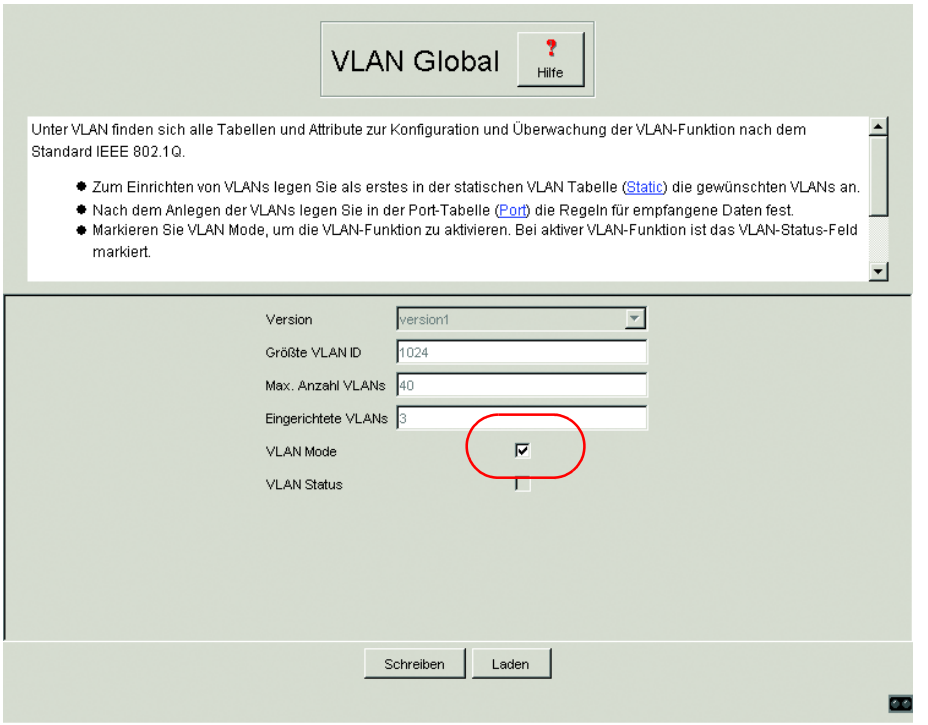


Abb. 83: VLAN-Modus global aktivieren

☐ Markieren Sie VLAN Mode, um die VLAN-Funktion zu aktivieren. Bei aktiver VLAN-Funktion ist das VLAN-Status-Feld markiert.

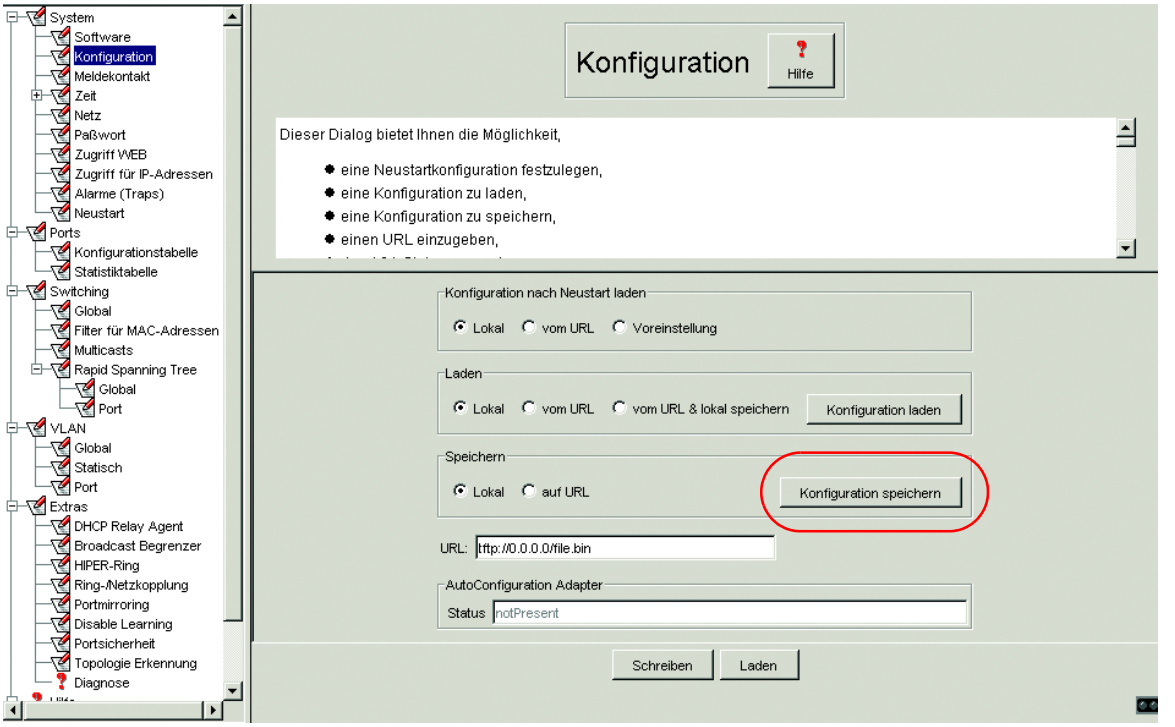


Abb. 84: Konfiguration nicht-flüchtig speichern

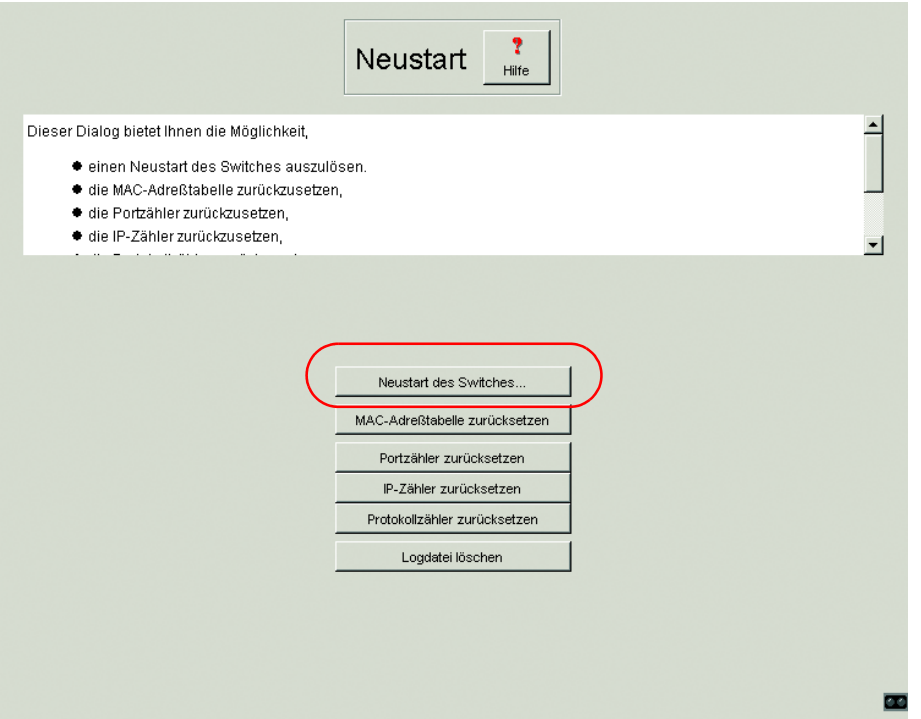


Abb. 85: Den Switch neu starten.

5.7 Extras

Das Menü Extras bietet die:

- Konfiguration des DHCP Relay Agenten
- Konfiguration der Broadcast-Begrenzung
- Konfiguration der HIPER-Ring-Funktion,
- Konfiguration der redundanten Kopplung von HIPER-Ringen und Netzsegmenten,
- Einstellung des Portmirroring,
- Disable Learning und
- Einstellung der Portsicherheit.

5.7.1 DHCP Relay Agent

Dieser Dialog ermöglicht Ihnen, den DHCP Relay Agenten zu Konfigurieren. Der DHCP Relay Agent ist eine Funktion, die in diesem Switch integriert ist (siehe "System-Konfiguration via DHCP Option 82" auf Seite 62).

☐ Geben Sie die DHCP-Server-IP-Adressen ein.
Sollte ein DHCP-Server nicht erreichbar sein, dann ermöglicht die Eingabe von bis zur drei weiteren DHCP-Server-IP-Adressen dem Switch das Ausweichen auf einen anderen DHCP-Server.

☐ Mit der Option 82 fügt der DHCP Relay Agent, der eine DHCP-Anforderung empfängt, der Anforderung ein „Option 82“-Feld an, sofern die empfangene Anforderung noch kein solches Feld besitzt.
Bei ausgeschalteter Funktion leitet der Switch zwar angehängte „Option 82“-Felder weiter, fügt jedoch keine an. Geben Sie in „Typ“ an, in welchem Format der DHCP Relay Agent die Gerätekennung dieses Switches in das „Option 82“-Feld einfügen soll.
Zur Auswahl stehen:
– IP-Adresse
– MAC-Adresse (Lieferzustand)
– Systemname (client-ID).
– other (frei definierbare ID, die Sie in der folgenden Zeile eingeben können)
„RemoteID-Eintrag für DHCP-Server“ zeigt Ihnen den Wert an, den Sie bei der Konfiguration Ihres DHCP-Servers eintragen.
„Typ Anzeige“ zeigt die Gerätekennung im ausgewählten Form an.

▶ Die Tabellenspalte „Circuit-ID“ zeigt Ihnen den Wert an, den Sie bei der Konfiguration Ihres DHCP-Servers eintragen. Die „Circuit ID“ enthält neben der Portnummer auch die ID des VLANs von dem die DHCP Anfrage empfangen wurde.

Beispiel für die Konfiguration Ihres DHCP-Servers (siehe Abb. 115):
Typ: `mac`
RemoteID-Eintrag für DHCP-Server: `00 06 00 80 63 00 06 1E`
Circuit-ID: `B3 06 00 00 01 00 01 01`
Hieraus resultiert der Eintrag für die „Harwareadresse“ im DHCP-Server:
`B30600000100010100060080630006 1E`

☐ Die Tabellenspalte „Relay-Funktion ein/aus“ bietet Ihnen die Möglichkeit, diese Funktion pro Port ein-/auszuschalten.

☐ In der Spalte „Hirschmann-Agent“ kreuzen Sie die Ports an, an denen ein Switch von Hirschmann angeschlossen ist.

5.7.2 Broadcast-Begrenzer

Broadcast-Begrenzer bietet Ihnen die Möglichkeit, die maximale Anzahl der erlaubten Broadcasts pro Port ausgangsseitig zu definieren.

Das Ankreuzfeld „Broadcast Begrenzer Modus“ bietet Ihnen die Möglichkeit, den Broadcast-Begrenzer an allen Ports ein/auszuschalten.

Einstellmöglichkeiten pro Port:

- = 0, keine Begrenzung der Broadcasts ausgangsseitig an diesem Port.
- > 0, maximale Anzahl der Broadcasts, die pro Sekunde ausgangsseitig an diesem Port gesendet werden.

Weitere Informationen zum Broadcast Begrenzer finden Sie unter "Broadcast Begrenzer" auf Seite 101.

5.7.3 Konfiguration der HIPER-Ring-Funktion

Dieser Dialog zeigt Ihnen die Funktion dieses Switches im HIPER-Ring an. Das Konzept des HIPER-Rings erlaubt den Aufbau hochverfügbarer, ringförmiger Netzstrukturen. Innerhalb einer solchen Ringtopologie werden Netzkomponenten, die den HIPER-Ring unterstützen, über ihre Ringports miteinander verbunden. Dabei übernimmt genau ein Redundanz Manager die Kontrolle über den Ring.
Der RS2-../.. wird über die HIPER-Ring-Ports (Ports 6 und 7) in den Ring integriert. Das Ein-/Ausschalten des Redundanz Managers erfolgt über einen Schalter direkt am Switch (siehe Abb. 1). Der Status des Redundanzmanagers ist aktiv, wenn der Ring offen ist. Dies ist der Fall, wenn z.B. eine Datenleitung oder Netzkomponente innerhalb des Rings ausgefallen ist.

Hinweis: Für die Ringports sind folgende Einstellungen erforderlich (siehe "Port-Konfigurationstabelle" auf Seite 181):
– 100 Mbit/s
– Vollduplex
– Autonegotiation aus
– Port an.

Information
„Redundanz gewährleistet“ zeigt Ihnen an, daß eine von der Funktion betroffene Leitung ausfallen kann und eine redundante Strecke die Funktion der ausgefallenen Strecke übernehmen wird.

„Konfigurationsfehler“ zeigt Ihnen an, ob die Funktion unvollständig oder falsch konfiguriert ist.

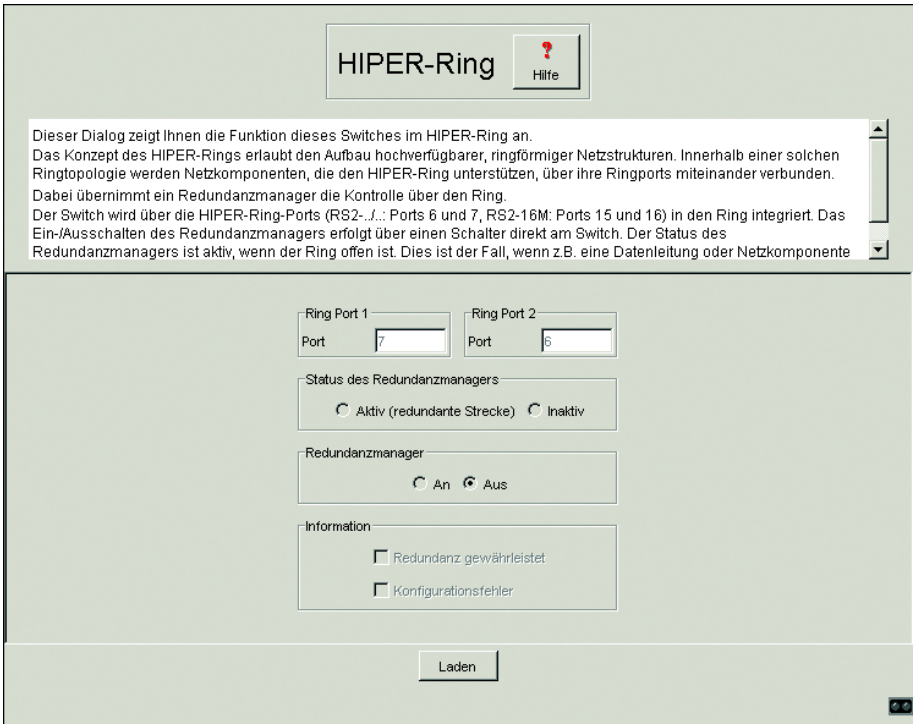


Abb. 86: Dialog HIPER-Ring

5.7.4 Konfiguration der redundanten Kopplung von HIPER-Ringen und Netzsegmenten

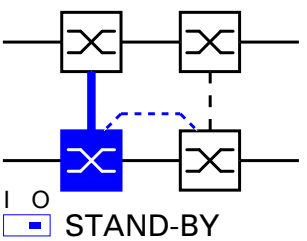
Die im RS2-../.. eingebaute Steuerungsintelligenz erlaubt die redundante Kopplung von HIPER-Ringen und Netzsegmenten. Die Verbindung zweier Netzsegmente erfolgt über zwei getrennte Pfade mit je einem RS2-../...Der Switch in der redundanten Strecke bekommt über die DIP-Schalter-Einstellung „STAND-BY“ die Redundanzfunktion zugeordnet.
Der Switch in der redundanten Strecke und der Switch in der Hauptstrecke teilen sich über die Steuerleitung ihre Betriebszustände mit.

Hinweis: Aus Gründen der Redundanzsicherheit schließt sich die Kombination von Rapid Spanning Tree und Netz-/Ringkopplung aus.

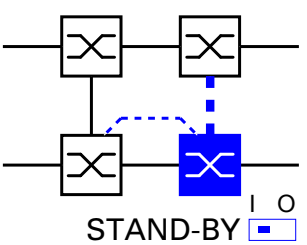
Dieser Dialog bietet Ihnen die Möglichkeit, die redundante Kopplung von Netzsegmenten zu konfigurieren.

Konfiguration wählen

☐ Wählen Sie als erstes die gewünschte Konfiguration:
Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch. Der Dialog zeigt in Abhängigkeit der STAND-BY-DIP-Schalterstellung die möglichen Konfigurationen an. Möchten Sie eine der ausgegrauten Konfigurationen wählen, dann bringen Sie den DIP-Schalter am Switch in die entsprechende Stellung.



Zwei-Switch-Haupt-Kopplung mit Steuerleitung:
Die Kopplung zwischen zwei Netzen erfolgt über die Hauptleitung (dicke blaue Linie), die mit dem Kopplungsport verbunden ist. Beim Ausfall der Hauptleitung übernimmt die Stand-by-Leitung (gestrichelte, schwarze Linie), die mit dem Partner-Kopplungsport verbunden ist, die Kopplung der beiden Netze. Die Kopplung erfolgt über zwei Switches. Sie konfigurieren mit dieser Auswahl diesen Switch als den Switch, an dem Sie die Hauptleitung anschließen. Die Switche übermitteln ihre Kontrollpakete über die Steuerleitung.



Zwei-Switch-Stand-by-Kopplung mit Steuerleitung:
Die Kopplung zwischen zwei Netzen erfolgt über die Hauptleitung (dünne senkrechte Linie), die mit dem Partner-Kopplungsport verbunden ist. Beim Ausfall der Hauptleitung übernimmt die Stand-by-Leitung (gestrichelte, dicke blaue Line), die mit dem Kopplungsport verbunden ist, die Kopplung der beiden Netze. Die Kopplung erfolgt über zwei Switches. Sie konfigurieren mit dieser Auswahl diesen Switch als den Switch, an dem Sie die Stand-by-Leitung anschließen. Die Switche übermitteln ihre Kontrollpakete über die Steuerleitung.

Port auswählen

Der Switch, an dem Sie die Hauptleitung und der Switch, an dem Sie die Stand-by-Leitung anschließen, sind Partner bezüglich der Kopplung. Verbinden Sie die beiden Partner über ihre Ringports.

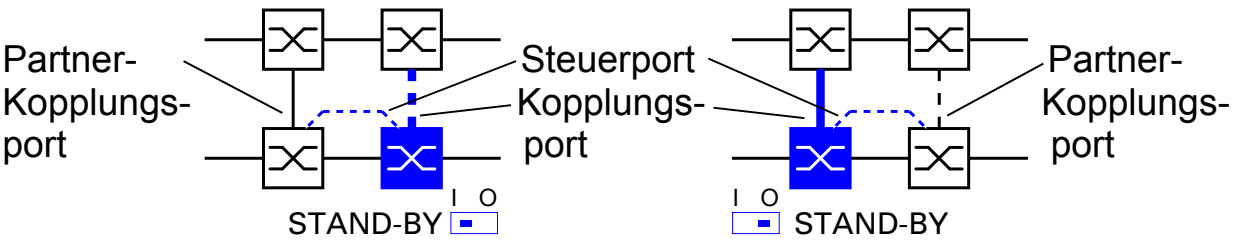


Abb. 87: Kopplungsport – Partner-Kopplungsport

☐ Wählen Sie den Kopplungsport aus.
Mit "Kopplungsport" legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen:
– Bei der STAND-BY-DIP-Schalterstellung OFF schließen Sie die Hauptleitung am Kopplungsport an.
– Bei der STAND-BY-DIP-Schalterstellung ON schließen Sie die Stand-by-Leitung am Kopplungsport an.

Switch	Steuerport	Kopplungsport
RS2-../..	Stand-by-Port (ausschließlich mit RS2-../.. kombinierbar)	Port 1
RS2-16M	einstellbar (Lieferzustand: Port 2)	einstellbar (Lieferzustand: Port 1)
MICE	einstellbar (Lieferzustand: Port 1.3)	einstellbar (Lieferzustand: Port 1.4)
MACH 3000	einstellbar	einstellbar

Tab. 15: Portzuordnung für die redundante Kopplung

☐ Wählen Sie, sofern von der Konfiguration vorgesehen, den Steuerport. Mit „Steuerport“ legen Sie fest, an welchen Port Sie die Steuerleitung anschließen.

- „Portmodus“ zeigt Ihnen die DIP-Schalter-Stellung am Gerät für die Redundanzfunktion an.
- „Portstatus“ zeigt Ihnen an, welchen Status der Port gerade tatsächlich hat.

Hinweis: Für die Kopplungsports sind folgende Einstellungen erforderlich (siehe "Port-Konfigurationstabelle" auf Seite 181):
– Autonegotiation an
– Port an.

- „IP-Adresse“ zeigt Ihnen die IP-Adresse des Partners an, soweit dieser schon im Netz in Betrieb ist.

Funktion

Dieser Rahmen zeigt den Funktionsstatus der Kopplung an.

Information

„Redundanz gewährleistet“ zeigt Ihnen an, daß eine der betroffenen Leitungen ausfallen kann und eine redundante Strecke die Funktion der ausgefallenen Strecke übernehmen wird.
„Konfigurationsfehler“ zeigt Ihnen an, ob die Funktion vollständig und richtig konfiguriert ist.

Redundanzmodus

Mit der Einstellung „Redundante Ring-/Netzkopplung“ ist entweder die Hauptleitung oder die Stand-by-Leitung aktiv. Niemals sind beide Leitungen gleichzeitig aktiv.

Bei der Einstellung „Erweiterte Redundanz“ sind Hauptleitung und Stand-by-Leitung gleichzeitig aktiv, wenn die Verbindungsleitung zwischen den Switches im angekoppelten Netz ausfällt.
Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie diese Einstellung nur, wenn Ihre Anwendung Paketdoppelungen erkennt.

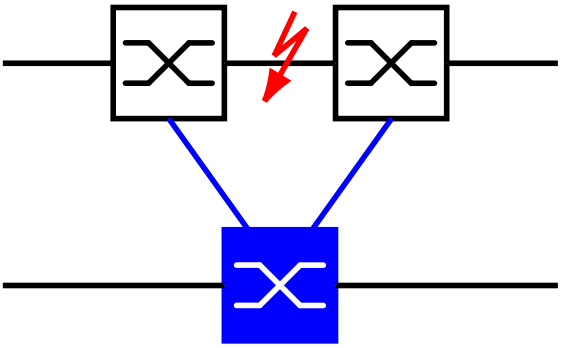


Abb. 88: Erweiterte Redundanz

Hinweis: Um dauerhafte Schleifen (Loops) zu vermeiden, setzt der Switch den Portstatus von Steuerport und Kopplungsport auf aus, wenn Sie:
– die Funktion ausschalten oder
– die Konfiguration wechseln
während die Verbindungen an diesen Ports in Betrieb sind.

- **Kopplungsmodus**
  Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.
  „Ring“: Wählen Sie „Ring“, wenn Sie einen HIPER-Ring ankoppeln.
  „Netz“: Wählen Sie „Netz“, wenn Sie eine Linienstruktur ankoppeln.

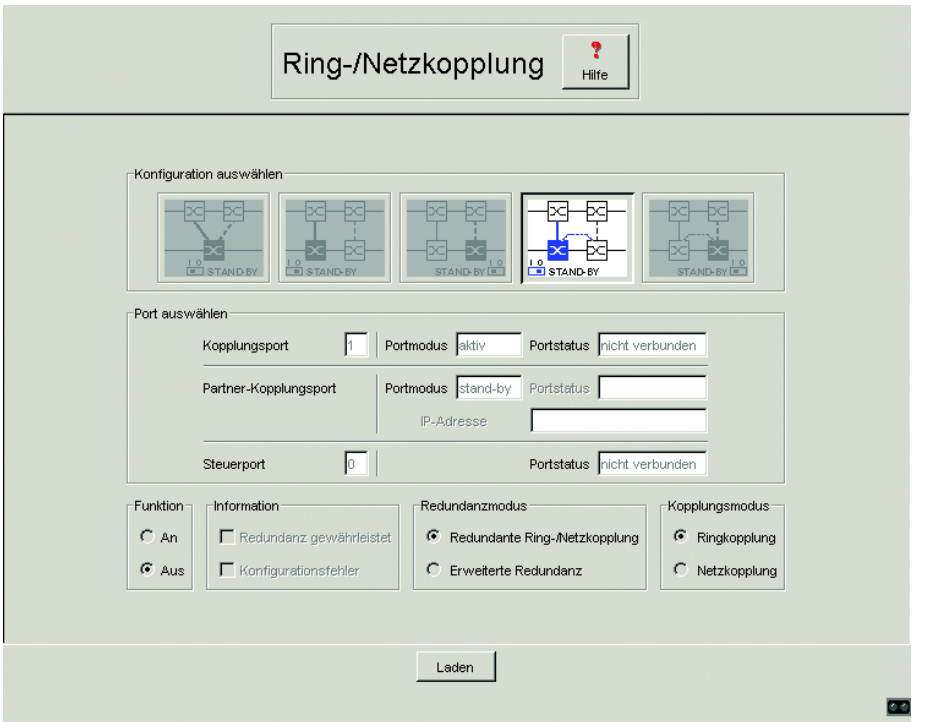


Abb. 89: Dialog Ring-/Netzkopplung

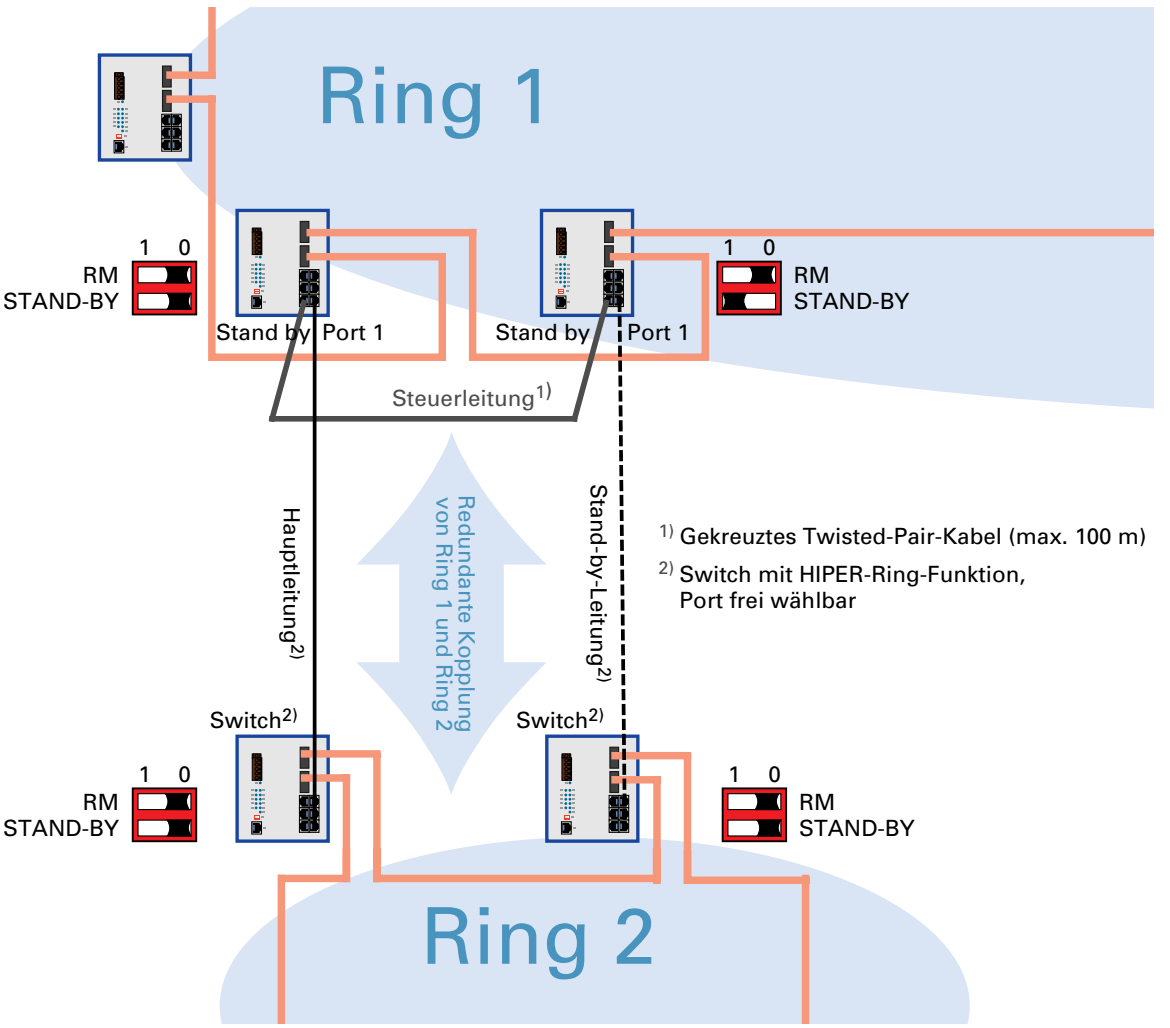


Abb. 90: Beispiel Konfiguration HIPER-Ring Kopplung

5.7.5 Einstellung des Portmirroring

Dieser Dialog bietet Ihnen die Möglichkeit, die Portmirroring Funktion des Switches zu konfigurieren und zu aktivieren. Beim Portmirroring wird der Datenverkehr eines Quellports zu einem festgelegten Port kopiert. Der Datenverkehr am Quellport wird beim Portmirroring nicht beeinflußt.
Ein am festgelegten Port angeschlossenes Management-Werkzeug, wie z.B. ein RMON-Probe, kann so den Datenverkehr des Quellports beobachten.

Hinweis: Bei aktivem Portmirroring dient der festgelegte Port ausschließlich zur Beobachtung.

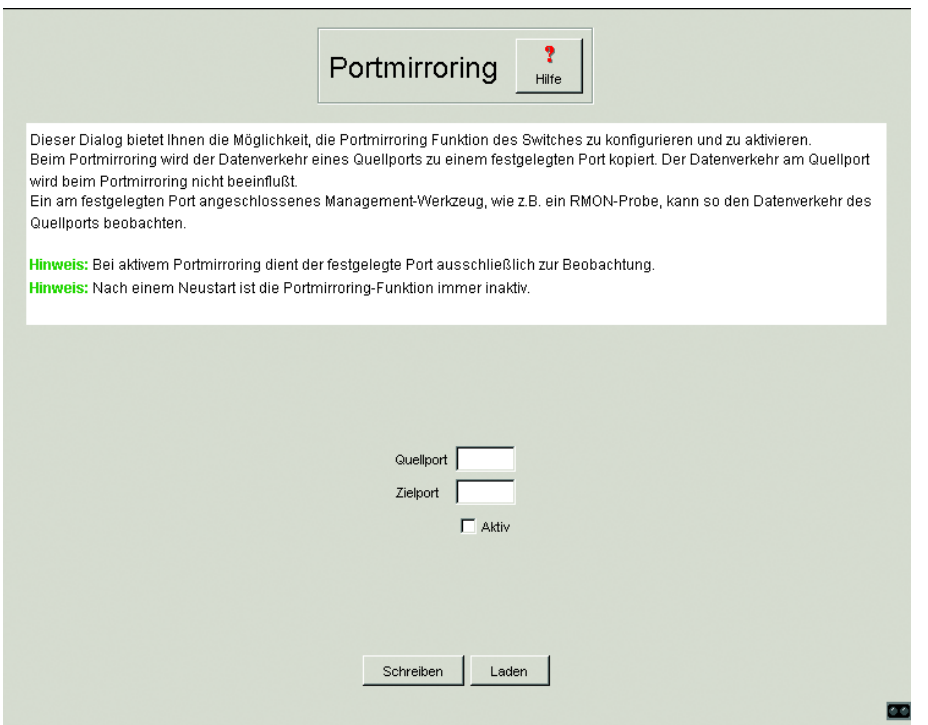


Abb. 91: Dialog Portmirroring

5.7.6 Ein-/Ausschalten der Lern-Funktion

Dieser Dialog bietet Ihnen die Möglichkeit, die Daten aller Ports zu beobachten. Mit dem Ankreuzen der Disable Learning-Funktion schalten Sie die Lern-Funktion des RS2-../.. aus. Damit überträgt der RS2-../.. alle Daten von allen Ports an alle Ports.

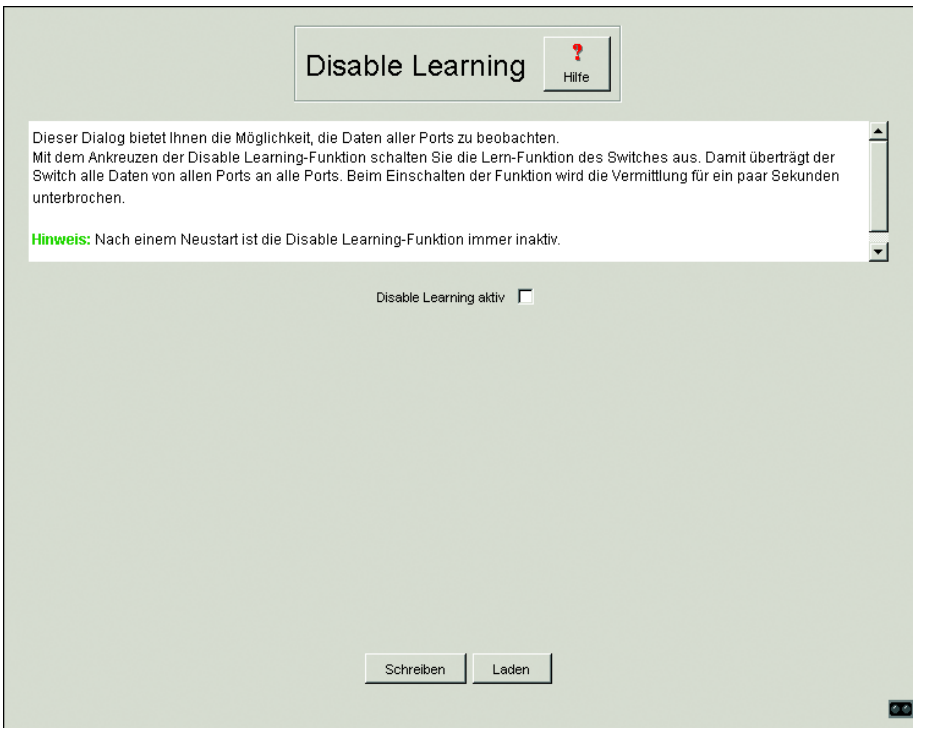


Abb. 92: Dialog Disable Learning

5.7.7 Einstellung der Portsicherheit

Dieser Dialog bietet Ihnen die Möglichkeit, für jeden Port festzulegen, von welchem Endgerät Daten empfangen und an andere Ports vermittelt werden dürfen. Diese Funktion schützt vor einem unbefugten Zugriff auf das Netz.

☐ Wählen Sie zunächst, ob Sie die MAC-basierte oder die IP-basierte Portsicherheit wünschen.

☐ Falls Sie MAC-basiert gewählt haben, geben Sie in der Spalte "erlaubte MAC-Adresse" die MAC-Adresse des Gerätes ein, mit dem ein Datenaustausch an diesem Port erlaubt ist. Der Eintrag 00:00:00:00:00:00 erlaubt jedem Gerät einen Datenaustausch.

► Die Spalte „aktuelle MAC-Adresse“ zeigt die MAC-Adresse des Gerätes an, von dem zuletzt Daten empfangen wurden. Sie können einen Eintrag aus der Spalte „aktuelle MAC-Adresse“ mit der gedrückten linken Maustaste in die Spalte „erlaubte MAC-Adresse“ kopieren

☐ Falls Sie IP-basiert gewählt haben, geben Sie in der Spalte "erlaubte IP-Adresse" die IP-Adresse des Gerätes ein, mit dem ein Datenaustausch an diesem Port erlaubt ist. Der Eintrag 0.0.0.0 erlaubt jedem Gerät einen Datenaustausch.

☐ In der Spalte „Aktion“ wählen Sie aus, ob nach einem unberechtigten Zugriff
- keine Aktion ausgelöst wird (none) oder
- ein Alarm (Trap) geschickt wird (trapOnly) oder
- der Port abgeschaltet und ein Alarm (Trap) geschickt wird (portDisable).

Hinweis: Ein Alarm (Trap) kann nur gesendet werden, wenn unter Alarme (Traps) mindestens ein Empfänger eingetragen ist und der entsprechende Status sowie „Authentication“ angekreuzt ist.

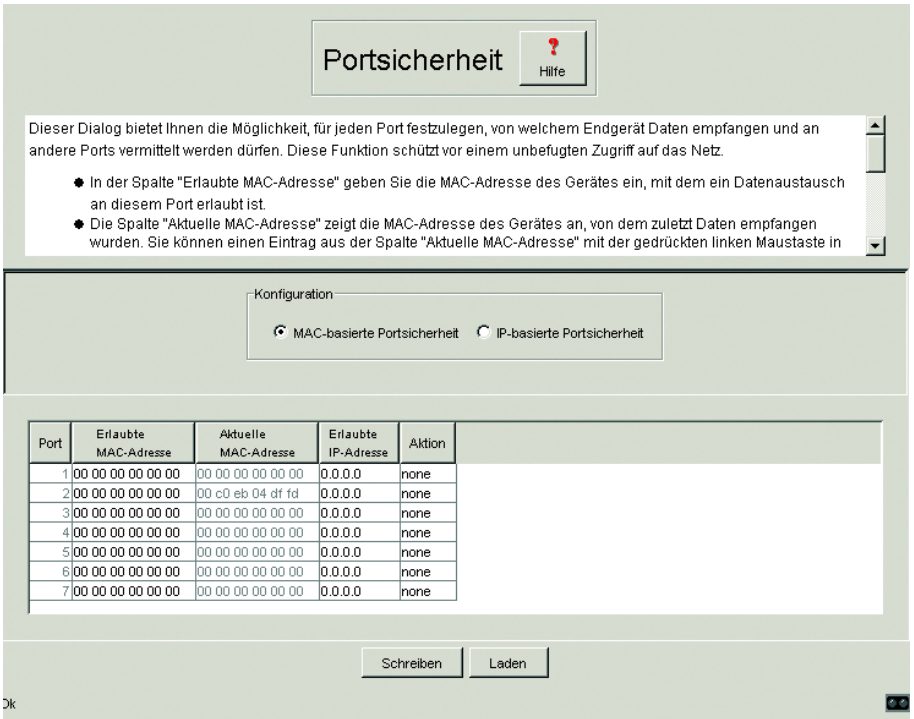


Abb. 93: Dialog Portsicherheit

5.7.8 Topologie-Erkennung

Dieser Dialog bietet Ihnen die Möglichkeit, die Funktion zur Topologie-Erkennung ein/auszuschalten.
Eine Tabelle zeigt Ihnen die gesammelten Informationen zu Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagementstation in der Lage, die Struktur Ihres Netzes darzustellen (siehe "Topologie-Erkennung" auf Seite 135).

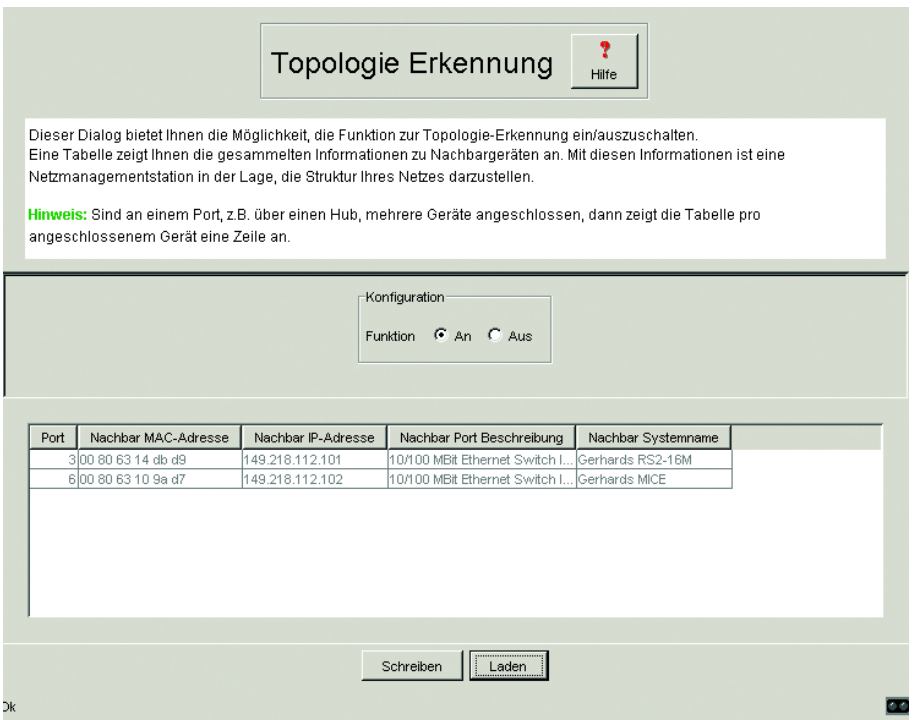


Abb. 94: Topologie-Erkennung

Hinweis: Sind an einem Port, z.B. über einen Hub, mehrere Geräte angeschlossen, dann zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

5.7.9 Diagnose

Zur Diagnose stehen folgende Berichte zur Verfügung. Sie geben im Service-Fall dem Techniker die notwendigen Informationen.

- Systeminformation
- Logfile

6 Management Information BASE MIB

Die Management Information Base MIB ist als abstrakte Baumstruktur angelegt.
Die Verzweigungspunkte sind die **Objektklassen**. Die „Blätter“ der MIB tragen die Bezeichnung **generische Objektklassen**.
Die **Instanzierung** der generischen Objektklassen, das heißt die abstrakte Struktur auf die Realität abbilden, erfolgt z. B. durch die Angabe des Ports oder der Quelladresse (Source Address) soweit dies zur eindeutigen Identifizierung nötig ist.
Diesen Instanzen sind Werte (Integer, TimeTicks, Counter oder Octet String) zugeordnet, die gelesen und teilweise auch verändert werden können. Die **Object Description** oder der **Object-ID** (OID) bezeichnet die Objektklasse. Mit dem **Subidentifier** (SID) werden sie instanziert.

Beispiel:
Die generische Objektklasse

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

ist die Beschreibung der abstrakten Information „Netzteilstatus“. Es läßt sich daraus noch kein Wert auslesen, es ist ja auch noch nicht bekannt, welches Netzteil gemeint ist.
Durch die Angabe des Subidentifiers (2) wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziert, und bezeichnet so den Betriebszustand des Netzteils 2. Diese Instanz bekommt einen Wert zugewiesen, der gelesen werden kann. Damit liefert die Instanz „get `1.3.6.1.4.1.248.14.1.2.1.3`.2“ als Antwort „1“, das heißt, das Netzteil ist betriebsbereit.

Einige verwendete Abkürzungen in der MIB:

Comm	Gruppen-Zugriffsrecht
con	Konfiguration
Descr	Beschreibung
Fan	Lüfter
ID	Identifizierer
Lwr	unterer (z. B. Grenzwert)

PS	Spannungsversorgung
Pwr	Stromversorgung
sys	System
UI	Benutzer-Schnittstelle (User Interface)
Upr	oberer (z. B. Grenzwert)
ven	vendor = Hersteller (Hirschmann)

Definition der verwendeten Syntaxbegriffe:

Integer	Ganze Zahl im Bereich von 0-2^{32}
IP-Adresse	xxx.xxx.xxx.xxx (xxx = ganze Zahl im Bereich von 0-255)
MAC-Adresse	12stellige Hexzahl nach ISO/IEC 8802-3
Object Identifier	x.x.x.x… (z. B. 1.3.6.1.1.4.1.248…)
Octet String	ASCII-Zeichen-Kette
PSID	Spannungsversorgungsidentifikation (Nummer des Netzteils)
TimeTicks	Stop-Uhr, verronnene Zeit = Zahlenwert/100 in Sekunden Zahlenwert = ganze Zahl im Bereich von 0-2^{32}
Timeout	Zeitwert in hundertstel Sekunden Zeitwert = ganze Zahl im Bereich von 0-2^{32}
Typfeld	4stellige Hexzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl (0-2^{32}), deren Wert beim Auftreten bestimmter Ereignisse um eins erhöht wird.

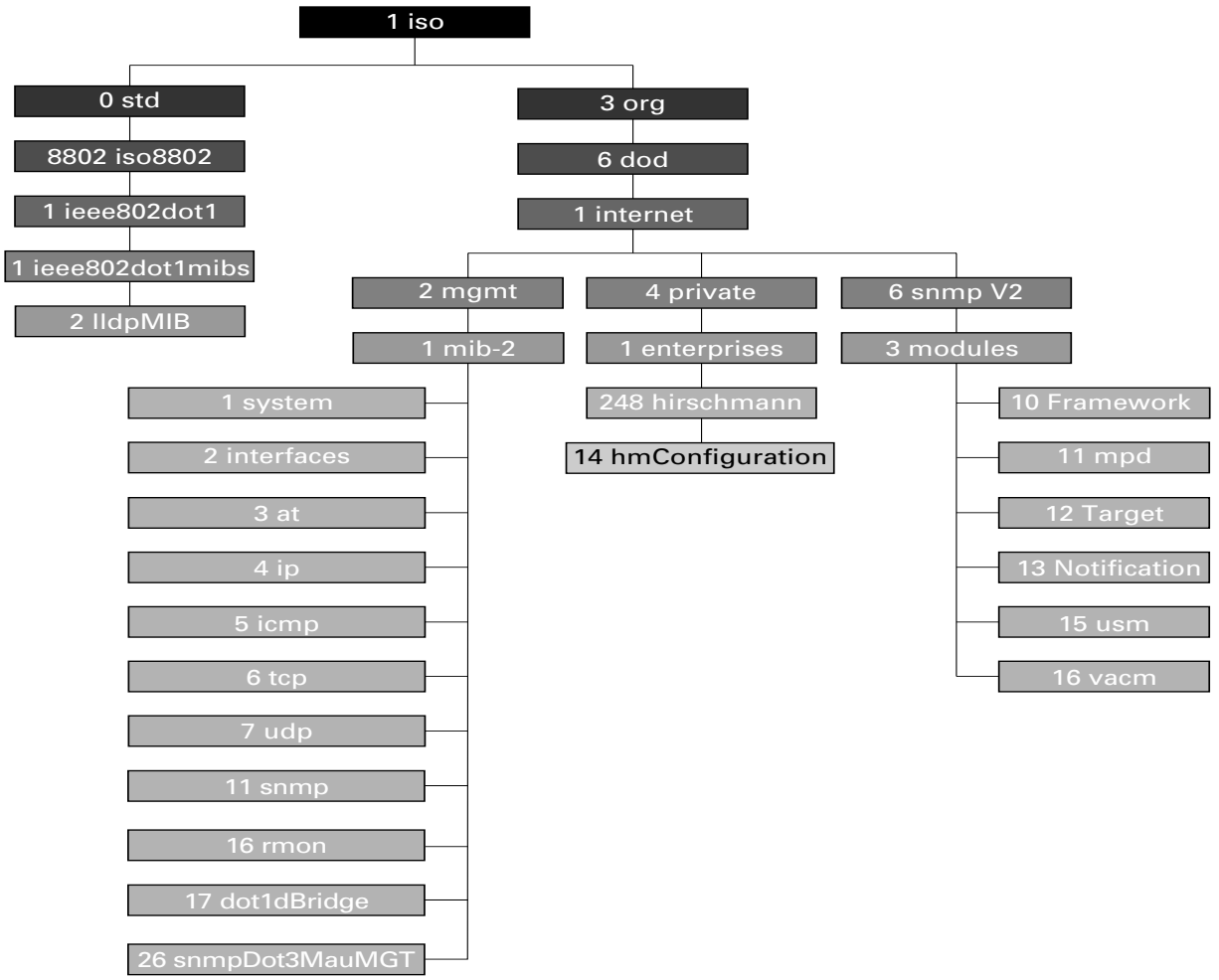


Abb. 95: Baumstruktur der Hirschmann-MIB

6.1 MIB II

6.1.1 System-Gruppe (1.3.6.1.2.1.1)

Die System-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält systembezogene Objekte. Hat ein Agent keinen Wert für eine Variable, dann wird mit einem String der Länge 0 geantwortet.

(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 (Größe: 0-255)
Zugriff	lesen
Beschreibung	Eine verbale Beschreibung des Eintrags. Dieser Wert sollte den vollen Namen und Versionsnummer von - Typ der Systemhardware - Operationssystem-Software und - Netzwerksoftware enthalten. Die Beschreibung darf nur aus druckbaren ASCII-Zeichen bestehen.

sysObjectID

OID1.3.6.1.2.1.1.2.0

Syntax	Objekt-Identifizierer
Zugriff	lesen
Beschreibung	Die Autorisierungs-Identifikation des Herstellers des Netzwerk-Management-Subsystems, welches in diesem Gerät integriert ist. Dieser Wert ist innerhalb des SMI enterprices subtree (1.3.6.1.4.1) plaziert und beschreibt welche Art von Gerät verwaltet wird. Zum Beispiel: wenn dem Hersteller "Hirschmann GmbH" der subtree 1.3.6.1.4.1.248 zugewiesen ist, dann kann er seiner Brücke den Identifizierer 1.3.6.1.4.1.248.2.1 zuordnen.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	TimeTicks
Zugriff	lesen
Beschreibung	Die Zeit in hundertstel Sekunden seit dem letzten Zurücksetzen der Netzwerk-Management-Einheit.

sysContact

OID1.3.6.1.2.1.1.4.0

Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Die verbale Identifikation der Kontaktperson für diesen verwalteten Knoten zusammen mit einer Information, wie diese Person erreichbar ist.

sysName

OID1.3.6.1.2.1.1.5.0

Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Einen für die Administration bezeichnenden Namen für diesen Knoten. Vereinbarungsgemäß ist dies der voll qualifizierende Namen in der Domäne.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet String (Größe: 0-255)
Zugriff	lesen und schreiben
Beschreibung	Der physikalische Ort, an dem sich dieser Knoten befindet (z. B. "Treppenhaus, 3. OG").

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0-127)
Zugriff	lesen
Beschreibung	Dieser Wert bezeichnet eine Menge von Diensten, welche dieses Gerät anbietet. Er ist eine Summe aus mehreren Summanden. Für jeden Layer des OSI Referenzmodells gibt es einen Summanden in der Form (2^{L-1}), wobei L den Layer bezeichnet. Z. B.: Für einen Knoten, der in erster Linie Routing-Funktionen ausführt, ist der Wert $(2^{3-1}) = 4$. Für einen Knoten, der ein Host ist, welcher Applikationsdienste anbietet, ist der Wert $(2^{4-1}) + (2^{7-1}) = 72$.

6.1.2 Interface-Gruppe (1.3.6.1.2.1.2)

Die Interface-Gruppe enthält Informationen über die Geräteschnittstellen.

(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-Gruppe (1.3.6.1.2.1.3)

Die Address-Translation-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen über die Adressenzuordnung.

(3) `at`

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

6.1.4 Internet-Protocol-Gruppe (1.3.6.1.2.1.4)

Die Internet-Protocol-Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen, die die IP-Vermittlung betreffen.

(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-Gruppe (1.3.6.1.2.1.5)

Die Internet Control Message Protocol Gruppe hat für alle Systeme Pflichtcharakter. Sie enthält Informationen zur Fehlerbehandlung und Steuerung im Internet-Datenverkehr.

(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-Gruppe (1.3.6.1.2.1.6)

Die Transfer-Control-Protocol-Gruppe hat für alle Systeme mit implementiertem TCP Pflichtcharakter. Instanzen von Objekten, die Informationen über eine bestimmte TCP-Verbindung beschreiben, haben nur solange Bestand, wie die Verbindung besteht.

(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-Gruppe (1.3.6.1.2.1.7)

Die User-Datagram-Protocol-Gruppe hat für alle Systeme mit implementiertem UDP Pflichtcharakter.

(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-Gruppe (1.3.6.1.2.1.11)

Die Simple-Network-Management-Protocol-Gruppe hat für alle Systeme Pflichtcharakter. In SNMP-Einrichtungen, welche optimiert sind, entweder nur einen Agenten oder nur eine Managementstation zu unterstützen, werden einige der aufgeführten Objekte mit dem Wert "0" beschrieben sein.

(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-Gruppe (1.3.6.1.2.1.16)

Dieser Teil der MIB liefert dem Netzmanagement ständig aktuelle und historische Daten der Netzkomponenten. Die Konfiguration von Alarmen und Ereignissen steuert die Auswertung von Zählern der Netzkomponenten. Das Ergebnis der Auswertung teilen die Agenten in Abhängigkeit von der Konfiguration mittels Traps der Managementstation mit.

```
(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)

Dieser Teil der MIB beinhaltet brückenspezifische Objekte.

(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
|--(5) dot1dStatic
|   |--(1) dot1dStaticTable
|   |   |--(1) dot1dStaticEntry
|   |   |   |--(1) dot1dStaticAddress
|   |   |   |--(2) dot1dStaticReceivePort
|   |   |   |--(3) dot1dStaticAllowedToGoTo
|   |   |   |--(4) dot1dStaticStatus
|--(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
|   |   |--(3) dot1dGarp
|   |   |   |--(1) dot1dPortGarpTable
|   |   |   |   |--(1) dot1dPortGarpEntry
|   |   |   |   |   |--(1) dot1dPortGarpJoinTime
|   |   |   |   |   |--(2) dot1dPortGarpLeaveTime
|   |   |   |   |   |--(3) dot1dPortGarpLeaveAllTime
|   |   |--(4) dot1dGmrp
|   |   |   |--(1) dot1dPortGmrpTable
|   |   |   |   |--(1) dot1dPortGmrpEntry
|   |   |   |   |   |--(1) dot1dPortGmrpStatus
|   |   |   |   |   |--(2) dot1dPortGmrpFailedRegistrations
|   |   |   |   |   |--(3) dot1dPortGmrpLastPduOrigin
|   |--(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
|   |   |   |   |--(3) dot1qTpGroupTable
|   |   |   |   |   |--(1) dot1qTpGroupEntry
```

```
|  |  |  |  |  |--(1) dot1qTpGroupAddress
|  |  |  |  |  |--(2) dot1qTpGroupEgressPorts
|  |  |  |  |  |--(3) dot1qTpGroupLearnt
|  |  |  |--(4) dot1qForwardAllTable
|  |  |  |  |--(1) dot1qForwardAllEntry
|  |  |  |  |  |--(1) dot1qForwardAllPorts
|  |  |  |  |  |--(2) dot1qForwardAllStaticPorts
|  |  |  |  |  |--(3) dot1qForwardAllForbiddenPorts
|  |  |  |--(5) dot1qForwardUnregisteredTable
|  |  |  |  |--(1) dot1qForwardUnregisteredEntry
|  |  |  |  |  |--(1) dot1qForwardUnregisteredPorts
|  |  |  |  |  |--(2) dot1qForwardUnregisteredStaticPorts
|  |  |  |  |  |--(3) dot1qForwardUnregisteredForbiddenPorts
|  |  |--(3) dot1qStatic
|  |  |  |--(1) dot1qStaticUnicastTable
|  |  |  |  |--(1) dot1qStaticUnicastEntry
|  |  |  |  |  |--(1) dot1qStaticUnicastAddress
|  |  |  |  |  |--(2) dot1qStaticUnicastReceivePort
|  |  |  |  |  |--(3) dot1qStaticUnicastAllowedToGoTo
|  |  |  |  |  |--(4) dot1qStaticUnicastStatus
|  |  |  |--(2) dot1qStaticMulticastTable
|  |  |  |  |--(1) dot1qStaticMulticastEntry
|  |  |  |  |  |--(1) dot1qStaticMulticastAddress
|  |  |  |  |  |--(2) dot1qStaticMulticastReceivePort
|  |  |  |  |  |--(3) dot1qStaticMulticastStaticEgressPorts
|  |  |  |  |  |--(4) dot1qStaticMulticastForbiddenEgressPorts
|  |  |  |  |  |--(5) dot1qStaticMulticastStatus
|  |  |--(4) dot1qVlan
|  |  |  |--(1) dot1qVlanNumDeletes
|  |  |  |  |--(3) dot1qVlanStaticTable
|  |  |  |  |  |--(1) dot1qVlanStaticEntry
|  |  |  |  |  |  |--(1) dot1qVlanStaticName
|  |  |  |  |  |  |--(2) dot1qVlanStaticEgressPorts
|  |  |  |  |  |  |--(3) dot1qVlanForbiddenEgressPorts
|  |  |  |  |  |  |--(4) dot1qVlanStaticUntaggedPorts
|  |  |  |  |  |  |--(5) dot1qVlanStaticRowStatus
|  |  |  |  |--(5) dot1qPortVlanTable
|  |  |  |  |  |--(1) dot1qPortVlanEntry
|  |  |  |  |  |  |--(1) dot1qPvid
|  |  |  |  |  |  |--(2) dot1qPortAcceptableFrameTypes
|  |  |  |  |  |  |--(3) dot1qPortIngressFiltering
|  |  |  |  |  |  |--(4) dot1qPortGvrpStatus
|  |  |  |  |  |  |--(5) dot1qPortGvrpFailedRegistrations
|  |  |  |  |  |  |
```

| | | | | | |--(6) dot1qPortGvrpLastPduOrigin

6.1.11 MAU-Management-Gruppe (1.3.6.1.2.1.26)

Die MAU-Management-Gruppe dient zur Festlegung der Autonegotiation-Parameter.

(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

Die Private MIB dient zur Konfiguration der gerätespezifischen Eigenschaften des RS2-../...
Aus der Privaten MIB hmConfiguration (OID = 1.3.6.1.4.1.248.14) sind die Gruppen

- 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)

im RS2-../.. implementiert.

6.2.1 Geräte-Gruppe

Die Geräte-Gruppe enthält Informationen über den Zustand der Hardware des RS2-../...

```
(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
|   |   |   |   |--(15) hmIfaceStpBpduGuardEnable
|   |   |   |   |--(16) hmIfaceStpBpduGuardStatus
|   |   |--(20) hmSysChassisName
|   |   |--(21) hmSysStpEnable
|   |   |--(22) hmSysFlowControl
|   |   |--(23) hmSysBOOTPEnable
|   |   |--(24) hmSysDHCPEnable
|   |   |--(25) hmSysTelnetEnable
|   |   |--(26) hmSysHTTPEnable
|   |   |--(27) hmSysPlugAndPlay
|   |   |--(29) hmBcastLimiterMode
|   |   |--(30) hmSystemTime
|   |   |--(31) hmSystemTimeSource
|   |   |--(32) hmSysStpBPDUGuardEnable
|   |--(2) hmPSTable
|   |   |--(1) hmPSEntry
|   |   |   |--(1) hmPSSysID
|   |   |   |--(2) hmPSID
|   |   |   |--(3) hmPSState
|   |--(5) hmCurrentAddressTable
|   |   |--(1) hmCurrentAddressEntry
```

```
|   |   |   |--(1) hmCurrentAddress
|   |   |   |--(2) hmCurrentAddressReceivePort
|   |   |   |--(3) hmCurrentAddressStaticEgressPorts
|   |   |   |--(4) hmCurrentAddressEgressPorts
|   |   |   |--(5) hmCurrentAddressStatus
|   |--(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
|   |   |--(11) hmRS2VlanGroup
|   |   |   |--(1) hmRS2VlanMode
|   |   |   |--(2) hmRS2VlanStatus
|   |   |--(12) hmRS2SelftestGroup
|   |   |   |--(1) hmRS2SelftestResult
|   |   |   |--(2) hmRS2SelftestMode
|   |   |--(13) hmRS2PSGroup
|   |   |   |--(1) hmRS2PSAlarm
|   |--(12) hmAUIGroup
|   |   |--(10) hmAUIModuleTable
|   |   |   |--(1) hmAUIModuleEntry
|   |   |   |   |--(1) hmAUIModuleID
|   |   |   |   |--(2) hmAUIModuleDTEPowerMonitor
|   |   |--(11) hmAUIPortTable
|   |   |   |--(1) hmAUIPortEntry
|   |   |   |   |--(1) hmAUIPortID
|   |   |   |   |--(2) hmAUIPortDTEPower
```

| | | | |--(3) hmAUIPortSQETest

6.2.2 Management-Gruppe

Die Management-Gruppe enthält Parameter zur Konfiguration des Management-Agenten.

(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
      - (12) hmNetSNTPTimeAdjustThreshold
    - (40) hmNetPTPGroup
      - (1) hmNetPTPConfiguration
        - (1) hmNetPTPEnable
        - (2) hmNetPTPAction
        - (3) hmNetPTPClockMode
        - (4) hmNetPTPSlavePort
        - (5) hmNetPTPIsSynchronized
        - (6) hmNetPTPSyncLowerBound
        - (7) hmNetPTPSyncUpperBound
        - (8) hmNetPTPClockStratum
        - (9) hmNetPTPClockIdentifier

```
|  |  |  |  |
|  |  |  |  |--(10) hmNetPTPClockVariance
|  |  |  |  |--(11) hmNetPTPPreferredMaster
|  |  |  |  |--(12) hmNetPTPSyncInterval
|  |  |  |  |--(13) hmNetPTPSubdomainName
|  |  |  |  |--(14) hmNetPTPOffsetFromMasterNanoSecs
|  |  |  |  |--(15) hmNetPTPAbsMaxOffset
|  |  |  |  |--(16) hmNetPTPOneWayDelayNanoSecs
|  |  |  |  |--(17) hmNetPTPTimeSeconds
|  |  |  |  |--(18) hmNetPTPObservedDrift
|  |  |  |  |--(19) hmNetPTPPiIntegral
|  |  |  |  |--(20) hmNetPTPParentUUID
|  |  |  |  |--(21) hmNetPTPGrandmasterUUID
|  |  |  |  |--(22) hmNetPTPCurrentUTCOffset
|  |  |  |  |--(23) hmNetPTPleap59
|  |  |  |  |--(24) hmNetPTPleap61
|  |  |  |  |--(25) hmNetPTPStepsRemoved
|  |  |  |  |--(26) hmNetPTPEpochNumber
|  |  |  |  |--(27) hmNetPTPStaticDrift
|  |  |  |--(2) hmNetPTPPortTable
|  |  |  |  |--(1) hmNetPTPPortEntry
|  |  |  |  |  |--(1) hmNetPTPPortID
|  |  |  |  |  |--(2) hmNetPTPPortState
|  |  |  |  |  |--(3) hmNetPTPPortBurstEnable
|  |  |  |  |  |--(4) hmNetPTPPortEnable
|  |  |--(50) hmNetSNMPGroup
|  |  |  |--(1) hmNetSNMPv1Status
|  |  |  |--(2) hmNetSNMPv2Status
|  |  |  |--(3) hmNetSNMPv3Status
|  |  |  |--(4) hmNetSNMPAccessStatus
|  |  |  |--(5) hmNetSNMPSynchronizeV1V3Status
|  |--(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
|   |--(10) hmMulticast
|   |   |--(1) hmIGMPGroup
|   |   |   |--(2) hmIGMPSnoop
|   |   |   |   |--(1) hmIGMPSnoopStatus
|   |   |   |   |--(2) hmIGMPSnoopUnknownMode
|   |   |   |   |--(3) hmIGMPSnoopAgingTime
|   |   |   |   |   |--(10) hmIGMPSnoopQueryTable
|   |   |   |   |   |   |--(1) hmIGMPSnoopQueryEntry
|   |   |   |   |   |   |   |--(1) hmIGMPSnoopQueryVlanIndex
|   |   |   |   |   |   |   |--(2) hmIGMPSnoopQueryPorts
|   |   |   |   |   |--(11) hmIGMPSnoopFilterTable
|   |   |   |   |   |   |--(1) hmIGMPSnoopFilterEntry
|   |   |   |   |   |   |   |--(1) hmIGMPSnoopFilterVlanIndex
|   |   |   |   |   |   |   |--(2) hmIGMPSnoopFilterAddress
|   |   |   |   |   |   |   |--(3) hmIGMPSnoopFilterLearntPorts
|   |   |   |   |   |--(12) hmIGMPSnoopForwardAllTable
|   |   |   |   |   |   |--(1) hmIGMPSnoopForwardAllEntry
|   |   |   |   |   |   |   |--(1) hmIGMPSnoopForwardAllVlanIndex
|   |   |   |   |   |   |   |--(2) hmIGMPSnoopForwardAllStaticPorts
|   |   |   |   |   |--(13) hmIGMPSnoopQueryStaticTable
|   |   |   |   |   |   |--(1) hmIGMPSnoopQueryStaticEntry
|   |   |   |   |   |   |   |--(1) hmIGMPSnoopQueryStaticVlanIndex
|   |   |   |   |   |   |   |--(2) hmIGMPSnoopQueryStaticPorts
|   |   |   |   |   |--(100) hmIGMPQuerierGroup
|   |   |   |   |   |   |--(1) hmIGMPQuerierStatus
|   |   |   |   |   |   |--(2) hmIGMPQuerierMode
|   |   |   |   |   |   |--(3) hmIGMPQuerierTransmitInterval
|   |   |   |   |   |   |--(4) hmIGMPQuerierMaxResponseTime
|   |   |   |   |   |   |--(5) hmIGMPQuerierProtocolVersion
|   |--(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 Benutzer-Gruppen-Gruppe

Die Benutzer-Gruppen-Gruppe enthält Parameter zur Konfiguration der Benutzer-Gruppen-Funktion.

(14) hmConfiguration

```
|--(3) hmUserGroup
|   |--(4) hmPortSecurityTable
|   |   |--(1) hmPortSecurityEntry
|   |   |   |--(1) hmPortSecSlotID
|   |   |   |--(2) hmPortSecPortID
|   |   |   |--(3) hmPortSecPermission
|   |   |   |--(4) hmPortSecAllowedUserID
|   |   |   |--(5) hmPortSecAllowedGroupIDs
|   |   |   |--(6) hmPortSecConnectedUserID
|   |   |   |--(7) hmPortSecAction
|   |   |   |--(8) hmPortSecAutoReconfigure
|   |   |   |--(9) hmPortSecPortStatus
|   |   |   |--(10) hmPortSecAllowedUserIPID
```

6.2.4 HIPER-Ring-Redundanz-Gruppe

Die HIPER-Ring-Redundanz-Gruppe enthält Parameter zur Konfiguration der HIPER-Ring-Redundanz.

(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
|   |--(2) hmRingCouplingTable
|   |   |--(1) hmRingCouplingEntry
|   |   |   |--(1) hmRingCplInterconnGroupID
|   |   |   |--(2) hmRingCplInterconnIfIndex
|   |   |   |--(3) hmRingCplInterconnIfOpState
|   |   |   |--(4) hmRingCplControlGroupID
|   |   |   |--(5) hmRingCplControlIfIndex
|   |   |   |--(6) hmRingCplControlIfOpState
|   |   |   |--(7) hmRingCplControlMode
|   |   |   |--(8) hmRingCplPartnerIpAddr
|   |   |   |--(9) hmRingCplPartnerInterconnGroupID
|   |   |   |--(10) hmRingCplPartnerInterconnIfIndex
|   |   |   |--(11) hmRingCplPartnerInterconnIfOpState
|   |   |   |--(12) hmRingCplOperState
|   |   |   |--(13) hmRingCplMode
|   |   |   |--(14) hmRingCplRowStatus
|   |   |   |--(15) hmRingCplConfigOperState
|   |   |   |--(16) hmRingCplCouplingLinks
|   |   |   |--(17) hmRingCplExtendedDiag
|   |   |   |--(18) hmRingCplNetCoupling
```

6.2.5 Topologie-Erkennung-Gruppe

Die Topologie-Erkennungs-Gruppe enthält Parameter zur Topologie-Erkennung.

```
(14) hmConfiguration
   |--(7) hmLLDP
   |   |--(1) hmLLDPConfig
   |   |   |--(1) hmLLDPAdminStatus
   |   |   |--(10) hmLLDPInterfaceTable
   |   |   |   |--(1) hmLLDPIfEntry
   |   |   |   |   |   |--(1) hmLLDPIfaceGroupID
   |   |   |   |   |   |--(2) hmLLDPIfaceID
   |   |   |   |   |   |--(3) hmLLDPIfaceHirmaMode
```

6.3 SNMP V2 Module MIB

Die SNMP V2 Module MIB basiert auf der SNMP-Mib “Simple-Network-Management-Protocol-Gruppe (1.3.6.1.2.1.11)” auf Seite 239.

6.3.1 Framework-Gruppe (1.3.6.1.6.3.10)

Die Framework-Gruppe enthält Parameter zur Beschreibung von SNMP-Management-Grundstrukturen.

(3) `snmpModules`

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

6.3.2 MPD-Gruppe (1.3.6.1.6.3.11)

Die MPD-Gruppe (Message Processing and Dispatching) enthält Parameter zur Verteilung von SNMP-Nachrichten, die womöglich verschiedenen SNMP-Versionen entsprechen.

(3) snmpModules

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

6.3.3 Target-Gruppe (1.3.6.1.6.3.12)

Die Target-Gruppe enthält Parameter zur Spezifikation von Zielen von SNMP-Management-Operationen.

```
(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-Gruppe (1.3.6.1.6.3.13)

Die Notification-Gruppe enthält Parameter zur Spezifikation von Zielen von Filtermeldungen.

(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-Gruppe (1.3.6.1.6.3.15)

Die USM-Gruppe (User-based Security Model) definiert Elemente zur Unterstützung der Sicherheit von SNMP-Nachrichten-Niveaus.

(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-Gruppe (1.3.6.1.6.3.15)

Die VACM-Gruppe (View-based Access Control Model) definiert Elemente zur Zugriffskontrolle von Management-Informationen.

```
(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
```

6.4 IEEE802DOT1-MIB - D10

Die IEEE802DOT1-MIB enthält unter anderem die LLDP-MIB. Die LLDP-MIB beschreibt das Link Layer Discovery Protocol (siehe “Topologie-Erkennung” auf Seite 135).

6.4.1 LLDP-MIB (1.0.8802.1.1.2)

Die LLDP-MIB enthält Parameter zur Beschreibung der topologischen Anbindung eines Gerätes an ein LAN.

```
(3) lldpMIB
   |-- (1) lldpObjects
   |   |-- (1) lldpMessageTxInterval
   |   |-- (2) lldpMessageTxHoldMultiplier
   |   |-- (3) lldpReinitDelay
   |   |-- (4) lldpTxDelay
   |   |-- (5) lldpNotificationInterval
   |   |-- (6) lldpPortConfigTable
   |   |   |-- (1) lldpPortConfigEntry
   |   |   |   |-- (1) lldpPortConfigPortNum
   |   |   |   |-- (2) lldpPortConfigAdminStatus
   |   |   |   |-- (3) lldpPortConfigNotificationEnable
   |   |   |   |-- (4) lldpPortConfigTLVsTxEnable
   |   |-- (7) lldpConfigManAddrTable
   |   |   |-- (1) lldpConfigManAddrEntry
   |   |   |   |-- (1) lldpConfigManAddrPortsTxEnable
   |-- (2) lldpStatistics
   |   |-- (1) lldpStatsRemTablesLastChangeTime
   |   |-- (2) lldpStatsRemTablesInserts
   |   |-- (3) lldpStatsRemTablesDeletes
   |   |-- (4) lldpStatsREmTablesDrops
   |   |-- (5) lldpStatsRemTablesAgeouts
   |   |
```

```
|   |-- (6) lldpStatsPortTable
|   |   |-- (1) lldpStatsPortEntry
|   |   |   |-- (1) lldpStatsPortNum
|   |   |   |-- (2) lldpStatsPortFramesDiscardedTotal
|   |   |   |-- (3) lldpStatsPortFramesInErrors
|   |   |   |-- (4) lldpStatsPortFramesInTotal
|   |   |   |-- (5) lldpStatsPortFramesOutTotal
|   |   |   |-- (6) lldpStatsPortTLVsDiscardedTotal
|   |   |   |-- (7) lldpStatsPortTLVsUnrecognizedTotal
|   |   |   |-- (9) lldpStatsPortAgeouts
|-- (3) lldpLocalSystemData
|   |-- (1) lldpLocChassisIdSubtype
|   |-- (2) lldpLocChassisId
|   |-- (3) lldpLocSysName
|   |-- (4) lldpLocSysDesc
|   |-- (5) lldpLocSysCapSupported
|   |-- (6) lldpLocSysCapEnabled
|   |-- (7) lldpLocPortTable
|   |   |-- (1) lldpLocPortEntry
|   |   |   |-- (1) lldpLocPortNum
|   |   |   |-- (2) lldpLocPortType
|   |   |   |-- (3) lldpLocPortId
|   |   |   |-- (4) lldpLocPortDesc
|   |-- (8) lldpLocManAddrTable
|   |   |-- (1) lldpLocManAddrEntry
|   |   |   |-- (1) lldpLocManAddrSubtype
|   |   |   |-- (2) lldpLocManAddr
|   |   |   |-- (3) lldpLocManAddrLen
|   |   |   |-- (4) lldpLocManAddrIfSubtype
|   |   |   |-- (5) lldpLocManAddrIfId
|   |   |   |-- (6) lldpLocManAddrOID
|-- (4) lldpRemoteSystemsData
|   |-- (1) lldpRemTable
|   |   |-- (1) lldpRemEntry
|   |   |   |-- (1) lldpRemTimeMark
|   |   |   |-- (2) lldpRemLocalPortNum
|   |   |   |-- (3) lldpRemIndex
|   |   |   |-- (4) lldpRemChassisIdSubtype
|   |   |   |-- (5) lldpRemChassisId
|   |   |   |-- (6) lldpRemPortIdSubtype
|   |   |   |-- (7) lldpRemPortId
|   |   |   |-- (8) lldpRemPortDesc
|   |   |   |-- (9) lldpRemSysName
|   |   |   |
```

```
|   |   |   |-- (10) lldpRemSysDesc
|   |   |   |-- (11) lldpRemSysCapSupported
|   |   |   |-- (12) lldpRemSysCapEnabled
|   |-- (2) lldpRemManAddrTable
|   |   |-- (1) lldpRemManAddrEntry
|   |   |   |-- (1) lldpRemManAddrSubtype
|   |   |   |-- (2) lldpRemManAddr
|   |   |   |-- (3) lldpRemManAddrIfSubtype
|   |   |   |-- (4) lldpRemManAddrIfId
|   |   |   |-- (5) lldpRemManAddrOID
|   |-- (3) lldpRemUnkownTLVTable
|   |-- (4) lldpRemOrgDefInfoTable
|-- (5) lldpExtensions
|   |-- (32962) lldpXdot1MIB
|   |   |-- (1) lldpXdot1Objects
|   |   |   |-- (1) lldpXdot1Config
|   |   |   |   |-- (1) lldpXdot1ConfigPortVlanTable
|   |   |   |   |   |-- (1) lldpXdot1ConfigPortVlanEntry
|   |   |   |   |   |   |-- (1) lldpXdot1ConfigPortVlanTxEnable
|   |   |   |   |-- (2) lldpXdot1ConfigVlanNameTable
|   |   |   |   |   |-- (1) lldpXdot1ConfigVlanNameEntry
|   |   |   |   |   |   |-- (1) lldpXdot1ConfigVlanNameTxEnable
|   |   |   |   |-- (3) lldpXdot1ConfigProtoVlanTable
|   |   |   |   |   |-- (1) lldpXdot1ConfigProtoVlanEntry
|   |   |   |   |   |   |-- (1) lldpXdot1ConfigProtoVlanTxEnable
|   |   |   |   |-- (4) lldpXdot1ConfigProtocolTable
|   |   |   |   |   |-- (1) lldpXdot1ConfigProtocolEntry
|   |   |   |   |   |   |-- (1) lldpXdot1ConfigProtocolTxEnable
|   |   |   |-- (2) lldpXdot1LocalData
|   |   |   |   |-- (1) lldpXdot1LocTable
|   |   |   |   |   |-- (1) lldpXdot1LocEntry
|   |   |   |   |   |   |-- (1) lldpXdot1LocPortVlanId
|   |   |   |   |-- (2) lldpXdot1LocProtoVlanTable
|   |   |   |   |   |-- (1) lldpXdot1LocProtoVlanEntry
|   |   |   |   |   |   |-- (1) lldpXdot1LocProtoVlanId
|   |   |   |   |   |   |-- (2) lldpXdot1LocProtoVlanSupported
|   |   |   |   |   |   |-- (3) lldpXdot1LocProtoVlanEnabled
|   |   |   |   |-- (3) lldpXdot1LocVlanNameTable
|   |   |   |   |   |-- (1) lldpXdot1LocVlanNameEntry
|   |   |   |   |   |   |-- (1) lldpXdot1LocVlanId
|   |   |   |   |   |   |-- (2) lldpXdot1LocVlanName
|   |   |   |   |-- (4) lldpXdot1LocProtocolTable
|   |   |   |   |   |-- (1) lldpXdot1LocProtocolEntry
```

```
|  |  |  |  |  |  |-- (1) lldpXdot1LocProtocolIndex
|  |  |  |  |  |  |-- (2) lldpXdot1LocProtocolId
|  |  |  |-- (3) lldpXdot1RemoteData
|  |  |  |  |-- (1) lldpXdot1RemTable
|  |  |  |  |  |-- (1) lldpXdot1RemEntry
|  |  |  |  |  |  |-- (1) lldpXdot1RemPortVlanId
|  |  |  |  |-- (2) lldpXdot1RemProtoVlanTable
|  |  |  |  |  |-- (1) lldpXdot1RemProtoVlanEntry
|  |  |  |  |  |  |-- (1) lldpXdot1RemProtoVlanId
|  |  |  |  |  |  |-- (2) lldpXdot1RemProtoVlanSupported
|  |  |  |  |  |  |-- (3) lldpXdot1RemProtoVlanEnabled
|  |  |  |  |-- (3) lldpXdot1RemVlanNameTable
|  |  |  |  |  |-- (1) lldpXdot1RemVlanNameEntry
|  |  |  |  |  |  |-- (1) lldpXdot1RemVlanId
|  |  |  |  |  |  |-- (2) lldpXdot1RemVlanName
|  |  |  |  |-- (4) lldpXdot1RemProtocolTable
|  |  |  |  |  |-- (1) lldpXdot1RemProtocolEntry
|  |  |  |  |  |  |-- (1) lldpXdot1RemProtocolIndex
|  |  |  |  |  |  |-- (2) lldpXdot1RemProtocolId
|  |-- (4623) lldpXdot3MIB
|  |  |-- (1) lldpXdot3Objects
|  |  |  |-- (1) lldpXdot3Config
|  |  |  |  |-- (1) lldpXdot3PortConfigTable
|  |  |  |  |  |-- (1) lldpXdot3PortConfigEntry
|  |  |  |  |  |  |-- (1) lldpXdot3PortConfigTLVsTxEnable
|  |  |  |-- (2) lldpXdot3LocalData
|  |  |  |  |-- (1) lldpXdot3LocPortTable
|  |  |  |  |  |-- (1) lldpXdot3LocPortEntry
|  |  |  |  |  |  |-- (1) lldpXdot3LocPortAutoNegSupported
|  |  |  |  |  |  |-- (2) lldpXdot3LocPortAutoNegEnabled
|  |  |  |  |  |  |-- (3) lldpXdot3LocPortPMDCapability
|  |  |  |  |  |  |-- (4) lldpXdot3LocPortPMDDefaultConfig
|  |  |  |  |  |  |-- (5) lldpXdot3LocPortFaultIndication
|  |  |  |  |-- (2) lldpXdot3LocPowerTable
|  |  |  |  |  |-- (1) lldpXdot3LocPowerEntry
|  |  |  |  |  |  |-- (1) lldpXdot3LocPowerPortClass
|  |  |  |  |  |  |-- (2) lldpXdot3LocPowerMDISupported
|  |  |  |  |  |  |-- (3) lldpXdot3LocPowerMDIEnabled
|  |  |  |  |  |  |-- (4) lldpXdot3LocPowerPairControlable
|  |  |  |  |  |  |-- (5) lldpXdot3LocPowerPairs
|  |  |  |  |  |  |-- (6) lldpXdot3LocPowerClass
|  |  |  |  |-- (3) lldpXdot3LocLinkAggTable
|  |  |  |  |  |-- (1) lldpXdot3LocLinkAggEntry
```

```
|  |  |  |  |  |  |-- (1) lldpXdot3LocLinkAggStatus
|  |  |  |  |  |  |-- (2) lldpXdot3LocLinkAggPortId
|  |  |  |-- (3) lldpXdot3RemoteData
|  |  |  |  |-- (1) lldpXdot3RemPortTable
|  |  |  |  |  |-- (1) lldpXdot3RemPortEntry
|  |  |  |  |  |  |-- (1) lldpXdot3RemPortAutoNegSupported
|  |  |  |  |  |  |-- (2) lldpXdot3RemPortAutoNegEnabled
|  |  |  |  |  |  |-- (3) lldpXdot3RemPortPMDCapability
|  |  |  |  |  |  |-- (4) lldpXdot3RemPortPMDDefaultConfig
|  |  |  |  |  |  |-- (5) lldpXdot3RemPortFaultIndication
|  |  |  |  |-- (2) lldpXdot3RemPowerTable
|  |  |  |  |  |-- (1) lldpXdot3RemPowerEntry
|  |  |  |  |  |  |-- (1) lldpXdot3RemPowerPortClass
|  |  |  |  |  |  |-- (2) lldpXdot3RemPowerMDISupported
|  |  |  |  |  |  |-- (3) lldpXdot3RemPowerMDIEnabled
|  |  |  |  |  |  |-- (4) lldpXdot3RemPowerPairControlable
|  |  |  |  |  |  |-- (5) lldpXdot3RemPowerPairs
|  |  |  |  |  |  |-- (6) lldpXdot3RemPowerClass
|  |  |  |  |-- (3) lldpXdot3RemLinkAggTable
|  |  |  |  |  |-- (1) lldpXdot3RemLinkAggEntry
|  |  |  |  |  |  |-- (1) lldpXdot3RemLinkAggStatus
|  |  |  |  |  |  |-- (2) lldpXdot3RemLinkAggPortId
```

7 User Interface

Das User Interface bietet dem Anwender die Möglichkeit einige Funktionen des RS2-../.. menügeführt zu bedienen.

Folgende Menüpunkte stehen zur Auswahl:
- System Parameter
- Switching General
- Switch Security
- Port Configuration / Statistics
- Port Mirroring / Disable Learning
- Redundant Ring / Net Coupling
- Configuration
- Update
- Password
- Ping
- System Reset

7.1 Öffnen des User Interfaces

☐ Nach dem Verbinden des RS2-../.. mit einem VT100-Terminal über V.24 drücken Sie eine Taste. Auf dem Bildschirm erscheint ein Fenster für die Paßwort-Eingabe.
Nur ein Benutzer kann auf das User Interface zugreifen.

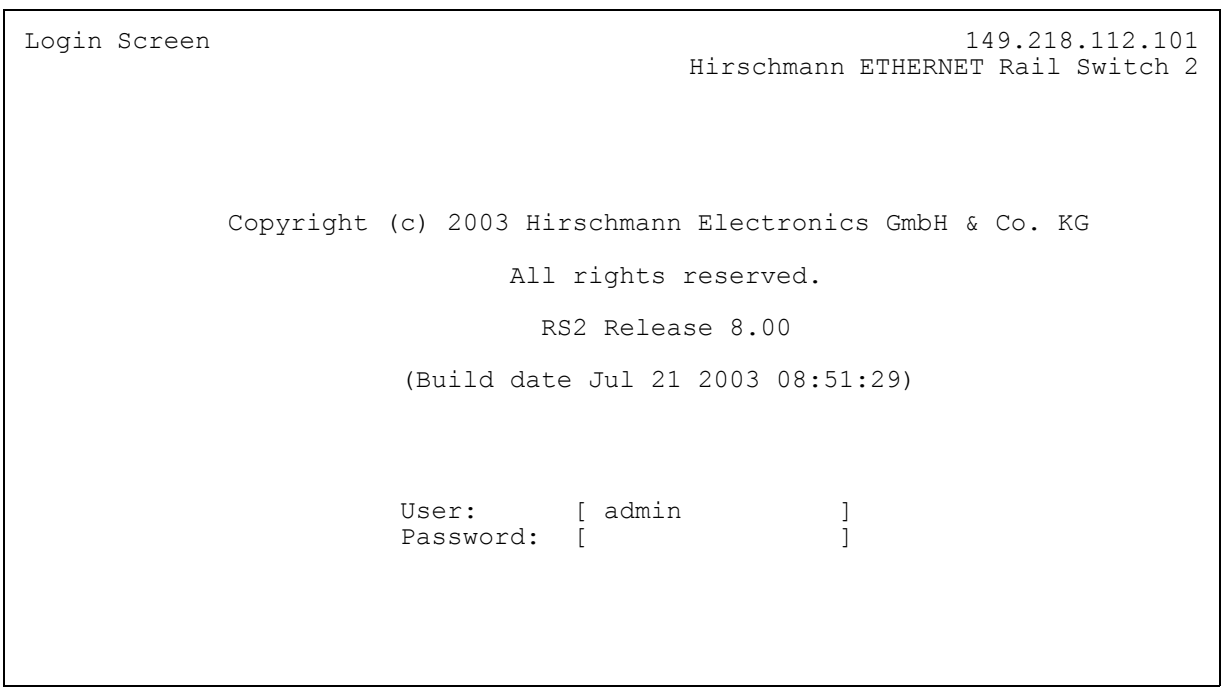


Abb. 96: Einloggen in das User Interface Programm

☐ Geben Sie das Paßwort ein. Im Lieferzustand ist das Paßwort **`private`** eingetragen. Sie können das Paßwort später im User Interface (siehe “Password” auf Seite 290) oder über das WWW-Interface ändern. Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

Der Hauptmenü-Bildschirm erscheint.

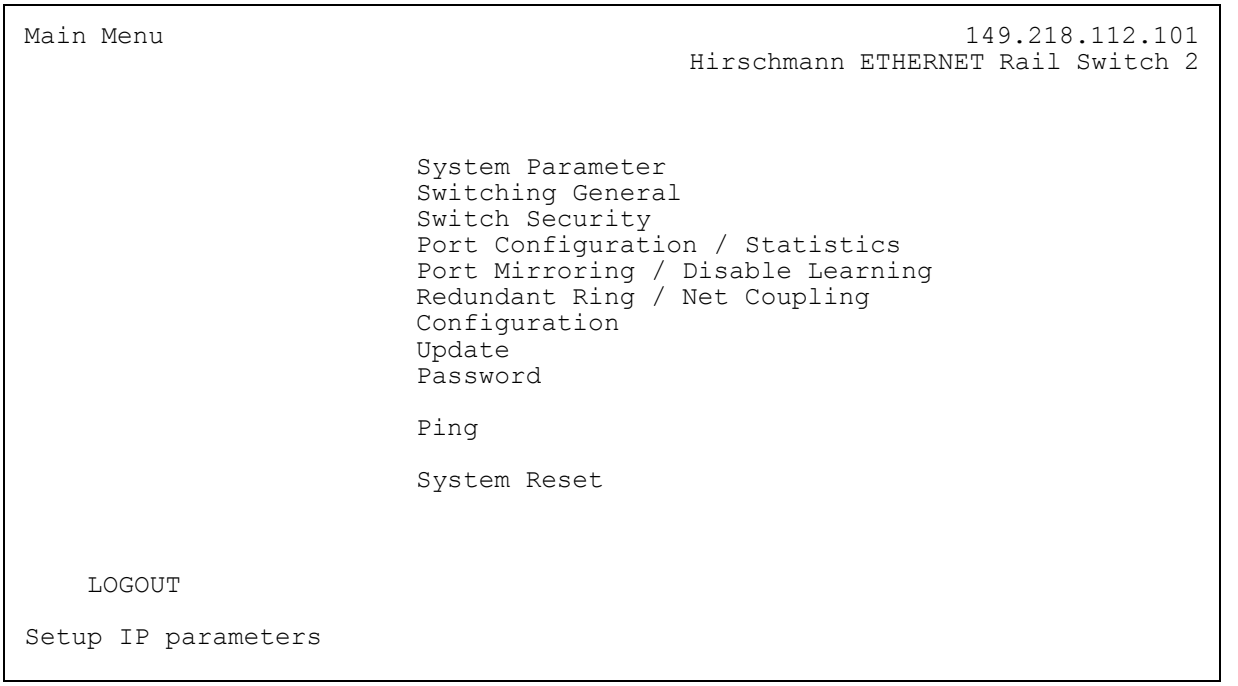


Abb. 97: Hauptmenü

7.2 Bedienen des User Interfaces

- Die Fortbewegung des Cursors geschieht mit den Pfeiltasten oder der Tabulatortaste.
- Das Umschalten vorgegebener Werte in einem Auswahlfeld geschieht beim Drücken der Leertaste.
- Die vorgenommenen Einstellungen werden übernommen, wenn der Cursor auf dem Feld APPLY steht und die Eingabetaste gedrückt wird.
- Die unterste Zeile enthält einen Hilfstext zu dem ausgewählten Punkt.
- Zum Verlassen des User Interfaces wählen Sie `LOGOUT` im Hauptmenü und drücken Sie die Eingabetaste.

Das Hauptmenü besteht aus 7 Untermenüs.

7.2.1 System Parameter

Dieses Menü dient

- zur Eingabe von
  – IP-Adresse,
  – Subnetz Maske,
  – Gateway IP-Adresse und
  – VLAN ID.
- zum Aktivieren/Deaktivieren von BOOTP/DHCP.
- zur Anzeige der MAC-Adresse des RS2-../...

```
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        ]
                          VLAN ID (0=all)   : [0   ]

                          IP Configuration : < LOCAL >

                          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)
```

Abb. 98: Menü System Parameter

- **IP-Adresse**
  Geben Sie hier die IP-Adresse dieses RS2-../.. ein. Im Lieferzustand ist die Adresse 0.0.0.0 eingetragen.

- **Subnetzmaske**
  Falls Sie in einem großen Netz arbeiten und Netzmasken nutzen, können Sie hier die Netzmaske des Subnetzes, mit dem Ihr RS2-../.. verbunden ist, angeben. Im Lieferzustand ist die IP-Adresse 0.0.0.0 eingetragen.

- **Gateway IP-Adresse**
  Geben Sie hier die IP-Adresse des Gateways ein, über welches der RS2-../.. andere Subnetze adressieren soll. Wenn kein solches Gateway vorhanden ist, kann die Eingabe entfallen. Im Lieferzustand ist die IP-Adresse 0.0.0.0 eingetragen.

VLAN ID

Dieser Eintrag bietet Ihnen die Möglichkeit, dem Agenten ein VLAN zuzuweisen. Mit dem Eintrag 0 ist der Agent aus jedem VLAN erreichbar.

IP-Konfiguration

☐ Wählen Sie den gewünschten IP-Konfigurations-Modus aus. Durch drücken der Leertaste stehen folgend Möglichkeiten zur Wahl:

– `Local`
– `BOOTP`
– `DHCP`

Nach dem Durchführen von APPLY ist er ausgewählte Modus aktiv (siehe “Grundeinstellungen” auf Seite 45).

MAC-Adresse

Dieses Feld zeigt die MAC-Adresse des Gerätes an.

System Name

☐ Benennen Sie Ihren RS2-../.. mit einem beliebigen Namen (siehe “System-Konfiguration via DHCP (dynamic host configuration protocol)” auf Seite 59).

7.2.2 Switching General

Der Switch unterstützt Rapid Spanning Tree, IGMP und GMRP sowie VLANs.

☐ Zum Aktivieren wählen Sie die Zeile aus. Durch drücken der Leertaste wechselt die Einstellung von `Disable` auf `Enable`.
Nach dem Durchführen von APPLY ist die Funktion sofort aktiv.

```
Switching General                                          149.218.112.101
                                                Hirschmann ETHERNET Rail Switch 2



   Rapid Spanning Tree : < Disable     >
   GMRP                : < Disable >
   IGMP-Snooping       : < Disable >


   VLAN Mode:   < Disable >
   VLAN Status:   Disable

   Note:

   GMRP and IGMP-Snooping can not be enabled at the same time.

   APPLY changes the state of the object immediately.



   MAIN MENU  APPLY

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

Abb. 99: Menü Switching General

7.2.3 Switch Security

Der Zugriff auf den Switch ist möglich über:

- V.24
- Telnet
- Web.

☐ Um den Zugriff über Telnet oder das Web freizugeben, wählen Sie die Telnet- oder Web-Zeile aus. Durch drücken der Leertaste wechselt die Einstellung von `Disable` auf `Enable`.
Nach dem Durchführen von APPLY ist die neue Einstellung sofort aktiv.

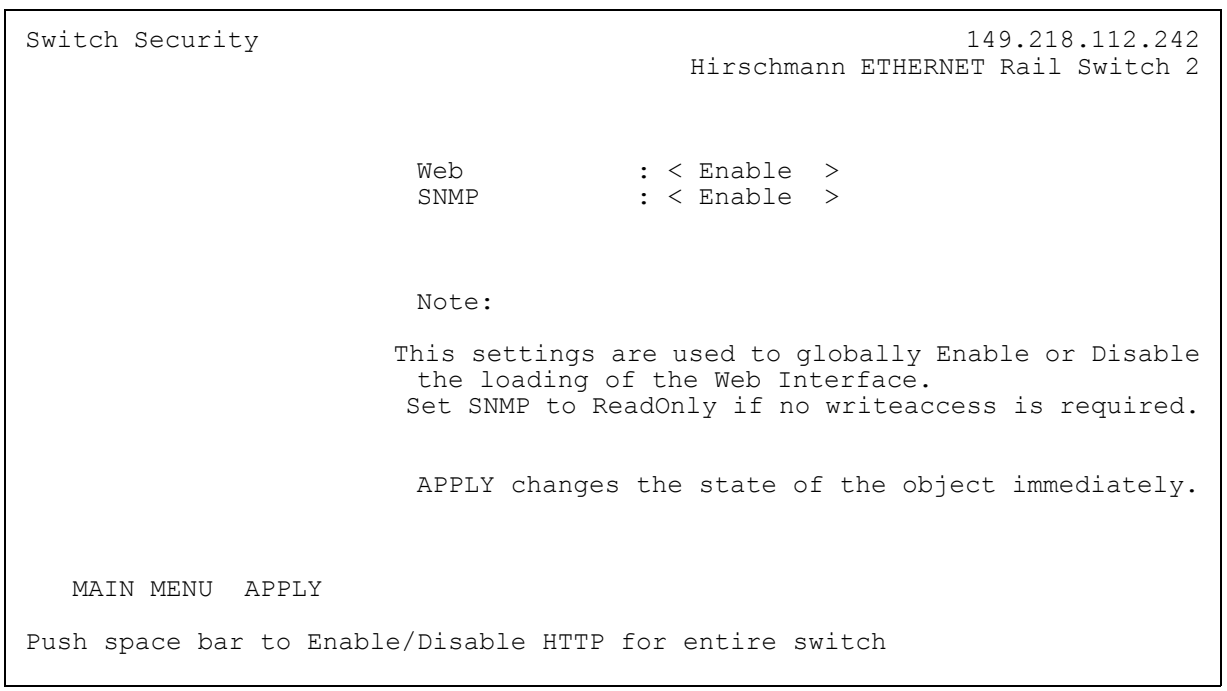


Abb. 100: Menü Switch Security

7.2.4 Port Configuration / Statistics

Dieses Menü dient zur Portkonfiguration und zur Anzeige der Portstatistik.

☐ Geben Sie zunächst die Portnummer ein und drücken Sie die Eingabetaste.

☐ Hinter `Port Name` können Sie einen beliebigen Namen für diesen Port eingeben.

- State
  - `Disable` schaltet den Port ab
  - `Enable` schaltet den Port ein
- Übertragungsgeschwindigkeit
  - `autonegotiate` aktiviert die Autonegotiation-Funktion
  - `10MHDX` 10 Mbit/s, halbduplex
  - `10MFDX` 10 Mbit/s, vollduplex
  - `100MHDX` 100 Mbit/s, halbduplex
  - `100MFDX` 100 Mbit/s, vollduplex

```
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
```

Abb. 101: Menü Portkonfiguration

7.2.5 Port Mirroring / Disable Learning

Dieser Dialog bietet Ihnen die Möglichkeit, die Daten aller Ports zu beobachten (Monitoring).

- Mit der Auswahl `Disable Learning` schalten Sie die Lern-Funktion des RS2-../.. aus. Damit überträgt der RS2-../.. alle Daten von allen Ports an alle Ports.
- Mit der Auswahl `Port Mirroring` spiegelt der RS2-../.. alle Sende-/ Empfangsdaten des "Source port" auf den "Destination port". Für die anderen Ports arbeitet der RS2-../.. wie ein normaler Switch
- Mit der Auswahl `Normal Switching` schalten Sie die Lernfunktion des RS2-../.. ein und er arbeitet wie ein normaler Switch.

Hinweis: Nach einem Neustart ist die Einstellung `Normal Switching` aktiv.

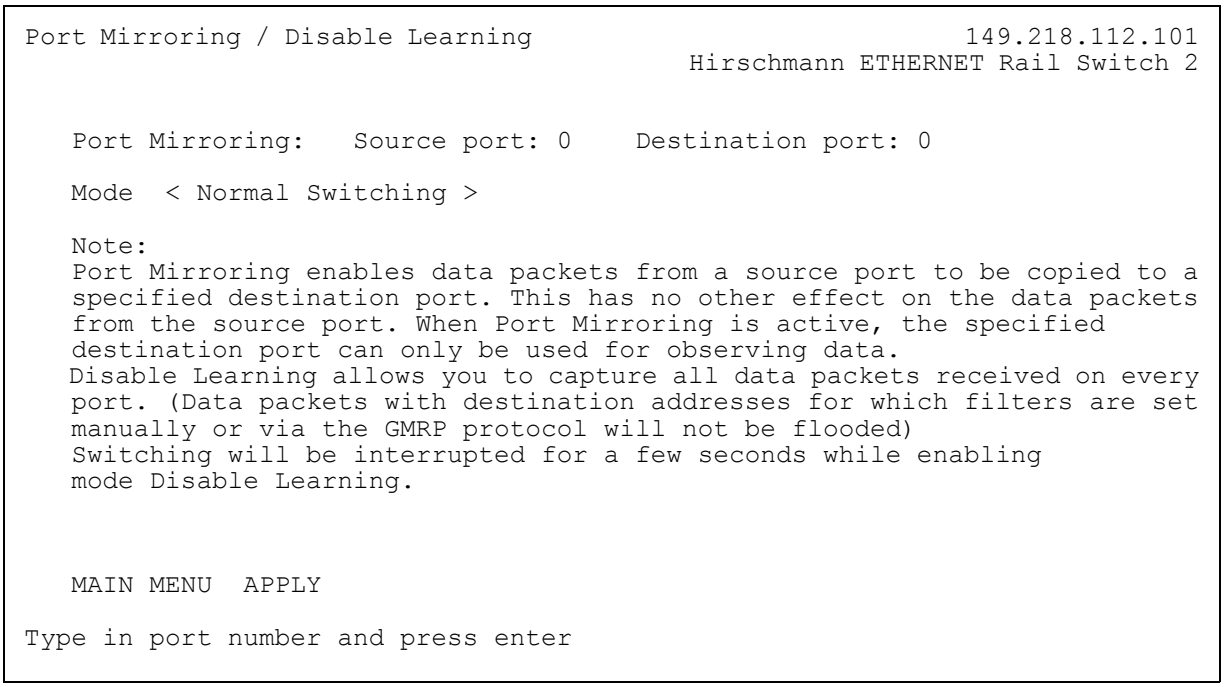


Abb. 102: Menü Disable Learning

7.2.6 Redundant Ring / Net Coupling

Dieser Dialog bietet Ihnen die Möglichkeit, die redundante Kopplung von Netzsegmenten (siehe “Redundante Kopplung von HIPER-Ringen und Netzsegmenten” auf Seite 127 und “Konfiguration der redundanten Kopplung von HIPER-Ringen und Netzsegmenten” auf Seite 211) zu konfigurieren.

- „Configuration“ bietet Ihnen die Möglichkeit, die Konfiguration der Kopplung auszuwählen.
  - `dual active control port`: Kopplungsport und Partner-Kopplungsport sind verteilt auf zwei Switche, die mit der Steuerleitung verbunden sind.
  - `single`: Kopplungsport und Partner-Kopplungsport befinden sich auf einem Switch.
  - `dual active`: Kopplungsport und Partner-Kopplungsport sind verteilt auf zwei Switche.
    Die Einstellung "Stand-by" für den Switch in der redundanten Strecke nehmen Sie mit dem 2poligen DIP-Schalter am Gerät vor.
- „Coupling Port“ ist der Port 1.
- „Partner Port“ ist der Kopplungsport am Partner-Switch.
- „Control Port“ ist der „Stand-by"-.
- „Extended Redundancy“ schaltet beim Ausfall der Verbindungsleitung zwischen den Switches im angekoppelten Netz die Haupt- und die Stand-by-Leitung gleichzeitig aktiv.
  - `No`: keine erweiterte Redundanz
  - `Yes`: erweiterte Redundanz.
- „Coupling Mode“ Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.
  - `Ring`: Wählen Sie `Ring`, wenn Sie einen HIPER-Ring ankoppeln.
  - `Net`: Wählen Sie `Net`, wenn Sie eine Linienstruktur ankoppeln.
- „Operation“ zeigt den Funktionsstatus der Kopplung an.

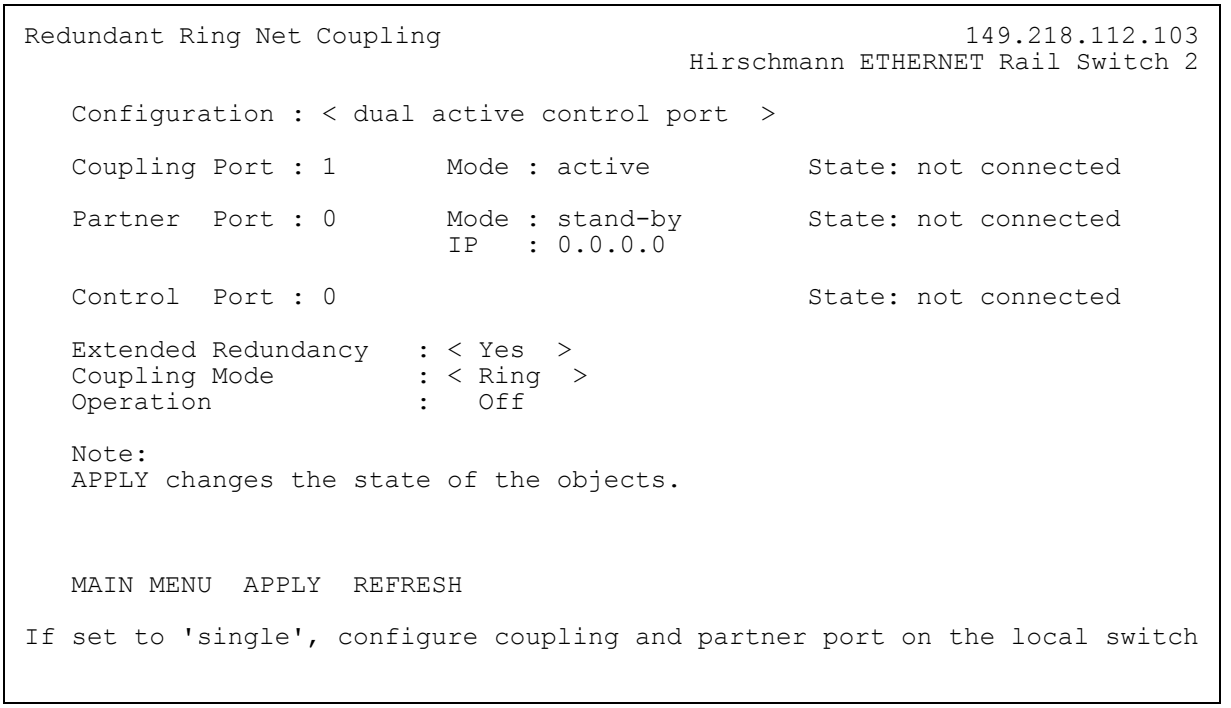


Abb. 103: Menü Redundant Net Coupling

Hinweis: Für die Datenports sind folgende Einstellungen erforderlich:
– Autonegotiation an
– Port an.

7.2.7 Configuration

Der RS2-../.. kennt zwei Konfigurationseinstellungen:
- die voreingestellte und
- die vom Benutzer definierte.

Dieses Untermenü bietet die Möglichkeit, eine vom Benutzer definierte Konfiguration zu speichern.
Diese Konfiguration kann
– automatisch während eines Neustarts oder
– nach einem Neustart mit der voreingestellten Konfiguration wieder geladen werden.

Mit `Load after reset` bestimmen Sie, welche Konfigurationseinstellung nach einem Neustart aktiv sein wird:
– `default` lädt die voreingestellte Konfiguration,
– `local` lädt die vom Benutzer definierte Konfiguration aus dem Flash-Speicher,
– `remote` lädt die vom Benutzer definierte Konfiguration aus der Konfigurationsdatei vom tftp-Server.

Mit `Load` bestimmen Sie, welche Konfigurationseinstellung geladen wird:
– `local` lädt die vom Benutzer definierte Konfiguration aus dem Flash-Speicher,
– `remote` lädt die vom Benutzer definierte Konfiguration aus der Konfigurationsdatei vom tftp-Server.

Mit `Save` bestimmen Sie, wo die Konfigurationseinstellung gespeichert wird:
– `local` speichert die vom Benutzer definierte Konfiguration in den Flash-Speicher,
– `remote` speichert die vom Benutzer definierte Konfiguration als Konfigurationsdatei auf den tftp-Server.
– `configadapter` speichert die vom Benutzer definierte Konfiguration in den AutoConfiguration Adapter und in den Flash-Speicher.

Änderungen in diesem Fenster werden mit `APPLY` übernommen.

Der Pfad für die Ablage der Konfigurationsdaten auf dem tftp-Server steht in der Zeile „URL“.
tftp ist nicht in der Lage, neue Dateien anzulegen. Deshalb legen Sie eine leere Datei auf dem tftp-Server an, bevor Sie die Konfiguration „Auf URL speichern“.

Beispiel zum Speichern auf einem tftp-Server

- ☐ Öffnen Sie in einem Editor eine neue Datei.
- ☐ Speichern Sie die leere Datei in den entsprechenden Pfad des tftp-Servers mit dem Dateinamen, z.B. `RS2/RS2_01.cfg`
- ☐ Geben Sie in der Zeile „URL“ den Pfad des tftp-Servers ein, z.B. `tftp://149.218.112.214/RS2/RS2_01.cfg`.

Hinweis: Die Konfigurationsdatei enthält alle Konfigurationsdaten, auch das Paßwort. Achten Sie deshalb auf die Zugriffsrechte auf dem tftp-Server.

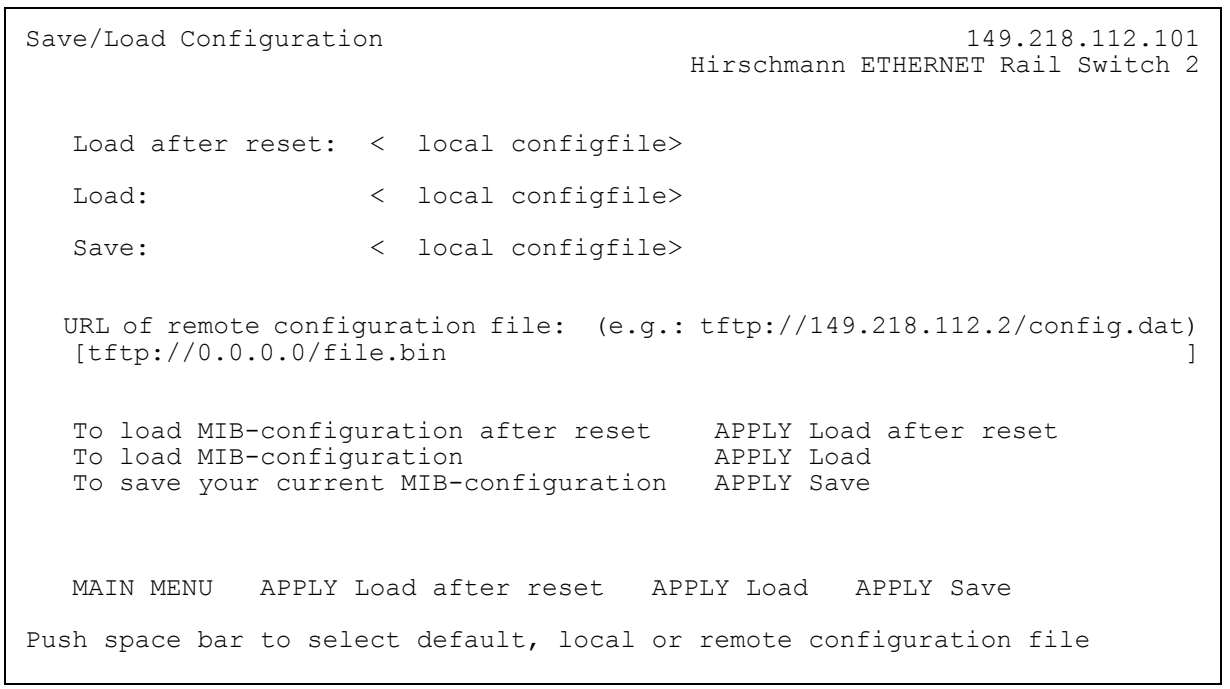


Abb. 104: Menü Save/Load Configuration

Die Auswahl des AutoConfiguration Adapters ACA für eine Speicheroperation öffnet nach `Apply` ein neues Fenster mit der Aufforderung:

- ☐ Ziehen Sie das Terminalkabel vom RS2-../.. ab und stekken Sie den ACA in den V.24-Anschluß des RS2-../...

Danach führt der RS2-../.. die Speicheroperation durch. Die LEDs RM und Standby zeigen den Status der Speicheroperation an.

Anzeige	Bedeutung
LEDs blinken alternativ	Fehler bei der Speicheroperation
LEDs blinken synchron; 2 mal pro Sekunde	Laden der Konfiguration vom ACA
LEDs blinken synchron 1 mal Pro Sekunde	Speichern der Konfiguration in den ACA

Tab. 16: Anzeige der Speicheroperation beim ACA

Der Übergang vom blinkenden in einen statischen Zustand der LEDs zeigt das Ende der Speicheroperation an.

☐ Um das User Interface weiter bedienen zu können, ziehen Sie den ACA vom RS2-../.. ab und stecken Sie das Terminalkabel in den V.24-Anschluß des RS2-../...

```
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
```

Abb. 105: Menü Speicheroperation AutoConfiguration Adapter

7.2.8 Update

Bevor Sie ein Update durchführen können, benötigen Sie die korrekte Pfadangabe zur Update-Datei.

☐ Geben Sie im Feld `URL of update file` den korrekten Pfad ein und drücken Sie die Eingabetaste.

In der Zeile `Reset` wählen Sie, ob der RS2-../.. gleich nach dem Laden des Updates oder erst zu einem späteren Zeitpunkt einen Neustart durchführen soll.

Mit `Apply` wird das Update geladen. Nach einem Neustart ist es aktiv.

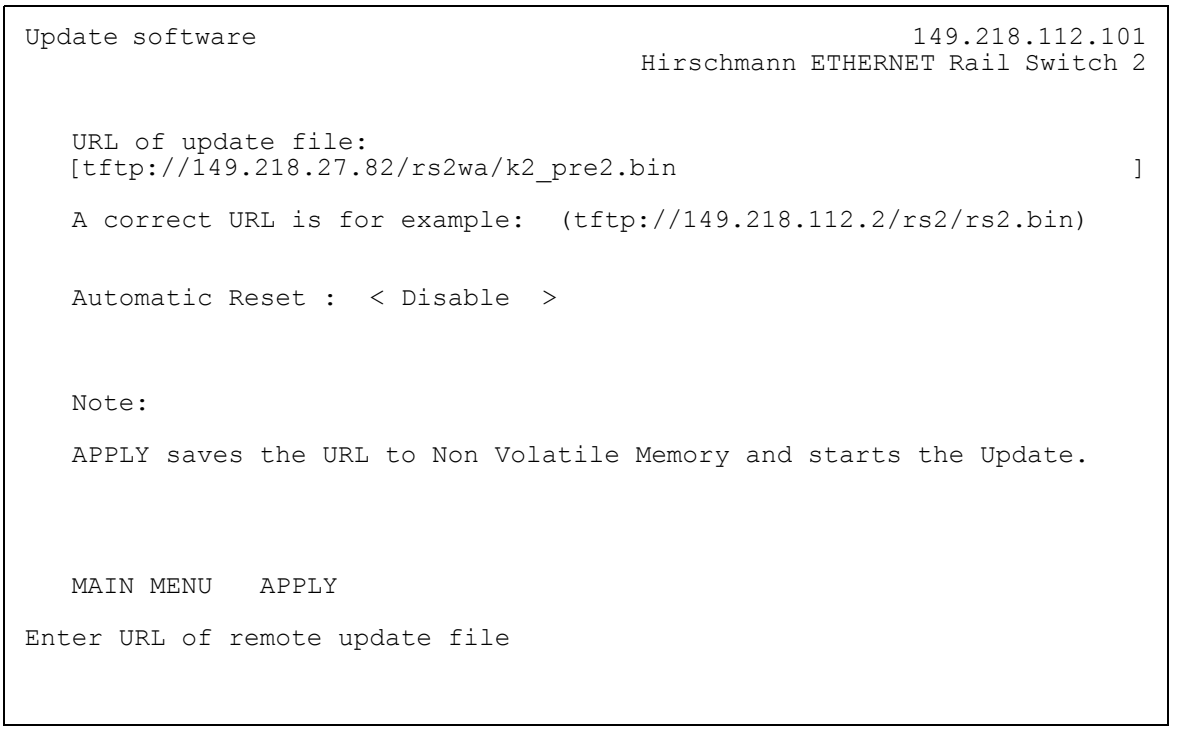


Abb. 106: Menü Update RS2-../..

7.2.9 Password

Um Ihren RS2-../.. vor unberechtigten Zugriffen zu schützen, ändern Sie in diesem Untermenü das Schreib-/Lesepaßwort für SNMP Version 3 und das Schreib-/Lesepaßwort für SNMP Version 1/2c.

☐ Das Web-based Interface und das User Interface kommunizieren über SNMP Version 3. Wählen Sie "SNMPv1/2c YES", um mit früheren Versionen von SNMP kommunizieren zu können.

☐ Geben Sie im Feld `Old SNMPv3 Password` Ihr altes Paßwort ein und drücken Sie die Eingabetaste.

☐ Geben Sie im Feld `New SNMPv3 Password` Ihr neues Paßwort ein und drücken Sie die Eingabetaste.

☐ Wiederholen Sie die Eingabe Ihres neuen Paßwortes im Feld `Retype SNMPv3 Password` und drücken Sie die Eingabetaste.

☐ Geben Sie im Feld `SNMPv1/2c Password` Ihr neues Paßwort ein und drücken Sie die Eingabetaste.

☐ Wiederholen Sie die Eingabe Ihres neuen Paßwortes im Feld `Retype SNMPv1/2c Password` und drücken Sie die Eingabetaste.

☐ Um die neuen Paßwörter zu übernehmen, wählen Sie `APPLY` und drükken Sie die Eingabetaste.

☐ Damit die neuen Paßwörter nach einem Neustart wieder verfügbar sind, speichern sie diese Konfiguration (siehe “Configuration” auf Seite 286).

```
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
```

Abb. 107: Menü Change Password

7.2.10 Ping

Das Menü Ping dient zur Prüfung der Erreichbarkeit eines anderen Netzteilnehmers.

☐ Geben Sie im Feld `IP Address of host` die IP-Adresse des gewünschten Teilnehmers ein und drücken Sie die Eingabetaste.

Mit `Apply` wird die Antwort des gewünschten Teilnehmers abgerufen.

Je nach Erreichbarkeit des Teilnehmers erhalten Sie die Antwort:

`Host alive` oder
`Host not alive`.

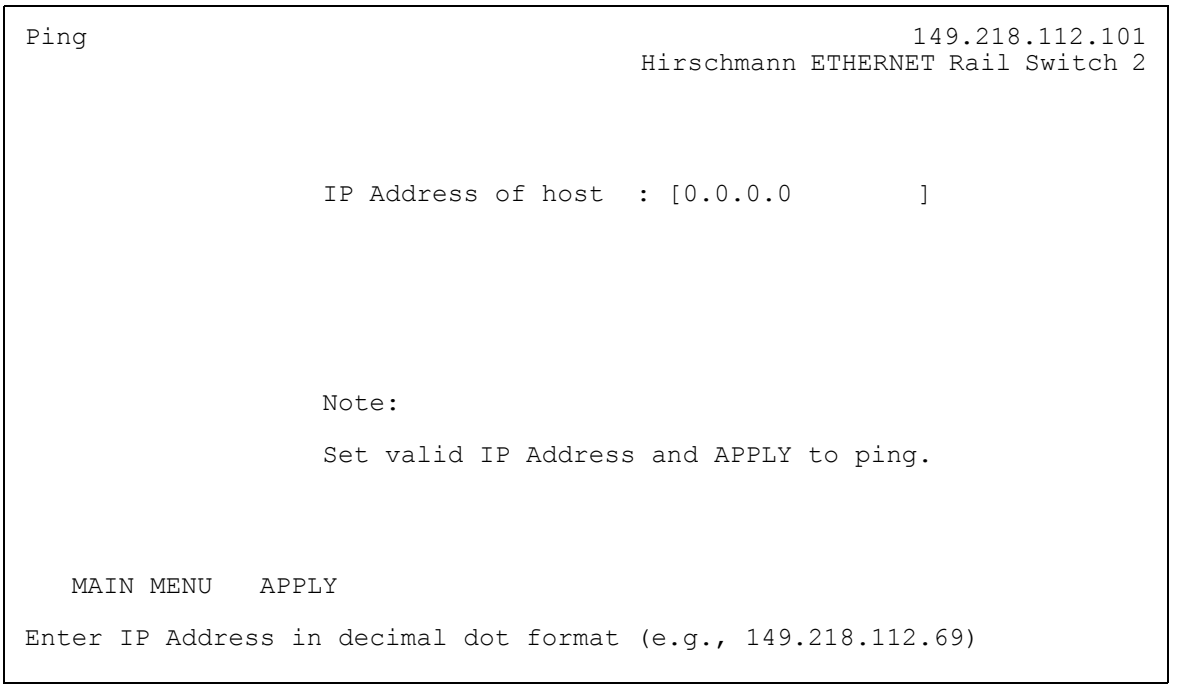


Abb. 108: Menü Ping

7.2.11 System Reset

☐ Zum Ausführen eines Neustarts wählen Sie die `Confirm Reset`-Zeile aus.
Durch drücken der Leertaste wechstelt die Einstellung von `No` auf `Yes`.
Nach dem Durchführen von `APPLY` führt der Switch einen Neustart durch.

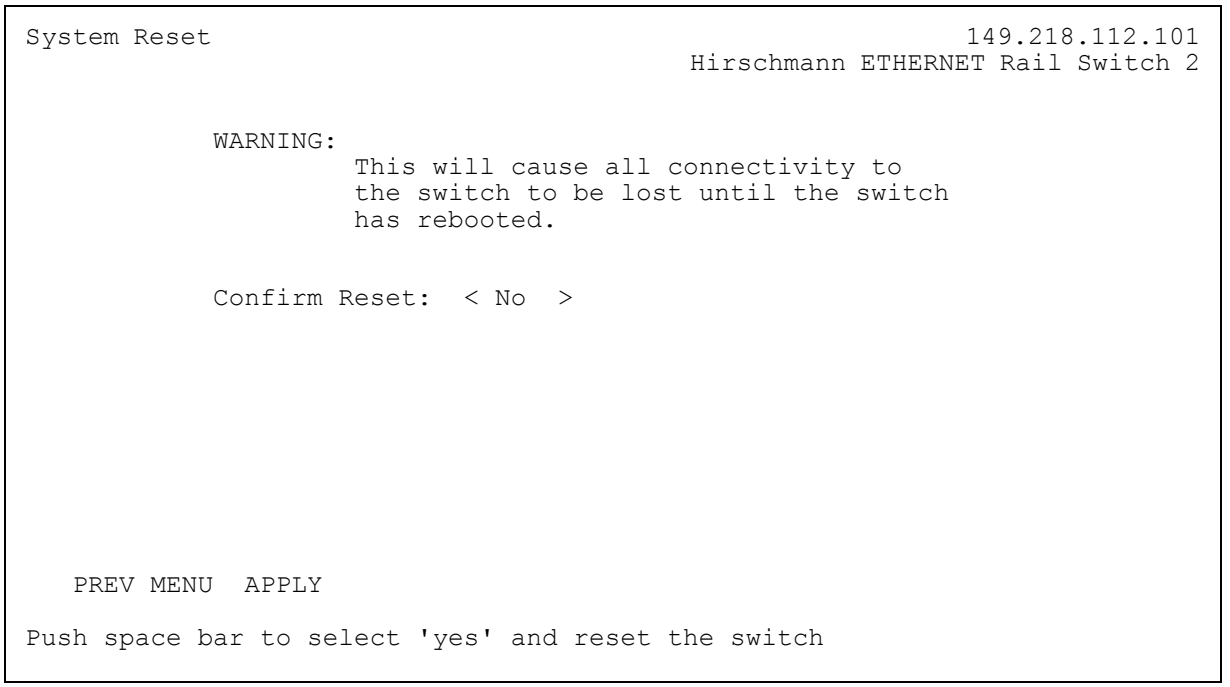


Abb. 109: Menü System Reset

A Anhang

Häufig gestellte Fragen

Antworten zu häufig gestellten Fragen finden Sie in den Internetseiten von Hirschmann:

`www.hirschmann.com`

Unter `Produkte/Service` im Geschäftsbereich `Automation and Network Solutions` gibt es auf den Seiten `Produkte` die Rubrik `FAQ`.

Detaillierte Information zu allen Dienstleistungen des Hirschmann Competence Centers finden Sie auf der Web-Seite http://www.hicomcenter.com/.

DHCP-Server Option 82 einrichten

Auf der CDROM, die dem Switch bei der Lieferung beiliegt, finden Sie die Software für einen DHCP-Server der Firma Softwareentwicklung, IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

☐ Zur Installation des DHCP-Servers auf Ihrem PC
legen Sie die CDROM in das CD-Laufwerk Ihres PCs und
wählen Sie unter Zusatzsoftware "haneWIN DHCP-Server".
Führen Sie die Installation gemäß des Installationsassistenten durch.

☐ Starten Sie das Programm `DHCP Server`.

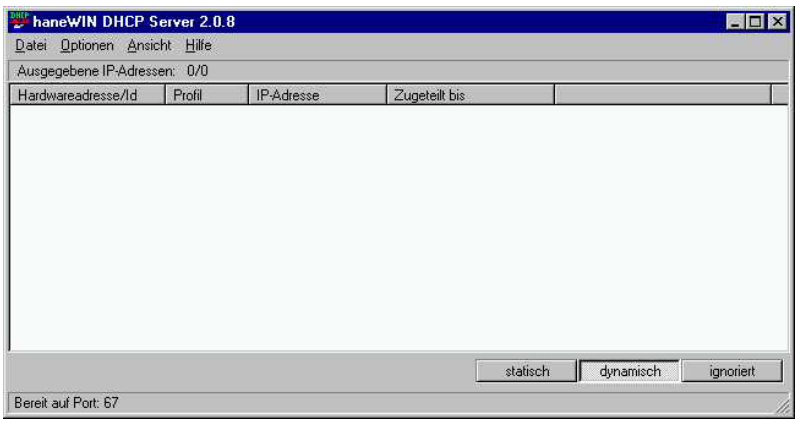


Abb. 110: Startfenster des DHCP-Servers

☐ Wählen Sie `statisch`.

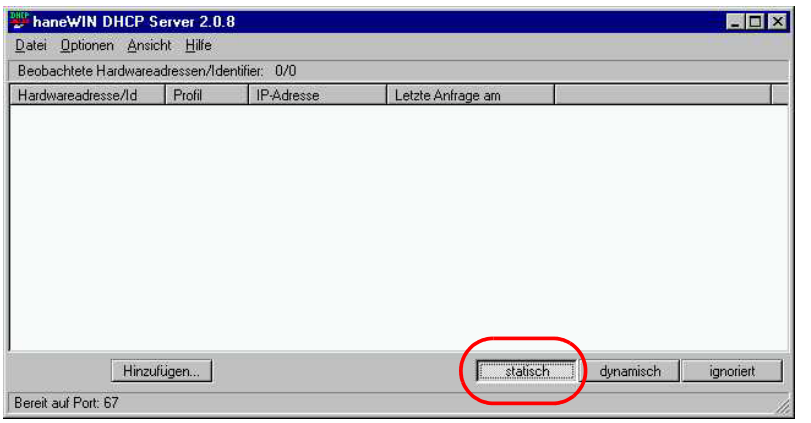


Abb. 111: Statische Adreßeingabe

☐ Öffnen Sie das Fenster für die Programmeinstellungen in der Menüleiste: `Optionen:Einstellungen` und wählen Sie die Karteikarte `DHCP`.

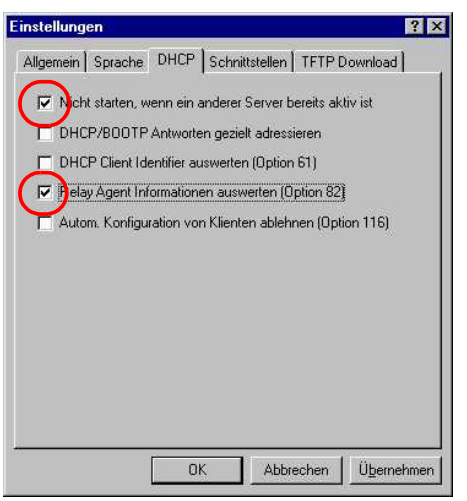


Abb. 112: DHCP-Einstellung

☐ Wählen Sie die Karteikarte `DHCP`. Nehmen Sie die im Bild dargestellten Einstellungen vor und klicken Sie auf `OK`.

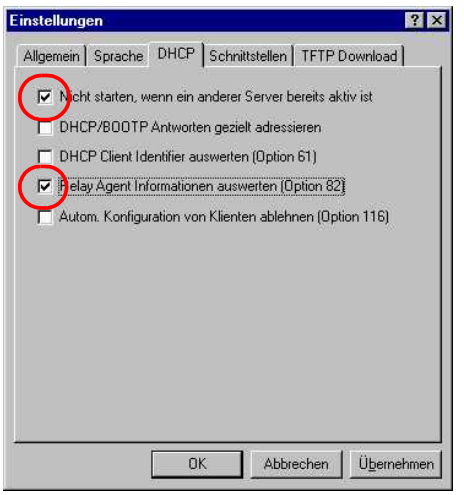


Abb. 113: DHCP-Einstellung

☐ Zur Eingabe der statischen Adressen klicken Sie auf `Hinzufügen`.

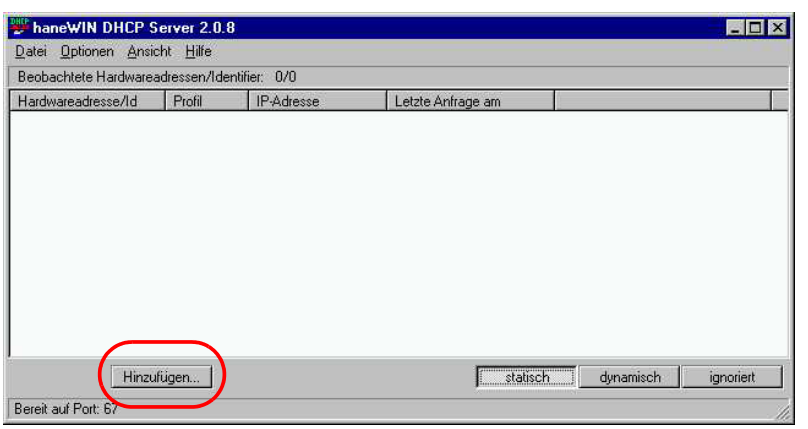


Abb. 114: Statische Adressen hinzufügen

☐ Wählen Sie `Circuit Identifier` und `Remote Identifier`.

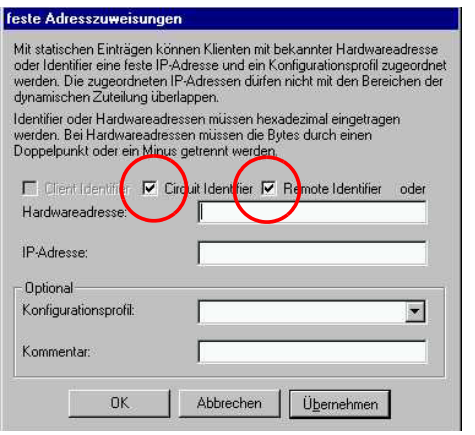


Abb. 115: Voreinstellung für die feste Adreßzuweisung

☐ Tragen Sie in das Feld `Hardwareadresse` den `Circuit Identifier` und den `Remote Identifier` ein, siehe “DHCP Relay Agent” auf Seite 208.
Mit `Hardwareadresse` kennzeichnen Sie den Switch und den Port, an welchen ein Gerät angeschlossen wird, dem Sie die `IP-Adresse` in der Zeile darunter zuweisen wollen.

Die Hardwareadresse hat folgende Form:

`ciclhhvvvvssmmpprirlxxxxxxxxxxxx`

- `ci`: Subidentifier für Typ des Circuit ID
- `cl`: Länge des Circuit ID
- `hh`: Hirschmann-Identifier: `01`, wenn an dem Port ein Hirschmann-Switch angeschlossen wird, sonst `00`.
- `vvvv`: VLAN ID der DHCP-Anfrage (Voreinstelung: 0001 = VLAN 1)
- `ss`: Steckplatz im Switch, auf dem sich das Modul mit dem Port befindet, an dem das Gerät angeschlossen wird. Geben Sie den Wert `00` an.
- `mm`: Modul mit dem Port, an dem das Gerät angeschlossen wird. Geben Sie den Wert `00` an.
- `pp`: Port an dem das Gerät angeschlossen wird.
- `ri`: Subidentifier für Typ des Remote ID
- `rl`: Länge des Remote ID

- xxxxxxxxxxxx: Remote ID des Switches (z.B. MAC-Adresse), an dem ein Gerät angeschlossen wird.

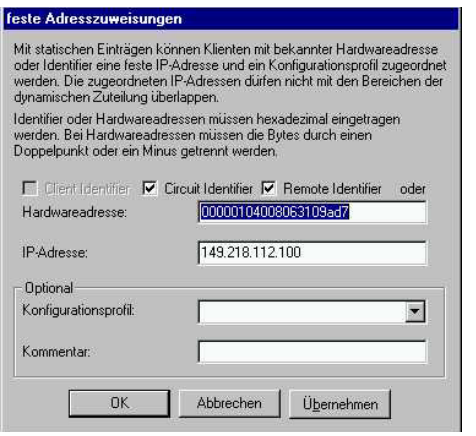


Abb. 116: Eintragen der Adressen

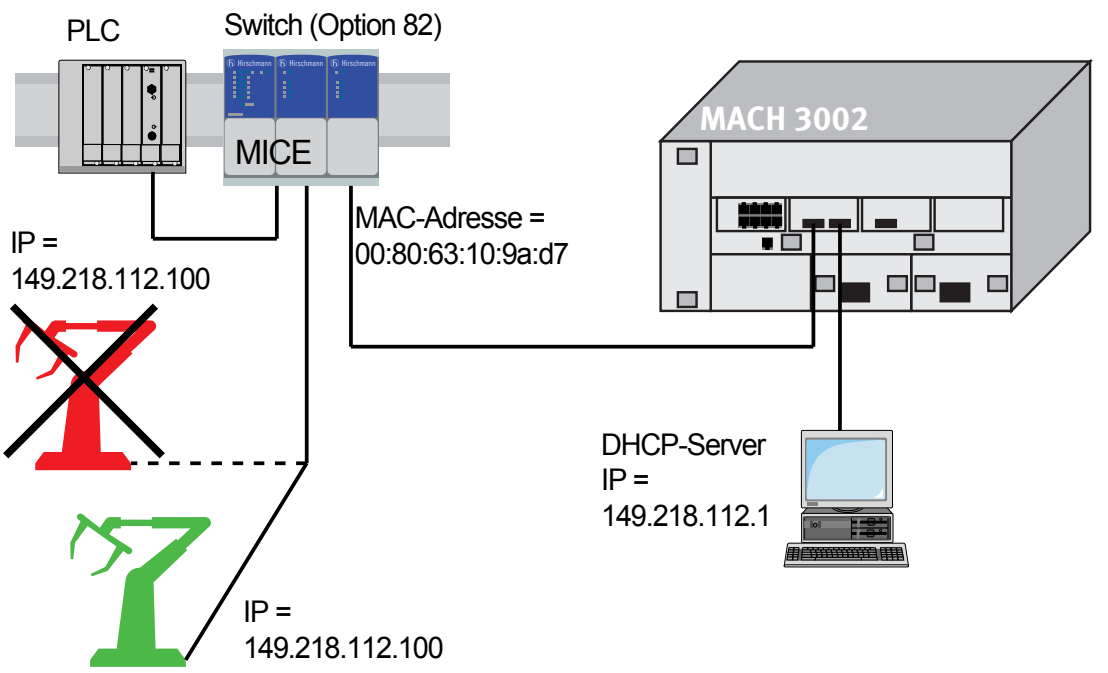


Abb. 117: Anwendungsbeispiel für den Einsatz von Option 82

Zugrundeliegende Normen und Standards

Liste der Normen und Standards:

- EN 61000-6-2:2001 Fachgrundnorm – Störfestigkeit Industriebereich
- EN 55022:1998 + A1 2000 + A2 2003 – Funkstöreigenschaften für Einrichtungen der Informationstechnik
- EN 60950:2001 – Sicherheit von Einrichtungen der Informationstechnik
- EN 61131-2:2003 – Speicherprogrammierbare Steuerungen
- FCC 47 CFR Part 15:2003 – Code of Federal Regulations
- Germanischer Lloyd, Klassifizierungs- und Bauvorschriften VI-7-3 Part 1 Ed.2003.
- 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 Technology Equipment.

Geräte mit Zertifizierung sind mit Zertifizierungskennzeichen versehen.

Liste der RFCs

- 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-Normen

IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree
IEEE 802.1 D-1998	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1 Q	Tagging
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, GVRP)
IEEE 802.1 w.2001	Rapid Reconfiguration
IEEE 802.3-2002	Ethernet
IEEE 802.1 AB	Link Layer Discovery Protocol
IEEE 1588-2002	Precision Time Protocol

Zertifizierungen

Die folgende Tabelle zeigt den Status der Zertifizierungen der RS2-../..-Produktfamilie.

Standard	RS2-../..
EN 61131-2	erfüllt
CE	erfüllt
FCC 47 CFR Part 15	erfüllt
cUL 508 / CSA C22.2 No.142	ja
cUL 1604 / CSA C22.2 No.213	ja
cUL 60950 / CSA C22.2 No.950	ja
Germanischer Lloyd	ja

Tab. 17: Zertifizierungen, aktueller Status siehe www.hirschmann.com

Technische Daten

RS2-../..

Abmessungen B x H x T	110 x 131 x 111 mm
Masse	460 g
Hutschienenbefestigung	nach IEC 60715:1981 + A1:1995

Stromversorgung

Betriebsspannung	24 V DC, -25% +33% Sicherheitskleinspannung (SELV/ PELV), redundante Eingänge entkoppelt. Relevant für Nord Amerika: Nec Class 2 power source max. 5A.
Leistungsaufnahme/Leistungsabgabe	
mit FX-Port(s)	max. 9 W bei 24 V DC 30,1 Btu (IT)/h
mit 2 TX/Ports	7,5 W bei 24 V DC 25,6 Btu (IT)/h)
Überstromschutz am Eingang	nicht wechselbare Schmelzsicherung

Umgebung

Umgebungstemperatur	Umgebende Luft: 0 °C bis 55 °C
Lagerungstemperatur	Umgebende Luft: -25 °C bis +70 °C
Luftfeuchtigkeit	10% bis 95% (nicht kondensierend)
Luftdruck	bis 2000 m (795 hPa), größere Höhe auf Anfrage
Verschmutzungsgrad	2

Schutzklassen

Laserschutz	Klasse 1 nach EN 60825-1 (2001)
Schutzklasse	IP 20

EMV-Störfestigkeit

EN 61000-4-2	Elektrostatische Entladung Kontaktentladung: Prüfschärfegrad 3 (6 kV) Luftentladung: Prüfschärfegrad 3 (8 kV)
EN 61000-4-3	Elektromagnetisches Feld Prüfschärfegrad 3 (10 V/m; 80 - 2000 MHz)
EN 61000-4-4	Schnelle Transienten (Burst) Prüfschärfegrad 3 (2 kV power line, 1 kV data line)
EN 61000-4-5	Stoßspannungen (Surge) Power Line symmetrisch: Prüfschärfegrad 2 (1kV) unsymmetrisch: Prüfschärfegrad 3 (2kV); Data Line Prüfschärfegrad 2 (1kV)
EN 61000-4-6	Leitungsgeführte Störspannungen Prüfschärfegrad 3 10 V (150 kHz - 80 MHz)

EMV-Störaussendung

EN 55022	Class A
FCC 47 CFR Part 15	Class A
Germanischer Lloyd	Klassifizierungs- und Bauvorschriften VI-7-3 Part 1 Ed.2001

Festigkeit

Vibration	IEC 60068-2-6 Test FC Prüfschärfegrade nach IEC 61131-2 und Germanischer Lloyd Richtlinien für die Durchführung von Baumusterprüfungen Teil 1
Schock	EC 60068-2-27 Test Ea Prüfschärfegrad nach IEC 61131-2

Netzausdehnung TP-Port 10BASE-T/100BASE-TX

Länge eines TP-Segmentes	typ. 100 m

Netzausdehnung LWL-Port 100BASE-FX

Systemdämpfung	
50/125 µm-Faser, multimode	0-8 dB (RS2-FX/FX, RS2-FX/FX-ST)
62,5/125 µm-Faser, multimode	0-11 dB (RS2-FX/FX, RS2-FX/FX-ST)
9/125 µm-Faser, singlemode	0-16 dB (RS2-FX-SM/FX-SM)
Wellenlänge	1300 nm
9/125 µm-Faser, singlemode	7-29 dB (RS2-FX-LH/FX-LH)
Wellenlänge	1550 nm

Beispiel für LWL-Leitungslänge	
50/125 µm-Faser, multimode	5 km (RS2-FX/FX, RS2-FX/FX-ST) Faserdaten: 1,0 dB/km, 800 MHz*km
62,5/125 µm-Faser, multimode	4 km (RS2-FX/FX, RS2-FX/FX-ST) Faserdaten: 1,0 dB/km, 500 MHz*km
9/125 µm-Faser, singlemode	30 km (RS2-FX-SM/FX-SM) Faserdaten: 1300 nm, 0,4 dB/km 3,5 ps/(nm*km)
9/125 µm-Faser, singlemode	24-86,6 km (RS2-FX-LH/FX-LH) Faserdaten: 1550 nm, 0,3 dB/km 19 ps/(nm*km)

Software

Switch	
Latency	max. 27 µs
MAC-Adreß-Tabelle	bis zu 4000 Einträge
Statische Adressfilter	bis zu 280 Einträge (im RM-Modus: 0 Unicast-Einträge)
VLAN	
VLAN ID	1 bis 1024
Anzahl VLANs	max. 40 gleichzeitig pro Switch max. 40 gleichzeitig pro Port
Anzahl VLANs mit GMRP	
in VLAN 1	max. 40 gleichzeitig pro Switch
in VLAN 1	max. 40 gleichzeitig pro Port

Lieferumfang

Rail Switch RS2-../.. inkl.	Klemmblock für die Versorgungs-spannung Handbuch RS2-../.. auf CDROM Beschreibung und Betriebsanleitung

Bestellnummer

RS2-TX/TX	943 654-
RS2-FX/FX	943 653-
RS2-FX/FX-ST	943 716-
RS2-FX-SM/FX-SM	943 655-
RS2-FX-SM/FX-LH	943 747-
RS2-FX-LH/FX-LH	943 648-

Zubehör

Taschenbuch "Grundlagen Industrial ETHERNET und TCP/IP"	280 710-834
AutoConfiguration Adapter ACA	943 751-001
Terminalkabel	943 301-001
5poliger Klemmblock (50 Stück)	943 845-001
Rail Power Supply RPS 30	943 662-003
Rail Power Supply RPS 60	943 662-001
Rail Power Supply RPS 120	943 662-011
Netzmanagement Software HiVision	943 471-100
OPC-Server Software HiOPC	943 055 - 001

Literaturhinweise

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

[2] „TCP/IP"
W.R. Stevens
Hüthig-Verlag 2004
ISBN 3-8266-5042-5

[3] Hirschmann Taschenbuch
„Grundlagen Industrial ETHERNET und TCP/IP“
280 710-834

[4] Hirschmann Handbuch
„MultiLAN Switch“
943 309-001

[5] Hirschmann Handbuch
„ETHERNET“
943 320-001

[6] Hirschmann Handbuch
„Netzmanagent HiVision“
039 583-620

[7] Hirschmann Handbuch
„HiOPC Server Interface“
039 504-001

Copyright integrierter Software

RSTP library - Rapid Spanning Tree (802.1t, 802.1w)

GNU LESSER GENERAL PUBLIC LICENSE

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 Ran-
dom Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice
```

That's all there is to it!

Bouncy Castle Crypto APIs (Java)

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.

Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, damit der Einsatz dieses Produkts problemlos erfolgen kann. Ihre Kommentare und Anregungen unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre **Beurteilung** für diese Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Graphiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

.....

.....

.....

.....

.....

.....

.....

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

.....

.....

.....

.....

Allgemeine Kommentare:

.....

.....

.....

.....

Firma / Abteilung .....

Name / Telefonnummer .....

Straße .....

PLZ / Ort .....

Datum / Unterschrift .....

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer 07127/14-1798 oder
- an

  Hirschmann Electronics GmbH & Co. KG
  Abteilung AMM
  Stuttgarter Str. 45-51

  72654 Neckartenzlingen

Stichwortverzeichnis

V

W

Z

HIRSCHMANN