

WAGO-ETHERNET-Zubehör 852



852-1305/000-001

Industrial-Managed-Switch

**8Port 1000BASE-T; 4Slot 1000BASE-SX/-LX; EXT;
USB**

© 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	11
1.1	Gültigkeitsbereich	11
1.2	Urheberschutz	11
1.3	Symbole	12
1.4	Darstellung der Zahlensysteme	13
1.5	Schriftkonventionen	13
2	Wichtige Erläuterungen	14
2.1	Rechtliche Grundlagen	14
2.1.1	Änderungsvorbehalt	14
2.1.2	Personalqualifikation	14
2.1.3	Bestimmungsgemäße Verwendung der Industrial-Switches	14
2.1.4	Technischer Zustand der Geräte	15
2.1.5	Richtlinien und Bestimmungen für die Verwendung der Industrial-Switches	15
2.2	Sicherheitshinweise	16
2.3	Spezielle Einsatzbestimmungen für ETHERNET-Geräte	18
3	Einleitung	19
3.1	Lieferumfang	19
3.2	Industrial ETHERNET-Technologie	19
3.3	Switching-Technologie	20
3.4	Autonegotiation	20
3.5	Autocrossing	21
3.6	Store-and-Forward-Switching-Modus	21
3.7	Übertragungsmethoden	21
4	Gerätebeschreibung	22
4.1	Ansicht	23
4.1.1	Frontansicht	23
4.1.2	Draufsicht	25
4.2	Anschlüsse	26
4.2.1	Erdungsschraube	26
4.2.2	Spannungsversorgung (PWR/RPS)	27
4.2.3	Netzwerkanschlüsse	28
4.2.3.1	RJ-45-Anschluss	29
4.2.3.2	USB-Anschluss	29
4.2.3.3	10/100/1000BASE-T-Anschlüsse	29
4.2.3.4	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
4.5.1	Hardware- und Softwareversion	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	Normen und Richtlinien	38
4.8	Zulassungen	39
5	Montieren	40
5.1	Montageort	40
5.2	Montage auf Tragschiene	40
5.3	Demontage von der Tragschiene	40
6	Geräte anschließen	41
6.1	Spannungsversorgung	41
6.2	Externer Alarmkontakt-Anschluss	42
6.3	Anschluss Konsolenanschlusskabel	42
6.4	Anschluss 1000BASE-SX/LX, Glasfaser	43
6.5	Anschluss 10/100/1000Base-T-Ports	44
7	Funktionsbeschreibung	45
7.1	Grundeinstellungen	45
7.1.1	Jumbo Frame	45
7.1.2	SNTP	45
7.1.3	Management Host	47
7.1.4	MAC-Management	47
7.1.4.1	Static MAC	48
7.1.4.2	Blacklisting (MAC-Blacklist)	48
7.1.5	Port-Spiegelung (Port Mirroring)	49
7.1.6	Port-Einstellungen (Port Settings)	49
7.2	Erweiterte Einstellungen	53
7.2.1	Bandbreiten-Regelung	53
7.2.1.1	QoS („Quality of Service“)	53
7.2.1.2	Bandbreitenbegrenzung	60
7.2.1.2.1	Sturmbegrenzung (Storm Control)	60
7.2.1.2.2	Bandbreitenbegrenzung (Rate Limitation)	60
7.2.2	IGMP Snooping	61
7.2.2.1	Multicast-VLAN-Registrierung (MVR)	64
7.2.2.2	Static Multicast (Multicast-Adresse)	67
7.2.3	VLAN	70
7.2.3.1	Port-Isolation	72
7.2.3.2	GARP/GVRP	73
7.2.3.3	Q-in-Q	75
7.2.3.3.1	Port-basiertes Q-in-Q	78
7.2.3.3.2	Selektives Q-in-Q	79
7.2.4	DHCP-Relay	80
7.2.5	DHCP Options	82
7.2.6	DHCP-Server	84
7.2.7	Dual Homing	85
7.2.8	Dual Ring	86
7.2.9	ERPS	87

7.2.10	Link Aggregation	90
7.2.10.1	Static Trunk	90
7.2.10.2	LACP	90
7.2.11	LLDP	92
7.2.12	Loop Detection (Schleifenerkennung)	93
7.2.13	Jet Ring	94
7.2.14	Static Route	95
7.2.15	Spanning Tree Protocol (STP)	96
7.2.16	Xpress-Ring	101
7.3	Security	102
7.3.1	IP Source Guard	102
7.3.1.1	DHCP Snooping	103
7.3.1.1.1	Server Screening	105
7.3.1.2	Binding Table	105
7.3.1.3	ARP Inspection	106
7.3.1.3.1	Filter Table	107
7.3.2	Access-Control-Liste (ACL)	108
7.3.3	Kommunikationsstandard IEEE 802.1X	109
7.3.4	Port Security	113
7.3.4.1	Sticky-MAC-Einstellungen	113
7.4	Monitor	114
7.4.1	Alarm	114
7.4.2	Systeminformationen	114
7.4.3	Port-Statistik	114
7.4.4	Port-Auslastung	114
7.4.5	RMON Statistiken	114
7.4.6	SFP	115
7.4.6.1	DDMI	115
7.4.7	Traffic Monitor	115
7.5	Management	116
7.5.1	SNMP	116
7.5.2	SNMP Trap	117
7.5.3	SNMPv3	117
7.5.4	Auto Provision	117
7.5.5	Mail-Alarm	119
7.5.6	Ping	119
7.5.7	USB-Funktionen	120
7.5.7.1	Upload der Firmware	120
7.5.7.2	Speichern der Konfigurationsdatei	121
7.5.7.3	Speichern der Syslog-Datei	121
7.5.7.4	Upload der Konfigurationsdatei	121
8	Konfigurieren	123
8.1	Übersicht der Konfigurationsoptionen	123
8.1.1	Telnet-Port	124
8.2	Konsolen-Port	125
9	Web-Based-Management-System (WBM)	126
9.1	Systemstatus	130
9.1.1	Systeminformationen	130
9.2	Grundeinstellungen	132

9.2.1	Allgemeine Einstellungen	132
9.2.1.1	System	132
9.2.1.2	Jumbo Frame	134
9.2.1.3	SNTP	135
9.2.1.4	Management-Host	138
9.2.2	MAC Management	139
9.2.2.1	Statische MAC-Einstellungen	139
9.2.2.2	MAC-Tabelle	141
9.2.2.3	Age-Time-Einstellung	142
9.2.2.4	Blacklisting	143
9.2.3	Port-Spiegelung	144
9.2.4	Port-Einstellungen	146
9.2.4.1	Allgemeine Einstellungen	146
9.2.4.2	Informationen	148
9.3	Erweiterte Einstellungen	149
9.3.1	Bandbreiten-Regelung	149
9.3.1.1	QoS	149
9.3.1.1.1	Port-Priorität	149
9.3.1.1.2	IP-DiffServ (DSCP)	150
9.3.1.1.3	Priorität/Queue-Zuordnung	151
9.3.1.1.4	Schedule-Modus	152
9.3.1.2	Bandbreitenbegrenzung	154
9.3.1.2.1	Sturmbegrenzung	154
9.3.1.2.2	Bandbreitenbegrenzung	156
9.3.2	IGMP Snooping	158
9.3.2.1	IGMP Snooping	158
9.3.2.1.1	Allgemeine Einstellungen	158
9.3.2.1.2	Port-Einstellungen	160
9.3.2.1.3	Querier-Einstellungen	162
9.3.2.2	IGMP-Filter	163
9.3.2.2.1	Allgemeine Einstellungen	163
9.3.2.2.2	Multicast-Gruppen	164
9.3.2.2.3	Port-Einstellungen	165
9.3.2.3	Multicast-VLAN-Registrierung	166
9.3.2.3.1	MVR-Einstellungen	166
9.3.2.3.2	Gruppeneinstellungen	168
9.3.2.4	Static Multicast	169
9.3.2.5	Multicast Statistics	170
9.3.3	VLAN	171
9.3.3.1	Port Isolation	171
9.3.3.2	VLAN	173
9.3.3.2.1	VLAN-Einstellungen	173
9.3.3.2.2	Tag-Einstellungen	175
9.3.3.2.3	Port-Einstellungen	176
9.3.3.3	GARP VLAN Registration Protocol	178
9.3.3.3.1	GVRP	178
9.3.3.3.2	GARP Timer	180
9.3.3.4	IP Subnet VLAN	182
9.3.3.5	MAC VLAN	183
9.3.3.6	Protokoll VLAN	184

9.3.3.7	Q-in-Q	185
9.3.3.7.1	VLAN Stacking.....	185
9.3.3.7.2	Port-based Q-in-Q.....	187
9.3.3.7.3	Selektive Q-in-Q.....	188
9.3.4	DHCP Relay	190
9.3.5	DHCP Options	191
9.3.6	DHCP-Server	193
9.3.6.1	Allgemeine Einstellungen	193
9.3.6.2	Pool-Einstellungen.....	195
9.3.6.3	Binding Information.....	199
9.3.6.4	Statistics.....	200
9.3.7	Dual Homing	201
9.3.8	Dual Ring	203
9.3.9	ERPS.....	205
9.3.9.1	Ringeinstellungen.....	205
9.3.9.2	Instance-Einstellungen	209
9.3.10	Link Aggregation	210
9.3.10.1	Static Trunk	210
9.3.10.2	LACP.....	212
9.3.10.3	LACP Info.....	214
9.3.11	LLDP.....	216
9.3.11.1	LLDP-Einstellungen.....	216
9.3.11.2	Nächster Nachbar	218
9.3.12	Loop Detection.....	219
9.3.13	Jet Ring.....	221
9.3.14	Modbus	223
9.3.15	Static Route	224
9.3.16	Spanning Tree Protocol (STP)	226
9.3.16.1	Allgemeine Einstellungen	226
9.3.16.2	Port-Parameter.....	228
9.3.16.3	STP-Status.....	231
9.3.17	Xpress Ring	232
9.4	Sicherheit	234
9.4.1	IP Source Guard	234
9.4.1.1	DHCP Snooping	234
9.4.1.1.1	DHCP Snooping	234
9.4.1.1.2	Port-Einstellungen.....	236
9.4.1.1.3	Server-Screening	237
9.4.1.2	DHCP-Snooping-Binding-Tabelle	238
9.4.1.2.1	Static-Entry-Einstellungen.....	238
9.4.1.2.2	Binding-Tabelle	240
9.4.1.3	ARP-Überprüfung.....	241
9.4.1.3.1	ARP-Überprüfung	241
9.4.1.3.2	Filtertabelle	243
9.4.2	Access-Control-Liste (ACL).....	244
9.4.3	IEEE 802.1X	248
9.4.3.1	Globale Einstellungen.....	248
9.4.3.2	Port-Einstellungen	251
9.4.4	Port Security	255
9.4.4.1	Port Security.....	255

9.4.4.2	Sticky-MAC-Einstellungen	257
9.5	Monitor	258
9.5.1	Alarminformationen	258
9.5.2	Systeminformationen	259
9.5.3	Port-Statistik	261
9.5.4	Port-Auslastung	262
9.5.5	RMON-Statistiken	263
9.5.6	SFP-Information	266
9.5.7	Traffic-Monitor	269
9.6	Management	272
9.6.1	SNMP	272
9.6.1.1	SNMP	272
9.6.1.1.1	SNMP-Einstellungen	272
9.6.1.1.2	Community Name	273
9.6.1.2	SNMP-Trap	275
9.6.1.2.1	Trap-Receiver-Einstellungen	275
9.6.1.2.2	Trap Event Status	277
9.6.1.2.3	Trap-Port-Einstellungen	278
9.6.1.3	SNMPv3-Konfiguration	279
9.6.1.3.1	SNMPv3-User	279
9.6.1.3.2	SNMPv3-Gruppen	281
9.6.1.3.3	SNMPv3 View	282
9.6.2	Auto Provision	283
9.6.3	Mail-Alarm	284
9.6.4	Wartung	286
9.6.4.1	Konfiguration	286
9.6.4.2	Firmware	288
9.6.4.3	Neustart	289
9.6.4.4	Protokolle	290
9.6.5	System Log	292
9.6.6	Ping	294
9.6.7	USB-Funktionen	295
9.6.8	Benutzerkonto	297
10	Anhang	299
10.1	Konsolenanschluss (RJ-45 zu DB9)	299
10.2	RJ-45-Kabel	300
10.3	Configuring in the Command Line Interface (CLI)	301
10.3.1	System Status	301
10.3.1.1	System Information	301
10.3.2	Basic Settings	302
10.3.2.1	System	302
10.3.2.1.1	Jumbo Frame	303
10.3.2.1.2	SNTP	304
10.3.2.1.3	Management Host	305
10.3.2.2	MAC Management	306
10.3.2.2.1	Blackhole MAC	306
10.3.2.3	Port Mirroring	307
10.3.2.4	Port Settings	308
10.3.3	Advanced Settings	309

10.3.3.1	Bandwidth Control	309
10.3.3.1.1	QoS	309
10.3.3.1.2	Rate Limitation	310
10.3.3.1.2.1	Storm Control	310
10.3.3.2	IGMP Snooping	311
10.3.3.2.1	IGMP Snooping Querier	313
10.3.3.2.2	IGMP Snooping Filtering	313
10.3.3.2.3	MVR	314
10.3.3.2.4	Multicast Address	315
10.3.3.3	VLAN	315
10.3.3.3.1	Port Isolation	315
10.3.3.3.2	VLAN Settings	316
10.3.3.3.3	GARP/GVRP	317
10.3.3.3.4	IP Subnet VLAN	318
10.3.3.3.5	MAC VLAN	318
10.3.3.3.6	Protocol VLAN	319
10.3.3.3.7	Q-in-Q	320
10.3.3.3.7.1	VLAN Stacking	320
10.3.3.4	DHCP Relay	321
10.3.3.5	DHCP Options	322
10.3.3.6	Dual Homing	322
10.3.3.7	ERPS	323
10.3.3.8	Link Aggregation	324
10.3.3.8.1	LACP	325
10.3.3.9	LLDP	326
10.3.3.10	Loop Detection	327
10.3.3.11	Modbus	328
10.3.3.12	Static Route	328
10.3.3.13	STP	330
10.3.3.13.1	MSTP	332
10.3.3.14	Xpress Ring	333
10.3.4	Security	334
10.3.4.1	IP Source Guard	334
10.3.4.1.1	DHCP Snooping	334
10.3.4.1.1.1	Server Screening	335
10.3.4.1.2	Binding Table	335
10.3.4.1.3	ARP Inspection	336
10.3.4.1.3.1	Filter Table	336
10.3.4.2	Access Control List	337
10.3.4.3	802.1X	339
10.3.4.4	Port Security	340
10.3.5	Monitor	341
10.3.5.1	Alarm	341
10.3.5.2	Monitor Information	341
10.3.5.3	Port Statistics	341
10.3.5.4	Port Utilization	341
10.3.5.5	RMON Statistics	341
10.3.5.6	SFP Information	341
10.3.5.7	Traffic Monitor	342
10.3.6	Management	343

10.3.6.1	SNMP	343
10.3.6.1.1	SNMP	343
10.3.6.1.2	SNMP Trap	344
10.3.6.1.2.1	Port Trap Settings	344
10.3.6.1.3	SNMPv3	345
10.3.6.2	Auto Provision	346
10.3.6.3	Mail Alarm	346
10.3.6.4	Maintenance	347
10.3.6.4.1	Reboot	348
10.3.6.5	System Log	348
10.3.6.6	USB Flash	349
10.3.6.7	User Account	350
10.4	MODBUS/TCP-Tabellen	351
10.4.1	Datenformat und Funktionscode	351
10.4.2	MODBUS-Register	352
Abbildungsverzeichnis		387
Tabellenverzeichnis		391

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“ (852-1305/000-001).

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.
- 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 802.1x
- IEEE 802.1ab
- IEEE802.1ad
- IEEE 1588v2
- ITU-T G8032v1/v2

Die Switches verfügen über eine Spannungsversorgung mit einem Versorgungsspannungsbereich 12 ... 48 V.

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

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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 852-1305/000-001 ist ein industrieller, konfigurierbarer ETHERNET-Switch mit 8 10/100/1000BASE-T-Ports.

Der Industrial-Managed-Switch lässt sich einfach konfigurieren und installieren und ist deshalb in zahlreichen Anwendungen einsetzbar.

Durch seine 4 SFP-Slots kann der Industrial-Managed-Switch auch in ausgedehnten Netzwerken eingebunden werden.

Die integrierte USB-Schnittstelle ermöglicht Firmware-Updates und die Konfiguration des Switches über ein USB-Speichermedium.

4.1 Ansicht

4.1.1 Frontansicht

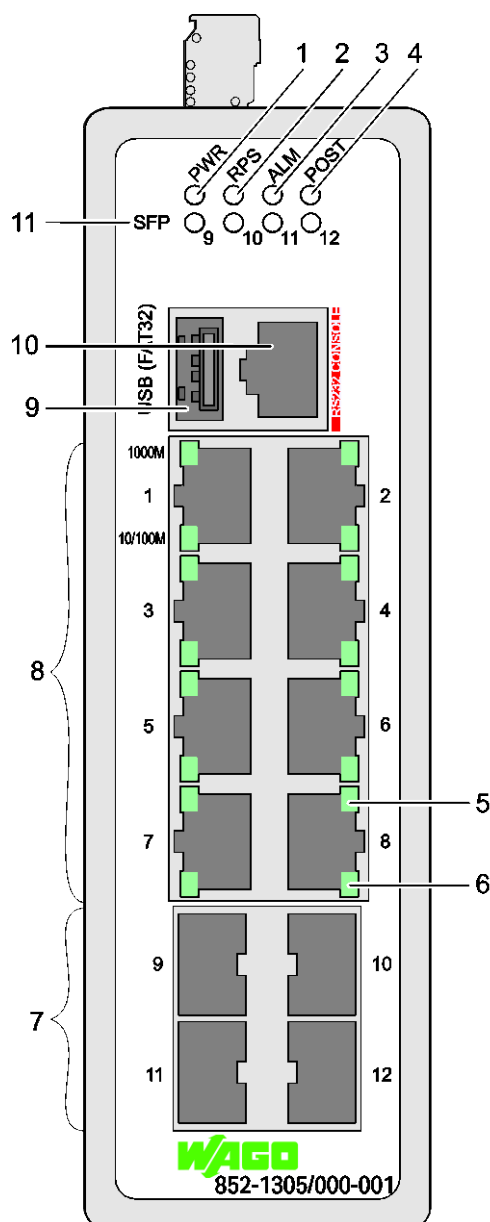


Abbildung 1: Frontansicht des Industrial-Managed-Switches

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“
4	POST	Status-LED POST	„Gerätebeschreibung“ > „Anzeigeelemente“

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

Pos.	Bezeichnung	Bedeutung	Details siehe Kapitel
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	-	USB-Anschluss	„Gerätebeschreibung“ > ... > „Netzwerkanschlüsse“
10	-	Anschluss 1 x RJ-45 (RS-232)	„Gerätebeschreibung“ > „Anschlüsse“
11	SFP	Status-LED SFP-Port LNK/ACT (4) (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“

4.1.2 Draufsicht

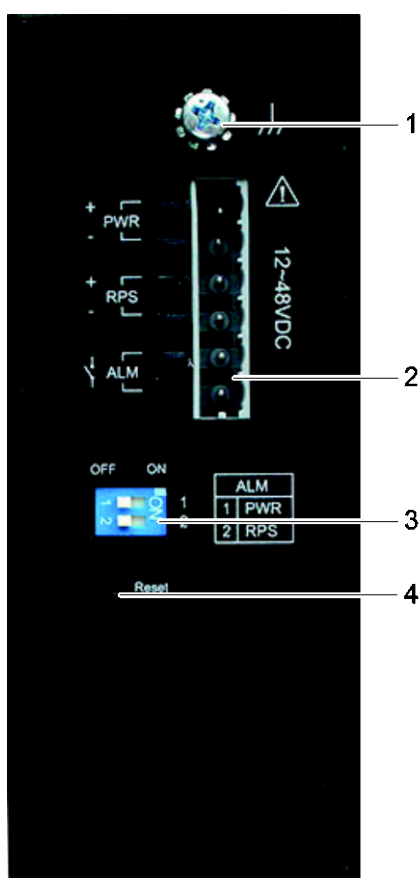


Abbildung 2: Draufsicht des Industrial-Managed-Switches

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	Reset	Taste Reset	„Gerätebeschreibung“ > „Bedienelemente“

4.2 Anschlüsse

4.2.1 Erdungsschraube

Der Switch muss geerdet werden.

Verbinden Sie dazu die Erdungsschraube mit dem Erdpotential.

Betreiben Sie den Switch nicht ohne einen entsprechend installierten Schutzleiter.

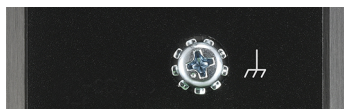


Abbildung 3: Erdungsschraube

4.2.2 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
	ALM	Kontakt für externen Alarm
	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.

4.2.3 Netzwerkanschlüsse

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

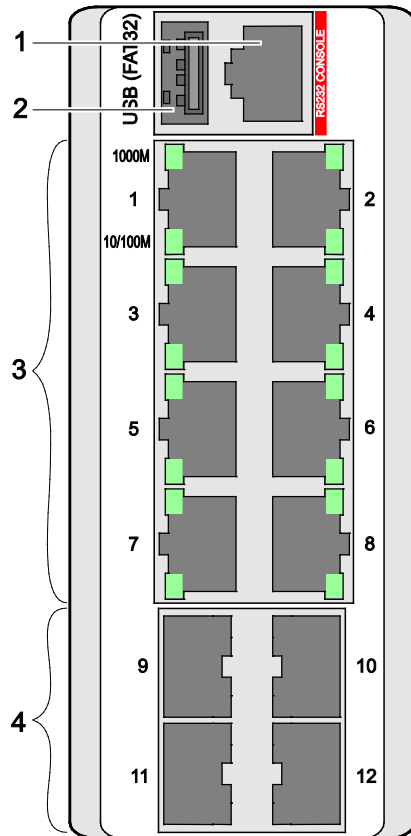


Abbildung 5: Netzwerkanschlüsse

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	-	USB-Anschluss	„Gerätebeschreibung“ > ... > „USB-Anschluss“
3	-	Anschluss 8 x RJ-45 (10/100/1000BASE-T)	„Gerätebeschreibung“ > ... „10/100/1000BASE-T-Anschlüsse“
4	-	Anschluss 4 x SFP (1000BASE-SX/-LX, Glasfaser)	„Gerätebeschreibung“ > ... „1000BASE-SX/-LX-Anschlüsse“

4.2.3.1 RJ-45-Anschluss

Der Anschluss an die ETHERNET-basierenden 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).

4.2.3.2 USB-Anschluss

Über die USB-Schnittstelle des Switch können folgende Funktionen ausgeführt werden:

- Upload der Firmware,
- Speichern der Konfigurationsdatei
- Speichern der Syslog-Datei
- Upload der Konfigurationsdatei

4.2.3.3 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

4.2.3.4 1000BASE-SX/-LX-Anschlüsse

Die 1000BASE-SX/-LX-Anschlüsse sind für den Anschluss der Gigabit-SFP-Module konzipiert, die Übertragungsgeschwindigkeiten von 100/1000 Mbit/s unterstützen.

4.3 Anzeigeelemente

Der Industrial-Managed-Switch ist mit Geräte-LEDs sowie mit Anschluss-LEDs ausgestattet. Anhand der Geräte-LEDs können Sie den Status des Switches schnell erkennen, die Anschluss-LEDs geben Auskunft über die Verbindungsaktionen.

4.3.1 Geräte-LEDs

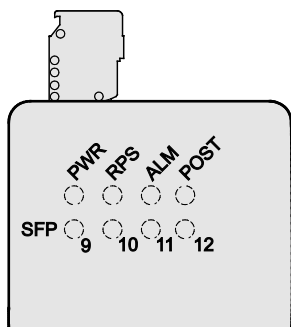


Abbildung 6: Geräte-LEDs

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	Alarm-LED	Rot	Ausfall einer Portverbindung, sonstiger Alarm.
		Aus	Es wird kein Alarm gemeldet.
POST	Power-On-Self-Test-LED	Blinkt	Die POST-Funktion wird ausgeführt.
		Grün	Der POST ist abgeschlossen.
		Aus	Keine Betriebsspannung oder Fehler bei der POST-Funktion erkannt.
SFP	9 ... 12 SFP-Port LNK/ACT-LED	Grün	Leuchtet, wenn der Anschluss verbunden ist.
		Blinkt	Datenverkehr wird über den Anschluss geleitet.
		Aus	Am Anschluss ist keine gültige Verbindung hergestellt.

4.3.2 Anschluss-LEDs

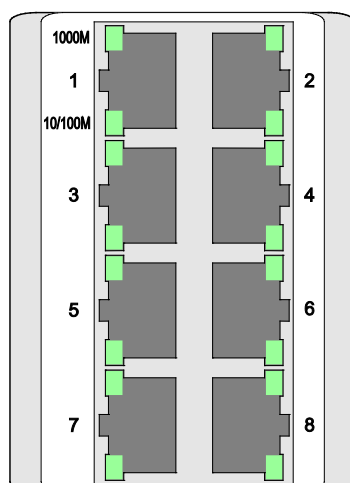


Abbildung 7: Anschluss-LEDs

Tabelle 8: Legende zur Abbildung „Anschluss-LEDs“

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.
10/100 M	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 zwei DIP-Schalter für die Alarmkonfigurationen. Bei aktivierter Alarmberichtsfunktion wird der Alarmkontakt bei Eintreten des Ereignisses geschaltet.

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

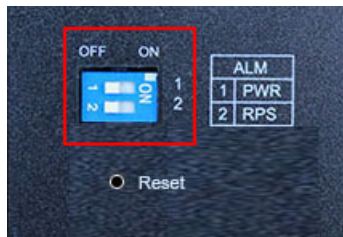


Abbildung 8: DIP-Schalter

Tabelle 9: Legende zur Abbildung „DIP-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.

Die Alarmfunktion kann 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 Alarmfunktion des Anschlusses 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 die entsprechende Alarmfunktion, die sie aktivieren wollen.
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

4.5.1 Hardware- und Softwareversion

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

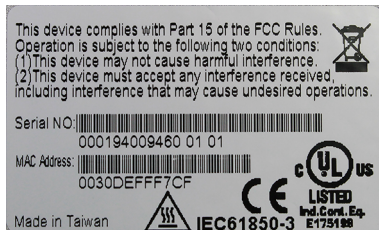


Abbildung 10: Aufkleber

Tabelle 11: Legende zur Abbildung „Aufkleber“

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	Tragschienenbefestigung	50 mm
Höhe	Tragschienenbefestigung	120 mm (ab Oberkante Tragschiene)
Tiefe	Tragschienenbefestigung	162 mm
Gewicht		955 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	10 KB
Wellenlänge Lichtleiter	abhängig vom SFP-Modul
Maximale Längen	10/100/ 1000BASE-T: 100 m; Glasfaser: von 2 km bis 80 km RS-232: 15 m

4.6.3 Versorgung

Tabelle 14: Technische Daten – Versorgung

Versorgungsspannung	DC 12 ... 48 V DC 24 V (DNV) DC 24/48 V (LR)
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 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 Prioritization IEEE 802.1x Port Authentication IEEE 802.1ab Link Layer Discovery Protocol (LLDP) IEEE 802.3ad Link Aggregation IEEE 1588v2 Precision Time Protocol (PTP) ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

4.6.5 Umgebungsbedingungen

Tabelle 16: Technische Daten – Umgebungsbedingungen

Umgebungstemperatur, Betrieb	-40 ... +70 °C (gültig für UL 61010) -40 ... +70 °C (gültig für CE) -40 ... +70 °C (gültig für IEC 61850-3) -25 ... +70 °C (DNV) +5 ... +70 °C (LR)
Umgebungstemperatur, Lagerung	-40 ... +85 °C
UL 61010 Nutzung Verschmutzungsgrad	Indoor 2
Relative Feuchte (ohne Betauung)	10 ... 95 %
Vibrationsfestigkeit	Gemäß IEC 60068-2-6
Schockfestigkeit	Gemäß IEC 60068-2-27
EMV-Störfestigkeit	EN 55024 EN 61000-6-2 IEC 61000-4-2 IEC 61000-4-3 IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-6 IEC 61000-4-8
EMV-Störaussendung	FCC Part 15 EN 55011: Klasse A EN 55032: Klasse A EN 61000-6-4:

4.7 Normen und Richtlinien

Energieversorgung

gemäß. IEC 61850-3:2013

4.8 Zulassungen

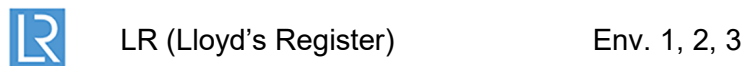
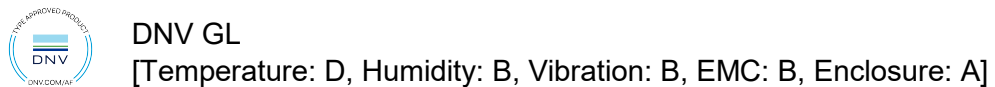
Folgende Zulassungen wurden für das WAGO-ETHERNET-Zubehör „Industrial-Managed-Switch“ (852-1305/000-001) erteilt:



Folgende Zulassungen wurden für das WAGO-ETHERNET-Zubehör „Industrial-Managed-Switch“ (852-1305/000-001) erteilt:



Folgende Schiffszulassungen wurden für das WAGO-ETHERNET-Zubehör „Industrial-Managed-Switch“ (852-1305/000-001) erteilt:



Hinweis



Gültig ab Hardwareversion 02!

Diese Schiffszulassungen sind nur gültig ab Hardwareversion 02. Switches mit der Hardwareversion 01 haben keine Schiffszulassungen!

Die Hardwareversionen 01 und 02 sind aus technischer Sicht identisch. Bei der Hardwareversion 02 wurden das Etikett und der Beipackzettel an die Anforderungen der Schiffszulassungen angepasst.

5 Montieren

5.1 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.

5.2 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.

5.3 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.

6 Geräte anschließen

6.1 Spannungsversorgung

Der Switch verwendet eine Gleichstromversorgung, die für 12 ... 48 V ausgelegt ist.

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

6.2 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 PWR/RPS:
 - a Versorgungsfehler (Stromleitung ist unterbrochen, Versorgungsstörung, etc.)
 - b Die Eingangsversorgungsspannung liegt außerhalb der Spezifikationen (12 ... 48 V)
- 2 Fehler im Jet-Ring oder ERPS-Ring

6.3 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“ > ... > „Konsolenport“ erläutert.

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

6.4 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“).

6.5 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“).

7 Funktionsbeschreibung

7.1 Grundeinstellungen

7.1.1 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.

7.1.2 SNTP

Das SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) ist ein Protokoll zur Synchronisation der Uhrzeit zwischen einem Time-Server (NTP-Server („**N**etwork **T**ime **P**rotocol“) und SNTP-Server) und der Systemzeit im ETHERNET-Gerät. Das Protokoll wird über einen UDP-Port abgearbeitet. Ausschließlich die Unicast-Adressierung wird unterstützt.

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.
-

7.1.3 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.

7.1.4 MAC-Management

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

Dynamische Adresse

Beim Empfang von Frames vergibt der Switch eine 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.

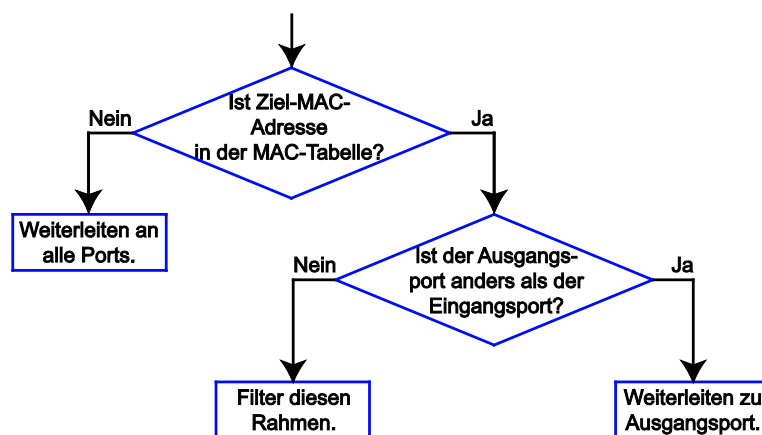


Abbildung 11: Ablaufdiagramm der MAC-Adresstabelle

7.1.4.1 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.

7.1.4.2 Blacklisting (MAC-Blacklist)

Dieser Typ von MAC-Adresseinträgen wird manuell eingetragen. Der Switch weist Pakete ab, die solche MAC-Adressen als Quelle oder Ziel haben, die in „Blackhole“-MAC-Adresseinträgen enthalten sind. „Blackhole“-Einträge werden konfiguriert, um Frames mit spezifischen MAC-Quell- oder Zieladressen herauszufiltern.

7.1.5 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.

7.1.6 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.

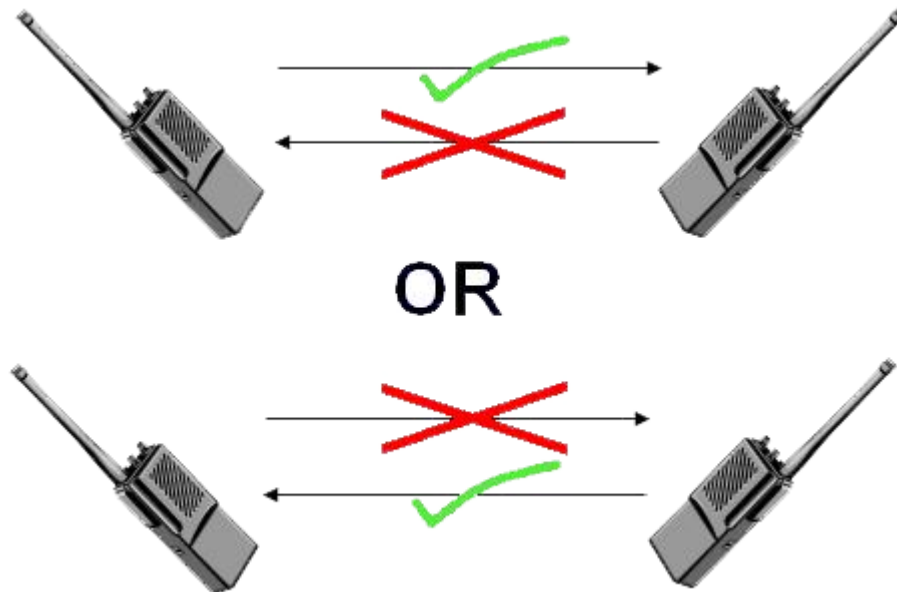


Abbildung 12: Halbduplexmodus

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 13: Vollduplexmodus

Loopback-Test

In einem „Loopback“-Test wird ein Signal von einem Kommunikationsgerät ausgesendet und anschließend wieder zu ihm zurückgeleitet („looped back“). Dabei erfolgen eine Überprüfung der ordnungsgemäßen Funktion des Gerätes und eine Suche nach fehlerhaften Knoten im Netzwerk.

Bei einer Art von „Loopback“-Test wird ein spezieller Stecker, ein so genannter „wrap plug“ (Rückkopplungsstecker) in den Port eines Kommunikationsgerätes gesteckt. Der Stecker bewirkt, dass übertragende Daten (vom Ausgang) wieder als Empfangsdaten (zum Eingang) zurückgeleitet werden und somit ein geschlossener Kommunikationskreislauf an einem einzelnen Computer simuliert werden kann.

Auto MDI/MDIX

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

Auto-MDIX („**A**utomatic **M**edium-**D**ependent 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-Ports (z. B. der Netzwerk-Port eines PC und der eines Routers, Hubs oder Switches, mit dem dieser z. B. verbunden ist) selbständig die maximal mögliche Übertragungsrate und das Duplexverfahren erkennen und entsprechend automatisch einstellen.

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 Übertragungsrate durch Signalerkennung am Kabel und verwendet den Halbduplexmodus.

Ist die Autonegotiation beim 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.

Flusskontrolle (Flow Control)

Die Flusskontrolle (Flow Control) 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 Flusskontrolle im Vollduplexmodus und die „Backpressure Flow Control“ (Gegendruck-Datenflusskontrolle) im Halbduplexmodus.

Bei der Flusskontrolle 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 „Backpressure 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.

7.2 Erweiterte Einstellungen

7.2.1 Bandbreiten-Regelung

7.2.1.1 QoS („Quality of Service“)

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, ein entsprechend seiner relativen Wichtigkeit eine Priorität zugewiesen und ein Engpassmanagement und Techniken zur Engpassvermeidung angewendet werden, um ihm 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 beim Switch 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 seinen 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.

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	CFI

- TPID („**T**ag **P**rotocol **I**dentifier“, 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 („**T**ag **C**ontrol **I**nformation“)
 - PCP („**P**riority **C**ode **P**oint“, Prioritätsinformationsfeld)
Ein 3-Bit-Feld, das sich auf die IEEE 802.1p-Priorität bezieht. 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 („**C**anonical **F**ormat **I**ndicator“, Kanonischer Formatindikator)
Ein 1-Bit-Feld. 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 („**V**LAN **I**dentifier“, VLAN-Kennung)
Ein 12-Bit-Feld, in dem das VLAN spezifiziert wird, 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 17: 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.

7.2.1.2 Bandbreitenbegrenzung

7.2.1.2.1 Sturmbegrenzung (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).

7.2.1.2.2 Bandbreitenbegrenzung (Rate Limitation)

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

7.2.2 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 physischen 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“ beim Switch aktivieren bzw. deaktivieren. Dies gilt auch für spezifische VLANs. Wird „IGMP Snooping“ beim 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“ beim 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.

7.2.2.1 Multicast-VLAN-Registrierung (MVR)

MVR („**M**ulticast **V**LAN **R**egistration“, Multicast-VLAN-Anmeldung), durch die ein Medienserver einen Multicast-Stream in ein einzelnes Multicast-VLAN übertragen kann und wobei sich die den VLAN-Stream empfangenden Clients in unterschiedlichen VLANs befinden können. Clients in unterschiedlichen VLANs können der Multicast-Gruppe beitreten oder sie verlassen, indem sie einfach eine „IGMP Join Message“ oder „IGMP Leave Message“ an einen Empfänger-Port senden. Der zu einer Multicast-Gruppen gehörende Empfänger-Port kann den Multicast-Stream vom Medienserver empfangen. Ohne die Unterstützung durch MVR müssten sich der Multicast-Stream vom Medienserver und die Teilnehmer im selben VLAN befinden.

- Quell-Ports: Die Quell-Ports des Streams.
- Empfänger-Ports: Die Ports der Clients.
- Ports mit Tag: Konfigurieren Sie Ports mit Tags, um sie als Quell-Ports oder Empfänger-Ports zuzuordnen.

MVR-Modus

- **Dynamischer Modus**
Wenn in den MVR-Einstellungen der dynamische Modus aktiviert ist, wird die „IGMP Report Message“ vom Empfänger-Port zu den Quell-Ports des Multicast-Routers übertragen. Der Multicast-Router kann dynamisch erkennen, welche Multicast-Gruppen an welcher Schnittstelle vorhanden sind.
- **Kompatibilitätsmodus**
Wenn in den MVR-Einstellungen der Kompatibilitätsmodus aktiviert ist, wird die vom Empfänger-Port gesendete „IGMP Report Message“ nicht zu den Quell-Ports des Multicast-Routers übertragen. Der Multicast-Router muss statisch konfiguriert werden.
- **Betriebsmodus**
Join Operation (Beitrittsmodus)
Ein Teilnehmer sendet eine „IGMP Report Message“ an den Switch, um einem entsprechendem Multicast beizutreten. Der nächste Schritt hängt davon ab, ob die „IGMP Report Message“ zu der im Switch konfigurierten Multicast-MAC-Adresse passt oder nicht. Wenn sie passt, modifiziert die Switch-CPU die Hardware-Adresstabelle, um diesen Empfänger-Port und das VLAN als Weiterleitungsziel für das MVLAN aufzunehmen.
- **Leave Operation** (Austrittsmodus)
Ein Teilnehmer sendet eine „IGMP Leave Message“ an den Switch, um den Multicast zu verlassen. Die Switch-CPU sendet eine gruppenspezifische „IGMP Query“ an den Empfänger-Port des VLANs. Wenn es in dem VLAN einen anderen Teilnehmer gibt, muss dieser innerhalb der maximalen Antwortzeit antworten. Gibt es keinen Teilnehmer, wird der Switch diesen Empfänger-Port löschen.

- Immediate Leave Operation (Sofortaustrittsmodus)**
 Ein Teilnehmer sendet eine „IGMP Leave Message“ an den Switch, um den Multicast zu verlassen. Die Teilnehmer müssen nicht warten, bis die Switch-CPU eine gruppenspezifische „IGMP Query“ an den Empfänger-Port des VLANs sendet. Der Switch wird diesen Empfänger-Port sofort löschen.

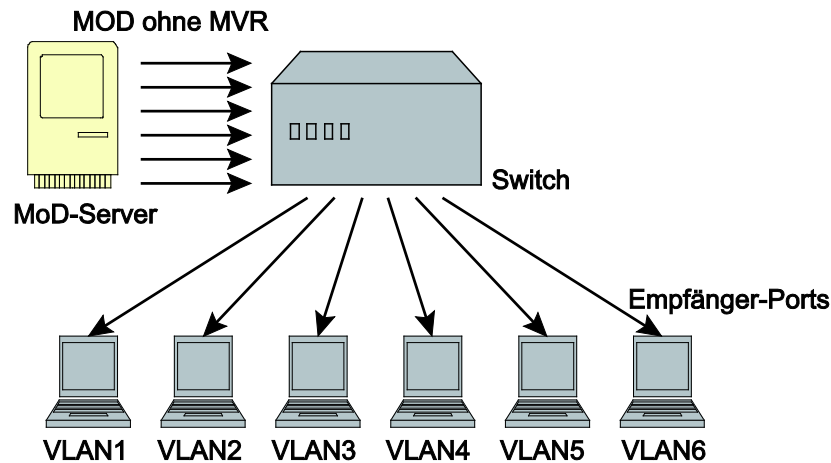


Abbildung 14: MOD ohne MVR

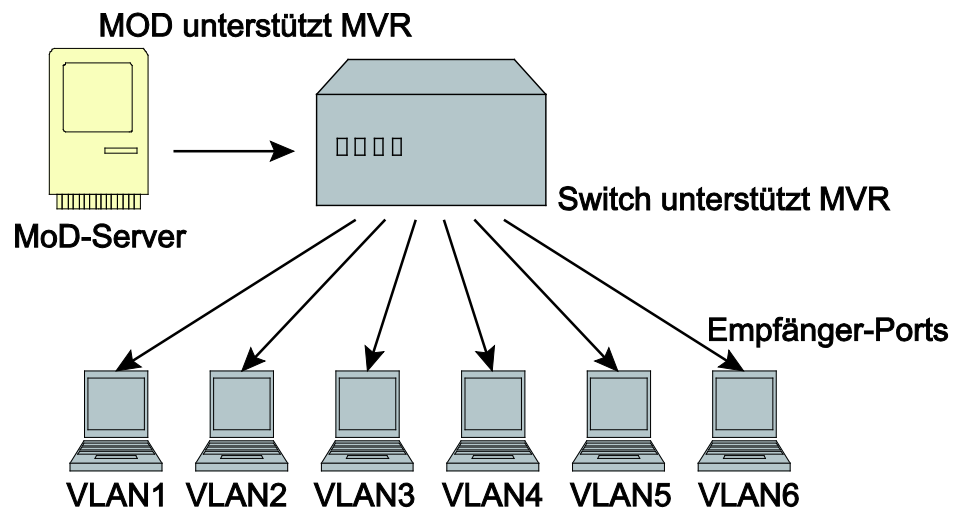


Abbildung 15: MOD unterstützt MVR

Default-Konfiguration für eine neue MVR:

MVR-VLAN-Informationen

VLAN-ID:	2
Name:	MVR2
Active:	Aktiviert
Modus:	Dynamisch
Quell-Port(s):	Keine(r)
Empfänger-Port(s):	Keine(r)
Port(s) mit Tag:	Keine(r)

Der Switch ermöglicht dem Benutzer die Erstellung von bis zu 250 Gruppen.
Der Switch ermöglicht dem Benutzer die Erstellung von bis zu 16 MVRs.

Hinweis**Hinweise**

- IGMP Snooping“ und MVR können unabhängig voneinander aktiviert werden.
- „IGMP Snooping“ und MVR nutzen dieselben IGMP-Timer.
- MVR kann IGMPv3-Meldungen erkennen.
- Gruppeneinträge wie eine IGMPv3-Meldung werden vom Switch ebenso wie die folgenden Gruppeneintragstypen nicht als Mitgliedschaftsmeldungen behandelt. Diese Gruppeneintragstypen sind „MODE_IS_INCLUDE“, „CHANGE_TO_INCLUDE_MODE“, „ALLOW_NEW_SOURCES“ und „BLOCK_OLD_SOURCES“.
- Verwenden Sie die Gruppenadresse X.0.0.1 nicht für Ihren Multicast-Stream. Das System erkennt und protokolliert die Adresse 224.0.0.1 für den dynamischen „Querier Port“. Die Gruppenadresse X.0.0.1 könnte einen Konflikt mit 224.0.0.1 verursachen.
- Die unteren 23 Bit der 28-Bit-Multicast-IP-Adresse werden in die 23 Bit des verfügbaren ETHERNET-Adressraumes zugeordnet. Bei der Konfiguration der Gruppenadresse vergleicht der Switch nur die unteren 23 Bit.
- Der CLI-Befehl „group 1 start-address 224.1.1.1 6“ erstellt 6 Gruppen. Das bedeutet, dass eine IP einer Gruppe entspricht.
- Der MVR-Name sollte aus einer Kombination aus Zahlen oder Buchstaben bestehen.
- Der Gruppenname sollte aus einer Kombination aus Zahlen oder Buchstaben bestehen.

7.2.2.2 Static Multicast (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, wodurch die Netzwerksoftware in den Host die jeweils nicht benötigten Pakete verwerfen muss.

Tabelle 18: 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.

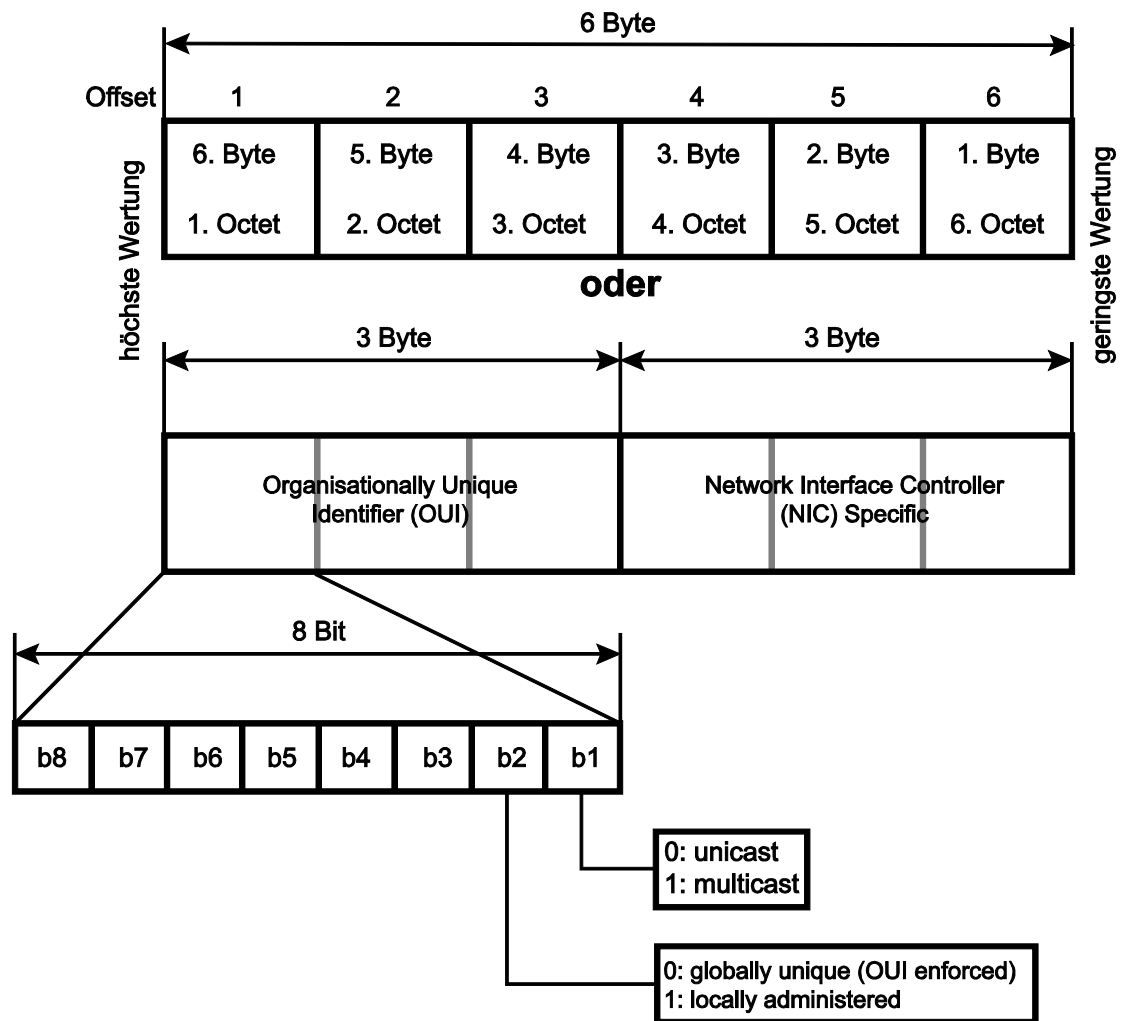


Abbildung 16: Multicast-Adresse

Tabelle 19: 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 „AllSPFRouters“-Adresse. Sie wird zum Senden von „Hello-Paketen“ an alle OSPF-Router in einem Netzwerksegment verwendet.
224.0.0.6	Die „OSPF AllDRouters“-Adresse. Sie wird zum Senden von OSPF-Routing-Informationen an „OSPF Designated Router“ in einem Netzwerksegment verwendet.
224.0.0.9	Das RIP („Routing Information Protocol“) Version 2 der Gruppenadresse. Es wird zum Senden von Routing-Informationen an alle RIPv2-kompatiblen Router in einem Netzwerksegment verwendet.

Tabelle 19: IP-Multicast-Adressen

IP-Multicast-Adresse	Beschreibung
224.0.0.10	Die EIGRP-Gruppenadresse. Sie 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

7.2.3 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 ausgegeben 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 application-specific integrated circuit (ASIC, einer anwendungsspezifischen integrierten Schaltung) ausgeführt wird, bringt dies große Leistungsvorteile. Ein ASIC ermöglicht eine „Port-to-VLAN“-Zuordnung auf Hardwareebene.

7.2.3.1 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 zwei 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 diesem Port verwaltet werden.

7.2.3.2 GARP/GVRP

GARP („**G**eneric **A**tttribute **R**egistration **P**rotocol“) und GVRP („**G**ARP **V**LAN **R**egistration **P**rotocol oder **G**eneric **V**LAN **R**egistration **P**rotocol“) sind Branchenstandardprotokolle, die in IEEE 802.1p beschrieben sind. GVRP ist eine GARP-Applikation, die 802.1Q-konformes „VLAN Pruning“ und dynamische VLAN-Erstellung an „802.1Q Trunk Ports“ ermöglicht.

Mit GVRP kann ein Switch VLAN-Konfigurationsinformationen mit anderen GVRP-Switches austauschen, nicht benötigte Broadcast-Daten und unbekannte Unicast-Daten löschen („Pruning“) sowie VLANs in Switches, die durch „802.1Q Trunk Ports“ miteinander verbunden sind, dynamisch erstellen.

GVRP nutzt GID („**G**roup **I**dentification“) und GIP, die gemeinsame Zustandsautomatenbeschreibungen („State Machine Descriptions“) und gemeinsamen Informationsübertragungsmechanismen, die für den Einsatz in GARP-basierten Anwendungen definiert sind. GVRP kann nur über „802.1Q Trunk Links“ betrieben werden. GVRP bereinigt „Trunk Links“, sodass nur aktive VLANs über Trunk-Verbindungen übertragen werden. GVRP wartet auf Verbindungsanfragen von den Switches, bevor es dem Trunk ein VLAN hinzufügt. GVRP-Aktualisierungen und Haltezeitgeber können verändert werden. GVRP-Ports können in verschiedenen Modi betrieben werden, um zu steuern, wie sie VLANs bereinigen. Die Konfiguration des GVRP ermöglicht ein dynamisches Hinzufügen und Verwalten von VLANs in einer VLAN-Datenbank zur Unterstützung von „Trunking“-Prozessen.

GVRP erlaubt sozusagen die Propagation von VLAN-Informationen von Gerät zu Gerät. Mit GVRP kann ein einzelner Switch für alle für das Netzwerk benötigten VLANs manuell konfiguriert werden, woraufhin alle anderen Switches im Netzwerk diese VLANs dynamisch erkennen können. Endknoten können in jeden Switch gesteckt werden und sich mit dem gewünschten VLAN verbinden. Für Endknoten, die GVRP nutzen möchten, werden GVRP-fähige Netzwerkkarten (NICs) benötigt. Die GVRP-fähige Netzwerkkarte wird mit dem bzw. den gewünschten VLANs konfiguriert und dann mit einem GVRP-aktivierten Switch verbunden. Die Netzwerkkarte kommuniziert mit dem Switch, sobald die Konnektivität zwischen der Netzwerkkarte und dem Switch gegeben ist.

Registration Mode (Anmeldungsmodus):

- **Normal**
Der Anmeldungsmodus „normal“ erlaubt die dynamische Erstellung (sofern dynamische VLAN-Erstellung aktiviert ist), Anmeldung und Abmeldung von VLANs am Trunk-Port. Der Modus „Normal“ ist die Default-Einstellung.
- **Forbidden**
Der Anmeldungsmodus „forbidden“ (verboten) meldet alle VLANs (außer VLAN 1) ab und verhindert jede weitere Erstellung oder Anmeldung von VLANs am Trunk-Port.

- **Fixed**
Der Anmeldungsmodus „fixed“ erlaubt die manuelle Erstellung und Anmeldung von VLANs, verhindert VLAN-Abmeldungen und meldet alle bekannten VLANs an anderen Ports am Trunk-Port an. (Gleiches gilt für statisches VLAN)

GVRP-Timer:

- **Join Timer**
Der „Join Timer“ spezifiziert die maximale Zeit in Millisekunden, die die Schnittstelle wartet, bevor sie mit dem Senden von VLAN-Meldungen beginnt.
- **Leave Timer**
Der „Leave Timer“ spezifiziert die maximale Zeit in Millisekunden, die die Schnittstelle nach dem Empfang einer „Leave Message“ wartet, bevor die Schnittstelle das in der Nachricht spezifizierte VLAN verlässt.
- **Leaveall Timer**
Der „Leaveall Timer“ spezifiziert das Zeitintervall in Millisekunden, nach dem „Leaveall Messages“ an Schnittstellen gesendet werden. „Leaveall Messages“ können dabei helfen, Informationen über die derzeitigen GVRP-VLAN-Mitgliedschaften im Netzwerk zu aktualisieren.

7.2.3.3 Q-in-Q

„Q-in-Q Tunneling“ wird auch als „VLAN Stacking“ bezeichnet. Dabei wird die 802.1Q-Doppel-Tag-Technologie genutzt. Q-in-Q wird von ISPs (Internetdiensteanbietern) benötigt, die TLS („Transparent LAN Services“) verwenden, und die ihre eigenen VLANs unabhängig von den Kunden-VLANs betreiben. Normalerweise verbindet jedes Diensteanbieter-VLAN eine Gruppe von Standorten eines Kunden miteinander. Ein Diensteanbieter-VLAN kann jedoch auch von mehreren Kunden gemeinsam genutzt werden, wenn sie dieselben Endpunkte und QoS-Anforderungen des VLANs aufweisen. Das sogenannte „Double Tagging“ stellt eine vergleichsweise einfachere Methode zur Implementierung eines transparenten LANs dar. Dies wird durch die Kapselung von „ETHERNET Frames“ erreicht. Dabei wird ein zweiter bzw. äußerer VLAN-Tag in die „ETHERNET Frames“ eingebettet, die über die eingangsseitige PE („Provider Edge“, Netzwerkendpunkt auf Anbieterseite) gesendet werden. Dieser VLAN-Tag entspricht dem VLAN des Diensteanbieters. Wenn der Frame die Ziel-PE erreicht, wird das Diensteanbieter-VLAN geöffnet. Die Zieladresse des gekapselten Frames und die VLAN-ID werden für weitere L2-Entscheidungen verwendet, ähnlich wie ein „ETHERNET Frame“, der aus einem physischen ETHERNET-Port ankommt. Der Diensteanbieter-VLAN-Tag bestimmt die Mitgliedschaft im VPLS („Virtual Private LAN Service“). Das Double-Tagging aggregiert mehrere VLANs innerhalb eines anderen VLANs und ermöglicht eine private, dedizierte ETHERNET-Verbindung zwischen Kunden, die ihr Subnetz über mehrere Netzwerke transparent erreichen möchten. Dadurch können Diensteanbieter ihre eigenen VLANs erstellen, ohne durch „Double Tagging“ mit Kunden-VLANs in Kontakt zu kommen. Dies ermöglicht die Verbindung von Kunden mit ISPs und ASPs („Application Service Providers“, Anwendungsdiensteanbietern).

Die mit den Diensteanbieter-VLANs verbundenen Ports werden als „Tunnel Ports“ und die mit Kunden-VLANs verbundenen Ports werden als „Access Ports“ (Abonnementen-/Kunden-Ports) bezeichnet. Wenn ein Port als „Tunnel Port“ konfiguriert ist, werden alle ausgehenden Pakete an diesem Port mit einem SPVLAN-Tag (SPVID und 1p-Priorität) übertragen. Das eingehende Paket kann zwei Tags (SPVLAN + CVLAN), einen Tag (SPVLAN oder CVLAN) oder gar keinen Tag haben. In jedem Fall wird ein Paket mit einem SPVLAN-Tag gesendet. Wenn ein Port als „Access Port“ konfiguriert ist, können eingehende Pakete nur einen CVLAN-Tag (CVID und 1p-Priorität) oder gar keinen Tag haben. Somit haben alle von „Access Ports“ gesendeten Pakete entweder keinen Tag oder einen Einzel-Tag (CVLAN). Wenn ein Port als normaler Port konfiguriert ist, wird er „Double Tagging Frames“ ignorieren.

Double Tagging Format

Ein VLAN-Tag (Dienstanbieter-„VLAN Stacking“ oder Kunden-IEEE 802.1Q) besteht aus folgenden drei Feldern:

TPID	Priorität	VID

TPID

TPID („Tag Protocol Identifier“) ist ein Standard-ETHERNET-Code, der den Frame identifiziert und anzeigt, ob dieser eine IEEE 802.1Q-Tag-Information enthält. Der Wert in diesem Feld ist 0x8100 wie in IEEE 802.1Q beschrieben. Andere Anbieter können auch einen anderen Wert, wie etwa 0x9100, verwenden.

„Tunnel TPID“ ist der „VLAN Stacking“-Tag-Typ, den der Switch ausgehenden Frames hinzufügt, die durch einen „Tunnel Port“ der PE-Geräte des Dienstanbieters gesendet werden.

Priorität

Die Priorität bezieht sich auf den Standard IEEE 802.1p, die es dem Dienstanbieter erlaubt, Datenpakete auf Grundlage ihrer Serviceklasse („Class of Service“, CoS) zu priorisieren, für die der Kunde bezahlt hat. Dabei stellt die „0“ die niedrigste und die „7“ die höchste Prioritätsebene dar.

VID

VID („VLAN-ID“). SP-VID ist die VID für den zweiten bzw. äußeren VLAN-Tag (des Dienstanbieters). CVID ist die VID für den ersten bzw. inneren VLAN-Tag (des Kunden).

Im Folgenden werden die Frame-Formate für einen „ETHERNET Frame“ ohne Tag, einen 802.1Q-Frame mit Einzel-Tag (Kunde) und einen 802.1Q-Frame mit Doppel-Tag (Dienstanbieter) dargestellt.

Frame ohne Tag	DA		Len oder Etype	Daten	FCS						
Frame mit Einzel-Tag	DA	SA	TPID	P	VID	Len oder Etype	Daten	FCS			
Frame mit Doppel-Tag	DA	SA	Tunnel-TPID	P	VID	TPID	P	VID	Len oder Etype	Daten	FCS

DA Destination Address (Zieladresse)

SA Source Address (Quelladresse)

Tunnel TPID An einem „Tunnel Port“ hinzugefügter „Tag Protocol Identifier“

VID VLAN-ID

Len oder Etype Länge oder ETHERNET-Frame-Typ

Daten Frame-Daten

FCS Frame Check Sequence (Prüfsummenfeld)

Rollen von Ports beim VLAN Stacking

Beim „VLAN Stacking“ kann jeder Port eine von drei „Rollen“ zugewiesen bekommen: Normal, „Access Port“ oder „Tunnel Port“.

- Wählen Sie Normal für „normale“ (kein „VLAN Stacking“) IEEE 802.1Q-Frame-Vermittlungen.
- Wählen Sie „Access Port“ für Eingangs-Ports an PE-Geräten des Diensteanbieters. Der eingehende Frame wird als Frame ohne Tag behandelt, sodass ein zweiter VLAN-Tag (äußerer VLAN-Tag) hinzugefügt werden kann.
- Wählen Sie „Tunnel Port“ für Ausgangs-Ports im PE-Bereich des Anbieternetzes. Alle zu Kunden gehörenden VLANs können in einem einzelnen Dienstanbieter-VLAN aggregiert werden (unter Verwendung eines äußeren VLAN-Tags, der durch die SP-VID definiert wird).

Hinweis



Konfiguration Q-in-Q

Damit die Frames mit Doppel-Tag korrekt vermittelt werden können, müssen Benutzer im Q-in-Q-Switch ein Dienstanbieter-VLAN (SPVLAN) konfigurieren. Dann können diese Tags entsprechend der SP-VID korrekt vermittelt werden. Im SPVLAN sollten alle zugehörigen „Tunnel“- und „Access Ports“ aufgeführt sein. Außerdem müssen die „Tunnel-Ports“ als Ports mit Tag und die „Access Ports“ als Ports ohne Tag konfiguriert werden.

7.2.3.3.1 Port-basiertes Q-in-Q

Durch Q-in-Q-Kapselung können 802.1Q-Pakete mit Einzel-Tag in Q-in-Q-Pakete mit Doppel-Tag konvertiert werden. Die Q-in-Q-Kapselung kann auf Grundlage von Ports oder von Datenpaketen erfolgen. Beim port-basierten Q-in-Q werden alle eingehenden Pakete an einem Port mit dem gleichen äußeren SPVID-Tag gekapselt. Dieser Modus ist weniger flexibel.

In der folgenden Abbildung sind X und Y Kunden des Dienstbiernetzwerks (SPN) mit VPN-Tunnel zwischen ihren entsprechenden Haupt- und Nebengeschäftsstellen. Beide haben für ihre VLAN-Gruppe einen identischen VLAN-Tag. Der Dienstanbieter kann diese beiden VLANs innerhalb seines Netzwerks unterscheiden, indem er an seinem PE-Gerät A dem Kunden X den Tag 100 und dem Kunden Y den Tag 200 hinzufügt und diese Tags anschließend am PE-Gerät B wieder entfernt, wenn die Daten-Frames das Netzwerk wieder verlassen.

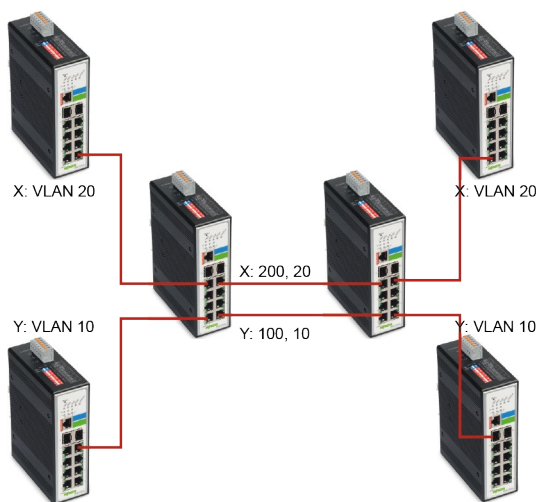


Abbildung 17: Port-basiertes Q in Q

Dieses Beispiel zeigt, wie Switch A mit Port 1 am Switch konfiguriert wird, um eingehende Frames mit der Dienstanbieter-VID von 200 (mit dem Netzwerk von Kunde X verbundene Ports) zu kennzeichnen und wie Port 7 konfiguriert wird, um eingehende Frames mit der Dienstanbieter-VID von 100 (mit dem Netzwerk von Kunde Y verbundene Ports) zu kennzeichnen. Außerdem wird gezeigt, wie die Prioritäten für Port 1 bis 3 und Port 7 bis 4 zuzuordnen sind.

7.2.3.3.2 Selektives Q-in-Q

Das auf Datenverkehr basierende Q-in-Q wird auch als selektives Q-in-Q bezeichnet. Es ermöglicht dem Switch den an einem Port eingehenden Frames entsprechend ihrer inneren VLAN-Tags unterschiedliche äußere VLAN-Tags hinzuzufügen. Im selektiven Q-in-Q-Modus nimmt der Switch eine Klassifizierung des an einem Port eingehenden Datenverkehrs auf Grundlage der VLAN-ID vor. Wenn ein Benutzer für unterschiedliche Services unterschiedliche VLAN-IDs verwendet, kann der Datenverkehr anhand der VLAN-IDs klassifiziert werden. Beispiel: Die VLAN-ID 100 wird für das Surfen im Internet an einem PC vergeben, die VLAN-ID 200 für IPTV (IP-Fernsehen) und die VLAN-ID 300 für VIP-Kunden. Nach Empfang der Benutzerdaten kennzeichnet der Switch den Datenverkehr durch Internet-Surfen am PC mit 500 als äußeren SPVID-Tag, die IPTV-Daten mit 600 und die Daten von VIP-Kunden mit 700.

Das folgende Beispiel zeigt die Konfiguration von Port 3 am Switch, um eingehende Frames mit den Tags für unterschiedliche VIDs und Prioritäten des Dienstansbieters zu versehen.

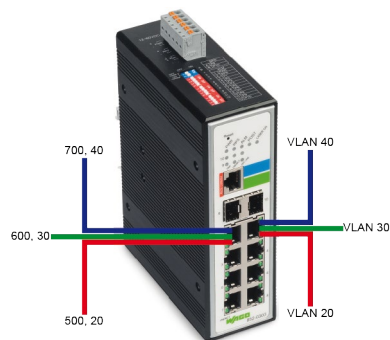


Abbildung 18: Konfigurationsbeispiel

7.2.4 DHCP-Relay

Da die „DHCPDISCOVER“-Nachricht („Dynamic Host Configuration Protocol“) eine Broadcast-Nachricht ist und Broadcasts nur andere Segmente durchlaufen, wenn sie explizit geroutet werden, müssen Sie in der Router-Schnittstelle unter Umständen einen „DHCP Relay Agent“ konfigurieren, damit alle „DHCPDISCOVER“-Nachrichten zu Ihrem DHCP-Server weitergeleitet werden können. Alternativ dazu können Sie den Router auch so konfigurieren, dass er DHCP-Nachrichten und BOOTP-Nachrichten weiterleitet. In einem Routing-Netzwerk bräuchten Sie „DHCP Relay Agents“, wenn Sie vorhaben, nur einen DHCP-Server zu implementieren.

Das „DHCP Relay“, das entweder ein Host oder ein IP-Router ist, wartet auf DHCP-Client-Nachrichten, die über ein Subnetz eintreffen und leitet diese dann direkt zu einem konfigurierten DHCP-Server. Der DHCP-Server sendet DHCP-Antwortnachrichten direkt zurück an den „DHCP Relay Agent“, der diese anschließend weiterleitet zum DHCP-Client. Der DHCP-Administrator nutzt „DHCP Relay Agents“ zur Zusammenfassung von DHCP-Servern, damit nicht in jedem Subnetz ein eigener DHCP-Server vorhanden sein muss.

In kleineren Netzwerken verwendet DHCP zumeist Broadcasts, aber unter bestimmten Umständen werden auch Unicast-Adressen verwendet. Dies kann der Fall sein, wenn Netzwerke einen einzelnen DHCP-Server haben, der IP-Adressen für mehrere Subnetze bereitstellt. Ein Router für ein solches Subnetz empfängt die DHCP-Broadcasts und konvertiert sie in Unicasts (mit einer MAC/IP-Zieladresse des konfigurierten DHCP-Servers, MAC/IP-Quelladresse des Routers selbst). Das GIADDR-Feld auf der DHCP-Hauptseite beinhaltet die IP-Adresse der Schnittstelle im Router, über die er die DHCP-Anfrage empfangen hat. Der DHCP-Server verwendet das GIADDR-Feld zur Identifizierung des Subnetzes für das Gerät und wählt eine IP-Adresse aus dem richtigen Pool aus. Daraufhin sendet der DHCP-Server die „DHCP OFFER“ über Unicast zurück zum Router, der diese dann in einen Broadcast zurückkonvertiert und in das korrekte Subnetz sendet, in dem sich das Gerät befindet, das eine Adresse angefordert hat.

Konfigurationen

Ein Benutzer kann „DHCP Relay“ beim Switch aktivieren bzw. deaktivieren. Dies kann auch für ein spezifisches VLAN erfolgen. Wenn „DHCP Relay“ beim Switch deaktiviert ist, ist es in allen VLANs deaktiviert, auch wenn es für einzelne VLANs aktiviert wurde.

Anwendungen

- **Anwendung 1 (über einen Router)**
DHCP-Client-1 und DHCP-Client-2 befinden sich in unterschiedlichen IP-Segmenten. Die IP-Adresse erhalten sie jedoch vom selben DHCP-Server.

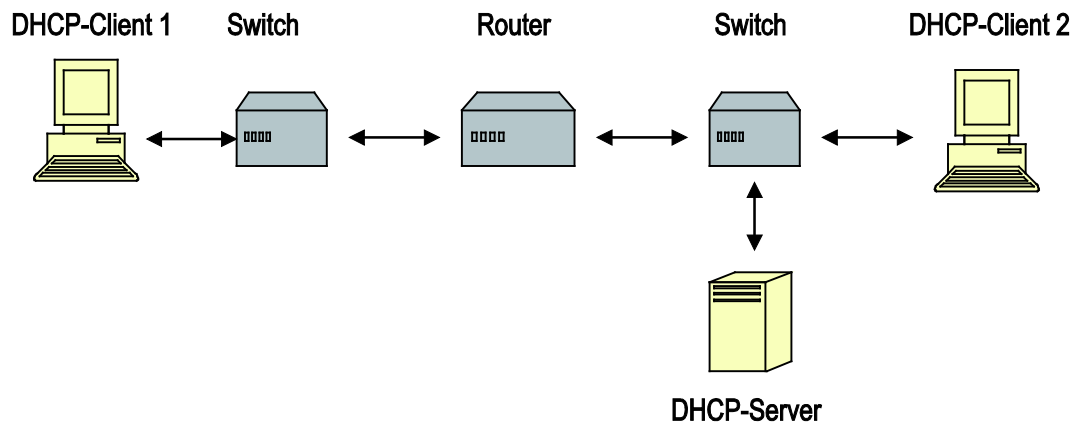


Abbildung 19: Anwendung 1 (über einen Router)

- **Anwendung 2 (Lokal in verschiedenen VLANs)**
DHCP-Client-1 und DHCP-Client-2 befinden sich in unterschiedlichen VLANs. Die IP-Adresse erhalten sie jedoch vom selben DHCP-Server.

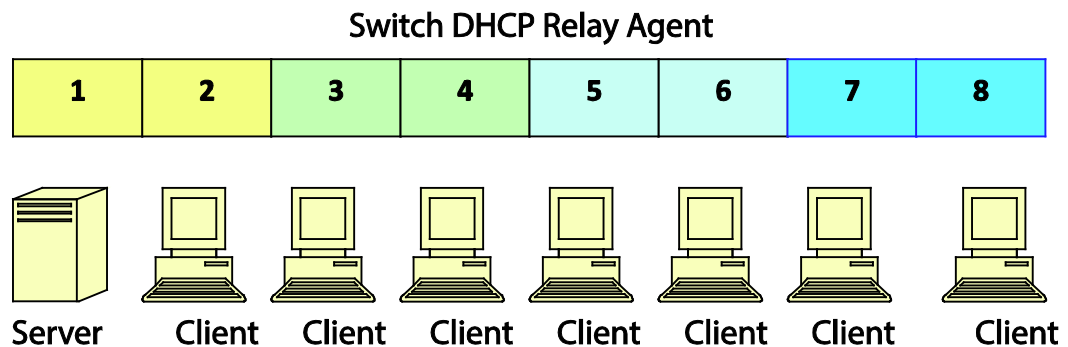


Abbildung 20: Anwendung 2 (Lokal in verschiedenen VLANs)

VLAN 1: Port 1, 2 (Management-VLAN)
 VLAN 2: Port 3, 4
 VLAN 3: Port 5, 6
 VLAN 4: Port 7, 8

DHCP-Server -> Port 1.
 DHCP-Client -> Port 2, 3, 4, 5, 6, 7, 8.

Ergebnis: Mit Port 2, 3, 4, 5, 6, 7 und 8 verbundene Hosts können eine IP vom DHCP-Server erhalten.

Hinweis



Verbindung des DHCP-Servers

Der DHCP-Server muss mit den Teilnehmer-Ports des Management-VLANs verbunden sein.
 Das „DHCP Relay“ im Management-VLAN muss aktiviert sein.

7.2.5 DHCP Options

DHCP („**D**ynamic **H**ost **C**onfiguration **P**rotocol“) ist eine Weiterentwicklung von BootP und ist zu diesem rückwärtskompatibel.

„DHCP Option 82“ ist die „**DHCP** Relay Agent Information **Option**“.

Die Option 82 wurde entwickelt, um es dem „DHCP Relay Agent“ zu ermöglichen, anchlusspezifische Informationen in eine Anfrage einzufügen, die zu einem DHCP-Server weitergeleitet wird. Die Option nutzt im Besonderen zwei Unteroptionen: Die „Circuit-ID“ (Anschlusskennung) und die „Remote-ID“ (Endgeräteerkennung).

Die „DHCP Option 82“ arbeitet auf Grundlage von „DHCP Snooping“ oder/und „DHCP Relay“.

Der Switch überwacht DHCP-Pakete und hängt unter „DHCPDISCOVER“- und „DHCPREQUEST“-Pakete einige Informationen an. Anschließend entfernt der Switch die „DHCP Option 82“ von den „DHCPOFFER“- und „DHCPACK“-Paketen. Der DHCP-Server weist dann entsprechend dieser Informationen dem Client eine IP-Domäne zu.

Die maximale Länge für diese Informationen beträgt 32 Zeichen.

In Großstädten und bevölkerungsreichen Umgebungen mit ETHERNET-Zugang kann DHCP die Zuweisung von IP-Adressen für eine große Anzahl von Teilnehmern zentral verwalten. Wenn die „DHCP Option 82“-Funktion beim Switch aktiviert ist, kann ein Teilnehmergerät durch den Switch-Port identifiziert werden, über das es sich mit dem Netzwerk verbindet (zusätzlich zu seiner MAC-Adresse). Auch wenn sich mehrere Hosts im Teilnehmer-LAN über denselben Port am Switch verbinden, kann jeder einzelne Host eindeutig identifiziert werden.

Wenn die „DHCP Snooping Information Option 82“ beim Switch aktiviert wird, erfolgt dieser Ablauf von Ereignissen:

- Der Host (DHCP-Client) generiert eine DHCP-Anfrage und sendet sie ins Netzwerk.
- Wenn der Switch die DHCP-Anfrage empfängt, fügt er dem Paket die „Option 82“-Informationen hinzu. Diese Informationen enthalten die MAC-Adresse des Switches (die Unteroption „Remote-ID“), den „Port Identifier“ und den „VLAN-Mod-Port“, von dem das Paket empfangen wurde (die Unteroption „Circuit-ID“).
- Wenn die IP-Adresse des „Relay Agents“ konfiguriert wurde, fügt der Switch dem DHCP-Paket die IP-Adresse hinzu.
- Der Switch leitet die DHCP-Anfrage mit dem Option-82-Feld an den DHCP-Server weiter.
- Der DHCP-Server empfängt das Paket. Ist der Server Option-82-fähig, kann er die „Remote ID“, die „Circuit ID“ oder beide nutzen, um IP-Adressen zuzuweisen und Richtlinien zu implementieren, wie etwa die Begrenzung der IP-Adressanzahl, die einer einzelnen „Remote ID“ oder „Circuit ID“ zugewiesen werden kann. Anschließend überträgt der DHCP-Server das Option-82-Feld in die DHCP-Antwort.

- Der DHCP-Server leitet die Antwort als Unicast zum Switch weiter, wenn die Anfrage an den Server vom Switch übertragen wurde. Wenn sich Client und Server im selben Subnetz befinden, leitet der Server die Antwort als Broadcast weiter. Der Switch verifiziert daraufhin die ursprünglich eingetragenen Option-82-Daten, indem er das Feld der „Remote ID“ und unter Umständen auch das der „Circuit ID“ überprüft. Der Switch entfernt das Option-82-Feld und leitet das Paket zum Switch-Port weiter, der mit dem DHCP-Client verbunden ist und die DHCP-Anfrage gesendet hat.

Option Frame Format

Tabelle 20: Option Frame Format

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	...	iN

Das „Agent Information Field“ (Informationsfeld des Agenten) besteht aus einer Abfolge von Tupel (Unteroption/Länge/Wert) für jede Unteroption, die auf folgende Weise codiert sind:

Tabelle 21: Option Frame Format

Unteroption	Len	Unteroptionswert					
1	N	s1	s2	s3	s4	...	sN

DHCP Agent Code der Unteroption	Beschreibung der Unteroption
-----	-----
1	Unteroption „Agent Circuit ID“
2	Unteroption „Agent Remote ID“

Tabelle 22: Frame-Format der Unteroption „Circuit ID“

Unteroptionstyp	Länge	„Circuit ID“- Typ	Länge	VLAN	Modul	Port
1	6	0	4	2	1	1

Tabelle 23: Frame-Format der Unteroption „Remote ID“

Unteroptionstyp	Länge	„Circuit ID“- Typ	Länge	MAC-Adresse
2	8	0	6	6

Tabelle 24: Format der Unteroption „Circuit ID“

Code	Len	Unteroptionstyp	Länge	Slot-ID	Port-ID	VLAN-ID	Information
0x52	0x0c	0x01	0x0a	0x01	0x01	0x0002	justin

7.2.6 DHCP-Server

Bei der Konfiguration der Netzwerkparameter über DHCP sendet das ETHERNET-Gerät nach der Initialisierung eigenständig eine Client-Anfrage an den DHCP-Server. Diese Anfrage ist ein Broadcast-Telegramm, das die Hardware-Adresse (MAC-ID, MAC-Adresse) des ETHERNET-Gerätes enthält.

Der DHCP-Server erhält die Anfrage. Dieser Server verwaltet einen Pool von IP-Adressen und speichert für jede IP-Adresse die zugehörige MAC-Adresse und weiteren Parameter. Ist die anfragende MAC-Adresse schon im Pool enthalten, antwortet der Server mit der bereits hinterlegten IP-Adresse. Der DHCP-Server antwortet aber auch auf Antworten von bislang unbekannten MAC-Adressen: Hat er noch freie IP-Adressen in seinem Bereich, weist er einer dieser freien IP-Adresse die neue MAC-Adresse zu und schickt danach die Antwort.

Das ETHERNET-Gerät wartet auf die Antwort des DHCP-Servers. Ankommende Pakete enthalten unter anderem die IP-Adresse und die MAC-Adresse des ETHERNET-Gerätes. An der MAC-Adresse erkennt ein ETHERNET-Gerät, ob die Nachricht für ihn bestimmt ist, und übernimmt bei Übereinstimmung die gesendete IP-Adresse in sein Netzwerk-Interface.

Erfolgt keine Antwort, wird die Anfrage nach 4 Sekunden erneut gesendet, dann eine weitere nach 8 Sekunden und die letzte nach 16 Sekunden.

Bleiben alle Anfragen ohne Antwort, erfolgt eine Fehlermeldung.

Hinweis**DHCP-Konfiguration wird nicht gespeichert!**

Beachten Sie, dass die Netzwerk-Konfiguration über DHCP im Gegensatz zu der Verwendung von BootP nicht gespeichert wird. Das Gerät erhält beim nächsten Start des Systems eine neue IP-Adresse.

Der Unterschied zwischen BootP und DHCP besteht darin, dass beide Protokolle verschiedene Zuordnungsverfahren verwenden.

7.2.7 Dual Homing

Mit „Dual Homing“ wird eine Netzwerktopologie beschrieben, in der ein Gerät über zwei unabhängige Netzzugriffspunkte („Points of Attachment“) mit einem Netzwerk verbunden ist. Ein Zugriffspunkt stellt die primäre Verbindung her und der andere dient als Reserve, falls die Primärverbindung ausfällt.

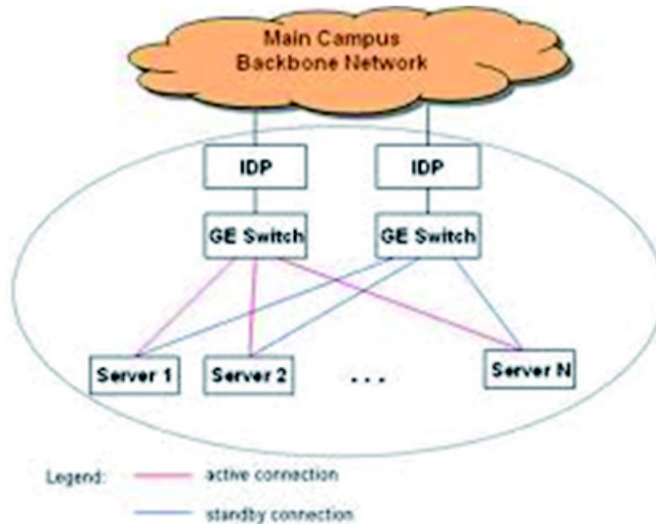


Abbildung 21: Dual Homing

Beispielsweise könnten Primär- und Sekundärverbindung auf unterschiedliche Art mit dem Internet verbunden sein. Die Primärverbindung könnte mit einem physischen Netzwerk und die Sekundärverbindung über ein drahtloses Netzwerk verbunden sein. Mit aktivierter Funktion „Dual Homing“ verbindet sich ein Gerät standardmäßig über die Primärverbindung, während die Sekundärverbindung unterbrochen bleibt. Wenn der Port oder alle Ports der Primärverbindung ausfallen, wechselt das Gerät zur Sekundärverbindung. Wenn in dieser Situation die Sekundärverbindung auch ausfällt, bleibt das Gerät inaktiv. Die Sekundärverbindung funktioniert nur, wenn nur die Primärverbindung unterbrochen ist.

7.2.8 Dual Ring

Mit der Funktion „Dual Ring“ können 2 benachbarte Ringe über einen Switch miteinander verbunden werden, ohne dass zusätzliche Ports oder Leitungen benötigt werden. Mit dieser Konfiguration wird die benötigte Gesamt-Port-Zahl reduziert und Verkabelungskosten gespart, da eine zusätzliche Leitung nicht notwendig ist.

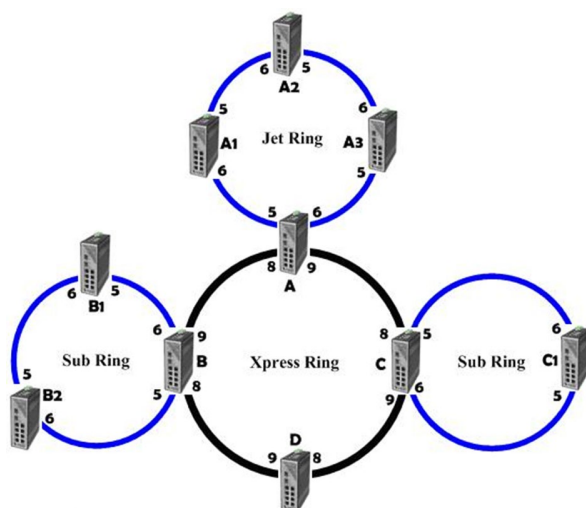


Abbildung 22: Dual Ring Switch ABC

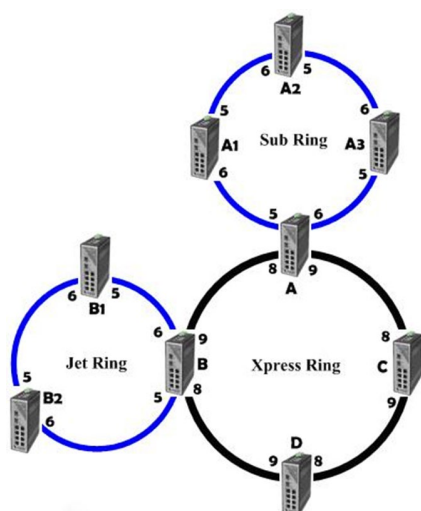


Abbildung 23: Dual Ring Switch AB

Zusätzlich können auch weitere WAGO-ETHERNET-Endgeräte in den Jet-Ring integriert werden. Hierbei muss bei den Geräten der Fast-Aging-Mechanismus aktiviert sein.

Hinweis



Weitere Informationen

Weiterführende Informationen finden Sie in den Handbüchern zu den WAGO-ETHERNET-Endgeräten.

Diese Handbücher finden Sie zum Download unter www.wago.com.

7.2.9 ERPS

Die Funktion ERPS („**ETHERNET Ring Protection Switching**“) implementiert gemäß dem ITU-T-Standard G.8032 einen Schutzschaltungsmechanismus für Ring-Topologien in der ETHERNET-Schicht. Dabei schützt das Protokoll ERP („**ETHERNET Ring Protection**“) den ETHERNET-Datenverkehr in einer Ring-Topologie und stellt gleichzeitig sicher, dass in der ETHERNET-Schicht innerhalb des Rings keine Schleifen entstehen können. Die Schleifenbildung wird durch das Blockieren des Datenverkehrs an einem zuvor festgelegten oder ausgefallenen Link verhindert.

Die Schutzfunktion für ETHERNET-Ringe beinhaltet Folgendes:

- Verhinderung von Schleifenbildungen
- Einsatz von Erkennungs-, Weiterleitungs- und Filterdatenbank- (FDB) Mechanismen

Um das Entstehen einer Schleife zu verhindern, wird sichergestellt, dass der Datenverkehr zu jeder Zeit über alle Ring-Links geleitet werden kann – außer an einem Link. Dieser besondere Ring-Link dient als Reserveverbindung und wird als RPL („**Ring Protection Link**“) bezeichnet. Im normalen Betrieb wird er blockiert und somit nicht für den Datenverkehr von Services verwendet. Für das Blockieren des Datenverkehrs an einem Ende des RPL ist ein spezifischer ETHERNET-Ringknoten, der „RPL Owner“, verantwortlich. Wenn es im ETHERNET-Ring zu einem Ausfall kommt, hebt der „RPL Owner“-Knoten die Blockierung an seinem Ende des RPL auf, sofern der RPL nicht ausgefallen ist, und gibt den Datenverkehr über den RPL frei. Auch der benachbarte ETHERNET-Ringknoten des RPL, der „RPL Neighbour“-Knoten, kann den Datenverkehr an seinem Ende des RPL blockieren oder freigeben.

Die ETHERNET-Ringe können ein Multiring-/Kettennetzwerk unterstützen, das aus ETHERNET-Ringen besteht, die über einen oder mehrere Punkte miteinander verbunden sind. Das in dieser Empfehlung definierte Protokoll und die Schutzschaltungsmechanismen können unter folgenden Voraussetzungen in einem Multiring-/Kettennetzwerk angewendet werden:

- In den ETHERNET-Ringverbindungen findet keine gemeinsame Nutzung der R-APS-Kanäle statt.
- Das Steuerungsverfahren für den ETHERNET-Ringschutz („ERP Control Process“) steuert in nur einem ETHERNET-Ring alle Verkehrskanäle und alle R-APS-Kanäle (z. B. das Blockieren oder Durchleiten) an allen Ring-Ports.
- Jeder Hauptring oder Unterring verfügt über seinen eigenen RPL.

In einem nicht überlasteten ETHERNET-Ring, in dem sich alle ETHERNET-Ringknoten im Leerlaufzustand befinden (d. h., es gibt keine erkannten Ausfälle, keinen aktiven automatischen oder externen Befehl und es werden nur R-APS (NR, RB) -Nachrichten empfangen), dessen Glasfaser-Ringumfang kleiner als 1.200 km ist und das weniger als 16 ETHERNET-Ringknoten hat, soll die Umschaltzeit (die Transferzeit, wie sie in ITU-T G.808.1 definiert ist) bei einem Ausfall eines Ring-Links weniger als 50 ms betragen.

Die Architektur des Ringschutzes stützt sich auf das APS-Protokoll zur Koordinierung der Ringschutzfunktionen in einem ETHERNET-Ring.

Der Switch unterstützt bis zu sechs Ringe.

Guard Timer

Alle Ringteilnehmer nutzen einen „Guard Timer“ (Zeitüberwachung). Dieser verhindert, dass sich eine geschlossene Schleife bilden kann und dass Ringteilnehmer veraltete R-APS-Nachrichten verwenden. Der „Guard Timer“ wird aktiviert, wenn ein Ringteilnehmer Informationen über eine lokale Umschaltanfrage empfängt, wie etwa nach den Befehlen SF („**S**witch **F**ail“), MS („**M**anual **S**witch“) oder FS („**F**orced **S**witch“). Nach Ablauf des Timers beginnt der Ringteilnehmer mit der Ausführung der Aktionen, die er vom R-APS empfängt. Dieser Timer kann nicht angehalten werden.

WTR Timer

Der „WTR Timer“ („**W**ait **T**o **R**estore **T**imer“, Wartezeitgeber) wird vom „RPL Owner“ genutzt. Der „WTR Timer“ geht in den Rücksetzungsmodus über, um ein wiederholtes Auslösen der Schutzschaltung durch Port-Fluktuationen oder periodische Signalausfallfehler zu verhindern. Nach Ablauf des Timers sendet der „RPL Owner“ eine R-APS (NR, RB) -Nachricht durch den Ring.

WTB Timer

Der „WTB Timer“ („**W**ait **T**o **B**lock **T**imer“, Blockade-Timer) wird beim „RPL Owner“ aktiviert. Der „RPL Owner“ nutzt die „WTB Timer“, bevor er eine RPL-Blockierung initiiert, und kehrt wieder in den Leerlaufzustand zurück, wenn ein Benutzer Befehle für den FS- oder MS-Zustand eingegeben hat. Da in einem Ring mehrere FS-Befehle nebeneinander aktiv sein können, stellt der „WTB Timer“ sicher, dass das Löschen eines einzelnen FS-Befehls nicht gleich das erneute Blockieren des RPL zur Folge hat. Der „WTB Timer“ soll 5 Sekunden länger laufen als der „Guard Timer“, damit ein sendender Ringteilnehmer ausreichend Zeit zum Versand zweier R-APS-Nachrichten erhält und der Ring den latenten Zustand erkennen kann. Bei der Löschung eines MS-Befehls verhindert der „WTB Timer“ das Entstehen einer geschlossenen Schleife, weil der „RPL Owner“-Knoten während des Wiederherstellungsprozesses nicht auf eine veraltete dezentrale MS-Anfrage reagieren wird.

Hold-off Timer

Jeder Ringteilnehmer nutzt einen „Hold-off Timer“, um die Meldung über einen Port-Ausfall zu verzögern. Nach Ablauf des Timers überprüft der Ringteilnehmer den Port-Status. Besteht das Problem weiterhin, wird eine Meldung versendet. Besteht kein Problem, wird auch keine Meldung versendet.

ERPS mit und ohne Rückschaltmodus

Das ERPS nutzt einen rückschaltenden und einen nicht rückschaltenden Betriebsmodus („revertive and non-revertive operation“). Wenn im

Rückschaltmodus die Bedingungen, die eine Umschaltung ausgelöst haben, nicht mehr vorhanden sind, wird der Verkehrskanal zur funktionierenden Transportentität wiederhergestellt, d. h., auf dem RPL blockiert. Nach Beseitigung eines Fehlerzustandes wird der Verkehrskanal erst nach Ablauf eines „WTR Timer“ wieder zurückgeschaltet, um zu verhindern, dass Schutzzustände wegen periodisch auftretender Fehler hin- und herwechseln. Ohne den Rückschaltmodus wird der Verkehrskanal den RPL nach Beseitigung einer Umschaltbedingung weiterhin nutzen, sofern der RPL nicht ausgefallen ist.

Control VLAN

Das „Control VLAN“ (Steuerungs-VLAN) ist eine Domäne, in der nur ERPS-Steuerungspakete übertragen werden. Dadurch, dass in diesem VLAN keine anderen Pakete übertragen werden, kommt es beim ERPS zu keinerlei Verzögerungen. Daher muss bei der Konfiguration eines Steuerungs-VLANs für einen Ring darauf geachtet werden, dass es ein neues VLAN ist. Das ERPS erstellt das Steuerungs-VLAN und seine Teilnehmer-Ports automatisch. Ein Teilnehmer-Port darf nur einen rechten und einen linken Port haben.

Im ERPS werden Steuerungs- und Datenpakete in unterschiedliche VLANs aufgeteilt.

Die Steuerungspakete werden in einem Steuerungs-VLAN übertragen.

Instanz

Bei ERPS Version 2 ist eine Instanz ein Profil, das ein Steuerungs-VLAN und ein oder mehrere Daten-VLANs für das ERPS spezifiziert. So werden die Steuerungs- und Datenpakete im ERPS auf verschiedene VLANs aufgeteilt. Die Steuerungspakete werden im Steuerungs-VLAN und die Datenpakete in einem oder in mehreren Daten-VLANs übertragen. Auf diese Weise kann ein Benutzer einem ERPS-Ring einfach einer Instanz zuweisen.

Wenn im ERPS Version 1 ein Port durch das ERPS blockiert wird, werden alle Pakete blockiert.

Wird im ERPS Version 2 ein Port durch einen ERPS-Ring blockiert, werden nur die zu den VLANs in dieser Instanz gehörenden Pakete blockiert.

Hinweis



Steuerungs-VLAN und Instanz

In CLI- oder Web-Konfigurationen gibt es Einstellungen für das Steuerungs-VLAN und für die Instanz.

Wurde das Steuerungs-VLAN für einen Ring konfiguriert und es soll eine Instanz für den Ring konfiguriert werden, dann muss das Steuerungs-VLAN für die Instanz dasselbe wie das des Rings sein. Anderenfalls wird ein Fehler angezeigt. Wenn Sie diese Instanz dennoch verwenden möchten, können Sie zuerst das Steuerungs-VLAN so einrichten, dass es dasselbe ist wie das für die Instanz. Anschließend können Sie die Instanz konfigurieren.

7.2.10 Link Aggregation

7.2.10.1 Static Trunk

„Link Aggregation“ (auch „Trunking“ genannt, parallele Link-Bündelung) ist die Gruppierung physischer Ports zu einem logischen Link mit höherer Kapazität. Bei der Bündelung von Ports kann es kostengünstiger sein, mehrere weniger schnelle Links zu verwenden als einen einzelnen schnellen, aber teuren „Port Link“ nicht vollständig auszunutzen.

Je mehr Ports jedoch gebündelt werden, desto weniger stehen danach zur Verfügung. Eine „Trunk Group“ ist ein logischer Link, der mehrere Ports enthält. Der Switch unterstützt sowohl statische als auch dynamische „Link Aggregation“.

Hinweis



„Link Aggregation“

In einem gut geplanten Netzwerk ist es empfehlenswert, nur die statische „Link Aggregation“ anzuwenden. Dies gewährleistet eine erhöhte Netzwerkstabilität und Kontrolle über „Trunk Groups“ für Ihren Switch.

7.2.10.2 LACP

Der Switch unterstützt gemäß dem Standard IEEE 802.3ad statisches und dynamisches (LACP) „Port Trunking“. Im Standard IEEE 802.3ad wird das LACP („Link **A**ggregation **C**ontrol **P**rotocol“) für die dynamische Erstellung und Verwaltung von „Trunk Groups“ beschrieben.

Bei der Aktivierung der „LACP Link Aggregation“ bei einem Port kann sich dieser mit den Ports am anderen Ende der Verbindung automatisch verbinden, um „Trunk Groups“ zu erstellen. LACP erlaubt außerdem Port-Redundanz, d. h., dass wenn ein aktiver Port ausfällt, ein anderer Port als „Ersatz“ aktiv wird, ohne dass ein Benutzer eingreifen muss.

Dabei ist Folgendes zu beachten:

- Alle Ports müssen über eine Punkt-zu-Punkt-Verbindung mit demselben ETHERNET-Switch verbunden und für das „LACP Trunking“ konfiguriert sein.
- LACP funktioniert nur über Vollduplexverbindungen.
- Alle Ports in derselben „Trunk Group“ müssen in Bezug auf Medientyp, Geschwindigkeit, Duplexmodus und Einstellungen für „Flow Control“ übereinstimmen.
- Konfigurieren Sie „Trunk Groups“ oder LACPs, bevor Sie eine Verbindung zum ETHERNET-Switch herstellen, um Schleifen in der Netzwerktopologie zu vermeiden.

Systempriorität

Mit der LACP-Systempriorität wird die Mitgliedschaft in einer LAG („**L**ink **A**ggregation **G**roup“) bestimmt und das Gerät für andere Switches während der LAG-Negotiationen identifiziert.

Der Switch mit der niedrigsten Systempriorität (und niedrigsten Port-Nummer, wenn die Systempriorität die gleiche ist) wird zum „Server“ des LACP. Dieser Server steuert den Betrieb der LACP-Einstellungen. Je niedriger die Nummer ist, desto höher ist die Prioritätsebene.

System-ID

Die „LACP System ID“ ist eine Kombination aus dem LACP-Systemprioritätswert und der MAC-Adresse des Routers.

Administrative Key

Der „Administrative Key“ (Administrativer Schlüsselwert) definiert die Fähigkeit eines Ports, sich mit anderen Ports zu verbinden. Diese Fähigkeit wird von folgenden Faktoren bestimmt:

- Die physischen Eigenschaften des Ports, wie z. B. Datenrate, Duplexfähigkeit und Punkt-zu-Punkt- oder geteiltes Übertragungsmedium.
- Die von Ihnen eingerichteten Konfigurationsbeschränkungen.

Port-Priorität

Die Port-Priorität legt fest, welche Ports in den Stand-by-Modus übergehen, wenn es eine Hardwarebeschränkung gibt, die die Bündelung aller kompatiblen Ports verhindert.

7.2.11 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 Management-Adresse 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.

7.2.12 Loop Detection (Schleifenerkennung)

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 Sondenpakete, um zu erkennen, ob der Port mit einem Netzwerk im Schleifenzustand verbunden ist. Der Switch schaltet einen Port ab, wenn er erkennt, dass Sondenpakete 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.

7.2.13 Jet Ring

Durch die Einrichtung der Jet-Ring-Funktion (redundante Verbindung) in einem Netzwerk werden kritische Verbindungen besser vor Fehlern und Netzwerkschleifen geschützt. Außerdem verringert sich die Netzwerkausfallzeit auf weniger als 300 ms.

Mithilfe der Jet-Ring-Funktion können Nutzer einen sekundären Pfad zum Netzwerk einrichten. Dadurch wird für den Fall, dass eine Verbindung abrupt unterbrochen oder abgebrochen wird, eine Datenübertragungssicherungsroute bereitgestellt. Diese Funktion ist für industrielle Anwendungszwecke extrem wichtig, da es durch einen Verbindungsfehler bei einer Verbindung ohne Sicherung zu einer Netzwerkausfallzeit von mehreren Minuten und somit schwerwiegenden Verlusten kommen kann.

Das Jet-Ring-Protokoll dient zur Optimierung der sekundären Kommunikationsverbindung und zur Bereitstellung einer sehr schnellen Verbindungswiederherstellungsdauer. Durch die Jet-Ring-Funktion erfolgt eine automatische Bestimmung eines Switches als „Master“ des Netzwerks und eine automatische Blockierung von Anschlüssen. So wird verhindert, dass Pakete alle sekundären Schleifensegmente des Netzwerks durchlaufen. Falls ein Ring-Segment aufgrund eines Verbindungsfehlers vom Rest des Netzwerks getrennt wird, wird der Ring durch das Jet-Ring-Protokoll automatisch erneut so angepasst, dass der Teil des Netzwerks, der getrennt wurde, den Kontakt mit dem restlichen Netzwerk wiederherstellt.

Schritt 1

Die Jet-Ring-Funktion in der nachfolgenden Grafik ist für die Verbindung von vier Einheiten von Industrial-Managed-Switches anwendbar.

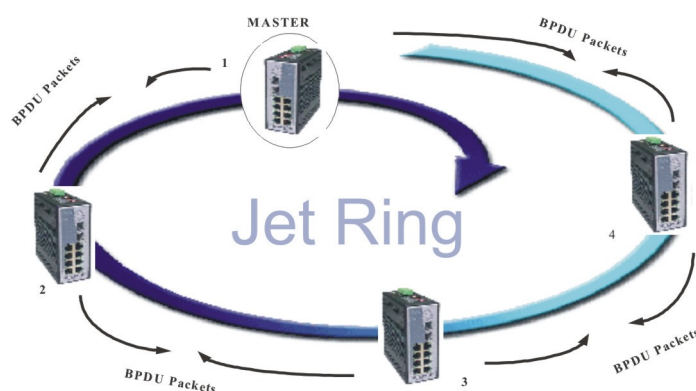


Abbildung 24: Jet Ring

Schritt 2

Durch die Jet-Ring-Funktion wird dann automatisch der Arbitr-Switch ausgewählt, das Netzwerk ist daraufhin funktionsbereit.

7.2.14 Static Route

Statische Routen definieren explizite Pfade zwischen zwei Endsystemen. Diese Pfade werden bei der Installation eines Netzwerks definiert und in der Regel als feste Routingtabelle im Router abgespeichert. Die Endgeräte sind jeweils einem Router zugeordnet, über den sie erreichbar sind und andere Ziele erreichen können. Statische Routen können nicht automatisch aktualisiert werden. Wenn sich eine Netzwerkänderung ergibt, müssen die statischen Routen manuell neu konfiguriert werden. Statische Routen verbrauchen weniger Bandbreite als dynamische Routen. Es werden keine CPU-Zyklen verwendet, um Routing-Aktualisierungen zu berechnen und zu analysieren.

IP-Weiterleitung

Die IP-Weiterleitung ermöglicht die Bereitstellung von IP-Paketen zwischen Hosts über Netzwerkgrenzen hinweg. Wenn sich zwei Hosts nicht in einem Netzwerk befinden, müssen die Daten über einen Router geleitet werden, welcher die beiden Netzwerke miteinander verbindet. Im Fall von großen Netzwerken, wie z. B. dem Internet, können es auch mehrere Router sein. Beim Anlegen von Routen wird immer nur der nächste Host auf dem Weg zum Zielhost angegeben und nicht die vollständige Route. Wenn die Daten über mehrere Router transportiert werden, müssen auf den dazwischen liegenden Routern ebenfalls Routen zum nachfolgenden Router angelegt werden.

Die IP-Weiterleitung funktioniert sowohl als Router als auch als Inter-VLAN-Routing mit Trunk-Stick.

Die Routing-Datenbank spielt eine wichtige Rolle bei der Weiterleitung der Pakete. Router füllen die Routingdatenbank entweder durch manuelle Konfigurationen oder mit Hilfe dynamischer Routingprotokolle auf.

Manuelle Routing-Konfigurationen werden als statische Routen bezeichnet. Immer wenn ein IP-Paket von einem Router empfangen wird, ruft es die Ziel-IP-Adresse ab und sucht in der Routing-Tabelle nach der längsten Präfix-Übereinstimmungsrouten. Das Paket wird dem zugewiesenen nächsten Host in der Route weitergeleitet.

7.2.15 Spanning Tree Protocol (STP)

Das (R)STP („**R**apid **S**panning **T**ree **P**rotocol“) kann Netzwerkschleifen erkennen und aufbrechen sowie „Backup 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“ (aufspannenden Baumes) 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 Quell-Adressen 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 25: 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 beim 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-Negotiationen 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 Port“ bestimmt. Der Switch mit der höchsten Priorität wird zum STA-Root-Switch. Haben jedoch alle Switche 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 Spannbauums.

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 Bridge Protocol Data Units (BPDU) an alle Bridges und stellt über die in den BPDU-Datenpaketen enthaltenen Konfigurationsdaten die Netzkonfiguration fest.

7.2.16 Xpress-Ring

Der Xpress-Ring stellt eine reaktionsschnelle Ringtechnologie mit Selbstheilungsfunktion dar, durch die unterbrochene Verbindungen in Netzwerken innerhalb von 50 ms wiederhergestellt werden können.

Schnelle Verbindungswiederherstellung und Ringredundanz sind wichtige Funktionen zur Erhöhung der Zuverlässigkeit in Nonstop-Systemen.

Ein gut geplantes Netzwerk mit einem Arbiter-Switch und Ring-Ports kann bei Segmentausfällen innerhalb sehr kurzer Zeit wiederhergestellt werden.

Es gibt für einen Switch im Xpress-Ring nur zwei Rollen: entweder „Forwarder“ (Weiterleitender) oder „Arbiter“ (Entscheider). Es kann immer nur einen Arbiter-Switch geben, während alle anderen Switches „Forwarder“ sind.

Einer der Ring-Ports des Arbiter-Switches wird in den blockierten Zustand versetzt. Wenn eine der Ringverbindungen ausfällt, wird dieser blockierte Port in den weiterleitenden Zustand versetzt.

7.3 Security

7.3.1 IP Source Guard

„IP Source Guard“ (IP-Quelladressschutz) ist eine Sicherheitsfunktion, die den IP-Datenverkehr an ungesicherten Layer2-Ports auf Grundlage einer „DHCP Snooping“-Datenbankanbindung oder einer manuell konfigurierten IP-Quellanbindung filtert. Mit dieser Funktion können Angriffe wie „IP Spoofing“ (Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse) verhindert werden, wenn ein Host versucht, die IP-Adresse eines anderen Hosts zu fälschen. Jeder IP-Datenverkehr, der an der Schnittstelle mit einer anderen als der (über DHCP oder statische Konfiguration) zugewiesenen IP-Quelladresse eingeht, wird an ungesicherten Layer2-Ports herausgefiltert.

Diese Funktion wird an ungesicherten Layer2-Schnittstellen in Kombination mit „DHCP Snooping“ verwendet. Dabei wird eine IP-Quellanbindungstabelle manuell konfiguriert (statische IP-Quellanbindung) oder aus Informationen der Funktion „DHCP Snooping“ erstellt und verwendet. Jeder Eintrag in dieser Tabelle enthält die IP-Adresse und die zugehörigen MAC- und VLAN-Adressen. Der „IP Source Guard“ unterstützt nur Layer2-Ports, einschließlich „Access Ports“ und „Trunk Ports“.

Der „IP Source Guard“ umfasst folgende Funktionen:

1. DHCP Snooping
2. DHCP-Anbindungstabelle
3. ARP-Überprüfung
4. Blacklist Filter (ARP-Überprüfung mit MAC-Adressfiltertabelle)

7.3.1.1 DHCP Snooping

„DHCP Snooping“ ist eine DHCP-Sicherheitsfunktion, die durch Filterung ungesicherter DHCP-Nachrichten und Erstellung und Nutzung einer „DHCP Snooping“-Datenbankanbindung (auch als „DHCP Snooping“-Anbindungstabelle bekannt) die Netzwerksicherheit erhöht.

„DHCP Snooping“ agiert als Firewall zwischen ungesicherten Hosts und DHCP-Servern. Es kann zur Unterscheidung zwischen ungesicherten Schnittstellen, die mit Endbenutzern verbunden sind, und gesicherten Schnittstellen, die mit einem DHCP-Server oder anderen Switch verbunden sind, eingesetzt werden.

Die „DHCP Snooping“-Anbindungstabelle enthält MAC-Adresse, IP-Adresse, „Lease Time“ (Leihdauer), Anbindungsart, VLAN-Nummer und Informationen über die lokalen ungesicherten Schnittstellen eines Switches.

Wenn ein Switch ein Paket von einer ungesicherten Schnittstelle empfängt und die Schnittstelle zu einem VLAN gehört, in dem „DHCP Snooping“ aktiviert ist, vergleicht der Switch die MAC-Quelladresse mit der Hardwareadresse des DHCP-Clients. Stimmen die Adressen überein (der Normalfall), leitet der Switch das Paket weiter. Wenn sie nicht übereinstimmen, verwirft er es.

Der Switch verwirft ein DHCP-Paket, wenn eine der folgenden Situationen eintritt:

- Ein Paket von einem DHCP-Server, wie etwa DHCP OFFER, DHCP ACK, DHCP NAK oder DHCP LEASE QUERY, wird über einen ungesicherten Port empfangen.
- Es wird ein Paket über eine ungesicherte Schnittstelle empfangen, und die MAC-Quelladresse und die Hardwareadresse des DHCP-Clients stimmen mit keiner der aktuellen Anbindungen überein.

Mit „DHCP Snooping“ können nicht autorisierte DHCP-Pakete im Netzwerk herausgefiltert und eine Anbindungstabelle dynamisch erstellt werden. Dadurch wird verhindert, dass Clients IP-Adressen von nicht autorisierten DHCP-Servern erhalten.

Trusted vs. Untrusted Ports

Für das „DHCP Snooping“ ist jeder Port entweder ein „Trusted Port“ (gesicherter Port) oder ein „Untrusted Port“ (ungesicherter Port). Diese Einstellung ist unabhängig von der „Trusted/Untrusted“-Einstellung für die ARP-Überprüfung. Sie können auch die maximale Anzahl der DHCP-Pakete spezifizieren, die jeder Port („trusted“ oder „untrusted“) pro Sekunde empfangen kann.

„Trusted Ports“ sind mit DHCP-Servern oder Switches verbunden. Der Switch wird DHCP-Pakete von „Trusted Ports“ nur dann verwerfen, wenn die Übertragungsrate der empfangenen DHCP-Pakete zu hoch ist. Der Switch erlernt von den „Trusted Ports“ die dynamischen Anbindungen.

Hinweis**DHCP-Anfragen**

Der Switch wird alle DHCP-Anfragen verwerfen, wenn „DHCP Snooping“ aktiviert ist, aber keine „Trusted Ports“ vorhanden sind.

„Untrusted Ports“ sind mit Teilnehmern verbunden. Der Switch wird DHCP-Pakete von diesen Ports in folgenden Situationen verwerfen:

- Das Paket ist ein DHCP-Serverpaket (z. B. „OFFER“, „ACK“ oder „NACK“).
- Die MAC-Quelladresse und die IP-Quelladresse in einem Paket stimmen mit keiner der aktuellen Anbindungen überein.
- Die MAC-Quelladresse und der Quell-Port in einem „RELEASE“- oder „DECLINE“-Paket stimmen mit keiner der aktuellen Anbindungen überein.
- Die Übertragungsrate der empfangenen DHCP-Pakete ist zu hoch.

Datenbank für DHCP Snooping

Der Switch speichert die Anbindungstabelle im flüchtigen Speicher. Wenn der Switch neu startet, lädt er die statischen Anbindungen aus dem permanenten Speicher, verliert dabei aber die dynamischen Anbindungen, sodass die Geräte im Netzwerk DHCP-Anfragen erneut senden müssen.

Konfiguration von DHCP Snooping

Führen Sie zur Konfiguration von „DHCP Snooping“ beim Switch die folgenden Schritte aus:

1. Aktivieren Sie „DHCP Snooping“ beim Switch.
2. Aktivieren Sie „DHCP Snooping“ für jedes VLAN.
3. Konfigurieren Sie „Trusted Ports“ und „Untrusted Ports“.
4. Konfigurieren Sie die statischen Anbindungen.

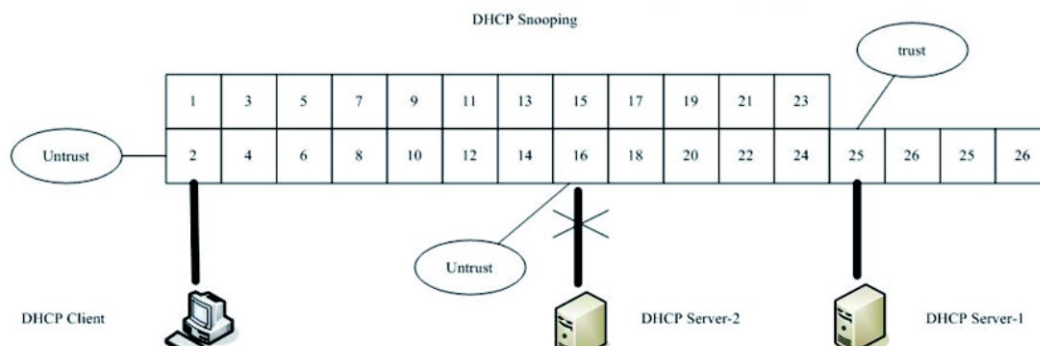
Hinweis**DHCP Snooping**

Der Switch wird alle DHCP-Anfragen verwerfen, wenn „DHCP Snooping“ aktiviert ist, aber keine „Trusted Ports“ vorhanden sind.

Wenn die Verbindung zu einem Port ausfällt, werden die von diesem Port erlernten Einträge aus der „DHCP Snooping“-Anbindungstabelle gelöscht.

Sie müssen das globale „DHCP Snooping“ und „DHCP Snooping“ für VLANs zuerst aktivieren.

- 1 Erstellung und Verwaltung eine Anbindungstabelle für die ARP-Überprüfungsfunktion.
- 2 Filtern der Pakete von DHCP-Servern, die mit einem „Untrusted Port“ verbunden sind.



Die Pakete von DHCP-Servern, die mit einem „Untrusted Port“ verbunden sind, werden herausgefiltert.

Der Switch unterstützt „Server Screening“ – eine Funktion, die den Zugriff von „Rogue DHCP Servers“ (nicht autorisierte, ungültige DHCP-Server) verhindert. Das bedeutet, wenn ein oder mehrere DHCP-Server im Netzwerk vorhanden sind und DHCP-Dienste für unterschiedliche, getrennte Client-Gruppen anbieten, werden die Pakete eines gültigen DHCP-Servers zum Client weitergeleitet.

Wenn keine DHCP-Server konfiguriert werden, bedeutet das, dass alle DHCP-Server gültig sind.

In der „DHCP Snooping“-Anbindungstabelle werden die Host-Informationen aufgezeichnet, die durch das „DHCP Snooping“ (dynamisch) oder durch Benutzer (statisch) eingetragen wurden. Die ARP-Überprüfung verwendet diese Tabelle, um zu entscheiden, ob ARP-Pakete weitergeleitet oder verworfen werden sollen. Von ungültigen Hosts gesendete ARP-Pakete werden verworfen. Nach Ablauf der „Lease Time“ wird der Eintrag aus der Tabelle gelöscht.

Statische Anbindungen werden durch die MAC-Adresse und die VLAN-ID eindeutig erkannt. Jede MAC-Adresse und VLAN-ID kann nur zu einer statischen Anbindung gehören. Wenn Sie eine statische Anbindung mit der MAC-Adresse und VLAN-ID einer bereits bestehenden Anbindung erstellen, wird die neue statische Anbindung die alte ersetzen.

Anbindungen werden beim „DHCP Snooping“ und der ARP-Überprüfung zur Unterscheidung von autorisierten und nicht autorisierten Paketen im Netzwerk verwendet. Der Switch erkennt die dynamischen Anbindungen durch das „Snooping“ bei DHCP-Paketen und die statischen Informationen durch die manuellen Einträge aus dem Menü „Static Entry Settings“.

7.3.1.3 ARP Inspection

Die dynamische „ARP Inspection“ („**A**ddress **R**esolution **P**rotocol **I**nspection“, ARP-Überprüfung) ist eine Sicherheitsfunktion, bei der ARP-Pakete in einem Netzwerk überprüft werden. Bei der dynamischen ARP-Überprüfung werden IP-zu-MAC-Adressanbindungen mit Einträgen aus einer gesicherten Datenbank (der „DHCP Snooping“-Datenbank) abgeglichen, bevor ein Paket weitergeleitet wird. Das dynamische ARP fängt ARP-Pakete mit ungültigen IP-zu-MAC-Adressanbindungen ab, protokolliert sie und verwirft sie anschließend. Diese Funktion bietet Schutz vor bestimmten „Man-in-the-Middle“-Angriffen.

Die dynamische ARP-Überprüfung stellt sicher, dass nur gültige ARP-Anfragen und -Antworten weitergeleitet werden.

Der Switch führt folgende Prozesse aus:

- Abfangen aller ARP-Anfragen und -Antworten an ungesicherten Ports.
- Überprüfung aller abgefangenen Pakete auf gültige IP-zu-MAC-Adressanbindung vor der Aktualisierung des lokalen ARP-Caches oder vor der Weiterleitung eines Paketes an das entsprechende Ziel.

Trusted Port und Untrusted Port

- Diese Einstellung ist unabhängig von der „Trusted/Untrusted“-Einstellung für das „DHCP Snooping“.
- Der Switch wird in keinem Fall ARP-Pakete von „Trusted Ports“ verwerfen.
- Der Switch wird ARP-Pakete von „Untrusted Ports“ verwerfen, wenn die Informationen des Senders in den ARP-Paketen mit keiner der aktuellen Anbindungen übereinstimmen.
- Normalerweise sind die „Trusted Ports“ die „Uplink Ports“ und die „Untrusted Ports“ mit Teilnehmern verbunden.

Konfigurationen

Die ARP-Überprüfung kann beim Switch von Benutzern aktiviert bzw. deaktiviert werden. Dies kann auch für ein spezifisches VLAN erfolgen. Wenn die ARP-Überprüfung beim Switch deaktiviert ist, ist sie in allen VLANs deaktiviert, auch wenn sie für einzelne VLANs aktiviert wurde.

Hinweis



Globaler Zustand/VLAN-Zustand

Es gibt einen globalen Zustand und einzelne VLAN-Zustände.

Wird der globale Zustand deaktiviert, wird die ARP-Überprüfung beim Switch deaktiviert, auch wenn einzelne VLAN-Zustände aktiviert wurden.

Wird der globale Zustand für die ARP-Überprüfung aktiviert, muss diese Funktion für spezifische VLANs vom Benutzer einzeln aktiviert werden.

7.3.1.3.1 Filter Table

Bei der dynamischen ARP-Überprüfung werden IP-zu-MAC-Adressanbindungen mit Einträgen aus einer gesicherten Datenbank (der „DHCP Snooping“-Datenbank) abgeglichen, bevor ein Paket weitergeleitet wird. Wenn der Switch ein nicht autorisiertes ARP-Paket erkennt, wird er automatisch einen MAC-Adressfilter erstellen, um den Datenverkehr von der MAC-Quelladresse und der Quell-VLAN-ID dieses Paketes zu blockieren. Außerdem wird der Switch regelmäßig Einträge löschen, deren „Age Time“ abgelaufen ist.

- Wenn das System bei aktivierter ARP-Überprüfung ungültige Hosts erkennt, wird es einen Filtereintrag in der MAC-Adresstabelle erstellen.
- Wenn eine Port-Verbindung bei deaktivierter ARP-Überprüfung ausfällt, wird der Switch die MAC-Filtereinträge für diesen Port löschen.
- Wenn eine Port-Verbindung bei aktivierter ARP-Überprüfung ausfällt, wird der Switch die MAC-Filtereinträge für diesen Port löschen.
- Die maximale Anzahl von Einträgen in der MAC-Adressfiltertabelle beträgt 256.
- Wenn die MAC-Adressfiltertabelle für die ARP-Überprüfung voll ist und der Switch ein nicht autorisiertes ARP-Paket empfängt, wird er automatisch ein „SYSLOG“ (Systemprotokoll) erstellen und das ARP-Paket verwerfen. Das Systemprotokoll wird nur einmalig erstellt.

7.3.2 Access-Control-Liste (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.

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 Regel-Treffer entsprechenden Richtlinie mit höchster Priorität ausgeführt.

7.3.3 Kommunikationsstandard IEEE 802.1X

Der IEEE 802.1X ist ein IEEE-Standard für port-basierte Netzwerkzugriffssteuerungen (wobei „Port“ hier einen einzelnen Zugriffspunkt auf eine LAN-Infrastruktur bezeichnet). Dieser Standard ist ein Bestandteil der IEEE 802.1-Gruppe von Netzwerkprotokollen. Er stellt einen Authentifizierungsmechanismus für Geräte bereit, die sich mit einem LAN verbinden möchten, und wird entweder eine Punkt-zu-Punkt-Verbindung einrichten oder diese verweigern, wenn die Authentifizierung fehlschlägt. Er wird für die meisten drahtlosen 802.11-Zugriffspunkte eingesetzt und arbeitet auf Grundlage des EAP („**E**xtensible **A**uthentication **P**rotocol“, Erweitertes Authentifizierungsprotokoll).

IEEE 802.1X verwendet eine port-basierte Authentifizierung, bei der die Kommunikation zwischen einem sog. „Supplicant“ (Anfragesteller), einem „Authenticator“ (Authentikator) und einem Authentifizierungsserver verwendet wird. Der Anfragesteller ist zumeist die Software auf einem Client-Gerät, wie etwa einem Laptop, der Authentikator kann ein drahtgebundener ETHERNET-Switch oder drahtloser Zugriffspunkt sein und der Authentifizierungsserver ist für gewöhnlich eine RADIUS („**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice“)-Datenbank.

Der Authentikator agiert als eine Art Wächter für das geschützte Netzwerk. Der Anfragesteller (z. B. ein Client-Gerät) erhält so lange keinen Zugriff auf die geschützte Seite des Netzwerks durch den Authentikator, bis seine Identität authentifiziert wurde. Bei der port-basierten 802.1X-Authentifizierung muss der Anfragesteller dem Authentikator Anmeldeinformationen bereitstellen, wie etwa Benutzername und Passwort oder ein digitales Zertifikat, die daraufhin vom Authentikator zum Authentifizierungsserver zur Verifizierung weitergeleitet werden. Wenn die Anmeldeinformationen gültig sind (mit den Einträgen in der Datenbank des Authentifizierungsservers übereinstimmen), erhält der Anfragesteller (das Client-Gerät) Zugriff auf die Ressourcen auf der geschützten Netzwerkseite.

Bei Erkennung eines neuen Clients („Supplicant“) wird der Port am Switch („Authenticator“) aktiviert und in den Zustand „unauthorized“ (unberechtigt) versetzt. In diesem Zustand können nur 802.1X-Daten ausgetauscht werden und anderer Datenverkehr, wie etwa DHCP und HTTP, wird auf der Netzwerkschicht (Layer 3) blockiert. Der Authentikator sendet eine EAP-Identitätsabfrage an den Anfragesteller und dieser antwortet mit einem EAP-Antwortpaket, das der Authentikator zum Authentifizierungsserver weiterleitet. Wenn der Authentifizierungsserver die Anfrage akzeptiert hat, versetzt der Authentikator den Port in den Zustand „authorized“ (berechtigt) und hebt die Blockade des Datenverkehrs auf. Meldet sich der Anfragesteller ab, sendet er dabei eine EAP-Abmeldenachricht an den Authentikator. Dieser versetzt den Port dann wieder in den Zustand „unauthorized“ und blockiert damit erneut alle Nicht-EAP-Daten.

RADIUS-Server

Der RADIUS-Server („**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice“, Authentifizierungsdienst für sich einwählende Benutzer) ist ein Client-Server-basiertes Sicherheitsprotokoll zur Authentifizierung und zur Kontrolle der Netzzugriffsberechtigung.

Der RADIUS-Server RADIUS arbeitet mit dem Challenge-Response-Verfahren (Aufforderung-Antwort-Verfahren) und unterstützt die zentrale Administration von Benutzerdaten wie Benutzererkennung, Passwörter, Rufnummern, Zugriffsrechte und auch Account-Daten und besteht aus einem Accounting- und Authentifizierungsprotokoll.

In Kombination mit DHCP und PPP kann die Konfiguration der sich einwählenden Systeme mit RADIUS automatisch geschehen.

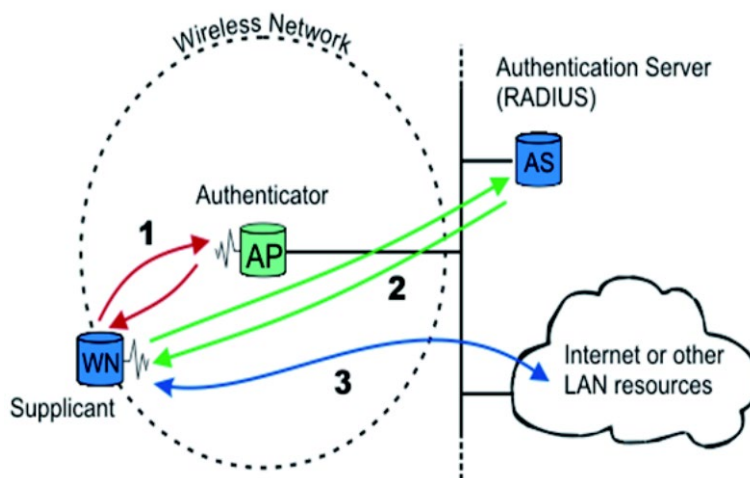


Abbildung 26: IEEE 802.1X

In der folgenden Abbildung wird veranschaulicht, wie das Authentifizierungsverfahren für einen Port mit aktivierter IEEE 802.1X-Authentifizierung abläuft. Der Switch verlangt vom Client Anmeldeinformationen in Form von Benutzername und Passwort.

Nachdem der Client seine Anmeldeinformationen übermittelt hat, sendet der Switch eine Authentifizierungsanfrage an den RADIUS-Server. Der RADIUS-Server überprüft daraufhin, ob der Client Zugriff auf den Port erhalten darf.

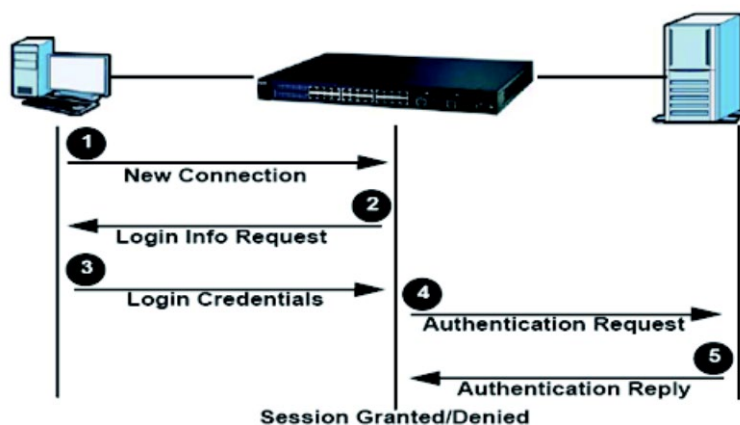


Abbildung 27: RADIUS-Server

Lokale Benutzerkonten

Durch die lokale Speicherung von Benutzerprofilen im Switch kann der Switch ohne Interaktion mit dem Authentifizierungsserver Benutzer authentifizieren. Es gibt jedoch eine Begrenzung auf 6 Benutzer, die auf diese Weise authentifiziert werden können.

Gast-VLAN

Die Funktion Gast-VLAN bei der port-basierten IEEE 802.1X-Authentifizierung beim Switch bietet Clients eingeschränkte Dienste, wie etwa das Herunterladen des IEEE 802.1X-Clients. Diese Clients können ihr System daraufhin mit der IEEE 802.1X-Authentifizierung aktualisieren.

Wird an einem IEEE 802.1X -Port ein Gast-VLAN aktiviert, wird der Switch die Clients, von denen er keine Antwort auf seine EAP-Anfrage bzw. kein „Identity Frame“ empfängt oder Clients, die keine EAPOL-Pakete („EAP over LAN“-Pakete) senden, einem Gast-VLAN zuweisen.

Port-Parameter

- **Admin Control Direction**

Beide	- Ist die 802.1X-Port-Authentifizierung für einen Benutzer fehlgeschlagen, werden am Port eingehende und ausgehende Pakete am Port verworfen.
Eingehend	- Ist die 802.1X-Port-Authentifizierung für einen Benutzer fehlgeschlagen, werden nur am Port eingehende Pakete verworfen.

- **Re-Authentication**

Mit dieser Funktion wird spezifiziert, ob ein Teilnehmer den Benutzernamen und das Passwort regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.

- **Reauth-Period**

Mit der „Reauth-Period“ (Authentifizierungsintervall) wird spezifiziert, in welchem zeitlichen Abstand ein Teilnehmer den Benutzernamen und das Passwort erneut eingeben muss, um mit dem Port verbunden zu bleiben. Der zulässige Wertebereich für dieses Feld ist 0 bis 65535 Sekunden.

- **Port Control Mode**

„Auto“	Benutzer können nach der Authentifizierung auf das Netzwerk zugreifen.
Force-authorized“	Benutzer können ohne Authentifizierung auf das Netzwerk zugreifen.
„force-unauthorized“	Benutzer können nicht auf das Netzwerk zugreifen.

- **Quiet Period**
Mit der „Quiet Period“ (Passivitätszeitraum) wird der Zeitraum spezifiziert, den ein Client warten muss, bevor er die nächste Authentifizierungsanfrage stellen darf. Dadurch wird eine Überlastung des Switches durch fortlaufende Anfragen von Clients verhindert. Der zulässige Wertebereich für dieses Feld ist 0 bis 65535 Sekunden.
- **Server-Timeout**
Der Wert für den „Server-Timeout“ (Server-Zeitlimit) gibt das Zeitlimit für den Authentifizierungsserver an.
- **Supp-Timeout**
Der Wert für den „Supp-Timeout“ (Anfragestellerzeitlimit) ist der Initialisierungswert für das Zeitlimit eines Anfragestellers.
- **Max-req Time**
Mit der „Max-req Time“ (Max. Anfragen) wird festgelegt, wie oft der Switch versuchen wird, sich mit dem Authentifizierungsserver zu verbinden, bevor er den Server als nicht verbunden ansieht. Der zulässige Bereich für dieses Feld beträgt 1 bis 10 Versuche.

7.3.4 Port Security

Der Switch empfängt die MAC-Adresse eines Gerätes, das mit einem bestimmten Port direkt verbunden ist, und erlaubt die Weiterleitung von Daten. Die Funktionen des Switches ermöglichen die Kontrolle darüber, welche und wie viele Geräte sich mit einem Switch-Port verbinden können.

Mit den „Port Security“-Funktionen kann die maximale Anzahl von MAC-Adressen pro Schnittstelle spezifiziert werden. Wird diese Anzahl überschritten, werden eingehende Pakete mit neuen MAC-Adressen verworfen. Dies kann mithilfe einer MAC-Adresstabelle überprüft werden. Diese Begrenzung umfasst auch die statischen MAC-Adressen.

Hinweis



Zustandsänderung eines Ports am Switch

Wenn ein Port am Switch vom deaktivierten in den aktivierten Zustand versetzt wird, sind alle, von diesem Port aufgezeichneten MAC-Adressen, verworfen worden.

7.3.4.1 Sticky-MAC-Einstellungen

Die Port Security mit Sticky-MAC-Adressen bietet viele der gleichen Vorteile wie Port-Sicherheit mit statischen MAC-Adressen, aber Sticky-MAC-Adressen können dynamisch gelernt werden. Die Port-Sicherheit mit Sticky-MAC-Adressen behält dynamisch erlernte MAC-Adressen während einer Link-Down-Bedingung bei.

7.4 Monitor

7.4.1 Alarm

Diese Funktion benachrichtigt den Netzwerkadministrator über alle abnormen Situationen innerhalb des Netzwerks.

Hinweis



Alarm-DIP-Schalter

Mit dem Alarm-DIP-Schalter kann ein Benutzer konfigurieren, ob eine Alarmmeldung versendet werden soll, wenn ein entsprechendes Ereignis eintritt.

Beispiel

P1:	ON (AN)	– Der Switch sendet eine Alarmmeldung, wenn die Verbindung an Port 1 ausfällt.
PWR:	ON	– Der Switch sendet eine Alarmmeldung, wenn die primäre Spannungsversorgung unterbrochen wird.
RPS:	ON	– Der Switch sendet eine Alarmmeldung, wenn die redundante Spannungsversorgung unterbrochen wird.

7.4.2 Systeminformationen

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

7.4.3 Port-Statistik

Mit dieser Funktion werden die Statistiken der Ports überwacht und z. B. die Anzahl der empfangenen und gesendeten Datenpakete angezeigt.

7.4.4 Port-Auslastung

Mit dieser Funktion wird die Auslastung der Ports angezeigt.

7.4.5 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 („Maximum Transmission Unit“) besitzen.

7.4.6 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.

7.4.6.1 DDMI

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)

7.4.7 Traffic Monitor

Die Funktion „Traffic Monitor“ (Überwachung des Datenverkehrs) kann sowohl für einen spezifischen Port als auch global beim 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.

7.5 Management

7.5.1 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 Management-Informationen, Status- und Statistikdaten zwischen einzelnen Netzwerkkomponenten und einem Management-System 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.

7.5.2 SNMP Trap

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

7.5.3 SNMPv3

In der Version 3 von SNMP ist der Nachrichtenaustausch an Benutzerkonten gebunden. Jedes Gerät, das die eingestellten Passwörter kennt, kann Werte aus dem ETHERNET-Gerät lesen bzw. schreiben. Bei SNMPv3 können die Nutzdaten der SNMP-Nachrichten auch verschlüsselt übertragen werden. Damit können die angefragten und zu schreibenden Werte nicht über ETHERNET mitgehört werden, so dass SNMPv3 häufig in sicherheitsrelevanten Netzwerken zum Einsatz kommt.

7.5.4 Auto Provision

Die Funktion „Auto Provision“ (Automatische Bereitstellung) ist ein von Diensteanbietern bereitgestellter Service, durch den Remote-Geräte schnell, einfach und automatisch von einem dezentralen Standort aus konfiguriert oder mit Firmware aktualisiert werden können.

1. Ist diese Funktion aktiviert, wird der Switch zuerst eine Informationsdatei vom Server des Diensteanbieters heruntergeladen.

Der Dateiname wird nach folgender Benennungsregel gebildet:

Serie_Modell_Autoprovision.txt

Beispiel: 852_1505_Autoprovision.txt

Die Datei besteht aus folgenden Inhalten:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=5228-000-1.0.0.b1
Firmware_Image_File=5228-000-1.0.0.b1.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=5228-000-1.0.0.b1.save
Global_Configuration_Reboot=0
```

Specific_Configuration_State=0

Specific_Configuration_Reboot=0

2. Ist der Wert von „AUTO_PROVISION_VER“ höher als der der aktuellen Version der „Auto Provision“, fahren Sie fort mit Schritt 3 – falls nicht, warten Sie bitte 24 Stunden und beginnen Sie erneut mit Schritt 1.
3. Ist „Firmware_Upgrade_State =1“, fahren Sie fort mit Schritt 4 – falls nicht, fahren Sie fort mit Schritt 6.
4. Weicht die „Firmware_Version“ von der aktuellen Firmware-Version ab, laden Sie bitte das „Firmware_Image_File“ herunter und aktualisieren Sie die Firmware.
5. War die Aktualisierung der Firmware erfolgreich und ist „Firmware_Reboot=1“, wird „reboot_flag=1“ ausgeführt.
6. Ist „Global_Configuration_State =1“, laden Sie bitte das „Global_Configuration_File“ herunter und aktualisieren Sie die Konfiguration – falls nicht, fahren Sie fort mit Schritt 8.
7. War die Aktualisierung der Konfiguration erfolgreich und ist „Global_Configuration_Reboot =1“, wird „reboot_flag=1“ ausgeführt.
8. Ist „Global_Configuration_State =1“, laden Sie bitte die spezifische Konfigurationsdatei herunter und aktualisieren Sie die Konfiguration – falls nicht, fahren Sie fort mit Schritt 10. Die Benennung lautet: „Serie_Modell_“ mit 12-Bit-MAC-Ziffern, z. B. „852_1505_00e04c8196b9.txt“.
9. War die Aktualisierung der Konfiguration erfolgreich und ist „Specific_Configuration_Reboot =1“, wird „reboot_flag=1“ ausgeführt.
10. Ist „reboot_flag=1“, speichern Sie die ausgeführte Konfiguration und starten Sie den Switch neu – falls nicht, warten Sie bitte 24 Stunden und beginnen Sie erneut mit Schritt 1.

7.5.5 Mail-Alarm

Der „Mail Alarm“ (E-Mail-Alarm) sendet einen E-Mail-Trap an einen zuvor definierten Administrator, wenn bestimmte Ereignisse eintreten. Diese Ereignisse werden im Folgenden genannt:

System Reboot (Systemneustart):	Das System führt einen Warm- oder Kaltstart aus.
Port Link Change (Port-Verbindungsänderung):	Ein Port-Verbindung wird hergestellt oder fällt aus.
Configuration Change (Konfigurationsänderung):	Die Systemkonfigurationen im NV-RAM wurden aktualisiert.
Firmware Upgrade (Firmware-Aktualisierung):	Die System-Firmware wurde aktualisiert.
User Login (Benutzeranmeldung):	Ein Benutzer hat sich im System angemeldet.
Port Blocked (Port-Blockierung):	Ein Port wird durch die „Loop Detection“ oder den „BPDU Guard“ blockiert.

7.5.6 Ping

Mit dem Ping-Befehl wird die Erreichbarkeit eines ETHERNET-Teilnehmers überprüft.

Ping basiert darauf, dass ein Programmiergerät ein ICMP-Echo-Request absetzt und auf einen ICMP-Echo-Response des angesprochenen ETHERNET-Teilnehmers wartet.

7.5.7 USB-Funktionen

Mit der USB-Schnittstelle des Switch können folgende Funktionen ausgeführt werden:

- Upload der Firmware
- Speichern der Konfigurationsdatei
- Speichern der Syslog-Datei
- Upload der Konfigurationsdatei

Im Auslieferungszustand sind diese Funktionen deaktiviert. Die Funktionen können über das Web-Based-Management oder die CLI-Kommandos aktiviert werden. Beim erstmaligen Einstecken des USB-Sticks wird automatisch die notwendige Ordnerstruktur auf dem USB-Stick erzeugt.

7.5.7.1 Upload der Firmware

Laden Sie die Firmware-Datei wie folgt auf den Switch:

1. Erstellen Sie auf dem USB-Stick (Dateisystem FAT32) einen Ordner mit der Artikelbezeichnung des Switches (z. B. 852-1505_000-001).

Name	Änderungsdatum	Typ	Größe
 852-1505_000-001	22.05.2019 14:06	Dateiordner	

Abbildung 28: USB-Funktionen, Ordner anlegen

Hinweis



Name des Ordners

Der Name des Ordners muss immer ohne Sonderzeichen angelegt werden! Ersetzen Sie beim Anlegen des Ordners den Schrägstrich in der Artikelbezeichnung durch einen Unterstrich.

2. Kopieren Sie die neue Firmware-Datei in diesen Ordner.

Name	Änderungsdatum	Typ	Größe
 0030deff19b	23.05.2019 14:18	Dateiordner	
 852-1505_000-001-058-1.0.2.b5.fw	22.02.2019 17:10	FW-Datei	14.328 KB

Abbildung 29: USB-Funktionen, Firmware in Ordner

Hinweis



Inhalt des Ordners

In diesem Ordner darf sich nur eine Firmware-Datei befinden. Sind mehr als eine Firmware-Datei vorhanden, wird das Upload der Firmware abgebrochen.

3. Stecken Sie den USB-Stick in den USB-Anschluss des Switch.

- Die neue Firmware-Version wird automatisch auf den Switch übertragen. Während des Upload-Vorgangs blinkt die LED POST grün. Nach Abschluss des Upload-Vorgangs leuchtet die LED POST grün.

Hinweis



USB-Stick nicht entfernen!

Der USB-Stick darf während eines Firmware-Updates nicht herausgezogen werden.

Hinweis



Stromversorgung während des Updates nicht unterbrechen!

Die Stromversorgung darf während eines FW-Updates nicht unterbrochen werden.

7.5.7.2 Speichern der Konfigurationsdatei

- Stecken Sie den USB-Stick (Dateisystem FAT32) in den USB-Anschluss des Switch.
- Die Konfigurationsdatei wird automatisch auf den Stick übertragen. Während des Speicherns blinkt die Status-LED POST grün. Nach Abschluss des Speicherns leuchtet die Status-LED POST grün.

Configuration File Name Format: config_YYYYMMDDhhmmss.cfg

7.5.7.3 Speichern der Syslog-Datei

- Stecken Sie den USB-Stick (Dateisystem FAT32) in den USB-Anschluss des Switch.
- Die Syslog-Datei wird automatisch auf den Stick übertragen.

SYSLOG File Name Format: flash_YYYYMMDDhhmmss.log

Während des Speicherns blinkt die Status-LED POST grün.
Nach Abschluss des Speicherns leuchtet die Status-LED POST grün.

7.5.7.4 Upload der Konfigurationsdatei

Laden Sie die Konfigurationsdatei wie folgt auf den Switch:

- Erstellen Sie auf dem USB-Stick (Dateisystem FAT32) einen Ordner mit der Artikelbezeichnung des Switches (z. B. 852-1505_000-001).

Name	Änderungsdatum	Typ	Größe
 852-1505_000-001	22.05.2019 14:06	Dateiordner	

Abbildung 30: USB-Funktionen, Ordner anlegen

Hinweis**Name des Ordners**

Der Name des Ordners muss immer ohne Sonderzeichen angelegt werden! Ersetzen Sie beim Anlegen des Ordners den Schrägstrich in der Artikelbezeichnung durch einen Unterstrich.

2. Kopieren Sie die Konfigurationsdatei in diesen Ordner.

Name	Änderungsdatum	Typ	Größe
 config_20190523141835.cfg	23.05.2019 14:18	CFG-Datei	2 KB
 flash_20190523141835.log	23.05.2019 14:18	Textdokument	4 KB

Abbildung 31: USB-Funktionen, Konfigurationsdatei in Ordner

3. Stecken Sie den USB-Stick in den USB-Anschluss des Switch.
4. Die neue Version der Konfigurationsdatei wird automatisch auf den Switch übertragen.
Während des Upload-Vorgangs blinkt die Status-LED POST grün.
Nach Abschluss des Upload-Vorgangs leuchtet die Status-LED POST grün.

8 Konfigurieren

8.1 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“.

Konsolenport

Über den Konsolenport an der Vorderseite des Industrial-Managed-Switch (lokal) kann über einen integrierten Verwaltungsagenten das CLI („**C**ommand **L**ine Interface“) 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 Standard-Webbrowser 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“.

8.1.1 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 26: Default-Einstellungen für den Telnet-Port

Einstellung	Default-Wert
IP Address (IP-Adresse)	192.168.1.254
Subnet Mask (Subnetzmaske)	255.255.255.0
Default Gateway (Default-Gateway)	0.0.0.0
Management VLAN (Management-VLAN)	1
Default Username	admin
Default Password	wago

3. Vergewissern Sie sich, dass sich die IP-Adresse des Computers im selben Subnetz befindet – es sei denn, Sie greifen über einen oder mehrere Router auf den Switch zu.

8.2 Konsolen-Port

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 die Telnet mit folgenden Einstellungen:

Tabelle 27: 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 28: Anmeldebildschirm

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

9 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.

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 Web-Browser (z. B. Microsoft Internet-Explorer oder Mozilla Firefox).
2. Geben Sie in der Adresszeile die IP-Adresse des Feldbuskopplers/-controllers 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 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 29: Übersicht - Navigationslinks und WBM-Seiten

Navigationslinks und WBM-Seiten	
▶ [Systemstatus]	
	• Systeminformation
▶ [Grundeinstellungen]	
	• Allgemeine Einstellungen • MAC Management • Port-Spiegelung • Port-Einstellungen

► [Erweiterte Einstellungen]**[Bandbreiten-Regelung]**

- QoS
- Bandbreitenbegrenzung

[IGMP-Snooping]

- IGMP Snooping
- IGMP-Filter
- MVR
- Static Multicast
- Multicast Statistics

[VLAN]

- Port Isolation
- VLAN
- GVRP
- IP-Subnet-VLAN
- MAC VLAN
- Protokoll VLAN
- Q-in-Q
- DHCP Relay
- DHCP Options
- DHCP-Server
- Dual Homing
- Dual Ring
- ERPS
- Link Aggregation
- LLDP
- Loop Detection
- Jet Ring
- Modbus
- Static Route
- STP
- Xpress Ring

▶ [Security]
[IP Source Guard] • DHCP Snooping • Binding-Tabelle • ARP-Überprüfung • Access-Control-Liste • IEEE 802.1X • Port Security
▶ [Monitor]
• Alarm • Systeminformationen • Port-Statistik • Port-Auslastung • RMON-Statistiken • SFP-Informationen • Traffic-Monitor
▶ [Management]
[SNMP] • SNMP • SNMP Trap • SNMPv3 • Auto Provision • Mail-Alarm • Wartung • System Log • Ping • USB-Funktionen • Benutzerkonto • Open source License • Wago Licenses

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

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

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

9.1 Systemstatus

9.1.1 Systeminformationen

Systeminformation	
Systeminformation	
Modellname	852-1305/000-001
Host-Name	L2SWITCH
Boot Code Version	V1.3.9.S0
Current Running Firmware	Primary Firmware
Primary Firmware:	
Firmware-Version	V1.0.2.S0
Built Date	Mon Jun 17 12:58:41 CST 2019
Prüfsumme	563a5d97
Secondary Firmware:	
Firmware-Version	V1.0.2.S0
Built Date	Mon Mar 11 16:31:08 CST 2019
Prüfsumme	c2b02ce2
DHCP Client	Ausschalten
IP-Adresse	192.168.1.253
Subnet-Maske	255.255.255.0
Default Gateway	0.0.0.0
MAC-Adresse	00:30:de:ff:f1:8c
Seriennummer	00018A004194
Management VLAN	1
CPU-Auslastung	2 %
Speicherauslastung	Total: 514236 KB, Free: 464768 KB, Usage: 9.62 %
Aktuelle Uhrzeit	2000-6-6, 13:26:57
System Uptime	0 days, 0 hours, 9 minutes, 38 seconds
DHCPv6 Client	Ausschalten
Lokale IPv6-Adresse	fe80::230:deff:feff:f18c/64
IPv6 Default Gateway	
Globale IPv6-Adresse	
Aktualisieren	

Abbildung 32: WBM-Seite „Systeminformation“

Tabelle 30: WBM-Seite "Systeminformation"

Parameter	Beschreibung
Modellname	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
Host-Name	In diesem Anzeigefeld wird der Host-Name des Switches angezeigt.
Boot Code Version	In diesem Anzeigefeld wird die Boot Code Version angezeigt.
Current Running Firmware	Aktuell verwendete Firmware
Primary Firmware	
Firmware-Version	In diesem Anzeigefeld wird die Versionsnummer der aktuell installierten primären Firmware angezeigt.
Built Date	In diesem Anzeigefeld wird das Erstellungsdatum der aktuell installierten primären Firmware angezeigt.
Prüfsumme	In diesem Anzeigefeld wird die Prüfsumme der aktuell installierten primären Firmware angezeigt.
Secondary Firmware	
Firmware-Version	In diesem Anzeigefeld wird die Versionsnummer der aktuell installierten sekundären Firmware angezeigt.
Built Date	In diesem Anzeigefeld wird das Erstellungsdatum der aktuell installierten sekundären Firmware angezeigt.
Prüfsumme	In diesem Anzeigefeld wird die Prüfsumme der aktuell installierten sekundären Firmware angezeigt.
DHCP Client	In diesem Anzeigefeld wird angezeigt, ob die DHCP-Client-Funktion aktiviert ist.
IP-Adresse	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt.
Subnet-Maske	In diesem Anzeigefeld wird die Subnet-Maske des Switches angezeigt.
Default Gateway	In diesem Anzeigefeld wird das Default Gateway des Switches angezeigt.
MAC-Adresse	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 Anzeigefeld wird angezeigt, wie lange der Switch nach dem Einschalten läuft (Tage, Stunden, Minuten und Sekunden).
DHCPv6 Client	In diesem Anzeigefeld wird angezeigt, ob der DHCPv6 Client ein oder ausgeschaltet ist.
Lokale IPv6-Adresse	In diesem Anzeigefeld wird die lokale IPv6-Adresse angezeigt.
IPv6-Default Gateway	In diesem Anzeigefeld wird das Default Gateway des Switches angezeigt.
Globale IPv6-Adresse	In diesem Anzeigefeld wird angezeigt, ob auch die globale IPv6-Adresse mit eingegeben wurde.
Aktualisieren	Um die Informationen auf dieser Seite zu aktualisieren, klicken Sie diese Schaltfläche.

9.2 Grundeinstellungen

9.2.1 Allgemeine Einstellungen

9.2.1.1 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) and 'IPv4-Einstellungen' (IPv4 Settings). The 'Systemeinstellungen' section includes fields for 'Hostname' (set to 'L2SWITCH') and 'Management VLAN' (set to '1'). The 'IPv4-Einstellungen' section includes a 'DHCP Client' dropdown (set to 'Ausschalten') with an 'Aktualisieren' button, and fields for 'IP-Adresse' (192.168.1.254), 'Subnet-Maske' (255.255.255.0), and 'Default Gateway' (0.0.0.0). Below these are the 'IPv6-Einstellungen' (IPv6 Settings) section, which includes a 'DHCPv6 Client' dropdown (set to 'Ausschalten') with an 'Aktualisieren' button, a 'Globale IPv6-Adresse' field, and a 'Default Gateway' dropdown (set to 'Gesetzt') with an empty input field. At the bottom of the page are three buttons: 'Anwenden', 'Aktualisieren', and 'Konfiguration speichern'.

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

Abbildung 33: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

Tabelle 31: 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	192.168.1.254	Geben Sie im Eingabefeld die IP-Adresse des Switches in Dezimalpunktschreibweise ein.
Subnet-Maske	255.255.255.0	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.

9.2.1.2 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 Setting

Port		Jumbo Frame
From:	1 ▼	to: 1 ▼
		10240 ▼
Apply Refresh		

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

Abbildung 34: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“

Tabelle 32: 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	

9.2.1.3 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

at

0

o'clock

Endzeitpunkt

Erster

Sonntag

of

Januar

at

0

o'clock

Anwenden

Aktualisieren

Konfiguration speichern

Abbildung 35: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“

Tabelle 33: 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 33: 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).	

9.2.1.4 Management-Host

Hinweis**Weitere Information**

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

Allgemeine Einstellungen

System Jumbo Frame SNTP **Management Host**

Management-Host-Einstellungen

Management Host: Subnet-Maske:

Anwenden Aktualisieren Konfiguration speichern

Management-Host-Liste

Nr.	Management Host (IP/Mask)	Aktion
1	192.168.1.3/1	Löschen

Abbildung 36: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“

Tabelle 34: 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.

9.2.2 MAC Management

Hinweis



Weitere Information

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

9.2.2.1 Statische MAC-Einstellungen

Hinweis



Weitere Information

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

The screenshot displays the 'MAC Management' web interface. At the top, there are four tabs: 'Statische MAC-Einstellungen' (selected), 'MAC-Tabelle', 'Age-Time-Einstellung', and 'Blacklisting'. Below the tabs, the 'Statische MAC-Einstellungen' section contains three input fields: 'MAC-Adresse', 'VLAN ID', and 'Port'. The 'Port' field is a dropdown menu currently showing '1'. Below these fields are three buttons: 'Anwenden', 'Aktualisieren', and 'Konfiguration speichern'. Below this section is the 'Statische MAC-Tabelle' which contains a table with the following data:

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

At the bottom right of the table, it says 'Anzahl der Einträge : 1'.

Abbildung 37: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“

Tabelle 35: 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.

9.2.2.2 MAC-Tabelle

MAC Management

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

MAC-Tabelle

Typ anzeigen

Alle ▼

Anwenden

Aktualisieren

Löschen

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

Anzahl der Einträge : **3**

Seite hoch

Seite runter

Seite: 1/1

Seite: 1

Anwenden

Abbildung 38: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“

Tabelle 36: 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.

9.2.2.3 Age-Time-Einstellung

Abbildung 39: WBM-Seite „MAC Management“ – Register „Age-Time-Einstellung“

Tabelle 37: „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“ (Löschzeit) ein. Gültiger Bereich: 0 oder 20 ... 400 s.

9.2.2.4 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.

Abbildung 40: WBM-Seite „MAC Management“ – Register „Blacklisting“

Tabelle 38: 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.

9.2.3 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 41: WBM-Seite „Port-Spiegelung“

Tabelle 39: 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.

9.2.4 Port-Einstellungen

9.2.4.1 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 42: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“

Tabelle 40: 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.

9.2.4.2 Informationen

Port-Einstellungen

Allgemeine Einstellungen **Informationen**

Port-Einstellungen

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

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 43: WBM-Seite „Port-Einstellungen“ – Register „Informationen“

Tabelle 41: 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

9.3 Erweiterte Einstellungen

9.3.1 Bandbreiten-Regelung

9.3.1.1 QoS

Hinweis



Weitere Information

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

9.3.1.1.1 Port-Priorität

Abbildung 44: WBM-Seite „QoS“ – Register „Port-Priorität“

Tabelle 42: WBM-Seite „QoS“ – Register „Port-Priorität“

Port-Prioritäts-Einstellungen		
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-Priorität“ wird die hier angegebene Priorität zugewiesen.

9.3.1.1.2 IP-DiffServ (DSCP)

QoS

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

DSCP-Einstellungen

Modus

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

Tabelle 43: 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

9.3.1.1.3 Priorität/Queue-Zuordnung

Abbildung 46: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“

Tabelle 44: 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 45: Default-Einstellungen

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

9.3.1.1.4 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 47: WBM-Seite „QoS“ – Register „Schedule-Modus“

Tabelle 46: 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. Dann können Sie „Strict Priority Queuing (SPQ)“ ändern.

9.3.1.2 Bandbreitenbegrenzung

9.3.1.2.1 Sturmbegrenzung

Hinweis**Weitere Information**

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

Bandbreitenbegrenzung

Sturmbegrenzung **Bandbreitenbegrenzung**

Sturmbegrenzungseinstellungen

Bandbreitenbegrenzungs-Mode

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

Deaktivieren:0. Eine Einheit ist ca. 652 pps

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 48: WBM-Seite „Bandbreitenbegrenzung“ – Register „Sturmbegrenzung“

Tabelle 47: WBM-Seite „Rate Limitation“ – Register „Broadcast-Sturmkontrolle“

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.

9.3.1.2.2 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)

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 49: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“

Tabelle 48: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“

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

9.3.2 IGMP Snooping

Hinweis



Weitere Information

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

9.3.2.1 IGMP Snooping

9.3.2.1.1 Allgemeine Einstellungen

IGMP Snooping

Allgemeine Einstellungen
Port-Einstellungen
Querier-Einstellungen

IGMP-Snooping-Einstellungen

IGMP-Snooping-Status

Ausschalten ▾

Status der Berichtsunterdrückung

Ausschalten ▾

IGMP-Snooping-VLAN-Status

Hinzufügen ▾

Unbekannte Multicast-Pakete

Verwerfen ▾

Anwenden
Aktualisieren
Konfiguration speichern

IGMP-Snooping-Status

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

Abbildung 50: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“

Tabelle 49: 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.
Status der Bereichsunterdrückung	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Status der Bereichsunterdrückung“ beim „IGMP Snooping“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Status der Bereichsunterdrückung“ beim „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.
Status der Bereichsunterdrückung	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob die Funktion „Status der Bereichsunterdrückung“ beim „IGMP Snooping“ aktiviert oder deaktiviert ist.
IGMP-Snooping-VLAN-Status	Keine 1 ... 4094	In diesem Anzeigefeld werden die VLANs angezeigt, in denen der Switch „IGMP Snooping“ ausführt. Es wird „Keine“ 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.

9.3.2.1.2 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 51: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“

Tabelle 50: 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.

9.3.2.1.3 Querier-Einstellungen

IGMP Snooping

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

Querier-Einstellungen

Querier-Status: **Ausschalten** ▼

Querier-VLAN-Status: **Hinzufügen** ▼

Anwenden Aktualisieren Konfiguration speichern

Querier Status

Querier-Status	Ausschalten
Querier-VLAN-Status	Keine

Abbildung 52: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“

Tabelle 51: 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 VLAN-ID einzugeben.
	Löschen	Wählen Sie im Auswahlfeld „Löschen“, um 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.

9.3.2.2 IGMP-Filter

9.3.2.2.1 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 53: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“

Tabelle 52: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“

IGMP-Filtering-Einstellungen		
Parameter	Standardwert	Beschreibung
IGMP Filtering State	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.

9.3.2.2.2 Multicast-Gruppem

IGMP-Filter

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

Gruppeneinstellung

Profil :

Gruppen	Startadresse	Endadresse
1 ↓		

Gruppenstatus

Profil	Typ	Gruppen	Startadresse	Endadresse	Aktion

Abbildung 54: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“

Tabelle 53: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“

Gruppeneinstellung		
Parameter	Standardwert	Beschreibung
Profil		Wählen Sie im Auswahlfeld das Profil aus, das Sie für eine Gruppe konfigurieren möchten.
Gruppen	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.
Gruppen	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.

9.3.2.2.3 Port-Einstellungen

IGMP-Filter

[Allgemeine Einstellungen](#)
[Multicast-Gruppen](#)
[Port-Einstellungen](#)

Port-Einstellungen

Profil :

Port

☐ Alle auswählen
 ☒ Alle deaktivieren

☐ 1 ☐ 3 ☐ 5 ☐ 7 ☐ 9
☐ 2 ☐ 4 ☐ 6 ☐ 8 ☐ 10

Port-status

Profil	Typ	Ports

Abbildung 55: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“

Tabelle 54: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“

Tabellensicht: WDM Seite „GWI“ 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 ...	☐	☐	Der Port ist nicht aktiviert..	
	☐ 10 (12)		☒	Der Port ist 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.

9.3.2.3 Multicast-VLAN-Registrierung

Hinweis



Weitere Information

Weitere Informationen zu „**Multicast-VLAN-Registration**“ (MVR) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.2.3.1 MVR-Einstellungen

Multicast-VLAN-Registrierung

MVR-Einstellungen
Gruppeneinstellungen

MVR-Einstellungen

VLAN ID

Name

Priority Override Ausschalten

Status Einschalten

Modus Dynamisch

IEEE802.1p-Priorität 0

Source Ports (ex. 1,3,5-8)

Receiver Ports (ex. 1,3,5-8)

Tagged Ports (ex. 1,3,5-8)

Anwenden
Aktualisieren
Konfiguration speichern

MVR-Status

VLAN ID	3	Name	Floor1	Priority override	Ausschalten
Status	Ausschalten	Modus	Dynamisch	IEEE802.1p-Priorität	0
Source Ports	Keine				
Receiver Ports	Keine				
Tagged Ports	Keine				

Löschen

Abbildung 56: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „MVR-Einstellungen“

Tabelle 55: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „MVR-Einstellungen“

MVR-Einstellungen		
Parameter	Standardwert	Beschreibung
VLAN ID		Geben Sie im Eingabefeld die VLAN ID ein.
Name		Geben Sie im Eingabefeld den Namen für die MVR ein.
Priority Override	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die MVR zu aktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die MVR zu deaktivieren.
Modus	Dynamisch	Wählen Sie im Auswahlfeld „Dynamisch“, um den dynamischen Modus für die MVR zu konfigurieren.
	Kompatibel	Wählen Sie im Auswahlfeld „Kompatibel“, um den kompatiblen Modus für die MVR zu konfigurieren.
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 „802.1p Tag-Priorität“ wird die hier angegebene Priorität zugewiesen.
Source Ports	1 ... 8	Geben Sie im Eingabefeld den Source Port oder Source-Port-Bereich für die MVR ein. Normalerweise sind die Source Ports mit dem „Streaming Server“ verbunden.
Receiver Ports	1 ... 8	Geben Sie im Eingabefeld den Receiver Port oder Receiver-Port-Bereich für die MVR ein. Normalerweise sind die Receiver Ports mit dem „Streaming Client“ verbunden.
Tagged Ports	1 ... 8	Geben Sie im Eingabefeld den Port mit Tag oder Port-Bereich mit Tags für die MVR ein. Gleiches gilt für VLAN Ports mit Tag.
MVR-Status		
Parameter	Standardwert	Beschreibung
VLAN ID		In diesem Anzeigefeld wird die VLAN ID angezeigt.
Name		In diesem Anzeigefeld wird der von Ihnen gewählte Name angezeigt.
Priority override	Ausschalten Einschalten	In diesem Anzeigefeld wird der Status angezeigt.
Status	Ausschalten Einschalten	In diesem Anzeigefeld wird der Status des MVR angezeigt.
Modus	Dynamisch Kompatibel	In diesem Anzeigefeld wird der Modus des MVR angezeigt.
IEEE 802.1p-Priorität	0 ... 7	In diesem Anzeigefeld wird die von Ihnen gewählte Priorität für die Pakete angezeigt.
Source Ports	1 ... 8	In diesem Anzeigefeld wird der Source Port oder Source-Port-Bereich für die MVR angezeigt.
Receiver Ports	1 ... 8	In diesem Anzeigefeld wird der Receiver Port oder Receiver-Port-Bereich für die MVR angezeigt.
Tagged Ports	1 ... 8	In diesem Anzeigefeld wird der Port mit Tag oder Port-Bereich mit Tags für die MVR angezeigt.

9.3.2.3.2 Gruppeneinstellungen

Abbildung 57: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „Gruppeneinstellungen“

Tabelle 56: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „Gruppeneinstellungen“

Gruppeneinstellungen		
Parameter	Standardwert	Beschreibung
MRV VLAN		Wählen Sie im Auswahlfeld die Anzahl der MVR VLAN aus.
Gruppenname		Geben Sie im Eingabefeld den Gruppennamen für die MVR ein.
Startadresse		Geben Sie im Eingabefeld die Multicast-Startadresse ein.
Menge		Geben Sie im Eingabefeld die Anzahl der Multicast-Adressen ein.
Gruppenstatus		
Parameter	Standardwert	Beschreibung
MRV VLAN		In diesem Anzeigefeld wird die Anzahl der MVR VLAN angezeigt.
Gruppenname		In diesem Anzeigefeld wird der von Ihnen gewählte Gruppenname angezeigt.
Adressbereich		In diesem Anzeigefeld wird Multicast-Startadresse angezeigt.
Löschen		Klicken Sie auf [Löschen] , um diese Einstellung zu löschen.
Gesamte Gruppe löschen		Klicken Sie auf [Gesamt Gruppe löschen] , um die Einstellungen der gesamten Gruppe zu löschen.

9.3.2.4 Static Multicast

Hinweis



Weitere Information

Weitere Informationen zu „Static Multicast“ finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 58: WBM-Seite „Static Multicast“

Tabelle 57: WBM-Seite „Static Multicast“

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.

9.3.2.5 Multicast Statistics

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 59: WBM-Seite „Multicast Statistics“

Tabelle 58: WBM-Seite „Multicast Statistics“

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.
VID		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.

9.3.3 VLAN

Hinweis



Weitere Information

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

9.3.3.1 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

	Egress Port												
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 60: WBM-Seite „Port Isolation“

Tabelle 59: WBM-Seite „Port Isolation“

Tabellensatz: WDM: 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.	
Egress Port			Ein Egress Port ist ein ausgehender Port, über den ein Datenpaket gesendet wird. Die Auswahl eines Ports als Egress Port bedeutet, dass er mit dem Port, den Sie gerade konfigurieren, kommunizieren wird.	
	Alle auswählen	☐	☐	Es ist kein Egress Port ausgewählt.
			☒	Es sind alle Egress Ports ausgewählt.
	Alle deaktivieren	☐	☐	Es ist kein Egress Port deaktiviert.
			☒	Es sind alle Egress Ports deaktiviert.
	☐ 0 (CPU) ... ☐ 10 (12)	☐	☐	Der Egress Port ist nicht aktiviert.
			☒	Der Egress 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.
Egress Port			-	„-“ zeigt an, dass die Pakete des Ports nicht zu diesem Port gesendet werden können.

9.3.3.2 VLAN

9.3.3.2.1 VLAN-Einstellungen

VLAN

VLAN-Einstellungen

Tag-Einstellungen

Port-Einstellungen

VLAN-Einstellungen

VLAN ID		VLAN Name	Member Port
von:		an:	

Anwenden

Aktualisieren

Konfiguration speichern

VLAN List

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

Abbildung 61: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“

Tabelle 60: 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.
Member 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 List			
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.
Member 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.

9.3.3.2.2 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 62: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“

Tabelle 61: 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.	

9.3.3.2.3 Port-Einstellungen

VLAN

VLAN-Einstellungen
Tag-Einstellungen
Port-Einstellungen

Port-Einstellungen

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

Anwenden
Aktualisieren
Konfiguration speichern

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 63: WBM-Seite „VLAN“ – Register „Port-Einstellungen“

Tabelle 62: 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.
Acceptable Frame			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.
		Untagged Frame	Wählen Sie im Auswahlfeld „untagged Frame“, wenn an diesem Port nur Frames ohne Tag akzeptiert werden sollen. Alle Frames mit Tag werden verworfen.
		tagged Frame	Wählen Sie im Auswahlfeld „tagged Frame“, 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.
Acceptable Frame		Alle untagged Frame tagged Frame	In dieser Spalte werden die für diesen Port zulässigen Frame-Typen angezeigt.

9.3.3.3 GARP VLAN Registration Protocol

Hinweis**Weitere Information**

Weitere Informationen zu „GARP/GVRP“ (**G**eneric **A**tttribute **R**egistration **P**rotocol/**G**ARP **V**LAN **R**egistration **P**rotocol oder **G**eneric **V**LAN **R**egistration **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.3.3.1 GVRP

GARP VLAN Registration Protocol

GVRP

GARP Timer

GVRP-Einstellungen

GVRP-Status

Ausschalten ▼

Port	Status	Registration Mode
von: 1 ▼ an: 1 ▼	Einschalten ▼	Verboten ▼

Anwenden
Aktualisieren
Konfiguration speichern

GVRP-Status

Port	Status	Registration Mode	Port	Status	Registration Mode
1	Einschalten	Verboten	2	Ausschalten	-
3	Ausschalten	-	4	Ausschalten	-
5	Ausschalten	-	6	Ausschalten	-
7	Ausschalten	-	8	Ausschalten	-
9	Ausschalten	-	10	Ausschalten	-
11	Ausschalten	-	12	Ausschalten	-

Abbildung 64: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GVRP“

Tabelle 63: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GVRP“

GVRP-Einstellungen		
Parameter		Standardwert
		Beschreibung
GVRP-Status		Ausschalten
		Wählen Sie im Auswahlfeld „Ausschalten“, um die „GVRP“-Funktion zu deaktivieren.
		Einschalten
		Wählen Sie im Auswahlfeld „Einschalten“, um die „GVRP“-Funktion zu aktivieren und die VLAN-Konfigurationsinformationen mit anderen GVRP-Switches auszutauschen.
Port	von:	1
	an:	1
		Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, bei dem Sie die GVRP-Einstellungen konfigurieren möchten.
		Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, bei dem Sie die GVRP-Einstellungen konfigurieren möchten.
Status		Ausschalten
		Wählen Sie im Auswahlfeld „Ausschalten“ zur Deaktivierung der „GVRP“-Funktion für den Port.
		Einschalten
		Wählen Sie im Auswahlfeld „Einschalten“ zur Aktivierung der „GVRP“-Funktion für den Port.
Registration Mode		Normal
		Wählen Sie im Auswahlfeld „Normal“, um die dynamische Erstellung (sofern dynamische VLAN-Erstellung aktiviert ist), Anmeldung und Abmeldung von VLANs am Trunk-Port zuzulassen.
		Verboten
		Wählen Sie im Auswahlfeld „Verboten“, um alle VLANs (außer VLAN 1) abzumelden und jede weitere Erstellung oder Anmeldung von VLANs am „Trunk Port“ zu verhindern.
GVRP-Status		
Parameter		Standardwert
		Beschreibung
Port		1 ... 10 (12)
		In dieser Spalte werden die Port-Nummern angezeigt.
Status		Ausschalten Einschalten
		In dieser Spalte wird der eingestellte Status angezeigt.
Registration Mode		Normal Verboten
		In dieser Spalte wird der ausgewählte Registration Mode angezeigt.

9.3.3.3.2 GARP Timer**Hinweis****Größe der Werte für „join“, „leave“ und „leave all“**

Der Wert für „leave“ muss größer sein als der dreifache Wert für „join“ (leave $\geq$ join x 3).

Der Wert für „leave all“ muss größer sein als der Wert für „leave“ (leave all $>$ leave).

GARP VLAN Registration Protocol

GVRP
GARP Timer

GARP-Timer-Einstellungen

Port	Join Time	Leave Time	Leave All Time
von: 1 ▼ an: 1 ▼	20	60	1000

2*Join Time < Leave Time < Leave All Time
Zeiteinheit:(centi-sec)

Anwenden
Aktualisieren
Konfiguration speichern

GARP-Timer-Status

Port	Join Time	Hold Time	Leave Time	Leave All Time
1	20	10	60	1000
2	20	10	60	1000
3	20	10	60	1000
4	20	10	60	1000
5	20	10	60	1000
6	20	10	60	1000
7	20	10	60	1000
8	20	10	60	1000
9	20	10	60	1000
10	20	10	60	1000
11	20	10	60	1000
12	20	10	60	1000

Abbildung 65: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GARP Timer“

Tabelle 64: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GARP Timer“

GARP Timer			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um den GARP Timer zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um den GARP Timer zu konfigurieren.
Join Time		20	Geben Sie im Eingabefeld die maximale Zeit in Millisekunden ein, die die Schnittstelle wartet, bevor sie mit dem Senden von VLAN-Meldungen beginnt.
Leave Time		60	Geben Sie im Eingabefeld die maximale Zeit in Millisekunden ein, die die Schnittstelle nach dem Empfang einer „Leave Message“ wartet, bevor die Schnittstelle das in der Meldung spezifizierte VLAN verlässt.
Leave All Time		1000	Geben Sie im Eingabefeld das Zeitintervall in Millisekunden ein, nach dem Leave-all-Meldungen an Schnittstellen gesendet werden. Leave-all-Meldungen können dabei helfen, Informationen über die derzeitigen GVRP-VLAN-Mitgliedschaften im Netzwerk zu aktualisieren.
GARP-Timer-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Join Time			In dieser Spalte wird die Join Time angezeigt.
Hold Time			In dieser Spalte wird die Hold Time angezeigt.
Leave Time			In dieser Spalte wird die Leave Time angezeigt.
Leave All Time			In dieser Spalte wird die Leave All Time angezeigt.

9.3.3.5 MAC VLAN

Hinweis



Weitere Information

Weitere Informationen zu „MAC VLAN“ (**M**edia **A**ccess **C**ontrol-**V**irtual **L**ocal **A**rea **N**etwork) 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 67: WBM-Seite „MAC VLAN“

Tabelle 66: 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.

9.3.3.6 Protokoll VLAN

Protokoll VLAN					
MAC-VLAN-Einstellungen					
Frame Type	Ethernet Type	VLAN	Port-Liste		
EthernetII ▼					
Anwenden Aktualisieren Konfiguration speichern					
Protokoll VLAN-Tabelle					
Index	Frame Type	Ethernet Type	VLAN	Port-Liste	Aktion

Abbildung 68: WBM-Seite „Protokoll VLAN“

Tabelle 67: WBM-Seite „Protokoll VLAN“

MAC-VLAN-Einstellungen		
Parameter	Standardwert	Beschreibung
Frame Type	ETHERNETII	Wählen Sie im Auswahlfeld „ETHERNETII“, wenn Sie diesen Frame-Typ konfigurieren möchten.
	NonLLC-SNAP	Wählen Sie im Auswahlfeld „NonLLC-SNAP“, wenn Sie diesen Frame-Typ konfigurieren möchten.
	LLC-SNAP	Wählen Sie im Auswahlfeld „LLC-SNAP“, wenn Sie diesen Frame-Typ konfigurieren möchten.
ETHERNET Type		Geben Sie im Eingabefeld den ETHERNET-Typ ein. (z. B. 0800)
VLAN	1 ... 4094	Geben Sie im Eingabefeld die VLAN ID ein. Gültiger Bereich: 1 ... 4094
Port-Liste	1 ... 10 (12)	Geben Sie im Eingabefeld den Port oder die Port-Gruppe (z. B. 1 – 3) für die Protokoll-VLAN ein
Protokoll-VLAN-Tabelle		
Parameter	Standardwert	Beschreibung
Index		In dieser Spalte wird die Anzahl der Einträge angezeigt.
Frame Type		In dieser Spalte wird der Frame-Typ angezeigt.
ETHERNET Type		In dieser Spalte wird der ETHERNET-Typ angezeigt.
VLAN		In dieser Spalte wird die VLAN-ID angezeigt.
Port-Liste		In dieser Spalte wird die Port-Liste angezeigt.
Aktion		Klicken Sie auf [Löschen] , um die Multicast-Adressen zu löschen.

9.3.3.7 Q-in-Q

Hinweis



Weitere Information

Weitere Informationen zu „Q-in-Q“ finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.3.7.1 VLAN Stacking

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

VLAN-Stacking-Einstellungen

Aktion Ausschalten ▾

Tunnel TPID Index	TPID
1 (Default) ▾	8100 (0000~ffff)

Port	Tunnel TPID Index
von: 1 ▾ an: 1 ▾	1 (Default) ▾

Anwenden
Aktualisieren
Konfiguration speichern

VLAN-Stacking-Status

Tunnel TPID Index	TPID
1	8100
2	8100
3	8100
4	8100
5	8100
6	8100

Port	Tunnel TPID Index (TPID)	Port	Tunnel TPID Index (TPID)
1	1 (8100)	2	1 (8100)
3	1 (8100)	4	1 (8100)
5	1 (8100)	6	1 (8100)
7	1 (8100)	8	1 (8100)
9	1 (8100)	10	1 (8100)
11	1 (8100)	12	1 (8100)

Abbildung 69: WBM-Seite „Q-in-Q“ – Register „VLAN Stacking“

Tabelle 68: WBM-Seite „Q-in-Q“ – Register „VLAN Stacking“

VLAN-Stacking-Einstellungen			
Parameter		Standardwert	Beschreibung
Aktion		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „VLAN Stacking“ zu deaktivieren.
		Port-based	Wählen Sie im Auswahlfeld „Port-based“, um die Funktion „VLAN Stacking“ portbasiert auszuführen.
		Selektiv	Wählen Sie im Auswahlfeld „Selektiv“, um die Funktion „VLAN Stacking“ selektiv auszuführen.
Tunnel TPID Index		1 (Default) ... 6	Wählen Sie im Auswahlfeld eine Tabellenindexnummer aus.
TPID (0000~ffff)			Geben Sie im Eingabefeld einen Wert für die TPID. Gültiger Bereich: 0000 ... ffff
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „VLAN Stacking“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „VLAN Stacking“ zu konfigurieren.
Tunnel TPID Index		1 (Default) ... 6	Wählen Sie im Auswahlfeld einen „Tunnel TPID Index“ aus.
VLAN-Stacking-Status			
Parameter		Standardwert	Beschreibung
Tunnel TPID Index		1 ... 6	In dieser Spalte wird die Tabellenindexnummer angezeigt.
TPID		0000 ... ffff	In dieser Spalte wird die TPID angezeigt.
Port		1 ... 10 (12)	In dieser Spalte wird die Port-Nummer angezeigt.
Tunnel TPID Index (TPID)			In dieser Spalte wird die Indexnummer für den spezifischen Port angezeigt.

9.3.3.7.2 Port-based Q-in-Q

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Port-basiertes Q-in-Q

Port	Role	SPVID	Priorität
von: 1 an: 1	Normal	1 (1~4094)	0

Port-basierter Q-in-Q-Status

Port	Role	SPVID	Priorität	Port	Role	SPVID	Priorität
1	Normal	1	0	2	Normal	1	0
3	Normal	1	0	4	Normal	1	0
5	Normal	1	0	6	Normal	1	0
7	Normal	1	0	8	Normal	1	0
9	Normal	1	0	10	Normal	1	0
11	Normal	1	0	12	Normal	1	0

Abbildung 70: WBM-Seite „Q-in-Q“ – Register „Port-based Q-in-Q“

Tabelle 69: WBM-Seite „Q-in-Q“ – Register „Port-based Q-in-Q“

Port-basiertes Q-in-Q			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „O-in-Q“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „O-in-Q“ zu konfigurieren.
Role		Normal	Wählen Sie im Auswahlfeld „Normal“, um diese Role für den spezifischen Port auszuwählen.
		Access	Wählen Sie im Auswahlfeld „Access“, um diese Role für den spezifischen Port auszuwählen.
		Tunnel	Wählen Sie im Auswahlfeld „Tunnel“, um diese Role für den spezifischen Port auszuwählen.
SPVID (1~4094)		1	Geben Sie im Eingabefeld das Dienstanbieter-VLAN „SPVID“ ein. Gültiger Bereich: 1 ... 4094
Priorität		0 ... 7	Wählen Sie im Auswahlfeld die jeweilige Priorität für den spezifischen Port aus. 0 = niedrigste Priorität 7 = höchste Priorität
Port-basierter Q-in-Q-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte wird die Port-Nummer angezeigt.
Role			In dieser Spalte wird die Rolle des spezifischen Ports angezeigt.
SPVID			In dieser Spalte wird die SPVID angezeigt.
Priorität			In dieser Spalte wird die Priorität für den spezifischen Port angezeigt.

9.3.3.7.3 Selektive Q-in-Q

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Selective Q-in-Q-Einstellungen

Name

Access-Ports (ex. 1,3,5-6)

Tunnel-Ports (ex. 1,3,5-6)

CVID (Bereich: 1~4094)

SPVID (Bereich: 1~4094)

Priorität ▼

Aktion ▼

Selectiver Q-in-Q-Status

Nr.	Name	Access-Ports	Tunnel-Ports	CVID	SPVID	Priorität	Aktion	Ausschalten
1	Floor1	2	3	1	1	0	Einschalten	Löschen

Abbildung 71: WBM-Seite „Q-in-Q“ – Register „Selektive Q-in-Q“

Tabelle 70: WBM-Seite „Q-in-Q“ – Register „Selektive Q-in-Q“

Selektive Q-in-Q-Einstellungen		
Parameter	Standardwert	Beschreibung
Name		Geben Sie im Eingabefeld den Namen für das selektive Q-in-Q-Profil ein.
Access-Ports (ex. 1,3,5-6)		Geben Sie im Eingabefeld den Access-Port oder Access-Port-Bereich ein.
Tunnel-Ports (ex. 1,3,5-6)		Geben Sie im Eingabefeld den Tunnel-Port oder Tunnel-Port-Bereich ein.
CVID (Bereich: 1~4094)		Geben Sie im Eingabefeld ein Kunden-VLAN „CVID“ ein. Gültiger Bereich: 1 ... 4094
SPVID (Bereich: 1~4094)		Geben Sie im Eingabefeld ein Dienstanbieter-VLAN „SPVID“ ein. Gültiger Bereich: 1 ... 4094
Priorität	0 ... 7	Wählen Sie im Auswahlfeld die jeweilige Prioritätsebene aus. 0 = niedrigste Priorität 7 = höchste Priorität
Aktion	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Selektiver Q-in-Q Status		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Index-Nr. angezeigt.
Name		In dieser Spalte wird der Name des selektiven Q-in-Q-Profiles angezeigt.
Access-Ports		In dieser Spalte wird der Access-Port angezeigt.
Tunnel-Ports		In dieser Spalte wird der Tunnel-Port angezeigt.
CVID		In dieser Spalte wird das Kunden-VLAN „CVID“ angezeigt.
SPVID		In dieser Spalte wird das Dienstanbieter-VLAN „SPVID“ angezeigt.
Priorität	0 ... 7	In dieser Spalte wird die jeweilige Prioritätsebene angezeigt. 0 = niedrigste Priorität 7 = höchste Priorität
Aktion	Ausschalten Einschalten	In dieser Spalte wird die gewählte Aktion angezeigt.
Ausschalten		Klicken Sie auf [Löschen] , um die Selektiven Q-in-Q-Einstellungen zu löschen.

9.3.4 DHCP Relay

Hinweis



Weitere Information

Weitere Informationen zu „DHCP Relay“ (**D**ynamic **H**ost **C**onfiguration **P**rotocol **R**elay) finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 72: WBM-Seite „DHCP Relay“

Tabelle 71: WBM-Seite „DHCP Relay“

DHCP-Relay-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um „DHCP Relay“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „DHCP Relay“ zu aktivieren.
VLAN-Status	Ergänzen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, bei denen der Switch „DHCP Relay“ 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 „DHCP Relay“ ausführen soll.
DHCP-Server-IP	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse des DHCP-Servers ein.
DHCP-Relay-Status		
Parameter	Standardwert	Beschreibung
DHCP-Relay-Status	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob „DHCP Relay“ aktiviert oder deaktiviert ist.
Aktiviert auf VLAN	Keiner 0 ... 4094	In diesem Anzeigefeld wird angezeigt, ob ein VLAN benutzt wird.
DHCP-Server-IP		In diesem Anzeigefeld wird die IP-Adresse des DHCP-Servers angezeigt.

9.3.5 DHCP Options

Hinweis



Weitere Information

Weitere Informationen zu „DHCP Options“ finden Sie im Kapitel „Funktionsbeschreibung“.

DHCP Options

DHCP-Option-82-Einstellungen

Option-82-Status

Einschalten ▾

Option 82 Frame

1

Option 82 Shelf

0

Option 82 Slot

0

Circuit-ID String

%HOSTNAME+%SPACE+eth/+%FRAME/+%SHELF/+%SLOT+:+%PORT+

Remote-ID Form

%HOSTNAME+%SPACE+eth/+%FRAME/+%SHELF/+%SLOT+:+%PORT+

Option-82-Command-Status

Port

1 ▾

Option-82-Status

Einschalten ▾

Circuit-ID String

Remote-ID String

Anwenden

Aktualisieren

Konfiguration speichern

Option-82-Command-Status

Port 1

Option 82 State

Enable

Circuit-ID String

Remote-ID String

Port 2

Option 82 State

Disable

Circuit-ID String

Remote-ID String

Abbildung 73: WBM-Seite „DHCP Options“

Tabelle 72: WBM-Seite „DHCP Options“

DHCP-Option-82-Einstellungen		
Parameter	Standardwert	Beschreibung
Option-82-Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „DHCP Option 82“ beim Switch zu deaktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um „DHCP Option 82“ beim Switch zu aktivieren.
Option 82 Frame	1	Geben Sie im Eingabefeld die gewünschte Frame-Nummer ein.
Option 82 Shelf	0	Geben Sie im Eingabefeld die gewünschte Shelf-Nummer ein, um den Switch eindeutig zu identifizieren.
Option 82 Slot	0	Geben Sie im Eingabefeld die gewünschte Slot-Nummer ein, um den Switch eindeutig zu identifizieren.
Circuit-ID String	%HOSTNAME+ %SPACE+eth/+ %FRAME+/% SHELF+/%SL OT+:%PORT+ _+%SVLAN+:+ %CVLAN	In diesem Eingabefeld haben Sie die Möglichkeit, den angefügten String anzupassen.
Remote-ID Form	%HOSTNAME+ %SPACE+eth/+ %FRAME+/% SHELF+/%SL OT+:%PORT+ _+%SVLAN+:+ %CVLAN	In diesem Eingabefeld haben Sie die Möglichkeit, den angefügten String anzupassen.
Option-82-Command-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	Wählen Sie im Auswahlfeld einen Port aus.
Option-82-Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „Option 82 Command State“ beim Switch zu deaktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um „Option 82 Command State“ beim Switch zu aktivieren.
Circuit-ID String		Geben Sie im Eingabefeld den „Circuit-ID String“ ein.
Remote-ID String		Geben Sie im Eingabefeld den „Remote-ID String“ ein.
Option-82-Command-Status		
Parameter	Standardwert	Beschreibung
Port 1 ... 10 (12)		In diesem Anzeigefeld werden die Port-Nummern angezeigt.
Option-82-Status		In diesem Anzeigefeld wird der „Option-82-Status“ angezeigt.
Circuit-ID String		In diesem Anzeigefeld wird der „Circuit-ID String“ angezeigt.
Remote-ID String		In diesem Anzeigefeld wird der „Remote-ID String“ angezeigt.

9.3.6 DHCP-Server

Hinweis



Weitere Information

Weitere Informationen zum „DHCP-Server“ finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.6.1 Allgemeine Einstellungen

The screenshot shows the 'DHCP-Server' configuration interface. At the top, there's a title bar 'DHCP-Server' and four tabs: 'Allgemeine Einstellungen' (selected), 'Pool-Einstellungen', 'Binding Information', and 'Statistics'. Below the tabs, the 'Allgemeine Einstellungen' section contains several configuration fields: 'Status' (dropdown menu set to 'Ausschalten'), 'Offer Reuse Timeout' (text input '5' with a note '(Bereich: 1~120)'), 'Nächste Server-Adresse' (text input '0.0.0.0'), 'Boot File Name' (empty text input), 'Echo ICMP Mode' (dropdown menu set to 'Ausschalten'), and 'Globale Option' (dropdown menu set to 'Keine', with a secondary dropdown set to 'Ascii' and an empty text input). At the bottom of this section are three buttons: 'Anwenden', 'Aktualisieren', and 'Konfiguration speichern'. Below this is a section titled 'Globaler Option-Status' which contains a table with two columns: 'Option' and 'Option-Wert'.

Option	Option-Wert

Abbildung 74: WBM-Seite „DHCP-Server“ – Register „Allgemeine Einstellungen“

Tabelle 73: WBM-Seite „DHCP-Server“ – Register „Allgemeine Einstellungen“

Allgemeine Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „DHCP-Server“ zu aktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „DHCP-Server“ zu deaktivieren.
Offer Reuse Timeout (Bereich: 1~120)		Geben Sie im Eingabefeld den max. Zeitraum ein, nach dem eine angebotene IP-Adresse an den Pool der freien Adressen zurückgegeben werden kann. Gültiger Bereich: 1 ... 120
Nächste Server-Adresse	0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse für den nächsten Server ein.
Boot File Name		Geben Sie im Eingabefeld den Namen der Boot-Datei ein, die verwendet wird, um das Boot-Image zu identifizieren.
Echo ICMP Mode	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Echo ICMP Mode“ zu aktivieren. Bevor der Server einem Client eine bestimmte IP-Adresse anbietet, wird eine ICMP-Anfrage erstellt, um sicherzustellen, dass die Adresse die angeboten werden soll, von keinem Host im Netzwerk verwendet wird.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Echo ICMP Mode“ zu deaktivieren.
Globale Option		In diesem Auswahlfeld werden die globale Option und deren Format konfiguriert. Globale Optionen stehen DHCP-Clients nur dann zur Verfügung, wenn es keine hostspezifische Option gibt und keine poolspezifische Option.
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keine globale Option konfigurieren möchten.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um eine globale Option hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entferne“, um eine globale Option zu entfernen.
	Ascii	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die globale Option im Ascii-Code eingeben oder entfernen.
	IP	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die IP-Adresse der globalen Option eingeben oder entfernen.
Globaler Option-Status		
Parameter	Standardwert	Beschreibung
Option		In dieser Spalte wird die Tabellenindexnummer angezeigt.
Option-Wert		In dieser Spalte wird die TPID angezeigt.

9.3.6.2 Pool-Einstellungen

DHCP-Server

Allgemeine Einstellungen **Pool-Einstellungen** Binding Information Statistics

Pool-Einstellungen

Pool ID			(1~500)	Status	Ausschalten
Host-IP-Adresse				Netzwerk	/
VLAN	Keine			Leihdauer	Uhrzeit 1440
				(minutes)	
Default Router	Keine			Ausgenommene IP-Adresse	Keine
Domain Name				DNS-Server	Keine
NetBIOS-Node-Typ	Keine			NetBIOS-Server	Keine
Option	Keine	Ascii			Keine
	(0~255)			Host Option	Keine
					(xx:xx:xx:xx:xx:xx)
					(0~255)

Pool-Status

Angezeigter Pool:

Pool ID	5	Pool Status	Inactive
Subnet	255.255.255.255	Subnet Mask	255.255.255.255
Start IP Address	0.0.0.0	End IP Address	0.0.0.0
Host IP Address	Not assigned yet	Lease Time(minutes)	1440
VLAN	None	Excluded IP Address	None

Abbildung 75: WBM-Seite „DHCP-Server“ – Register „Pool-Einstellungen“

Tabelle 74: WBM-Seite „DHCP-Server“ – Register „Pool-Einstellungen“

Allgemeine Einstellungen		
Parameter	Standardwert	Beschreibung
Pool ID (1~8)		Geben Sie im Eingabefeld die Pool-ID ein. Gültiger Bereich: 1 ... 8
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Pool-Einstellungen zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Pool-Einstellungen zu aktivieren.
Host-IP-Adresse		Geben Sie im Eingabefeld die „Host-IP-Adresse“ ein, die als Quell-IP-Adresse beim Senden von Paketen verwendet wird.
Netzwerk		Geben Sie im Eingabefeld die Netzwerk-Adresse ein.
VLAN		In diesem Auswahlfeld wird das VLAN ausgewählt.
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie kein VLAN eingeben möchten.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um VLAN hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um VLAN zu entfernen.
Leihdauer (minutes)	Uhrzeit	Wählen Sie im Auswahlfeld „Uhrzeit“, um die Zeitspanne einzugeben, die der Client die vom Server zugewiesene IP-Adresse verwenden kann
	Unbegrenzt	Wählen Sie im Auswahlfeld „Unbegrenzt“, wenn Sie die Zeitspanne unbegrenzt wählen wollen.
Default Router		In diesem Auswahlfeld wird der Default Router ausgewählt.
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen „Default Router“ auswählen wollen.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen „Default Router“ hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um einen „Default Router“ zu entfernen.
Ausgenommene IP-Adresse		In diesem Auswahlfeld wird die ausgenommen IP-Adresse ausgewählt.
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen „Default Router“ auswählen wollen.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen „Default Router“ hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um einen „Default Router“ zu entfernen.
Domain Name		Geben Sie im Eingabefeld den Namen der Domain ein.
DNS-Server		In diesem Auswahlfeld wird der DNS-Server ausgewählt.
	Keine	In diesem Auswahlfeld wird der DNS-Server ausgewählt.
	Hinzufügen	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen „DNS-Server“ auswählen wollen.
	Entfernen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen „DNS-Server“ hinzuzufügen.

NetBIOS-Node-Typ	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen „NetBios-Node-Typ“ auswählen wollen.
	B-Node	Wählen Sie im Auswahlfeld „B-Node“, wenn Sie diesen „NetBios-Node-Typ“ auswählen wollen.
	H-Node	Wählen Sie im Auswahlfeld „H-Node“, wenn Sie diesen „NetBios-Node-Typ“ auswählen wollen.
	M-Node	Wählen Sie im Auswahlfeld „M-Node“, wenn Sie diesen „NetBios-Node-Typ“ auswählen wollen.
	P-Node	Wählen Sie im Auswahlfeld „P-Node“, wenn Sie diesen „NetBios-Node-Typ“ auswählen wollen.
	Remove Node	Wählen Sie im Auswahlfeld „Remove Node“, wenn Sie diesen „NetBios-Node-Typ“ auswählen wollen.
NetBIOS-Server		In diesem Auswahlfeld wird der NetBIOS-Server ausgewählt.
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen „NetBios-Server“ auswählen wollen.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen „NetBios-Server“ hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um einen „NetBios-Server“ zu entfernen.
Option (0~255)		In diesem Auswahlfeld werden die Option und deren Format konfiguriert. Gültiger Bereich: 0 ... 255
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keine Option auswählen wollen.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um eine „Option“ hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um eine „Option“ zu entfernen.
	Ascii	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die Option im Ascii-Code eingeben oder entfernen.
	IP	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die IP-Adresse der Option eingeben oder entfernen.
Host Option xx:xx:xx:xx:xx:xx (0~255)		In diesem Auswahlfeld werden die Host Option und deren Format konfiguriert. Gültiger Bereich: 0 ... 255
	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keine Option auswählen wollen.
	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um eine „Option“ hinzuzufügen.
	Entfernen	Wählen Sie im Auswahlfeld „Entfernen“, um eine „Option“ zu entfernen.
	Ascii	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die Option im Ascii-Code eingeben oder entfernen.
	IP	Haben Sie „Hinzufügen“ oder „Entfernen“ gewählt, können Sie in diesem Eingabefeld die IP-Adresse der Option eingeben oder entfernen.

Globaler Option-Status		
Parameter	Standardwert	Beschreibung
Angezeigter Pool	Alle 1 ... 8	Wählen Sie im Auswahlfeld den entsprechenden Pool aus.
Pool ID		In diesem Anzeigefeld wird die Pool ID angezeigt.
Pool Status		In diesem Anzeigefeld wird angezeigt, ob der Pool aktiviert oder deaktiviert ist.
Subnet		In diesem Anzeigefeld wird das Subnet angezeigt.
Subnet Mask		In diesem Anzeigefeld wird die Subnet Mask angezeigt.
Start IP Address		In diesem Anzeigefeld wird die Start IP Address angezeigt.
End IP Address		In diesem Anzeigefeld wird die End IP Address angezeigt.
Host IP Address		In diesem Anzeigefeld wird die Host IP Address angezeigt.
Lease Time		In diesem Anzeigefeld wird die Leihdauer in Minuten angezeigt.
VLAN		In diesem Anzeigefeld wird das VLAN angezeigt.
Ausgenommene IP-Adresse		In diesem Anzeigefeld wird die ausgenommene IP-Adresse angezeigt.

9.3.6.3 Binding Information

Abbildung 76: WBM-Seite „DHCP-Server“ – Register „Binding Information“

Tabelle 75: WBM-Seite „DHCP-Server“ – Register „Binding Information“

Binding Information		
Parameter	Standardwert	Beschreibung
IP-Adresse		In dieser Spalte wird die IP-Adresse angezeigt.
MAC-Adresse		In dieser Spalte wird die MAC-Adresse angezeigt.
Status		In dieser Spalte wird der Status angezeigt.
Lease Expire Timer		In dieser Spalte wird der Lease Expire Timer angezeigt.

9.3.6.4 Statistics

DHCP-Server				
Allgemeine Einstellungen	Pool-Einstellungen	Binding Information	Statistics	
Received Message Packets				
DHCP Discover	DHCP Request	DHCP Decline	DHCP Release	DHCP Inform
0	0	0	0	0
Sent Message Packets				
DHCP Offer		DHCP Ack		DHCP Nack
0		0		0
Aktualisieren				

Abbildung 77: WBM-Seite „DHCP-Server“ – Register „Statistics“

Tabelle 76: WBM-Seite „DHCP-Server“ – Register „Statistics“

Received Message Packets		
Parameter	Standardwert	Beschreibung
DHCP Discover		In dieser Spalte wird DHCP Discover angezeigt.
DHCP Request		In dieser Spalte wird DHCP Request angezeigt.
DHCP Decline		In dieser Spalte wird DHCP Decline angezeigt.
DHCP Release		In dieser Spalte wird DHCP Inform angezeigt.
Sent Message Packets		
Parameter	Standardwert	Beschreibung
DHCP Offer		In dieser Spalte wird DHCP Offer angezeigt.
DHCP Ack		In dieser Spalte wird DHCP Ack angezeigt.
DHCP Nack		In dieser Spalte wird DHCP Nack angezeigt.

9.3.7 Dual Homing

Hinweis



Weitere Information

Weitere Informationen zu „Dual Homing“ finden Sie im Kapitel „Funktionsbeschreibung“.

Dual Homing

Dual-Homing-Einstellungen

Status Einschalten ▼

Gruppen-ID 1 ▼

Gruppenstatus Ausschalten ▼

Primärer Kanal Hinzufügen ▼ Port ▼ 1

Sekundärer Kanal Hinzufügen ▼ Port ▼ 2

Anwenden Aktualisieren Konfiguration speichern

Dual-Homing-Status

Gruppen-ID	1
Gruppenstatus	Ausschalten
Primärer Kanal	Port 1
Sekundärer Kanal	Port 2
Gruppen-ID	2
Gruppenstatus	Ausschalten
Primärer Kanal	Keine
Sekundärer Kanal	Keine
Gruppen-ID	3
Gruppenstatus	Ausschalten
Primärer Kanal	Keine
Sekundärer Kanal	Keine
Gruppen-ID	4
Gruppenstatus	Ausschalten
Primärer Kanal	Keine
Sekundärer Kanal	Keine

Abbildung 78: WBM-Seite „Dual Homing“

Tabelle 77: WBM-Seite „Dual Homing“

Dual-Homing-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „Dual Homing“ zu aktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um „Dual Homing“ zu deaktivieren.
Gruppen-ID	1 ... 4	Wählen Sie im Auswahlfeld eine Dual-Homing-Gruppe aus, die Sie sich ansehen möchten.
Gruppenstatus	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Primärer Kanal	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen primären Kanal hinzuzufügen.
	Reset	Wählen Sie im Auswahlfeld „Reset“, um den primären Kanal wieder zurückzusetzen.
	Port	In diesem Feld wird der primäre Kanal konfiguriert. Wählen Sie im Auswahlfeld „Port“, um nur einen einzelnen Port zu konfigurieren.
	Trunk	In diesem Feld wird der sekundäre Kanal konfiguriert. Wählen Sie im Auswahlfeld „Trunk“, um nur eine einzelne „Trunk Group“ zu konfigurieren.
		Geben Sie im Eingabefeld die Nummer des primären Kanals ein.
Sekundärer Kanal	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um einen sekundären Kanal hinzuzufügen.
	Reset	Wählen Sie im Auswahlfeld „Reset“, um den sekundären Kanal wieder zurückzusetzen.
	Port	In diesem Feld wird der sekundäre Kanal konfiguriert. Wählen Sie im Auswahlfeld „Port“, um nur einen einzelnen Port zu konfigurieren.
	Trunk	In diesem Feld wird der sekundäre Kanal konfiguriert. Wählen Sie im Auswahlfeld „Trunk“, um nur eine einzelne „Trunk Group“ zu konfigurieren.
		Geben Sie im Eingabefeld die Nummer des sekundären Kanals ein.
Dual-Homing-Status		
Parameter	Standardwert	Beschreibung
Gruppen-ID	1 ... 4	In diesem Anzeigefeld wird die Dual-Homing-Gruppen-ID angezeigt.
Gruppenstatus	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, welchen Status „Dual Homing“ besitzt.
Primärer Kanal	Keine Port 1 ... 10 (12)	In diesem Anzeigefeld wird der ausgewählte primäre Kanal angezeigt.
Sekundärer Kanal	Keine Port 1 ... 10 (12)	In diesem Anzeigefeld wird der ausgewählte sekundäre Kanal angezeigt.

9.3.8 Dual Ring

Hinweis



Weitere Information

Weitere Informationen zum „Dual Ring“ finden Sie im Kapitel „Funktionsbeschreibung“.

Dual Ring

Dual-Ring-Einstellungen

Status	Ausschalten ▼
Xpress Ring Role	Forwarder ▼
Xpress Ring PORT-1	Keine ▼
Xpress Ring PORT-2	Keine ▼
Xpress-Ring-Destination-MAC-Adresse (Letztes Byte)	f0
Subring PORT-1	Keine ▼
Subring PORT-2	Keine ▼

Dual-Ring-Status

Xpress-Ring-PORT-1-Status	Keine Verbindung
Xpress-Ring-PORT-2-Status	Keine Verbindung
Subring-PORT-1-Status	Keine Verbindung
Subring-PORT-2-Status	Keine Verbindung
Subring-Bridge-Role	Ausschalten
Subring-Master-Bridge-MAC	00:00:00:00:00:00

Abbildung 79: WBM-Seite „Dual Ring“

Tabelle 78: WBM-Seite „Dual Ring“

Dual-Ring-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um „Dual Ring“ zu deaktivieren.
	Einschalten	Wählen Sie „Einschalten“, um „Dual Ring“ zu aktivieren.
Xpress Ring Role	Forwarder	Wählen Sie im Auswahlfeld „Forwarder“, wenn der Switch im Xpress Ring als Forwarder arbeiten soll.
	Arbiter	Wählen Sie im Auswahlfeld „Arbiter“, wenn der Switch im XPress Ring als Arbiter arbeiten soll.
Xpress Ring PORT-1	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen Port auswählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den Port 1 im Xpress Ring aus.
Xpress Ring PORT-2	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen Port auswählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den Port 2 im Xpress Ring aus.
Xpress-Ring Destination-MAC-Adresse (Letztes Byte)	f0	Geben Sie im Eingabefeld die Xpress-Ring-Kennung ein.
Subring PORT-1	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen Port auswählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den Port 1 im Jetring aus.
Subring PORT-2	Keine	Wählen Sie im Auswahlfeld „Keine“, wenn Sie keinen Port auswählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den Port 2 im Jet Ring aus.
Dual-Ring-Status		
Parameter	Standardwert	Beschreibung
Xpress-Ring-PORT-1-Status	Forwarding Blocking	In diesem Anzeigefeld wird angezeigt, welchen Status der Xpress Ring Port-1 besitzt.
Xpress-Ring-PORT-2-Status	Forwarding Blocking	In diesem Anzeigefeld wird angezeigt, welchen Status der Xpress Ring Port-2 besitzt.
Subring-PORT-1-Status	Forwarding Blocking	In diesem Anzeigefeld wird angezeigt, welchen Status der Jet Ring Port-1 besitzt.
Subring-PORT-2-Status	Forwarding Blocking	In diesem Anzeigefeld wird angezeigt, welchen Status der Jet Ring Port-2 besitzt.
Subring-Bridge-Role	Forwarder Master	In diesem Anzeigefeld wird die Rolle des Switch im Xpress Ring angezeigt.
Subring-Master-Bridge-MAC		In diesem Anzeigefeld wird die MAC ID des Jet Rings angezeigt.

9.3.9 ERPS

Hinweis



Weitere Information

Weitere Informationen zu „ERPS“ (ETHERNET Ring Protection Switching) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.9.1 Ringeinstellungen

ERPS

Ringeinstellungen
Instance-Einstellungen

ERPS-Global-Einstellungen

Globaler Status Ausschalten ▾

ERPS-Ring-Einstellungen

Ring ID (1~255) Ring Name Instance 0 (0:Ausschalten, 0~30) Control VLAN (1~4094) Holdoff Timer (ms) 0 (0~10000) MEL 7 (0~7) Linker Port Keine ▾ Normal ▾ Linker Port-Enhance-Mode Ausschalten ▾ Diagnose über Relais Ausschalten ▾	Status Ausschalten ▾ Revertive Einschalten ▾ Ring Typ Major-ring ▾ Version v2 ▾ WTR Timer (min) 300 (5~720) Guard Timer (ms) 500 (10~2000) Rechter Port Keine ▾ Normal ▾ Rechter Port-Enhance-Mode Ausschalten ▾

Anwenden
Aktualisieren
Konfiguration speichern

ERPS Ring-Status

Ring ID	249	Status	Ausschalten
Ring Name	Ring249	Revertive	Einschalten
Instance	Keine	Ring Typ	Major-ring
Control VLAN	249	Version	v2
Holdoff Timer (ms)	0	WTR Timer (min)	300
MEL	7	Guard Timer (ms)	500
Linker Port	Keine	Rechter Port	Keine
Linker Port-Typ	Normal	Rechter Port-Typ	Normal
Linker Port-Enhance-Mode	Ausschalten	Rechter Port-Enhance-Mode	Ausschalten
Linker Port-Status	N/A	Rechter Port-Status	N/A
Ring-Status	Initialization	Diagnose über Relais	Disable

Löschen

Abbildung 80: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

Tabelle 79: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

ERPS-Global-Einstellungen		
Parameter	Standardwert	Beschreibung
Globaler Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „ERPS“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „ERPS“ zu aktivieren.
ERPS-Ring-Einstellungen		
Parameter	Standardwert	Beschreibung
Ring ID (1~255)		Geben Sie im Eingabefeld die Ring ID ein. Gültiger Bereich: 1 ... 255
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um den Zustand des Rings zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Zustand des Rings zu aktivieren.
Ring Name		Geben Sie im Eingabefeld den Namen des Rings ein (max. 32 Zeichen). (z. B. Major-Ring ID255)
Revertive	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Rückschaltmodus zu aktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um den Rückschaltmodus zu deaktivieren.
Instance (0:Ausschalten, 0~30)		Geben Sie im Eingabefeld die Instanz für den Ring ein. Gültiger Bereich: 0 ... 30 0 („Ausschalten“) bedeutet, dass das ERPS in Version 1 betrieben wird. Das Steuerungs-VLAN der Instanz sollte dasselbe wie das darunterliegende Steuerungs-VLAN sein.
Ring Typ	Major-ring	Wählen Sie im Auswahlfeld „Major-ring“, wenn der Switch im Major-Ring arbeiten soll.
	Sub-ring	Wählen Sie im Auswahlfeld „Sub-ring“, wenn der Switch im Sub-Ring arbeiten soll.
Control VLAN (1~4094)	1 ... 4094	Geben Sie im Eingabefeld die VLAN ID ein, die als Domäne für die ERPS-Steuerungspakete dient. Gültiger Bereich: 1 ... 4094
Version	v2	Wählen Sie im Auswahlfeld „v2“, wenn Sie die Version 2 der „ERPS“-Funktion nutzen möchten.
	v1	Wählen Sie im Auswahlfeld „v1“, wenn Sie die Version 1 der „ERPS“-Funktion nutzen möchten.
Holdoff Timer (ms) (0~10000)	0	Geben Sie im Eingabefeld den Wert für den „Holdoff Timer“ für den Ring ein. Zeitraum: 0 ... 10000 ms.
WTR Timer (min) (5~720)	300	Geben Sie im Eingabefeld den Wert für den „WTR Timer“ für den Ring ein. Zeitraum: 5 ... 720 min
MEL (0~7)	7	Geben Sie im Eingabefeld den Wert für das „Control MEL“ (M aintenance E ntity G roup L evel) für den Ring ein. Der MEL gibt die Priorität an. 0 = niedrigste Priorität 7 = höchste Priorität

Tabelle 79: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

Guard Timer (ms) (10~2000)	500	Geben Sie in diesem Eingabefeld den Wert für den „Guard Timer“ für den Ring ein. Zeitraum: 10 ... 2000 ms.
Linker Port		In diesem Auswahlfeld werden der linke Port und dessen Typ für den Ring konfiguriert.
	Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie keinen Port auswählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den entsprechenden Port aus.
	Normal	Wählen Sie im Auswahlfeld „Normal“, wenn dem Port keine spezielle Funktion im ERPS-Ring zugewiesen ist.
	Nachbar	Wählen Sie im Auswahlfeld „Nachbar“, wenn der benachbarte Port die Funktion „Nachbar“ besitzt.
	Owner	Wählen Sie im Auswahlfeld „Owner“, wenn der Port die Funktion „Owner“ in ERPS-Ring einnehmen soll.
Rechter Port		In diesem Auswahlfeld werden der rechte Port und dessen Typ für den Ring konfiguriert.
	Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie keinen Port wählen wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den entsprechenden Port aus.
	Normal	Wählen Sie im Auswahlfeld „Normal“, wenn dem Port keine spezielle Funktion im ERPS-Ring zugewiesen ist.
	Nachbar	Wählen Sie im Auswahlfeld „Nachbar“, wenn der benachbarte Port die Funktion „Nachbar“ besitzt.
	Owner	Wählen Sie im Auswahlfeld „Owner“, wenn der Port die Funktion „Owner“ in ERPS-Ring einnehmen soll.
Linker Port-Enhance-Mode	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn an diesem Port ein Gerät angeschlossen ist, das ERPS unterstützt.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn an diesem Port ein Gerät angeschlossen ist, das ERPS nicht unterstützt. Beachten Sie dabei die Aging Time des angeschlossenen Gerätes.
Rechter Port-Enhance-Mode	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn an diesem Port ein Gerät angeschlossen ist, das ERPS unterstützt.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn an diesem Port ein Gerät angeschlossen ist, das ERPS nicht unterstützt. Beachten Sie dabei die Aging Time des angeschlossenen Gerätes.
Diagnose über Relais	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Diagnose über das Relais zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Diagnose über das Relais zu aktivieren.

Tabelle 79: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

ERPS-Ring-Status		
Parameter	Standardwert	Beschreibung
Ring ID	1 ... 255	In diesem Anzeigefeld wird die Ring ID angezeigt.
Status	Ausschalten Einschalten	In diesem Anzeigefeld wird der Zustand des Ringes angezeigt.
Ring Name		In diesem Anzeigefeld wird der Name des Ringes angezeigt.
Revertive	Einschalten Ausschalten	In diesem Anzeigefeld wird der Zustand des Rückschaltmodus angezeigt.
Instance		In diesem Anzeigefeld wird die Instanz für den Ring angezeigt.
Ring Typ	Major-ring Sub-ring	In diesem Anzeigefeld wird der Typ des Ringes angezeigt.
Control VLAN	1 ... 4084	In diesem Anzeigefeld wird das VLAN der Steuerung angezeigt.
Version	v2 v1	In diesem Anzeigefeld wird die Version der „ERPS“-Funktion angezeigt.
Holdoff Timer (ms)	0 ... 10000	In diesem Anzeigefeld wird die Zeit für den „Holdoff Timer“ angezeigt.
WTR Timer (min)	5 ... 12	In diesem Anzeigefeld wird die Zeit für den „WTR Timer“ angezeigt.
MEL	0 ... 7	In diesem Anzeigefeld wird der Wert für das „Control MEL“ angezeigt.
Guard Timer (ms)	10 ... 2000	In diesem Anzeigefeld wird die Zeit für den „Guard Timer“ angezeigt.
Linker Port	Keiner 1 ... 10 (12)	In diesem Anzeigefeld wird die Port-Nummer des linken Ports angezeigt.
Rechter Port	Keiner 1 ... 10 (12)	In diesem Anzeigefeld wird die Port-Nummer des rechten Ports angezeigt.
Linker Port-Typ	Normal Nachbar Owner	In diesem Anzeigefeld wird der Typ des linken Ports angezeigt.
Rechter Port-Typ	Normal Nachbar Owner	In diesem Anzeigefeld wird der Typ des rechten Ports angezeigt.
Linker Port-Enhance-Mode	Einschalten Ausschalten	In diesem Anzeigefeld wird Status des linken Ports angezeigt.
Rechter Port-Enhance-Mode	Einschalten Ausschalten	In diesem Anzeigefeld wird Status des rechten Ports angezeigt.
Linker Port-Status	Weiterleitung Blockierung	In diesem Anzeigefeld wird der aktuelle Status des linken Ports angezeigt.
Rechter Port-Status	Weiterleitung Blockierung	In diesem Anzeigefeld wird der aktuelle Status des rechten Ports angezeigt.
Ring-Status	Schutz Leerlauf	In diesem Anzeigefeld wird der Ringstatus angezeigt.
Alarmrelais	Einschalten Ausschalten	In diesem Anzeigefeld wird Status des Alarm-Relais angezeigt.
Löschen		Klicken Sie auf [Löschen] , um diese Einstellung zu löschen.

9.3.9.2 Instance-Einstellungen

ERPS Instance

Instance-Einstellungen

Instance: 1 (1~30)
Control VLAN: 2
Data VLAN: 3

Anwenden Aktualisieren Konfiguration speichern

Instance-Status

Instance	1		
Control VLAN	2	Data VLAN	3
Löschen			

Abbildung 81: WBM-Seite „ERPS“ – Register „Instance-Einstellungen“

Tabelle 80: WBM-Seite „ERPS“ – Register „Instance-Einstellungen“

Instance-Einstellungen		
Parameter	Standardwert	Beschreibung
Instance (1~30)		Geben Sie im Eingabefeld die Instanz ID ein. Gültiger Bereich: 1 ... 30
Control VLAN		Geben Sie im Eingabefeld die VLAN der Steuerung für die Instanz ein. Gültiger Bereich: 1 ... 4094
Data VLAN		Geben Sie im Eingabefeld den Wert für das Daten-VLAN für die Instanz ein. Gültiger Bereich: 1 ... 4094 Es können ein oder mehrere Daten-VLANs konfiguriert werden.
Instance-Status		
Parameter	Standardwert	Beschreibung
Instance	1 ... 31	In diesem Anzeigefeld wird die Instanz-ID angezeigt.
Control VLAN	1 ... 4094	In diesem Anzeigefeld wird das Steuerungs-VLAN der Instanz angezeigt.
Data VLAN	1 ... 4094	In diesem Anzeigefeld wird das Daten-VLAN der Instanz angezeigt.
Löschen		Klicken Sie auf [Löschen] , um diese Einstellung zu löschen.

9.3.10 Link Aggregation

Hinweis



Weitere Information

Weitere Informationen zu „Link Aggregation“ finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.10.1 Static Trunk

Link Aggregation

StaticTrunk
LACP
LACP info.

Statische-Trunk-Einstellungen

Gruppenstatus Gruppe 1 Ausschalten

Load Balance MAC

Member Ports

☐ Alle auswählen ☐ Alle deaktivieren

☐ 1 ☐ 3 ☐ 5 ☐ 7

☐ 9 ☐ 11

☐ 2 ☐ 4 ☐ 6 ☐ 8

☐ 10 ☐ 12

Anwenden
Aktualisieren
Konfiguration speichern

Trunk-Gruppenstatus

Gruppen-ID	Status	Load Balance	Member Ports
1	Ausschalten	MAC	
2	Ausschalten	MAC	
3	Ausschalten	MAC	
4	Ausschalten	MAC	
5	Ausschalten	MAC	
6	Ausschalten	MAC	

Member-Ports: T ist ein Trunk-Member-Port, aber es besteht keine Verbindung, A ist ein Trunk-Member-Port und es besteht eine Verbindung.

Abbildung 82: WBM-Seite „Link Aggregation“ – Register „Static Trunk“

Tabelle 81: WBM-Seite „Link Aggregation“ – Register „Static Trunk“

Abbildung 5-1: WZM-Schnittstelle „Trunk-Gruppenstatus“

Register „Trunk-Gruppenstatus“

Static-Trunk-Einstellungen				
Parameter		Standardwert	Beschreibung	
Gruppenstatus		Gruppe 1 ... Gruppe 6	Wählen Sie im Auswahlfeld eine Gruppenkennung für diese „Trunk-Gruppe“ (ein logischer Link, der mehrere Ports enthält) aus.	
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um eine statische „Trunk-Gruppe“ zu deaktivieren.	
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um eine statische „Trunk-Gruppe“ zu verwenden.	
Load Balance		MAC	Wählen Sie im Auswahlfeld „MAC“, um den Algorithmus für den Lastausgleich einer spezifischen „Trunk-Gruppe“ zu konfigurieren.	
		IP	Wählen Sie im Auswahlfeld „IP“, um den Algorithmus für den Lastausgleich einer spezifischen „Trunk-Gruppe“ zu konfigurieren.	
Member Ports	Alle auswählen	☐	☐	Es ist kein Port ausgewählt, der zu der statischen „Trunk-Gruppe“ hinzugefügt werden soll.
			☒	Es sind alle Ports ausgewählt, die zu der statischen „Trunk-Gruppe“ hinzugefügt werden sollen.
	Alle deaktivieren	☐	☐	Es ist kein Port deaktiviert.
			☒	Es sind alle Ports deaktiviert.
	☐ 1 ...	☐	☐	Der Port ist nicht aktiviert.
	☐ 10 (12)		☒	Der Port ist aktiviert.
Trunk-Gruppenstatus				
Parameter		Standardwert	Beschreibung	
Gruppen-ID		1 ... 6	In dieser Spalte wird die Gruppen-ID für eine „Trunk-Gruppe“ (ein logischer Link, der mehrere Ports enthält) angezeigt.	
Status		Ausschalten Einschalten	In dieser Spalte wird angezeigt, ob eine „Trunk-Gruppe“ aktiviert oder deaktiviert ist.	
Load Balance		1 ... 6	In dieser Spalte werden die Richtlinien für den Lastausgleich der „Trunk-Gruppe“ angezeigt.	
Member Ports			In dieser Spalte werden die Ports angezeigt, die der statischen „Trunk-Gruppe“ zugeordnet sind.	

9.3.10.2 LACP**Hinweis****Weitere Information**

Weitere Informationen zu „LACP“ (Link **A**ggregation **C**ontrol **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

Link Aggregation

StaticTrunk
LACP
LACP info.

LACP-Einstellungen

Status Einschalten ▾

System-Priorität

Gruppe LACP Gruppe 1 ▾ Ausschalten ▾

Port-Priorität von: - ▾ ~ - ▾ :

LACP-Gruppenstatus

Gruppen-ID	LACP-Status
1	Ausschalten
2	Ausschalten
3	Ausschalten
4	Ausschalten
5	Ausschalten
6	Ausschalten

LACP-Port-Prioritätsstatus

Port	Priorität	Port	Priorität
1	32768	2	32768
3	32768	4	32768
5	32768	6	32768
7	32768	8	32768
9	32768	10	32768
11	32768	12	32768

Abbildung 83: WBM-Seite „Link Aggregation“ – Register „LACP“

Tabelle 82: WBM-Seite „Link Aggregation“ – Register „LACP“

LACP-Einstellungen			
Parameter		Standardwert	Beschreibung
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie das „Link Aggregation Control Protocol“ (LACP) nicht verwenden möchten.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Link Aggregation Control Protocol“ (LACP) zu aktivieren.
Systempriorität		1 ... 65535	Wählen Sie im Auswahlfeld die LACP-Systempriorität aus. Tragen Sie eine Zahl ein, um die Priorität eines aktiven Ports mit „Link Aggregation Control Protocol“ (LACP) festzulegen. Je niedriger die Zahl ist, desto höher ist die Prioritätsebene.
Gruppe LACP		Gruppe 1 ... Gruppe 6	Wählen Sie im Auswahlfeld eine „Trunk-Gruppen-ID“ aus.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um das LACP für diese „Trunk-Gruppen-ID“ zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das LACP für diese „Trunk-Gruppe“ zu aktivieren.
Port-Priorität	von:	-	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie die LACP-Priorität konfigurieren möchten.
	an:	-	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie die LACP-Priorität konfigurieren möchten.
		32768	Die Default-Systempriorität ist 32768.
LACP-Gruppenstatus			
Parameter		Standardwert	Beschreibung
Gruppen-ID		1 ... 6	In dieser Spalte wird die LACP-Gruppen-ID angezeigt.
LACP-Status		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob das LACP für eine Gruppe aktiviert oder deaktiviert ist.
LACP-Port-Prioritätsstatus			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte wird die Port-ID angezeigt.
Priorität		1 ... 65535	In dieser Spalte wird die LACP-Priorität des Ports angezeigt.

9.3.10.3 LACP Info.

Link Aggregation

Static-Trunk
LACP
LACP-info.

LACP-Information

Gruppen-ID

Gruppen-ID	1						
Nachbarinformationen							
Port	Systempriorität	System-ID	Port	Age	Port-Status	Port-Priorität	Oper-Key
1	-	-	-	-	-	-	-
2	0	00:00:00:00:00:00	1	187s	0x00	48868	0
Interne Information							
Port	Port Priority	Admin-Key	Oper Key	Port State			
1	18	0	0	0x00			
2	18	0	0	0x00			

Neighbor Information: '-' means the port is link down.

Abbildung 84: WBM-Seite „Link Aggregation“ – Register „LACP Info.“

Tabelle 83: WBM-Seite „Link Aggregation“ – Register „LACP Info.“

LACP-Information		
Parameter	Standardwert	Beschreibung
Gruppen-ID	-	Wählen Sie im Auswahlfeld eine LACP-Gruppe aus, die Sie sich ansehen möchten.
Nachbarinformationen		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	In dieser Spalte wird die LACP-ID des Teilnehmer-Ports angezeigt.
Systempriorität	0 ... 65535	In dieser Spalte wird die LACP-Systempriorität angezeigt.
System-ID		In dieser Spalte wird die System-ID des benachbarten Switches angezeigt.
Port	1 ... 10 (12)	In dieser Spalte wird die ID des direkt verbundenen Ports des benachbarten Switches angezeigt.
Age		In dieser Spalte wird der verfügbare Zeitraum für die LACP-Informationen des benachbarten Switches angezeigt.
Port-Status		In dieser Spalte wird der Zustand des direkt verbundenen Ports am benachbarten Switch angezeigt.
Port-Priorität		In dieser Spalte wird die Priorität des direkt verbundenen Ports am benachbarten Switch angezeigt.
Oper-Key		In dieser Spalte wird der „Oper-Key“ des benachbarten Switches angezeigt.
Interne Information		
Parameter	Standardwert	Beschreibung
Port		In dieser Spalte wird die LACP-ID des Teilnehmer-Ports angezeigt.
Port-Priorität		In dieser Spalte wird die Port-Priorität des LACP-Teilnehmer-Ports angezeigt.
Admin-Key		In dieser Spalte wird der „Admin-Key“ des LACP-Teilnehmer-Ports angezeigt.
Oper-Key		In dieser Spalte wird der „Oper-Key“ des LACP-Teilnehmer-Ports angezeigt.
Port-Status		In dieser Spalte wird der Port-Zustand des LACP-Teilnehmer-Ports angezeigt.

9.3.11 LLDP

Hinweis



Weitere Information

Weitere Informationen zu „LLDP“ (Link Layer Discovery Protocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.11.1 LLDP-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 85: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“

Tabelle 84: 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 Sekunden (Bereich: 1~3600)
Tx Hold		4 Mal (Bereich 2~100)
Time To Live		120 Sekunden
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
		Beschreibung
		In dieser Spalte werden die Port-Nummern angezeigt.
		In dieser Spalte wird angezeigt, ob „LLDP“ aktiviert oder deaktiviert ist.

9.3.11.2 Nächster Nachbar

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 86: WBM-Seite „LLDP“ – Register „Nächste“

Tabelle 85: WBM-Seite „LLDP“ – Register „Nächste“

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.
Local 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.

9.3.12 Loop Detection

Hinweis



Weitere Information

Weitere Informationen zu „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 87: WBM-Seite „Loop Detection“

Tabelle 86: WBM-Seite „Loop Detection“

Loop-Detection-Einstellungen			
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.
Manual Recovery		Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie die Loop Detection am Port ausschalten.
		Freischalten	Wählen Sie im Auswahlfeld „Freischalten“, wenn Sie die Funktionen „Status“ und „Loop Korrektur“ nicht verändern wollen.
Recovery Status		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
Loop-Detection-Status			
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.
Recovery Status		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 „Recovery Status“ angezeigt.

9.3.13 Jet Ring

Hinweis



Weitere Information

Weitere Informationen zu „Jet Ring“ finden Sie im Kapitel „Funktionsbeschreibung“.

Jet-Ring

Jet-Ring-Einstellungen

Status

Einschalten ▾

Alarm Relay

Ausschalten ▾

Master-Bridge-MAC

00:30:DE:FF:E7:5F

Jet-Ring-Teilnehmeranzahl

1

Bridge-Role

Learning...

Anwenden

Aktualisieren

Konfiguration speichern

Jet Ring Status

Port	Port-Status	Ring-Port
1	Keine Verbindung	
2	Keine Verbindung	
3	Keine Verbindung	
4	Keine Verbindung	
5	Keine Verbindung	
6	Keine Verbindung	
7	Keine Verbindung	
8	Keine Verbindung	
9	Forwarding	
10	Keine Verbindung	
11	Keine Verbindung	
12	Keine Verbindung	

Abbildung 88: WBM-Seite „Jet Ring“

Tabelle 87: WBM-Seite „Jet Ring“

Jet-Ring-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Jet Ring“-Funktion an einzelnen Ports zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „Jet Ring“-Funktion an einzelnen Ports zu aktivieren.
Diagnose über Relais	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Diagnose über das Relais zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Diagnose über das Relais zu aktivieren.
Jet-Ring-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Port Status	Keine Verbindung Forwarding Blocking	In dieser Spalte wird der Port-Status angezeigt.
Ring-Port	ja	In dieser Spalte wird angezeigt, ob der Port in einem Ring arbeitet.

9.3.14 Modbus

Abbildung 89: WBM-Seite „Modbus“

Tabelle 88: WBM-Seite „Modbus“

Modbus-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die „MODBUS“-Funktion an einzelnen Ports zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „MODBUS“-Funktion an einzelnen Ports zu aktivieren.
Verbindung		In diesem Anzeigefeld wird die Verbindung angezeigt.

Hinweis



Modbus-Register

Die Tabelle „Modbus-Register“ finden Sie im Kapitel „Anhang“ > ... > „Modbus-Register“.

9.3.15 Static Route

Hinweis



Weitere Information

Weitere Informationen zu „Static Route“ finden Sie im Kapitel „Funktionsbeschreibung“.

Static Route

Globale Einstellungen

IP-Weiterleitung Ausschalten ▾

IP ARP Proxy Einschalten ▾

IPv4-ARP-Tabelle Hinzufügen ▾ IP:
MAC:

IPv6-ARP-Tabelle Hinzufügen ▾ IP:
MAC:

Route Settings

VLAN:

IPv4 Hinzufügen ▾ Interface Route ▾ IP/M:
IP:

IPv6 Hinzufügen ▾ Interface Route ▾ IP/M:
IP:

Anwenden
Aktualisieren
Konfiguration speichern

Status

Typ: ARP ▾ Alle ▾ Zeigen

Abbildung 90: WBM-Seite „Static Route“

Tabelle 89: WBM-Seite „Static Route“

Tabellensatz: WZM: Seite „Status Route“

Globale Einstellungen			
Parameter	Standardwert	Beschreibung	
IP-Weiterleitung	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.	
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.	
IP ARP Proxy	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Route global als ARP-Proxy zu deaktivieren.	
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Route global als ARP-Proxy zu aktivieren.	
IPv4-ARP-Tabelle	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um der ARP-Tabelle einen statischen IPv4-ARP-Eintrag hinzuzufügen.	
	Löschen	Wählen Sie im Auswahlfeld „Löschen“, um in der ARP-Tabelle einen statischen IPv4-ARP-Eintrag zu löschen.	
IPv6-ARP-Tabelle	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um der ARP-Tabelle einen statischen IPv6-ARP-Eintrag hinzuzufügen.	
	Löschen	Wählen Sie im Auswahlfeld „Löschen“, um in der ARP-Tabelle einen statischen IPv6-ARP-Eintrag zu löschen.	
Route Settings			
Parameter	Standardwert	Beschreibung	
VLAN		Tragen Sie im Eingabefeld ein spezifisches Interface-VLAN ein.	
IPv4 IPv6	Hinzufügen	Wählen Sie im Auswahlfeld „Hinzufügen“, um dem Interface VLAN eine Route hinzuzufügen. Wählen Sie über das benachbarte Auswahlfeld den Routentyp aus (Interface Route / Static Route)	
	Löschen	Wählen Sie im Auswahlfeld „Löschen“, um eine Route zu löschen. Wählen Sie über das benachbarte Auswahlfeld den Routentyp aus (Interface Route / Static Route)	
IP/M		Geben Sie im Eingabefeld die IP-Adresse und die Netzmaske ein.	
IP		Geben Sie im Eingabefeld die statische Routenadresse für den statischen Routentyp ein.	
Status			
Parameter	Standardwert	Beschreibung	
Typ	ARP	Alle	Zeigt die Konfigurationen von ARP-Tabelle / Host-Tabelle und Routen an.
		IPv4	
		IPv6	
	Host	Alle	
		IPv4	
		IPv6	
	Route	Alle	
		IPv4	
		IPv6	

9.3.16 Spanning Tree Protocol (STP)

Hinweis



Weitere Information

Weitere Informationen zu „Spanning Tree Protocol“ (STP) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.16.1 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)

Beziehungsformel:
 $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Hello Time

(Bereich:1-10)

Priorität

(Bereich:0-61440)

Pathcost Method

Abbildung 91: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“

Tabelle 90: 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-Parameter		
Parameter	Standardwert	Beschreibung
Forward Delay (Bereich: 4~30)	15	Geben Sie im Eingabefeld die Zeit „Forward Delay“ ein. Gültiger Bereich: 4 ... 30 s
Max Age (Bereich: 6~40)	20	Geben Sie im Eingabefeld die Zeit „Max Age“ ein. Gültiger Bereich: 6 ... 40 s
Hello Time (Bereich: 1~10)	2	Geben Sie im Eingabefeld die Zeit für die „Hello Time“ ein. Gültiger Bereich: 1 ... 10 s
Priorität (Bereich: 0~61440)	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
Pathcost Method	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

9.3.16.2 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 ▼	Einschalten ▼	4	128	Ausschalten ▼	Ausschalten ▼	Ausschalten ▼	Ausschalten ▼
an: 1 ▼							

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 92: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Tabelle 91: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Port-Parameter-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
Aktiv		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.
Path Cost			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 Port-Typ „Edge-Port“ für den spezifischen Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Port-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 91: 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.
Aktiv	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	Verwerfen Blocking Listening Learning Weiterleitung Disabled	In dieser Spalte wird der Port-Status angezeigt.
Path Cost	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.

9.3.16.3 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 93: WBM-Seite „Spanning Tree Protocol“ – Register „STP-Status“

Tabelle 92: 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 „Forward Delay“.
Forward Delay		In diesem Anzeigefeld wird die maximale Zeit (in Sekunden) angezeigt, die der Root-Switch wartet, bevor er Zustände ändert.
Aktueller Bridge-Status		
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 Delay“ angezeigt.
Path Cost		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.

9.3.17 Xpress Ring

Hinweis



Weitere Information

Weitere Informationen zum „Xpress Ring“ finden Sie im Kapitel „Funktionsbeschreibung“.

Xpress Ring

Xpress-Ring-Einstellungen

Globaler Status : Ausschalten ▼

	Ring1	Ring2
Status	Ausschalt ▼	Ausschalt ▼
Ziel-MAC-Adresse (letztes byte)	f0	f1
Role	Forwarder ▼	Forwarder ▼
Primärer Port	Keine ▼	Keine ▼
Sekundärer Port	Keine ▼	Keine ▼

Anwenden
Aktualisieren
Konfiguration speichern

Xpress-Ring-Status

	Ring1	Ring2
Status	Ausschalten	Ausschalten
Ziel-MAC-Adresse	01:80:c2:ff:ff:f0	01:80:c2:ff:ff:f1
Role	Forwarder	Forwarder
Primärer Port	N/A (Keine Verbindung)	N/A (Keine Verbindung)
Sekundärer Port	N/A (Keine Verbindung)	N/A (Keine Verbindung)

Abbildung 94: WBM-Seite „Xpress Ring“

Tabelle 93: WBM-Seite „Xpress Ring“

Xpress-Ring-Einstellungen		
Parameter	Standardwert	Beschreibung
Globaler Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Xpress Ring“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Xpress Ring“ zu aktivieren.
Ring 1		In dieser Spalte können Sie die Konfigurationen für den Ring 1 vornehmen.
Ring 2		In dieser Spalte können Sie die Konfigurationen für den Ring 2 vornehmen.
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Xpress Ring“ für den jeweiligen Ring zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Xpress Ring“ für den jeweiligen Ring zu deaktivieren.
Ziel-MAC-Adresse (letztes Byte)		Geben Sie im Eingabefeld die MAC-Adresse des jeweiligen Rings ein.
Role	Forwarder	Wählen Sie im Auswahlfeld die Rolle „Forwarder“ für den Switch aus.
	Arbiter	Wählen Sie im Auswahlfeld die Rolle „Arbiter“ für den Switch aus.
Primärer Port	Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie keinen primären Port im Ring aktivieren wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den entsprechenden primären Port aus.
Sekundärer Port	Keiner	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie keinen sekundären Port im Ring aktivieren wollen.
	1 ... 10 (12)	Wählen Sie im Auswahlfeld den entsprechenden sekundären Port aus.
Xpress-Ring-Status		
Parameter	Standardwert	Beschreibung
Status	Ausschalten Einschalten	In diesem Anzeigefeld wird der aktuelle Zustand des Xpress Rings angezeigt.
Ring 1		In dieser Spalte werden die Konfigurationen für den Ring 1 angezeigt.
Ring 2		In dieser Spalte werden die Konfigurationen für den Ring 2 angezeigt.
Ziel-MAC-Adresse		In diesem Anzeigefeld wird das letzte Byte der jeweiligen MAC-Adresse des Xpress Rings angezeigt.
Role	Forwarder Arbiter	In diesem Anzeigefeld wird die Rolle des Switches angezeigt.
Primärer Port	N/A (keine Verbindung 0 ... 10 (12) (Forwarding, Blocking)	In diesem Anzeigefeld wird der Status des primären Ports angezeigt.
Sekundärer Port	N/A (keine Verbindung 0 ... 10 (12) (Forwarding, Blocking)	In diesem Anzeigefeld wird der Status des sekundären Ports angezeigt.

9.4 Sicherheit

9.4.1 IP Source Guard

Hinweis



Weitere Information

Weitere Informationen zu „IP Source Guard“ (IP-Quelladressschutz) finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.1.1 DHCP Snooping

Hinweis



Weitere Information

Weitere Informationen zu „DHCP Snooping“ (Dynamic Host Configuration Protocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.1.1.1 DHCP Snooping

DHCP-Snooping	
DHCP-Snooping Port-Einstellungen Server-Screening	
DHCP-Snooping-Einstellungen	
Status	Ausschalten ▼
VLAN-Status	Hinzufügen ▼
Anwenden Aktualisieren Konfiguration speichern	
DHCP-Snooping-Status	
DHCP-Snooping-Status	Ausschalten
Einschalten an VLAN	Keine

Abbildung 95: WBM-Seite „DHCP Snooping“ – Register „DHCP Snooping“

Tabelle 94: WBM-Seite „DHP Snooping“ – Register „DHCP Snooping“

DHCP-Snooping-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie diese Funktion nicht verwenden möchten.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „DHCP Snooping“ zu aktivieren. Sie müssen diese Funktion anschließend noch für spezifische VLANs aktivieren sowie „Trusted Ports“ konfigurieren.
	Hinweis 	DHCP-Anfragen konfigurieren Der Switch wird alle DHCP-Anfragen verwerfen, wenn „DHCP Snooping“ aktiviert ist, aber keine „Trusted Ports“ vorhanden sind. Wählen Sie „Ausschalten“, wenn Sie diese Funktion nicht verwenden möchten.
VLAN-Status	Ergänzen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, für die das „DHCP Snooping“ aktiviert werden 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, für die das „DHCP Snooping“ deaktiviert werden soll.
DHCP-Snooping-Status		
Parameter	Standardwert	Beschreibung
DHCP-Snooping-Status	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob „DHCP Snooping“ aktiviert oder deaktiviert ist.
Einschalten an VLAN	Keiner 1 ... 4094	In diesem Anzeigefeld werden die VLANs angezeigt, für die die Funktion „DHCP Snooping“ aktiviert ist. Es wird „Keiner“ angezeigt, wenn keine VLANs dafür spezifiziert wurden.

9.4.1.1.2 Port-Einstellungen

DHCP-Snooping

DHCP-Snooping Port-Einstellungen Server-Screening

Port-Einstellungen

Port von: an:

Trust

Maximale Host-Anzahl (Bereich: 1-32)

Port-Status

Port	Trust	Maximale Host-Anzahl	Port	Trust	Maximale Host-Anzahl
1	Nein	32	2	Nein	32
3	Nein	32	4	Nein	32
5	Nein	32	6	Nein	32
7	Nein	32	8	Nein	32
9	Nein	32	10	Nein	32
11	Nein	32	12	Nein	32

Abbildung 96: WBM-Seite „DHCP Snooping“ – Register „Port-Einstellungen“

Tabelle 95: WBM-Seite „DHCP Snooping“ – Register „Port-Einstellungen“

Port-Einstellungen			
Parameter		Standardwert	Beschreibung
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die maximale Anzahl von Hosts angeben möchten.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die maximale Anzahl von Hosts angeben möchten.
Trust		Nein	Wählen Sie im Auswahlfeld „Nein“, wenn der spezifizierte Port kein „Trusted Port“ sein soll.
		Ja	Wählen Sie im Auswahlfeld „Ja“, wenn der spezifizierte Port ein „Trusted Port“ sein soll.
Maximale Host-Anzahl (Bereich: 1~32)		32	Geben Sie im Eingabefeld die maximale Anzahl von Hosts ein, die sich gleichzeitig mit einem Port verbinden dürfen. Gültiger Bereich: 1 ... 32
Port-Status			
Parameter		Standardwert	Beschreibung
Port		1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Trust		Nein Ja	In dieser Spalte wird der Status des „Trusted Port“ angezeigt.
Maximale Host-Anzahl			In dieser Spalte wird die maximale Anzahl von Hosts, die sich gleichzeitig mit einem Port verbinden dürfen, angezeigt.

9.4.1.1.3 Server-Screening

Hinweis



Weitere Information

Weitere Informationen zu „Server-Screening“ finden Sie im Kapitel „Funktionsbeschreibung“.

DHCP-Snooping		
DHCP-Snooping Port-Einstellungen Server-Screening		
Server-Screening-Einstellungen		
IP-Adresse		
Anwenden Aktualisieren Konfiguration speichern		
Server-Screening-Liste		
Nr.	IP-Adresse	Aktion
1	225.225.225.225	Löschen

Abbildung 97: WBM-Seite „DHCP Snooping“ – Register „Server-Screening“

Tabelle 96: WBM-Seite „DHP Snooping“ – Register „Server-Screening“

Server-Screening-Einstellungen		
Parameter	Standardwert	Beschreibung
IP-Adresse		Geben Sie im Eingabefeld die IP-Adresse eines gültigen DHCP-Servers ein
Server-Screening-Liste		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Indexnummer des DHCP-Servereintrags angezeigt. Klicken Sie auf die Nummer, um den Eintrag zu modifizieren.
IP-Adresse		In dieser Spalte wird die IP-Adresse des DHCP-Servers angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

9.4.1.2 DHCP-Snooping-Binding-Tabelle

Hinweis**Weitere Information**

Weitere Informationen zur „DHCP-Snooping-Binding-Tabelle“ finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.1.2.1 Static-Entry-Einstellungen

DHCP-Snooping-Binding-Tabelle

Static-Entry-Einstellungen **Binding-Tabelle**

Static-Entry-Einstellungen

MAC-Adresse

IP-Adresse

VLAN ID

Port ▼

Static-Binding-Tabelle

Nr.	MAC-Adresse	IP-Adresse	Gültigkeitsdauer (Stunden)	VLAN	Port	Typ	Aktion

Abbildung 98: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Static-Entry-Einstellungen“

Tabelle 97: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Static-Entry-Einstellungen“

Static-Entry-Einstellungen		
Parameter	Standardwert	Beschreibung
MAC-Adresse		Geben Sie im Eingabefeld die MAC-Source-Adresse für die Verbindung ein.
IP-Adresse		Geben Sie im Eingabefeld die der MAC-Source-Adresse zugewiesene IP-Adresse für die Verbindung ein.
VLAN-ID		Geben Sie im Eingabefeld die Source-VLAN-ID für die Verbindung ein.
Port	1 ... 10 (12)	Wählen Sie im Auswahlfeld den physikalischen Port der Verbindung aus.
Static-Binding-Tabelle		
Parameter	Standardwert	Beschreibung
Nr.	1 ... 10 (12)	In dieser Spalte werden die fortlaufenden Nummern für jede Verbindung angezeigt. Klicken Sie darauf, um die bestehenden Einträge zu aktualisieren.
MAC-Adresse		In dieser Spalte wird die MAC-Adresse für die Verbindung angezeigt.
IP-Adresse		In dieser Spalte wird die der MAC-Source-Adresse zugewiesene IP-Adresse für die Verbindung angezeigt.
Gültigkeitsdauer (Stunden)		In dieser Spalte wird angezeigt, wie lange die Verbindung gültig ist.
VLAN		In dieser Spalte wird die Source-VLAN-ID für die Verbindung angezeigt.
Port	1 ... 10 (12)	In dieser Spalte wird die Port-Nummer für die Verbindung angezeigt.
Typ	Static Dynamic	In dieser Spalte angezeigt, wie die Verbindung dem Switch mitgeteilt wurde. „Static“: Diese Verbindung wurde manuell durch einen Administrator eingetragen. „Dynamic“: Diese Verbindung wurde durch Informationen aus dem „DHCP-Snooping“ eingetragen.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

9.4.1.2.2 Binding-Tabelle

Abbildung 99: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Binding-Tabelle“

Tabelle 98: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Binding-Tabelle“

DHCP-Snooping-Binding-Tabelle		
Parameter	Standardwert	Beschreibung
Anzeigeart	Alle	Wählen Sie im Auswahlfeld „Alle“, wenn Sie alle Einträge der Binding-Tabelle anzeigen möchten.
	Dynamisch	Wählen Sie im Auswahlfeld „Dynamisch“, wenn Sie die dynamischen Einträge der Binding-Tabelle anzeigen möchten.
	Statisch	Wählen Sie im Auswahlfeld „Statisch“, wenn Sie die statischen Einträge der Binding-Tabelle anzeigen möchten.
Parameter	Standardwert	Beschreibung
Alle	1 ... 10 (12)	In dieser Spalte werden die fortlaufenden Nummern für jede Verbindung angezeigt. Klicken Sie darauf, um die bestehenden Einträge zu aktualisieren.
MAC-Adresse		In dieser Spalte wird die MAC-Adresse für die Verbindung angezeigt.
IP-Adresse		In dieser Spalte wird die der MAC-Source-Adresse zugewiesene IP-Adresse für die Verbindung angezeigt.
Gültigkeitsdauer (Stunden)		In dieser Spalte wird angezeigt, wie lange die Verbindung gültig ist.
VLAN		In dieser Spalte wird die Source-VLAN-ID für die Verbindung angezeigt.
Port		In dieser Spalte wird die Port-Nummer für die Verbindung angezeigt. Bleibt dieses Feld leer, wird die Verbindung auf alle Ports übertragen.
Typ	Static Dynamic	In dieser Spalte wird angezeigt, wie die Verbindung dem Switch mitgeteilt wurde. „Static“: Diese Verbindung wurde manuell durch einen Administrator eingetragen. „Dynamic“: Diese Verbindung wurde durch Informationen aus dem „DHCP-Snooping“ eingetragen.

9.4.1.3 ARP-Überprüfung

Hinweis



Weitere Information

Weitere Informationen zur ARP-Überprüfung („**A**ddres **R**esolution **P**rotocol-Überprüfung“) finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.1.3.1 ARP-Überprüfung

ARP-Überprüfung

ARP-ÜberprüfungFilter-Tabelle

ARP-Inspection-Einstellungen

StatusAusschalten
VLAN-StatusHinzufügen
Trusted Ports
☐ Alle auswählen ☐ Auswahl aufheben
☐ 1 ☐ 3 ☐ 5 ☐ 7 ☐ 9 ☐ 11
☐ 2 ☐ 4 ☐ 6 ☐ 8 ☐ 10 ☐ 12
AnwendenAktualisierenKonfiguration speichern

ARP-Inspektionsstatus

ARP-Inspektionsstatus	Ausschalten
Einschalten an VLAN	Keine
Trusted Ports	Keine

Abbildung 100: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“

Tabelle 99: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“

ARP-Überprüfung-Einstellungen				
Parameter		Standardwert	Beschreibung	
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die ARP-Überprüfung beim Switch deaktivieren möchten.	
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die ARP-Überprüfung beim Switch aktivieren möchten.	
VLAN-Status		Ergänzen	Wählen Sie im Auswahlfeld „Ergänzen“ und tragen Sie die VLANs ein, für die die ARP-Überprüfung beim Switch aktiviert werden 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 keine ARP-Überprüfung ausführen soll.	
Trusted Ports			Wählen Sie die Ports aus, die Sie als „Trusted Ports“ auswählen bzw. abwählen möchten. Der Switch wird in keinem Fall ARP-Pakete von „Trusted Ports“ verwerfen. Der Switch wird DHCP-Pakete von „Untrusted Ports“ in folgenden Situationen verwerfen: - Die Senderinformationen in einem ARP-Paket stimmen mit keiner der aktuellen Verbindungen überein. - Die Übertragungsrate der empfangenen DHCP-Pakete ist zu hoch. Sie können die maximale Rate für den Empfang an „Untrusted Ports“ spezifizieren.	
	Auswählen Alle	☐	☐	Es ist kein Port als „Trusted“ ausgewählt.
			☒	Es sind alle Ports als „Trusted“ ausgewählt.
	Auswahl aufheben	☐	☐	Es ist kein Port als „Trusted“ deaktiviert.
			☒	Es sind alle Ports als „Trusted“ deaktiviert.
	☐ 1 ... ☐ 10 (12)	☐	☐	Der Port ist nicht aktiviert.
			☒	Der Port ist aktiviert.
ARP-Inspektionsstatus				
Parameter		Standardwert	Beschreibung	
ARP-Inspektionsstatus		Ausschalten Einschalten	In diesem Anzeigefeld wird der aktuelle Status der ARP-Überprüfung angezeigt.	
Einschalten an VLAN		Keine 1 ... 10 (12)	In diesem Anzeigefeld werden die VLAN-IDs angezeigt, für die die ARP-Überprüfung aktiviert ist.	
Trusted Ports		Keine 1 ... 10 (12)	In diesem Anzeigefeld werden die Ports angezeigt, die als „Trusted Ports“ spezifiziert sind.	

9.4.1.3.2 Filtertabelle

Hinweis



Weitere Information

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

ARP-Überprüfung

ARP-Überprüfung
Filter-Tabelle

Filter-Age-Time-Einstellungen

Filter Age Time min (Bereich: 1-10080)

Anwenden
Aktualisieren
Konfiguration speichern

Filter-Tabelle

Nr.	MAC-Adresse	VLAN	Port	Ablaufzeit (min)	Aktion
Anzahl: 0 Datensatz(s)					

Abbildung 101: WBM-Seite „ARP-Überprüfung“ – Register „Filtertabelle“

Tabelle 100: WBM-Seite „ARP-Überprüfung“ – Register „Filtertabelle“

Filter-Age-Time-Einstellungen		
Parameter	Standardwert	Beschreibung
Filter-Age-Time min (Bereich: 1~10080)	5	Geben Sie im Eingabefeld eine Zeitangabe ein, wie lange ein MAC-Adressfiltereintrag im Switch bestehen bleiben soll, nachdem der Switch ein nicht autorisiertes ARP-Paket empfangen hat. Zeitraum: 1 ... 10.080 min Nach Ablauf dieser Zeit wird der Switch den Eintrag automatisch löschen. Diese Einstellung hat keine Auswirkung auf bereits bestehende MAC-Adressfilter.
Filtertabelle		
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte werden die fortlaufenden Nummern jedes MAC-Adressfiltereintrags angezeigt.
MAC-Adresse		In dieser Spalte werden die MAC-Source-Adressen im MAC-Adressfilter angezeigt.
VLAN		In dieser Spalte werden die Source-VLAN-IDs im MAC-Adressfilter angezeigt.
Port		In dieser Spalte werden die Source-Ports der verworfenen ARP-Pakete angezeigt.
Ablaufzeit (min)		In dieser Spalte wird angezeigt, wie lange (in Minuten) ein MAC-Adressfiltereintrag im Switch bestehen bleibt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.
Anzahl		In diesem Anzeigefeld wird die Gesamtanzahl der aktuellen MAC-Adressfiltereinträge angezeigt, die der Switch aufgrund erkannter, nicht autorisierter ARP-Pakete erstellt hat.

9.4.2 Access-Control-Liste (ACL)

Hinweis



Weitere Information

Weitere Informationen zur „Access-Control-Liste“ finden Sie im Kapitel „Funktionsbeschreibung“.

Access-Control-Liste

Access-Control-Listen-Einstellungen

IP Type	IPv4 ▾				
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			
DSCP	beliebig ▾		0 ▾		
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 ▾	-- ▾			
Anwenden Aktualisieren Konfiguration speichern					

Access-Control-Listen-Status

IP Type	IPv4				
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		
DSCP	Any				
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				
Löschen					

Abbildung 102: WBM-Seite „Access-Control-Liste“

Tabelle 101: WBM-Seite „Access-Control-Liste“

Access-Control-Listen-Einstellungen		
Parameter	Standardwert	Beschreibung
IP-Typ	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.
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, weiter zu leiten.
	Verwerfen	Wählen Sie im Auswahlfeld „Verwerfen“, um Datenpakete, die den Angaben entsprechen zu verwerfen.
	DSCP	Wählen Sie im Auswahlfeld „DSCP“, um Datenpaketen, die den Angaben entsprechen, eine neue Priorität zu geben. (nur bei IPv4)
ETHERNET-Typ (nur bei IPv4)	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 (nur bei IPv4)	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 (nur bei IPv4)		Geben Sie im Eingabefeld die Source-MAC-ID der Bitmap-Maske für MAC-Source-Adressen von Datenpaketen 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 (nur bei IPv4)	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 (nur bei IPv4)		Geben Sie im Eingabefeld die Destination-MAC-Adresse der Bitmap-Maske für MAC-Destination-Adressen von Datenpaketen 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.

Tabelle 101: WBM-Seite „Access-Control-Liste“

DSCP (nur bei IPv4)	beliebig	Wählen Sie im Auswahlfeld „beliebig“, damit jede DSCP-Priorität für die Zugriffskontrollliste gültig ist.	
	Andere	0 ... 63	Wählen Sie im Auswahlfeld die DSCP-Priorität aus.
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.	
Maske der Source-IP-Adresse		Geben Sie im Eingabefeld die Source-IP-Adresse der Bitmap-Maske für IP-Source-Adressen von Datenpaketen 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 Datenpaketen 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 Protocol	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 101: WBM-Seite „Access-Control-Liste“

Access-Control-Liste-Status		
Parameter	Standardwert	Beschreibung
IP-Typ	IPv4 IPv6	In diesem Anzeigefeld wird der gewählte IP-Typ angezeigt.
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 (nur bei IPv4)	beliebig Andere	In diesem Anzeigefeld wird der ETHERNET-Typ angezeigt.
VLAN	beliebig Andere	In diesem Anzeigefeld wird die VLAN-ID angezeigt.
Source-MAC-Adresse (nur bei IPv4)	beliebig Andere	In diesem Anzeigefeld wird die Source-Mac-Adresse angezeigt.
Maske der Source-MAC-Adresse (nur bei IPv4)		In diesem Anzeigefeld wird die Source-MAC-ID der Bitmap-Maske angezeigt.
Destination-MAC-Adresse (nur bei IPv4)	beliebig Andere	In diesem Anzeigefeld wird die Destination-MAC-Adresse angezeigt.
Maske der Destination-MAC-Adresse (nur bei IPv4)		In diesem Anzeigefeld wird die Destination-MAC-ID der Bitmap-Maske angezeigt.
DSCP (nur bei IPv4)	beliebig Andere	In diesem Anzeigefeld wird die DSCP-Priorität angezeigt.
IP Protocol	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-Adresse angezeigt.
Maske der Destination-IP-Adresse		In diesem Anzeigefeld wird die Destination-IP-Adresse 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	In diesem Anzeigefeld wird das Source-Interface angezeigt.

9.4.3 IEEE 802.1X

Hinweis



Weitere Information

Weitere Informationen zum Standard „IEEE 802.1X“ finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.3.1 Globale Einstellungen

IEEE802.1X			
Globale Einstellungen		Port-Einstellungen	
Globale Einstellungen			
Status	Ausschalten ▾		
Authentifizierungsverfahren	Lokal ▾		
Gast-VLAN	0		
Primärer Radius-Server	IP :	UDP Port :	Shared Key :
Sekundärer Radius-Server	IP :	UDP Port :	Shared Key :
Lokal authentifizierter Benutzer	Keine ▾ User Name : Password :		
Anwenden Aktualisieren Konfiguration speichern			
Globaler Status			
Status	Ausschalten		
Authentifizierungsverfahren	Lokal		
Gast-VLAN	0		
Primärer Radius-Server	IP : -	UDP Port : -	Shared Key : -
Sekundärer Radius-Server	IP : -	UDP Port : -	Shared Key : -
Lokal authentifizierter Benutzer	admin,		

Abbildung 103: WBM-Seite „IEEE 802.1X“ – Register „Globale Einstellungen“

Tabelle 102: WBM-Seite „IEEE 802.1X“ – Register „Globale Einstellungen“

Globale Einstellungen			
Parameter	Standardwert	Beschreibung	
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die IEEE-802.1X-Authentifizierung beim Switch zu deaktivieren.	
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die IEEE-802.1X-Authentifizierung beim Switch zu aktivieren.	
		Hinweis  IEEE-802.1X-Authentifizierung Sie müssen erst die IEEE-802.1X-Authentifizierung beim Switch aktivieren, bevor sie diese Funktion für einzelne Ports konfigurieren können.	
Authentifizierungsverfahren	Lokal	Wählen Sie im Auswahlfeld „Lokal“, um die Benutzergruppen „Gast“ und „Benutzer“ der Benutzerkontendatenbank des Switches zur Authentifizierung zu nutzen. Die Anzahl der Konten, die gleichzeitig nebeneinander bestehen können, ist jedoch begrenzt.	
	Radius	Wählen Sie im Auswahlfeld „Radius“, um das Sicherheitsprotokoll, das im Gegensatz zur internen Benutzerdatenbank in Geräten mit begrenzter Speicherkapazität einen externen Server zur Benutzerauthentifizierung nutzt, zu aktivieren. Grundsätzlich ermöglicht „Radius“ die Validierung einer unbegrenzten Anzahl von Benutzern von einem zentralen Standort aus.	
Gast-VLAN		In diesem Anzeigefeld wird die VLAN-ID konfiguriert.	
Primärer Radius-Server		Haben Sie beim Authentifizierungsverfahren „Radius“ ausgewählt, wird der primäre Radius-Server für alle Authentifizierungsanfragen verwendet.	
	IP:	Geben Sie im Eingabefeld die IP-Adresse des externen Radius-Servers in Dezimalpunktschreibweise ein.	
	UDP-Port:	Geben Sie im Eingabefeld den UDP-Port ein	
	Shared Key:	Geben Sie in diesem Eingabefeld ein Passwort (aus bis 32 alphanumerischen Zeichen) ein, das Sie als gemeinsamen Schlüssel für die Verbindung zwischen dem externen Radius-Server und dem Switch verwenden. Dieser Schlüssel darf nicht über das Netzwerk gesendet werden. Die Schlüssel auf dem externen Radius-Server und dem Switch müssen identisch sein.	

Tabelle 102: WBM-Seite „IEEE 802.1X“ – Register „Globale Einstellungen“

Globale Einstellungen				
Parameter		Standardwert	Beschreibung	
Sekundärer Radius-Server			Dies ist der Back-up-Server, der nur zum Einsatz kommt, wenn der primäre Radius-Server ausfällt.	
	IP:		Geben Sie im Eingabefeld die IP-Adresse des externen Radius-Servers in Dezimalpunktschreibweise ein.	
	UDP-Port:	0 ... 65535	Geben Sie im Eingabefeld Port-Nummer des Radius-Servers ein.	
	Shared Key:		Geben Sie im Eingabefeld ein Passwort (aus bis 32 alphanumerischen Zeichen) ein, das Sie als gemeinsamen Schlüssel für die Verbindung zwischen dem externen Radius-Server und dem Switch verwenden. Dieser Schlüssel darf nicht über das Netzwerk gesendet werden. Die Schlüssel auf dem externen Radius-Server und dem Switch müssen identisch sein.	
Lokal authentifizierter Benutzer			In diesen Eingabefeldern werden der User Name und das Passwort angezeigt, ergänzt oder gelöscht.	
		Keine	Haben Sie im Auswahlfeld „Keine“ gewählt, dann können Sie den User Name und das Passwort nicht ändern.	
		Löschen	User Name:	Haben Sie im Auswahlfeld „Löschen“ gewählt, können Sie den User Name ändern.
		Hinzufügen	Password:	Haben Sie im Auswahlfeld „Ergänzen“ gewählt, können Sie den User Name und das Passwort ändern.
Globaler Status				
Parameter		Standardwert	Beschreibung	
Status		Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob die IEEE-802.1X-Authentifizierung aktiviert oder deaktiviert ist.	
Authentifizierungsverfahren		Lokal Radius	In diesem Anzeigefeld wird das Authentifizierungsverfahren angezeigt.	
Gast-VLAN			In diesem Anzeigefeld wird das Gast-VLAN angezeigt.	
Primärer Radius-Server	IP:		In diesen Anzeigefeldern werden die IP-Adresse, der UDP-Port und der gemeinsame Schlüssel für den primären Radius-Server angezeigt. Die Felder sind leer, wenn keine Konfiguration ausgeführt wurde.	
	UDP-Port:			
	Shared Key:			
Sekundärer Radius-Server	IP:		In diesen Anzeigefeldern werden die IP-Adresse, der UDP-Port und der gemeinsame Schlüssel für den sekundären Radius-Server angezeigt. Die Felder sind leer, wenn keine Konfiguration ausgeführt wurde.	
	UDP-Port:			
	Shared Key:			
Lokal authentifizierter Benutzer		admin,	In diesem Anzeigefeld wird die Auflistung der angemeldeten User angezeigt.	

9.4.3.2 Port-Einstellungen

IEEE802.1X

Globale Einstellungen
Port-Einstellungen

Port-Einstellungen

Port von: an:
IEEE802.1X-Status Ausschalten

Control Direction	Erneute Authentifizierung	Port Control Mode	Guest VLAN	Max-req Times
Beide	Ausschalten	Auto	Ausschalten	2

Reauth-period	Quiet-period	Supp-timeout	Server-timeout	Default-Einstellungen setzen!
3600	20	30	16	☐

Hinweis: Nicht alle Ports gleichzeitig auf "Einschalten" einstellen.

Anwenden
Aktualisieren
Konfiguration speichern

Port-Status

Port	IEEE802.1X-Status	Control Direction	Erneute Authentifizierung	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
2	Einschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
3	Einschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
4	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
5	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
6	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
7	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
8	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
9	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
10	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
11	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
12	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16

Abbildung 104: WBM-Seite „IEEE-802.1X“ – Register „Port-Einstellungen“

Tabelle 103: WBM-Seite „IEEE-802.1X“ – 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.
IEEE-802.1X-Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die IEEE-802.1X-Authentifizierung für den Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die IEEE-802.1X-Authentifizierung für den Port zu aktivieren.
		Hinweis  IEEE-802.1X-Authentifizierung Sie müssen erst die IEEE-802.1X-Authentifizierung beim Switch aktivieren, bevor sie diese Funktion für einzelne Ports konfigurieren können.	
Control-Direction		Beide	Wählen Sie im Auswahlfeld „Beide“, wenn nach der fehlgeschlagenen IEEE-802.1X-Port-Authentifizierung eines Benutzers sowohl am Port eingehende als auch ausgehende Datenpakete verworfen werden sollen.
		Eingang	Wählen Sie im Auswahlfeld „Eingang“, wenn nach der fehlgeschlagenen IEEE-802.1X-Port-Authentifizierung eines Benutzers nur am Port eingehende Datenpakete verworfen werden sollen.
Erneute Authentifizierung		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn ein Teilnehmer den Benutzernamen und das Passwort nicht regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn ein Teilnehmer den Benutzernamen und das Passwort regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.
Port Control Mode		Auto	Wählen Sie im Auswahlfeld „Auto“, um die Authentifizierung für den Port zu aktivieren.
		Autorisierung erzwingen	Wählen Sie im Auswahlfeld „Autorisierung erzwingen“, um eine permanente Authentifizierung für den Port zu aktivieren.
		Nicht-Autorisierung erzwingen	Wählen Sie im Auswahlfeld „Nicht-Autorisierung erzwingen“, um eine permanente Verweigerung der Authentifizierung für den Port zu aktivieren. Dadurch können an diesem Port keine Datenpakete weitergeleitet werden.
Guest VLAN		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um das Gast-VLAN an dem Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das Gast-VLAN an dem Port zu aktivieren.
Max-req Times		2	Geben Sie im Eingabefeld einen Wert für die maximal erforderlichen Zeiträume ein, die der Switch versuchen soll, sich mit dem Authentifizierungsserver zu verbinden, bevor er den Server als nicht verbunden ansieht.

Tabelle 103: WBM-Seite „IEEE-802.1X“ – Register „Port-Einstellungen“

Reauth-period	3600	Geben Sie in diesem Eingabefeld einen Wert für den zeitlichen Abstand ein, in dem ein Teilnehmer den Benutzernamen und das Passwort erneut eingeben muss, um mit dem Port verbunden zu bleiben.	
Quiet-period	60	Geben Sie im Eingabefeld einen Wert für den Zeitraum ein, den ein Client warten muss, bevor er die nächste Authentifizierungsanfrage stellen darf. Dadurch wird eine Überlastung des Switches durch fortlaufende Anfragen von Clients verhindert.	
Supp-timeout	30	Geben Sie im Eingabefeld einen Wert für die Zeit ein, die der Switch warten muss, bevor er mit dem Server kommuniziert.	
Server-timeout	30	Geben Sie im Eingabefeld einen Wert für die Zeit ein, die der Switch auf die Antwort des Authentifizierungsservers warten soll.	
Default-Einstellungen setzen!	☐	☐	Es werden keine angepassten Einstellungen für die IEEE-802.1X-Port-Authentifizierung auf die Default-Werte zurückgesetzt.
		☒	Es werden die angepassten Einstellungen für die IEEE-802.1X-Port-Authentifizierung auf die Default-Werte zurückgesetzt.

Tabelle 103: WBM-Seite „IEEE-802.1X“ – Register „Port-Einstellungen“

Port-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
IEEE-802.1X-Status	Ausschalten Einschalten	In dieser Spalte wird angezeigt, ob die IEEE-802.1X-Authentifizierung für einen Port aktiviert oder deaktiviert ist.
Control-Direction	Beide Eingang	In dieser Spalte wird die „Control-Direction“ angezeigt.
Erneute Authentifizierung	Ausschalten Einschalten	In dieser Spalte wird angezeigt, ob der Teilnehmer den Benutzernamen und das Passwort regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.
Port Control Mode	Auto, Autorisierung erzwingen, Nicht-Autorisierung erzwingen	In dieser Spalte wird der Port-Control-Mode angezeigt.
Guest VLAN	Ausschalten Einschalten	In dieser Spalte wird die Gast-VLAN-Einstellung für Hosts angezeigt, bei denen die Authentifizierung fehlgeschlagen ist.
Max-req Times	1 ... 10	In dieser Spalte wird angezeigt, wie oft der Switch versuchen wird, sich mit dem Authentifizierungsserver zu verbinden, bevor er den Server als nicht verbunden ansieht.
Reauth-period	0 ... 65535	In dieser Spalte wird angezeigt, in welchem zeitlichen Abstand ein Teilnehmer den Benutzernamen und das Passwort erneut eingeben muss, um mit dem Port verbunden zu bleiben.
Quiet-period	0 ... 65535	In dieser Spalte wird der Zeitraum angezeigt, den ein Client warten muss, bevor er die nächste Authentifizierungsanfrage stellen darf.
Supp-timeout	0 ... 65535	In dieser Spalte wird angezeigt, wie lange der Switch warten soll, bevor er mit dem Server kommuniziert.
Server-timeout	0 ... 65535	In dieser Spalte wird angezeigt, wie lange der Switch warten soll, bevor er mit dem Client kommuniziert.

9.4.4 Port Security

9.4.4.1 Port Security

Hinweis



Weitere Information

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

Port Security

Port Security
Sticky-MAC-Einstellungen

Port-Security-Einstellungen

Port Security Ausschalten

Port	Status	Sticky Status	Maximale MAC-Adresse
von: 1 an: 1	Ausschalten	Ausschalten	5 (1~1000)

Anwenden
Aktualisieren
Konfiguration speichern

Port-Security-Status

Port	Status	Sticky Status	Maximale MAC-Adresse	Port	Status	Sticky Status	Maximale MAC-Adresse
1	Ausschalten	Ausschalten	5	2	Ausschalten	Ausschalten	5
3	Ausschalten	Ausschalten	5	4	Ausschalten	Ausschalten	5
5	Ausschalten	Ausschalten	5	6	Ausschalten	Ausschalten	5
7	Ausschalten	Ausschalten	5	8	Ausschalten	Ausschalten	5
9	Ausschalten	Ausschalten	5	10	Ausschalten	Ausschalten	5
11	Ausschalten	Ausschalten	5	12	Ausschalten	Ausschalten	5

Abbildung 105: WBM-Seite „Port Security“ – Register „Port Security“

Tabelle 104: WBM-Seite „Port Security“ – Register „Port Security“

Port-Security-Einstellungen			
Parameter		Standardwert	Beschreibung
Port Security		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Port-Sicherheit beim Switch zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Port-Sicherheit beim Switch zu aktivieren.
Port	von:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Sicherheit“ zu konfigurieren.
	an:	1	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port-Sicherheit“ zu konfigurieren.
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Port-Sicherheit für einen Port bzw. Port-Bereich zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Port-Sicherheit für einen Port bzw. Port-Bereich zu aktivieren.
Maximale MAC-Adresse (1~1000)		5	Geben Sie im Eingabefeld die maximale Anzahl der MAC-Adressen pro Schnittstelle ein.
Port-Security-Status			
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 Port-Sicherheit aktiviert oder deaktiviert ist.
Maximale MAC-Adresse		0 ... 1000	In dieser Spalte wird die maximale Anzahl von MAC-Adressen angezeigt.

9.4.4.2 Sticky-MAC-Einstellungen

Hinweis



Weitere Information

Weitere Informationen zu „Sticky-MAC-Einstellungen“ finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 106: WBM-Seite „Port Security“ – Register „Sticky-MAC-Einstellungen“

Tabelle 105: WBM-Seite „Port Security“ – Register „Sticky-MAC-Einstellungen“

Sticky-MAC-Einstellungen		
Parameter	Standardwert	Beschreibung
MAC-Adresse		Geben Sie im Eingabefeld die MAC-Adresse für die Verbindung ein.
VLAN-ID		Geben Sie im Eingabefeld die Source-VLAN-ID für die Verbindung ein.
Port	1 ... 10 (12)	Wählen Sie im Auswahlfeld den physikalischen Port der Verbindung aus.
Port-Security-Status		
Parameter	Standardwert	Beschreibung
MAC-Adresse		In dieser Spalte wird die MAC-Adresse für die Verbindung angezeigt.
VLAN ID		In dieser Spalte wird die VLAN ID für die Verbindung angezeigt.
Port	1 ... 10 (12)	In dieser Spalte werden die Port-Nummern angezeigt.
Aktion		Klicken Sie auf [Löschen] , um einen bestimmten Eintrag zu löschen.

9.5 Monitor

9.5.1 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 107: WBM-Seite „Alarminformationen“

Tabelle 106: 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 (12) 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.

9.5.2 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 108: WBM-Seite „Systeminformationen“

Tabelle 107: WBM-Seite „Systeminformationen“

Hardware-Informationen		
Parameter	Standardwert	Beschreibung
Temperatureinheit	Celsius (C)	Wählen Sie im Auswahlfeld „Celsius (C)“, wenn Sie die Temperatur in Celsius anzeigen wollen.
	Fahrenheit (F)	Wählen Sie im Auswahlfeld „Fahrenheit (F)“, wenn Sie die Temperatur in Fahrenheit anzeigen wollen.
Hardware-Monitor-Alarm	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Hardware-Monitor-Alarm“ zu aktivieren.
	Ausschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Hardware-Monitor-Alarm“ zu deaktivieren.
Hardware-Information		
Parameter	Standardwert	Beschreibung
Temperatur (C)		
Aktuelle		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)		
Aktuelle		In dieser Spalte wird die aktuelle Spannung für die Eingänge „1,0 V IN“, „1,8 V IN“ und „5,0 V IN“ angezeigt.
MAX		In dieser Spalte wird die maximale Spannung für die Eingänge „1,0 V IN“, „1,8 V IN“ und „5,0 V IN“ angezeigt.
MIN		In dieser Spalte wird die minimale Spannung für die Eingänge „1,0 V IN“, „1,8 V IN“ und „5,0 V IN“ angezeigt.
Schwelle		In dieser Spalte wird die eingestellte Schwelle angezeigt.
Status		In dieser Spalte wird der Status angezeigt.

9.5.3 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 109: WBM-Seite „Port-Statistik“

Tabelle 108: WBM-Seite „Port-Statistik“

Port-Statistik		
Parameter	Standardwert	Beschreibung
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Receive Drops		In dieser Spalte wird die Anzahl der verworfenen Datenpakete auf der Empfangsleitung angezeigt.
Transmit Drops		In dieser Spalte wird die Anzahl der verworfenen Datenpakete auf der Sendeleitung angezeigt.
Receive Errors		In dieser Spalte werden die Fehler auf der Empfangsleitung angezeigt.
Transmit Errors		In dieser Spalte werden die Fehler auf der Sendeleitung angezeigt.
Receive Packets		In dieser Spalte wird die Anzahl der seit dem Einschalten empfangenen Datenpakete angezeigt.
Transmit Packets		In dieser Spalte wird die Anzahl der seit dem Einschalten gesendeten Datenpakete angezeigt.
Receive Bytes		In dieser Spalte wird die Anzahl der empfangenen Bytes auf dem Port seit dem Einschalten angezeigt.
Transmit Byte		In dieser Spalte wird die Anzahl der gesendeten Bytes auf dem Port seit dem Einschalten angezeigt.

9.5.4 Port-Auslastung

Hinweis



Weitere Information

Weitere Informationen zu „Port-Auslastung“ finden Sie im Kapitel „Funktionsbeschreibung“.

Port-Auslastung					
Status der Port-Auslastung					
Port	Geschwindigkeit	RX Traffic Auslastung(%)	RX Traffic Auslastung(bps)	TX Traffic Auslastung(%)	TX Traffic Auslastung(bps)
1	1000	0.00	0	0.00	170
8	100	0.12	120738	0.43	438445
11	1000	0.00	170	0.00	0
Aktualisieren					

Abbildung 110: WBM-Seite „Port-Auslastung“

Tabelle 109: WBM-Seite „Port-Auslastung“

Status der Port-Auslastung		
Parameter	Standardwert	Beschreibung
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Geschwindigkeit		In dieser Spalte wird die Transferringeschwindigkeit angezeigt.
RX-Traffic-Auslastung (%)		In dieser Spalte wird die prozentuale Auslastung der RX-Bandbreite angezeigt.
RX-Traffic-Auslastung (bps)		In dieser Spalte wird die Auslastung der RX-Bandbreite in bps angezeigt.
TX- Traffic-Auslastung (%)		In dieser Spalte wird die prozentuale Nutzung der TX-Bandbreite angezeigt.
RX- Traffic-Auslastung (bps)		In dieser Spalte wird die Nutzung der RX-Bandbreite in bps angezeigt.

9.5.5 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	CRCAAlignErrors 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 111: WBM-Seite „RMON-Statistiken“

Tabelle 110: WBM-Seite „RMON-Statistiken“

RMON-Statistiken			
Parameter		Standardwert	Beschreibung
Port		-	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie keine Statistik ansehen möchten.
		1 ... 10 (12) Alle	Wählen Sie im Auswahlfeld einen Port oder alle Ports aus, für den (die) Sie die RMON-Statistiken anzeigen möchten.
Port x (aktiv)			
Parameter		Standardwert	Beschreibung
Inbound	Total Octets		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt.
	BroadcastPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Broadcast-Pakete angezeigt.
	UnicastPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Unicast-Pakete angezeigt.
	Non-unicastPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Summe der Broadcast-Pakete und Multicast-Pakete angezeigt.
	MulticastPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Multicast-Pakete angezeigt.
	Fragmentierte Pkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen fragmentierten Datenpakete angezeigt.
	UndersizePkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu kleinen Datenpakete angezeigt.
	OversizePkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu großen Datenpakete angezeigt.
	DiscardsPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die verworfenen wurden.
	ErrorPkts		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die fehlerhaft waren.
	UnknownPkts		In diesem Anzeigefeld wird die Anzahl der von diesem Port empfangenen Datenpakete angezeigt, die als Ziel ein unbekanntes oder nicht unterstütztes Protokoll enthielten.
	AlignError		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-AlignErrors		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.
	DropEvents		In diesem Anzeigefeld wird die Anzahl der verworfenen Datenpakete angezeigt.

Tabelle 110: WBM-Seite „RMON-Statistiken“

Outbound	Total Octets		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt.
	BroadcastPkts		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Broadcast-Pakete angezeigt.
	UnicastPkts		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Non-unicastPkts		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Collisions		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	LateCollision		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	SingleCollision		In diesem Anzeigefeld wird die Anzahl der Einzelkollisionen der gesendeten Datenpakete angezeigt.
	MultipleCollision		In diesem Anzeigefeld wird die Anzahl der Mehrfachkollisionen der gesendeten Datenpakete angezeigt.
	DiscardPkts		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die verworfenen wurden.
	ErrorPkts		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die fehlerhaft waren.
#(Anzahl) der Datenpakete, welche mit einer Länge von ? empfangen wurden.	64 Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 64 Oktetten hatten.
	65 bis 127 Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 65 bis 127 Oktetten hatten.
	128 bis 255 Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 128 bis 255 Oktetten hatten.
	256 bis 511 Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 256 bis 511 Oktetten hatten.
	512 bis 1023 Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 512 bis 1023 Oktetten hatten.
	1024 bis max. Octets		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von mehr als 1024 Oktetten hatten.

9.5.6 SFP-Information

Hinweis



Weitere Information

Weitere Informationen zu „SFP“ (Small Form-factor Pluggable) finden Sie im Kapitel „Funktionsbeschreibung“.

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 112: WBM-Seite „SFP-Information“

Tabelle 111: WBM-Seite „SFP-Information“

SFP-Information		
Parameter	Standardwert	Beschreibung
Port	-	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie kein SFP-Modul gesteckt haben
	9, 10, (11, 12)	Wählen Sie im Auswahlfeld den Port aus, in dem Sie ein SFP-Modul gesteckt haben.
SFP-Information		
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		In diesem Anzeigefeld wird die Wellenlänge angezeigt.
Übertragungsentfernung		In diesem Anzeigefeld wird die Übertragungsentfernung angezeigt.
DDM-Unterstützung		In diesem Anzeigefeld wird angezeigt, ob das SFP-Modul das DDM („Dynamic Device Mapping“) unterstützt.
Hersteller		In diesem Anzeigefeld wird der Name des SFP-Anbieters angezeigt.
Teilenummer		In diesem Anzeigefeld wird die Teilenummer angezeigt.
Revisionsstand		In diesem Anzeigefeld wird der Revisionsstand der Teilenummer angezeigt.
Seriennummer		In diesem Anzeigefeld wird die Seriennummer (ASCII) angezeigt.
Datum		In diesem Anzeigefeld wird das Datum der Version angezeigt.

Tabelle 111: WBM-Seite „SFP-Information“

DDMI-Informationen		
Parameter	Standardwert	Beschreibung
Aktuell		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		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		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		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		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)

9.5.7 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	Sperrzeit
von: 1 ▾	Ausschalten ▾	Keine ▾	Broadcast ▾	100	Einschalten ▾	1	3
an: 1 ▾							

Anwenden Aktualisieren Konfiguration speichern

Traffic-Monitor-Status

Port	Status	Status	Pakettyp	Paketrate(pps)	Recovery-Status	Recovery-Zeit	Sperrzeit
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 113: WBM-Seite „Traffic-Monitor“

Tabelle 112: 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	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		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.
		Freischalten	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.
Recovery-Zeit		1	Geben Sie im Eingabefeld die Recovery-Zeit für die Funktion „Traffic-Monitor“ an diesen Ports ein. Gültiger Bereich: 1 ... 60 Minuten
Sperrzeit		3	Geben Sie im Eingabefeld einen Wert für die „Sperrzeit“ beim „Traffic-Monitor“ ein.

Tabelle 112: WBM-Seite „Traffic-Monitor“

Traffic-Monitor-Status		
Parameter	Standardwert	Beschreibung
Port	1 ... 10 (12)	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	1 ... 60	In dieser Spalte wird die gewählte Recovery-Zeit angezeigt.
Sperrzeit	3	In dieser Spalte wird die gewählte „Sperrzeit“ angezeigt.

9.6 Management

9.6.1 SNMP

9.6.1.1 SNMP

Hinweis



Weitere Information

Weitere Informationen zu „SNMP“ (Simple Network Management Protocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.6.1.1.1 SNMP-Einstellungen

Abbildung 114: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“

Tabelle 113: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“

SNMP-Einstellungen		
Parameter	Standardwert	Beschreibung
SNMP-Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um das SNMP beim Switch zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das SNMP beim 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.

9.6.1.1.2 Community Name

SNMP

SNMP Settings **Community Name**

Community Name Settings

Community String	Rights	IP version	Network ID of Trusted Host	Number of Mask Bit
	Read-Only ▾	IPv4 ▾		

Community Name List

No.	Community String	Rights	IP version	Network ID of Trusted Host	Number of Mask Bit	Action

Abbildung 115: WBM-Seite „SNMP“ – Register „Community Name“

Tabelle 114: 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 beim Switch zu konfigurieren.
IP-Version	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.
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 Strings“ 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.
IP-Version	IPv4 IPv6	In diesem Anzeigefeld wird der gewählte IP-Typ 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.

9.6.1.2 SNMP-Trap

Hinweis



Weitere Information

Weitere Informationen zu „SNMP-Trap“ (Simple Network Management Protocol Trap) finden Sie im Kapitel „Funktionsbeschreibung“.

9.6.1.2.1 Trap-Receiver-Einstellungen

SNMP Trap					
Trap Receiver-Einstellungen			Trap Event Status	Trap Port-Einstellungen	
Trap-Receiver-Einstellungen					
IP-Version	IP-Adresse	Version	Community String		
IPv4 ▾		v1 ▾			
Anwenden Aktualisieren Konfiguration speichern					
Trap-Receiver-Liste					
Nr.	IP-Version	IP-Adresse	Version	Community String	Action

Abbildung 116: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“

Tabelle 115: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“

Trap-Receiver-Einstellungen		
Parameter	Standardwert	Beschreibung
IP-Version	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.
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-Version	IPv4 IPv6	In dieser Spalte wird der gewählte IP-Typ angezeigt.
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.

9.6.1.2.2 Trap Event Status

Abbildung 117: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“

Tabelle 116: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“

Trap-Event-State-Einstellungen		
Parameter	Standardwert	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)
xpress-ring	☒	Aktiviert / Deaktiviert das SNMP-Trap, wenn der Port von „Xpress Ring“ blockiert wird.
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.
pd-alive	☒	Aktiviert / Deaktiviert das SNMP-Trap, wenn das PD-Gerät keine Antworten hat.
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.
config-change	☒	Aktiviert / Deaktiviert das SNMP-Trap, wenn die Konfiguration geändert wird.

9.6.1.2.3 Trap-Port-Einstellungen

SNMP Trap

Trap Receiver-Einstellungen Trap Event Status **Trap Port-Einstellungen**

Port Link-Change Trap Einstellung

Port	Status
von: 1 ▼ an: 1 ▼	Einschalten ▼
Anwenden Aktualisieren	

Port Link-Change Trap 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 118: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“

Tabelle 117: 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.
State		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.

9.6.1.3 SNMPv3-Konfiguration

9.6.1.3.1 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

noauth ▾

Auth-Algorithmus

MD5 ▾

Auth Password

Priv-Algorithmus

DES ▾

Priv Password

Anwenden

Aktualisieren

Konfiguration speichern

SNMPv3-User-Status

User Name	Gruppenname	Auth Protokoll	Priv Protokoll	Rowstatus	Aktion
user1	qwe	No Auth	No Priv	Active	Löschen

Abbildung 119: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“

Tabelle 118: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“

SNMPv3-User-Einstellungen		
Parameter	Standardwert	Beschreibung
User Name		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.
Security Level		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
User Name		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.

9.6.1.3.2 SNMPv3-Gruppen

SNMPv3-Konfiguration

SNMPv3 User
SNMPv3-Gruppen
SNMPv3 View

SNMPv3-Gruppeneinstellungen

Gruppenname

Security Level noauth ▼

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 120: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-Gruppen“

Tabelle 119: 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.
Security Level		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 Model		In dieser Spalte wird das gewählte Sicherheitslevel angezeigt.
Security Level		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.

9.6.1.3.3 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 121: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3 View“

Tabelle 120: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3 View“

SNMPv3-View-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.

9.6.2 Auto Provision

Hinweis



Weitere Information

Weitere Informationen zur „Auto Provision“ (Automatische Bereitstellung) finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 122: WBM-Seite „Auto Provision“

Tabelle 121: WBM-Seite „Auto Provision“

Auto-Provision-Einstellungen		
Parameter	Standardwert	Beschreibung
Status	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Auto Provision“ beim Switch zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Auto Provision“ beim Switch zu aktivieren.
Status	Ausschalten	In diesem Anzeigefeld wird der Status der „Auto Provision“ angezeigt.
Version	0	In diesem Anzeigefeld wird die Version angezeigt.
Protokoll	FTP	Wählen Sie im Auswahlfeld „FTP“ („File Transfer Protocol“), wenn Sie diesen Typ als Auto-Provision-Server wählen möchten.
	TFTP	Wählen Sie im Auswahlfeld „TFTP“ („Trivial File Transfer Protocol“), wenn Sie diesen Typ als Auto-Provision-Server wählen möchten.
	HTTP	Wählen Sie im Auswahlfeld „HTTP“ („Hypertext Transfer Protocol“), wenn Sie diesen Typ als Auto-Provision-Server wählen möchten.
Server-IP-Adresse		Geben Sie im Eingabefeld die ID für die IP-Subnetzmaske des Servers in Dezimalpunktschreibweise ein.
User Name		Geben Sie im Eingabefeld den Namen für den FTP-Server ein.
Password		Geben Sie im Eingabefeld das Passwort für den FTP-Server ein.
Verzeichnis		Wählen Sie in diesem Eingabefeld die Ordnerstruktur des FTP-Servers aus.

9.6.3 Mail-Alarm

Hinweis**Weitere Information**

Weitere Informationen zum „Mail-Alarm“ finden Sie im Kapitel „Funktionsbeschreibung“.

Mail-Alarm

Mail-Alarm-Einstellungen

Status:

Server-IP-Adresse: Server-Port: (Default:25)

Account Name: Account Password:

Mail von:

Mail an:

UTF-8 encoding:

Trap-Status :

☐ Alle auswählen ☐ Alle deaktivieren

☐ Systemneustart ☐ Port-Link-Änderung ☐ Konfigurationsänderung ☐ Firmware Upgrade

☐ User Login ☐ Port gesperrt ☐ Alarmierung

Abbildung 123: WBM-Seite „Mail-Alarm“

Tabelle 122: WBM-Seite „Mail-Alarm“

Mail-Alarm-Einstellungen				
Parameter		Standardwert	Beschreibung	
Status		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion „Mail-Alarm“ zu deaktivieren.	
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Mail-Alarm“ zu aktivieren.	
Server-IP-Adresse		IP	Wählen Sie im Auswahlfeld „IP“, wenn Sie die Server-IP des Mail-Servers nutzen möchten.	
		IPv6	Wählen Sie im Auswahlfeld „IPv6“, wenn Sie die Server-IP des IPv6-Servers nutzen möchten.	
		Domain	Wählen Sie im Auswahlfeld „Domain“, wenn Sie die Domain-Adresse des Mail-Servers nutzen möchten.	
		0.0.0.0	Geben Sie im Eingabefeld die IP-Adresse ein.	
Server-Port (Default:25)		25	Geben Sie im Eingabefeld den TCP-Port für das SMTP ein.	
Account Name			Geben Sie im Eingabefeld den Namen des E-Mail-Kontos ein.	
Account Password			Geben Sie im Eingabefeld das Passwort des E-Mail-Kontos ein.	
Mail von			Geben Sie im Eingabefeld den Namen des E-Mail-Absenders ein.	
Mail an			Geben Sie im Eingabefeld den Namen des E-Mail-Empfängers ein.	
Trap-Status	Alle auswählen	☐	☐	Es ist kein Port für das Versenden von Ereignis-Traps ausgewählt.
			☒	Es sind alle Ports für das Versenden von Ereignis-Traps ausgewählt.
	Alle deaktivieren	☐	☐	Es ist kein Port für das Versenden von Ereignis-Traps deaktiviert.
			☒	Es sind alle Ports für das Versenden von Ereignis-Traps deaktiviert.
	Systemneustart	☐	☐	Der Port ist nicht aktiviert..
			☒	Der Port ist aktiviert.
	Port-Link-Änderung	☐	☐	Es ist der Zustand „Port-Link-Änderung“ deaktiviert.
			☒	Es ist der Zustand „Port-Link-Änderung“ aktiviert.
	Konfigurations-änderung	☐	☐	Es ist der Zustand „Konfigurationsänderung“ deaktiviert.
			☒	Es ist der Zustand „Konfigurationsänderung“ aktiviert.
	Firmware Upgrade	☐	☐	Es ist der Zustand „Firmware Upgrade“ deaktiviert.
			☒	Es ist der Zustand „Firmware Upgrade“ aktiviert.
	User Login	☐	☐	Es ist der Zustand „User Login“ deaktiviert.
			☒	Es ist der Zustand „User Login“ aktiviert.
	Port gesperrt	☐	☐	Es ist der Zustand „Port gesperrt“ deaktiviert.
			☒	Es ist der Zustand „Port gesperrt“ aktiviert.
	Alarmierung	☐	☐	Es ist der Zustand „Alarmierung“ deaktiviert.
			☒	Es ist der Zustand „Alarmierung“ aktiviert.

9.6.4 Wartung

9.6.4.1 Konfiguration

Abbildung 124: WBM-Seite „Wartung“ – Register „Konfiguration“

Konfiguration Speichern

- Klicken Sie auf die Schaltfläche **[Konfiguration 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 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.

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.

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.

9.6.4.2 Firmware



Abbildung 125: 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.

9.6.4.3 Neustart



Abbildung 126: 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:

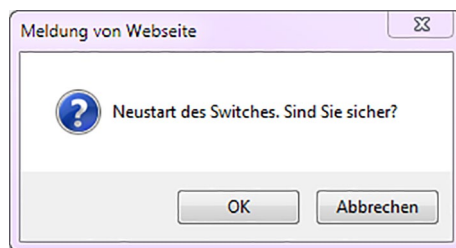


Abbildung 127: WBM-Seite „Wartung“ – Register „Rebooten“ – Meldung

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.

9.6.4.4 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 128: WBM-Seite „Wartung“ – Register „Protokolle“

Tabelle 123: 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.

9.6.5 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.

Note



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 Anzeigen Aktualisieren Löschen Speichern

```

<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 129: WBM-Seite „System-Log“

Tabelle 124: 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.

9.6.6 Ping

Hinweis



Weitere Information

Weitere Informationen zum Befehl „Ping“ finden Sie im Kapitel „Funktionsbeschreibung“.

Abbildung 130: WBM-Seite „Ping“

Tabelle 125: WBM-Seite „Ping“

Ping		
Parameter	Standardwert	Beschreibung
Target-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.

9.6.7 USB-Funktionen

Über die USB-Schnittstelle des Switch können folgende Funktionen ausgeführt werden:

- Upload der Firmware
- Speichern der Konfigurationsdatei
- Speichern der Syslog-Datei
- Upload der Konfigurationsdatei

USB-Funktionen

Konfiguration der USB-Funktionen

Funktion	Status
Firmware automatisch hochladen	Einschalten ▼
Konfigurationsdatei automatisch speichern	Einschalten ▼
Syslog-Datei automatisch speichern	Einschalten ▼
Konfigurationsdatei automatisch hochladen	Einschalten ▼

AnwendenAktualisierenKonfiguration speichern

USB-Funktionen

Konfiguration der USB-Funktionen

Funktion	Status
Firmware automatisch hochladen	Einschalten ▼
Konfigurationsdatei automatisch speichern	Einschalten ▼
Syslog-Datei automatisch speichern	Einschalten ▼
Konfigurationsdatei automatisch hochladen	Einschalten ▼

AnwendenAktualisierenKonfiguration speichern

Abbildung 131: WBM-Seite „USB-Funktionen“

Tabelle 126: WBM-Seite „USB-Funktionen“

Konfiguration der USB-Funktionen		
Parameter	Standardwert	Beschreibung
Funktion		In dieser Spalte können Sie die USB-Funktion auswählen.
Firmware automatisch hochladen Konfigurationsdatei automatisch speichern	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion zu aktivieren.
Syslog-Datei automatisch speichern Konfigurationsdatei automatisch hochladen	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um die Funktion zu deaktivieren.

9.6.8 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:

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 beim Switch anmelden und ein neues Konto einrichten.

Nr.	Name	Autorität	Aktion
1	admin	Admin	

Abbildung 132: WBM-Seite „Benutzerkonto“

Tabelle 127: 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.
User Authority		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.
Parameter	Standardwert	Beschreibung
Nr.		In dieser Spalte wird die Indexnummer eines Eintrags angezeigt.
Name		In dieser Spalte wird der Name des Benutzerkontos angezeigt.
Authorität		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.

10 Anhang

10.1 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:

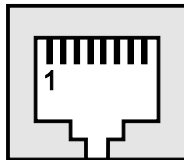


Abbildung 133: RJ-45 Anschlussbelegung

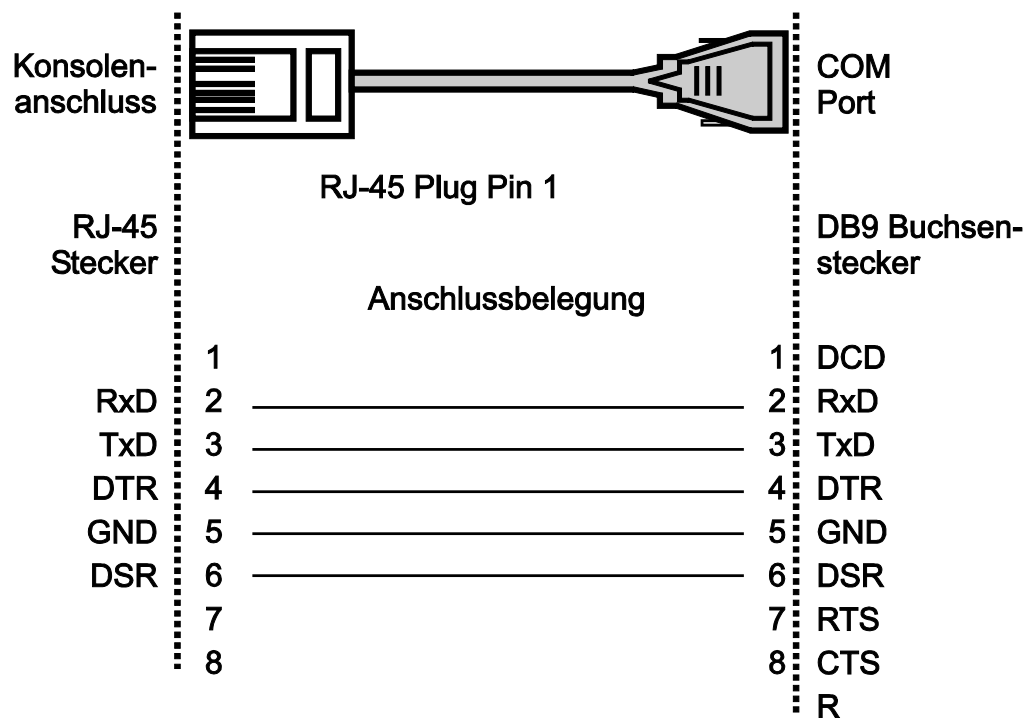


Abbildung 134: Anschlussbelegung RJ-45 zu DB9

10.2 RJ-45-Kabel

Verwenden Sie beim Anschließen Ihrer Netzwerkgeräte standardmäßige ETHERNET-Kabel. Die Anschlussbelegung ist wie folgt:

Tabelle 128: 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.

10.3 Configuring in the Command Line Interface (CLI)

10.3.1 System Status

10.3.1.1 System Information

Table 129: 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 address A.B.C.D/M	This command configures the static IP and subnet mask for the system.
interface	show	This command displays the current port configuration.
acl	show	This command displays the current access control list.
vlan	show	This command displays the current VLAN configuration.
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 utilization and memory information.
enable	show uptime	This command displays the system uptime.

10.3.2 Basic Settings

10.3.2.1 System

Table 130: 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.
eth0	ip ipv6-addressAAAA:BBBB:CCC C:DDDD:EEEE:FFFF:GG GG:HHHH/M	This command configures a global scope of IPv6 address and subnet mask for the system.
eth0	ip ipv6-addressdefault-gatewayAAAA:BBBB:CCC C:DDDD:EEEE:FFFF:GG GG:HHHH	This command configures a default gateway for the system.
eth0	ip ipv6-dhcp client (disable enable renew)	This command configures a DHCPv6 client function for the system.

10.3.2.1.1 Jumbo Frame

Table 131: 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.
configure	interface IFNAME	This command enters the interface configure node.
interface	jumboframe(10240 1522 1536 1552 9010 9216)	This command configures the maximum number of bytes of frame size.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	jumboframe(10240 1522 1536 1552 9010 9216)	This command configures the maximum number of bytes of frame size.

10.3.2.1.2 SNTP

Table 132: 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 ntp-server domain-name STRING	This command sets the domain names 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
```

10.3.2.1.3 Management Host

Table 133: 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
```

10.3.2.2 MAC Management

Table 134: 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
```

10.3.2.2.1 Blackhole MAC

Table 135: CLI "Blackhole MAC" Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current rejected MAC address only.
configure	mac-address-table refusal MACADDR vlan VLANID	This command configures the rejection of a MAC address in a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures the rejection of a MAC address.

Example

```
L2SWITCH(config)#mac-address-table refusal 00:11:22:33:44:55
```

```
L2SWITCH(config)#mac-address-table refusal 00:11:22:33:44:55 vlan 1
```

10.3.2.3 Port Mirroring

Table 136: 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 3-10 mode both*

10.3.2.4 Port Settings:

Table 137: 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	This command diagnostics the Ethernet cable and shows the broken distance.
interface	clean cable-test result	This command cleans the test result of the Ethernet cable test.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/PORTLISTS	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.

ExampleL2SWITCH#*configure terminal*L2SWITCH(config)#*interface gil/0/1*L2SWITCH(config-if)#*speed auto*

10.3.3 Advanced Settings

10.3.3.1 Bandwidth Control

10.3.3.1.1 QoS

Table 138: 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 802.1p mappings.

10.3.3.1.2 Rate Limitation

Table 139: 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*

10.3.3.1.2.1 Storm Control

Table 140: 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*

10.3.3.2 IGMP Snooping

Table 141: 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.
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.

if-range	igmp-querier-mode (auto fixed edge)	This command specifies whether or not and under what conditions the ports are (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
```

10.3.3.2.1 IGMP Snooping Querier

Table 142: 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.

10.3.3.2.2 IGMP Snooping Filtering

Table 143: 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/PORTLISTS	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.

10.3.3.2.3 MVR

Table 144: CLI "MVR" Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLANID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current "IGMP Snooping" configurations.
configure	mvr VLANID	This command creates the MVR configurations for the specific VLAN.
configure	no mvr VLANID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command creates a group configuration for the MVR.
MVR	no group NAME	This command deletes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic compatible)	This command configures the mode for the MVR. - Dynamic: Sends "IGMP reports" to all MVR source ports in the multicast VLAN. - Compatibility: The switch does not send any "IGMP Reports".
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port or receiver port range. Normally, the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the list of receiver ports.
MVR	source-port PORTLIST	This command sets the source port or source port range. Normally, the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the list of source ports.
MVR	tagged PORTLIST	This command assigns a tagged port or port range. The same applies to VLAN tagged ports.
MVR	no tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).
MVR	priority-override (disable enable)	This command enables/disables the multicast priority override.

10.3.3.2.4 Multicast Address

Table 145: 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.

10.3.3.3 VLAN

10.3.3.3.1 Port Isolation

Table 146: 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*

10.3.3.3.2 VLAN Settings

Table 147: 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 147: 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*

10.3.3.3.3 GARP/GVRP

Table 148: CLI "GARP/GVRP" Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations for one port or all ports.
enable	show garp timer	This command displays the timers for GARP.
configure	gvrp (disable enable)	This command disables/enables GVRP on the switch.
configure	no gvrp configuration	This command resets the GVRP configuration to the default setting.
interface	gvrp (disable enable)	This command disables/enables GVRP on a specific port.
interface	gvrp registration (normal forbidden)	This command configures the registration mode for GVRP on a specific port.
interface	no gvrp configuration	This command resets the GVRP configuration for a specific port to the default setting.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the "Join Time," "Leave Time" and "Leaveall Time" for GVRP on a specific port.
interface	no garp time	This command resets the Join, Leave and Leave all times for GVRP on a specific port to the default settings.

10.3.3.3.4 IP Subnet VLAN

Table 149: CLI "IP Subnet VLAN" Configuration

Node	Command	Description
enable	show ip-subnet-vlan	This command displays the all of the IP subnet vlan configurations.
configure	ip-subnet-vlan ip IPADDR mask IPADDR vlan <1-4094> priority <0-7>	This command creates an IP subnet vlan entry with the IP address, subnet mask, vlan and priority.
configure	no ip-subnet-vlan ip IPADDR	This command deletes an IP subnet vlan entry.
configure	no ip-subnet-vlan all	This command deletes all of the IP subnet vlan entries.

Example

```
L2SWITCH(config)#ip-subnet-vlan 192.168.203.1 mask 255.255.255.0 vlan2
priority 31
```

```
L2SWITCH#show ip-subnet-vlan
```

10.3.3.3.5 MAC VLAN

Table 150: 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
```

10.3.3.3.6 Protocol VLAN

Table 151: CLI "Protocol VLAN" Configuration

Node	Command	Description
enable	show protocol-vlan	This command displays the all of the protocol-vlan configurations.
configure	protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with ethernetII frame type.
configure	protocol-vlan frame-type nonLLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with nonLLC-SNAP frame type.
configure	protocol-vlan frame-type LLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with LLC-SNAP frame type.
configure	no protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID	This command deletes a protocol-vlan entry with ethernetII frame type.
configure	no protocol-vlan frame-type nonLLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with nonLLC-SNAP frame type and vlan.
configure	no protocol-vlan frame-type LLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with LLC-SNAP frame type and vlan.
configure	no protocol-vlan all	This command deletes all of the protocol-vlan entries.

Example

L2SWITCH(config)# *protocol-vlan frame-type LLC-SNAP vlan 12 ports 1-2*

L2SWITCH(config)# *protocol-vlan frame-type ethernetII ether-type 0800 vlan 14 ports 1-2*

10.3.3.3.7 Q-in-Q**10.3.3.3.7.1 VLAN Stacking**

Table 152: CLI "VLAN Stacking" Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current vlan-stacking type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
configure	vlan-stacking (disable port-based selective)	This command disables the vlan stacking or enable the vlan-stacking with port-based or selective on the switch.
configure	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with the name.
configure	no vlan-stacking selective-qinq STRINGS	This command removes the selective Q-in-Q profile with the name.
configure	vlan-stacking tpid-table index<2-6> value STRINGS	This command configures TPID table.
interface	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
interface	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the customer's VLAN range on the incoming packets.
qinq	spvid VLANID	This command sets the service provider's VLAN ID for outgoing packets in selective Q-in-Q.
qinq	priority <0-7>	This command sets priority in selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the access ports to apply the rule.
qinq	tunnel-ports PORTLISTS	This command specifies the tunnel ports to apply the rule.

Table 152: CLI "VLAN Stacking" Configuration

Node	Command	Description
qinq	end	The command exits the CLI Q-in-Q node and enters the CLI enable node.
qinq	exit	The command exits the CLI Q-in-Q node and enter the CLI configure node.
qinq	show	The command shows the current selective Q-in-Q profile configurations.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.

10.3.3.4 DHCP Relay

Table 153: CLI "DHCP Relay" Configuration

Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the DHCP relay.
configure	dhcp relay (disable enable)	This command disables/enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	This command configures the DHCP server's IP address.
configure	no dhcp helper-address	This command removes the DHCP server's IP address.

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)#*dhcp relay enable*

L2SWITCH(config)# *dhcp relay vlan 1*

L2SWITCH(config)# *dhcp helper-address 172.20.1.1*

10.3.3.5 DHCP Options

Table 154: CLI "DHCP Options" Configuration

Node	Command	Description
enable	show dhcp-options	This command displays the configurations and status for the DHCP option 66 and 67.
configure	dhcp-options option_66_67 (disable enable)	This command disables/enables the DHCP option 66 and 67 on the Switch.
configure	dhcp-options option_66_67 auto-backup	This command uploads the current configurations to TFTP server. The file name is vcmsh_config_MODEL-NAME_MAC if you didn't specify a filename for it.
configure	dhcp-options option_66_67 auto-backupfile FILENAME	This command configures a filename for the auto-backup function.

10.3.3.6 Dual Homing

Table 155: CLI "Dual Homing" Configuration

Node	Command	Description
enable	show dual-homing	This command displays the "Dual Homing" information.
configure	dual-homing (disable enable)	This command disables/enables the "Dual Homing" function in the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for "Dual Homing" from the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for "Dual Homing" from the system.
configure	dual-homing secondary-channel (port trunk) VALUE	This command configures the secondary channel for "Dual Homing" in the system. The channel can be a single port or a "Trunk Group".
configure	no dual-homing secondary-channel	This command deletes the secondary channel for "Dual Homing" from the system.

Example

```
L2SWITCH(config)# link-aggregation 1 ports 5-6
```

```
L2SWITCH(config)# link-aggregation 1 enable
```

```
L2SWITCH(config)# dual-homing primary-channel port 2
```

```
L2SWITCH(config)# dual-homing secondary -channel trunk 1
```

```
L2SWITCH(config)# dual-homing enable
```

10.3.3.7 ERPS

Table 156: CLI “ERPS” Configuration

Node	Command	Description
enable	show erps	This command displays the ERPS configurations.
enable	show erps instance	This command displays the ERPS instance configurations.
enable	show erps instance INSTANCE_ID	This command displays the specific ERPS instance configurations.
configure	erps enable	This command enables the global ERPS on the Switch.
configure	no erps enable	This command disables the global ERPS on the Switch.
configure	erps ring-id VALUE	This command creates an ERPS ring and its ID and enter ERPS node.
configure	erps instance	This command enters the instance configure node.
configure	no erps ring-id VALUE	This command creates an ERPS ring and enter ERPS node to configure detail ring configurations.
erps-ring	show	This command displays the configurations of the ring.
erps-ring	control-vlan	This command configures a control-vlan for the ERPS ring.
erps-ring	guard-timer	This command configures the Guard Timer for the ERPS ring. (default:500ms)
erps-ring	holdoff-timer	This command configures the Hold-off Timer for the ERPS ring. (default:0 ms)
erps-ring	left-port PORTID type [owner neighbor normal]	This command configures the left port and type for the ERPS ring.
erps-ring	mel VALUE	This command configures a Control MEL for the ERPS ring.
erps-ring	name STRING	This command configures a name for the ERPS ring.
erps-ring	revertive	This command configures the revertive mode for the ERPS ring.
erps-ring	no revertive	This command configures then on-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner neighbor normal]	This command configures the right port and type for the ERPS ring.
erps-ring	ring enable	This command enables the ring.
erps-ring	no ring enable	This command disables the ring.
erps-ring	version	This command configures a version for the ERPS ring.
erps-ring	wtr-timer	This command configures the WTR Timer for the ERPS ring. (default: 5 minutes)
config-erps-inst	instance INSTANCE_ID control-vlan VLAN_ID data-vlan VLAN_ID	This command configures a new instance and specifies its control vlan and data vlan.
config-erps-inst	no instance INSTANCE_ID	This command removes an instance.
config-erps-inst	show	This command displays all of the instance configurations.

10.3.3.8 Link Aggregation

Table 157: CLI “Link Aggregation” Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current configuration for “Trunking.”
configure	link-aggregation [GROUP_ID] (disable enable)	The command disables/enables “Trunking” for the specific “Trunk Group.”
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific “Trunk Group.”
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The command deletes ports from a specific “Trunk Group.”

Example

```
L2SWITCH(config)# configure terminal
```

```
L2SWITCH(config)# link-aggregation 1 enable
```

```
L2SWITCH(config)# link-aggregation 1 ports 1-4
```


10.3.3.8.1 LACP

Table 158: CLI "LACP" Configuration

Node	Command	Description
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor's information for the specific group or all groups.
enable	show lacp port_priority	This command c displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor's and partner's system ID.
configure	lacp (disable enable)	This command disables/enables the LACP on the switch.
configure	lacp GROUP_ID (disable enable)	This command disables/enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority<1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.
configure	interface range gigabitethernet1/0/PORTLI STS	This command enters the interface configure node.
if-range	lacp port_priority <1-65535>	This command configures the priority for the specific ports. Note: The default value is 32768.
if-range	no lacp port_priority	This command configures the default for the priority for the specific ports.

10.3.3.9 LLDP

Table 159: 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.

10.3.3.10 Loop Detection

Table 160: 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*

10.3.3.11 Modbus

Table 161: CLI "Modbus" Configuration

Node	Command	Description
enable	show modbus	This command displays the current Modbus configurations.
configure	modbus(disable enable)	This command disables/enables the Modbus on the switch.

10.3.3.12 Static Route

Table 162: CLI "Static Route" Configuration

Node	Command	Description
enable	show ip forwarding status	This command displays the current configuration of the ip forwarding status.
enable	show ip routes(all ipv4 ipv6)	This command displays the configurations of IPv4 or IPv6 or both routes from routing table.
enable	show ip arp(all ipv4 ipv6)	This command displays dynamic and static IPv4 or IPv6 or both ARP entries in ARP table.
enable	show ip hosts(all ipv4 ipv6)	This command displays assigned IPv4 or IPv6 or both addresses for interfaces in router.
configure	ip forwarding enable	This command enables layer 3 IPv4 and IPv6 forwarding/routing globally.
configure	no ip forwarding enable	This command disables layer 3 IPv4 and IPv6 forwarding/routing globally. This will delete all assigned IP addresses and static routes from interfaces.
configure	ip arp proxy enable	This command enables route to act as an ARP proxy globally; It will be useful in Inter VLAN routing.
configure	no ip arp proxy enable	This command disables route to act as an ARP proxy.
configure	ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command allows adding static IPv4 ARP entry in ARP table.
configure	ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command allows adding static IPv4 ARP entry in ARP table.
configure	ipv6 arp <IPv6_ADDR><MAC_ADDR>	This command allows adding static IPv6 ARP entry in ARP table.
configure	no ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command deletes a static IPv4 ARP entry from ARP table.
configure	interface vlan VLAN-ID	This command enters the L3 interface node.
L3 interface	ipv4 address A.B.C.D/M	This command assigns a specified IPv4 interface route to the interface. We can assign multiple IPv4 interface route to a single interface with different IP segment. If this configuration is a first IP assigning to the interface then automatically interface is enabled for routing.

Table 162: CLI "Static Route" Configuration

Node	Command	Description
L3 interface	ipv6 address <IPv6_ADDR>/M	This command assigns a specified IPv6 interface route to the interface. We can assign only one IPv6 interface route for an interface vlan. If this configuration is a first IP assigning to the interface then it automatically enables the interface with routing.
L3 interface	no ipv4 address A.B.C.D/M	This command deletes a specified IPv4 interface route from the interface vlan. This command deletes all dependent static routes on the specified IPv4 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface.
L3 interface	no ipv4 address <IPv6_ADDR>/M	This command deletes a specified IPv6 interface route from the interface. This command deletes all dependent static routes on the specified IPv6 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface vlan.
L3 interface	ipv4 route A.B.C.D/M A.B.C.D	This command configures anIPv4 static route onto the specified interface vlan.
L3 interface	ipv6 route <IPv6_ADDR>/M <IPv6_ADDR>	This command configures anIPv6 static route onto the specified interface vlan.
L3 interface	no ipv4 route A.B.C.D/M A.B.C.D	This command deletes a specified IPv4 static route from an interface vlan.
L3 interface	no ipv6 route<IPv6_ADDR>/M <IPv6_ADDR>	This command deletes a specified IPv6 static route from an interface vlan.

10.3.3.13 STP

Table 163: 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 163: 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 bpdufilter(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.

10.3.3.13.1 MSTP

Table 164: CLI "MSTP" Configuration

Node	Command	Description
enable	show spanning-tree mst configuration	This command displays the MSTP configurations.
enable	show spanning-tree mst instance	This command displays all of the instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63>	This command displays specific instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63>interface IFNAME	This command displays specific instance configurations on an interface of the MSTP.
enable	show spanning-tree mst interface IFNAME	This command displays the configurations on an interface of the MSTP.
enable	show spanning-tree mst root	This command displays the root bridge configurations.
configure	spanning-tree(disable enable)	This command enables / disables the spanning tree.
configure	spanning-tree mode mst	This command configures the mode of the spanning tree. (one of the three modes STP/RSTP/MSTP.)
configure	spanning-tree mst forward-time	This command configures the forward time for the MSTP.
configure	no spanning-tree mst forward-time	This command resets the forward time for the MSTP. The default forward delay time is 15 seconds.
configure	spanning-tree mst hello-time	This command configures the hello time for the MSTP.
configure	no spanning-tree mst hello-time	This command resets the hello time for the MSTP. The default hello time is 2 seconds.
configure	spanning-tree mst max-age	This command configures the maximum age time for the MSTP.
configure	no spanning-tree mst max-age	This command resets the maximum age time for the MSTP. The default maximum age time is 20 seconds.
configure	spanning-tree mst max-hops	This command configures the maximum hop count.
configure	no spanning-tree mst max-hops	This command resets the maximum hop count. The default maximum hop count is 20.
configure	spanning-tree mst instance STRING priority <0-61440>	This command resets the maximum hop count. The default maximum hop count is 20.
configure	no spanning-tree mst instance STRING priority	This command resets the priority for the specific instance.
interface	spanning-tree mst instance STRING cost <1-200000000>	This command configures a cost on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING cost	This command resets the cost on the specific port for the MSTP.
interface	spanning-tree mst instance STRING port-priority <0-240>	This command configures a priority on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING port-priority	This command resets the priority on the specific port for the MSTP.
configure	spanning-tree mst configuration	This command enters the MSTP configure node.

Table 164: CLI "MSTP" Configuration

Node	Command	Description
configure	no spanning-tree mst configuration	This command resets all of configurations for the MSTP.
mst	apply	This command applies configurations to current instant.
mst	instance	This command configures the instance and vlan map.
mst	name	This command configures a region name for the MSTP.
mst	no name	This command reset the region name for the MSTP.
mst	revision	This command configures the revision for the MSTP.
mst	no revision	This command resets the revision for the MSTP.
mst	show (current pending)	This command shows the MSTP configures. Current – the working configurations. Pending – the not applied configurations.

Example

L2SWITCH(config)# *spanning-tree mst configuration*

L2SWITCH(config)# *name MSTP*

L2SWITCH(config)# *revision 1*

L2SWITCH(config)# *instance 1 vlan 1-10*

10.3.3.14 Xpress Ring

Table 165: CLI "Xpress Ring" Configuration

Node	Command	Description
enable	show xpress-ring	This command displays the current Xpress-Ring configurations.
configure	xpress-ring(disable enable)	This command enables/disables the Xpress-Ring on the Switch.
configure	xpress-ring ring (RING1 RING2) state (disable enable)	This command enables/disables the ring on the Switch.
configure	xpress-ring ring (RING1 RING2) last-byte-destination-mac VALUE	This command configures the last byte of the destination MAC for the ring on the Switch.
configure	xpress-ring ring (RING1 RING2) role (forwarder arbiter)	This command configures the role (forwarder/arbiter) for the ring on the Switch.
configure	xpress-ring ring (RING1 RING2) primary-port PORTID	This command configures the primary port for the ring on the Switch. Note: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.
configure	xpress-ring ring (RING1 RING2) secondary-port PORTID	This command configures the secondary port for the ring on the Switch. Note: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.

10.3.4 Security

10.3.4.1 IP Source Guard

10.3.4.1.1 DHCP Snooping

Table 166: CLI “DHCP Snooping” Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current “DHCP Snooping” configurations.
configure	dhcp-snooping (disable enable)	This command disables/enables “DHCP Snooping” on the switch.
configure	dhcp-snooping vlan VLANID	This command enables the “DHCP Snooping” function on a VLAN or VLAN range.
configure	no dhcp-snooping vlan VLANID	This command disables the “DHCP Snooping” function on a VLAN or VLAN range.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	dhcp-snooping host	This command configures the maximum host count for the specific ports.
if-range	no dhcp-snooping host	This command configures the maximum host count to default for the specific ports.
if-range	dhcp-snooping trust	This command configures the trust port for the specific ports.
if-range	no dhcp-snooping trust	This command configures the un-trust port for the specific ports.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#dhcp-snooping enable
```

```
L2SWITCH(config)#dhcp-snooping vlan 1
```

```
L2SWITCH(config)#interface 1/0/1
```

```
L2SWITCH(config-if)#dhcp-snooping trust
```

10.3.4.1.1.1 Server Screening

Table 167: CLI "Server Screening" Configuration

Node	Command	Description
enable	show dhcp-snooping server	This command displays the IP address of the valid DHCP server.
configure	dhcp-snooping server IPADDR	This command configures the IP address of a valid DHCP server.
configure	no dhcp-snooping server IPADDR	This command deletes the IP address of a valid DHCP server.

10.3.4.1.2 Binding Table

Table 168: CLI "Binding Table" Configuration

Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current "DHCP Snooping" binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLANID port PORT_NO	This command configures a static host in the "DHCP Snooping" binding table.
configure	no dhcp-snooping binding mac MACADDR	This command deletes a static host from the "DHCP Snooping" binding table.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1 port 2*

L2SWITCH(config)#*no dhcp-snooping binding mac 00:11:22:33:44:55*

L2SWITCH#*show dhcp-snooping binding*

10.3.4.1.3 ARP Inspection

Table 169: CLI “ARP Inspection” Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current configurations for the ARP Inspection.
configure	arp-inspection (disable enable)	This command disables/enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLANID	This command enables the ARP Inspection function on a VLAN or VLAN range.
configure	no arp-inspection vlan VLANID	This command disables the ARP Inspection function on a VLAN or VLAN range.
interface	arp-inspection trust	This command configures the “Trusted Port” for the specific port.
interface	no arp-inspection trust	This command configures the “Untrusted Port” for the specific port.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#arp-inspection enable
```

```
L2SWITCH(config)#arp-inspection vlan 1
```

```
L2SWITCH(config)#interface 1/0/1
```

```
L2SWITCH(config-if)#arp-inspection trust
```

10.3.4.1.3.1 Filter Table

Table 170: CLI “Filter Table” Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current MAC address filter for the ARP Inspection.
configure	arp-inspection mac-filter age VALUE	This command configures the “Age Time” for the MAP address filter entries of the ARP Inspection.
configure	clear arp-inspection mac-filter	This command clears all of entries in the filter table.
configure	no arp-inspection mac-filter mac MACADDR vlan VLANID	This command deletes a MAC address filter entry from the MAC filter table of the ARP Inspection.

10.3.4.2 Access Control List

Table 171: CLI "Access Control List" Configuration

Node	Command	Description
enable	show access-list	This command displays all access control profiles.
configure	access-list STRING ip-type (ipv4 ipv6)	This command creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6.
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	action dscp remarking <0-63>	This command activates this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.
acl	action 802.1p remarking <0-7>	This command activates this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	This command configures the 802.1p value for the profile.
acl	dscp VALUE	This command configures the DSCP value for the profile.
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 AMC 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.

Table 171: CLI "Access Control List" Configuration

Node	Command	Description
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.
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
```

10.3.4.3 802.1X

Table 172: CLI “802.1X” Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1X configurations.
enable	show dot1x username	This command displays the current user accounts for local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable enable)	This command enables/disables 802.1X authentication on the switch.
configure	dot1x authentic-method (local radius)	This command configures the 802.1X authentication method.
configure	no dot1x authentic-method	This command sets the 802.1X authentication method to the default setting.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary RADIUS server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary RADIUS server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary RADIUS server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary RADIUS server.
configure	no dot1x radius secondary-server-ip	This command deletes the secondary RADIUS server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable enable)	This command enables/disables the local .1x accounting records.
configure	dot1x guest-vlan VLANID	This command configures the guest VLAN.
configure	no dot1x guest-vlan	This command deletes the guest VLAN.
interface	dot1x admin-control-direction (both in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command resets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the “Max Req Times” of a port (1 to 10).
interface	dot1x port-control (auto force-authorized force-unauthorized)	This command configures the port control mode for the port.
interface	dot1x authentication (disable enable)	This command enables/disables 802.1X authentication on the port.
interface	dot1x reauthentication (disable enable)	This command enables/disables the authentication interval on the port.
interface	dot1x timeout quiet-period	This command configures the “Quiet Period” value on the port.

Table 172: CLI "802.1X" Configuration

Node	Command	Description
interface	dot1x timeout server-timeout	This command configures the server timeout value on the port.
interface	dot1x timeout reauth-period	This command configures the authentication interval value on the port.
interface	dot1x timeout supp-timeout	This command configures the supplicant timeout value on the port.
interface	dot1x guest-vlan (disable enable)	This command configures the 802.1X state on the port.

10.3.4.4 Port Security

Table 173: CLI "Port Security" Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
config	port-security (disable enable)	This command enables/disables the global port security function.
interface	port-security (disable enable)	This command enables/disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum number of MAC address entries for the specific port.

10.3.5 Monitor

10.3.5.1 Alarm

Table 174: CLI "Alarm" Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

10.3.5.2 Monitor Information

Table 175: CLI "Monitor Information" Configuration

Node	Command	Description
enable	show hardware-monitor (C F)	This command displays hardware operation information.

10.3.5.3 Port Statistics

Table 176: CLI "Port Statistics" Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

10.3.5.4 Port Utilization

Table 177: CLI "Port Statistics" Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

10.3.5.5 RMON Statistics

Table 178: 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.

10.3.5.6 SFP Information

Table 179: 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.

10.3.5.7 Traffic Monitor

Table 180: 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.

10.3.6 Management

10.3.6.1 SNMP

10.3.6.1.1 SNMP

Table 181: 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*

10.3.6.1.2 SNMP Trap

Table 182: 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.

10.3.6.1.2.1 Port Trap Settings

Table 183: 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.

10.3.6.1.3 SNMPv3

Table 184: 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.

10.3.6.2 Auto Provision

Table 185: CLI "Auto Provision" Configuration

Node	Command	Description
enable	show auto-provision	This command displays the current auto provision configurations.
configure	auto-provision	This command enters the auto-provision node.
auto-provision	show	This command displays the current auto provision configurations.
auto-provision	active (enable disable)	This command enables/disables the auto provision function.
auto-provision	server-address IPADDR	This command configures the auto provision server's IP.
auto-provision	protocol (tftp http ftp)	The command configurations the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	The command configurations the username and password for the FTP server.
auto-provision	folder STRING	The command configurations the folder for the auto provision server.
auto-provision	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

10.3.6.3 Mail Alarm

Table 186: CLI "Mail Alarm" Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the Mail Alarm configurations.
configure	mail-alarm (disable enable)	This command disables/enables the Mail Alarm function.
configure	mail-alarm auth-account	This command configures the Mail server authentication account.
configure	mail-alarm mail-from	This command configures the mail sender.
configure	mail-alarm mail-to	This command configures the mail receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures the mail server IP address and the TCP port.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the mail server IP address and configures 25 as the server's TCP port.
configure	mail-alarm trap-event (reboot link- change config. firmware login port-blocked alarm) (disable enable)	This command disables/enables mail trap events.

10.3.6.4 Maintenance

Table 187: 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*

10.3.6.4.1 Reboot

Table 188: CLI "Reboot" Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	http server	This command enables the http on the Switch.
configure	no http server	This command disables the http on the Switch.
configure	http server port VALUE	This command configures the TCP port for the HTTP server.
configure	no http server port	This command resets the HTTP TCP port to 80.
configure	https server	This command enables the https on the Switch.
configure	no https server	This command disables the https on the Switch.
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	telnet server port VALUE	This command configures the TCP port for the TELNET server.
configure	no telnet server port	This command resets the TELNET TCP port to 23.

10.3.6.5 System Log

Table 189: 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 ipv6-ip IPADDR	The command configures the syslog server's IP address in IPv6 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#syslog-server ipv4-ip 192.168.200.106
```

```
L2SWITCH(config)#syslog-server enable
```


10.3.6.6 USB Flash

Table 190: CLI “USB Flash” Configuration

Node	Command	Description
enable	show usb status	This command displays the current USB function configurations.
configure	usb auto-upgrade-fw (disable enable)	This command disables/enables the USB upgrade firmware automatically.
configure	usb auto-download-config (disable enable)	This command disables/enables the USB download configuration file automatically.
configure	usb auto-download-syslog (disable enable)	This command disables/enables the USB download syslog file automatically.

Example

L2SWITCH#*show usb status*

L2SWITCH#*configure terminal*

L2SWITCH(config)#*usb auto-upgrade-fw enable*

L2SWITCH(config)#*usb auto-download-config enable*

L2SWITCH(config)#*usb auto-download-syslog enable*

10.3.6.7 User Account

Table 191: CLI "System Log" 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	The command deletes an existing user account.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#add user q q admin
```

```
L2SWITCH(config)#add user 1 1 normal
```

10.4 MODBUS/TCP-Tabellen

10.4.1 Datenformat und Funktionscode

MODBUS TCP unterstützt verschiedene Typen von Datenformaten zum Lesen.
Die wichtigsten 4 Arten sind:

Tabelle 192: Datenformat und Funktionscode

Datenzugriffstyp		Funktionscode	Funktionsname	Hinweis
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Wird nicht unterstützt.
	Internal Bits or Physical Coils	1	Read Coils	Wird nicht unterstützt.
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	
	Physical Output	3	Read Holding Registers	Wird nicht unterstützt.

10.4.2 MODBUS-Register

Die MODBUS-Adressraum der Industrial-Managed-Switches beginnt bei 1000 (dezimal) für den Funktionscode 4.

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
1000	3E8	1	HEX	Vendor ID = 0x30DE
1001	3E9	16	ASCII	Vendor Name = “WAGO” Word 0 Hi byte = ‘W’ Word 0 Lo byte = ‘A’ Word 1 Hi byte = ‘G’ Word 1 Lo byte = ‘O’ Word 2 Hi byte = ‘\0’
1032	408	16	ASCII	Product Name = “852-1305/000-001” Word 0 Hi byte = ‘8’ Word 0 Lo byte = ‘5’ Word 1 Hi byte = ‘2’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘3’ Word 3 Hi byte = ‘0’ Word 3 Lo byte = ‘5’ Word 4 Hi byte = ‘/’ Word 4 Lo byte = ‘0’ Word 5 Hi byte = ‘0’ Word 5 Lo byte = ‘0’ Word 6 Hi byte = ‘-’ Word 6 Lo byte = ‘0’ Word 7 Hi byte = ‘0’ Word 7 Lo byte = ‘1’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0’
1064	428	7	ASCII	Product Serial Number Ex: Serial No=A0000000000001

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
1080	438	12	ASCII	Firmware Version=" V1.0.2.S0" Word 0 Hi byte = 'V' Word 0 Lo byte = '1' Word 1 Hi byte = '.' Word 1 Lo byte = '0' Word 2 Hi byte = '.' Word 2 Lo byte = '2' Word 3 Hi byte = '.' Word 3 Lo byte = 'S' Word 4 Hi byte = '0' Word 4 Lo byte = '\0' Word 5 Hi byte = '\0' Word 5 Lo byte = '\0' Word 6 Hi byte = '\0' Word 6 Lo byte = '\0' Word 7 Hi byte = '\0' Word 7 Lo byte = '\0' Word 8 Hi byte = '\0' Word 8 Lo byte = '\0'
1096	448	16	ASCII	Firmware Release Date="Mon Jun 17 12:58:41 CST 2019"
1112	458	3	HEX	ETHERNET MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
1128	468	1	HEX	Power 1 (PWR) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage < 11.7V 0x0002: input voltage > 57V 0x0003: No PWR input
1129	469	1	HEX	Power 2(RPS) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage < 11.7V 0x0002: input voltage > 57V 0x0003: No RPS input
1144	478	1	HEX	Fault LED Status 0x0000: No 0x0001: Yes

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
Port Information				
		1	HEX	1256 (Port 1) ... 1267 (Port 12) Port 1 to 12 Link Status
				0x0000: Link down
1256	4E8			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1257	4E9			0x0002: 10M-Full-FC_OFF
1258	4EA			0x0003: 10M-Half-FC_ON
1259	4EB			0x0004: 10M-Half-FC_OFF
1260	4EC			0x0005: 100M-Full-FC_ON
1261	4ED			0x0006: 100M-Full-FC_OFF
1262	4EE			0x0007: 100M-Half-FC_ON
1263	4EF			0x0008: 100M-Half-FC_OFF
1264	4F0			0x0009: 1000M-Full-FC_ON
1265	4F1			0x000A: 1000M-Full-FC_OFF
1266	4F2			0x000B: 1000M-Half-FC_ON
1267	4F3			0x000C: 1000M-Half-FC_OFF
				0xFFFF: No port
		32	ASCII	Port 1 to 12 Medium
1512	5E8			Port Description = "100TX, RJ45." Or "1000TX, SFP."
1544	608			Word 0 Hi byte = '1'
1576	628			Word 0 Lo byte = '0'
1608	648			Word 1 Hi byte = '0'
1640	668			Word 1 Lo byte = 'T'
1672	688			...
1704	6A8			Word 4 Hi byte = '4'
1736	6C8			Word 4 Lo byte = '5'
1768	6E8			Word 5 Hi byte = '.'
1800	708			Word 5 Lo byte = '\0'
1832	728			
1864	748			
		2	HEX	2024 (Port 1) ... 2046 (Port 12) Port 1 to 12 Tx Packets
2024	7E8			Ex: port 1 Tx Packet Amount = 0x87654321
2026	7EA			Word 0 = 8765
2028	7EB			Word 1 = 4321
2030	7EE			
2032	7F0			
2034	7F2			
2036	7F4			
2038	7F6			
2040	7F8			
2042	7FA			
2044	7FC			
2046	7FE			

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
		2	HEX	2088 (Port 1) ... 2110 (Port 12) Port 1 to 12 Rx Packets
2088	828			Ex: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2090	82A			
2092	82C			
2094	82E			
2096	830			
2098	832			
2100	834			
2102	836			
2104	838			
2106	83A			
2108	83C			
2110	83E			
		2	HEX	2152 (Port 1) ... 2174 (Port 12) Port 1 to 12 Tx Error Packets
2152	868			Ex: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
2154	86A			
2156	86C			
2158	86E			
2160	870			
2162	872			
2164	874			
2166	876			
2168	878			
2170	87A			
2172	87C			
2174	87E			
		2	HEX	2216 (Port 1) ... 2238 (Port 12) Port 1 to 12 Rx Error Packets
2216	8A8			Ex: port 1 Rx Error Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2218	8AA			
2220	8AC			
2222	8AE			
2224	8B0			
2226	8B2			
2228	8B4			
2230	8B6			
2232	8B8			
2234	8BA			
2236	8BC			
2238	8BE			

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
Redundancy & Ring Information				
2280	8E8	1	HEX	Spanning Tree Status
				0x0000 : none
				0x0001 : STP
				0x0002 : RSTP
				0x0003 : MSTP
2281	8E9	1	HEX	Xpress-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2282	8EA	1	HEX	Jet-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2283	8EB	1	HEX	Dual-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2284	8EC	1	HEX	ERPS Status
				0x0000 : Disabled
				0x0001 : Enabled
2296	8F8	1	HEX	Xpress-ring Status Ring 1
				0x0000 : Disabled
				0x0001 : Enabled
2297	8F9	1	HEX	Xpress-ring Status Ring 2
				0x0000 : Disabled
				0x0001 : Enabled
2298	8FA	3	HEX	Xpress-ring MAC Ring 1
				Ex:
				Word 0 Hi byte = 0 x 00
				Word 0 Lo byte = 0 x 01
				Word 1 Hi byte = 0 x 02
				Word 1 Lo byte = 0 x 03
				Word 2 Hi byte = 0 x 04
				Word 2 Lo byte = 0 x 05
2301	8FD	3	HEX	Xpress-ring MAC Ring 2
				Ex:
				Word 0 Hi byte = 0 x 00
				Word 0 Lo byte = 0 x 01
				Word 1 Hi byte = 0 x 02
				Word 1 Lo byte = 0 x 03
				Word 2 Hi byte = 0 x 04
				Word 2 Lo byte = 0 x 05
2304	900	1	HEX	Primary Port of Xpress_Ring 1
				Ex: Port 5 = 0x0005
2305	901	1	HEX	Secondary Port of Xpress_Ring 1
				Ex: Port 6 = 0x0006

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
2306	902	1	HEX	Primary Port of Xpress_Ring 2 Ex: Port 5 = 0x0005
2307	903	1	HEX	Secondary Port of Xpress_Ring 2 Ex: Port 6 = 0x0006
2308	904	1	HEX	Xpress-ring Role Ring 1 0x0000 : Forwarder 0x0001 : Arbiter
2309	905	1	HEX	Xpress-ring Role Ring 2 0x0000 : Forwarder 0x0001 : Arbiter
2310	906	1	HEX	Xpress-ring Current status for Ring 1 Primary Port 0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2311	907	1	HEX	Xpress-ring Current status for Ring 1 Secondary Port 0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2312	908	1	HEX	Xpress-ring Current status for Ring 2 Primary Port 0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2313	909	1	HEX	Xpress-ring Current status for Ring 2 Secondary Port 0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
Jet-Ring Information				
2536	9E8	1	HEX	Jet Ring State 0x0000: Disabled. 0x0001: Enabled.
2537	9E9	3	HEX	Master Bridge MAC: Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.
2540	9EC	1	HEX	Jet Ring Total Nodes: Ex: When total nodes is 255(0xff). Word 0, high byte=0x00. Word 0, low byte=0xff.
2541	9ED	1	HEX	Bridge Role: 0x0000: Learning. 0x0001: Master. 0x0002: Arbiter. 0x0003: Forwarder. 0x0004: Pre-Forwarder.
		1	HEX	2552 (Port 1) ... 2563 (Port 12) Port Role (Port 1 to Port 12)
2552	9F8			0x0000: Disabled.
2553	9F9			0x0001: Listening.
2554	9FA			0x0002: Learning.
2555	9FB			0x0003: Forwarding.
2556	9FC			0x0004: Blocking.
2557	9FD			0x0005: No connection.
2558	9FE			
2559	9FF			
2560	A00			
2561	A01			
2562	A02			
2563	A03			

Tabelle 193: MODBUS-Register

Table 100: M02500 Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
		1	HEX	2584 (Port 1) ... 2595 (Port 12) Ring Role (Port 1 to Port 12)
2584	A18			0x0000: No
2585	A19			0x0001: Yes
2586	A1A			
2587	A1B			
2588	A1C			
2589	A1D			
2590	A1E			
2591	A1F			
2592	A20			
2593	A21			
2594	A22			
2595	A23			
Dual-Ring Information				
2792	AE8	1	HEX	Dual-Ring State: 0x0000: Disabled. 0x0001: Enabled.
2793	AE9	3	HEX	Xpress-ring MAC for Dual-Ring: Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.
2796	AEC	1	HEX	Xpress-ring Role for Dual-Ring: 0x0000 : Forwarder 0x0001 : Arbiter

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
2797	AED	1	HEX	Xpress-ring Current status for Dual-Ring Port-1 – (Primary Port) High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
2798	AEE	1	HEX	Xpress-ring Current status for Dual-Ring Port-2 – (Secondary Port) High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
2799	AEF	3	HEX	Sub-Ring Master Bridge MAC : Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.
2802	AF2	1	HEX	Jet Ring Total Nodes for Sub-Ring. Ex: When total nodes is 255(0xff). Word 0, high byte=0x00. Word 0, low byte=0xff.
2803	AF3	1	HEX	Bridge Role for Sub-Ring: 0x0000: Learning. 0x0001: Master. 0x0002: Arbiter. 0x0003: Forwarder. 0x0004: Pre-Forwarder.
2804	AF4	1	HEX	Sub-ring Current status for Dual-Ring Subport-1 – (Primary Port) High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
2805	AF5	1	HEX	Subport-2 – (Secondary Port) High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
ERPS Information(Active Ring Only)				
3048	BE8	1	HEX	Ring ID for ERPSn (n=1) Ex: 0x001 Ring ID=1
3049	BE9	1	HEX	State for ring of ERPS 0x0000: Disabled. 0x0001: Enabled.
3050	BEA	33	ASCII	Name of Ring Ring Name = "Ring1" Word 1 Lo byte = 'R' Word 2 Lo byte = 'i' Word 3 Lo byte = 'n' Word 4 Lo byte = 'g' Word 5 Lo byte = '1' Word 6 Lo byte = '\0'
3083	C0B	1	HEX	Version & Ring Type High byte – Version. Low byte – Ring Type. 0x01:Major-ring 0x02:Sub-ring Ex: 0x0201– Version2, Type:Major-ring
3084	C0C	1	HEX	Instance of Ring Ex: 0x0001 Instance ID=1
3085	C0D	1	HEX	Control VLAN of Ring E:0x000b Control VLAN=11

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3086	C0E	1	HEX	Right Port of Ring High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0502– Port 5, RPL Owner
3087	C0F	1	HEX	Left Port of Ring High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0303– Port 3, RPL Neighbour
3088	C10	1	HEX	Ring port state High byte –Left port state. Low byte – Right port state. 0x00: No connection 0x01: Forwarding 0x02: Blocking Ex: 0x0001– Left Port No connection Right Port Forwarding
3089	C11	1	HEX	Ring ID for ERPSn (n=2)
3090	C12	1		State of ERPS Ring
3091	C13	33	ASCII	Name of Ring
3124	C34	1	HEX	Version & Ring Type
3125	C35	1		Instance of Ring
3126	C36	1		Control VLAN of Ring
3127	C37	1		Right Port of Ring
3128	C38	1		Left Port of Ring
3129	C39	1		Ring port state
3130	C3A	1	HEX	Ring ID for ERPSn (n=3)
3131	C3B	1		State of ERPS Ring
3132	C3C	33	ASCII	Name of Ring
3165	C5D	1	HEX	Version & Ring Type
3166	C5E	1		Instance of Ring
3167	C5F	1		Control VLAN of Ring
3168	C60	1		Right Port of Ring
3169	C61	1		Left Port of Ring
3170	C62	1		Ring port state

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3171	C63	1	HEX	Ring ID for ERPSn (n=4)
3172	C64	1		State of ERPS Ring
3173	C65	33	ASCII	Name of Ring
3206	C86	1	HEX	Version & Ring Type
3207	C87	1		Instance of Ring
3208	C88	1		Control VLAN of Ring
3209	C89	1		Right Port of Ring
3210	C8A	1		Left Port of Ring
3211	C8B	1		Ring port state
3212	C8C	1	HEX	Ring ID for ERPSn (n=5)
3213	C8D	1		State of ERPS Ring
3214	C8E	33		Name of Ring
3247	CAF	1		Version & Ring Type
3248	CB0	1		Instance of Ring
3249	CB1	1		Control VLAN of Ring
3250	CB2	1		Right Port of Ring
3251	CB3	1		Left Port of Ring
3252	CB4	1		Ring port state
3253	CB5	1	HEX	Ring ID for ERPSn (n=6)
3254	CB6	1		State of ERPS Ring
3255	CB7	33	ASCII	Name of Ring
3288	CD8	1	HEX	Version & Ring Type
3289	CD9	1		Instance of Ring
3290	CDA	1		Control VLAN of Ring
3291	CDB	1		Right Port of Ring
3292	CDC	1		Left Port of Ring
3293	CDD	1		Ring port state

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
MSTP Information				
3304	CE8	1	HEX	Instance ID (Fixed 0x00, 0)
				High byte –Instance ID. Low byte –Used State. 0x01: used 0x00: non used
3305	CE9	3	HEX	Root bridge MAC
				Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3308	CEC	1	HEX	Port 1 status High byte –Port No. Low byte –Port Status. b'0:1 Type 00: Bound(STP) 01: Bound(RSTP) 10: Bound(MSTP) 11: Internal(MSTP) b'2 P2P 0: non P2P 1: P2P b'3:4 State 00: Blocking 01: Learning 10: Forwarding b'5:7 Role 000: Master 001:Alternate 010: Root 011: Designated 100: Backup 101: Disabled 110: Boundary 111: Unknow
3309	CED			Port 2 status
3310	CEE			Port 3 status
3311	CEF			Port 4 status
3312	CF0			Port 5 status
3313	CF1			Port 6 status
3314	CF2			Port 7 status
3315	CF3			Port 8 status
3316	CF4			Port 9 status
3317	CF5			Port 10 status
3318	CF6			Port 11 status
3319	CF7			Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3336	D08	1	HEX	Instance ID (Fixed 0x00, 1)
3337	D09	3		Root bridge MAC
3340	D0C	1		Port 1 status
3341	D0D	1		Port 2 status
3342	D0E	1		Port 3 status
3343	D0F	1		Port 4 status
3344	D10	1		Port 5 status
3345	D11	1		Port 6 status
3346	D12	1		Port 7 status
3347	D13	1		Port 8 status
3348	D14	1		Port 9 status
3349	D15	1		Port 10 status
3350	D16	1		Port 11 status
3351	D17	1		Port 12 status
3368	D28	1	HEX	Instance ID (Fixed 0x00, 2)
3369	D29	3		Root bridge MAC
3372	D2C	1		Port 1 status
3373	D2D	1		Port 2 status
3374	D2E	1		Port 3 status
3375	D2F	1		Port 4 status
3376	D30	1		Port 5 status
3377	D31	1		Port 6 status
3378	D32	1		Port 7 status
3379	D33	1		Port 8 status
3380	D34	1		Port 9 status
3381	D35	1		Port 10 status
3382	D36	1		Port 11 status
3383	D37	1		Port 12 status
3400	D48	1	HEX	Instance ID (Fixed 0x00, 3)
3401	D49	3		Root bridge MAC
3404	D4C	1		Port 1 status
3405	D4D	1		Port 2 status
3406	D4E	1		Port 3 status
3407	D4F	1		Port 4 status
3408	D50	1		Port 5 status
3409	D51	1		Port 6 status
3410	D52	1		Port 7 status
3411	D53	1		Port 8 status
3412	D54	1		Port 9 status
3413	D55	1		Port 10 status
3414	D56	1		Port 11 status
3415	D57	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3432	D68	1	HEX	Instance ID (Fixed 0x00, 4)
3433	D69	3		Root bridge MAC
3436	D6C	1		Port 1 status
3437	D6D	1		Port 2 status
3438	D6E	1		Port 3 status
3439	D6F	1		Port 4 status
3440	D70	1		Port 5 status
3441	D71	1		Port 6 status
3442	D72	1		Port 7 status
3443	D73	1		Port 8 status
3444	D74	1		Port 9 status
3445	D75	1		Port 10 status
3446	D76	1		Port 11 status
3447	D77	1		Port 12 status
3464	D88	1	HEX	Instance ID (Fixed 0x00, 5)
3465	D89	3		Root bridge MAC
3468	D8C	1		Port 1 status
3469	D8D	1		Port 2 status
3470	D8E	1		Port 3 status
3471	D8F	1		Port 4 status
3472	D90	1		Port 5 status
3473	D91	1		Port 6 status
3474	D92	1		Port 7 status
3475	D93	1		Port 8 status
3476	D94	1		Port 9 status
3477	D95	1		Port 10 status
3478	D96	1		Port 11 status
3479	D97	1		Port 12 status
3496	DA8	1	HEX	Instance ID (Fixed 0x00, 6)
3497	DA9	3		Root bridge MAC
3500	DAC	1		Port 1 status
3501	DAD	1		Port 2 status
3502	DAE	1		Port 3 status
3503	DAF	1		Port 4 status
3504	DB0	1		Port 5 status
3505	DB1	1		Port 6 status
3506	DB2	1		Port 7 status
3507	DB3	1		Port 8 status
3508	DB4	1		Port 9 status
3509	DB5	1		Port 10 status
3510	DB6	1		Port 11 status
3511	DB7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3528	DC8	1	HEX	Instance ID (Fixed 0x00, 7)
3529	DC9	3		Root bridge MAC
3532	DCC	1		Port 1 status
3533	DCD	1		Port 2 status
3534	DCE	1		Port 3 status
3535	DCF	1		Port 4 status
3536	DD0	1		Port 5 status
3537	DD1	1		Port 6 status
3538	DD2	1		Port 7 status
3539	DD3	1		Port 8 status
3540	DD4	1		Port 9 status
3541	DD5	1		Port 10 status
3542	DD6	1		Port 11 status
3543	DD7	1		Port 12 status
3560	DE8	1	HEX	Instance ID (Fixed 0x00, 8)
3561	DE9	3		Root bridge MAC
3564	DEC	1		Port 1 status
3565	DED	1		Port 2 status
3566	DEE	1		Port 3 status
3567	DEF	1		Port 4 status
3568	DF0	1		Port 5 status
3569	DF1	1		Port 6 status
3570	DF2	1		Port 7 status
3571	DF3	1		Port 8 status
3572	DF4	1		Port 9 status
3573	DF5	1		Port 10 status
3574	DF6	1		Port 11 status
3575	DF7	1		Port 12 status
3592	E08	1	HEX	Instance ID (Fixed 0x00, 9)
3593	E09	3		Root bridge MAC
3596	E0C	1		Port 1 status
3597	E0D	1		Port 2 status
3598	E0E	1		Port 3 status
3599	E0F	1		Port 4 status
3600	E10	1		Port 5 status
3601	E11	1		Port 6 status
3602	E12	1		Port 7 status
3603	E13	1		Port 8 status
3604	E14	1		Port 9 status
3605	E15	1		Port 10 status
3606	E16	1		Port 11 status
3607	E17	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3624	E28	1	HEX	Instance ID (Fixed 0x00, 10)
3625	E29	3		Root bridge MAC
3628	E2C	1		Port 1 status
3629	E2D	1		Port 2 status
3630	E2E	1		Port 3 status
3631	E2F	1		Port 4 status
3632	E30	1		Port 5 status
3633	E31	1		Port 6 status
3634	E32	1		Port 7 status
3635	E33	1		Port 8 status
3636	E34	1		Port 9 status
3637	E35	1		Port 10 status
3638	E36	1		Port 11 status
3639	E37	1		Port 12 status
3656	E48	1	HEX	Instance ID (Fixed 0x00, 11)
3657	E49	3		Root bridge MAC
3660	E4C	1		Port 1 status
3661	E4D	1		Port 2 status
3662	E4E	1		Port 3 status
3663	E4F	1		Port 4 status
3664	E50	1		Port 5 status
3665	E51	1		Port 6 status
3666	E52	1		Port 7 status
3667	E53	1		Port 8 status
3668	E54	1		Port 9 status
3669	E55	1		Port 10 status
3670	E56	1		Port 11 status
3671	E57	1		Port 12 status
3688	E68	1	HEX	Instance ID (Fixed 0x00, 12)
3689	E69	3		Root bridge MAC
3692	E6C	1		Port 1 status
3693	E6D	1		Port 2 status
3694	E6E	1		Port 3 status
3695	E6F	1		Port 4 status
3696	E70	1		Port 5 status
3697	E71	1		Port 6 status
3698	E72	1		Port 7 status
3699	E73	1		Port 8 status
3700	E74	1		Port 9 status
3701	E75	1		Port 10 status
3702	E76	1		Port 11 status
3703	E77	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3720	E88	1	HEX	Instance ID (Fixed 0x00, 13)
3721	E89	3		Root bridge MAC
3724	E8C	1		Port 1 status
3725	E8D	1		Port 2 status
3726	E8E	1		Port 3 status
3727	E8F	1		Port 4 status
3728	E90	1		Port 5 status
3729	E91	1		Port 6 status
3730	E92	1		Port 7 status
3731	E93	1		Port 8 status
3732	E94	1		Port 9 status
3733	E95	1		Port 10 status
3734	E96	1		Port 11 status
3735	E97	1		Port 12 status
3752	EA8	1	HEX	Instance ID (Fixed 0x00, 14)
3753	EA9	3		Root bridge MAC
3756	EAC	1		Port 1 status
3757	EAD	1		Port 2 status
3758	EAE	1		Port 3 status
3759	EAF	1		Port 4 status
3760	EB0	1		Port 5 status
3761	EB1	1		Port 6 status
3762	EB2	1		Port 7 status
3763	EB3	1		Port 8 status
3764	EB4	1		Port 9 status
3765	EB5	1		Port 10 status
3766	EB6	1		Port 11 status
3767	EB7	1		Port 12 status
3784	EC8	1	HEX	Instance ID (Fixed 0x00, 15)
3785	EC9	3		Root bridge MAC
3788	ECC	1		Port 1 status
3789	ECD	1		Port 2 status
3790	ECE	1		Port 3 status
3791	ECF	1		Port 4 status
3792	ED0	1		Port 5 status
3793	ED1	1		Port 6 status
3794	ED2	1		Port 7 status
3795	ED3	1		Port 8 status
3796	ED4	1		Port 9 status
3797	ED5	1		Port 10 status
3798	ED6	1		Port 11 status
3799	ED7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3816	EE8	1	HEX	Instance ID (Fixed 0x00, 16)
3817	EE9	3		Root bridge MAC
3820	EEC	1		Port 1 status
3821	EED	1		Port 2 status
3822	EEE	1		Port 3 status
3823	EEF	1		Port 4 status
3824	EF0	1		Port 5 status
3825	EF1	1		Port 6 status
3826	EF2	1		Port 7 status
3827	EF3	1		Port 8 status
3828	EF4	1		Port 9 status
3829	EF5	1		Port 10 status
3830	EF6	1		Port 11 status
3831	EF7	1		Port 12 status
3848	F08	1	HEX	Instance ID (Fixed 0x00, 17)
3849	F09	3		Root bridge MAC
3852	F0C	1		Port 1 status
3853	F0D	1		Port 2 status
3854	F0E	1		Port 3 status
3855	F0F	1		Port 4 status
3856	F10	1		Port 5 status
3857	F11	1		Port 6 status
3858	F12	1		Port 7 status
3859	F13	1		Port 8 status
3860	F14	1		Port 9 status
3861	F15	1		Port 10 status
3862	F16	1		Port 11 status
3863	F17	1		Port 12 status
3880	F28	1	HEX	Instance ID (Fixed 0x00, 18)
3881	F29	3		Root bridge MAC
3884	F2C	1		Port 1 status
3885	F2D	1		Port 2 status
3886	F2E	1		Port 3 status
3887	F2F	1		Port 4 status
3888	F30	1		Port 5 status
3889	F31	1		Port 6 status
3890	F32	1		Port 7 status
3891	F33	1		Port 8 status
3892	F34	1		Port 9 status
3893	F35	1		Port 10 status
3894	F36	1		Port 11 status
3895	F37	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
3912	F48	1	HEX	Instance ID (Fixed 0x00, 19)
3913	F49	3		Root bridge MAC
3916	F4C	1		Port 1 status
3917	F4D	1		Port 2 status
3918	F4E	1		Port 3 status
3919	F4F	1		Port 4 status
3920	F50	1		Port 5 status
3921	F51	1		Port 6 status
3922	F52	1		Port 7 status
3923	F53	1		Port 8 status
3924	F54	1		Port 9 status
3925	F55	1		Port 10 status
3926	F56	1		Port 11 status
3927	F57	1		Port 12 status
3944	F68	1	HEX	Instance ID (Fixed 0x00, 20)
3945	F69	3		Root bridge MAC
3948	F6C	1		Port 1 status
3949	F6D	1		Port 2 status
3950	F6E	1		Port 3 status
3951	F6F	1		Port 4 status
3952	F70	1		Port 5 status
3953	F71	1		Port 6 status
3954	F72	1		Port 7 status
3955	F73	1		Port 8 status
3956	F74	1		Port 9 status
3957	F75	1		Port 10 status
3958	F76	1		Port 11 status
3959	F77	1		Port 12 status
3976	F88	1	HEX	Instance ID (Fixed 0x00, 21)
3977	F89	3		Root bridge MAC
3980	F8C	1		Port 1 status
3981	F8D	1		Port 2 status
3982	F8E	1		Port 3 status
3983	F8F	1		Port 4 status
3984	F90	1		Port 5 status
3985	F91	1		Port 6 status
3986	F92	1		Port 7 status
3987	F93	1		Port 8 status
3988	F94	1		Port 9 status
3989	F95	1		Port 10 status
3990	F96	1		Port 11 status
3991	F97	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4008	FA8	1	HEX	Instance ID (Fixed 0x00, 22)
4009	FA9	3		Root bridge MAC
4012	FAC	1		Port 1 status
4013	FAD	1		Port 2 status
4014	FAE	1		Port 3 status
4015	FAF	1		Port 4 status
4016	FB0	1		Port 5 status
4017	FB1	1		Port 6 status
4018	FB2	1		Port 7 status
4019	FB3	1		Port 8 status
4020	FB4	1		Port 9 status
4021	FB5	1		Port 10 status
4022	FB6	1		Port 11 status
4023	FB7	1		Port 12 status
4040	FC8	1	HEX	Instance ID (Fixed 0x00, 23)
4041	FC9	3		Root bridge MAC
4044	FCC	1		Port 1 status
4045	FCD	1		Port 2 status
4046	FCE	1		Port 3 status
4047	FCF	1		Port 4 status
4048	FD0	1		Port 5 status
4049	FD1	1		Port 6 status
4050	FD2	1		Port 7 status
4051	FD3	1		Port 8 status
4052	FD4	1		Port 9 status
4053	FD5	1		Port 10 status
4054	FD6	1		Port 11 status
4055	FD7	1		Port 12 status
4072	FE8	1	HEX	Instance ID (Fixed 0x00, 24)
4073	FE9	3		Root bridge MAC
4076	FEC	1		Port 1 status
4077	FED	1		Port 2 status
4078	FEE	1		Port 3 status
4079	FEF	1		Port 4 status
4080	FF0	1		Port 5 status
4081	FF1	1		Port 6 status
4082	FF2	1		Port 7 status
4083	FF3	1		Port 8 status
4084	FF4	1		Port 9 status
4085	FF5	1		Port 10 status
4086	FF6	1		Port 11 status
4087	FF7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4104	1008	1	HEX	Instance ID (Fixed 0x00, 25)
4105	1009	3		Root bridge MAC
4108	100C	1		Port 1 status
4109	100D	1		Port 2 status
4110	100E	1		Port 3 status
4111	100F	1		Port 4 status
4112	1010	1		Port 5 status
4113	1011	1		Port 6 status
4114	1012	1		Port 7 status
4115	1013	1		Port 8 status
4116	1014	1		Port 9 status
4117	1015	1		Port 10 status
4118	1016	1		Port 11 status
4119	1017	1		Port 12 status
4136	1028	1	HEX	Instance ID (Fixed 0x00, 26)
4137	1029	3		Root bridge MAC
4140	102C	1		Port 1 status
4141	102D	1		Port 2 status
4142	102E	1		Port 3 status
4143	102F	1		Port 4 status
4144	1030	1		Port 5 status
4145	1031	1		Port 6 status
4146	1032	1		Port 7 status
4147	1033	1		Port 8 status
4148	1034	1		Port 9 status
4149	1035	1		Port 10 status
4150	1036	1		Port 11 status
4151	1037	1		Port 12 status
4168	1048	1	HEX	Instance ID (Fixed 0x00, 27)
4169	1049	3		Root bridge MAC
4172	104C	1		Port 1 status
4173	104D	1		Port 2 status
4174	104E	1		Port 3 status
4175	104F	1		Port 4 status
4176	1050	1		Port 5 status
4177	1051	1		Port 6 status
4178	1052	1		Port 7 status
4179	1053	1		Port 8 status
4180	1054	1		Port 9 status
4181	1055	1		Port 10 status
4182	1056	1		Port 11 status
4183	1057	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4200	1068	1	HEX	Instance ID (Fixed 0x00, 28)
4201	1069	3		Root bridge MAC
4204	106C	1		Port 1 status
4205	106D	1		Port 2 status
4206	106E	1		Port 3 status
4207	106F	1		Port 4 status
4208	1070	1		Port 5 status
4209	1071	1		Port 6 status
4210	1072	1		Port 7 status
4211	1073	1		Port 8 status
4212	1074	1		Port 9 status
4213	1075	1		Port 10 status
4214	1076	1		Port 11 status
4215	1077	1		Port 12 status
4232	1088	1	HEX	Instance ID (Fixed 0x00, 29)
4233	1089	3		Root bridge MAC
4236	108C	1		Port 1 status
4237	108D	1		Port 2 status
4238	108E	1		Port 3 status
4239	108F	1		Port 4 status
4240	1090	1		Port 5 status
4241	1091	1		Port 6 status
4242	1092	1		Port 7 status
4243	1093	1		Port 8 status
4244	1094	1		Port 9 status
4245	1095	1		Port 10 status
4246	1096	1		Port 11 status
4247	1097	1		Port 12 status
4264	10A8	1	HEX	Instance ID (Fixed 0x00, 30)
4265	10A9	3		Root bridge MAC
4268	10AC	1		Port 1 status
4269	10AD	1		Port 2 status
4270	10AE	1		Port 3 status
4271	10AF	1		Port 4 status
4272	10B0	1		Port 5 status
4273	10B1	1		Port 6 status
4274	10B2	1		Port 7 status
4275	10B3	1		Port 8 status
4276	10B4	1		Port 9 status
4277	10B5	1		Port 10 status
4278	10B6	1		Port 11 status
4279	10B7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4296	10C8	1	HEX	Instance ID (Fixed 0x00, 31)
4297	10C9	3		Root bridge MAC
4300	10CC	1		Port 1 status
4301	10CD	1		Port 2 status
4302	10CE	1		Port 3 status
4303	10CF	1		Port 4 status
4304	10D0	1		Port 5 status
4305	10D1	1		Port 6 status
4306	10D2	1		Port 7 status
4307	10D3	1		Port 8 status
4308	10D4	1		Port 9 status
4309	10D5	1		Port 10 status
4310	10D6	1		Port 11 status
4311	10D7	1		Port 12 status
4328	10E8	1	HEX	Instance ID (Fixed 0x00, 32)
4329	10E9	3		Root bridge MAC
4332	10EC	1		Port 1 status
4333	10ED	1		Port 2 status
4334	10EE	1		Port 3 status
4335	10EF	1		Port 4 status
4336	10F0	1		Port 5 status
4337	10F1	1		Port 6 status
4338	10F2	1		Port 7 status
4339	10F3	1		Port 8 status
4340	10F4	1		Port 9 status
4341	10F5	1		Port 10 status
4342	10F6	1		Port 11 status
4343	10F7	1		Port 12 status
4360	1108	1	HEX	Instance ID (Fixed 0x00, 33)
4361	1109	3		Root bridge MAC
4364	110C	1		Port 1 status
4365	110D	1		Port 2 status
4366	110E	1		Port 3 status
4367	110F	1		Port 4 status
4368	1110	1		Port 5 status
4369	1111	1		Port 6 status
4370	1112	1		Port 7 status
4371	1113	1		Port 8 status
4372	1114	1		Port 9 status
4373	1115	1		Port 10 status
4374	1116	1		Port 11 status
4375	1117	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4392	1128	1	HEX	Instance ID (Fixed 0x00, 34)
4393	1129	3		Root bridge MAC
4396	112C	1		Port 1 status
4397	112D	1		Port 2 status
4398	112E	1		Port 3 status
4399	112F	1		Port 4 status
4400	1130	1		Port 5 status
4401	1131	1		Port 6 status
4402	1132	1		Port 7 status
4403	1133	1		Port 8 status
4404	1134	1		Port 9 status
4405	1135	1		Port 10 status
4406	1136	1		Port 11 status
4407	1137	1		Port 12 status
4424	1148	1	HEX	Instance ID (Fixed 0x00, 35)
4425	1149	3		Root bridge MAC
4428	114C	1		Port 1 status
4429	114D	1		Port 2 status
4430	114E	1		Port 3 status
4431	114F	1		Port 4 status
4432	1150	1		Port 5 status
4433	1151	1		Port 6 status
4434	1152	1		Port 7 status
4435	1153	1		Port 8 status
4436	1154	1		Port 9 status
4437	1155	1		Port 10 status
4438	1156	1		Port 11 status
4439	1157	1		Port 12 status
4456	1168	1	HEX	Instance ID (Fixed 0x00, 36)
4457	1169	3		Root bridge MAC
4460	116C	1		Port 1 status
4461	116D	1		Port 2 status
4462	116E	1		Port 3 status
4463	116F	1		Port 4 status
4464	1170	1		Port 5 status
4465	1171	1		Port 6 status
4466	1172	1		Port 7 status
4467	1173	1		Port 8 status
4468	1174	1		Port 9 status
4469	1175	1		Port 10 status
4470	1176	1		Port 11 status
4471	1177	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4488	1188	1	HEX	Instance ID (Fixed 0x00, 37)
4489	1189	3		Root bridge MAC
4492	118C	1		Port 1 status
4493	118D	1		Port 2 status
4494	118E	1		Port 3 status
4495	118F	1		Port 4 status
4496	1190	1		Port 5 status
4497	1191	1		Port 6 status
4498	1192	1		Port 7 status
4499	1193	1		Port 8 status
4500	1194	1		Port 9 status
4501	1195	1		Port 10 status
4502	1196	1		Port 11 status
4503	1197	1		Port 12 status
4520	11A8	1	HEX	Instance ID (Fixed 0x00, 38)
4521	11A9	3		Root bridge MAC
4524	11AC	1		Port 1 status
4525	11AD	1		Port 2 status
4526	11AE	1		Port 3 status
4527	11AF	1		Port 4 status
4528	11B0	1		Port 5 status
4529	11B1	1		Port 6 status
4530	11B2	1		Port 7 status
4531	11B3	1		Port 8 status
4532	11B4	1		Port 9 status
4533	11B5	1		Port 10 status
4534	11B6	1		Port 11 status
4535	11B7	1		Port 12 status
4552	11C8	1	HEX	Instance ID (Fixed 0x00, 39)
4553	11C9	3		Root bridge MAC
4556	11CC	1		Port 1 status
4557	11CD	1		Port 2 status
4558	11CE	1		Port 3 status
4559	11CF	1		Port 4 status
4560	11D0	1		Port 5 status
4561	11D1	1		Port 6 status
4562	11D2	1		Port 7 status
4563	11D3	1		Port 8 status
4564	11D4	1		Port 9 status
4565	11D5	1		Port 10 status
4566	11D6	1		Port 11 status
4567	11D7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4584	11E8	1	HEX	Instance ID (Fixed 0x00, 40)
4585	11E9	3		Root bridge MAC
4588	11EC	1		Port 1 status
4589	11ED	1		Port 2 status
4590	11EE	1		Port 3 status
4591	11EF	1		Port 4 status
4592	11F0	1		Port 5 status
4593	11F1	1		Port 6 status
4594	11F2	1		Port 7 status
4595	11F3	1		Port 8 status
4596	11F4	1		Port 9 status
4597	11F5	1		Port 10 status
4598	11F6	1		Port 11 status
4599	11F7	1		Port 12 status
4616	1208	1	HEX	Instance ID (Fixed 0x00, 41)
4617	1209	3		Root bridge MAC
4620	120C	1		Port 1 status
4621	120D	1		Port 2 status
4622	120E	1		Port 3 status
4623	120F	1		Port 4 status
4624	1210	1		Port 5 status
4625	1211	1		Port 6 status
4626	1212	1		Port 7 status
4627	1213	1		Port 8 status
4628	1214	1		Port 9 status
4629	1215	1		Port 10 status
4630	1216	1		Port 11 status
4631	1217	1		Port 12 status
4648	1228	1	HEX	Instance ID (Fixed 0x00, 42)
4649	1229	3		Root bridge MAC
4652	122C	1		Port 1 status
4653	122D	1		Port 2 status
4654	122E	1		Port 3 status
4655	122F	1		Port 4 status
4656	1230	1		Port 5 status
4657	1231	1		Port 6 status
4658	1232	1		Port 7 status
4659	1233	1		Port 8 status
4660	1234	1		Port 9 status
4661	1235	1		Port 10 status
4662	1236	1		Port 11 status
4663	1237	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4680	1248	1	HEX	Instance ID (Fixed 0x00, 43)
4681	1249	3		Root bridge MAC
4684	124C	1		Port 1 status
4685	124D	1		Port 2 status
4686	124E	1		Port 3 status
4687	124F	1		Port 4 status
4688	1250	1		Port 5 status
4689	1251	1		Port 6 status
4690	1252	1		Port 7 status
4691	1253	1		Port 8 status
4692	1254	1		Port 9 status
4693	1255	1		Port 10 status
4694	1256	1		Port 11 status
4695	1257	1		Port 12 status
4712	1268	1	HEX	Instance ID (Fixed 0x00, 44)
4713	1269	3		Root bridge MAC
4716	126C	1		Port 1 status
4717	126D	1		Port 2 status
4718	126E	1		Port 3 status
4719	126F	1		Port 4 status
4720	1270	1		Port 5 status
4721	1271	1		Port 6 status
4722	1272	1		Port 7 status
4723	1273	1		Port 8 status
4724	1274	1		Port 9 status
4725	1275	1		Port 10 status
4726	1276	1		Port 11 status
4727	1277	1		Port 12 status
4744	1288	1	HEX	Instance ID (Fixed 0x00, 45)
4745	1289	3		Root bridge MAC
4748	128C	1		Port 1 status
4749	128D	1		Port 2 status
4750	128E	1		Port 3 status
4751	128F	1		Port 4 status
4752	1290	1		Port 5 status
4753	1291	1		Port 6 status
4754	1292	1		Port 7 status
4755	1293	1		Port 8 status
4756	1294	1		Port 9 status
4757	1295	1		Port 10 status
4758	1296	1		Port 11 status
4759	1297	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4776	12A8	1	HEX	Instance ID (Fixed 0x00, 46)
4777	12A9	3		Root bridge MAC
4780	12AC	1		Port 1 status
4781	12AD	1		Port 2 status
4782	12AE	1		Port 3 status
4783	12AF	1		Port 4 status
4784	12B0	1		Port 5 status
4785	12B1	1		Port 6 status
4786	12B2	1		Port 7 status
4787	12B3	1		Port 8 status
4788	12B4	1		Port 9 status
4789	12B5	1		Port 10 status
4790	12B6	1		Port 11 status
4791	12B7	1		Port 12 status
4808	12C8	1	HEX	Instance ID (Fixed 0x00, 47)
4809	12C9	3		Root bridge MAC
4812	12CC	1		Port 1 status
4813	12CD	1		Port 2 status
4814	12CE	1		Port 3 status
4815	12CF	1		Port 4 status
4816	12D0	1		Port 5 status
4817	12D1	1		Port 6 status
4818	12D2	1		Port 7 status
4819	12D3	1		Port 8 status
4820	12D4	1		Port 9 status
4821	12D5	1		Port 10 status
4822	12D6	1		Port 11 status
4823	12D7	1		Port 12 status
4840	12E8	1	HEX	Instance ID (Fixed 0x00, 48)
4841	12E9	3		Root bridge MAC
4844	12EC	1		Port 1 status
4845	12ED	1		Port 2 status
4846	12EE	1		Port 3 status
4847	12EF	1		Port 4 status
4848	12F0	1		Port 5 status
4849	12F1	1		Port 6 status
4850	12F2	1		Port 7 status
4851	12F3	1		Port 8 status
4852	12F4	1		Port 9 status
4853	12F5	1		Port 10 status
4854	12F6	1		Port 11 status
4855	12F7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4872	1308	1	HEX	Instance ID (Fixed 0x00, 49)
4873	1309	3		Root bridge MAC
4876	130C	1		Port 1 status
4877	130D	1		Port 2 status
4878	130E	1		Port 3 status
4879	130F	1		Port 4 status
4880	1310	1		Port 5 status
4881	1311	1		Port 6 status
4882	1312	1		Port 7 status
4883	1313	1		Port 8 status
4884	1314	1		Port 9 status
4885	1315	1		Port 10 status
4886	1316	1		Port 11 status
4887	1317	1		Port 12 status
4904	1328	1	HEX	Instance ID (Fixed 0x00, 50)
4905	1329	3		Root bridge MAC
4908	132C	1		Port 1 status
4909	132D	1		Port 2 status
4910	132E	1		Port 3 status
4911	132F	1		Port 4 status
4912	1330	1		Port 5 status
4913	1331	1		Port 6 status
4914	1332	1		Port 7 status
4915	1333	1		Port 8 status
4916	1334	1		Port 9 status
4917	1335	1		Port 10 status
4918	1336	1		Port 11 status
4919	1337	1		Port 12 status
4936	1348	1	HEX	Instance ID (Fixed 0x00, 51)
4937	1349	3		Root bridge MAC
4940	134C	1		Port 1 status
4941	134D	1		Port 2 status
4942	134E	1		Port 3 status
4943	134F	1		Port 4 status
4944	1350	1		Port 5 status
4945	1351	1		Port 6 status
4946	1352	1		Port 7 status
4947	1353	1		Port 8 status
4948	1354	1		Port 9 status
4949	1355	1		Port 10 status
4950	1356	1		Port 11 status
4951	1357	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
4970	136A	1	HEX	Instance ID (Fixed 0x00, 52)
4971	136B	3		Root bridge MAC
4972	136C	1		Port 1 status
4973	136D	1		Port 2 status
4974	136E	1		Port 3 status
4975	136F	1		Port 4 status
4976	1370	1		Port 5 status
4977	1371	1		Port 6 status
4978	1372	1		Port 7 status
4979	1373	1		Port 8 status
4980	1374	1		Port 9 status
4981	1375	1		Port 10 status
4982	1376	1		Port 11 status
4983	1377	1		Port 12 status
5000	1388	1	HEX	Instance ID (Fixed 0x00, 53)
5001	1389	3		Root bridge MAC
5004	138C	1		Port 1 status
5005	138D	1		Port 2 status
5006	138E	1		Port 3 status
5007	138F	1		Port 4 status
5008	1390	1		Port 5 status
5009	1391	1		Port 6 status
5010	1392	1		Port 7 status
5011	1393	1		Port 8 status
5012	1394	1		Port 9 status
5013	1395	1		Port 10 status
5014	1396	1		Port 11 status
5015	1397	1		Port 12 status
5032	13A8	1	HEX	Instance ID (Fixed 0x00, 54)
5033	13A9	3		Root bridge MAC
5036	13AC	1		Port 1 status
5037	13AD	1		Port 2 status
5038	13AE	1		Port 3 status
5039	13AF	1		Port 4 status
5040	13B0	1		Port 5 status
5041	13B1	1		Port 6 status
5042	13B2	1		Port 7 status
5043	13B3	1		Port 8 status
5044	13B4	1		Port 9 status
5045	13B5	1		Port 10 status
5046	13B6	1		Port 11 status
5047	13B7	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
5064	13C8	1	HEX	Instance ID (Fixed 0x00, 55)
5065	13C9	3		Root bridge MAC
5068	13CC	1		Port 1 status
5069	13CD	1		Port 2 status
5070	13CE	1		Port 3 status
5071	13CF	1		Port 4 status
5072	13D0	1		Port 5 status
5073	13D1	1		Port 6 status
5074	13D2	1		Port 7 status
5075	13D3	1		Port 8 status
5076	13D4	1		Port 9 status
5077	13D5	1		Port 10 status
5078	13D6	1		Port 11 status
5079	13D7	1		Port 12 status
5096	13E8	1	HEX	Instance ID (Fixed 0x00, 56)
5097	13E9	3		Root bridge MAC
5100	13EC	1		Port 1 status
5101	13ED	1		Port 2 status
5102	13EE	1		Port 3 status
5103	13EF	1		Port 4 status
5104	13F0	1		Port 5 status
5105	13F1	1		Port 6 status
5106	13F2	1		Port 7 status
5107	13F3	1		Port 8 status
5108	13F4	1		Port 9 status
5109	13F5	1		Port 10 status
5110	13F6	1		Port 11 status
5111	13F7	1		Port 12 status
5130	140A	1	HEX	Instance ID (Fixed 0x00, 57)
5131	140B	3		Root bridge MAC
5132	140C	1		Port 1 status
5133	140D	1		Port 2 status
5134	140E	1		Port 3 status
5135	140F	1		Port 4 status
5136	1410	1		Port 5 status
5137	1411	1		Port 6 status
5138	1412	1		Port 7 status
5139	1413	1		Port 8 status
5140	1414	1		Port 9 status
5141	1415	1		Port 10 status
5142	1416	1		Port 11 status
5143	1417	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
5160	1428	1	HEX	Instance ID (Fixed 0x00, 58)
5161	1429	3		Root bridge MAC
5164	142C	1		Port 1 status
5165	142D	1		Port 2 status
5166	142E	1		Port 3 status
5167	142F	1		Port 4 status
5168	1430	1		Port 5 status
5169	1431	1		Port 6 status
5170	1432	1		Port 7 status
5171	1433	1		Port 8 status
5172	1434	1		Port 9 status
5173	1435	1		Port 10 status
5174	1436	1		Port 11 status
5175	1437	1		Port 12 status
5192	1448	1	HEX	Instance ID (Fixed 0x00, 59)
5193	1449	3		Root bridge MAC
5196	144C	1		Port 1 status
5197	144D	1		Port 2 status
5198	144E	1		Port 3 status
5199	144F	1		Port 4 status
5200	1450	1		Port 5 status
5201	1451	1		Port 6 status
5202	1452	1		Port 7 status
5203	1453	1		Port 8 status
5204	1454	1		Port 9 status
5205	1455	1		Port 10 status
5206	1456	1		Port 11 status
5207	1457	1		Port 12 status
5224	1468	1	HEX	Instance ID (Fixed 0x00, 60)
5225	1469	3		Root bridge MAC
5228	146C	1		Port 1 status
5229	146D	1		Port 2 status
5230	146E	1		Port 3 status
5231	146F	1		Port 4 status
5232	1470	1		Port 5 status
5233	1471	1		Port 6 status
5234	1472	1		Port 7 status
5235	1473	1		Port 8 status
5236	1474	1		Port 9 status
5237	1475	1		Port 10 status
5238	1476	1		Port 11 status
5239	1477	1		Port 12 status

Tabelle 193: MODBUS-Register

Registeradresse		Daten- länge/ Word	Dar- stellung	Beschreibung
Dec	Hex			
Systeminformation				
5256	1488	1	HEX	Instance ID (Fixed 0x00, 61)
5257	1489	3		Root bridge MAC
5260	148C	1		Port 1 status
5261	148D	1		Port 2 status
5262	148E	1		Port 3 status
5263	148F	1		Port 4 status
5264	1490	1		Port 5 status
5265	1491	1		Port 6 status
5266	1492	1		Port 7 status
5267	1493	1		Port 8 status
5268	1494	1		Port 9 status
5269	1495	1		Port 10 status
5270	1496	1		Port 11 status
5271	1497	1		Port 12 status
5288	14A8	1	HEX	Instance ID (Fixed 0x00, 62)
5289	14A9	3		Root bridge MAC
5292	14AC	1		Port 1 status
5293	14AD	1		Port 2 status
5294	14AE	1		Port 3 status
5295	14AF	1		Port 4 status
5296	14B0	1		Port 5 status
5297	14B1	1		Port 6 status
5298	14B2	1		Port 7 status
5299	14B3	1		Port 8 status
5300	14B4	1		Port 9 status
5301	14B5	1		Port 10 status
5302	14B6	1		Port 11 status
5303	14B7	1		Port 12 status
5320	14C8	1	HEX	Instance ID (Fixed 0x00, 63)
5321	14C9	3		Root bridge MAC
5324	14CC	1		Port 1 status
5325	14CD	1		Port 2 status
5326	14CE	1		Port 3 status
5327	14CF	1		Port 4 status
5328	14D0	1		Port 5 status
5329	14D1	1		Port 6 status
5330	14D2	1		Port 7 status
5331	14D3	1		Port 8 status
5332	14D4	1		Port 9 status
5333	14D5	1		Port 10 status
5334	14D6	1		Port 11 status
5335	14D7	1		Port 12 status

Abbildungsverzeichnis

Abbildung 1: Frontansicht des Industrial-Managed-Switches.....	23
Abbildung 2: Draufsicht des Industrial-Managed-Switches	25
Abbildung 3: Erdungsschraube	26
Abbildung 4: Anschluss Spannungsversorgung (PWR/RPS).....	27
Abbildung 5: Netzwerkanschlüsse	28
Abbildung 6: Geräte-LEDs	30
Abbildung 7: Anschluss-LEDs	31
Abbildung 8: DIP-Schalter	32
Abbildung 9: Reset-Taster.....	33
Abbildung 10: Aufkleber	34
Abbildung 11: Ablaufdiagramm der MAC-Adresstabelle	48
Abbildung 12: Halbduplexmodus	50
Abbildung 13: Vollduplexmodus	50
Abbildung 14: MOD ohne MVR	65
Abbildung 15: MOD unterstützt MVR.....	65
Abbildung 16: Multicast-Adresse	68
Abbildung 17: Port-basiertes Q in Q	78
Abbildung 18: Konfigurationsbeispiel.....	79
Abbildung 19: Anwendung 1 (über einen Router)	81
Abbildung 20: Anwendung 2 (Lokal in verschiedenen VLANs)	81
Abbildung 21: Dual Homing.....	85
Abbildung 22: Dual Ring Switch ABC	86
Abbildung 23: Dual Ring Switch AB.....	86
Abbildung 24: Jet Ring	94
Abbildung 25: DHCP Snooping	105
Abbildung 26: IEEE 802.1X.....	110
Abbildung 27: RADIUS-Server	110
Abbildung 28: USB-Funktionen, Ordner anlegen.....	120
Abbildung 29: USB-Funktionen, Firmware in Ordner	120
Abbildung 30: USB-Funktionen, Ordner anlegen.....	121
Abbildung 31: USB-Funktionen, Konfigurationsdatei in Ordner	122
Abbildung 32: WBM-Seite „Systeminformation“	130
Abbildung 33: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	132
Abbildung 34: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“	134
Abbildung 35: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“	135
Abbildung 36: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“	138
Abbildung 37: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“	139
Abbildung 38: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“	141
Abbildung 39: WBM-Seite „MAC Management“ – Register „Age-Time-Einstellung“	142
Abbildung 40: WBM-Seite „MAC Management“ – Register „Blacklisting“	143
Abbildung 41: WBM-Seite „Port-Spiegelung“	144
Abbildung 42: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“	146

Abbildung 43: WBM-Seite „Port-Einstellungen“ – Register „Informationen“	148
Abbildung 44: WBM-Seite „QoS“ – Register „Port-Priorität“	149
Abbildung 45: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“	150
Abbildung 46: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“	151
Abbildung 47: WBM-Seite „QoS“ – Register „Schedule-Modus“	152
Abbildung 48: WBM-Seite „Bandbreitenbegrenzung“ – Register „Sturmbegrenzung“	154
Abbildung 49: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“	156
Abbildung 50: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“	158
Abbildung 51: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“ ..	160
Abbildung 52: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“	162
Abbildung 53: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“	163
Abbildung 54: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“	164
Abbildung 55: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“	165
Abbildung 56: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „MVR- Einstellungen“	166
Abbildung 57: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „Gruppeneinstellungen“	168
Abbildung 58: WBM-Seite „Static Multicast“	169
Abbildung 59: WBM-Seite „Multicast Statistics“	170
Abbildung 60: WBM-Seite „Port Isolation“	171
Abbildung 61: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“	173
Abbildung 62: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“	175
Abbildung 63: WBM-Seite „VLAN“ – Register „Port-Einstellungen“	176
Abbildung 64: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GVRP“	178
Abbildung 65: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GARP Timer“	180
Abbildung 66: WBM-Seite „IP Subnet VLAN“	182
Abbildung 67: WBM-Seite „MAC VLAN“	183
Abbildung 68: WBM-Seite „Protokoll VLAN“	184
Abbildung 69: WBM-Seite „Q-in-Q“ – Register „VLAN Stacking“	185
Abbildung 70: WBM-Seite „Q-in-Q“ – Register „Port-based Q-in-Q“	187
Abbildung 71: WBM-Seite „Q-in-Q“ – Register „Selektive Q-in-Q“	188
Abbildung 72: WBM-Seite „DHCP Relay“	190
Abbildung 73: WBM-Seite „DHCP Options“	191
Abbildung 74: WBM-Seite „DHCP-Server“ – Register „Allgemeine Einstellungen“	193
Abbildung 75: WBM-Seite „DHCP-Server“ – Register „Pool-Einstellungen“	195
Abbildung 76: WBM-Seite „DHCP-Server“ – Register „Binding Information“	199
Abbildung 77: WBM-Seite „DHCP-Server“ – Register „Statistics“	200
Abbildung 78: WBM-Seite „Dual Homing“	201
Abbildung 79: WBM-Seite „Dual Ring“	203
Abbildung 80: WBM-Seite „ERPS“ – Register „Ringeinstellungen“	205
Abbildung 81: WBM-Seite „ERPS“ – Register „Instance-Einstellungen“	209
Abbildung 82: WBM-Seite „Link Aggregation“ – Register „Static Trunk“	210

Abbildung 83: WBM-Seite „Link Aggregation“ – Register „LACP“	212
Abbildung 84: WBM-Seite „Link Aggregation“ – Register „LACP Info.“	214
Abbildung 85: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“	216
Abbildung 86: WBM-Seite „LLDP“ – Register „Nächste“	218
Abbildung 87: WBM-Seite „Loop Detection“	219
Abbildung 88: WBM-Seite „Jet Ring“	221
Abbildung 89: WBM-Seite „Modbus“	223
Abbildung 90: WBM-Seite „Static Route“	224
Abbildung 91: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“	226
Abbildung 92: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“	228
Abbildung 93: WBM-Seite „Spanning Tree Protocol“ – Register „STP-Status“	231
Abbildung 94: WBM-Seite „Xpress Ring“	232
Abbildung 95: WBM-Seite „DHCP Snooping“ – Register „DHCP Snooping“	234
Abbildung 96: WBM-Seite „DHCP Snooping“ – Register „Port-Einstellungen“	236
Abbildung 97: WBM-Seite „DHCP Snooping“ – Register „Server-Screening“	237
Abbildung 98: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Static- Entry-Einstellungen“	238
Abbildung 99: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Binding-Tabelle“	240
Abbildung 100: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“	241
Abbildung 101: WBM-Seite „ARP-Überprüfung“ – Register „Filtertabelle“	243
Abbildung 102: WBM-Seite „Access-Control-Liste“	244
Abbildung 103: WBM-Seite „IEEE 802.1X“ – Register „Globale Einstellungen“	248
Abbildung 104: WBM-Seite „IEEE-802.1X“ – Register „Port-Einstellungen“	251
Abbildung 105: WBM-Seite „Port Security“ – Register „Port Security“	255
Abbildung 106: WBM-Seite „Port Security“ – Register „Sticky-MAC-Einstellungen“	257
Abbildung 107: WBM-Seite „Alarminformationen“	258
Abbildung 108: WBM-Seite „Systeminformationen“	259
Abbildung 109: WBM-Seite „Port-Statistik“	261
Abbildung 110: WBM-Seite „Port-Auslastung“	262
Abbildung 111: WBM-Seite „RMON-Statistiken“	263
Abbildung 112: WBM-Seite „SFP-Information“	266
Abbildung 113: WBM-Seite „Traffic-Monitor“	269
Abbildung 114: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“	272
Abbildung 115: WBM-Seite „SNMP“ – Register „Community Name“	273
Abbildung 116: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver- Einstellungen“	275
Abbildung 117: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“	277
Abbildung 118: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“	278
Abbildung 119: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“	279
Abbildung 120: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3- Gruppen“	281
Abbildung 121: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3 View“	282

Abbildung 122: WBM-Seite „Auto Provision“	283
Abbildung 123: WBM-Seite „Mail-Alarm“	284
Abbildung 124: WBM-Seite „Wartung“ – Register „Konfiguration“	286
Abbildung 125: WBM-Seite „Wartung“ – Register „Firmware“	288
Abbildung 126: WBM-Seite „Wartung“ – Register „Neustart“	289
Abbildung 127: WBM-Seite „Wartung“ – Register „Rebooten“ – Meldung.....	289
Abbildung 128: WBM-Seite „Wartung“ – Register „Protokolle“	290
Abbildung 129: WBM-Seite „System-Log“	292
Abbildung 130: WBM-Seite „Ping“	294
Abbildung 131: WBM-Seite „USB-Funktionen“	295
Abbildung 132: WBM-Seite „Benutzerkonto“	297
Abbildung 133: RJ-45 Anschlussbelegung	299
Abbildung 134: Anschlussbelegung RJ-45 zu DB9.....	299

Tabellenverzeichnis

Tabelle 1: Darstellungen der Zahlensysteme	13
Tabelle 2: Schriftkonventionen	13
Tabelle 3: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“	23
Tabelle 4: Legende zur Abbildung „Frontansicht des Industrial-Managed-Switches“	25
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 „Anschluss-LEDs“	31
Tabelle 9: Legende zur Abbildung „DIP-Schalter“	32
Tabelle 10: Legende zur Abbildung „Reset-Taster“	33
Tabelle 11: Legende zur Abbildung „Aufkleber“	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: Prioritätsebenen	56
Tabelle 18: Multicast-Klassen und -Adressbereiche	67
Tabelle 19: IP-Multicast-Adressen	68
Tabelle 20: Option Frame Format	83
Tabelle 21: Option Frame Format	83
Tabelle 22: Frame-Format der Unteroption „Circuit ID“	83
Tabelle 23: Frame-Format der Unteroption „Remote ID“	83
Tabelle 24: Format der Unteroption „Circuit ID“	83
Tabelle 25: STP-Pfadkosten	98
Tabelle 26: Default-Einstellungen für den Telnet-Port	124
Tabelle 27: Default-Einstellungen für den Konsolen-Port	125
Tabelle 28: Anmeldebildschirm	125
Tabelle 29: Übersicht - Navigationslinks und WBM-Seiten	127
Tabelle 30: WBM-Seite „Systeminformation“	131
Tabelle 31: WBM-Seite „Allgemeine Einstellungen“ – Register „System“	133
Tabelle 32: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo Frame“	134
Tabelle 33: WBM-Seite „Allgemeine Einstellungen“ – Register „SNTP“	136
Tabelle 34: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“	138
Tabelle 35: WBM-Seite „MAC Management“ – Register „Statische MAC-Einstellungen“	140
Tabelle 36: WBM-Seite „MAC Management“ – Register „MAC-Tabelle“	141
Tabelle 37: „MAC Management“ – Register „Age-Time-Einstellung“	142
Tabelle 38: WBM-Seite „MAC Management“ – Register „Blacklisting“	143
Tabelle 39: WBM-Seite „Port-Spiegelung“	145
Tabelle 40: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine Einstellungen“	147
Tabelle 41: WBM-Seite „Port-Einstellungen“ – Register „Informationen“	148

Tabelle 42: WBM-Seite „QoS“ – Register „Port-Priorität“	149
Tabelle 43: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“	150
Tabelle 44: WBM-Seite „QoS“ – Register „Priorität/Queue-Zuordnung“	151
Tabelle 45: Default-Einstellungen	151
Tabelle 46: WBM-Seite „QoS“ – Register „Schedule- Modus“	153
Tabelle 47: WBM-Seite „Rate Limitation“ – Register „Broadcast-Sturmkontrolle“	155
Tabelle 48: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“	157
Tabelle 49: WBM-Seite „IGMP Snooping“ – Register „Allgemeine Einstellungen“	159
Tabelle 50: WBM-Seite „IGMP Snooping“ – Register „Port-Einstellungen“	161
Tabelle 51: WBM-Seite „IGMP Snooping“ – Register „Querier-Einstellungen“ ..	162
Tabelle 52: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“ ...	163
Tabelle 53: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“	164
Tabelle 54: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“	165
Tabelle 55: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „MVR-Einstellungen“	167
Tabelle 56: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „Gruppeneinstellungen“	168
Tabelle 57: WBM-Seite „Static Multicast“	169
Tabelle 58: WBM-Seite „Multicast Statistics“	170
Tabelle 59: WBM-Seite „Port Isolation“	172
Tabelle 60: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“	174
Tabelle 61: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“	175
Tabelle 62: WBM-Seite „VLAN“ – Register „Port-Einstellungen“	177
Tabelle 63: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GVRP“	179
Tabelle 64: WBM-Seite „GARP VLAN Registration Protocol“ – Register „GARP Timer“	181
Tabelle 65: WBM-Seite „IP Subnet VLAN“	182
Tabelle 66: WBM-Seite „MAC VLAN“	183
Tabelle 67: WBM-Seite „Protokoll VLAN“	184
Tabelle 68: WBM-Seite „Q-in-Q“ – Register „VLAN Stacking“	186
Tabelle 69: WBM-Seite „Q-in-Q“ – Register „Port-based Q-in-Q“	187
Tabelle 70: WBM-Seite „Q-in-Q“ – Register „Selektive Q-in-Q“	189
Tabelle 71: WBM-Seite „DHCP Relay“	190
Tabelle 72: WBM-Seite „DHCP Options“	192
Tabelle 73: WBM-Seite „DHCP-Server“ – Register „Allgemeine Einstellungen“ ..	194
Tabelle 74: WBM-Seite „DHCP-Server“ – Register „Pool-Einstellungen“	196
Tabelle 75: WBM-Seite „DHCP-Server“ – Register „Binding Information“	199
Tabelle 76: WBM-Seite „DHCP-Server“ – Register „Statistics“	200
Tabelle 77: WBM-Seite „Dual Homing“	202
Tabelle 78: WBM-Seite „Dual Ring“	204
Tabelle 79: WBM-Seite „ERPS“ – Register „Ringeinstellungen“	206
Tabelle 80: WBM-Seite „ERPS“ – Register „Instance-Einstellungen“	209
Tabelle 81: WBM-Seite „Link Aggregation“ – Register „Static Trunk“	211
Tabelle 82: WBM-Seite „Link Aggregation“ – Register „LACP“	213
Tabelle 83: WBM-Seite „Link Aggregation“ – Register „LACP Info.“	215
Tabelle 84: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“	217

Tabelle 85: WBM-Seite „LLDP“ – Register „Nächste“	218
Tabelle 86: WBM-Seite „Loop Detection“	220
Tabelle 87: WBM-Seite „Jet Ring“	222
Tabelle 88: WBM-Seite „Modbus“	223
Tabelle 89: WBM-Seite „Static Route“	225
Tabelle 90: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“	227
Tabelle 91: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“	229
Tabelle 92: WBM-Seite „STP“ – Register „STP-Status“	231
Tabelle 93: WBM-Seite „Xpress Ring“	233
Tabelle 94: WBM-Seite „DHP Snooping“ – Register „DHCP Snooping“	235
Tabelle 95: WBM-Seite „DHCP Snooping“ – Register „Port-Einstellungen“	236
Tabelle 96: WBM-Seite „DHP Snooping“ – Register „Server-Screening“	237
Tabelle 97: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Static- Entry-Einstellungen“	239
Tabelle 98: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Binding- Tabelle“	240
Tabelle 99: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“	242
Tabelle 100: WBM-Seite „ARP-Überprüfung“ – Register „Filtertabelle“	243
Tabelle 101: WBM-Seite „Access-Control-Liste“	245
Tabelle 102: WBM-Seite „IEEE 802.1X“ – Register „Globale Einstellungen“	249
Tabelle 103: WBM-Seite „IEEE-802.1X“ – Register „Port-Einstellungen“	252
Tabelle 104: WBM-Seite „Port Security“ – Register „Port Security“	256
Tabelle 105: WBM-Seite „Port Security“ – Register „Sticky-MAC-Einstellungen“	257
Tabelle 106: WBM-Seite „Alarminformationen“	258
Tabelle 107: WBM-Seite „Systeminformationen“	260
Tabelle 108: WBM-Seite „Port-Statistik“	261
Tabelle 109: WBM-Seite „Port-Auslastung“	262
Tabelle 110: WBM-Seite „RMON-Statistiken“	264
Tabelle 111: WBM-Seite „SFP-Information“	267
Tabelle 112: WBM-Seite „Traffic-Monitor“	270
Tabelle 113: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“	272
Tabelle 114: WBM-Seite „SNMP“ – Register „Community Name“	274
Tabelle 115: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“	276
Tabelle 116: WBM-Seite „SNMP Trap“ – Register „Trap Event Status“	277
Tabelle 117: WBM-Seite „SNMP-Trap“ – Register „Trap-Port-Einstellungen“	278
Tabelle 118: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-User“	280
Tabelle 119: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3-Gruppen“	281
Tabelle 120: WBM-Seite „SNMPv3-Konfiguration“ – Register „SNMPv3 View“	282
Tabelle 121: WBM-Seite „Auto Provision“	283
Tabelle 122: WBM-Seite „Mail-Alarm“	285
Tabelle 123: WBM-Seite „Wartung“ – Register „Protokolle“	291
Tabelle 124: WBM-Seite „System-Log“	293
Tabelle 125: WBM-Seite „Ping“	294
Tabelle 126: WBM-Seite „USB-Funktionen“	296
Tabelle 127: WBM-Seite „Benutzerkonto“	298
Tabelle 128: RJ-45-Kabel	300

Table 129: CLI "System Information" Configuration	301
Table 130: CLI "System" Configuration	302
Table 131: CLI "Jumbo Frame" Configuration	303
Table 132: CLI "SNTP" Configuration	304
Table 133: CLI "Management Host" Configuration	305
Table 134: CLI "MAC Management" Configuration	306
Table 135: CLI "Blackhole MAC" Configuration	306
Table 136: CLI "Port Mirroring" Configuration	307
Table 137: CLI "Port Settings" Configuration	308
Table 138: CLI "QoS" Configuration	309
Table 139: CLI "Rate Limitation" Configuration	310
Table 140: CLI "Storm Control" Configuration	310
Table 141: CLI "IGMP Snooping" Configuration	311
Table 142: CLI "IGMP Snooping Querier" Configuration	313
Table 143: CLI "IGMP Snooping Filtering" Configuration	313
Table 144: CLI "MVR" Configuration	314
Table 145: CLI "Multicast Address" Configuration	315
Table 146: CLI "Port Isolation" Configuration	315
Table 147: CLI "VLAN Settings" Configuration	316
Table 148: CLI "GARP/GVRP" Configuration	317
Table 149: CLI "IP Subnet VLAN" Configuration	318
Table 150: CLI "MAC VLAN" Configuration	318
Table 151: CLI "Protocol VLAN" Configuration	319
Table 152: CLI "VLAN Stacking" Configuration	320
Table 153: CLI "DHCP Relay" Configuration	321
Table 154: CLI "DHCP Options" Configuration	322
Table 155: CLI "Dual Homing" Configuration	322
Table 156: CLI "ERPS" Configuration	323
Table 157: CLI "Link Aggregation" Configuration	324
Table 158: CLI "LACP" Configuration	325
Table 159: CLI "LLDP" Configuration	326
Table 160: CLI "Loop Detection" Configuration	327
Table 161: CLI "Modbus" Configuration	328
Table 162: CLI "Static Route" Configuration	328
Table 163: CLI "STP" Configuration	330
Table 164: CLI "MSTP" Configuration	332
Table 165: CLI "Xpress Ring" Configuration	333
Table 166: CLI "DHCP Snooping" Configuration	334
Table 167: CLI "Server Screening" Configuration	335
Table 168: CLI "Binding Table" Configuration	335
Table 169: CLI "ARP Inspection" Configuration	336
Table 170: CLI "Filter Table" Configuration	336
Table 171: CLI "Access Control List" Configuration	337
Table 172: CLI "802.1X" Configuration	339
Table 173: CLI "Port Security" Configuration	340
Table 174: CLI "Alarm" Configuration	341
Table 175: CLI "Monitor Information" Configuration	341
Table 176: CLI "Port Statistics" Configuration	341
Table 177: CLI "Port Statistics" Configuration	341
Table 178: CLI "RMON Statistics" Configuration	341

Table 179: CLI "SFP Information" Configuration.....	341
Table 180: CLI "Traffic Monitor" Configuration.....	342
Table 181: CLI "SNMP" Configuration	343
Table 182: CLI "SNMP Trap" Configuration.....	344
Table 183: CLI "Port Trap Settings" Configuration.....	344
Table 184: CLI "SNMPv3" Configuration	345
Table 185: CLI "Auto Provision" Configuration	346
Table 186: CLI "Mail Alarm" Configuration.....	346
Table 187: CLI "Maintenance" Configuration	347
Table 188: CLI "Reboot" Configuration.....	348
Table 189: CLI "System Log" Configuration.....	348
Table 190: CLI "USB Flash" Configuration	349
Table 191: CLI "System Log" Configuration.....	350
Tabelle 192: Datenformat und Funktionscode	351
Tabelle 193: MODBUS-Register	352



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