TECHDOCS

Handbuch

WAGO-ETHERNET-Zubehör 852

852-1305

8/4-Port 1000BASE-T/1000BASE-SX/LX

Industrial-Managed-Switch, 8 Ports 1000BASE-T, 4 Slots 1000BASE-SX/LX

Version 1.2.0

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

Inhaltsverzeichnis

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 „8/4-Port 1000BASE-T/1000BASE-SX/LX“ (852-1305).

1.2 Urheberschutz

1.3 Symbole

GEFAHR

Warnung vor Personenschäden!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung 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 Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

WARNUNG

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

VORSICHT

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit geringem Risiko, die leichte oder mittlere Körperverletzung 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
kursiv	Namen von Pfaden und Dateien werden kursiv dargestellt z. B.: *C:\Programme\WAGO Software*
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. DIN EN418).

- Ihre Installationsausrüstung muss den EMV-Richtlinien entsprechen, damit elektromagnetische Beeinflussungen ausgeschlossen werden können.

- Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß DIN 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 Unfallverhütungs-vorschriften 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, da die Funktion der betroffenen Geräte langfristig nicht sichergestellt ist.

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 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

Das Switch-Angebot von WAGO sorgt für die Skalierbarkeit Ihrer Netzwerkinfrastruktur mit hervorragenden elektrischen und mechanischen Eigenschaften. Die robusten Geräte sind für den Industrieeinsatz ausgelegt und voll kompatibel zu den Standards IEEE 802.3, 802.3u, 802.3w, 802.3z, 802.3x, 802.3ab, 802.3ad, 802.1d, 802.1q, 802.1p und 802.1x.
Sie verfügen über eine Spannungsversorgung mit einem Versorgungsspannungsbereich 12 … 60 V. Leistungsmerkmale wie Autonegotiation und Auto-MDI/MDIX (crossover) an allen 10/100/1000BASE-T-Ports sind realisiert.

3.3 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.

Der Industrial-Managed-Switch wurde zur einfachen Installation in einer Fertigungsumgebung entwickelt, wo Vibrationen, Erschütterungen, Hitze und Hochfrequenzstörungen zum Alltag gehören.

Aufgrund seiner kompakten Bauform bietet der Industrial-Managed-Switch vor allem eine einfache Montage auf der Tragschiene und kann auch in Umgebungen mit begrenztem Platzangebot installiert werden.

Der Industrial-Managed-Switch kann durch die Hintereinanderschaltung von zwei oder mehr Switches erweitert werden. Da alle Anschlüsse 100 Mbit/s unterstützen, ist diese Reihenschaltung für den Industrial-Managed- Switch von jedem Anschluss aus und mit jeglicher Anzahl von Switches möglich.

Der Industrial-Managed-Switch verfügt über eine Vielzahl von Managementfunktionen, mit denen Sie gewünschte Kommunikationsparameter einfach konfigurieren können, um das Netzwerkverhalten auf unterschiedlichste Weise zu überwachen. Zusätzlich dazu verfügt der Industrial-Managed-Switch über duale redundante Leistungseingänge zur Maximierung der Zuverlässigkeit und Netzwerkverfügbarkeit. Durch die weiteren integrierten Funktionen dieser leistungsstarken und zugleich kostengünstigen Paketlösung, wie etwa Autonegotiation, „Rate Limitation“ (Ratenbegrenzung), „Port Isolation“ (Port-Trennung) etc., können Sie Ihre Netzwerkleistung optimieren und erhalten eine hohe Netzwerksicherheit.

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

Weitere Schlüsselfunktionen:

- Acht (8) 10/100/1000BASE-T, vier (4) 1000BASE-SX/LX (Glasfaser-Transceiver vom Typ SFP) und ein (1) Konsolenanschluss (RJ-45)
- Diagnose-LEDs auf der Vorderseite
- Web-basiert/SNMP-Management
- Redundante DC-Spannungsversorgung
- Großer Verspannungsbereich: 12 … 60 V
- DIP-Schalter für Freigabe von Alarmfunktionen
- Voll kompatibel zu den Standards IEEE 802.3, 802.3u, 802.3z, 802.3x, 802.3ad, 802.3ab, 802.1d, 802.1q, 802.1p, 802.1w, 802.1x
- Implementierte Funktionen:
  - Dual Ring
  - ERPS
  - Jet Ring
  - Xpress-Ring (Redundanter Ring, Umkonfiguration < 50 ms)
- Non-blocking, Store-and-Forward-Switching, Rapid Spanning Tree-Protocol (RSTP)
- Autonegotiation an allen 10/100/1000Base-T-Ports
- Auto-MDI/MDIX (crossover) an allen 10/100/1000BASE-T-Ports
- VLAN (802.1q) VID
- IGMP-Snooping für Multicast-Filterung
- Port-Konfiguration, -Status, -Statistik
- Port-Trunking
- SNMP v1/v2 und RMON
- Stabiles Metall-IP30-Gehäuse
- Funktionsfähig bei Vibrationen/Erschütterungen

4 Gerätebeschreibung

Der 852-1305 ist ein industrieller ETHERNET-Switch mit 8 10/100/1000BASE-T-Ports, Autonegotiation und Auto-MDI-/MDI-X-Erkennung an jedem Port.
Durch die 8 Ports des Industrial-Managed-Switches können mehrere Segmente zur Reduzierung der Netzwerküberlastung gebildet werden und jedem Benutzerknoten eine eigene Bandbreite zugewiesen werden.

Weiterhin besitzt der Industrial-Managed-Switch 852-1305 4 Ports mit SFP-1000BASE-SX/LX für den Anschluss von Multi-Mode- oder Single-Mode-Glasfaserkabeln für Wellenlängen von 850 nm (SX), 1310 nm (LX) und 1550 nm (ZX).
Der 852-1305 ist eine kostengünstige Lösung, um auf die wachsende Nachfrage nach IP-basierter, industrieller Kommunikation reagieren zu können.
Der Industrial-Managed-Switch lässt sich einfach konfigurieren und installieren und ist insbesondere für kleine und mittlere Netzwerke geeignet.

4.1 Ansicht

4.1.1 Frontansicht

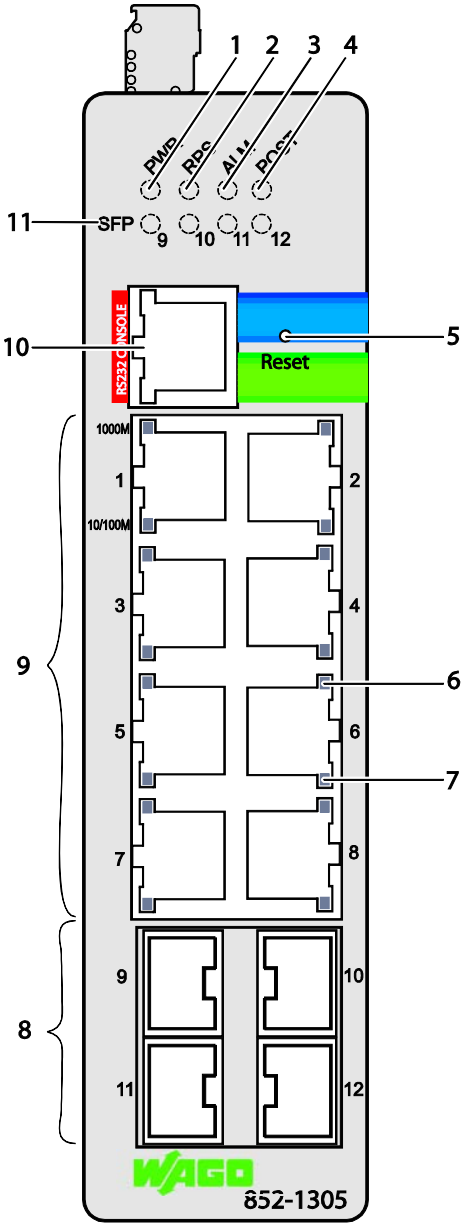


Abbildung 1: Frontansicht des Industrial-Managed-Switches

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

Pos.	Be-zeichnung	Bedeutung	Details siehe Kapitel
1	PWR	Status-LED Versorgungsspannung	„Gerätebeschreibung“ > „Anzeigeelemente“
2	RPS	Status-LED-Redundante Versorgungsspannung	„Gerätebeschreibung“ > „Anzeigeelemente“
3	ALM	Staus-LED Alarm	„Gerätebeschreibung“ > „Anzeigeelemente“
4	POST	Status-LED POST	„Gerätebeschreibung“ > „Anzeigeelemente“

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

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

4.1.2 Draufsicht

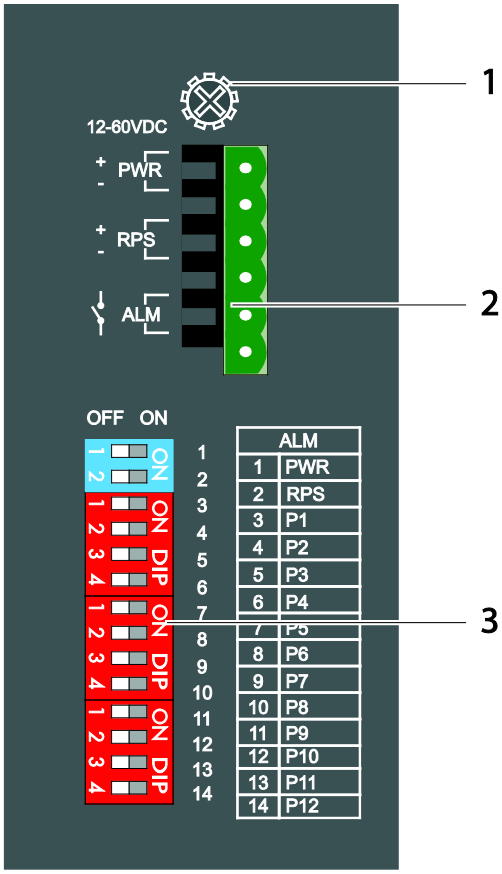


Abbildung 2: Draufsicht des Industrial-Managed-Switches

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

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

4.2 Anschlüsse

4.2.1 Spannungsversorgung (PWR/RPS)

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

Die Stiftleiste hat folgende Belegung:

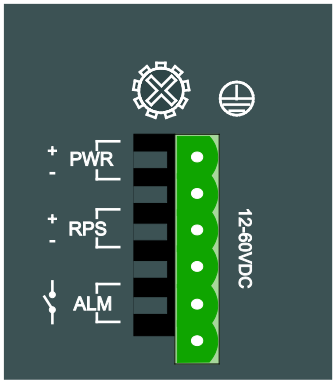


Abbildung 3: Anschluss Spannungsversorgung (PWR/RPS)

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.

4.2.2 Netzwerkanschlüsse

Der Industrial-Managed-Switch verwendet Anschlüsse mit Glasfaser- oder Kupfersteckern, die mit ETHERNET- und/oder Fast-ETHERNET-Protokollen funktionsfähig sind.

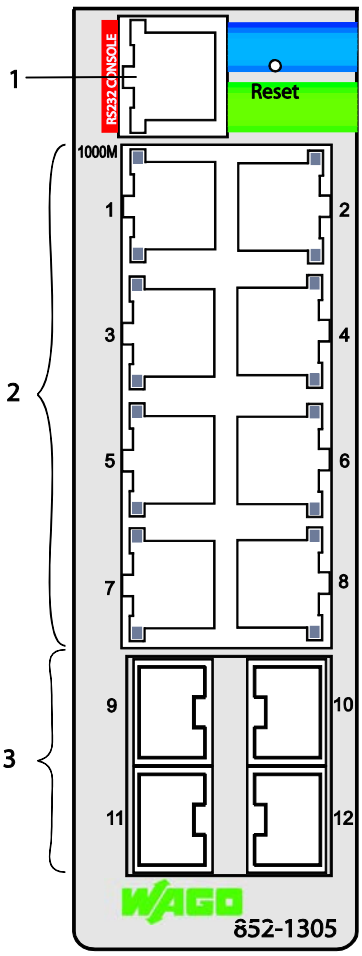


Abbildung 4: Netzwerkanschlüsse

Tabelle 6: Legende zur Abbildung „Netzwerkanschlüsse“

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

4.2.2.1 RJ-45-Anschluss

Der Anschluss an die ETHERNET-basierenden Feldbusse erfolgt über die RJ-45-Steckverbinder, auch „Westernstecker“ genannt, die über einen integrierten Switch mit dem Feldbuscontroller verbunden sind.
Der integrierte Switch arbeitet im Store-and-Forward-Betrieb und unterstützt für jeden Port die Übertragungsgeschwindigkeiten 10/100 Mbit/s sowie die Übertragungsmodi voll- bzw. halbduplex.
Die RJ-45-Buchse ist entsprechend den Vorgaben für 100BASE-TX beschaltet. Als Verbindungsleitung wird vom ETHERNET-Standard ein Twisted-Pair-Kabel der Kategorie 5e vorgeschrieben. Dabei können Leitungen des Typs S-UTP (Screened-Unshielded Twisted Pair) sowie STP (Shielded Twisted Pair) mit einer maximalen Segmentlänge von 100 m benutzt werden.
Die Anschlussstelle ist so konzipiert, dass nach Steckeranschluss ein Einbau in einen 80 mm hohen Schaltkasten möglich ist.

4.2.2.2 1000BASE-SX/LX-Anschlüsse

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

4.2.2.3 10/100/1000BASE-T-Anschlüsse

Die 10/100/1000BASE-T-Anschlüsse unterstützen die Netzwerkgeschwindigkeiten 10 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 Netzwerkkabel einfach in die Anschlüsse zu stecken, diese passen sich dann an die Endknotengeräte an.
Folgende Kabel werden für die RJ-45-Anschlüsse empfohlen:

- 10 m – Cat 3 oder besser / 100 m – Cat 5e oder besser

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

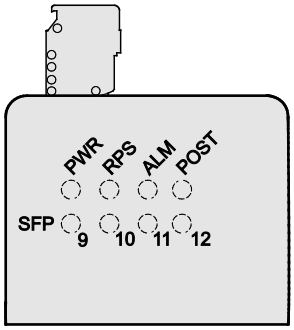


Abbildung 5: Geräte-LEDs

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.
		Aus	Es wird kein Alarm gemeldet.
POST	Power-On-Self-Test-LED	Blinkt	Der Selbsttest wird ausgeführt.
		Grün	Der Switch ist betriebsbereit.
		Aus	Der Switch ist nicht betriebsbereit

Tabelle 7: Legende zur Abbildung „Geräte-LEDs“

LED		Name	Status	Beschreibung
SFP	9	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.
	10	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.
	11	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.
	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

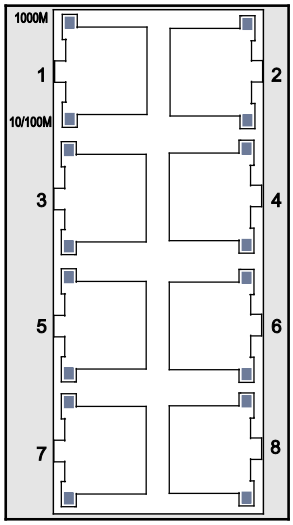


Abbildung 6: Anschluss-LEDs

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-Switch befinden sich DIP-Schalter für die Alarm- und Arbiter-Konfigurationen.

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

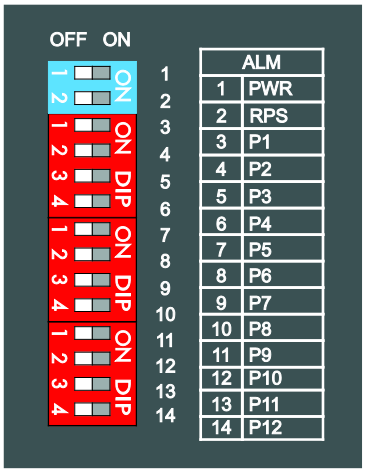


Abbildung 7: DIP-Schalter

Tabelle 9: Legende zur Abbildung „DIP-Schalter“

Nr.	Name	Status	Beschreibung
1	PWR	ON	Die Alarmberichtfunktion für das primäre Netzteil ist aktiviert.
		OFF	Die Alarmberichtfunktion für das primäre Netzteil ist deaktiviert.
2	RPS	ON	Die Alarmberichtfunktion für das sekundäre Netzteil ist aktiviert.
		OFF	Die Alarmberichtfunktion für das sekundäre Netzteil ist deaktiviert.
3 … 14	P1 … P12	ON	Die Alarmberichtfunktion für die Verbindung von Anschluss x ist aktiviert.
		OFF	Die Alarmberichtfunktion für die Verbindung von Anschluss x ist deaktiviert.

Sowohl jeder Anschluss als auch der externe Alarm oder die redundante Stromversorgung können 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 alle DIP-Schalter auf „OFF“.

2 Installieren Sie den Industrial-Managed-Switch in Ihrem Netzwerk.

3 Wählen Sie den (die) Port(s), der zu überwachen ist oder der den Alarm aktivieren soll.

4 Stellen Sie den DIP-Schalter des entsprechenden Anschlusses auf „ON“.

5 Schalten Sie den Industrial-Managed-Switch ein.

4.4.2 Reset-Taster

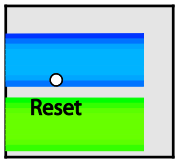


Abbildung 8: Reset-Taster

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 9: Aufkleber (Beispiel)

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

Nr.	Beschreibung „Serial NO“
02	Firmwareversion
01	Hardwareversion

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		910 g
Schutzart		IP30

4.6.2 Systemdaten

Tabelle 13: Technische Daten – Systemdaten

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

4.6.3 Versorgung

Tabelle 14: Technische Daten – Versorgung

Versorgungsspannung	DC 12 … 60 V
Leistungsaufnahme max.	18 W

4.6.4 Kommunikation

Tabelle 15: Technische Daten – Kommunikation

Ports	8 x 10/10/1000BASE-T (RJ-45); 4 x SFP 1000BASE-SX/LX, Glasfaser; 1 x RS-232 (RJ-45)
Standards	IEEE 802.3u 100BASE-TX/FX; IEEE 802.3ad Link Aggregation; IEEE 802.3 10BASE-T; IEEE 802.1d Spanning Tree Protocol; IEEE 802.3x Flow Control; IEEE 802.1p CoS Prioritization; IEEE 802.1q VLAN Tagging; IEEE 802.3ab LLDP; IEEE 802.3ab 1000BASE-T; IEEE 802.3w RSTP; IEEE 802.3z 1000BASE-SX/LX; IEEE 802.1x Port Authentication
Topologie	Ring und Stern

4.6.5 Umgebungsbedingungen

Tabelle 16: Technische Daten – Umgebungsbedingungen

Umgebungstemperatur, Betrieb	-40 … +70 °C
Umgebungstemperatur, Betrieb, DNV GL (Temperaturklasse D)	-25 … +70 °C
Umgebungstemperatur, Lagerung	-40 …+80 °C
Relative Feuchte (ohne Betauung)	95 %
Vibrationsfestigkeit	Gemäß IEC 60068-2-6
Schockfestigkeit	Gemäß IEC 60068-2-27
EMV-1-Störfestigkeit	Gemäß EN 61000-6-2
EMV-1-Störaussendung	Gemäß EN 61000-6-4
Standardkompass Sicherheitsabstand 0,3 Grad Durchbiegung	750 mm
Lenkung, Standby, Notfallkompass Sicherheitsabstand 1,0 Grad Durchbiegung	500 mm

4.7 Zulassungen

Folgende Zulassungen wurden für das WAGO-ETHERNET-Zubehör „8/4-Port 1000BASE-T/1000BASE-SX/LX“ (852-1305) erteilt:

CE Konformitätskennzeichnung

Folgende Zulassungen sind für das WAGO-ETHERNET-Zubehör „8/4-Port 1000BASE-T/1000BASE-SX/LX“ (852-1305) in Vorbereitung:

c UL us Ordinary Locations UL61010-2-201

Folgende Schiffszulassungen wurden für das WAGO-ETHERNET-Zubehör „8/4-Port 1000BASE-T/1000BASE-SX/LX“ (852-1305) erteilt:

DNV GL
[Temperature: D, Humidity: B, Vibration: C, EMC: B, Enclosure: A]

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 Industrial-Managed-Switch verwendet eine Gleichstromversorgung, die für 48 … 57 V ausgelegt ist.

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

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

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

1 Überprüfen Sie, ob die Netz-LED an der Vorderseite leuchtet, wenn das Gerät eingeschaltet ist. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig eingesteckt ist und fest sitzt.

2 Falls ein sekundäres Netzteil angeschlossen ist, leuchtet die RPS-LED.

3 Leiter PWR +/-:
Zum Anschließen oder Lösen der Leiter betätigen Sie in der Federleiste direkt die Feder mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder lösen ihn.

4 Für den Backup-Gleichstromanschluss führen Sie dieselben Schritte wie oben aus. Stecken Sie die Leiter in die Federleiste (in gekennzeichneter „RPS +/-„ Position).

5 Falls die Federleiste noch nicht in die Stiftleiste des Switches gesteckt wurde, stecken Sie sie jetzt ein.

6 Überprüfen Sie, ob die Netz-LED an der Oberseite leuchtet, wenn das Gerät mit Spannung versorgt wird. Ist dies nicht der Fall, vergewissern Sie sich, dass das Netzkabel richtig eingesteckt 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 Verbindungsfehler (z. B. getrennte Leitung, Geräteausfall, etc.)

2 PWR/RPS:
   a Versorgungsfehler (Stromleitung ist unterbrochen, Versorgungsstörung, etc.)
   b Die Eingangsversorgungsspannung liegt außerhalb der Spezifikationen (12 … 60 V)

3 Fehler im Jet-Ring oder ERPS-Ring (Enhancement Mode).

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 Auto-Negotiation.

1 Verbinden Sie ein Ende eines verdrillten Kabels vom Typ Category 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 1500 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 für „Jumbo Frames“ hat Auswirkungen auf alle Ports.

Übersteigt die Größe eines Paketes die des „Jumbo Frames“, wird das Paket verworfen.

7.1.2 SNTP

Das SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) ist ein Protokoll zur Synchronisierung von Uhren in Computersystemen. Es ist eine weniger komplexe Implementierung eines NTP („**N**etwork **T**ime **P**rotocol“).

SNTP verwendet die koordinierte Weltzeit UTC („**C**oordinated **U**niversal **T**ime, französisch: **T**emps **U**niversel **C**oordonné“). Es werden keine Informationen über Zeitzonen oder Sommerzeiten übertragen. Diese Informationen liegen außerhalb des Protokollbereichs und müssen separat bezogen werden.

Der SNTP-Port ist 123.

Hinweis

Hinweis

1. Der SNTP-Server antwortet immer mit der aktuellen koordinierten Weltzeit UTC.
2. Empfängt der Switch die SNTP-Antwortzeit, gleicht er diese Zeit mit der Zeitzonenkonfiguration 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 („**M**edia **A**ccess **C**ontrol **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 empfangenem Port, dem VLAN und einer „Age Time“ (Lebensdauer) in der Adresstabelle abspeichert. Wenn die „Age Time“ abgelaufen ist, wird der Adresseintrag aus der Adressstabelle 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.

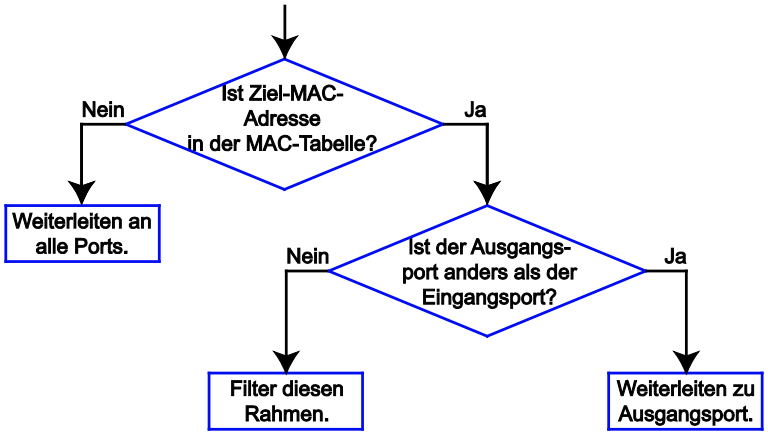


Abbildung 10: Ablaufdiagramm der MAC-Adresstabelle

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 MAC-Blacklist (Blacklisting)

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 („**I**ntrusion **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 verbunden 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.

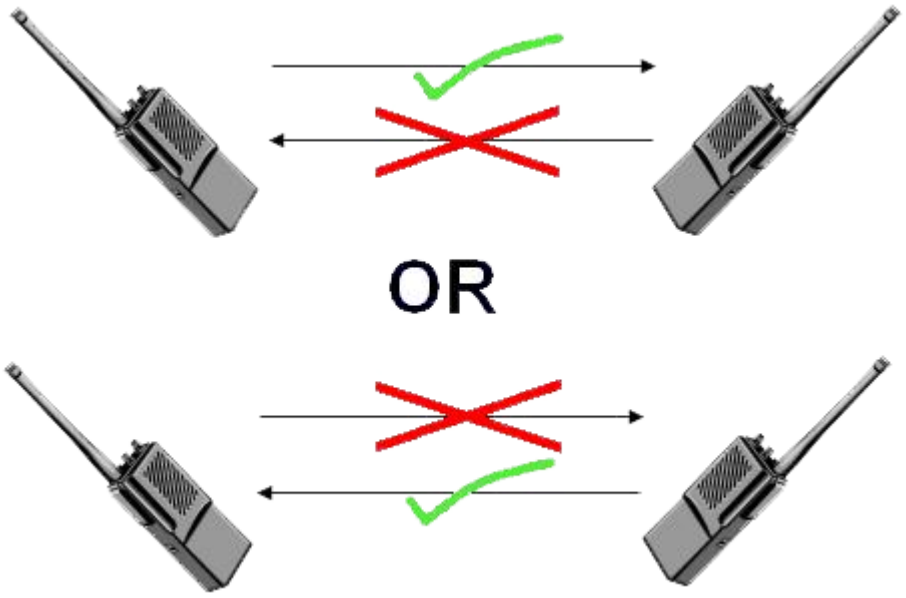


Abbildung 11: Halbduplexmodus

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 12: 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) zurückleitet werden und somit ein geschlossener Kommunikationskreislauf an einem einzelnen Computer simuliert werden kann.

Auto MDI/MDIX

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

Auto-MDIX („**Aut**omatic **M**edium-**D**ependent **I**nterface **C**rossover“) ist eine im Port integrierte Netzwerktechnologie, die die erforderliche Netzwerkkabelart („Straight-Through“- oder „Crossover“-Kabel) automatisch erkennt und die Verbindung entsprechend konfiguriert.
Dadurch werden „Crossover“-Kabel zur Verbindung von Geräten überflüssig.
Die Schnittstelle korrigiert falsche Verkabelungen automatisch.
Damit Auto-MDIX korrekt funktioniert, muss die Geschwindigkeit für die Schnittstelle und in der Duplexeinstellung auf „Auto“ eingestellt sein.

Autonegotiation

Autonegotiation ist ein Verfahren, bei dem zwei miteinander verbundene ETHERNET-Netzwerk-Ports (z. B. der Netzwerk-Port eines PC und der eines Routers, Hubs oder Switches, mit dem dieser z. B. verbunden ist) selbständig die maximal mögliche Übertragungsgeschwindigkeit und das Duplexverfahren miteinander auszuhandeln und konfigurieren.
Autonegotiation gilt nur für Mehrdrahtverbindungen (Twisted-Pair-Kabel) – nicht aber für WLAN-, Glasfaser- oder Koaxialkabelverbindungen.

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

Flow Control

Die „Flow Control“ (Datenflusssteuerung) reguliert die Übertragung von Signalen, indem sie sie der Bandbreite am Eingangs-Port anpasst.
Ein hoher Datenverkehr am Port reduziert die Bandbreite und kann den Pufferspeicher überlaufen lassen, wodurch es zu Paket- und Frame-Verlusten kommen kann.

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

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

7.2.1.1 QoS

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

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

Bei der Konfiguration der Funktion QoS (**„Q**uality **o**f **S**ervice“, Dienstgüte) kann ein spezifischer Datenverkehr ausgewählt, 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 („**D**ifferentiated **S**ervices **C**ode **P**oints“, 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	1 Bit	12 Bit
TPID (0x8100)	Priorität	CFI	VID

- TPID („**T**ag **P**rotocol **Id**entifier“, 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 **Id**entifier“, 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 („**Diff**erentiated **Serv**ices“) ist eine Computernetzwerkarchitektur, die einen einfachen, skalierbaren und grobkörnigen Mechanismus zur Klassifizierung, Netzwerkverkehrsverwaltung und Bereitstellung von QoS („**Q**uality **o**f **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 Rate Limitation

7.2.1.2.1 Storm Control

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

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

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

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

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“ („**I**nternet **G**roup **M**anagement **P**rotocol **Snooping**“) 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 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.

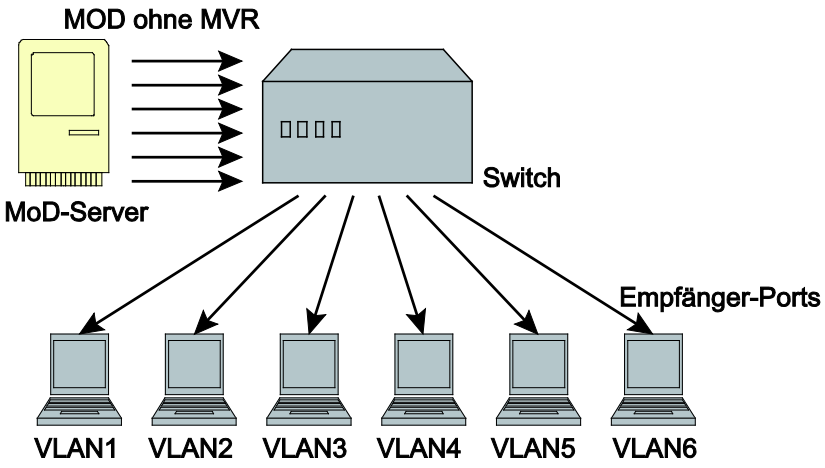


Abbildung 13: MOD ohne MVR

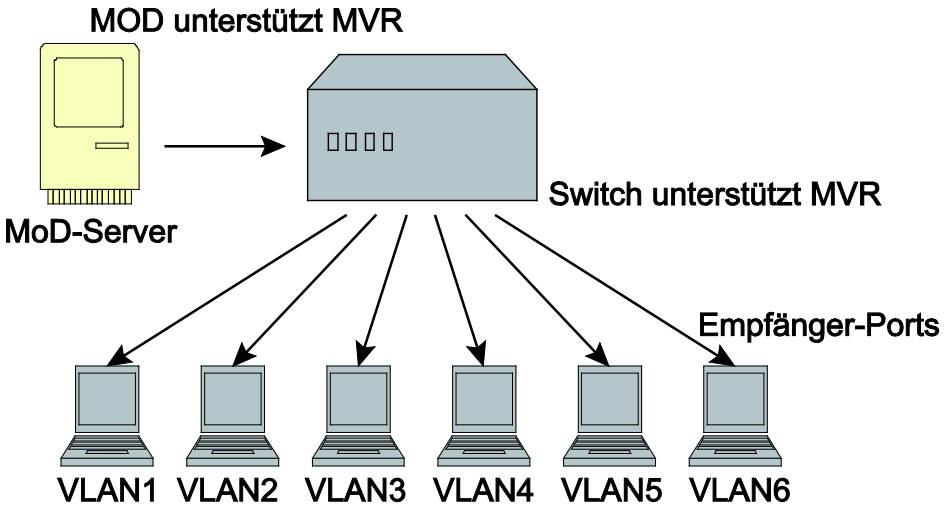


Abbildung 14: MOD unterstützt MVR

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 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.

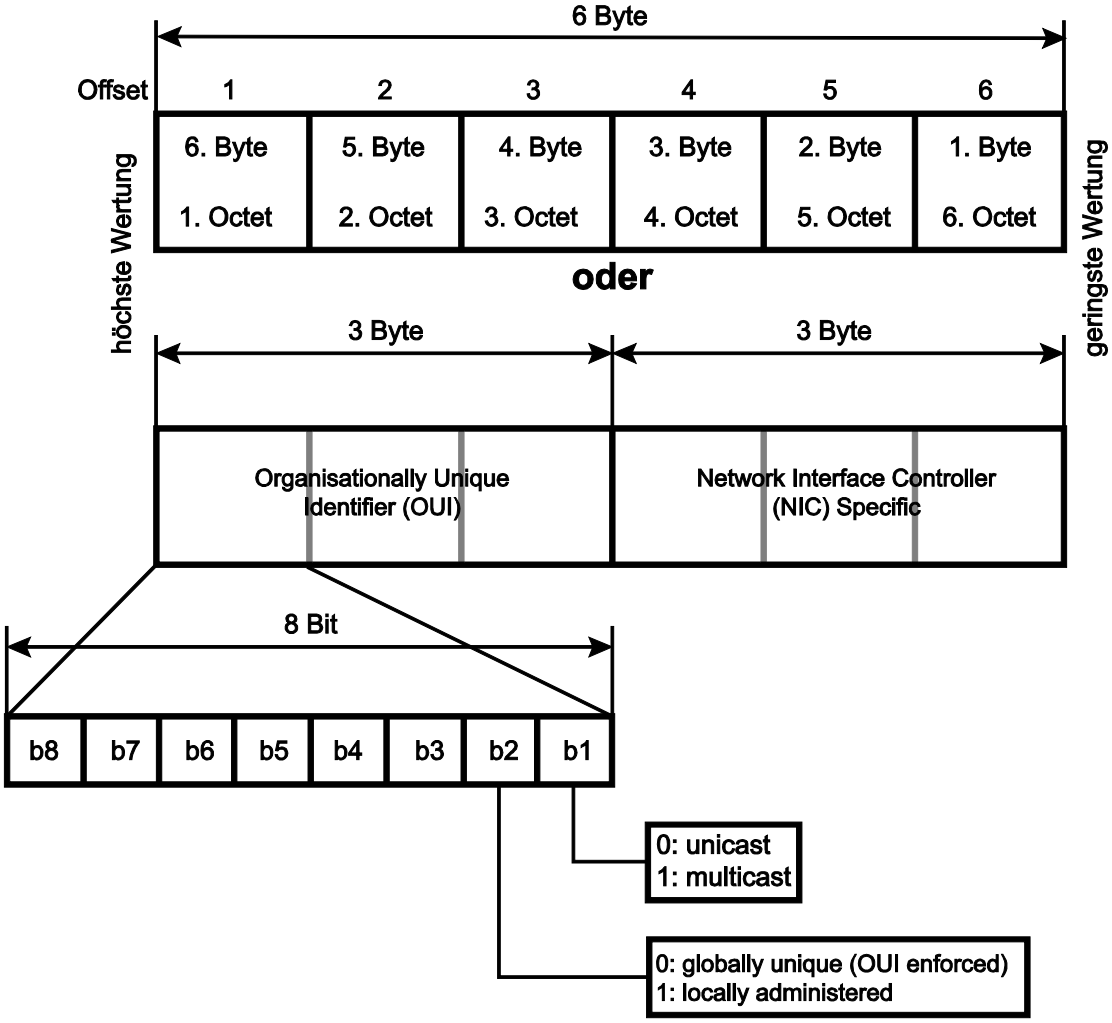


Abbildung 15: Multicast-Adresse

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 („**V**irtuelles **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 („**V**LAN-**ID**“) ist die Kennzeichnung des VLANs, die im Wesentlichen vom Standard 802.1Q verwendet wird. Sie besteht aus12 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 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-Identifier) 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**ttribute **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 **Id**entification“) 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 (Internetdienstanbietern) benötigt, die TLS („**T**ransparent **L**AN **S**ervices“) verwenden, und die ihre eigenen VLANs unabhängig von den Kunden-VLANs betreiben. Normalerweise verbindet jedes Dienstanbieter-VLAN eine Gruppe von Standorten eines Kunden miteinander. Ein Dienstanbieter-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 („**P**rovider **E**dge“, Netzwerkendpunkt auf Anbieterseite) gesendet werden. Dieser VLAN-Tag entspricht dem VLAN des Dienstanbieters. Wenn der Frame die Ziel-PE erreicht, wird das Dienstanbieter-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 Dienstanbieter-VLAN-Tag bestimmt die Mitgliedschaft im VPLS („**V**irtual **P**rivate **L**AN **S**ervice“). 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 Dienstanbieter 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 („**A**pplication **S**ervice **P**roviders“, Anwendungsdienstanbietern).

Die mit den Dienstanbieter-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 („**T**ag **P**rotocol **I**dentifier“) 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 („**V**LAN-**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	Date n	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 Dienstanbieters. 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 Dienstanbieternetzwerks (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.

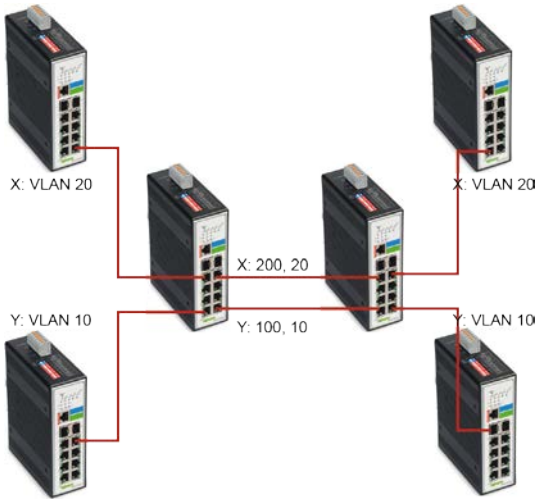


Abbildung 16: Port-basiertes Q in Q

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 Dienstanbieters zu versehen.

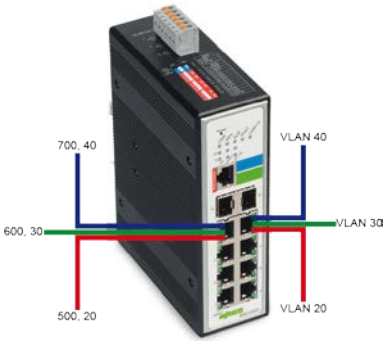


Abbildung 17: Konfigurationsbeispiel

7.2.4 DHCP-Relay

Da die „DHCPDISCOVER“-Nachricht 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.

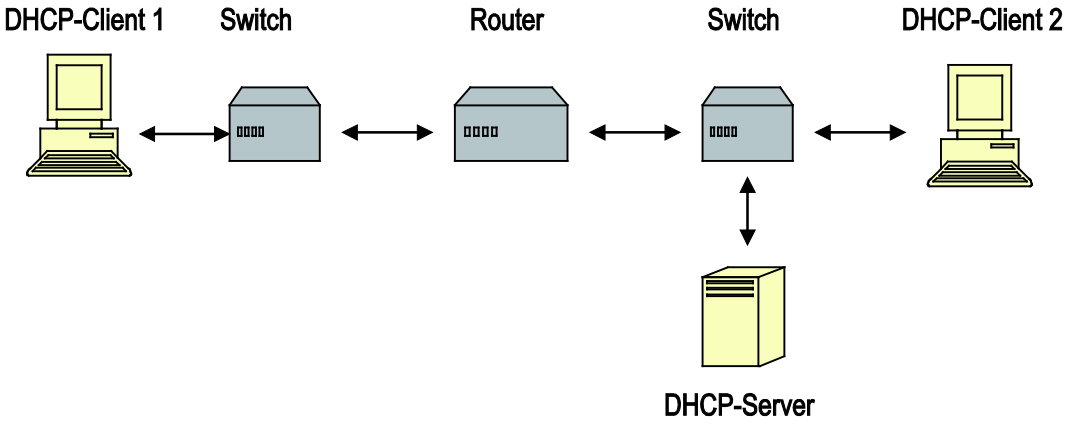


Abbildung 18: Anwendung 1 (über einen Router)

- **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.

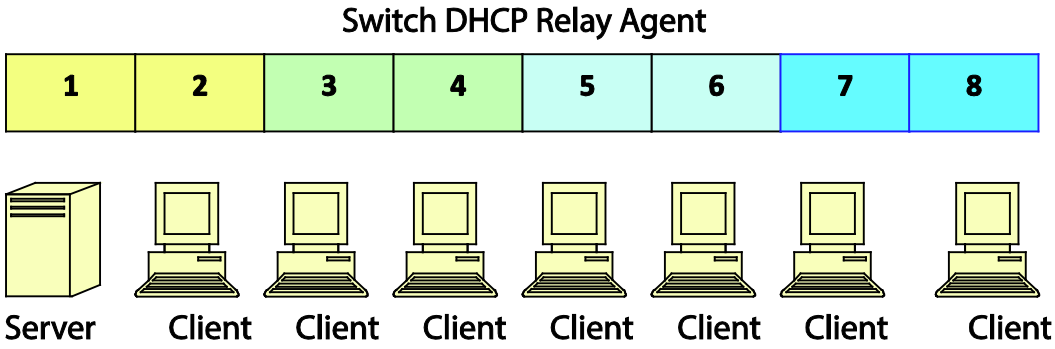


Abbildung 19: Anwendung 2 (Lokal in verschiedenen VLANs)

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 Relay Option 82

„DHCP Option 82“ („**DHCP** Relay Agent Information **Option**“). Die Option 82 wurde entwickelt, um es dem „DHCP Relay Agent“ zu ermöglichen, anschlussspezifische 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“ (Endgerätekennung).

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 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.

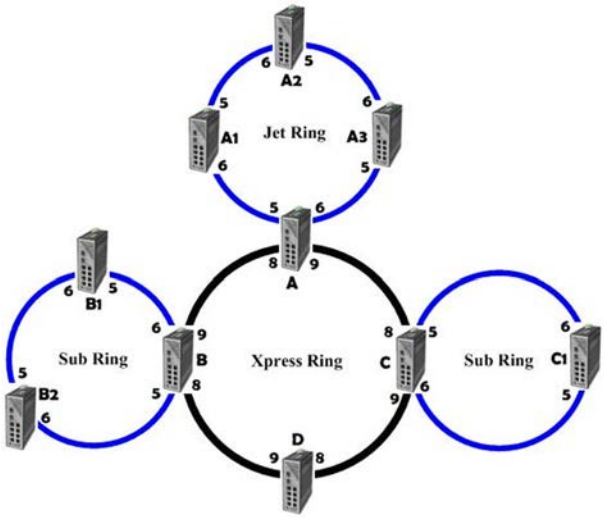


Abbildung 20: Dual Ring Switch ABC

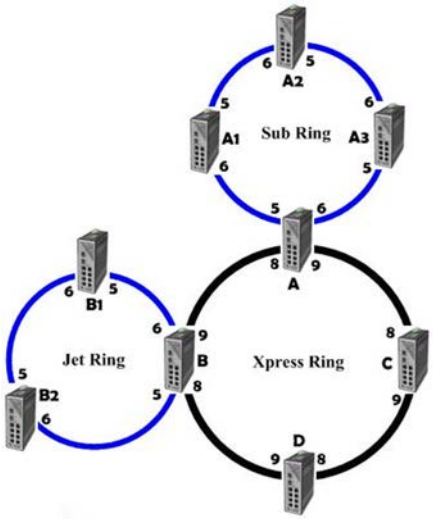


Abbildung 21: Dual Ring Switch AB

7.2.7 ERPS

Die Funktion ERPS („**E**THERNET **R**ing **P**rotection **S**witching“) implementiert gemäß dem ITU-T-Standard G.8032 einen Schutzschaltungsmechanismus für Ring-Topologien in der ETHERNET-Schicht. Dabei schützt das Protokoll ERP („**E**THERNET **R**ing **P**rotection“) 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 („**R**ing **P**rotection **L**ink“) 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 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 **Timer**“, 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 **Timer**“, 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.

7.2.8 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.

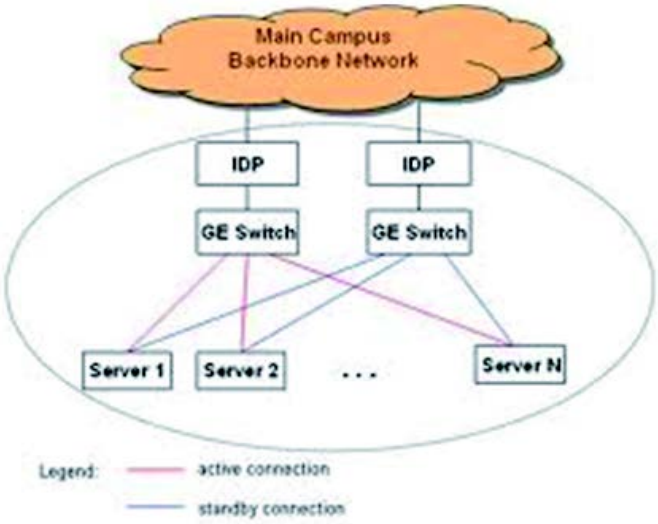


Abbildung 22: Dual Homing

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.

7.2.9 Link Aggregation

7.2.9.1 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.

7.2.9.2 LACP

Der Switch unterstützt gemäß dem Standard IEEE 802.3ad statisches und dynamisches (LACP) „Port Trunking“. Im Standard IEEE 802.3ad wird das LACP („**L**ink **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.

7.2.10 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 Base“) gespeichert. Dadurch wird einem NMS („**N**etwork **M**anagement **S**ystem“) ermöglicht, mittels eines Managementprotokolls, wie etwa dem SNTP („**S**imple **N**etwork **M**anagement **P**rotocol“), auf diese Informationen zuzugreifen.

7.2.11 Schleifenerkennung (Loop Detection)

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

Die „Loop Detection“ sendet regelmäßig 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.

7.2.12 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.

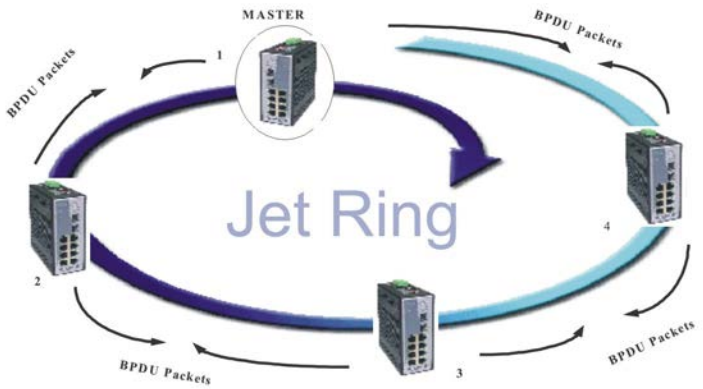


Abbildung 23: Jet Ring

Schritt 2

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

7.2.13 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 Konfigurationsnachtichten (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 Spannbaums.
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.

7.2.14 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 Sicherheit

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 DHCPOFFER, DHCPACK, DHCPNAK oder DHCPLEASEQUERY, 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.

Die wichtigsten Aufgaben des „DHCP Snooping“ sind:

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

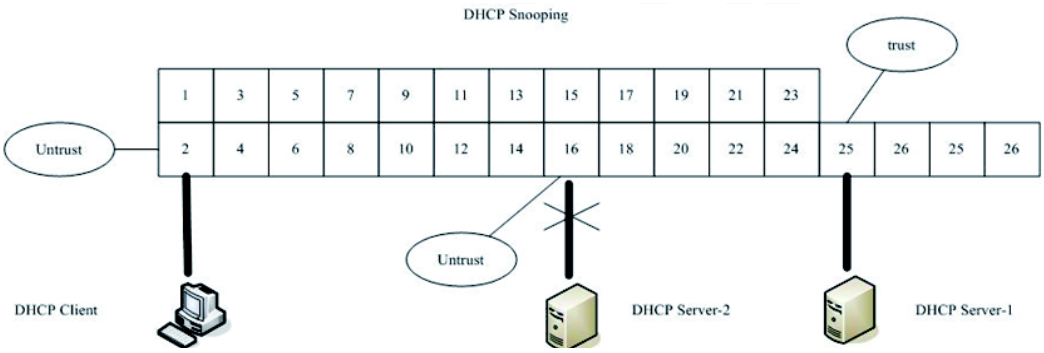


Abbildung 24: DHCP Snooping

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

7.3.1.1.1 Server Screening

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.

Ist diese Funktion aktiviert, muss zuvor auch die Funktion „DHCP Snooping“ aktiviert sein. Der Switch ermöglicht die Konfiguration von bis zu drei gültigen DHCP-Servern.

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

7.3.1.2 Binding Table

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 **Inspection**“, 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 Zugriffskontrollliste ACL

Die ACL („**A**ccess **C**ontrol List“, 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.

7.3.3 802.1x

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).

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-**I**n **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-**I**n **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 Benutzerkennung, 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.

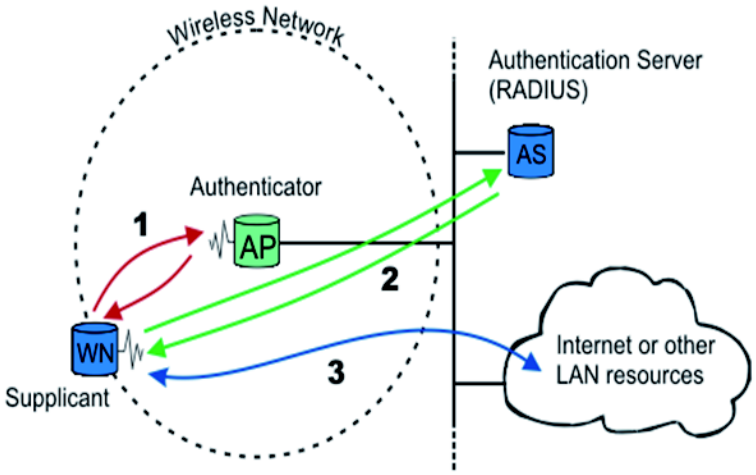


Abbildung 25: 802.1x

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.

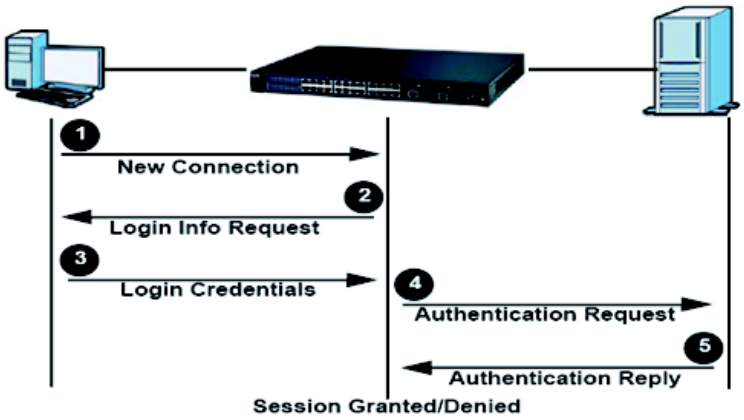


Abbildung 26: RADIUS-Server

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.

7.4 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 Monitor Informationen

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

7.4.3 RMON Statistiken

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

Jabber

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

7.4.4 SFP

SFP („**S**mall **F**orm-factor **P**luggable“) sind kleine standardisierte Module für Netzwerkverbindungen.
SFP bezeichnet eine modulare Schnittstelle zur Unterstützung verschiedener Übertragungsmedien und wird in der Netzwerktechnik zur Flexibilisierung von Schnittstellen verwendet.

7.4.4.1 DDM

DDM („**D**ynamic **D**evice **M**apping“) ist eine Technologie für KVM-Switches mit USB-Anschlüssen, die manchmal als Alternative zu der Standard-USB-Tastatur und -Maus-Emulation benutzt wird.

7.4.5 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 Paketrate 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

Das SNMP („**S**imple **N**etwork **M**anagement **P**rotocol“) wird in Netzwerkverwaltungssystemen verwendet, um angeschlossene Geräte auf Zustände hin zu überwachen, die die Aufmerksamkeit eines Administrators erfordern. SNMP ist ein Bestandteil der durch die IETF („**I**nternet **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 das Trap empfängt, kann nach weiteren Informationen nachfragen.

7.5.3 Auto Provision

Die Funktion „Auto Provision“ (Automatische Bereitstellung) ist ein von Dienstanbietern 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 Dienstanbieters herunterladen.

   Der Dateiname wird nach folgender Benennungsregel gebildet:
   Model_Name_Autoprovision.txt

   Beispiel: MEN-**5210_Autoprovision.t**xt

   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: „Model_Name _“ mit 12-Bit-MAC-Ziffern, z. B. „MEN-5210_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.

7.5.4 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.

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 **I**nterface“) aufgerufen werden

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

Der Verwaltungsagent umfasst auch einen eingebetteten HTTP-Webagenten. Auf diesen Webagenten kann mit einem 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**	
	FW-Version 01	**ab FW-Version 02**
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	admin
Default Password	Wago1951	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.

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

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	
	FW-Version 01	ab FW-Version 02
Default Username (Default-Benutzername)	admin	admin
Default Password (Default-Passwort)	Wago1951	wago

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.

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

9 Im Web-Based-Management-System (WBM) konfigurieren

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:
   Firmware-Version 01: User = „admin“
   Passwort = „Wago1951“
   Firmware-Version 02: 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]**
• Systeminformationen
▶ **[Grundeinstellungen]**
• Allgemeine Einstellungen • MAC-Management • Port-Mirroring • Port-Einstellungen

▶ **[Erweiterte Einstellungen]**

▶ **[Bandbreiten-Einstellungen]**

- QoS
- Bandbreitenbegrenzung

▶ **[IMGP-Snooping]** ▶

- IGMP-Snooping
- IGMP-Filter
- MVR
- Statische Multicast-Adressen
- Multicast-Statistiken

▶ **[VLAN]** ▶

- Port-Isolation
- VLAN
- GVRP
- IP-Subnet-VLAN
- MAC-VLAN
- Protokoll-VLAN
- Q-in-Q

- DHCP-Relay
- DHCP-Optionen
- Dual-Homing
- Dual-Ring
- ERPS
- Link-Aggregation
- LLDP
- Schleifenerkennung
- Jet-Ring
- MODBUS
- STP
- Xpress-Ring

▶ **[Sicherheit]**

[IP-Source-Guard] ▶

- DHCP-Snooping
- DHCP-Snooping-Binding-Table
- ARP-Überprüfung

- Access-Control-Liste
- IEEE 802.1x
- Port-Sicherheit

▶ [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
- Benutzerkonto

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

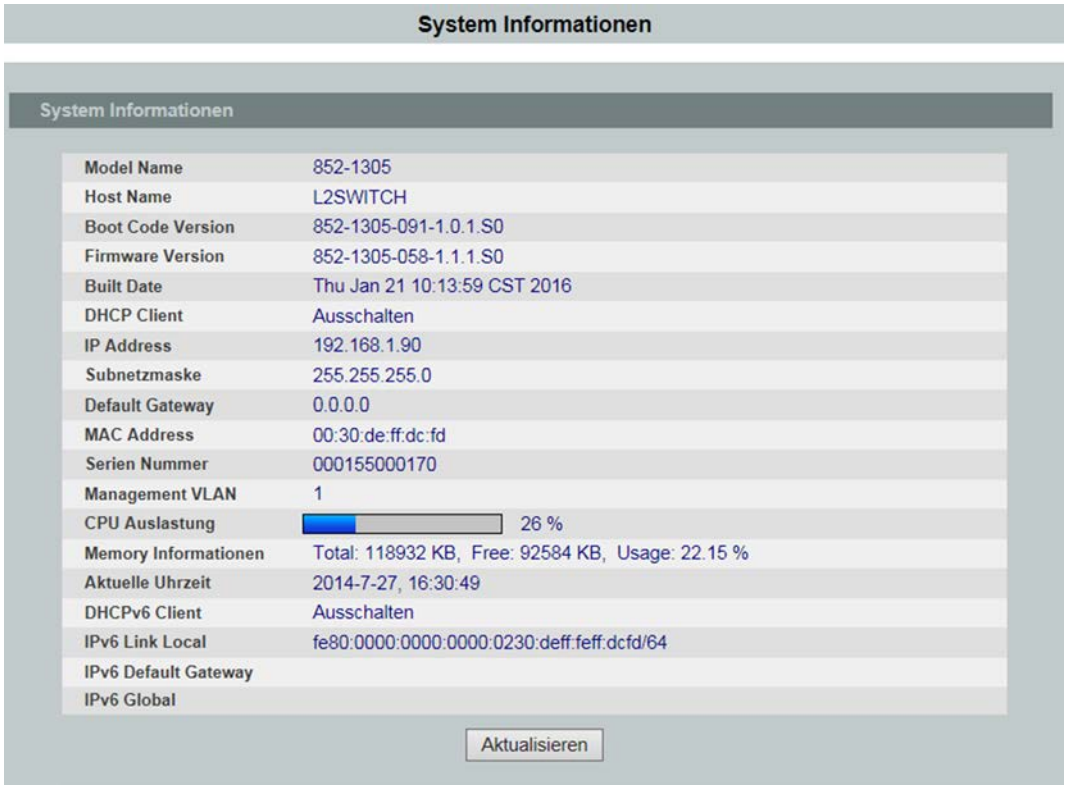


Abbildung 27: WBM-Seite „Systeminformation“

Tabelle 30: WBM-Seite “Systeminformation”

Parameter	Beschreibung
Model Name	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
Host Name	In diesem Anzeigefeld wird der Hostname des Switches angezeigt.
Boot Code Version	In diesem Anzeigefeld wird die Boot-Code-Version angezeigt.
Firmware Version	In diesem Anzeigefeld wird die Versionsnummer der aktuell installierten Firmware angezeigt.
Built Date	In diesem Anzeigefeld wird das Erstellungsdatum der aktuell installierten Firmware angezeigt.
DHCP Client	In diesem Anzeigefeld wird angezeigt, ob die DHCP-Client-Funktion aktiviert ist.
IP Address	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt.
[Subnetzmaske]	In diesem Anzeigefeld wird die Subnet-Maske des Switches angezeigt.
Default Gateway	In diesem Anzeigefeld wird das Default-Gateway des Switches angezeigt.
MAC Address	In diesem Anzeigefeld wird die MAC (Media-Access-Control)-Adresse des Switches angezeigt.
[Serien Nummer]	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.
Memory Informationen	In diesem Anzeigefeld wird der gesamte, sowie der momentan verfügbare („Free“) und verwendete („Used“) Speicher des Switches angezeigt.
Aktuelle Uhrzeit	In diesem Anzeigefeld wird das aktuelle Datum (yyyy-mm-dd) und die aktuelle Uhrzeit (hh:mm:ss) angezeigt.
[DHCPv6 Client]	In diesem Anzeigefeld wird angezeigt, ob der DHCPv6-Client ein oder ausgeschaltet ist.
[IPv6 Link Local]	In diesem Anzeigefeld wird die IPv6-Link-Local-Adresse angezeigt.
[IPv6 Default Gateway]	In diesem Anzeigefeld wird das Default-Gateway des Switches angezeigt.
[IPv6 Link Global]	In diesem Anzeigefeld wird angezeigt, ob auch die globale IPv6-Link-Adresse mit eingeben 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

Abbildung 28: 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.

Tabelle 31: WBM-Seite „Allgemeine Einstellungen“ – Register „System“

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	**192.168.0.254**	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.
IPv6-Adresse		In diesem Anzeigefeld wird die IPv6-Adresse angezeigt.
Default-Gateway	**Nicht gesetzt**	Wählen Sie im Auswahlfeld „Nicht gesetzt“, wenn Sie die IP-Adresse nicht eingeben wollen
	Gesetz	Wählen Sie im Auswahlfeld „Gesetzt“, wenn Sie die IP-Adresse eingeben wollen Geben Sie die IP-Adresse des ausgehenden Default-Gateways in Dezimalpunktschreibweise ein.

9.2.1.2 Jumbo-Frame

Hinweis

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

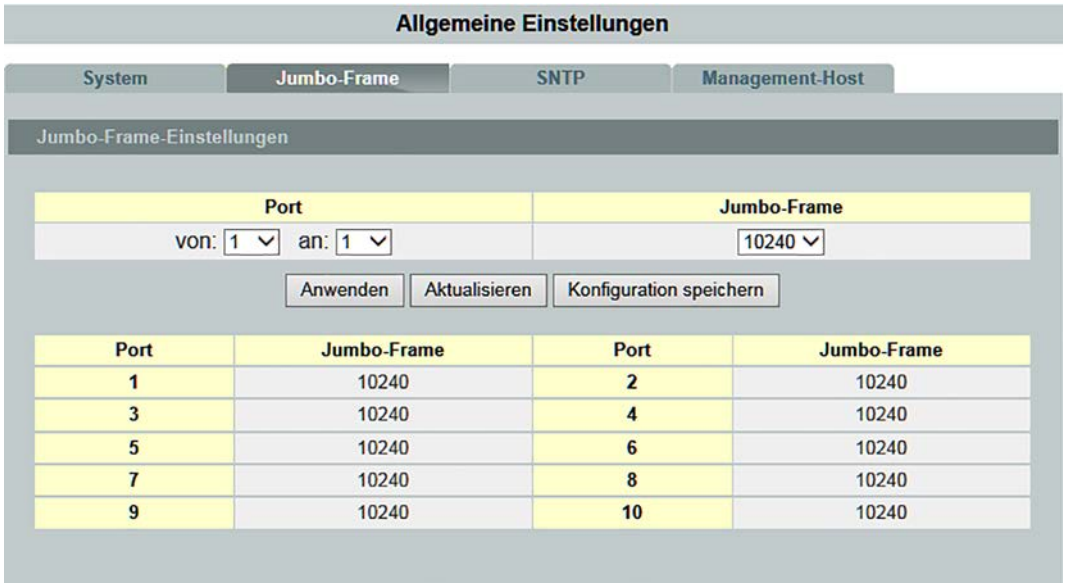


Abbildung 29: WBM-Seite „Allgemeine Einstellungen“ – Register „Jumbo-Frame“

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	In dieser Spalte werden die Port-Nummern angezeigt.
Jumbo-Frame		1522 1536 1552 9010 9216 10240	In dieser Spalte wird die maximale Byte-Anzahl für einen Jumbo-Frame angezeigt.

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“.

Abbildung 30: 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.	
		○	Wählen Sie diese Option, wenn Sie die IP-Adresse eines Zeitservers eingeben. Der Switch wird 60 Sekunden lang nach einem Zeitserver suchen.	
	0.0.0.0	◉	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“

Sommerzeiteinstellungen		
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-Zeitzonen 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-Zeitzonen 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“.

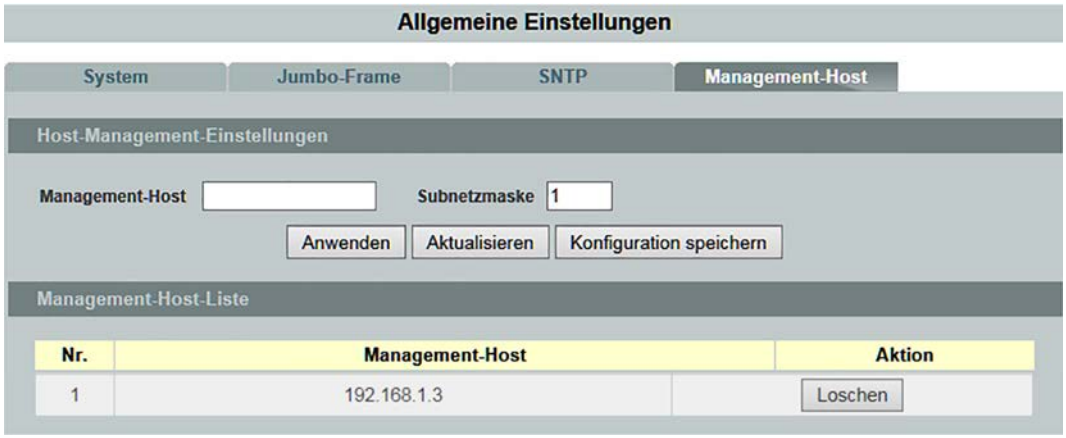


Abbildung 31: WBM-Seite „Allgemeine Einstellungen“ – Register „Management-Host“

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.
Subnetzmaske		Geben Sie im Eingabefeld die Nr. der Subnetzmaske-Adresse des Management-Host 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		In dieser Spalte werden die 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“.

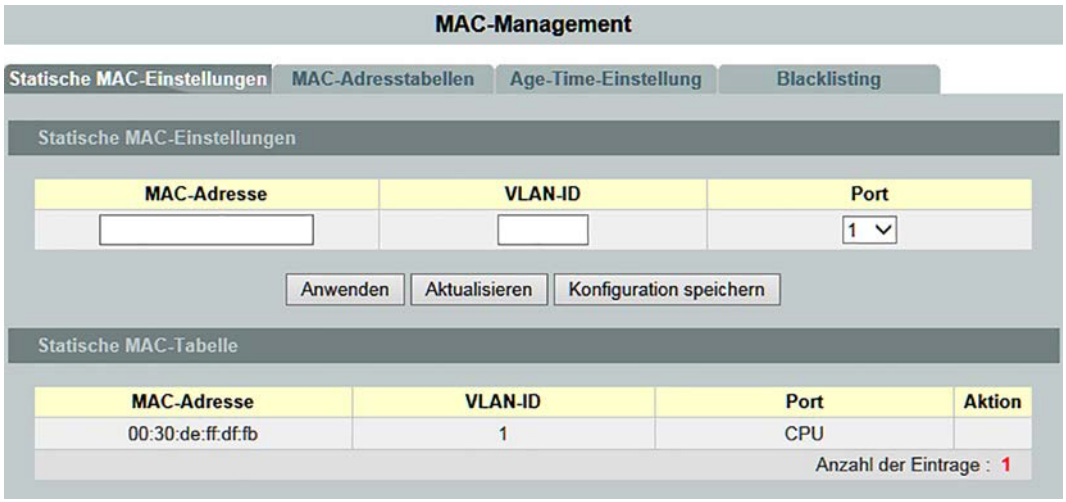


Abbildung 32: WBM-Seite „MAC-Management“ – Register „Statische MAC-Einstellungen“

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.

Tabelle 35: WBM-Seite „MAC-Management“ – Register „Statische MAC-Einstellungen“

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	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-Adresstabellen

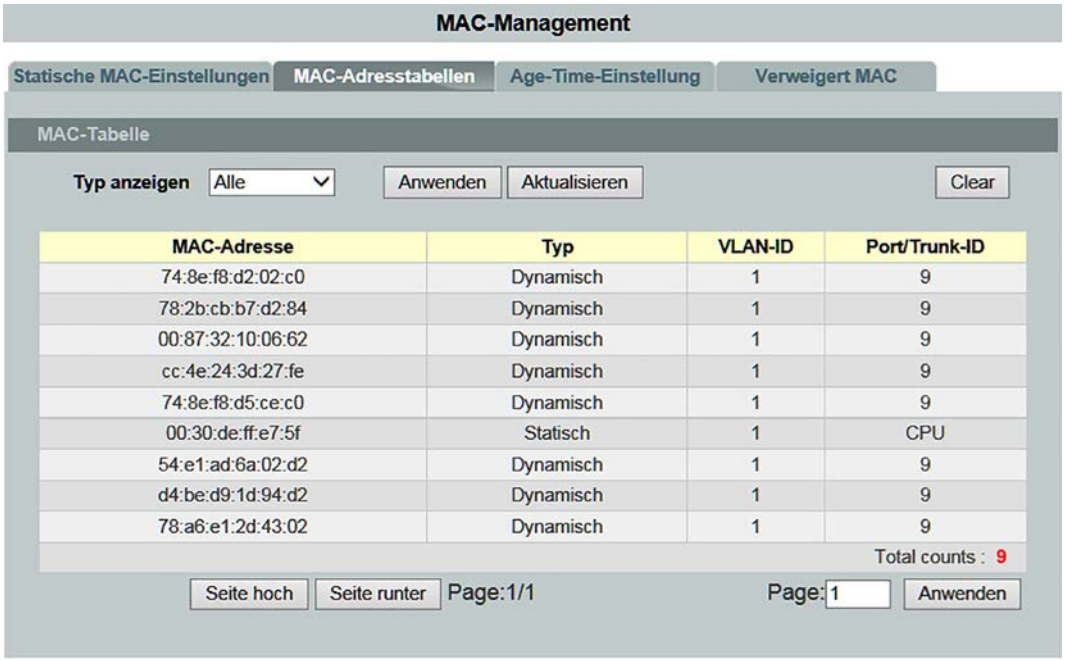


Abbildung 33: WBM-Seite „MAC-Management“ – Register „MAC-Adresstabellen“

Tabelle 36: WBM-Seite „MAC-Management“ – Register „MAC-Adresstabellen“

MAC-Adresstabellen		
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.
Totale Anzahl		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.

9.2.2.3 Age-Time-Einstellung

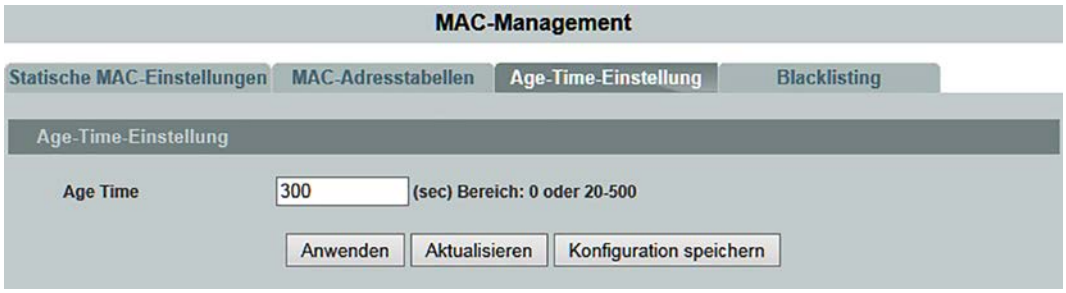


Abbildung 34: WBM-Seite „MAC-Management“ – Register „Age-Time-Einstellung“

Tabelle 37: „MAC-Management“ – Register „Age-Time-Einstellung“

Age-Time-Einstellung		
Parameter	**Standardwert**	**Beschreibung**
Age Time (sec) (Bereich:0 oder 20-500)	**300**	Geben Sie im Eingabefeld die Age Time (Löschzeit) ein. Gültiger Bereich: 0 oder 20 … 500 s.

9.2.2.4 Blacklisting

Hinweis

Weitere Information

Weitere Informationen zur „MAC-Blacklist (Blacklisting)“ finden Sie im Kapitel „Funktionsbeschreibung“.

Hinweis

Maximale Anzahl von MAC-Blacklist-Einträgen

Es können bis zu 20 Einträge konfiguriert werden.

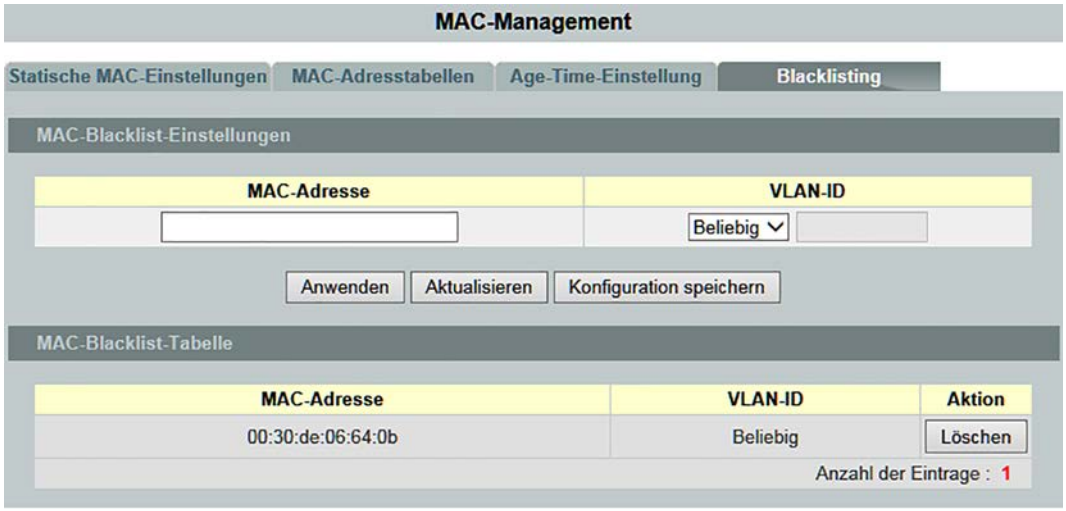


Abbildung 35: WBM-Seite „MAC-Management“ – Register „Blacklisting“

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

MAC-Blacklist-Einstellungen		
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-Mirroring

Hinweis

Weitere Information

Weitere Informationen zum „Port-Mirroring“ 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.

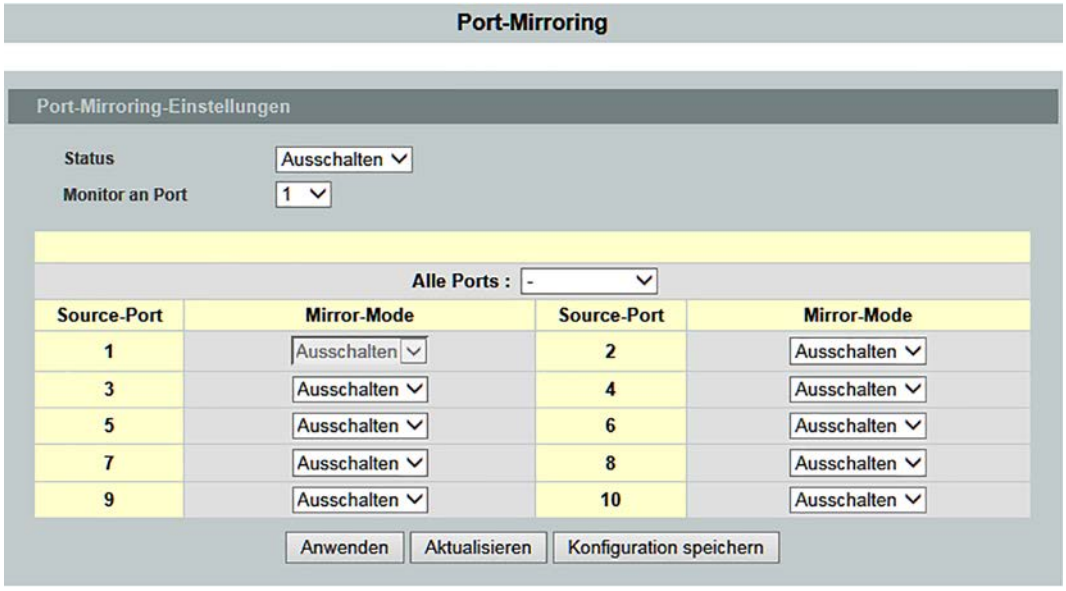


Abbildung 36: WBM-Seite „Port-Mirroring“

Tabelle 39: WBM-Seite „Port-Mirroring“

Port-Mirroring-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um das „Port-Mirroring“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Port-Mirroring“ zu aktivieren.
Monitor an Port	**1** … 10	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. Nehmen Sie hier nur Einstellungen vor, wenn diese für alle Ports gelten sollen. Beginnen Sie hier mit allgemeinen Einstellungen und nehmen Sie anschließend Einstellungen für einzelne Ports vor.
	Ausschalten	
	Ingress	
	Egress	
	Beide	
Source-Port	1 … 10	In dieser Spalte wird die Nummer der einzelnen Source-Ports angezeigt.
Mirror-Mode	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

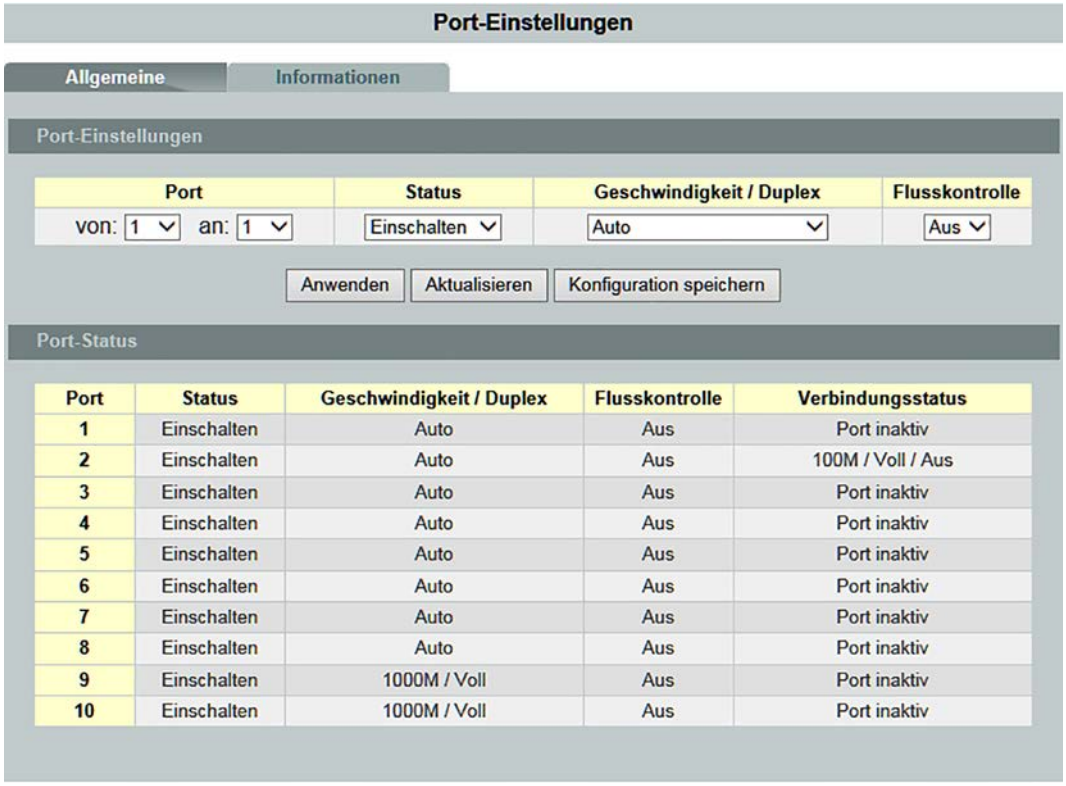


Abbildung 37: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine“

Tabelle 40: WBM-Seite „Port-Einstellungen“ – Register „Allgemeine“

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		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um den Port zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um den Port zu aktivieren.
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	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.
Verbindungsstatus			In dieser Spalte wird der Verbindungsstatus 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

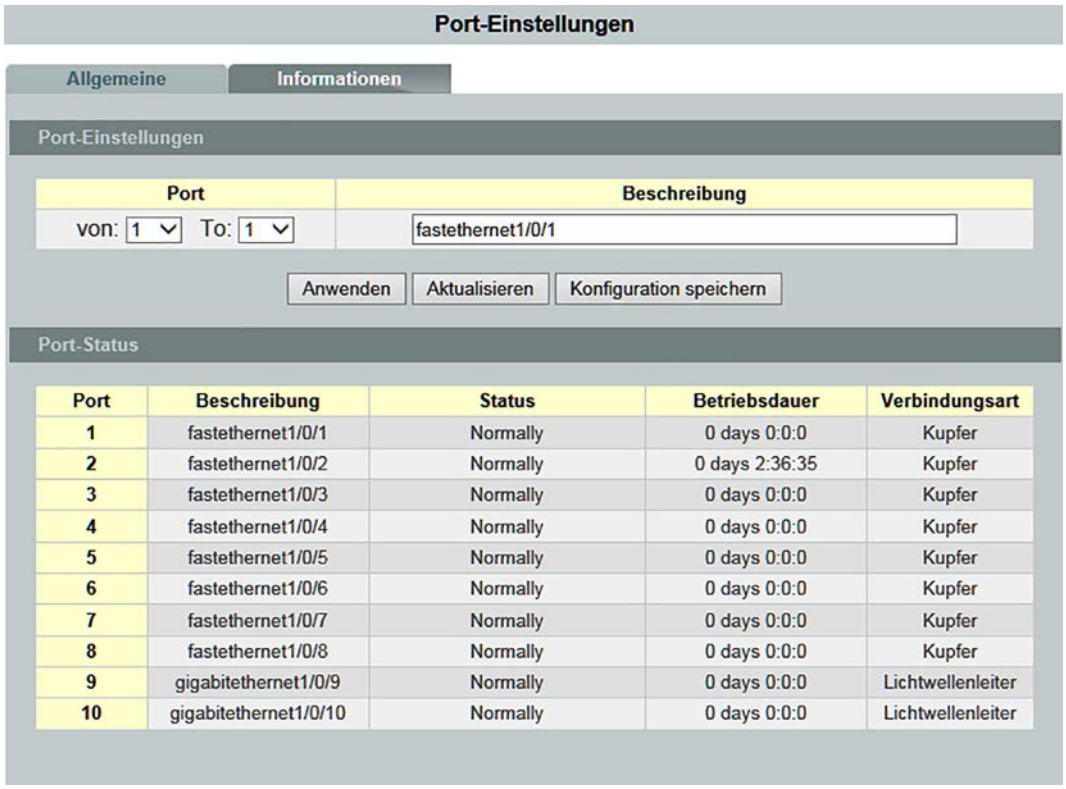


Abbildung 38: WBM-Seite „Port-Einstellungen“ – Register „Informationen“

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	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		 Kupfer Lichtwellenleiter	In dieser Spalte wird die Art der Verbindung angezeigt. Kupferdraht Lichtwellenleiter

9.3 Erweiterte Einstellungen

9.3.1 Bandbreiten-Einstellungen

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

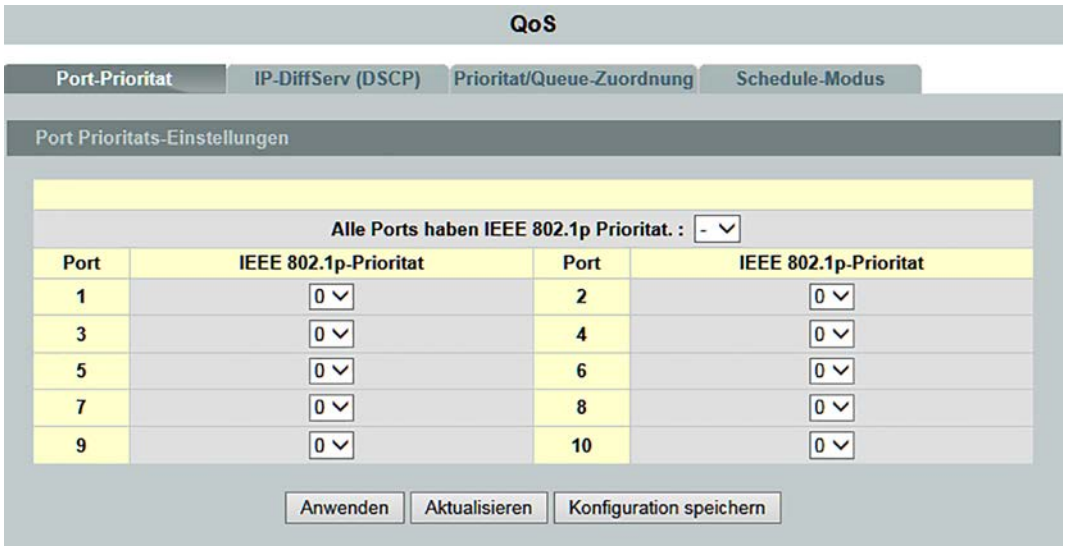


Abbildung 39: WBM-Seite „QoS“ – Register „Port-Priorität“

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	In dieser Spalte werden die Port-Nummern angezeigt.
IEEE 802.1p-Priorität	**0** … 7	Wählen Sie im Auswahlfeld eine Priorität für Pakete aus, die an diesem Port empfangen werden. Nur einem Paket ohne eine „IEEE 802.1p-Tag-Priority“ wird die hier angegebene Priorität zugewiesen.

9.3.1.1.2 IP-DiffServ (DSCP)

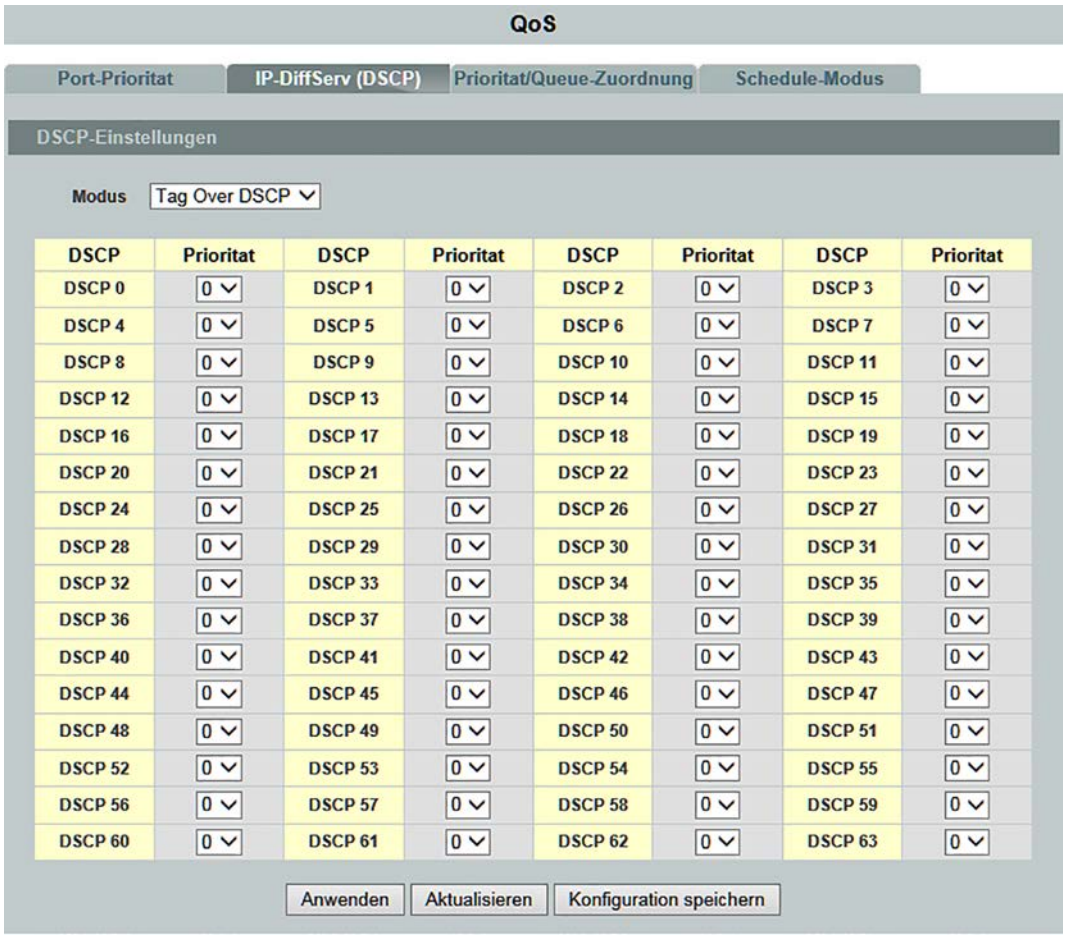


Abbildung 40: WBM-Seite „QoS“ – Register „IP-DiffServ (DSCP)“

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 niedere 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 41: 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

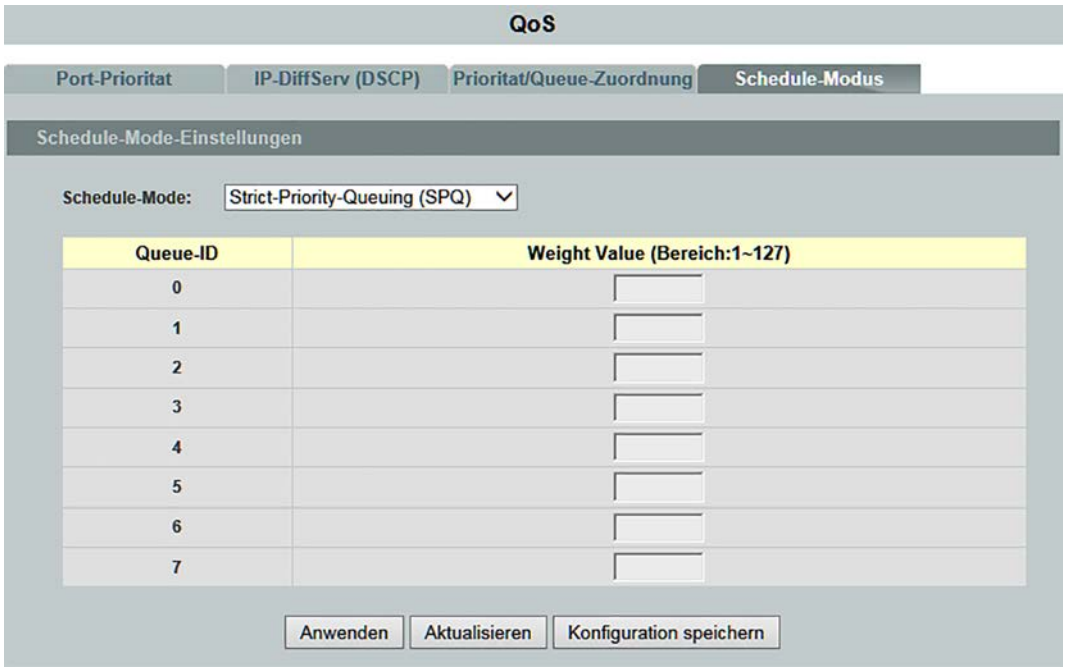


Abbildung 42: WBM-Seite „QoS“ – Register „Schedule-Modus“

Tabelle 46: WBM-Seite „QoS“ – Register „Schedule Modus“

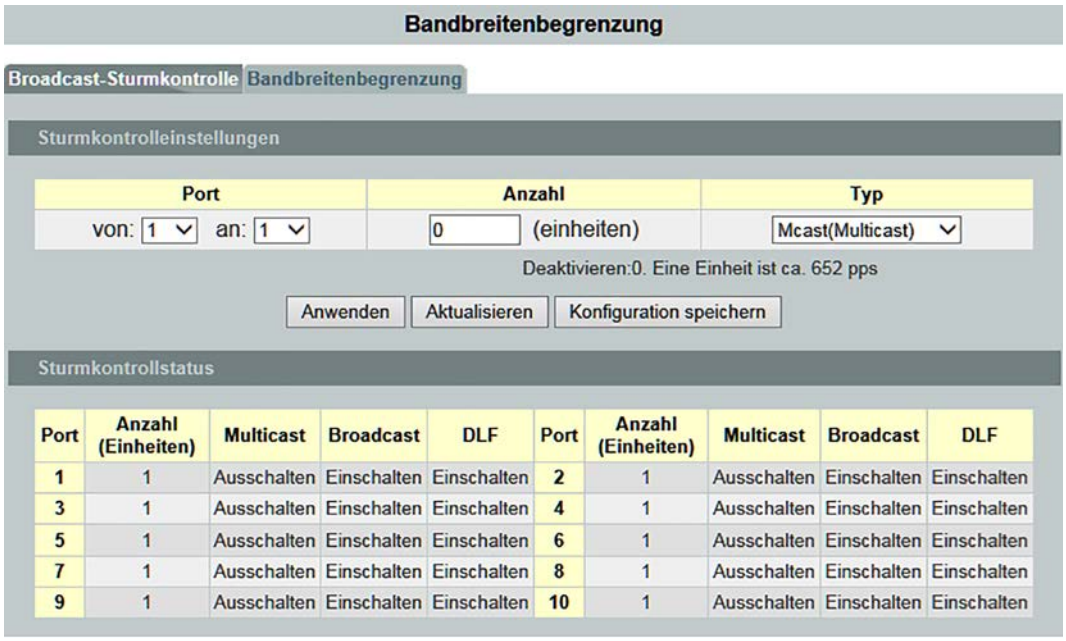
Schedule-Modus-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Schedule-Mode	**Strict Priority Queuing (SPQ)**	Wählen Sie im Auswahlfeld „Strict Priority Queuing (SPQ)“, wenn Sie die Hardware Priority Queues der Reihe nach abarbeiten wollen.
	Weighted Round Robin (WRR)	Wählen Sie im Auswahlfeld „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 Broadcast-Sturmkontrolle

Hinweis **Weitere Information**

Weitere Informationen zu „Broadcast-Sturmkontrolle“ finden Sie im Kapitel „Funktionsbeschreibung“.



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

Abbildung 43: WBM-Seite „Bandbreitenbegrenzung“ – Register „Broadcast-Sturmkontrolle“

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

Sturmkontrolleinstellungen			
Parameter		**Standardwert**	**Beschreibung**
Port	von:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Sturmkontrolleinstellungen“ zu konfigurieren.
	an:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Sturmkontrolleinstellungen“ 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 „Mcat+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	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“.

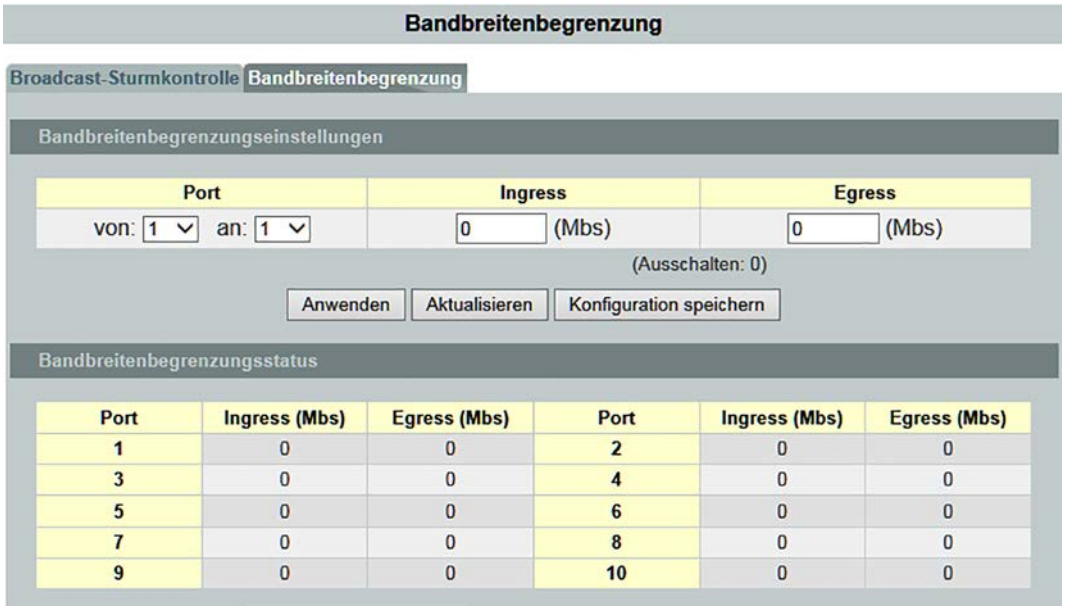


Abbildung 44: WBM-Seite „Bandbreitenbegrenzung“ – Register „Bandbreitenbegrenzung“

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

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

9.3.2 IGMP-Snooping

Hinweis **Weitere Information**

Weitere Informationen zu „IGMP-Snooping“ (**I**nternet **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

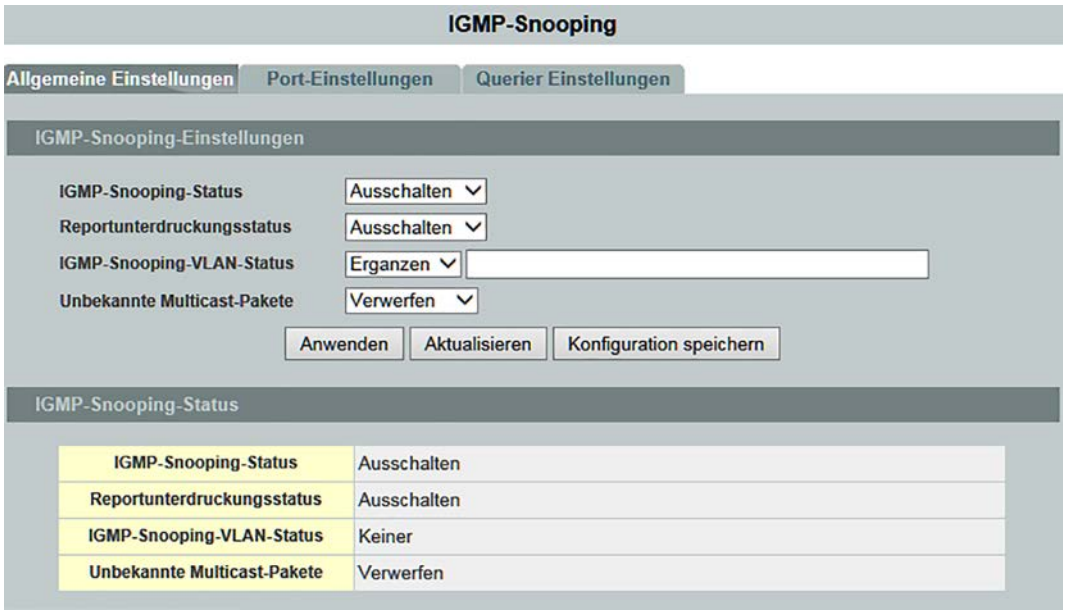
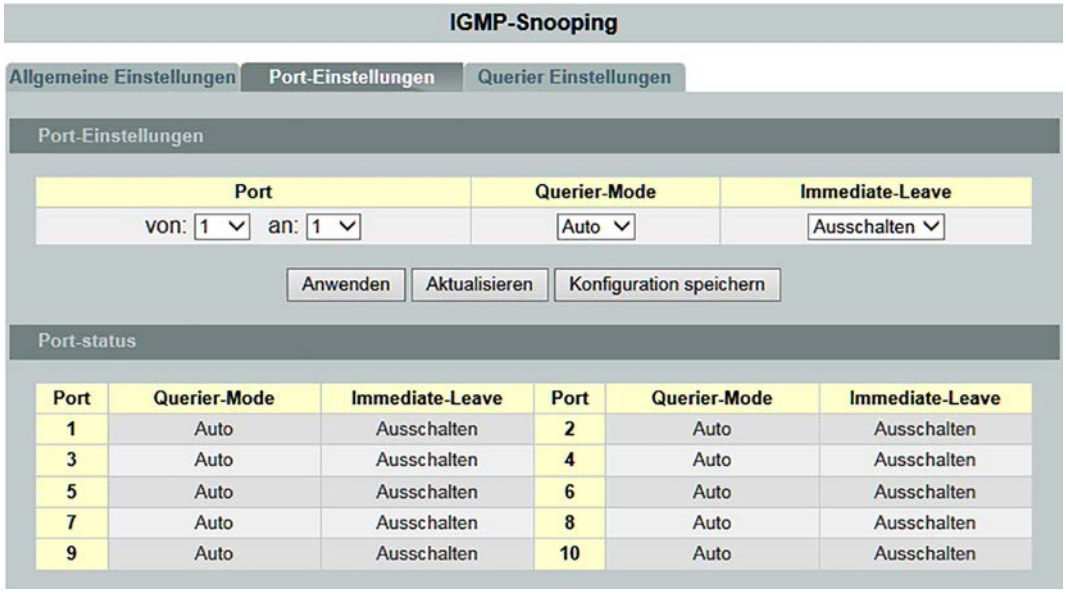


Abbildung 45: WBM-Seite „IGMP-Snooping“ – Register „Allgemeine Einstellungen“

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.
Reportunterdrückungs-status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um die „Reportunterdrückungsfunktion“ beim „IGMP-Snooping“ zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die „Reportunterdrückungsfunktion“ 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.
Reportunterdrückungs-status	Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob die „Reportunterdrückungsfunktion“-Funktion beim „IGMP-Snooping“ aktiviert oder deaktiviert ist.
IGMP-Snooping-VLAN-Status	Keiner 1 … 4094	In diesem Anzeigefeld werden die VLANs angezeigt, in denen der Switch „IGMP-Snooping“ ausführt. Es wird „Keiner“ angezeigt, wenn noch für keinen Port „IGMP-Snooping“ aktiviert wurde.
Unbekannte Multicast-Pakete	Verwerfen Weiterleiten	In diesem Anzeigefeld wird angezeigt, ob der Switch unbekannte Multicast-Pakete verwirft oder an alle Ports weiterleitet.

9.3.2.1.2 Port-Einstellungen



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

Abbildung 46: 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	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

Abbildung 47: 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

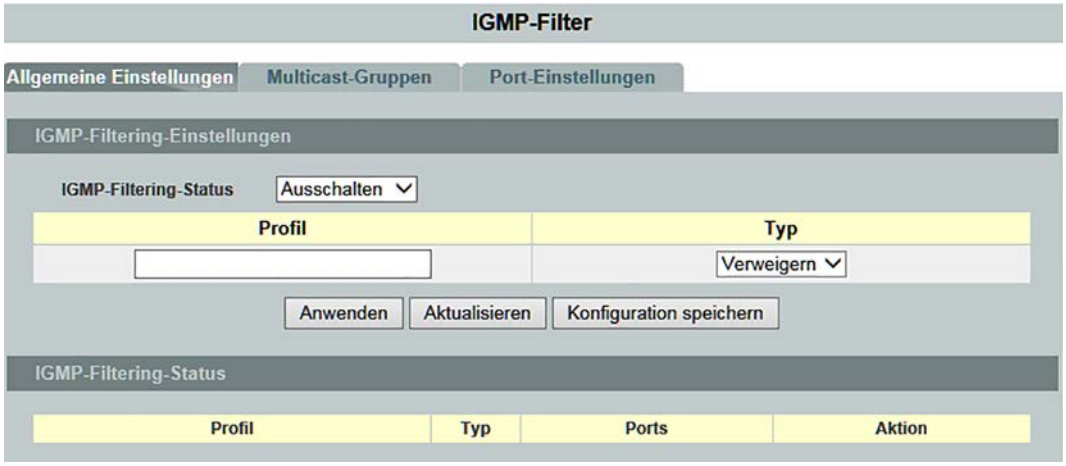


Abbildung 48: WBM-Seite „IGMP-Filter“ – Register „Allgemeine Einstellungen“

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

IGMP-Filtering-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
IGMP-Filtering-Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
Profil		Geben Sie im Eingabefeld den Namen für den IGMP-Filter ein.
Typ	**Verweigern**	Wählen Sie im Auswahlfeld „Verweigern“, um den Zugang zur Gruppe zu verweigern.
	Erlauben	Wählen Sie im Auswahlfeld „Erlauben“, um den Zugang zur Gruppe zu gewähren.
IGMP-Filtering-Status		
Parameter	**Standardwert**	**Beschreibung**
Profil		In dieser Spalte wird der Name des Profils angezeigt. Klicken Sie auf den Namen, um das Profil zu modifizieren.
Typ	Verweigern Erlauben	In dieser Spalte wird der Handlungstyp angezeigt.
Ports	1 … 10	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-Gruppen

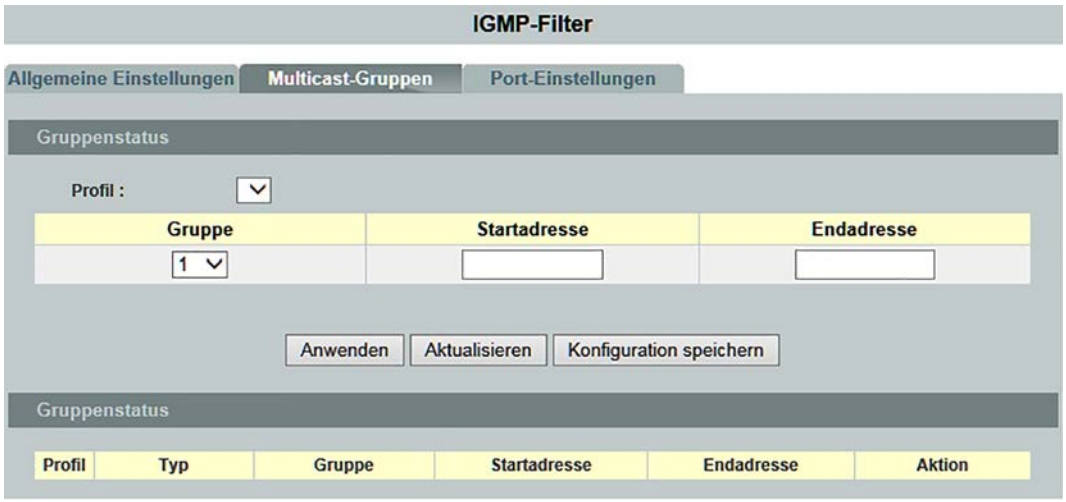


Abbildung 49: WBM-Seite „IGMP-Filter“ – Register „Multicast-Gruppen“

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

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

9.3.2.2.3 Port-Einstellungen

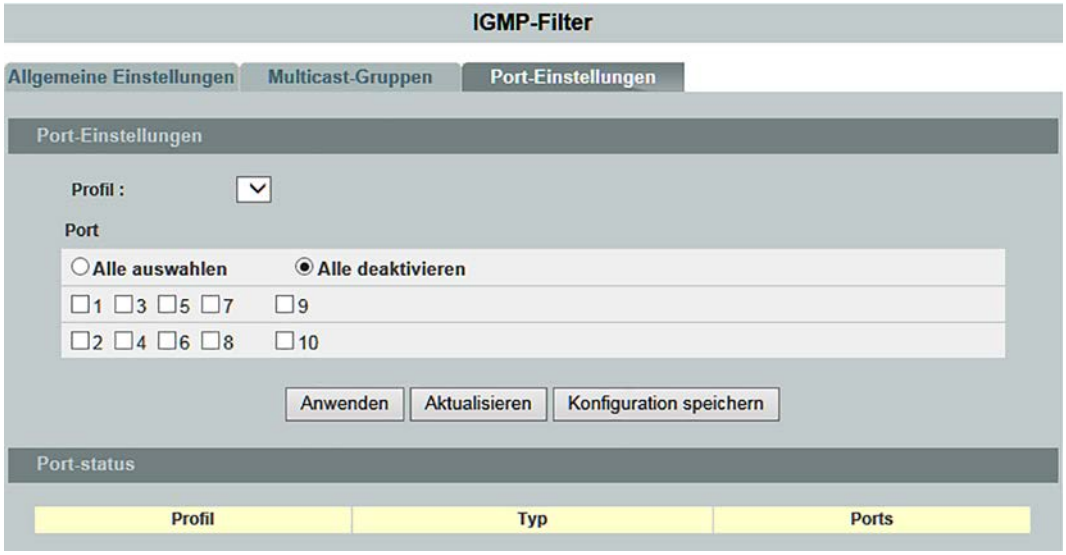


Abbildung 50: WBM-Seite „IGMP-Filter“ – Register „Port-Einstellungen“

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

Port-Einstellungen				
Parameter		**Standardwert**	**Beschreibung**	
Profil			Wählen Sie im Auswahlfeld das Profil aus, das Sie für eine Gruppe konfigurieren möchten.	
Port	Alle auswählen	○	○	Es ist kein Port ausgewählt.
			◉	Es sind alle Ports ausgewählt.
	Alle deaktivieren	○	○	Es ist kein Port deaktiviert.
			◉	Es sind alle Ports deaktiviert.
	☐ 1 … ☐ 10	☐	☐	Der Port ist nicht aktiviert..
			☑	Der Port ist aktiviert.
Port-Status				
Parameter		**Standardwert**	**Beschreibung**	
Profil			In dieser Spalte wird der Name des Profils angezeigt.	
Typ			In dieser Spalte wird der Handlungstyp angezeigt.	
Ports		1 … 10	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 „**M**ulticast-**V**LAN-**R**egistration“ (MVR) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.2.3.1 MVR-Einstellungen

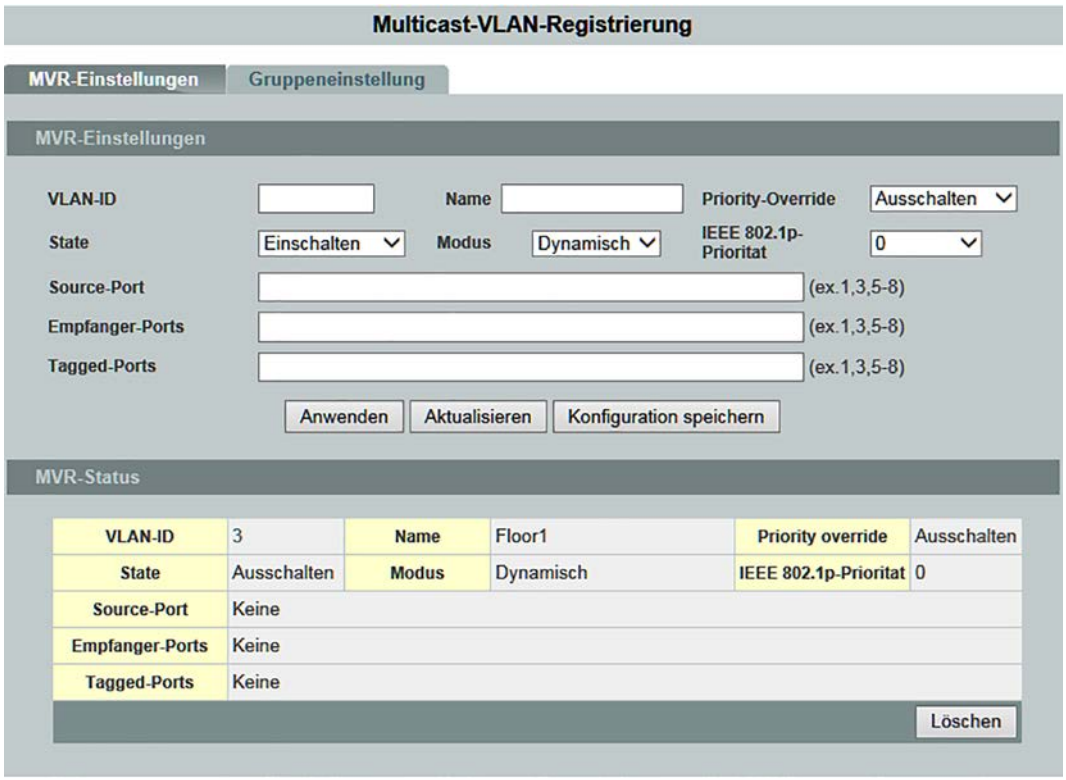


Abbildung 51: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „MVR-Einstellungen“

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.
State	**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.
Empfänger-Ports	1 … 8	Geben Sie im Eingabefeld den Empfänger-Port oder Empfänger-Port-Bereich für die MVR ein. Normalerweise sind die Source-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.
State	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.
Empfänger-Ports	1 … 8	In diesem Anzeigefeld wird der Empfänger-Port oder Empfänger-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 Gruppeneinstellung

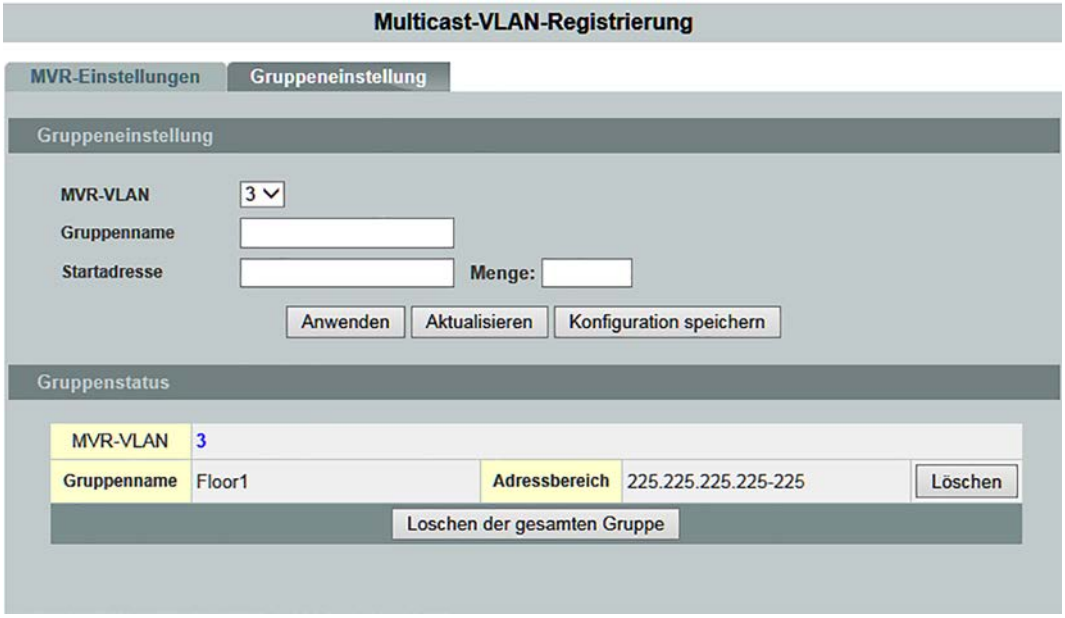


Abbildung 52: WBM-Seite „Multicast-VLAN-Registrierung“ – Register „Gruppeneinstellung“

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

Gruppeneinstellung		
Parameter	**Standardwert**	**Beschreibung**
MRV-VLAN	1 … 10	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	1 … 10	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.
Löschen der gesamten Gruppe		Klicken Sie auf **[Löschen der gesamten Gruppe]**, um die Einstellungen der gesamten Gruppe zu löschen.

9.3.2.4 Statische Multicast-Adressen

Hinweis

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

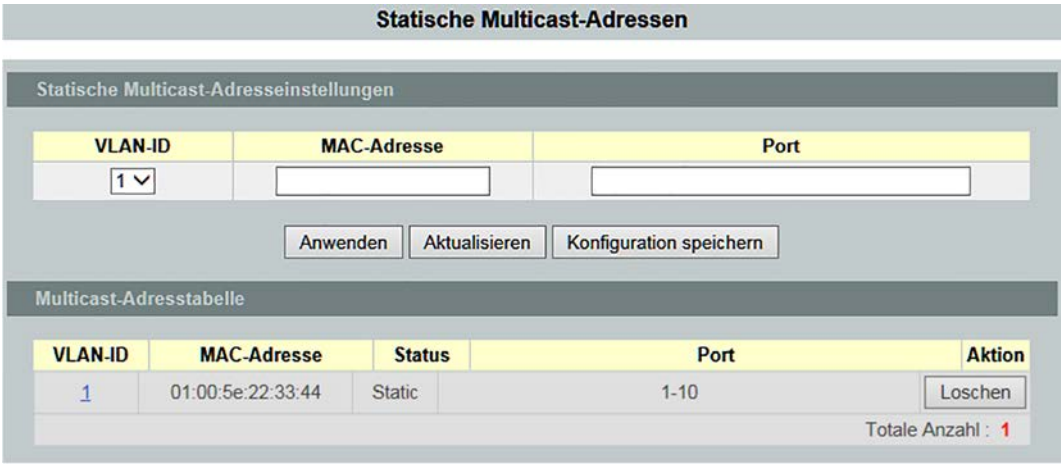


Abbildung 53: WBM-Seite „Statische Multicast-Adressen“

Tabelle 57: WBM-Seite „Statische Multicast-Adressen“

Statische Multicast-Adresseinstellungen		
Parameter	**Standardwert**	**Beschreibung**
VLAN-ID	**1**	Wählen Sie im Auswahlfeld die VLAN-ID aus, die Sie konfigurieren möchten.
MAC-Adresse		Geben Sie in Eingabefeld die Multicast-MAC-Adresse des jeweiligen Rings ein. Konfigurieren Sie eine Multicast-MAC, die keine „Age Time“ erhalten soll. Das gültige Format ist: 0x:0x:0x:0x:0x:0x.
Port		Geben Sie im Eingabefeld den Teilnehmer-Port für die Multicast-Adresse ein.
Multicast-Adresstabelle		
Parameter	**Standardwert**	**Beschreibung**
VLAN-ID	0 … 4094	In dieser Spalte werden die ausgewählten VLAN-ID angezeigt.
MAC-Adresse		In dieser Spalte werden die Multicast-Adressen angezeigt.
Status		In dieser Spalte wird der Status der Multicast-Adressen angezeigt.
Port	1 … 10	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-Statistiken

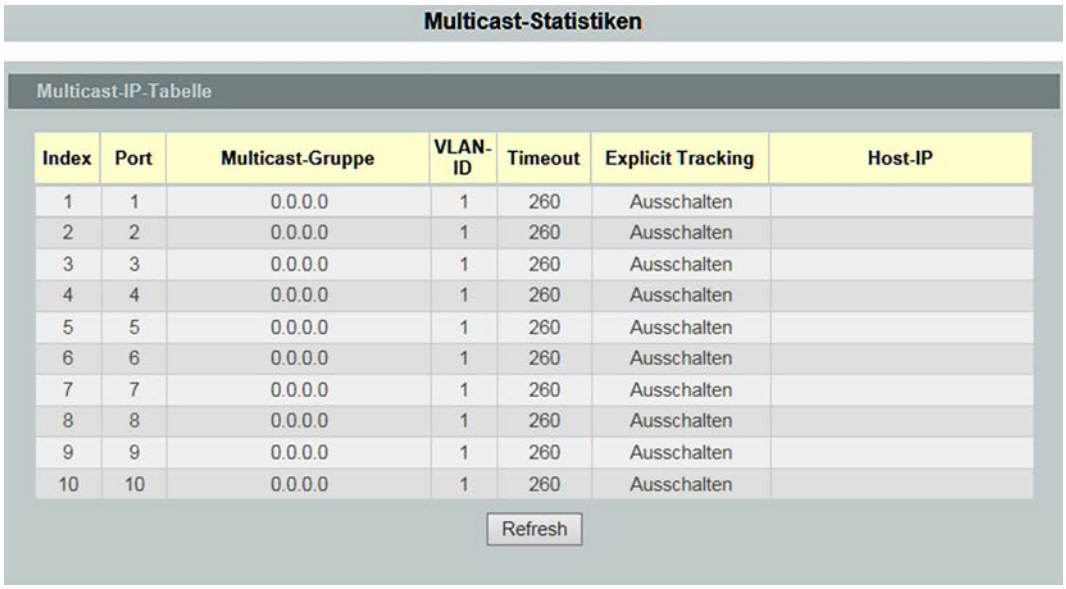


Abbildung 54: WBM-Seite „Multicast-Statistiken“

Tabelle 58: WBM-Seite „Multicast-Statistiken“

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

9.3.3 VLAN

Hinweis **Weitere Information**

Weitere Informationen zu „VLAN“ (**V**irtual **L**ocal **A**rea **N**etwork) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.3.1 Port-Isolation

Hinweis **Weitere Information**

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

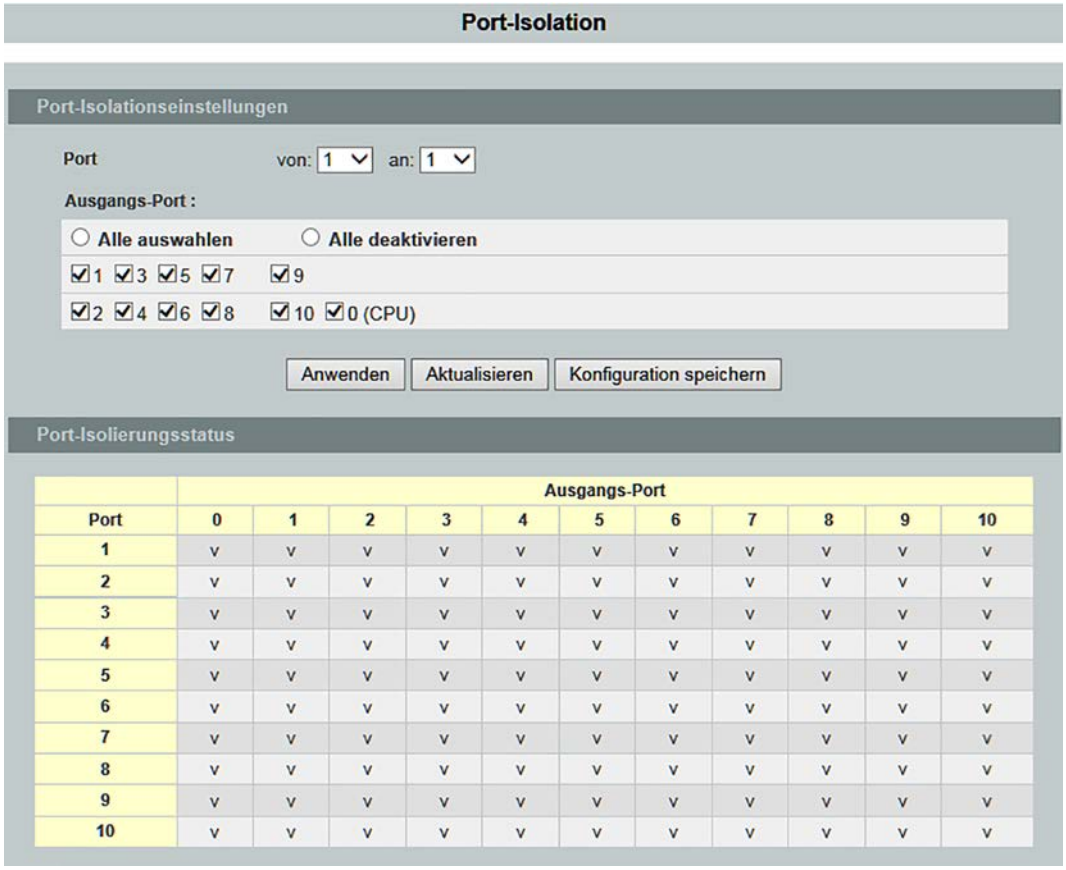


Abbildung 55: WBM-Seite „Port-Isolation“

Tabelle 59: WBM-Seite „Port-Isolation“

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

9.3.3.2 VLAN

9.3.3.2.1 VLAN-Einstellungen

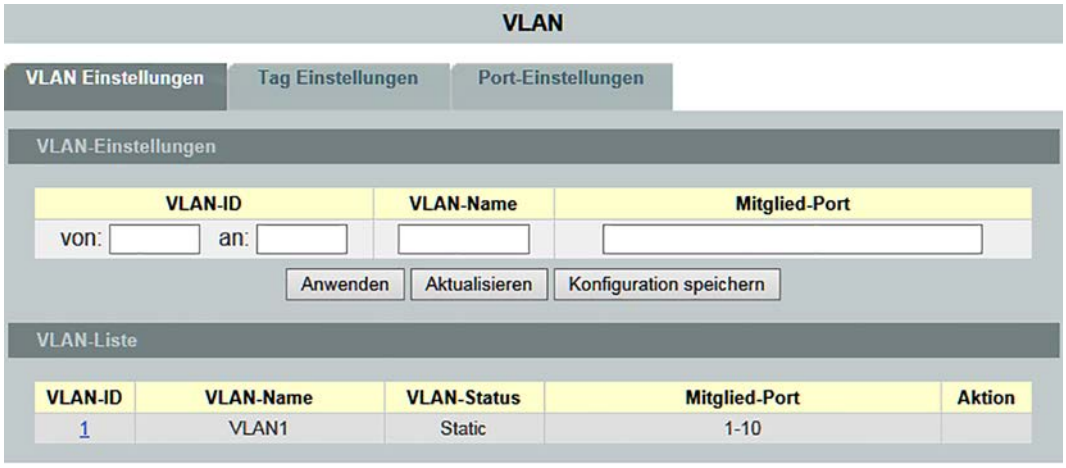


Abbildung 56: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“

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.
Mitglied-Port			Geben Sie im Eingabefeld die Port-Nummern ein, die der Switch dem VLAN als Teilnehmer zuordnen soll. Sie können mehrere einzelne Port-Nummern bzw. -Bereiche angeben, indem Sie Einzel-Ports durch Komma (,) trennen bzw. bei Port-Bereichen einen Bindestrich (-) verwenden.

Tabelle 60: WBM-Seite „VLAN“ – Register „VLAN-Einstellungen“

VLAN-Liste		
Parameter	**Standardwert**	**Beschreibung**
VLAN-ID	1 … 4094	In dieser Spalte wird die Indexnummer des VLAN-Eintrags angezeigt. Klicken Sie auf die Nummer, um den VLAN-Eintrag zu modifizieren.
VLAN Name		In dieser Spalte wird der Name des VLANs angezeigt.
VLAN Status	Static Dynamic 802.1Q-VLAN	In dieser Spalte wird der Status des VLANs angezeigt.
Mitglied Port	1-10	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

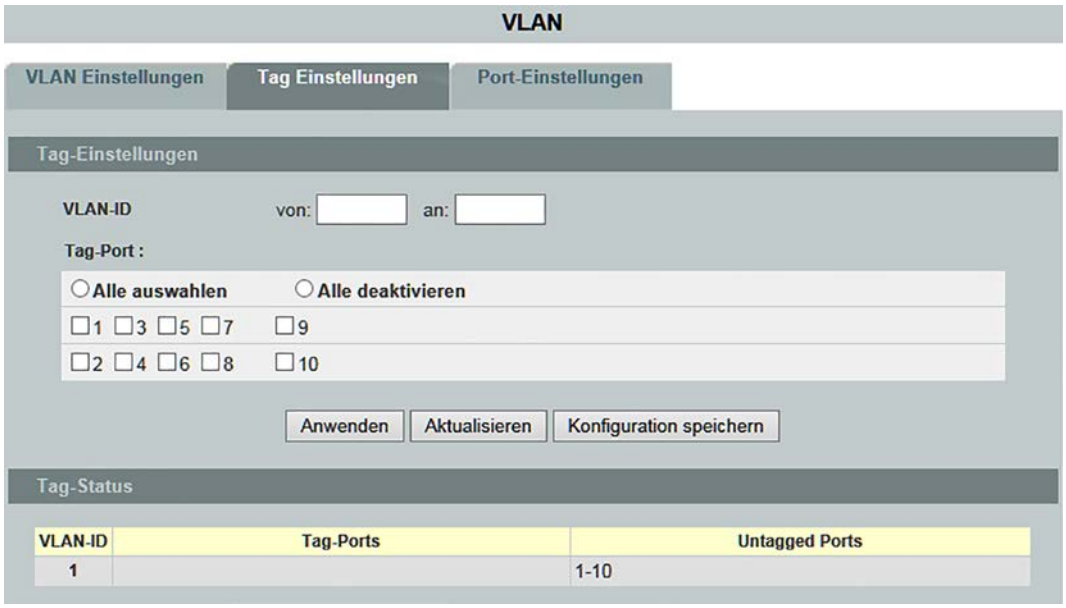


Abbildung 57: WBM-Seite „VLAN“ – Register „Tag-Einstellungen“

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	☐	☐	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

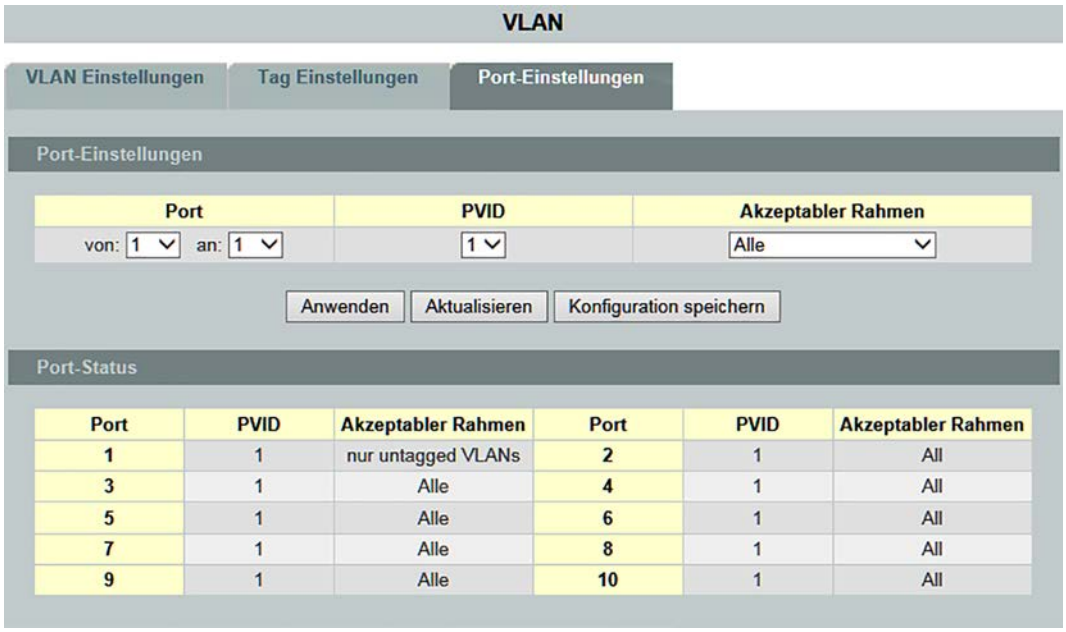


Abbildung 58: WBM-Seite „VLAN“ – Register „Port-Einstellungen“

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

9.3.3.3 GARP-VLAN-Registration-Protocol

Hinweis

Weitere Information

Weitere Informationen zu „GARP/GVRP“ (**G**eneric **A**ttribute **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

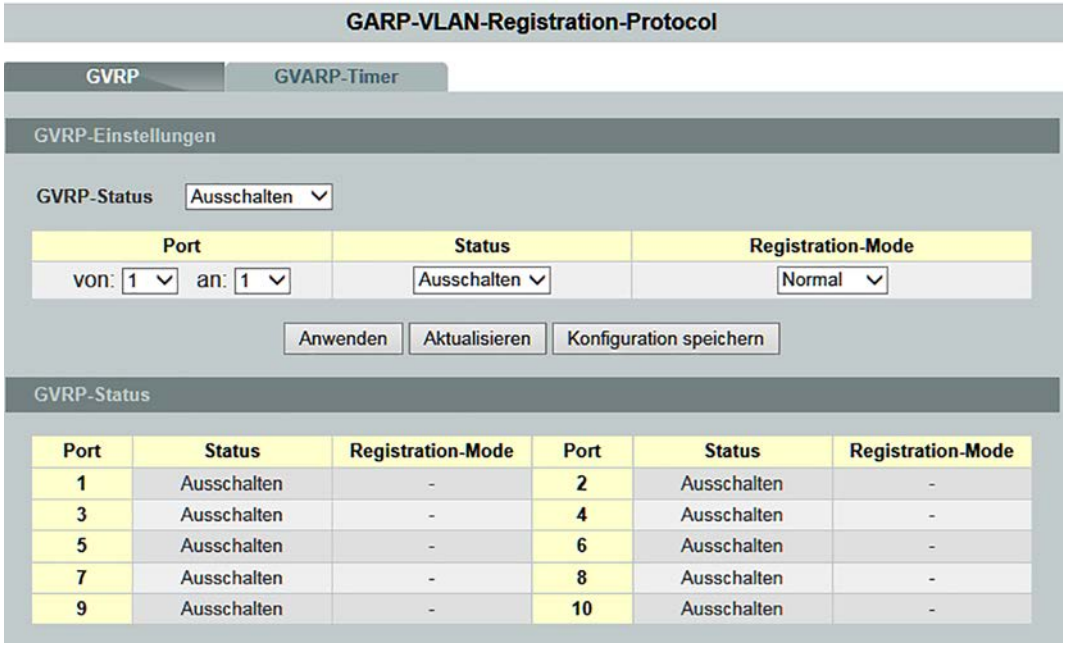


Abbildung 59: WBM-Seite „GARP-VLAN-Registration-Protocol“ – Register „GVRP“

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**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, bei dem Sie die GVRP-Einstellungen konfigurieren möchten.
	an:	**1**	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	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 >= join x 3).
Der Wert für „leave all“ muss größer sein als der Wert für „leave“ (leave all > leave).

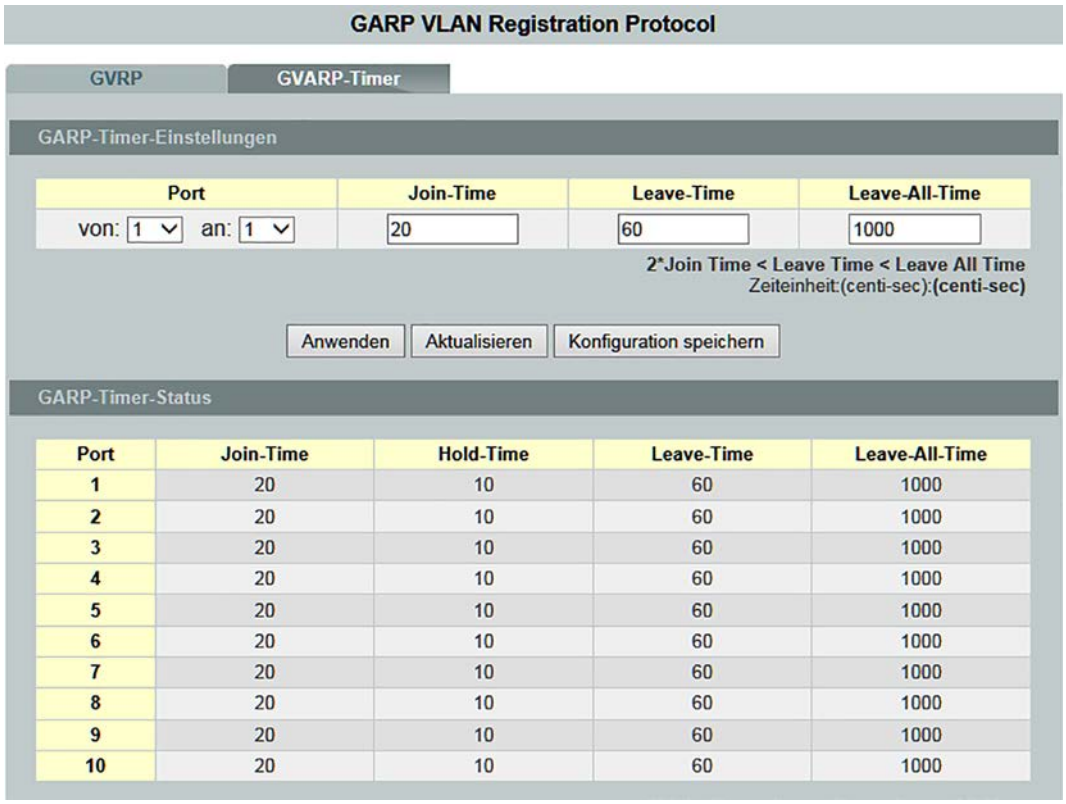


Abbildung 60: WBM-Seite „GARP-VLAN-Registration-Protocol“ – Register „GARP-Timer“

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 eint, 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	In dieser Spalte werden die Port-Nummern angezeigt.
Join-Time			In dieser Spalte wird die Join-Time angezeigt.
Hold-Time		**10**	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.

9.3.3.4 IP-Subnet-VLAN

Hinweis

Weitere Information
Weitere Informationen zu „IP-Subnet-VLAN“ finden Sie im Kapitel „Funktionsbeschreibung“.

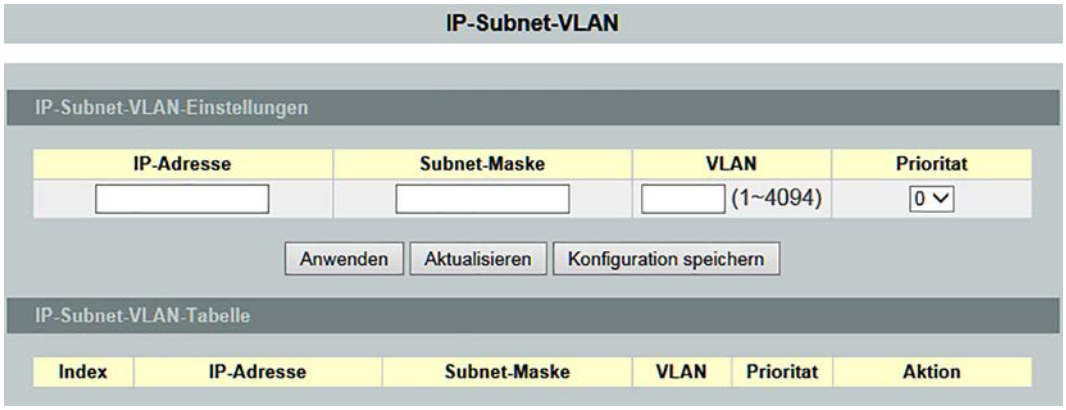


Abbildung 61: WBM-Seite „IP-Subnet-VLAN“

Tabelle 65: WBM-Seite „IP-Subnet-VLAN“

IP-Subnet-VLAN-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
IP-Adresse		Geben Sie im Eingabefeld die IP-Adresse des IP-Subnet-VLAN ein.
Subnet-Maske		Geben Sie im Eingabefeld die Subnet-Maske des Switches in Dezimalpunktschreibweise ein.
VLAN (1~4094)		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
IP-Subnet-VLAN-Tabelle		
Parameter	**Standardwert**	**Beschreibung**
Index	1 … 10	In dieser Spalte wird die Anzahl der Einträge angezeigt.
IP-Adresse		In dieser Spalte wird die IP-Adresse des IP-Subnet-VLAN angezeigt.
Subnet Maske		In dieser Spalte wird die Subnet-Maske des IP-Subnet-VLAN 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 IP-Subnet-VLAN-Adressen zu löschen.

9.3.3.5 MAC-VLAN

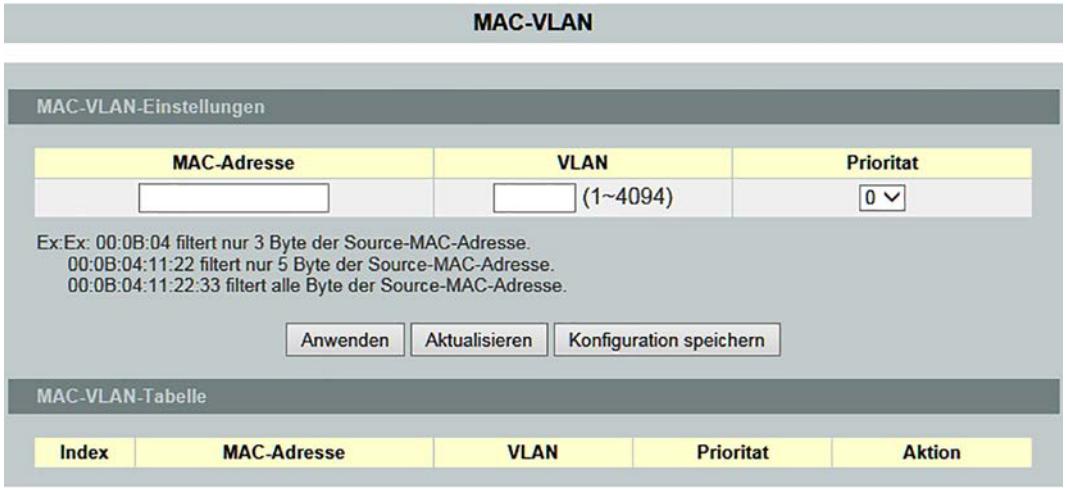


Abbildung 62: WBM-Seite „MAC-VLAN“

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

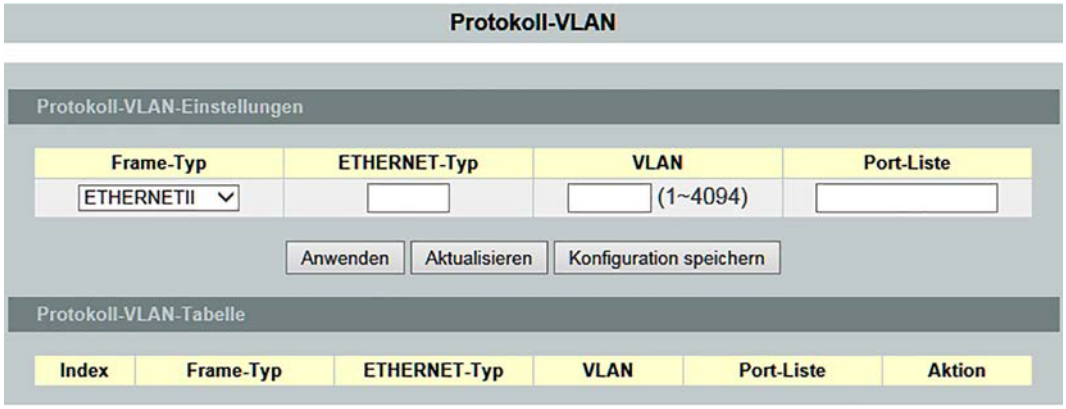


Abbildung 63: WBM-Seite „Protokoll-VLAN“

Tabelle 67: WBM-Seite „Protokoll-VLAN“

Protokoll-VLAN-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Frame-Typ	**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-Typ		Geben Sie im Eingabefeld den ETHERNET-Typ ein. (z. B. 0800)
VLAN (1~4094)	1 … 4094	Geben Sie im Eingabefeld die VLAN-ID ein. Gültiger Bereich: 1 … 4094
Port-Liste	1 … 10	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-Typ		In dieser Spalte wird der Frame-Typ angezeigt.
ETHERNET-Typ		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

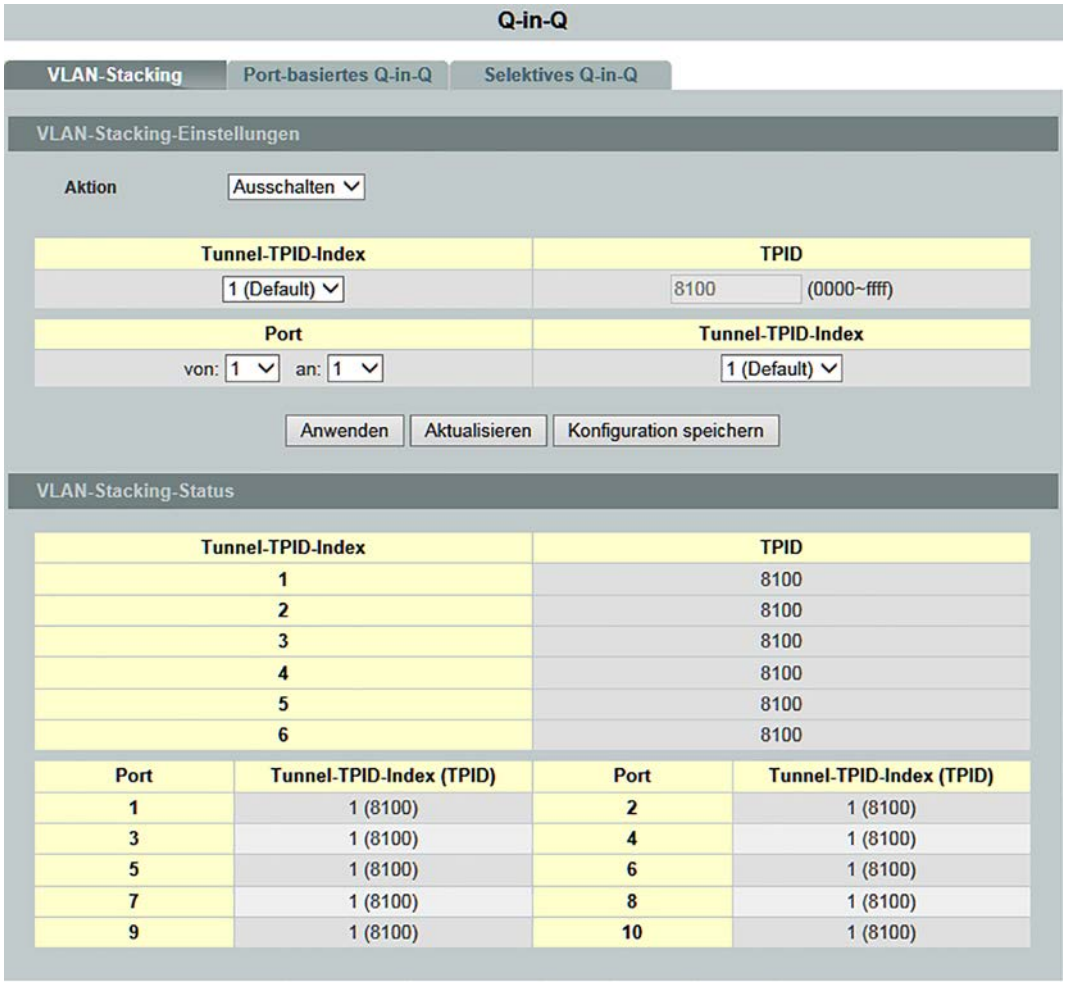


Abbildung 64: WBM-Seite „Q-in-Q“ – Register „VLAN-Stacking“

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-basiert	Wählen Sie im Auswahlfeld „Port-basiert“, 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	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-basiertes Q-in-Q

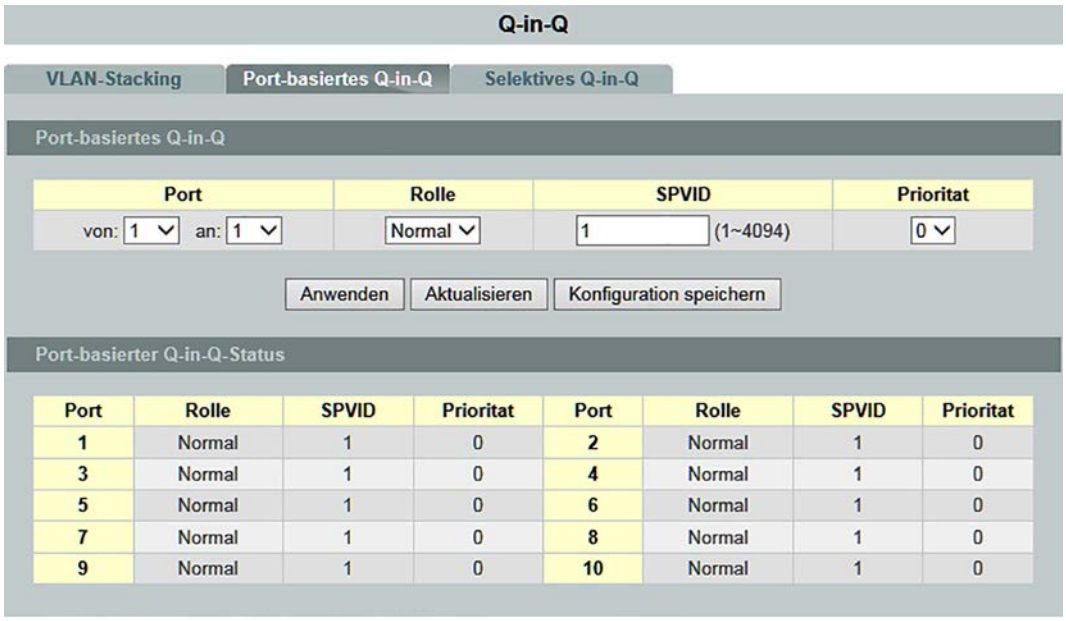


Abbildung 65: WBM-Seite „Q-in-Q“ – Register „Port-basiertes Q-in-Q“

Tabelle 69: WBM-Seite „Q-in-Q“ – Register „Port-basiertes 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.
Rolle		**Normal**	Wählen Sie im Auswahlfeld „Normal“, um diese Rolle für den spezifischen Port auszuwählen.
		Access	Wählen Sie im Auswahlfeld „Access“, um diese Rolle für den spezifischen Port auszuwählen.
		Tunnel	Wählen Sie im Auswahlfeld „Tunnel“, um diese Rolle 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	In dieser Spalte wird die Port-Nummer angezeigt.
Rolle			In dieser Spalte wird die Rolle des spezifischen Ports angezeigt.
SPVID		1 … 10	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

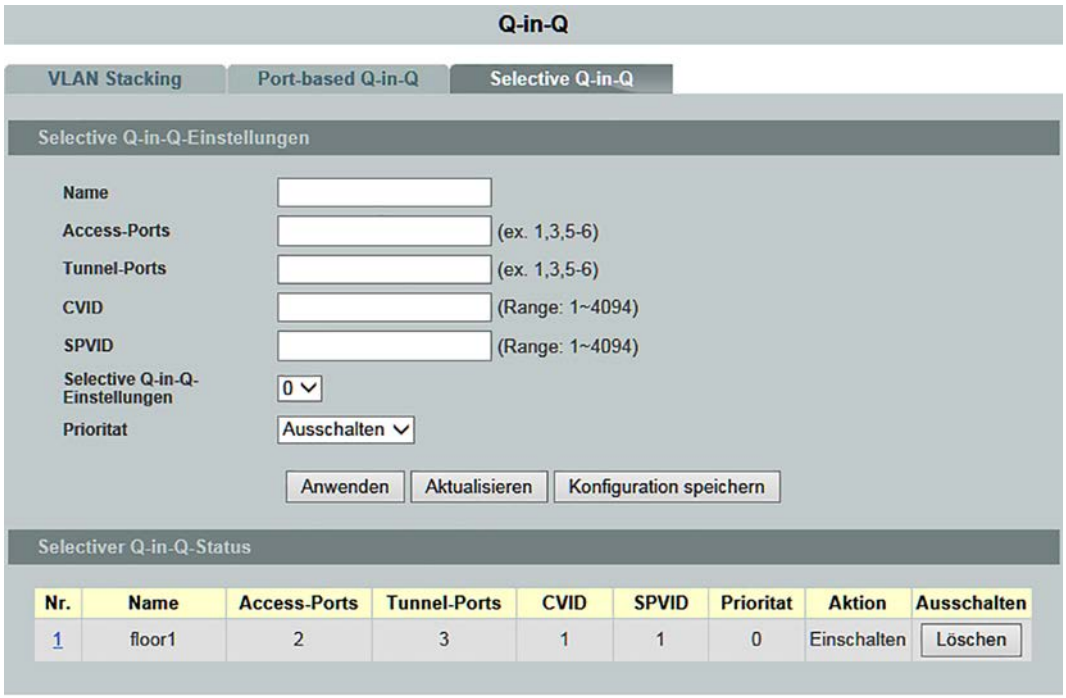


Abbildung 66: WBM-Seite „Q-in-Q“ – Register „Selektive Q-in-Q“

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 (Range: 1~4094)		Geben Sie im Eingabefeld ein Kunden-VLAN „CVID“ ein. Gültiger Bereich: 1 … 4094
SPVID (Range: 1~4094)		Geben Sie im Eingabefeld ein Dienstanbieter-VLAN „SPVID“ ein. Gültiger Bereich: 1 … 4094
Selektive Q-in-Q-Einstellungen	**0** … 7	Wählen Sie im Auswahlfeld die jeweilige Prioritätsebene aus. 0 = niedrigste Priorität 7 = höchste Priorität
Priorität	**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-Profils 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 **Relay**) finden Sie im Kapitel „Funktionsbeschreibung“.

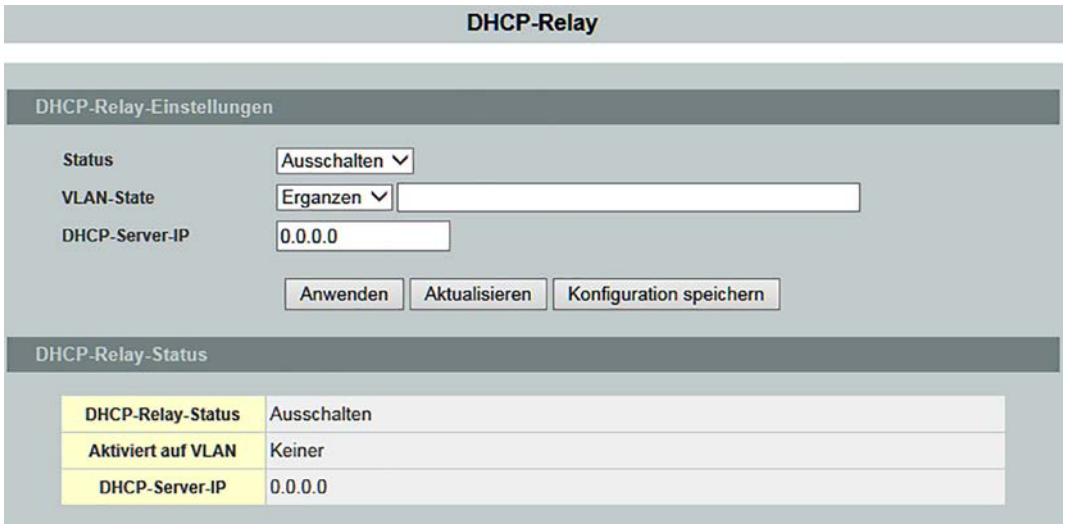


Abbildung 67: WBM-Seite „DHCP-Relay“

Tabelle 71: WBM-Seite „DHCP-Relay“

DHCP-Relay-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „DHCP Relay“ zu aktivieren.
VLAN-State	**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-Optionen

9.3.5.1 Option 82

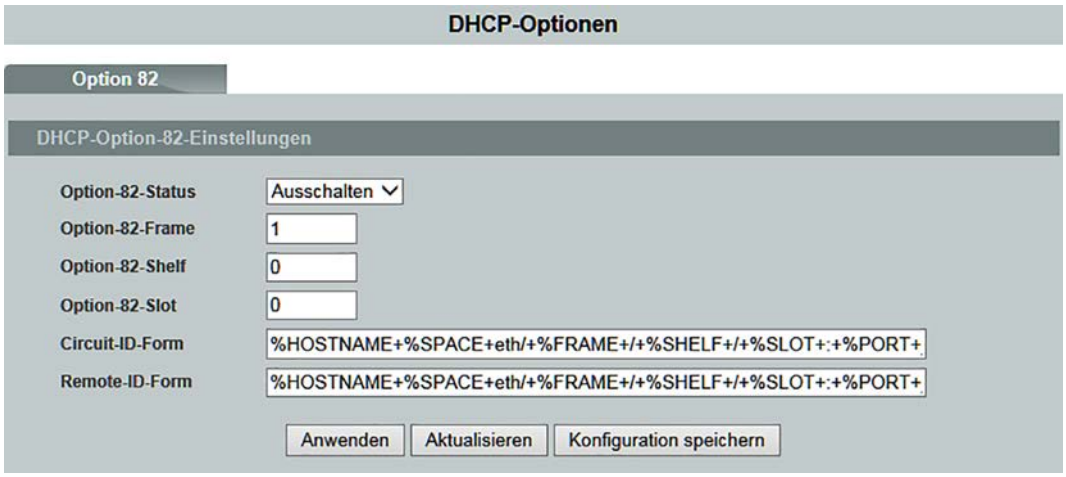


Abbildung 68: WBM-Seite „DHCP-Optionen“ – Register „Option 82“

Tabelle 72: WBM-Seite „DHCP-Optionen“ – Register „Option 82“

DHCP-Option-82-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Option-82-Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „DHCP Relay 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-Form	**%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN**	In diesem Eingabefeld haben Sie die Möglichkeit, den angefügten String anzupassen.
Remote-ID-Form	**%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN**	In diesem Eingabefeld haben Sie die Möglichkeit, den angefügten String anzupassen.

9.3.6 Dual-Homing

Hinweis **Weitere Information**

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

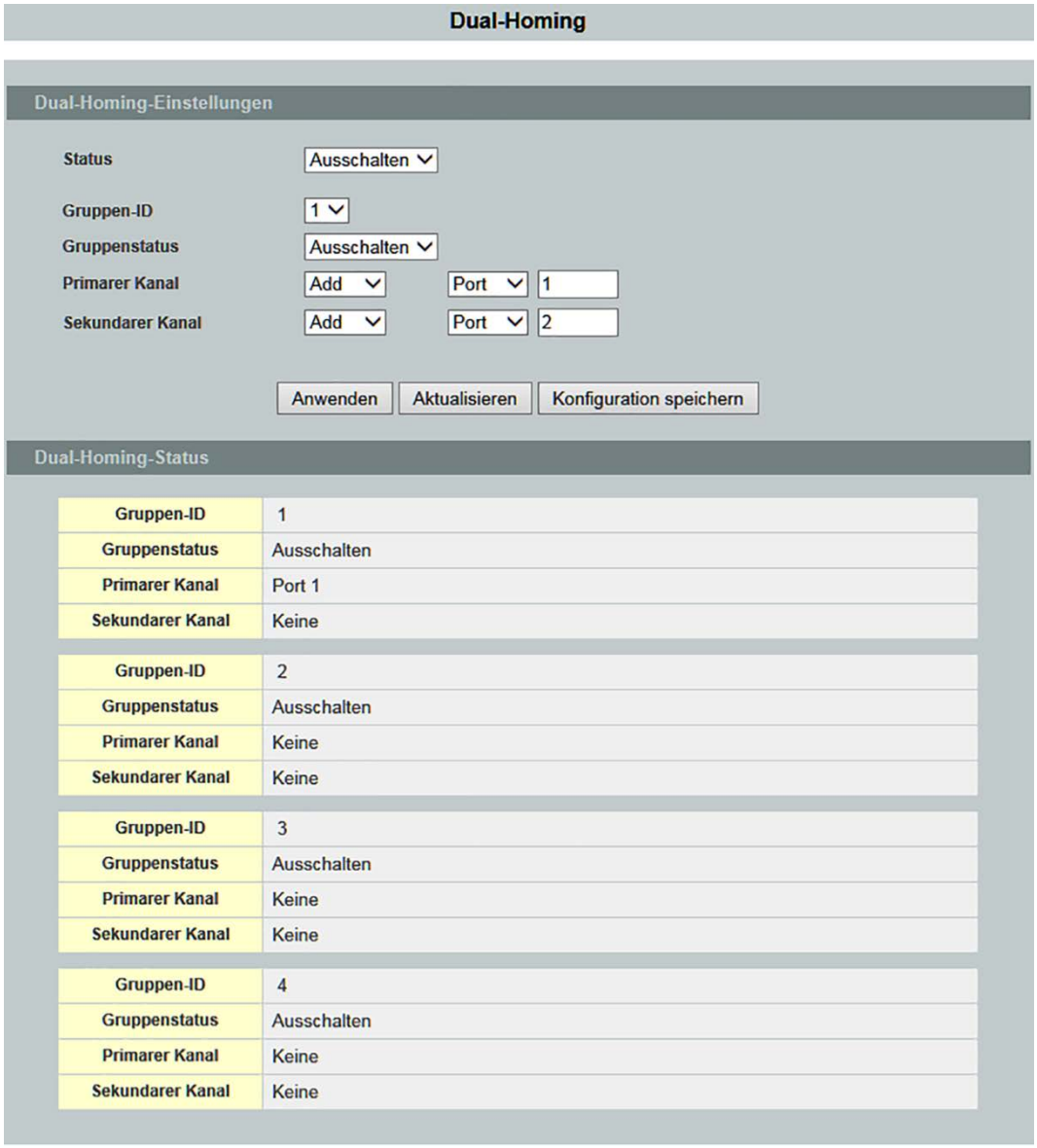


Abbildung 69: WBM-Seite „Dual-Homing“

Tabelle 73: WBM-Seite „Dual-Homing“

Dual-Homing-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um „Dual-Homing“ zu aktivieren.
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 „Dual-Homing“ zu aktivieren.
Primärer Kanal	**Add**	Wählen Sie im Auswahlfeld „Add“, 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	**Add**	Wählen Sie im Auswahlfeld „Add“, 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	In diesem Anzeigefeld wird der ausgewählte primäre Kanal angezeigt.
Sekundärer Kanal	Keine Port 1 … 10	In diesem Anzeigefeld wird der ausgewählte sekundäre Kanal angezeigt.

9.3.7 Dual-Ring

Hinweis

Weitere Information

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

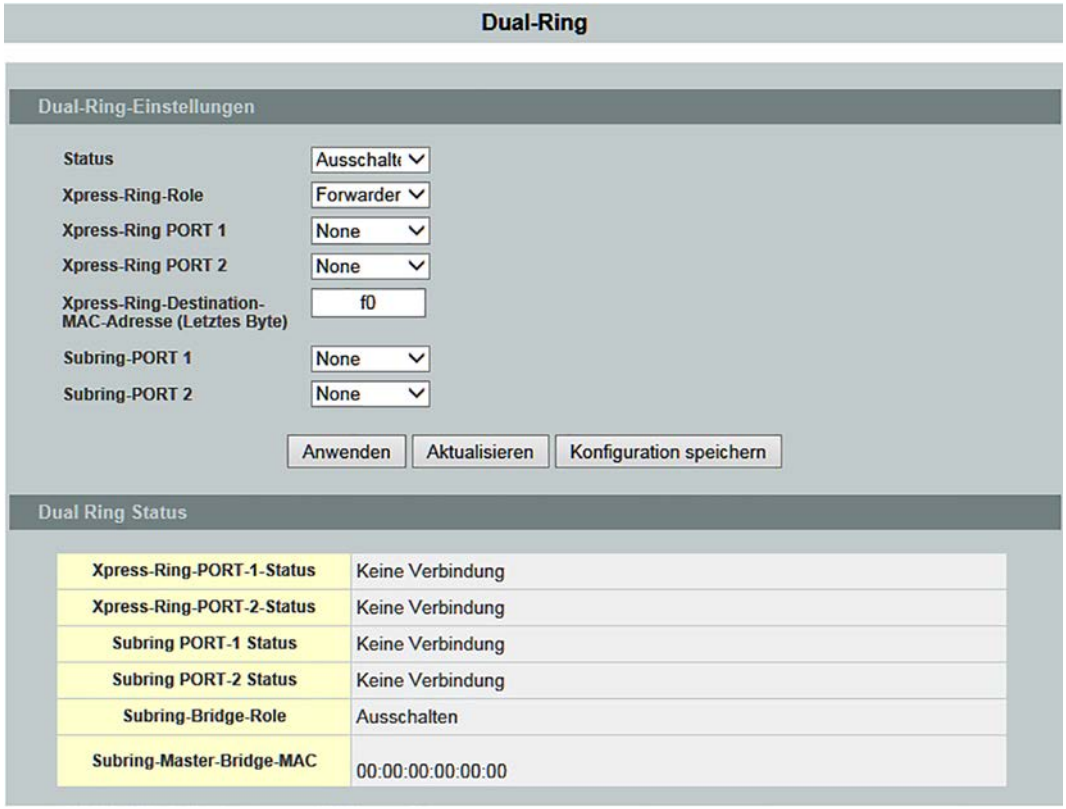


Abbildung 70: WBM-Seite „Dual-Ring“

Tabelle 74: WBM-Seite „Dual-Ring“

Dual-Ring-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion 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	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen Port auswählen wollen.
	1 … 10	Wählen Sie im Auswahlfeld den Port 1 im Xpress-Ring aus.
Xpress-Ring PORT 2	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen Port auswählen wollen.
	1 … 10	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	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen Port auswählen wollen.
	1 … 10	Wählen Sie im Auswahlfeld den Port 1 im Jetring aus.
Subring-PORT 2	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen Port auswählen wollen.
	1 … 10	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.

9.3.8 ERPS

Hinweis **Weitere Information**

Weitere Informationen zu „ERPS“ (**E**THERNET **R**ing **P**rotection **S**witching) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.8.1 Ringeinstellungen

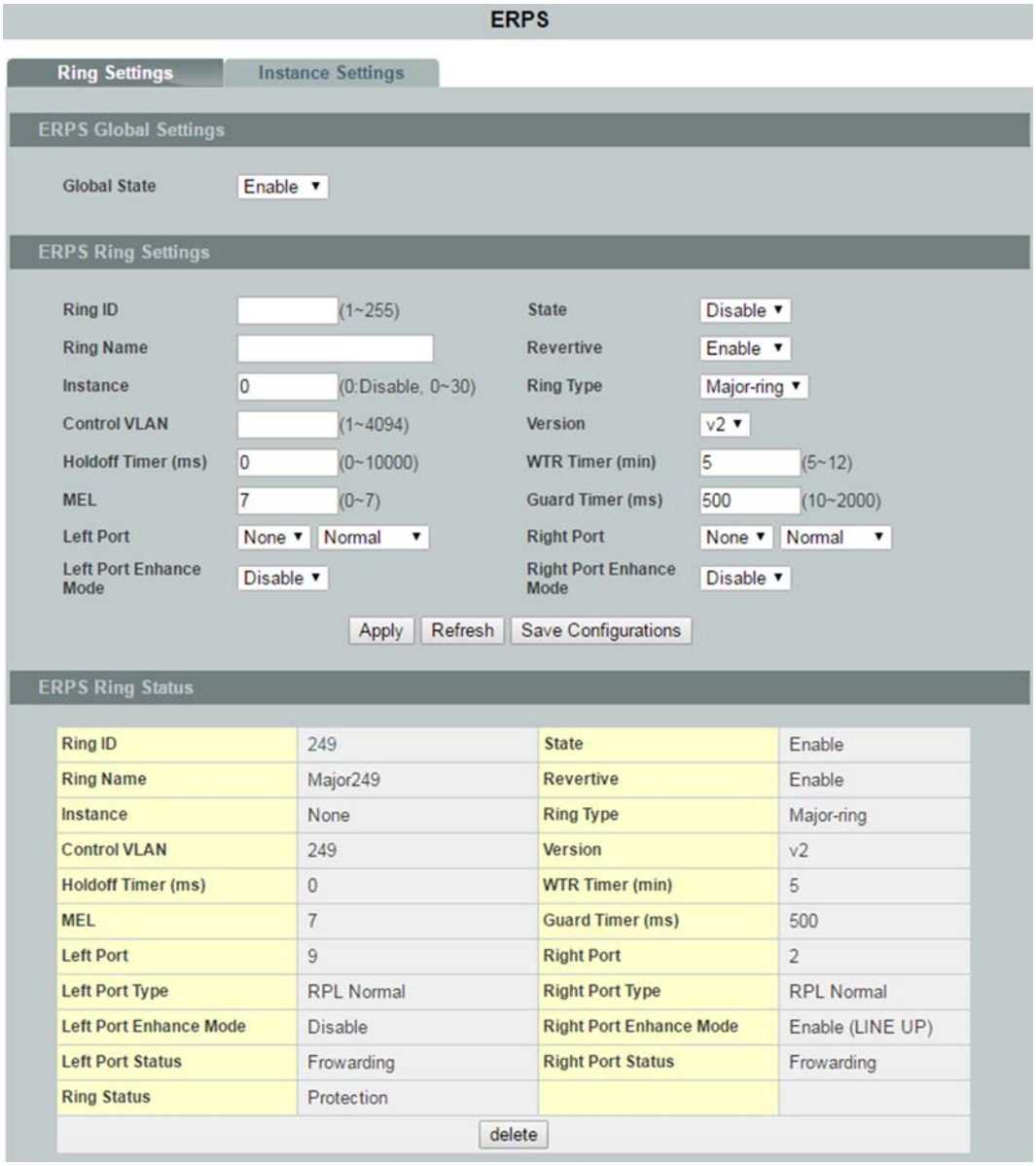


Abbildung 71: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

Tabelle 75: 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.
Ringname		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:Disable, 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 Group **L**evel) für den Ring ein. Der MEL gibt die Priorität an. 0 = niedrigste Priorität 7 = höchste Priorität

Tabelle 75: 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	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	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.
Alarm Relay	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, wenn das Alarm-Relais **nicht** bei einem geöffneten ERPS (Enhancement Mode) schalten soll.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, wenn das Alarm-Relais bei einem geöffneten ERPS (Enhancement Mode) schalten soll.
ERPS-Ringstatus		
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.

Tabelle 75: WBM-Seite „ERPS“ – Register „Ringeinstellungen“

Ringname		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	In diesem Anzeigefeld wird die Port-Nummer des linken Ports angezeigt.
Rechter Port	Keiner 1 … 10	In diesem Anzeigefeld wird die Port-Nummer des rechten Ports angezeigt.
Linker Port-Typ	RPL Normal Nachbar Owner	In diesem Anzeigefeld wird der Typ des linken Ports angezeigt.
Rechter Port-Typ	RPL 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.
Alarm Relay	Ausschalten Einschalten	In diesem Anzeigefeld wird der aktuelle Status des Alarmrelais angezeigt.
Ringstatus	Schutz Leerlauf	In diesem Anzeigefeld wird der Ringstatus angezeigt.
Löschen		Klicken Sie auf **[Löschen]**, um diese Einstellung zu löschen.

9.3.8.2 Instance-Einstellungen

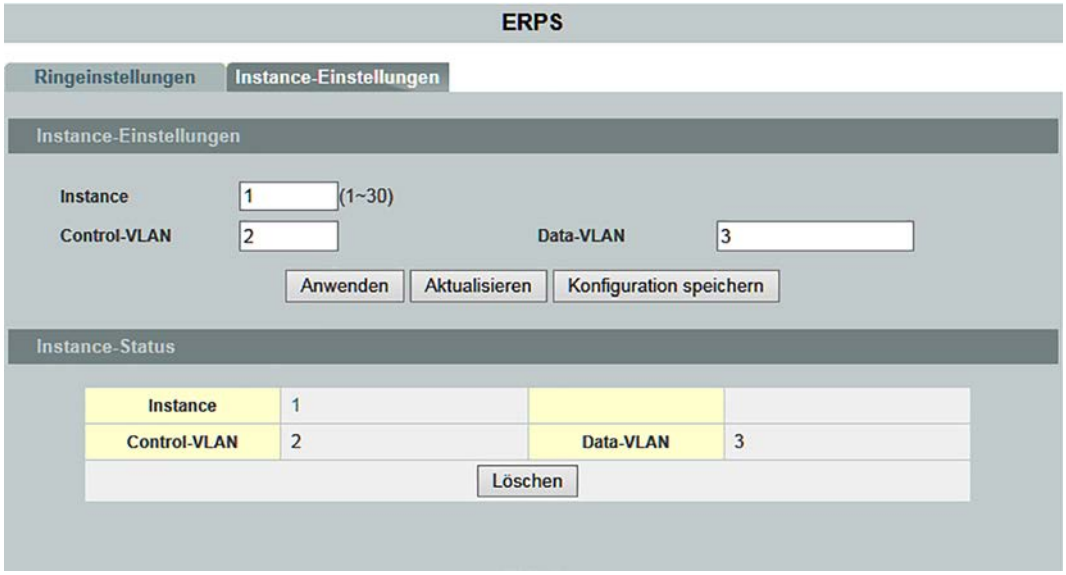


Abbildung 72: WBM-Seite „ERPS“ – Register „Instance-Einstellungen“

Tabelle 76: 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.

9.3.9 Link-Aggregation

9.3.9.1 Static-Trunk

Hinweis

Weitere Information

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

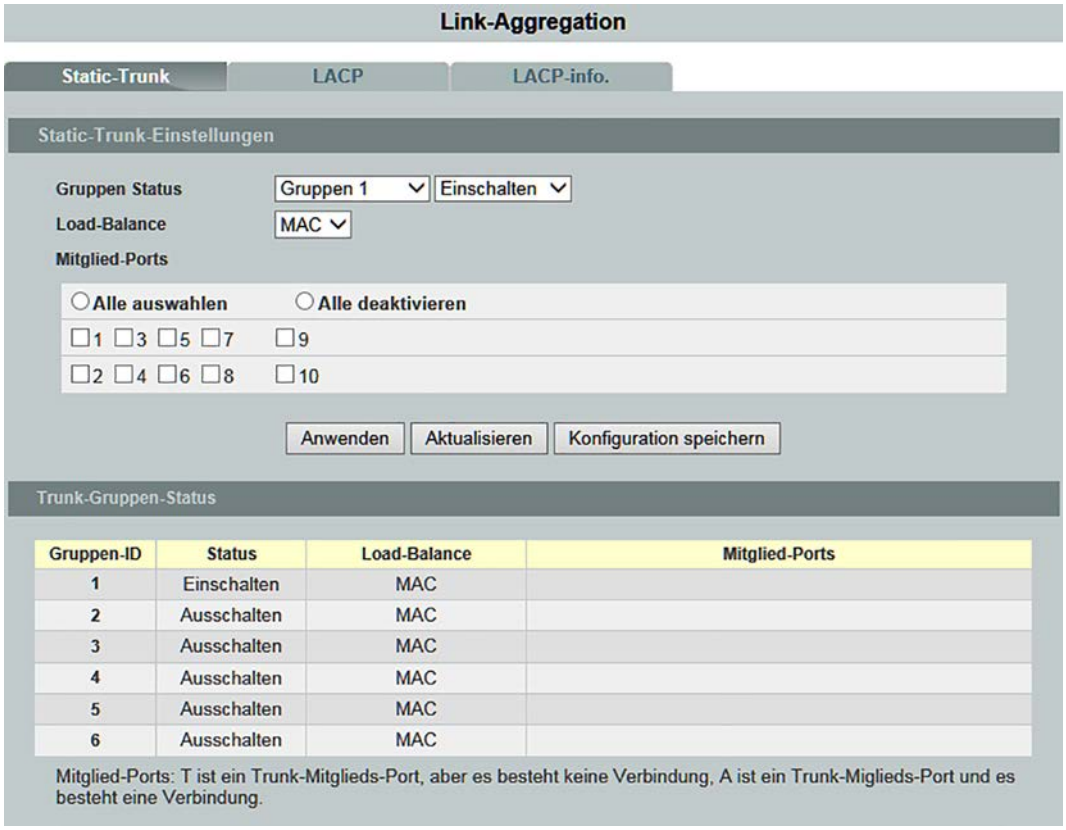


Abbildung 73: WBM-Seite „Link-Aggregation“ – Register „Static-Trunk“

Tabelle 77: WBM-Seite „Link-Aggregation“ – Register „Static-Trunk“

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.	
Mitglied-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 … ☐ 10	☐	☐	Der Port ist nicht aktiviert.
			☑	Der Port ist aktiviert.
Trunk-Gruppen-Status				
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.	
Mitglied-Ports			In dieser Spalte werden die Ports angezeigt, die der statischen „Trunk-Gruppe“ zugeordnet sind.	

9.3.9.2 LACP

Hinweis

Weitere Information

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

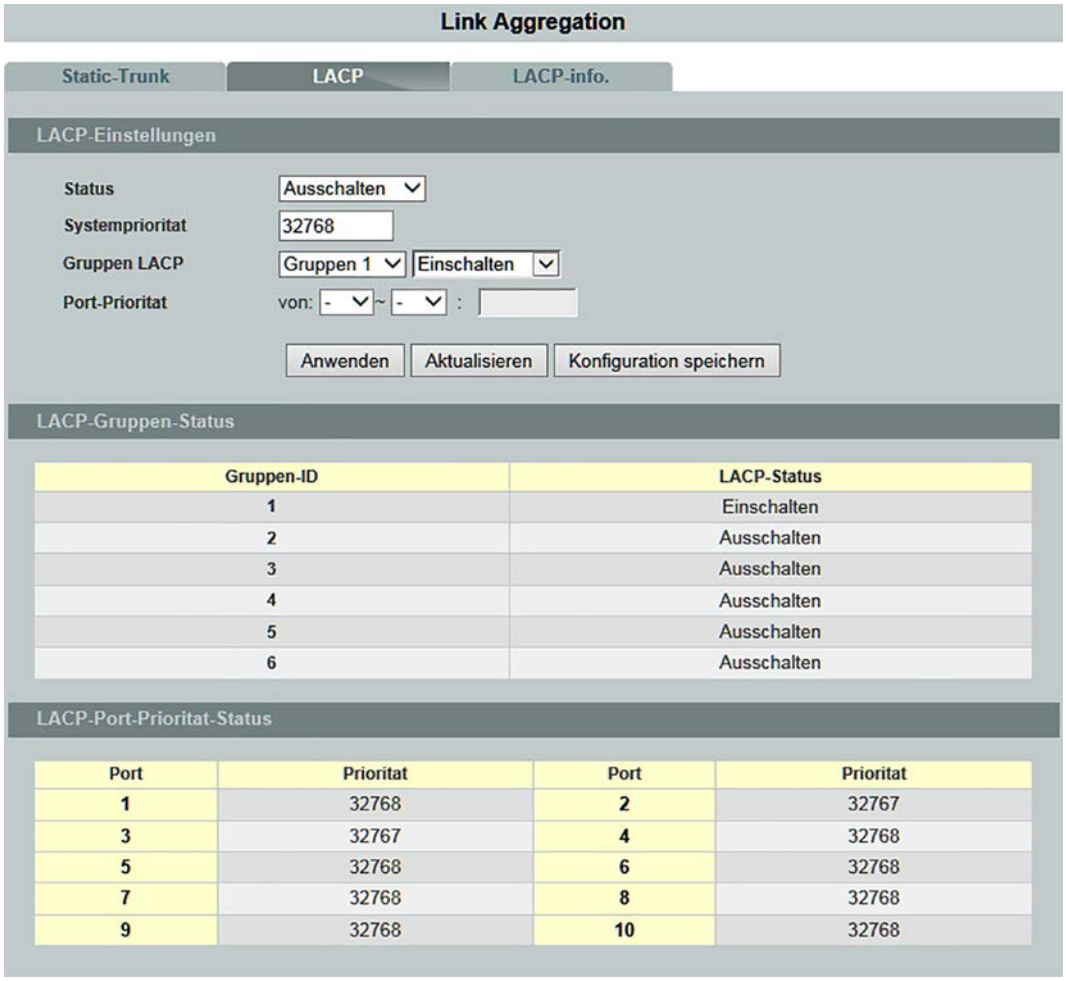


Abbildung 74: WBM-Seite „Link-Aggregation“ – Register „LACP“

Tabelle 78: WBM-Seite „Link-Aggregation“ – Register „LACP“

LACP-Einstellungen			
Parameter		**Standardwert**	**Beschreibung**
Status		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie das 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.
Gruppen-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-Gruppen-Status			
Parameter		**Standardwert**	**Beschreibung**
Gruppen-ID		1 … 6	In diesem 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-Priorität-Status			
Parameter		**Standardwert**	**Beschreibung**
Port		1 … 10	In dieser Spalte wird die Port-ID angezeigt.
Priorität		1 … 65535	In dieser Spalte wird die LACP-Priorität des Ports angezeigt.

9.3.9.3 LACP-Info.

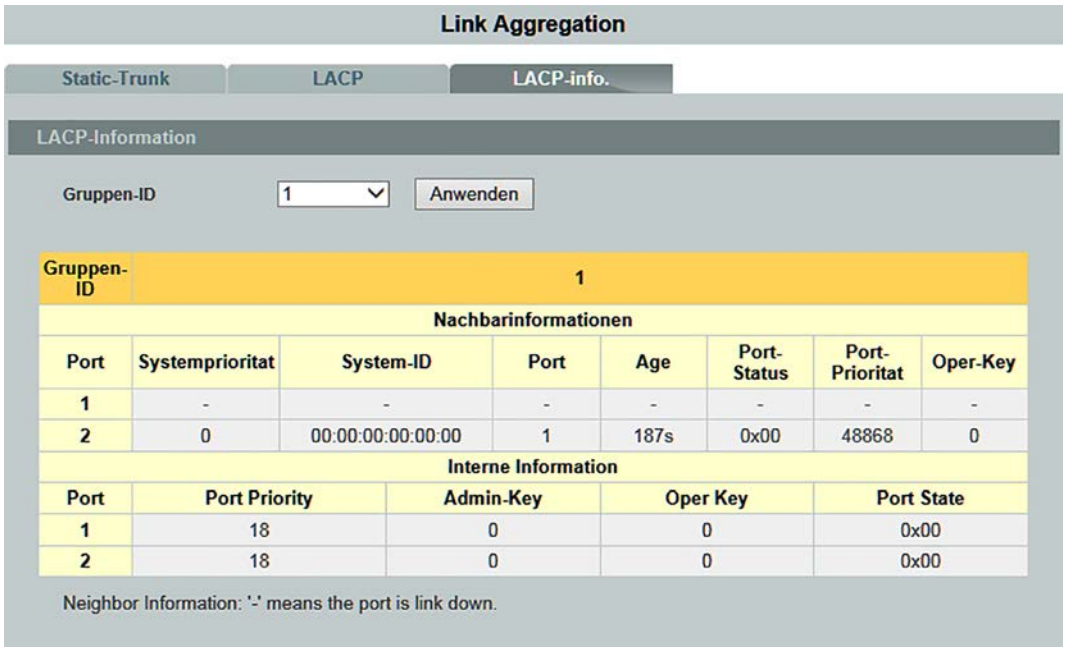


Abbildung 75: WBM-Seite „Link-Aggregation“ – Register „LACP-Info.“

Tabelle 79: 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	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	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 Priority		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 State		In dieser Spalte wird der Port-Zustand des LACP-Teilnehmer-Ports angezeigt.

9.3.10 LLDP

Hinweis **Weitere Information**

Weitere Informationen zu „LLDP“ (**L**ink **L**ayer **D**iscovery **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.10.1 Einstellungen

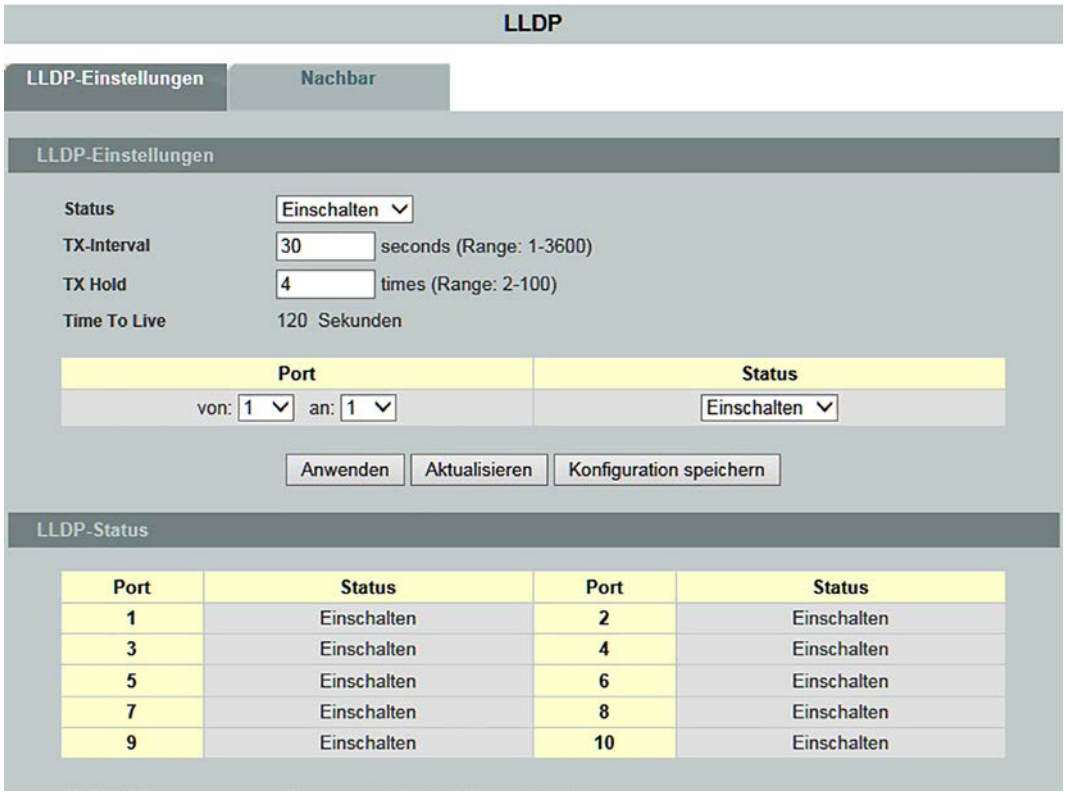


Abbildung 76: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“

Tabelle 80: WBM-Seite „LLDP“ – Register „LLDP-Einstellungen“

LLDP-Einstellungen			
Parameter		**Standardwert**	**Beschreibung**
Status		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die LLDP-Funktion für den Switch global zu aktivieren.
TX-Interval		**30**	Geben Sie im Eingabefeld den Wert für das „TX-Interval“ (Übertragungsintervall) für die LLDP-Pakete ein.
TX-Hold		**4**	Geben Sie im Eingabefeld den Wert für die „TX-Hold-Time“ (TX-Haltezeit) ein, die die TTL der Nachricht des Switches bestimmt. (TTL = tx-hold * tx-interval)
Time To Live		**120**	In diesem Anzeigefeld wird die Lebenszeit für die Informationen des Switches angezeigt.
Port	von:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung des „LLDP“ konfigurieren möchten.
	an:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung des „LLDP“ konfigurieren möchten.
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**	**Beschreibung**
Port		1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Status		Ausschalten Einschalten	In dieser Spalte wird angezeigt, ob „LLDP“ aktiviert oder deaktiviert ist.

9.3.10.2 Nachbar

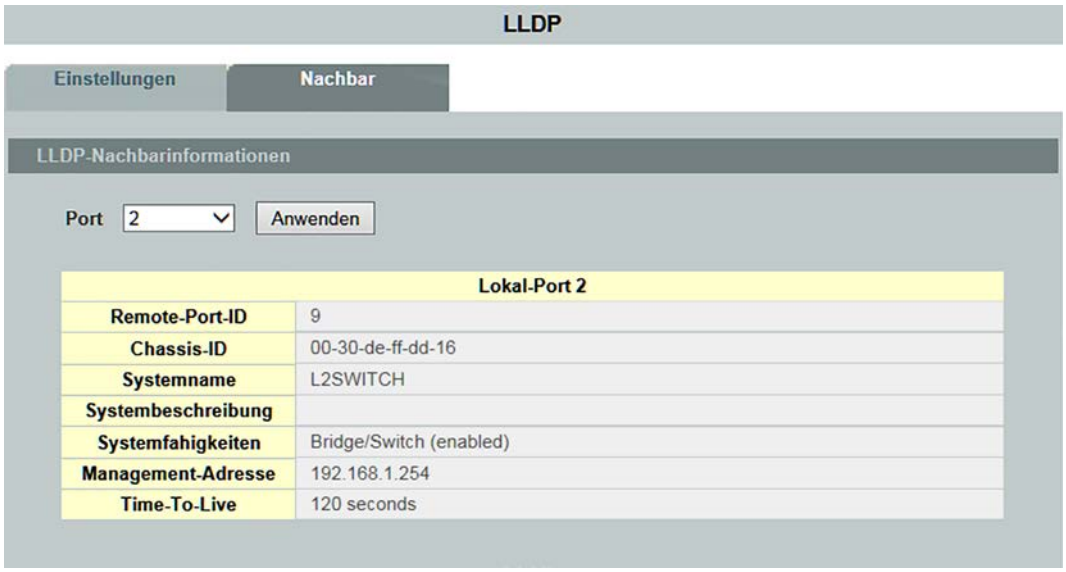


Abbildung 77: WBM-Seite „LLDP“ – Register „Nachbar“

Tabelle 81: WBM-Seite „LLDP“ – Register „Nachbar“

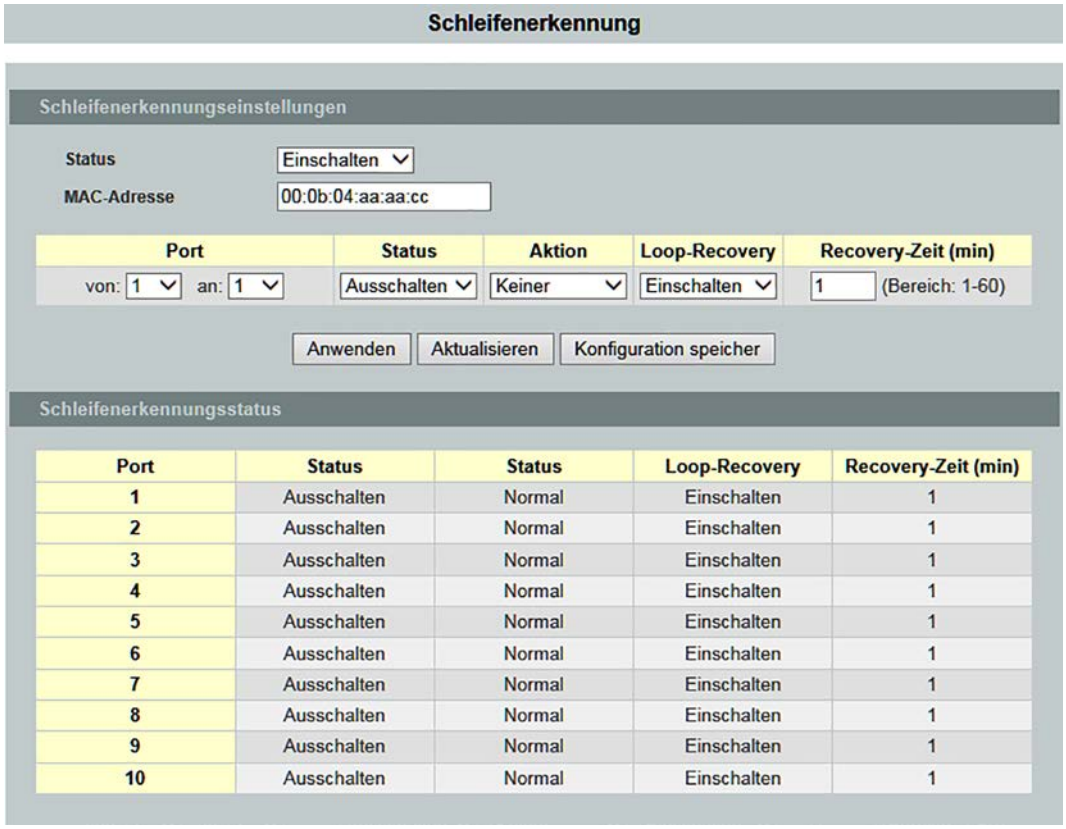
LLDP-Nachbarinformationen		
Parameter	**Standardwert**	**Beschreibung**
Port	**Alle**	Wählen Sie im Auswahlfeld „Alle“, wenn Sie von allen Nachbar-Ports Informationen angezeigt bekommen möchten.
	1 … 10	Wählen Sie im Auswahlfeld einen Port aus, von dessen Nachbar-Port Sie Informationen angezeigt bekommen möchten.
Lokal-Port	1 … 10	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-Adresse		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.

9.3.11 Schleifenerkennung (Loop Detection)

Hinweis

Weitere Information

Weitere Informationen zu „Schleifenerkennung“ (Loop Detection) finden Sie im Kapitel „Funktionsbeschreibung“.



Port	Status	Status	Loop-Recovery	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

Abbildung 78: WBM-Seite „Schleifenerkennung“

Tabelle 82: WBM-Seite „Schleifenerkennung“

Schleifenerkennungseinstellungen			
Parameter		**Standardwert**	**Beschreibung**
Status		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um diese Funktion zu aktivieren.
MAC-Adresse			Geben Sie im Eingabefeld die MAC-Zieladresse ein, an die die Sonderpakete gesendet werden sollen. Empfängt der Port dieselben Pakete, wird er abgeschaltet.
Port	von:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Guard Protection“ (Schleifenschutz) konfigurieren möchten.
	an:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Guard Protection“ (Schleifenschutz) konfigurieren möchten.
Status		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
		Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um die Funktion „Loop Guard“ (Schleifenschutz) für den Switch zu aktivieren.
Aktion		**Keiner**	Wählen Sie im Auswahlfeld „Keiner“, wenn Sie die Schleifenerkennung am Port ausschalten.
		Freischalten	Wählen Sie im Auswahlfeld „Freischalten“, wenn Sie die Funktionen „Status“ und „Loop Korrektur“ nicht verändern wollen.
Loop-Recovery		**Einschalten**	Wählen Sie im Auswahlfeld „Einschalten“, damit sich der Port nach Ablauf der zugewiesenen „Recovery-Zeit“ automatisch reaktiviert.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
Recovery-Zeit (min) (Bereich: 1~60)		**1**	Geben Sie im Eingabefeld den Wert für die „Recovery-Zeit“ (in Minuten) ein, die der Switch wartet, bevor er den Port reaktiviert. Zeitraum: 1 … 60 min
Schleifenerkennungsstatus			
Parameter		**Standardwert**	**Beschreibung**
Port		1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Status		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob die Funktion „Loop Guard“ aktiviert oder deaktiviert ist.
Status		Keiner Normal	In dieser Spalte wird angezeigt, ob ein Port blockiert wird.
Loop-Recovery		Einschalten Ausschalten	In dieser Spalte wird angezeigt, ob die Funktion „Loop-Recovery“ aktiviert oder deaktiviert ist.
Recovery-Zeit (min)		1 … 50	In dieser Spalte wird die „Recovery-Zeit“ für die Funktion „Loop-Recovery“ angezeigt.

9.3.12 Jet-Ring

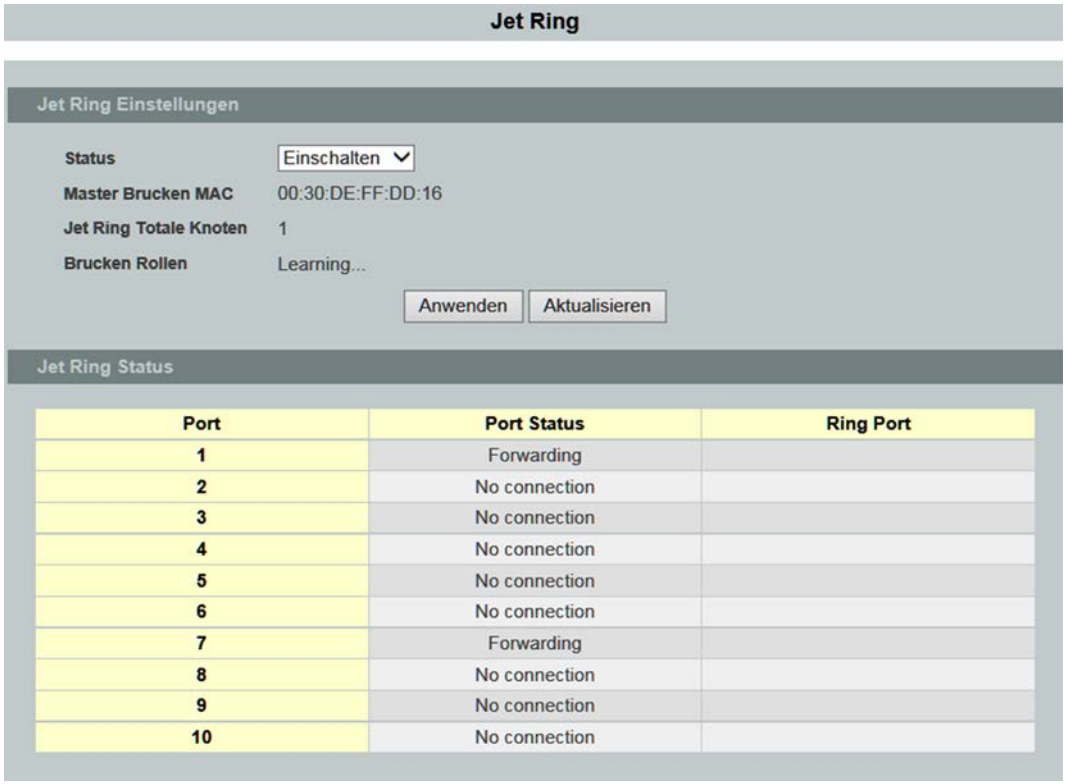


Abbildung 79: WBM-Seite „Jet-Ring“

Tabelle 83: 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.
Alarm Relay	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um
Master Brucken MAC (Master Bridge MAC)		In diesem Anzeigefeld wird die IP-Adresse des Jet-Ring-Masters angezeigt.
Jet Ring Totale Knoten		In diesem Anzeigefeld wird die Anzahl der Switche im Jet-Ring angezeigt.
Bridge Role		In diesem Anzeigefeld wird die Funktion des Switches im Jet Ring angezeigt.
Jet-Ring-Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Port Status	No connection 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.

9.3.13 MODBUS

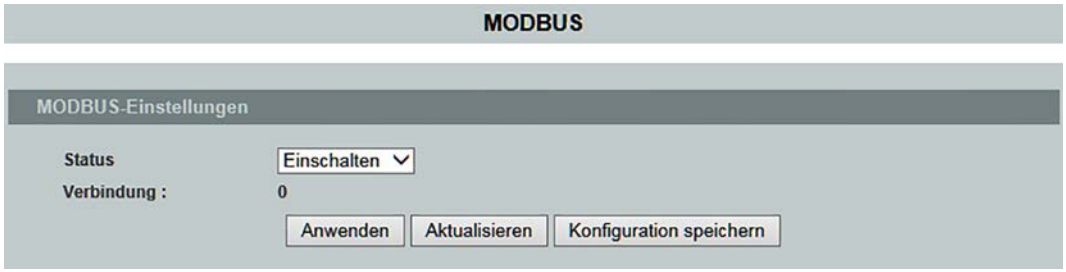


Abbildung 80: WBM-Seite „MODBUS“

Tabelle 84: 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.

9.3.14 Spanning Tree Protocol

Hinweis **Weitere Information**

Weitere Informationen zu „**S**panning **T**ree **P**rotocol“ (STP) finden Sie im Kapitel „Funktionsbeschreibung“.

9.3.14.1 Allgemeine Einstellungen

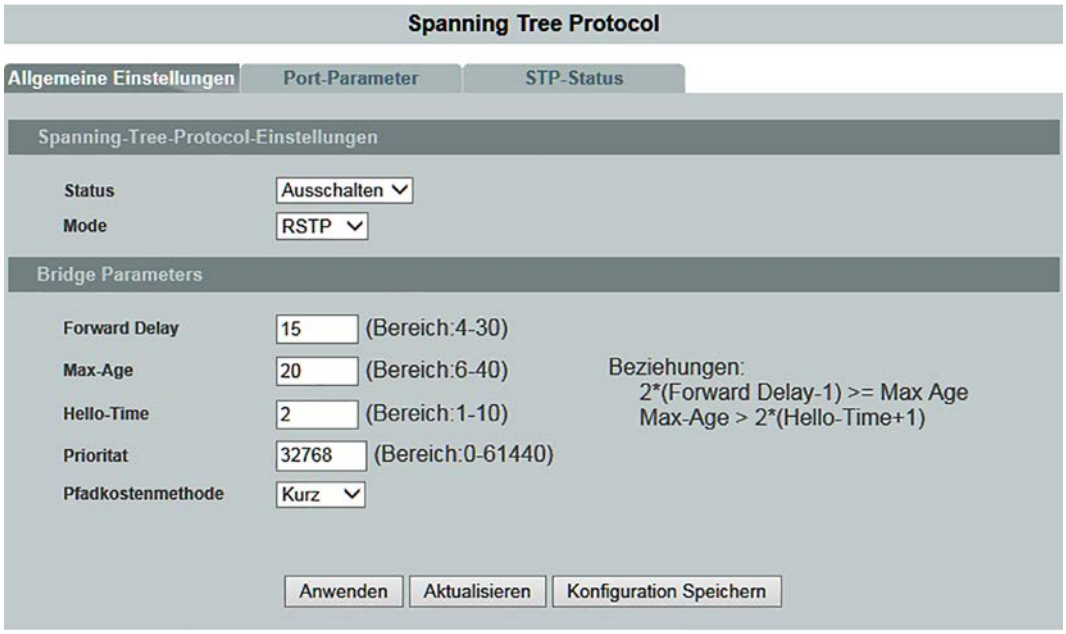


Abbildung 81: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“

Tabelle 85: WBM-Seite „Spanning Tree Protocol“ – Register „Allgemeine Einstellungen“

Spanning-Tree-Protocol-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Status	**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um diese Funktion zu deaktivieren.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, um das „Spanning Tree Protocol“ (STP) oder das „Rapid Spanning Tree Protocol“ (RSTP) zu verwenden.
Mode	**RSTP**	Wählen Sie im Auswahlfeld „RSTP“, wenn Sie das schnellere „Rapid Spanning Tree Protocol“ verwenden möchten.
	MSTP	Wählen Sie im Auswahlfeld „MSTP“, wenn Sie das „Multiple Spanning Tree Protocol“ verwenden möchten.
	STP	Wählen Sie im Auswahlfeld „STP“, wenn Sie das „Spanning Tree Protocol“ verwenden möchten.
Bridge Parameters		
Parameter	**Standardwert**	**Beschreibung**
Forward Delay	**15**	Geben Sie im Eingabefeld die Zeit „Forward Delay“ ein. Gültiger Bereich: 4 … 30 s
Max-Age	**20**	Geben Sie im Eingabefeld die Zeit „Max-Age“ ein. Gültiger Bereich: 6 … 40 s
Hello-Time	**2**	Geben Sie im Eingabefeld die Zeit für die „Hello-Time“ ein. Gültiger Bereich: 1 … 10 s
Priorität	**32768**	Geben Sie im Eingabefeld einen Wert für die Priorität ein. Je niedriger der von Ihnen zugewiesene numerische Wert ist, desto höher ist die Priorität dieser Bridge. Gültiger Bereich: 0 … 61440
Pfadkostenmethode	**Kurz**	Wählen Sie im Auswahlfeld „Kurz“, wenn Sie eine Größe von 16 Bit und eine Übertragungsgeschwindigkeit bis zu 10 GBit wählen möchten. 10 MBit = 100 100 MBit = 19 1 GBit = 4 10 GBit = 2
	Lang	Wählen Sie im Auswahlfeld „Lang“, wenn Sie eine Größe von 32 Bit und eine Übertragungsgeschwindigkeit bis zu 10 TBit wählen möchten. 10 MBit = 2000000 100 MBit = 200000 1 GBit = 20000 10 GBit = 2000 100 GBit = 200 1 TBit = 20

9.3.14.2 Port-Parameter

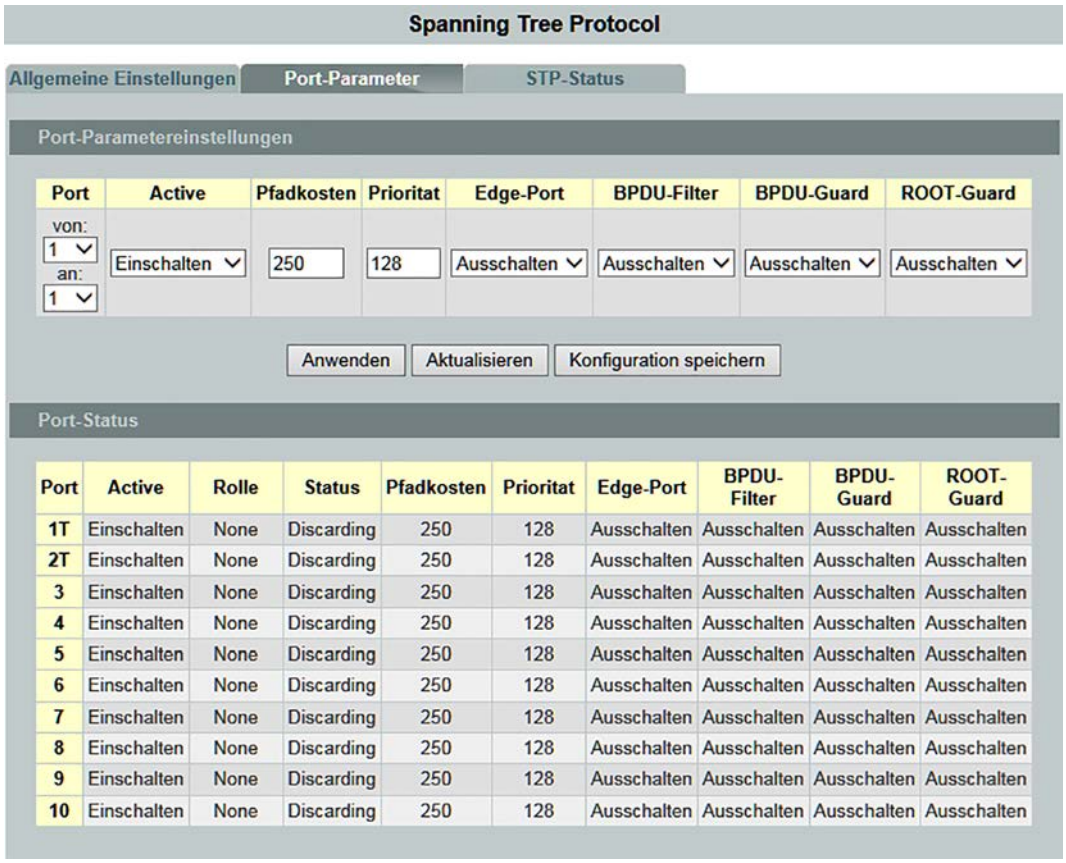


Abbildung 82: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Tabelle 86: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Port-Parametereinstellungen			
Parameter		**Standardwert**	**Beschreibung**
Port	From:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
	To:	**1**	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP-Funktion“ zu konfigurieren.
Active		**Einschalten**	Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die STP-Funktion für den spezifischen Port aktivieren möchten.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die STP-Funktion für den spezifischen Port deaktivieren möchten.
Pfadkosten		**250**	Geben Sie im Eingabefeld den Wert für die Pfadkosten für den spezifischen Port ein.
Priorität		**128**	Geben Sie im Eingabefeld den Wert für die Priorität für den spezifischen Port ein.
Edge-Port		**Ausschalten**	Wählen Sie im Auswahlfeld „Ausschalten“, um den 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 86: WBM-Seite „Spanning Tree Protocol“ – Register „Port-Parameter“

Port-Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Active	**Einschalten** Ausschalten	In dieser Spalte wird der Zustand der STP-Funktion angezeigt.
Rolle	Alternated Designated Root Backup None	In dieser Spalte wird die Rolle des Ports angezeigt.
Status	Discarding Blocking Listening Learning Forwarding Disabled	In dieser Spalte wird der Port-Status angezeigt.
Pfadkosten	0 … 65535	In dieser Spalte werden die Pfadkosten des Ports angezeigt.
Priorität	0 … 61440	In dieser Spalte wird die Priorität des Ports angezeigt.
Edge-Port	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „Edge-Port“ angezeigt.
BPDU-Filter	Ausschalten Einschalten	In dieser Spalte wird der Zustand der BPDU-Filterfunktion angezeigt.
BPDU-Guard	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „BPDU-Guard“ angezeigt.
ROOT-Guard	Ausschalten Einschalten	In dieser Spalte wird der Zustand der Funktion „Root-Guard“ angezeigt.

9.3.14.3 STP-Status

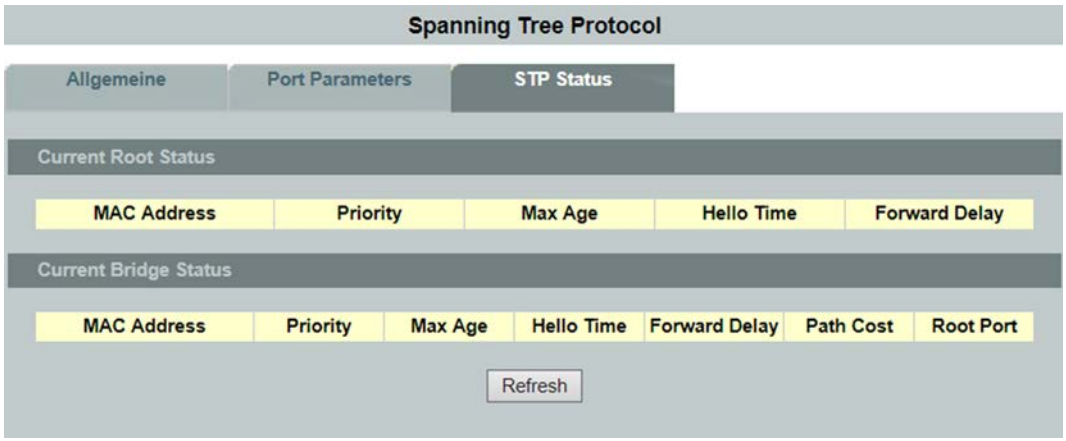


Abbildung 83: WBM-Seite „Spanning Tree Protocol“ – Register „STP-Status“

Tabelle 87: WBM-Seite „STP“ – Register „STP-Status“

Aktueller Root-Status		
Parameter	**Standardwert**	**Beschreibung**
MAC-Adresse		In diesem Anzeigefeld wird die MAC-Adresse der „Root-Bridge“ angezeigt.
Priorität		In diesem Anzeigefeld wird die Priorität der „Root-Bridge“ angezeigt. Auch dieser Switch kann die „Root-Bridge“ sein.
Max Age		In diesem Anzeigefeld wird das „Max Age“ der „Root-Bridge“ angezeigt.
Hello-Time		In diesem Anzeigefeld wird die „Hello-Time“ der „Root-Bridge“ angezeigt. Die „Root-Bridge“ bestimmt „Hello-Time“, „Max-Age“ und „Forwarding-Delay“.
Forward-Delay		In diesem Anzeigefeld wird die maximale Zeit (in Sekunden) angezeigt, die der Root-Switch wartet, bevor er Zustände ändert.
Aktueller Bridge-Zustand		
Parameter	**Standardwert**	**Beschreibung**
MAC-Adresse		In diesem Anzeigefeld wird die MAC-Adresse der aktuellen Bridge angezeigt.
Priorität		In diesem Anzeigefeld wird die Priorität angezeigt.
Max-Age		In diesem Anzeigefeld wird das „Max-Age“ angezeigt.
Hello-Time		In diesem Anzeigefeld wird die „Hello-Time“ angezeigt.
Forward-Delay		In diesem Anzeigefeld wird die „Forward-Time“ angezeigt.
Pfadkosten		In diesem Anzeigefeld werden die Pfadkosten angezeigt.
ROOT-Port		In diesem Anzeigefeld wird die Nummer des Ports am Switch angezeigt, über den der Switch mit der Root des „Spanning Tree“ kommunizieren muss.

9.3.15 Xpress-Ring

Hinweis **Weitere Information**

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

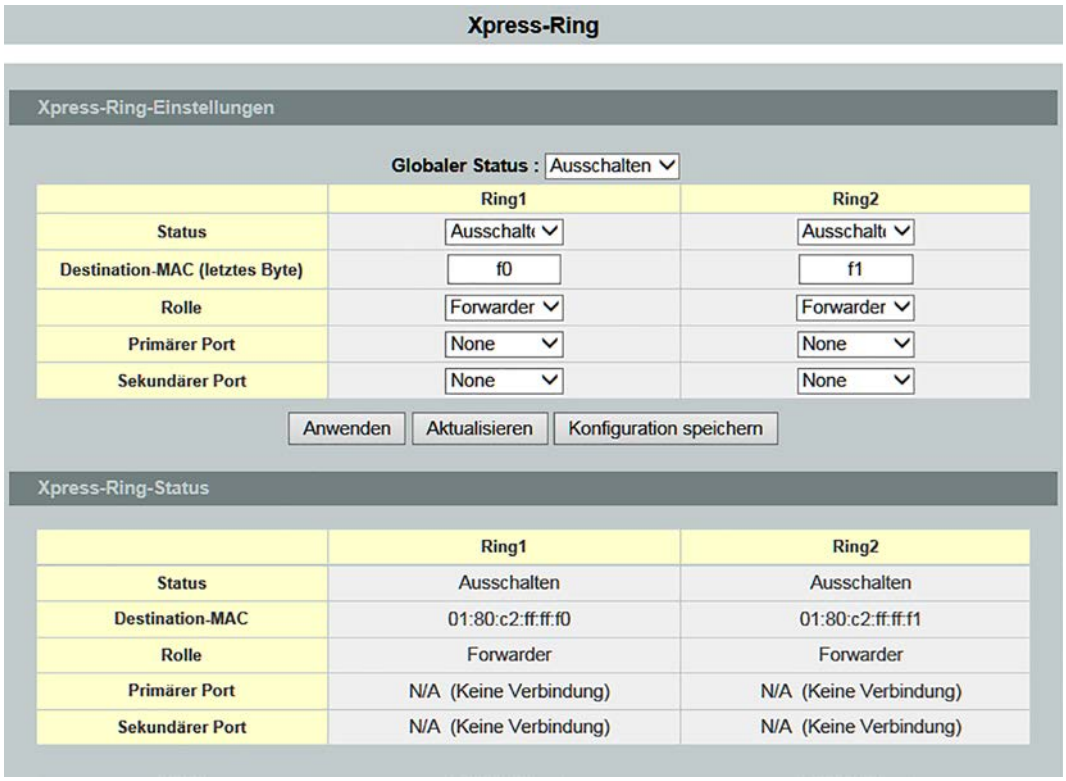


Abbildung 84: WBM-Seite „Xpress-Ring“

Tabelle 88: 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.
Destination-MAC (letztes Byte)		Geben Sie im Eingabefeld die MAC-Adresse des jeweiligen Rings ein.
Rolle	**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	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen primären Port im Ring aktivieren wollen.
	1 … 10	Wählen Sie im Auswahlfeld den entsprechenden primären Port aus.
Sekundärer Port	**None**	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen sekundären Port im Ring aktivieren wollen.
	1 … 10	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.
Destination-MAC		In diesem Anzeigefeld wird das letzte Byte der jeweiligen MAC-Adresse des Xpress-Rings angezeigt.
Rolle	Forwarder Arbiter	In diesem Anzeigefeld wird die Rolle des Switches angezeigt.
Primärer Port	N/A (keine Verbindung 0 … 10 (Forwarding, Blocking)	In diesem Anzeigefeld wird der Status des primären Ports angezeigt.
Sekundärer Port	N/A (keine Verbindung 0 … 10 (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“ (**D**ynamic **H**ost **C**onfiguration **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

9.4.1.1.1 DHCP-Snooping

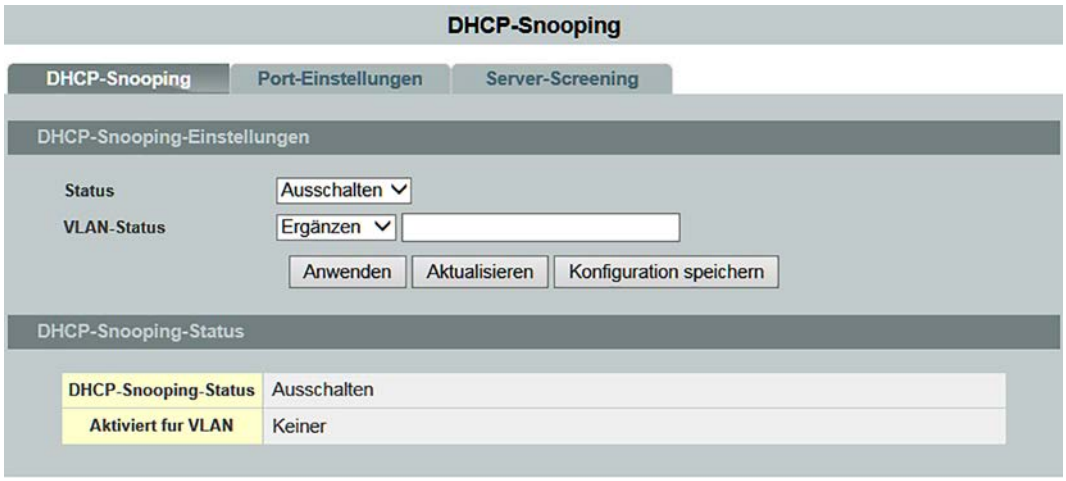


Abbildung 85: WBM-Seite „DHCP-Snooping“ – Register „DHCP-Snooping“

Tabelle 89: 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.
Aktiviert für 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

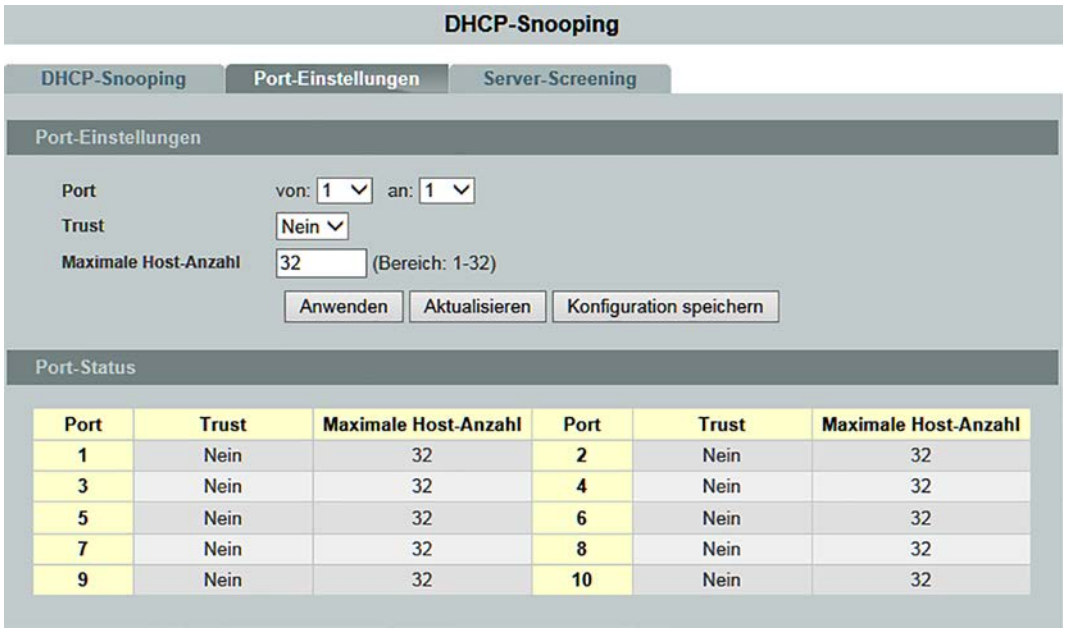


Abbildung 86: WBM-Seite „DHCP-Snooping“ – Register „Port-Einstellungen“

Tabelle 90: 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	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“.

Abbildung 87: WBM-Seite „DHCP-Snooping“ – Register „Server-Screening“

Tabelle 91: 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 Statischer Eintrag

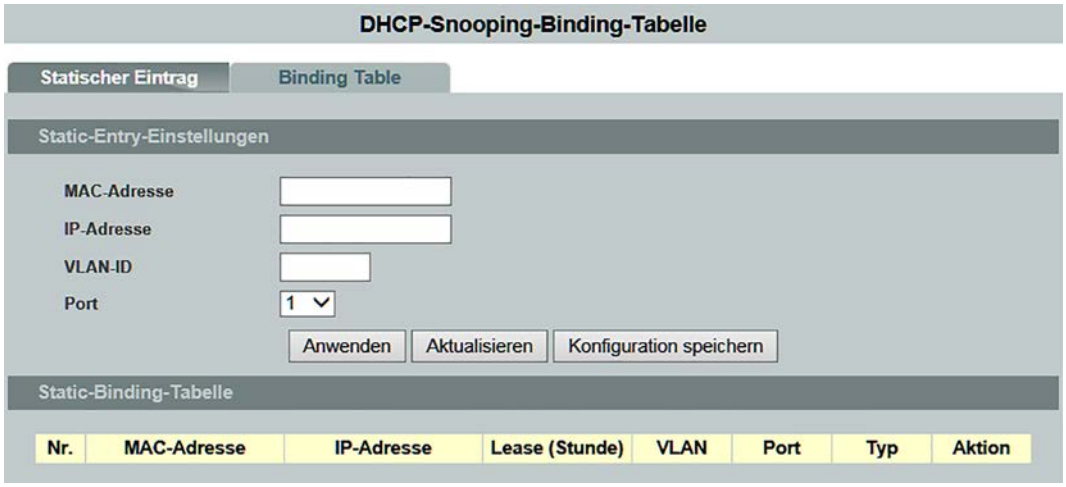


Abbildung 88: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Statischer Eintrag“

Tabelle 92: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Statischer Eintrag“

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	Wählen Sie im Auswahlfeld den physikalischen Port der Verbindung aus.
Static-Binding-Tabelle		
Parameter	**Standardwert**	**Beschreibung**
Nr.	1 … 10	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.
Lease (Stunde)		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	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

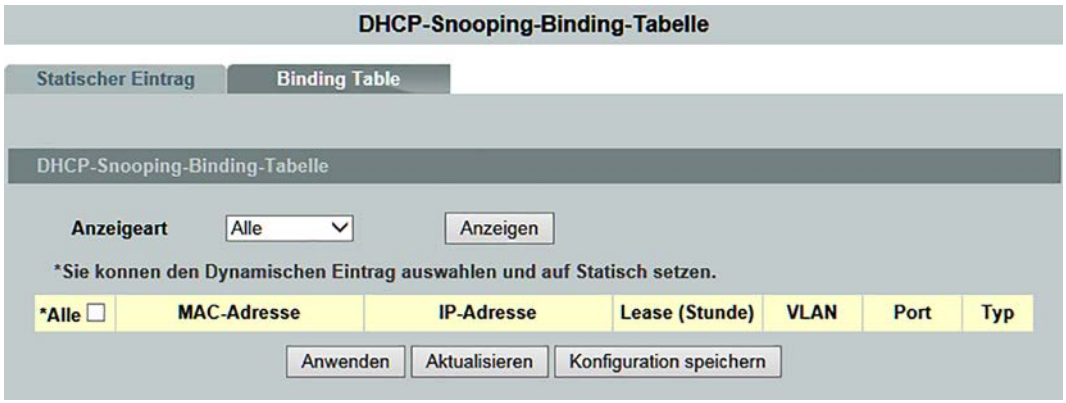


Abbildung 89: WBM-Seite „DHCP-Snooping-Binding-Tabelle“ – Register „Binding-Tabelle“

Tabelle 93: 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	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.
Lease (Stunde)		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

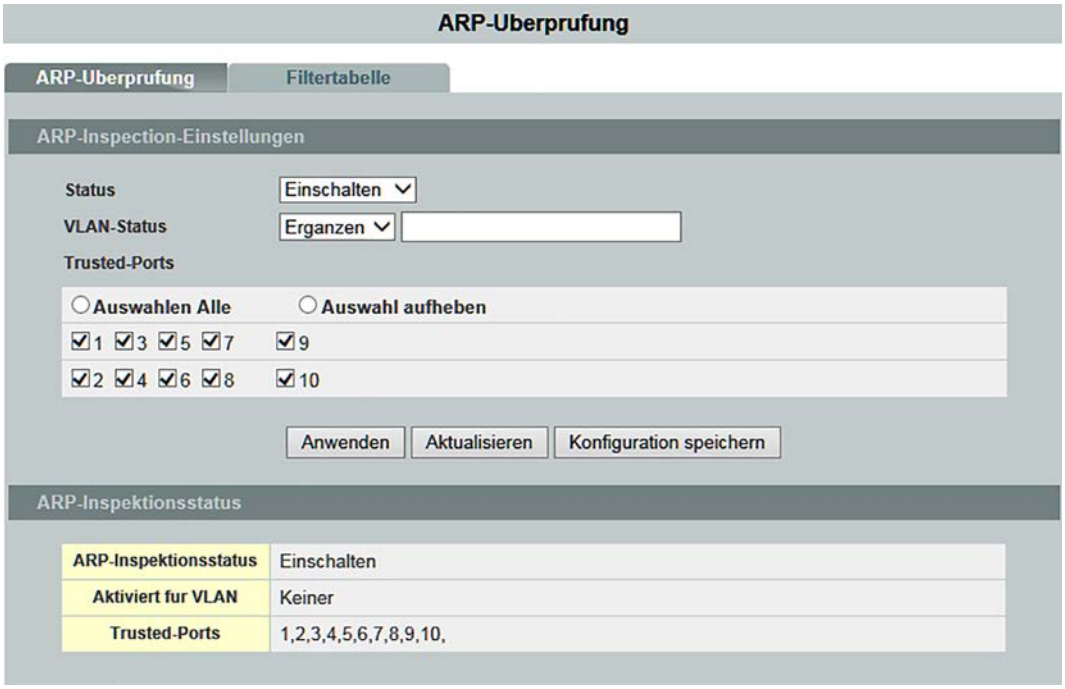


Abbildung 90: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“

Tabelle 94: WBM-Seite „ARP-Überprüfung“ – Register „ARP-Überprüfung“

ARP-Inspection-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	☐	☐	Der Port ist nicht aktiviert..
			☑	Der Port ist aktiviert.
ARP-Inspectionsstatus				
Parameter		**Standardwert**	**Beschreibung**	
ARP-Inspectionsstatus		Ausschalten Einschalten	In diesem Anzeigefeld wird der aktuelle Status der ARP-Überprüfung angezeigt.	
Aktiviert für VLAN		Keiner 1 … 10	In diesem Anzeigefeld werden die VLAN-IDs angezeigt, für die die ARP-Überprüfung aktiviert ist.	
Trusted-Ports		Keiner 1 … 10	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“.

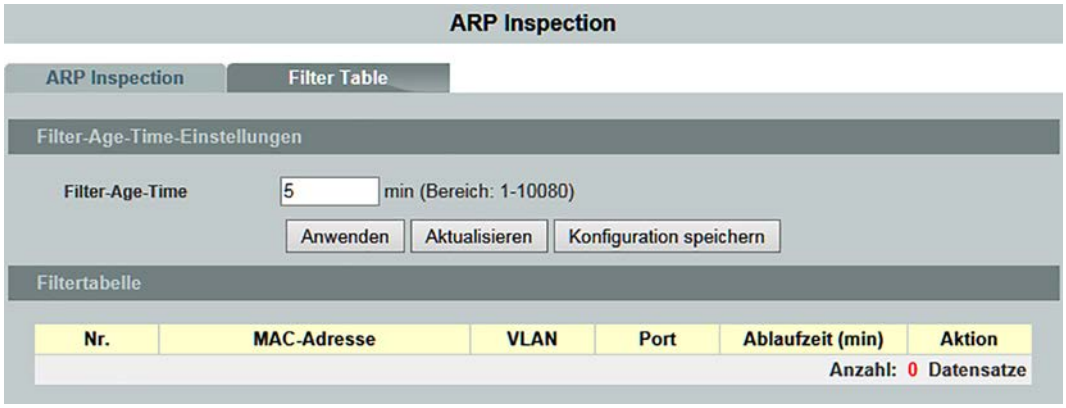


Abbildung 91: WBM-Seite „ARP-Überprüfung“ – Register „Filtertabelle“

Tabelle 95: 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

Hinweis

Weitere Information

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

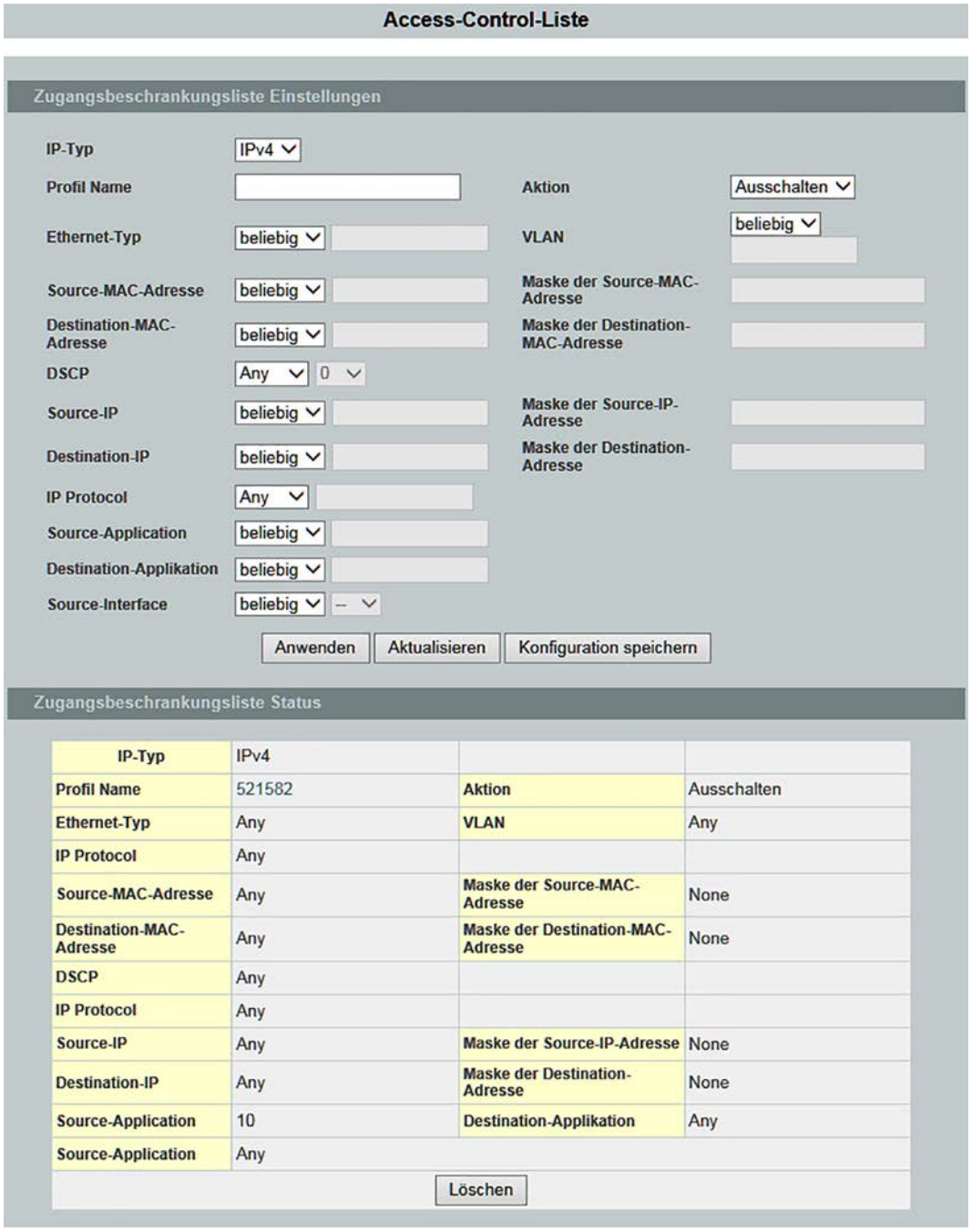


Abbildung 92: WBM-Seite „Access-Control-Liste“

Tabelle 96: WBM-Seite „Access-Control-Liste“

Access-Control-Liste-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 Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Source- MAC-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine MAC-Adresse filtern, die im MAC-Source-Adressfeld eingetragen wurde.
Destination-MAC-Adresse (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 Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Destination-MAC-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine MAC-Adresse filtern, die im MAC-Destination-Adressfeld eingetragen wurde.

Tabelle 96: WBM-Seite „Access-Control-Liste“

DSCP (nur bei IPv4)	**Any**	Wählen Sie im Auswahlfeld „Any“, damit jede DSCP-Priorität für die Zugriffskontrollliste gültig ist.	
	Other	**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 Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Source-IP“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine IP-Adresse filtern, die im IP-Source-Adressfeld eingetragen wurde.	
Destination-IP	**beliebig**	Wählen Sie im Auswahlfeld „beliebig“, damit jede IP-Adresse gültig ist.	
	Andere	Wählen Sie im Auswahlfeld „Andere“, um die Destination-IP-Adresse in die Access-Control-Liste einzutragen.	
Maske der Destination-IP-Adresse		Geben Sie im Eingabefeld die Destination-IP-Adresse der Bitmap-Maske für IP-Destination-Adressen von Paketen ein, die gefiltert werden sollen. Haben Sie im Auswahlfeld „Destination-IP-Adresse“ „beliebig“ gewählt, bleibt dieses Feld leer. Dann wird das Profil nur die eine IP-Adresse filtern, die im IP-Destination-Adressfeld eingetragen wurde.	
IP-Protokoll	**Any**	Wählen Sie im Auswahlfeld „Any“, damit jedes IP-Protokoll für die Access-Control-Liste gültig ist.	
	Other	Geben Sie im Auswahlfeld „Other“, 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	Geben Sie im Eingabefeld den physikalischen Port ein, für den dieser Eintrag in der Access-Control-Liste gültig ist.

Tabelle 96: WBM-Seite „Access-Control-Liste“

Access-Control-Liste-Status		
Parameter	**Standardwert**	**Beschreibung**
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)	Any Other	In diesem Anzeigefeld wird die DSCP-Priorität angezeigt.
IP-Protokoll	Any Other	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	beliebig Andere	In diesem Anzeigefeld wird die Destination-IP angezeigt.
Maske der Destination-IP-Adresse		In diesem Anzeigefeld wird die Destination-IP-ID der Bitmap-Maske angezeigt.
Source-Applikation	beliebig Andere	In diesem Anzeigefeld wird die Source-Applikation angezeigt.
Destination-Applikation	beliebig Andere	In diesem Anzeigefeld wird die Destination-Applikation angezeigt.
Source-Interface	1 … 10	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

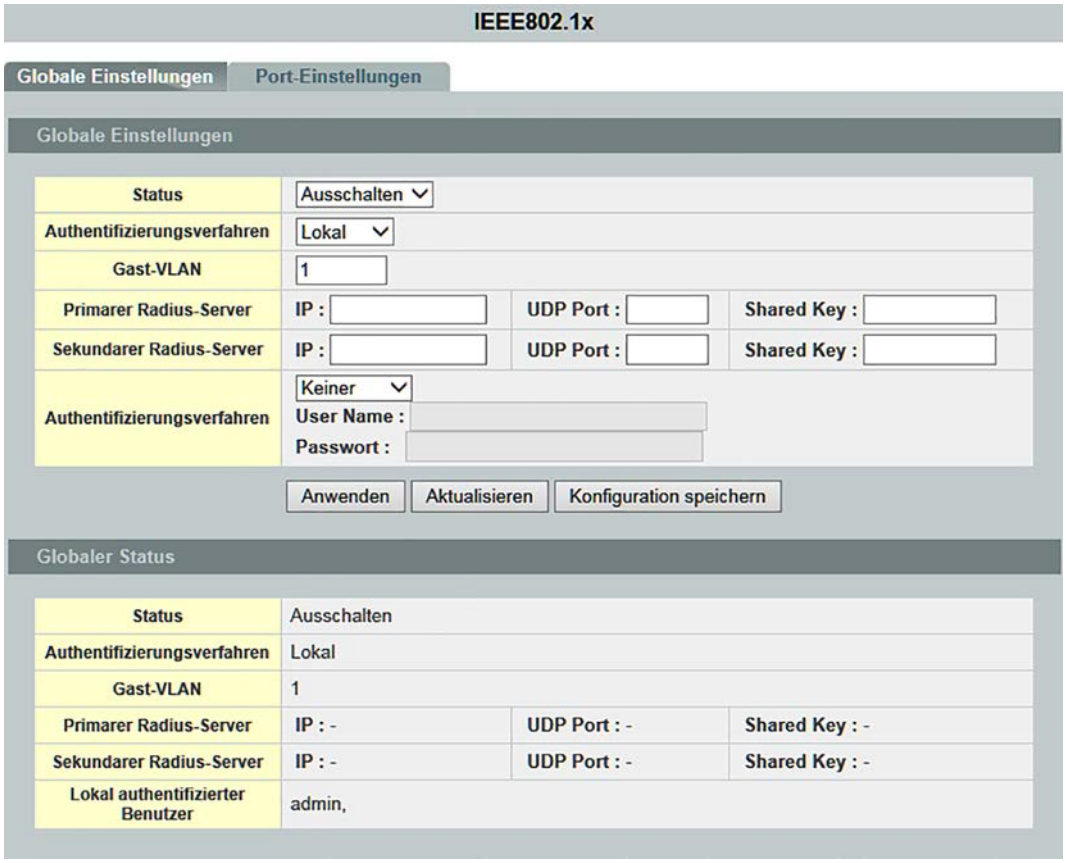


Abbildung 93: WBM-Seite „IEEE 802.1x“ – Register „Globale Einstellungen“

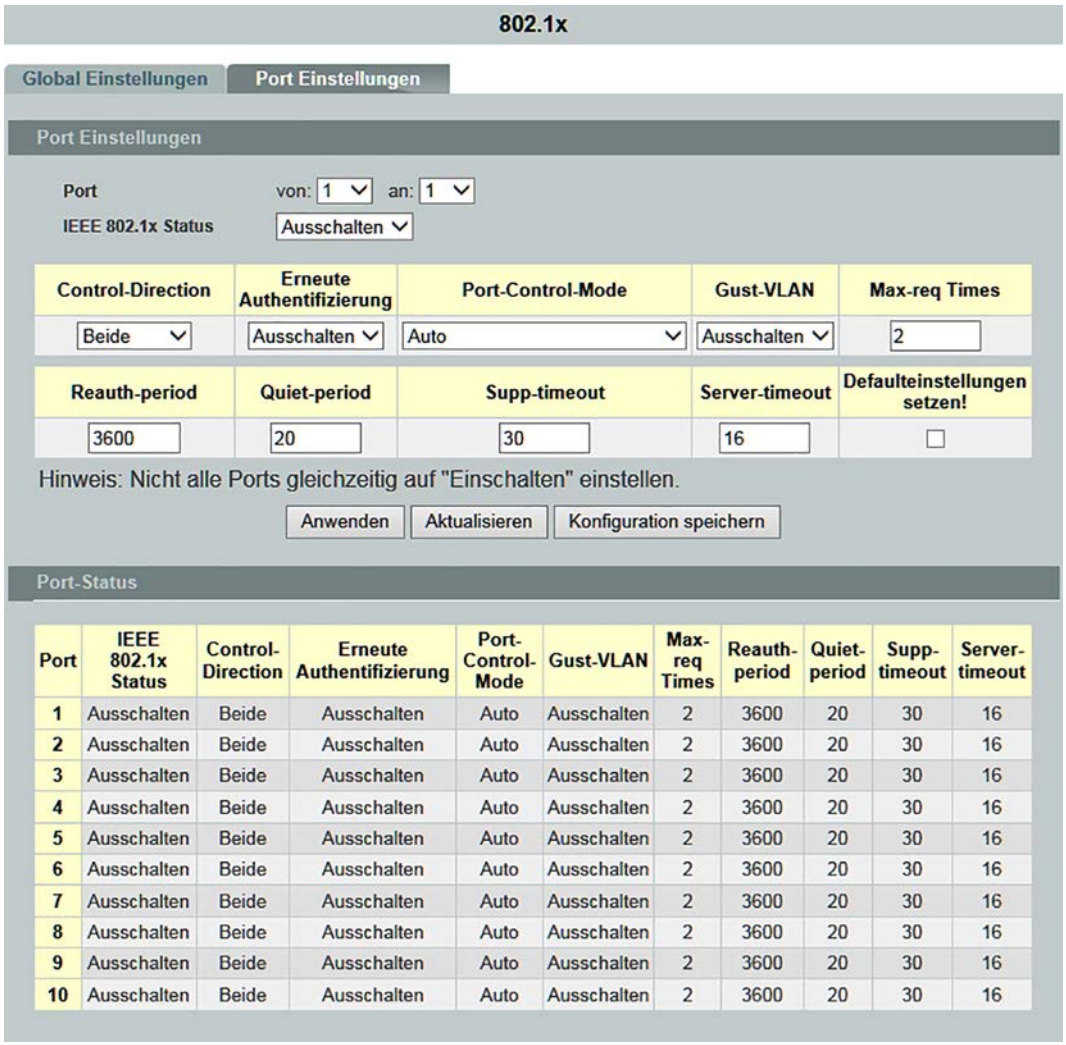
Tabelle 97: WBM-Seite „IEEE 802.1x“ – Register „Globale Einstellungen“

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.
Authentifizierungs-verfahren		**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 externem 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 97: WBM-Seite „IEEE 802.1x“ – Register „Globale Einstellungen“

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 externem 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.	
Authentifizierungs-verfahren			In diesen Eingabefeldern werden der User-Name und das Passwort angezeigt, ergänzt oder gelöscht.	
		Keiner	Haben Sie im Auswahlfeld „Keiner“ 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.
		Ergänzen	Password:	Haben Sie im Auswahlfeld „Ergänzen“ gewählt, können Sie den User Name und das Password ändern.
Globaler Status				
Parameter		**Standardwert**	**Beschreibung**	
Status		Ausschalten Einschalten	In diesem Anzeigefeld wird angezeigt, ob die IEEE-802.1x-Authentifizierung aktiviert oder deaktiviert ist.	
Authentifizierungs-verfahren		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



Port	IEEE 802.1x Status	Control-Direction	Erneute Authentifizierung	Port-Control-Mode	Gust-VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
2	Ausschalten	Beide	Ausschalten	Auto	Ausschalten	2	3600	20	30	16
3	Ausschalten	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

Abbildung 94: WBM-Seite „IEEE-802.1x“ – Register „Port-Einstellungen“

Tabelle 98: 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 Pakete verworfen werden sollen.
		Eingang	Wählen Sie im Auswahlfeld „Eingang“, wenn nach der fehlgeschlagenen IEEE-802.1x-Port-Authentifizierung eines Benutzers nur am Port eingehende Pakete 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 Pakete weitergeleitet werden.
Gast-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 98: 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 98: WBM-Seite „IEEE-802.1x“ – Register „Port-Einstellungen“

Port-Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 **...** 10	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.
Gast-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-Sicherheit

Hinweis **Weitere Information**

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

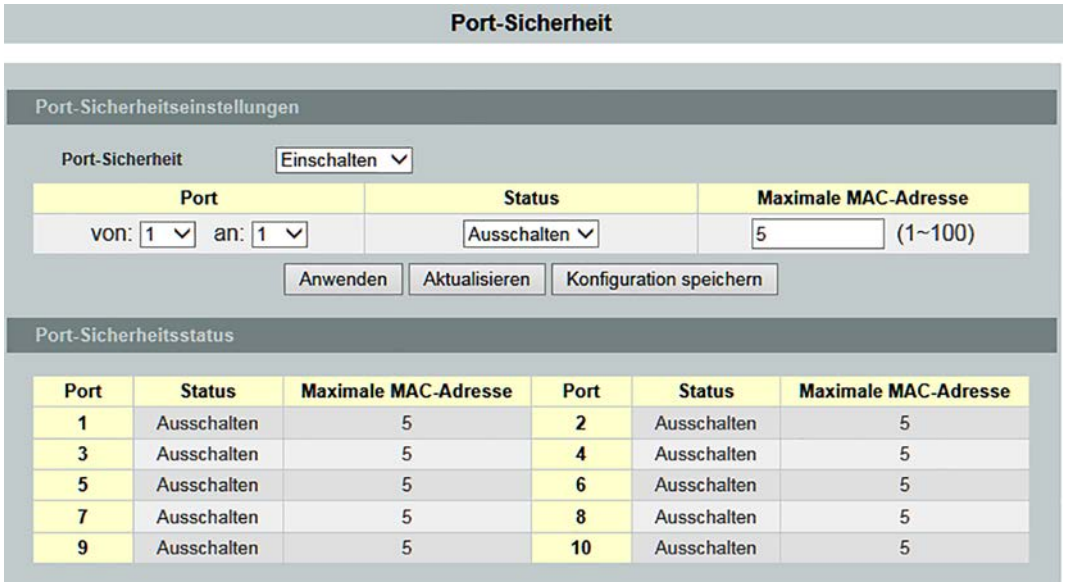


Abbildung 95: WBM-Seite „Port-Sicherheit“

Tabelle 99: WBM-Seite „Port-Sicherheit“

Port-Sicherheitseinstellungen			
Parameter		**Standardwert**	**Beschreibung**
Port-Sicherheit		**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 (1~30)		**5**	Geben Sie im Eingabefeld die maximale Anzahl der MAC-Adressen pro Schnittstelle ein.
Port-Sicherheitsstatus			
Parameter		**Standardwert**	**Beschreibung**
Port		1 … 10	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 … 30	In dieser Spalte wird die maximale Anzahl von MAC-Adressen angezeigt.

9.5 Monitor

9.5.1 Alarminformationen

Hinweis

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

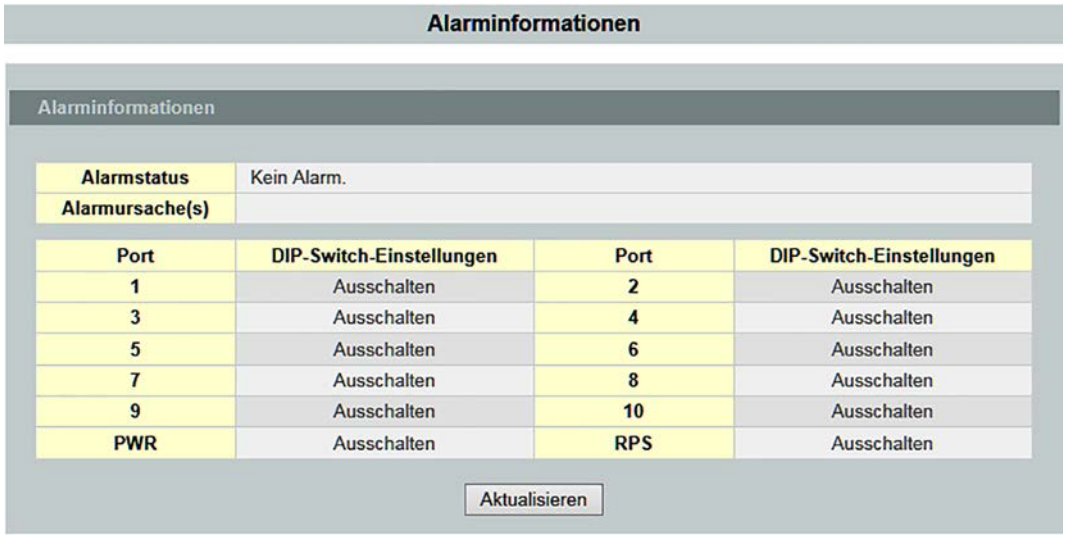


Abbildung 96: WBM-Seite „Alarminformationen“

Tabelle 100: WBM-Seite „Alarminformationen“

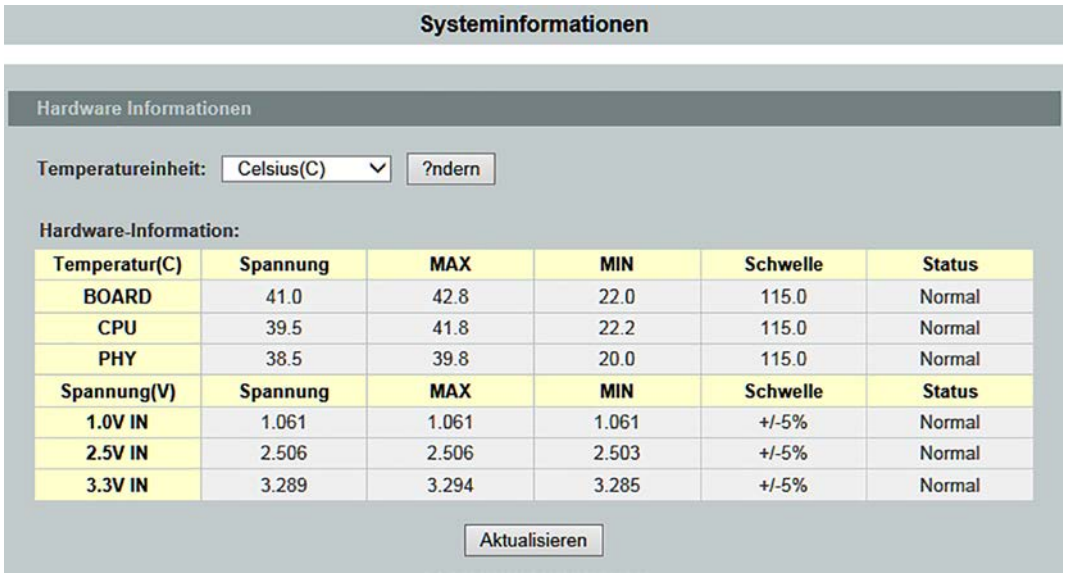
Alarminformationen		
Parameter	**Standardwert**	**Beschreibung**
Alarmstatus		In diesem Anzeigefeld wird angezeigt, ob Alarmereignisse stattgefunden haben.
Alarmursache		In diesem Anzeigefeld werden die Details zu den Alarmereignissen angezeigt.
Port	0 … 10 PWR RPS	In dieser Spalte wird die Bezeichnung des DIP-Schalters angezeigt.
DIP-Switch-Einstellungen	Einschalten Ausschalten	In dieser Spalte wird der aktuelle Status des DIP-Schalters angezeigt.

9.5.2 Systeminformationen

Hinweis

Weitere Information

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



Temperatur(C)	Spannung	MAX	MIN	Schwelle	Status
BOARD	41.0	42.8	22.0	115.0	Normal
CPU	39.5	41.8	22.2	115.0	Normal
PHY	38.5	39.8	20.0	115.0	Normal
Spannung(V)	**Spannung**	**MAX**	**MIN**	**Schwelle**	**Status**
1.0V IN	1.061	1.061	1.061	+/-5%	Normal
2.5V IN	2.506	2.506	2.503	+/-5%	Normal
3.3V IN	3.289	3.294	3.285	+/-5%	Normal

Abbildung 97: WBM-Seite „Systeminformationen“

Tabelle 101: WBM-Seite „Systeminformationen“

Hardware-Informationen		
Parameter	**Standardwert**	**Beschreibung**
Temperatureinheit	**Celsius (C)**	Wählen Sie Sie im Auswahlfeld „Celsius (C)“, wenn Sie die Temperatur in Celsius anzeigen wollen.
	Fahrenheit (F)	Wählen Sie Sie im Auswahlfeld „Fahrenheit (F)“, wenn Sie die Temperatur in Fahrenheit anzeigen wollen.
Hardware-Information		
Parameter	**Standardwert**	**Beschreibung**
Temperatur (C)		
Aktuell		In dieser Spalte wird die aktuelle Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
MAX		In dieser Spalte wird die maximale Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
MIN		In dieser Spalte wird die minimale Temperatur der Hauptplatine „BOARD“, der „CPU“ und dem MAC-Chip „PHY“ angezeigt.
Schwelle		In dieser Spalte wird die eingestellte Schwelle angezeigt.
Status		In dieser Spalte wird der Status angezeigt.
Spannung (V)		
Aktuell		In dieser Spalte wird die aktuelle Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
MAX		In dieser Spalte wird die maximale Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
MIN		In dieser Spalte wird die minimale Spannung für die Eingänge „1,0 V IN“, „2,5 V IN“ und „3,3 V IN“ angezeigt.
Schwelle		In dieser Spalte wird die eingestellte Schwelle angezeigt.
Status		In dieser Spalte wird der Status angezeigt.

9.5.3 Port-Statistik

Hinweis **Weitere Information**

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

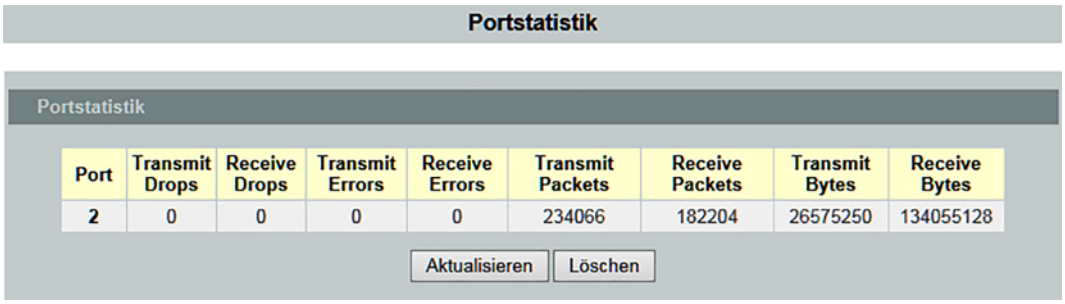


Abbildung 98: WBM-Seite „Port-Statistik“

Tabelle 102: WBM-Seite „Port-Statistik“

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

9.5.4 Port-Auslastung

Hinweis

Weitere Information

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

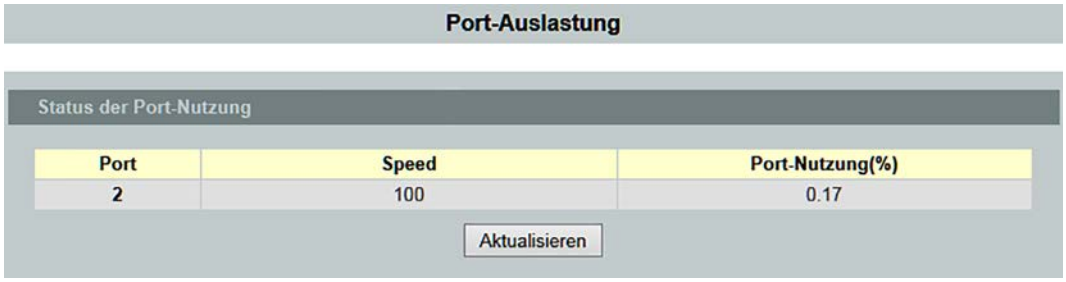


Abbildung 99: WBM-Seite „Port-Auslastung“

Tabelle 103: WBM-Seite „Port-Auslastung“

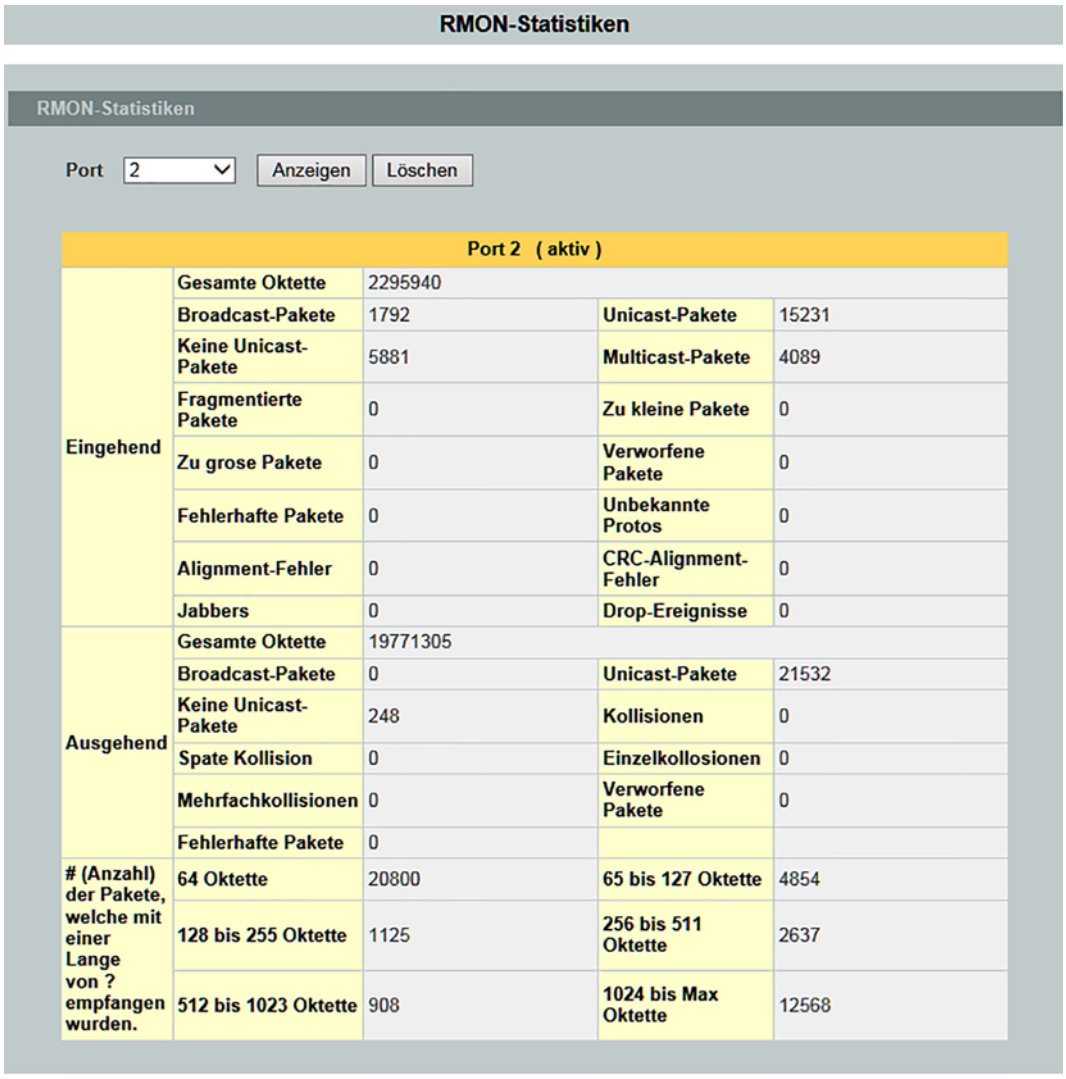
Status der Port-Nutzung		
Parameter	**Standardwert**	**Beschreibung**
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Speed		In dieser Spalte wird die Transfergeschwindigkeit angezeigt.
Port-Nutzung (%)		In dieser Spalte wird die prozentuale Auslastung der Bandbreite angezeigt.

9.5.5 RMON-Statistiken

Hinweis

Weitere Information

Weitere Informationen zu „RMON-Statistiken“ finden Sie im Kapitel „Funktionsbeschreibung“.



RMON-Statistiken

Port 2 (aktiv)

Eingehend	Gesamte Oktette	2295940		
	Broadcast-Pakete	1792	Unicast-Pakete	15231
	Keine Unicast-Pakete	5881	Multicast-Pakete	4089
	Fragmentierte Pakete	0	Zu kleine Pakete	0
	Zu grose Pakete	0	Verworfene Pakete	0
	Fehlerhafte Pakete	0	Unbekannte Protos	0
	Alignment-Fehler	0	CRC-Alignment-Fehler	0
	Jabbers	0	Drop-Ereignisse	0
Ausgehend	Gesamte Oktette	19771305		
	Broadcast-Pakete	0	Unicast-Pakete	21532
	Keine Unicast-Pakete	248	Kollisionen	0
	Spate Kollision	0	Einzelkollosionen	0
	Mehrfachkollisionen	0	Verworfene Pakete	0
	Fehlerhafte Pakete	0		
# (Anzahl) der Pakete, welche mit einer Lange von ? empfangen wurden.	64 Oktette	20800	65 bis 127 Oktette	4854
	128 bis 255 Oktette	1125	256 bis 511 Oktette	2637
	512 bis 1023 Oktette	908	1024 bis Max Oktette	12568

Abbildung 100: WBM-Seite „RMON-Statistiken“

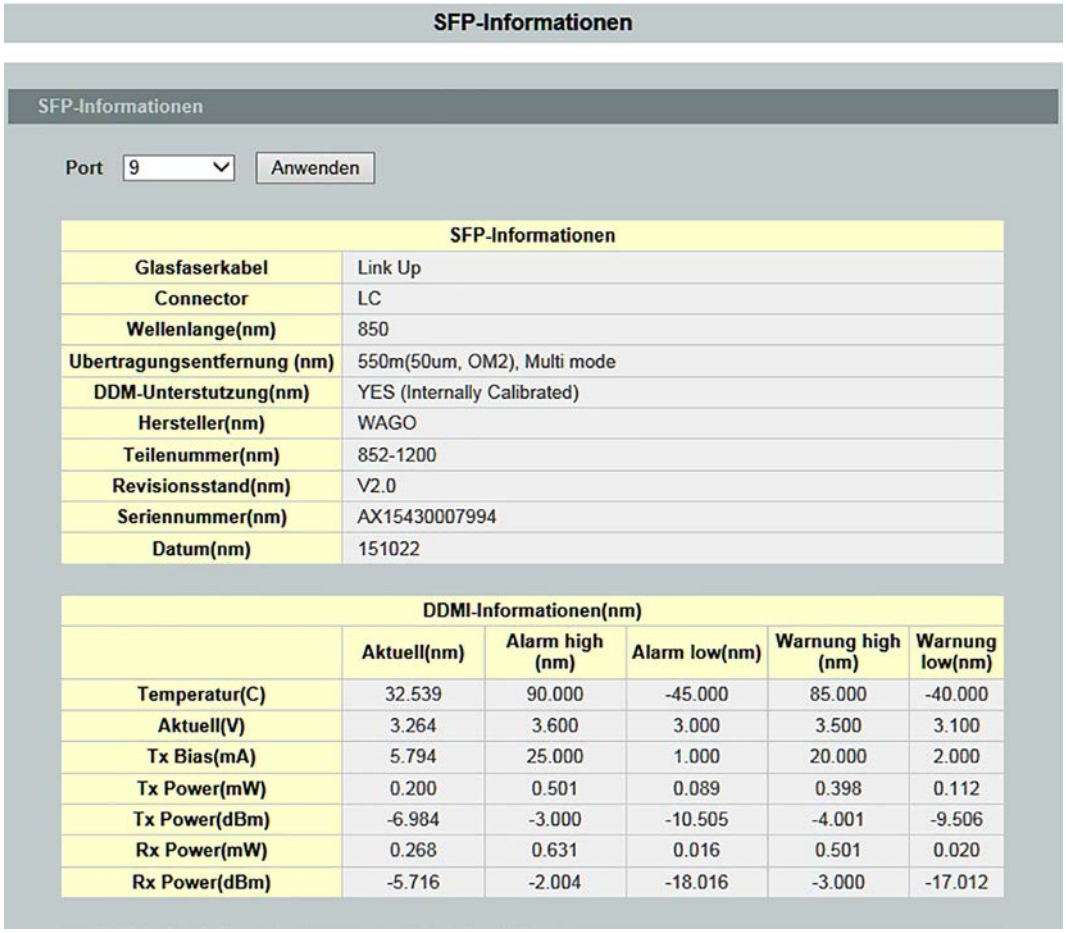
Tabelle 104: WBM-Seite „RMON-Statistiken“

RMON-Statistiken			
Parameter		**Standardwert**	**Beschreibung**
Port		**-**	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie keine Statistik ansehen möchten.
		1 … 10 Alle	Wählen Sie im Auswahlfeld einen Port oder alle Ports aus, für den (die) Sie die RMON-Statistiken anzeigen möchten.
Ausgewählter Port (s) (aktiv)			
Parameter		**Standardwert**	**Beschreibung**
Ein-gehend	Gesamte Oktette		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt.
	Broadcast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Broadcast-Pakete angezeigt.
	Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Unicast-Pakete angezeigt.
	Keine Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Summe der Broadcast-Pakete und Multicast-Pakete angezeigt.
	Multicast-Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Multicast-Pakete angezeigt.
	Fragmentierte Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen fragmentierten Datenpakete angezeigt.
	Zu kleine Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu kleinen Datenpakete angezeigt.
	Zu große Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen zu großen Datenpakete angezeigt.
	Verworfene Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die verworfenen wurden.
	Fehlerhafte Pakete		In diesem Anzeigefeld wird die Anzahl der auf dem Port empfangenen Datenpakete angezeigt, die fehlerhaft waren.
	Unbekannte Protos		In diesem Anzeigefeld wird die Anzahl der von diesem Port empfangenen Pakete angezeigt, die als Ziel ein unbekanntes oder nicht unterstütztes Protokoll enthielten.
	Alignment-fehler		In diesem Anzeigefeld wir die Anzahl der empfangenen Datenpakete angezeigt, bei der die Gesamtzahl an Bits eines empfangenen Frames nicht durch 8 teilbar ist.
	CRC-Alignment-fehler		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete mit Checksummenfehler angezeigt.
	Jabbers		In diesem Anzeigefeld wird die Anzahl der von diesem Port empfangenen Jabber angezeigt.
	Drop-Ereignisse		In diesem Anzeigefeld wird die Anzahl der verworfenen Datenpakete angezeigt.

Tabelle 104: WBM-Seite „RMON-Statistiken“

Aus-gehend	Gesamte Oktette		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt.
	Broadcast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Broadcast-Pakete angezeigt.
	Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Keine Unicast-Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Unicast-Pakete angezeigt.
	Kollisionen		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	Späte Kollision		In diesem Anzeigefeld wird Anzahl der Datenpakete angezeigt, die gesendet werden sollten, kollidiert sind und verworfen wurden.
	Einzel-kollisionen		In diesem Anzeigefeld wird die Anzahl der Einzelkollisionen der gesendeten Datenpakete angezeigt.
	Mehrfach-kollisionen		In diesem Anzeigefeld wird die Anzahl der Mehrfachkollisionen der gesendeten Datenpakete angezeigt.
	Verworfene Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die verworfenen wurden.
	Fehlerhafte Pakete		In diesem Anzeigefeld wird die Anzahl der von dem Port gesendeten Datenpakete angezeigt, die fehlerhaft waren.
#(Anzahl) der Pakete, welche mit einer Länge von ? empfan-gen wurden.	64 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 64 Oktetten hatten.
	65 bis 127 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 65 bis 127 Oktetten hatten.
	128 bis 255 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 128 bis 255 Oktetten hatten.
	256 bis 511 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 256 bis 511 Oktetten hatten.
	512 bis 1023 Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von 512 bis 1023 Oktetten hatten.
	1024 bis max. Oktette		In diesem Anzeigefeld wird die Anzahl der empfangenen Datenpakete angezeigt, die eine Länge von mehr als 1024 Oktetten hatten.

9.5.6 SFP-Informationen



SFP-Informationen	
Glasfaserkabel	Link Up
Connector	LC
Wellenlange(nm)	850
Ubertragungsentfernung (nm)	550m(50um, OM2), Multi mode
DDM-Unterstutzung(nm)	YES (Internally Calibrated)
Hersteller(nm)	WAGO
Teilenummer(nm)	852-1200
Revisionsstand(nm)	V2.0
Seriennummer(nm)	AX15430007994
Datum(nm)	151022

DDMI-Informationen(nm)					
	Aktuell(nm)	Alarm high (nm)	Alarm low(nm)	Warnung high (nm)	Warnung low(nm)
Temperatur(C)	32.539	90.000	-45.000	85.000	-40.000
Aktuell(V)	3.264	3.600	3.000	3.500	3.100
Tx Bias(mA)	5.794	25.000	1.000	20.000	2.000
Tx Power(mW)	0.200	0.501	0.089	0.398	0.112
Tx Power(dBm)	-6.984	-3.000	-10.505	-4.001	-9.506
Rx Power(mW)	0.268	0.631	0.016	0.501	0.020
Rx Power(dBm)	-5.716	-2.004	-18.016	-3.000	-17.012

Abbildung 101: WBM-Seite „SFP-Informationen“

Tabelle 105: WBM-Seite „SFP-Informationen“

SFP-Informationen		
Parameter	**Standardwert**	**Beschreibung**
Port	**-**	Wählen Sie im Auswahlfeld „-“ aus, wenn Sie kein SFP-Modul gesteckt haben
	9, 10	Wählen Sie im Auswahlfeld den Port aus, in dem Sie ein SFP-Modul gesteckt haben.
SFP-Informationen		
Parameter	**Standardwert**	**Beschreibung**
Glasfaserkabel		In diesem Anzeigefeld wird angezeigt, ob ein Glasfaserkabel angeschlossen ist.
Connector		In diesem Anzeigefeld wird der Code für den optischen Anschlusssteckertyp angezeigt.
Wellenlänge (nm)		In diesem Anzeigefeld wird die Wellenlänge angezeigt.
Übertragungsentfernung (nm)		In diesem Anzeigefeld wird die Übertragungsentfernung angezeigt.
DDM-Unterstützung (nm)		In diesem Anzeigefeld wird angezeigt, ob das SFP-Modul das DDM („**D**ynamic **D**evice **M**apping“) unterstützt.
Hersteller (nm)		In diesem Anzeigefeld wird der Name des SFP-Anbieters angezeigt.
Teilenummer (nm)		In diesem Anzeigefeld wird die Teilenummer angezeigt.
Revisionsstand (nm)		In diesem Anzeigefeld wird der Revisionsstand der Teilenummer angezeigt.
Seriennummer (nm)		In diesem Anzeigefeld wird die Seriennummer (ASCII) angezeigt.
Datum (nm)		In diesem Anzeigefeld wird das Datum der Version angezeigt.
DDMI-Informationen (nm)		
Parameter	**Standardwert**	**Beschreibung**
Aktuell (nm)		In dieser Spalte werden die aktuellen Werte der Temperatur, der Spannung, von Tx Bias, Tx Power und Rx Power angezeigt.
Alarm high (nm)		In dieser Spalte werden die „Alarm high“-Werte der Temperatur, der Spannung, von Tx Bias, Tx Power und Rx Power angezeigt.
Alarm low (nm)		In dieser Spalte werden die „Alarm low“-Werte der Temperatur, der Spannung, von Tx Bias, Tx Power und Rx Power angezeigt.
Warnung high (nm)		In dieser Spalte werden die „Warnung high“-Werte der Temperatur, der Spannung, von Tx Bias, Tx Power und Rx Power angezeigt.
Warnung low (nm)		In dieser Spalte werden die „Warnung low“-Werte der Temperatur, der Spannung, von Tx Bias, Tx Power und Rx Power angezeigt.

9.5.7 Traffic-Monitor

Hinweis

Weitere Information

Weitere Informationen zum „Traffic-Monitor“ finden Sie im Kapitel „Funktionsbeschreibung“.

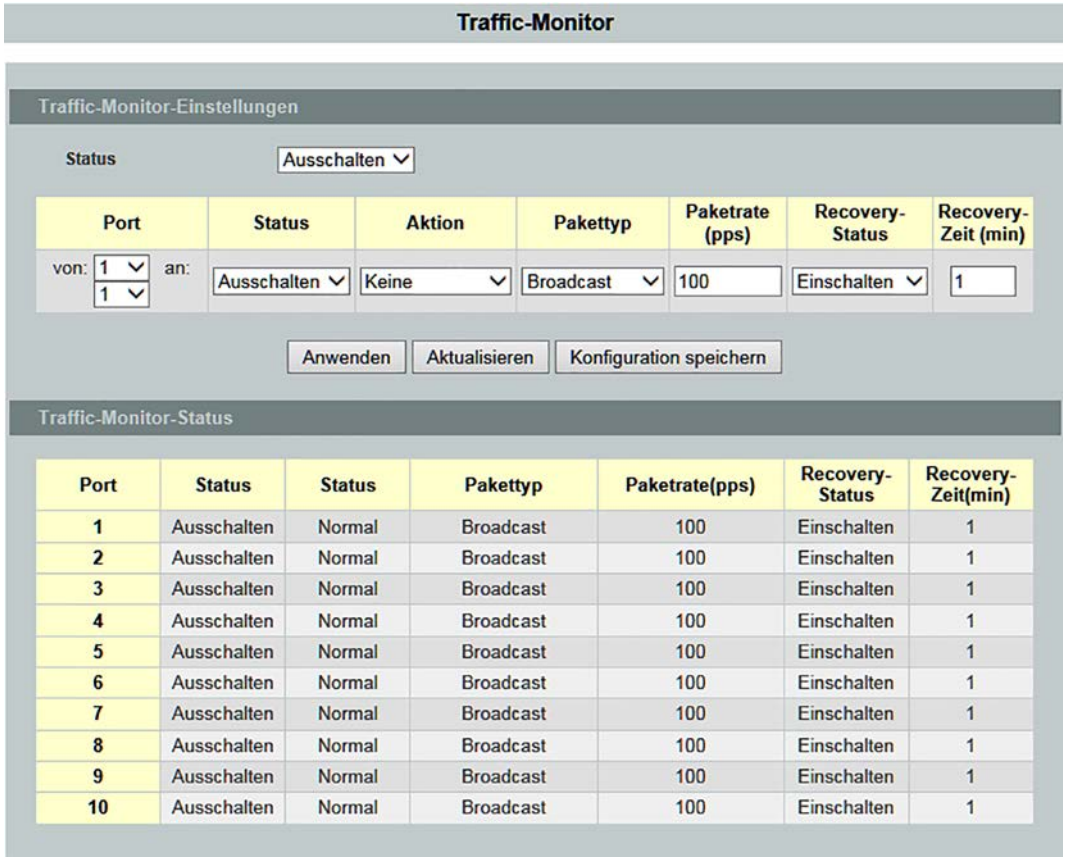


Abbildung 102: WBM-Seite „Traffic-Monitor“

Tabelle 106: 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.
		Unblock	Wählen Sie im Auswahlfeld „Nicht blockiert“, wenn Sie die Blockierung von Ports aufheben möchten.
Pakettyp		**Broadcast**	Wählen Sie im Auswahlfeld „Broadcast“, wenn Sie diesen als Pakettyp überwachen möchten.
		Multicast	Wählen Sie im Auswahlfeld „Multicast“, wenn Sie diesen als Pakettyp überwachen möchten.
		Bcast+Mcast	Wählen Sie im Auswahlfeld „Bcast+Mcast“, wenn Sie diese beiden als Pakettypen überwachen möchten.
Paketrate (pps)			Geben Sie im Eingabefeld die Paketrate ein, die überwacht werden soll.
Recovery-Status		**Einschalten**	Wählen Sie im Auswahlfeld „Einschalten“, wenn Sie die Recovery-Funktion beim „Traffic-Monitor“ für den Port oder Port-Bereich aktivieren möchten.
		Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, wenn Sie die Recovery-Funktion beim „Traffic-Monitor“ für den Port oder Port-Bereich deaktivieren möchten.
Recovery-Zeit (min)		**1** … 60	Geben Sie im Eingabefeld einen Wert für die „Recovery-Time“ beim „Traffic-Monitor“ ein.
Traffic-Monitor-Status			
Parameter		**Standardwert**	**Beschreibung**
Port		1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Status		Ausschalten Einschalten	In dieser Spalte wird der Status des spezifischen Port angezeigt.
Status		Normal	In dieser Spalte wird der Status des Betriebszustandes angezeigt.
Pakettyp		Broadcast Multicast Bcast+Mcast	In dieser Spalte wird der Typ des Datenpaketes angezeigt.
Paketrate (pps)			In dieser Spalte wird die gewählte Paketrate angezeigt.
Recovery-Status		Einschalten Ausschalten	In dieser Spalte wird der Status der gewählten Recovery-Funktion angezeigt.
Recovery-Zeit (min)		1 … 60	In dieser Spalte wird die gewählte Recovery-Zeit angezeigt.

9.6 Management

9.6.1 SNMP

9.6.1.1 SNMP

9.6.1.1.1 SNMP-Einstellungen

Hinweis **Weitere Information**

Weitere Informationen zu „SNMP“ (**S**imple **N**etwork **M**anagement **P**rotocol) finden Sie im Kapitel „Funktionsbeschreibung“.

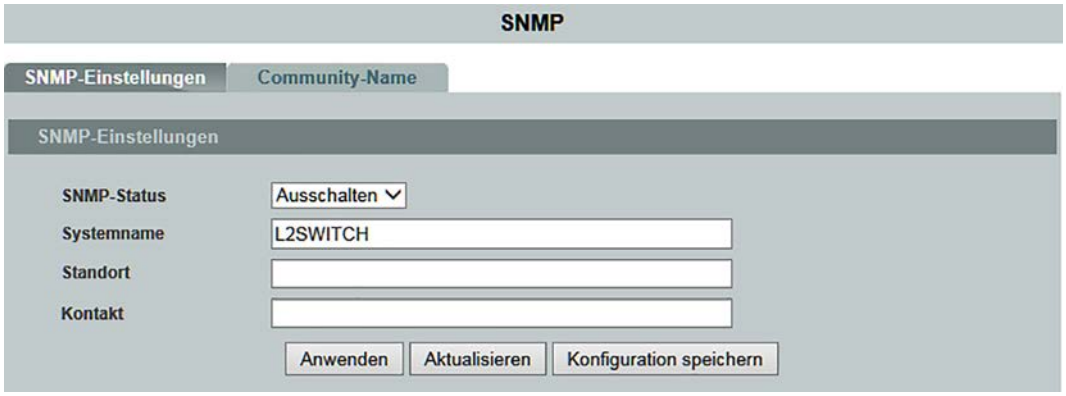


Abbildung 103: WBM-Seite „SNMP“ – Register „SNMP-Einstellungen“

Tabelle 107: 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	**192.168.0.254**	Geben Sie im Eingabefeld die IP-Adresse (Standortinformation) des Switches in Dezimalpunktschreibweise ein.
Kontakt	**255.255.255.0**	Geben Sie im Eingabefeld die IP-Subnetzmaske des Switches in Dezimalpunktschreibweise ein.

9.6.1.1.2 Community-Name

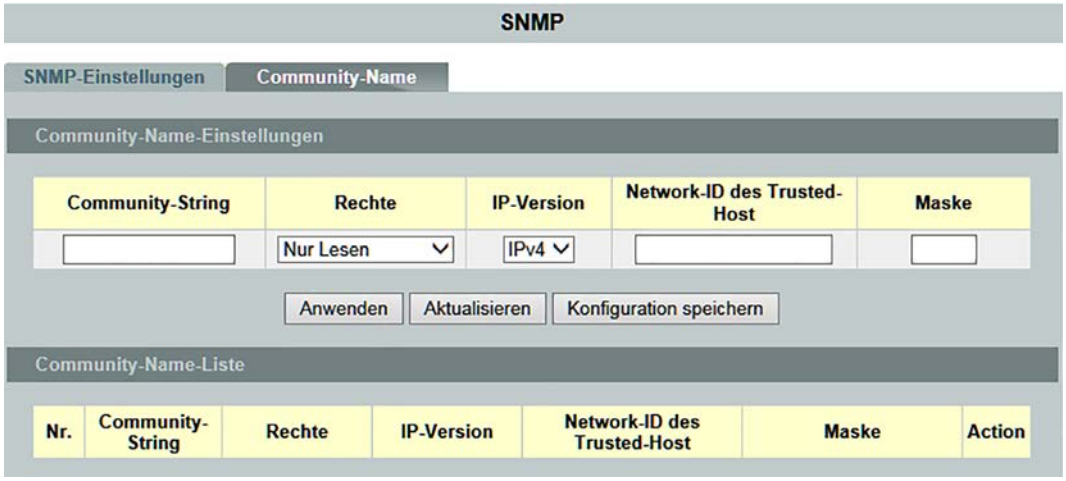


Abbildung 104: WBM-Seite „SNMP“ – Register „Community-Name“

Tabelle 108: 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).
Maske		Geben Sie im Eingabefeld die IP-Adresse der Subnetzmaske der dezentralen SNMP-Managementstation in Dezimalpunktschreibweise ein (z. B. 255.255.255.0).
Community-Name-Liste		
Parameter	**Standardwert**	**Beschreibung**
Nr.		In dieser Spalte wird die Nummer der „Community“ angezeigt. Sie dient ausschließlich der Identifizierung. Klicken Sie auf eine Nummer, um die Einstellung einer spezifischen „Community“ zu modifizieren.
Community-String		In dieser Spalte wird der „SNMP-Community-String“ angezeigt. Dies ist ein Textelement, das als Passwort fungiert.
Rechte	Nur Lesen, Lesen/ Schreiben	In dieser Spalte werden die Berechtigungen für den „SNMP-Community-String“ angezeigt.
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.
Maske		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

9.6.1.2.1 Trap-Receiver-Einstellungen

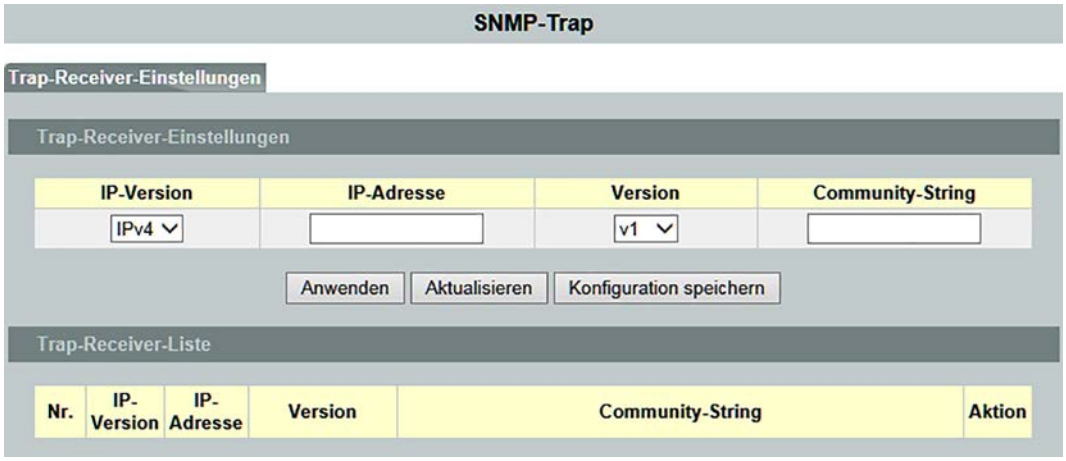


Abbildung 105: WBM-Seite „SNMP-Trap“ – Register „Trap-Receiver-Einstellungen“

Tabelle 109: 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.

9.6.1.3 Auto-Provision

Hinweis

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

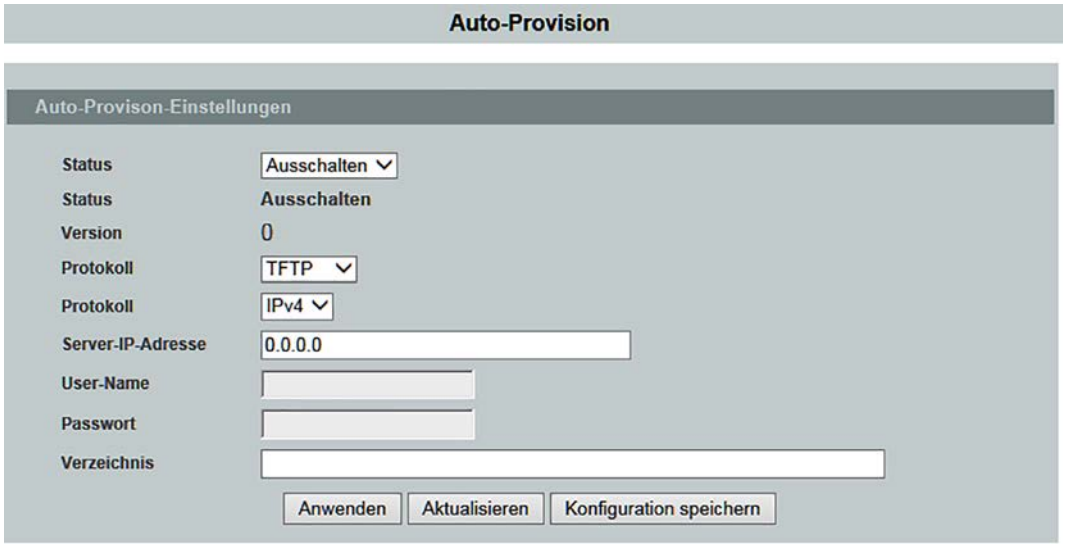


Abbildung 106: WBM-Seite „Auto-Provision“

Tabelle 110: 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 wir der Status der „Auto-Provision“ angezeigt.
Version	**0**	In diesem Anzeigefeld wird die Version angezeigt.
Protokoll	**FTP**	Wählen Sie im Auswahlfeld „FTP“ („**F**ile **T**ransfer **P**rotocol“), wenn Sie diesen Typ als Auto-Provision-Server wählen möchten.
	TFTP	Wählen Sie im Auswahlfeld „TFTP“ („**T**rivial **F**ile **T**ransfer **P**rotocol“), wenn Sie diesen Typ als Auto-Provision-Server wählen möchten.
	HTTP	Wählen Sie im Auswahlfeld „HTTP“ („**H**yper**t**ext **T**ransfer **P**rotocol“), 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.
Passwort		Geben Sie im Eingabefeld das Passwort für den FTP-Server ein.
Verzeichnis		Wählen Sie in diesem Eingabefeld die Ordnerstruktur des FTP-Servers aus.

9.6.1.3.1 Mail-Alarm

Hinweis

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

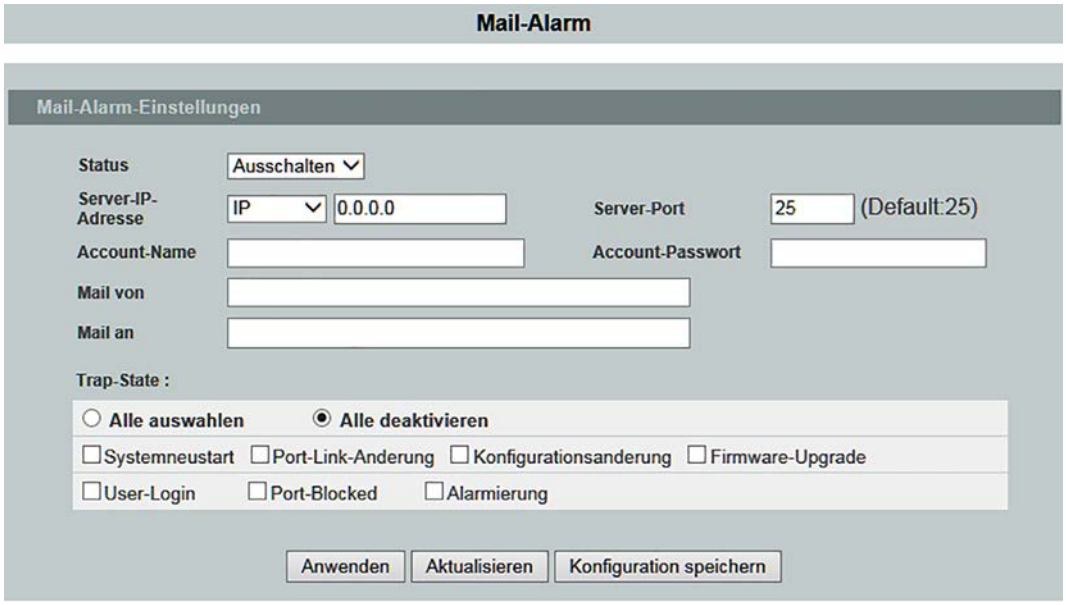


Abbildung 107: WBM-Seite „Mail-Alarm“

Tabelle 111: 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 Domian-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 State	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-Blocked	☐	☐	Es ist der Zustand „Port-Blocked“ deaktiviert.
			☑	Es ist der Zustand „Port-Blocked“ aktiviert.
	Alarmierung	☐	☐	Es ist der Zustand „Alarmierung“ deaktiviert.
			☑	Es ist der Zustand „Alarmierung“ aktiviert.

9.6.1.3.2 Wartung

9.6.1.3.3 Konfiguration

Abbildung 108: WBM-Seite „Wartung“ – Register „Konfiguration“

Konfiguration Speichern

- Klicken Sie auf die Schaltfläche **[Speichern]**, um die aktuellen Einstellungen im NV-RAM (Flash) zu speichern.

Upload und Download der Konfiguration

Führen Sie die nachfolgenden Schritte aus, um die Konfigurationsdatei auf Ihrem PC zu speichern.

1. Wählen Sie „Download drücken, um die Konfigurationsdatei auf Ihrem PC zu speichern“.
2. Klicken Sie auf die Schaltfläche **[Download]**, um den Download zu beginnen.

Führen Sie die nachfolgenden Schritte aus, um die Konfigurationsdatei vom PC auf den Switch hochzuladen.

1. Wählen Sie „Die Konfigurationsdatei auf den Switch laden“.

2. Klicken Sie auf die Schaltfläche **[Datei auswählen]**.
   Wählen Sie die Konfigurationsdatei mit Angabe des vollständigen Pfads aus.

3. Klicken Sie auf die Schaltfläche **[Upload]**, um das Hochladen zu beginnen.

Konfiguration zurücksetzen

- Klicken Sie auf die Schaltfläche **[Reset]**, um die Konfiguration des Switches auf die Werkseinstellungen zurückzusetzen.

Der Konfigurationsstatus

Wurden Änderungen an den Konfigurationen vorgenommen, wird „Die Konfigurationen wurden verändert“ angezeigt.

Wurden keine Änderungen an den Konfigurationen vorgenommen, wird „Die User Konfigurationsdatei ist auf default. Die Konfigurationen sind Standardwerte.“ angezeigt.

9.6.2 Firmware

Abbildung 109: 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.

9.6.3 Rebooten

Abbildung 110: WBM-Seite „Wartung“ – Register „Rebooten“

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:

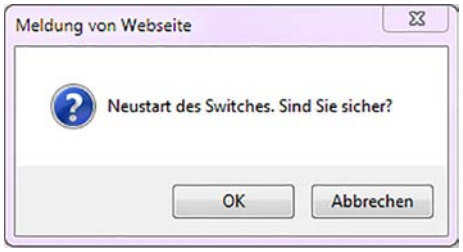


Abbildung 111: WBM-Seite „Wartung“ – Register „Rebooten“ – Meldung

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 Protokolle

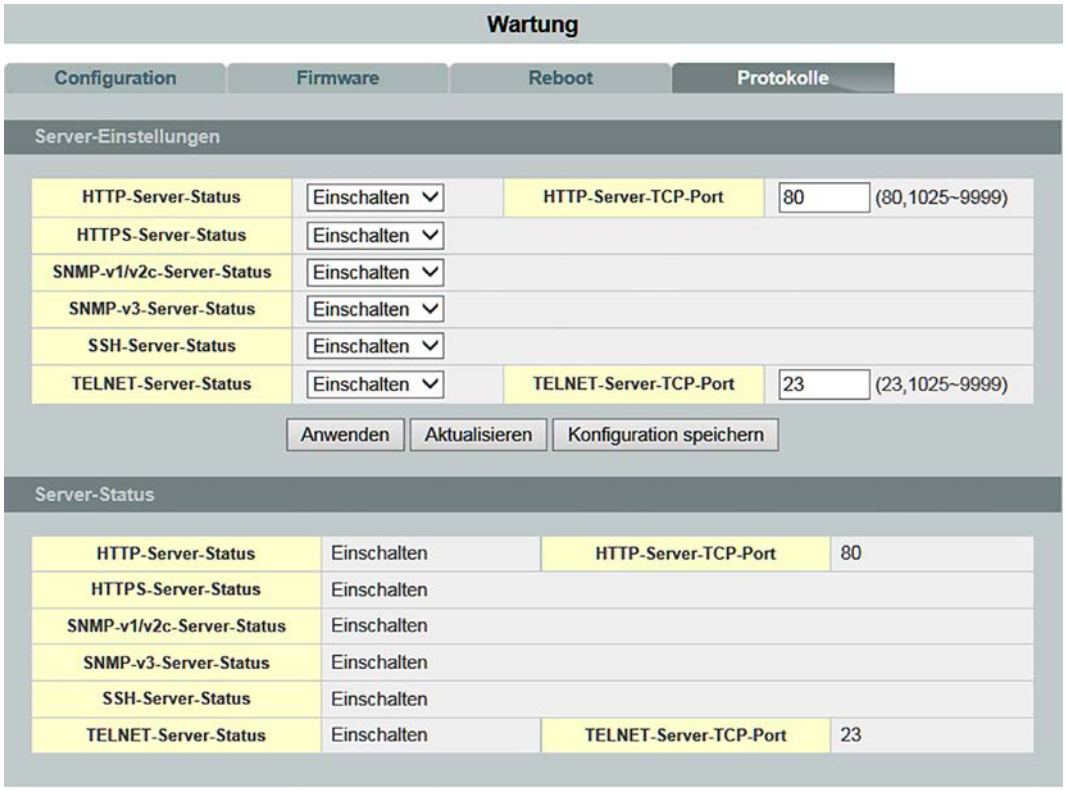


Abbildung 112: WBM-Seite „Wartung“ – Register „Protokolle“

Tabelle 112: WBM-Seite „Wartung“ – Register „Protokolle“

Server-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
HTTP-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „HTTP-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „HTTP-Server“ zu deaktivieren.
HTTP-Server-TCP-Port (80, 1025~9999)	**80** 1025 … 9999	Geben Sie im Eingabefeld den „HTTP-Server-TCP-Port“ ein.
HTTPS-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „HTTPS-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „HTTPS-Server“ zu deaktivieren.
SNMP-v1/v2c-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „SNMP-v1/v2c-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SNMP-v1/v2c-Server“ zu deaktivieren.
SNMP-v3-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „SNMP-v3-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SNMP-v3-Server“ zu deaktivieren.
SSH-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „SSH-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „SSH-Server“ zu deaktivieren.
Telnet-Server-Status	**Einschalten**	Wählen Sie „Einschalten“, um den „Telnet-Server“ zu aktivieren.
	Ausschalten	Wählen Sie „Ausschalten“, um den „Telnet-Server“ zu deaktivieren.
Telnet-Server-TCP-Port (23, 1025~9999)	**23** 1025 … 9999	Geben Sie im Eingabefeld den „Telnet-Server-TCP-Port“ ein.
Server-Status		
Parameter	**Standardwert**	**Beschreibung**
HTTP-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des HTTP-Servers angezeigt.
HTTP-Server-TCP-Port	80 1025 … 9999	In diesem Anzeigefeld wird der HTTP-Server-TCP-Port angezeigt.
HTTPS-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des HTTPS-Servers angezeigt.
SNMP-v1/v2c-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SNMP-v1/v2c-Servers angezeigt.
SNMP-v3-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SNMP-v3-Servers angezeigt.
SSH-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des SSH-Servers angezeigt.
Telnet-Server-Status	Einschalten Ausschalten	In diesem Anzeigefeld wird der Status des Telnet-Servers angezeigt.
Telnet-Server-TCP-Port	23 1025 … 9999	In diesem Anzeigefeld wird der Telnet-Server-TCP-Port angezeigt.

9.6.4.1 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.

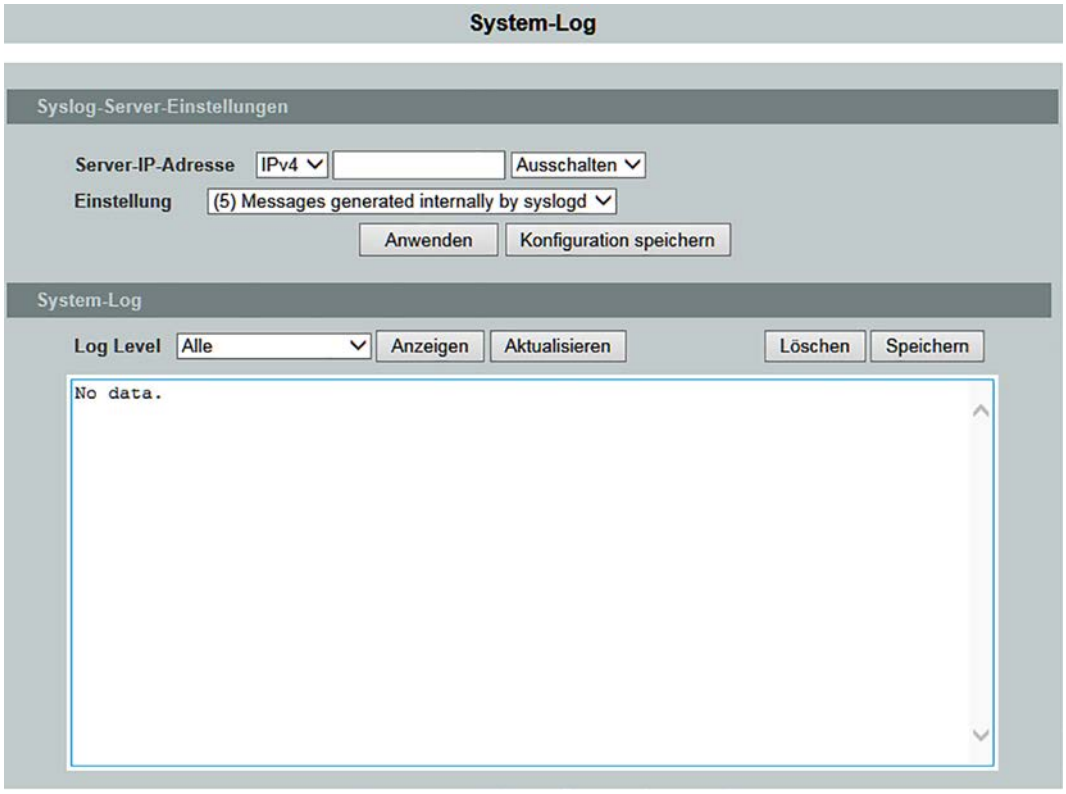


Abbildung 113: WBM-Seite „System-Log“

Tabelle 113: WBM-Seite „System-Log“

Syslog-Server-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
Server-IP-Adresse	**IPv4**	Wählen Sie im Auswahlfeld „IPv4“, wenn Sie diese Version des Internetprotokolls wählen möchten.
	IPv6	Wählen Sie im Auswahlfeld „IPv6“, wenn Sie diese Version des Internetprotokolls wählen möchten.
		Geben Sie im Eingabefeld die IP-Adresse in Dezimalpunktschreibweise ein (z. B.: 192.168.1.1).
	Ausschalten	Wählen Sie im Auswahlfeld „Ausschalten“, damit der Switch alle neuen Protokollnachrichten nicht an den Syslog-Server sendet.
	Einschalten	Wählen Sie im Auswahlfeld „Einschalten“, damit der Switch alle neuen Protokollnachrichten nicht an den Syslog-Server sendet.
Einstellung	(1) User-level messages	Wählen Sie im Auswahlfeld „(1) User-level messages“, wenn Sie die benutzerspezifischen Meldungen anzeigen wollen.
	(5) Messages generated internally by syslogd	Wählen Sie im Auswahlfeld „(5) Messages generated internally by syslogd“, wenn Sie die intern von syslog erzeugten Meldungen anzeigen wollen.
	(14) Log alert	
	(16) Local use 0	
	(17) Local use 1	
	(18) Local use 2	
	(19) Local use 3	
	(20) Local use 4	
	(21) Local use 5	
	(22) Local use 6	
	(23) Local use 7	
System-Log		
Parameter	**Standardwert**	**Beschreibung**
Log-Level	**Alle**	Wählen Sie im Auswahlfeld „Alle“, wenn Sie alle Protokollnachrichten anzeigen wollen.
	1:Alarm	Wählen Sie im Auswahlfeld „Alarm“, wenn Sie die Log-Meldungen anzeigen wollen.
	2:kritisch	Wählen Sie im Auswahlfeld „kritisch“, wenn Sie die kritischen Protokollnachricht anzeigen wollen.
	3:Fehler	Wählen Sie im Auswahlfeld „Fehler“, wenn Sie die Fehler anzeigen wollen.
	4:Warnung	Wählen Sie im Auswahlfeld „Warnung“, wenn Sie die Warnungen anzeigen wollen.
	5:Bekanntmachung	Wählen Sie im Auswahlfeld „Bekanntmachung“, wenn Sie die Bekanntmachungen anzeigen wollen.
	6:Information	Wählen Sie im Auswahlfeld „Information“, wenn Sie alle Informationen anzeigen wollen.

9.6.4.2 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:
Firmware-Version 01: User Name = „admin“
User Password = „Wago1951“
Firmware-Version 02: 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.

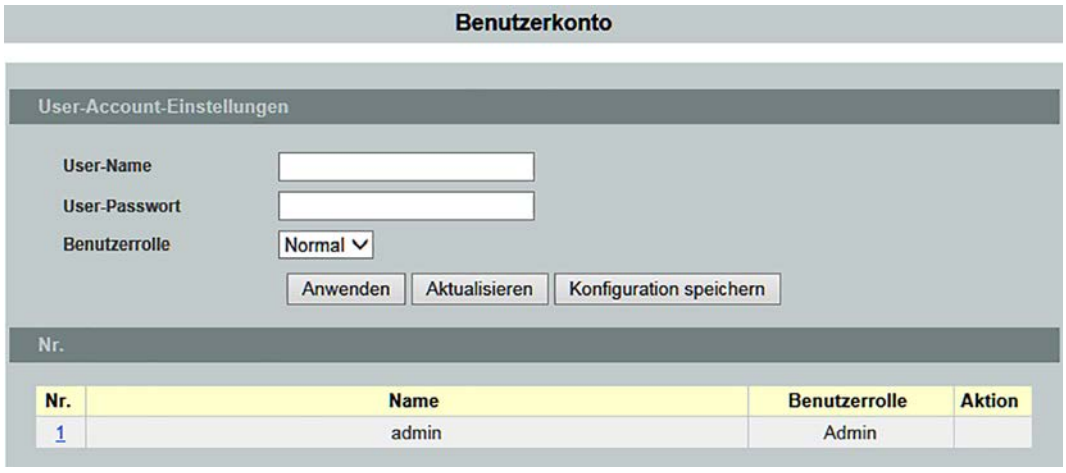


Abbildung 114: WBM-Seite „Benutzerkonto“

Tabelle 114: WBM-Seite „Benutzerkonto“

User-Account-Einstellungen		
Parameter	**Standardwert**	**Beschreibung**
User-Name		Geben Sie im Eingabefeld einen neuen Benutzernamen ein oder modifizieren Sie einen bereits bestehenden Benutzernamen.
User-Passwort		Geben Sie im Eingabefeld ein neues Passwort ein oder modifizieren Sie ein bereits bestehendes Passwort. Sie können bis zu 32 alphanumerische Zeichen oder Zahlen eintragen.
Benutzerrolle		In diesem Auswahlfeld wählen Sie die Art des Benutzerkontos aus.
	Normal	Wählen Sie im Auswahlfeld “Normal“, wenn Sie nur eine Leseberechtigung für dieses Benutzerkonto benötigen.
	Admin	Wählen Sie im Auswahlfeld “Admin“, wenn Sie eine Schreib- und Leseberechtigung für dieses Benutzerkonto benötigen.
Nr.		
Parameter	**Standardwert**	**Beschreibung**
Nr.		In dieser Spalte wird die Indexnummer eines Eintrags angezeigt.
Name		In dieser Spalte wird der Name des Benutzerkontos angezeigt.
Benutzerrolle		In dieser Spalte wird die Art des Benutzerkontos angezeigt.
Aktion		Klicken Sie auf die Schaltfläche **[Löschen]**, um ein Benutzerkonto zu löschen.
		Hinweis  **Löschen Administratorkonto** Das letzte Administratorkonto kann nicht gelöscht werden.

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:

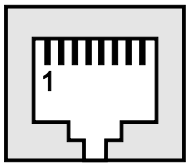


Abbildung 115: RJ-45 Anschlussbelegung

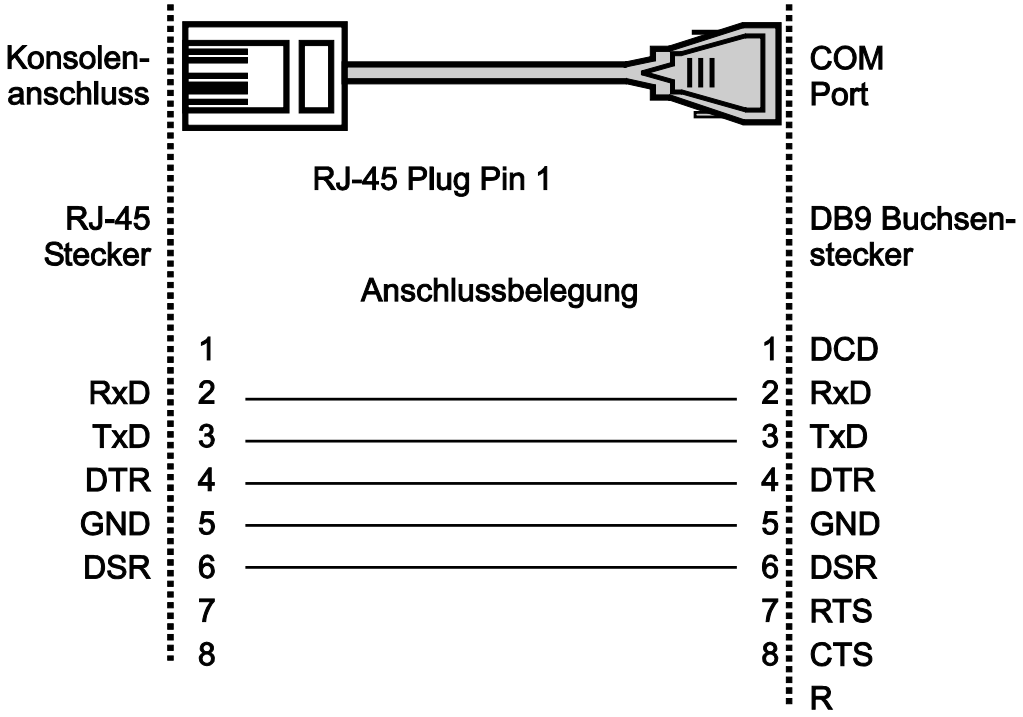


Abbildung 116: Anschlussbelegung RJ-45 zu DB9

10.2 RJ-45-Kabel

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

Tabelle 115: 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 Im Command Line Interface (CLI) konfigurieren

10.3.1 Systemstatus

10.3.1.1 Systeminformationen

Tabelle 116: CLI-Konfiguration „Systeminformationen“

Knoten	Befehl	Beschreibung
enable	show hostname	Mit diesem Befehl wird der Netzwerkname des Systems angezeigt.
enable	show interface eth0	Mit diesem Befehl werden die aktuellen Eth0-Konfigurationen angezeigt.
enable	show model	Mit diesem Befehl werden die Systeminformationen angezeigt.
enable	show running-config	Mit diesem Befehl werden die aktuellen Betriebskonfigurationen angezeigt.
enable	show system-info	Mit diesem Befehl werden CPU-Auslastung und Speicherinformationen des Systems angezeigt.
enable	show uptime	Mit diesem Befehl wird die Systembetriebszeit angezeigt.

10.3.2 Grundeinstellungen

10.3.2.1 System

Tabelle 117: CLI-Konfiguration „System“

Knoten	Befehl	Beschreibung
configure	reboot	Mit diesem Befehl wird das System neu gestartet.
configure	hostname STRINGS	Mit diesem Befehl wird der Netzwerkname des Systems definiert.
configure	interface eth0	Mit diesem Befehl wird der eth0-Schnittstellenknoten zur Konfiguration der System-IP eingetragen.
eth0	ip address A.B.C.D/M	Mit diesem Befehl werden die statische IP und die Subnetzmaske für das System konfiguriert.
eth0	ip address default-gateway A.B.C.D	Mit diesem Befehl wird das Default-Gateway des Systems konfiguriert.
eth0	ip dhcp client (disable|enable|renew)	Mit diesem Befehl wird die DHCP-Client-Funktion für das System konfiguriert. „Disable“ (Deaktivieren): Verwenden Sie eine statische IP-Adresse für den Switch. „Enable“ (Aktivieren) und „Renew“ (Erneuern): Verwenden Sie den DHCP-Client, um eine IP-Adresse vom DHCP-Server zu beziehen.
eth0	management vlan VLAN_ID	Mit diesem Befehl wird das Management-VLAN konfiguriert.

10.3.2.2 Jumbo Frame

Tabelle 118: CLI-Konfiguration „Jumbo Frame“

Knoten	Befehl	Beschreibung
enable	show jumboframe	Mit diesem Befehl werden die derzeitigen Einstellungen für „Jumbo Frames“ angezeigt.
configure	jumboframe (10240|1522|1536|1552|9216)	Mit diesem Befehl wird die maximale Byte-Anzahl für Frame-Größen konfiguriert.

10.3.2.3 SNTP

Tabelle 119: CLI-Konfiguration „SNTP“

Knoten	Befehl	Beschreibung
enable	show time	Mit diesem Befehl wird die aktuelle Uhrzeit- und Datumskonfiguration angezeigt.
configure	time HOUR:MINUTE:SECOND	Mit diesem Befehl wird die aktuelle Uhrzeit des Switches festgelegt. hour (Std.): 0-23 min (Min.): 0-59 sec (Sek.): 0-59 Hinweis: Wenn Sie die Sommerzeit erst nach Datum und Uhrzeit konfigurieren, wird der Switch die Sommerzeit anwenden.
configure	time date YEAR/MONTH/DAY	Mit diesem Befehl wird das aktuelle Datum des Switches festgelegt. year (Jahr): 1970- month (Monat): 1-12 day (Tag): 1-31
configure	time daylight-saving-time	Mit diesem Befehl wird die Sommerzeit aktiviert.
configure	time daylight-saving-time start-date <month> <day> <hour>	Mit diesem Befehl wird das Startdatum für die Sommerzeit festgelegt.
configure	time daylight-saving-time end-date <month> <day> <hour>	Mit diesem Befehl wird das Enddatum für die Sommerzeit festgelegt.
configure	no time daylight-saving-time	Mit diesem Befehl wird die Sommerzeit deaktiviert.
configure	time ntp-server IP_ADDRESS	Mit diesem Befehl wird die IP-Adresse des Zeitservers festgelegt.
configure	no time ntp-server	Mit diesem Befehl werden die NTP-Servereinstellungen deaktiviert.
configure	time timezone operator (+|-) hour (VALUE 0~14) min (VALUE 00 or 30)	Mit diesem Befehl wird der Zeitunterschied zwischen UTC (ehemals GMT) und der Zeitzone festgelegt.

Beispiel

L2SWITCH(config)#*time ntp-server 192.5.41.41*

L2SWITCH(config)#*time timezone operator + hour 8 min 0*

10.3.2.4 Management Host

Tabelle 120: CLI-Konfiguration „Management Host“

Knoten	Befehl	Beschreibung
enable	show interface eth0	Mit diesem Befehl werden alle eth0-Schnittstellenkonfigurationen angezeigt.
eth0	show	Mit diesem Befehl werden alle eth0-Schnittstellenkonfigurationen angezeigt.
eth0	management host A.B.C.D	Mit diesem Befehl wird eine Management-Host-Adresse hinzugefügt.
eth0	no management host A.B.C.D	Mit diesem Befehl wird eine Management-Host-Adresse gelöscht.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface eth0*

L2SWITCH(config-if)#*management host 192.168.200.106*

10.3.2.5 MAC Management

Tabelle 121: CLI-Konfiguration „MAC Management“

Knoten	Befehl	Beschreibung
enable	show mac-address-table aging-time	Mit diesem Befehl wird die aktuelle „Age Time“ der MAC-Adresstabelle angezeigt.
enable	show mac-address-table (static|dynamic)	Mit diesem Befehl werden die aktuellen statischen/dynamischen Unicast-Adresseinträge angezeigt.
enable	show mac-address-table port PORT_ID	Mit diesem Befehl werden die aktuellen Unicast-Adresseinträge angezeigt, die von dem spezifischen Port erkannt wurden.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	Mit diesem Befehl wird ein statischer Unicast-Eintrag konfiguriert.
configure	no mac-address-table static MACADDR vlan VLANID	Mit diesem Befehl wird ein statischer Unicast-Eintrag aus der Adresstabelle gelöscht.

Beispiel

L2SWITCH(config)#*mac-address-table static 00:11:22:33:44:55 vlan 1 port 1*

10.3.2.6 Blackhole MAC

Tabelle 122: CLI-Konfiguration „Blackhole MAC“

Knoten	Befehl	Beschreibung
enable	show mac-address-table refusal	Mit diesem Befehl wird nur die aktuell zurückgewiesene MAC-Adresse angezeigt.
configure	mac-address-table refusal MACADDR vlan VLANID	Mit diesem Befehl wird die Zurückweisung einer MAC-Adresse in einem spezifischen VLAN konfiguriert.
configure	mac-address-table refusal MACADDR	Mit diesem Befehl wird die Zurückweisung einer MAC-Adresse konfiguriert.

10.3.2.7 Port-Spiegelung (Port Mirroring)

Tabelle 123: CLI-Konfiguration „(Port-Spiegelung (Port Mirroring))“

Knoten	Befehl	Beschreibung
enable	show mirror	Mit diesem Befehl werden die aktuellen Konfigurationen für das „Port Mirroring“ angezeigt.
configure	mirror (disable|enable)	Mit diesem Befehl wird das „Port Mirroring“ beim Switch deaktiviert bzw. aktiviert.
configure	mirror destination port PORT_ID	Mit diesem Befehl wird der Monitor-Port für das „Port Mirroring“ spezifiziert.
configure	mirror source ports PORT_LIST mode (both|ingress|egress)	Mit diesem Befehl wird ein Port oder ein Port-Bereich als Source-Port(s) für das „Port Mirroring“ hinzugefügt.
configure	no mirror source ports PORT_LIST	Mit diesem Befehl wird ein Port oder ein Port-Bereich als Source-Port(s) für das „Port Mirroring“ entfernt.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*mirror enable*

L2SWITCH(config)#*mirror destination port 2*

L2SWITCH(config)#*mirror source ports 3-10 mode both*

10.3.2.8 Port Settings

Tabelle 124: CLI-Konfiguration „Port Settings“

Knoten	Befehl	Beschreibung
enable	show interface IFNAME	Mit diesem Befehl werden die aktuellen Port-Konfigurationen angezeigt.
interface	show	Mit diesem Befehl werden die aktuellen Port-Konfigurationen angezeigt.
interface	loopback (none | phy)	Mit diesem Befehl wird ein „Loopback“-Modus für einen bestimmten Port spezifiziert.
interface	flowcontrol (off | on)	Mit diesem Befehl wird die „Flow Control“ für einen Port deaktiviert bzw. aktiviert.
interface	speed (auto|10-full||10-half100-full|100-half)	Mit diesem Befehl werden Geschwindigkeit und Duplexmodus für einen Port konfiguriert.
interface	shutdown (Abschaltung)	Mit diesem Befehl wird ein spezifischer Port deaktiviert.
interface	no shutdown	Mit diesem Befehl wird ein spezifischer Port aktiviert.
interface	loopback (none|mac)	Mit diesem Befehl wird die Übertragung oder die Datentransportinfrastruktur getestet.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface fa1/0/1*

L2SWITCH(config-if)#*speed auto*

L2SWITCH#*show interface fastethernet1/0/1*

10.3.3 Erweiterte Einstellungen

10.3.3.1 Bandbreitenkontrolle

10.3.3.2 QoS

Tabelle 125: CLI-Konfiguration „QoS“

Knoten	Befehl	Beschreibung
enable	show queue cos-map	Mit diesem Befehl wird die aktuelle 802.1p-Prioritätenzuordnung an die „Service Queue“ angezeigt.
enable	show qos mode	Mit diesem Befehl wird der aktuelle IEEE 802.1p-QoS-Modus angezeigt.
configure	queue cos-map PRIORITY QUEUE_ID	Mit diesem Befehl wird die 802.1p-Prioritätenzuordnung der „Service Queue“ konfiguriert.
configure	no queue cos-map	Mit diesem Befehl wird die Default-Einstellung bei der 802.1p-Prioritätenzuordnung der „Service Queue“ angewendet.
configure	qos mode high-first	Mit diesem Befehl wird der QoS-Modus auf „high_first“ gesetzt, sodass jede „Hardware Queue“ erst alle ihre Pakete in ihren Puffer übertragen muss, bevor die nächste niedrigere Priorität ihre Pakete übertragen darf.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	Mit diesem Befehl wird der QoS-Modus auf „Weighted Round Robin“ gesetzt.
interface	default-priority	Mit diesem Befehl kann ein Benutzer spezifizieren, welche Priorität den vom Switch empfangenen Paketen ohne Tag standardmäßig zugewiesen wird. Der in diesem Befehl eingetragene Prioritätswert legt fest, zu welchen „Hardware Priority Queues“ das Paket weitergeleitet wird. Default-Wert: 0.
interface	no default-priority	Mit diesem Befehl wird die Default-Priorität des spezifischen Ports auf 0 gesetzt.

10.3.3.3 Rate Limitation

Tabelle 126: CLI-Konfiguration „Rate Limitation“

Knoten	Befehl	Beschreibung
enable	show bandwidth-limit	Mit diesem Befehl werden die aktuellen Konfigurationen der „Rate Limitation“ angezeigt.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für ausgehende Pakete aktiviert und die Begrenzung eingestellt.
configure	no bandwidth-limit egress ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für ausgehende Pakete deaktiviert.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für eingehende Pakete aktiviert und die Begrenzung eingestellt.
configure	no bandwidth-limit ingress ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für eingehende Pakete deaktiviert.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*bandwidth-limit egress 1 ports 1-8*

L2SWITCH(config)#*bandwidth-limit ingress 1 ports 1-8*

10.3.3.4 Storm Control

Tabelle 127: CLI-Konfiguration „Storm Control“

Knoten	Befehl	Beschreibung
enable	show storm-control	Mit diesem Befehl werden die aktuellen Konfigurationen für die „Storm Control“ angezeigt.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für Broadcast-, Multicast- oder DLF-Pakete aktiviert und für einen spezifizierten Typ eingestellt.
configure	no storm-control type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Mit diesem Befehl wird die Bandbreitenbegrenzung für Broadcast-, Multicast- oder DLF-Pakete deaktiviert.

Beispiel

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*

10.3.3.5 IGMP Snooping

Tabelle 128: CLI-Konfiguration „IGMP Snooping“

Knoten	Befehl	Beschreibung
enable	show igmp-snooping	Mit diesem Befehl werden die aktuellen Konfigurationen für das „IGMP Snooping“ angezeigt.
configure	igmp-snooping (disable | enable)	Mit diesem Befehl wird das „IGMP Snooping“ für den Switch deaktiviert bzw. aktiviert.
configure	igmp-snooping vlan VLAN_ID	Mit diesem Befehl wird das „IGMP Snooping“ für ein VLAN oder einen VLAN-Bereich aktiviert.
configure	no igmp-snooping vlan VLAN_ID	Mit diesem Befehl wird die „IGMP Snooping“-Funktion für ein VLAN oder einen VLAN-Bereich deaktiviert.
configure	igmp-snooping querier (disable | enable)	Mit diesem Befehl wird der „IGMP Snooping Querier“ für den Switch deaktiviert bzw. aktiviert.
configure	igmp-snooping querier vlan VLAN_ID	Mit diesem Befehl wird die „IGMP Snooping Querier“-Funktion für ein VLAN oder einen VLAN-Bereich aktiviert.
configure	no igmp-snooping querier vlan VLAN_ID	Mit diesem Befehl wird die „IGMP Snooping Querier“-Funktion für ein VLAN oder einen VLAN-Bereich deaktiviert.
configure	igmp-snooping unknown-multicast (drop|flooding)	Mit diesem Befehl wird die Verfahrensweise mit unbekannten Multicast-Paketen konfiguriert, wenn die „IGMP Snooping“-Funktion aktiviert ist. drop: Alle unbekannten Multicast-Pakete werden verworfen.
configure	igmp-snooping report-suppression (disable|enable)	Mit diesem Befehl wird die „IGMP Snooping Report Suppression“ für den Switch deaktiviert bzw. aktiviert.
interface	igmp-querier-mode (auto | fixed | edge)	Mit diesem Befehl wird spezifiziert, ob und unter welchen Bedingungen der bzw. die Ports „IGMP Query Ports“ sind. Der Switch leitet die „IGMP Join/Leave“-Pakete an einen „IGMP Query Port“ weiter und verhält sich so als wäre der Port mit einem IGMP-Multicast-Router (oder -Server) verbunden. Dabei muss auch „IGMP Snooping“ aktiviert sein (Default-Einstellung: „Auto“).
interface	igmp-immediate-leave	Mit diesem Befehl wird die „Immediate Leave“-Funktion beim „IGMP Snooping“ für eine spezifische Schnittstelle aktiviert.
interface	no igmp-immediate-leave	Mit diesem Befehl wird die „Immediate Leave“-Funktion beim „IGMP Snooping“ für eine spezifische Schnittstelle deaktiviert.

Beispiel

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*

10.3.3.6 MVR

Tabelle 129: CLI-Konfiguration „MVR“

Knoten	Befehl	Beschreibung
enable	show mvr	Mit diesem Befehl werden die aktuellen MVR-Konfigurationen angezeigt.
enable	show mvr vlan VLANID	Mit diesem Befehl werden die aktuellen MVR-Konfigurationen des spezifischen VLANs angezeigt.
enable	show igmp-snooping	Mit diesem Befehl werden die aktuellen Konfigurationen für das „IGMP Snooping“ angezeigt.
configure	mvr VLANID	Mit diesem Befehl werden die MVR-Konfigurationen für das spezifische VLAN erstellt.
configure	no mvr VLANID	Mit diesem Befehl werden die MVR-Konfigurationen für das spezifische VLAN deaktiviert.
MVR	group NAME	Mit diesem Befehl wird eine Gruppenkonfiguration für die MVR erstellt.
MVR	no group NAME	Mit diesem Befehl werden die Gruppenkonfigurationen aus der MVR entfernt.
MVR	inactive	Mit diesem Befehl werden die MVR-Einstellungen deaktiviert.
MVR	no inactive	Mit diesem Befehl werden die MVR-Einstellungen aktiviert.
MVR	mode (dynamic | compatible)	Mit diesem Befehl wird der Modus für die MVR konfiguriert. - Dynamisch: Es werden „IGMP Reports“ an alle MVR-Source-Ports im Multicast-VLAN gesendet. - Kompatibilität: Der Switch wird keine „IGMP Reports“ senden.
MVR	name STRING	Mit diesem Befehl wird der Name für die MVR konfiguriert.
MVR	no name	Mit diesem Befehl wird der Default-Name für die MVR konfiguriert.
MVR	receiver-port PORTLIST	Mit diesem Befehl wird ein Empfänger-Port oder Empfänger-Port-Bereich zugeordnet. Normalerweise sind die Source-Ports mit dem „Streaming Client“ verbunden.
MVR	no receiver-port PORTLIST	Mit diesem Befehl wird ein Port oder ein Port-Bereich aus der Liste der Empfänger-Ports entfernt.
MVR	source-port PORTLIST	Mit diesem Befehl wird ein Source-Port oder Source-Port-Bereich zugeordnet. Normalerweise sind die Source-Ports mit dem „Streaming Server“ verbunden.
MVR	no source-port PORTLIST	Mit diesem Befehl wird ein Port oder ein Port-Bereich aus der Liste der Source-Ports entfernt.
MVR	tagged PORTLIST	Mit diesem Befehl wird ein Port mit Tag oder Port-Bereich mit Tags zugeordnet. Gleiches gilt für VLAN-Ports mit Tag.
MVR	no tagged PORTLIST	

10.3.3.7 Multicast-Adresse

Tabelle 130: CLI-Konfiguration „Multicast-Adresse“

Knoten	Befehl	Beschreibung
enable	show mac-address-table multicast	Mit diesem Befehl werden die aktuellen statischen/dynamischen Multicast-Adresseinträge angezeigt.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	Mit diesem Befehl wird ein statischer Multicast-Eintrag konfiguriert.
configure	no mac-address-table multicast MACADDR	Mit diesem Befehl wird ein statischer Multicast-Eintrag aus der Adresstabelle gelöscht.

10.3.3.8 VLAN

10.3.3.8.1 Port-Isolation

Tabelle 131: CLI-Konfiguration „Port-Isolation“

Knoten	Befehl	Beschreibung
enable	show port-isolation	Mit diesem Befehl werden die aktuellen Konfigurationen der „Port-Isolation“ angezeigt. „V“ zeigt an, dass die Pakete des Ports zu diesem Port gesendet werden können. „-“ zeigt an, dass die Pakete des Ports nicht zu diesem Port gesendet werden können.
interface	port-isolation ports PORTLISTS	Mit diesem Befehl wird ein Port oder Port-Bereich konfiguriert, Datenpakete von einem spezifischen Port weiterzuleiten.
interface	no port-isolation	Mit diesem Befehl werden alle Ports konfiguriert, Datenpakete von einem spezifischen Port weiterzuleiten.

Beispiel

L2SWITCH(config)#*interface 1/0/2*

L2SWITCH(config-if)#*port-isolation ports 3-10*

10.3.3.8.2 VLAN-Einstellungen

Tabelle 132: CLI-Konfiguration „VLAN-Einstellungen“

Knoten	Befehl	Beschreibung
enable	show vlan VLANID	Mit diesem Befehl werden die VLAN-Konfigurationen angezeigt.
configure	vlan <1~4094>	Mit diesem Befehl wird ein VLAN aktiviert und der VLAN-Knoten eingetragen.
configure	no vlan <1~4094>	Mit diesem Befehl wird ein VLAN gelöscht.
vlan	show	Mit diesem Befehl werden die aktuellen VLAN-Konfigurationen angezeigt.
vlan	name STRING	Mit diesem Befehl wird einem spezifischen VLAN ein Name zugewiesen. Der VLAN-Name sollte aus einer Kombination aus Zahlen, Buchstaben, Bindestrichen (-) oder Unterstrichen (_) bestehen. Die maximale Zeichenlänge für den Namen ist 16.
vlan	no name	Dieser Befehl setzt den VLAN-Namen auf die Default-Einstellung zurück. Hinweis: Der Default-VLAN-Name setzt sich wie folgt zusammen: „VLAN“+VLAN_ID, VLAN1, VLAN2, …
vlan	fixed PORT_LIST	Mit diesem Befehl werden Ports einer VLAN-Gruppe als Teilnehmer dauerhaft zugeordnet.
vlan	no fixed	Mit diesem Befehl werden alle dauerhaft zugeordneten Ports aus einem VLAN entfernt.
vlan	tagged PORT_LIST	Mit diesem Befehl werden Ports einer VLAN-Gruppe als Teilnehmer mit Tag dauerhaft zugeordnet. Diese Ports bzw. dieser Port sollte ein dauerhaft zugeordneter Teilnehmer einer VLAN-Gruppe sein.
vlan	no tagged	Mit diesem Befehl werden alle dauerhaft zugeordneten Ports mit Tag aus einem VLAN entfernt.
vlan	untagged PORT_LIST	Mit diesem Befehl werden Ports einer VLAN-Gruppe als Teilnehmer ohne Tag dauerhaft zugeordnet. Diese Ports bzw. dieser Port sollte ein dauerhaft zugeordneter Teilnehmer einer VLAN-Gruppe sein.
vlan	no untagged	Mit diesem Befehl werden alle Ports ohne Tag aus einem VLAN entfernt.
vlan	acceptable frame type (all | tagged | untagged)	Mit diesem Befehl wird der zulässige Frame-Typ konfiguriert.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*vlan 2*

L2SWITCH(config-vlan)#*fixed 1*-6

L2SWITCH(config-vlan)#*untagged 1-3*

10.3.3.9 GARP/GVRP

Tabelle 133: CLI-Konfiguration „GARP/GVRP“

Knoten	Befehl	Beschreibung
enable	show gvrp configuration	Mit diesem Befehl werden die GVRP-Konfigurationen angezeigt.
enable	show gvrp statistics	Mit diesem Befehl werden die GVRP-Konfigurationen für einen oder für alle Ports angezeigt.
enable	show garp timer	Mit diesem Befehl werden die Timer für das GARP angezeigt.
configure	gvrp (disable | enable)	Mit diesem Befehl wird das GVRP für den Switch deaktiviert bzw. aktiviert.
configure	no gvrp configuration	Mit diesem Befehl wird die GVRP-Konfiguration auf die Default-Einstellung zurückgesetzt.
interface	gvrp (disable | enable)	Mit diesem Befehl wird das GVRP für einen spezifischen Port deaktiviert bzw. aktiviert.
interface	gvrp registration (normal | forbidden)	Mit diesem Befehl wird der Anmeldungsmodus des GVRP für einen spezifischen Port konfiguriert.
interface	no gvrp configuration	Mit diesem Befehl wird die GVRP-Konfiguration für einen spezifischen Port auf die Default-Einstellung zurückgesetzt.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	Mit diesem Befehl werden die „Join Time“, „Leave Time“ und „Leaveall Time“ des GVRP für einen spezifischen Port konfiguriert.
interface	no garp time	Mit diesem Befehl werden die Join-, Leave- und Leaveall-Zeit des GVRP für einen spezifischen Port auf die Default-Einstellungen zurückgesetzt.

10.3.3.10 Q-in-Q

10.3.3.10.1 VLAN-Stacking

Tabelle 134: CLI-Konfiguration „VLAN-Stacking“

Knoten	Befehl	Beschreibung
enable	show vlan-stacking	Mit diesem Befehl wird der aktuelle „VLAN Stacking“-Typ angezeigt.
enable	show vlan-stacking selective-qinq	Mit diesem Befehl werden die selektiven Q-in-Q-Konfigurationen angezeigt.
enable	show vlan-stacking portbased-qinq	Mit diesem Befehl werden die port-basierten Q-in-Q-Konfigurationen angezeigt.
enable	show vlan-stacking tpid-inform	Mit diesem Befehl werden die TPID-Konfigurationen angezeigt.
config	vlan-stacking (disable | port-based | selective)	Mit diesem Befehl wird entweder das „VLAN Stacking“ deaktiviert oder das port-basierte bzw. selektive „VLAN Stacking“ beim Switch aktiviert.
config	vlan-stacking selective-qinq STRINGS	Mit diesem Befehl wird ein selektives Q-in-Q-Profil mit Namen erstellt.
config	no vlan-stacking selective-qinq STRINGS	Mit diesem Befehl wird ein selektives Q-in-Q-Profil mit Namen gelöscht.
config	vlan-stacking tpid-table index <2-6> value STRINGS	Mit diesem Befehl wird die TPID-Tabelle konfiguriert.
interface	vlan-stacking port-based priority <0~7>	Mit diesem Befehl wird die Priorität im port-basierten Q-in-Q zugeordnet.
interface	vlan-stacking port-based role (tunnel | access | normal)	Mit diesem Befehl wird dem Port beim „VLAN Stacking“ eine Rolle zugeordnet.
interface	vlan-stacking port-based spvid <1~4096>	Mit diesem Befehl wird die Dienstanbieter-VID des spezifizierten Ports zugeordnet.
interface	vlan-stacking tunnel-tpid index <1-6>	Mit diesem Befehl wird die TPID einem „Q-in-Q Tunnel Port“ zugeordnet.
qinq	active	Mit diesem Befehl wird das selektive Q-in-Q-Profil aktiviert.
qinq	inactive	Mit diesem Befehl wird das selektive Q-in-Q-Profil deaktiviert.
qinq	cvid VLANID	Mit diesem Befehl wird der VLAN-Bereich des Dienstanbieters für eingehende Pakete spezifiziert.
qinq	spvid VLANID	Mit diesem Befehl wird die VLAN-ID des Dienstanbieters für ausgehende Pakete im selektiven Q-in-Q zugeordnet.
qinq	priority <0-7>	Mit diesem Befehl wird die Priorität im selektiven Q-in-Q zugeordnet.
qinq	access-ports PORTLISTS	Mit diesem Befehl werden die „Access-Ports“ spezifiziert, die die Regel anwenden sollen.
qinq	tunnel-ports PORTLISTS	Mit diesem Befehl werden die „Tunnel-Ports“ spezifiziert, die die Regel anwenden sollen.
qinq	end	Mit diesem Befehl verlassen Sie den „CLI Q-in-Q“-Knoten und aktivieren den „CLI enable“-Knoten.
qinq	exit	Mit diesem Befehl verlassen Sie den „CLI Q-in-Q“-Knoten und aktivieren den „CLI configure“-Knoten.
qinq	show	Mit diesem Befehl werden die aktuellen Konfigurationen des selektiven Q-in-Q-Profils angezeigt.

10.3.3.11 DHCP Relay

Tabelle 135: CLI-Konfiguration „DHCP Relay“

Knoten	Befehl	Beschreibung
enable	show dhcp relay	Mit diesem Befehl werden die aktuellen Konfigurationen für das „DHCP Relay“ angezeigt.
configure	dhcp relay (disable | enable)	Mit diesem Befehl wird das „DHCP Relay“ beim Switch deaktiviert bzw. aktiviert.
configure	dhcp relay vlan VLAN_RANGE	Mit diesem Befehl wird die Funktion „DHCP Relay“ für ein VLAN oder einen VLAN-Bereich aktiviert.
configure	no dhcp relay vlan VLAN_RANGE	Mit diesem Befehl wird die Funktion „DHCP Relay“ für ein VLAN oder einen VLAN-Bereich deaktiviert.
configure	dhcp helper-address IP_ADDRESS	Mit diesem Befehl wird die IP-Adresse des DHCP-Servers konfiguriert.
configure	no dhcp helper-address	Mit diesem Befehl wird die IP-Adresse des DHCP-Servers entfernt.
configure	dhcp option82 (disable | enable)	Mit diesem Befehl wird die Funktion „DHCP Relay Option 82“ beim Switch deaktiviert bzw. aktiviert.
configure	dhcp option82 information STRING	Mit diesem Befehl werden die Informationen für die Funktion „DHCP Relay Option 82“ konfiguriert.
configure	no dhcp option82 information	Mit diesem Befehl werden die Informationen für die Funktion „DHCP Relay Option 82“ entfernt.

Beispiel

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*

L2SWITCH(config)#*dhcp option82 enable*

L2SWITCH(config)#*dhcp option82 information Justin*

10.3.3.12 Dual Homing

Tabelle 136: CLI-Konfiguration „Dual Homing“

Knoten	Befehl	Beschreibung
enable	show dual-homing	Mit diesem Befehl werden die Informationen von „Dual Homing“ angezeigt.
configure	dual-homing (disable | enable)	Mit diesem Befehl wird die Funktion „Dual Homing“ im System deaktiviert bzw. aktiviert.
configure	no dual-homing primary-channel	Mit diesem Befehl wird der Primärkanal für das „Dual Homing“ aus dem System entfernt.
configure	no dual-homing primary-channel	Mit diesem Befehl wird der Primärkanal für das „Dual Homing“ aus dem System entfernt.
configure	dual-homing secondary-channel (port | trunk) VALUE	Mit diesem Befehl wird der Sekundärkanal für das „Dual Homing“ im System konfiguriert. Der Kanal kann aus nur einem einzelnen Port oder aus einer „Trunk Group“ bestehen.
configure	no dual-homing secondary-channel	Mit diesem Befehl wird der Sekundärkanal für das „Dual Homing“ aus dem System entfernt.

Beispiel

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*

10.3.3.13 Link Aggregation

Tabelle 137: CLI-Konfiguration „Link Aggregation“

Knoten	Befehl	Beschreibung
enable	show link-aggregation	Mit diesem Befehl werden die aktuellen Konfigurationen für das „Trunking“ angezeigt.
configure	link-aggregation [GROUP_ID] (disable | enable)	Mit diesem Befehl wird das „Trunking“ für eine spezifische „Trunk Group“ deaktiviert bzw. aktiviert.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	Mit diesem Befehl werden Ports zu einer spezifischen „Trunk Group“ hinzugefügt.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	Mit diesem Befehl werden Ports aus einer spezifischen „Trunk Group“ entfernt.

10.3.3.14 LACP

Tabelle 138: CLI-Konfiguration „LACP“

Knoten	Befehl	Beschreibung
enable	show trunk	Mit diesem Befehl werden die aktuellen Konfigurationen für das „Trunking“ angezeigt.
enable	show lacp counters [GROUP_ID]	Mit diesem Befehl werden die LACP-Zähler für eine spezifische oder alle Gruppen angezeigt.
enable	show lacp internal [GROUP_ID]	Mit diesem Befehl werden die internen LACP-Informationen für eine spezifische oder alle Gruppen angezeigt.
enable	show lacp neighbor [GROUP_ID]	Mit diesem Befehl werden die LACP-Nachbarinformationen für eine spezifische oder alle Gruppen angezeigt.
enable	show lacp port_priority	Mit diesem Befehl wird die Port-Priorität für das LACP angezeigt.
enable	show lacp sys_id	Mit diesem Befehl wird die System-ID vom „LACP Actor“ und „LACP Partner“ angezeigt.
configure	Lacp (disable | enable)	Mit diesem Befehl wird das LACP für den Switch deaktiviert bzw. aktiviert.
configure	Lacp GROUP_ID (disable | enable)	Mit diesem Befehl wird das LACP für eine spezifische „Trunk Group“ deaktiviert bzw. aktiviert.
configure	clear lacp counters [PORT_ID]	Mit diesem Befehl werden die LACP-Statistiken für einen spezifischen oder alle Ports gelöscht.
configure	lacp system-priority <1-65535>	Mit diesem Befehl wird die Systempriorität für das LACP konfiguriert. Hinweis: Der Default-Wert ist 32768.
configure	no lacp system-priority	Mit diesem Befehl wird die Default-Einstellung für die Systempriorität des LACPs konfiguriert.
interface	lacp port_priority <1-65535>	Mit diesem Befehl wird die Priorität für den spezifischen Port konfiguriert.
interface	no lacp port_priority	Hinweis: Der Default-Wert ist 32768.

10.3.3.15 LLDP

Tabelle 139: CLI-Konfiguration „LLDP“

Knoten	Befehl	Beschreibung
enable	show lldp	Mit diesem Befehl werden die LLDP-Konfigurationen angezeigt.
enable	show lldp neighbor	Mit diesem Befehl werden alle Informationen der Port-Nachbarn angezeigt.
configure	lldp (disable | enable)	Mit diesem Befehl wird die LLDP-Funktion für den Switch global aktiviert bzw. deaktiviert.
configure	lldp tx-interval	Mit diesem Befehl wird das Übertragungsintervall für LLDP-Pakete konfiguriert.
configure	lldp tx-hold	Mit diesem Befehl wird die „tx-Hold Time“ (tx-Haltezeit) konfiguriert, die die TTL der Nachricht des Switches bestimmt. (TTL = tx-hold * tx-interval)
interface	lldp-agent (disable | enable | rx-only | tx-only)	Mit diesem Befehl wird die Agent-Funktion des LLDPs konfiguriert. „disable“: Das LLDP wird bei einem spezifischen Port deaktiviert. „enable“: Das LLDP-Paket wird von einem spezifischen Port übertragen und empfangen. „tx-only“: Das LLDP-Paket wird von einem spezifischen Port nur übertragen. „rx-only“: Das LLDP-Paket wird von einem spezifischen Port nur empfangen.

10.3.3.16 Loop Detection

Tabelle 140: CLI-Konfiguration „Loop Detection“

Knoten	Befehl	Beschreibung
enable	show loop-detection	Mit diesem Befehl werden die aktuellen Konfigurationen für die „Loop Detection“ angezeigt.
configure	loop-detection (disable | enable)	Mit diesem Befehl wird die „Loop Detection“ für den Switch deaktiviert bzw. aktiviert.
configure	loop-detection address MACADDR	Mit diesem Befehl wird die MAC-Zieladresse für die Sondenpakete der „Loop Detection“ konfiguriert.
configure	no loop-detection address	Dieser Befehl setzt die MAC-Zieladresse auf die Default-Einstellung (00:0b:04:AA:AA:AB) zurück.
interface	loop-detection (disable | enable)	Mit diesem Befehl wird die „Loop Detection“ für einen spezifischen Port deaktiviert bzw. aktiviert.
interface	no shutdown	Mit diesem Befehl wird ein spezifischer Port aktiviert. Der Befehl kann einen durch die „Loop Detection“ blockierten Port aktivieren.
interface	loop-detection recovery (disable | enable)	Mit diesem Befehl wird „Recovery“-Funktion für einen Port deaktiviert bzw. aktiviert.
interface	loop-detection recovery time VALUE	Mit diesem Befehl wird der Zeitraum für die „Recovery Time“ konfiguriert.

Beispiel

L2SWITCH(config)#*loop-detection enable*

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

L2SWITCH(config-if)#*loop-detection enable*

L2SWITCH(config-if)#*loop-detection recovery enable*

L2SWITCH(config-if)#*loop-detection recovery time 10*

10.3.3.17 STP

Tabelle 141: CLI-Konfiguration „STP“

Knoten	Befehl	Beschreibung
enable	show spanning-tree active	Mit diesem Befehl werden nur die STP-Informationen für aktive Ports angezeigt.
enable	show spanning-tree blockedports	Mit diesem Befehl werden nur die STP-Informationen für blockierte Ports angezeigt.
enable	show spanning-tree port detail PORT_ID	Mit diesem Befehl werden die STP-Informationen für den Schnittstellen-Port angezeigt.
enable	show spanning-tree statistics PORT_ID	Mit diesem Befehl werden die STP-Informationen für den Schnittstellen-Port angezeigt.
enable	show spanning-tree summary	Mit diesem Befehl wird eine Zusammenfassung der Port-Zustände und -Konfigurationen angezeigt.
enable	clear spanning-tree counters	Mit diesem Befehl wird die STP-Statistik für alle Ports gelöscht.
enable	clear spanning-tree counters PORT_ID	Mit diesem Befehl wird die STP-Statistik für einen spezifischen Port gelöscht.
configure	spanning-tree (disable | enable)	Mit diesem Befehl wird die STP-Funktion im System deaktiviert bzw. aktiviert.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	Mit diesem Befehl werden die Bridge-Zeiten („Forward Delay“, „Max Age“, „Hello Time“) konfiguriert.
configure	no spanning-tree algorithm-timer	Mit diesem Befehl werden die Default-Werte für „Forward Delay“, „Max Age“ und „Hello Time“ konfiguriert.
configure	spanning-tree forward-time <4-30>	Mit diesem Befehl wird der Zeitraum für die „Forward Delay“ (in Sekunden) der Bridge konfiguriert.
configure	no spanning-tree forward-time	Mit diesem Befehl werden die Default-Werte für die „Forward Delay“ konfiguriert.
configure	spanning-tree hello-time <1-10>	Mit diesem Befehl wird der Zeitraum für die „Hello Time“ (in Sekunden) der Bridge konfiguriert.
configure	no spanning-tree hello-time	Mit diesem Befehl werden die Default-Werte für die „Hello Time“ konfiguriert.
configure	spanning-tree max-age <6-40>	Mit diesem Befehl wird der Zeitraum für das „Max Age“ (in Sekunden) der Bridge-Nachrichten konfiguriert.
configure	no spanning-tree max-age	Mit diesem Befehl werden die Default-Werte für das „Max Age“ konfiguriert.
configure	spanning-tree mode (rstp | stp)	Mit diesem Befehl wird der STP-Modus konfiguriert.
configure	spanning-tree pathcost method (short | long)	Mit diesem Befehl wird die Methode für die Pfadkosten konfiguriert.
configure	spanning-tree priority <0-61440>	Mit diesem Befehl wird die Priorität für das System konfiguriert.
configure	no spanning-tree priority	Mit diesem Befehl werden die Default-Werte für die Systempriorität konfiguriert.
interface	spanning-tree bpdufilter (disable | enable)	Mit diesem Befehl wird die Funktion „BPDU Filter“ aktiviert bzw. deaktiviert.
interface	spanning-tree bpduguard (disable | enable)	Mit diesem Befehl wird die Funktion „BPDU Guard“ aktiviert bzw. deaktiviert.
interface	spanning-tree edge-port (disable | enable)	Mit diesem Befehl wird die Einstellung „Edge Port“ aktiviert bzw. deaktiviert.

Tabelle 141: CLI-Konfiguration „STP“

Knoten	Befehl	Beschreibung
interface	spanning-tree cost VALUE	Mit diesem Befehl werden die Kosten für den spezifischen Port konfiguriert. Kostenbereich: 16-Bit-basierter Wertebereich von 1 bis 65.535, 32-Bit-basierter Wertebereich von 1 bis 200.000.000.
interface	no spanning-tree cost	Mit diesem Befehl werden die Pfadkosten des spezifischen Ports auf den Default-Wert gesetzt.
interface	spanning-tree port-priority <0-240>	Mit diesem Befehl wird die Port-Priorität für den spezifischen Port konfiguriert. Default-Wert: 128.
interface	no spanning-tree port-priority	Mit diesem Befehl wird die Priorität des spezifischen Ports auf den Default-Wert gesetzt.

10.3.3.18 Xpress Ring

Tabelle 142: CLI-Konfiguration „Xpress Ring“

Knoten	Befehl	Beschreibung
enable	show xpress-ring	Mit diesem Befehl wird der aktuelle Status des Xpress-Rings angezeigt.
config	xpress-ring (disable | enable)	Mit diesem Befehl wird die Xpress-Ring-Funktion für den Switch aktiviert bzw. deaktiviert.
config	xpress-ring role (forwarder | arbiter)	Mit diesem Befehl wird die Rolle („Forwarder“ oder „Arbiter“) für den Switch konfiguriert.
config	xpress-ring ring-port1	Mit diesem Befehl wird ein Port des Rings konfiguriert.
config	xpress-ring ring-port2	Mit diesem Befehl wird der andere Port des Rings konfiguriert.

10.3.4 Sicherheit

10.3.4.1 DHCP Snooping

Tabelle 143: CLI-Konfiguration „DHCP Snooping“

Knoten	Befehl	Beschreibung
enable	show dhcp-snooping	Mit diesem Befehl werden die aktuellen Konfigurationen für das „DHCP Snooping“ angezeigt.
configure	dhcp-snooping (disable | enable)	Mit diesem Befehl wird das „DHCP Snooping“ für den Switch deaktiviert bzw. aktiviert.
configure	dhcp-snooping vlan VLANID	Mit diesem Befehl wird das „DHCP Snooping“ für ein VLAN oder einen VLAN-Bereich aktiviert.
configure	no dhcp-snooping vlan VLANID	Mit diesem Befehl wird die „DHCP Snooping“-Funktion für ein VLAN oder einen VLAN-Bereich deaktiviert.
configure	dhcp option82 (disable | enable)	Mit diesem Befehl wird die Funktion „DHCP Relay Option 82“ deaktiviert bzw. aktiviert.
configure	dhcp option82 information STRING	Mit diesem Befehl werden die Informationen für die Funktion „DHCP Relay Option 82“ konfiguriert.
configure	no dhcp option82 information	Mit diesem Befehl werden die Informationen für die Funktion „DHCP Relay Option 82“ entfernt.
interface	dhcp-snooping host	Mit diesem Befehl wird die maximale Anzahl von Hosts für den spezifischen Port konfiguriert.
interface	no dhcp-snooping host	Mit diesem Befehl wird die maximale Anzahl von Hosts für den spezifischen Port auf den Default-Wert gesetzt.
interface	dhcp-snooping trust	Mit diesem Befehl wird der „Trusted-Port“ für den spezifischen Port konfiguriert.
interface	no dhcp-snooping trust	Mit diesem Befehl wird der „Untrusted-Port“ für den spezifischen Port konfiguriert.

Beispiel

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*

L2SWITCH(config)#*dhcp option82 enable*

L2SWITCH(config)#*dhcp option82 information Test01*

10.3.4.2 Server Screening

Tabelle 144: CLI-Konfiguration „Server Screening“

Knoten	Befehl	Beschreibung
enable	show dhcp-snooping server	Mit diesem Befehl wird die IP-Adresse des gültigen DHCP-Servers angezeigt.
configure	dhcp-snooping server IPADDR	Mit diesem Befehl wird die IP-Adresse eines gültigen DHCP-Servers konfiguriert.
configure	no dhcp-snooping server IPADDR	Mit diesem Befehl wird die IP-Adresse eines gültigen DHCP-Servers gelöscht.

10.3.4.3 Binding Table

Tabelle 145: CLI-Konfiguration „Binding Table“

Knoten	Befehl	Beschreibung
enable	show dhcp-snooping binding	Mit diesem Befehl wird die aktuelle „DHCP Snooping“-Anbindungstabelle angezeigt.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLANID port PORT_NO	Mit diesem Befehl wird ein statischer Host in der „DHCP Snooping“-Anbindungstabelle konfiguriert.
configure	no dhcp-snooping binding mac MACADDR	Mit diesem Befehl wird ein statischer Host aus der „DHCP Snooping“-Anbindungstabelle gelöscht.

Beispiel

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*

10.3.4.4 ARP Inspection

Tabelle 146: CLI-Konfiguration „ARP Inspection“

Knoten	Befehl	Beschreibung
enable	show arp-inspection	Mit diesem Befehl werden die aktuellen Konfigurationen für die ARP-Überprüfung angezeigt.
configure	arp-inspection (disable | enable)	Mit diesem Befehl wird die ARP-Überprüfung beim Switch aktiviert bzw. deaktiviert.
configure	arp-inspection vlan VLANID	Mit diesem Befehl wird die ARP-Überprüfung für ein VLAN oder einen VLAN-Bereich aktiviert.
configure	no arp-inspection vlan VLANID	Mit diesem Befehl wird die ARP-Überprüfung für ein VLAN oder einen VLAN-Bereich deaktiviert.
interface	arp-inspection trust	Mit diesem Befehl wird der „Trusted-Port“ für den spezifischen Port konfiguriert.
interface	no arp-inspection trust	Mit diesem Befehl wird der „Untrusted-Port“ für den spezifischen Port konfiguriert.

Beispiel

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*

10.3.4.5 Filter Table

Tabelle 147: CLI-Konfiguration „Filter Table“

Knoten	Befehl	Beschreibung
enable	show arp-inspection mac-filter	Mit diesem Befehl werden die aktuellen MAC-Adressfilter für die ARP-Überprüfung angezeigt.
configure	arp-inspection mac-filter age VALUE	Mit diesem Befehl wird die „Age Time“ für MAC-Adressfiltereinträge der ARP-Überprüfung konfiguriert.
configure	no arp-inspection mac-filter mac MACADDR	Mit diesem Befehl wird ein MAC-Adressfiltereintrag aus der MAC-Filtertabelle der ARP-Überprüfung gelöscht.

10.3.4.6 Zugriffskontrollliste

Tabelle 148: CLI-Konfiguration „Zugriffskontrollliste“

Knoten	Befehl	Beschreibung
enable	show access-list	Mit diesem Befehl werden alle Zugriffssteuerungsprofile angezeigt.
configure	access-list STRING	Mit diesem Befehl wird ein neues Zugriffssteuerungsprofil erstellt. Dabei bezeichnet „STRING“ den Profilnamen.
configure	no access-list STRING	Mit diesem Befehl wird ein Zugriffssteuerungsprofil gelöscht.
acl	show	Mit diesem Befehl wird das aktuelle Zugriffssteuerungsprofil angezeigt.
acl	action (disable | drop | permit)	Mit diesem Befehl wird das Profil verarbeitet. „disable“: Das Profil wird deaktiviert. „drop“: Wenn Pakete mit dem Profil übereinstimmen, werden sie verworfen. „permit“: Wenn Pakete mit dem Profil übereinstimmen, werden sie weitergeleitet.
acl	destination mac host MACADDR	Mit diesem Befehl werden die MAC-Zieladresse und die Maske für das Profil konfiguriert.
acl	destination mac MACADDR MACADDR	Mit diesem Befehl werden die MAC-Zieladresse und die Maske für das Profil konfiguriert.
acl	destination mac MACADDR MACADDR	Mit diesem Befehl werden die MAC-Zieladresse und die Maske für das Profil konfiguriert. Der zweite Parameter „MACADDR“ ist die Maske (z. B.: ffff.ffff.0000) für das Profil.
acl	no destination mac	Mit diesem Befehl wird die MAC-Zieladresse aus dem Profil entfernt.
acl	ethertype STRING	Mit diesem Befehl wird der ETHERNET-Typ für das Profil konfiguriert. Dabei bezeichnet „STRING“ einen Hexadezimalwert, z. B.: 08AA.
acl	no ethertype	Mit diesem Befehl wird die Begrenzung des ETHERNET-Typs aus dem Profil entfernt.
acl	source mac host MACADDR	Mit diesem Befehl werden die MAC-Quelladresse und die Maske für das Profil konfiguriert.
acl	source mac MACADDR MACADDR	Mit diesem Befehl werden die MAC-Quelladresse und die Maske für das Profil konfiguriert.
acl	no source mac	Mit diesem Befehl werden die MAC-Quelladresse und die Maske aus dem Profil entfernt.
acl	source ip host IPADDR	Mit diesem Befehl wird die IP-Quelladresse für das Profil konfiguriert.
acl	source ip IPADDR IPMASK	Mit diesem Befehl werden die IP-Quelladresse und die Maske für das Profil konfiguriert.
acl	no source ip	Mit diesem Befehl wird die IP-Quelladresse aus dem Profil entfernt.
acl	destination ip host IPADDR	Mit diesem Befehl wird eine spezifische IP-Zieladresse für das Profil konfiguriert.
acl	destination ip IPADDR IPMASK	Mit diesem Befehl werden die IP-Zieladresse und die Maske für das Profil konfiguriert.
acl	no destination ip	Mit diesem Befehl wird die IP-Zieladresse aus dem Profil entfernt.
acl	l4-source-port IPADDR	Mit diesem Befehl wird der UDP/TCP-Quell-Port für das Profil konfiguriert.

Tabelle 148: CLI-Konfiguration „Zugriffskontrollliste“

Knoten	Befehl	Beschreibung
acl	no l4-source-port IPADDR	Mit diesem Befehl wird der UDP/TCP-Quell-Port aus dem Profil entfernt.
acl	L4-destination-port PORT	Mit diesem Befehl wird der UDP/TCP-Ziel-Port für das Profil konfiguriert.
acl	no l4-destination-port	Mit diesem Befehl wird der UDP/TCP-Ziel-Port aus dem Profil entfernt.
acl	vlan VLANID	Mit diesem Befehl wird das VLAN für das Profil konfiguriert.
acl	no vlan	Mit diesem Befehl wird die Begrenzung des VLANs aus dem Profil entfernt.
acl	source interface PORT_ID	Mit diesem Befehl wird die Quellschnittstelle für das Profil konfiguriert.
acl	no source interface PORT_ID	Mit diesem Befehl wird die Quellschnittstelle aus dem Profil entfernt.

10.3.4.7 802.1x

Tabelle 149: CLI-Konfiguration „802.1x“

Knoten	Befehl	Beschreibung
enable	show dot1x	Mit diesem Befehl werden die aktuellen 802.1x-Konfigurationen angezeigt.
enable	show dot1x username	Mit diesem Befehl werden die aktuellen Benutzerkonten für die lokale Authentifizierung angezeigt.
enable	show dot1x accounting-record	Mit diesem Befehl werden die lokalen Konteneinträge angezeigt.
configure	dot1x authentication (disable | enable)	Mit diesem Befehl wird die 802.1x-Authentifizierung für den Switch aktiviert bzw. deaktiviert.
configure	dot1x authentic-method (local | radius)	Mit diesem Befehl wird die Methode für die 802.1x-Authentifizierung konfiguriert.
configure	no dot1x authentic-method	Mit diesem Befehl wird die Methode für die 802.1x-Authentifizierung auf die Default-Einstellung gesetzt.
configure	dot1x radius primary-server-ip <IP> port PORTID	Mit diesem Befehl wird der primäre Radiusserver konfiguriert.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	Mit diesem Befehl wird der primäre Radiusserver konfiguriert.
configure	dot1x radius secondary-server-ip <IP> port PORTID	Mit diesem Befehl wird der sekundäre Radiusserver konfiguriert.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	Mit diesem Befehl wird der sekundäre Radiusserver konfiguriert.
configure	no dot1x radius secondary-server-ip	Mit diesem Befehl wird der sekundäre Radiusserver entfernt.
configure	dot1x username <STRING> passwd <STRING>	Mit diesem Befehl wird ein Benutzerkonto für die lokale Authentifizierung konfiguriert.
configure	no dot1x username <STRING>	Mit diesem Befehl wird ein Benutzerkonto für die lokale Authentifizierung entfernt.
configure	dot1x accounting (disable|enable)	Mit diesem Befehl werden die lokalen .1x-Konteneinträge aktiviert bzw. deaktiviert.
configure	dot1x guest-vlan VLANID	Mit diesem Befehl wird das Gast-VLAN konfiguriert.
configure	no dot1x guest-vlan	Mit diesem Befehl wird das Gast-VLAN entfernt.
interface	dot1x admin-control-direction (both|in)	Mit diesem Befehl wird die Steuerungsrichtung für die Paketblockierung konfiguriert.
interface	dot1x default	Mit diesem Befehl wird die Port-Konfiguration auf die Default-Einstellungen zurückgesetzt.
interface	dot1x max-req <1-10>	Mit diesem Befehl wird die Funktion „Max-req Times“ für einen Port konfiguriert (1 bis 10).
interface	dot1x port-control (auto | force-authorized | force-unauthorized)	Mit diesem Befehl wird der Port-Steuerungsmodus für den Port konfiguriert.
interface	dot1x authentication (disable | enable)	Mit diesem Befehl wird die 802.1x-Authentifizierung für den Port deaktiviert bzw. aktiviert.
interface	dot1x reauthentication (disable | enable)	Mit diesem Befehl wird das Authentifizierungsintervall für den Port deaktiviert bzw. aktiviert.
interface	dot1x timeout quiet-period	Mit diesem Befehl wird der Wert für die „Quiet Period“ (Passivitätszeitraum) des Ports konfiguriert.

Tabelle 149: CLI-Konfiguration „802.1x“

Knoten	Befehl	Beschreibung
interface	dot1x timeout server-timeout	Mit diesem Befehl wird der Wert für das Server-Zeitlimit des Ports konfiguriert.
interface	dot1x timeout reauth-period	Mit diesem Befehl wird der Wert für das Authentifizierungsintervall des Ports konfiguriert.
interface	dot1x timeout supp-timeout	Mit diesem Befehl wird der Wert für das Anfragestellerzeitlimit des Ports konfiguriert.
interface	dot1x guest-vlan (disable | enable)	Mit diesem Befehl wird der 802.1x-Zustand für den Port konfiguriert.

10.3.4.8 Port Security

Tabelle 150: CLI-Konfiguration „Port Security“

Knoten	Befehl	Beschreibung
enable	show port-security	Mit diesem Befehl werden die aktuellen Konfigurationen für die Port-Sicherheit angezeigt.
config	port-security (disable | enable)	Mit diesem Befehl wird die Funktion Port-Sicherheit global aktiviert bzw. deaktiviert.
interface	port-security (disable | enable)	Mit diesem Befehl wird die Funktion Port-Sicherheit für den spezifischen Port aktiviert bzw. deaktiviert.
interface	port-security limit VALUE	Mit diesem Befehl wird die maximale Anzahl von MAC-Adresseinträgen für den spezifischen Port konfiguriert.

10.3.5 Monitor

10.3.5.1 Alarm

Tabelle 151: CLI-Konfiguration „Alarm“

Knoten	Befehl	Beschreibung
enable	show alarm-info	Mit diesem Befehl werden die Alarminformationen angezeigt.

10.3.5.2 Monitor-Informationen

Tabelle 152: CLI-Konfiguration „Monitor-Informationen“

Knoten	Befehl	Beschreibung
enable	show hardware-monitor (C|F)	Mit diesem Befehl werden Informationen zum Hardwarebetrieb angezeigt.

10.3.5.3 RMON-Statistiken

Tabelle 153: CLI-Konfiguration „RMON-Statistiken“

Knoten	Befehl	Beschreibung
enable	show rmon statistics	Mit diesem Befehl werden die RMON-Statistiken angezeigt.
configure	clear rmon statistics [IFNAME]	Mit diesem Befehl werden die RMON-Statistiken für einen oder für alle Ports gelöscht.

10.3.5.4 SFP-Informationen

Tabelle 154: CLI-Konfiguration „SFP-Informationen“

Knoten	Befehl	Beschreibung
enable	show sfp info port PORT_ID	Mit diesem Befehl werden die SFP-Informationen angezeigt.
enable	show sfp ddmi port PORT_ID	Mit diesem Befehl wird der SFP-DDMI-Status angezeigt.

10.3.5.5 Traffic Monitor

Tabelle 155: CLI-Konfiguration „Traffic Monitor“

Knoten	Befehl	Beschreibung
enable	show traffic-monitor	Mit diesem Befehl werden die Konfigurationen und der aktuelle Status für den „Traffic Monitor“ angezeigt.
configure	traffic-monitor (disable | enable)	Mit diesem Befehl wird der „Traffic Monitor“ beim Switch aktiviert bzw. deaktiviert.
interface	traffic-monitor rate RATE_LIMIT type (bcast | mcast | bcast+mcast)	Mit diesem Befehl werden Paketrate und Pakettyp für den „Traffic Monitor“ bei einem spezifischen Port konfiguriert. mcast: Broadcast-Paket. mcast: Multicast-Paket. Die Rate sollte höher als 50 pps sein.
interface	traffic-monitor (disable | enable)	Mit diesem Befehl wird der „Traffic Monitor“ für einen spezifischen Port aktiviert bzw. deaktiviert.
interface	traffic-monitor recovery (disable | enable)	Mit diesem Befehl wird die „Recovery“-Funktion beim „Traffic Monitor“ für einen spezifischen Port aktiviert bzw. deaktiviert.
interface	traffic-monitor recovery time VALUE	Mit diesem Befehl wird die „Recovery Time“ beim „Traffic Monitor“ für einen spezifischen Port konfiguriert.

10.3.6 Management

10.3.6.1 SNMP

Tabelle 156: CLI-Konfiguration „SNMP“

Knoten	Befehl	Beschreibung
enable	show snmp	Mit diesem Befehl werden die SNMP-Konfigurationen angezeigt.
configure	snmp community STRING (ro | rw) trusted-host IPADDR	Mit diesem Befehl wird der Name für die „SNMP Community“ konfiguriert.
configure	snmp (disable | enable)	Mit diesem Befehl wird das SNMP für den Switch deaktiviert bzw. aktiviert.
configure	snmp system-contact STRING	Mit diesem Befehl werden die Kontaktinformationen für das System konfiguriert.
configure	snmp system-location STRING	Mit diesem Befehl werden die Standortinformationen des Systems konfiguriert.
configure	snmp system-name STRING	Mit diesem Befehl wird dem System ein Name zugewiesen.
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	Mit diesem Befehl werden die Konfigurationen für den Trap-Empfänger, einschließlich IP-Adresse, Version (v1 oder v2c) und die „Community“, eingerichtet.

Beispiel

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*

10.3.6.2 Auto Provision

Tabelle 157: CLI-Konfiguration „Auto Provision“

Knoten	Befehl	Beschreibung
auto-provision	show	Mit diesem Befehl werden die aktuellen Konfigurationen für die „Auto Provision“ angezeigt.
auto-provision	active (enable | disable)	Mit diesem Befehl wird die Funktion „Auto Provision“ aktiviert bzw. deaktiviert.
auto-provision	server-address IPADDR	Mit diesem Befehl wird die IP-Adresse des Servers für die „Auto Provision“ festgelegt.
auto-provision	protocol (tftp | http | ftp)	Mit diesem Befehl wird das Aktualisierungsprotokoll konfiguriert.
auto-provision	FTP-user username STRING password STRING	Mit diesem Befehl werden Benutzername und Passwort für den FTP-Server konfiguriert.
auto-provision	folder STRING	Mit diesem Befehl wird der Ordner für den Server der „Auto Provision“ festgelegt.
auto-provision	version <0-65535>	Mit diesem Befehl wird die Version der „Auto Provision“ beim Switch konfiguriert.
auto-provision	no folder	Mit diesem Befehl wird der Ordner auf die Default-Einstellung zurückgesetzt.
auto-provision	no FTP-user	Mit diesem Befehl werden Benutzername und Passwort auf die Default-Einstellung zurückgesetzt.

10.3.6.3 Mail Alarm

Tabelle 158: CLI-Konfiguration „Mail Alarm“

Knoten	Befehl	Beschreibung
enable	show mail-alarm	Mit diesem Befehl werden die Konfigurationen für den „Mail Alarm“ angezeigt.
configure	mail-alarm (disable | enable)	Mit diesem Befehl wird die Funktion „Mail Alarm“ aktiviert bzw. deaktiviert.
configure	mail-alarm mail-from	Mit diesem Befehl wird der E-Mail-Absender konfiguriert.
configure	mail-alarm mail-to	Mit diesem Befehl wird der E-Mail-Empfänger konfiguriert.
configure	mail-alarm server-ip IPADDR server-port VALUE	Mit diesem Befehl werden IP-Adresse und TCP-Port des Mail-Servers konfiguriert.
configure	mail-alarm server-ip IPADDR server-port Default	Mit diesem Befehl wird die IP-Adresse des Mail-Servers konfiguriert und sein TCP-Port auf den Wert 25 gesetzt.
configure	mail-alarm trap-event (reboot | link-change | config. | firmware | login | port-blocked) (disable|enable)	Mit diesem Befehl wird das Versenden von Ereignis-Traps aktiviert bzw. deaktiviert.

10.3.6.4 Wartung

Tabelle 159: CLI-Konfiguration „Wartung“

Knoten	Befehl	Beschreibung
configure	reboot	Mit diesem Befehl wird das System neu gestartet.
configure	reload default-config	Mit diesem Befehl wird die Systemkonfiguration auf die Default-Einstellungen zurückgesetzt. Hinweis: Das System wird automatisch neu gestartet, damit die Konfigurationen angewendet werden.
configure	write memory	Mit diesem Befehl werden die aktuellen Betriebskonfigurationen in die Konfigurationsdatei geschrieben.
configure	archive download-config <URL PATH>	Mit diesem Befehl wird eine aktualisierte Konfigurationsdatei vom TFTP-Server heruntergeladen. Wobei <URL PATH> für Folgendes stehen kann: 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>	Mit diesem Befehl wird die aktuelle Konfigurationsdatei auf den TFTP-Server hochgeladen.
configure	archive download-fw <URL PATH>	Mit diesem Befehl wird eine aktualisierte Firmware-Datei vom TFTP-/FTP-/HTTP-Server heruntergeladen. Wobei <URL PATH> für Folgendes stehen kann: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Beispiel

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*

10.3.6.5 System Log

Tabelle 160: CLI-Konfiguration „System Log“

Knoten	Befehl	Beschreibung
enable	show syslog	Mit diesem Befehl werden alle im Switch aufgezeichneten Protokollnachrichten angezeigt.
enable	show syslog level LEVEL	Mit diesem Befehl wird die im Switch aufgezeichnete Protokollnachricht mit der Ebene „LEVEL“ angezeigt.
enable	show syslog server	Mit diesem Befehl werden die Konfigurationen des Syslog-Servers angezeigt.
configure	syslog (disable | enable)	Mit diesem Befehl wird die Systemprotokollfunktion aktiviert bzw. deaktiviert.
configure	syslog ip IPADDR	Mit diesem Befehl wird die IP-Adresse des Syslog-Servers konfiguriert.

Beispiel

L2SWITCH#*configure terminal*

L2SWITCH(config)#*syslog-server ip 192.168.200.106*

L2SWITCH(config)#*syslog-server enable*

10.3.6.6 User Account

Tabelle 161: CLI-Konfiguration „System Log“

Knoten	Befehl	Beschreibung
enable	show user account	Mit diesem Befehl werden die aktuellen Benutzerkonten angezeigt.
configure	add user USER_ACCOUNT PASSWORD (normal | admin)	Mit diesem Befehl wird ein neues Benutzerkonto hinzugefügt.
configure	delete user USER_ACCOUNT	Mit diesem Befehl wird ein bestehendes Benutzerkonto gelöscht.

Beispiel

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. The wichtigsten 4 Arten sind:

Tabelle 162: Datenformat und Funktionscode

Datenzugriffstyp		Funk-tionscode	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-Basisadresse des Industrial-Managed-Switches ist 1001 (dezimal) für Funktionscode 4.

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
Systeminformation			
0x0000	1 word	HEX	Vendor ID = 0x0b04
0x0001	16 words	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’
0x1020	16 words	ASCII	Product Name = “INS-8528”
			Word 0 Hi byte = ‘I’
			Word 0 Lo byte = ‘N’
			Word 1 Hi byte = ‘S’
			Word 1 Lo byte = ‘-’
			Word 2 Hi byte = ‘8’
			Word 2 Lo byte = ‘5’
			Word 3 Hi byte = ‘2’
			Word 3 Lo byte = ‘8’
			Word 4 Hi byte = ‘\0’
			Word 4 Lo byte = ‘\0’
0x0040	7 words		Product Serial Number
			Ex: Serial No=A000000000001

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0050	12 words	ASCII	Firmware Version=” 8528-000-1.1.0.b1”
			Word 0 Hi byte = ‘8’
			Word 0 Lo byte = ‘5’
			Word 1 Hi byte = ‘2’
			Word 1 Lo byte = ‘8’
			Word 2 Hi byte = ‘-’
			Word 2 Lo byte = ‘0’
			Word 3 Hi byte = ‘0’
			Word 3 Lo byte = ‘0’
			Word 4 Hi byte = ‘-’
			Word 4 Lo byte = ‘1’
			Word 5 Hi byte = ‘.’
			Word 5 Lo byte = ‘1’
			Word 6 Hi byte = ‘.’
			Word 6 Lo byte = ‘0’
			Word 7 Hi byte = ‘.’
			Word 7 Lo byte = ‘b’
			Word 8 Hi byte = ‘1’
			Word 8 Lo byte = ‘\0’
0x0060	16 words	ASCII	Firmware Release Date=” Mon Sep 30 18:51:45 2013”
0x0070	3 words	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
0x0080	1 word	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
0x0081	1 word	HEX	**Power 2(RPS) Alarm, DIP switch 1 need ON**
			0x0000: no alarm
			0x0001: input voltage < 11.7V
			0x0002: input voltage > 57V
			0x0003: No RPSinput
0x0090	1 word	HEX	**Fault LED Status**
			0x0000: No
			0x0001: Yes

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
Port Information			
0x0100 to 0x0109	1 word	HEX	Port 1 to 10 Link Status
			0x0000: Link down
			0x0001: 10M-Full-FC_ON (FC: Flow Control)
			0x0002: 10M-Full-FC_OFF
			0x0003: 10M-Half-FC_ON
			0x0004: 10M-Half-FC_OFF
			0x0005: 100M-Full-FC_ON
			0x0006: 100M-Full-FC_OFF
			0x0007: 100M-Half-FC_ON
			0x0008: 100M-Half-FC_OFF
			0x0009: 1000M-Full-FC_ON
			0x000A: 1000M-Full-FC_OFF
			0x000B: 1000M-Half-FC_ON
			0x000C: 1000M-Half-FC_OFF
			0xFFFF: No port
0x0200 to 0x021f (port 1) 0x0220 to 0x023f (port 2) … 0x0320 to 0x033f (port 10)	20 words	ASCII	Port 1 to 10 Medium
			Port Description = “100TX,RJ45.” Or
			“1000TX,SFP.”
			Word 0 Hi byte = ‘1’
			Word 0 Lo byte = ‘0’
			Word 1 Hi byte = ‘0’
			Word 1 Lo byte = ‘T’
			…
			Word 4 Hi byte = ‘4’
			Word 4 Lo byte = ‘5’
			Word 5 Hi byte = ‘.’
			Word 5 Lo byte = ‘\0’
0x0400 to 0x0413 (port 1 to 10)	2 words	HEX	Port 1 to 10 Tx Packets
			Ex: port 1 Tx Packet Amount = 0x87654321
			Word 0 =8765
			Word 1 = 4321
0x0440 to 0x0453 (port 1 to 10)	2 words	HEX	Port 1 to 10 Rx Packets
			Ex: port 1 Rx Packet Amount = 0x123456
			Word 0 = 0012
			Word 1 = 3456
0x0480 to 0x0493 (port 1 to 10)	2 words	HEX	Port 1 to 10 Tx Error Packets
			Ex: port 1 Tx Error Packet Amount = 0x87654321
			Word 0 =8765
			Word 1 = 4321
0x04C0 to 0x04D3 (port 1 to 10)	2 words	HEX	Port 1 to 10 Rx Error Packets
			Ex: port 1 Rx Error Packet Amount = 0x123456
			Word 0 = 0012
			Word 1 = 3456

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
Redundancy & Ring Information			
0x0500	2 word	HEX	**Spanning Tree Status**
			0x0000 : none
			0x0001 : STP
			0x0002 : RSTP
			0x0003 : MSTP
0x0501	1 word	HEX	**Xpress-ring Status**
			0x0000 : Disabled
			0x0001 : Enabled
0x0502	1 word	HEX	**Jet-ring Status**
			0x0000 : Disabled
			0x0001 : Enabled
0x0503	1 word	HEX	**Dual-ring Status**
			0x0000 : Disabled
			0x0001 : Enabled
0x0504	1 word	HEX	**ERPS Status**
			0x0000 : Disabled
			0x0001 : Enabled
0x0510	2 word	HEX	**Xpress-ring Status**
			Ring 1
			0x0000 : **Disabled**
			0x0001 : **Enabled**
0x0511			***Ring 2***
			0x0000 : **Disabled**
			0x0001 : **Enabled**
0x0512	6 word	HEX	**Xpress-ring MAC**
			Ring 1
			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
0x0515			***Ring 2***
			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
0x0518	2 word	HEX	**Xpress-ring Role**
			Ring 1
			0x0000 : **Forwarder**
			0x0001 : **Arbiter**
0x0519			***Ring 2***
			0x0000 : **Forwarder**
			0x0001 : **Arbiter**

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0520	2 word	HEX	**Xpress-ring Current status for Ring 1**
			Ring 1 – Primary Port
			0x0000 : No connection
			0x0001 : Forwarding
			0x0002 : Blocking
0x0521			***Ring 1 – Secondary Port***
			0x0000 : No connection
			0x0001 : Forwarding
			0x0002 : Blocking
0x0522	2 word	HEX	**Xpress-ring Current status for Ring 2**
			Ring 2 – Primary Port
			0x0000 : No connection
			0x0001 : Forwarding
			0x0002 : Blocking
0x0523			***Ring 2 – Secondary Port***
			0x0000 : No connection
			0x0001 : Forwarding
			0x0002 : Blocking
Jet-Ring Information			
0x0600	1 word	Hex	Jet Ring State
			0x0000: Disabled.
			0x0001: Enabled.
0x0601	3 word	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.
0x0604	1 word	Hex	Jet Ring Total Nodes.
			Ex: When total nodes is 255(0xff).
			Word 0, high byte=0x00.
			Word 0, low byte=0xff.
0x0605	1 word	Hex	Bridge Role:
			0x0000: Learning.
			0x0001: Master.
			0x0002: Arbiter.
			0x0003: Forwarder.
			0x0004: Pre-Forwarder.
0x0610 to 0x062F	1 word	Hex	Port Role:
			0x0000: Disabled.
			0x0001: Listening.
			0x0002: Learning.
			0x0003: Forwarding.
			0x0004: Blocking.
			0x0005: No connection.

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0630 to 0x064F	1 word	Hex	Ring Port:
			0x0000: No
			0x0001: Yes
Dual-Ring Information			
0x0700	1 word	Hex	**Dual- Ring State:**
			0x0000: Disabled.
			0x0001: Enabled.
0x0701	3 word	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.
0x0704	1 word	Hex	**Xpress-ring Role for Dual-Ring:**
			0x0000 : **Forwarder**
			0x0001 : **Arbiter**
0x0705	2 word	Hex	**Xpress-ring Current status for Dual-Ring**
			Port-1 – (Primary Port)
			High byte – Port No.
			0x01~ 0x0a: Port 1~Port 10
			Low byte – Port Status
			0x00 : No connection
			0x01 : Forwarding
			0x02 : Blocking
			Ex: 0x0501– Port 5 Forwarding
			0x0b02 – Port 12 Blocking
0x0706			***Port-2 – (Secondary Port)***
			High byte – Port No.
			0x01~ 0x0a: Port 1~Port 10
			Low byte – Port Status
			0x00 : No connection
			0x01 : Forwarding
			0x02 : Blocking
			Ex: 0x0501– Port 5 Forwarding
			0x0b02 – Port 12 Blocking
0x0707	3 word	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.
0x070a	1 word	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.

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x070b	1 word	Hex	**Bridge Role for Sub-Ring:**
			0x0000: Learning.
			0x0001: Master.
			0x0002: Arbiter.
			0x0003: Forwarder.
			0x0004: Pre-Forwarder.
0x070c	2 Word	Hex	**Sub-ring Current status for Dual-Ring**
			Subport-1 – (Primary Port)
			High byte – Port No.
			0x01~ 0x0a: Port 1~Port 10
			Low byte – Port Status
			0x00 : No connection
			0x01 : Forwarding
			0x02 : Blocking
			Ex: 0x0501– Port 5 Forwarding
			0x0b02 – Port 12 Blocking
0x070d			***Subport-2 – (Secondary Port)***
			High byte – Port No.
			0x01~ 0x0a: Port 1~Port 10
			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)			
0x0800	1 word	Hex	**Ring ID for ERPSn (n=1)**
			Ex: 0x001 Ring ID=1
0x0801	1 word	Hex	**State for ring of ERPS**
			0x0000: Disabled.
			0x0001: Enabled.
0x0802	33 words	Hex	**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’
0x0823	1 word	Hex	**Version & Ring Type**
			High byte – Version.
			Low byte – Ring Type.
			0x01:Major-ring
			0x02:Sub-ring
			Ex: 0x0201– Version2, Type:Major-ring
0x0824	1 word	Hex	**Instance of Ring**
			Ex: 0x0001 Instance ID=1

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0825	1 word	Hex	**Control VLAN of Ring**
			E:0x000b Control VLAN=11
0x0826	1 word	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
0x0827	1 word	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
0x0828	1 word	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
0x0829	1 word	Hex	**Ring ID for ERPSn (n=2)**
0x082a	1 word	Hex	**State for ring of ERPS**
0x082b	33 words	Hex	**Name of Ring**
0x084c	1 word	Hex	**Version & Ring Type**
0x084d	1 word	Hex	**Instance of Ring**
0x084e	1 word	Hex	**Control VLAN of Ring**
0x084f	1 word	Hex	**Right Port of Ring**
0x0850	1 word	Hex	**Left Port of Ring**
0x0851	1 word	Hex	**Ring port state**
0x0852	1 word	Hex	**Ring ID for ERPSn (n=3)**
0x0853	1 word	Hex	**State for ring of ERPS**
0x0854	33 words	Hex	**Name of Ring**
0x0875	1 word	Hex	**Version & Ring Type**
0x0876	1 word	Hex	**Instance of Ring**
0x0877	1 word	Hex	**Control VLAN of Ring**
0x0878	1 word	Hex	**Right Port of Ring**
0x0879	1 word	Hex	**Left Port of Ring**
0x087a	1 word	Hex	**Ring port state**

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x087b	1 word	Hex	**Ring ID for ERPSn (n=4)**
0x087c	1 word	Hex	**State for ring of ERPS**
0x087d	33 words	Hex	**Name of Ring**
0x089e	1 word	Hex	**Version & Ring Type**
0x089f	1 word	Hex	**Instance of Ring**
0x08a0	1 word	Hex	**Control VLAN of Ring**
0x08a1	1 word	Hex	**Right Port of Ring**
0x08a2	1 word	Hex	**Left Port of Ring**
0x08a3	1 word	Hex	**Ring port state**
0x08a4	1 word	Hex	**Ring ID for ERPSn (n=5)**
0x08a5	1 word	Hex	**State for ring of ERPS**
0x08a6	33 words	Hex	**Name of Ring**
0x08c7	1 word	Hex	**Version & Ring Type**
0x08c8	1 word	Hex	**Instance of Ring**
0x08c9	1 word	Hex	**Control VLAN of Ring**
0x08ca	1 word	Hex	**Right Port of Ring**
0x08cb	1 word	Hex	**Left Port of Ring**
0x08cc	1 word	Hex	**Ring port state**
0x08cd	1 word	Hex	**Ring ID for ERPSn (n=6)**
0x08ce	1 word	Hex	**State for ring of ERPS**
0x08cf	33 words	Hex	**Name of Ring**
0x08f0	1 word	Hex	**Version & Ring Type**
0x08f1	1 word	Hex	**Instance of Ring**
0x08f2	1 word	Hex	**Control VLAN of Ring**
0x08f3	1 word	Hex	**Right Port of Ring**
0x08f4	1 word	Hex	**Left Port of Ring**
0x08f5	1 word	Hex	**Ring port state**
MSTP Information			
0x0900	1 word	Hex	**Instance ID (Fixed 0x00, 0)**
			High byte –Instance ID.
			Low byte –Used State.
			0x01: used
			0x00: non used
0x0901	3 word	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 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0904	1 word	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
0x0905	1 word	Hex	**Port 2 status**
0x0906	1 word	Hex	**Port 3 status**
0x0907	1 word	Hex	**Port 4 status**
0x0908	1 word	Hex	**Port 5 status**
0x0909	1 word	Hex	**Port 6 status**
0x090a	1 word	Hex	**Port 7 status**
0x090b	1 word	Hex	**Port 8 status**
0x090c	1 word	Hex	**Port 9 status**
0x090d	1 word	Hex	**Port 10 status**
0x090e	1 word	Hex	**Port 11 status**
0x090f	1 word	Hex	**Port 12 status**
0x0920	1 word	Hex	**Instance ID (Fixed 0x01, 1)**
0x0940	1 word	Hex	**Instance ID (Fixed 0x02, 2)**
0x0960	1 word	Hex	**Instance ID (Fixed 0x03, 3)**
0x0980	1 word	Hex	**Instance ID (Fixed 0x04, 4)**
0x09a0	1 word	Hex	**Instance ID (Fixed 0x05, 5)**
0x09c0	1 word	Hex	**Instance ID (Fixed 0x06, 6)**
0x09e0	1 word	Hex	**Instance ID (Fixed 0x07, 7)**
0x0a00	1 word	Hex	**Instance ID (Fixed 0x08, 8)**
0x0a20	1 word	Hex	**Instance ID (Fixed 0x09, 9)**
0x0a40	1 word	Hex	**Instance ID (Fixed 0x0a, 10)**
0x0a60	1 word	Hex	**Instance ID (Fixed 0x0b, 11)**
0x0a80	1 word	Hex	**Instance ID (Fixed 0x0c, 12)**
0x0aa0	1 word	Hex	**Instance ID (Fixed 0x0d, 13)**

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x0ac0	1 word	Hex	**Instance ID (Fixed 0x0e, 14)**
0x0ae0	1 word	Hex	**Instance ID (Fixed 0x0f, 15)**
0x0b00	1 word	Hex	**Instance ID (Fixed 0x10, 16)**
0x0b20	1 word	Hex	**Instance ID (Fixed 0x11, 17)**
0x0b40	1 word	Hex	**Instance ID (Fixed 0x12, 18)**
0x0b60	1 word	Hex	**Instance ID (Fixed 0x13, 19)**
0x0b80	1 word	Hex	**Instance ID (Fixed 0x14, 20)**
0x0ba0	1 word	Hex	**Instance ID (Fixed 0x15, 21)**
0x0bc0	1 word	Hex	**Instance ID (Fixed 0x16, 22)**
0x0be0	1 word	Hex	**Instance ID (Fixed 0x17, 23)**
0x0c00	1 word	Hex	**Instance ID (Fixed 0x18, 24)**
0x0c20	1 word	Hex	**Instance ID (Fixed 0x19, 25)**
0x0c40	1 word	Hex	**Instance ID (Fixed 0x1a, 26)**
0x0c60	1 word	Hex	**Instance ID (Fixed 0x1b, 27)**
0x0c80	1 word	Hex	**Instance ID (Fixed 0x1c, 28)**
0x0ca0	1 word	Hex	**Instance ID (Fixed 0x1d, 29)**
0x0cc0	1 word	Hex	**Instance ID (Fixed 0x1e,30)**
0x0ce0	1 word	Hex	**Instance ID (Fixed 0x1f, 31)**
0x0d00	1 word	Hex	**Instance ID (Fixed 0x20, 32)**
0x0d20	1 word	Hex	**Instance ID (Fixed 0x21, 33)**
0x0d40	1 word	Hex	**Instance ID (Fixed 0x22, 34)**
0x0d60	1 word	Hex	**Instance ID (Fixed 0x23, 36)**
0x0d80	1 word	Hex	**Instance ID (Fixed 0x24, 36)**
0x0da0	1 word	Hex	**Instance ID (Fixed 0x25, 37)**
0x0dc0	1 word	Hex	**Instance ID (Fixed 0x26, 38)**
0x0de0	1 word	Hex	**Instance ID (Fixed 0x27, 39)**
0x0e00	1 word	Hex	**Instance ID (Fixed 0x28, 40)**
0x0e20	1 word	Hex	**Instance ID (Fixed 0x29, 41)**
0x0e40	1 word	Hex	**Instance ID (Fixed 0x2a, 42)**
0x0e60	1 word	Hex	**Instance ID (Fixed 0x2b, 43)**
0x0e80	1 word	Hex	**Instance ID (Fixed 0x2c, 44)**
0x0ea0	1 word	Hex	**Instance ID (Fixed 0x2d, 45)**
0x0ec0	1 word	Hex	**Instance ID (Fixed 0x2e, 46)**
0x0ee0	1 word	Hex	**Instance ID (Fixed 0x2f, 47)**
0x0f00	1 word	Hex	**Instance ID (Fixed 0x30, 48)**
0x0f20	1 word	Hex	**Instance ID (Fixed 0x31, 49)**
0x0f40	1 word	Hex	**Instance ID (Fixed 0x32, 50)**
0x0f60	1 word	Hex	**Instance ID (Fixed 0x33, 51)**
0x0f80	1 word	Hex	**Instance ID (Fixed 0x34, 52)**
0x0fa0	1 word	Hex	**Instance ID (Fixed 0x35, 53)**
0x0fc0	1 word	Hex	**Instance ID (Fixed 0x36, 54)**
0x0fe0	1 word	Hex	**Instance ID (Fixed 0x37, 55)**

Tabelle 163: MODBUS-Register

Register-adresse	Datentyp	Dar-stellung	Beschreibung
0x1000	1 word	Hex	**Instance ID (Fixed 0x38, 56)**
0x1020	1 word	Hex	**Instance ID (Fixed 0x39, 57)**
0x1040	1 word	Hex	**Instance ID (Fixed 0x3a, 58)**
0x1060	1 word	Hex	**Instance ID (Fixed 0x3b, 59)**
0x1080	1 word	Hex	**Instance ID (Fixed 0x3c, 60)**
0x10a0	1 word	Hex	**Instance ID (Fixed 0x3d, 61)**
0x10c0	1 word	Hex	**Instance ID (Fixed 0x3e, 62)**
0x10e0	1 word	Hex	**Instance ID (Fixed 0x3f, 63)**

Abbildungsverzeichnis

Tabellenverzeichnis

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