

WAGO-ETHERNET-Zubehör 852



852-1605

Industrial-Managed-Switch

**8 Ports 1000BASE-T, 4 x 1000BASE-SX/LX,
PROFINET; EXT**

© 2019 WAGO Kontakttechnik GmbH & Co. KG
Alle Rechte vorbehalten.

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Tel.: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technischer Support

Tel.: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich Fehler, trotz aller Sorgfalt, nie vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: documentation@wago.com

Wir weisen darauf hin, dass die im Handbuch verwendeten Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen einem Warenzeichenschutz, Markenzeichenschutz oder patentrechtlichem Schutz unterliegen.

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.

Inhaltsverzeichnis

1	Hinweise zu dieser Dokumentation	10
1.1	Gültigkeitsbereich	10
1.2	Urheberschutz	10
1.3	Symbole	11
1.4	Darstellung der Zahlensysteme	12
1.5	Schriftkonventionen	12
2	Wichtige Erläuterungen	13
2.1	Rechtliche Grundlagen	13
2.1.1	Änderungsvorbehalt	13
2.1.2	Personalqualifikation	13
2.1.3	Bestimmungsgemäße Verwendung der Industrial-Switches	13
2.1.4	Technischer Zustand der Geräte	14
2.1.5	Richtlinien und Bestimmungen für die Verwendung der Industrial-Switches	14
2.2	Sicherheitshinweise	15
2.3	Spezielle Einsatzbestimmungen für ETHERNET-Geräte	17
3	Einleitung	18
3.1	Lieferumfang	18
3.2	Industrial-ETHERNET-Technologie	18
3.3	PROFINET	19
3.4	Switching-Technologie	21
3.5	Autonegotiation	21
3.6	Autocrossing	22
3.7	Store-and-Forward-Switching-Modus	22
3.8	Übertragungsmethoden	22
4	Gerätebeschreibung	23
4.1	Ansicht	24
4.1.1	Frontansicht	24
4.1.2	Draufsicht	26
4.2	Anschlüsse	27
4.2.1	Spannungsversorgung (PWR/RPS)	27
4.2.2	Netzwerkanschlüsse	28
4.2.2.1	RJ-45-Anschluss	29
4.2.2.2	10/100/1000BASE-T-Anschlüsse	29
4.2.2.3	1000BASE-SX/-LX-Anschlüsse	29
4.3	Anzeigeelemente	30
4.3.1	Geräte-LEDs	30
4.3.2	Anschluss-LEDs	31
4.4	Bedienelemente	32
4.4.1	DIP-Schalter	32
4.4.2	Reset-Taster	33
4.5	Aufkleber	34
4.6	Technische Daten	35
4.6.1	Gerätedaten	35
4.6.2	Systemdaten	35

4.6.3	Versorgung	35
4.6.4	Kommunikation	36
4.6.5	Umgebungsbedingungen	37
4.7	Zulassungen	38
5	PROFINET	39
5.1	Systemübersicht	39
5.1.1	Aufbau	39
5.1.1.1	Geräteklassen	39
5.1.1.2	Gerätemodell eines IO-Devices	40
5.2	Kommunikation	43
5.3	Datenübertragung	45
5.3.1	Real-Time-Kommunikation	45
5.3.2	Übertragungsmethoden	45
5.3.3	Übertragungsarten	45
5.3.4	Telegrammaufbau	47
5.4	Adressierung	48
5.4.1	Gerätename	48
5.5	Konformitätsklassen („Conformance Classes“)	49
5.6	Medienredundanz	52
5.7	Protokolle	54
5.8	PROFINET-Managed-Switch	56
5.9	GSDML-Datei	57
5.9.1	Einleitung	57
5.9.2	Aufbau einer GSDML-Datei	58
5.9.3	Eindeutige Identifizierung von IO-Devices	60
5.10	Projektieren über GSDML-Datei	61
5.10.1	Konfigurieren	61
5.10.1.1	Projektierungstools (Übersicht)	62
5.10.1.2	Allgemeines Vorgehen zum Projektieren eines PROFINET- Systems	63
5.10.1.3	Laden des Projektes in den IO-Controller	65
5.10.2	Parameter	66
5.10.2.1	Bereich „Allgemein“	66
5.10.2.2	Bereich „PROFINET-Schnittstelle [X1]“	67
5.10.2.3	Bereich „Erweiterte Optionen“	68
5.10.2.4	Bereich „Port 1“	70
5.10.2.5	Bereich „Port-Optionen“	71
5.10.2.6	Bereich „Identification & Maintenance“	72
5.10.2.7	Bereich „Prozessalarme“	73
5.10.2.8	Bereich „Baugruppenparameter“	74
5.10.2.9	Bereich „E/A-Adressen“	76
5.11	Zyklische I/O-Daten	77
5.11.1	Beispiel für zyklische I/O-Daten	78
5.12	DAP-Parameter	81
5.13	Zugriff über Konsolen-Port (CLI)	85
5.13.1	Vergabe der IP-Adresse mit dem Konsolen-Port	85
5.14	Parametrieren über WBM im PROFINET-Modus	89
5.14.1	Systemstatus	92
5.14.1.1	Systeminformationen	92

5.14.2	Grundeinstellungen	94
5.14.2.1	Allgemeine Einstellungen	94
5.14.2.1.1	System.....	94
5.14.2.2	Port-Spiegelung.....	96
5.14.2.3	Port-Einstellungen	98
5.14.3	PROFINET	99
5.14.3.1	PROFINET Setting	99
5.14.3.2	Informationen	100
5.14.3.3	Diagnoseliste.....	101
5.14.4	Erweiterte Einstellungen	102
5.14.4.1	MRP	102
5.14.5	Management.....	105
5.14.5.1	Datei hochladen	105
5.14.5.1.1	Benutzerkonto.....	105
6	Montieren.....	106
6.1	Montageort	106
6.2	Montage auf Tragschiene	106
6.3	Demontage von der Tragschiene.....	106
7	Geräte anschließen	107
7.1	Spannungsversorgung	107
7.2	Externer Alarmkontakt-Anschluss.....	109
7.3	Anschluss Konsolenanschlusskabel	109
7.4	Anschluss 1000BASE-SX/LX, Glasfaser	110
7.5	Anschluss 10/100/1000Base-T-Ports.....	111
8	Funktionsbeschreibung.....	112
8.1	Grundeinstellungen	112
8.1.1	Jumbo Frame.....	112
8.1.2	SNTP	112
8.1.3	Management Host.....	113
8.1.4	MAC-Management.....	113
8.1.4.1	Static MAC	114
8.1.5	Port-Spiegelung (Port Mirroring)	115
8.1.6	Port-Einstellungen (Port Settings)	115
8.2	Erweiterte Einstellungen	119
8.2.1	Bandbreitenkontrolle	119
8.2.1.1	QoS.....	119
8.2.1.2	Rate Limitation	126
8.2.1.2.1	Storm Control.....	126
8.2.1.2.2	Bandbreitenbegrenzung (Rate Limitation).....	126
8.2.2	IGMP Snooping.....	127
8.2.2.1	Multicast-Adresse	130
8.2.3	VLAN	133
8.2.3.1	Port-Isolation	135
8.2.4	LLDP.....	136
8.2.5	MAC based VLAN.....	136
8.2.6	Schleifenerkennung (Loop Detection)	137
8.2.7	STP.....	138
8.3	Sicherheit	144

8.3.1	Zugriffskontrollliste ACL	144
8.4	Monitor	145
8.4.1	Alarm	145
8.4.2	Monitor Informationen	145
8.4.3	RMON Statistiken	145
8.4.4	SFP	145
8.4.4.1	SFP-Informationen	146
8.4.5	Traffic Monitor	146
8.5	Management	147
8.5.1	SNMP	147
8.5.1.1	SNMP Trap	148
9	Konfigurieren	149
9.1	Übersicht der Konfigurationsoptionen	149
9.1.1	Telnet-Port	150
9.2	Konsolenport	151
10	Web-Based-Management-System (WBM)	152
10.1	Systemstatus	155
10.1.1	Systeminformation	155
10.2	Grundeinstellungen	157
10.2.1	Allgemeine Einstellungen	157
10.2.1.1	System	157
10.2.1.2	Jumbo Frame	159
10.2.1.3	SNTP	160
10.2.1.4	Management-Host	163
10.2.2	MAC Management	164
10.2.2.1	Statische MAC-Einstellungen	164
10.2.2.2	MAC-Tabelle	166
10.2.2.3	Age-Time-Einstellung	167
10.2.2.4	Blacklisting	168
10.2.3	Port-Spiegelung	169
10.2.4	Port-Einstellungen	171
10.2.4.1	Allgemeine Einstellungen	171
10.2.4.2	Informationen	173
10.3	PROFINET	174
10.4	Erweiterte Einstellungen	174
10.4.1	Bandbreiten-Regelung	174
10.4.1.1	QoS	174
10.4.1.1.1	Port-Priorität	174
10.4.1.1.2	IP-DiffServ (DSCP)	175
10.4.1.1.3	Priorität/Queue-Zuordnung	176
10.4.1.1.4	Schedule-Modus	177
10.4.1.2	Bandbreitenbegrenzung	179
10.4.1.2.1	Sturmbegrenzung	179
10.4.1.2.2	Bandbreitenbegrenzung	181
10.4.2	IGMP-Snooping	182
10.4.2.1	IGMP-Snooping	182
10.4.2.1.1	Allgemeine Einstellungen	182
10.4.2.1.2	Port-Einstellungen	184
10.4.2.1.3	Querier-Einstellungen	186

10.4.2.2	IGMP-Filter	187
10.4.2.2.1	Allgemeine Einstellungen	187
10.4.2.2.2	Multicast-Gruppen	188
10.4.2.2.3	Port-Einstellungen	189
10.4.2.3	Statische Multicast-Adressen	190
10.4.2.4	Multicast-Statistiken	191
10.4.3	VLAN	192
10.4.3.1	Port Isolation	192
10.4.3.2	VLAN	194
10.4.3.2.1	VLAN-Einstellungen	194
10.4.3.2.2	Tag-Einstellungen	196
10.4.3.2.3	Port-Einstellungen	197
10.4.3.3	MAC-VLAN	199
10.4.4	LLDP	200
10.4.4.1	Einstellungen	200
10.4.4.2	Nachbarerkennung	202
10.4.5	Schleifenerkennung (Loop Detection)	203
10.4.6	MRP	205
10.4.7	Spanning Tree Protocol	208
10.4.7.1	Allgemeine Einstellungen	208
10.4.7.2	Port-Parameter	210
10.4.7.3	STP-Status	213
10.5	Sicherheit	214
10.5.1	Access-Control-Liste	214
10.6	Monitor	218
10.6.1	Alarminformationen	218
10.6.2	Systeminformationen	219
10.6.3	Port-Statistik	221
10.6.4	Port-Auslastung	222
10.6.5	RMON-Statistiken	223
10.6.6	SFP-Informationen	226
10.6.7	Traffic-Monitor	229
10.7	Management	232
10.7.1	SNMP	232
10.7.1.1	SNMP	232
10.7.1.1.1	SNMP-Einstellungen	232
10.7.1.1.2	Community-Name	233
10.7.1.2	SNMP-Trap	235
10.7.1.2.1	Trap-Receiver-Einstellungen	235
10.7.1.2.2	Trap Event Status	236
10.7.1.2.3	Trap-Port-Einstellungen	237
10.7.1.3	SNMPv3-Konfiguration	238
10.7.1.3.1	SNMPv3-User	238
10.7.1.3.2	SNMPv3-Gruppen	240
10.7.1.3.3	SNMPv3-View	241
10.7.2	Wartung	242
10.7.2.1	Konfiguration	242
10.7.2.2	Firmware	244
10.7.2.3	Neustart	245
10.7.2.4	Protokolle	246

10.7.3	System-Log.....	248
10.7.4	Upload File.....	250
10.7.5	Ping	251
10.7.6	Benutzerkonto.....	252
11	Anhang	254
11.1	Konsolenanschluss (RJ-45 zu DB9)	254
11.2	RJ-45-Kabel	255
11.3	Configuring in the Command Line Interface (CLI) (Zugriff über Konsole (CLI)).....	256
11.3.1	System Status.....	256
11.3.1.1	System Information.....	256
11.3.2	Basic Settings	257
11.3.2.1	System	257
11.3.2.1.1	Jumbo Frame.....	258
11.3.2.1.2	SNTP	258
11.3.2.1.3	Management Host.....	259
11.3.2.2	MAC Management.....	260
11.3.2.3	Port Mirroring.....	260
11.3.2.4	Port Settings.....	261
11.3.3	Advanced Settings	262
11.3.3.1	Bandwidth Control	262
11.3.3.1.1	QoS	262
11.3.3.1.2	Rate Limitation	263
11.3.3.1.2.1	Storm Control	263
11.3.3.2	IGMP Snooping	264
11.3.3.2.1	IGMP Snooping Querier.....	266
11.3.3.2.2	IGMP Snooping Filtering	266
11.3.3.3	Multicast Address	267
11.3.3.4	VLAN.....	267
11.3.3.4.1	Port-Isolation.....	267
11.3.3.4.2	VLAN Settings	268
11.3.3.4.3	MAC VLAN	269
11.3.3.5	LLDP	270
11.3.3.6	Loop Detection	271
11.3.3.7	MRP	272
11.3.3.8	STP.....	273
11.3.4	Security.....	275
11.3.4.1	Access Control List.....	275
11.3.5	Monitor.....	277
11.3.5.1	Alarm.....	277
11.3.5.2	Monitor Information.....	277
11.3.5.3	Port Statistics	277
11.3.5.4	Port Utilization	277
11.3.5.5	RMON Statistics	277
11.3.5.6	SFP Information	277
11.3.5.7	Traffic Monitor	278
11.3.6	Management.....	279
11.3.6.1	SNMP.....	279
11.3.6.1.1	SNMP	279

11.3.6.1.2	SNMP Trap	280
11.3.6.1.2.1	Port Trap Settings	280
11.3.6.1.3	SNMPv3	281
11.3.6.2	Maintenance	282
11.3.6.2.1	Reboot	282
11.3.6.3	System Log	283
11.3.6.4	User Account	283
Abbildungsverzeichnis		284
Tabellenverzeichnis		287

1 Hinweise zu dieser Dokumentation

Hinweis



Dokumentation aufbewahren!

Diese Dokumentation ist Teil des Produkts. Bewahren Sie deshalb die Dokumentation während der gesamten Nutzungsdauer des Produkts auf. Geben Sie die Dokumentation an jeden nachfolgenden Benutzer des Produkts weiter. Stellen Sie darüber hinaus sicher, dass gegebenenfalls jede erhaltene Ergänzung in die Dokumentation mit aufgenommen wird.

1.1 Gültigkeitsbereich

Die vorliegende Dokumentation gilt für das WAGO-ETHERNET-Zubehör „Industrial-Managed-Switch“ (852-1605).

1.2 Urheberrecht

Diese Dokumentation, einschließlich aller darin befindlichen Abbildungen, ist urheberrechtlich geschützt. Jede Weiterverwendung dieser Dokumentation, die von den urheberrechtlichen Bestimmungen abweicht, ist nicht gestattet. Die Reproduktion, Übersetzung in andere Sprachen sowie die elektronische und fototechnische Archivierung und Veränderung bedarf der schriftlichen Genehmigung der WAGO Kontakttechnik GmbH & Co. KG, Minden. Zuwiderhandlungen ziehen einen Schadenersatzanspruch nach sich.

1.3 Symbole

GEFAHR



Warnung vor Personenschäden!

Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körpervverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

GEFAHR



Warnung vor Personenschäden durch elektrischen Strom!

Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körpervverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

WARNUNG



Warnung vor Personenschäden!

Kennzeichnet eine mögliche Gefährdung mit mittlerem Risiko, die Tod oder (schwere) Körpervverletzung zur Folge haben kann, wenn sie nicht vermieden wird.

VORSICHT



Warnung vor Personenschäden!

Kennzeichnet eine mögliche Gefährdung mit geringem Risiko, die leichte oder mittlere Körpervverletzung zur Folge haben könnte, wenn sie nicht vermieden wird.

ACHTUNG



Warnung vor Sachschäden!

Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

ESD



Warnung vor Sachschäden durch elektrostatische Aufladung!

Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

Hinweis



Wichtiger Hinweis!

Kennzeichnet eine mögliche Fehlfunktion, die aber keinen Sachschaden zur Folge hat, wenn sie nicht vermieden wird.

Information



Weitere Information

Weist auf weitere Informationen hin, die kein wesentlicher Bestandteil dieser Dokumentation sind (z. B. Internet).

1.4 Darstellung der Zahlensysteme

Tabelle 1: Darstellungen der Zahlensysteme

Zahlensystem	Beispiel	Bemerkung
Dezimal	100	Normale Schreibweise
Hexadezimal	0x64	C-Notation
Binär	'100' '0110.0100'	In Hochkomma, Nibble durch Punkt getrennt

1.5 Schriftkonventionen

Tabelle 2: Schriftkonventionen

Schriftart	Bedeutung
<i>kursiv</i>	Namen von Pfaden und Dateien werden kursiv dargestellt z. B.: <i>C:\Programme\WAGO Software</i>
Menü	Menüpunkte werden fett dargestellt z. B.: Speichern
>	Ein „Größer als“- Zeichen zwischen zwei Namen bedeutet die Auswahl eines Menüpunktes aus einem Menü z. B.: Datei > Neu
Eingabe	Bezeichnungen von Eingabe- oder Auswahlfeldern werden fett dargestellt z. B.: Messbereichsanfang
„Wert“	Eingabe- oder Auswahlwerte werden in Anführungszeichen dargestellt z. B.: Geben Sie unter Messbereichsanfang den Wert „4 mA“ ein.
[Button]	Schaltflächenbeschriftungen in Dialogen werden fett dargestellt und in eckige Klammern eingefasst z. B.: [Eingabe]
[Taste]	Tastenbeschriftungen auf der Tastatur werden fett dargestellt und in eckige Klammern eingefasst z. B.: [F5]

2 Wichtige Erläuterungen

Dieses Kapitel beinhaltet ausschließlich eine Zusammenfassung der wichtigsten Sicherheitsbestimmungen und Hinweise. Diese werden in den einzelnen Kapiteln wieder aufgenommen. Zum Schutz vor Personenschäden und zur Vorbeugung von Sachschäden an Geräten ist es notwendig, die Sicherheitsrichtlinien sorgfältig zu lesen und einzuhalten.

2.1 Rechtliche Grundlagen

2.1.1 Änderungsvorbehalt

Die WAGO Kontakttechnik GmbH & Co. KG behält sich Änderungen vor. Alle Rechte für den Fall der Patenterteilung oder des Gebrauchsmusterschutzes sind der WAGO Kontakttechnik GmbH & Co. KG vorbehalten. Fremdprodukte werden stets ohne Vermerk auf Patentrechte genannt. Die Existenz solcher Rechte ist daher nicht auszuschließen.

2.1.2 Personalqualifikation

Sämtliche Arbeitsschritte, die an den Geräten der Serie 852 durchgeführt werden, dürfen nur von Elektrofachkräften mit ausreichenden Kenntnissen im Bereich der Automatisierungstechnik vorgenommen werden. Diese müssen mit den aktuellen Normen und Richtlinien für die Geräte und das Automatisierungsumfeld vertraut sein.

Alle Eingriffe in die Steuerung sind stets von Fachkräften mit ausreichenden Kenntnissen in der SPS-Programmierung durchzuführen.

2.1.3 Bestimmungsgemäße Verwendung der Industrial-Switches

Das Gerät wurde für die Schutzklasse IP30 entwickelt. Es ist geschützt gegen das Eindringen fester Objekte und Fremdkörper mit einem Durchmesser von bis zu 2,5 mm, aber nicht gegen das Eindringen von Wasser. Sofern nicht anders angegeben, darf das Gerät in feuchten und staubigen Umgebungen nicht betrieben werden.

2.1.4 Technischer Zustand der Geräte

Die Geräte werden ab Werk für den jeweiligen Anwendungsfall mit einer festen Hard- und Softwarekonfiguration ausgeliefert. Sie enthalten keine durch den Anwender zu wartenden oder zu reparierenden Teile. Folgende Handlungen bewirken den Haftungsausschluss der WAGO Kontakttechnik GmbH & Co. KG:

- Reparaturen,
- Veränderungen an der Hard- oder Software, die nicht in der Bedienungsanleitung beschrieben sind,
- nicht bestimmungsgemäßer Gebrauch der Komponenten.

Weitere Einzelheiten ergeben sich aus den vertraglichen Vereinbarungen. Wünsche an eine abgewandelte bzw. neue Hard- oder Softwarekonfiguration richten Sie bitte an die WAGO Kontakttechnik GmbH & Co. KG.

2.1.5 Richtlinien und Bestimmungen für die Verwendung der Industrial-Switches

Beachten Sie folgende für die Installation relevante Richtlinien und Bestimmungen:

- Daten- und Netzleitungen müssen gemäß Richtlinien angeschlossen und installiert werden, damit Installationsfehler vermieden und Gefahren für die Mitarbeiter ausgeschlossen werden.
- Beachten Sie beim Installieren, Starten, Warten und Reparieren die Bestimmungen Ihres Gerätes zur Unfallverhütung (z. B. DGUV Vorschrift 3 „Elektrische Anlagen und Betriebsmittel“).
- Not-Aus-Funktionen und -Geräte dürfen nicht deaktiviert oder anderweitig unwirksam gemacht werden. Siehe relevante Richtlinien (z. B. EN 418).
- Ihre Installationsausrüstung muss den EMV-Richtlinien entsprechen, damit elektromagnetische Beeinflussungen ausgeschlossen werden können.
- Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß EN 61340-5-1/-3. Stellen Sie bei der Verwendung der Module sicher, dass die Umgebungsfaktoren (Personen, Arbeitsplatz und Verpackung) geerdet sind.
- Die für die Installation von Switch-Gehäusen geltenden Richtlinien und Bestimmungen müssen eingehalten werden.

2.2 Sicherheitshinweise

Beim Einbauen des Gerätes in Ihre Anlage und während des Betriebes sind folgende Sicherheitshinweise zu beachten:

GEFAHR



Nicht an Geräten unter Spannung arbeiten!

Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie es montieren, Störungen beheben oder Wartungsarbeiten vornehmen.

GEFAHR



Nur in Gehäusen, Schränken oder elektrischen Betriebsräumen einbauen!

WAGO-ETHERNET-Geräte der Serie 852 sind offene Betriebsmittel. Bauen Sie diese ausschließlich in abschließbaren Gehäusen, Schränken oder in elektrischen Betriebsräumen ein. Ermöglichen Sie nur autorisiertem Fachpersonal den Zugang mittels Schlüssel oder Werkzeug.

GEFAHR



Unfallverhütungsvorschriften beachten!

Beachten Sie bei Montage, Inbetriebnahme, Betrieb, Wartung und Störbehebung die für Ihre Maschine/Anlage zutreffenden Unfallverhütungsvorschriften wie beispielsweise die DGUV Vorschrift 3 „Elektrische Anlagen und Betriebsmittel“.

GEFAHR



Auf normgerechten Anschluss achten!

Zur Vermeidung von Gefahren für das Personal und Störungen an Ihrer Anlage, verlegen Sie die Daten- und Versorgungsleitungen normgerecht und achten Sie auf die korrekte Anschlussbelegung. Beachten Sie die für Ihre Anwendung zutreffenden EMV-Richtlinien.

ACHTUNG



Nicht in Telekommunikationsnetzen einsetzen!

Verwenden Sie Geräte mit ETHERNET-/RJ-45-Anschluss ausschließlich in LANs. Verbinden Sie diese Geräte niemals mit Telekommunikationsnetzen, wie z. B. mit Analog- oder ISDN-Telefonanlagen.

ACHTUNG



Defekte oder beschädigte Geräte austauschen!

Tauschen Sie defekte oder beschädigte Geräte (z. B. bei deformierten Kontakten) aus.

ACHTUNG



Geräte vor kriechenden und isolierenden Stoffen schützen!

Die Geräte sind unbeständig gegen Stoffe, die kriechende und isolierende Eigenschaften besitzen, z. B. Aerosole, Silikone, Triglyceride (Bestandteil einiger Handcremes). Sollten Sie nicht ausschließen können, dass diese Stoffe im Umfeld der Geräte auftreten, bauen Sie die Geräte in ein Gehäuse ein, das resistent gegen oben genannte Stoffe ist. Verwenden Sie generell zur Handhabung der Geräte saubere Werkzeuge und Materialien.

ACHTUNG**Nur mit zulässigen Materialien reinigen!**

Reinigen Sie das Gehäuse und verschmutzte Kontakte mit Propanol.

ACHTUNG**Kein Kontaktspray verwenden!**

Verwenden Sie kein Kontaktspray, da in Verbindung mit Verunreinigungen die Funktion der Kontaktstelle beeinträchtigt werden kann.

ACHTUNG**Verpolungen vermeiden!**

Vermeiden Sie die Verpolung der Daten- und Versorgungsleitungen, da dies zu Schäden an den Geräten führen kann.

ESD**Elektrostatische Entladung vermeiden!**

In den Geräten sind elektronische Komponenten integriert, die Sie durch elektrostatische Entladung bei Berührung zerstören können. Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß DIN EN 61340-5-1/-3. Achten Sie beim Umgang mit den Geräten auf gute Erdung der Umgebung (Personen, Arbeitsplatz und Verpackung).

VORSICHT**Warnung vor Laserstrahlung!**

Sehen Sie nicht in die Öffnungen der Anschlüsse hinein, wenn kein Kabel angeschlossen ist, um sich nicht der Strahlung auszusetzen.

Es kann eine nicht sichtbare Laserstrahlung emittieren.

Dabei handelt es sich um eine Laser Klasse 1 nach EN 60825-1.

Hinweis**Funkstörungen im Wohnbereich**

Dieses Gerät ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

2.3 Spezielle Einsatzbestimmungen für ETHERNET-Geräte

Wo nicht speziell beschrieben, sind ETHERNET-Geräte für den Einsatz in lokalen Netzwerken bestimmt. Beachten Sie folgende Hinweise, wenn Sie ETHERNET-Geräte in Ihrer Anlage einsetzen:

- Verbinden Sie Steuerungskomponenten und Steuerungsnetzwerke nicht direkt mit einem offenen Netzwerk wie dem Internet oder einem Büronetzwerk. WAGO empfiehlt, Steuerungskomponenten und Steuerungsnetzwerke hinter einer Firewall anzubringen.
- Schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. für WAGO-I/O-CHECK und CODESYS), um die Gefahr von Cyber-Angriffen zu verringern und damit die Cyber-Security zu erhöhen.
Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.
- Beschränken Sie den physikalischen und elektronischen Zugang zu sämtlichen Automatisierungskomponenten auf einen autorisierten Personenkreis.
- Ändern Sie vor der ersten Inbetriebnahme unbedingt die standardmäßig eingestellten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.
- Ändern Sie regelmäßig die verwendeten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.
- Ist ein Fernzugriff auf Steuerungskomponenten und Steuerungsnetzwerke erforderlich, sollte ein „Virtual Private Network“ (VPN) genutzt werden.
- Führen Sie regelmäßig eine Bedrohungsanalyse durch. So können Sie prüfen, ob die getroffenen Maßnahmen Ihrem Schutzbedürfnis entsprechen.
- Wenden Sie in der sicherheitsgerichteten Gestaltung Ihrer Anlage „Defense-in-depth“-Mechanismen an, um den Zugriff und die Kontrolle auf individuelle Produkte und Netzwerke einzuschränken.

3 Einleitung

3.1 Lieferumfang

- 1 Industrial-Managed-Switch mit Federleiste
- Schutzabdeckungen für nicht verwendete Anschlüsse
- Datenkabel RS-232 für CLI

3.2 Industrial-ETHERNET-Technologie

Die robusten Switches sind für den Industrieinsatz ausgelegt und kompatibel zu folgenden Standards:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3z
- IEEE 802.3x
- IEEE 802.1d
- IEEE 802.1w
- IEEE 802.1s
- IEEE 802.1Q
- IEEE 802.1p
- IEEE 802.1ab
- PROFINET

Die Switches verfügen über eine Spannungsversorgung mit einem Versorgungsspannungsbereich 12 ... 60 V.

Leistungsmerkmale wie Autonegotiation und Auto-MDI/MDIX (crossover) an allen 10/100/1000BASE-T-Ports sind realisiert.

3.3 PROFINET

Das Echtzeit-ETHERNET-Kommunikationssystem PROFINET ist eines der flexibelsten und verbreitetsten Feldbussysteme in der Automatisierungstechnik. Aufgrund der weltweiten Marktpräsenz ist PROFINET in vielen Branchen bekannt und akzeptiert. Hersteller und Anwender sind weltweit organisiert in der PROFIBUS & PROFINET International (PI).

PROFINET gilt als Nachfolger des konventionellen Feldbusses PROFIBUS und wird deshalb häufig gewählt, sobald die Kommunikation von konventionellen Feldbussen auf ein ETHERNET-basiertes Feldbussystem umgestellt wird. Technisch bietet PROFINET eine Reihe von Vorzügen, die je nach Anforderung der Einsatzumgebung den Ausschlag für dieses Feldbussystem geben können. Auch auf Grund dieser Vorzüge kann PROFINET in den unterschiedlichsten Branchen eingesetzt werden.

PROFINET erlaubt eine Kombination von Standard-ETHERNET-Teilnehmern mit Echtzeiteilnehmern im selben Netzwerk. PROFINET stellt sicher, dass die Feldbuskommunikation nicht durch Standardkommunikation auf Basis von TCP/IP gestört wird. Diese Flexibilität bietet einen großen Vorteil gegenüber anderen ETHERNET-Echtzeitsystemen, bei denen Standard-IT-Geräte gar nicht oder nur an ausgewiesenen Stellen ins Netzwerk integriert werden dürfen bzw. nur bei laufender Steuerung in die Kommunikation einbezogen werden. In der Abbildung „Parallele Nutzung von Standard ETHERNET und PROFINET“ wird diese parallele Nutzung über dieselbe physikalische Verbindung schematisch dargestellt.

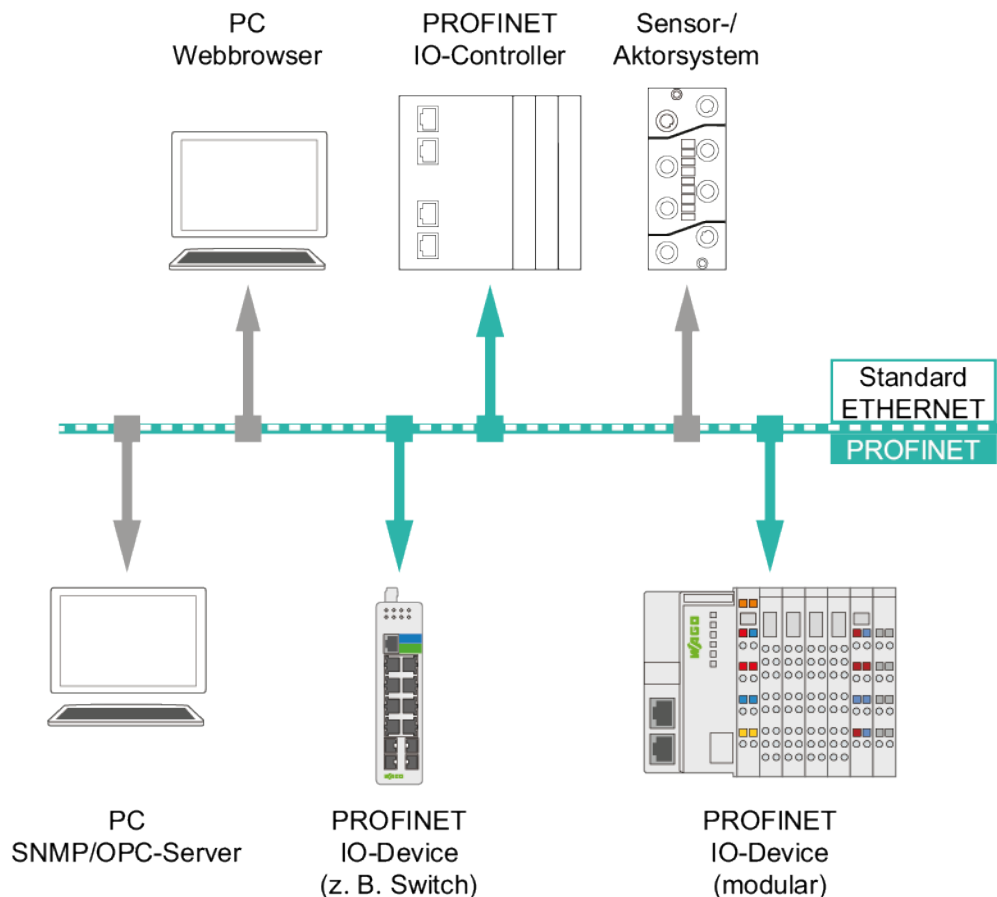


Abbildung 1: Parallele Nutzung von Standard ETHERNET und PROFINET

Bei PROFINET erfolgt eine Trennung von echtzeitfähigen und nicht-echtzeitfähigen Geräten. Diese Trennung erfolgt je nach Echtzeitklasse (RT_Class) unterschiedlich:

- Bei RT_Class_1 erfolgt die Trennung dadurch, dass die Echtzeittelegramme über VLAN priorisiert werden.
- Bei RT_Class_3 erfolgt die Trennung über spezielle PROFINET-Switches, die eine Bandbreitenreservierung für die Echtzeittelegramme vornehmen.

Durch diese Trennung von echtzeitfähigen und nicht-echtzeitfähigen Geräten ist gewährleistet, dass jedes Standard-IT-Gerät an jeder Stelle eines PROFINET-Netzwerkes betrieben werden kann, ohne dass besondere Vorkehrungen hinsichtlich der physikalischen Anschaltung getroffen werden müssen.

An jeder Schnittstelle im Automatisierungsnetzwerk kann jedes beliebige ETHERNET-fähige Gerät angeschlossen werden. Bei RT_Class_1 muss dabei die zulässige Netzlast des Standarddatenverkehrs berücksichtigt werden.

Von jeder Schnittstelle im Automatisierungsnetzwerk aus kann mit Hilfe eines PCs eine Diagnose vorgenommen werden, ohne dass der Betriebszustand des Automatisierungssystems dabei relevant ist. Diese Funktion ermöglicht die optimale physikalische Anpassung der Netzwerkstruktur an die vorliegenden Gegebenheiten und funktioniert ohne jede Einschränkung hinsichtlich der physikalischen Topologie:

- Ringtopologie (nur bei Nutzung eines Protokolls zur Medienredundanz, z. B. MRP)
- Linientopologie
- Sterntopologie
- vermaschtes Netzwerk

In vielen Fällen wird dadurch auch ein Zusammenlegen vormals getrennter Netzwerke unter Beachtung der zulässigen Netzlast möglich.

3.4 Switching-Technologie

Im Industrial ETHERNET wird vorwiegend die Switching-Technologie genutzt. Bei dieser Technologie kann jeder Netzwerkteilnehmer jederzeit senden, da er immer über eine freie Punkt-zu-Punkt-Verbindung zum nächsten Switch verfügt. Diese Verbindung ist bidirektional, das heißt, die Teilnehmer können gleichzeitig senden und empfangen (Vollduplex).

Der gezielte Einsatz der Switching-Technologie kann die Echtzeitfähigkeit erhöhen, da durch die Punkt-zu-Punkt-Verbindung Kollisionen in der Netzwerkkommunikation vermieden werden.

3.5 Autonegotiation

Autonegotiation ermöglicht es dem Switch, für jeden Port und den daran angeschlossenen Teilnehmer bzw. die Teilnehmer die Übertragungsrate und die Betriebsart zu erkennen und entsprechend automatisch einzustellen. Dabei wird der höchstmögliche Modus (Übertragungsgeschwindigkeit und Betriebsart) eingestellt.

Autonegotiation ist für ETHERNET-Teilnehmer verfügbar, die über Kupferkabel mit dem Switch verbunden sind.

Somit ist der Switch ein Plug-and-Play-fähiges Gerät.

3.6 Autocrossing

Autocrossing (MDI/MDI-X, „Medium Dependent Interface“) führt bei Bedarf eine automatische Kreuzung der Sende- und Empfangsleitungen an Twisted-Pair-Schnittstellen durch. Damit kann der Anwender 1:1 verdrahtete Kabel und gekreuzt verdrahtete Kabel (Cross-over-Kabel) gleichermaßen einsetzen.

3.7 Store-and-Forward-Switching-Modus

Im Modus „Store and Forward“ speichert der ETHERNET-Switch das komplette Datentelegramm zwischen, überprüft es auf Fehler (CRC-Prüfsumme) und ordnet es bei Fehlerfreiheit in eine Warteschlange ein. Anschließend wird das Datentelegramm (MAC-Tabelle) selektiv an denjenigen Port weitergeleitet, der auf den adressierten Knoten Zugriff hat.

Die Verzögerungszeit, die das Datentelegramm zum Passieren des Store-and-Forward-Switches benötigt, ist von der Telegrammlänge abhängig.

Vorteil von „Store and Forward“:

Die Datentelegramme werden auf ihre Korrektheit und Gültigkeit geprüft. Dadurch wird verhindert, dass fehlerhafte bzw. beschädigte Datentelegramme über das Netzwerk verteilt werden.

3.8 Übertragungsmethoden

Die Datenübertragung in ETHERNET-Netzwerken kann über 2 Modi realisiert werden:

- Halbduplex (Half Duplex)
 - Ein ETHERNET-Gerät kann zu einem Zeitpunkt entweder nur empfangen oder nur senden.
 - Die Erkennung von Kollisionen (CSMA/CD) ist aktiv.
 - Die Netzausdehnung ist durch die Laufzeitverzögerungen der Geräte und Übertragungsmedien begrenzt.
- Vollduplex (Full Duplex)
 - Ein ETHERNET-Gerät kann gleichzeitig Daten empfangen und senden.
 - Die Erkennung von Kollisionen (CSMA/CD) ist ausgeschaltet.
 - Die Netzausdehnung hängt nur von den Leistungsgrenzen der verwendeten Sende- und Empfangskomponenten ab.

4 Gerätebeschreibung

Der 852-1605 ist ein industrieller, konfigurierbarer ETHERNET-Switch mit 8 Kupfer-Ports 10/100/1000BASE-T und 4 Slots SFP-1000BASE-SX/LX. Entsprechende SFP-Module sind optional erhältlich.

Der Switch besitzt u. a. folgende Merkmale:

- ein robustes Gehäuse
- eine redundante Spannungsversorgung
- eine Funktionsüberwachung mit Relais

Eine einfache Integration ins Automatisierungssystem erfolgt mit Hilfe der PROFINET-Gerätebeschreibungsdatei (GSD).

4.1 Ansicht

4.1.1 Frontansicht

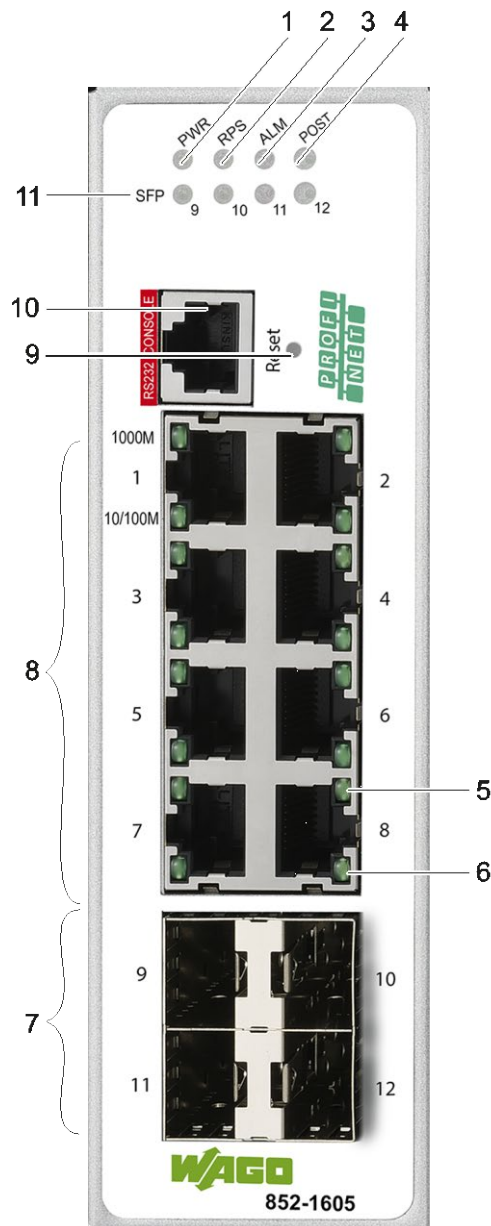


Abbildung 2: Frontansicht des Industrial-Managed-Switches

Tabelle 3: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“

Pos.	Bezeichnung	Bedeutung	Details siehe Kapitel
1	PWR	Status-LED Versorgungsspannung	„Gerätebeschreibung“ > „Anzeigeelemente“
2	RPS	Status-LED Redundante Versorgungsspannung	„Gerätebeschreibung“ > „Anzeigeelemente“
3	ALM	Status-LED Alarm	„Gerätebeschreibung“ > „Anzeigeelemente“

Tabelle 3: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“

Pos.	Bezeichnung	Bedeutung	Details siehe Kapitel
4	POST	Status-LED POST	„Gerätebeschreibung“ > „Anzeigeelemente“
5	-	Status-LED T-Port – 1000-Mbit/s (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“
6	-	Status-LED T-Port – 10/100-Mbit/s (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“
7	-	Anschluss 4 x SFP (1000BASE-SX/-LX, Glasfaser)	„Gerätebeschreibung“ > „Anschlüsse“
8	-	Anschluss 8 x RJ-45 (10/100/1000BASE-T)	„Gerätebeschreibung“ > „Anschlüsse“
9	Reset	Taste Reset	„Gerätebeschreibung“ > „Bedienelemente“
10	-	Anschluss 1 x RJ-45 (RS-232)	„Gerätebeschreibung“ > „Anschlüsse“
11	SFP	Status-LED SFP-Port LNK/ACT (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“

4.1.2 Draufsicht

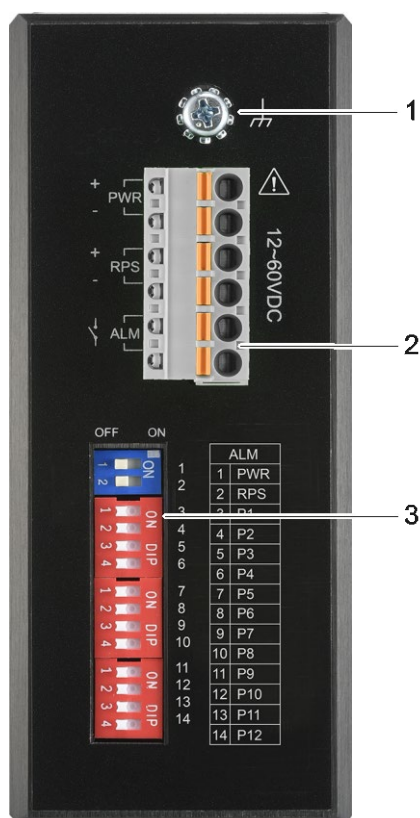


Abbildung 3: Draufsicht des Industrial-Managed-Switches

Tabelle 4: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“

Pos.	Bezeichnung	Bedeutung	Details siehe Kapitel
1	-	Erdungsschraube	-
2	-	Stecker (Stiftleiste) für Leistungsaufnahme (PWR/RPS/ALM) und potentialfreier Alarmkontakt	„Gerätebeschreibung“ > „Anschlüsse“
3	-	DIP-Schalter	„Gerätebeschreibung“ > „Bedienelemente“

4.2 Anschlüsse

4.2.1 Spannungsversorgung (PWR/RPS)

Die Federleiste (Bestell-Nr. 2231-106/026-000) kann problemlos mit der auf der Oberseite des Switches befindlichen 6-poligen Stiftleiste verbunden werden.

Die Stiftleiste hat folgende Belegung:



Abbildung 4: Anschluss Spannungsversorgung (PWR/RPS)

Tabelle 5: Legende zur Abbildung „Anschluss Spannungsversorgung (PWR/RPS)“

Anschluss	Bezeichnung	Beschreibung
+	PWR	Primärer Gleichstromeingang
-	PWR	Primärer Gleichstromeingang
+	RPS	Sekundärer Gleichstromeingang
-	RPS	Sekundärer Gleichstromeingang
	HW ALM	Kontakt für externen Alarm
	HW ALM	Kontakt für externen Alarm

ESD



Warnung vor Sachschäden durch elektrostatische Aufladung!

Switch für Gleichstrombetrieb: Die Stromversorgung erfolgt über eine externe Gleichstromquelle. Da der Switch keinen Netzschalter hat, schaltet er sich sofort ein, nachdem Sie das Netzteil in die Steckdose gesteckt haben.

4.2.2 Netzwerkanschlüsse

Der Industrial-Managed-Switch verwendet Anschlüsse mit Glasfaser- oder Kupfersteckern und unterstützt ETHERNET, Fast-ETHERNET und Gigabit Ethernet.

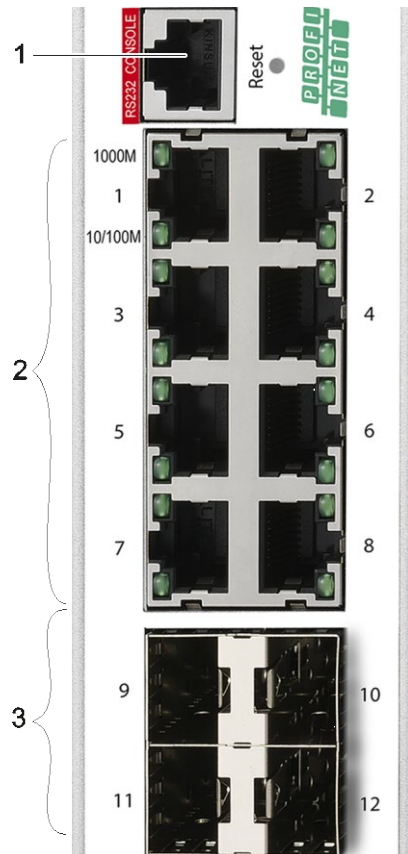


Abbildung 5: Netzwerkanschlüsse

Tabelle 6: Legende zur Abbildung „Netzwerkanschlüsse“

Pos.	Bezeichnung	Bedeutung	Details siehe Kapitel
1	-	Anschluss 1 x RJ-45 (RS-232-Port)	„Gerätebeschreibung“ > ... > „RJ-45-Anschluss“
2	-	Anschluss 8 x RJ-45 (10/100/1000BASE-T)	„Gerätebeschreibung“ > ... „10/100/1000BASE-T-Anschlüsse“
3	-	Anschluss 4 x SFP (1000BASE-SX/-LX, Glasfaser)	„Gerätebeschreibung“ > ... „1000BASE-SX/-LX-Anschlüsse“

4.2.2.1 RJ-45-Anschluss

Der Anschluss an die ETHERNET-basierten Feldbusse erfolgt über die RJ-45-Steckverbinder.

Die Pinbelegung für ETHERNET-RJ-45-Steckverbinder ist in der Richtlinie EIA/TIA 568 festgelegt.

Die Aderfarben entsprechen ebenfalls dieser Richtlinie. Pinbelegung und Aderfarbe unterscheiden sich nach der belegten Aderzahl (4- oder 8-adrig).

4.2.2.2 10/100/1000BASE-T-Anschlüsse

Die 10/100/1000BASE-T-Anschlüsse unterstützen die Netzwerkgeschwindigkeiten 10 Mbit/s, 100 Mbit/s und 1000 Mbit/s und können im Halb- und im Vollduplex-Übertragungsmodus betrieben werden. Außerdem bieten die Anschlüsse eine automatische Crossover-Erkennung (Auto-MDI/MDI-X) und sind damit Plug-and-Play-fähig. Sie brauchen die Netzkabel einfach in die Anschlüsse zu stecken; diese passen sich dann an die Endknotengeräte an. Folgendes Kabel wird für die RJ-45-Anschlüsse empfohlen:

- Kat. 5e oder besser mit einer Kabellänge von max. 100 m

4.2.2.3 1000BASE-SX/-LX-Anschlüsse

Die 1000BASE-SX/-LX-Anschlüsse sind für den Anschluss der Gigabit-SFP-Module konzipiert, die Übertragungsgeschwindigkeiten von 1000 Mbit/s unterstützen.

4.3 Anzeigeelemente

Der Industrial-Managed-Switch ist mit Geräte-LEDs sowie mit Anschluss-LEDs ausgestattet.

4.3.1 Geräte-LEDs

Anhand der Geräte-LEDs können Sie den Status des Switches schnell erkennen.

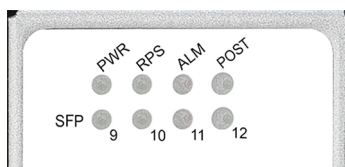


Abbildung 6: Geräte-LEDs

Tabelle 7: Legende zur Abbildung „Geräte-LEDs“

LED		Name	Status	Beschreibung
PWR		Primary-Power-LED	Grün	Der Industrial-Managed-Switch verwendet das primäre Netzteil.
			Aus	Das primäre Netzteil ist ausgeschaltet oder weist einen Fehler auf.
RPS		Redundant-Power-System-LED	Grün	Der Industrial-Managed-Switch verwendet das redundante Netzteil.
			Aus	Das redundante Netzteil ist ausgeschaltet oder weist einen Fehler auf.
ALM ¹⁾		Alarm-LED	Rot	Ausfall einer Portverbindung, sonstiger Alarm; der Alarmkontakt wird aktiviert.
			Aus	Es wird kein Alarm gemeldet.
ALM ²⁾		Alarm-LED	Rot	PROFINET-Fehler liegt vor.
			Blinkt	Keine „Application Relation“ vorhanden
			Aus	Es wird kein Alarm gemeldet.
POST		Power-On-Self-Test-LED	Grün	Der Switch ist betriebsbereit oder in Betrieb.
			Aus	Der Switch ist nicht betriebsbereit.
SFP	9 ... 12	SFP-Port-LED	Grün	Leuchtet, wenn der Anschluss verbunden ist.
			Blinkt	Datenverkehr wird über den Anschluss geleitet.
			Aus	Am Anschluss ist keine gültige Verbindung hergestellt.

¹⁾ PROFINET-Modus nicht aktiv

²⁾ PROFINET-Modus aktiv; Alarmkontakt wird nicht über die PROFINET-Diagnose gesteuert.

4.3.2 Anschluss-LEDs

Die Anschluss-LEDs geben Auskunft über die Verbindungsaktionen.

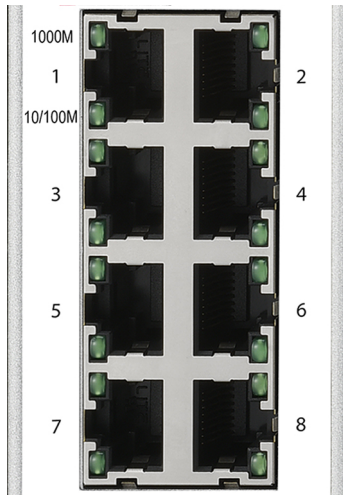


Abbildung 7: LEDs für RJ-45-Anschlüsse

Tabelle 8: Legende zur Abbildung „LEDs für RJ-45-Anschlüsse“

LED	Name	Status	Beschreibung
1000M	1000BASE T-Ports-LED (1 LED für jeden Anschluss)	Grün	Anschluss ist mit 1000 Mbit/s in Betrieb.
		Blinkt	Datenverkehr wird über den Anschluss geleitet.
		Aus	Am Anschluss ist keine gültige Verbindung hergestellt.
10/100M	10/100BASE T-Ports-LED (1 LED für jeden Anschluss)	Grün	Anschluss ist mit 10/100 Mbit/s in Betrieb.
		Blinkt	Datenverkehr wird über den Anschluss geleitet.
		Aus	Am Anschluss ist keine gültige Verbindung hergestellt.

4.4 Bedienelemente

4.4.1 DIP-Schalter

An der Oberseite des Industrial-Managed-Switches befinden sich DIP-Schalter für die Alarmkonfigurationen. Bei aktivierter Alarmberichtsfunktion wird der Alarmkontakt bei Eintreten des Ereignisses geschaltet.

Bei nicht aktivem PROFINET-Modus erfolgt bei Aktivierung der Alarmberichtsfunktion zusätzlich die Anzeige über die Geräte-LED „ALM“ (siehe Kapitel „Anzeigeelemente“).

Die Bedeutungen der DIP-Schalter-Einstellungen sind nachfolgend erläutert:

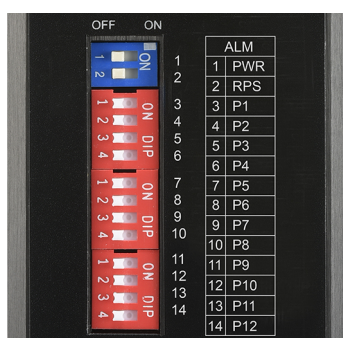


Abbildung 8: DIP-Schalter

Tabelle 9: Legende zur Abbildung „DIP-Schalter“

Tabell 3: Legende zur Abbildung „DIN“-Schalter

Nr.	Name	Status	Beschreibung
1	PWR	ON	Die Alarmberichtsfunktion für das primäre Netzteil ist aktiviert.
		OFF	Die Alarmberichtsfunktion für das primäre Netzteil ist deaktiviert.
2	RPS	ON	Die Alarmberichtsfunktion für das sekundäre Netzteil ist aktiviert.
		OFF	Die Alarmberichtsfunktion für das sekundäre Netzteil ist deaktiviert.
3	P1	ON	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 1 ist aktiviert.
		OFF	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 1 ist deaktiviert.
...			
10	P8	ON	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 8 ist aktiviert.
		OFF	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 8 ist deaktiviert.
11	P9	ON	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 9 (SFP) ist aktiviert.
		OFF	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 9 (SFP) ist deaktiviert.

Tabelle 9: Legende zur Abbildung „DIP-Schalter“

Nr.	Name	Status	Beschreibung
...			
14	P12	ON	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 12 (SFP) ist aktiviert.
		OFF	Die Alarmberichtsfunktion bei Verbindungsfehler für Port 12 (SFP) ist deaktiviert.

Die Alarmfunktion kann sowohl für jeden Anschluss als auch für die primäre oder die redundante Stromversorgung über DIP-Schalter vom Anwender manuell ein- und ausgeschaltet werden.

Der DIP-Schalter muss auf „ON“ stehen, um die entsprechende Alarmfunktion aktivieren zu können. Die Default-Einstellung ist „OFF“.

Zur Konfigurierung und Einstellung der DIP-Schalter empfiehlt sich folgendes Vorgehen bei der ersten Installation:

1. Stellen Sie die DIP-Schalter auf „OFF“.
2. Installieren Sie den Industrial-Managed-Switch in Ihrem Netzwerk.
3. Wählen Sie den Port, der zu überwachen ist oder der den Alarm aktivieren soll. Eine Mehrfachauswahl kann erfolgen.
4. Stellen Sie den DIP-Schalter des entsprechenden Anschlusses auf „ON“.
5. Schalten Sie den Industrial-Managed-Switch ein.

4.4.2 Reset-Taster



Abbildung 9: Reset-Taster

Tabelle 10: Legende zur Abbildung „Reset-Taster“

Name	Status	Beschreibung
Reset	Drücken Sie den Reset-Taster 2 Sekunden lang und lassen Sie ihn wieder los.	Das System wird neu gestartet.

Hinweis



Wichtiger Hinweis!

Verwenden Sie zum Drücken des Reset-Tasters einen geeigneten Gegenstand (z. B. einen Kugelschreiber oder eine aufgebogene Büroklammer).

4.5 Aufkleber

Auf der Rückseite des Industrial-Managed-Switches befindet sich ein Aufkleber mit der „Serial NO“ und der „MAC Address“.

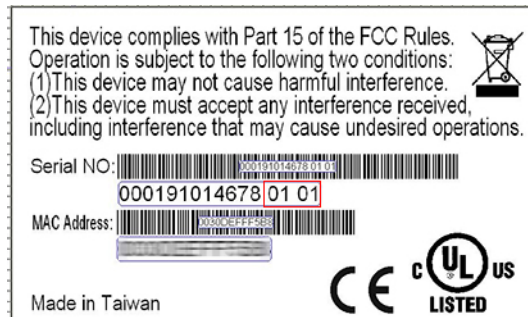


Abbildung 10: Aufkleber (Beispiel)

Tabelle 11: Legende zur Abbildung „Aufkleber (Beispiel)“

Nr.	Beschreibung „Serial NO“
01	Firmwareversion (linke Ziffernfolge)
01	Hardwareversion (rechte Ziffernfolge)

4.6 Technische Daten

4.6.1 Gerätedaten

Tabelle 12: Technische Daten – Gerätedaten

Breite	50 mm
Höhe	162 mm (ab Oberkante Tragschiene)
Tiefe	120 mm
Gewicht	945 g
Schutzart	IP30

4.6.2 Systemdaten

Tabelle 13: Technische Daten – Systemdaten

MAC-Tabelle	bis 16000 Adressen
VLAN	Port-based und Tag-based (4094 VIDs)
Jumbo Frame Size	10240 Byte
Wellenlänge Lichtleiter	abhängig vom SFP-Modul
Maximale Längen	10/100/ 1000BASE-T: 100 m; Glasfaser: 2 ... 80 km RS-232: 15 m

4.6.3 Versorgung

Tabelle 14: Technische Daten – Versorgung

Versorgungsspannung	DC 12 ... 60 V
Leistungsaufnahme max.	18 W

4.6.4 Kommunikation

Tabelle 15: Technische Daten – Kommunikation

Konfiguration und Update	1 x USB-Host 2.0
Ports (Kupfer; RJ-45)	8 x 10/100/1000BASE-T 1 x RS-232
Ports (LWL)	4 x 1000BASE-SX/-LX
Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/-FX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Class of Service IEEE 802.1ab Link Layer Discovery Protocol (LLDP) PROFINET CC-B
Netzwerkmanagement	• CLI durch Konsolenport, Telnet und SSH • RJ-45-Port für lokales Management • Web-based Management • Statusanzeige und Ereignisreport über Web-based Management • Port-Management • Autonegotiation • Duplex-Modus • 802.3x Flow Control • Unterstützung Jumbo Frame • SNMP v1 und v2c Management • SNMP Trap • Link UP/Down • Konfigurationswechsel • Kaltstart • Warmstart • Trap-Übertragung: 5 Ziele • Bereitstellung von Fehler-, Leistungs-, Konfigurations- und Sicherheitsmanagement • RMON: 4 RMON-Gruppen 1, 2, 3, 9 (Verlauf, Statistik, Alarme und Ereignisse) für verbessertes Traffic-Management, Überwachung und Analyse

Netzwerksicherheit	• ACL • Port-basierte Authentifizierung des Netzwerkzugriffs • MAC-basierte Authentifizierung des Netzwerkzugriffs • SNMP v3 Sicherheit • SSH • Web-Authentifizierung
--------------------	--

4.6.5 Umgebungsbedingungen

Tabelle 16: Technische Daten – Umgebungsbedingungen

Umgebungstemperatur, Betrieb	-40 ... +70 °C
Umgebungstemperatur, Lagerung	-40 ...+80 °C
Relative Feuchte (ohne Betauung)	10 ... 95 %
Vibrationsfestigkeit gemäß	EN 60068-2-6
Schockfestigkeit gemäß	EN 60068-2-27
EMV-Störfestigkeit gemäß	EN 55024 EN 61000-6-2 EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8
EMV-Störaussendung gemäß	FCC Part 15 EN 55022: Klasse A EN 55011: Klasse A EN 61000-6-4

4.7 Zulassungen

Folgende Zulassungen wurden für das WAGO-ETHERNET-Zubehör „Industrial-Managed-Switch“ (852-1605) erteilt:



Konformitätskennzeichnung



Ordinary
Locations

UL61010-2-201 (E175199)

5 PROFINET

5.1 Systemübersicht

5.1.1 Aufbau

5.1.1.1 Geräteklassen

Der Prozessdatenaustausch bei PROFINET IO erfolgt nach dem Provider-Consumer-Modell:

- „Provider“ erzeugen Daten und versenden diese über Datentelegramme ohne konkrete Anforderung.
- „Consumer“ empfangen Daten und verarbeiten diese.

Tabelle 17: Beispiele für Provider und Consumer

Daten	Provider	Consumer
Prozessdaten (Eingänge)	IO-Devices	IO-Controller
Prozessdaten (Ausgänge)	IO-Controller	IO-Devices
Parameterdaten	IO-Controller	IO-Devices

PROFINET IO definiert folgende Geräteklassen (siehe auch Abbildung „Geräteklassen bei PROFINET IO“):

- **IO-Controller:**
Ein IO-Controller ist typischerweise Bestandteil einer überlagerten SPS („**S**peicher-**P**rogrammierbare **S**teuerung“), in der das Automatisierungsprogramm abläuft und die eingehenden Prozess- und Diagnosedaten verarbeitet werden. Der IO-Controller ist der Provider der Ausgangs- und Parameterdaten und der Consumer der Eingangsdaten der IO-Devices.
- **IO-Device:**
Ein IO-Device ist ein dezentral angeordnetes Feldgerät, das über PROFINET IO an einen oder mehrere IO-Controller angekoppelt wird. Ein IO-Device ist der Provider der Eingangsdaten und der Consumer der Ausgangs- und Parameterdaten.
Die PROFINET-Switches von WAGO sind IO-Devices.
 - **I-Device:**
Ein I-Device ist ein intelligentes IO-Device mit einer integrierten Steuerungseinheit (z. B. eine integrierte SPS), das vorverarbeitende Funktionen übernehmen kann (z. B. I/O-Systeme). Ein I-Device ist der Provider der Eingangsdaten und der Consumer der Ausgangs- und Parameterdaten.
- **IO-Supervisor:**
Der IO-Supervisor (z. B. eine Engineering-Station) ist typischerweise ein PG („**P**rogrammier**g**erät“), PC oder HMI („**H**uman **M**achine **I**nterface“) für

die Inbetriebsetzung oder Diagnose. Der Einsatz des IO-Supervisors wird oft nur temporär für die Projektierung des Netzwerkes und für die Konfiguration des IO-Controllers benötigt.

In einem PROFINET-IO-System gibt es immer mindestens 1 IO-Controller und 1 oder mehrere IO-Devices. Der IO-Supervisor ist während der Inbetriebnahme und zur Fehlersuche meist nur temporär eingebunden.

5.1.1.2 Gerätemodell eines IO-Devices

PROFINET unterstützt IO-Devices in folgenden Ausführungen:

- **Kompakte Feldgeräte:**
Der Ausbaugrad ist im Auslieferungszustand bereits festgelegt und kann durch den Anwender nicht verändert werden.
- **Modulare Feldgeräte:**
Der Ausbaugrad kann beim Projektieren der Anlage individuell an den Einsatzfall angepasst werden.

Zur Beschreibung der technischen und funktionellen Möglichkeiten der IO-Devices dient das Gerätemodell. Dieses Gerätemodell ist in der GSDML-Datei durch den DAP („**D**evice **A**ccess **P**oint“) für eine bestimmte Gerätefamilie festgelegt. Ein DAP ist der Zugangspunkt für die Kommunikation des Feldgerätes mit der ETHERNET-Schnittstelle und dem Automatisierungsprogramm.

Für das Gerätemodell eines IO-Devices sind folgende Strukturen standardisiert:

- Der **DAP** kennzeichnet das IO-Device als Einheit.
- Der **Slot** kennzeichnet den physikalischen Steckplatz eines I/O-Moduls in einem modularen IO-Device. Anhand der Slots werden die projektierten Module adressiert. Diese Module enthalten wiederum 1 oder mehrere Subslots für den Datenaustausch.
- Die **Subslots** innerhalb eines Slots bilden die eigentliche Schnittstelle zu den Ein- und Ausgängen und damit zum Prozess. Die Granularität eines Subslots und damit die Aufteilung der I/O-Daten ist herstellerspezifisch. Der Dateninhalt eines Subslots wird immer durch eine Statusinformation begleitet, die die Gültigkeit der Daten bestimmt. Jeder Slot muss mindestens 1 Subslot beinhalten.
- Der **Index** gilt nur für den azyklischen Datenaustausch. Der Index spezifiziert die Daten, die innerhalb eines Slots bzw. Subslots geschrieben oder gelesen werden können. Bestimmte Indexe sind normativ festgelegt. Weitere Indexe können herstellerspezifisch definiert werden.

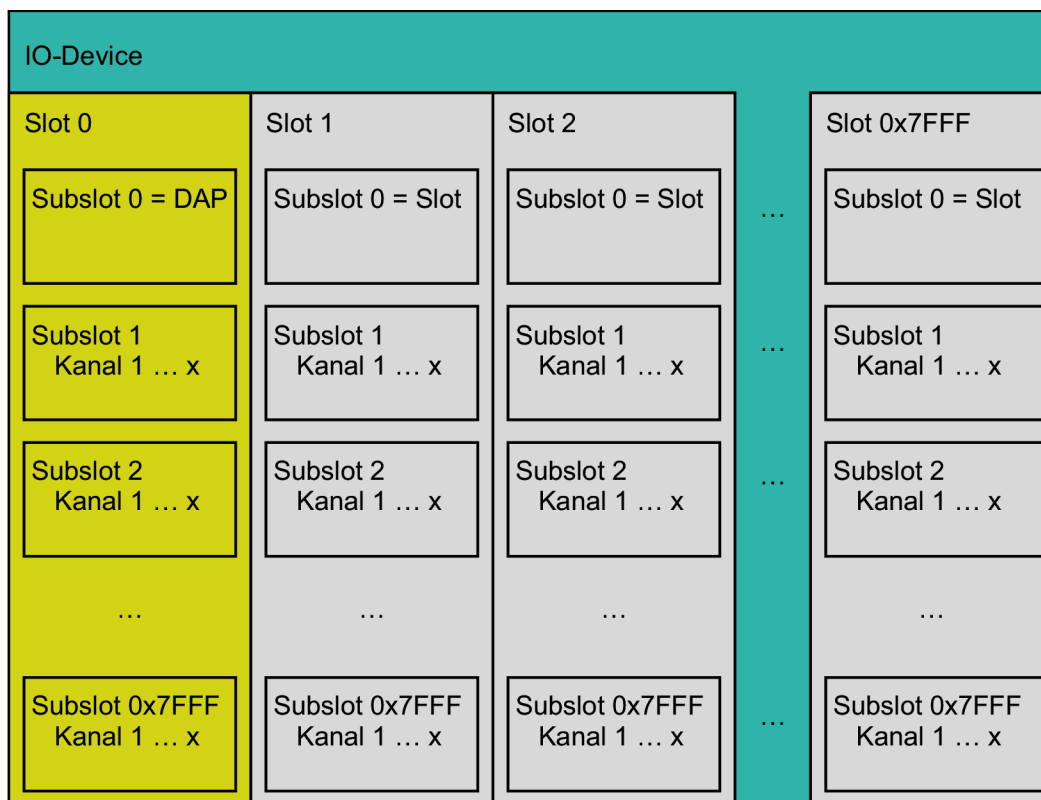


Abbildung 11: Adressierung der Daten eines IO-Devices über Slots bzw. Subslots

Die Adressierung der Daten erfolgt in Abhängigkeit von der Übertragungsart:

Tabelle 18: Adressierung der Daten in Abhängigkeit von der Übertragungsart

Übertragungsart	Adressierung durch Kombination von		
	Slot	Subslot	Index
Zyklisch	X	X	–
Azyklisch	X	X	X

Die Angabe der Slot/Subslot-Kombination kann herstellerspezifisch festgelegt werden.

Der PROFINET-Managed-Switch von WAGO enthält nur den Slot 0. Die Zuordnung der Subslots ist in der folgenden Abbildung dargestellt. Jeder Switch-Port entspricht einem Sub-Slot.

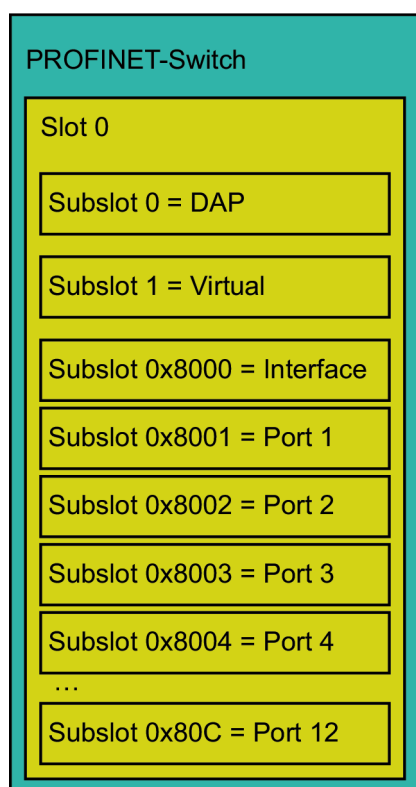


Abbildung 12: Zuordnung der Subslots im PROFINET-Managed-Switch von WAGO

5.2 Kommunikation

In PROFINET-Netzwerken erfolgt die Kommunikation über Industrial ETHERNET.

Für den Aufbau der Kommunikation zwischen dem IO-Controller und einem IO-Device (z. B. der PROFINET-Managed-Switch von WAGO) müssen die Kommunikationswege etabliert werden. Diese Kommunikationswege werden beim Systemanlauf vom IO-Controller anhand der Projektierungsdaten eingerichtet. Damit ist die Kommunikationsbeziehung für den Datenaustausch eindeutig spezifiziert.

Jeder Datenaustausch ist in eine AR („**A**pplication **R**elation“) eingebettet. Über die AR werden allgemeine Kommunikationsparameter sowie herstellerspezifische Parameter geladen.

Bei PROFINET sind folgende ARs definiert:

- Implizite AR
Diese AR definiert eine Applikationsbeziehung zwischen IO-Controller bzw. IO-Supervisor und dem IO-Device zum azyklischen Lesen von Daten aus dem IO-Device. Schreibzugriffe sind bei einer impliziten AR nicht erlaubt. Diese AR muss nicht explizit etabliert werden, sondern ist standardmäßig immer im Zugriff der IO-Devices.
- IOCAR („**I**O-**C**ontroller **A**pplication **R**elation“)
Diese AR dient dem Austausch von zyklischen Eingabe- und Ausgabedaten, von azyklischen Daten sowie von bidirektionalen Alarmen.
- IOSAR („**I**O-**S**upervisor **A**pplication **R**elation“)
Diese AR dient dem Datenaustausch zwischen einem IO-Supervisor und dem IO-Device sowie der Übernahme eines oder mehrerer Submodule eines IO-Devices, die entsprechenden IO-Controllern zugeordnet sind. Der Datenaustausch kann dem einer IOCAR entsprechen.

Innerhalb der AR spezifizieren sogenannte CRs („**C**ommunication **R**elation“) die Daten eindeutig:

- Record Data CR (R-CR):
Kommunikationskanal für den azyklischen Datenaustausch
- IO Data CR (IO-CR):
Kommunikationskanäle für den zyklischen Datenaustausch (Eingangs- und Ausgangsdaten)

- Alarm CR (A-CR):
Kommunikationskanal für die Alarme

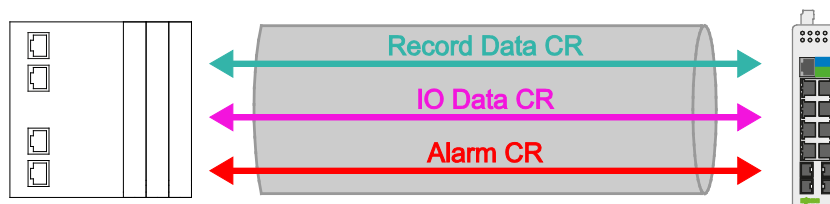


Abbildung 13: Kommunikationsbeziehungen bei PROFINET

In einem PROFINET-System mit PROFINET-Managed-Switches von WAGO können mehrere IO-Controller eingesetzt werden. Dabei kann 1 IO-Controller zu mehreren IO-Devices jeweils 1 AR aufbauen.

5.3 Datenübertragung

Die Übertragung von Prozessdaten in PROFINET-Netzwerken erfolgt grundsätzlich in Echtzeit (RT = „**Real Time**“). Zusätzlich können Datentelegramme auch in NRT („**Non-Real Time**“) über Standard ETHERNET übertragen werden. PROFINET nutzt folgende Möglichkeiten:

- NRT-Kommunikation innerhalb von und zwischen Netzwerken:
Diese Kommunikation entspricht der „normalen“ Kommunikation in ETHERNET-Netzwerken. Echtzeitbedingungen werden nicht eingehalten. Diese Kommunikation kann z. B. zu HMI-Geräten aufgebaut werden.
- RT-Kommunikation innerhalb eines Netzwerkes:
Diese Kommunikation zielt auf ein hohes Maß an Determinismus ab. Dafür nutzt sie den RT-Kanal. UDP/IP wird in dieser Konstellation nicht verwendet.
- RT-Kommunikation zwischen Netzwerken:
Diese Kommunikation erfolgt mit zusätzlicher Protokollierung. Dafür nutzt sie den RT-Kanal. Zusätzlich wird UDP/IP verwendet.

5.3.1 Real-Time-Kommunikation

Datentelegramme im PROFINET-Format werden gemäß IEEE 802.1Q gegenüber Standarddatentelegrammen priorisiert. Damit ist der in der Automatisierungstechnik erforderliche Determinismus sichergestellt. Bei diesem Verfahren werden die Daten über priorisierte ETHERNET-Datentelegramme übertragen.

5.3.2 Übertragungsmethoden

Die Datenübertragung in PROFINET-Netzwerken erfolgt im Vollduplexmodus („Full Duplex“):

- Ein PROFINET-Gerät kann gleichzeitig Daten empfangen oder senden.
- Die Erkennung von Kollisionen (CSMA/CD) ist ausgeschaltet.
- Die Netzausdehnung hängt nur von den Leistungsgrenzen der verwendeten Sende- und Empfangskomponenten ab.

5.3.3 Übertragungsarten

PROFINET unterstützt die folgenden Übertragungsarten:

Azyklische Übertragung

Azyklisch erfolgt die Übertragung von Daten für:

- die Etablierung der Echtzeitverbindung (Verbindungsaufbau)
- die Parametrierung des PROFINET-Managed-Switches sowie seiner Submodule
- das Lesen von Diagnoseinformationen

- das Auslesen von Identifikations-, Maintenance- bzw. Wartungsinformationen
- das Lesen von I/O-Daten
- das Lesen von Alarminformationen
- u. a.

Zyklische Übertragung

Zyklisch erfolgt die Übertragung von Prozessdaten und anderen Nutzdaten.

Die zyklischen I/O-Daten werden als Real-Time-Daten unquittiert übertragen. Die Zykluszeit kann individuell parametrierbar werden.

Die Überwachung der Datenverbindung erfolgt anhand einer Zeitüberwachung, die aus einem Vielfachen der parametrierbaren Sendezykluszeit abgeleitet wird.

Bei der Übertragung im Echtzeittelegramm werden die Daten eines Subslots durch Nutzdatenbegleiter (Providerstatus) ergänzt. Diese Statusinformationen werden vom jeweiligen Consumer der I/O-Daten ausgewertet. Somit kann dieser Consumer die Gültigkeit der Daten allein aus dem zyklischen Datenaustausch beurteilen. In die Gegenrichtung werden dafür die Statusinformationen des Consumers an den Provider übertragen.

Abhängig vom E/A-Typ eines Submoduls können Provider- und Consumerstatus auch in beide Richtungen übertragen werden.

Die Datentelegramme enthalten im Anschluss an die Daten weitere Statusinformationen (APDU-Status). Das Ausbleiben der zyklischen Daten wird vom jeweiligen Consumer der Kommunikationsbeziehung überwacht. Bleibt der Empfang der Daten innerhalb der projektierten Überwachungszeit aus, baut der entsprechende Consumer die Verbindung ab.

5.3.4 Telegrammaufbau

Ein Datentelegramm bei PROFINET ist nach folgender Struktur aufgebaut:

Dest. addr.	Source addr.	VLAN tag	Ether type	FrameID	Application data	Cycle counter	Data status	Transfer status	FCS
-------------	--------------	----------	------------	---------	------------------	---------------	-------------	-----------------	-----

Tabelle 19: Bereiche im PROFINET-Telegramm

Bereich	Umfang	Beschreibung
Dest. addr.	6 Byte	Zieladresse (MAC-Adresse)
Source addr.	6 Byte	Quelladresse (MAC-Adresse)
VLAN tag	4 Byte	Dient der Übertragung der Priorität.
Ether type	2 Byte	0x8892 → Telegrammtyp PROFINET RT
FrameID	2 Byte	Enthält die ausgetauschte FrameID (siehe auch Tabelle „Beispiele für ‚FrameID‘“).
Application data	0 Byte ... 1440 Byte	Anwenderdaten
Cycle counter	2 Byte	Enthält die Zyklusnummer in Vielfachen von 31,25 µs. Beispiel: Zykluszeit = 4 ms: Cycle counter = 128 (128 × 31,25 µs = 4 ms)
Data status	1 Byte	Enthält Angaben zum Datenstatus (siehe Tabelle „Beispiel für ‚Data status‘“).
Transfer status	1 Byte	RT_Class_1: 0 RT_Class_3: 0/1 (1 = Ersatzframe)
FCS	4 Byte	Prüfsumme zum Erkennen von Übertragungsfehlern

5.4 Adressierung

Die Adressierung eines Gerätes in einem PROFINET-Netzwerk besteht aus mehreren Komponenten:

- dem Gerätenamen
- der MAC-Adresse
- der IP-Adressierung (IP-Adresse, Subnetzmaske und Gateway-Adresse)

Im Auslieferungszustand hat der PROFINET-Managed-Switch folgende IP-Adresse: **0.0.0.0**

Dem PROFINET-Switch wird über das Protokoll DCP eine IP-Adresse zugewiesen. Diese Zuweisung kann z. B. durch den IO-Controller erfolgen.

5.4.1 Geräteiname

Bevor ein IO-Device von einem IO-Controller angesprochen werden kann, müssen beide Geräte einen Gerätenamen erhalten. Bei PROFINET ist diese Vorgehensweise gewählt worden, weil Namen einfacher zu handhaben sind als IP-Adressen.

Hinweis



Die Verwendung von Zeichen ist eingeschränkt!

PROFINET unterstützt nur ausgewählte Zeichen bei der Namensvergabe. Zu diesen Zeichen gehören die Ziffern 0 ... 9, die Kleinbuchstaben a ... z, der Bindestrich „-“ und der Punkt „.“.

Der Geräteiname kann maximal 127 Zeichen enthalten, wobei zwischen Bindestrichen und Punkten bis zu 63 Buchstaben oder Ziffern verwendet werden können.

Leerzeichen sind nicht erlaubt!

Im Auslieferungszustand hat der PROFINET-Managed-Switch noch keinen Gerätenamen. Der PROFINET-Managed-Switch ist jedoch erst nach der Zuweisung eines Gerätenamens durch einen IO-Supervisor (PG oder PC) für einen IO-Controller im Netzwerk identifizierbar. Nach anschließender Zuweisung der IP-Einstellungen kann die Verbindung anhand der Projektierungsdaten etabliert werden.

5.5 Konformitätsklassen („Conformance Classes“)

Die Anforderungen an eine Anwendung mit PROFINET IO können in 3 aufeinander aufbauende Konformitätsklassen („CC“ = „Conformance Classes“) eingeteilt werden. In der Norm IEC 61784-2 werden die 3 Konformitätsklassen **CC-A**, **CC-B** und **CC-C** für PROFINET definiert.



Abbildung 14: Übersicht der Konformitätsklassen A bis C

Diesen 3 Konformitätsklassen können bestimmten Anwendungen zugeordnet werden:

CC-A: Anlagenautomation („Plant Control“)

- Entspricht den Anforderungen einer einfachen Anlagenautomation.
- Die eingesetzten PROFINET-Geräte sind zertifiziert.
- Bietet Grundfunktionen für PROFINET IO mit RT-Kommunikation.
- Alle IT-Services können uneingeschränkt eingesetzt werden.
- Für Zykluszeiten von bis zu 100 ms (z. B. in einer Anlagenautomation)
- Die Verwendung einer bestehenden Gebäudeverkabelung ist möglich.
- Definition der Einbindung von drahtlosen Systemen wie *Bluetooth®* oder WLAN.
- Festlegung der Einbindung von bestehenden Feldbussen wie PROFIBUS, INTERBUS oder DeviceNet (herstellerübergreifend)
- Sicherheitskonzepte für den Zugriff aus dem Internet für Remote-Diagnose ohne Eingriffsmöglichkeiten durch Unbefugte

CC-B: Maschinenautomation („Machine Control“)

- Entspricht den Anforderungen für die Maschinenautomation.
- Geräte und Netzwerkinfrastruktur müssen zertifiziert sein.
- Erweitert das Konzept um eine Netzwerkdiagnose über IT-Mechanismen und um Topologieinformationen.
- Die Funktion „Systemredundanz“ (z. B. bei Prozessautomatisierung) ist in einer Erweiterung der CC-B zur CC-B(PA) enthalten.
- Für Zykluszeiten der Datenübertragung von bis zu 10 ms (z. B. eine SPS als typischer Controller für eine Maschine)
- Die Infrastruktur muss klar definierten Richtlinien folgen.
- Nur PROFINET-Komponenten sind erlaubt. Auch die Switches und Kabel müssen die Mindestanforderungen von PROFINET erfüllen.
- Kabel müssen eine durchgehende Schirmung aufweisen, um die EMV-Festigkeit zu gewährleisten.

CC-C: Bewegungsautomation („Motion Control“)

- Erfüllt die Anforderungen für die Bewegungsautomation.
- Geräte und Netzwerkinfrastruktur müssen zertifiziert sein.
- Beschreibt die Basisfunktionen für Geräte mit hardwareunterstützter Bandbreitenreservierung und Synchronisation (IRT-Kommunikation).
- Bildet die Basis für takttsynchrone Applikationen.
- Für Zykluszeiten von unter 1 ms (z. B. zur Kontrolle von Bewegungen)
- Alle Komponenten müssen Klasse-C-Geräte sein und können zeitlich synchronisiert werden.
- Isochrone Kommunikation ist die Voraussetzung zum Erreichen der geforderten Zykluszeiten. Isochron sind die Teilnehmer dann, wenn sie alle die gleiche Zeit haben („Uhrenabgleich“).

Die einzelnen Konformitätsklassen können miteinander kombiniert werden. Ein System mit PROFINET IO kann unterschiedliche Konformitätsklassen umfassen. Auch mehrere Zonen derselben Konformitätsklasse sind problemlos möglich.

Damit diese Aufteilung realisiert werden kann, müssen die Geräte einer Konformitätsklasse bestimmte Mindestanforderungen betreffend der implementierten Funktionen und Protokolle erfüllen.

Tabelle 20: Vergleich Konformitätsklassen

Anforderung	Klasse A (CC-A)	Klasse B (CC-B)	Klasse C (CC-C)
Basisfunktionen	• RT-Kommunikation • Zyklische E/A • Parameter • Alarme	• RT-Kommunikation • Zyklische E/A • Parameter • Alarme • Netzwerkdiagnose • Topologieinformationen • Systemredundanz	• RT-Kommunikation • Zyklische E/A • Parameter • Alarme • Netzwerkdiagnose • Topologieinformationen • Reservierte Bandbreite (IRT) • Synchronisation
Verkabelung	Gemäß IEC 61784-5-3 und IEC 24702 • Kupfer • LWL • Drahtlos	Gemäß IEC 61784-5-3 • Kupfer • LWL	Gemäß IEC 61784-5-3 • Kupfer • LWL
Typischer Einsatz	• Infrastrukturbauten • Gebäudeautomation	• Fertigungsautomation • Prozessautomation	• Motion control

In der Praxis können Geräte, die der Konformitätsklasse CC-A entsprechen, durchaus einzelne Funktionalitäten aus CC-B oder auch CC-C enthalten.

5.6 Medienredundanz

PROFINET realisiert Medienredundanz mit Hilfe des MRP-Protokolls. Dabei werden die PROFINET-Geräte in einer Ringtopologie angeordnet.

In der Ringtopologie übernimmt 1 Gerät die Rolle des Redundanzmanagers. Alle anderen Geräte im Ring sind Redundanzclients.

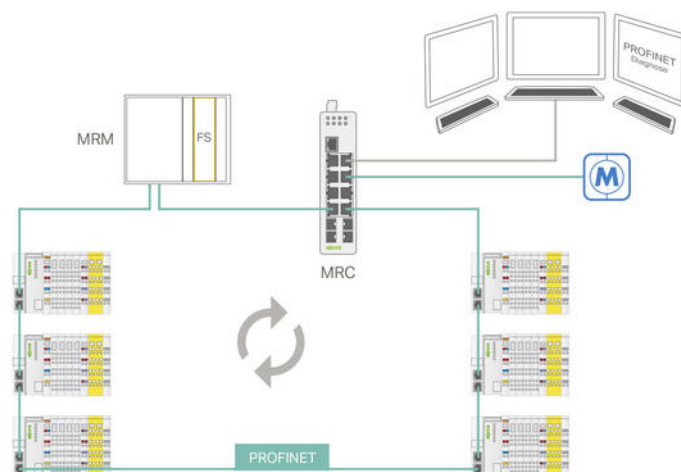


Abbildung 15: Medienredundanz bei PROFINET (Ringtopologie)

Tabelle 21: Legende zur Abbildung „Medienredundanz bei PROFINET (Ringtopologie)“

Kürzel	Bedeutung
MRM	Redundanzmanager
MRC	Redundanzclient

Die Auswahl und Festlegung der Ringports erfolgt während der Projektierung. Dabei kann jeder Port am Produkt als Redundanzmanager oder als Redundanzclient fungieren.

Funktion der Medienredundanz

Bei störungsfreier Kommunikation wird im Redundanzmanager einer der beiden Ringports blockiert. Somit ist gewährleistet, dass keine Datentelegramme kreisen. Aus der Sicht der Datenkommunikation wird der Ring zu einer Linientopologie.

Der Redundanzmanager überwacht die Ringtopologie auf Unterbrechungen, indem er Testtelegramme von beiden Ringports versendet. Die Testtelegramme durchlaufen die Ringtopologie in beiden Richtungen, bis sie am jeweils anderen Ringport des Redundanzmanagers ankommen. Wird der Empfang eines der Testtelegramme nicht bestätigt, liegt eine Unterbrechung der Kommunikation vor. Diese Unterbrechung kann verschiedene Ursachen haben:

- Durch Ausfall der Verbindung zwischen 2 Geräten
- Durch Ausfall eines Geräts in der Ringtopologie

Liegt eine Unterbrechung vor, schaltet der Redundanzmanager seine beiden Ringports durch. Über diesen Ersatzweg wird wieder eine funktionierende Verbindung zwischen allen verbleibenden Geräten in Form einer Linientopologie hergestellt.

Die Zeit zwischen Ringunterbrechung und Wiederherstellung einer funktionsfähigen Linientopologie wird als Rekonfigurationszeit bezeichnet.

Sobald die Unterbrechung behoben ist, werden die ursprünglichen Übertragungswege wiederhergestellt, die beiden Ringports im Redundanzmanager voneinander getrennt und die Redundanzclients über den Wechsel informiert. Die Redundanzclients benutzen anschließend die bekannten Wege zu den anderen Geräten.

Alle Geräte (IO-Controller, IO-Devices, Switches usw.), die über eine Ringtopologie verbunden sind, müssen die Funktion „Medienredundanz“ unterstützen. Diese Geräte bilden eine sogenannte Redundanzdomäne.

Die Funktion „Medienredundanz“ wird beim PROFINET-Managed-Switch über folgendes Verfahren realisiert:

MRP („Media Redundancy Protocol“)

Dieses Redundanzverfahren ist das Standardverfahren und basiert auf der Norm IEC 61158, Type 10 „PROFINET“. Bei diesem Verfahren können maximal 50 Geräte über eine Ringtopologie verbunden werden. Die typische Rekonfigurationszeit beträgt 200 ms.

Folgende Voraussetzungen müssen für einen störungsfreien Betrieb mit MRP erfüllt sein:

- Alle Geräte, die über die Ringtopologie verbunden sind, müssen MRP unterstützen.
- Die Funktion „MRP“ muss bei allen Geräten aktiviert sein.
- Alle Geräte müssen über ihre Ringports miteinander verbunden sein.
- Die Ringtopologie darf aus max. 50 Geräte bestehen.
- Bei den Geräten ist keine IRT-Funktionalität eingestellt.

5.7 Protokolle

In diesem Kapitel werden PROFINET-Protokolle aufgeführt, die im PROFINET-Managed-Switch zum Einsatz kommen.

DCP

Über DCP („**D**ynamic **C**onfiguration **P**rotocol“) gemäß IEC 61158 können Geräte in einem ETHERNET-System konfiguriert werden. So können z. B. an unadressierte Geräte Gerätenamen und IP-Einstellungen verteilt werden, damit diese Geräte über das IP-Protokoll im Netzwerk erreichbar sind.

Für die Abfrage und Vergabe der Adressinformationen stellt DCP verschiedene Dienste zur Verfügung, z. B.:

- DCP_Identify-Abfragen
- DCP_Get-Dienste
- DCP_Set-Dienste

Das ETHERNET-Gerät befindet sich bei der ersten Inbetriebnahme in der Werkseinstellung. Ein GeräteName ist nicht vorhanden (Leerstring, NIL) und die IP-Einstellungen **Adresse**, **Subnetzmaske** und **Standard-Gateway** sind jeweils auf 0.0.0.0 eingestellt.

Das ETHERNET-Gerät ist erst über ICMP erreichbar, nachdem ihm über entsprechende DCP_Set-Dienste ein GeräteName und gültige IP-Einstellungen zugewiesen wurden.

LLDP

LLDP („**L**ink **L**ayer **D**iscovery **P**rotocol“) ist ein Protokoll auf der Schicht 2 des ISO/OSI-Referenzmodells.

LLDP ermöglicht einem ETHERNET-Gerät im LAN („**L**ocal **A**rea **N**etwork“), Informationen über sich selbst zu versenden und von benachbarten Geräten Informationen zu empfangen. Das Gerät speichert die empfangenen Informationen in seiner LLDP-MIB („**M**anagement **I**nformation **B**ase“), die von einem Netzwerkmanagement-System über SNMP ausgelesen werden kann.

LLDP-Telegramme werden mit dem EtherType 0x88CC sowohl in periodischen Abständen als auch bei LLDP-MIB-Änderungen an die Multicast-MAC-Adresse **01:80:C2:00:00:0E** versendet. Die Telegramme werden nur vom unmittelbaren Nachbarn in Netzwerk empfangen und verarbeitet.

MRP

MRP („**M**edia **R**edundancy **P**rotocol“) ist spezifiziert gemäß IEC 62439 und ermöglicht im Fehlerfall die Umschaltung der Kommunikationswege für TCP/IP- und RT_Class_1-Verkehr innerhalb von 200 ms. Zur Anwendung dieses Verfahrens sind 1 MRM („**M**edia **R**edundancy **M**anager“) sowie 1 oder mehrere, in einer Ringtopologie angeordnete MRCs („**M**edia-**R**edundancy **C**lients“)

erforderlich. Somit müssen die installierten Geräte über mindestens 2 ETHERNET-Ports verfügen.

Der MRM ist in der Regel in einem IO-Controller oder einem PROFINET-Switch realisiert. Der MRM wickelt den Telegrammverkehr zu den in der Ringtopologie befindlichen Geräten im fehlerfreien Betrieb lediglich über 1 der beiden Ringports ab. Dadurch trennt er die Ringtopologie in eine virtuelle Linientopologie auf. Der MRM überprüft darüber hinaus die projektierte Ringtopologie mittels zyklisch rotierender Testtelegramme auf eventuelle Unterbrechungen. Diese Testtelegramme werden von den MRC lediglich zum nächsten Teilnehmer durchgereicht. Empfängt der MRM die an seinem ersten Ringport ausgesendeten Testtelegramme an seinem zweiten Ringport nicht zurück, prüft er, an welcher Stelle die Ringtopologie unterbrochen wurde. Anschließend schaltet er den Telegrammverkehr zu den nicht mehr über den ersten Ringport erreichbaren Teilnehmern auf den zweiten Ringport um.

RTC

RTC („Real Time Cyclic“) ist ein zyklisches PROFINET-Protokoll.

Mit der Echtzeittechnologie werden TCP/IP-Schichten umgangen, sodass die deterministische Leistung von Anwendungen eine Geschwindigkeit von 1 bis 10 Millisekunden erreicht. Damit ist PROFINET RT ideal für Anwendungen, bei denen die Steuerung von digitalen und analogen I/Os für Produktionszyklen entscheidend ist. Durch das Überspringen von TCP/IP und die Übertragung von Datennachrichten von der physikalischen ETHERNET-Schicht zur Anwendungsschicht bietet „PROFINET Real Time“ einen hochpräzisen Determinismus.

5.8 PROFINET-Managed-Switch

Der PROFINET-Managed-Switch besitzt die folgenden PROFINET-Eigenschaften:

Zyklische Funktionen (PROFINET RT):

- Minimales Intervall: 32 ms
- Erweiterter und Legacy Start-up
- Verbindungsaufbau unterstützt:
 - 1x IOC_AR, 1x DA_AR
 - 1x Input CR
 - 1x Output CR
 - 1x Alarm CR

Azyklische Funktionen:

- Verbundener Modus:
 - Diagnoseinformationen des IO-Devices lesen (Record).
 - Verschiedene Konfigurationsparameter schreiben.
 - Ausgabe von Alarmen an einen IO-Controller
- Nichtverbundener Modus:
 - Diagnoseinformationen des IO-Devices lesen (Record).

Allgemeine Funktionen:

- MRP-Client/-Manager, Single-Instanz (frei pro Port konfigurierbar)
- LLDP & LLDP MIB
- Einfacher Austausch von Geräten
- Netload II zertifiziert.

Die folgenden Funktionen werden nicht unterstützt:

- DHCP
- FSU
- Shared Input
- Shared Device
- IOS_AR
- IOS_AR TakeOver
- IRT, RT_CLASS_3 Data Exchange
- PROFIenergy
- Precision Transparent Clock Protocol (PTCP)

5.9 GSDML-Datei

5.9.1 Einleitung

Alle IO-Devices sind in ihren technischen und funktionellen Eigenschaften in einer herstellerspezifischen Datei beschrieben. Diese GSDML-Datei („**General Station Description Markup Language**“) ist XML-basiert. Sie enthält alle Daten, die für das Engineering und für den Datenaustausch des IO-Controllers benötigt werden. Dazu gehören unter anderem:

- Beschreibung der einzelnen IO-Devices (Ein- und Ausgabegeräte)
- Möglichkeiten des Einsatzes der E/A-Geräte zu den Slots
- Parameter, die zum korrekten Betreiben der IO-Devices erforderlich sind
- Diagnosen und deren Bedeutungen, die von einem IO-Device geliefert werden
- Beschreibung von mehreren Geräten einer Familie in einer Datei

Die GSD-Datei ist mehrsprachig ausgelegt.

Der Name einer GSD-Datei entspricht dem folgenden Schema:

GSDML-<version>-<Manufacturer>-<Devicename>-<Date>.xml

Beispiel der Bezeichnung einer GSD-Datei:

GSDML-V2.33-WAGO-852-20190213.xml

5.9.2 Aufbau einer GSDML-Datei

Der Inhalt der GSDML-Datei ist gemäß ISO 15745 aufgebaut.

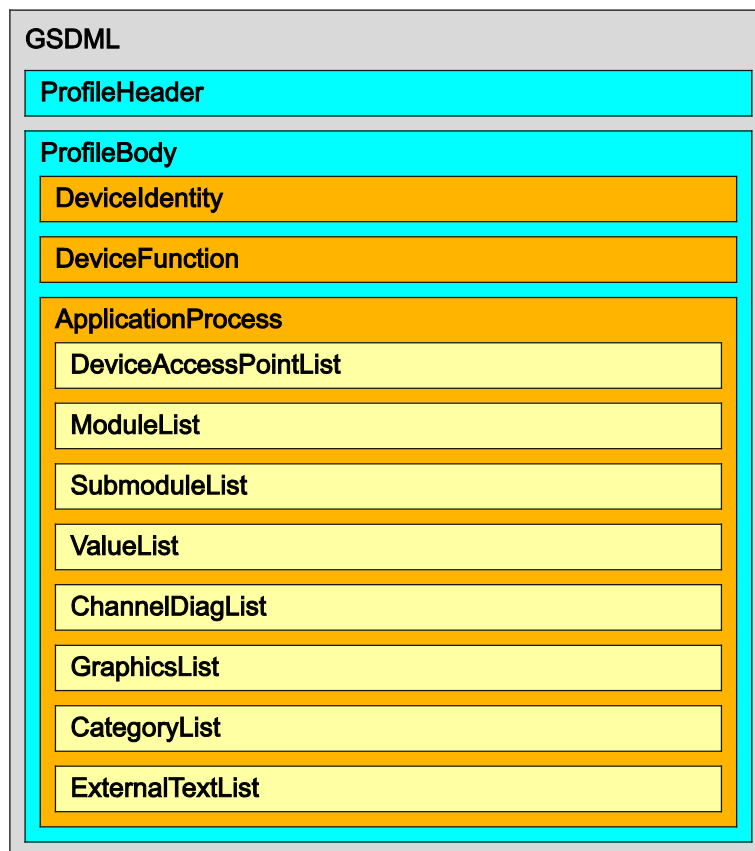


Abbildung 16: Allgemeiner Aufbau einer GSDML-Datei

ProfileHeader

Aufbau und Inhalt wird durch den Standard vorgegeben.
Enthalten sind folgende Angaben:

- ProfileIdentification
- ProfileRevision
- ProfileName
- ProfileSource
- ProfileClassID
- ISO15745Reference

ProfileBody

Enthält alle gerätespezifischen Daten des IO-Devices bzw. der Gerätefamilie.

Der Bereich ProfileBody gliedert sich in:

- DeviceIdentity
- DeviceFunction
- ApplicationProcess

DeviceIdentity

Enthält Informationen zur Identifikation des IO-Devices.

Besteht aus:

- der Vendor_ID
(Diese ID wird von der PNO vergeben und enthält die Firmenkennung. Sie ist für jeden Hersteller eindeutig.)
- der Device_ID
(Die Device_ID kann herstellerspezifisch definiert werden.)
- dem InfoText (Beschreibung der Gerätefamilie) und
- dem VendorNamen.

DeviceFunction

Informationen zur Funktion der Gerätefamilie

ApplicationProcess

Enthält die eigentlichen Daten zum IO-Device

Der Bereich gliedert sich in:

- DeviceAccessPointList
- ModuleList
- SubmoduleList
- ValueList
- ChannelDiagList
- GraphicsList
- CategoryList
- ExternalTextList

DeviceAccessPointList

Enthält die Beschreibungen aller innerhalb der Gerätefamilie verfügbaren Busanschlüssen (DAP = „**Device Access Point**“).

Dazu gehören u. a.:

- ModuleInfo (Name, Beschreibung, Artikelnummer, Versionsstand u. a.)
- CertificationInfo (Conformance, Application und NetLoad Class)
- SubslotList
- IOConfigData (Maximale Länge der übertragenen Daten)
- UseableModules (nur bei modular aufgebauten IO-Devices)
- VirtualSubmoduleList
- SystemDefinedSubmoduleList
- Graphics (Systemdarstellung des IO-Devices)

ModuleList

Enthält die Beschreibungen der einzelnen Module des IO-Devices.

SubmoduleList

Enthält die Beschreibungen der einzelnen Submodule eines IO-Devices.

ValueList

Enthält die Parameter, die für das IO-Device eingestellt werden können sowie die Zuordnung zwischen Wert und Bezeichnung.
Die Bezeichnung wird über die **TextID** in der **ExternalTextList** bestimmt.

ChannelDiagList

Enthält die Zuordnung eines Fehlers zu dem entsprechenden Text.
Der entsprechende Text wird über die ID in der **ExternalTextList** bestimmt.

GraphicsList

Enthält die Verweise auf die Grafiksymbole aller IO-Devices der Gerätefamilie.

CategoryList

Enthält die Zuordnung der Module zu einer bestimmten Kategorie.
Diese Zuordnung dient der Gliederung des Modulkatalogs für dieses IO-Device in der jeweiligen Engineering-Software.

ExternalTextList

Enthält sämtliche Texte, die über die entsprechende **TextID** in den anderen Bereichen der GSDML-Datei referenziert werden können.
Diese Liste kann sprachspezifisch aufgebaut werden.

5.9.3 Eindeutige Identifizierung von IO-Devices

Die eindeutige Identifikation von IO-Devices in einer GSDML-Datei wird durch die folgenden Kennungen bestimmt:

- Vendor_ID (Herstellerkennung; siehe **DeviceIdentity**)
- Device_ID (eindeutige Geräteerkennung; siehe **DeviceIdentity**)
- Modul-ID (eindeutige Kennung aller Module, die innerhalb eines bestimmten IO-Devices verwendet werden können; siehe **ModuleList**)
- Submodul-ID (eindeutige Kennung aller Submodule, die innerhalb eines bestimmten Moduls verwendet werden können; siehe **SubmoduleList**)

5.10 Projektieren über GSDML-Datei

In diesem Kapitel wird die allgemeine Vorgehensweise beschrieben, ohne auf herstellerspezifische Konfigurationstools einzugehen. Die Beschreibungen zu diesen Konfigurationstools finden Sie bei dem jeweiligen Hersteller.

Das Projektieren des PROFINET-Managed-Switches besteht im Wesentlichen aus folgenden Phasen:

- 1 Planen (Einbinden in die Topologie usw.)
- 2 Parametrieren/Konfigurieren über Projektierungstool
- 3 Netzwerkaufbau
- 4 Test
- 5 In Betrieb nehmen

5.10.1 Konfigurieren

Das eigentliche Konfigurieren des PROFINET-Managed-Switches mit Hilfe eines Projektierungstools kann beginnen, wenn die folgenden Voraussetzungen erfüllt sind:

- Die Auswahlphase der Geräte und der Netzwerktopologie ist abgeschlossen.
- Alle weiteren Fragen des allgemeinen Planens sind ebenfalls geklärt.

Hinweis



Dokumentation des Projektierungstools beachten!

Dieses Kapitel enthält allgemeine Hinweise zum Konfigurieren des PROFINET-Systems.

Zum Bedienen des eingesetzten Projektierungstools nutzen Sie bitte die Dokumentation des entsprechenden Herstellers.

Prinzipiell kann das Konfigurieren über 2 verschiedene Wege erfolgen:

- **Offline**
An das Projektierungstool ist zunächst kein reales PROFINET-System angeschlossen. Das Projekt wird mit den geplanten Geräten und der geplanten Topologie erstellt und konfiguriert. Anschließend wird das reale PROFINET-System an das Projektierungstool angeschlossen und das erstellte Projekt wird in den realen IO-Controller geladen.
- **Online**
An das Projektierungstool ist ein reales PROFINET-System angeschlossen. Das Projekt wird mit der realen Konfiguration erstellt und in den IO-Controller geladen.

Das generelle Vorgehen ist bei beiden Methoden vergleichbar. Im Weiteren wird das Vorgehen für eine Offlinekonfiguration beschrieben.

5.10.1.1 Projektierungstools (Übersicht)

Für das Planen, Projektieren und Konfigurieren eines PROFINET-Systems stehen verschiedene, herstellerspezifische Projektierungstools zur Auswahl.

Die folgende Tabelle enthält eine Auswahl von PROFINET-Projektierungstools verschiedener Hersteller. Die Auflistung erfolgt alphabetisch. Sie erhebt keinen Anspruch auf Vollständigkeit und stellt keine Wertung dar.

Tabelle 22: Übersicht Projektierungstools

Hersteller	Projektierungstool
3S	CODESYS
Beckhoff	TwinCAT
Hilscher	SYCON.net
Phoenix Contact	PCWorx
Siemens	STEP 7 (TIA Portal)

Das allgemeine Vorgehen zum Projektieren ist bei allen Projektierungstools weitestgehend identisch.

Das einzusetzende Projektierungstool sollte mindestens folgende Aufgaben erfüllen können:

- Verwalten von PROFINET-Geräten im Hardwarekatalog
- Vernetzen von Geräten in einer (grafischen) Netzwerkansicht und/oder in einer Hardwarekonfigurationsansicht
- Zuweisen von Namen und Adressen der Geräte
- Onlinebeobachtung und -steuerung von Variablen
- Onlinezugriff auf die Prozessdaten
- Diagnose der PROFINET-Geräte
- Diagnose der Netzwerkgeräte (z. B. der Switches)
- Darstellen des Projekts in einer hierarchischen Struktur (z. B. einer Baumstruktur)
- Überprüfen des Projekts auf Konsistenz, Fehlerfreiheit und Einhaltung des Mengengerüsts
- Unterstützen des Anwenders bei der Erstellung der Anlagendokumentation

In den folgenden Beschreibungen wird beispielhaft das Tool „TIA“ von Siemens verwendet.

Hinweis



Anwendungshinweis beachten!

Eine detaillierte Anleitung zum Konfigurieren des PROFINET-Managed-Switches mit dem Projektierungstool „TIA“ von Siemens finden Sie im Anwendungshinweis „TIA Portal – WAGO PROFINET Managed Switches“. Dieses Dokument können Sie im Internet unter www.wago.com herunterladen.

5.10.1.2 Allgemeines Vorgehen zum Projektieren eines PROFINET-Systems

Die nachfolgend aufgeführten Schritte können sich je nach eingesetztem Projektierungstool unterscheiden. Prinzipiell ist das beschriebene Vorgehen aber identisch.

1. Importieren Sie, falls erforderlich, die entsprechenden GSD-Dateien für die neuen PROFINET-Geräte.
Bei einem bestehenden Projekt ist ein erneuter Import der GSD-Datei meist nur dann erforderlich, wenn ein IO-Device durch I/O-Modultypen erweitert wird, die in dem entsprechenden IO-Device noch nicht enthalten sind.
2. Für ein neues PROFINET-System legen Sie im Projektierungstool ein neues Projekt an.
Für eine Erweiterung eines bestehenden PROFINET-Systems öffnen Sie ein vorhandenes Projekt.
3. Fügen Sie die neuen PROFINET-Geräte als Geräteinstanzen aus dem Hardwarekatalog in das geöffnete Projekt ein.
4. Ordnen Sie den neuen PROFINET-Geräten entsprechend der Planung die geplanten Gerätenamen bzw. IP-Adressen zu (falls erforderlich).
Ab der Conformance Class B muss jeder PROFINET-Netzwerkteilnehmer einen Gerätenamen und eine IP-Adresse erhalten.
Vergeben Sie möglichst „sprechende“ Gerätenamen, um eine schnellere Wiedererkennbarkeit zu erreichen (z. B. bei Diagnosemeldungen).
Je nach verwendetem Projektierungstool und eingesetzter Datenstruktur kann die Zuweisung von Gerätenamen und/oder IP-Adressen automatisch erfolgen.
5. Handelt es sich bei dem PROFINET-Gerät um ein modulares IO-Device (z. B. ein WAGO-I/O-SYSTEM), wählen Sie die zum Einsatz kommenden Module aus dem Hardwarekatalog aus und fügen Sie diese in das Projekt ein. Passen Sie den Aufbau der Eingangs- und Ausgangsdaten anhand der entsprechenden Submodule an.
Damit wird u. a. der Aufbau der Prozessabbilder für die Eingangs- und die Ausgangsdaten festgelegt.

Information



Größe der Prozessabbilder beachten!

Die Größe der Prozessabbilder ermittelt sich aus der Summe der Eingangs- bzw. Ausgangsdaten aller am PROFINET-Knoten konfigurierten Module bzw. Submodule. Durch die gezielte Auswahl geeigneter Submodultypen für die digitalen Module haben Sie geräteabhängig die Möglichkeit, den Aufbau der Prozessabbilder für die Eingangs- und Ausgangsdaten optimiert zu konfigurieren.

Der Inhalt der Prozessabbilder wird während des Echtzeitdatenverkehrs mit dem IO-Controller ausgetauscht.

6. Vernetzen Sie die neuen PROFINET-Geräte entsprechend der geplanten Topologie.
Die Darstellung der Topologie hängt vom verwendeten Projektierungstool ab und kann von der realen Topologie abweichen.
7. Passen Sie bei Bedarf die stationsübergreifenden Einstellungen am entsprechenden Submodul des IO-Devices an.
8. Passen Sie bei den IO-Devices bei Bedarf die Parametrierungen für die projektierten Module bzw. Submodule an.
9. Wählen Sie die Kommunikationsklasse (NRT oder RT) am entsprechenden Submodul des IO-Devices aus.
10. Überprüfen Sie die Aktualisierungszeit bzw. den Sendezyklus und die Verbindungsüberwachung der Verbindung zum IO-Controller und passen Sie bei Bedarf diese Einstellungen an.
11. Wenn Sie die Station in einem medienredundanten Netzwerk (Ringtopologie) einsetzen wollen, weisen Sie dem IO-Device die Rolle des MRP-Clients zu und passen Sie bei Bedarf den Namen der MRP-Domäne an.
12. Überprüfen Sie die Verbindungseinstellungen an den Submodulen der IO-Device-Ports und passen Sie diese bei Bedarf an.
13. Führen Sie eine Prüfung des projektierten PROFINET-Systems durch und speichern Sie es anschließend.
Das Projektierungstool prüft z. B. auf logische Korrektheit des projektierten Systems sowie auf Einhaltung des vorgegebenen Mengengerüsts.
14. Dokumentieren Sie das projektierte PROFINET-System.
Je nach eingesetztem Projektierungstool kann dieses Dokumentieren automatisch erfolgen.
15. Falls erforderlich, erstellen Sie die entsprechenden Anwenderprogramme bzw. passen Sie diese an und testen Sie die Änderungen.
Der Umfang dieses Schrittes hängt im Wesentlichen davon ab, ob ein komplett neues PROFINET-System erstellt oder ein bestehendes erweitert wird.
16. Falls erforderlich, passen Sie die Benutzerverwaltung an:
 - Erstellen neuer Benutzerrollen
 - Anlegen von Benutzern
 - Vergabe der entsprechenden Rechte

Hinweis**Nicht verwendete Ports deaktivieren!**

Gemäß der Richtlinie „PROFINET Security“ der PNO müssen nicht verwendete Ports deaktiviert werden.

Damit ist die Offlinekonfiguration zunächst beendet.

5.10.1.3 Laden des Projektes in den IO-Controller

Um das Projekt in den IO-Controller laden zu können, müssen Sie Ihre geplante PROFINET-Systemkonfiguration realisieren und die Topologie aufbauen.

Anschließend können Sie die Projektierungsphase wie folgt abschließen:

1. Erstellen Sie bei Bedarf mit den Bordmitteln des Projektierungstools die SOLL-Konfiguration des PROFINET-Netzwerks.
Die SOLL-Konfiguration ist für die Einbindung des IO-Devices in eine IRT-Domäne zwingend erforderlich.
Ebenfalls vorausgesetzt wird die Bekanntgabe der SOLL-Konfiguration, wenn Sie den Gerätetausch ohne anschließende, toolbasierte „Stationstaufe“ durchführen wollen.
Bei Übereinstimmung von SOLL- und IST-Konfiguration können Sie bei Bedarf bei der Erstinbetriebnahme auf eine toolbasierte Stationstaufe verzichten.
2. Schalten Sie im Anschluss die Versorgungsspannung für den Feldbuskoppler ein.
3. Alternativ zur topologiebasierten Stationstaufe können Sie den Gerätenamen über ein DCP-Tool zuweisen.
Falls vorhanden, können Sie den Gerätenamen auch wahlweise über DIP-Schalter definieren.
4. Laden Sie die Systemdaten auf den IO-Controller.

Nachdem die Systemdaten erfolgreich geladen wurden, kann der Datenaustausch zwischen IO-Controller und IO-Device erfolgen.

5.10.2 Parameter

Die Parameter des PROFINET-Managed-Switches können über das eingesetzte Projektierungstool eingestellt werden.

Nach den Abbildungen werden die einzelnen Parameter erklärt und der Bezug zur GSDML-Datei aufgezeigt.

In den folgenden Beschreibungen wird beispielhaft das Tool „TIA“ von Siemens verwendet.

Hinweis



Anwendungshinweis beachten!

Eine detaillierte Anleitung zum Konfigurieren des PROFINET-Managed-Switches mit dem Projektierungstool „TIA“ von Siemens finden Sie im Anwendungshinweis „TIA Portal – WAGO PROFINET Managed Switches“. Dieses Dokument können Sie im Internet unter www.wago.com herunterladen.

5.10.2.1 Bereich „Allgemein“

The screenshot shows the 'Allgemein' (General) configuration window in the TIA Portal. The left sidebar contains a tree view with the following structure:

- Allgemein
 - Kataloginformation
 - PROFINET-Schnittstelle [X1]
 - Allgemein
 - Ethernet-Adressen
 - Erweiterte Optionen
 - Schnittstellen-Optionen
 - Medienredundanz
 - Echtzeit-Einstellungen
 - Port 1 - 100/1000 Base-TX Vollduplex [X1 P1 R]
 - Allgemein
 - Portverschaltung
 - Port-Optionen
 - Port 2 - 100/1000 Base-TX Vollduplex [X1 P2 R]
 - Port 3 - 100/1000 Base-TX Vollduplex [X1 P3 R]
 - Port 4 - 100/1000 Base-TX Vollduplex [X1 P4 R]
 - Port 5 - 100/1000 Base-TX Vollduplex [X1 P5 R]
 - Port 6 - 100/1000 Base-TX Vollduplex [X1 P6 R]
 - Port 7 - 100/1000 Base-TX Vollduplex [X1 P7 R]
 - Port 8 - 100/1000 Base-TX Vollduplex [X1 P8 R]
 - Port 9 - 1000 Basis-X Vollduplex [X1 P9 R]
 - Port 10 - 1000 Basis-X Vollduplex [X1 P10 R]
 - Port 11 - 1000 Basis-X Vollduplex [X1 P11 R]
 - Port 12 - 1000 Basis-X Vollduplex [X1 P12 R]
 - Identifikation & Maintenance
 - Prozessalarme
 - Baugruppenparameter
 - Statusdiagnose
 - Konfiguration der Portspiegelung
 - Baugruppenausfall
 - E/A-Adressen

The main configuration area on the right is divided into two sections:

- Allgemein**
 - Name: wago-
 - Autor:
 - Kommentar:
 - Baugruppenträger: 0
 - Steckplatz: 0
- Kataloginformation**
 - Kurzbezeichnung: 852-V1.2.0
 - Beschreibung:
 - Artikel-Nr.: 852-
 - Firmware-Version: V1.2.0
 - Hardware-Erzeugnisstand: 1
 - GSD-Datei: gsdml-v2.33-wago-852-20190213.xml
 - Ausgabestand ändern

Abbildung 17: PROFINET-Parameter – Bereich „Allgemein“

Tabelle 23: PROFINET-Parameter für Bereich „Allgemein“

Parameter	Beschreibung	Tag in der GSDML
Name	Name des DAP	DeviceAccessPointItem [DNS_CompatibleName]
Autor	Bearbeiter des Gerätes im Projektierungstool	–
Kommentar	Kommentarfeld	–
Baugruppenträger	Genauere Beschreibung des Einbauorts	–
Steckplatz	Genauere Beschreibung des Einbauorts	–
Kurzbezeichnung	Name des Moduls	ModuleInfo/Name
Beschreibung	Beschreibung des Moduls	ModuleInfo/InfoText
Artikel-Nr.	Artikelnummer des Moduls	ModuleInfo/OrderNumber
Firmware-Version	Version der Firmware	ModuleInfo/SoftwareRelease
Hardware-Erzeugnisstand	Version der Hardware	ModuleInfo/HardwareRelease
GSD-Datei	Name der GSDML-Datei	–

5.10.2.2 Bereich „PROFINET-Schnittstelle [X1]“

The screenshot displays the configuration interface for the PROFINET-Schnittstelle [X1]. The left-hand navigation pane shows a tree structure with the following items: Allgemein, Kataloginformation, PROFINET-Schnittstelle [X1] (selected), Ethernet-Adressen, Erweiterte Optionen, Schnittstellen-Optionen, Medienredundanz, Echtzeit-Einstellungen, IO-Zyklus, Port 1 - 100/1000 Base-TX Vollduplex [X1 P1 R], Port 2 - 100/1000 Base-TX Vollduplex [X1 P2 R], Port 3 - 100/1000 Base-TX Vollduplex [X1 P3 R], Port 4 - 100/1000 Base-TX Vollduplex [X1 P4 R], Port 5 - 100/1000 Base-TX Vollduplex [X1 P5 R], Port 6 - 100/1000 Base-TX Vollduplex [X1 P6 R], Port 7 - 100/1000 Base-TX Vollduplex [X1 P7 R], Port 8 - 100/1000 Base-TX Vollduplex [X1 P8 R], Port 9 - 1000 Basis-X Vollduplex [X1 P9 R], Port 10 - 1000 Basis-X Vollduplex [X1 P10 R], Port 11 - 1000 Basis-X Vollduplex [X1 P11 R], Port 12 - 1000 Basis-X Vollduplex [X1 P12 R], Identification & Maintenance, Prozessalarmer, Baugruppenparameter, Statusdiagnose, Konfiguration der Portspiegelung, Baugruppenausfall, and E/A-Adressen.

The main configuration area is titled 'PROFINET-Schnittstelle [X1]' and contains the following sections:

- Allgemein:** Fields for 'Name' (Schnittstelle) and 'Kommentar'.
- Ethernet-Adressen:** A section titled 'Schnittstelle vernetzt mit' with a 'Subnetz' field set to 'PN/IE_1' and a button 'Neues Subnetz hinzufügen'.
- IP-Protokoll:** Fields for 'IP-Adresse' (192.168.1.4), 'Subnetzmaske' (255.255.255.0), and 'Router-Adresse' (0.0.0.0). Checkboxes for 'Router-Einstellungen mit IO-Controller synchronisieren' (checked) and 'Router verwenden' (unchecked).
- PROFINET:** A checkbox 'PROFINET-Gerätenamen automatisch generieren' (checked). Fields for 'PROFINET-Gerätename' (wago-), 'Konvertierter Name' (wago-), and 'Gerätenummer' (3).

Abbildung 18: PROFINET-Parameter – Bereich „PROFINET-Schnittstelle [X1]“

Tabelle 24: PROFINET-Parameter für Bereich „PROFINET-Schnittstelle [X1]“

Parameter	Beschreibung	Tag in der GSDML
Name	Bezeichnung der Schnittstelle	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem
Kommentar	Kommentarfeld	–
Subnetz	Bezeichnung des Subnetzes	–
IP-Adresse	IP-Adresse (Default: 0.0.0.0)	–
Subnetzmaske	Subnetzmaske	–
PROFINET-Gerätename	Gerätename; kann automatisch aus der GSDML-Datei übernommen werden.	DeviceAccessPointItem [DNS_CompatibleName]
Konvertierter Name	Gerätename; wird automatisch aus der GSDML-Datei übernommen.	DeviceAccessPointItem [DNS_CompatibleName]
Gerätenummer	Gerätenummer im Netzwerk	–

5.10.2.3 Bereich „Erweiterte Optionen“

The screenshot displays the configuration interface for a PROFINET interface. The left sidebar shows a tree view with the following structure:

- Allgemein
 - Kataloginformation
 - PROFINET-Schnittstelle [X1]
 - Allgemein
 - Ethernet-Adressen
 - Erweiterte Optionen** (selected)
 - Schnittstellen-Optionen
 - Medienredundanz
 - Echtzeit-Einstellungen
 - IO-Zyklus
 - Port 1 - 100/1000 Base-TX Vollduplex [X1 P1 R]
 - Allgemein
 - Portverschaltung
 - Port-Optionen
 - Port 2 - 100/1000 Base-TX Vollduplex [X1 P2 R]
 - Port 3 - 100/1000 Base-TX Vollduplex [X1 P3 R]
 - Port 4 - 100/1000 Base-TX Vollduplex [X1 P4 R]
 - Port 5 - 100/1000 Base-TX Vollduplex [X1 P5 R]
 - Port 6 - 100/1000 Base-TX Vollduplex [X1 P6 R]
 - Port 7 - 100/1000 Base-TX Vollduplex [X1 P7 R]
 - Port 8 - 100/1000 Base-TX Vollduplex [X1 P8 R]
 - Port 9 - 1000 Basis-X Vollduplex [X1 P9 R]
 - Port 10 - 1000 Basis-X Vollduplex [X1 P10 R]
 - Port 11 - 1000 Basis-X Vollduplex [X1 P11 R]
 - Port 12 - 1000 Basis-X Vollduplex [X1 P12 R]
 - Identification & Maintenance
 - Prozessalarmer
 - Baugruppenparameter
 - Statusdiagnose
 - Konfiguration der Portspiegelung
 - Baugruppenausfall
 - E/A-Adressen

The main configuration area shows the following settings:

- Erweiterte Optionen**
 - Schnittstellen-Optionen**
 - ☐ Priorisierter Hochlauf
 - ☐ IEC V2.2 LLDP Modus verwenden
 - Medienredundanz**
 - MRP-Domain: mrpdomain-1
 - Medienredundanzrolle: Nicht Teilnehmer des Rings
 - Ringport 1: Schnittstelle [X1] | Port 1 - 100/1000 Base-TX Vol
 - Ringport 2: Schnittstelle [X1] | Port 2 - 100/1000 Base-TX Vol
 - ☐ Diagnosealarme
 - Domain-Einstellungen
 - Echtzeit-Einstellungen**
 - IO-Zyklus**
- Aktualisierungszeit**
 - ☒ Aktualisierungszeit automatisch berechnen
 - ☐ Aktualisierungszeit manuell einstellen
 - Aktualisierungszeit: 32.000
 - ☐ Aktualisierungszeit bei Änderung des Sende
- Ansprechüberwachungszeit**
 - Akzeptierte Aktualisierungszyklen ohne IO-Daten: 3
 - Ansprechüberwachungszeit: 96.000

Abbildung 19: PROFINET-Parameter – Bereich „Erweiterte Optionen“

Tabelle 25: PROFINET-Parameter für Bereich „Erweiterte Optionen“

Parameter	Beschreibung	Tag in der GSDML
MRP-Domain	Name des MRP	–
Medienredundanzrolle	Client (MRC) oder Manager (MRM) im Ring	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ MediaRedundancy
Ringport 1	Angabe des 1. Ports, der dem MRP-Ring zugeordnet ist	–
Ringport 2	Angabe des 2. Ports, der dem MRP-Ring zugeordnet ist	–
Aktualisierungszeit	Zykluszeit für I/O-Daten	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ ApplicationRelations
Akzeptierte Aktualisierungszyklen ...	Faktor der Aktualisierungszeit, nach dem ein Fehler generiert wird.	–
Ansprechüberwachungszeit	Produkt aus Aktualisierungszeit und Faktor	–

5.10.2.4 Bereich „Port 1“

Die folgenden Beschreibungen sind beispielhaft für Port 1 dargestellt. Sie gelten entsprechend auch für die Ports 2 bis 12.

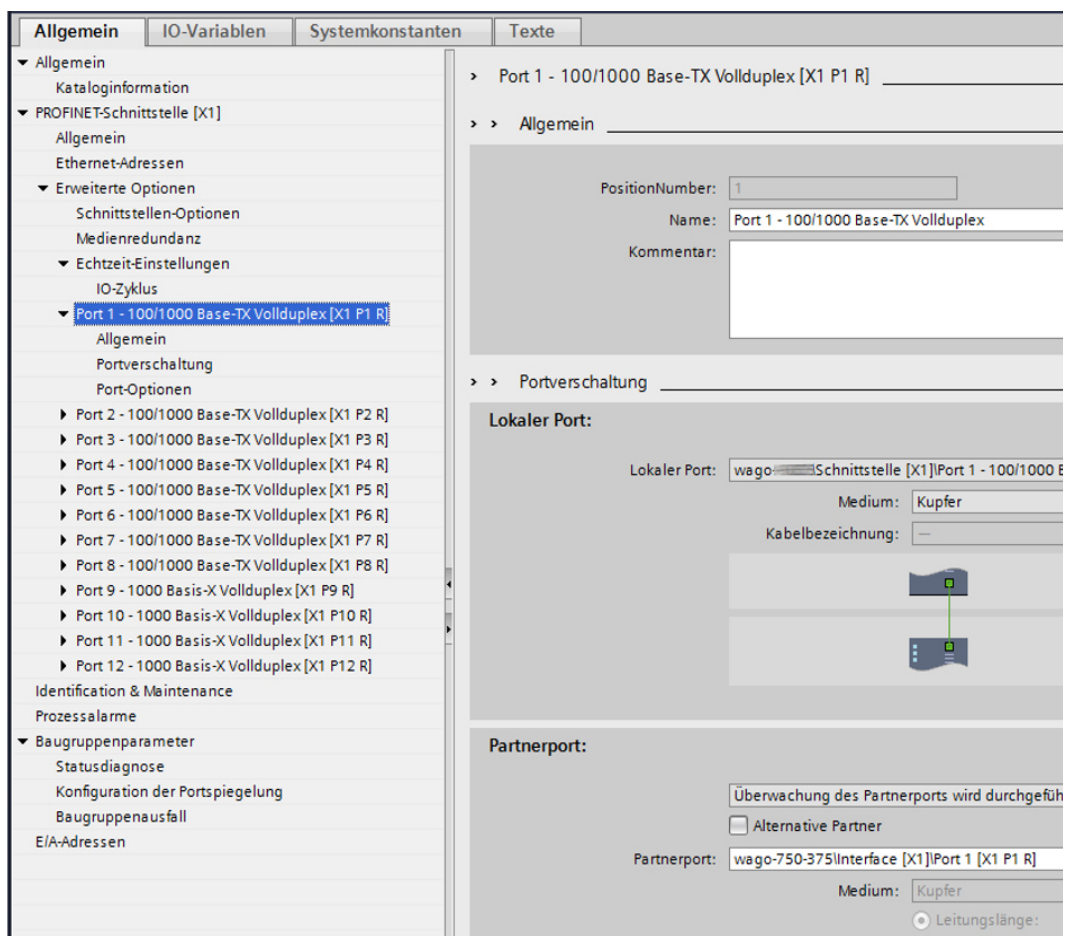


Abbildung 20: PROFINET-Parameter – Bereich „Port 1“

Tabelle 26: PROFINET-Parameter für Bereich „Port 1“

Parameter	Beschreibung	Tag in der GSDML
Name	Bezeichnung des Ports	SystemDefinedSubmoduleList/ PortSubmoduleItem
Kommentar	Kommentarfeld	–
Lokaler Port	Ortsangabe des lokalen Ports	–
Medium	Übertragungsmedium	–
Partnerport	Angeschlossener Port	–

5.10.2.5 Bereich „Port-Optionen“

Die folgenden Beschreibungen sind beispielhaft für Port 1 dargestellt. Sie gelten entsprechend auch für die Ports 2 bis 12.

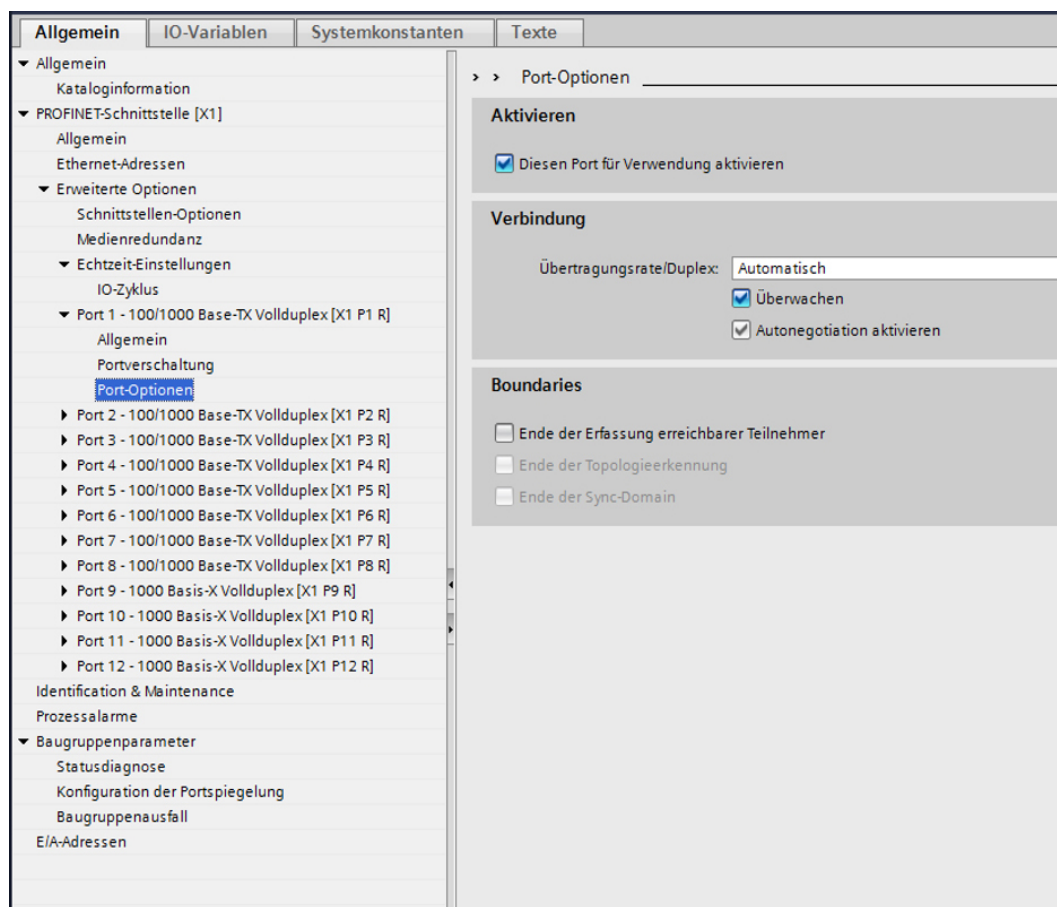


Abbildung 21: PROFINET-Parameter – Bereich „Allgemein“

Tabelle 27: PROFINET-Parameter für Bereich „Erweiterte Optionen“

Parameter	Beschreibung	Tag in der GSDML
Aktivieren	Port aktivieren/deaktivieren.	–
Übertragungsrate/Duplex	Einstellung von Übertragungsrate und Duplex-Modus	ValueList/ ValueItem[ID="ID_RV_PORT_RATE"]
Überwachen	Überwachen aktivieren/deaktivieren.	–
Autonegotiation aktivieren	Autonegotiation aktivieren/deaktivieren.	–

5.10.2.6 Bereich „Identification & Maintenance“

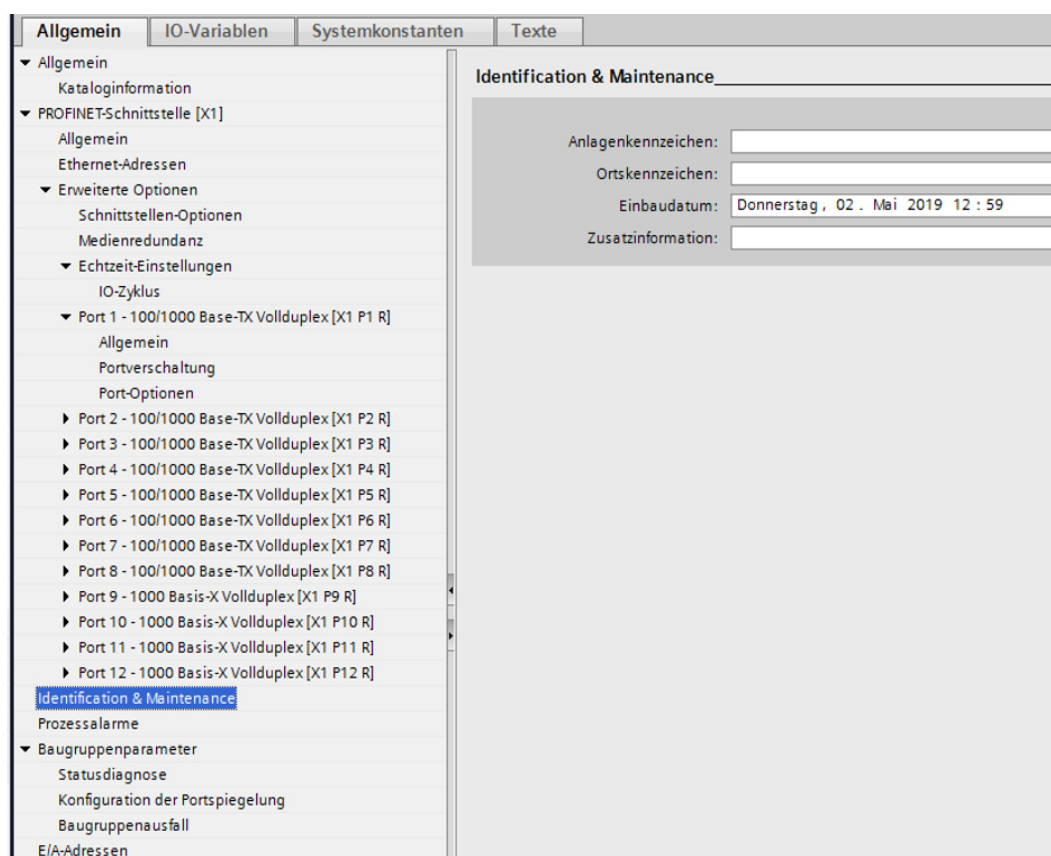


Abbildung 22: PROFINET-Parameter – Bereich „Identification & Maintenance“

Tabelle 28: PROFINET-Parameter für Bereich „Identification & Maintenance“

Parameter	Beschreibung	Tag in der GSDML
Anlagenkennzeichen	Kennzeichnung der Anlage	–
Ortskennzeichen	Kennzeichen des Einbauorts	–
Einbaudatum	Datum für den Einbau	–
Zusatzinformation	Kommentarfeld	–

5.10.2.7 Bereich „Prozessalarme“

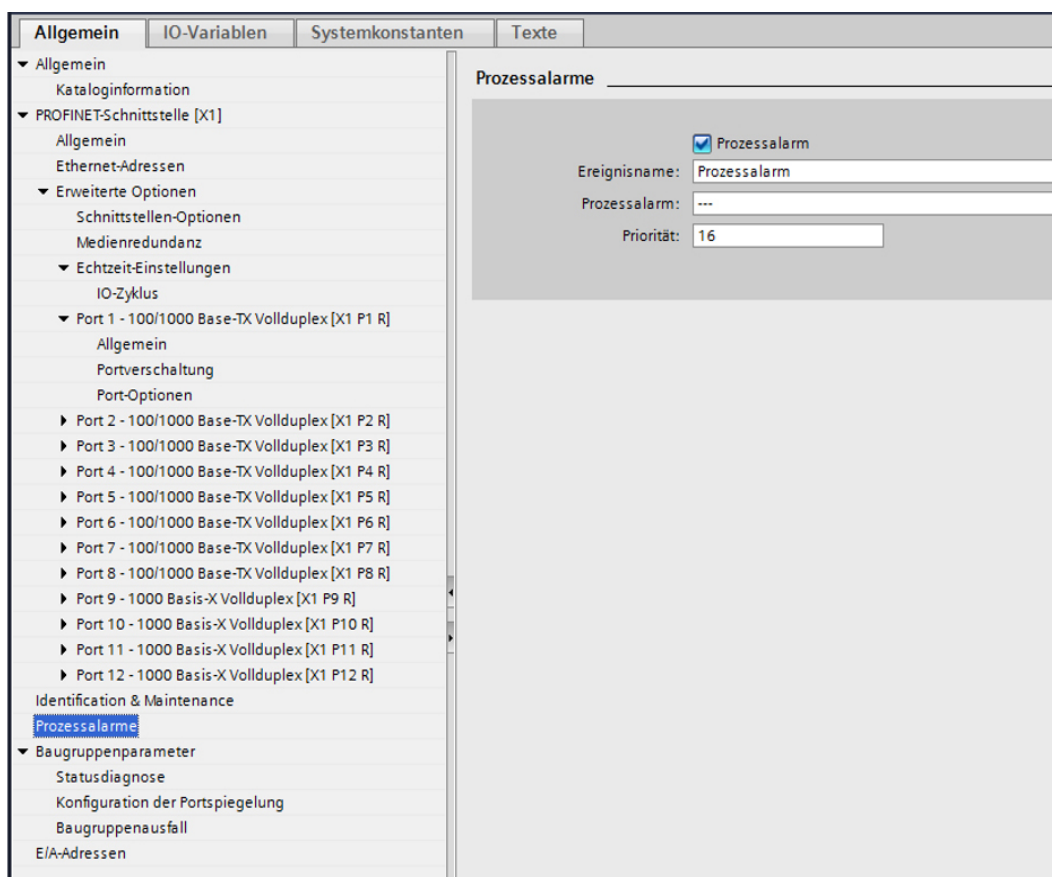


Abbildung 23: PROFINET-Parameter – Bereich „Prozessalarme“

Tabelle 29: PROFINET-Parameter für Bereich „Prozessalarme“

Parameter	Beschreibung	Tag in der GSDML
Ereignisname	Name des Alarms	–
Prozessalarm	Prozessalarmüberwachung aktivieren/deaktivieren.	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem
Priorität	Priorität für die Datenübermittlung	–

5.10.2.8 Bereich „Baugruppenparameter“

Allgemein	IO-Variablen	Systemkonstanten	Texte
▼ Allgemein - Kataloginformation ▼ PROFINET-Schnittstelle [X1] - Allgemein - Ethernet-Adressen ▼ Erweiterte Optionen - Schnittstellen-Optionen - Medienredundanz ▼ Echtzeit-Einstellungen - IO-Zyklus ▼ Port 1 - 100/1000 Base-TX Vollduplex [X1 P1 R] - Allgemein - Portverschaltung - Port-Optionen ▶ Port 2 - 100/1000 Base-TX Vollduplex [X1 P2 R] ▶ Port 3 - 100/1000 Base-TX Vollduplex [X1 P3 R] ▶ Port 4 - 100/1000 Base-TX Vollduplex [X1 P4 R] ▶ Port 5 - 100/1000 Base-TX Vollduplex [X1 P5 R] ▶ Port 6 - 100/1000 Base-TX Vollduplex [X1 P6 R] ▶ Port 7 - 100/1000 Base-TX Vollduplex [X1 P7 R] ▶ Port 8 - 100/1000 Base-TX Vollduplex [X1 P8 R] ▶ Port 9 - 1000 Basis-X Vollduplex [X1 P9 R] ▶ Port 10 - 1000 Basis-X Vollduplex [X1 P10 R] ▶ Port 11 - 1000 Basis-X Vollduplex [X1 P11 R] ▶ Port 12 - 1000 Basis-X Vollduplex [X1 P12 R] - Identification & Maintenance - Prozessalarmer ▼ Baugruppenparameter - Statusdiagnose - Konfiguration der Portspiegelung - Baugruppenausfall - E/A-Adressen	Baugruppenparameter Statusdiagnose PWR-Diagnose: aktiviert RPS-Diagnose: deaktiviert Überhitzungsdiagnose: deaktiviert Konfiguration der Portspiegelung Portspiegelung: deaktiviert Spiegel zu Port: 1 Eingang von Port 1: deaktiviert Eingang von Port 2: deaktiviert Eingang von Port 3: deaktiviert Eingang von Port 4: deaktiviert Eingang von Port 5: deaktiviert Eingang von Port 6: deaktiviert Eingang von Port 7: deaktiviert Eingang von Port 8: deaktiviert Eingang von Port 9: deaktiviert Eingang von Port 10: deaktiviert Eingang von Port 11: deaktiviert Eingang von Port 12: deaktiviert Ausgang von Port 1: deaktiviert Ausgang von Port 2: deaktiviert Ausgang von Port 3: deaktiviert Ausgang von Port 4: deaktiviert Ausgang von Port 5: deaktiviert Ausgang von Port 6: deaktiviert Ausgang von Port 7: deaktiviert Ausgang von Port 8: deaktiviert Ausgang von Port 9: deaktiviert Ausgang von Port 10: deaktiviert Ausgang von Port 11: deaktiviert Ausgang von Port 12: deaktiviert Baugruppenausfall Bei der Einstellung "Letzten Wert halten" dürfen Eingangswerte bei Baugruppenausfall: Eingangswert 0		

Abbildung 24: PROFINET-Parameter – Bereich „Baugruppenparameter“

Tabelle 30: PROFINET-Parameter für Bereich „Baugruppenparameter“

Parameter	Beschreibung	Tag in der GSDML
PWR-Diagnose	Diagnose „Primäre Spannungsversorgung“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “2”]
RPS-Diagnose	Diagnose „Sekundäre Spannungsversorgung“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “3”]
Überhitzungsdiagnose	Diagnose „Überhitzung“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “5”]
Portspiegelung	Portspiegelung aktiviert/deaktiviert	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Spiegel zu Port	Angabe, zu welchem Port gespiegelt werden soll.	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Eingang von Port (x)	Portspiegelung „Eingang“ für Port (x) aktiviert/deaktiviert	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Ausgang von Port (x)	Portspiegelung „Ausgang“ für Port (x) aktiviert/deaktiviert	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Eingangswerte bei Baugruppenausfall	Angabe, welcher Wert bei Ausfall der Baugruppe verwendet wird.	–

5.10.2.9 Bereich „E/A-Adressen“

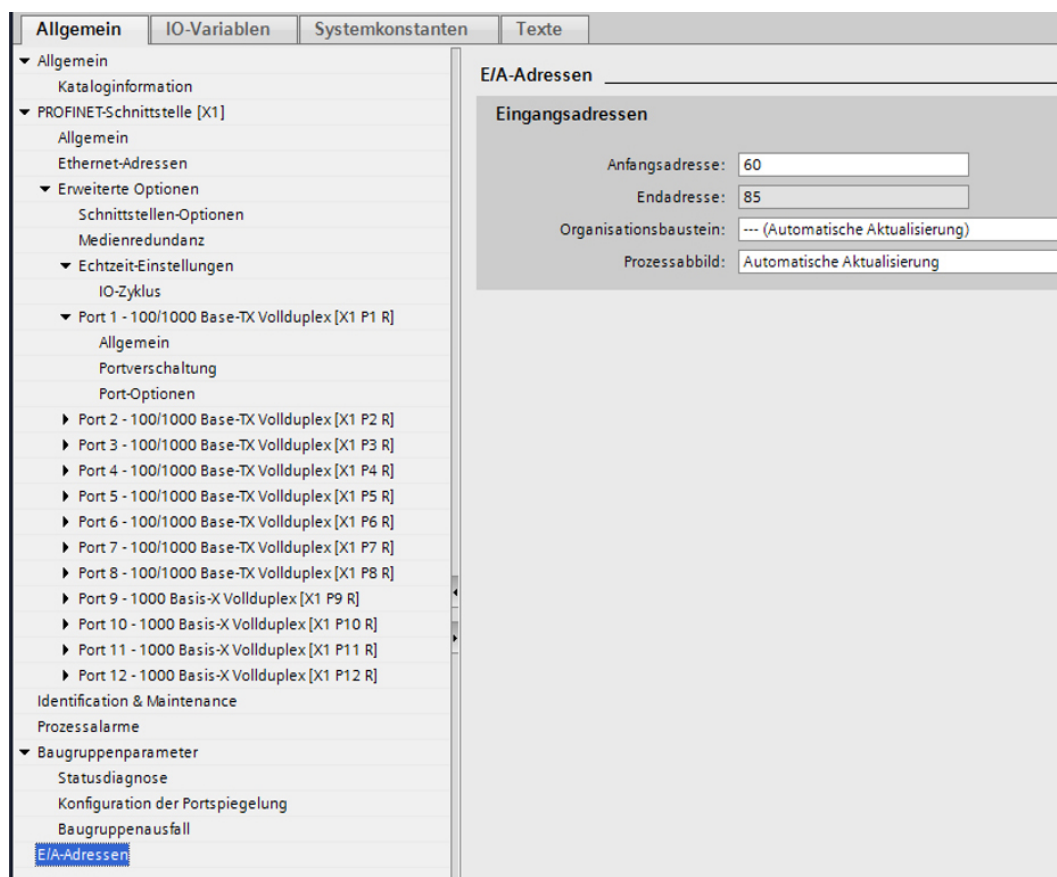


Abbildung 25: PROFINET-Parameter – Bereich „E/A-Adressen“

Tabelle 31: PROFINET-Parameter für Bereich „E/A-Adressen“

Parameter	Beschreibung	Tag in der GSDML
Anfangsadresse	Startadresse des zyklischen Adressabbildes	–
Endadresse	Wird automatisch generiert	–
Organisationsbaustein	Aktualisierung des Organisationsbausteins	–
Prozessabbild	Aktualisierung des Prozessabbildes der I/O-Daten	–

5.11 Zyklische I/O-Daten

Zyklische I/O-Daten werden immer zur angegebenen Periodendauer zwischen SPS und Switches gesendet. Diese Daten werden nahezu in Echtzeit übertragen. Beispielsweise sind Statusinformationen der Switches und Variablen, die in den Switch geschrieben werden sollen, typischerweise Teil der zyklischen Daten.

Zyklische I/O-Daten sind an die Submodule gebunden.

Der Subslot 0 wird standardmäßig nicht für I/O-Submodule verwendet.

PROFINET unterscheidet zwischen 3 Typen von Submodulen:

- Virtuelle Submodule,
- Interface-Submodule und
- Port-Submodule.

Alle diese Submodule können mit I/O-Daten verknüpft werden.

Das virtuelle Submodul ist immer im Subslot 1 enthalten.

Der PROFINET-Managed-Switch definiert alle zyklischen I/O-Daten nur im virtuellen Submodul. Dieses virtuelle Submodul ist dem Slot 0/SubSlot 1 zugeordnet.

Die zyklischen I/O-Daten umfassen 26 Bytes. Die ersten 2 Bytes der Daten zeigen die Diagnoseinformationen des Geräts an. Die folgenden 24 Bytes bezeichnen die Port-Statusinformationen (2 Bytes Daten pro Port-Information).

Die zyklischen I/O-Daten werden nur generiert, wenn sie über das jeweilige Projektierungstool entsprechend konfiguriert wurden.

Das Format für die zyklischen I/O-Daten wird in der folgenden Übersicht dargestellt.

Tabelle 32: Format für zyklische I/O-Daten – PROFINET

Byte Offset	Umfang	Beschreibung
0	16 Bit	Diagnosestatus des PROFINET-Managed-Switches
2	16 Bit	Status PORT 1
4	16 Bit	Status PORT 2
6	16 Bit	Status PORT 3
8	16 Bit	Status PORT 4
10	16 Bit	Status PORT 5
12	16 Bit	Status PORT 6
14	16 Bit	Status PORT 7
16	16 Bit	Status PORT 8
18	16 Bit	Status PORT 9
20	16 Bit	Status PORT 10
22	16 Bit	Status PORT 11
24	16 Bit	Status PORT 12

5.11.1 Beispiel für zyklische I/O-Daten

Das folgende Beispiel basiert auf dem Projektierungstool „TIA“ von Siemens.

Für die zyklischen IO-Daten, die mit Slot 0/SubSlot 1 adressiert sind, generiert das TIA-Portal automatisch eine Mapping-Adresse, nachdem sie per Drag & Drop aus dem Hardwarekatalog in die Netzwerkansicht gezogen wurden.

Der Benutzer kann die Abbildungsadresse verwenden, um über die SPS-Tags auf jedes Bit von Daten zuzugreifen.

Die Daten werden im Format WORD (16 Bit) dargestellt.

In der folgenden Übersicht finden Sie die detaillierte Struktur der Daten:

Tabelle 33: Zyklischer Eingang für die Gerätediagnose

TAG	Bit	Beschreibung	Wert	Bemerkung
DIAG.%X0	0	pn_diagcode_board_temp	0 = NO 1 = YES	Überhitzung Mainboard
DIAG.%X1	1	pn_diagcode_cpu_temp	0 = NO 1 = YES	Überhitzung CPU
DIAG.%X2	2	pn_diagcode_phy_temp	0 = NO 1 = YES	Überhitzung PHY
DIAG.%X3	3	pn_diagcode_pwr_ovolt	0 = NO 1 = YES	Überspannung primäre Spannungsversorgung
DIAG.%X4	4	pn_diagcode_rps_ovolt	0 = NO 1 = YES	Überspannung sekundäre Spannungsversorgung

Tabelle 33: Zyklischer Eingang für die Gerätediagnose

TAG	Bit	Beschreibung	Wert	Bemerkung
DIAG.%X5	5	pn_diagcode_pwr_uvolt	0 = NO 1 = YES	Unterspannung primäre Spannungs- versorgung
DIAG.%X6	6	pn_diagcode_rps_uvolt	0 = NO 1 = YES	Unterspannung sekundäre Spannungs- versorgung
DIAG.%X7	7	pn_diagcode_pwr_nopwr	0 = NO 1 = YES	Primäre Spannungs- versorgung nicht vorhanden.
DIAG.%X8	8	pn_diagcode_rps_nopwr	0 = NO 1 = YES	Sekundäre Spannungs- versorgung nicht vorhanden.
DIAG.%X9	9	MRP Ring State	0 = Inaktiv 1 = Aktiv	
DIAG.%X10	10	MRP Ring Running Status	0 = Zu 1 = Offen	Hinweis: Nur sinnvoll bei DIAG.%X9 = 1
DIAG.%X11 ... DIAG.%X14	11 ... 14	Reserviert		
DIAG.%X15	15	Device Status	0 = OK 1 = Fehler	PROFINET-Stack erzeugt keinen Alarm bei: DIAG.%X15 = 0

Tabelle 34: Zyklischer Eingang für Status Port Pn (n = 1 ... 12)

TAG	Bit	Beschreibung	Wert	Bemerkung
Pn.%X0	0	Port Power Status	0 = Aus 1 = An	
Pn.%X1	1	Port Duplex Mode	0 = Full Duplex 1 = Half Duplex	
Pn.%X2	2	Port Link Status	0 = Link Aus 1 = Link An	
Pn.%X3	3	Port Speed	0b000 = 10M 0b001 = 100M 0b010 = 1000M 0b111 = Auto	Dieses Bit wird mit Pn.%X4 und Pn.%X5 kombiniert.
Pn.%X4	4			
Pn.%X5	5			
Pn.%X6	6	Port Current Link Activity	1 = Disable 2 = Block 3 = Listen 4 = Learn 5 = Forward	Dieses Bit wird mit Pn.%X7 und Pn.%X8 kombiniert.
Pn.%X7	7			
Pn.%X8	8			
Pn.%X9	9	Port LLDP Admin Status	0 = Disabled 1 = Txonly 2 = Rxonly 3 = TxRx	Dieses Bit wird mit Pn.%X10 kombiniert.
Pn.%X10	10			
Pn.%X11	11	Reserviert		
...	...			
Pn.%X15	15			

5.12 DAP-Parameter

DAP-Parameter werden für die Konfiguration des IO-Devices verwendet. Nach dem Hochfahren des IO-Devices werden diese Parameter übertragen:

- Der IO-Controller liest diese Parameter vom IO-Device, um die Funktionen des IO-Devices zu erhalten.
- Der IO-Controller schreibt diese Parameter auf das IO-Device, um die Funktionen des IO-Devices zu konfigurieren.

Für den PROFINET-Managed-Switch werden die folgenden DAP-Parameter zur Verfügung gestellt:

Tabelle 35: DAP-Parameter für WAGO PROFINET-Switch

Index	SubSlot	Zugriff	Länge	Beschreibung
1	0x1	R/W	3	Diagnosemeldungen aktivieren/deaktivieren.
2	0x8001 ... 0x800C	R	6	Lesen des Port-Status (pro Port)
3	0x1	R	12	Lesen der Gerätediagnosen
4	0x1	R/W	10	Konfigurieren der Funktion Port-Spiegelung

Nachfolgend finden Sie die detaillierte Datenstruktur der einzelnen Parameterindizes.

INDEX=1

Tabelle 36: Diagnosemeldungen aktivieren/deaktivieren

Offset	Wert	Beschreibung	Default-Wert
0	0	Alarm „PWR Diagnose“ aktivieren.	0
	1	Alarm „PWR Diagnose“ deaktivieren.	
1	0	Alarm „RPS Diagnose“ aktivieren.	0
	1	Alarm „RPS Diagnose“ deaktivieren.	
2	0	Temperaturdiagnose aktivieren.	0
	1	Temperaturdiagnose deaktivieren.	

INDEX=2

Tabelle 37: Lesen des Port-Status (pro Port)

Offset	Wert	Beschreibung	Default-Wert
0	0	Port ausgeschaltet	0
	1	Port eingeschaltet	
1	0	Port: Modus – Vollduplex	0
	1	Port: Modus – Halbduplex	
2	0	Port: Link – Aus	0
	1	Port: Link – Ein	
3	0	Port: Übertragungsgeschwindigkeit – 10 Mbit/s	0
	1	Port: Übertragungsgeschwindigkeit – 100 Mbit/s	
	2	Port: Übertragungsgeschwindigkeit – 1 Gbit/s	
	7	Port: Übertragungsgeschwindigkeit – Automatisch	
4	1	Port: Link Aktivität – Disabled	5
	2	Port: Link Aktivität – Blocked	
	3	Port: Link Aktivität – Listen	
	4	Port: Link Aktivität – Learn	
	5	Port: Link Aktivität – Forward	
5	0	Port: Status LLDP Admin – Disabled	0
	1	Port: Status LLDP Admin – Tx only	
	2	Port: Status LLDP Admin – Rx only	
	3	Port: Status LLDP Admin – Tx/Rx	

INDEX=3

Tabelle 38: Lesen der Gerätediagnosen

Offset	Wert	Beschreibung	Default-Wert
0	0	Mainboard – Keine Überhitzung	0
	1	Mainboard – Überhitzung	
1	0	CPU – Keine Überhitzung	0
	1	CPU – Überhitzung	
2	0	ETHERNET PHY – Keine Überhitzung	0
	1	ETHERNET PHY – Überhitzung	
3	0	PWR – Keine Überspannung	0
	1	PWR – Überspannung	
4	0	RPS – Keine Überspannung	0
	1	RPS – Überspannung	
5	0	PWR – Keine Unterspannung	0
	1	PWR – Unterspannung	
6	0	RPS – Keine Unterspannung	0
	1	RPS – Unterspannung	
7	0	PWR hat Spannung.	0
	1	PWR hat keine Spannung.	
8	0	RPS hat Spannung.	0
	1	RPS hat keine Spannung.	
9	0	MRP-Ring deaktiviert	0
	1	MRP-Ring aktiviert	
10	0	MRP-Ring geöffnet (sinnvoll, wenn Byte 9 = 1)	0
	1	MRP-Ring geschlossen (sinnvoll, wenn Byte 9 = 1)	
11	0	Gerät hat Fehler (Alarm).	0
	1	Gerät funktioniert normal, kein Alarm gesetzt.	

INDEX=4, Configure Port Mirror

Tabelle 39: Konfigurieren der Funktion Port-Spiegelung

Byte Offset	Bit Offset	Wert	Beschreibung	Default-Wert
0	–	0	Port-Spiegelung deaktivieren.	0
		1	Port-Spiegelung aktivieren.	
1	–	0 ... 255	Ziel-Port für Spiegelung	0
2	0	0	Spiegelung für Eingang Port 1 deaktivieren.	0
		1	Spiegelung für Eingang Port 1 aktivieren.	
	1	0	Spiegelung für Eingang Port 2 deaktivieren.	0
		1	Spiegelung für Eingang Port 2 aktivieren.	
...				
3	3	0	Spiegelung für Eingang Port 12 deaktivieren.	0
		1	Spiegelung für Eingang Port 12 aktivieren.	
...				
6	0	0	Spiegelung für Ausgang Port 1 deaktivieren.	0
		1	Spiegelung für Ausgang Port 1 aktivieren.	
...				
9	7	0	Spiegelung für Ausgang Port 12 deaktivieren.	0
		1	Spiegelung für Ausgang Port 12 aktivieren.	

Im Gegensatz zu den zyklischen I/O-Daten erfolgt der Zugriff auf die DAP-Parameter über RDREC/WRREC-Funktionsbausteine (z. B. in TIA; siehe auch den Anwendungshinweis zum PROFINET-Managed-Switch von WAGO).

5.13 Zugriff über Konsolen-Port (CLI)

5.13.1 Vergabe der IP-Adresse mit dem Konsolen-Port

Der PROFINET-Managed-Switch wird mit folgenden IPv4-Einstellungen ausgeliefert.

- IP-Adresse 0.0.0.0
- Subnet-Maske 0.0.0.0
- Default-Gateway 0.0.0.0

Im PROFINET-Modus können die Netzwerkparameter ausschließlich durch das Engineering-Tool oder den PROFINET-Controller vergeben werden.

Im Folgenden wird beschrieben, wie mit Hilfe des Konsolen-Ports die IP-Adresse des PROFINET-Managed-Switch konfiguriert werden kann.

1. Verbinden Sie den Computer über ein geeignetes Kabel mit dem Konsolen-Port am Switch.
2. Verwenden Sie die folgenden Einstellungen für den Konsolen-Port:

Tabelle 40: Default-Einstellungen für den Konsolen-Port

Einstellung	Default-Wert
Baud Rate (Baudrate)	38400
Parity (Parität)	None (keine)
Number of Data Bits (Anzahl der Datenbits)	8
Number of Stop Bits (Anzahl der Stoppbits)	1
Flow Control	None

3. Drücken Sie **[EINGABE]**, um den Anmeldebildschirm aufzurufen.

```
L2SWITCH login:
```

4. Geben Sie **[admin]** ein, um in den CLI-Modus zu gelangen.

```
PN-SWITCH login: admin
PN-SWITCH>
```

5. Geben Sie **[enable]** ein, um in den privilegierten Modus zu wechseln. Verwenden Sie die folgenden Standardwerte für den Benutzernamen und das Passwort.

```
PN-SWITCH>enable
user:admin
password: wago
```

6. Geben Sie **[show running config]** ein, um die aktuelle Konfiguration des Gerätes zu sehen.

```
PN-SWITCH#show running-config
Current configuration:
vlan 1
name VLAN1
fixed 1-12
!
interface gigabitethernet1/0/1
!
interface gigabitethernet1/0/2
!
interface gigabitethernet1/0/3
!
interface gigabitethernet1/0/4
!
interface gigabitethernet1/0/5
!
interface gigabitethernet1/0/6
!
interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
interface gigabitethernet1/0/10
!
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 0.0.0.0/0
ip address default-gateway 0.0.0.0
!
profinet enable
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-1605
```

7. Geben Sie **[configure terminal]** ein, um das Gerät zu konfigurieren.

```
PN-SWITCH#configure terminal
PN-SWITCH(config)#
```

8. Geben Sie **[profinet disable]** ein, um PROFINET am Gerät zu deaktivieren.

```
PN-SWITCH(config)#profinet disable  
Success!
```

9. Geben Sie **[interface eth0]** ein, um die Netzwerkparameter des Switches zu konfigurieren.

```
PN-SWITCH(config)#interface eth0  
PN-SWITCH(config-if)#
```

10. Geben Sie **[ip address 192.168.1.254/24]** ein, um eine neue IP-Adresse (z. B. 192.168.1.254) bzw. Subnetzwerk-Maske (z. B. 255.255.255.0) zu konfigurieren.

```
PN-SWITCH(config-if)#ip 192.168.1.254/24  
Warning: Default gateway works in different subnet from IP.
```

11. Geben Sie **[exit]** ein, um das Konfigurationsmenü der Netzwerkparameter zu verlassen.

```
PN-SWITCH(config-if)#exit  
PN-SWITCH(config)#
```

12. Geben Sie **[exit]** ein, um das Konfigurationsmenü des Geräts zu verlassen.

```
PN-SWITCH(config)#exit  
PN-SWITCH#
```

13. Geben Sie **[show running config]** ein, um die aktuelle Konfiguration des Gerätes zu sehen.

```
PN-SWITCH#show running-config  
Current configuration:  
vlan 1  
name VLAN1  
fixed 1-12  
!  
interface gigabitethernet1/0/1  
!  
interface gigabitethernet1/0/2  
!  
interface gigabitethernet1/0/3  
!  
interface gigabitethernet1/0/4  
!  
interface gigabitethernet1/0/5  
!  
interface gigabitethernet1/0/6  
!
```

```

interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
interface gigabitethernet1/0/10
!
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 192.168.1.254/24
ip address default-gateway 0.0.0.0
!
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-1605

```

Jetzt können Sie den PROFINET-Managed-Switch unter der IP-Adresse 192.168.1.254 mit Ihrem Webbrowser erreichen.

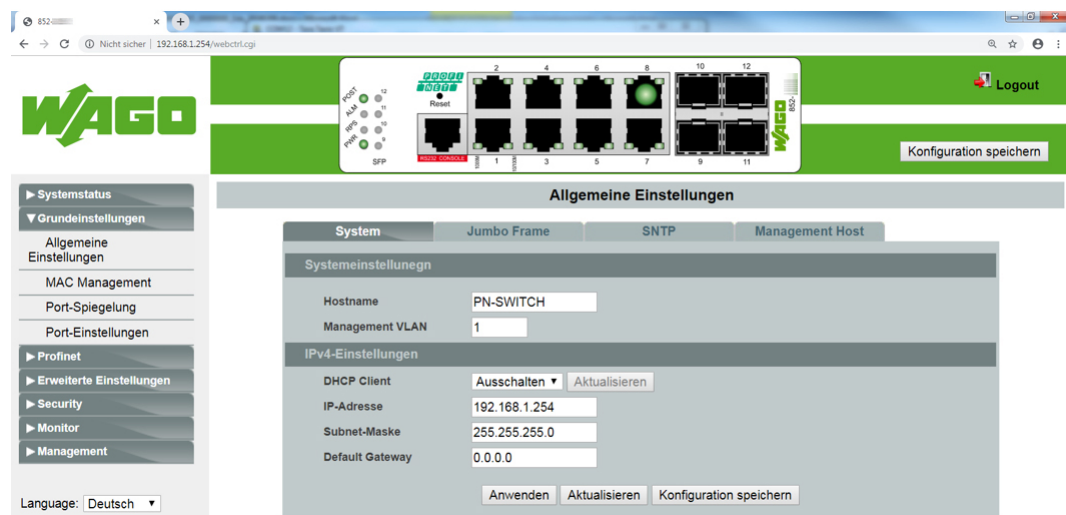


Abbildung 26: Aufrufen des PROFINET-Managed-Switches über das WBM

5.14 Parametrieren über WBM im PROFINET-Modus

Für die Konfiguration und Verwaltung des PROFINET-Managed-Switches stehen Ihnen ein internes Dateisystem und ein integrierter Webserver zur Verfügung, die als WBM („**Web-Based-Management-System**“) bezeichnet werden.

Der PROFINET-Managed-Switch wird mit aktiviertem PROFINET-Modus ausgeliefert. In diesem Auslieferungszustand gelten folgende Einstellungen:

- IP-Adresse: 0.0.0.0
- Subnet-Maske: 0.0.0.0

Um WBM nutzen zu können, muss zunächst eine IP-Adresse vergeben werden. Dazu gibt es verschiedene Möglichkeiten:

- über ein entsprechendes Projektierungstool (siehe Kapitel „Projektieren“)
- über den Konsolen-Port (siehe auch Kapitel „Zugriff über Konsole (CLI)“)
- über DCP mit einem externen Tool (z. B. PRONETA von Siemens oder PROFINET Commander)

Im PROFINET-Modus ist nur eine eingeschränkte WBM-Funktionalität gegeben.

Hinweis



Weitere Informationen zum WBM

In diesem Kapitel finden Sie die Beschreibung der Funktionalitäten, die im aktivierten PROFINET-Modus mit dem WBM realisiert werden können. Ausführliche Informationen zum WBM finden Sie im Kapitel „Im Web-Based-Management-System (WBM) konfigurieren“.

Ist der PROFINET-Modus aktiv, wird eine Vielzahl von Parametern durch den IO-Controller konfiguriert. Ist eine Konfiguration im WBM nicht möglich, wird dieses durch folgenden Satz **„Die Konfiguration erfolgt im PROFINET-Modus durch den PNIO-Controller“** im WBM gekennzeichnet.

Das WBM ist unter der konfigurierten IP-Adresse erreichbar.

Auf den intern gespeicherten HTML-Seiten erhalten Sie auslesbare Informationen über die Konfiguration und den Status des Feldbusknotens.

Außerdem ändern Sie hier die Konfiguration des Gerätes.

Darüber hinaus können Sie über das implementierte Dateisystem auch selbst erstellte HTML-Seiten hinterlegen.

Hinweis



Nach Änderungen an der Konfiguration immer einen Neustart durchführen!

Damit geänderte Konfigurationseinstellungen wirksam werden, führen Sie nach Ihren Änderungen immer einen Systemneustart durch.

1. Zum Öffnen des WBM starten Sie Ihren Webbrowser. Für die Nutzung des WBM wird die Verwendung eines aktuellen Browsers von Google Chrom oder Firefox empfohlen.
2. Geben Sie in der Adresszeile die IP-Adresse des PROFINET-Managed-Switches ein.
3. Bestätigen Sie mit **[Enter]**.
4. Geben Sie im Anmeldefenster Ihren Benutzernamen und das Passwort ein:

Default-User = „admin“

Default-Passwort = „wago“

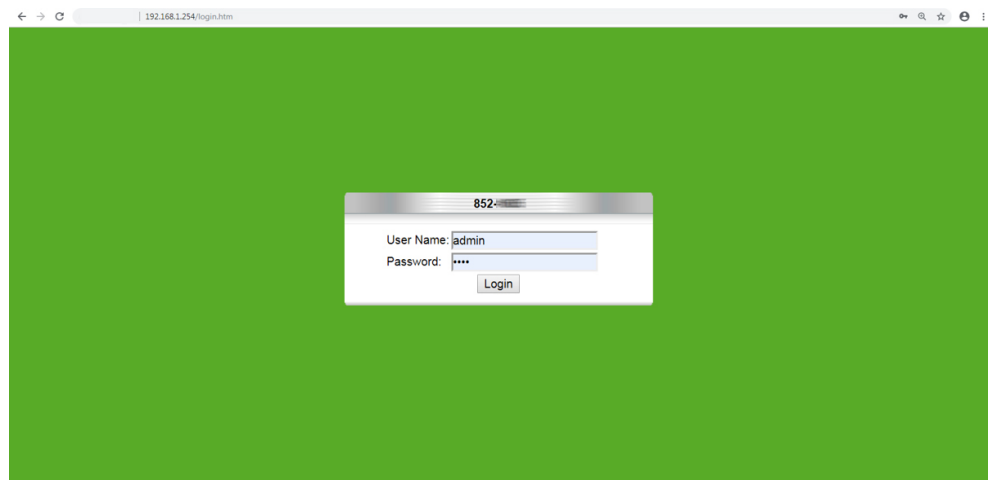


Abbildung 27: Anmeldefenster für WBM

WAGO empfiehlt, nach dem 1. Log-in den Benutzernamen und das Passwort zu ändern. Diese Einstellungen finden Sie im Menü **Management > SNMP > Benutzerkonto**.

5. Die Startseite des WBM wird aufgebaut.
6. Führen Sie die gewünschten Einstellungen durch.
7. Bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Übernehmen]**, **[Aktualisieren]** oder **[Anwenden]** oder verwerfen Sie Ihre Änderungen mit der Schaltfläche **[Löschen]** oder **[Verwerfen]**.
8. Damit die Einstellungen übernommen werden, bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Konfiguration Speichern]**.

Über die Links der Navigationsleiste erreichen Sie die entsprechenden WBM-Seiten:

Tabelle 41: Übersicht - Navigationslinks und WBM-Seiten

Navigationslinks und WBM-Seiten
► [Systemstatus]
• Systeminformationen
► [Grundeinstellungen]
• Allgemeine Einstellungen • Port-Mirroring • Port-Einstellungen
► [PROFINET]
• Konfiguration • Informationen • Diagnose
► [Erweiterte Einstellungen]
• MRP
► [Sicherheit]
► [Monitor]
► [Management]
[SNMP] • Upload-File • Benutzerkonto

Auf diesen WBM-Seiten können die Einstellungen/Konfigurationen des PROFINET-Managed-Switches vorgenommen werden.

Auf einigen WBM-Seiten existieren für die Einstellungen/Konfigurationen Registerseiten.

Die Default-Werte sind **fett** hervorgehoben dargestellt.

5.14.1 Systemstatus

5.14.1.1 Systeminformationen

Systeminformation	
Modellname	852- 
Host-Name	PN-SWITCH
Boot Code Version	V1.3.9.S0
Profinet Software	
Version	V1.2.0
MD5 Checksum	c91b249410198ba0a5125166504b645d
PN Boot Image	
Firmware-Version	V1.2.1.S0
Built Date	Sun Apr 28 17:03:45 CST 2019
Prüfsumme	dd8815a4
DHCP Client	Ausschalten
IP-Adresse	192.168.1.254
Subnet-Maske	255.255.255.0
Default Gateway	0.0.0.0
MAC-Adresse	00:30:de:ff:f5:b8
Seriennummer	0001910146780101
Management VLAN	1
CPU-Auslastung	1 %
Speicherauslastung	Total: 118996 KB, Free: 90044 KB, Usage: 24.33 %
Aktuelle Uhrzeit	2000-1-23, 17:14:41
System Uptime	0 days, 6 hours, 21 minutes, 2 seconds
Aktualisieren	

Abbildung 28: WBM-Seite „Systeminformationen“

Tabelle 42: WBM-Seite „Systeminformationen“ (Beispiel 852-1605 übertragbar auf 852-0602, -0603)

Parameter	Beschreibung
Modellname	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
Host-Name	In diesem Anzeigefeld wird der Hostname des Switches angezeigt.
Boot Code Version	In diesem Anzeigefeld wird die Boot-Code-Version angezeigt.
Profinet Software Version	Identifikationsnummer der „Profinet Software Version“
Profinet Software MD5 Prüfsumme	Prüfsumme der „Profinet Software Version“
PN Boot Image Firmware-Version	In diesem Feld wird die Version des „PN Boot Images“ angezeigt.
PN Boot Image Build Date	In diesem Feld wird das Datum der Firmwareerzeugung angezeigt.
PN Boot Image Prüfsumme	In diesem Feld wird die Prüfsumme des „PN Boot Images“ angezeigt
DHCP Client	In diesem Anzeigefeld wird angezeigt, ob die DHCP-Client-Funktion aktiviert ist.
IP Address	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt.
Subnet Mask	In diesem Anzeigefeld wird die „Subnet Mask“ des Switches angezeigt.
Default Gateway	In diesem Anzeigefeld wird das Default-Gateway des Switches angezeigt.
MAC Address	In diesem Anzeigefeld wird die MAC-(Media-Access-Control-)Adresse des Switches angezeigt.
Seriennummer	In diesem Anzeigefeld wird die Seriennummer angezeigt.
Management-VLAN	In diesem Anzeigefeld wird die VLAN-ID angezeigt, die für die Verwaltungsprozesse des Switches benötigt wird.
CPU-Auslastung	In diesem Anzeigefeld wird die prozentuale Systemauslastung des Switches angezeigt.
Speicherauslastung	In diesem Anzeigefeld wird der gesamte („Total“) sowie der momentan verfügbare („Free“) und verwendete („Usage“) Speicher des Switches angezeigt.
Aktuelle Uhrzeit	In diesem Anzeigefeld wird das aktuelle Datum (yyyy-mm-dd) und die aktuelle Uhrzeit (hh:mm:ss) angezeigt.
System Uptime	In diesem Feld wird angezeigt, wie lange der Switch nach dem Einschalten läuft: Tage, Stunden, Minuten und Sekunden.

5.14.2 Grundeinstellungen

5.14.2.1 Allgemeine Einstellungen

5.14.2.1.1 System

The screenshot shows the 'Allgemeine Einstellungen' (General Settings) page in the WBM interface, with the 'System' tab selected. The page is divided into two main sections: 'Systemeinstellungen' (System Settings) and 'IPv4-Einstellungen' (IPv4 Settings).

Systemeinstellungen:

- Hostname: PN-SWITCH
- Management VLAN: 1

IPv4-Einstellungen:

- DHCP Client: Ausschalten (dropdown menu) with an 'Aktualisieren' (Update) button next to it.
- IP-Adresse: 192.168.1.254
- Subnet-Maske: 255.255.255.0
- Default Gateway: 0.0.0.0

At the bottom of the IPv4 settings section, there are three buttons: 'Anwenden' (Apply), 'Aktualisieren' (Update), and 'Konfiguration speichern' (Save Configuration).

Abbildung 29: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

Tabelle 43: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

Systemeinstellungen		
Parameter	Standardwert	Beschreibung
Hostname	PN-SWITCH	Geben Sie im Eingabefeld bis zu 64 alphanumerische Zeichen für den Namen Ihres Switches ein. Der Hostname sollte aus einer Kombination aus Zahlen, Buchstaben, Bindestrichen (-) oder Unterstrichen (_) bestehen.
Management VLAN	1	Geben Sie im Eingabefeld eine VLAN-Gruppe ein, die Zugriff auf den Switch erhalten soll. Gültiger VLAN-Bereich: 1 ... 4094.
		Hinweis  Konfiguration eines Management-VLANs Vor der Konfiguration eines Management-VLANs müssen Sie zuerst ein Management-VLAN erstellen und diesem mindestens einen Teilnehmer-Port zuweisen.
IPv4-Einstellungen		
Parameter	Standardwert	Beschreibung
DHCP Client	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die IP-Adresse des Switches manuell konfigurieren möchten.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit der Switch seine IP-Adresse von einem DHCP-Server automatisch bezieht. Klicken Sie auf [Aktualisieren] , damit der Switch erneut eine IP-Adresse vom DHCP-Server bezieht.
IP-Adresse	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse des Switches in Dezimalpunktschreibweise ein.
Subnet-Maske	0.0.0.0	Geben Sie im Eingabefeld die IP-Subnet-Maske des Switches in Dezimalpunktschreibweise ein.
Default Gateway	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse des ausgehenden Default-Gateways in Dezimalpunktschreibweise ein.

5.14.2.2 Port-Spiegelung

ACHTUNG



Fehlerhafte Spiegelung kann Applikation stören!

Durch die fehlerhafte Spiegelung von Ports kann die Applikation gestört, beziehungsweise instabil werden. In diesem Fall kann der Switch im PROFINET-Modus einfach neu gestartet werden. Der IO-Controller überschreibt damit die fehlerhaften Einstellungen mit der aktuellen Konfiguration.

Port-Spiegelung

Port-Spiegelung-Einstellungen

Status Ausschalten ▾
 Überwachung an Port 1 ▾

Alle Ports : - ▾

Source Port	Spiegel-Modus	Source Port	Spiegel-Modus
1	Ausschalten ▾	2	Ausschalten ▾
3	Ausschalten ▾	4	Ausschalten ▾
5	Ausschalten ▾	6	Ausschalten ▾
7	Ausschalten ▾	8	Ausschalten ▾
9	Ausschalten ▾	10	Ausschalten ▾
11	Ausschalten ▾	12	Ausschalten ▾

Anwenden
Aktualisieren
Konfiguration speichern

Abbildung 30: WBM-Seite „Port-Spiegelung-Einstellungen“

Tabelle 44: WBM-Seite „Port-Spiegelung-Einstellungen“

Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Port-Spiegelung“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Port-Spiegelung“ zu aktivieren.
Überwachung an Port	1 ... 10 (12)	Wählen Sie im Auswahlfeld einen Port aus, der mit einem „Network Traffic Analyzer“ verbunden werden soll.
Alle Ports:	–	Einstellungen in diesem Auswahlfeld wirken sich auf alle Ports aus.
	Ausschalten	Nehmen Sie hier nur Einstellungen vor, wenn diese für alle Ports gelten sollen.
	Ingress	
	Egress	Beginnen Sie hier mit allgemeinen Einstellungen und nehmen Sie anschließend Einstellungen für einzelne Ports vor.
	Beide	
Source Port	1 ... 10 (12)	In dieser Spalte wird die Nummer der einzelnen „Source Ports“ angezeigt.
Spiegel-Modus	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn kein Datenverkehr von den spezifizierten „Source Ports“ zum Monitor Port kopiert werden soll.
	Ingress	Wählen Sie im Auswahlfeld „Ingress“, um nur die Eingangsdaten (eingehende) der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.
	Egress	Wählen Sie im Auswahlfeld „Egress“, um nur die Ausgangsdaten (ausgehende) der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.
	Beide	Wählen Sie im Auswahlfeld „Beide“, um beide (ein- und ausgehende) Daten der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.

Der PROFINET-Managed-Switch erlaubt eine Multi-Port-Spiegelung. D. h., mehrere Ports können auf einen Ziel-Port gespiegelt werden.

Das Rücksetzen dieser Einstellungen kann über ein Reset bzw. Reboot des Switches erfolgen.

5.14.2.3 Port-Einstellungen

Port-Einstellungen

Allgemeine Einstellungen
Informationen

Port-Einstellungen

Port	Status	Geschwindigkeit / Duplex	Flusskontrolle
von: 1 ▼ an: 1 ▼	Einschalten ▼	Auto ▼	Aus ▼

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	Status	Geschwindigkeit / Duplex	Flusskontrolle	Link Status
1	Einschalten	Auto	Aus	Link inaktiv
2	Einschalten	Auto	Aus	Link inaktiv
3	Einschalten	Auto	Aus	Link inaktiv
4	Einschalten	Auto	Aus	Link inaktiv
5	Einschalten	Auto	Aus	Link inaktiv
6	Einschalten	Auto	Aus	Link inaktiv
7	Einschalten	Auto	Aus	Link inaktiv
8	Einschalten	Auto	Aus	1000M / Voll / Aus
9	Einschalten	Auto	Aus	Link inaktiv
10	Einschalten	Auto	Aus	Link inaktiv
11	Einschalten	Auto	Aus	Link inaktiv
12	Einschalten	Auto	Aus	Link inaktiv

Abbildung 31: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“

Im PROFINET-Modus dient diese Seite nur zur Information. Das Ändern von Einstellungen ist nicht möglich.

5.14.3 PROFINET

5.14.3.1 PROFINET Setting



Abbildung 32: WBM-Seite „PROFINET Setting“

Im Auslieferungszustand ist der PROFINET-Modus eingeschaltet.

ACHTUNG



WBM-Einstellungen im PROFINET-Modus können zu Fehlfunktionen führen!

Befindet sich der PROFINET-Managed-Switch im PROFINET-Modus, wird er durch den IO-Controller konfiguriert. Veränderungen der Einstellungen im WBM können zu einer Fehlfunktion des Switches im PROFINET-Netzwerk führen.

Durch ein Reset des Switches wird die Konfiguration durch den IO-Controller neu auf das Gerät geladen. Fehlerhafte Konfigurationen werden damit überschrieben.

Tabelle 45: WBM-Seite „PROFINET Setting“

Parameter	Standardwert	Beschreibung
Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie „PROFINET Setting“ einschalten möchten.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie „PROFINET Setting“ einschalten möchten.

5.14.3.2 Informationen

Device Data	
Device Name	wagopnswitch
I&M0	
Hersteller-ID	011d
Profilspezifischer Typ	Active Network Infrastructure Component(6)
Auftragsnummer	852-
Seriennummer	0001910146780101
Hardware Revision	1
Software Revision	V1.2.0
Revisionsanzahl	1
I&M1	
Tag-Funktion	
Tag-Position	
I&M2	
Date	
I&M3	
Deskriptor	
I&M4	
Unterschrift	
Anwenden Aktualisieren	

Abbildung 33: WBM-Seite „Informationen“

5.14.3.3 Diagnoseliste

Diagnoseliste			
SubSlot	Schwere	Err/Ext. Err	Kanal/USI/Fehler
Aktualisieren			

Abbildung 34: WBM-Seite „Diagnoseliste“

Diese Seite dient zur Anzeige der vorhandenen Diagnosen.

5.14.4 Erweiterte Einstellungen

5.14.4.1 MRP

MRP Global Settings

Global State Ausschalten ▾

MRP Settings

Ring ID Hinzufügen ▾

Modus Hinzufügen ▾ Client ▾

Port-1 Hinzufügen ▾

Port-2 Hinzufügen ▾

Status Ausschalten ▾

Uuid Hinzufügen ▾

VLAN Hinzufügen ▾ Bereich: 1~4094

Anwenden

Aktualisieren

MRP Status

Typ: Alle ▾ Zeigen

MRP Status	Ausschalten		
Ring ID	1	Ring Status	Ausschalten
Device Mode	Client	State Machine Mode	Not Running
Uuid	ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff		
VLAN ID	1		
Port-1	1	Port-1-mode	Port Down
Port-2	2	Port-2-mode	Port Down

Abbildung 35: WBM-Seite „MRP“

Tabelle 46: WBM-Seite „MRP“

MRP Global Settings		
Parameter	Standardwert	Beschreibung
Global State	Ausschalten	Wählen Sie im Auswahlfeld "Ausschalten", um diese Funktion der globalen MRP zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld "Einschalten", um diese Funktion der globalen MRP zu aktivieren.
MRP Settings		
Parameter	Standardwert	Beschreibung
Ring ID	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um eine (neuen) Ring-ID einzugeben.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um eine Ring-ID zu löschen.
Modus	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den Switch entweder als Client (MRC) oder Manager (MRM) zu konfigurieren.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um die Konfiguration des Switches entweder als Client (MRC) oder Manager (MRM) zu löschen.
Port 1	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den primären Anschluss für den MRP-Ring hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um den primären Anschluss für den MRP-Ring zu löschen.
Port 2	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den sekundären Anschluss für den MRP-Ring hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um den sekundären Anschluss für den MRP-Ring zu löschen.
Status	Ausschalten	Wählen Sie im Auswahlfeld "Ausschalten", um den jeweiligen Ring einzuschalten.
	Einschalten	Wählen Sie im Auswahlfeld "Ausschalten", um den jeweiligen Ring einzuschalten.
UUID	Hinzufügen	Konfiguriert den "Universal Unique Identifier" (UUID) für den MRP-Ring. Dies ist eine Zeichenkette im hexadezimalen Format, die den Ring darstellt, zu dem dieser Schalter gehört. Beispiel: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Entfernen	
VLAN	Hinzufügen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, für die dieser Ring aktiviert werden soll. Gültiger Bereich der VLAN-IDs: 1 ... 4094. Verwenden Sie ein Komma (,) bzw. einen Bindestrich (-), um einzelne VLANs bzw. VLAN-Bereiche anzugeben.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen" und geben Sie die VLANs ein, in denen der Switch nicht aktiviert werden soll.

Tabelle 46: WBM-Seite „MRP“

MRP Status		
Parameter	Standardwert	Beschreibung
Typ	Alle	Wählen Sie im Auswahlfeld „Alle“ aus, wenn Sie alle MRP-Status anzeigen möchten.
	Ring-ID	Wählen Sie im Auswahlfeld die Ring-ID aus, für die der MRP-Status der ausgewählten Ring ID angezeigt werden soll.
MRP Status	–	In diesem Anzeigefeld wird der aktuelle Zustand des jeweiligen MRP-Rings angezeigt.
Ring ID	–	In diesem Anzeigefeld wird die ID-Nummer des MRP-Rings angezeigt.
Device Mode	–	In diesem Anzeigefeld wird der Modus des Switches angezeigt: Client (CRM)/Manager (MRM)
Uuid	–	In diesem Anzeigefeld wird die zugewiesene UUID angezeigt.
Vlan ID	–	In diesem Anzeigefeld wird angezeigt, in welchem VLAN dieser Ring gehört.
Port-1	–	In diesem Anzeigefeld wird der zugeordnete Port des Switches angezeigt.
Port-2	–	In diesem Anzeigefeld wird der zugeordnete Port des Switches angezeigt.
Ring Status	–	In diesem Anzeigefeld wird der aktuelle Status des MRP-Rings angezeigt.
State Machine Mode	–	In diesem Anzeigefeld wird angezeigt, ob die MRP-Zustandsmaschine läuft oder nicht.
Port-1-mode	–	In diesem Anzeigefeld wird Status des Ports angezeigt: (port down/port up).
Port-2-mode	–	In diesem Anzeigefeld wird Status des Ports angezeigt: (port down/port up).

5.14.5 Management

5.14.5.1 Datei hochladen

Im PROFINET-Managed-Switch sind die GSDML-Datei und die MIB-Datei eingebettet.

Sie können diese Dateien über den Browser in das WBM laden.

Abbildung 36: WBM-Seite „Datei hochladen“

Tabelle 47: WBM-Seite „Datei hochladen“

Parameter	Standardwert	Beschreibung
Dateityp	MIB	Auswahl, ob die MIB- oder die GSDML-Datei in das WBM geladen werden soll

5.14.5.1.1 Benutzerkonto

Nr.	Name	Authoritat	Aktion
1	admin	Admin	

Abbildung 37: WBM-Seite „Benutzerkonto“

Tabelle 48: WBM-Seite „Benutzerkonto“

Parameter	Standardwert	Beschreibung
User Name	admin	Angabe des Benutzernamens
User Password	wago	Angabe des Passworts
User Authority	Admin	Festlegen der Berechtigungsgruppe des aktuellen Anwenders

6 Montieren

6.1 Montageort

Die Auswahl des Installationsortes kann die Leistung des Industrial-Managed-Switches sehr beeinflussen. Wir empfehlen, bei der Auswahl eines Standortes Folgendes zu berücksichtigen:

- Installieren Sie den Industrial-Managed-Switch an einem geeigneten Standort. Im Kapitel „Gerätebeschreibung“ > ... > „Technische Daten“ erhalten Sie Informationen zu akzeptablen Betriebsbereichen bezüglich Temperatur und Luftfeuchtigkeit.

Vergewissern Sie sich, dass die Wärmeabgabe vom Industrial-Managed-Switch gewährleistet und die Belüftung um ihn herum angemessen ist. Platzieren Sie keine schweren Objekte auf dem Industrial-Managed-Switch.

6.2 Montage auf Tragschiene

Die Tragschiene muss die im System integrierten EMV-Maßnahmen und die Schirmung über die I/O-Modul-Anschlüsse optimal unterstützen.

Hängen Sie den Industrial-Managed-Switch von oben auf die Tragschiene und rasten Sie ihn ein.

6.3 Demontage von der Tragschiene

Zum Entfernen von der Tragschiene müssen Sie ein geeignetes Werkzeug in die unter dem Industrial-Managed-Switch befindliche Metalllasche einführen und die Metalllasche nach unten auslenken.

Danach können Sie den Industrial-Managed-Switch unten von der Tragschiene lösen und nach oben hin abnehmen.

7 Geräte anschließen

7.1 Spannungsversorgung

Der Industrial-Managed-Switch verwendet eine Gleichstromversorgung, die für 12 ... 60 V ausgelegt ist.

Die primäre und sekundäre Netzverbindung wird über eine 6-polige Steckverbindung hergestellt, die sich an der Oberseite des Industrial-Managed-Switches befindet.

Die Federleiste (Bestellnr. 2231-106/026-000) umfasst 6 Anschlussklemmen und kann problemlos per Hand mit der auf der Oberseite des Switches befindlichen 6-poligen Stiftleiste verbunden und wieder gelöst werden.

Das Netzteil des Industrial-Managed-Switches stellt sich automatisch auf die lokale Stromquelle ein und kann auch eingeschaltet werden, wenn keine oder nicht alle Patchkabel angeschlossen sind.

1. Schließen Sie einen geeigneten Erdungsleiter an die Erdungsschraube an der Oberseite des Switches an.

Hinweis



Erdung des Switches

Durch die Erdung des Switches werden elektromagnetische Störungen infolge von elektromagnetischer Störstrahlung verhindert. Beachten Sie dazu die entsprechenden Normen für EMV-gerechte Installationen.

2. Falls die Federleiste noch nicht in die Stiftleiste des Switches gesteckt wurde, stecken Sie sie jetzt. Überprüfen Sie den festen Sitz der Federleiste durch leichtes Rütteln.
3. PWR +/-:
Zum Anschließen oder Lösen der Leiter für die primäre Spannungsversorgung betätigen Sie in der Federleiste die Feder direkt mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder entfernen ihn.
4. Ist ein primäres Netzteil angeschlossen und aktiv, leuchtet die LED „PWR“ an der Vorderseite. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig verbunden ist und fest sitzt.
5. RPS +/-:
Zum Anschließen oder Lösen der Leiter für die sekundäre Spannungsversorgung betätigen Sie in der Federleiste direkt die Feder mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder entfernen ihn.

6. Ist ein sekundäres Netzteil angeschlossen und aktiv, leuchtet die LED „RPS“ an der Vorderseite. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig verbunden ist und fest sitzt.

7.2 Externer Alarmkontakt-Anschluss

Der Industrial-Managed-Switch verfügt über eine Alarmkontakt-Anschlussstelle auf der Oberseite. Die genaue Vorgehensweise zum Anschluss der Alarmkontakt-Versorgungsleiter an beide ALM-Kontakte der 6-poligen Federleiste entnehmen Sie dem Kapitel „Spannungsversorgung (PWR/RPS)“ (es handelt sich um die gleiche Vorgehensweise).

Sie können den potentialfreien Alarmkontakt an ein Diagnosesystem anschließen, das in der Schaltzentrale oder in der Fabrikhalle des Anwenders schon installiert ist. Wenn ein Fehler auftritt, wird zur Aktivierung des externen Alarms ein Signal vom Industrial Switch durch den Alarmkontakt gesendet. Der Alarmkontakt hat zwei Anschlüsse, die als Fehlerleitung zum Anschluss der Alarmanlage dienen.

Ein Alarm wird in folgenden Fällen gemeldet:

- 1 Verbindungsfehler (z. B. getrennte Leitung, Geräteausfall etc.)
- 2 PWR/RPS:
 - a Versorgungsfehler (Stromleitung ist unterbrochen, Versorgungsstörung etc.)
 - b Die Eingangsversorgungsspannung liegt außerhalb der Spezifikationen (12 ... 60 V).

7.3 Anschluss Konsolenanschlusskabel

Der Konsolenanschluss (RJ-45) ermöglicht die lokale Verwaltung.

1. Stecken Sie die RJ-45-Seite des (8-Stift-RJ-45-zu-DB9-) Kabels in den RJ-45-Konsolenanschluss am Industrial-Managed-Switch und das andere Ende in den COM-Anschluss des Computers.
2. Konfigurieren Sie die HyperTerminal-Einstellungen wie im Kapitel „Konfigurieren“ > ... > „Konsolen-Port“ erläutert.

Informationen zur Anschlussbelegung des Konsolenanschlusses (8-Stift-RJ-45) finden Sie im Kapitel „Anhang“ > ... > „Konsolenanschluss (RJ-45 zu DB9)“ beschrieben.

7.4 Anschluss 1000BASE-SX/LX, Glasfaser

Achten Sie beim Verbinden des Glasfaserkabels mit einem 1000BASE-SX/LX-Anschluss am Industrial-Managed-Switch auf die Verwendung des richtigen Steckertyps (LC) und SFP-Moduls.

Es gibt verschiedene Arten von Mehrfachmoden-, Einzelmoden- oder WDM-SFP-Modulen.

Führen Sie die nachfolgenden Schritte aus, um das vorkonfektionierte Glasfaserkabel ordnungsgemäß anzuschließen:

Hinweis



Gummiabdeckungen

Entfernen Sie die Gummiabdeckungen des 1000BASE-SX/LX-Anschlusses und bewahren Sie diese auf.

Ist kein SFP-Modul angeschlossen, sollte der Anschluss zum Schutz der Glasfasern mit der Gummiabdeckung verschlossen sein.

1. Stecken Sie die jeweiligen SFP-Module ein und verriegeln Sie diese.
2. Stellen Sie sicher, dass die Glasfaseranschlüsse sauber sind. Sie können die Kabelstecker reinigen, indem Sie diese mit einem sauberen Tuch oder einem mit etwas Ethanol getränkten Wattebausch abwischen. Verschmutzte Glasfaserkabelenden beeinträchtigen die Qualität des Lichts, das über das Kabel übertragen wird, und führen zu einer verminderten Leistung am Anschluss.
3. Verbinden Sie den LC-Stecker mit dem jeweiligen SFP-Modul des Industrial-Managed-Switches.

Hinweis



Korrekte Verbindung des Glasfaserkabels am SFP-Modul

Für eine korrekte Verbindung den Stecker des Glasfaserkabels hörbar am SFP-Modul einrasten.

4. Überprüfen Sie die entsprechende Anschluss-LED am Industrial-Managed-Switch darauf, ob die Verbindung hergestellt ist (siehe Kapitel „Gerätebeschreibung“ > ... > „Anzeigeelemente“).

7.5 Anschluss 10/100/1000Base-T-Ports

Die 10/100/1000Base-T-Ports (RJ-45-Ethernet-Anschlüsse) des Industrial-Managed-Switches unterstützen sowohl Autosensing als auch Autonegotiation.

1. Verbinden Sie ein Ende eines verdrehten Kabels vom Typ Kategorie 3/4/5/5e mit einem verfügbaren RJ-45-Anschluss am Industrial-Managed-Switch und das andere Ende mit dem Anschluss des ausgewählten Netzwerkknotens.
2. Überprüfen Sie die entsprechende Anschluss-LED am Industrial-Managed-Switch darauf, ob die Verbindung hergestellt ist.
(siehe Kapitel „Anzeigeelemente“ > ... > „Anschluss-LEDs“).

8 Funktionsbeschreibung

8.1 Grundeinstellungen

8.1.1 Jumbo Frame

„Jumbo Frames“ sind ETHERNET-Frames mit einer Größe von mehr als 1518 Byte. Sie können die Effizienz von Datenübertragungen in einem Netzwerk erhöhen. Je größer die „Jumbo Frames“, desto besser ist die Netzwerkleistung.

Hinweis



Einstellungen der „Jumbo Frames“

Die Einstellung der Größe der „Jumbo Frames“ gilt für jeden Port des Switches.

Alle angeschlossenen Netzwerkteilnehmer müssen die gleiche Größe des „Jumbo Frames“ unterstützen.

Datenpakete, die größer als der eingestellte „Jumbo Frame“ sind, werden vom entsprechenden Netzwerkteilnehmer verworfen.

8.1.2 SNTP

Das SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) ist ein Protokoll zur Synchronisierung von Uhren in Computersystemen. Es ist eine weniger komplexe Implementierung eines NTP („**N**etwork **T**ime **P**rotocol“). SNTP verwendet die koordinierte Weltzeit UTC („**C**oordinated **U**niversal **T**ime“, französisch: „**T**emps **U**niversel **C**oordonné“). Es werden keine Informationen über Zeitzonen oder Sommerzeiten übertragen. Diese Informationen liegen außerhalb des Protokollbereichs und müssen separat bezogen werden.

Der SNTP-Port ist 123.

Hinweis



Hinweis

1. Der SNTP-Server antwortet immer mit der aktuellen koordinierten Weltzeit UTC.
2. Empfängt der Switch die SNTP-Antwortzeit, gleicht er diese Zeit mit der Zeitonenkonfiguration ab und konfiguriert die Zeit für den Switch entsprechend.
3. Ist keine IP-Adresse für einen Zeitserver konfiguriert, versendet der Switch keine SNTP-Abfragepakete.
4. Empfängt der Switch keine SNTP-Antwortpakete, wiederholt er die Abfrage ohne zeitliche Beschränkung alle zehn Sekunden.
5. Erhält der Switch eine SNTP-Antwort, wiederholt er die Zeitabfrage an den NTP-Server stündlich.
6. Nach Änderung der Zeitzone und des NTP-Servers wiederholt der Switch den Abfrageprozess.
7. Kein Default-SNTP-Server.

8.1.3 Management Host

Der Management Host begrenzt die Anzahl der Hosts, die den Switch verwalten können. In den Default-Einstellungen gibt es keinen „Management Host“. Das liegt daran, dass jeder Host den Switch über Telnet oder Webbrowser verwalten kann. Wenn ein Benutzer einen oder mehrere Hosts konfiguriert hat, kann der Switch nur durch diese Hosts verwaltet werden. Die Funktion ermöglicht es Benutzern, bis zu drei Einträge für die Management-IPs zu konfigurieren.

8.1.4 MAC-Management

Die MAC-Adresse („**Media Access Control Adresse**“, Hardwareadresse für die Zugriffssteuerung) ist in einem Netzwerk die einzigartige Hardwarenummer eines Gerätes.

Dynamische Adresse

Beim Empfang von Frames empfängt der Switch die MAC-Quelladresse, die er zusammen mit dem empfangenen Port, dem VLAN und einer „Age Time“ (Lebensdauer) in der Adresstabelle abspeichert. Wenn die „Age Time“ abgelaufen ist, wird der Adresseintrag aus der Adresstabelle wieder gelöscht.

Statische Adresse

Eine von Benutzern festgelegte statische Adresse erhält keine „Age Time“ und wird damit auch nicht vom Switch gelöscht. Die statische Adresse kann nur von einem Benutzer gelöscht werden. Der Switch unterstützt eine Adresstabelle mit einer Größe von bis zu 16 K.

Statische und dynamische Adressen teilen sich dieselbe Adresstabelle.

MAC Table

Die „MAC Table“ (MAC-Adresstabelle, die auch als Filterdatenbank bezeichnet wird) zeigt, welche Frames an die Ports des Switches weitergeleitet oder herausgefiltert werden.

Sendet ein Gerät, das zu einer VLAN-Gruppe gehören kann, ein Datenpaket, das an einen Port am Switch weitergeleitet wird, kann die MAC-Adresse des Gerätes aus der MAC-Adresstabelle des Switches abgelesen werden.

Dabei wird auch angezeigt, ob es sich um eine dynamische (vom Switch bezogene) oder statische (manuell festgelegte) MAC-Adresse handelt.

MAC-Adresstabelle

Der Switch nutzt die MAC-Adresstabelle, um zu bestimmen, wie er Frames weiterleitet (siehe Abbildung unten).

1. Der Switch überprüft einen empfangenen Frame und erkennt den Port, von dem die MAC-Quelladresse stammt.

2. Der Switch prüft, ob die MAC-Zieladresse des Frames mit einer bereits erkannten MAC-Quelladresse in der MAC-Adresstabelle übereinstimmt.
 - Ist dem Switch der Port für diese MAC-Adresse bereits bekannt, leitet er den Frame zu diesem Port weiter.
 - Ist dem Switch der Port für diese MAC-Adresse noch nicht bekannt, leitet er den Frame zu allen Ports weiter. Ein „Port Flooding“ (zu häufiges Weiterleiten an alle Ports) kann zu Netzwerkengpässen führen.
 - Ist dem Switch der Port für diese MAC-Adresse bereits bekannt und sind der Ziel-Port und der Eingangs-Port aber identisch, wird der Frame gefiltert.

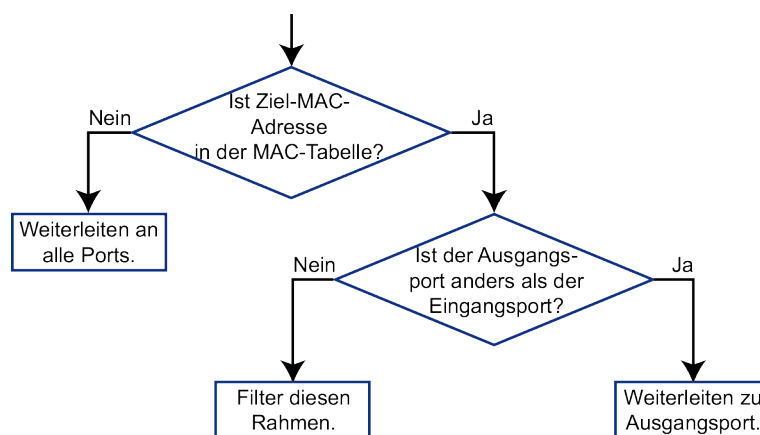


Abbildung 38: Ablaufdiagramm der MAC-Adresstabelle

8.1.4.1 Static MAC

Statische MAC-Adressen

Eine statische MAC-Adresse ist eine Adresse, die manuell in die MAC-Adresstabelle eingetragen wurde. Statische MAC-Adressen erhalten keine „Age Time“. Wenn Sie Regeln für statische MAC-Adressen einrichten, stellen Sie diese Adressen für einen Port ein. Dies kann den Datenübertragungsbedarf verringern.

8.1.5 Port-Spiegelung (Port Mirroring)

Die Port-Spiegelung wird bei Switches eingesetzt, um Kopien von gesendeten/empfangenen Netzwerkpaketen aus einem oder mehreren Bereichen an eine Netzwerküberwachung oder an einen anderen Switch-Port (Monitor-Port) zu senden.

Die Port-Spiegelung wird in Netzwerksystemen eingesetzt, bei denen eine Überwachung des Netzwerkverkehrs erforderlich ist, wie etwa in einem IDS („Intrusion **D**etection **S**ystem“, Angriffserkennungssystem).

Die Port-Spiegelung kann zusammen mit einem NTA („**N**etwork **T**raffic **A**nalyzer“, Programm zur Analyse des Netzwerkverkehrs) dabei helfen, den Netzwerkverkehr zu überwachen. Dabei können Benutzer bei ausgewählten Ports („Source Ports“, Quell-Ports) die eingehenden und/oder ausgehenden Datenpakete überwachen lassen.

Quellmodus

- „Ingress“ (Eingang): Die eingehenden Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.
- „Egress“ (Ausgang): Die ausgehenden Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.
- Beide: Sowohl eingehende als auch ausgehende Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.

Hinweis



Hinweis

1. Der Monitor-Port kann kein Mitglied einer „Trunk Port“-Gruppe sein.
2. Der Monitor-Port kann kein Eingangs- oder Ausgangs-Port sein.
3. Wenn ein Port als Quell-Port konfiguriert wurde und ein Benutzer ihn anschließend als Ziel-Port konfiguriert, wird der Port automatisch aus den Quell-Ports gelöscht.

8.1.6 Port-Einstellungen (Port Settings)

Duplexmodus

Ein Duplexkommunikationssystem ist ein System, das aus zwei miteinander verbundenen Geräten besteht, die wechselseitig miteinander kommunizieren können.

Halbduplex

In einem Halbduplexsystem kann über den gleichen Port in beide Richtungen kommuniziert werden, aber immer nur nacheinander (nicht gleichzeitig). Dabei empfängt ein Gerät ein Signal und muss dann warten, bis das andere Gerät das Senden beendet, bevor es antworten kann.

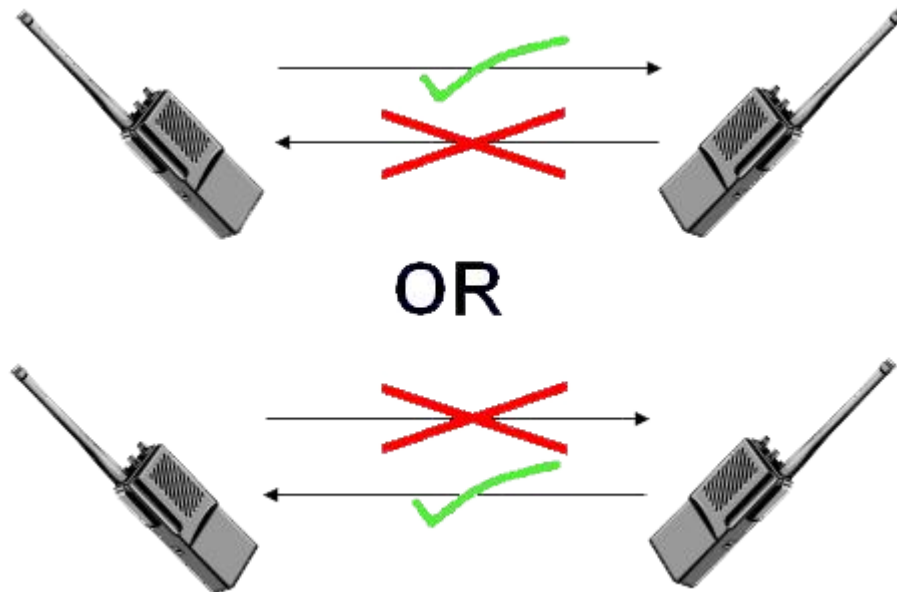


Abbildung 39: Halbduplexmodus

Vollduplex

Ein Vollduplexsystem (auch Doppelduplexsystem genannt) erlaubt die gleichzeitige Kommunikation in beide Richtungen. Beispielsweise ist das Telefonfestnetz ein Vollduplexsystem, weil dort beide Sprecher gleichzeitig sprechen und hören können.



Abbildung 40: Vollduplexmodus

Auto MDI/MDIX

MDI („**M**edium-**D**eendent Interface“) ist eine mediumabhängige Schnittstelle in der Informationstechnik und ein Teil der Sende-/Empfangseinheit (Transceiver) eines Netzwerkgerätes.

Auto-MDIX („**A**utomatic **M**edium-**D**eendent Interface **C**rossover“) ist eine im Port integrierte Netzwerktechnologie, die die erforderliche Netzkabelart („Straight-Through“- oder „Crossover“-Kabel) automatisch erkennt und die Verbindung entsprechend konfiguriert.

Dadurch werden „Crossover“-Kabel zur Verbindung von Geräten überflüssig.

Die Schnittstelle korrigiert falsche Verkabelungen automatisch.

Damit Auto-MDIX korrekt funktioniert, muss die Geschwindigkeit für die Schnittstelle und in der Duplexeinstellung auf „Auto“ eingestellt sein.

Autonegotiation

Autonegotiation ist ein Verfahren, bei dem zwei miteinander verbundene ETHERNET-Netzwerk-Ports (z. B. der Netzwerk-Port eines PC und der eines Routers, Hubs oder Switches, mit dem dieser z. B. verbunden ist) selbstständig die maximal mögliche Übertragungsgeschwindigkeit und das Duplexverfahren untereinander zu vereinbaren und konfigurieren.

Autonegotiation gilt nur für Mehrdrahtverbindungen (Twisted-Pair-Kabel) – nicht aber für WLAN-, Glasfaser- oder Koaxialkabelverbindungen.

Unterstützt der Port keine Autonegotiation oder ist diese Funktion abgeschaltet, bestimmt der Switch die Verbindungsgeschwindigkeit durch Signalerkennung am Kabel und verwendet den Halbduplexmodus.

Ist die Autonegotiation am Switch ausgeschaltet, verwendet ein Port bei der Verbindungsherstellung seine vorkonfigurierten Einstellungen für Geschwindigkeit und Duplexmodus.

Deshalb sollte sichergestellt sein, dass am Port dieselben Einstellungen vorgenommen wurden, damit die Verbindung hergestellt werden kann.

Flow Control

Die „Flow Control“ (Datenflusssteuerung) reguliert die Übertragung von Signalen, indem sie sie der Bandbreite am Eingangs-Port anpasst.

Ein hoher Datenverkehr am Port reduziert die Bandbreite und kann den Pufferspeicher überlaufen lassen, wodurch es zu Paket- und Frame-Verlusten kommen kann.

Gemäß IEEE 802.3x verwendet der Switch die „Flow Control“ im Vollduplexmodus und die „Back Pressure Flow Control“ (Gegendruck-Datenflusskontrolle) im Halbduplexmodus.

Bei der „Flow Control“ sendet der Switch im Vollduplexmodus ein Pausensignal zum Sender-Port, damit dieser vorübergehend das Senden von Signalen einstellt, wenn der Pufferspeicher des Empfänger-Ports überzulaufen droht.

Bei der „Back-Pressure Flow Control“ sendet der Switch im Halbduplexmodus ein Kollisionssignal zum Sender-Port (er imitiert sozusagen den Status einer Paketkollision), damit dieser das Senden vorübergehend einstellt und die Signale erst später erneut sendet.

Hinweis



Unterstützung des „Force-Mode“

1000 BASE-T unterstützt den „Force Mode“ nicht.

8.2 Erweiterte Einstellungen

8.2.1 Bandbreitenkontrolle

8.2.1.1 QoS

Jeder Ausgangs-Port unterstützt bis zu acht „Transmit Queues“ (Ausgabewarteschlangen). Dabei enthält jede „Transmit Queue“ eine Liste, in der die Übertragungsreihenfolge der Pakete spezifiziert ist. Jeder eingehende Frame wird zu einer der acht „Transmit Queues“ des zugewiesenen Ausgangs-Ports auf Basis seiner Priorität weitergeleitet. Der Ausgangs-Port überträgt die Pakete von jeder der acht „Transmit Queues“ entsprechend eines konfigurierbaren Abfolgealgorithmus, der aus einer Kombination aus SP („**S**trict **P**riority“, Vorrangsregelung) und/oder WRR („**W**eighted **R**ound **R**obin“, Zeitscheibenverfahren) bestehen kann.

Im Normalfall arbeiten Netzwerke nach Art der bestmöglichen Übertragungsmöglichkeit, d. h., dass jeder Datenverkehr die gleiche Priorität und gleiche Chance erhält, in angemessener Zeit übertragen zu werden. Kommt es zu Engpässen, hat so auch jeder Datenverkehr die gleiche Chance, verworfen zu werden.

Bei der Konfiguration der Funktion QoS („**Q**uality **o**f **S**ervice“, Dienstgüte) kann ein spezifischer Datenverkehr ausgewählt, ihm entsprechend seiner relativen Wichtigkeit eine Priorität zugewiesen und ein Engpassmanagement und Techniken zur Engpassvermeidung angewendet werden, um für den Datenverkehr eine Vorzugsbehandlung zu erreichen. Die Implementierung von QoS in einem Netzwerk verbessert die Vorhersagbarkeit der Netzwerkleistung und erhöht die Effizienz der Bandbreitennutzung.

Der Industrial-Managed-Switch unterstützt „802.1p Priority Queuing“ (eine Art Vorrangwarteschlange gemäß dem Standard 802.1p). Der Switch verfügt über acht „Priority Queues“. Diese sind in Klassen unterteilt, wobei Klasse 7 die höchste und Klasse 0 die niedrigste Priorität darstellt. Diese acht im Standard IEEE 802.1p (p0 bis p7) spezifizierten Prioritätsklassen sind den „Priority Queues“ des Switches wie folgt zugeordnet:

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

Das „Priority Scheduling“ (Zeitaufteilungsverfahren) wird durch die oben genannten „Priority Queues“ implementiert. Der Switch arbeitet die vier „Hardware Priority Queues“ der Reihe nach ab, wobei er mit der höchsten „Priority Queue“ (3) beginnt und mit der niedrigsten (0) endet. Jede „Hardware Queue“ überträgt alle ihre Pakete in den Puffer des Switches, bevor der nächsten niedrigeren Priorität erlaubt wird, ihre Pakete zu übertragen. Hat die niedrigste „Hardware Priority Queue“ all ihre Pakete übertragen, beginnt die höchste erneut, ihre Pakete zu übertragen, die sie zwischenzeitlich empfangen hat.

QoS-Erweiterung

Der Switch kann so konfiguriert werden, dass er einen Datenverkehr priorisiert, auch wenn die eingehenden Pakete keine „IEEE 802.1p Priority Tags“ (IEEE 802.1p-Prioritätsmarkierungen) haben oder bestehende „Priority Tags“ nach eigenen Vorgaben verändern. Der Switch ermöglicht es Ihnen, eine der folgenden Methoden zur Zuweisung von Prioritäten an eingehende Pakete anzuwenden:

- 802.1p Tag Priority
 - Weisen Sie Paketen Prioritäten auf Basis ihrer „802.1p Tag Priority“ zu.
- Port-basierter QoS
 - Weisen Sie Paketen Prioritäten auf Basis des Eingangs-Ports am Switch zu.
- DSCP-basierter QoS
 - Weisen Sie Paketen Prioritäten auf Basis ihrer DSCP („Differentiated Services Code Points“, Servicetypwerte) zu.

Hinweis**Erweiterte QoS-Methoden**

Erweiterte QoS-Methoden betreffen nur die interne Zuordnung in der „Priority Queue“ für den Switch. Der Switch nimmt keine Veränderung des IEEE 802.1p-Wertes für die Ausgangs-Frames vor.

Sie können entweder eine der oben genannten Möglichkeiten zur Änderung der Priorisierung von eingehenden Paketen nutzen oder überhaupt keine Einstellungen für die QoS-Erweiterung des Switches vornehmen.

802.1p-Priorität

Beim Einsatz des 802.1p-Prioritätsmechanismus wird überprüft, ob ein Paket einen gültigen „802.1p Priority Tag“ hat. Ist ein Tag vorhanden, wird das Paket auf Basis seines Prioritätswertes einer programmierbaren „Egress Queue“ (Ausgangswarteschlange) zugewiesen. Die „Tag Priority“ kann jeder verfügbaren „Queue“ zugewiesen werden.

ETHERNET-Paket

6	6	2	42-1496	4
DA	SA	Typ/Länge	Daten	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q-Rag	Typ/Länge	Daten	FCS

802.1Q-Tag

2 Byte		2 Byte	
Tag Protocol Identifier (TPID)		Tag Control Information (TCI)	
16 Bit		3 Bit	12 Bit
TPID (0x8100)		Priorität	VID

- **TPID („Tag Protocol Identifier“, Tag-Protokollkennung)**
Ein 16-Bit-Feld wird auf den Wert 0x8100 gesetzt, um den Frame als einen „IEEE 802.1Q Tag Frame“ zu erkennen.
- **TCI („Tag Control Information“)**
 - **PCP („Priority Code Point“, Prioritätsinformationsfeld)**
Dieses Feld belegt 3 Bit und bezieht sich auf die IEEE 802.1p-Priorität. Es zeigt die Frame-Prioritätsebene von 0 (niedrigste) bis 7 (höchste) an, wodurch unterschiedlichen Datenverkehrsklassen (Sprache, Video, Daten etc.) eine Priorität zugewiesen werden kann.
 - **CFI („Canonical Format Indicator“, Kanonischer Formatindikator)**
Dieses Feld belegt 1 Bit. Ist der Wert dieses Feldes 1, hat die MAC-Adresse ein nicht-kanonisches Format. Ist der Wert 0, hat die MAC-Adresse ein kanonisches Format. Für ETHERNET-Switches ist dieser Wert immer auf 0 gesetzt. CFI wird für die Kompatibilität zwischen ETHERNET- und „Token Ring“-Netzwerken genutzt. Wenn ein an einem ETHERNET-Port empfangener Frame einen CFI von 1 hat, sollte dieser Frame nicht an einen Port ohne Tag ausgegeben werden.
 - **VID („VLAN Identifier“, VLAN-Kennung)**
Dieses Feld belegt 12 Bit und spezifiziert das VLAN, zu dem der Frame gehört. Der Wert 0 bedeutet, dass der Frame keinem VLAN angehört und dass der „802.1Q Tag“ hier nur eine Priorität angibt und als „Priority Tag“ dient. Der Hexadezimalwert 0xFFF ist für Implementierungszwecke reserviert. Alle anderen Werte können als „VLAN Identifier“ genutzt werden, sodass bis zu 4094 VLANs unterstützt werden. In „Bridges“ wird VLAN 1 häufig für das Management reserviert.

Prioritätsebenen

PCP („**P**riority **C**ode **P**oint“):

Tabelle 49: Prioritätsebenen

PCP	Netzwerkpriorität	Datenverkehrsmerkmale
1	0 (niedrigste)	„Background“ (Hintergrund)
0	1	„Best Effort“
2	2	„Excellent Effort“
3	3	„Critical Applications“ (Kritische Anwendungen)
4	4	Video, <100 ms Latenz
5	5	Video, < 10 ms Latenz
6	6	Internetwork-Steuerung
7	7 (höchste)	Netzwerksteuerung

DiffServ (DSCP)

DiffServ („**D**ifferentiated **S**ervices“) ist eine Computernetzwerkarchitektur, die einen einfachen, skalierbaren und grobkörnigen Mechanismus zur Klassifizierung, Netzwerkverkehrsverwaltung und Bereitstellung von QoS- („**Q**uality of **S**ervice“-)Garantien in modernen IP-Netzwerken spezifiziert. DiffServ kann beispielsweise für einen GS („**G**arantierten **S**ervice“) mit geringer Latenz für kritischen Netzwerkverkehr, wie etwa Sprach- oder Videodaten, eingesetzt werden, wohingegen nicht-kritischer Datenverkehr, wie z. B. Webdaten oder Dateitransfer, einfache „Best Effort“-Garantien erhalten.

DSCP („**D**ifferentiated **S**ervices **C**ode **P**oint“) ist ein 6-Bit-Feld im Header von IP-Paketen, das der Paketklassifizierung dient. DSCP ersetzt die veraltete IP-Precedence (IP-Präzedenz) – ein 3-Bit-Feld im „Type of Service“-Byte des IP-Headers, das ursprünglich zur Klassifizierung und Priorisierung von Datenverkehrsarten eingesetzt wurde.

Beim Einsatz des DiffServ-Prioritätsmechanismus wird ein Paket auf Grundlage des DSCP-Feldes im IP-Header klassifiziert. Ist der Tag vorhanden, wird das Paket entsprechend seines „Tag Priority“-Wertes an eine programmierbare „Egress Queue“ weitergeleitet. Die „Tag Priority“ kann jeder verfügbaren „Queue“ zugeordnet werden.

Version	IHL	Type of Service (Servicetyp)	Gesamtlänge	
Kennzeichnung			Flags	Fragment Offset
Time to Live (Lebenszeit)		Protokoll	Header-Prüfsumme	
Quelladresse				
Zieladresse				
Optionen				Padding (Auffüllen)

Beispiel eines Internetdatenpaket-Headers

„Type of Service“ im IP-Header: 8 Bit

Das Feld „Type of Service“ beinhaltet Angaben zu den abstrakten Parametern der gewünschten „Quality of Service“. Diese Parameter werden zur manuellen Auswahl der eigentlichen Serviceparameter genutzt, wenn ein Datenpaket durch ein bestimmtes Netzwerk geleitet werden soll. Einige Netzwerke bieten eine Servicepräzedenz an, die Datenverkehr mit hoher Präzedenz bevorzugter behandelt als anderen Datenverkehr (im Allgemeinen akzeptieren sie bei hoher Netzwerkauslastung nur Daten ab einer ausreichend hohen Präzedenzebene). Die günstigste Auswahl ist ein Kompromiss zwischen geringer Verzögerung, hoher Zuverlässigkeit und hohem Durchsatz.

Bit 0 ... 2	Präzedenz.	
Bit 3	0 = Normale Verzögerung	1 = Geringe Verzögerung
Bit 4	0 = Normaler Durchsatz	1 = Hoher Durchsatz
Bit 5	0 = Normale Zuverlässigkeit	1 = Hohe Zuverlässigkeit
Bit 6 ... 7	Reserviert für zukünftige Nutzung.	

```

0   1   2   3   4   5   6   7   0   1   2   3
4   5   6   7

+-----+-----+-----+-----+-----+-----+-----+
| PRÄZEDENZ | D | T | R | 0 | 0 |
+-----+-----+-----+-----+-----+-----+-----+

```

Präzedenz

111 – Netzwerksteuerung
 110 – Internetwork-Steuerung
 101 – CRITIC/ECP
 100 – Flash Override
 011 – Flash
 010 – Immediate
 001 – Priorität
 000 – Routine

Das Spezifizieren der Parameter für Verzögerung, Durchsatz und Zuverlässigkeit kann die Servicekosten erhöhen. In vielen Netzwerken bedeutet die Bevorzugung einer dieser Parameter die Benachteiligung eines anderen. Abgesehen von sehr speziellen Fällen sollten in den meisten Fällen höchstens zwei dieser drei Parameter spezifiziert werden.

Die Angabe des „Type of Service“ wird genutzt, um die Art der Verarbeitung eines Datenpaketes zu spezifizieren, während es durch ein Netzwerk übertragen wird. Beispielzuordnungen des „Internet Type of Service“ zum tatsächlich bereitgestellten Service in Netzwerken, wie etwa AUTODIN II, ARPANET, SATNET und PRNET werden unter „Service Mappings“ (Servicezuordnungen) genannt.

Die Präzedenzzuordnung der Netzwerksteuerung sollte nur innerhalb eines Netzwerks verwendet werden. Die tatsächliche Verwendung und Steuerung dieser Zuordnung hängt vom jeweiligen Netzwerk ab. Die Zuordnung der Internetwork-Steuerung sollte nur von den Initiatoren der Gateway-Steuerung vorgenommen werden.

Wenn diese Präzedenzzuordnungen für ein bestimmtes Netzwerk gelten sollen, ist dieses Netzwerk für die Kontrolle von Zugriff und Verwendung dieser Zuordnungen verantwortlich.

DSCP	Priorität	DSCP	Priorität	DSCP	Priorität
0	0	1	0	2	0
...					
60	0	61	0	62	0
62	0				

Beispiel:

IP-Header

DSCP=50 -> 45 C8 ...

Queuing Algorithms

Durch „Queuing Algorithms“ (Warteschlangenalgorithmen) können Switches separate „Queues“ für Pakete einrichten, die aus jeder einzelnen Quelle oder jedem Datenfluss stammen können, und so verhindern, dass eine Quelle die Bandbreite für sich allein beansprucht.

SPQ

Beim SPQ („**S**trict **P**riority **Q**ueuing“) werden die vier „Hardware Priority Queues“ der Reihe nach abgearbeitet – zuerst die mit der höchsten Priorität (3) und zuletzt die mit der niedrigsten (0). Jede „Hardware Queue“ überträgt alle ihre Pakete in den Puffer, bevor der nächsten niedrigeren Priorität erlaubt wird, ihre Pakete zu übertragen. Hat die niedrigste „Hardware Priority Queue“ all ihre Pakete übertragen, beginnt die höchste erneut, ihre Pakete zu übertragen, die sie zwischenzeitlich empfangen hat.

WRR

RR („**R**ound **R**obin“) ist eine Art Rundlaufverfahren, das erst aktiv wird, wenn an einem Port mehr Datenverkehr ansteht als er verarbeiten kann. Dabei wird einer „Queue“ unabhängig vom eingehenden Datenverkehr an diesem Port eine begrenzte Bandbreite zur Verfügung gestellt. Daraufhin wird diese „Queue“ ans Ende der Liste gesetzt. Dann erhält die nächste „Queue“ dieselbe Bandbreite, wird ans Ende der Liste gesetzt und so weiter, bis alle „Queues“ abgearbeitet sind. Das ganze Verfahren setzt sich in einer Art Kreislauf fort, bis an einer „Queue“ kein Datenverkehr mehr ansteht.

WRR („**W**eighted **R**ound **R**obin“) nutzt die gleichen Algorithmen wie das „Round Robin“-Verfahren, nur werden die „Queues“ hier auf Basis ihrer Priorität und Gewichtung (der Wert, den Sie im Feld „Weight Value“ eintragen) eingeteilt, statt ihnen eine feste Bandbreite zuzuweisen. WRR wird nur aktiviert, wenn an einem Port mehr Datenverkehr ansteht als er verarbeiten kann. „Queues“ mit höherer Gewichtung werden bevorzugter abgearbeitet als andere mit geringerer Gewichtung. Dieser Mechanismus ist sehr effizient, weil er die gesamte verfügbare Bandbreite unter verschiedenen „Traffic Queues“ aufteilt und sie jenen zuteilt, die noch nicht abgearbeitet wurden.

Hinweis



Funktion DiffServ

DiffServ ist beim Industrial-Managed-Switch deaktiviert.

Bei Deaktivierung von DiffServ wird die „802.1p Tag Priority“ verwendet.

8.2.1.2 Rate Limitation

8.2.1.2.1 Storm Control

Wenn ein Broadcast-Sturm eintritt, wird das Netzwerk fortlaufend mit Broadcast- oder Multicast-Datenpaketen überhäuft. Broadcast-Stürme können mit zunehmender Anzahl dieser Pakete die Netzwerkkonnektivität vollständig lahmlegen.

„Storm Control“ (Sturmkontrolle) schützt die Switch-Bandbreite vor Paketüberflutungen, einschließlich Broadcast-Paketen, Multicast-Paketen und DLF („**D**estination **L**ookup **F**ailure“, Zieladressfehler). Die Rate ist ein Grenzwert, der die Gesamtanzahl bestimmter Pakettypen begrenzt. Wenn z. B. Broadcast- und Multicast-Optionen ausgewählt sind, wird die Gesamtanzahl der pro Sekunde übertragenen Pakete dieser Typen den Grenzwert nicht überschreiten.

Die „Broadcast Storm Control“ begrenzt die Anzahl von Broadcast-, Multicast- und unbekannten Unicast- (auch als „Destination Lookup Failure“- oder DLF-bezeichneten) Paketen, die vom Switch pro Sekunde an den Ports empfangen werden können. Ist die maximale Anzahl dieser Pakete pro Sekunde erreicht, werden alle nachfolgenden Pakete verworfen. Aktivieren Sie diese Funktion, wenn Sie die Anzahl dieser Pakete im Netzwerk verringern möchten.

Die Einheit der „Storm Control“ ist 625 pps (Pakete pro Sekunde).

8.2.1.2.2 Bandbreitenbegrenzung (Rate Limitation)

Die „Rate Limitation“ dient zur Steuerung der Rate von Daten, die an einer Netzwerkschnittstelle empfangen oder übertragen werden können.

8.2.2 IGMP Snooping

Das „IGMP Snooping“ („Internet **G**roup **M**anagement **P**rotocol **S**nooping“) wird für Multicast-Datenverkehr eingesetzt. Der Switch kann dabei passiv an den IGMP-Paketen „schnüffeln“, die zwischen IP-Multicast-Routern bzw. -Switches und IP-Multicast-Hosts übertragen werden, um so ihre Zugehörigkeit zu einer IP-Multicast-Gruppe zu erkennen. „IGMP Snooping“ ermöglicht es einem Switch, Multicast-Gruppen zu erkennen, ohne dass diese erst von einem Benutzer manuell konfiguriert werden müssen.

Er überprüft die durch ihn geleiteten IGMP-Pakete, liest ihre Gruppenanmeldeinformationen aus und konfiguriert das Multicasting entsprechend.

Der Switch leitet den Multicast-Datenverkehr an seine Multicast-Zielgruppen (die er durch das „IGMP Snooping“ oder Ihre manuelle Konfiguration erkannt hat) über Ports weiter, die Mitglieder dieser Gruppen sind. „IGMP Snooping“ erzeugt keinen zusätzlichen Netzwerkverkehr, sodass der durch den Switch geleitete Multicast-Datenverkehr deutlich reduziert werden kann.

Der Switch kann „IGMP Snooping“ bei bis zu 4094 VLANs ausführen. Sie können den Switch so konfigurieren, dass er die Zugehörigkeit zu Multicast-Gruppen in allen VLANs automatisch erkennt. Der Switch führt dann das „IGMP Snooping“ in den ersten VLANs aus, die IGMP-Pakete senden.

Dieser Modus wird als Automodus bezeichnet. Alternativ dazu können Sie VLANs, in denen „IGMP Snooping“ ausgeführt werden soll, auch selbst spezifizieren. Dies wird dann als „Fixed Mode“ bezeichnet. In diesem „Fixed Mode“ wird der Switch nur in den VLANs Multicast-Gruppenzugehörigkeiten erkennen, die Sie zuvor eindeutig als eine „IGMP Snooping“-VLAN hinzugefügt haben.

Immediate Leave

Wenn Sie den „IGMP Immediate Leave“-Befehl aktivieren, wird der Switch einen Port sofort entfernen, sobald er eine „Leave Message“ mit IGMP-Version 2 an diesem Port empfängt. Sie sollten die „Immediate Leave“-Funktion nur dann einsetzen, wenn es an jedem Port im VLAN nur einen einzigen Empfänger gibt („Immediate Leave“ wird nur von Hosts mit IGMP-Version 2 unterstützt).

Der Switch nutzt die „Immediate Leave“-Funktion beim „IGMP Snooping“, um eine Schnittstelle aus der Weiterleitungstabelle zu entfernen, die eine „Leave Message“ sendet, ohne dass der Switch gruppenspezifische Anfragen an die Schnittstelle senden muss. Die VLAN-Schnittstelle wird aus dem Multicast-Verzeichnis der Multicast-Gruppe gelöscht, die in der ursprünglichen „Leave Message“ spezifiziert wurde. „Immediate Leave“ gewährleistet ein optimales Bandbreitenmanagement für alle Hosts in einem vermittelten Netzwerk, auch wenn mehrere Multicast-Gruppen gleichzeitig betrieben werden.

Fast Leave

Der Switch ermöglicht die Konfiguration einer Verzögerungszeit. Nach Ablauf dieser Zeit entfernt der Switch eine Schnittstelle aus der Multicast-Gruppe.

Last Member Query Interval

Das „Last Member Query Interval“ (Abfrageintervall des letzten Mitglieds) ist die maximale Antwortzeit, die in gruppenspezifischen Abfragen als Antwort auf „Leave Group“-Nachrichten gesendet wird, und zeigt außerdem auch die Dauer zwischen gruppenspezifischen Abfragemeldungen an.

Wenn der Switch ohne aktivierte „Immediate Leave“-Funktion eine „IGMP Leave Message“ von einem Teilnehmer an einem Empfänger-Port empfängt, sendet er eine IGMP-spezifische Abfrage an diesen Port und wartet auf die IGMP-Gruppenmitgliedschaftsmeldungen. Empfängt er innerhalb einer konfigurierten Zeit keine Meldungen, wird der Empfänger-Port aus der Multicast-Gruppe ausgeschlossen.

IGMP Querier

Pro physischem Netzwerk gibt es normalerweise nur einen „Querier“ (Abfrager). Alle Multicast-Router beginnen ihren Betrieb als „Querier“ für jedes angeschlossene Netzwerk. Wenn ein Multicast-Router eine „Query Message“ von einem Router mit niedrigerer IP-Adresse empfängt, MUSS er zu einem Nicht-„Querier“ in diesem Netzwerk werden. Wenn ein Router über einen bestimmten Zeitraum [„Other Querier Present Interval“, Abfrageintervall nach Präsenz anderer „Querier“] keine „Query Message“ von einem anderen Router empfängt, übernimmt er die Rolle als „Querier“. Router senden regelmäßig [„Query Interval“] eine „General Query“ (allgemeine Abfrage) in alle angeschlossenen Netzwerke, für den der Router der „Querier“ ist, um Mitgliedschaftsinformationen zu sammeln. Bei der Inbetriebnahme SOLLTE ein Router „General Queries“ senden [„Startup Query Count“, „Query“-Anzahl bei Inbetriebnahme], die zeitlich eng beieinander liegen [„Startup Query Interval“, „Query Interval“ bei Inbetriebnahme], damit er schnell und zuverlässig Mitgliedschaftsinformationen erfassen kann. Eine „General Query“ richtet sich an eine All-Systems-Multicast-Gruppe (224.0.0.1), hat einen Gruppenadressfeldwert von 0 und hat eine maximale Antwortzeit von [„Query Response Interval“, „Query“-Antwortintervall].

Port IGMP Querier Mode

- Auto
 - Der Switch nutzt den Port als „IGMP Query Port“, wenn der Port „IGMP Query“-Pakete empfängt.
- Fixed
 - Der Switch wird den/die Port(s) immer als „IGMP Query Port(s)“ nutzen. Dieser Modus wird verwendet, wenn ein IGMP-Multicast-Server mit dem/den Port(s) verbunden wird.
 - Der Switch wird die „Report/Leave“-Pakete des Clients immer an den Port weiterleiten. Normalerweise ist der Port mit einem IGMP-Server verbunden.
- Edge
 - Der Switch wird den Port nicht als „IGMP Query Port“ nutzen.
 - Die an diesem Port empfangenen „IGMP Query“-Pakete werden verworfen. Normalerweise ist der Port mit einem IGMP-Client verbunden.

Hinweis



Weiterleiten der „IGMP Join/Leave“-Pakete

Der Industrial-Managed-Switch wird die „IGMP Join/Leave“-Pakete an den Query-Port weiterleiten.

IGMP Proxy Snooping

Durch „IGMP Proxy Snooping“ kann die Anzahl der durch einen IGMP-Router gesendeten „Reports“ und „Leaves“ reduziert werden.

Konfigurationen

Der Benutzer kann „IGMP Snooping“ am Switch aktivieren bzw. deaktivieren. Dies gilt auch für spezifische VLANs. Wird „IGMP Snooping“ am Switch deaktiviert, wird es für alle VLANs deaktiviert, auch wenn bei einigen VLANs das „IGMP Snooping“ aktiviert ist.

Hinweis



VLAN-Zustände

Es gibt einen globalen Zustand und einzelne VLAN-Zustände. Wird der globale Zustand deaktiviert, wird das „IGMP Snooping“ am Switch deaktiviert, auch wenn einzelne VLAN-Zustände aktiviert wurden. Wird der globale Zustand für das „IGMP Snooping“ aktiviert, muss diese Funktion für spezifische VLANs vom Benutzer einzeln aktiviert werden.

8.2.2.1 Multicast-Adresse

Eine Multicast-Adresse bezieht sich auf eine Gruppe interessierter Empfänger. Gemäß dem Standard RFC 3171 sind die Adressen 224.0.0.0 bis 239.255.255.255 (ehemals Klasse-D-Adressen) in IPv4 als Multicast-Adressen reserviert.

Das erste Oktett (01) beinhaltet das Broadcast-/Multicast-Bit. Die unteren 23 Bit der 28-Bit-Multicast-IP-Adresse werden in die 23 Bit des verfügbaren ETHERNET-Adressraumes zugeordnet. Dies stellt eine Mehrdeutigkeit bei der Übertragung von Paketen dar. Wenn sich zwei Hosts im selben Subnetz bei unterschiedlichen Multicast-Gruppen anmelden, deren Adressen sich nur in den ersten 5 Bit unterscheiden, werden beide ETHERNET-Pakete für beide Multicast-Gruppen an beide Hosts gesendet. Die Netzwerksoftware muss in den Host die jeweils nicht benötigten Pakete verwerfen.

Tabelle 50: Multicast-Klassen und -Adressbereiche

Klasse	Adressbereich	Unterstützung
Klasse A	1.0.0.1 bis 126.255.255.254	Unterstützung für 16 Millionen Hosts in jedem der 127 Netzwerke
Klasse B	128.1.0.1 bis 191.255.255.254	Unterstützung für 65.000 Hosts in jedem der 16.000 Netzwerke
Klasse C	192.0.1.1 bis 223.255.254.254	Unterstützung für 254 Hosts in jedem der 2 Millionen Netzwerke
Klasse D	224.0.0.0 bis 239.255.255.255	Reserviert für Multicast-Gruppen.
Klasse E	240.0.0.0 bis 254.255.255.254	Reserviert für zukünftige Nutzung oder für Forschungs- und Entwicklungszwecke.

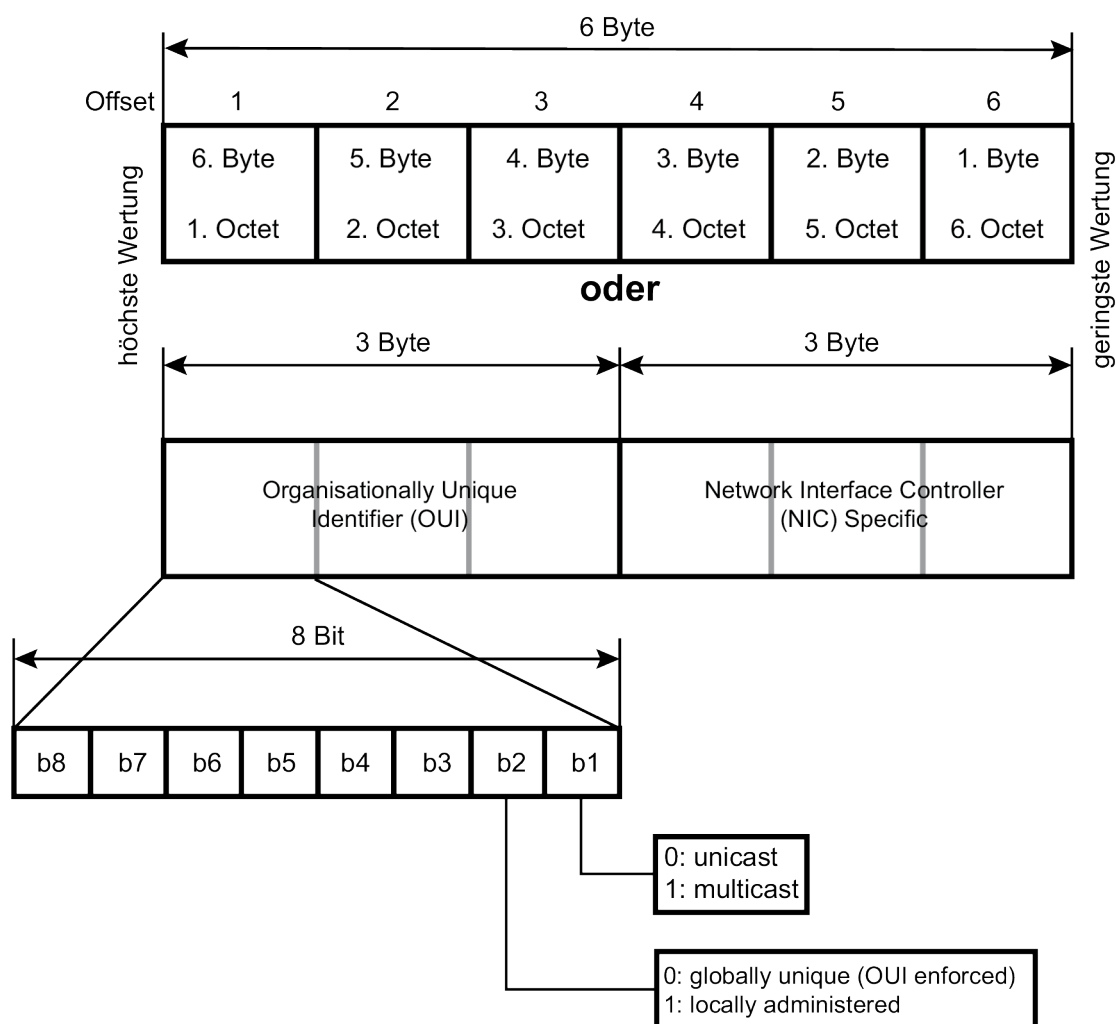


Abbildung 41: Multicast-Adresse

Tabelle 51: IP-Multicast-Adressen

IP-Multicast-Adresse	Beschreibung
224.0.0.0	Basisadresse (reserviert)
224.0.0.1	„All Hosts Multicast“-Gruppe, die alle Systeme im selben Netzwerksegment enthält
224.0.0.2	„All Routers Multicast“-Gruppe, die alle Router im selben Netzwerksegment enthält
224.0.0.5	„Open Shortest Path First“ (OSPF-Protokoll), die „All OSPF Routers“-Adresse Diese Adresse wird zum Senden von „Hello-Paketen“ an alle OSPF-Router in einem Netzwerksegment verwendet.
224.0.0.6	Die „OSPF All DR Routers“-Adresse Diese Adresse wird zum Senden von OSPF-Routing-Informationen an „OSPF Designated Router“ in einem Netzwerksegment verwendet.

Tabelle 51: IP-Multicast-Adressen

IP-Multicast-Adresse	Beschreibung
224.0.0.9	RIP („Routing Information Protocol“) Version 2 der Gruppenadresse Dieses Protokoll wird zum Senden von Routing-Informationen an alle RIPv2-kompatiblen Router in einem Netzwerksegment verwendet.
224.0.0.10	EIGRP-Gruppenadresse Diese Adresse wird zum Senden von EIGRP-Routing-Informationen an alle EIGRP-Router in einem Netzwerksegment verwendet.
224.0.0.13	PIM Version 2 („Protocol Independent Multicast“)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 („Internet Group Management Protocol“)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast-DNS-Adresse
224.0.0.252	„Link-local Multicast Name Resolution“-Adresse
224.0.1.1	„Network Time Protocol“-Adresse
224.0.1.39	„Cisco Auto-RP-Announce“-Adresse
224.0.1.40	„Cisco Auto-RP-Discovery“-Adresse
224.0.1.41	„H.323 Gatekeeper Discovery“-Adresse

8.2.3 VLAN

Ein VLAN („**Virtuelles LAN**“) ist eine Gruppe aus Hosts mit einheitlichen Anforderungen, die unabhängig von ihrem physischen Standort so kommunizieren als würden sie einer Broadcast-Domäne angehören. Ein VLAN hat die gleichen Attribute wie ein physisches LAN, aber es ermöglicht die Gruppierung von Endstationen, auch wenn sich diese nicht am selben Netzwerk-Switch befinden. Die Neukonfiguration des Netzwerks kann so über Software, statt über räumlich versetzte Geräte erfolgen.

VID („**VLAN-ID**“) ist die Kennzeichnung des VLANs, die im Wesentlichen vom Standard IEEE 802.1Q verwendet wird. Sie besteht aus 12 Bit und ermöglicht die Kennzeichnung von 4096 (2^{12}) VLANs. Von den 4096 möglichen VIDs wird die VID 0 zur Kennzeichnung von „Priority Frames“ verwendet und der Wert 4095 (FFF) reserviert, sodass maximal 4094 VLAN-Konfigurationen möglich sind.

Ein „Tagged VLAN“ (VLAN mit Tag) nutzt einen eindeutigen Tag (die VLAN-ID) im MAC-Header, um die VLAN-Zugehörigkeit eines Frames unabhängig von den „Bridges“ zu identifizieren, ganz gleich, auf welchem Switch der Tag erzeugt wurde. VLANs können statisch (manuell durch Benutzer) oder dynamisch über das GVRP („GARP VLAN Registration Protocol“) eingerichtet werden. Die VLAN-ID ordnet ein Frame einem bestimmten VLAN zu und stellt die Informationen bereit, die Switches zur Verarbeitung des Frames innerhalb des Netzwerks benötigen. Ein Frame mit Tag ist vier Byte länger als ein Frame ohne Tag und enthält zwei Byte für den TPID (den „Tag Protocol Identifier“, der sich im Feld Typ/Länge des „ETHERNET Frames“ befindet) und zwei Byte für die TCI (die „Tag Control Information“, die nach dem Quelladressfeld des „ETHERNET Frames“ beginnt).

Der CFI („Canonical Format Indicator“) ist ein 1-Bit-Datenfeld, dessen Wert für ETHERNET-Switches immer 0 ist. Wenn ein an einem ETHERNET-Port empfangener Frame einen CFI von 1 hat, sollte dieser Frame nicht an einen Port ohne Tag übermittelt werden. Die verbleibenden 12 Bit definieren die VLAN-ID, womit sich eine mögliche Anzahl von maximal 4096 VLANs ergibt. Hier gilt zu beachten, dass Benutzerpriorität und VLAN-ID unabhängig voneinander sind. Ein Frame mit einer VID (VLAN-Identifizier) von null (0) wird als „Priority Frame“ bezeichnet, d. h., dass nur die Prioritätsebene relevant ist und die Default-VID des Eingangs-Ports als VID des Frames verwendet wird. Bei den möglichen 4096 VIDs wird eine VID von 0 zur Identifikation von „Priority Frames“ verwendet und der Wert 4095 (FFF) reserviert, sodass maximal 4094 VLAN-Konfigurationen möglich sind.

TPID	Benutzerpriorität	CFI	VLAN-ID
2 Byte	3 Bit	1 Bit	12 Bit

- **Weitergeleitete Frames mit und ohne Tag**

Jeder Port des Switches kann Frames mit und ohne Tags weiterleiten. Bei der Weiterleitung eines Frames von einem 802.1Q-VLAN-unterstützenden Switch zu einem ohne diese Unterstützung, muss der Switch zuerst entscheiden, wohin er den Frame weiterleitet und dann den VLAN-Tag entfernen. Im umgekehrten Fall muss der Switch zuerst entscheiden, wohin er den Frame weiterleitet und dann den VLAN-Tag hinzufügen, der der Default-ID des Eingangs-Ports entspricht. Die Default-PVID für alle Ports ist „VLAN 1“, was aber geändert werden kann.

Ein Broadcast-Frame (oder ein Multicast-Frame für eine Multicast-Gruppe, die dem System bekannt ist) wird nur für Ports dupliziert, die Teilnehmer der VID sind (außer dem Eingangs-Port selbst) und somit auf eine spezifische Domäne begrenzt.

- **Port-basiertes 802.1Q-VLAN**

Als Teilnehmer eines port-basierten VLANs wird der Port einem spezifischen VLAN zugewiesen, unabhängig davon, welcher Benutzer oder welches Gerät mit dem Port verbunden ist. Das bedeutet, dass alle mit diesem Port verbundenen Benutzer Teilnehmer desselben VLANs sind. Normalerweise nimmt der Netzwerkadministrator die VLAN-Zuordnung vor. Die Port-Konfiguration ist statisch und kann nicht automatisch in ein anderes VLAN verändert werden, ohne dass eine manuelle Neukonfiguration durchgeführt wird.

Wie auch bei anderen VLAN-Verfahren können die mit dieser Methode weitergeleiteten Pakete nicht in andere VLAN-Domänen oder Netzwerke übertragen werden. Nachdem ein Port einem VLAN zugewiesen wurde, kann er ohne Einsatz eines Layer-3-Gerätes keine Daten von Geräten eines anderen VLANs empfangen oder an sie senden.

Das an den Port angeschlossene Gerät kann nicht erkennen, dass ein VLAN vorhanden ist. Das Gerät erkennt lediglich, dass es Teil eines Subnetzes ist und mit allen anderen Netzteilnehmern kommunizieren kann, indem es einfach Informationen über die Kabelverbindung sendet. Der Switch ist für die Identifikation von Informationen verantwortlich, die aus einem spezifischen VLAN stammen, und muss sicherstellen, dass diese Informationen zu allen Teilnehmern des VLANs übertragen werden. Außerdem muss der Switch sicherstellen, dass diese Information nicht von Ports aus einem anderen VLAN empfangen werden können.

Dieser Ansatz ist simpel, schnell und einfach zu verwalten, weil er keine komplexen Zuordnungstabellen für die VLAN-Segmentierung benötigt. Wenn die „Port-to-VLAN“-Verbindung mit einem „**A**pplication-**S**pecific **I**ntegrated **C**ircuit“ (ASIC, einer anwendungsspezifischen integrierten Schaltung) ausgeführt wird, bringt dies große Leistungsvorteile. Ein ASIC ermöglicht eine „Port-to-VLAN“-Zuordnung auf Hardwareebene.

8.2.3.1 Port-Isolation

Die „Port-Isolation“ (Port-Trennung) ist eine port-basierte, virtuelle LAN-Funktion. Sie partitioniert die vermittelnden Ports in virtuelle private Domänen, die einzeln zugewiesen werden. Eine Datenvermittlung außerhalb der privaten Domäne des Switches ist nicht erlaubt. Die VLAN-Tag-Informationen der Pakete werden ignoriert.

Mit dieser Funktion können für jeden Port ein oder mehrere Ausgangs-Ports konfiguriert werden, um für diesen spezifischen Port die von ihm empfangenen Daten weiterzuleiten. Wenn der CPU-Port (Port 0) kein Ausgangs-Port für einen spezifischen Port ist, kann der mit dem spezifischen Port verbundene Host den Switch nicht verwalten.

Wenn Sie die Kommunikation zwischen 2 Teilnehmer-Ports zulassen möchten, müssen Sie den Ausgangs-Port für beide Ports definieren. CPU bezeichnet den Management-Port des Switches. Er bildet standardmäßig ein VLAN mit allen ETHERNET-Ports. Wenn er mit einem spezifischen Port kein VLAN bildet, kann der Switch nicht über diesen Port verwaltet werden.

8.2.4 LLDP

Das in diesem Standard beschriebene LLDP („**L**ink **L**ayer **D**iscovery **P**rotocol“) ermöglicht es Stationen, die mit einem LAN gemäß IEEE 802 verbunden sind, Informationen an andere, an dasselbe LAN angeschlossene Stationen, zu senden. Diese Informationen beinhalten wesentliche Funktionen des Systems dieser Station, einschließlich der Managementadresse oder Adressen einer Entität oder Entitäten, die das Management dieser Funktionen bereitstellen, sowie die Identifizierung des Stationszugangspunktes zum IEEE802-LAN, den diese Managemententität oder -entitäten benötigen.

Die durch dieses Protokoll verteilten Informationen werden von den Empfängern in einer normalen MIB („**M**anagement **I**nformation **B**ase“) gespeichert. Dadurch wird einem NMS („**N**etwork **M**anagement **S**ystem“) ermöglicht, mittels eines Managementprotokolls, wie etwa dem SNMP („**S**imple **N**etwork **M**anagement **P**rotocol“), auf diese Informationen zuzugreifen.

8.2.5 MAC based VLAN

Das MAC-basierte VLAN ermöglicht es Benutzern, einzelne Datenpakete aufgrund der MAC-Adresse einem VLAN priorisiert zuzuordnen.

8.2.6 Schleifenerkennung (Loop Detection)

Die „Loop Detection“ (Schleifenerkennung) behandelt Probleme mit Schleifen in der Netzwerkperipherie. Diese Probleme können entstehen, wenn ein Port mit einem Switch verbunden ist, der sich in einem Schleifenzustand befindet. Ein Schleifenzustand entsteht durch Benutzerfehler. Dies tritt auf, wenn zwei Ports an einem Switch mit demselben Kabel verbunden sind. Wenn ein Switch im Schleifenzustand Broadcast-Nachrichten sendet, werden diese zum Switch zurückgeleitet und immer wieder und wieder erneut gesendet, sodass ein sogenannter „Broadcast-Sturm“ entsteht.

Die „Loop Detection“ sendet regelmäßig spezielle Multicast-Pakete, um zu erkennen, ob der Port mit einem Netzwerk im Schleifenzustand verbunden ist. Der Switch schaltet einen Port ab, wenn er erkennt, dass diese speziellen Multicast-Pakete wieder zum selben Port zurückgeleitet werden.

Loop Recovery

Bei aktivierter „Loop Detection“ sendet der Switch alle zwei Sekunden ein Sondenpaket und wartet auf den Empfang dieses Pakets. Empfängt er das Paket am selben Port, deaktiviert er diesen Port. Nach einem bestimmten Zeitraum, der „Recovery Time“ (Wiederherstellungszeit), aktiviert er den Port wieder und führt die „Loop Detection“ erneut aus.

Der Switch erstellt ein „Syslog“ (Systemprotokoll), interne Protokollnachrichten und auch „SNMP Traps“ (SNMP-Überwachungsdateien), wenn er einen Port nach einer „Loop Detection“ deaktiviert hat.

8.2.7 STP

Das (R)STP („**R**apid **S**panning **T**ree **P**rotocol“) kann Netzwerkschleifen erkennen und aufbrechen sowie „Back-up Links“ (Ersatzverbindungen) zwischen Switches, Bridges oder Routern bereitstellen. Es ermöglicht einem Switch, mit anderen (R)STP-fähigen Switches im Netzwerk zu interagieren, um sicherzustellen, dass zwischen zwei gegebenen Stationen im Netzwerk immer nur eine Verbindung besteht.

Der Switch unterstützt sowohl das STP als auch das RSTP, wie sie in den folgenden Standards definiert sind:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

Der Switch nutzt das IEEE 802.1w RSTP, das eine schnellere Konvergenz des „Spanning Tree“ ermöglicht als das STP (der Switch ist auch abwärtskompatibel mit nur STP-fähigen Bridges). Mit dem RSTP werden Informationen über Topologieänderungen direkt von dem Gerät durch das Netzwerk propagiert, das eine Topologieänderung verursacht hat. Beim STP gibt es größere Verzögerungen, weil das Gerät, das eine Topologieänderung verursacht, zuerst die „Root Bridge“ benachrichtigt und diese dann das Netzwerk. Sowohl das RSTP als auch das STP entfernen ungewollt erlernte Adressen aus der Filterdatenbank.

- Beim STP gibt es die Port-Zustände „Blocking“, „Listening“, „Learning“ und „Forwarding“.
- Beim RSTP gibt es die Port-Zustände „Discarding“, „Learning“ und „Forwarding“.

Port-Zustände bei STP-Switches

- **„Blocking“**
Wenn ein Port einen „Switching Loop“ (eine Schleifenverbindung zwischen zwei Ports) erzeugt, können keine Benutzerdaten mehr gesendet oder empfangen werden. Der Port kann aber in den Zustand „Forwarding“ (Weiterleitungsmodus) übergehen, sofern die anderen aktiven Verbindungen ausfallen und der Algorithmus des „Spanning Tree“ bestimmt, dass der Port in diesen Modus übergehen darf. Im Zustand „Blocking“ können immer noch BPDU-Daten empfangen und gesendet werden.
- **„Listening“**
Der Switch verarbeitet BPDUs und wartet auf mögliche neue Informationen, durch die er in den Zustand „Blocking“ zurückversetzt werden würde.
- **„Learning“**
Auch wenn der Port noch keine Frames (Pakete) weiterleitet, kann er Quelladressen von empfangenen Frames erlernen und sie der Filterdatenbank („Switching Database“) hinzufügen.

- **„Forwarding“**
Der Port ist im normalen Betriebsmodus und empfängt und sendet Daten. Das STP überwacht eingehende BPDUs daraufhin, ob sie anzeigen, dass der Port in den Zustand „Blocking“ übergehen soll, um eine Schleife zu verhindern.
- **„Disabled“**
Dies ist, genau genommen, kein Teil des STP, da ein Netzwerkadministrator einen Port manuell deaktivieren kann.

Port-Rollen bei RSTP-Bridges

- **„Root“**
Der „Root Port“ ist ein weiterleitender Port, der Daten von der „Non-Root Bridge“ zur „Root Bridge“ am besten übertragen kann.
- **„Designated“**
Dies ist ein weiterleitender Port für jedes LAN-Segment.
- **„Alternate“**
Dieser Port stellt einen alternativen Pfad zur „Root Bridge“ dar. Der Pfad verläuft jedoch anders als beim „Root Port“.
- **„Backup“**
Dieser Port dient als Ersatz-/redundanter Pfad zu einem Segment, mit dem ein anderer „Bridge Port“ bereits verbunden ist.
- **„Disabled“**
Dies ist eigentlich kein Teil des STP, da ein Netzwerkadministrator einen Port manuell deaktivieren kann.

Hinweis



STP/RSTP

In diesem Dokument bezieht sich die Bezeichnung „STP“ sowohl auf das STP als auch auf das RSTP.

STP-Terminologie

Root Bridge

Die „Root Bridge“ ist die „Base“ (Wurzel) des sich aufspannenden Baumes.

Path Cost

Die Pfadkosten („Path Cost“) sind die Kosten für die Übertragung eines Frames durch den Port in das LAN. Dabei sollte dieser Wert an die Übertragungsgeschwindigkeit angepasst werden.

Der gültige Bereich liegt bei 1 bis 200000000. Es ist wahrscheinlicher, dass ein Pfad mit höheren Kosten vom STP blockiert wird, wenn eine Netzwerkschleife erkannt wird.

- **„Path Cost Short“** ist die ursprüngliche Größe mit einem 16-Bit-Wert. Damit kann nur eine Geschwindigkeit bis 10 GBit berücksichtigt werden.
- **„Path Cost Long“** steht für einen 32-Bit-Wert. Damit wird eine Geschwindigkeit bis zu 10 TBit unterstützt.

Tabelle 52: STP-Pfadkosten

Übertragungs- geschwindigkeit	Empfohlener Wert	Empfohlener Bereich	Zulässiger Bereich
4 MBit/s	250	100 ... 1000	1 ... 65535
10 MBit/s	100	50 ... 600	1 ... 65535
16 MBit/s	62	40 ... 400	1 ... 65535
100 MBit/s	19	10 ... 60	1 ... 65535
1 GBit/s	4	3 ... 10	1 ... 65535
10 GBit/s	2	1 ... 5	1 ... 65535

- Jede „Bridge“ kommuniziert mit der „Root Bridge“ über den „Root Port“. Der „Root Port“ ist der Port am Switch mit den geringsten Pfadkosten zur „Root Bridge“ (die „Root Path Cost“). Wenn es keinen „Root Port“ gibt, wird der Switch zur „Root Bridge“ für das „Spanning Tree“-Netzwerk.
- Für jedes LAN-Segment wird eine „Designated Bridge“ ausgewählt. Unter allen mit dem LAN verbundenen Bridges hat sie die geringsten Pfadkosten zur „Root Bridge“.

Forward Time (Forward Delay)

Die „Forward Time“ (Weiterleitungszeit) ist die maximale Zeit (in Sekunden), die der Switch wartet, bevor er Zustände ändert. Diese Verzögerung ist erforderlich, weil jeder Switch erst Informationen über Topologieänderungen empfangen muss, bevor er Frames weiterleitet. Außerdem benötigt jeder Port Zeit, um Informationen über Konflikte zu empfangen, die ihn zurück in den blockierten Zustand versetzen würden – anderenfalls könnten vorübergehende Datenschleifen entstehen. Der gültige Bereich ist 4 bis 30 Sekunden.

Max Age

Das „Max Age“ (Maximales Alter) ist die maximale Zeit (in Sekunden), die der Switch ohne eine BPDU („**B**ridge **P**rotocol **D**ata **U**nit“, Konfigurationsnachricht) zu empfangen, warten kann, bevor er versucht, mit der Rekonfiguration zu beginnen. Alle Switch-Ports (außer „Designated Ports“) empfangen in regelmäßigen Abständen BPDUs. Jeder Port, der STP-Informationen (aus der letzten BPDU) verlernt, wird zum „Designated Port“ für das angeschlossene LAN. Wenn dies ein „Root Port“ ist, wird aus den an das Netzwerk angeschlossenen Switch-Ports ein neuer „Root Port“ gewählt.

Hello Time

Die „Hello Time“ ist das Zeitintervall in Sekunden zwischen den vom Root-Switch versendeten Konfigurationsnachrichten (BPDU „Bridge Protocol Data Unit“).

STP

Nachdem eine Bridge den kostengünstigsten „Spanning Tree“ mit dem STP bestimmt hat, aktiviert sie den „Root Port“ und die „Designated Ports“ für die angeschlossenen LANs und deaktiviert alle anderen am STP beteiligten Ports. Daher werden Netzwerkpakete nur zwischen aktivierten Ports weitergeleitet und mögliche Netzwerkschleifen können verhindert werden.

STP-fähige Switches tauschen regelmäßig BPDUs untereinander aus. Wenn sich in einem per Bridge gekoppelten LAN die Topologie ändert, wird ein neuer Baum aufgespannt. Sobald eine stabile Netzwerktopologie eingerichtet ist, warten alle Bridges auf „Hello BPDUs“, die von der „Root Bridge“ übertragen werden. Wenn eine Bridge nach einem zuvor definierten Intervall („Max Age“) keine „Hello BPDUs“ empfängt, geht die Bridge davon aus, dass die Verbindung zur „Root Bridge“ unterbrochen ist. Daraufhin beginnt die Bridge-Negotiation mit anderen Bridges, um das Netzwerk neu zu konfigurieren und wieder eine gültige Netzwerktopologie einzurichten.

Edge Port

„Edge Ports“ sind mit einem LAN verbunden, an das keine anderen Bridges angeschlossen sind. Diese Ports können direkt in den Zustand „Forwarding“ übergehen. Das RSTP überwacht diese Ports dennoch auf Empfang von BPDUs, falls eine Bridge angeschlossen wird. RSTP kann so konfiguriert werden, dass es „Edge Ports“ automatisch erkennt. Sobald die Bridge erkennt, dass eine BPDU bei einem „Edge Port“ eingeht, verliert dieser seinen Status als „Edge Port“.

Forward Delay

Die „Forward Delay“ (Weiterleitungsverzögerung) ist die maximale Zeit (in Sekunden), die das Root-Gerät wartet, bevor es Zustände ändert (z. B. von „Listening“ zu „Learning“ zu „Forwarding“). Der gültige Bereich liegt bei 4 bis 30 Sekunden.

Transmission Limit

Mit dem „Transmission Limit“ (Übertragungsgrenze) wird das minimale Intervall zwischen der Übertragung aufeinanderfolgender RSTP-BPDUs konfiguriert. Diese Funktion kann nur im RSTP-Modus aktiviert werden. Der gültige Bereich liegt bei 1 bis 10 Sekunden.

Bridge Priority

Über die „Bridge Priority“ (Priorität der Bridge) wird die Auswahl des Root-Switches, des Root-Ports und des „Designated Ports“ bestimmt. Der Switch mit der höchsten Priorität wird zum STA-Root-Switch. Haben jedoch alle Switches die gleiche Priorität, wird der Switch mit der niedrigsten MAC-Adresse das Root-Switch.

Port-Priorität

Die Port-Priorität wird im Switch konfiguriert. Ein niedriger numerischer Wert zeigt eine hohe Priorität an. Es ist wahrscheinlicher, dass ein Port mit geringerer Priorität vom STP blockiert wird, wenn eine Netzwerkschleife erkannt wird. Der gültige Bereich liegt bei 0 bis 240.

BPDU Guard

Diese Einstellung wird für jeden Port einzeln konfiguriert. Wenn der Port im „BDU Guard“ aktiviert ist und eine BPDU empfängt, wird er in den Zustand „Disabled“ wechseln, um eine fehlerhafte Umgebung zu vermeiden. Der Benutzer muss den Port manuell aktivieren.

BPDU Filter

Mit dieser Funktion wird ein Filter für das Senden oder Empfangen von BPDUs in einem Switch-Port eingerichtet. Wenn ein Port BPDUs empfängt, werden diese verworfen. Bei gleichzeitiger Aktivierung von „BPDU Filter“ und „BPDU Guard“ hat ersterer die höhere Priorität.

Hinweis

BPDU Filter und BPDU Guard

Bei gleichzeitiger Aktivierung von „BPDU Filter“ und „BPDU Guard“ hat ersterer die höhere Priorität.

Root Guard

Die Funktion „Root Guard“ zwingt eine Schnittstelle dazu, ein „Designated Port“ zu werden, um zu verhindern, dass benachbarte Switches zu einem Root-Switch werden. Diese Funktion bietet eine Möglichkeit, die Auswahl der „Root Bridge“ in einem Netzwerk festzulegen. Sie verhindert, dass ein „Designated Port“ zum „Root Port“ werden kann. Wenn ein Port mit der Funktion „Root Guard“ eine höherwertige BPDU empfängt, wird der Port in einen Root-inkonsistenten (praktisch dem Zustand „Listening“ gleichzusetzenden) Zustand versetzt, um so den Status der aktuellen „Root Bridge“ aufrechtzuerhalten. Der Port kann in den Zustand „Forwarding“ übergehen, wenn er über den Zeitraum von drei „Hello Times“ keine höherwertigen BPDUs mehr empfängt.

MSTP

Das MSTP („**M**ultiple **S**panning **T**ree **P**rotocol“) ist eine Erweiterung des RSTPs. Es ermöglicht im Zusammenhang mit VLANs („Virtual Local Area Networks“) verschiedene Instanzen des „Spanning Trees“.

Für ein VLAN oder eine Gruppe von VLANs können also voneinander unabhängige STP-Instanzen gebildet werden, die innerhalb eines LANs jeweils eigene unterschiedliche Spannbäume nutzen.

Beim MSTP-Verfahren wird eine Root-Bridge bestimmt und die geringsten Streckenkosten zwischen der Root-Bridge und den angebotenen Root-Ports der einzelnen Brücken. Die Root-Bridge sendet „**B**ridge **P**rotocol **D**ata **U**nits“ (BPDU) an alle Bridges und stellt über die in den BPDU-Datenpaketen enthaltenen Konfigurationsdaten die Netzkonfiguration fest.

8.3 Sicherheit

8.3.1 Zugriffskontrollliste ACL

Die ACL („**A**ccess **C**ontrol **L**ist“, Zugriffskontrollliste) ist eine Liste mit Berechtigungen, die an ein Objekt angehängt ist. Sie spezifiziert, wer oder was Zugriff auf ein Objekt erhält und welche Operationen mit dem Objekt durchgeführt werden dürfen.

Die ACL-Funktion ermöglicht es Benutzern, einige Regeln zur Zurückweisung von Paketen festzulegen, die von spezifischen Eingangs-Ports oder allen Ports empfangen werden. Durch diese Regeln werden die MAC-Quell- und Zieladressen von Paketen überprüft. Entsprechen die Pakete diesen Regeln, wird das System die Aktion „deny“ (Verweigern) ausführen. Das heißt, dass die Pakete zurückgewiesen werden.

Das Filtern der Pakete kann erfolgen nach:

- einer MAC- oder IP-Adresse der Quelle
- einer MAC- oder IP-Adresse des Ziels
- einem Bereich von MAC- oder IP-Adressen
- frei wählbaren Quell- bzw. Ziel-Ports (z. B. UDP oder TCP)

Die „Action Resolution Engine“ sammelt die Informationen (Aktions- und Messergebnisse) aus den Treffern unter den Einträgen: Wird mehr als einer Regel entsprochen, werden Aktionen und Messungen/Zähler aus der dem Regeltreffer entsprechenden Richtlinie mit höchster Priorität ausgeführt.

8.4 Monitor

8.4.1 Alarm

Diese Funktion benachrichtigt den Netzwerkadministrator über bestimmte Ereignisse und Situationen innerhalb des Netzwerks.

Beispiel

- P1: ON – Die Verbindung an Port 1 ist ausgefallen.
- PWR: ON – Die primäre Spannungsversorgung ist unterbrochen.
- RPS: ON – Die sekundäre Spannungsversorgung ist unterbrochen.

8.4.2 Monitor Informationen

Mit dieser Funktion werden einige Hardwareinformationen angezeigt, die der Systemüberwachung und Gewährleistung des ordnungsgemäßen Netzwerkbetriebs dienen.

8.4.3 RMON Statistiken

Mit dieser Funktion können RMON-Statistiken überwacht oder gelöscht werden.

Jabber

Als Jabber („Geplapper“) werden Teilnehmer an einem Netzwerk wie ETHERNET bezeichnet, welche Datenpakete länger als die zulässige MTU („**M**aximum **T**ransmission **U**nit“) besitzen.

8.4.4 SFP

SFP („**S**mall **F**orm-factor **P**luggable“) sind kleine standardisierte Module für Netzwerkverbindungen.

SFP bezeichnet eine modulare Schnittstelle zur Unterstützung verschiedener Übertragungsmedien und wird in der Netzwerktechnik zur Flexibilisierung von Schnittstellen verwendet.

8.4.4.1 SFP-Informationen

DDMI („**D**igital **D**iagnostics **M**onitoring **I**nterface“) ist eine Technologie, die es den Benutzern ermöglicht, folgende Echtzeitparameter in SFP-Modulen zu überwachen:

- Spannung
- Bias-Strom
- Eingangsleistung
- Ausgangsleistung
- Temperatur
- Glasfaserkabel
- Verbinder
- Wellenlänge
- Übertragungslänge
- DDM-Unterstützung
- Handler: Name
- Handler: Artikelnummer
- Handler: Revision
- Handler: Schlüsselnummer
- Datumsangabe (kodiert)

8.4.5 Traffic Monitor

Die Funktion „Traffic Monitor“ (Überwachung des Datenverkehrs) kann sowohl für einen spezifischen Port als auch global am Switch aktiviert bzw. deaktiviert werden. Mit dieser Funktion kann die Datenrate von Broadcast-, Multicast- oder Broadcast- und Multicast-Paketen überwacht werden. Wenn die Paketrage die Spezifikation für einen Benutzer überschreitet, wird der Port blockiert. Wenn die Funktion „Recovery“ (Wiederherstellung) aktiviert ist, wird der Port nach Ablauf der „Recovery Time“ (Wiederherstellungszeit) reaktiviert.

8.5 Management

8.5.1 SNMP

SNMP („**S**imple **N**etwork **M**anagement **P**rotocol“) stellt einen Standard für das Management von ETHERNET-Geräten in einem TCP/IP-Netzwerk dar. Es dient dem Transport von Kontrolldaten, die den Austausch von Managementinformationen, Status- und Statistikdaten zwischen einzelnen Netzwerkkomponenten und einem Managementsystem ermöglichen.

SNMP ist ein Bestandteil der durch die IETF („Internet **E**ngineering **T**ask **F**orce) definierten „Internet Protocol Suite“ (Internetprotokollfamilie). Es besteht aus einer Reihe von Standards für die Netzwerkverwaltung, einschließlich eines Anwendungsschichtprotokolls, eines Datenbankschemas und einer Reihe von Datenbankobjekten.

SNMP stellt Verwaltungsdaten in Form von Variablen der verwalteten Systeme dar, die die Systemkonfiguration beschreiben. Diese Variablen können daraufhin von Verwaltungsanwendungen abgefragt (und manchmal auch verändert) werden.

Unterstützung von MIBs

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 ETHERNET Interface MIB
- RFC 1757 RMON Group 1,2,3,9

Ein „SNMP Community String“ ist ein Textelement, das als Passwort fungiert. Es wird zur Authentifizierung von Nachrichten verwendet, die zwischen der Managementstation (dem SNMP-Manager) und einem Gerät (dem SNMP-Agenten) ausgetauscht werden. Dieser String ist in jedem Paket enthalten, das zwischen diesen beiden Punkten übertragen wird.

Die „SNMP Community“ fungiert als Passwort und wird zur Definition der Sicherheitsparameter von SNMP-Clients in SNMPv1- und SNMPv2c-Umgebungen verwendet. Die normale „SNMP Community“ für SNMP v1 und SNMP v2c lautet „public“, so lange SNMP v3 nicht aktiviert ist. Ist SNMP v3 aktiviert, müssen die „Communities“ für SNMP v1 und v2c spezifisch sein und können nicht gemeinsam genutzt werden.

Netzwerk-ID des „Trusted Host“:

Die IP-Adresse ist eine Kombination aus der Netzwerk-ID und der Host-ID.

- Network-ID = (Host-IP und Maske).
- Ein Benutzer muss nur die Netzwerk-ID eintragen und die Host-ID bei „0“ belassen. Wenn ein Benutzer eine Host-ID, wie etwa 192.168.1.102, einträgt, wird das System die Host-ID auf 192.168.1.0 zurücksetzen.

Hinweis**Community String**

Es sollte Benutzern nur erlaubt sein, den „Community String“ und Berechtigungen zu konfigurieren.

Wenn ein Benutzer den „Community String“ und die Berechtigungen mit der Netzwerk-ID des „Trusted Host“ = 0.0.0.0 und der Subnetzmaske = 0.0.0.0 konfiguriert, bedeutet das, dass alle Hosts mit diesem „Community String“ auf den Switch zugreifen können.

8.5.1.1 SNMP Trap

Ein Trap ist eine unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist. Der SNMP-Manager, der das Trap empfängt, kann nach weiteren Informationen nachfragen.

9 Konfigurieren

9.1 Übersicht der Konfigurationsoptionen

Für erweiterte Verwaltungsfunktionen bietet der Industrial-Managed-Switch 2 Möglichkeiten:

Telnet-/SSH-Port

Über den Telnet-Port kann per Netzwerk eine menügesteuerte Benutzeroberfläche mit dem WBM („**W**eb **B**ased **M**anagement“) aufgerufen werden.

Hinweis



Weitere Informationen

Die ausführliche Beschreibung finden Sie im Kapitel „Im Web-Based-Management-System (WBM) konfigurieren“.

Konsolen-Port

Über den Konsolen-Port an der Vorderseite des Industrial-Managed-Switch (lokal) kann über einen integrierten Verwaltungsagenten das CLI („**C**ommand **L**ine **I**nterface“) aufgerufen werden.

Der Verwaltungsagent basiert auf SNMP (Simple Network Management Protocol). Mithilfe dieses SNMP-Agenten kann der Industrial-Managed-Switch von jedem PC im Netzwerk aus mit einer Verwaltungssoftware verwaltet werden.

Der Verwaltungsagent umfasst auch einen eingebetteten HTTP-Webagenten. Auf diesen Webagenten kann mit einem Standardwebbrowser von jedem an das Netzwerk angeschlossenen PC aus zugegriffen werden.

Hinweis



Weitere Informationen

Die ausführliche Beschreibung finden Sie im Kapitel „Anhang“ > ... > „Im Command Line Interface (CLI) konfigurieren“.

9.1.1 Telnet-Port

1. Verbinden Sie den Computer mit einem der ETHERNET-Ports.
2. Eröffnen Sie eine Telnet-Sitzung zur IP-Adresse des Switches. Verwenden Sie die Default-Werte, wenn dies Ihre erste Anmeldung ist.

Tabelle 53: Default-Einstellungen für den Telnet-Port

Einstellung	Default-Wert
IP Address (IP-Adresse)	0.0.0.0
Subnet Mask (Subnetzmaske)	0.0.0.0
Default Gateway (Default-Gateway)	0.0.0.0
Management VLAN (Management-VLAN)	1
Default Username	admin
Default Password	wago

Hinweis



Hinweise zur Vergabe der IP-Adresse beachten!

Das Gerät hat im Auslieferungszustand die IP-Adresse 0.0.0.0 und kann nicht direkt über den Telnet-Port angesprochen werden. Die Vergabe der IP-Adresse muss über DCP oder über CLI erfolgen. Ausführliche Informationen zur Vorgehensweise finden Sie im Kapitel „PROFINET“.

9.2 Konsolenport

Vor dem Zugriff auf den integrierten Verwaltungsagenten des Industrial-Managed-Switches über eine Netzwerkverbindung müssen Sie diesen zunächst über eine lokale Verbindung oder das BOOTP-Protokoll mit der Default- IP-Adresse, einer Teilnetzmaske und einem Standard-Gateway konfigurieren.

Nach der Konfigurierung der IP-Parameter des Industrial-Managed-Switches können Sie von jeder Stelle innerhalb des angeschlossenen Netzwerks aus oder per Internet auf das integrierte Konfigurationsprogramm zugreifen. Das integrierte Konfigurationsprogramm kann per Telnet von jedem an das Netzwerk angeschlossenen Computer aus aufgerufen werden. Außerdem kann es von jedem Computer aus über einen Webbrowser verwaltet werden.

Hinweis



Voraussetzung für die Herstellung der Verbindung

Stellen Sie sicher, dass das Terminal bzw. der PC für die Verbindung mit den oben genannten Einstellungen konfiguriert ist. Andernfalls wird keine Verbindung hergestellt.

1. Verbinden Sie den Computer über ein geeignetes Kabel mit dem Konsolen-Port am Switch.

Details zur Kabelanschlussbelegung finden Sie im Kapitel „Anhang“ > ... > „RJ-45-Kabel“.

2. Verwenden Sie einen Terminalemulator (PuTTY) mit folgenden Einstellungen:

Tabelle 54: Default-Einstellungen für den Konsolen-Port

Einstellung	Default-Wert
Baud Rate (Baudrate)	38400
Parity (Parität)	None (keine)
Number of Data Bits (Anzahl der Datenbits)	8
Number of Stop Bits (Anzahl der Stoppbits)	1
Flow Control	None

3. Drücken Sie **[EINGABE]**, um den Anmeldebildschirm aufzurufen.

Tabelle 55: Anmeldebildschirm

Einstellung	Default-Wert
Default Username (Default-Benutzername)	admin
Default Password (Default-Passwort)	wago

Hinweis



Vorgehensweise beachten!

Die genaue Vorgehensweise zum Aufbau der Verbindung und zur Vergabe der IP-Adresse über CLI finden Sie im Kapitel „PROFINET“ > „Zugriff über Konsolenport (CLI)“.

10 Web-Based-Management-System (WBM)

Für die Konfiguration und Verwaltung des Systems stehen Ihnen ein internes Dateisystem und ein integrierter Webserver zur Verfügung, die als Web-Based-Management-System, kurz WBM, bezeichnet werden.

Hinweis



Im Auslieferungszustand WBM nur eingeschränkt nutzbar!

Im Auslieferungszustand befindet sich der Switch im PROFINET-Modus. In diesem Modus ist das WBM nur eingeschränkt nutzbar (siehe Kapitel „PROFINET“).

Zur Nutzung des vollen WBM-Funktionsumfangs muss der PROFINET-Modus des Switches deaktiviert werden.

Auf den intern gespeicherten HTML-Seiten erhalten Sie auslesbare Informationen über die Konfiguration und den Status des Feldbusknotens. Außerdem ändern Sie hier die Konfiguration des Gerätes. Darüber hinaus können Sie über das implementierte Dateisystem auch selbst erstellte HTML-Seiten hinterlegen.

Hinweis



Nach Änderungen an der Konfiguration immer einen Neustart durchführen!

Damit geänderte Konfigurationseinstellungen wirksam werden, führen Sie nach Ihren Änderungen immer einen Systemneustart durch.

1. Zum Öffnen des WBM starten Sie einen Webbrowser (z. B. Microsoft Internet-Explorer oder Mozilla Firefox).
2. Geben Sie in der Adresszeile die IP-Adresse des Produkts ein.
3. Bestätigen Sie mit **[Enter]**.
4. Geben Sie im Abfragedialog Ihren Benutzernamen und das Passwort ein:

User = „admin“
Passwort = „wago“
5. Die Startseite des WBM wird aufgebaut.
6. Führen Sie die gewünschten Einstellungen durch.
7. Bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Übernehmen]**, **[Aktualisieren]** oder **[Anwenden]** oder verworfen Sie Ihre Änderungen mit der Schaltfläche **[Löschen]** oder **[Verwerfen]**.
8. Damit die Einstellungen übernommen werden, bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Konfiguration Speichern]**.

Über die Links der Navigationsleiste erreichen Sie die entsprechenden WBM-Seiten:

Tabelle 56: Übersicht – Navigationslinks und WBM-Seiten

Navigationslinks und WBM-Seiten	
► [Systemstatus]	
	• Systeminformationen
► [Grundeinstellungen]	
	• Allgemeine Einstellungen • MAC-Management • Port-Mirroring • Port-Einstellungen
► [PROFINET]	
	• Konfiguration • Informationen • Diagnose
► [Erweiterte Einstellungen]	
	[Bandbreiten-Regelung] • QoS • Bandbreitenbegrenzung [IGMP-Snooping] • IGMP-Snooping • IGMP-Filter • Multicast-Adresse • Multicast-IP-Statistiken [VLAN] • Port-Isolation • VLAN • MAC-VLAN • LLDP • Loop Detection • MRP • STP (RSTP/MSTP)
► [Sicherheit]	
	• Zugriffskontrollliste
► [Monitor]	
	• Alarm • Systeminformationen • Port-Statistik • Port-Auslastung

- RMON-Statistiken
- SFP-Informationen
- Traffic-Monitor

► **[Management]**

[SNMP]

- SNMP
- SNMP-Trap
- SNMPv3

- Wartung
- System-Log
- Upload File
- Ping
- Benutzerkonto
- Open source License
- Wago Licenses

Auf diesen WBM-Seiten können die Einstellungen/Konfigurationen des Industrial-Managed-Switches vorgenommen werden.

Auf einigen WBM-Seiten existieren für die Einstellungen/Konfigurationen Registerseiten.

Die Default-Werte sind **fett** hervorgehoben dargestellt.

10.1 Systemstatus

10.1.1 Systeminformation

Systeminformation	
Modellname	852- 
Host-Name	PN-SWITCH
Boot Code Version	V1.3.9.S0
Profinet Software	
Version	V1.2.0
MD5 Checksum	c91b249410198ba0a5125166504b645d
PN Boot Image	
Firmware-Version	V1.2.1.S0
Built Date	Sun Apr 28 17:03:45 CST 2019
Prüfsumme	dd8815a4
DHCP Client	Ausschalten
IP-Adresse	192.168.1.254
Subnet-Maske	255.255.255.0
Default Gateway	0.0.0.0
MAC-Adresse	00:30:de:ff:f5:b8
Seriennummer	0001910146780101
Management VLAN	1
CPU-Auslastung	1 %
Speicherauslastung	Total: 118996 KB, Free: 90044 KB, Usage: 24.33 %
Aktuelle Uhrzeit	2000-1-23, 17:14:41
System Uptime	0 days, 6 hours, 21 minutes, 2 seconds
Aktualisieren	

Abbildung 42: WBM-Seite „Systeminformation“

Tabelle 57: WBM-Seite "Systeminformation"

Parameter	Beschreibung
Modellname	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
Host-Name	In diesem Anzeigefeld wird der Hostname des Switches angezeigt.
Boot Code Version	In diesem Anzeigefeld wird die Boot-Code-Version angezeigt.
Profinet Software Version	Identifikationsnummer der „Profinet Software Version“
Profinet Software MD5 Prüfsumme	Prüfsumme der „Profinet Software Version“
PN Boot Image Firmware-Version	In diesem Feld wird die Version des „PN Boot Images“ angezeigt.
PN Boot Image Build Date	In diesem Feld wird das Datum der Firmwareerzeugung angezeigt.
PN Boot Image Prüfsumme	In diesem Feld wird die Prüfsumme des „PN Boot Images“ angezeigt
DHCP Client	In diesem Anzeigefeld wird angezeigt, ob die DHCP-Client-Funktion aktiviert ist.
IP Address	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt.
Subnet Mask	In diesem Anzeigefeld wird die „Subnet Mask“ des Switches angezeigt.
Default Gateway	In diesem Anzeigefeld wird das Default-Gateway des Switches angezeigt.
MAC Address	In diesem Anzeigefeld wird die MAC-(Media-Access-Control-)Adresse des Switches angezeigt.
Seriennummer	In diesem Anzeigefeld wird die Seriennummer angezeigt.
Management-VLAN	In diesem Anzeigefeld wird die VLAN-ID angezeigt, die für die Verwaltungsprozesse des Switches benötigt wird.
CPU-Auslastung	In diesem Anzeigefeld wird die prozentuale Systemauslastung des Switches angezeigt.
Speicherauslastung	In diesem Anzeigefeld wird der gesamte („Total“) sowie der momentan verfügbare („Free“) und verwendete („Usage“) Speicher des Switches angezeigt.
Aktuelle Uhrzeit	In diesem Anzeigefeld wird das aktuelle Datum (yyyy-mm-dd) und die aktuelle Uhrzeit (hh:mm:ss) angezeigt.
System Uptime	In diesem Feld wird angezeigt, wie lange der Switch nach dem Einschalten läuft (Tage, Stunden, Minuten und Sekunden).

10.2 Grundeinstellungen

10.2.1 Allgemeine Einstellungen

10.2.1.1 System

The screenshot shows the 'Allgemeine Einstellungen' (General Settings) page in the WBM interface, specifically the 'System' tab. The page is divided into several sections: 'Systemeinstellungen' (System Settings) with fields for 'Hostname' (L2SWITCH) and 'Management VLAN' (1); 'IPv4-Einstellungen' (IPv4 Settings) with fields for 'DHCP Client' (Ausschalten), 'IP-Adresse' (192.168.1.254), 'Subnet-Maske' (255.255.255.0), and 'Default Gateway' (0.0.0.0); and 'IPv6-Einstellungen' (IPv6 Settings) with fields for 'DHCPv6 Client' (Ausschalten), 'Globale IPv6-Adresse' (empty), and 'Default Gateway' (Gesetzt). There are buttons for 'Aktualisieren' (Update) and 'Anwenden' (Apply) at the bottom.

Allgemeine Einstellungen			
System	Jumbo Frame	SNTP	Management Host
Systemeinstellungen			
Hostname	L2SWITCH		
Management VLAN	1		
IPv4-Einstellungen			
DHCP Client	Ausschalten		
IP-Adresse	192.168.1.254		
Subnet-Maske	255.255.255.0		
Default Gateway	0.0.0.0		
IPv6-Einstellungen			
DHCPv6 Client	Ausschalten		
Globale IPv6-Adresse			
Default Gateway	Gesetzt		
Anwenden Aktualisieren Konfiguration speichern			

Abbildung 43: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

Tabelle 58: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

Systemeinstellungen		
Parameter	Standardwert	Beschreibung
Hostname	L2SWITCH	Geben Sie im Eingabefeld bis zu 64 alphanumerische Zeichen für den Namen Ihres Switches ein. Der Hostname sollte aus einer Kombination aus Zahlen, Buchstaben, Bindestrichen (-) oder Unterstrichen (_) bestehen.
Management VLAN	1	Geben Sie im Eingabefeld eine VLAN-Gruppe ein, die Zugriff auf den Switch erhalten soll. Gültiger VLAN-Bereich: 1 ... 4094.
		Hinweis  Konfiguration eines Management-VLANs Vor der Konfiguration eines Management VLANs müssen Sie zuerst ein Management VLAN erstellen und diesem mindestens einen Teilnehmer-Port zuweisen.
IPv4-Einstellungen		
Parameter	Standardwert	Beschreibung
DHCP Client	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die IP-Adresse des Switches manuell konfigurieren möchten.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit der Switch seine IP-Adresse von einem DHCP-Server automatisch bezieht. Klicken Sie auf [Aktualisieren] , damit der Switch erneut eine IP-Adresse vom DHCP-Server bezieht.
IP-Adresse	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse des Switches in Dezimalpunktschreibweise ein.
Subnet-Maske	0.0.0.0	Geben Sie im Eingabefeld die IP-Subnet-Maske des Switches in Dezimalpunktschreibweise ein.
Default Gateway	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse des ausgehenden Default-Gateways in Dezimalpunktschreibweise ein.
IPv6-Einstellungen		
Parameter	Standardwert	Beschreibung
DHCPv6 Client	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die IP-Adresse des Switches manuell konfigurieren möchten.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit der Switch seine IP-Adresse per DHCP automatisch bezieht. Klicken Sie auf [Aktualisieren] , damit der Switch die Werte aktualisiert.
Globale IPv6-Adresse		In diesem Anzeigefeld wird die globale IPv6-Adresse angezeigt.
Default Gateway	Gesetzt	Wählen Sie im Auswahlfeld „Gesetzt“, wenn Sie die IP-Adresse eingeben wollen. Geben Sie die IP-Adresse des ausgehenden Default-Gateways in Dezimalpunktschreibweise ein.
	Nicht gesetzt	Wählen Sie im Auswahlfeld „Nicht gesetzt“, wenn Sie die IP-Adresse nicht eingeben wollen.

10.2.1.2 Jumbo Frame

Hinweis



Weitere Information

Weitere Informationen zum „Jumbo Frame“ finden Sie im Kapitel „Funktionsbeschreibung“.

General Settings				
System		Jumbo Frame	SNTP	Management Host
Jumbo Frame Settings				
Port		Frame Size		
From: 1 To: 1		10240		
Apply Refresh Save Configurations				
Port	Jumbo Frame	Port	Jumbo Frame	
1	10240	2	10240	
3	10240	4	10240	
5	10240	6	10240	
7	10240	8	10240	
9	10240	10	10240	
11	10240	12	10240	

Abbildung 44: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“

Tabelle 59: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“

Jumbo-Frame-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um den Jumbo Frame zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um den Jumbo Frame zu konfigurieren.
Jumbo Frame		10240	Wählen Sie im Auswahlfeld für alle Ports die maximale Byte-Anzahl für einen „Jumbo Frame“ aus. Je höher die Frame-Größe, desto besser ist die Netzwerkleistung.
		1522	
		1536	
		1552	
		9010	
		9216	
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Jumbo Frame		1522	In dieser Spalte wird die maximale Byte-Anzahl für einen „Jumbo Frame“ angezeigt.
		1536	
		1552	
		9010	
		9216	
		10240	

10.2.1.3 SNTP**Hinweis****Weitere Information**

Weitere Informationen zu „SNTP“ (**S**imple **N**etwork **T**ime **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

Allgemeine Einstellungen	
System	Jumbo Frame
SNTP	Management Host
Aktuelles Datum und Uhrzeit	
Aktuelle Uhrzeit	10:33:40 (UTC)
Aktuelles Datum	2019-05-13
Datum- und Uhrzeiteinstellungen	
☒ Direkteingabe Neue Uhrzeit: 2019 . 5 . 13 / 10 : 33 : 40 (yyyy.mm.dd / hh:mm:ss)	
☐ Freigabe Network Time Protocol NTP Server: ☐ ntp0.fau.de - Europe ☒ IP 0.0.0.0 Zeitzone: +0000 (+hh / -hh / +hhmm / -hhmm)	
Sommerzeit-Einstellungen	
Status	Ausschalten
Startzeitpunkt	Erster Sonntag of Januar 0 o'clock
Endzeitpunkt	Erster Sonntag of Januar 0 o'clock
Anwenden Aktualisieren Konfiguration speichern	

Abbildung 45: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“

Tabelle 60: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“

Aktuelles Datum und Uhrzeit		
Parameter	Standardwert	Beschreibung
Aktuelle Uhrzeit		In diesem Anzeigefeld wird die aktuelle Uhrzeit angezeigt, wenn Sie dieses Menü öffnen bzw. aktualisieren.
Aktuelles Datum		In diesem Anzeigefeld wird das aktuelle Datum angezeigt, wenn Sie dieses Menü öffnen bzw. aktualisieren.
Datum- und Uhrzeiteinstellungen		
Parameter	Standardwert	Beschreibung
Direkteingabe	Neue Uhrzeit ☐	Wählen Sie diese Option, wenn Sie Zeit und Datum für das System manuell einstellen möchten. Tragen Sie das neue Datum im Format Jahr/Monat/Tag und die aktuelle Uhrzeit im Format Stunden/Minuten/Sekunden ein. Nachdem Sie auf [Anwenden] geklickt haben, erscheinen die neuen Angaben in den Anzeigefeldern „Aktuelle Uhrzeit“ und „Aktuelles Datum“.
Freigabe Network Time-Protocol		Wählen Sie diese Option, wenn Sie das Network Time Protocol (NTP) für den Zeitdienst verwenden möchten.
	NTP-Server ☒	☒ Wählen Sie diese Option, wenn Sie einen vordefinierten Zeitserver nutzen wollen. Der Switch wird 60 Sekunden lang nach einem Zeitserver suchen.
	0.0.0.0	☐ Wählen Sie diese Option, wenn Sie die IP-Adresse eines Zeitservers eingeben. Der Switch wird 60 Sekunden lang nach einem Zeitserver suchen.
		☒ IP Geben Sie die IP-Adresse des NTP-Servers in Dezimalpunktschreibweise ein.
		☐ Domain Name Geben Sie die Domain-Adresse des Switches ein.
	Zeitzone +0000	Geben Sie den Zeitunterschied zwischen UTC („Universal Time Coordinated“, ehemals GMT, „Greenwich Mean Time“) und der Zeitzone in hh:mm ein.

Tabelle 60: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“

Sommerzeit-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie „Ausschalten“, wenn Sie die Sommerzeit nicht verwenden möchten
	Einschalten	Wählen Sie „Einschalten“, wenn Sie die Sommerzeit verwenden möchten
Startzeitpunkt ¹⁾		Tragen Sie Datum und Uhrzeit für den Beginn der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.
Stoptzeitpunkt ²⁾		Tragen Sie Datum und Uhrzeit für das Ende der Sommerzeit ein, falls Sie diese Option aktiviert haben. Die Zeit wird im 24-Stunden-Format angezeigt.
¹⁾	In den meisten Teilen der USA beginnt die Sommerzeit am zweiten Sonntag im März. In jeder Zeitzone der USA beginnt die Sommerzeit um 02:00 Uhr Ortszeit. Dementsprechend müssten Sie die Auswahl „Zweiter, Sonntag, März“ und „2:00“ („Zweiter, Sonntag, März“ und „2:00“) einstellen. In der EU beginnt die Sommerzeit am letzten Sonntag im März. Sie beginnt in allen EU-Zeitzone zum selben Zeitpunkt (01:00 Uhr GMT oder UTC). Dementsprechend müssten Sie die Auswahl „Letzter, Sonntag, März“ („Letzter, Sonntag, März“) einstellen sowie in das letzte Feld die Uhrzeit entsprechend Ihrer Zeitzone eintragen. Für Deutschland müssten Sie beispielsweise „2:00“ eintragen, weil die Sommerzeit in Deutschland eine Stunde vor der GMT oder UTC liegt (GMT+1).	
²⁾	In den USA endet die Sommerzeit am letzten Sonntag im Oktober. In jeder Zeitzone der USA endet sie um 02:00 Uhr Ortszeit. Dementsprechend müssten Sie die Auswahl „Erster, Sonntag, November“ und „2:00“ („Erster, Sonntag, November“ und „2:00“) einstellen. In der EU endet die Sommerzeit am letzten Sonntag im Oktober. Sie endet in allen EU-Zeitzone zum selben Zeitpunkt (01:00 Uhr GMT oder UTC). Dementsprechend müssten Sie die Auswahl „Letzter, Sonntag, Oktober“ („Letzter, Sonntag, Oktober“) einstellen sowie in das letzte Feld die Uhrzeit entsprechend Ihrer Zeitzone eintragen. Für Deutschland müssten Sie beispielsweise „2:00“ eintragen, weil die Sommerzeit in Deutschland eine Stunde vor der GMT oder UTC liegt (GMT+1).	

10.2.1.4 Management-Host

Hinweis



Weitere Information

Weitere Informationen zum „Management-Host“ finden Sie im Kapitel „Funktionsbeschreibung“.

The screenshot shows the 'Allgemeine Einstellungen' (General Settings) page in the WBM interface. The 'Management Host' tab is selected. Under 'Management-Host-Einstellungen', there are input fields for 'Management Host' and 'Subnet-Maske', with buttons 'Anwenden', 'Aktualisieren', and 'Konfiguration speichern'. Below this is the 'Management-Host-Liste' table, which contains one entry with the number 1, the IP address 192.168.1.3/1, and a 'Löschen' (Delete) button.

Abbildung 46: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“

Tabelle 61: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“

Management-Host-Einstellungen		
Parameter	Standardwert	Beschreibung
Management Host		Geben Sie im Eingabefeld die IP-Adresse des „Management Host“ in Dezimalpunktschreibweise ein.
Subnet-Maske		Geben Sie im Eingabefeld die Nr. der Subnet-Maske-Adresse des „Management Hosts“ in Dezimalpunktschreibweise ein.
Management-Host-Liste		
Parameter	Standardwert	Beschreibung
Nr.	1 ... 3	In dieser Spalte werden die fortlaufenden Nummern jedes „Management Hosts“ angezeigt.
Management Host (IP/Mask)		In dieser Spalte werden die IP-Adressen des „Management Hosts“ angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

10.2.2 MAC Management

Hinweis



Weitere Information

Weitere Informationen zum „MAC Management“ finden Sie im Kapitel „Funktionsbeschreibung“.

10.2.2.1 Statische MAC-Einstellungen

Hinweis



Weitere Information

Weitere Informationen zu „Statische MAC-Einstellungen“ (Statische MAC-Adresse) finden Sie im Kapitel „Funktionsbeschreibung“.

MAC Management

Statische MAC-Einstellungen
MAC-Tabelle
Age-Time-Einstellung
Blacklisting

Statische MAC-Einstellungen

MAC-Adresse	VLAN ID	Port
		1 ▾

Anwenden
Aktualisieren
Konfiguration speichern

Statische MAC-Tabelle

MAC-Adresse	VLAN ID	Port	Aktion
00:30:de:ff:f1:9b	1	CPU	

Anzahl der Einträge : 1

Abbildung 47: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“

Tabelle 62: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“

Statische MAC-Einstellungen		
Parameter	Standardwert	Beschreibung
MAC-Adresse		Geben Sie im Eingabefeld die MAC-Adresse eines Computers oder Gerätes ein, die in die MAC-Adresstabelle aufgenommen werden soll. Das gültige Format ist: hh:hh:hh:hh:hh:hh.
VLAN ID		Geben Sie in diesem Eingabefeld die „VLAN ID“ ein, die dem Computer oder Gerät zugewiesen werden soll.
Port	1	Wählen Sie im Auswahlfeld einen Port aus, mit dem der Computer oder das Gerät verbunden ist.
Statische MAC-Tabelle		
Parameter	Standardwert	Beschreibung
MAC-Adresse		In dieser Spalte werden die manuell eingetragenen MAC-Adresseinträge angezeigt.
VLAN ID		In dieser Spalte wird die „VLAN ID“ der manuell eingetragenen MAC-Adresseinträge angezeigt.
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern der manuell eingetragenen MAC-Adresseinträge angezeigt. Die MAC-Adresse „CPU“ ist die MAC-Adresse des Switch.
Aktion		Klicken Sie auf [Löschen] , um die manuell eingetragene MAC-Adresse aus der MAC-Adresstabelle zu löschen. Die MAC-Adresse des Switches kann nicht aus der Tabelle der statischen MAC-Adressen gelöscht werden.
Anzahl der Einträge		In diesem Anzeigefeld wird die Gesamtanzahl der Einträge in der Statischen MAC-Adress-Tabelle angezeigt.

10.2.2.2 MAC-Tabelle

The screenshot shows the 'MAC Management' interface with the 'MAC-Tabelle' tab selected. It includes a table with columns for MAC-Adresse, Typ, VLAN ID, and Port/Trunk ID. The table contains three entries. Below the table, there are controls for 'Typ anzeigen' (set to 'Alle'), 'Anwenden', 'Aktualisieren', 'Loschen', and pagination options (Seite hoch, Seite runter, Seite: 1/1, Seite: 1, Anwenden). The text 'Anzahl der Einträge : 3' is displayed below the table.

MAC-Adresse	Typ	VLAN ID	Port/Trunk ID
00:10:18:af:b7:d4	Dynamisch	1	8
00:30:de:ff:f1:8c	Dynamisch	1	11
00:30:de:ff:f1:9b	Statisch	1	CPU

Abbildung 48: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“

Tabelle 63: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“

MAC-Tabelle		
Parameter	Standardwert	Beschreibung
Typ anzeigen	[Alle]	Wählen Sie im Auswahlfeld „Alle“, um alle MAC-Adresseinträge anzuzeigen.
	Statisch	Wählen Sie im Auswahlfeld „Statisch“, um die statischen MAC-Adresseinträge anzuzeigen.
	Dynamisch	Wählen Sie im Auswahlfeld „Dynamisch“, um die dynamischen MAC-Adresseinträge anzuzeigen.
	Port	Wählen Sie im Auswahlfeld „Port“, um die entsprechenden MAC-Adresseinträge anzuzeigen.
	MAC	Wählen Sie im Auswahlfeld „MAC“, um die entsprechenden MAC-Adresseinträge anzuzeigen.
MAC-Adresse		In dieser Spalte werden die MAC-Adressen angezeigt.
Typ		In dieser Spalte wird angezeigt, ob der Eintrag manuell eingetragen (statisch) oder vom Switch bezogen (dynamisch) wurde.
VLAN ID		In dieser Spalte wird die „VLAN ID“ des MAC-Adresseintrags angezeigt.
Port/Trunk ID		In dieser Spalte wird die Port-Nummer angezeigt, mit der der MAC-Adresseintrag verbunden ist. „CPU“ meint hier den MAC-Adresseintrag des Switches.
Anzahl der Einträge		In diesem Anzeigefeld wird die Gesamtanzahl der Einträge in der MAC-Adress-Tabelle angezeigt.
Seite hoch		Bei sehr vielen MAC-Adresseinträgen kann mit dieser Schaltfläche nach oben gescrollt werden.
Seite runter		Bei sehr vielen MAC-Adresseinträgen kann mit dieser Schaltfläche nach unten gescrollt werden.
Seite		In diesem Anzeigefeld wird die aktuelle Seite der MAC-Adress-Tabelle angezeigt.

10.2.2.3 Age-Time-Einstellung

Abbildung 49: WBM-Seite „MAC Management“ – Register „Age-Time-Einstellung“

Tabelle 64: „MAC Management“ – Register „Age-Time-Einstellung“

Age-Time-Einstellung		
Parameter	Standardwert	Beschreibung
Age Time (sec) (Bereich: 20-400 or 0:Ausschalten)	300	Geben Sie im Eingabefeld die „Age Time“ (Lebensdauer) ein. Gültiger Bereich: 0 oder 20 ... 400 s.

10.2.2.4 Blacklisting

Hinweis**Weitere Information**

Weitere Informationen zu „Blacklisting“ finden Sie im Kapitel „Funktionsbeschreibung“.

Hinweis**Maximale Anzahl von MAC-Blacklist-Einträgen**

Es können bis zu 20 Einträge konfiguriert werden.

The screenshot shows the 'MAC Management' interface with the 'Blacklisting' tab selected. It includes input fields for 'MAC-Adresse' and 'VLAN ID' (with a dropdown set to 'Beliebig'). Below these are buttons for 'Anwenden', 'Aktualisieren', and 'Konfiguration speichern'. A table titled 'MAC-Blacklist-Tabelle' contains one entry with MAC-Adresse '00:30:de:06:64:0b', VLAN ID 'Beliebig', and a 'Löschen' button. At the bottom right, it states 'Anzahl der Einträge : 1'.

Abbildung 50: WBM-Seite „MAC Management“ – Register „Blacklisting“

Tabelle 65: WBM-Seite „MAC Management“ – Register „Blacklisting“

Blacklisting		
Parameter	Standardwert	Beschreibung
MAC-Adresse		Geben Sie im Eingabefeld die MAC-Adresse eines Computers oder Gerätes ein, den oder das sie zurückweisen möchten. Das gültige Format ist: hh:hh:hh:hh:hh:hh.
VLAN ID	Beliebig	Der Switch erhält eine beliebige „VLAN ID“.
	VLAN	Geben Sie im Eingabefeld eine „VLAN ID“ ein, die Sie dem Computer oder dem Gerät zuweisen möchten.
MAC-Blacklist-Tabelle		
Parameter	Standardwert	Beschreibung
MAC-Adresse		In dieser Spalte werden die MAC-Adressen angezeigt.
VLAN ID		In dieser Spalte wird die „VLAN ID“ der MAC-Adresseinträge angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen manuell eingetragenen MAC-Adresseintrag aus der Blacklist-Tabelle zu löschen.
Anzahl der Einträge		In diesem Anzeigefeld wird die Gesamtanzahl der Einträge in der der Blacklist-Tabelle angezeigt.

10.2.3 Port-Spiegelung

Hinweis



Weitere Information

Weitere Informationen zur „Port-Spiegelung“ finden Sie im Kapitel „Funktionsbeschreibung“.

Hinweis



Monitor-Port

Der Monitor-Port kann kein Mitglied einer „Trunk Port“-Gruppe sein.
Der Monitor-Port kann kein Eingangs- oder Ausgangs-Port sein.
Wenn ein Port als Source-Port konfiguriert wurde und ein Benutzer ihn anschließend als Ziel-Port konfiguriert, wird der Port automatisch aus den Source-Ports gelöscht.

Port-Spiegelung

Port-Spiegelung-Einstellungen

Status Ausschalten ▾

Überwachung an Port 1 ▾

Alle Ports : - ▾

Source Port	Spiegel-Modus	Source Port	Spiegel-Modus
1	Ausschalten ▾	2	Ausschalten ▾
3	Ausschalten ▾	4	Ausschalten ▾
5	Ausschalten ▾	6	Ausschalten ▾
7	Ausschalten ▾	8	Ausschalten ▾
9	Ausschalten ▾	10	Ausschalten ▾
11	Ausschalten ▾	12	Ausschalten ▾

Anwenden
Aktualisieren
Konfiguration speichern

Abbildung 51: WBM-Seite „Port-Spiegelung“

Tabelle 66: WBM-Seite „Port-Spiegelung“

Port-Spiegelung-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Port-Spiegelung“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Port-Spiegelung“ zu aktivieren.
Überwachung an Port	1 ... 10 (12)	Wählen Sie im Auswahlfeld einen Port aus, der mit einem „Network Traffic Analyzer“ verbunden werden soll.
Alle Ports	-	Einstellungen in diesem Auswahlfeld wirken sich auf alle Ports aus.
	Ausschalten	Nehmen Sie hier nur Einstellungen vor, wenn diese für alle Ports gelten sollen.
	Ingress	Beginnen Sie hier mit allgemeinen Einstellungen und nehmen Sie anschließend Einstellungen für einzelne Ports vor.
	Egress	
	Beide	
Source Port	1 ... 10 (12)	In dieser Spalte wird die Nummer der einzelnen „Source Ports“ angezeigt.
Spiegel-Modus	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn kein Datenverkehr von den spezifizierten „Source Ports“ zum Monitor Port kopiert werden soll.
	Ingress	Wählen Sie im Auswahlfeld „Ingress“, um nur die Eingangsdaten (eingehende) der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.
	Egress	Wählen Sie im Auswahlfeld „Egress“, um nur die Ausgangsdaten (ausgehende) der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.
	Beide	Wählen Sie im Auswahlfeld „Beide“, um beide (ein- und ausgehende) Daten der spezifizierten „Source Ports“ zum „Monitor Port“ zu kopieren.

10.2.4 Port-Einstellungen

10.2.4.1 Allgemeine Einstellungen

Port-Einstellungen

Allgemeine Einstellungen
Informationen

Port-Einstellungen

Port	Status	Geschwindigkeit / Duplex	Flusskontrolle
von: 1 ▼ an: 1 ▼	Einschalten ▼	Auto ▼	Aus ▼

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	Status	Geschwindigkeit / Duplex	Flusskontrolle	Link Status
1	Einschalten	Auto	Aus	Link inaktiv
2	Einschalten	Auto	Aus	Link inaktiv
3	Einschalten	Auto	Aus	Link inaktiv
4	Einschalten	Auto	Aus	Link inaktiv
5	Einschalten	Auto	Aus	Link inaktiv
6	Einschalten	Auto	Aus	Link inaktiv
7	Einschalten	Auto	Aus	Link inaktiv
8	Einschalten	Auto	Aus	100M / Voll / Aus
9	Einschalten	Auto	Aus	Link inaktiv
10	Einschalten	Auto	Aus	Link inaktiv
11	Einschalten	Auto	Aus	1000M / Voll / Aus
12	Einschalten	Auto	Aus	Link inaktiv

Abbildung 52: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“

Tabelle 67: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“

Port-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren wollen.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren wollen.
Status		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Port zu aktivieren.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um den Port zu deaktivieren.
Geschwindigkeit/Duplex		Auto	Wählen Sie im Auswahlfeld Geschwindigkeit und Duplexmodus für den Port aus.
		10 Mbit/s / Vollduplex	
		10 Mbit/s / Halbduplex	
		100 Mbit/s / Vollduplex	
		100 Mbit/s / Halbduplex	
		1000 Mbit/s / Vollduplex	
Flusskontrolle		Aus	Wählen Sie im Auswahlfeld „Aus“, um den Zugriff auf die Pufferressourcen der Ports zu deaktivieren und den Betrieb des Switches im Netzwerk zu unterbrechen.
		An	Wählen Sie im Auswahlfeld „An“, um Zugriff auf die Pufferressourcen der Ports zu erhalten und einen verlustfreien Betrieb der Switches im Netzwerk sicherzustellen.
Port-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Status			In dieser Spalte wird angezeigt, ob ein Port aktiviert oder deaktiviert ist.
Geschwindigkeit/ Duplexmodus			In dieser Spalte wird angezeigt, für welche Geschwindigkeit (10 Mbit/s, 100 Mbit/s oder 1000 Mbit/s) und für welchen Duplexmodus (voll- oder halbduplex) ein Port konfiguriert wurde.
Flusskontrolle			In dieser Spalte wird angezeigt, ob die „Flusskontrolle“ für einen Port auf „An“ oder „Aus“ eingestellt ist.
Link Status			In dieser Spalte wird der „Link Status“ eines Ports angezeigt. Ist der Port aktiv, werden die Geschwindigkeit, der Duplexmodus und die „Flusskontrolle“-Einstellung angezeigt. Die Anzeige „Link inaktiv“ zeigt an, dass der Port entweder deaktiviert oder an kein Gerät angeschlossen ist.

10.2.4.2 Informationen

Port-Einstellungen

Allgemeine Einstellungen
Informationen

Port-Einstellungen

Port	Beschreibung
von: 1 an: 1	gigabitethernet1/0/1

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	Beschreibung	Status	Betriebsdauer	Verbindungsart
1	gigabitethernet1/0/1	Normally	0 days 0:0:0	Copper
2	gigabitethernet1/0/2	Normally	0 days 0:0:0	Copper
3	gigabitethernet1/0/3	Normally	0 days 0:0:0	Copper
4	gigabitethernet1/0/4	Normally	0 days 0:0:0	Copper
5	gigabitethernet1/0/5	Normally	0 days 0:0:0	Copper
6	gigabitethernet1/0/6	Normally	0 days 0:0:0	Copper
7	gigabitethernet1/0/7	Normally	0 days 0:0:0	Copper
8	gigabitethernet1/0/8	Normally	5 days 4:1:52	Copper
9	gigabitethernet1/0/9	Normally	0 days 0:0:0	Fiber
10	gigabitethernet1/0/10	Normally	0 days 0:0:0	Fiber
11	gigabitethernet1/0/11	Normally	5 days 4:45:14	Fiber
12	gigabitethernet1/0/12	Normally	0 days 0:0:0	Fiber

Abbildung 53: WBM-Seite „Port-Einstellungen“ – Register „Informationen“

Tabelle 68: WBM-Seite „Port-Einstellungen“ – Register „Informationen“

Port-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie anzeigen wollen.
	zu:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie anzeigen wollen.
Beschreibung			Geben Sie im Eingabefeld den Namen für den Port ein.
Port-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Beschreibung			In dieser Spalte wird der Name des Ports angezeigt.
Status			In dieser Spalte wird der Status des Ports angezeigt.
Betriebsdauer			In dieser Spalte wird die Betriebsdauer des Portes angezeigt.
Verbindungsart		Copper Fiber	In dieser Spalte wird die Art der Verbindung angezeigt. Kupferdraht Lichtwellenleiter

10.3 PROFINET

Die Beschreibungen der WBM-Oberfläche im Bereich PROFINET finden Sie im Kapitel „PROFINET“.

10.4 Erweiterte Einstellungen

10.4.1 Bandbreiten-Regelung

10.4.1.1 QoS

Hinweis



Weitere Information

Weitere Informationen zu „QoS“ (Quality of Service) finden Sie im Kapitel „Funktionsbeschreibung“.

10.4.1.1.1 Port-Priorität

QoS

Port-Priorität | IP-DiffServ (DSCP) | Priorität/Queue-Zuordnung | Schedule-Modus

Port Prioritäts-Einstellungen

Alle Ports haben IEEE 802.1p Priorität : - ▾

Port	IEEE 802.1p-Priorität	Port	IEEE 802.1p-Priorität
1	0 ▾	2	0 ▾
3	0 ▾	4	0 ▾
5	0 ▾	6	0 ▾
7	0 ▾	8	0 ▾
9	0 ▾	10	0 ▾

Anwenden | Aktualisieren | Konfiguration speichern

Abbildung 54: WBM-Seite „QoS“ – Register „Port-Priorität“

Tabelle 69: WBM-Seite „QoS“ – Register „Port-Priorität“

Port-Prioritätseinstellungen		
Parameter	Standardwert	Beschreibung
Alle Ports haben IEEE 802.1p-Priorität.	-	Wählen Sie im Auswahlfeld den Wert der Priorität für alle Ports ein. Der Wert bestimmt die Paketpriorität und wird dem „Priority Tag“-Feld der eingehenden Pakete hinzugefügt.
	0 ... 7	0 = niedrigste Priorität 7 = höchste Priorität
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
IEEE 802.1p-Priorität	0 ... 7	Wählen Sie im Auswahlfeld eine Priorität für Pakete aus, die an diesem Port empfangen werden. Nur einem Paket ohne eine „IEEE 802.1p-Tag-Priority“ wird die hier angegebene Priorität zugewiesen.

10.4.1.1.2 IP-DiffServ (DSCP)

QoS

Port-Priorität
IP-DiffServ (DSCP)
Priorität/Queue-Zuordnung
Schedule-Modus

DSCP-Einstellungen

Modus Tag Over DSCP ▾

DSCP	Priorität	DSCP	Priorität	DSCP	Priorität	DSCP	Priorität
DSCP 0	0 ▾	DSCP 1	0 ▾	DSCP 2	0 ▾	DSCP 3	0 ▾
DSCP 4	0 ▾	DSCP 5	0 ▾	DSCP 6	0 ▾	DSCP 7	0 ▾
DSCP 8	0 ▾	DSCP 9	0 ▾	DSCP 10	0 ▾	DSCP 11	0 ▾
DSCP 12	0 ▾	DSCP 13	0 ▾	DSCP 14	0 ▾	DSCP 15	0 ▾
DSCP 16	0 ▾	DSCP 17	0 ▾	DSCP 18	0 ▾	DSCP 19	0 ▾
DSCP 20	0 ▾	DSCP 21	0 ▾	DSCP 22	0 ▾	DSCP 23	0 ▾
DSCP 24	0 ▾	DSCP 25	0 ▾	DSCP 26	0 ▾	DSCP 27	0 ▾
DSCP 28	0 ▾	DSCP 29	0 ▾	DSCP 30	0 ▾	DSCP 31	0 ▾
DSCP 32	0 ▾	DSCP 33	0 ▾	DSCP 34	0 ▾	DSCP 35	0 ▾
DSCP 36	0 ▾	DSCP 37	0 ▾	DSCP 38	0 ▾	DSCP 39	0 ▾
DSCP 40	0 ▾	DSCP 41	0 ▾	DSCP 42	0 ▾	DSCP 43	0 ▾
DSCP 44	0 ▾	DSCP 45	0 ▾	DSCP 46	0 ▾	DSCP 47	0 ▾
DSCP 48	0 ▾	DSCP 49	0 ▾	DSCP 50	0 ▾	DSCP 51	0 ▾
DSCP 52	0 ▾	DSCP 53	0 ▾	DSCP 54	0 ▾	DSCP 55	0 ▾
DSCP 56	0 ▾	DSCP 57	0 ▾	DSCP 58	0 ▾	DSCP 59	0 ▾
DSCP 60	0 ▾	DSCP 61	0 ▾	DSCP 62	0 ▾	DSCP 63	0 ▾

Anwenden
Aktualisieren
Konfiguration speichern

Abbildung 55: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“

Tabelle 70: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“

DSCP-Einstellungen		
Parameter	Standardwert	Beschreibung
Modus	Tag Over DSCP	Wählen Sie im Auswahlfeld „Tag Over DSCP“, wenn der 802.1p-Tag eine höhere Priorität erhält als der DSCP.
	DSCP Over Tag	Wählen Sie im Auswahlfeld „DSCP Over Tag“, wenn der 802.1p-Tag eine niedrigere Priorität erhält als der DSCP.
DSCP	DSCP 0 ... DSCP 63	In dieser Spalte werden die DSCP-Felder angezeigt.
Priorität	0 ... 7	Wählen Sie im Auswahlfeld die jeweilige Prioritätsebene aus. 0 = niedrigste Priorität 7 = höchste Priorität

10.4.1.1.3 Priorität/Queue-Zuordnung

QoS

Port-Priorität | IP-DiffServ (DSCP) | **Priorität/Queue-Zuordnung** | Schedule-Modus

Priorität/Queue-Mapping-Einstellungen

Auf Grundeinstellungen Zurücksetzen

Priorität	Queue-ID
0	1 ▼
1	0 ▼
2	2 ▼
3	3 ▼
4	4 ▼
5	5 ▼
6	6 ▼
7	7 ▼

Anwenden | Aktualisieren | Konfiguration speichern

Abbildung 56: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“

Tabelle 71: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“

Priorität/Queue-Mapping-Einstellungen		
Parameter	Standardwert	Beschreibung
Auf Grundeinstellungen zurücksetzen		Klicken Sie auf diese Schaltfläche, um die Priorität der „Queues“ auf Default-Werte zurückzusetzen.
Priorität	0 ... 7	In dieser Spalte wird die jeweilige Prioritätsebene angezeigt. 0 = niedrigste Priorität 7 = höchste Priorität
Queue-ID	0 ... 7	Wählen Sie im Auswahlfeld die Nummer einer „Queue“ für Pakete mit der Prioritätsebene.

Tabelle 72: Default-Einstellungen

Priorität	Queue-ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

10.4.1.1.4 Schedule-Modus

QoS

Port-Priorität

IP DiffServ (DSCP)

Priorität/Queue-Zuordnung

Schedule-Modus

Schedule-Modus-Einstellungen

Schedule-Modus:

High First(SPQ) ▾

Queue ID	Weight Value (Bereich:1~127)
0	
1	
2	
3	
4	
5	
6	
7	

Anwenden

Aktualisieren

Konfiguration speichern

Abbildung 57: WBM-Seite „QoS“ – Register „Schedule-Modus“

Tabelle 73: WBM-Seite „QoS“ – Register „Schedule-Modus“

Schedule-Modus-Einstellungen		
Parameter	Standardwert	Beschreibung
Schedule-Modus	Strict Priority Queuing (SPQ)	Wählen Sie im Auswahlfeld „Strict Priority Queuing (SPQ)“, wenn Sie die „Hardware Priority Queues“ der Reihe nach abarbeiten wollen.
	Weighted Round Robin (WRR)	Wählen Sie im Auswahlfeld „Weighted Round Robin (WRR)“, wenn Sie den Algorithmus auf Basis der Queue-Gewichtung (der Wert, den Sie im Feld Weight Value (Bereich: 1~127) eintragen) nutzen wollen. Queues mit höherer Gewichtung werden bevorzugter abgearbeitet als andere mit geringerer Gewichtung.
Queue ID	0 ... 7	In dieser Spalte wird angezeigt, welche „Queue“ konfiguriert wird. 0 = niedrigste Priorität 7 = höchste Priorität
Weight Value (Bereich: 1~127)	1 ... 127	Der „Weight Value“ kann nur konfiguriert werden, wenn „Weighted Round Robin (WRR)“ ausgewählt ist. Die Bandbreite wird unter den verschiedenen „Traffic Queues“ entsprechend ihrer Gewichtung aufgeteilt. 0 = niedrigste Priorität 127 = höchste Priorität
		Hinweis  Änderung des „Weight Value (Bereich: 1~127)“ Wenn Sie „Strict Priority Queuing (SPQ)“ ausgewählt haben, können Sie nicht den „Weight Value“ ändern. Dafür müssen Sie zunächst „Weighted Round Robin (WRR)“ wählen. Danach können Sie „Strict Priority Queuing (SPQ)“ ändern.

10.4.1.2 Bandbreitenbegrenzung

10.4.1.2.1 Sturmbegrenzung

Hinweis



Weitere Information

Weitere Informationen zur „Sturmbegrenzung“ finden Sie im Kapitel „Funktionsbeschreibung“.

Bandbreitenbegrenzung

Sturmbegrenzung
Bandbreitenbegrenzung

Sturmbegrenzungseinstellungen

Bandbreitenbegrenzungs-Mode pps

Port		Anzahl	Typ
von:	1	an: 1	0 (einheiten)
			Mcast(Multicast)

Deaktivieren:0. Eine Einheit ist ca. 652 pps

Anwenden
Aktualisieren
Konfiguration speichern

Sturmkontrollstatus

Port	Anzahl (einheiten)	Multicast	Broadcast	DLF	Port	Anzahl (einheiten)	Multicast	Broadcast	DLF
1	1	Ausschalten	Einschalten	Einschalten	2	1	Ausschalten	Einschalten	Einschalten
3	1	Ausschalten	Einschalten	Einschalten	4	1	Ausschalten	Einschalten	Einschalten
5	1	Ausschalten	Einschalten	Einschalten	6	1	Ausschalten	Einschalten	Einschalten
7	1	Ausschalten	Einschalten	Einschalten	8	1	Ausschalten	Einschalten	Einschalten
9	1	Ausschalten	Einschalten	Einschalten	10	1	Ausschalten	Einschalten	Einschalten
11	1	Ausschalten	Einschalten	Einschalten	12	1	Ausschalten	Einschalten	Einschalten

Abbildung 58: WBM-Seite „Bandbreitenbegrenzung“ – Register „Sturmbegrenzung“

Tabelle 74: WBM-Seite „Rate Limitation“ – Register „Sturmbegrenzung“

Sturmbegrenzungseinstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Sturmbegrenzungseinstellungen“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Sturmbegrenzungseinstellungen“ zu konfigurieren.
Anzahl (Einheiten)		0	Wählen Sie im Auswahlfeld die Anzahl der Pakete (des im Feld „Typ“ spezifizierten Typs) aus, die der Switch pro Sekunde empfangen kann.
Typ		Bcast (Broadcast)	Wählen Sie im Auswahlfeld „Bcast (Broadcast)“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Broadcast-Pakete festzulegen.
		Mcast (Multicast)	Wählen Sie im Auswahlfeld „Mcast (Multicast)“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Multicast-Pakete festzulegen.
		DLF	Wählen Sie im Auswahlfeld „DLF“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen DLF-Pakete festzulegen.
		Mcast+Bcast	Wählen Sie im Auswahlfeld „Mcast+Bcast“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Multicast-Pakete und Broadcast-Pakete festzulegen.
		Mcast+DLF	Wählen Sie im Auswahlfeld „Mcast+DLF“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Multicast-Pakete und DLF-Pakete festzulegen.
		Bcast+DLF	Wählen Sie im Auswahlfeld „Bcast+DLF“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Broadcast-Pakete und DLF-Pakete festzulegen.
		Mcast+Bcast+DLF	Wählen Sie im Auswahlfeld „Mcast+Bcast+DLF“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Multicast-Pakete, Broadcast-Pakete und DLF-Pakete festzulegen.
Sturmkontrollstatus			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Anzahl (Einheiten)			In dieser Spalte werden die Anzahl der Pakete angezeigt, die der Switch pro Sekunde empfangen kann.
Multicast		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für Multicast gilt.
Broadcast		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für Broadcast gibt.
DLF		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für DLF gibt.

10.4.1.2.2 Bandbreitenbegrenzung

Hinweis



Weitere Information

Weitere Informationen zur „Bandbreitenbegrenzung“ finden Sie im Kapitel „Funktionsbeschreibung“.

Bandbreitenbegrenzung

Sturmbegrenzung
Bandbreitenbegrenzung

Bandbreitenbegrenzungs-Einstellungen

Port	Ingress	Egress
von: 1 an: 1	0 (Mbps)	0 (Mbps)

(Ausschalten: 0)

Anwenden
Aktualisieren
Konfiguration speichern

Bandbreitenbegrenzungs-Status

Port	Ingress (Mbps)	Egress (Mbps)	Port	Ingress (Mbps)	Egress (Mbps)
1	0	0	2	0	0
3	0	0	4	0	0
5	0	0	6	0	0
7	0	0	8	0	0
9	0	0	10	0	0
11	0	0	12	0	0

Abbildung 59: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“

Tabelle 75: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“

Bandbreitenbegrenzungseinstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Bandbreitenbegrenzungseinstellungen“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Bandbreitenbegrenzungseinstellungen“ zu konfigurieren.
Ingress (Mbs)		0	Geben Sie im Eingabefeld die „Bandbreitenbegrenzung“ für eingehende Pakete ein. Port 1 ... 8 0 ... 100 Port 9 ... 10(12) 0 ... 1000
Egress (Mbs)		0	Geben Sie im Eingabefeld die „Bandbreitenbegrenzung“ für ausgehende Pakete ein.
Bandbreitenbegrenzungsstatus			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Ingress (Mbs)			In dieser Spalte werden die eingestellten Bandbreiten für Ingress angezeigt.
Egress (Mbs)			In dieser Spalte werden die eingestellten Bandbreiten für Egress angezeigt.

10.4.2 IGMP-Snooping

Hinweis



Weitere Information

Weitere Informationen zu „IGMP-Snooping“ (Internet **G**roup **M**anagement Protocol Snooping) finden Sie im Kapitel „Funktionsbeschreibung“.

10.4.2.1 IGMP-Snooping

10.4.2.1.1 Allgemeine Einstellungen

IGMP Snooping

Allgemeine Einstellungen
Port-Einstellungen
Querier-Einstellungen

IGMP-Snooping-Einstellungen

IGMP-Snooping-Status

Status der Berichtsunterdrückung

IGMP-Snooping-VLAN-Status

Unbekannte Multicast-Pakete

IGMP-Snooping-Status

IGMP-Snooping-Status	Ausschalten
Status der Berichtsunterdrückung	Ausschalten
IGMP-Snooping-VLAN-Status	Keine
Unbekannte Multicast-Pakete	Verwerfen

Abbildung 60: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“

Tabelle 76: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“

IGMP-Snooping-Einstellungen		
Parameter	Standardwert	Beschreibung
IGMP-Snooping-Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „IGMP-Snooping“ zu aktivieren und Multicast-Gruppendaten nur zu den Ports weiterzuleiten, die Mitglieder dieser Gruppe sind.
Reportunterdrückungsstatus	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Reportunterdrückungsfunktion“ bei aktivem „IGMP-Snooping“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „Reportunterdrückungsfunktion“ bei aktivem „IGMP-Snooping“ zu aktivieren.
IGMP-Snooping-VLAN-Status	Ergänzen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, bei denen der Switch „IGMP-Snooping“ ausführen soll. Gültiger Bereich der VLAN-IDs: 1 ... 4094. Verwenden Sie ein Komma (,) bzw. einen Bindestrich (-), um einzelne VLANs bzw. VLAN-Bereiche anzugeben.
	Löschen	Wählen Sie im Auswahlfeld „Löschen“ und tragen Sie die VLANs ein, in denen der Switch kein „IGMP-Snooping“ ausführen soll.
Unbekannte Multicast-Pakete		In diesem Auswahlfeld können Sie die Vorgehensweise des Switches beim Empfang unbekannter Multicast-Frames spezifizieren.
	Verwerfen	Wählen Sie im Auswahlfeld „Verwerfen“, wenn diese Frames verworfen werden sollen.
	Weiterleiten	Wählen Sie im Auswahlfeld „Weiterleiten“, wenn diese Frames an alle Ports weitergeleitet werden sollen.
IGMP-Snooping-Status		
Parameter	Standardwert	Beschreibung
IGMP-Snooping-Status	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob „IGMP-Snooping“ global aktiviert oder deaktiviert ist.
Reportunterdrückungsstatus	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob die „Reportunterdrückungsfunktion“-Funktion beim „IGMP-Snooping“ aktiviert oder deaktiviert ist.
IGMP-Snooping-VLAN-Status	Keiner 1 ... 4094	In diesem Anzeigefeld werden die VLANs angezeigt, in denen der Switch „IGMP-Snooping“ ausführt. Es wird „Keiner“ angezeigt, wenn noch für keinen Port „IGMP-Snooping“ aktiviert wurde.
Unbekannte Multicast-Pakete	Verwerfen Weiterleiten	In diesem Anzeigefeld wird angezeigt, ob der Switch unbekannte Multicast-Pakete verwirft oder an alle Ports weiterleitet.

10.4.2.1.2 Port-Einstellungen

IGMP Snooping

Allgemeine Einstellungen
Port-Einstellungen
Querier-Einstellungen

Port-Einstellungen

Port	Querier Mode	Immediate Leave
von: 1 ▼ an: 1 ▼	Auto ▼	Ausschalten ▼

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	Querier Mode	Immediate Leave	Port	Querier Mode	Immediate Leave
1	Auto	Ausschalten	2	Auto	Ausschalten
3	Auto	Ausschalten	4	Auto	Ausschalten
5	Auto	Ausschalten	6	Auto	Ausschalten
7	Auto	Ausschalten	8	Auto	Ausschalten
9	Auto	Ausschalten	10	Auto	Ausschalten
11	Auto	Ausschalten	12	Auto	Ausschalten

Abbildung 61: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“

Tabelle 77: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“

Port-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Einstellungen“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Einstellungen“ zu konfigurieren.
Querier Mode		Auto	Wählen Sie im Auswahlfeld die Einstellung „Auto“ aus, wenn der Switch den Port als einen „IGMP-Query-Port“ nutzen soll, wenn er „IGMP-Query“-Pakete empfängt.
		Fix	Wählen Sie im Auswahlfeld die Einstellung „Fix“ aus, wenn der Switch den bzw. die Ports immer als „IGMP-Query-Ports“ nutzt. Diese Einstellung wird verwendet, wenn ein IGMP-Multicast-Server mit dem bzw. den Ports verbunden ist.
		Edge	Wählen Sie im Auswahlfeld die Einstellung „Edge“ aus, wenn der Switch den Port nicht als „IGMP-Query-Port“ nutzt. In diesem Fall protokolliert der Switch nicht, dass ein IGMP-Router mit diesem Port verbunden ist, und leitet die „IGMP-Join/Leave“-Pakete auch nicht an diesen Port weiter.
Immediate Leave		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Immediate-Leave“-Funktion an einzelnen Ports zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „Immediate-Leave“-Funktion an einzelnen Ports zu aktivieren.
Port-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Querier Mode		Auto Fix Edge	In dieser Spalte wird der „Querier“-Modus für den spezifischen Port angezeigt.
Immediate Leave		Ausschalten Einschalten	In dieser Spalte wird die „Immediate Leave“-Einstellung für den spezifischen Port angezeigt.

10.4.2.1.3 Querier-Einstellungen

IGMP Snooping

Allgemeine Einstellungen Port-Einstellungen **Querier-Einstellungen**

Querier-Einstellungen

Querier-Status:

Querier-VLAN-Status:

Querier Status

Querier-Status	Ausschalten
Querier-VLAN-Status	Keine

Abbildung 62: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“

Tabelle 78: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“

Querier-Einstellungen		
Parameter	Standardwert	Beschreibung
Querier-Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Querier-VLAN-Status	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um die VLAN-ID einzugeben.
	Löschen	Wählen Sie im Auswahlfeld „Löschen“, um die VLAN-ID zu löschen.
Querier-Status		
Parameter	Standardwert	Beschreibung
Querier-Status	Ausschalten Einschalten	In diesem Anzeigefeld wird der Querier-Status angezeigt.
Querier-VLAN-Status	Keiner 0 ... 4094	In diesem Anzeigefeld wird die VLAN-ID angezeigt.

10.4.2.2 IGMP-Filter

10.4.2.2.1 Allgemeine Einstellungen

IGMP-Filter

Allgemeine Einstellungen | Multicast-Gruppen | Port-Einstellungen

IGMP-Filtering-Einstellungen

IGMP Filtering State: Ausschalten ▾

Profil	Typ
	Verweigern ▾

Anwenden Aktualisieren Konfiguration speichern

IGMP-Filtering-Status

Profil	Typ	Ports	Aktion
--------	-----	-------	--------

Abbildung 63: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“

Tabelle 79: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“

IGMP-Filtering-Einstellungen		
Parameter	Standardwert	Beschreibung
IGMP-Filtering-Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Profil		Geben Sie im Eingabefeld den Namen für den IGMP-Filter ein.
Typ	Verweigern	Wählen Sie im Auswahlfeld „Verweigern“, um den Zugang zur Gruppe zu verweigern.
	Erlauben	Wählen Sie im Auswahlfeld „Erlauben“, um den Zugang zur Gruppe zu gewähren.
IGMP-Filtering-Status		
Parameter	Standardwert	Beschreibung
Profil		In dieser Spalte wird der Name des Profils angezeigt. Klicken Sie auf den Namen, um das Profil zu modifizieren.
Typ	Verweigern Erlauben	In dieser Spalte wird der Handlungstyp angezeigt.
Ports	1 ... 10 (12)	In dieser Spalte werden die Ports angezeigt, für die das Profil des IGMP-Filters aktiviert ist.
Aktion	Löschen	Klicken Sie auf [Löschen] , um die Multicast-Adressen zu löschen.

10.4.2.2.2 Multicast-Gruppen

IGMP-Filter

Allgemeine Einstellungen **Multicast-Gruppen** Port-Einstellungen

Gruppeneinstellung

Profil :

Gruppen	Startadresse	Endadresse
1		

Anwenden Aktualisieren Konfiguration speichern

Gruppenstatus

Profil	Typ	Gruppen	Startadresse	Endadresse	Aktion
--------	-----	---------	--------------	------------	--------

Abbildung 64: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“

Tabelle 80: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“

Gruppenstatus		
Parameter	Standardwert	Beschreibung
Profil		Wählen Sie im Auswahlfeld das Profil aus, das Sie für eine Gruppe konfigurieren möchten.
Gruppe	1 ... 10	Wählen Sie im Auswahlfeld eine Multicast-Gruppe aus.
Startadresse		Geben Sie im Eingabefeld die erste Multicast-Adresse der Gruppe ein, die Sie konfigurieren möchten.
Endadresse		Geben Sie im Eingabefeld die letzte Multicast-Adresse der Gruppe ein, die Sie konfigurieren möchten.
Gruppenstatus		
Parameter	Standardwert	Beschreibung
Profil		In dieser Spalte wird der Name des Profils angezeigt.
Typ	Verweigern Erlauben	In dieser Spalte wird der Handlungstyp angezeigt.
Gruppe	1 ... 10	In dieser Spalte wird die Gruppe angezeigt.
Startadresse		In dieser Spalte wird die erste Multicast-Adresse angezeigt.
Endadresse		In dieser Spalte wird die letzte Multicast-Adresse angezeigt.
Aktion	Löschen	Klicken Sie auf [Löschen] , um die Multicast-Adressen zu löschen.

10.4.2.2.3 Port-Einstellungen

Abbildung 65: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“

Tabelle 81: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“

Port-Einstellungen				
Parameter		Standardwert	Beschreibung	
Profil			Wählen Sie im Auswahlfeld das Profil aus, das Sie für eine Gruppe konfigurieren möchten.	
Port	Alle auswählen	○	○	Es ist kein Port ausgewählt.
			●	Es sind alle Ports ausgewählt.
	Alle deaktivieren	○	○	Es ist kein Port deaktiviert.
			●	Es sind alle Ports deaktiviert.
	□ 1 ... □ 10 (12)	□	□	Der Port ist nicht aktiviert..
Port-Status				
Parameter		Standardwert	Beschreibung	
Profil			In dieser Spalte wird der Name des Profils angezeigt.	
Typ		Verweigern Erlauben	In dieser Spalte wird der Handlungstyp angezeigt.	
Ports		1 ... 10 (12)	In dieser Spalte werden die Ports angezeigt, für die das Profil des IGMP-Filters aktiviert ist.	

10.4.2.3 Statische Multicast-Adressen**Hinweis****Weitere Information**

Weitere Informationen zu „Statische Multicast-Adressen“ finden Sie im Kapitel „Funktionsbeschreibung“.

Static Multicast

Statische Multicast-Adresseinstellungen

VLAN ID	MAC-Adresse	Port
1 ▾		

Multicast-Adresstabelle

VLAN ID	MAC-Adresse	Status	Port	Aktion
1	01:00:5e:22:33:44	Statisch	1-12	Löschen

Anzahl der Einträge : 1

Abbildung 66: WBM-Seite „Statische Multicast-Adressen“

Tabelle 82: WBM-Seite „Statische Multicast-Adressen“

Statische Multicast-Adresseinstellungen		
Parameter	Standardwert	Beschreibung
VLAN-ID	1	Wählen Sie im Auswahlfeld die VLAN-ID aus, die Sie konfigurieren möchten.
MAC-Adresse		Geben Sie in Eingabefeld die Multicast-MAC-Adresse des jeweiligen Rings ein. Konfigurieren Sie eine Multicast-MAC, die keine „Age Time“ erhalten soll. Das gültige Format ist: 0x:0x:0x:0x:0x:0x.
Port		Geben Sie im Eingabefeld den Teilnehmer-Port für die Multicast-Adresse ein.
Multicast-Adresstabelle		
Parameter	Standardwert	Beschreibung
VLAN-ID	0 ... 4094	In dieser Spalte werden die ausgewählten VLAN-ID angezeigt.
MAC-Adresse		In dieser Spalte werden die Multicast-Adressen angezeigt.
Status		In dieser Spalte wird der Status der Multicast-Adressen angezeigt.
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Aktion		Klicken Sie auf [Löschen] , um die Multicast-Adressen zu löschen.
Anzahl der Einträge		In diesem Anzeigefeld wird die Gesamtanzahl der Einträge in der Multicast-Adress-Tabelle angezeigt.

10.4.2.4 Multicast-Statistiken

Multicast Statistics						
Multicast-IP-Tabelle						
Index	Port	Multicast-Gruppe	VID	Timeout	Explicit Tracking	Host IP
1	1	0.0.0.0	1	260	Ausschalten	
2	2	0.0.0.0	1	260	Ausschalten	
3	3	0.0.0.0	1	260	Ausschalten	
4	4	0.0.0.0	1	260	Ausschalten	
5	5	0.0.0.0	1	260	Ausschalten	
6	6	0.0.0.0	1	260	Ausschalten	
7	7	0.0.0.0	1	260	Ausschalten	
8	8	0.0.0.0	1	260	Ausschalten	
9	9	0.0.0.0	1	260	Ausschalten	
10	10	0.0.0.0	1	260	Ausschalten	
11	11	0.0.0.0	1	260	Ausschalten	
12	12	0.0.0.0	1	260	Ausschalten	

Aktualisieren

Abbildung 67: WBM-Seite „Multicast-Statistiken“

Tabelle 83: WBM-Seite „Multicast-Statistiken“

Multicast-IP-Tabelle		
Parameter	Standardwert	Beschreibung
Index	1 ... 10 (12)	In dieser Spalte wird die Anzahl der Einträge angezeigt.
Port	1 ... 10 (12)	In dieser Spalte wird die Port-Nummer angezeigt.
Multicast-Gruppe		In dieser Spalte wird die IP-Adresse der Multicast-Gruppe angezeigt.
VLAN-ID		In dieser Spalte wird die VLAN-ID angezeigt.
Timeout		In dieser Spalte wird die Timeout-Zeit angezeigt.
Explicit Tracking		In dieser Spalte wird angezeigt, ob „Explicit Tracking“ eingestellt ist.
Host-IP		In dieser Spalte wird die Host-IP angezeigt.

10.4.3 VLAN

Hinweis



Weitere Information

Weitere Informationen zu „VLAN“ (Virtual Local Area Network) finden Sie im Kapitel „Funktionsbeschreibung“.

10.4.3.1 Port Isolation

Hinweis



Weitere Information

Weitere Informationen zur „Port Isolation“ finden Sie im Kapitel „Funktionsbeschreibung“.

Port Isolation

Port-Isolationseinstellungen

Port von: an:

Egress Port :

☐ Alle auswählen ☐ Alle deaktivieren

☒ 1 ☒ 3 ☒ 5 ☒ 7 ☒ 9 ☒ 11

☒ 2 ☒ 4 ☒ 6 ☒ 8 ☒ 10 ☒ 12 ☒ 0 (CPU)

Port-Isolationsstatus

Port	Egress Port												
	0	1	2	3	4	5	6	7	8	9	10	11	12
1	v	v	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v	v	v	v
11	v	v	v	v	v	v	v	v	v	v	v	v	v
12	v	v	v	v	v	v	v	v	v	v	v	v	v

Abbildung 68: WBM-Seite „Port Isolation“

Tabelle 84: WBM-Seite „Port Isolation“

Port-Isolierungseinstellungen				
Parameter		Standardwert	Beschreibung	
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Isolation“ konfigurieren möchten.	
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Isolation“ konfigurieren möchten.	
Ausgangs-Port			Ein Ausgangs-Port ist ein ausgehender Port, über den ein Datenpaket gesendet wird. Die Auswahl eines Ports als Ausgangs-Port bedeutet, dass er mit dem Port, den Sie gerade konfigurieren, kommunizieren wird.	
	Alle auswählen	☐	☐	Es ist kein Ausgangs-Port ausgewählt.
			☒	Es sind alle Ausgangs-Ports ausgewählt.
	Alle deaktivieren	☐	☐	Es ist kein Ausgangs-Port deaktiviert.
			☒	Es sind alle Ausgangs-Ports deaktiviert.
	☐ 0 (CPU) ... ☐ 10 (12)	☐	☐	Der Ausgangs-Port ist nicht aktiviert.
			☒	Der Ausgangs-Port ist aktiviert.
Port-Isolierungsstatus				
Parameter		Standardwert	Beschreibung	
Port		V	V	„V“ zeigt an, dass die Pakete des Ports zu diesem Port gesendet werden können.
Ausgangs-Port			-	„-“ zeigt an, dass die Pakete des Ports nicht zu diesem Port gesendet werden können.

10.4.3.2 VLAN

10.4.3.2.1 VLAN-Einstellungen

VLAN

VLAN-Einstellungen
Tag-Einstellungen
Port-Einstellungen

VLAN-Einstellungen

VLAN ID	VLAN Name	Member Port
von: an:		

VLAN List

VLAN ID	VLAN Name	VLAN Status	Member Port	Aktion
1	VLAN1	Static	1-12	

Abbildung 69: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“

Tabelle 85: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“

VLAN-Einstellungen			
Parameter		Standardwert	Beschreibung
VLAN-ID	von:		Geben Sie im Eingabefeld die VLAN-ID für diesen Eintrag ein. Gültiger Bereich: 1 ... 4094
	an:		Geben Sie im Eingabefeld die VLAN-ID für diesen Eintrag ein. Gültiger Bereich: 1 ... 4094
VLAN-Name			Geben Sie im Eingabefeld zur eindeutigen Kennzeichnung einen aussagekräftigen Namen für das VLAN ein. Der VLAN-Name sollte aus einer Kombination aus Zahlen, Buchstaben, Bindestrichen (-) oder Unterstrichen (_) bestehen.
Mitglied-Port			Geben Sie im Eingabefeld die Port-Nummern ein, die der Switch dem VLAN als Teilnehmer zuordnen soll. Sie können mehrere einzelne Port-Nummern bzw. -Bereiche angeben, indem Sie Einzel-Ports durch Komma (,) trennen bzw. bei Port-Bereichen einen Bindestrich (-) verwenden.
VLAN-Liste			
Parameter		Standardwert	Beschreibung
VLAN-ID		1 ... 4094	In dieser Spalte wird die Indexnummer des VLAN-Eintrags angezeigt. Klicken Sie auf die Nummer, um den VLAN-Eintrag zu modifizieren.
VLAN Name			In dieser Spalte wird der Name des VLANs angezeigt.
VLAN Status		Static Dynamic 802.1Q-VLAN	In dieser Spalte wird der Status des VLANs angezeigt.
Mitglied-Port		1-10 (12)	In dieser Spalte wird angezeigt, welche Ports dem VLAN als Teilnehmer zugeordnet sind.
Aktion		Klicken Sie auf [Löschen] , um das VLAN zu löschen.	
		Hinweis 	Löschen VLAN1 Das Löschen von VLAN1 ist nicht möglich.

10.4.3.2.2 Tag-Einstellungen

VLAN

VLAN-Einstellungen
Tag-Einstellungen
Port-Einstellungen

Tag-Einstellungen

VLAN ID von: an:

Tag Port :

☐ Alle auswählen
☐ Alle deaktivieren

☐ 1 ☐ 3 ☐ 5 ☐ 7
☐ 9 ☐ 11

☐ 2 ☐ 4 ☐ 6 ☐ 8
☐ 10 ☐ 12

Tag-Status

VLAN ID	Tag Ports	Untagged Ports
1		1-12

Abbildung 70: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“

Tabelle 86: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“

Tag-Einstellungen				
Parameter		Standardwert	Beschreibung	
VLAN-ID	von:		Geben Sie im Eingabefeld die VLAN-ID für diesen Eintrag ein. Gültiger Bereich: 1 ... 4094	
	an:		Geben Sie im Eingabefeld die VLAN-ID für diesen Eintrag ein. Gültiger Bereich: 1 ... 4094	
Tag-Port	Alle auswählen	☐	☐	Es ist kein Port als Port mit Tag ausgewählt.
			☒	Es sind alle Ports als Port mit Tag ausgewählt.
	Alle deaktivieren	☐	☐	Es ist kein Port mit Tag deaktiviert.
			☒	Es sind alle Ports mit Tag deaktiviert.
	☐ 1 ... ☐ 10 (12)	☐	☐	Der Port ist nicht aktiviert.
			☒	Der Port ist aktiviert.
Tag-Status				
Parameter		Standardwert	Beschreibung	
VLAN-ID		1 ... 4094	In dieser Spalte wird die VLAN-ID angezeigt.	
Tag-Ports		1 ... 7	In dieser Spalte werden die Ports angezeigt, die als Ports mit Tag zugeordnet sind.	
Untagged-Ports		1 ... 7	In dieser Spalte werden die Ports angezeigt, die als Ports ohne Tag zugeordnet sind.	

10.4.3.2.3 Port-Einstellungen

VLAN

VLAN-Einstellungen
Tag-Einstellungen
Port-Einstellungen

Port-Einstellungen

Port	PVID	Acceptable Frame
von: 1 an: 1	1	Alle

Port-Status

Port	PVID	Acceptable Frame	Port	PVID	Acceptable Frame
1	1	untagged Frame	2	1	Alle
3	1	Alle	4	1	Alle
5	1	Alle	6	1	Alle
7	1	Alle	8	1	Alle
9	1	Alle	10	1	Alle
11	1	Alle	12	1	Alle

Abbildung 71: WBM-Seite „VLAN“ – Register „Port-Einstellungen“

Tabelle 87: WBM-Seite „VLAN“ – Register „Port-Einstellungen“

Port-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Einstellungen“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Einstellungen“ zu konfigurieren.
PVID		1	Wählen Sie im Auswahlfeld die PVID (Port-VLAN-ID-Nummer) aus.
Akzeptabler Rahmen			In diesem Auswahlfeld können Sie die für einen Port zulässigen Frame-Typen spezifizieren.
		Alle	Wählen Sie im Auswahlfeld „Alle“ aus, wenn an diesem Port alle Frames (mit und ohne Tag) akzeptiert werden sollen.
		nur untagged VLANs	Wählen Sie im Auswahlfeld „nur untagged VLANs“, wenn an diesem Port nur Frames ohne Tag akzeptiert werden sollen. Alle Frames mit Tag werden verworfen.
		nur tagged VLANs	Wählen Sie im Auswahlfeld „nur tagged VLANs“, wenn an diesem Port nur Frames mit Tag akzeptiert werden sollen. Alle Frames ohne Tag werden verworfen.
Port-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
PVID			In dieser Spalte werden die VLAN-ID-Nummern angezeigt.
Akzeptabler Rahmen		Alle nur untagged VLANs nur tagged VLANs	In dieser Spalte werden die für diesen Port zulässigen Frame-Typen angezeigt.

10.4.3.3 MAC-VLAN

Hinweis



Weitere Information

Weitere Informationen zu „MAC-VLAN“ (**Media Access Control-Virtual Local Area Network**) finden Sie im Kapitel „Funktionsbeschreibung“.

MAC VLAN

MAC-VLAN-Einstellungen

MAC-Adresse	VLAN	Priorität
		0 ▼

Ex:00:0B:04 filtert nur 3 Byte der Source-MAC-Adresse.
 00:0B:04:11:22 filtert nur 5 Byte der Source-MAC-Adresse.
 00:0B:04:11:22:33 filtert alle Byte der Source-MAC-Adresse.

MAC-VLAN-Tabelle

Index	MAC-Adresse	VLAN	Priorität	Aktion

Abbildung 72: WBM-Seite „MAC-VLAN“

Tabelle 88: WBM-Seite „MAC-VLAN“

MAC-VLAN-Einstellungen		
Parameter	Standardwert	Beschreibung
MAC-Adresse		Geben Sie im Eingabefeld die ersten drei oder mehr Byte der MAC-Adresse ein.
VLAN		Geben Sie im Eingabefeld den Wert für das MAC-VLAN für die Instanz ein. Gültiger Bereich: 1 ... 4094 Es können ein oder mehrere Daten-VLANs konfiguriert werden.
Priorität	0 ... 7	Wählen Sie im Auswahlfeld die jeweilige Priorität für den spezifischen Port aus. 0 = niedrigste Priorität 7 = höchste Priorität
MAC-VLAN-Tabelle		
Parameter	Standardwert	Beschreibung
Index	1 ... 10	In dieser Spalte wird die Anzahl der Einträge angezeigt.
MAC-Adresse		In dieser Spalte wird die MAC-Adresse angezeigt.
VLAN		In dieser Spalte wird die VLAN-ID für den spezifischen Port angezeigt.
Priorität	0 ... 7	In dieser Spalte wird die Priorität für den spezifischen Port angezeigt.
Aktion		Klicken Sie auf [Löschen] , um die Multicast-Adressen zu löschen.

10.4.4 LLDP

Hinweis



Weitere Information

Weitere Informationen zu „LLDP“ (Link Layer Discovery Protocol) finden Sie im Kapitel „Funktionsbeschreibung“.

10.4.4.1 Einstellungen

LLDP

LLDP-Einstellungen
Nächste

LLDP-Einstellungen

Status Ausschalten ▼

Tx Interval 30 Sekunden (Bereich: 1-3600)

Tx Hold 4 Mal (Bereich: 2-100)

Time To Live 120 Sekunden

Port	Status
von: 1 ▼ an: 1 ▼	Einschalten ▼

Anwenden
Aktualisieren
Konfiguration speichern

LLDP-Status

Port	Status	Port	Status
1	Einschalten	2	Einschalten
3	Einschalten	4	Einschalten
5	Einschalten	6	Einschalten
7	Einschalten	8	Einschalten
9	Einschalten	10	Einschalten
11	Einschalten	12	Einschalten

Abbildung 73: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“

Tabelle 89: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“

LLDP-Einstellungen		
Parameter		Standardwert
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um LLDP-Funktion für den Switch global zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „LLDP“-Funktion für den Switch global zu aktivieren.
TX-Interval	30	Geben Sie im Eingabefeld den Wert für das „TX-Interval“ (Übertragungsintervall) für die LLDP-Pakete ein.
TX-Hold	4	Geben Sie im Eingabefeld den Wert für die „TX-Hold-Time“ (TX-Haltezeit) ein, die die TTL der Nachricht des Switches bestimmt. (TTL = tx-hold * tx-interval)
Time To Live	120	In diesem Anzeigefeld wird die Lebenszeit für die Informationen des Switches angezeigt.
Port	von:	1
	an:	1
Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „LLDP“-Funktion an einzelnen Ports zu aktivieren.
	Rx Only	Wählen Sie im Auswahlfeld die Einstellung „Rx Only“ aus, wenn für den Switch bzw. die Ports immer „Rx Interval“ als Übertragungsintervall genutzt wird.
	Tx Only	Wählen Sie im Auswahlfeld die Einstellung „Tx Only“ aus, wenn für den Switch bzw. die Ports immer „Tx Interval“ als Übertragungsintervall genutzt wird.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „LLDP“-Funktion an einzelnen Ports zu deaktivieren.
LLDP-Status		
Parameter		Standardwert
Port		1 ... 10 (12)
Status		Ausschalten Einschalten
		In dieser Spalte wird angezeigt, ob „LLDP“ aktiviert oder deaktiviert ist.

10.4.4.2 Nachbarerkennung

LLDP

Einstellungen **Nächste**

LLDP-Nachbarinformationen

Port

Local Port 1	
Remote Port ID	GigabitEthernet1/0/8
Chassis ID	00-30-de-ff-f1-8c
Systemname	L2SWITCH
Systembeschreibung	WAGO/852-1305/000-001/V1.0.2.S0/Mon Mar 11 16:31:08 CST 2019
Systemfähigkeiten	Bridge/Switch (enabled)
Management IP	192.168.1.253
Time To Live	120 seconds

Abbildung 74: WBM-Seite „LLDP“ – Register „Nachbarerkennung“

Tabelle 90: WBM-Seite „LLDP“ – Register „Nachbarerkennung“

LLDP-Nachbarinformationen		
Parameter	Standardwert	Beschreibung
Port	Alle	Wählen Sie im Auswahlfeld „Alle“, wenn Sie von allen Nachbar-Ports Informationen angezeigt bekommen möchten.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld einen Port aus, von dessen Nachbar-Port Sie Informationen angezeigt bekommen möchten.
Lokal Port	1 ... 10 (12)	In diesem Anzeigefeld werden die Port-Nummern angezeigt.
Remote Port ID		In diesem Anzeigefeld wird die ID des verbundenen Ports angezeigt.
Chassis ID		In diesem Anzeigefeld wird die Chassis-ID des Nachbar-Ports angezeigt.
Systemname		In diesem Anzeigefeld wird der Systemname des Nachbar-Ports angezeigt.
Systembeschreibung		In diesem Anzeigefeld wird die Systembeschreibung des Nachbar-Ports angezeigt.
Systemfähigkeiten		In diesem Anzeigefeld werden die Systemfähigkeiten des Nachbar-Ports angezeigt.
Management IP		In diesem Anzeigefeld wird die Managementadresse des Nachbar-Ports angezeigt.
Time To Live		In diesem Anzeigefeld wird die Gültigkeitsdauer für die Informationen des Nachbar-Ports angezeigt.

10.4.5 Schleifenerkennung (Loop Detection)

Hinweis



Weitere Information

Weitere Informationen zu „Schleifenerkennung“ (Loop Detection) finden Sie im Kapitel „Funktionsbeschreibung“.

Loop Detection

Loop-Detection-Einstellungen

Status Ausschalten ▼

MAC-Adresse 00:0b:04:aa:aa:ab

Port	Status	Manual Recovery	Recovery Status	Recovery Zeit (min)
von: 1 ▼ an: 1 ▼	Ausschalten ▼	Keine ▼	Einschalten ▼	1 (Bereich: 1-60)

Anwenden Aktualisieren Konfiguration speichern

Loop-Detection-Status

Port	Status	Status	Recovery Status	Recovery Zeit (min)
1	Ausschalten	Normal	Einschalten	1
2	Ausschalten	Normal	Einschalten	1
3	Ausschalten	Normal	Einschalten	1
4	Ausschalten	Normal	Einschalten	1
5	Ausschalten	Normal	Einschalten	1
6	Ausschalten	Normal	Einschalten	1
7	Ausschalten	Normal	Einschalten	1
8	Ausschalten	Normal	Einschalten	1
9	Ausschalten	Normal	Einschalten	1
10	Ausschalten	Normal	Einschalten	1
11	Ausschalten	Normal	Einschalten	1
12	Ausschalten	Normal	Einschalten	1

Abbildung 75: WBM-Seite „Schleifenerkennung“

Tabelle 91: WBM-Seite „Schleifenerkennung“

Schleifenerkennungseinstellungen			
Parameter		Standardwert	Beschreibung
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
MAC-Adresse			Geben Sie im Eingabefeld die MAC-Zieladresse ein, an die die Sonderpakete gesendet werden sollen. Empfängt der Port dieselben Pakete, wird er abgeschaltet.
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Guard Protection“ (Schleifenschutz) konfigurieren möchten.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Guard Protection“ (Schleifenschutz) konfigurieren möchten.
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Loop Guard“ (Schleifenschutz) für den Switch zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Loop Guard“ (Schleifenschutz) für den Switch zu aktivieren.
Aktion		Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie die Schleifenerkennung am Port ausschalten.
		Freischalten	Wählen Sie im Auswahlfeld „Freischalten“, wenn Sie die Funktionen „Status“ und „Loop Korrektur“ nicht verändern wollen.
Loop-Recovery		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit sich der Port nach Ablauf der zugewiesenen „Recovery-Zeit“ automatisch reaktiviert.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
Recovery-Zeit (min) (Bereich: 1~60)		1	Geben Sie im Eingabefeld den Wert für die „Recovery-Zeit“ (in Minuten) ein, die der Switch wartet, bevor er den Port reaktiviert. Zeitraum: 1 ... 60 min
Schleifenerkennungsstatus			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Status		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob die Funktion „Loop Guard“ aktiviert oder deaktiviert ist.
Status		Keiner Normal	In dieser Spalte wird angezeigt, ob ein Port blockiert wird.
Loop-Recovery		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob die Funktion „Loop-Recovery“ aktiviert oder deaktiviert ist.
Recovery-Zeit (min)		1 ... 50	In dieser Spalte wird die „Recovery-Zeit“ für die Funktion „Loop-Recovery“ angezeigt.

10.4.6 MRP

MRP Global Settings

Global State
Ausschalten ▼

MRP Settings

Ring ID
Hinzufügen ▼

Status
Ausschalten ▼

Modus
Hinzufügen ▼
Client ▼

Uuid
Hinzufügen ▼

Port-1
Hinzufügen ▼

VLAN
Hinzufügen ▼
Bereich: 1~4094

Port-2
Hinzufügen ▼

Anwenden
Aktualisieren

MRP Status

Typ:
Alle ▼
Zeigen

MRP Status	Ausschalten		
Ring ID	1	Ring Status	Ausschalten
Device Mode	Client	State Machine Mode	Not Running
Uuid	ffff.ffff.ffff.ffff.ffff.ffff		
VLAN ID	1		
Port-1	1	Port-1-mode	Port Down
Port-2	2	Port-2-mode	Port Down

Abbildung 76: WBM-Seite „MRP Global Settings“

Tabelle 92: WBM-Seite „MRP“

MRP Global Settings		
Parameter	Standardwert	Beschreibung
Global State	Ausschalten	Wählen Sie im Auswahlfeld "Ausschalten", um diese Funktion der globalen MRP zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld "Einschalten", um diese Funktion der globalen MRP zu aktivieren.
MRP Settings		
Parameter	Standardwert	Beschreibung
Ring ID	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um eine (neuen) Ring-ID einzugeben.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um eine Ring-ID zu löschen.
Modus	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den Switch entweder als Client (MRC) oder Manager (MRM) zu konfigurieren.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um die Konfiguration des Switches entweder als Client (MRC) oder Manager (MRM) zu löschen.
Port 1	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den primären Anschluss für den MRP-Ring hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um den primären Anschluss für den MRP-Ring zu löschen.
Port 2	Hinzufügen	Wählen Sie im Auswahlfeld "Hinzufügen", um den sekundären Anschluss für den MRP-Ring hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen", um den sekundären Anschluss für den MRP-Ring zu löschen.
Status	Ausschalten	Wählen Sie im Auswahlfeld "Ausschalten", um den jeweiligen Ring einzuschalten.
	Einschalten	Wählen Sie im Auswahlfeld "Ausschalten", um den jeweiligen Ring einzuschalten.
UUID	Hinzufügen	Konfiguriert den "Universal Unique Identifier" (UUID) für den MRP-Ring. Dies ist eine Zeichenkette im hexadezimalen Format, die den Ring darstellt, zu dem dieser Schalter gehört. Beispiel: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Entfernen	
VLAN	Hinzufügen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, für die dieser Ring aktiviert werden soll. Gültiger Bereich der VLAN-IDs: 1 ... 4094. Verwenden Sie ein Komma (,) bzw. einen Bindestrich (-), um einzelne VLANs bzw. VLAN-Bereiche anzugeben.
	Entfernen	Wählen Sie im Auswahlfeld "Entfernen" und geben Sie die VLANs ein, in denen der Switch nicht aktiviert werden soll.

Tabelle 92: WBM-Seite „MRP“

MRP Status (aktueller Zustand des jeweiligen MRP-Rings)		
Parameter	Standardwert	Beschreibung
Typ	Alle	Wählen Sie im Auswahlfeld „Alle“ aus, wenn Sie alle MRP-Status anzeigen möchten.
	Ring_1 ... Ring_4	Wählen Sie im Auswahlfeld die Ring-ID aus, für die der MRP-Status der ausgewählten Ring ID angezeigt werden soll.
MRP Status	–	In diesem Anzeigefeld wird der aktuelle Zustand des jeweiligen MRP-Rings angezeigt.
Ring ID	–	In diesem Anzeigefeld wird die ID-Nummer des MRP-Rings angezeigt.
Device Mode	–	In diesem Anzeigefeld wird der Modus des Switches angezeigt: Client (CRM)/Manager (MRM)
Uuid	–	In diesem Anzeigefeld wird die zugewiesene UUID angezeigt.
Vlan ID	–	In diesem Anzeigefeld wird angezeigt, in welchem VLAN dieser Ring gehört.
Port-1	–	In diesem Anzeigefeld wird der zugeordnete Port des Switches angezeigt.
Port-2	–	In diesem Anzeigefeld wird der zugeordnete Port des Switches angezeigt.
Ring Status	–	In diesem Anzeigefeld wird der aktuelle Status des MRP-Rings angezeigt.
State Machine Mode	–	In diesem Anzeigefeld wird angezeigt, ob die MRP-Zustandsmaschine läuft oder nicht.
Port-1-mode	–	In diesem Anzeigefeld wird Status des Ports angezeigt: (port down/port up).
Port-2-mode	–	In diesem Anzeigefeld wird Status des Ports angezeigt: (port down/port up).

10.4.7 Spanning Tree Protocol

Hinweis



Weitere Information

Weitere Informationen zu „Spanning Tree Protocol“ (STP) finden Sie im Kapitel „Funktionsbeschreibung“.

10.4.7.1 Allgemeine Einstellungen

Spanning Tree Protocol

Allgemeine Einstellungen
Port-Parameter
STP-Status

Spanning-Tree-Protocol-Einstellungen

Status

Modus

Bridge-Parameter

Forward Delay

(Bereich:4-30)

Max Age

(Bereich:6-40)

Hello Time

(Bereich:1-10)

Priorität

(Bereich:0-61440)

Pathcost Method

Beziehungsformel:
 $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Abbildung 77: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“

Tabelle 93: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“

Spanning-Tree-Protocol-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Spanning Tree Protocol“ (STP) oder das „Rapid Spanning Tree Protocol“ (RSTP) zu verwenden.
Mode	RSTP	Wählen Sie im Auswahlfeld „RSTP“, wenn Sie das schnellere „Rapid Spanning Tree Protocol“ verwenden möchten.
	MSTP	Wählen Sie im Auswahlfeld „MSTP“, wenn Sie das „Multiple Spanning Tree Protocol“ verwenden möchten.
	STP	Wählen Sie im Auswahlfeld „STP“, wenn Sie das „Spanning Tree Protocol“ verwenden möchten.
Bridge Parameters		
Parameter	Standardwert	Beschreibung
Forward Delay	15	Geben Sie im Eingabefeld die Zeit „Forward Delay“ ein. Gültiger Bereich: 4 ... 30 s
Max-Age	20	Geben Sie im Eingabefeld die Zeit „Max-Age“ ein. Gültiger Bereich: 6 ... 40 s
Hello-Time	2	Geben Sie im Eingabefeld die Zeit für die „Hello-Time“ ein. Gültiger Bereich: 1 ... 10 s
Priorität	32768	Geben Sie im Eingabefeld einen Wert für die Priorität ein. Je niedriger der von Ihnen zugewiesene numerische Wert ist, desto höher ist die Priorität dieser Bridge. Gültiger Bereich: 0 ... 61440
Pfadkostenmethode	Kurz	Wählen Sie im Auswahlfeld „Kurz“, wenn Sie eine Größe von 16 Bit und eine Übertragungsgeschwindigkeit bis zu 10 GBit wählen möchten. 10 MBit = 100 100 MBit = 19 1 GBit = 4 10 GBit = 2
	Lang	Wählen Sie im Auswahlfeld „Lang“, wenn Sie eine Größe von 32 Bit und eine Übertragungsgeschwindigkeit bis zu 10 TBit wählen möchten. 10 MBit = 2000000 100 MBit = 200000 1 GBit = 20000 10 GBit = 2000 100 GBit = 200 1 TBit = 20

10.4.7.2 Port-Parameter

Spanning Tree Protocol

Allgemeine Einstellungen
Port-Parameter
STP-Status

Port-Parameter-Einstellungen

Port	Aktiv	Path Cost	Priorität	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
von: 1 ▼ an: 1 ▼	Einschalten ▼	4	128	Ausschalten ▼	Ausschalten ▼	Ausschalten ▼	Ausschalten ▼

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	Aktiv	Role	Status	Path Cost	Priorität	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Einschalten	Root	Weiterleitung	4	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
2	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
3	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
4	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
5	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
6	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
7	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
8	Einschalten	Designated	Weiterleitung	19	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
9	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
10	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
11	Einschalten	Alternated	Verwerfen	4	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten
12	Einschalten	Keine	Verwerfen	250	128	Ausschalten	Ausschalten	Ausschalten	Ausschalten

Abbildung 78: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Tabelle 94: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Port-Parametereinstellungen			
Parameter		Standardwert	Beschreibung
Port	From:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
	To:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
Active		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die „STP“-Funktion für den spezifischen Port aktivieren möchten.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die STP-Funktion für den spezifischen Port deaktivieren möchten.
Pfadkosten		250	Geben Sie im Eingabefeld den Wert für die Pfadkosten für den spezifischen Port ein.
Priorität		128	Geben Sie im Eingabefeld den Wert für die Priorität für den spezifischen Port ein.
Edge-Port		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um den Typ „Edge-Port“ für den spezifischen Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Typ „Edge-Port“ für den spezifischen Port zu aktivieren.
BPDU-Filter		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die BPDU-Filterfunktion für den spezifischen Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die BPDU-Filterfunktion für den spezifischen Port zu aktivieren.
BPDU-Guard		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „BPDU-Guard“ für den spezifischen Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „BPDU-Guard“ für den spezifischen Port zu aktivieren.
ROOT-Guard		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „ROOT-Guard“ für den spezifischen Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „ROOT-Guard“ für den spezifischen Port zu aktivieren.

Tabelle 94: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Port-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Active	Einschalten Ausschalten	In dieser Spalte wird der Zustand der „STP“-Funktion angezeigt.
Rolle	Alternated Designated Root Backup None	In dieser Spalte wird die Rolle des Ports angezeigt.
Status	Discarding Blocking Listening Learning Forwarding Disabled	In dieser Spalte wird der Port-Status angezeigt.
Pfadkosten	0 ... 65535	In dieser Spalte werden die Pfadkosten des Ports angezeigt.
Priorität	0 ... 61440	In dieser Spalte wird die Priorität des Ports angezeigt.
Edge-Port	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „Edge-Port“ angezeigt.
BPDU-Filter	Ausschalten Einschalten	In dieser Spalte wird der Zustand der BPDU-Filterfunktion angezeigt.
BPDU-Guard	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „BPDU-Guard“ angezeigt.
ROOT-Guard	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „Root-Guard“ angezeigt.

10.4.7.3 STP-Status

Spanning Tree Protocol

Allgemeine Einstellungen
Port-Parameter
STP-Status

Aktueller Root-Status

MAC-Adresse	Priorität	Max Age	Hello Time	Forward Delay
00:30:de:ff:f1:8c	32768	20	2	15

Aktueller Bridge-Status

MAC-Adresse	Priorität	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:30:de:ff:f1:9b	32768	20	2	15	4	1

Abbildung 79: WBM-Seite „Spanning Tree Protocol“ – Register „STP-Status“

Tabelle 95: WBM-Seite „STP“ – Register „STP-Status“

Aktueller Root-Status		
Parameter	Standardwert	Beschreibung
MAC-Adresse		In diesem Anzeigefeld wird die MAC-Adresse der „Root-Bridge“ angezeigt.
Priorität		In diesem Anzeigefeld wird die Priorität der „Root-Bridge“ angezeigt. Auch dieser Switch kann die „Root-Bridge“ sein.
Max Age		In diesem Anzeigefeld wird das „Max Age“ der „Root-Bridge“ angezeigt.
Hello-Time		In diesem Anzeigefeld wird die „Hello-Time“ der „Root-Bridge“ angezeigt. Die „Root-Bridge“ bestimmt „Hello-Time“, „Max-Age“ und „Forwarding-Delay“.
Forward-Delay		In diesem Anzeigefeld wird die maximale Zeit (in Sekunden) angezeigt, die der Root-Switch wartet, bevor er Zustände ändert.
Aktueller Bridge-Zustand		
Parameter	Standardwert	Beschreibung
MAC-Adresse		In diesem Anzeigefeld wird die MAC-Adresse der aktuellen Bridge angezeigt.
Priorität		In diesem Anzeigefeld wird die Priorität angezeigt.
Max-Age		In diesem Anzeigefeld wird das „Max-Age“ angezeigt.
Hello-Time		In diesem Anzeigefeld wird die „Hello-Time“ angezeigt.
Forward-Delay		In diesem Anzeigefeld wird die „Forward-Time“ angezeigt.
Pfadkosten		In diesem Anzeigefeld werden die Pfadkosten angezeigt.
ROOT-Port		In diesem Anzeigefeld wird die Nummer des Ports am Switch angezeigt, über den der Switch mit der Root des „Spanning Tree“ kommunizieren muss.

10.5 Sicherheit

10.5.1 Access-Control-Liste

Hinweis



Weitere Information

Weitere Informationen zur „Access-Control-Liste“ finden Sie im Kapitel „Funktionsbeschreibung“.

Access-Control-Liste

Access-Control-Listen-Einstellungen

Profilname		Aktion	Ausschalten
Ethernet-Typ	beliebig	VLAN	beliebig
Source-MAC-Adresse	beliebig	Maske der Source-MAC-Adresse	
Destination-MAC-Adresse	beliebig	Maske der Destination-MAC-Adresse	
Source IP	beliebig	Maske der Source-IP-Adresse	
Destination-IP-Adresse	beliebig	Maske der Destination-IP-Adresse	
IP Protocol	beliebig		
Source-Applikation	beliebig		
Destination Application	beliebig		
Source Interface	beliebig --		

Access-Control-Listen-Status

Profilname	521582	Aktion	Ausschalten
Ethernet-Typ	Any	VLAN	Any
IP Protocol	Any		
Source-MAC-Adresse	Any	Maske der Source-MAC-Adresse	None
Destination-MAC-Adresse	Any	Maske der Destination-MAC-Adresse	None
IP Protocol	Any		
Source IP	Any	Maske der Source-IP-Adresse	None
Destination-IP-Adresse	Any	Maske der Destination-IP-Adresse	None
Source-Applikation	10	Destination Application	Any
Source-Applikation	Any		

Abbildung 80: WBM-Seite „Access-Control-Liste“

Tabelle 96: WBM-Seite „Access-Control-Liste“

Access-Control-Liste-Einstellungen		
Parameter	Standardwert	Beschreibung
Profilname		Geben Sie im Eingabefeld den Namen des Profils ein.
Aktion	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Zugriffssteuerung zu deaktivieren.
	Erlaubnis	Wählen Sie im Auswahlfeld „Erlaubnis“, um Datenpakete, die den Angaben entsprechen, weiterzuleiten.
	Verwerfen	Wählen Sie im Auswahlfeld „Verwerfen“, um Datenpakete, die den Angaben entsprechen zu verwerfen.
ETHERNET-Typ	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jeder ETHERNET-Typ gültig ist.
	Andere	Wählen Sie im Auswahlfeld „Andere“, um einen ETHERNET-Typ zu spezifizieren, für den die Zugriffssteuerung gültig ist.
VLAN	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede VLAN-ID gültig ist.
	Andere	Wählen Sie im Auswahlfeld „Andere“, um eine bestimmte VLAN-ID in die Access-Control-Liste einzutragen.
Source-MAC-Adresse	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede MAC-Adresse gültig ist.
	Andere	Wählen Sie im Auswahlfeld „Andere“, um die MAC-Adresse für die Quelle in die Access-Control-Liste einzutragen.
Maske der Source-MAC-Adresse		Geben Sie im Eingabefeld die Source-MAC-ID der Bitmap-Maske für MAC-Source-Adressen von Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Source- MAC-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine MAC-Adresse filtern, die im MAC-Source-Adressfeld eingetragen wurde.
Destination-MAC-Adresse	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede MAC-Adresse gültig ist.
	Andere	Wählen Sie im Auswahlfeld „Andere“, um die Destination-MAC-Adresse in die Access-Control-Liste einzutragen.
Maske der Destination-MAC-Adresse		Geben Sie im Eingabefeld die Destination-MAC-Adresse der Bitmap-Maske für MAC-Destination-Adressen von Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Destination-MAC-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine MAC-Adresse filtern, die im MAC-Destination-Adressfeld eingetragen wurde.
Source-IP	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede IP-Adresse gültig ist.
	Andere	Wählen Sie im Auswahlfeld „Andere“, um die Source-IP-Adresse in die Access-Control-Liste einzutragen.

Tabelle 96: WBM-Seite „Access-Control-Liste“

Maske der Source-IP-Adresse		Geben Sie im Eingabefeld die Source-IP-Adresse der Bitmap-Maske für IP-Source-Adressen von Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Source-IP“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine IP-Adresse filtern, die im IP-Source-Adressfeld eingetragen wurde.	
Destination-IP-Adresse	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede IP-Adresse gültig ist.	
	Andere	Wählen Sie im Auswahlfeld „Andere“, um die Destination-IP-Adresse in die Access-Control-Liste einzutragen.	
Maske der Destination-IP-Adresse		Geben Sie im Eingabefeld die Destination-IP-Adresse der Bitmap-Maske für IP-Destination-Adressen von Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Destination-IP-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine IP-Adresse filtern, die im IP-Destination-Adressfeld eingetragen wurde.	
IP-Protokoll	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jedes IP-Protokoll für die Access-Control-Liste gültig ist.	
	Andere	Geben Sie im Auswahlfeld „Andere“, um das Protokoll einzugeben.	
Source-Applikation	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede Applikation gültig ist.	
	Andere	Wählen Sie im Auswahlfeld „Andere“, um den Source-Port (z. B. 2234) einzutragen.	
Destination-Applikation	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede Destination-Applikation gültig ist.	
	Andere	Wählen Sie im Auswahlfeld „Andere“, um den Destination-Port (z. B. 502) in die Access-Control-Liste einzutragen.	
Source-Interface	beliebig	Wählen Sie im Auswahlfeld „beliebig“, wenn jeder physikalische Port gültig ist.	
	Andere	1 ... 10 (12)	Geben Sie im Eingabefeld den physikalischen Port ein, für den dieser Eintrag in der Access-Control-Liste gültig ist.

Tabelle 96: WBM-Seite „Access-Control-Liste“

Access-Control-Liste-Status		
Parameter	Standardwert	Beschreibung
Profilname		In diesem Anzeigefeld wird der gewählte Name des Profils angezeigt.
Aktion	Ausschalten Erlaubnis Verwerfen DSCP	In diesem Anzeigefeld wird der Status der Zugriffssteuerung angezeigt. (DSCP nur bei IPv4)
ETHERNET-Typ	beliebig Andere	In diesem Anzeigefeld wird der ETHERNET-Typ angezeigt.
VLAN	beliebig Andere	In diesem Anzeigefeld wird die VLAN-ID angezeigt.
IP-Protokoll	beliebig Andere	In diesem Anzeigefeld wird das IP-Protokoll angezeigt.
Source-MAC-Adresse	beliebig Andere	In diesem Anzeigefeld wird die Source-Mac-Adresse angezeigt.
Maske der Source-MAC-Adresse		In diesem Anzeigefeld wird die Source-MAC-ID der Bitmap-Maske angezeigt.
Destination-MAC-Adresse	beliebig Andere	In diesem Anzeigefeld wird die Destination-MAC-Adresse angezeigt.
Maske der Destination-MAC-Adresse		In diesem Anzeigefeld wird die Destination-MAC-ID der Bitmap-Maske angezeigt.
IP-Protokoll	beliebig Andere	In diesem Anzeigefeld wird das IP-Protokoll angezeigt.
Source-IP	beliebig Andere	In diesem Anzeigefeld wird die Source-IP angezeigt.
Maske der Source-IP-Adresse		In diesem Anzeigefeld wird die Source-MAC-ID der Bitmap-Maske angezeigt.
Destination-IP-Adresse	beliebig Andere	In diesem Anzeigefeld wird die Destination-IP angezeigt.
Maske der Destination-IP-Adresse		In diesem Anzeigefeld wird die Destination-IP-ID der Bitmap-Maske angezeigt.
Source-Applikation	beliebig Andere	In diesem Anzeigefeld wird die Source-Applikation angezeigt.
Destination-Applikation	beliebig Andere	In diesem Anzeigefeld wird die Destination-Applikation angezeigt.
Source-Interface	1 ... 10 (12)	In diesem Anzeigefeld wird das Source-Interface angezeigt.

10.6 Monitor

10.6.1 Alarminformationen

Hinweis



Weitere Information

Weitere Informationen zum „Alarm“ finden Sie im Kapitel „Funktionsbeschreibung“.

Alarminformationen			
Alarminformationen			
Alarmstatus	Kein Alarm.		
Alarmursache(s)			
Port	DIP-Switch-Einstellungen	Port	DIP-Switch-Einstellungen
1	Ausschalten	2	Ausschalten
3	Ausschalten	4	Ausschalten
5	Ausschalten	6	Ausschalten
7	Ausschalten	8	Ausschalten
9	Ausschalten	10	Ausschalten
PWR	Ausschalten	RPS	Ausschalten
Aktualisieren			

Abbildung 81: WBM-Seite „Alarminformationen“

Tabelle 97: WBM-Seite „Alarminformationen“

Alarminformationen		
Parameter	Standardwert	Beschreibung
Alarmstatus		In diesem Anzeigefeld wird angezeigt, ob Alarmereignisse stattgefunden haben.
Alarmursache		In diesem Anzeigefeld werden die Details zu den Alarmereignissen angezeigt.
Port	0 ... 10 PWR RPS	In dieser Spalte wird die Bezeichnung des DIP-Schalters angezeigt.
DIP-Switch-Einstellungen	Einschalten Ausschalten	In dieser Spalte wird der aktuelle Status des DIP-Schalters angezeigt.

10.6.2 Systeminformationen

Hinweis



Weitere Information

Weitere Informationen zu „Systeminformationen“ finden Sie im Kapitel „Funktionsbeschreibung“.

Systeminformationen

Temperatureinheit: Celsius(C) ▼

Hardware-Monitor-Alarm: Einschalten ▼

Hardware-Information:

Temperatur(C)	Aktuelle	MAX	MIN	Schwelle	Status
BOARD	52.0	52.0	49.0	80.0	Normal
CPU	51.8	51.8	48.8	80.0	Normal
PHY	50.8	51.0	48.0	80.0	Normal
Spannung(V)	Aktuelle	MAX	MIN	Schwelle	Status
1.0V IN	0.998	0.998	0.988	+/-6%	Normal
1.8V IN	1.784	1.810	1.777	+/-6%	Normal
5.0V IN	5.002	5.048	4.970	+/-6%	Normal

Ändern
Aktualisieren
Konfiguration speichern

Abbildung 82: WBM-Seite „Systeminformationen“

Tabelle 98: WBM-Seite „Systeminformationen“

Hardware-Informationen		
Parameter	Standardwert	Beschreibung
Temperatureinheit	Celsius (C)	Wählen Sie Sie im Auswahlfeld „Celsius (C)“, wenn Sie die Temperatur in Celsius anzeigen wollen.
	Fahrenheit (F)	Wählen Sie Sie im Auswahlfeld „Fahrenheit (F)“, wenn Sie die Temperatur in Fahrenheit anzeigen wollen.
Hardware-Information		
Parameter	Standardwert	Beschreibung
Temperatur (C)		
Aktuell		In dieser Spalte wird die aktuelle Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
MAX		In dieser Spalte wird die maximale Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
MIN		In dieser Spalte wird die minimale Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
Schwelle		In dieser Spalte wird die eingestellte Schwelle angezeigt.
Status		In dieser Spalte wird der Status angezeigt.
Spannung (V)		
Aktuell		In dieser Spalte wird die aktuelle Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
MAX		In dieser Spalte wird die maximale Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
MIN		In dieser Spalte wird die minimale Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
Schwelle		In dieser Spalte wird die eingestellte Schwelle angezeigt.
Status		In dieser Spalte wird der Status angezeigt.

10.6.3 Port-Statistik

Hinweis



Weitere Information

Weitere Informationen zu „Port-Statistik“ finden Sie im Kapitel „Funktionsbeschreibung“.

Port-Statistik								
Port-Statistik								
Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
1	0	0	0	0	162814	219796	23349083	38606803
8	0	0	0	0	819139	869919	135491795	121217763
11	0	0	0	0	52316	917	3867677	118279
Aktualisieren Löschen								

Abbildung 83: WBM-Seite „Port-Statistik“

Tabelle 99: WBM-Seite „Port-Statistik“

Port-Statistik		
Parameter	Standardwert	Beschreibung
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Transmit Drops		In dieser Spalte wird die Anzahl der verworfenen Datenpakete auf der Sendeleitung angezeigt.
Receive Drops		In dieser Spalte wird die Anzahl der verworfenen Datenpakete auf der Empfangsleitung angezeigt.
Transmit Errors		In dieser Spalte werden die Fehler auf der Sendeleitung angezeigt.
Receive Errors		In dieser Spalte werden die Fehler auf der Empfangsleitung angezeigt.
Transmit Packets		In dieser Spalte wird die Anzahl der seit dem Einschalten gesendeten Datenpakete angezeigt.
Receive Packets		In dieser Spalte wird die Anzahl der seit dem Einschalten empfangenen Datenpakete angezeigt.
Transmit Byte		In dieser Spalte wird die Anzahl der gesendeten Bytes auf dem Port seit dem Einschalten angezeigt.
Receive Bytes		In dieser Spalte wird die Anzahl der empfangenen Bytes auf dem Port seit dem Einschalten angezeigt.

10.6.4 Port-Auslastung

Hinweis



Weitere Information

Weitere Informationen zu „Port-Auslastung“ finden Sie im Kapitel „Funktionsbeschreibung“.

Port-Auslastung					
Status der Port-Nutzung					
Port	Geschwindigkeit	RX Port-Nutzung(%)	RX Port-Nutzung (bps)	TX Port-Nutzung(%)	TX Port-Nutzung (bps)
9	1000	0.00	37325	0.02	272533
Aktualisieren					

Abbildung 84: WBM-Seite „Port-Auslastung“

Tabelle 100: WBM-Seite „Port-Auslastung“

Status der Port-Nutzung		
Parameter	Standardwert	Beschreibung
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Geschwindigkeit		In dieser Spalte wird die Transferringeschwindigkeit angezeigt.
RX-Port-Nutzung (%)		In dieser Spalte wird die prozentuale Auslastung der RX-Bandbreite angezeigt.
RX-Port-Nutzung (bps)		In dieser Spalte wird die Auslastung der RX-Bandbreite in bps angezeigt.
TX-Port-Nutzung (%)		In dieser Spalte wird die prozentuale Nutzung der TX-Bandbreite angezeigt.
RX-Port-Nutzung (bps)		In dieser Spalte wird die Nutzung der RX-Bandbreite in bps angezeigt.

10.6.5 RMON-Statistiken

Hinweis



Weitere Information

Weitere Informationen zu „RMON-Statistiken“ finden Sie im Kapitel „Funktionsbeschreibung“.

RMON-Statistiken			
RMON-Statistiken			
Port	8	Anzeigen	Löschen
Port 8 (aktiv)			
Eingehend	Total Octets	137360420	
	BroadcastPkts	355	UnicastPkts 829945
	Non-unicastPkts	920	MulticastPkts 565
	FragmentsPkts	0	UndersizePkts 0
	OversizePkts	0	DiscardsPkts 0
	ErrorPkts	0	UnknownProtos 0
	AlignError	0	CRCAlignErrors 0
	Jabbers	0	DropEvents 0
Outbound	Total Octets	123470045	
	BroadcastPkts	0	UnicastPkts 829548
	Non-unicastPkts	52526	Collisions 0
	LateCollision	0	SingleCollision 0
	MultipleCollision	0	DiscardsPkts 0
	ErrorPkts	0	
#(Anzahl) der Pakete, welche mit einer Länge von ? Empfangen wurden	64 Octets	1004222	65 bis 127 Octets 354385
	128 bis 255 Octets	134029	256 bis 511 Octets 143526
	512 bis 1023 Octets	37223	1024 bis Max Octets 39555

Abbildung 85: WBM-Seite „RMON-Statistiken“

Tabelle 101: WBM-Seite „RMON-Statistiken“

RMON-Statistiken			
Parameter		Standardwert	Beschreibung
Port		-	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie keine Statistik ansehen möchten.
		1 ... 10 Alle	Wählen Sie im Auswahlfeld einen Port oder alle Ports aus, für den (die) Sie die RMON-Statistiken anzeigen möchten.
Ausgewählter Port x (aktiv)			
Parameter		Standardwert	Beschreibung
Ein- gehend	Gesamte Oktette		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt.
	Broadcast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Broadcast-Pakete angezeigt.
	Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Unicast-Pakete angezeigt.
	Keine Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Summe der Broadcast-Pakete und Multicast-Pakete angezeigt.
	Multicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Multicast-Pakete angezeigt.
	Fragmentierte Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen fragmentierten Datenpakete angezeigt.
	Zu kleine Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu kleinen Datenpakete angezeigt.
	Zu große Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu großen Datenpakete angezeigt.
	Verworfen Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die verworfen wurden.
	Fehlerhafte Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die fehlerhaft waren.
	Unbekannte Protos		In diesem Anzeigefeld wird die Anzahl der von diesem Port empfangenen Pakete angezeigt, die als Ziel ein unbekanntes oder nicht unterstütztes Protokoll enthielten.
	Alignment-fehler		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, bei der die Gesamtzahl an Bits eines empfangenen Frames nicht durch 8 teilbar ist.
	CRC-Alignment-fehler		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete mit Checksummenfehler angezeigt.
	Jabbers		In diesem Anzeigefeld wird die Anzahl der von diesem Port empfangenen Jabber angezeigt.
	Drop-Ereignisse		In diesem Anzeigefeld wird die Anzahl der verworfenen Datenpakete angezeigt.

Tabelle 101: WBM-Seite „RMON-Statistiken“

Aus- gehend	Gesamte Oktette		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt.
	Broadcast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Broadcast-Pakete angezeigt.
	Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Keine Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Kollisionen		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	Späte Kollision		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	Einzelkollisionen		In diesem Anzeigefeld wird die Anzahl der Einzelkollisionen der gesendeten Datenpakete angezeigt.
	Mehrfachkollisionen		In diesem Anzeigefeld wird die Anzahl der Mehrfachkollisionen der gesendeten Datenpakete angezeigt.
	Verworfen Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die verworfenen wurden.
	Fehlerhafte Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die fehlerhaft waren.
#(Anzahl) der Pakete, welche mit einer Länge von ? empfangen wurden.	64 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 64 Oktetten hatten.
	65 bis 127 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 65 bis 127 Oktetten hatten.
	128 bis 255 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 128 bis 255 Oktetten hatten.
	256 bis 511 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 256 bis 511 Oktetten hatten.
	512 bis 1023 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 512 bis 1023 Oktetten hatten.
	1024 bis max. Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von mehr als 1024 Oktetten hatten.

10.6.6 SFP-Informationen

SFP-Information

SFP-Information

Port 11 Anwenden

SFP-Information	
Glasfaserkabel	Link Up
Connector	LC
Wellenlänge	850
Übertragungsentfernung	550m(50um, OM2), Multi mode
DDM-Unterstützung	YES (Internally Calibrated)
Hersteller	WAGO
Teilenummer	852-1200
Revisionsstand	V2.0
Seriennummer	AX15470009620
Datum	151120

DDMI-Informationen					
	Aktuell	Alarm high	Alarm low	Warnung high	Warnung low
Temperatur(C)	50.199	90.000	-45.000	85.000	-40.000
Spannung(V)	3.264	3.600	3.000	3.500	3.100
Tx Bias(mA)	6.088	25.000	1.000	20.000	2.000
Tx Power(mW)	0.195	0.501	0.089	0.398	0.112
Tx Power(dBm)	-7.100	-3.000	-10.505	-4.001	-9.506
Rx Power(mW)	0.242	0.631	0.016	0.501	0.020
Rx Power(dBm)	-6.160	-2.004	-18.016	-3.000	-17.012

Aktualisieren

Abbildung 86: WBM-Seite „SFP-Informationen“

Tabelle 102: WBM-Seite „SFP-Informationen“

SFP-Informationen		
Parameter	Standardwert	Beschreibung
Port	-	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie kein SFP-Modul gesteckt haben
	9, 10	Wählen Sie im Auswahlfeld den Port aus, in dem Sie ein SFP-Modul gesteckt haben.
SFP-Informationen		
Parameter	Standardwert	Beschreibung
Glasfaserkabel		In diesem Anzeigefeld wird angezeigt, ob ein Glasfaserkabel angeschlossen ist.
Connector		In diesem Anzeigefeld wird der Code für den optischen Anschlusssteckertyp angezeigt.
Wellenlänge (nm)		In diesem Anzeigefeld wird die Wellenlänge angezeigt.
Übertragungsentfernung (nm)		In diesem Anzeigefeld wird die Übertragungsentfernung angezeigt.
DDM-Unterstützung (nm)		In diesem Anzeigefeld wird angezeigt, ob das SFP-Modul das DDM („Dynamic Device Mapping“) unterstützt.
Hersteller (nm)		In diesem Anzeigefeld wird der Name des SFP-Anbieters angezeigt.
Teilenummer (nm)		In diesem Anzeigefeld wird die Teilenummer angezeigt.
Revisionsstand (nm)		In diesem Anzeigefeld wird der Revisionsstand der Teilenummer angezeigt.
Seriennummer (nm)		In diesem Anzeigefeld wird die Seriennummer (ASCII) angezeigt.
Datum (nm)		In diesem Anzeigefeld wird das Datum der Version angezeigt.

Tabelle 102: WBM-Seite „SFP-Informationen“

DDMI-Informationen (nm)		
Parameter	Standardwert	Beschreibung
Aktuell (nm)		In dieser Spalte werden folgende aktuellen Werte angezeigt: - Temperatur (C) - Spannung (V) - Tx-Bias (mA) - Tx-Power (mW) - Tx-Power (dBm) - Rx-Power (mW) - Rx-Power (dBm)
Alarm high (nm)		In dieser Spalte werden die „Alarm high“-Werte folgender Werte angezeigt: - Temperatur (C) - Spannung (V) - Tx-Bias (mA) - Tx-Power (mW) - Tx-Power (dBm) - Rx-Power (mW) - Rx-Power (dBm)
Alarm low (nm)		In dieser Spalte werden die „Alarm low“-Werte folgender Werte angezeigt: - Temperatur (C) - Spannung (V) - Tx-Bias (mA) - Tx-Power (mW) - Tx-Power (dBm) - Rx-Power (mW) - Rx-Power (dBm)
Warnung high (nm)		In dieser Spalte werden die „Warnung high“-Werte folgender Werte angezeigt: - Temperatur (C) - Spannung (V) - Tx-Bias (mA) - Tx-Power (mW) - Tx-Power (dBm) - Rx-Power (mW) - Rx-Power (dBm)
Warnung low (nm)		In dieser Spalte werden die „Warnung low“-Werte folgender Werte angezeigt: - Temperatur (C) - Spannung (V) - Tx-Bias (mA) - Tx-Power (mW) - Tx-Power (dBm) - Rx-Power (mW) - Rx-Power (dBm)

10.6.7 Traffic-Monitor

Hinweis



Weitere Information

Weitere Informationen zum „Traffic-Monitor“ finden Sie im Kapitel „Funktionsbeschreibung“.

Traffic-Monitor

Traffic-Monitor-Einstellungen

Status Ausschalten ▼

Port	Status	Aktion	Pakettyp	Paketrate (pps)	Recovery-Status	Recovery-Zeit(min)	Quarantänezeit
von: 1 ▼	Ausschalten ▼	Keine ▼	Broadcast ▼	100	Einschalten ▼	1	3
an: 1 ▼							
1 ▼							

Anwenden Aktualisieren Konfiguration speichern

Traffic-Monitor-Status

Port	Status	Status	Pakettyp	Paketrate(pps)	Recovery-Status	Recovery-Zeit(min)	Quarantänezeit
1	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
2	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
3	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
4	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
5	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
6	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
7	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
8	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
9	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
10	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
11	Ausschalten	Normal	Broadcast	100	Einschalten	1	3
12	Ausschalten	Normal	Broadcast	100	Einschalten	1	3

Abbildung 87: WBM-Seite „Traffic-Monitor“

Tabelle 103: WBM-Seite „Traffic-Monitor“

Traffic-Monitor-Einstellungen		
Parameter		Standardwert
		Beschreibung
Status		Ausschalten
		Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Traffic-Monitor“ global zu deaktivieren.
		Einschalten
		Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Traffic-Monitor“ global zu aktivieren.
Port	von:	1
	an:	1
		Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren möchten.
		Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren möchten.
Status		Ausschalten
		Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die Funktion „Traffic-Monitor“ für den Port oder Port-Bereich deaktivieren möchten.
		Einschalten
		Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die Funktion „Traffic-Monitor“ für den Port oder Port-Bereich aktivieren möchten.
Aktion		Keine
		Wählen Sie im Auswahlfeld „Keine“, wenn Sie die Blockierung von Ports nicht aufheben möchten.
		Unblock
		Wählen Sie im Auswahlfeld „Nicht blockiert“, wenn Sie die Blockierung von Ports aufheben möchten.
Pakettyp		Broadcast
		Wählen Sie im Auswahlfeld „Broadcast“, wenn Sie diesen als Pakettyp überwachen möchten.
		Multicast
		Wählen Sie im Auswahlfeld „Multicast“, wenn Sie diesen als Pakettyp überwachen möchten.
		Bcast+Mcast
		Wählen Sie im Auswahlfeld „Bcast+Mcast“, wenn Sie diese beiden als Pakettypen überwachen möchten.
Paketrate (pps)		
		Geben Sie im Eingabefeld die Paketrate ein, die überwacht werden soll.
Recovery-Status		Einschalten
		Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die Recovery-Funktion beim „Traffic-Monitor“ für den Port oder Port-Bereich aktivieren möchten.
		Ausschalten
		Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die Recovery-Funktion beim „Traffic-Monitor“ für den Port oder Port-Bereich deaktivieren möchten.
Paketrate (pps)		1
		Geben Sie im Eingabefeld die Paketrate ein, die überwacht werden soll.
Quarantänezeit		3
		Geben Sie im Eingabefeld einen Wert für die „Quarantänezeit“ beim „Traffic-Monitor“ ein.

Tabelle 103: WBM-Seite „Traffic-Monitor“

Traffic-Monitor-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10	In dieser Spalte werden die Port-Nummern angezeigt.
Status	Ausschalten Einschalten	In dieser Spalte wird der Status des spezifischen Port angezeigt.
Status	Normal	In dieser Spalte wird der Status des Betriebszustandes angezeigt.
Pakettyp	Broadcast Multicast Bcast+Mcast	In dieser Spalte wird der Typ des Datenpaketes angezeigt.
Paketrate (pps)		In dieser Spalte wird die gewählte Paketrate angezeigt.
Recovery-Status	Einschalten Ausschalten	In dieser Spalte wird der Status der gewählten Recovery-Funktion angezeigt.
Recovery-Zeit (min)	1 ... 60	In dieser Spalte wird die gewählte Recovery-Zeit angezeigt.
Quarantänezeit	3	In dieser Spalte wird die gewählte „Quarantänezeit“ angezeigt.

10.7 Management

10.7.1 SNMP

10.7.1.1 SNMP

10.7.1.1.1 SNMP-Einstellungen

Hinweis



Weitere Information

Weitere Informationen zu „SNMP“ (Simple Network Management Protocol) finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 88: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“

Tabelle 104: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“

SNMP-Einstellungen		
Parameter	Standardwert	Beschreibung
SNMP-Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um das SNMP am Switch zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das SNMP am Switch zu aktivieren.
Systemname	L2SWITCH	Geben Sie im Eingabefeld den Systemnamen für den Switch ein (Systemname und Host-Name sind identisch).
Standort	–	Geben Sie im Eingabefeld die IP-Adresse (Standortinformation) des Switches in Dezimalpunktschreibweise ein.
Kontakt	–	Geben Sie im Eingabefeld die IP-Subnetzmaske des Switches in Dezimalpunktschreibweise ein.

10.7.1.1.2 Community-Name

SNMP

SNMP-Einstellungen **Community Name**

Community-Name-Einstellungen

Community String	Rechte	Network-ID des Trusted-Host	Number of Mask Bit
	Nur Lesen ▼		

Anwenden Aktualisieren Konfiguration speichern

Community-Name-Liste

Nr.	Community String	Rechte	Network-ID des Trusted-Host	Number of Mask Bit	Aktion
-----	------------------	--------	-----------------------------	--------------------	--------

Abbildung 89: WBM-Seite „SNMP“ – Register „Community-Name“

Tabelle 105: WBM-Seite „SNMP“ – Register „Community-Name“

Community-Name-Einstellungen		
Parameter	Standardwert	Beschreibung
Community String		Geben Sie im Eingabefeld den „Community-String“ ein, der als Passwort für Anfragen von der Managementstation fungiert.
Rechte	Nur Lesen	Wählen Sie im Auswahlfeld „Nur Lesen“, damit der SNMP-Manager diese Strings nutzen kann, um Informationen vom Switch zu erhalten.
	Lesen/ Schreiben	Wählen Sie im Auswahlfeld „Lesen/Schreiben“, damit der SNMP-Manager diese Strings nutzen kann, um Einstellungen am Switch zu konfigurieren.
Network-ID des Trusted-Host		Geben Sie im Eingabefeld die IP-Adresse der dezentralen SNMP-Managementstation in Dezimalpunktschreibweise ein (z. B. 192.168.1.0).
Number of Mask Bit		Geben Sie im Eingabefeld die IP-Adresse der Subnetzmaske der dezentralen SNMP-Managementstation in Dezimalpunktschreibweise ein (z. B. 255.255.255.0).
Community-Name-Liste		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Nummer der „Community“ angezeigt. Sie dient ausschließlich der Identifizierung. Klicken Sie auf eine Nummer, um die Einstellung einer spezifischen „Community“ zu modifizieren.
Community String		In dieser Spalte wird der „SNMP-Community-String“ angezeigt. Dies ist ein Textelement, das als Passwort fungiert.
Rechte	Nur Lesen, Lesen/ Schreiben	In dieser Spalte werden die Berechtigungen für den „SNMP-Community-String“ angezeigt.
Network-ID des Trusted-Host		In dieser Spalte wird die IP-Adresse der dezentralen SNMP-Managementstation angezeigt, nachdem sie durch die Subnetzmaske modifiziert wurde.
Number of Mask Bit		In dieser Spalte wird die Subnetzmaske für die IP-Adresse der dezentralen SNMP-Managementstation angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen spezifischen „Community-String“ zu löschen.

10.7.1.2 SNMP-Trap

10.7.1.2.1 Trap-Receiver-Einstellungen

Abbildung 90: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“

Tabelle 106: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“

Trap-Receiver-Einstellungen		
Parameter	Standardwert	Beschreibung
IP-Adresse		Geben Sie im Eingabefeld die IP-Adresse der dezentralen Trap-Station in Dezimalpunktschreibweise ein.
Version	v1	Wählen Sie im Auswahlfeld „v1“ aus, wenn Sie die SNMP-Version v1 verwenden möchten.
	v2c	Wählen Sie im Auswahlfeld „v2c“ aus, wenn Sie die SNMP-Version v2c verwenden möchten.
Community String		Geben Sie im Eingabefeld die IP-Adresse der dezentralen SNMP-Managementstation in Dezimalpunktschreibweise ein (z. B. 192.168.1.0).
Trap-Receiver-Liste		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Nummer der „Community“ angezeigt. Sie dient ausschließlich der Identifizierung. Klicken Sie auf eine Nummer, um die Einstellung einer spezifischen „Community“ zu modifizieren.
IP-Adresse		In dieser Spalte wird die IP-Adresse der dezentralen Trap-Station angezeigt.
Version	v1 v2c	In dieser Spalte wird die verwendete SNMP-Version angezeigt.
Community-String		In dieser Spalte wird der von dieser dezentralen Trap-Station verwendete „Community-String“ angezeigt.
Aktion		Klicken Sie auf die Schaltfläche [Löschen] , um eine konfigurierte Trap-Empfängerstation zu löschen.

10.7.1.2.2 Trap Event Status

SNMP Trap

Trap Receiver-Einstellungen **Trap Event Status** Trap Port-Einstellungen

Trap Event State Einstellungen

☐ Alle auswählen ☐ Alle deaktivieren

☒ alarm-over-heat	☒ alarm-over-load
☒ alarm-power-fail	☒ bpdu
☒ dual-homing	☒ port-link-change
☒ loop-detection	☒ stp-topology-change
☒ port-admin-state-change	☒ traffic-monitor
☒ power-source-change	

Anwenden Aktualisieren

Abbildung 91: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“

Tabelle 107: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“

Trap-Event-State-Einstellungen		
Parameter	Standard-wert	Beschreibung
alarm-over-heat	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn die Temperatur des Systems zu hoch ist.
alarm-power-fail	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn die Systemleistung über Spannung/Unterspannung/liegt. RPS-Überspannung/RPS-Spannung.
dual-homing	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port durch „Dual Homing“ blockiert ist.
loop-detection	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port durch die Loop Detection blockiert wird.
port-admin-state-change	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port vom Administrator aktiviert/deaktiviert ist.
power-source-change	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn die Stromquelle geändert wurde. (AC zu DC oder DC zu AC)
alarm-over-load	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn das System überlastet ist.
bpdu	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port von „BPDU Guard/BPDU Root“ gesperrt ist. Status des „Guard/BPDU-Anschlusses“ geändert.
port-link-change	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port hoch/runter wechselt.
stp-topology-change	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn sich die STP-Topologie ändert.
traffic-monitor	☒	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port vom Traffic Monitor blockiert wird.

10.7.1.2.3 Trap-Port-Einstellungen

SNMP Trap

Trap Receiver-Einstellungen
Trap Event Status
Trap Port-Einstellungen

Port Link-Change Trap Settings

Port	Status
von: 1 an: 1	Enable

Port Link-Change Trap Status

Port	Status	Port	Status
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable

Abbildung 92: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“

Tabelle 108: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“

Port-Link-Change-Trap-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren möchten.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, den Sie konfigurieren möchten.
Status		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Port-Status zu aktivieren.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um den Port-Status zu deaktivieren.
Port-Link-Change-Trap-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte wird der Portbereich angezeigt.
Status		Einschalten Ausschalten	In diesem Anzeigefeld wird der Port-Status angezeigt.

10.7.1.3 SNMPv3-Konfiguration

10.7.1.3.1 SNMPv3-User

Hinweis**Weitere Information**

Weitere Informationen zur „SNMPv3“ finden Sie im Kapitel „Funktionsbeschreibung“.

SNMPv3-Konfiguration

SNMPv3 User SNMPv3-Gruppen SNMPv3 View

SNMPv3-User-Einstellungen

User Name:

Gruppenname:

Security Level:

Auth-Algorithmus:

Auth Password:

Priv-Algorithmus:

Priv Password:

SNMPv3-User-Status

User Name	Gruppenname	Auth Protokoll	Priv Protokoll	Rowstatus	Aktion
user1	qwe	No Auth	No Priv	Active	Löschen

Abbildung 93: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“

Tabelle 109: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“

SNMPv3-User-Einstellungen		
Parameter	Standardwert	Beschreibung
Nutzername		Geben Sie im Eingabefeld einen neuen Benutzernamen ein oder modifizieren Sie einen bereits bestehenden Benutzernamen.
Gruppenname		Geben Sie im Eingabefeld den Gruppennamen für die SNMPv3 ein.
Sicherheitslevel		In diesem Auswahlfeld wird der Sicherheitslevel ausgewählt.
	noauth	Haben Sie im Auswahlfeld „noauth“ gewählt, dann können Sie den „Auth-Algorithmus“ und den „Priv-Algorithmus“ nicht ändern.
	auth	Haben Sie im Auswahlfeld „auth“ gewählt, dann können Sie den „Auth-Algorithmus“ und das „Auth-Password“ ändern.
	priv	Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie den „Auth-Algorithmus“, das „Auth-Password“, den „Priv-Algorithmus“ und das „Priv-Password“ ändern.
Auth-Algorithmus	MD5	Haben Sie im Auswahlfeld „auth“ oder „priv“ gewählt, dann können Sie den „Auth-Algorithmus“ „MD5“ wählen.
	SHA	Haben Sie im Auswahlfeld „auth“ oder „priv“ gewählt, dann können Sie den „Auth-Algorithmus“ „SHA“ wählen.
Auth-Password		Haben Sie im Auswahlfeld „auth“ gewählt, dann können Sie im Eingabefeld ein Passwort (aus mindestens 8 alphanumerischen Zeichen) eingeben.
Priv-Algorithmus	DES	Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie im Auswahlfeld „DES“ wählen.
	AES	Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie im Auswahlfeld „AES“ wählen.
Priv-Password		Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie im Eingabefeld ein Passwort (aus mindestens 8 alphanumerischen Zeichen) eingeben.
SNMPv3-User-Status		
Parameter	Standardwert	Beschreibung
Nutzername		In dieser Spalte wird der Benutzername angezeigt.
Gruppenname		In dieser Spalte wird der Gruppenname angezeigt.
Auth-Protokoll		In dieser Spalte wird der gewählte „Auth-Algorithmus“ angezeigt.
Priv-Protokoll		In dieser Spalte wird der gewählte „Priv-Algorithmus“ angezeigt.
Rowstatus		In dieser Spalte wird der Rowstatus angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

10.7.1.3.2 SNMPv3-Gruppen

SNMPv3-Konfiguration

SNMPv3 User **SNMPv3-Gruppen** SNMPv3 View

SNMPv3-Gruppeneinstellungen

Gruppenname

Security Level

Read View

Write View

Notify View

SNMPv3-Gruppenstatus

Gruppenname	Security Model	Security Level	Read View	Write View	Notify View	Aktion
user1	v3	noauth	none	none	none	Löschen

Abbildung 94: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-Gruppen“

Tabelle 110: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-Gruppen“

SNMPv3-Gruppen-Einstellungen		
Parameter	Standardwert	Beschreibung
Gruppenname		Geben Sie im Eingabefeld den Gruppennamen für die SNMPv3-Gruppe ein.
Sicherheitslevel		In diesem Auswahlfeld wird der Sicherheitslevel ausgewählt.
	Noauth	Wählen Sie im Auswahlfeld den entsprechenden Sicherheitslevel aus.
	auth priv	
Read View		Geben Sie im Eingabefeld den Namen der Objekte ein, die in der Leseansicht verfügbar sein sollen. Geben Sie kein Objekt ein, sind alle Objekte lesbar.
Write View		Geben Sie im Eingabefeld den Namen der Objekte ein, auf die ein Schreibzugriff gewährt werden soll.
Notify View		Geben Sie im Eingabefeld den Namen des Objektes ein, das Benachrichtigungen der Benutzer empfangen kann.
SNMPv3-Gruppen-Status		
Parameter	Standardwert	Beschreibung
Gruppenname		In dieser Spalte wird der Gruppenname angezeigt.
Security Modell		In dieser Spalte wird das gewählte Sicherheitslevel angezeigt.
Sicherheitslevel		In dieser Spalte wird der gewählte „Sicherheitslevel“ angezeigt.
Read View		In dieser Spalte wird die „Read View“ angezeigt
Write View		In dieser Spalte wird die „Write View“ angezeigt
Notify View		In dieser Spalte wird die „Notify View“ angezeigt
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

10.7.1.3.3 SNMPv3-View

SNMPv3-Konfiguration

SNMPv3 User SNMPv3-Gruppen **SNMPv3 View**

SNMPv3-View-Einstellungen

Name:

Subtree:

Typ: ▼

SNMPv3-View-Status

Name	Subtree	Typ	Aktion
SNMPv3-View-Tabelle ist leer!			

Abbildung 95: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-View“

Tabelle 111: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-View“

SNMPv3-Ansicht-Einstellungen		
Parameter	Standardwert	Beschreibung
Name		Geben Sie im Eingabefeld den Namen für die SNMPv3-View ein.
Subtree		Geben Sie im Eingabefeld den Namen für den Subtree ein.
Typ	eingefügt	Haben Sie im Auswahlfeld „eingefügt“ gewählt, dann wird der Subtree eingefügt
	ausgegliedert	Haben Sie im Auswahlfeld „ausgegliedert“ gewählt, dann wird der Subtree nicht eingefügt.
SNMPv3-View-Status		
Parameter	Standardwert	Beschreibung
Name		In dieser Spalte wird der Name der SNMPv3-View angezeigt.
Subtree		In dieser Spalte wird der Name des Subtree angezeigt.
Typ	Eingefügt ausgegliedert	In dieser Spalte wird der gewählte Typ angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

10.7.2 Wartung

10.7.2.1 Konfiguration

Abbildung 96: WBM-Seite „Wartung“ – Register „Konfiguration“

Konfiguration Speichern

- Klicken Sie auf die Schaltfläche **[Speichern]**, um die aktuellen Einstellungen im NV-RAM (Flash) zu speichern.

Upload und Download der Konfiguration

Führen Sie die nachfolgenden Schritte aus, um die Konfigurationsdatei auf Ihrem PC zu speichern.

1. Wählen Sie „Download drücken, um die Konfigurationsdatei auf Ihrem PC zu speichern“.
2. Klicken Sie auf die Schaltfläche **[Download]**, um den Download zu beginnen.

Führen Sie die nachfolgenden Schritte aus, um die Konfigurationsdatei vom PC auf den Switch hochzuladen.

1. Wählen Sie „Die Konfigurationsdatei auf den Switch laden“.

2. Klicken Sie auf die Schaltfläche **[Datei auswählen]**.
Wählen Sie die Konfigurationsdatei mit Angabe des vollständigen Pfads aus.
3. Klicken Sie auf die Schaltfläche **[Upload]**, um das Hochladen zu beginnen.

Konfiguration zurücksetzen

- Klicken Sie auf die Schaltfläche **[Reset]**, um die Konfiguration des Switches auf die Werkseinstellungen zurückzusetzen.

Der Konfigurationsstatus

Wurden Änderungen an den Konfigurationen vorgenommen, wird „Die Konfigurationen wurden verändert“ angezeigt.

Wurden keine Änderungen an den Konfigurationen vorgenommen, wird „Die User Konfigurationsdatei ist auf default. Die Konfigurationen sind Standardwerte.“ angezeigt.

10.7.2.2 Firmware



Abbildung 97: WBM-Seite „Wartung“ – Register „Firmware“

Firmware-Upgrade

Führen Sie die nachfolgenden Schritte aus, um ein Update der Firmware des Switches durchzuführen.

1. Klicken Sie auf die Schaltfläche **[Datei auswählen]**.
Es erscheint ein Dateiauswahldialog. Wählen Sie darin die entsprechende Firmware-Datei aus.
2. Klicken Sie auf die Schaltfläche **[Upgrade]**, um die neue Firmware zu laden.

10.7.2.3 Neustart



Abbildung 98: WBM-Seite „Wartung“ – Register „Neustart“

Rebooten

Die Funktion „Rebooten“ ermöglicht es, den Switch ohne physisches Trennen der Spannungsversorgung neu zu starten.

Führen Sie die nachfolgenden Schritte aus, um den Switch neu zu starten.

1. Klicken Sie im Menü „Rebooten“ auf die Schaltfläche **[Rebooten]**.
Daraufhin wird folgendes Fenster angezeigt:

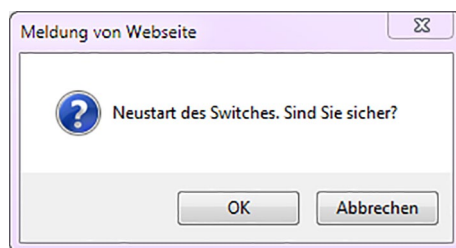


Abbildung 99: WBM-Seite „Wartung“ – Register „Rebooten“ – Meldung

2. Klicken Sie auf **[OK]** und warten Sie, bis der Switch neu gestartet ist. Dieser Vorgang kann bis zu zwei Minuten dauern. Die Konfiguration des Switches wird durch diesen Vorgang nicht verändert.

10.7.2.4 Protokolle

Wartung

Konfiguration
Firmware
Neustart
Protokolle

Server-Einstellungen

HTTP-Server-Status	Einschalten ▼	HTTP-Server-TCP-Port	80 (80,1025~9999)
HTTPS-Server-Status	Einschalten ▼		
SNMP-v1/v2c-Server-Status	Einschalten ▼		
SNMP-v3-Server-Status	Einschalten ▼		
SSH-Server-Status	Einschalten ▼		
TELNET-Server-Status	Einschalten ▼	TELNET-Server-TCP-Port	23 (23,1025~9999)

Anwenden
Aktualisieren
Konfiguration speichern

Server-Status

HTTP-Server-Status	Einschalten	HTTP-Server-TCP-Port	80
HTTPS-Server-Status	Einschalten		
SNMP-v1/v2c-Server-Status	Einschalten		
SNMP-v3-Server-Status	Einschalten		
SSH-Server-Status	Einschalten		
TELNET-Server-Status	Einschalten	TELNET-Server-TCP-Port	23

Abbildung 100: WBM-Seite „Wartung“ – Register „Protokolle“

Tabelle 112: WBM-Seite „Wartung“ – Register „Protokolle“

Server-Einstellungen		
Parameter	Standardwert	Beschreibung
HTTP-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „HTTP-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „HTTP-Server“ zu deaktivieren.
HTTP-Server-TCP-Port (80, 1025~9999)	80 1025 ... 9999	Geben Sie im Eingabefeld den „HTTP-Server-TCP-Port“ ein.
HTTPS-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „HTTPS-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „HTTPS-Server“ zu deaktivieren.
SNMP-v1/v2c-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „SNMP-v1/v2c-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SNMP-v1/v2c-Server“ zu deaktivieren.
SNMP-v3-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „SNMP-v3-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SNMP-v3-Server“ zu deaktivieren.
SSH-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „SSH-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SSH-Server“ zu deaktivieren.
Telnet-Server-Status	Einschalten	Wählen Sie „Einschalten“, um den „Telnet-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „Telnet-Server“ zu deaktivieren.
Telnet-Server-TCP-Port (23, 1025~9999)	23 1025 ... 9999	Geben Sie im Eingabefeld den „Telnet-Server-TCP-Port“ ein.
Server-Status		
Parameter	Standardwert	Beschreibung
HTTP-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des HTTP-Servers angezeigt.
HTTP-Server-TCP-Port	80 1025 ... 9999	In diesem Anzeigefeld wird der HTTP-Server-TCP-Port angezeigt.
HTTPS-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des HTTPS-Servers angezeigt.
SNMP-v1/v2c-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SNMP-v1/v2c-Servers angezeigt.
SNMP-v3-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SNMP-v3-Servers angezeigt.
SSH-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SSH-Servers angezeigt.
Telnet-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des Telnet-Servers angezeigt.
Telnet-Server-TCP-Port	23 1025 ... 9999	In diesem Anzeigefeld wird der Telnet-Server-TCP-Port angezeigt.

10.7.3 System-Log

Die Funktion „syslog“ (Systemprotokoll) zeichnet verschiedene Systeminformationen für das „Debugging“ (Fehlersuche) auf. Jeder Protokolleintrag zeichnet eine der folgenden Ebenen auf:

- Alert
- kritisch
- Fehler
- Warnung
- Bekanntmachung
- Information

Die Syslog-Funktion kann aktiviert oder deaktiviert werden. Die Default-Einstellung ist „deaktiviert“. Die Protokollnachricht wird im Dateisystem des Switches gespeichert. Wurde die IP-Adresse des Syslog-Servers konfiguriert, wird der Switch eine Kopie an ihn senden.

Hinweis



Größe der Protokollnachrichtendatei

Die Größe der Protokollnachrichtendatei ist auf 4 KB begrenzt. Ist die Datei voll, wird die jeweils älteste Nachricht ersetzt.

System Log

Syslog-Server-Einstellungen

Server-IP-Adresse IPv4 Ausschalten

Einstellung (5) Messages generated internally by syslog

System Log

Log Level Alle

```

<6> 2019 Mar 20 16:02:33 60003:System Cold Start!
<4> 2019 Mar 20 16:02:34 40005:Port 11 Link Up.
<4> 2019 Mar 20 16:02:43 40005:Port 1 Link Up.
<4> 2019 Mar 20 16:45:41 40004:Port 1 Link Down.
<4> 2019 Mar 20 16:45:56 40005:Port 8 Link Up.
<6> 2019 Mar 20 16:50:07 60001:User(admin) Login Succeeded!
<6> 2019 Mar 20 16:51:40 60005:Save configurations to file!
<6> 2019 Mar 20 21:14:18 60001:User(admin) Login Succeeded!
<6> 2019 Mar 21 20:52:14 60001:User(admin) Login Succeeded!
<6> 2019 Mar 22 15:32:02 60001:User(admin) Login Succeeded!
<6> 2019 Mar 22 16:25:14 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:27 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:51 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:56 60005:Save configurations to file!
<6> 2019 May 10 09:18:26 60005:Save configurations to file!
<6> 2019 May 10 13:48:22 60001:User(admin) Login Succeeded!
<6> 2019 May 13 07:46:04 60001:User(admin) Login Succeeded!
<6> 2019 May 13 10:05:11 60001:User(admin) Login Succeeded!

```

Abbildung 101: WBM-Seite „System-Log“

Tabelle 113: WBM-Seite „System-Log“

Syslog-Server-Einstellungen		
Parameter	Standardwert	Beschreibung
Server-IP-Adresse	IPv4	Wählen Sie im Auswahlfeld „IPv4“, wenn Sie diese Version des Internetprotokolls wählen möchten.
	IPv6	Wählen Sie im Auswahlfeld „IPv6“, wenn Sie diese Version des Internetprotokolls wählen möchten.
		Geben Sie im Eingabefeld die IP-Adresse in Dezimalpunktschreibweise ein (z. B.: 192.168.1.1).
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, damit der Switch alle neuen Protokollnachrichten nicht an den Syslog-Server sendet.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit der Switch alle neuen Protokollnachrichten nicht an den Syslog-Server sendet.
Einstellung	(1) User-level messages	Wählen Sie im Auswahlfeld „(1) User-level messages“, wenn Sie die benutzerspezifischen Meldungen anzeigen wollen.
	(5) Messages generated internally by syslogd	Wählen Sie im Auswahlfeld „(5) Messages generated internally by syslogd“, wenn Sie die intern von Syslog erzeugten Meldungen anzeigen wollen.
	(14) Log alert	
	(16) Local use 0	
	(17) Local use 1	
	(18) Local use 2	
	(19) Local use 3	
	(20) Local use 4	
	(21) Local use 5	
	(22) Local use 6	
	(23) Local use 7	
System-Log		
Parameter	Standardwert	Beschreibung
Log-Level	Alle	Wählen Sie im Auswahlfeld „Alle“, wenn Sie alle Protokollnachrichten anzeigen wollen.
	1:Alarm	Wählen Sie im Auswahlfeld „Alarm“, wenn Sie die Log-Meldungen anzeigen wollen.
	2:kritisch	Wählen Sie im Auswahlfeld „kritisch“, wenn Sie die kritischen Protokollnachricht anzeigen wollen.
	3:Fehler	Wählen Sie im Auswahlfeld „Fehler“, wenn Sie die Fehler anzeigen wollen.
	4:Warnung	Wählen Sie im Auswahlfeld „Warnung“, wenn Sie die Warnungen anzeigen wollen.
	5:Bekanntmachung	Wählen Sie im Auswahlfeld „Bekanntmachung“, wenn Sie die Bekanntmachungen anzeigen wollen.
	6:Information	Wählen Sie im Auswahlfeld „Information“, wenn Sie alle Informationen anzeigen wollen.

10.7.4 Upload File

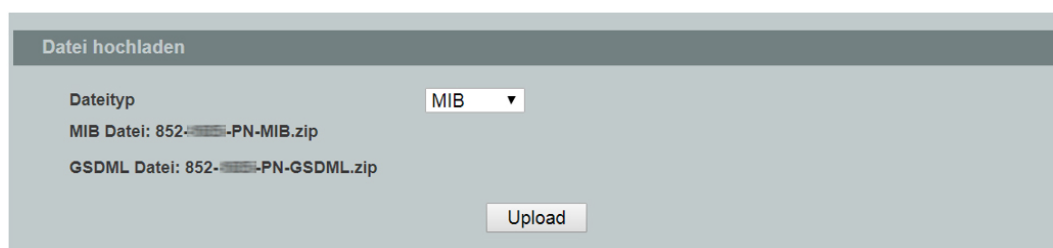


Abbildung 102: WBM-Seite „Datei hochladen“

Tabelle 114: WBM-Seite „Datei hochladen“

Parameter	Standardwert	Beschreibung
Dateityp	MIB	Auswahl, ob die MIB- oder die GSDML-Datei in das WBM geladen werden soll

10.7.5 Ping

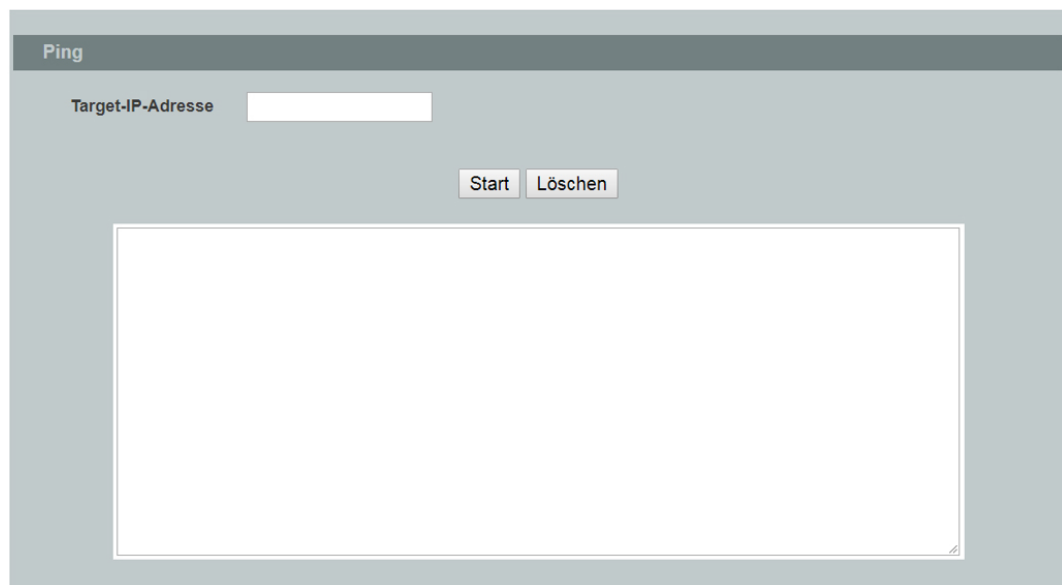


Abbildung 103: WBM-Seite „Ping“

Tabelle 115: WBM-Seite „Ping“

Parameter	Standardwert	Beschreibung
Target-IP-Adresse	–	Eingabe der Zieladresse

10.7.6 Benutzerkonto

Der Switch ermöglicht die Einrichtung von bis zu sechs Benutzerkonten. Der Benutzername und das Passwort müssen aus einer Kombination aus Zahlen oder Buchstaben des Alphabets bestehen. Das letzte Administratorkonto kann nicht gelöscht werden. Zur Nutzung der CLI oder des Web-Based-Managements muss sich ein Benutzer mit einem gültigen Benutzerkonto angemeldet haben.

Benutzerberechtigungen

Der Switch unterstützt zwei Arten von Benutzerkonten:

Die Default-Benutzerkonten haben folgende Anmeldeinformationen:

Firmwareversion 01: User Name = „admin“
 User Password = „wago“

- | | | |
|----|------------------------|---|
| 1. | Admin-Konten | Schreib-/Leseberechtigung |
| 2. | Normale Benutzerkonten | Nur Leseberechtigung
- Die Nutzung des privilegierten Modus in der CLI ist nicht möglich.
- Die Änderung von Konfigurationen im Web-Management ist nicht möglich. |

Außerdem unterstützt der Switch ein „Backdoor“-Benutzerkonto. Sollte ein Benutzer seinen Benutzernamen oder sein Passwort vergessen haben, kann der Switch ein „Backdoor“-Konto mit der MAC-Adresse des Systems einrichten. Dadurch kann sich ein Benutzer am Switch anmelden und ein neues Konto einrichten.

Nr.	Name	Autorität	Aktion
1	admin	Admin	

Abbildung 104: WBM-Seite „Benutzerkonto“

Tabelle 116: WBM-Seite „Benutzerkonto“

User-Account-Einstellungen		
Parameter	Standardwert	Beschreibung
User-Name		Geben Sie im Eingabefeld einen neuen Benutzernamen ein oder modifizieren Sie einen bereits bestehenden Benutzernamen.
User-Passwort		Geben Sie im Eingabefeld ein neues Passwort ein oder modifizieren Sie ein bereits bestehendes Passwort. Sie können bis zu 32 alphanumerische Zeichen oder Zahlen eintragen.
Benutzerrolle		In diesem Auswahlfeld wählen Sie die Art des Benutzerkontos aus.
	Normal	Wählen Sie im Auswahlfeld "Normal", wenn Sie nur eine Leseberechtigung für dieses Benutzerkonto benötigen.
	Admin	Wählen Sie im Auswahlfeld "Admin", wenn Sie eine Schreib- und Leseberechtigung für dieses Benutzerkonto benötigen.
Nr.		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Indexnummer eines Eintrags angezeigt.
Name		In dieser Spalte wird der Name des Benutzerkontos angezeigt.
Benutzerrolle		In dieser Spalte wird die Art des Benutzerkontos angezeigt.
Aktion		Klicken Sie auf die Schaltfläche [Löschen] , um ein Benutzerkonto zu löschen.
	Hinweis 	Löschen Administratorkonto Das letzte Administratorkonto kann nicht gelöscht werden.

11 Anhang

11.1 Konsolenanschluss (RJ-45 zu DB9)

Verwenden Sie zum Verbinden des Konsolenanschlusses des Industrial-Managed-Switches mit dem COM-Anschluss das mitgelieferte Konsolenkabel. Die Anschlussbelegung ist wie folgt:

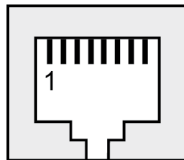


Abbildung 105: RJ-45 Anschlussbelegung

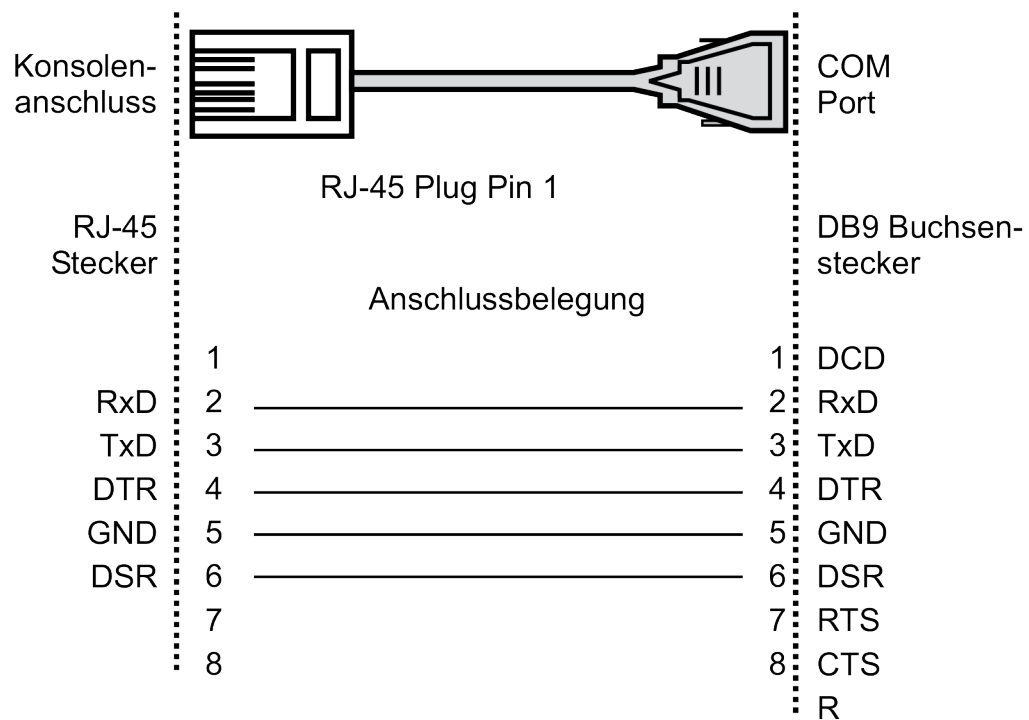


Abbildung 106: Anschlussbelegung RJ-45 zu DB9

11.2 RJ-45-Kabel

Verwenden Sie beim Anschließen Ihrer Netzwerkgeräte standardmäßige ETHERNET-Kabel. Die Anschlussbelegung ist wie folgt:

Tabelle 117: RJ-45-Kabel

Kontakt	Bezeichnung		Paar	Farbe (gemäß EIA/TIA 568B)
	4-adrig	8-adrig		
1	TD+	D1+	2	Weiß/Orange
2	TD-	D1-	2	Orange
3	RX+	D2+	3	Weiß/Grün
4	Nicht belegt	D3+	1	Blau
5	Nicht belegt	D3-	1	Weiß/Blau
6	RX-	D2-	3	Grün
7	Nicht belegt	D4+	4	Weiß/Braun
8	Nicht belegt	D4-	4	Braun

Hinweis



Funktionen am RJ-45-Anschluss

Der Industrial-Managed-Switch bietet die Funktionen Autocrossing und Autonegotiation am RJ-45-Anschluss.

11.3 Configuring in the Command Line Interface (CLI) (Zugriff über Konsole (CLI))

11.3.1 System Status

11.3.1.1 System Information

Table 118: CLI "System Information" Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
configure	reboot	This command reboots the system.
eth0	ip addressA.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
acl	show	This command displays the current access control profile.
vlan	show	This command displays the current VLAN configurations.
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system's CPU loading and memory information.
enable	show uptime	This command displays the system uptime.

11.3.2 Basic Settings

11.3.2.1 System

Table 119: CLI "System" Configuration

Node	Command	Description
enable	ping IPADDR [-c COUNT]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR s SIZE]	This command sends an echo request to the destination host. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-c COUNT -s SIZE]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-s SIZE -c COUNT]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
configure	reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system's network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	This command changes the mode to config mode.
configure	interface eth0	This command changes the mode to eth0 mode.
eth0	show	This command displays the eth0 configurations.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system's default gateway.
eth0	ip dhcp client (disable enable renew)	This command configures a DHCP client function for the system. "Disable": Use a static IP address for the switch. "Enable & Renew": Use the DHCP client to get an IP address from the DHCP server.
eth0	management vlan VLAN_ID	This command configures the management VLAN.

11.3.2.1.1 Jumbo Frame

Table 120: CLI “Jumbo Frame” Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240 1522 1536 1552 9216)	This command configures the maximum number of bytes of frame size for all ports.

11.3.2.1.2 SNTP

Table 121: CLI “SNTP” Configuration

Node	Command	Description
enable	show time	This command displays the current time and date configuration.
configure	time HOUR:MINUTE:SECOND	This command sets the current time of the switch. hour: 0-23 min: 0-59 sec: 0-59 Note: If you configure daylight saving time after you configure the date and time, the switch uses daylight saving time.
configure	time date YEAR/MONTH/DAY	This command sets the current date of the switch. year: 1970– month: 1–12 day: 1–31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving time on the switch.
configure	time daylight-saving-time start-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the start date of daylight saving time.
configure	time daylight-saving-time end-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the end date of daylight saving time.
configure	time ntp-server (disable enable)	This command disables/enables the NTP server settings.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of the time server.
configure	time timezone STRING	This command sets the time difference between UTC (formerly GMT) and the time zone. Valid range: –1200 ... +1200

Example

```
L2SWITCH(config)#time ntp-server 192.5.41.41
```

```
L2SWITCH(config)#time timezone +0800
```

```
L2SWITCH(config)#time ntp-server enable
```

```
L2SWITCH(config)#time daylight-saving-time start-date first Monday 6 0
```

```
L2SWITCH(config)#time daylight-saving-time end-date last Saturday 10 0
```

11.3.2.1.3 Management Host

Table 122: CLI "Management Host" Configuration

Node	Command	Description
enable	show interface eth0	The command displays all eth0 interface configurations.
eth0	show	The command displays all eth0 interface configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#interface eth0
```

```
L2SWITCH(config-if)#management host 192.168.200.106
```

11.3.2.2 MAC Management

Table 123: CLI "MAC Management" Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current "Age Time" for the MAC address table.
enable	show mac-address-table (static dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information of a specific MAC address table.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries recognized by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLANID	This command deletes a static unicast entry from the address table.
configure	mac-address-table aging-time VALUE	This command configures the MAC table "Age Time".
configure	clear mac address-table dynamic	This command deletes the dynamic address entries.

Example

```
L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1
```

11.3.2.3 Port Mirroring

Table 124: CLI "Port Mirroring" Configuration

Node	Command	Description
enable	show mirror	This command displays the current "Port Mirroring" configurations.
configure	mirror (disable enable)	This command disables/enables "Port Mirroring" on the switch.
configure	mirror destination port PORT_ID	This command specifies the monitor port for the port mirroring.
configure	mirror source ports PORT_LIST mode (both ingress egress)	This command adds a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command removes a port or a range of ports from the source ports of the port mirroring.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#mirror enable
```

```
L2SWITCH(config)#mirror destination port 2
```

```
L2SWITCH(config)#mirror source ports 3-11 mode both
```

11.3.2.4 Port Settings

Table 125: CLI "Port Settings" Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none mac)	This command tests the loopback mode of operation for the specific port.
interface	Flow control (off on)	This command disables/enables the flow control for the port.
interface	speed (auto 10-full 10-half 100-full 100-half)	This command configures the speed and duplex mode for a port.
interface	shutdown	This command disables a specific port.
interface	no shutdown	This command enables a specific port.
interface	description STRINGs	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
interface	cable test start	This command starts to diagnostics the Ethernet cable.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto 10-full 10-half 100-full 100-half 1000-full)	This command configures the speed and duplex for the port.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface fa1/0/1*

L2SWITCH(config-if)#*speed auto*

11.3.3 Advanced Settings

11.3.3.1 Bandwidth Control

11.3.3.1.1 QoS

Table 126: CLI “QoS” Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the “Service Queue”.
enable	show qos mode	This command displays the current IEEE 802.1p QoS mode.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping of the “Service Queue”.
configure	no queue cos-map	This command configures the default settings for the 802.1p priority mapping of the “Service Queue”.
configure	qos mode high-first	This command sets the QoS mode to “high_first” so every “Hardware Queue” transmits all packets in its buffer before permitting the next lower priority queue to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command sets the QoS mode to “Weighted Round Robin”.
interface	default-priority	This command allows the user to specify which priority is assigned by default to the untagged packets received by the switch. The priority value entered with this command is used to determine which of the “Hardware Priority Queues” the packet is forwarded to. Default: 0.
interface	no default-priority	This command sets the default priority for the specific port to 0.
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable enable)	This command disables/enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

11.3.3.1.2 Rate Limitation

Table 127: CLI "Rate Limitation" Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current "Rate Limitation" configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the rate limitation for outgoing packets and sets the limit.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the rate limitation for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the rate limitation for incoming packets and sets the limit.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the rate limitation for incoming packets.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*bandwidth-limit egress 1 ports 1-8*

L2SWITCH(config)#*bandwidth-limit ingress 1 ports 1-8*

11.3.3.1.2.1 Storm Control

Table 128: CLI "Storm Control" Configuration

Node	Command	Description
enable	show storm-control	This command displays the current "Storm Control" configurations.
configure	storm-control rate RATE_LIMIT type (bcast mcast DLF bcast+ mcast bcast+DLF mcast+ DLF bcast+mcast+DLF) ports PORTLISTS	This command enables the rate limitation for broadcast, multicast or DLF packets and sets the rate limitation for a specified type.
configure	no storm-control type (bcast mcast DLF bcast+ mcast bcast+DLF mcast+ DLF bcast+mcast+DLF) ports PORTLISTS	This command disables the rate limitation for broadcast, multicast or DLF packets.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*storm-control rate 1 type broadcast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type multicast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type DLF ports 1-6*

11.3.3.2 IGMP Snooping

Table 129: CLI "IGMP Snooping" Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current "IGMP Snooping" configurations.
enable	show igmp-snooping counters	This command displays the current IGMP snooping counters.
enable	show igmp-snooping querier	This command displays the current IGMP Queriers.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears all of the IGMP snooping counters.
configure	igmp-snooping (disable enable)	This command disables/enables "IGMP Snooping" on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables "IGMP Snooping" on a VLAN or VLAN range.
configure	no igmp-snooping vlan VLAN_ID	This command disables "IGMP Snooping" on a VLAN or VLAN range.
configure	igmp-snooping unknown-multicast(drop flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled.
configure	igmp-snooping report-suppression (disable enable)	This command disables/enables the "IGMP Snooping Report Suppression" function on the switch.
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port vlan)	This command clears the IGMP snooping counters for port or vlan.
interface	igmp-querier-mode (auto fixed edge)	This command specifies if and under what conditions the ports are "IGMP Query Ports". The switch forwards the "IGMP Join/Leave" packets to an "IGMP Query Port," treating the port as if it were connected to an IGMP multicast router (or server). "IGMP Snooping" must also be enabled (default: "Auto").
interface	igmp-immediate-leave	The command enables the "Immediate Leave" function for "IGMP Snooping" for a specific interface.
interface	no igmp-immediate-leave	The command disables the "Immediate Leave" function for "IGMP Snooping" for a specific interface.
interface	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific interface.
interface	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific interface.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific ports.
if-range	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific ports.

Table 129: CLI "IGMP Snooping" Configuration

Node	Command	Description
if-range	igmp-querier-mode (auto fixed edge)	This command specifies whether or not and under what conditions the ports are IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)

Example

```
L2SWITCH(config)#igmp-snooping enable
```

```
L2SWITCH(config)#igmp-snooping vlan 1
```

```
L2SWITCH(config)#igmp-snooping querier enable
```

```
L2SWITCH(config)#igmp-snooping querier vlan 1
```

```
L2SWITCH(config)#interface 1/0/1
```

```
L2SWITCH(config-if)#igmp-immediate-leave
```

```
L2SWITCH(config-if)# igmp-querier-mode fixed
```

```
L2SWITCH(config-if)# igmp-snooping group-limit 20
```

11.3.3.2.1 IGMP Snooping Querier

Table 130: CLI "IGMP Snooping Querier" Configuration

Node	Command	Description
configure	igmp-snooping querier (disable enable)	This command disables/enables the IGMP snooping querier on the Switch.
configure	igmp-snooping querier vlan VLANIDs	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANIDs	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.

11.3.3.2.2 IGMP Snooping Filtering

Table 131: CLI "IGMP Snooping Filtering" Configuration

Node	Command	Description
enable	show igmp-snooping filtering	This command displays the IGMP snooping filtering configurations.
configure	igmp-snooping filtering (enable disable)	This command enables/disables the IGMP snooping filtering profiles on the Switch.
configure	igmp-snooping filtering profile	This command enters the IGMP snooping filtering profiles configuration node.
configure	no igmp-snooping filtering all	This command removes all of the IGMP snooping filtering profiles from the Switch.
configure	no igmp-snooping filtering STRINGS	This command removes the IGMP snooping filtering profiles by name from the Switch.
config-igmp	Group GROUP_ID start-address START-ADDR end-address END-ADDR	This command configures the group configurations, including group index and start multicast address and end multicast address.
config-igmp	type (deny permit)	This command configures the type of deny or permit for the group.
config-igmp	no group GROUP-ID	This command removes the group configurations.
config-igmp	no group all	This command removes all of the group configurations.
config-igmp	type (deny permit)	This command configures the type of deny or permit for the group.
interface	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the specific port.
interface	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-config	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the range of ports.
if-config	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the range of ports.

11.3.3.3 Multicast Address

Table 132: CLI "Multicast Address" Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan VLANID	This command displays the current static/dynamic multicast address entries with a specific vlan.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command deletes a static multicast entry from the address table.

11.3.3.4 VLAN

11.3.3.4.1 Port-Isolation

Table 133: CLI "Port Isolation" Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current "Port Isolation" configurations. "V" indicates that the port's packets can be sent to this port. "-" indicates that the port's packets cannot be sent to this port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to forward traffic from a specific port.
interface	no port-isolation	This command configures all ports to forward data packets from a specific port.

Example

L2SWITCH(config)#*interface 1/0/2*

L2SWITCH(config-if)#*port-isolation ports 3-10*

11.3.3.4.2 VLAN Settings

Table 134: CLI "VLAN Settings" Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1–4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1–4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be a combination of numbers, letters, hyphens (-) and underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command resets the VLAN name to the default setting. Note: The default VLAN name is comprised as follows: "VLAN"+VLAN_ID, VLAN1, VLAN2, ...
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORT_LIST	This command assigns ports to a VLAN group as fixed subscribers.
vlan	no fixed PORTLISTS	This command deletes all fixed ports from a VLAN.
vlan	tagged PORT_LIST	This command assigns fixed ports to a VLAN group as tagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no tagged PORTLISTS	This command deletes all permanently assigned tagged ports from a VLAN.
vlan	untagged PORT_LIST	This command assigns fixed ports to a VLAN group as untagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no untagged PORTLISTS	This command deletes all untagged ports from a VLAN.
interface	acceptable frame type (all tagged untagged)	This command configures the acceptable frame type. All – acceptable all frame types. tagged – acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.

Table 134: CLI "VLAN Settings" Configuration

Node	Command	Description
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#vlan 2
```

```
L2SWITCH(config-vlan)#fixed 1-6
```

```
L2SWITCH(config-vlan)#untagged 1-3
```

11.3.3.4.3 MAC VLAN

Table 135: CLI "MAC VLAN" Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Example

```
L2SWITCH(config)# mac-vlan 00:01:02:03:04vlan 111 priority 1
```

```
L2SWITCH(config)# mac-vlan 00:01:02:22:04vlan 121 priority 1
```

```
L2SWITCH(config)# mac-vlan 00:01:22:22:04:05 vlan 221 priority 1
```

11.3.3.5 LLDP

Table 136: CLI "LLDP" Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all the information of the port neighbors.
configure	lldp (disable enable)	This command globally enables/disables the LLDP function on the switch.
configure	lldp tx-interval	This command configures the transmission interval for LLDP packets.
configure	lldp tx-hold	This command configures the "tx-Hold Time" that determines the TTL of the switch message. (TTL = tx-hold * tx-interval)
interface	lldp-agent (disable enable rx-only tx-only)	This command configures the Agent function for LLDP. "disable": LLDP is disabled for a specific port. "enable": The LLDP packet is transmitted on a specific port and received. "tx-only": The LLDP packet is only transmitted on a specific port. "rx-only": The LLDP packet is only received on a specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	lldp-agent (disable enable rx-only tx-only)	This command configures the LLDP agent function. "disable": Disable the LLDP on the specific port. "enable": Transmit and Receive the LLDP packet on the specific port. "tx-only": Transmit the LLDP packet on the specific port only. "rx-only": Receive the LLDP packet on the specific port.

11.3.3.6 Loop Detection

Table 137: CLI "Loop Detection" Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable enable)	This command disables/enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default. (00:0b:04:AA:AA:AB)
interface	loop-detection (disable enable)	This command disables/enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable enable)	This command enables/disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable enable)	This command disables/enables the loop detection on the ports.
if-range	loop-detection recovery (disable enable)	This command enables/disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example

L2SWITCH(config)#*loop-detection enable*

L2SWITCH(config)#*interface 1/0/1*

L2SWITCH(config-if)#*loop-detection enable*

11.3.3.7 MRP

Table 138: CLI "MRP" Configuration

Node	Command	Description
enable	show mrp information	This command displays the overall mrp's configured information and also global mrp settings
enable	show mrp ring-id [RING_ID]	This command displays the mrp information of the specific
configure	mrp enable	This command enables the media redundancy protocol on the switch.
configure	no mrp enable	This command disables media redundancy protocol on the switch.
configure	Mrp ring-id <1-4>	This command creates the particular ring with mentioned ID
enable	show mrp information	This command displays the overall mrp's configured information and also global mrp settings
enable	show mrp ring-id [RING_ID]	This command displays the mrp information of the specific
configure	mrp enable	This command enables the media redundancy protocol on the switch.
configure	no mrp enable	This command disables media redundancy protocol on the switch.
configure	Mrp ring-id <1-4>	This command creates the particular ring with mentioned ID
configure-mrp	ring uuid	This command configures the universal unique identifier (UUID) for the ring. It's a string in hexadecimal format representing the ring to which this switch belongs to. ex: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
configure-mrp	no ring enable	This command disables the particular ring
configure-mrp	no ring mode	This command removes the node mode.
configure-mrp	no ring port-1	This command removes the port-1 for the ring on the Switch.
configure-mrp	no ring port-2	This command removes the port-2 for the ring on the Switch.
configure-mrp	no ring vlan	This command removes the ring on that VLAN.
configure-mrp	no ring uuid	This command removes the universal unique identifier (UUID) for the ring.

11.3.3.8 STP

Table 139: CLI "STP" Configuration

Node	Command	Description
enable	show spanning-tree active	This command only displays STP information for active ports.
enable	show spanning-tree blocked ports	This command only displays STP information for blocked ports.
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree summary	This command displays a summary of the port states and configurations
enable	clear spanning-tree counters	This command clears the STP statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears the STP statistics for a specific port.
configure	spanning-tree (disable enable)	This command disables/enables the STP function in the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times ("Forward Delay", "Max Age", "Hello Time").
configure	no spanning-tree algorithm-timer	This command configures the default values for "Forward Delay", "Max Age" and "Hello Time."
configure	spanning-tree forward-time <4-30>	This command configures the "Forward Delay" period (in seconds) for the bridge.
configure	no spanning-tree forward-time	This command configures the default values for "Forward Delay".
configure	spanning-tree hello-time <1-10>	This command configures the "Hello Time" period (in seconds) for the bridge.
configure	no spanning-tree hello-time	This command configures the default values for the "Hello Time".
configure	spanning-tree max-age <6-40>	This command configures the "Max Age" period (in seconds) for bridge messages.
configure	no spanning-tree max-age	This command configures the default values for the "Max Age".
configure	spanning-tree mode (rstp stp)	This command configures the STP mode.
configure	spanning-tree pathcost method (short long)	This command configures the path cost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree bpdupfilter (disable enable)	This command configures enables/disables the "BPDU Filter" function.
interface	spanning-tree bpduguard (disable enable)	This command configures enables/disables the "BPDU Guard" function.
interface	spanning-tree edge-port (disable enable)	This command enables/disables the "Edge Port" setting.
interface	spanning-tree rootguard (disable enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
interface	spanning-tree edge-port(disable enable)	This command enables/disables the edge port setting for the specific port.

Table 139: CLI "STP" Configuration

Node	Command	Description
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	spanning-tree(disable enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdupfilter(disable enable)	This command configures enables/disables the bpdu filter function for the specific port.
if-range	spanning-tree bpduguard(disable enable)	This command configures enables/disables the bpdu guard function for the specific port.
if-range	spanning-tree rootguard(disable enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port(disable enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
if-range	no spanning-tree cost	This command configures the path cost to default for the specific port.
if-range	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

11.3.4 Security

11.3.4.1 Access Control List

Table 140: CLI "Access Control List" Configuration

Node	Command	Description
enable	show access-list	This command displays all access control profiles.
configure	access-list STRING	This command creates a new access control profile.
configure	no access-list STRING	This command deletes an access control profile.
acl	Show	This command displays the current access control profile.
acl	action (disable drop permit)	This command processes this profile. "disable": The profile is disabled. "drop": If packets match the profile, they are dropped. "permit": If packets match the profile, they are forwarded.
acl	destination mac hostMACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source MAC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.

Table 140: CLI "Access Control List" Configuration

Node	Command	Description
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Example:

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#access-list 111
```

```
L2SWITCH(config-acl)#vlan 2
```

```
L2SWITCH(config-acl)#source interface 1
```

```
L2SWITCH(config-acl)#show
```

11.3.5 Monitor

11.3.5.1 Alarm

Table 141: CLI "Alarm" Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

11.3.5.2 Monitor Information

Table 142: CLI "Monitor Information" Configuration

Node	Command	Description
enable	show hardware-monitor (C F)	This command displays hardware operation information.

11.3.5.3 Port Statistics

Table 143: CLI "Port Statistics" Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

11.3.5.4 Port Utilization

Table 144: CLI "Port Statistics" Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

11.3.5.5 RMON Statistics

Table 145: CLI "RMON Statistics" Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears the RMON statistics for one or all ports.

11.3.5.6 SFP Information

Table 146: CLI "SFP Information" Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

11.3.5.7 Traffic Monitor

Table 147: CLI “Traffic Monitor” Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the “Traffic Monitor” configurations and current status.
configure	traffic-monitor (disable enable)	This command enables/disables the “Traffic Monitor” on the switch.
interface	traffic-monitor (disable enable)	This command enables/disables the “Traffic Monitor” on a specific port.
interface	traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and type for the “Traffic Monitor” on a specific port. mcast: broadcast packet mcast: multicast packet The rate should be greater than 50 pps.
interface	traffic-monitor recovery (disable enable)	This command enables/disables the “Recover” function for the “Traffic Monitor” on a specific port.
interface	traffic-monitor recovery time VALUE	This command configures the “Recovery Time” for the “Traffic Monitor” on a specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	traffic-monitor (disable enable)	This command enables/disables the traffic monitor on the port.
if-range	traffic-monitor rateRATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.
if-range	traffic-monitor recovery (disable enable)	This command enables/disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.

11.3.6 Management

11.3.6.1 SNMP

11.3.6.1.1 SNMP

Table 148: CLI “SNMP” Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro rw) trusted-host IPADDR	This command configures the “SNMP Community” name.
configure	snmp (disable enable)	This command disables/enables SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command assigns a name to the system.
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver’s configurations, including the IP address, version (v1 or v2c) and “Community.”

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*snmp enable*

L2SWITCH(config)#*snmp community public rw trusted-host 192.168.200.106/24*

L2SWITCH(config)#*snmp trap-receiver 192.168.200.106 v2c public*

L2SWITCH(config)#*snmp system-contact IT engineer*

L2SWITCH(config)#*snmp system-location Wago*

11.3.6.1.2 SNMP Trap

Table 149: CLI "SNMP Trap" Configuration

Node	Command	Description
enable	show snmp trap-event	This command displays the SNMP configurations.
configure	snmp trap-event alarm-over-heat (disable/enable)	This command enables/disables the alarm-over-heat trap.
configure	snmp trap-event alarm-over-load (disable/enable)	This command enables/disables the alarm-over-load trap.
configure	snmp trap-event alarm-power-fail (enable/enable)	This command enables/disables the alarm-power-fail trap.
configure	snmp trap-event bpdu (disable/enable)	This command enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap.
configure	snmp trap-event dual-homing (disable/enable)	This command enables/disables the dual-homing trap.
configure	snmp trap-event dying-gasp (disable/enable)	This command enables/disables the dying-gasp trap.
configure	snmp trap-event loop-detection (disable/enable)	This command enables/disables the loop-detection trap.
configure	snmp trap-event pd-alive (disable/enable)	This command enables/disables the pd-alive trap.
configure	snmp trap-event port-admin-state-change (disable/enable)	This command enables/disables the port-admin-state-change trap.
configure	snmp trap-event port-link-change (disable/enable)	This command enables/disables the port-link-change trap.
configure	snmp trap-event power-source-change (disable/enable)	This command enables/disables the power-source-change trap.
configure	snmp trap-event stp-topology-change (disable/enable)	This command enables/disables the stp-topology-change trap.
configure	snmp trap-event traffic-monitor (disable/enable)	This command enables/disables the traffic-monitor trap.
configure	snmp trap-event xpress-ring (disable/enable)	This command enables/disables the xpress-ring trap.

11.3.6.1.2.1 Port Trap Settings

Table 150: CLI "Port Trap Settings" Configuration

Node	Command	Description
enable	show snmp port-link-change-trap	This command displays the SNMP port link-change trap configurations.
interface	snmp port-link-change-trap	This command enables the link change trap on the specific port.
interface	no snmp port-link-change-trap	This command disables the link change trap on the specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	snmp port-link-change-trap	This command enables the link change trap on the specific ports.
if-range	no snmp port-link-change-trap	This command disables the link change trap on the specific ports.

11.3.6.1.3 SNMPv3

Table 151: CLI "SNMPv3" Configuration

Node	Command	Description
enable	show snmp user	This command displays all snmp v3 users.
enable	show snmp group	This command displays all snmp v3 groups.
enable	show snmp view	This command displays all snmp v3 view.
configure	snmp user USERNAME GROUPNAME noauth	Configures v3 user of non- authentication.
configure	snmp user USERNAME GROUPNAME auth (MD5 SHA) STRINGS	Configures v3 user of authentication.
configure	snmp user USERNAME GROUPNAME priv (MD5 SHA) STRINGS des STRINGS	Configures v3 user osnmf authentication and encryption.
configure	snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non- authentication.
configure	snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication.
configure	snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	snmp view VIEWNAME STRINGS (included excluded)	To identify the subtree.
configure	no snmp user USERNAME GROUPNAME	This command removes a v3 user from switch.
configure	no snmp group GROUPNAME	This command removes a v3 group from switch.
configure	no snmp view VIEWNAME STRINGS	This command removes a v3 view from switch.

11.3.6.2 Maintenance

Table 152: CLI "Maintenance" Configuration

Node	Command	Description
enable	show config-change-status	This command displays the configurations status if there are default values.
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. Note: The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw<URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface eth0*

L2SWITCH(config-if)#*ip address 172.20.1.101/24*

L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*

L2SWITCH(config-if)#*management vlan 1*

11.3.6.2.1 Reboot

Table 153: CLI "Reboot" Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	web server	This command enables the web on the Switch.
configure	no web server	This command disables the web on the Switch.

11.3.6.3 System Log

Table 154: CLI "System Log" Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	clear syslog	The command clears the syslog message.
configure	syslog-server (disable enable)	The command disables/enables the syslog server function.
configure	syslog-server ipv4-ip IPADDR	The command configures the syslog server's IP address in IPv4 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#syslog-server ip 192.168.200.106
```

```
L2SWITCH(config)#syslog-server enable
```

11.3.6.4 User Account

Table 155: CLI "USB Flash" Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#add user q q admin
```

```
L2SWITCH(config)#add user 1 1 normal
```

Abbildungsverzeichnis

Abbildung 1: Parallele Nutzung von Standard ETHERNET und PROFINET	20
Abbildung 2: Frontansicht des Industrial-Managed-Switches	24
Abbildung 3: Draufsicht des Industrial-Managed-Switches	26
Abbildung 4: Anschluss Spannungsversorgung (PWR/RPS)	27
Abbildung 5: Netzwerkanschlüsse	28
Abbildung 6: Geräte-LEDs	30
Abbildung 7: LEDs für RJ-45-Anschlüsse	31
Abbildung 8: DIP-Schalter	32
Abbildung 9: Reset-Taster	33
Abbildung 10: Aufkleber (Beispiel)	34
Abbildung 11: Adressierung der Daten eines IO-Devices über Slots bzw. Subslots	41
Abbildung 12: Zuordnung der Subslots im PROFINET-Managed-Switch von WAGO	42
Abbildung 13: Kommunikationsbeziehungen bei PROFINET	44
Abbildung 14: Übersicht der Konformitätsklassen A bis C	49
Abbildung 15: Medienredundanz bei PROFINET (Ringtopologie)	52
Abbildung 16: Allgemeiner Aufbau einer GSDML-Datei	58
Abbildung 17: PROFINET-Parameter – Bereich „Allgemein“	66
Abbildung 18: PROFINET-Parameter – Bereich „PROFINET-Schnittstelle [X1]“	67
Abbildung 19: PROFINET-Parameter – Bereich „Erweiterte Optionen“	68
Abbildung 20: PROFINET-Parameter – Bereich „Port 1“	70
Abbildung 21: PROFINET-Parameter – Bereich „Allgemein“	71
Abbildung 22: PROFINET-Parameter – Bereich „Identification & Maintenance“	72
Abbildung 23: PROFINET-Parameter – Bereich „Prozessalarme“	73
Abbildung 24: PROFINET-Parameter – Bereich „Baugruppenparameter“	74
Abbildung 25: PROFINET-Parameter – Bereich „E/A-Adressen“	76
Abbildung 26: Aufrufen des PROFINET-Managed-Switches über das WBM	88
Abbildung 27: Anmeldefenster für WBM	90
Abbildung 28: WBM-Seite „Systeminformationen“	92
Abbildung 29: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	94
Abbildung 30: WBM-Seite „Port-Spiegelung-Einstellungen“	96
Abbildung 31: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“	98
Abbildung 32: WBM-Seite „PROFINET Setting“	99
Abbildung 33: WBM-Seite „Informationen“	100
Abbildung 34: WBM-Seite „Diagnoseliste“	101
Abbildung 35: WBM-Seite „MRP“	102
Abbildung 36: WBM-Seite „Datei hochladen“	105
Abbildung 37: WBM-Seite „Benutzerkonto“	105
Abbildung 38: Ablaufdiagramm der MAC-Adresstabelle	114
Abbildung 39: Halbduplexmodus	116
Abbildung 40: Vollduplexmodus	116
Abbildung 41: Multicast-Adresse	131
Abbildung 42: WBM-Seite „Systeminformation“	155
Abbildung 43: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	157

Abbildung 44: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“	159
Abbildung 45: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“	160
Abbildung 46: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“	163
Abbildung 47: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“	164
Abbildung 48: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“	166
Abbildung 49: WBM-Seite „MAC Management“ – Register „Age-Time-Einstellung“	167
Abbildung 50: WBM-Seite „MAC Management“ – Register „Blacklisting“	168
Abbildung 51: WBM-Seite „Port-Spiegelung“	169
Abbildung 52: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“	171
Abbildung 53: WBM-Seite „Port-Einstellungen“ – Register „Informationen“	173
Abbildung 54: WBM-Seite „QoS“ – Register „Port-Priorität“	174
Abbildung 55: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“	175
Abbildung 56: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“	176
Abbildung 57: WBM-Seite „QoS“ – Register „Schedule-Modus“	177
Abbildung 58: WBM-Seite „Bandbreitenbegrenzung“ – Register „Sturmbegrenzung“	179
Abbildung 59: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“	181
Abbildung 60: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“	182
Abbildung 61: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“ ...	184
Abbildung 62: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“	186
Abbildung 63: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“	187
Abbildung 64: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“	188
Abbildung 65: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“	189
Abbildung 66: WBM-Seite „Statische Multicast-Adressen“	190
Abbildung 67: WBM-Seite „Multicast-Statistiken“	191
Abbildung 68: WBM-Seite „Port Isolation“	192
Abbildung 69: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“	194
Abbildung 70: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“	196
Abbildung 71: WBM-Seite „VLAN“ – Register „Port-Einstellungen“	197
Abbildung 72: WBM-Seite „MAC-VLAN“	199
Abbildung 73: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“	200
Abbildung 74: WBM-Seite „LLDP“ – Register „Nachbarerkennung“	202
Abbildung 75: WBM-Seite „Schleifenerkennung“	203
Abbildung 76: WBM-Seite „MRP Global Settings“	205
Abbildung 77: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“	208
Abbildung 78: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“	210
Abbildung 79: WBM-Seite „Spanning Tree Protocol“ – Register „STP-Status“ ..	213
Abbildung 80: WBM-Seite „Access-Control-Liste“	214
Abbildung 81: WBM-Seite „Alarminformationen“	218

Abbildung 82: WBM-Seite „Systeminformationen“	219
Abbildung 83: WBM-Seite „Port-Statistik“	221
Abbildung 84: WBM-Seite „Port-Auslastung“	222
Abbildung 85: WBM-Seite „RMON-Statistiken“	223
Abbildung 86: WBM-Seite „SFP-Informationen“	226
Abbildung 87: WBM-Seite „Traffic-Monitor“	229
Abbildung 88: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“	232
Abbildung 89: WBM-Seite „SNMP“ – Register „Community-Name“	233
Abbildung 90: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver- Einstellungen“	235
Abbildung 91: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“	236
Abbildung 92: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“	237
Abbildung 93: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“	238
Abbildung 94: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3- Gruppen“	240
Abbildung 95: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-View“	241
Abbildung 96: WBM-Seite „Wartung“ – Register „Konfiguration“	242
Abbildung 97: WBM-Seite „Wartung“ – Register „Firmware“	244
Abbildung 98: WBM-Seite „Wartung“ – Register „Neustart“	245
Abbildung 99: WBM-Seite „Wartung“ – Register „Rebooten“ – Meldung	245
Abbildung 100: WBM-Seite „Wartung“ – Register „Protokolle“	246
Abbildung 101: WBM-Seite „System-Log“	248
Abbildung 102: WBM-Seite „Datei hochladen“	250
Abbildung 103: WBM-Seite „Ping“	251
Abbildung 104: WBM-Seite „Benutzerkonto“	252
Abbildung 105: RJ-45 Anschlussbelegung	254
Abbildung 106: Anschlussbelegung RJ-45 zu DB9	254

Tabellenverzeichnis

Tabelle 1: Darstellungen der Zahlensysteme	12
Tabelle 2: Schriftkonventionen	12
Tabelle 3: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“	24
Tabelle 4: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“	26
Tabelle 5: Legende zur Abbildung „Anschluss Spannungsversorgung (PWR/RPS)“	27
Tabelle 6: Legende zur Abbildung „Netzwerkanschlüsse“	28
Tabelle 7: Legende zur Abbildung „Geräte-LEDs“	30
Tabelle 8: Legende zur Abbildung „LEDs für RJ-45-Anschlüsse“	31
Tabelle 9: Legende zur Abbildung „DIP-Schalter“	32
Tabelle 10: Legende zur Abbildung „Reset-Taster“	33
Tabelle 11: Legende zur Abbildung „Aufkleber (Beispiel)“	34
Tabelle 12: Technische Daten – Gerätedaten	35
Tabelle 13: Technische Daten – Systemdaten	35
Tabelle 14: Technische Daten – Versorgung	35
Tabelle 15: Technische Daten – Kommunikation	36
Tabelle 16: Technische Daten – Umgebungsbedingungen	37
Tabelle 17: Beispiele für Provider und Consumer	39
Tabelle 18: Adressierung der Daten in Abhängigkeit von der Übertragungsart	41
Tabelle 19: Bereiche im PROFINET-Telegramm	47
Tabelle 20: Vergleich Konformitätsklassen	51
Tabelle 21: Legende zur Abbildung „Medienredundanz bei PROFINET (Ringtopologie)“	52
Tabelle 22: Übersicht Projektierungstools	62
Tabelle 23: PROFINET-Parameter für Bereich „Allgemein“	67
Tabelle 24: PROFINET-Parameter für Bereich „PROFINET-Schnittstelle [X1]“	68
Tabelle 25: PROFINET-Parameter für Bereich „Erweiterte Optionen“	69
Tabelle 26: PROFINET-Parameter für Bereich „Port 1“	70
Tabelle 27: PROFINET-Parameter für Bereich „Erweiterte Optionen“	71
Tabelle 28: PROFINET-Parameter für Bereich „Identification & Maintenance“	72
Tabelle 29: PROFINET-Parameter für Bereich „Prozessalarme“	73
Tabelle 30: PROFINET-Parameter für Bereich „Baugruppenparameter“	75
Tabelle 31: PROFINET-Parameter für Bereich „E/A-Adressen“	76
Tabelle 32: Format für zyklische I/O-Daten – PROFINET	78
Tabelle 33: Zyklischer Eingang für die Gerätediagnose	78
Tabelle 34: Zyklischer Eingang für Status Port Pn (n = 1 ... 12)	80
Tabelle 35: DAP-Parameter für WAGO PROFINET-Switch	81
Tabelle 36: Diagnosemeldungen aktivieren/deaktivieren	81
Tabelle 37: Lesen des Port-Status (pro Port)	82
Tabelle 38: Lesen der Gerätediagnosen	83
Tabelle 39: Konfigurieren der Funktion Port-Spiegelung	84
Tabelle 40: Default-Einstellungen für den Konsolen-Port	85
Tabelle 41: Übersicht - Navigationslinks und WBM-Seiten	91
Tabelle 42: WBM-Seite „Systeminformationen“ (Beispiel 852-1605 übertragbar auf 852-0602, -0603)	93

Tabelle 43: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	95
Tabelle 44: WBM-Seite „Port-Spiegelung-Einstellungen“	97
Tabelle 45: WBM-Seite „PROFINET Setting“	99
Tabelle 46: WBM-Seite „MRP“	103
Tabelle 47: WBM-Seite „Datei hochladen“	105
Tabelle 48: WBM-Seite „Benutzerkonto“	105
Tabelle 49: Prioritätsebenen.....	122
Tabelle 50: Multicast-Klassen und -Adressbereiche	130
Tabelle 51: IP-Multicast-Adressen.....	131
Tabelle 52: STP-Pfadkosten.....	140
Tabelle 53: Default-Einstellungen für den Telnet-Port	150
Tabelle 54: Default-Einstellungen für den Konsolen-Port	151
Tabelle 55: Anmeldebildschirm	151
Tabelle 56: Übersicht – Navigationslinks und WBM-Seiten	153
Tabelle 57: WBM-Seite „Systeminformation“	156
Tabelle 58: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	158
Tabelle 59: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“	159
Tabelle 60: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“	161
Tabelle 61: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“	163
Tabelle 62: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“	165
Tabelle 63: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“	166
Tabelle 64: „MAC Management“ – Register „Age-Time-Einstellung“	167
Tabelle 65: WBM-Seite „MAC Management“ – Register „Blacklisting“	168
Tabelle 66: WBM-Seite „Port-Spiegelung“	170
Tabelle 67: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“	172
Tabelle 68: WBM-Seite „Port-Einstellungen“ – Register „Informationen“	173
Tabelle 69: WBM-Seite „QoS“ – Register „Port-Priorität“	174
Tabelle 70: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“	175
Tabelle 71: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“	176
Tabelle 72: Default-Einstellungen.....	176
Tabelle 73: WBM-Seite „QoS“ – Register „Schedule-Modus“	178
Tabelle 74: WBM-Seite „Rate Limitation“ – Register „Sturmbegrenzung“	180
Tabelle 75: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“	181
Tabelle 76: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“	183
Tabelle 77: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“	185
Tabelle 78: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“	186
Tabelle 79: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“	187
Tabelle 80: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“	188
Tabelle 81: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“	189
Tabelle 82: WBM-Seite „Statische Multicast-Adressen“	190
Tabelle 83: WBM-Seite „Multicast-Statistiken“	191
Tabelle 84: WBM-Seite „Port Isolation“	193
Tabelle 85: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“	195
Tabelle 86: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“	196
Tabelle 87: WBM-Seite „VLAN“ – Register „Port-Einstellungen“	198

Tabelle 88: WBM-Seite „MAC-VLAN“	199
Tabelle 89: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“	201
Tabelle 90: WBM-Seite „LLDP“ – Register „Nachbarererkennung“	202
Tabelle 91: WBM-Seite „Schleifenerkennung“	204
Tabelle 92: WBM-Seite „MRP“	206
Tabelle 93: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“	209
Tabelle 94: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“	211
Tabelle 95: WBM-Seite „STP“ – Register „STP-Status“	213
Tabelle 96: WBM-Seite „Access-Control-Liste“	215
Tabelle 97: WBM-Seite „Alarminformationen“	218
Tabelle 98: WBM-Seite „Systeminformationen“	220
Tabelle 99: WBM-Seite „Port-Statistik“	221
Tabelle 100: WBM-Seite „Port-Auslastung“	222
Tabelle 101: WBM-Seite „RMON-Statistiken“	224
Tabelle 102: WBM-Seite „SFP-Informationen“	227
Tabelle 103: WBM-Seite „Traffic-Monitor“	230
Tabelle 104: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“	232
Tabelle 105: WBM-Seite „SNMP“ – Register „Community-Name“	234
Tabelle 106: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“	235
Tabelle 107: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“	236
Tabelle 108: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“	237
Tabelle 109: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“	239
Tabelle 110: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-Gruppen“	240
Tabelle 111: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-View“	241
Tabelle 112: WBM-Seite „Wartung“ – Register „Protokolle“	247
Tabelle 113: WBM-Seite „System-Log“	249
Tabelle 114: WBM-Seite „Datei hochladen“	250
Tabelle 115: WBM-Seite „Ping“	251
Tabelle 116: WBM-Seite „Benutzerkonto“	253
Tabelle 117: RJ-45-Kabel	255
Table 118: CLI “System Information” Configuration	256
Table 119: CLI “System” Configuration	257
Table 120: CLI “Jumbo Frame” Configuration	258
Table 121: CLI “SNTP” Configuration	258
Table 122: CLI “Management Host” Configuration	259
Table 123: CLI “MAC Management” Configuration	260
Table 124: CLI “Port Mirroring” Configuration	260
Table 125: CLI “Port Settings” Configuration	261
Table 126: CLI “QoS” Configuration	262
Table 127: CLI “Rate Limitation” Configuration	263
Table 128: CLI “Storm Control” Configuration	263
Table 129: CLI “IGMP Snooping” Configuration	264
Table 130: CLI “IGMP Snooping Querier” Configuration	266
Table 131: CLI “IGMP Snooping Filtering” Configuration	266
Table 132: CLI “Multicast Address” Configuration	267
Table 133: CLI “Port Isolation” Configuration	267
Table 134: CLI “VLAN Settings” Configuration	268

Table 135: CLI "MAC VLAN" Configuration	269
Table 136: CLI "LLDP" Configuration	270
Table 137: CLI "Loop Detection" Configuration.....	271
Table 138: CLI "MRP" Configuration	272
Table 139: CLI "STP" Configuration	273
Table 140: CLI "Access Control List" Configuration	275
Table 141: CLI "Alarm" Configuration	277
Table 142: CLI "Monitor Information" Configuration	277
Table 143: CLI "Port Statistics" Configuration.....	277
Table 144: CLI "Port Statistics" Configuration.....	277
Table 145: CLI "RMON Statistics" Configuration	277
Table 146: CLI "SFP Information" Configuration.....	277
Table 147: CLI "Traffic Monitor" Configuration.....	278
Table 148: CLI "SNMP" Configuration	279
Table 149: CLI "SNMP Trap" Configuration.....	280
Table 150: CLI "Port Trap Settings" Configuration.....	280
Table 151: CLI "SNMPv3" Configuration	281
Table 152: CLI "Maintenance" Configuration	282
Table 153: CLI "Reboot" Configuration	282
Table 154: CLI "System Log" Configuration.....	283
Table 155: CLI "USB Flash" Configuration	283



WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Telefax: 0571/887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com