TECHDOCS

Handbuch

WAGO-Industrial-Switches

852-1813/010-000

Lean-Managed-Switch

8 Ports 1000BASE-T; 2 Slots 1000-FX/TX

Version 1.0.0

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 „Lean-Managed-Switch“ (852-1813/010-000).

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. EN 418).

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

- Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß EN 61340-5-1/-3. Stellen Sie bei der Verwendung der Module sicher, dass die Umgebungsfaktoren (Personen, Arbeitsplatz und Verpackung) geerdet sind.

- Die für die Installation von Switch-Gehäusen geltenden Richtlinien und Bestimmungen müssen eingehalten werden.

2.2 Sicherheitshinweise

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

GEFAHR

Nicht an Geräten unter Spannung arbeiten!
Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie es montieren, Störungen beheben oder Wartungsarbeiten vornehmen.

GEFAHR

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

GEFAHR

Unfallverhütungsvorschriften beachten!
Beachten Sie bei Montage, Inbetriebnahme, Betrieb, Wartung und Störbehebung die für Ihre Maschine/Anlage zutreffenden 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.

ACHTUNG

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

ACHTUNG

Nur mit zulässigen Materialien reinigen!
Reinigen Sie das Gehäuse und verschmutzte Kontakte mit Propanol.

ACHTUNG

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

ACHTUNG

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

ESD

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

VORSICHT

Warnung vor Laserstrahlung!
Sehen Sie nicht in die Öffnungen der Anschlüsse hinein, wenn kein Kabel angeschlossen ist, um sich nicht der Strahlung auszusetzen.
Es kann eine nicht sichtbare Laserstrahlung emittieren.
Dabei handelt es sich um eine Laser Klasse 1 nach EN 60825-1.

Hinweis

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

2.3 Spezielle Einsatzbestimmungen für ETHERNET-Geräte

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

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

3 Einleitung

3.1 Lieferumfang

- 1 Industrial-Lean-Managed-Switch mit CAGE CLAMP®-Anschluss (Bestell-Nr. 2231-106/026-000)
- Schutzabdeckungen für nicht verwendete Anschlüsse
- Gebrauchs- und Montageanleitung

3.2 Industrial-ETHERNET-Technologie

Die robusten Lean-Managed-Switches sind für den Industrieeinsatz ausgelegt und kompatibel zu folgenden Standards:

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX/FX
- IEEE 802.3ab 1000BASE-T Ethernet
- IEEE 802.3z 1000BASE-SX/LX/ZX
- IEEE 802.3x Flow Control
- IEEE 802.1d Spanning Tree Protocol (STP)
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Prioritization
- IEEE 802.1x Port Authentication
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- IEEE 802.1AB LLDP-MED
- IEEE 802.3az Energy Efficient Ethernet (EEE)
- ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

Die Switches verfügen über eine Spannungsversorgung mit einem Versorgungsspannungsbereich 24 … 48 V.

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

3.3 Switching-Technologie

Im Industrial ETHERNET wird vorwiegend die Switching-Technologie genutzt. Bei dieser Technologie kann jeder Netzwerkteilnehmer jederzeit senden, da er immer über eine freie Punkt-zu-Punkt-Verbindung zum nächsten Switch verfügt. Diese Verbindung ist bidirektional, das heißt, die Teilnehmer können gleichzeitig senden und empfangen (Vollduplex).
Der gezielte Einsatz der Switching-Technologie kann die Echtzeitfähigkeit erhöhen, da durch die Punkt-zu-Punkt-Verbindung Kollisionen in der Netzwerkkommunikation vermieden werden.

3.4 Autonegotiation

Autonegotiation ermöglicht es dem Switch, für jeden Port und den daran angeschlossenen Teilnehmer bzw. die Teilnehmer die Übertragungsrate und die Betriebsart zu erkennen und entsprechend automatisch einzustellen. Dabei wird der höchstmögliche Modus (Übertragungsgeschwindigkeit und Betriebsart) eingestellt.
Autonegotiation ist für ETHERNET-Teilnehmer verfügbar, die über Kupferkabel mit dem Switch verbunden sind.
Somit ist der Switch ein Plug-and-Play-fähiges Gerät.

3.5 Autocrossing

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

3.6 Store-and-Forward-Switching-Modus

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

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

Vorteil von „Store and Forward“:
Die Datentelegramme werden auf ihre Korrektheit und Gültigkeit geprüft. Dadurch wird verhindert, dass fehlerhafte bzw. beschädigte Datentelegramme über das Netzwerk verteilt werden.

3.7 Übertragungsmethoden

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

- Halbduplex (Half Duplex)
  - Ein ETHERNET-Gerät kann zu einem Zeitpunkt entweder nur empfangen oder nur senden.
  - Die Erkennung von Kollisionen (CSMA/CD) ist aktiv.
  - Die Netzausdehnung ist durch die Laufzeitverzögerungen der Geräte und Übertragungsmedien begrenzt.

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

4 Gerätebeschreibung

Der 852-1813/010-000 ist ein industrieller, konfigurierbarer ETHERNET-Switch mit 8 Ports 10/100/1000BASE-T und 2 Ports SFP 100BASE-FX/1000BASE-LX/SX/ZX (SFP-Module sind optional erhältlich).
Der Switch besitzt ein robustes Gehäuse, eine redundante Spannungsversorgung und eine Funktionsüberwachung mit Relais. Der Switch bietet ein schlankes Netzwerkmanagement.: Inbetriebnahme und Diagnose sind intuitiv und ohne tiefgehende IT-Kenntnisse möglich.
Die Topology-Map stellt den Switch und die angeschlossenen Teilnehmer übersichtlich dar. Im Diagnose-Dashboard werden wichtige Diagnoseinformationen visualisiert.

Sicherheit:
- Netzwerksegmentierung gemäß IEEE802.1Q (max. 5 VLANs),
- Authentifizierung von Netzwerkteilnehmern gemäß IEEE802.1X,
- Firewall-Funktionen mit Hilfe der Access-Control-List (max. 32 Einträge),
- Service Control,
- Port Security

Verfügbarkeit:
- Rapid Spanning Tree Protocol (RSTP) für vermaschte und Ringnetzwerke,
- ETHERNET Ring Protection Switching (ERPS) für bis zu zwei Ringe pro Switch,
- Loop Detection und
- Storm Control an jedem Port

Konfiguration/Diagnose/Wartung:
- Port Mirroring,
- Modbus® Register,
- SNMP v3,
- SNMP-Traps Events,
- Alarm Threshold,
- Port Statistic,
- Back-up and Restore,
- System Log,
- Syslog Server,
- Commando Line Interface mit SSH/Telnet,
- Topology Map und
- Dashboard

4.1 Ansicht

4.1.1 Frontansicht

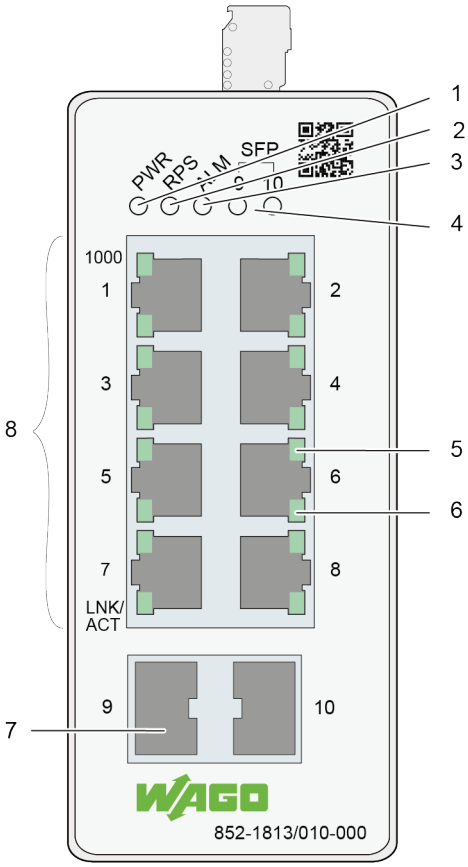


Abbildung 1: Frontansicht des Lean-Managed-Switches

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

Pos.	Be-zeich-nung	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	SFP	Status-LED SFP (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“
5	-	Status-LED T-Port 1000 Mbit/s (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“
6	-	Status-LED T-Port LNK/ACT (1 LED für jeden Anschluss)	„Gerätebeschreibung“ > „Anzeigeelemente“
7	-	Port SFP-Slot (1000BASE-SX/-LX/-ZX oder 100BASE-FX, Glasfaser (2)	„Gerätebeschreibung“ > „Anschlüsse“
8	-	Anschluss RJ-45 (10/100M/1000BASE-T) (8)	„Gerätebeschreibung“ > „Anschlüsse“

4.1.2 Draufsicht

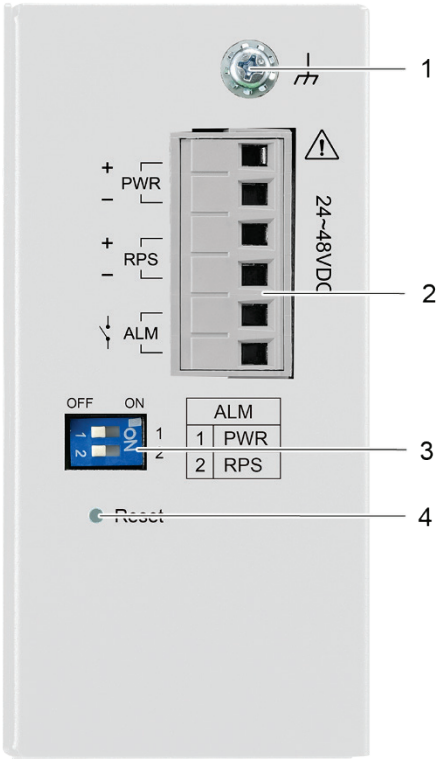


Abbildung 2: Draufsicht des Lean-Managed-Switches

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

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

4.2 Anschlüsse

4.2.1 Erdungsschraube

Der Switch muss geerdet werden.
Verbinden Sie dazu die Erdungsschraube mit dem Erdpotential.
Betreiben Sie den Switch nicht ohne einen entsprechend installierten Schutzleiter.

Abbildung 3: Erdungsschraube

4.2.2 Spannungsversorgung (PWR/RPS)

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

Die Stiftleiste hat folgende Belegung:

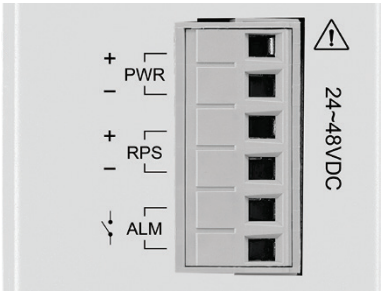


Abbildung 4: Anschluss Spannungsversorgung (PWR/RPS)

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

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

ESD

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

4.2.3 Netzwerkanschlüsse

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

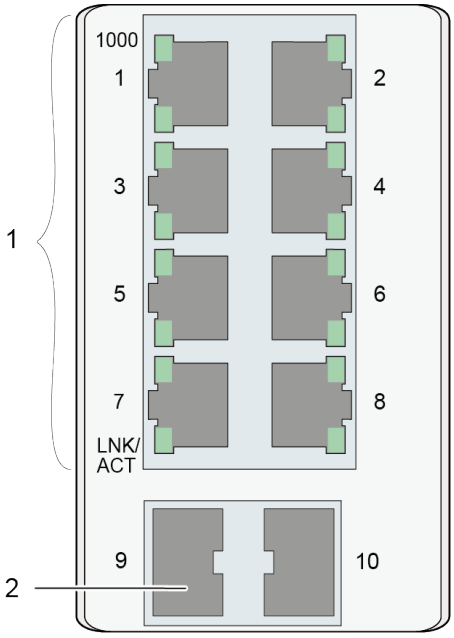


Abbildung 5: Netzwerkanschlüsse

Tabelle 6: Legende zur Abbildung „Netzwerkanschlüsse“

Pos.	Be-zeich-nung	Bedeutung	Details siehe Kapitel
1	-	Anschluss RJ-45 (10/100/1000BASE-T) (8)	„Gerätebeschreibung“ > … “10/100/1000BASE-T-Anschlüsse”
2	-	Anschluss SFP-Slots (1000BASE-SX/-LX/-ZX oder 100BASE-FX, Glasfaser) (2)	„Gerätebeschreibung“ > … „1000BASE-SX/-LX/-ZX oder 100BASE-FX-Anschlüsse“

4.2.3.1 RJ-45-Anschluss

Der Anschluss an die ETHERNET-basierten Feldbusse erfolgt über die RJ-45-Steckverbinder.
Die Pinbelegung für ETHERNET-RJ-45-Steckverbinder ist in der Richtlinie EIA/TIA 568 festgelegt.
Die Aderfarben entsprechen ebenfalls dieser Richtlinie. Pinbelegung und Aderfarbe unterscheiden sich nach der belegten Aderzahl (4- oder 8-adrig).

4.2.3.2 10/100/1000BASE-T-Anschlüsse

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

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

4.2.3.3 1000BASE-SX/-LX/-ZX oder 100BASE-FX-Anschlüsse

Die 1000BASE-SX/-LX/-ZX -Anschlüsse sind für den Anschluss der Gigabit-SFP-Module konzipiert, die Übertragungsgeschwindigkeiten von 100/1000 Mbit/s unterstützen.
Zusätzlich ist die Anbindung von 100BASE-FX mit einer Netzwerkgeschwindigkeit von 100 Mbit/s möglich.

4.3 Anzeigeelemente

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

4.3.1 Geräte-LEDs

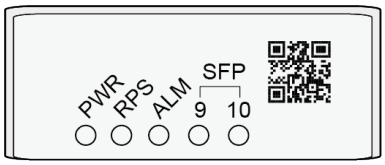


Abbildung 6: Geräte-LEDs

Tabelle 7: Legende zur Abbildung „Geräte-LEDs“

LED		Name	Status	Beschreibung
PWR		Primary Power LED	Grün	Verwendung des primären Netzteils
			Aus	Primäres Netzteil ausgeschaltet oder Fehler
RPS		Redundant Power System LED	Grün	Verwendung des sekundären Netzteils
			Aus	Sekundäres Netzteil ausgeschaltet oder Fehler
ALM		Alarm LED	Rot	Ausfall einer Port-Verbindung, sonstiger Alarm
			Aus	Kein Alarm gemeldet
SFP	9, 10	SFP-Anschluss-LED	Grün	SFP-Slot in Betrieb
			Blinkt	Datenverkehr über Anschluss
			Aus	Anschluss getrennt oder keine Verbindung

4.3.2 Anschluss-LEDs

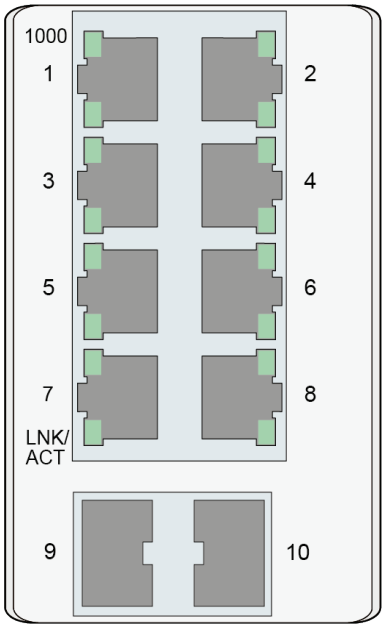


Abbildung 7: Anschluss-LEDs

Tabelle 8: Legende zur Abbildung „Anschluss-LEDs“

LED	Name	Status	Beschreibung
1000	1000BASE T-Anschluss-LED (1 LED für jeden Anschluss)	Grün	Anschluss mit 1000 Mbit/s in Betrieb
		Aus	Anschluss getrennt oder keine Verbindung
LNK/ACT	10/100BASE T-Anschluss-LED (1 LED für jeden Anschluss)	Grün	Anschluss mit 10/100/1000 Mbit/s in Betrieb
		Blinkt	Datenverkehr über Anschluss
		Aus	Anschluss getrennt oder keine Verbindung

4.4 Bedienelemente

4.4.1 DIP-Schalter

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

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

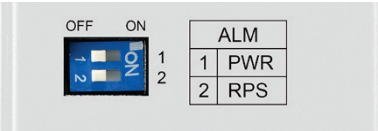


Abbildung 8: DIP-Schalter

Tabelle 9: Legende zur Abbildung „DIP-Schalter“

Nr.	Name	Status	Beschreibung
1	PWR	ON	Die 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.

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

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

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

1. Stellen Sie die DIP-Schalter auf „OFF“.
2. Installieren Sie den Lean-Managed-Switch in Ihrem Netzwerk.
3. Wählen Sie den die entsprechende Alarmfunktion, die sie aktivieren wollen.
4. Stellen Sie den DIP-Schalter des entsprechenden Anschlusses auf „ON“.
5. Schalten Sie den Lean-Managed-Switch ein.

4.4.2 Reset-Taster

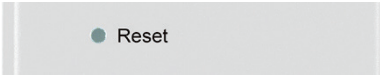


Abbildung 9: Reset-Taster

Tabelle 10: Legende zur Abbildung „Reset-Taster“

Name	Status	Beschreibung
Reset	Drücken Sie den Reset-Taster 2 Sekunden lang und lassen Sie ihn wieder los.	Das System wird neu gestartet.
Auslieferungszustand	Drücken Sie den Reset-Taster 10 Sekunden lang und lassen ihn wieder los.	Das System wird in den Auslieferungszustand zurückgesetzt.

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 Lean-Managed-Switches befindet sich ein Aufkleber mit der „MAC Address“ und der „Serial NO“.

Abbildung 10: Aufkleber

Tabelle 11: Legende zur Abbildung „Aufkleber“

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

4.6 Technische Daten

4.6.1 Gerätedaten

Tabelle 12: Technische Daten – Gerätedaten

Breite	50 mm
Höhe	116 mm (ab Oberkante Tragschiene)
Tiefe	100 mm
Gewicht	570 g
Schutzart	IP30

4.6.2 Systemdaten

Tabelle 13: Technische Daten – Systemdaten

MAC-Tabelle	bis 8000 Adresse
VLAN	Port-based und Tag-based (max. 5 VLANs)
Jumbo Frame Size	10 KB
Wellenlänge Lichtleiter	abhängig vom SFP-Modul
Maximum Längen	10/100/ 1000BASE-TX: 100 m; Glasfaser: abhängig vom SFP-Modul

4.6.3 Versorgung

Tabelle 3: Technische Daten – Versorgung

Versorgungsspannung	24 … 48 VDC (± 15 %) 24 … 48 VDC (UL)
Leistungsaufnahme, max.	11 W

4.6.4 Kommunikation

Tabelle 14: Technische Daten – Kommunikation

Ports (Kupfer; RJ-45)	8 x 10/100/1000BASE-T
Ports (LWL)	2 x 1000BASE-SX/-LX/-ZX oder 100BASE-FX (SFP-Slot)
Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/FX IEEE 802.3ab 1000BASE-T Ethernet IEEE 802.3z 1000BASE-SX/LX/ZX IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Prioritization IEEE 802.1x Port Authentication IEEE 802.1ab Link Layer Discovery Protocol (LLDP) IEEE 802.1AB LLDP-MED IEEE 802.3az Energy Efficient Ethernet (EEE) ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

4.6.5 Umgebungsbedingungen

Tabelle 15: Technische Daten – Umgebungsbedingungen

Umgebungstemperatur, Betrieb	-10 … +60 °C
Umgebungstemperatur, Lagerung	-40 … +85 °C
UL 61010 Nutzung Verschmutzungsgrad	Indoor 2
Relative Feuchte (Betrieb)	10 … 95 % (ohne Betauung)
Relative Feuchte (Lagerung)	5 … 95 % (ohne Betauung)
Vibrationsfestigkeit	gemäß IEC 60068-2-6
Schockfestigkeit	gemäß IEC 60068-2-27
EMV-Störfestigkeit	EN 55024 IEC 61000-4-2 IEC 61000-4-3 IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-6 IEC 61000-4-8 EN 61000-6-2
EMV-Störaussendung	FCC Part 15 Subpart B Klasse A EN 55011: Klasse A EN 55032: Klasse A EN 61000-6-4

4.7 Zulassungen

Folgende Zulassungen wurden für das WAGO-ETHERNET-Zubehör „Lean-Managed-Switch“ (852-1813/010-000) erteilt:

CE	Konformitätskennzeichnung	
c UL us	Ordinary Locations	UL61010-2-201 (E175199)

5 Montieren

5.1 Montageort

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

- Installieren Sie den Lean-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 Lean-Managed-Switch gewährleistet und die Belüftung um ihn herum angemessen ist. Platzieren Sie keine schweren Objekte auf dem Lean-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 Lean-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 Lean-Managed-Switch befindliche Metalllasche einführen und die Metalllasche nach unten auslenken.

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

6 Geräte anschließen

6.1 Spannungsversorgung

Der Switch verwendet eine Gleichstromversorgung, die für 24 … 48 V ausgelegt ist.

Die primäre und sekundäre Netzverbindung wird über eine 6-polige Steckverbindung hergestellt, die sich an der Oberseite des Lean-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 Switches stellt sich automatisch auf die lokale Stromquelle ein und kann auch eingeschaltet werden, wenn keine oder nicht alle Patchkabel angeschlossen sind.

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

2. Falls die Federleiste noch nicht in die Stiftleiste des Switches gesteckt wurde, stecken Sie sie jetzt. Überprüfen Sie den festen Sitz der Federleiste durch leichtes Rütteln.

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

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

5. RPS +/-:
   Zum Anschließen oder Lösen der Leiter für die sekundäre Spannungsversorgung betätigen Sie in der Federleiste direkt die Feder mit einem Schraubendreher oder Betätigungswerkzeug und führen den Leiter ein oder entfernen ihn.

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

6.2 Externer Alarmkontakt-Anschluss

Der Lean-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 Lean-Managed-Switch durch den Alarmkontakt gesendet. Der Alarmkontakt hat zwei Anschlüsse, die als Fehlerleitung zum Anschluss der Alarmanlage dienen.

Ein Alarm wird in folgenden Fällen gemeldet:

1 PWR/RPS:
   a Versorgungsfehler (Stromleitung ist unterbrochen, Versorgungsstörung, etc.)
   b Die Eingangsversorgungsspannung liegt außerhalb der Spezifikationen (24 … 48 V)
   c Port-Sperrung durch Loop-Detection
   d Broadcast/Multicast-Paketrate über dem Schwellwert

6.3 Anschluss 1000BASE-SX/-LX/-ZX, 100BASE-FX, Glasfaser

Achten Sie beim Verbinden des Glasfaserkabels mit einem 1000BASE-SX/-LX/-ZX oder mit einem 100BASE-FX-Anschluss am Industrial-witch 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- oder des 100BASE-FX-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-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-Switch darauf, ob die Verbindung hergestellt ist (siehe Kapitel „Gerätebeschreibung“ > … > „Anzeigeelemente“).

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

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

1. Verbinden Sie ein Ende eines verdrillten Kabels vom Typ Kategorie 3/4/5/5e mit einem verfügbaren RJ-45-Anschluss am Industrial-Switch und das andere Ende mit dem Anschluss des ausgewählten Netzwerkknotens.

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

7 Konfigurieren

7.1 Übersicht der Konfigurationsoptionen

Der Lean-Managed-Switch bietet drei Optionen für erweiterte Managementfunktionen:

7.1.1 Web-Based-Management

Eine menügesteuerte Benutzeroberfläche kann vom WBM („Web-Based-Management“) über die Protokolle „http“ oder „https“ aufgerufen werden.

Hinweis

Standardeinstellung
Standardmäßig ist der Lean-Managed-Switch auf das Protokoll „http“ eingestellt..

Hinweis

Weitere Informationen
Die ausführliche Beschreibung finden Sie im Kapitel „Konfiguration im Web-Based-Management-System (WBM)“.

7.1.2 Telnet- oder SSH-Verbindung

1. Verbinden Sie den Computer mit einem der ETHERNET-Ports.

2. Eröffnen Sie eine Telnet/SSH-Sitzung zur IP-Adresse des Switches. Verwenden Sie die Default-Werte, wenn dies Ihre erste Anmeldung ist.

Tabelle 16: Default-Einstellungen für den Telnet-Port

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

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

Hinweis

Verwendung von Protokoll „Telnet“
Wenn Sie das Protokoll „Telnet“ verwenden, müssen Sie diesen Dienst aktivieren (siehe Kapitel „Konfiguration im Web-Based-Management-System (WBM)“ > … > „Service Control“)

7.1.3 Zugriff über Konsolen-Port Command-Line-Interface (CLI)

Im Folgenden wird beschrieben, wie Sie die Gerätekonfiguration über den Konsolen-Port (CLI) anzeigen können.

1. Verbinden Sie den Computer über SSH oder Telnet mit dem Konsolen-Port (CLI) mit dem Switch.

2. Drücken Sie **[ENTER]**, um den Anmeldebildschirm aufzurufen.

```
L2SWITCH login:
```

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

```
L2SWITCH login: admin
L2SWITCH>
```

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

```
L2SWITCH>enable
user:admin
password: wago
```

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

```
L2SWITCH#show running-config
```

Hinweis

Weitere Informationen
Eine detaillierte Beschreibung finden Sie im Kapitel „Anhang“ > … > „Im Command Line Interface (CLI) konfigurieren“.

8 Diagnose mit Dashboard und Topologie-Map

Die Diagnosefunktion kann Benutzern und Netzwerkadministratoren bei der schnellen Zuordnung, Diagnose und Identifizierung von Problemen innerhalb eines Systems oder Netzwerks helfen. Es ist eine Art Netzwerkverwaltung, die dabei hilft, Probleme bei der Konnektivität, Leistung und anderen Netzwerkbereichen zu finden, und sie anschließend in einem Dashboard abbildet.

Hinweis

Ändern der Kachelfarben bei Schwellwertüberschreitungen
Zur Vereinfachung der Diagnose können Sie für den Fall einer Über- oder Unterschreitung eines Schwellwertes eine Änderung der Kachelfarben (rot, gelb und grün) einstellen (siehe Kapitel „Dashboard Configuration“).

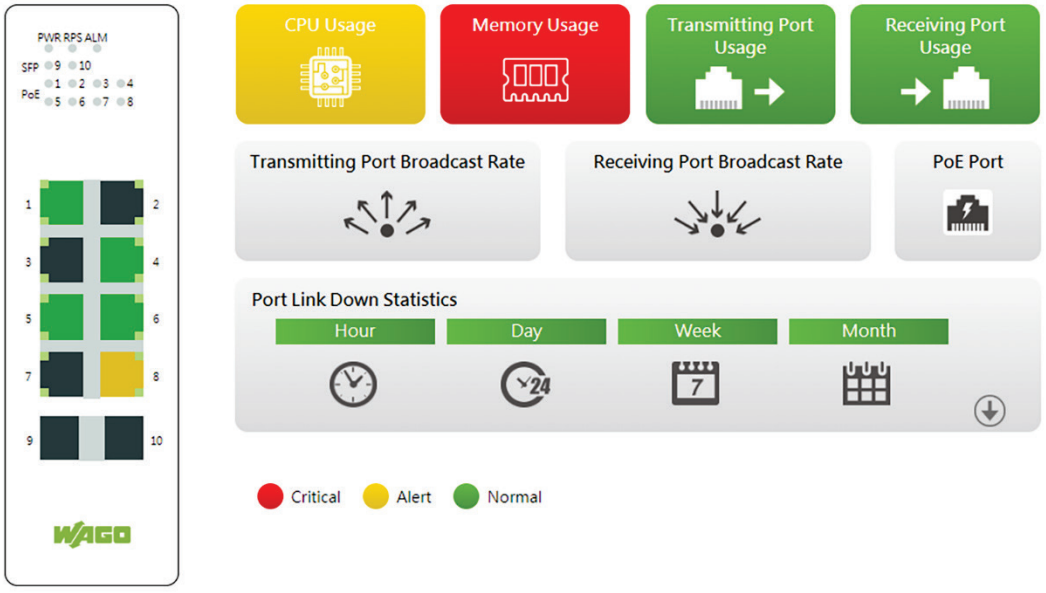


Abbildung 11: Dashboard (Beispiel)

8.1 Web-Based-Management für Diagnose-Funktion

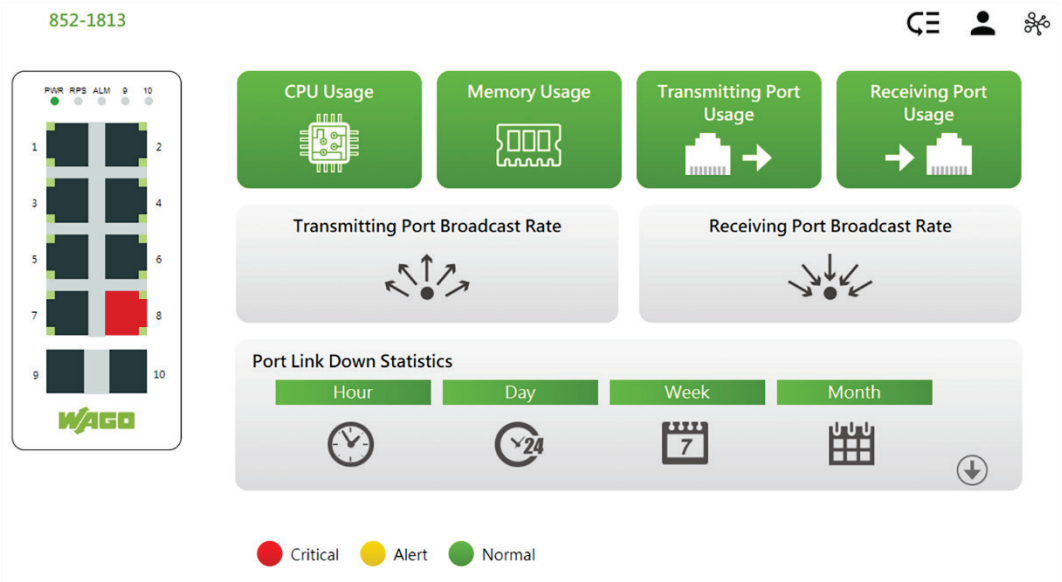


Abbildung 12: Dashboard

8.1.1 CPU-Auslastung

Benutzer können sich mit einem Klick die Auslastung der Switch-CPU als Prozentwert anzeigen lassen, wie unten dargestellt.

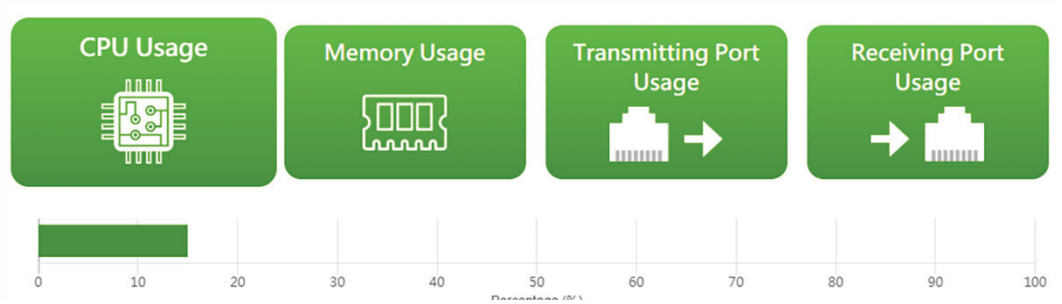


Abbildung 13: CPU-Auslastung

8.1.2 Speicherauslastung

Benutzer können sich mit einem Klick die Auslastung des Switch-Speichers als Prozentwert anzeigen lassen, wie unten dargestellt.

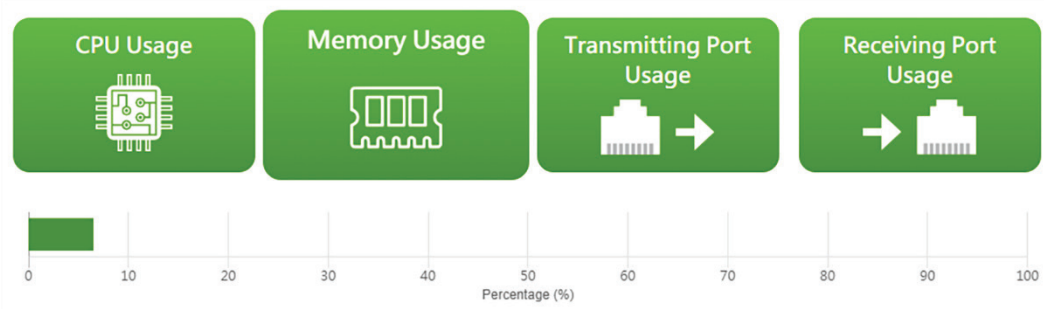


Abbildung 14: Speicherauslastung

8.1.3 Auslastung des Sende-Ports

Benutzer können sich mit einem Klick die Auslastung des Tx-Ports des Switches als Prozentwert anzeigen lassen, wie unten dargestellt.

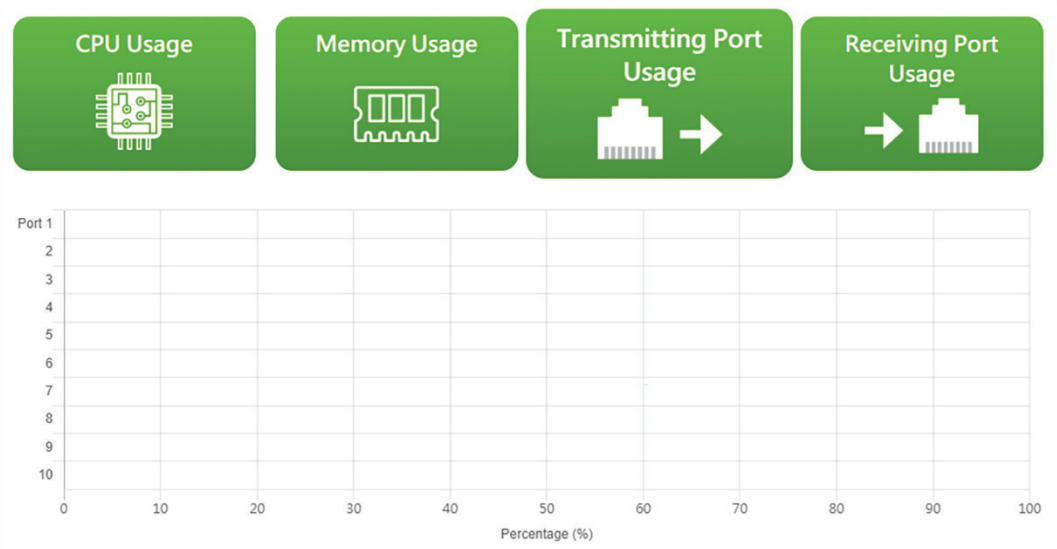


Abbildung 15: Auslastung des Sende-Ports (Beispiel)

8.1.4 Auslastung des Empfänger-Ports

Benutzer können sich mit einem Klick die Auslastung des Rx-Ports des Switches als Prozentwert anzeigen lassen, wie unten dargestellt.

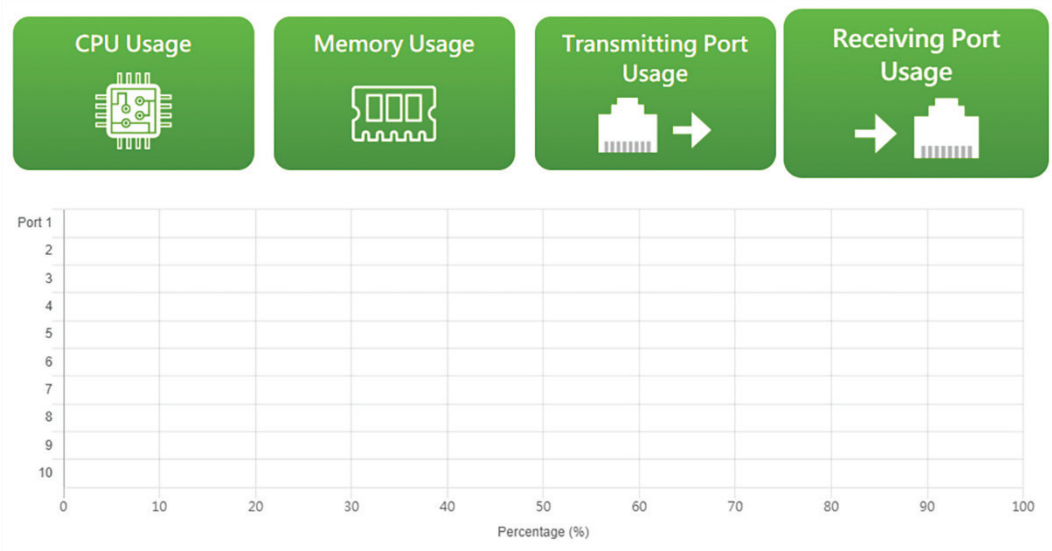


Abbildung 16: Auslastung des Empfänger-Ports (Beispiel)

8.1.5 Sende-Port-Broadcast-Rate

Benutzer können sich für jeden Port die Übertragungsrate des Sende-Ports anzeigen lassen.

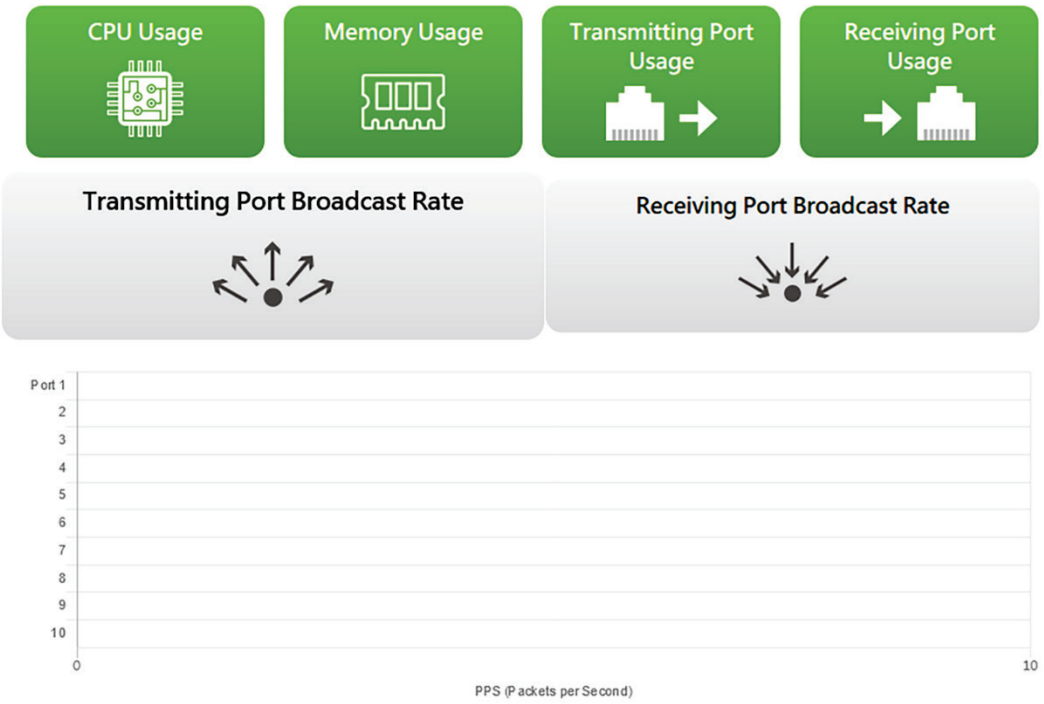


Abbildung 17: Sende-Port-Broadcast-Rate

8.1.6 Empfänger-Port-Broadcast-Rate

Benutzer können sich für jeden Port die Übertragungsrate des Empfangs-Ports anzeigen lassen.

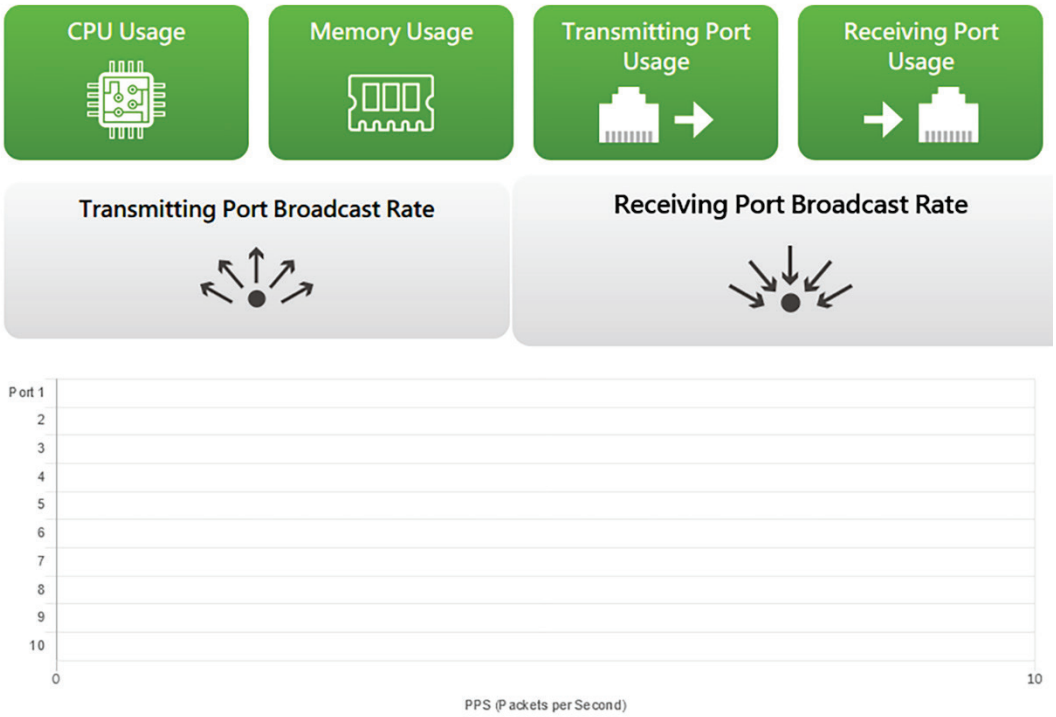
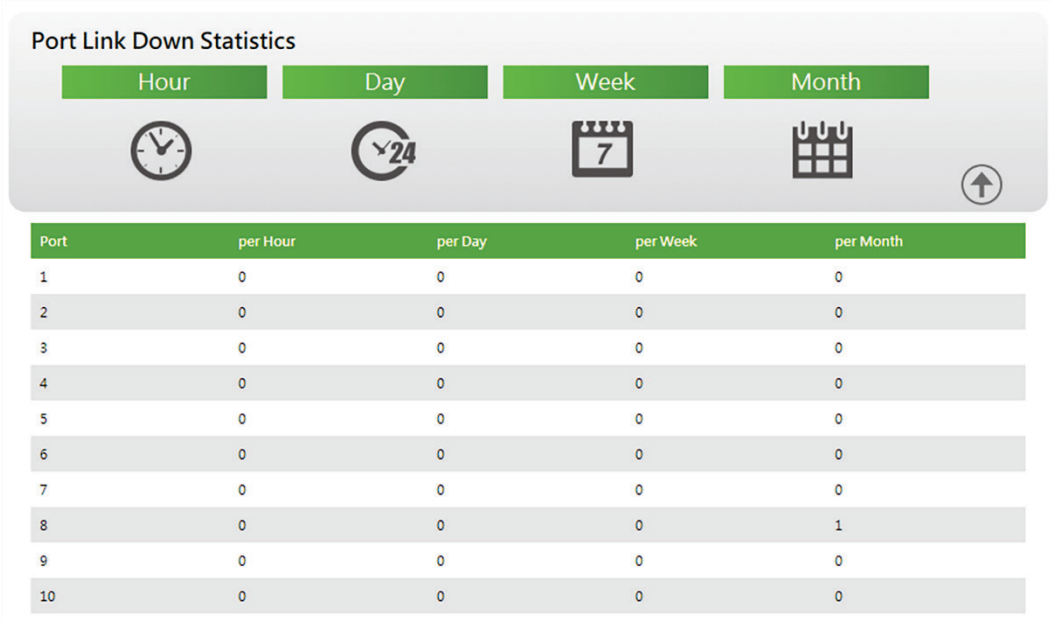


Abbildung 18: Empfänger-Port-Broadcast-Rate

8.1.7 Port-Link-Down-Statistik

Der Benutzer kann sich mit einem Klick in einer Übersicht anzeigen lassen, wie oft eine Port-Verbindung pro Stunde, Tag, Woche und Monat inaktiv („Link down“) war.

Mit dieser Funktion kann ein Wackelkontakt oder Kabelbruch eines Netzwerkkabels schnell und einfach lokalisiert werden.



Port	per Hour	per Day	per Week	per Month
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	1
9	0	0	0	0
10	0	0	0	0

Abbildung 19: Port Link Down Statistics (Beispiel)

8.2 Mauszeiger im Diagnose-Dashboard

Benutzer können ausführliche Informationen über Alarme, Warnungen und Auslastungen erhalten, wenn sie einfach den Mauszeiger darüber bewegen, wie unten dargestellt.

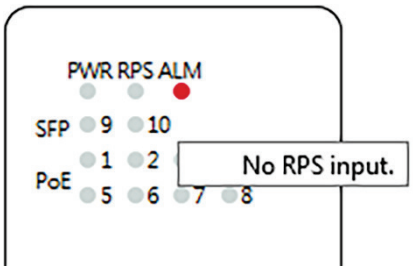


Abbildung 20: LED-Information

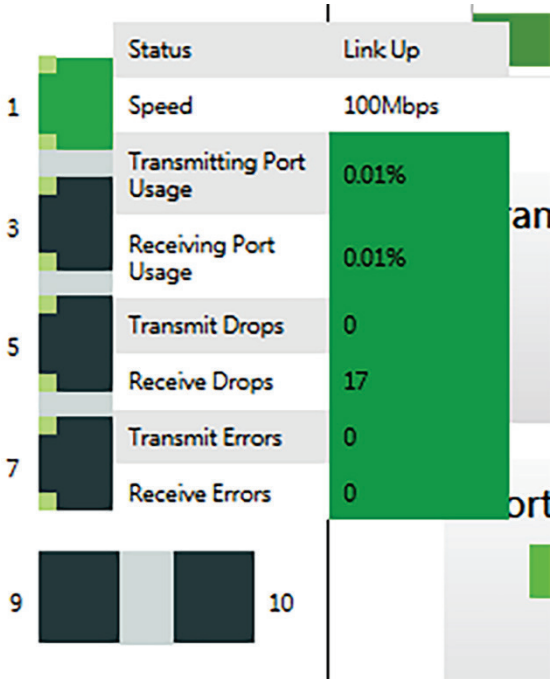


Abbildung 21: Anschlussinformation je Port (Beispiel)

Durch die Analyse der fehlerhaften Datenpakete (z.B. Transmit Errors) können Fehler bei der Kabelverlegung frühzeitig erkannt werden.

8.3 Collapse, User Login, Topology Map

Collapse option	Mit dieser Option kann ein Benutzer zum Dashboard zurückkehren.
User Login	Hier meldet sich ein Benutzer im Gerät an, um weitere Konfigurations- und Wartungseinstellungen vornehmen zu können.
Topology Map	Diese Karte zeigt dem Benutzer eine Übersicht über die Konnektivität.

Abbildung 22: Collapse, User Login, Topology Map

Wählt ein Benutzer „User Login“ (Anmeldung), wird er zum Anmeldefenster des Switches weitergeleitet, wie unten dargestellt.

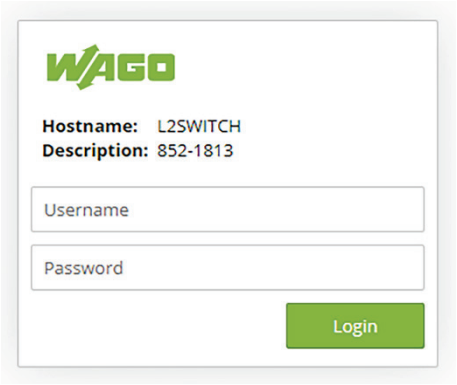


Abbildung 23: Log in

Tabelle 17: Log in

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

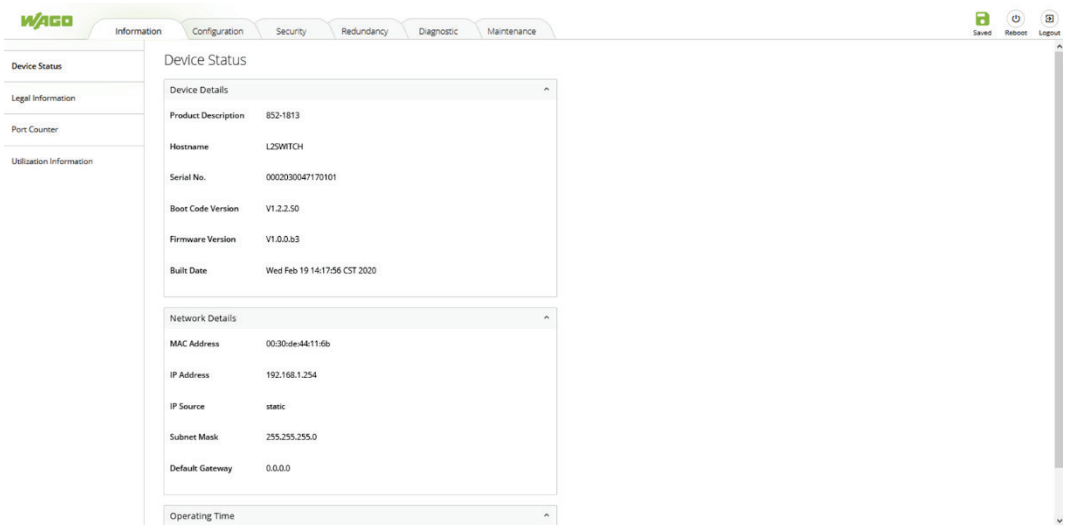


Abbildung 24: Tab “Information” – Menu “Device Status”

Hinweis

Das Web-Based-Management (WBM)

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

Nach Auswahl der Topologiekarte wird eine Übersicht der Netzwerkkonnektivität aufgerufen, wie unten dargestellt.

Der Switch bietet ein schlankes Netzwerkmanagement:

Die Diagnose ist intuitiv und ohne tiefgehende IT-Kenntnisse möglich. Die Topologiekarte stellt den Switch und die verbundenen Knoten übersichtlich dar. Wichtige Diagnoseinformationen werden visualisiert.

Wird an einem Port die Verbindung unterbrochen, färbt sich die Verbindungslinie rot.

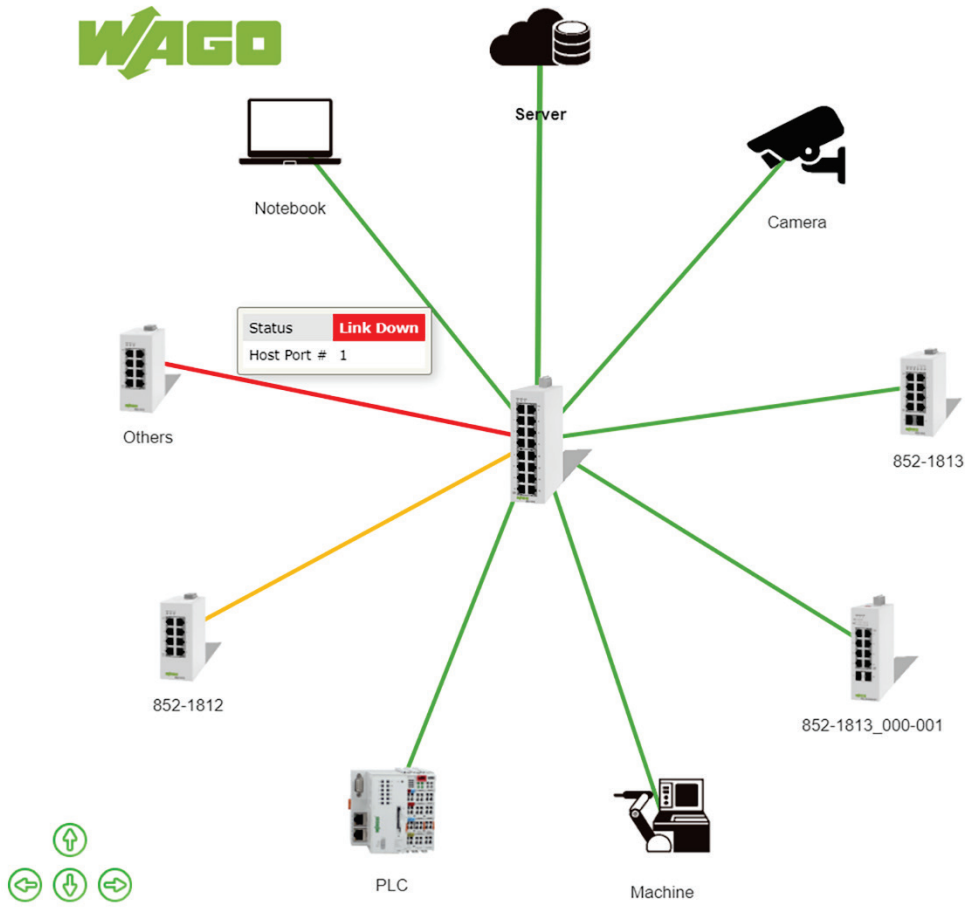


Abbildung 25: Topologiekarte – unterbrochene Verbindung an Port 1

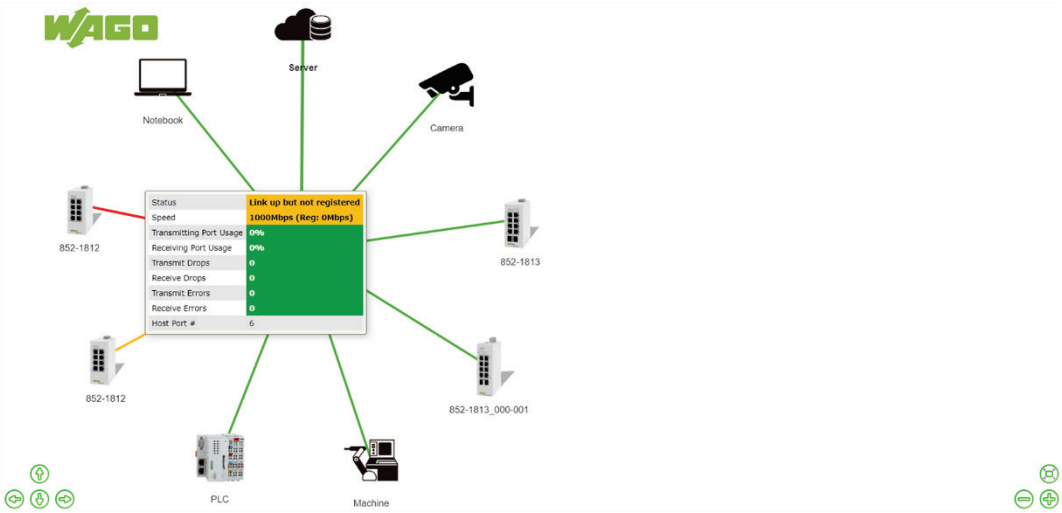


Abbildung 26: Topologiekarte – Verbindung nicht registriert

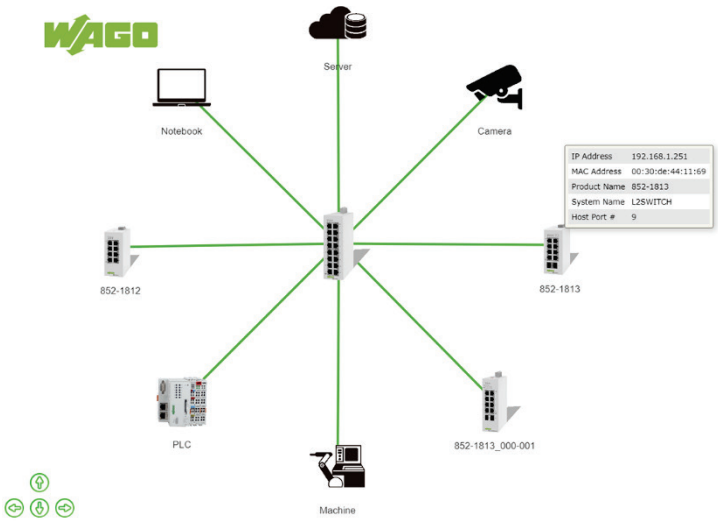


Abbildung 27: Topologiekarte – Verbindungsinformationen

9 Konfiguration im Web-Based-Management-System (WBM)

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

Auf den intern gespeicherten HTML-Seiten erhalten Sie auslesbare Informationen über die Konfiguration und den Status des Switches. Außerdem ändern Sie hier die Konfiguration des Gerätes.

Hinweis

Nach Änderungen an der Konfiguration immer einen Neustart durchführen!
Damit geänderte Konfigurationseinstellungen wirksam werden, führen Sie nach Ihren Änderungen immer einen Systemneustart durch.

1. Zum Öffnen des WBM starten Sie einen Webbrowser (z. B. Google Chrome oder Mozilla Firefox).

Hinweis

Standard-Einstellung
Standardmäßig ist der Lean-Managed-Switch auf das Protokoll „http“ eingestellt.

Hinweis

Verwendung des Protokolls „https“
Wenn Sie das Protokoll „https“ verwenden, müssen Sie diesen Dienst aktivieren. (siehe Kapitel „Service Control“).

2. Geben Sie die IP-Adresse des Switches ein.
3. Bestätigen Sie mit **[Enter]**.
4. Klicken Sie im Diagnose-Dashboard auf den Icon „User Login“ (siehe Abbildung „Log in“)
5. Geben Sie im Abfragedialog Ihren Benutzernamen und das Passwort ein:

   User = „admin“
   Passwort = „wago“
6. Die Startseite des WBM wird aufgebaut.
7. Führen Sie die gewünschten Einstellungen durch.
8. Bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Submit]** oder verwerfen Sie Ihre Änderungen mit der Schaltfläche **[Delete]**.
9. Damit die Einstellungen übernommen werden, bestätigen Sie Ihre Änderungen mit der Schaltfläche **[Save]**).

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

Tabelle 18: Übersicht – Navigationslinks und WBM-Seiten

Navigationslinks und WBM-Seiten
▶ **[Information]** **[Device Status]** • Device Details • Network Details • Operating Time **[Legal Information]** • WAGO Licenses • Open Source Licenses • WBM Licenses **[Port Counter]** • Port Counter **[Utilization Information]** • Utilization Information
▶ **[Configuration]**
[Device Discovery] • LLDP • LLDP Settings • LLDP Neighbor Information • Manual Registration • Manual Registration Settings • Manual Registration Information **[Interface]** • Loop Detection • Configuration Settings • Configuration Status • Mirror • Port Mirror Settings • Port Setup • Port Setup • Port Status • Port Priority • Port Priority Settings • Port Priority Status

[SNMP]

- Event Settings
  - Trap Event State Settings
- Port Event Settings
  - Port Link-Change Trap Settings
  - Port Link-Change Trap Status
- SNMP Setup
  - SNMP Setup
  - Community Name List
- SNMP Trap
  - Trap Receiver Settings
  - Trap Receiver List
- SNMPv3 Group
  - SNMPv3 Group Settings
  - SNMPv3 Group Status
- SNMPv3 User
  - SNMPv3 User Settings
  - SNMPv3 User Status
- SNMPv3 View
  - SNMPv3 View Settings
  - SNMPv3 View Status

[System Management]

- General Setup
  - TCP/IP Configuration
  - Hostname
  - Management VLAN
- SNTP
  - Current Time and Date
  - Time and Date Settings
- User Account
  - Add New User
  - User Account List

[Storm Control]

- Storm Control Settings
- Storm Control Status

▶ **[Security]**

[802.1X]

- Global Setup
  - Global Setup
  - Global Status
- Port Setup
  - Port Setup
  - Port Status

[ACL]

- Access Control List Settings
- Access Control List Status

[Port Security]

- Port Security Settings
- Port Security Status

[Service Control]

- Service Settings

[VLAN]

- Port Isolation
  - Port Isolation Settings
  - Egress Port
- VLAN Setup
  - VLAN Setup

▶ **[Redundancy]**

[ERPS]

- ERPS Setup
- Configuration Status

[STP/RSTP]

- STP/RSTP Setup
  - Spanning Tree Protocol Settings
- STP/RSTP Port Setup
  - Port Parameter Settings
  - Port Status

▶ **[Diagnostic]**

[Alarm]

- Information
  - Alarm Information
- DIP Status
  - DIP Switch Status
- Traffic Flooding
  - Traffic Flooding Settings
  - Traffic Flooding Status
- Port Utilization
  - Port Utilization Settings
  - Port Utilization Status

[Dashboard Configuration]

- Port Registration Learn
- Port Link Down Statistics
- Critical/Alert Thresholds

[Modbus]

- Modbus TCP Setting
- Modbus TCP Information

[SNMP]

- Event Settings
  - Trap Event State Settings
- Port Event Settings
  - Port Link-Change Trap Settings
  - Port Link-Change Trap Status
- SNMP Setup
  - SNMP Setup
  - Community Name List
- SNMP Trap
  - Trap Receiver Settings
  - Trap Receiver List
- SNMPv3 Group
  - SNMPv3 Group Settings
  - SNMPv3 Group Status
- SNMPv3 User
  - SNMPv3 User Settings
  - SNMPv3 User Status

	• SNMPv3 View
	  • SNMPv3 View Settings
	  • SNMPv3 View Status
	
	[System Log]
	  • Syslog Server Settings

▶	**[Maintenace]**
	• Reboot • Upgrade Firmware • Upload Configuration • Download Configuration • Reset Configuration

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 Information

9.1.1 Gerätestatus (Device Status)

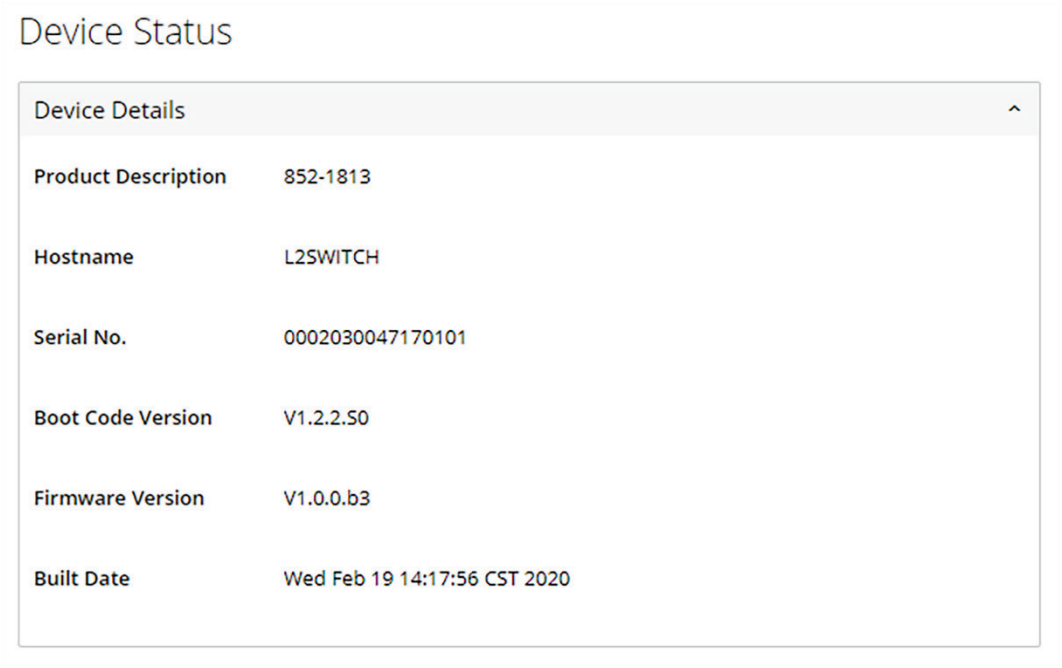


Abbildung 28: Register „Information“ – Menü „Device Status“ – „Device Details“

Tabelle 19: Register „Information“ – Menü „Device Status“ – „Device Details“

Parameter	Beschreibung
Product Description	In diesem Anzeigefeld wird der Modellname des Switches angezeigt.
Host Name	In diesem Anzeigefeld wird der „Host-Name“ des Switches angezeigt.
Serial No.	In diesem Anzeigefeld wird die Seriennummer angezeigt.
Boot Code Version	In diesem Anzeigefeld wird die „Boot Code Version“ angezeigt.
Built Date	In diesem Anzeigefeld wird das Erstellungsdatum der aktuell installierten primären Firmware angezeigt.

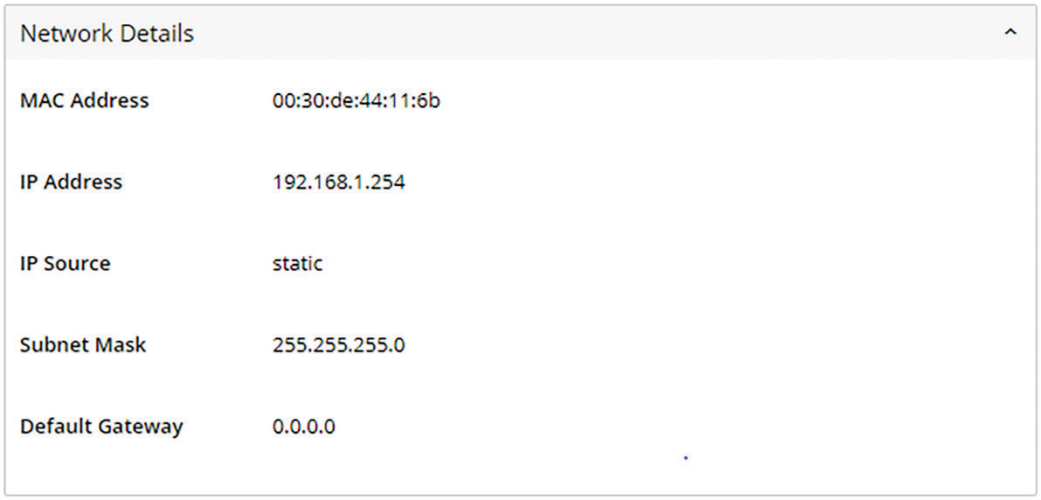


Abbildung 29: Register „Information“ – Menü „Device Status“ – „Network Details“

Tabelle 20: Register „Information“ – Menü „Device Status“ – „Network Details“

Parameter	Beschreibung
MAC Address	In diesem Anzeigefeld wird die MAC (Media-Access-Control)-Adresse des Switches angezeigt.
IP Address	In diesem Anzeigefeld wird die IP-Adresse des Switches angezeigt.
IP Source	In diesem Anzeigefeld wird die Static IP oder DHCP angezeigt.
Subnet Mask	In diesem Anzeigefeld wird die „Subnet Mask“ angezeigt.
Default Gateway	In diesem Anzeigefeld wird das „Default Gateway“ des Switches angezeigt.

Abbildung 30: Register „Information“ – Menü „Device Status“ – „Operating Time“

Tabelle 21: Register „Information“ – Menü „Device Status“ – „Operating Time“

Parameter	Beschreibung
Total	In diesem Anzeigefeld wird die Betriebszeit (dd:hh:mm:ss) angezeigt.

9.1.2 Rechtliche Informationen (Legal Information)

In diesem Menü finden Sie Informationen über:

- WAGO Licenses
- Open Source Licenses und
- WBM Licenses

9.1.3 Port-Zähler (Port Counter)

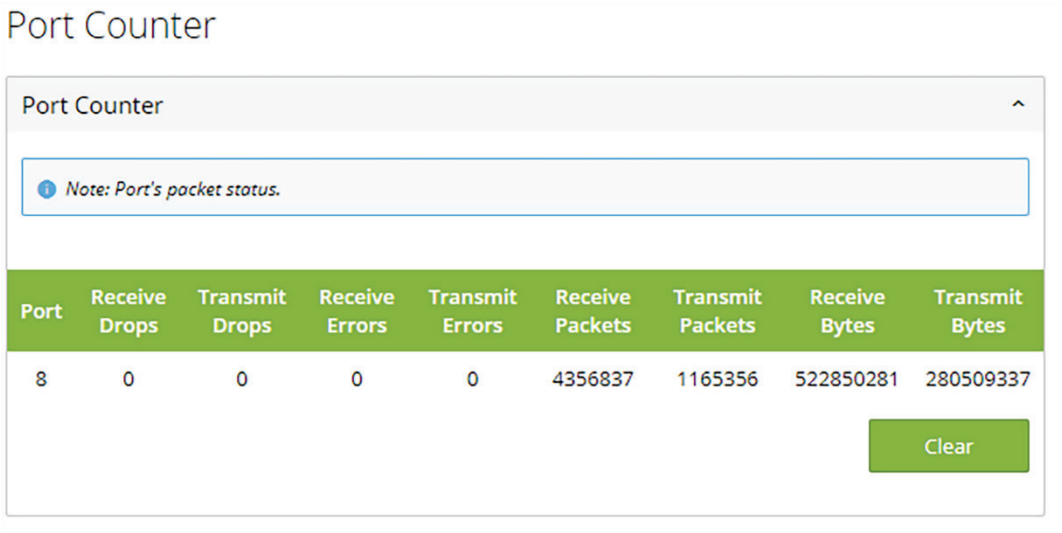


Abbildung 31: Register „Information“ – Menü „Port Counter“

Tabelle 22: Register „Information“ – Menü „Port Counter“

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

9.1.4 Auslastungsinformationen (Utilization Information)

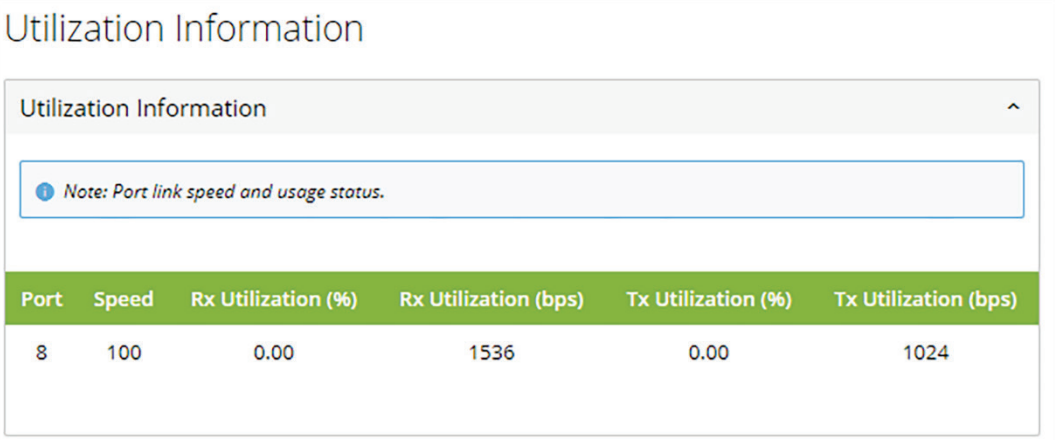


Abbildung 32: Register „Information“ – Menü „Utilization Information“

Tabelle 23: Register „Information“ – Menü „Utilization Information“

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

9.2 Konfiguration

9.2.1 Geräteerkennung (Device Discovery)

9.2.1.1 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.

Hinweis

Für Geräte mit LLDP-Protokoll:
Nach der Aktivierung erscheinen auf der Topologiekarte Informationen über Geräte mit LLDP-Protokoll. Die Switch-Informationen werden mit anderen Geräten geteilt, die mit demselben Netzwerk verbunden sind.

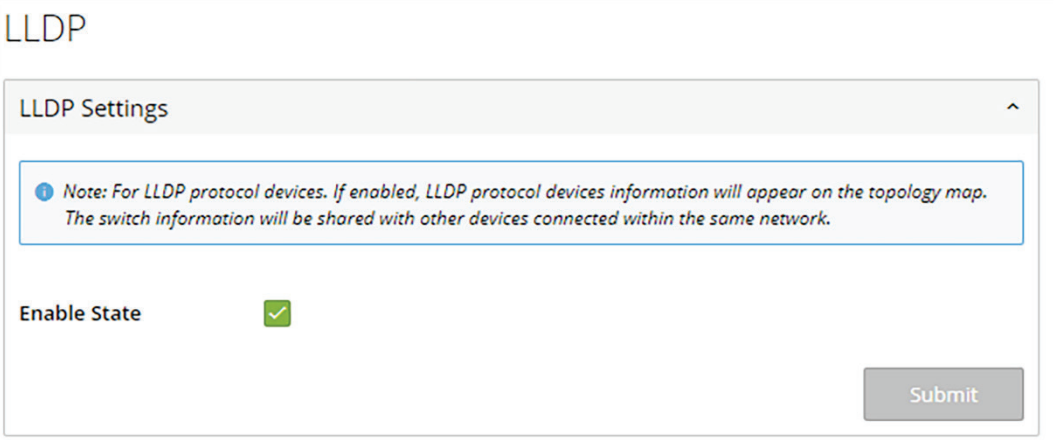


Abbildung 33: Register „Configuration“ – Menü „LLDP Settings“

Tabelle 24: Register „Configuration“ – Menü „LLDP Settings“

LLDP Settings			
Parameter	**Standardwert**	**Beschreibung**	
State	☑	☐	Die Funktion „LLDP“ für den Switch ist global deaktiviert.
		☑	Die Funktion „LLDP“ für den Switch ist global aktiviert.

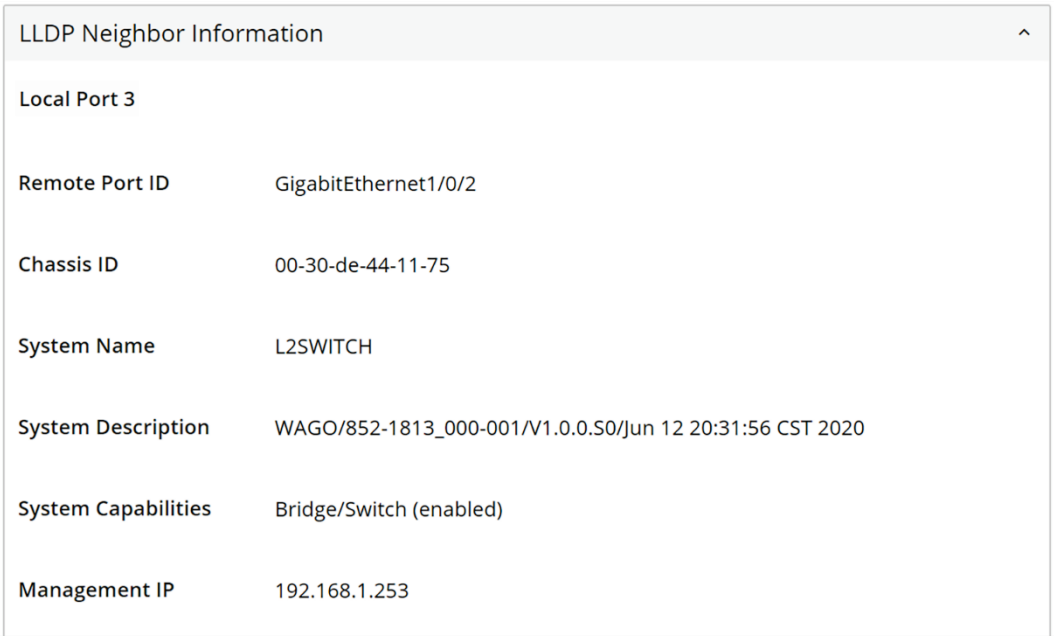


Abbildung 34: Register „Configuration“ – Menü „LLDP Neighbor Information“

Tabelle 25: Register „Configuration“ – Menü „LLDP Neighbor Information“

LLDP Neighbor Information		
Parameter	**Standardwert**	**Beschreibung**
Local Port X		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.
System Name		In diesem Anzeigefeld wird der Systemname des Nachbar-Ports angezeigt.
System Description		In diesem Anzeigefeld wird die Systembeschreibung des Nachbar-Ports angezeigt.
System Capabilities		In diesem Anzeigefeld werden die Systemfähigkeiten des Nachbar-Ports angezeigt.
Management IP		In diesem Anzeigefeld wird die Managementadresse des Nachbar-Ports angezeigt.

9.2.1.2 Manuelle Registrierung (Manual Registration)

Unterstützt ein Gerät im Netzwerk nicht LLDP, kann dieses Gerät über die manuelle Registrierung dem Switch bekannt gemacht werden.

Hinweis

Manuelle Eingabe der Geräteinformationen

Der Benutzer muss die Geräteinformationen manuell eingeben, damit sie auf der Toplogiekarte erscheinen.

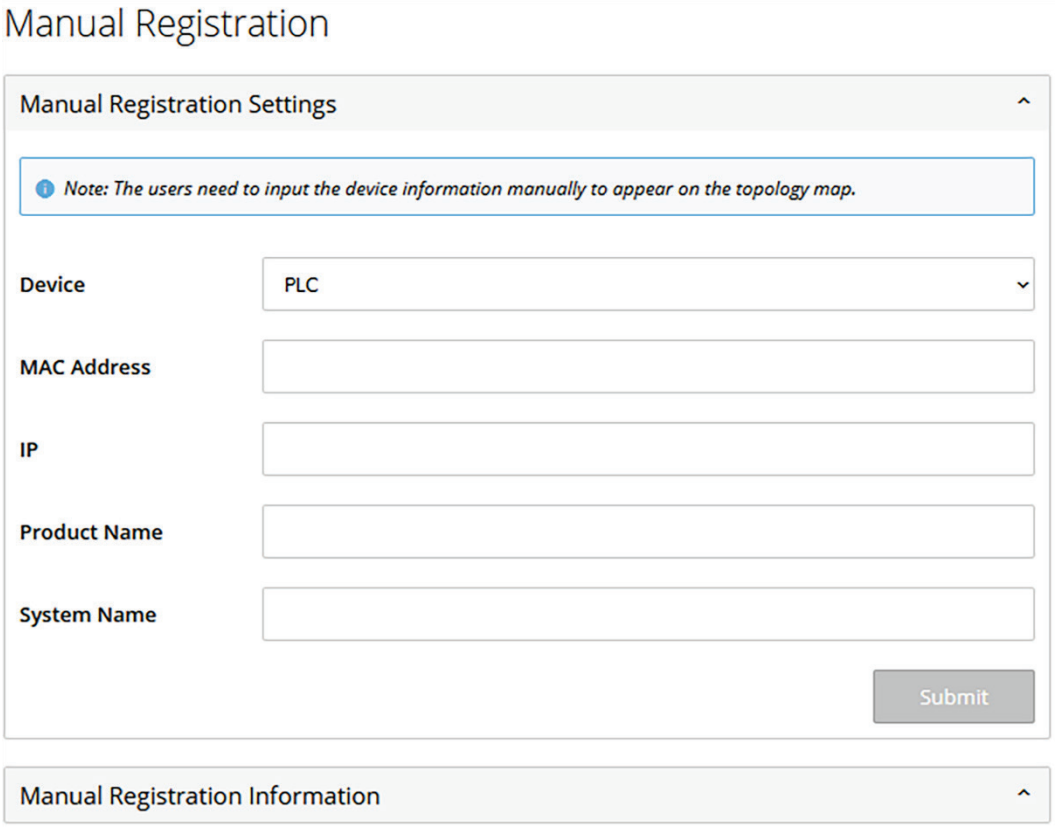


Abbildung 35: Register „Configuration“ – Menü „Manual Registration“

Tabelle 26: Register „Configuration“ – Menü „Manual Registration“

Manual Registration Settings		
Parameter	**Standardwert**	**Beschreibung**
Device	**PLC** Switch Camera Computer Display Machine Notebook Others Router Server Wireless	Wählen Sie im Auswahlfeld einen passenden Gerätenamen aus.
MAC Address		Geben Sie im Eingabefeld die MAC-Adresse des Gerätes ein.
IP		Geben Sie im Eingabefeld die IP-Adresse des Gerätes ein.
Product Name		Geben Sie im Eingabefeld den Produktnamen des Gerätes ein.
System Name		Geben Sie im Eingabefeld den Systemnamen des Gerätes ein.

9.2.2 Interface

9.2.2.1 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.

9.2.2.1.1 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.

Hinweis

Loop Detection
Loop Detection ist ein für Ethernet-Netzwerke entwickeltes Link-Layer-Protokoll. Eine Schnittstelle mit aktiver Loop Detection kann im gleichen Netzwerk Schleifen erkennen und entfernen.

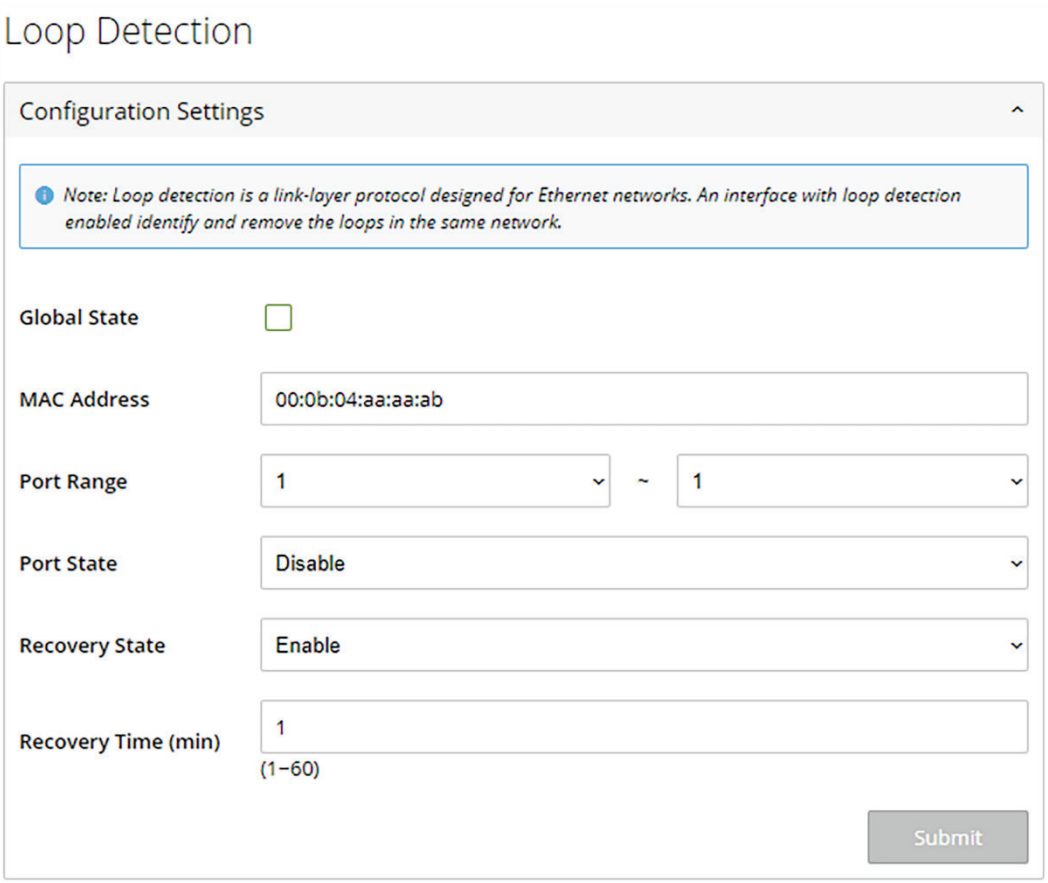


Abbildung 36: Register „Configuration“ – Menü „Loop Detection“ – „Configuration Settings“

Tabelle 27: Register „Configuration“ – Menü „Loop Detection“ – „Configuration Settings“

Configuration Settings			
Parameter	**Standardwert**	**Beschreibung**	
Global State	☑	☐	Die Funktion „Loop Detection“ ist für den Switch deaktiviert.
		☑	Die Funktion „Loop Detection“ ist für den Switch aktiviert.
MAC Address		Geben Sie im Eingabefeld die MAC-Zieladresse ein, an die die Sonderpakete gesendet werden sollen. Empfängt der Port dieselben Datenpakete, wird er abgeschaltet.	
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Detection“ (Schleifenschutz) konfigurieren möchten.	
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Loop Detection“ (Schleifenschutz) konfigurieren möchten.	
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die Funktion „Loop Detection“ für den Switch zu deaktivieren.	
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die Funktion „Loop Detection“ für den Switch zu deaktivieren.	
Recovery State	**Enable**	Wählen Sie im Auswahlfeld „Enable“, damit sich der Port nach Ablauf der zugewiesenen „Recovery-Zeit“ automatisch reaktiviert.	
	Disable	Wählen Sie im Auswahlfeld „Disable“, um diese Funktion zu deaktivieren.	
Recovery Time (min) (Range: 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	

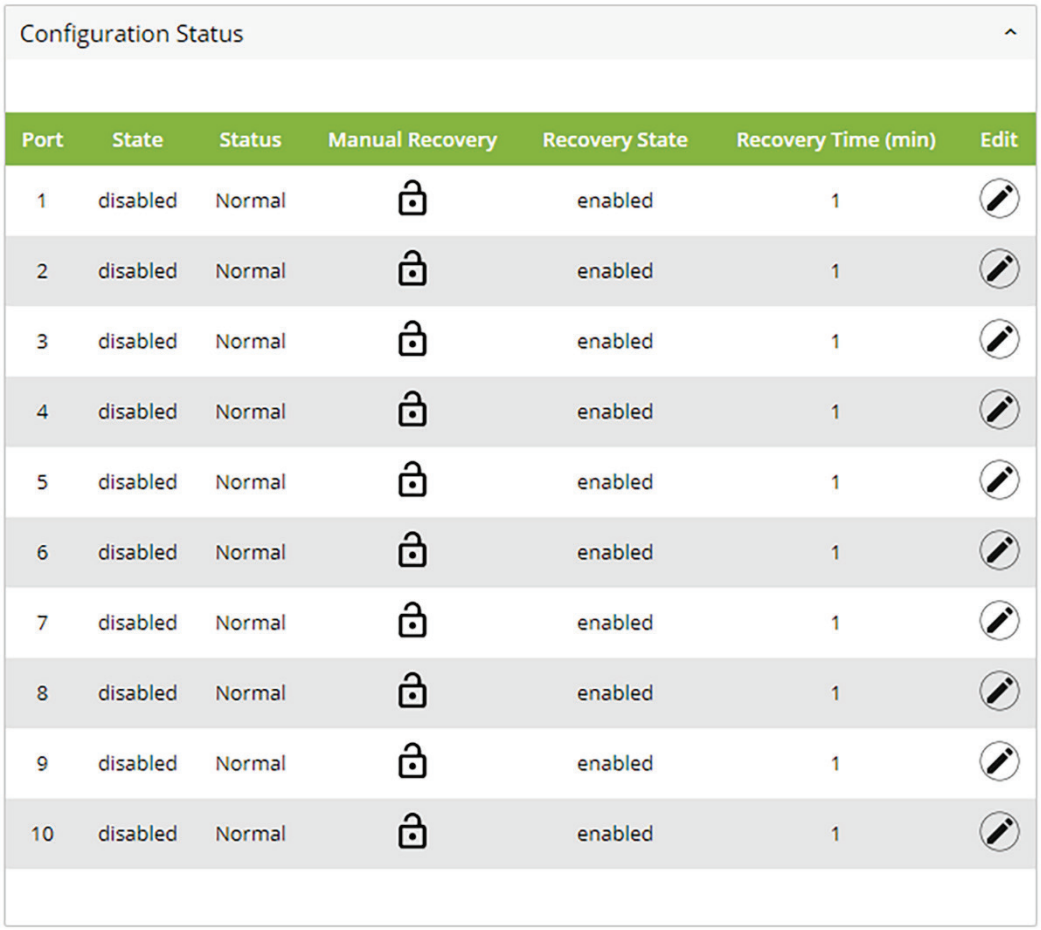


Abbildung 37: Register „Configuration“ – Menü „Loop Detection“ – „Configuration Status“

Tabelle 28: Register “Configuration” – Menü “Loop Detection” – “Configuration Status”

Loop Detection Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
State	Enable Disable	In dieser Spalte wird angezeigt, ob die Funktion „Loop Detection“ aktiviert oder deaktiviert ist.
Status	None Normal	In dieser Spalte wird angezeigt, ob ein Port blockiert wird.
Manual Recovery		In dieser Spalte wird angezeigt, ob die Funktion „Manual Recovery“ abgeschlossen ist oder nicht ist.
Recovery State	Enable Disable	In dieser Spalte wird angezeigt, ob die Funktion „Loop Recovery“ aktiviert oder deaktiviert ist.
Recovery Time (min)	1 … 60	In dieser Spalte wird die „Recovery Time“ für die Funktion „Loop Detection“ angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.2.2.2 Port-Spiegelung (Mirror)

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.

Source Mode

- „Ingress“ (Eingang): Die eingehenden Datenpakete werden kopiert und zum Monitor-Port weitergeleitet.
- „Egress“ (Ausgang): Die ausgehenden 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.

Hinweis

Verwendung der Port-Spiegelung

Die Port-Spiegelung wird zur Netzwerküberwachung verwendet. Dabei werden Kopien von Netzwerkpaketen, die an einem Port des Switches gesendet/empfangen wurden, an einen oder eine Reihe anderer Switch-Ports gesendet.

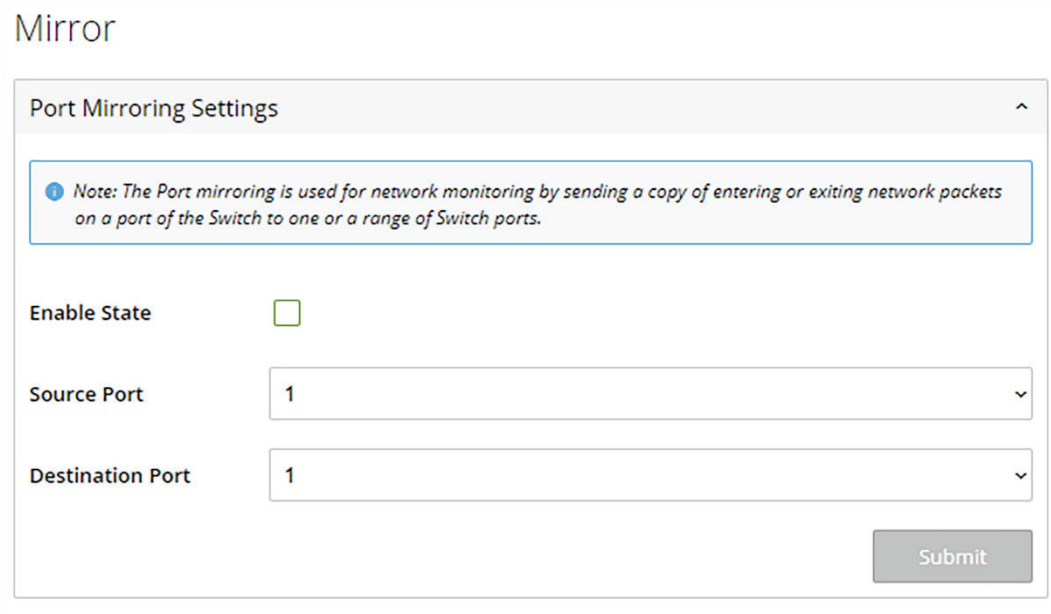


Abbildung 38: Register „Configuration“ – Menü „Mirror“ – „Port Mirroring Settings“

Tabelle 29: Register „Configuration“ – Menü „Mirror“ – „Port Mirroring Settings“

Port Mirror Settings			
Parameter	**Standardwert**	**Beschreibung**	
Enable State	☐	☐	Die Funktion „Mirror“ für den Switch ist deaktiviert.
		☑	Die Funktion „Mirror“ für den Switch ist aktiviert.
Source Port	1 … 10	Wählen Sie im Auswahlfeld einen Source-Port aus für die „Mirror“-Funktion aus.	
Destination Port	1 … 10	Wählen Sie im Auswahlfeld einen Destination-Port aus für die „Mirror“-Funktion aus.	

9.2.2.3 Port Setup

9.2.2.3.1 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.

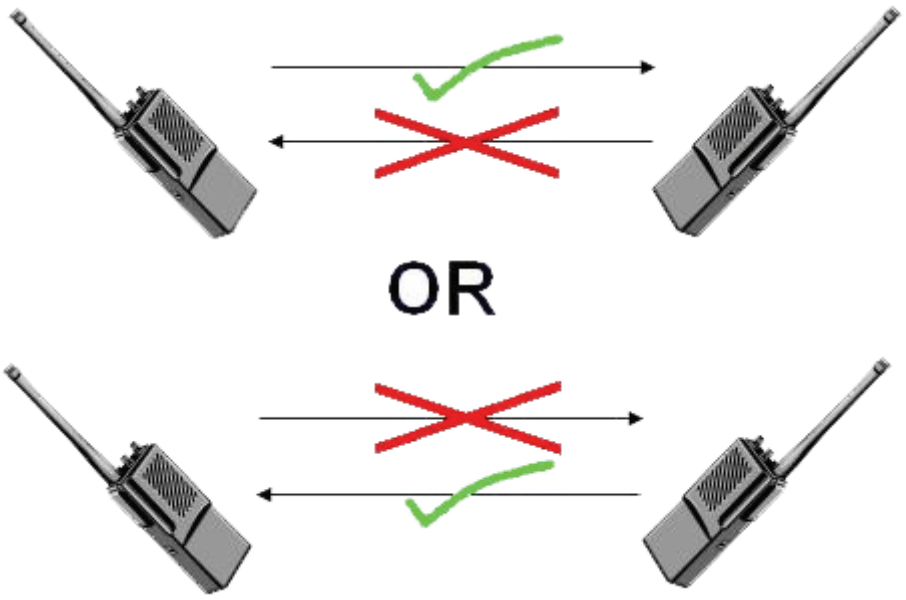


Abbildung 39: Halbduplexmodus

Vollduplex

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

Abbildung 40: Vollduplexmodus

Auto MDI/MDIX

MDI („**M**edium-**D**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-Ports (z. B. der Netzwerk-Port eines PC und der eines Routers, Hubs oder Switches, mit dem dieser z. B. verbunden ist) selbständig die maximal mögliche Übertragungsrate und das Duplexverfahren erkennen und entsprechend automatisch einstellen.
Autonegotiation gilt nur für Mehrdrahtverbindungen (Twisted-Pair-Kabel) – nicht aber für WLAN-, Glasfaser- oder Koaxialkabelverbindungen.

Unterstützt der Port keine Autonegotiation oder ist diese Funktion abgeschaltet, bestimmt der Switch die Übertragungsrate durch Signalerkennung am Kabel und verwendet den Halbduplexmodus.
Ist die Autonegotiation beim Switch ausgeschaltet, verwendet ein Port bei der Verbindungsherstellung seine vorkonfigurierten Einstellungen für Geschwindigkeit und Duplexmodus.
Deshalb sollte sichergestellt sein, dass am Port dieselben Einstellungen vorgenommen wurden, damit die Verbindung hergestellt werden kann.

Flusskontrolle (Flow Control)

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

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

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

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

Hinweis

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

Hinweis

Auswahl eines Port-Bereichs
Sie können einen ganzen Port-Bereich auswählen und dafür einen Duplexzustand (Geschwindigkeit) aktivieren bzw. deaktivieren.

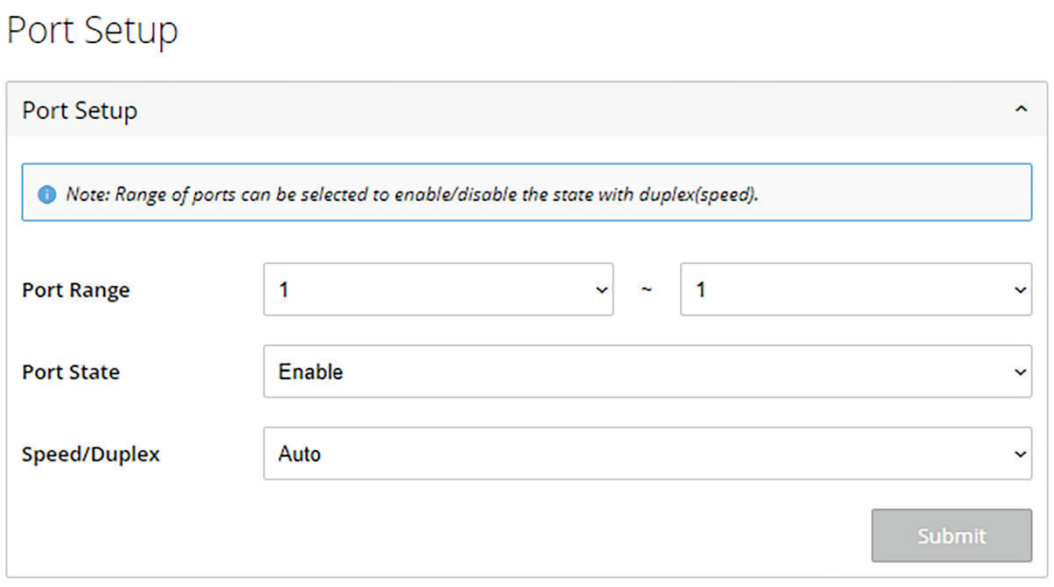


Abbildung 41: Register „Configuration“ – Menü „Port Setup“ – „Port Setup“

Tabelle 30: Register „Configuration“ – Menü „Port Setup“ – „Port Setup“

Port Setup		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, in dem Sie „Port Setup“ konfigurieren wollen.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, in dem Sie „Port Setup“ konfigurieren wollen.
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um den Port zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um den Port zu aktivieren.
Speed/Duplex	**Auto**	Wählen Sie im Auswahlfeld Geschwindigkeit und Duplexmodus für den Port aus.
	10 Mbit/s / Full	
	10 Mbit/s / Half	
	100 Mbit/s / Full	
	100 Mbit/s / Half	
	1000 Mbit/s / Full	

Port Status

Port	State	Speed/Duplex	Status	Link Status	Edit
1	enabled	Auto	Normally	Link Down	
2	enabled	Auto	Normally	Link Down	
3	enabled	Auto	Normally	Link Down	
4	enabled	Auto	Normally	Link Down	
5	enabled	Auto	Normally	Link Down	
6	enabled	Auto	Normally	Link Down	
7	enabled	Auto	Normally	Link Down	
8	enabled	Auto	Normally	100M / Full / On	
9	enabled	Auto	Normally	Link Down	
10	enabled	Auto	Normally	Link Down	

Abbildung 42: Register „Configuration“ – Menü „Port Setup“ – „Port Status“

Tabelle 31: Register „Configuration“ – Menü „Port Setup“ – „Port Status“

Port Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
State		In dieser Spalte wird angezeigt, ob ein Port aktiviert oder deaktiviert ist.
Speed/Duplex		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.
Status		In dieser Spalte werden die Abweichungen angezeigt.
Link Status		In dieser Spalte wird der „Link Status“ eines Ports angezeigt. Ist der Port aktiv, werden die Geschwindigkeit, der Duplexmodus und die „Flusskontrolle“-Einstellung angezeigt. Die Anzeige „Link inaktiv“ zeigt an, dass der Port entweder deaktiviert oder an kein Gerät angeschlossen ist.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.2.2.4 Priorisierung der ETHERNET-Ports (Port Priority)

Normalerweise arbeiten Netzwerke nach Art der bestmöglichen Übertragungsmöglichkeit, was bedeutet, dass jeder Datenverkehr je Port die gleiche Priorität und gleiche Chance erhält, in angemessener Zeit übertragen zu werden. Wenn es zu Engpässen kommt, hat so auch jedes Datenpaket die gleiche Chance, verworfen zu werden.

Mit der Funktion „Port Priority“ können Sie einen spezifischen Datenverkehr auswählen, ihm entsprechend seiner relativen Wichtigkeit eine Priorität zuweisen. Die Implementierung einer Port-Priorität in Ihrem Netzwerk verbessert die Vorhersagbarkeit der Netzwerkleistung und erhöht die Effizienz der Bandbreitennutzung.

Hinweis

Auswahl von Port-Prioritäten

Sie können einen Port-Bereich auswählen und ihm die Priorität „Low“, „Medium“ oder „High“ (Niedrig, Mittel oder Hoch) zuweisen.

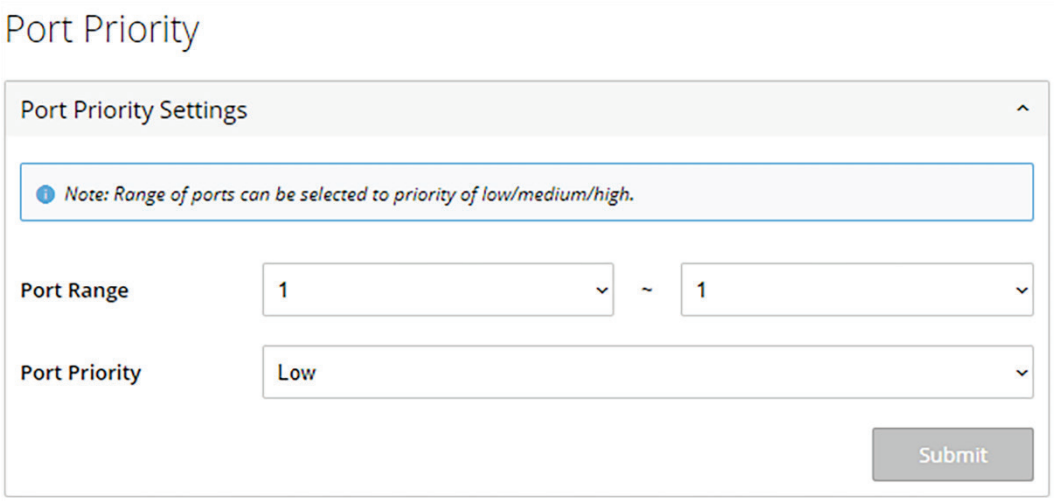


Abbildung 43: Register „Configuration“ – Menü „Port Priority“ – „Port Priority Settings“

Tabelle 32: Register „Configuration“ – Menü „Port Priority“ – „Port Priority Settings“

Port Priority Settings		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, in dem Sie „Port Priority“ konfigurieren wollen.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, in dem Sie „Port Priority“ konfigurieren wollen.
Port Priority	Low	Wählen Sie für Anwendungen mit hohen Datenverkehr im Auswahlfeld die Option „Low“.
	Medium	Wählen Sie für Anwendungen mit mittlerem Datenverkehr im Auswahlfeld die Option „Medium“.
	High	Wählen Sie für Anwendungen mit zeitkritischem Datenverkehr im Auswahlfeld die Option „High“.

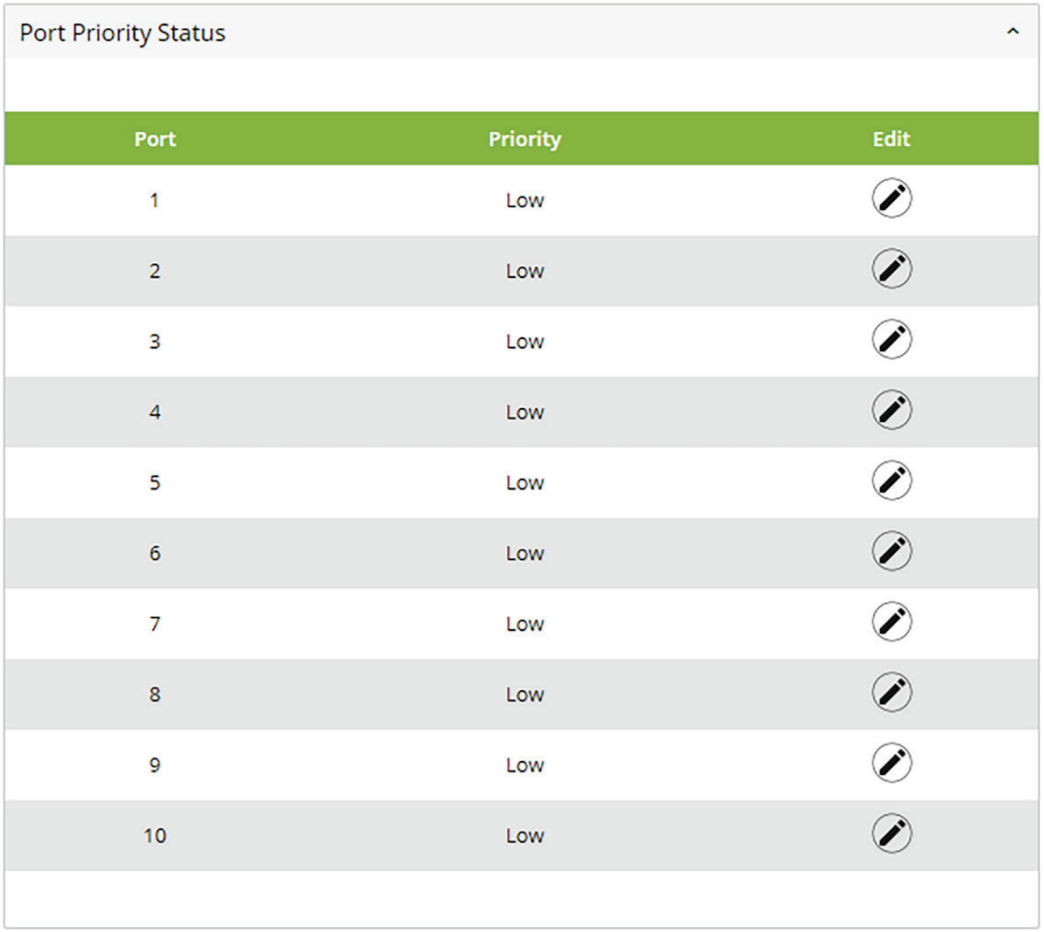


Abbildung 44: Register „Configuration“ – Menü „Port Priority“ – „Port Priority Status“

Tabelle 33: Register „Configuration“ – Menü „Port Priority“ – „Port Priority Status“

Port Priority Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Priority	Low Medium High	In dieser Spalte wird die Priorität der Portes angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

Hinweis

Priorisierung der Netzwerkgeräte

Bevorzugt sollten zeitkritische Netzwerkgeräte (z. B. SPS, Remote-IO) eine hohe und zeitunkritische Netzwerkgeräte (z. B. Kamera, Drucker) eine niedrige Priorität erhalten..

9.2.3 SNMP

Das „**S**imple **N**etwork **M**anagement **P**rotocol“ (SNMP) 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 Internet Engineering Task Force (IETF) 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.

Ein „SNMP Community String“ ist ein Textelement, das als Passwort fungiert. Es wird zur Authentifizierung von Nachrichten verwendet, die zwischen der Managementstation (der 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 SNMPv2cUmgebungen verwendet. Die normale „SNMP Community“ für SNMPv1 und SNMPv2c lautet „public“, solange SNMPv3 nicht aktiviert ist. Ist SNMPv3 aktiviert, müssen die „Communities“ für SNMPv1 und v2c spezifisch sein und können nicht gemeinsam genutzt werden.

9.2.3.1 Event Settings

Hinweis

Auswahl des Typs des SNMP-Trap-Events
Es können SNMP-Trap-Eventtypen ausgewählt werden, die den SNMP-Manager aufrufen.

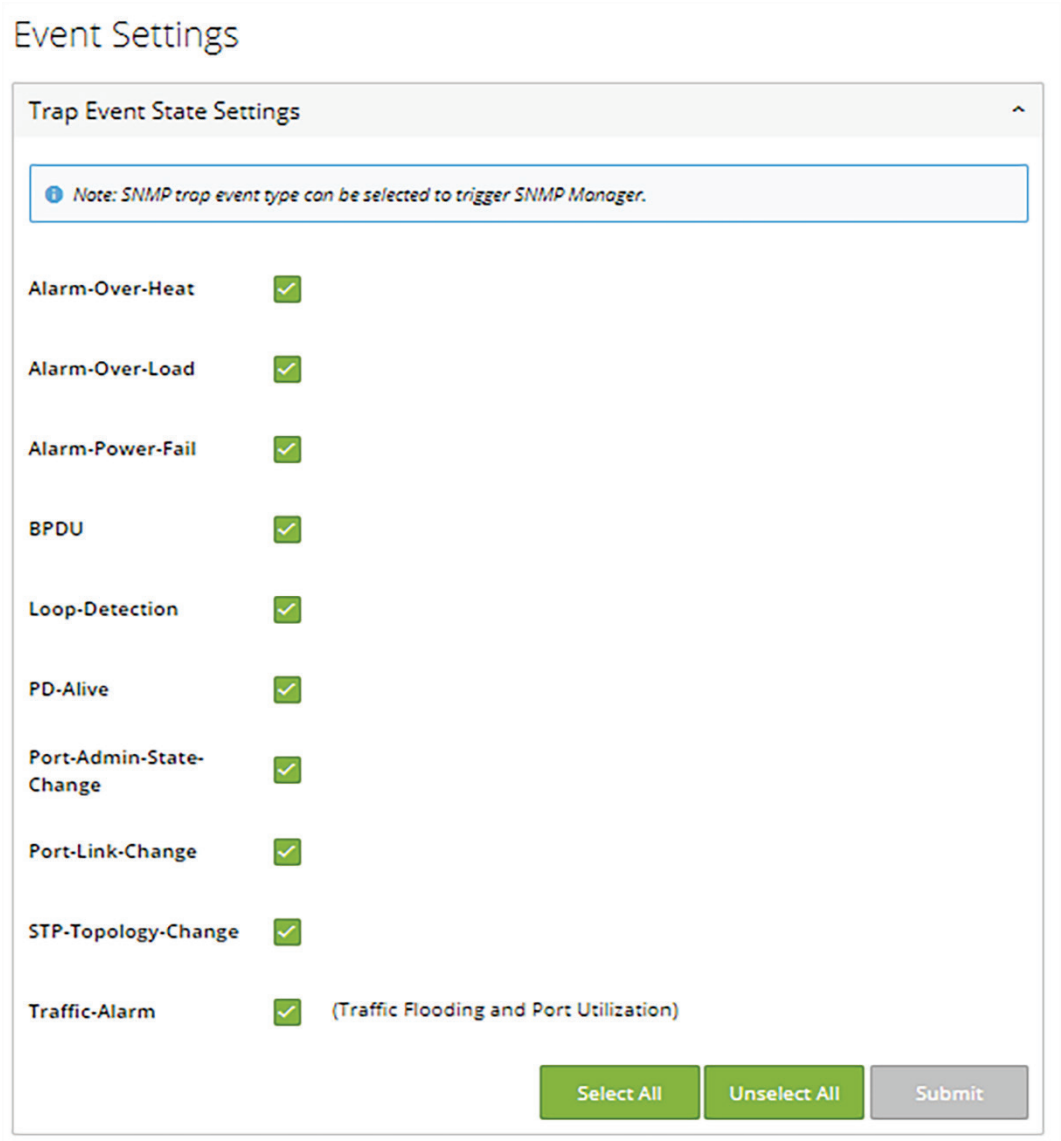


Abbildung 45: Register „Configuration“ – Menü „SNMP“ – „Event Settings“ – „Trap Event State Settings“

Tabelle 34: Register „Configuration“ – Menü „SNMP“ – „Event Settings“ – „Trap Event State Settings“

Trap Event State Settings		
Parameter	**Standardwert**	**Beschreibung**
Alarm-Over-Heat	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn die Temperatur des Systems zu hoch ist.
Alarm-Over-Load	☑	Aktiviert/deaktiviert den SNMP-Trap, wenn das System überlastet ist.
Alarm-Power-Fail	☑	Aktiviert/Deaktiviert das SNMP-Trap bei folgenden Zuständen der Systemleistung: - Überspannung - Unterspannung - RPS-Überspannung - RPS-Unterspannung
BPDU	☑	Aktiviert/Deaktiviert das SNMP-Trap, wenn der Port durch Folgendes blockiert wird: - BPDU Guard - BDPU Root - BPDU-Port-Zustandsänderung
Loop-Detection	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port durch die Loop Detection blockiert wird.
PD-Alive	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port vom Administrator aktiviert/deaktiviert ist.
Port-Admin-State-Change	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn der Port hoch/runter wechselt.
Port-Link-Change	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn sich die STP-Topologie ändert.
STP-Topology-Change	☑	Aktiviert/deaktiviert das SNMP-Trap, wenn sich die STP-Topologie ändert.
Traffic-Alarm (Traffic Flooding and Port Utilization)	☑	Aktiviert/deaktiviert den SNMP-Trap, wenn der Port durch den „Traffic Monitor“ blockiert wird.

9.2.3.2 Port Event Settings

Hinweis

Erzeugen von Port-Link-Change-Traps
Benutzer können die Erzeugung von Traps durch Port-Link-Änderungen für einzelne oder mehrere Ports aktivieren oder deaktivieren.

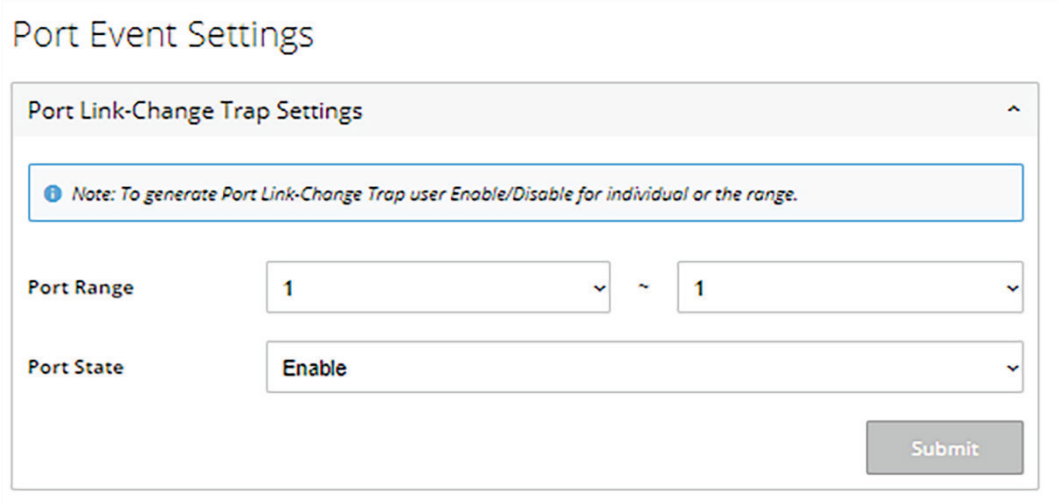


Abbildung 46: Register „Configuration“ – Menü „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“

Tabelle 35: Register „Configuration“ – Menü „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“

Port Link-Change Trap Settings		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Event Settings“ konfigurieren möchten.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Event Settings“ konfigurieren möchten.
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die Funktion „Port Event Settings“ für den Switch zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die Funktion „Port Event Settings“ für den Switch zu aktivieren.

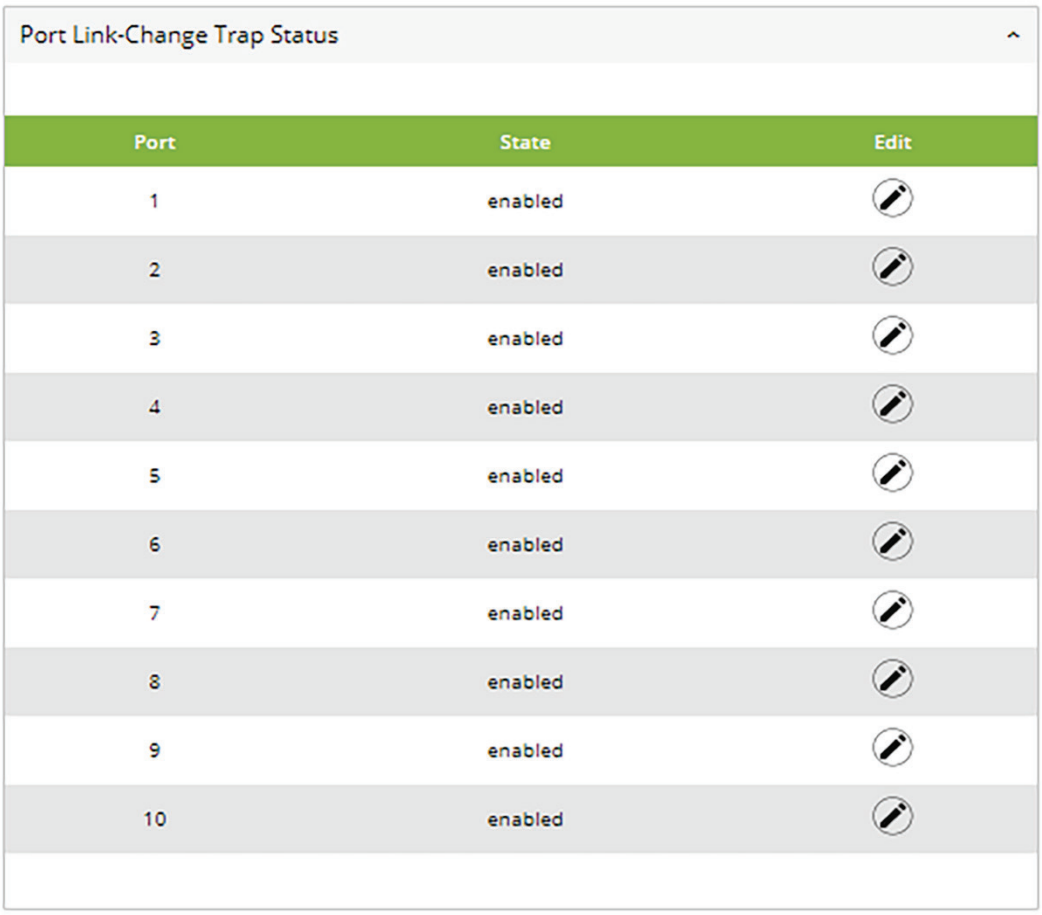


Abbildung 47: Register „Configuration“ – Menü „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“

Tabelle 36: Register „Configuration“ – Menü „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“

Port Link-Change Trap Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte wird der Portbereich angezeigt.
State	Enable Disable	In diesem Anzeigefeld wird der Port-Status angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.2.3.3 SNMP Setup

Hinweis

Simple Network Management Protocol (SNMP)
Hier können Sie die Dienste des „Simple Network Management Protocol“ (SNMP) konfigurieren.

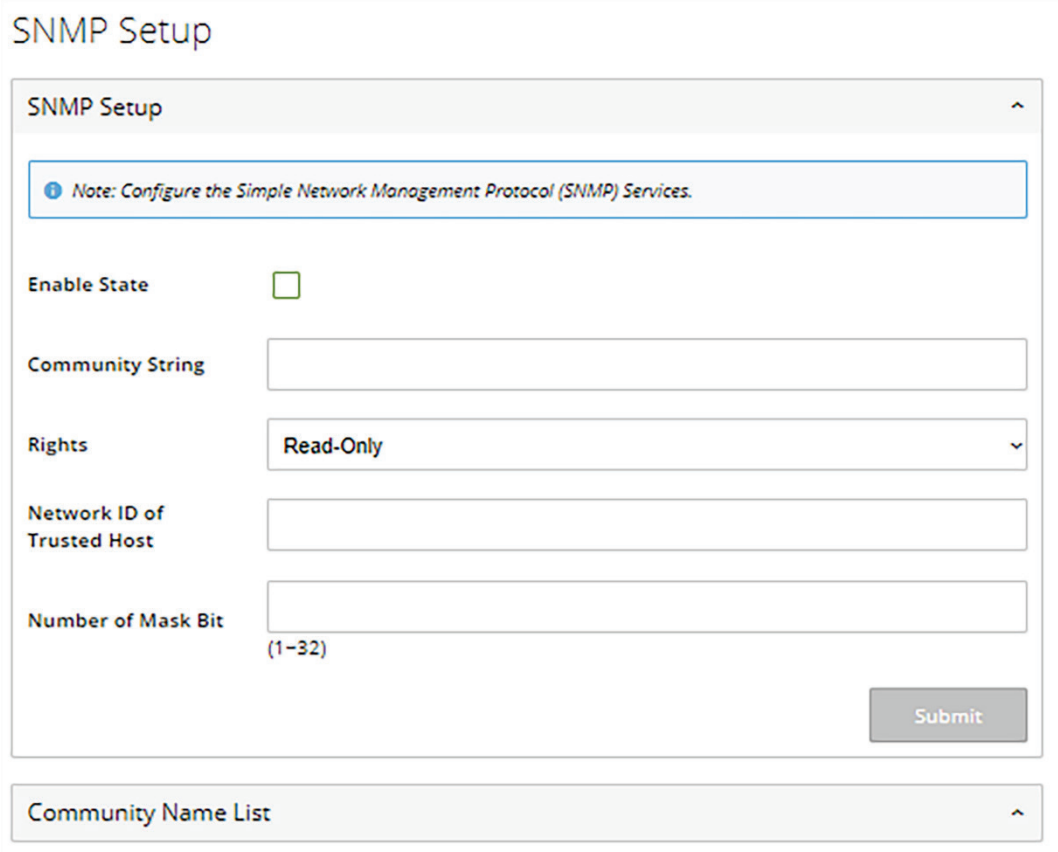


Abbildung 48: Register „Configuration“ – Menü „SNMP“ – „SNMP Setup“ – „SNMP Setup“

Tabelle 37: Register „Configuration“ – Menü „SNMP“ – „SNMP Setup“ – „SNMP Setup“

SNMP Setup			
Parameter	**Standardwert**	**Beschreibung**	
Enable State	☐	☐	Die Funktion „SNMP Setup“ ist für den Switch nicht aktiviert.
		☑	Die Funktion „SNMP Setup“ ist für den Switch aktiviert.
Community String		In diesem Feld wird der „Community String“ eingetragen, der als Passwort für Anfragen von der Managementstation fungiert. Dies ist ein Textelement, das als Passwort fungiert. Es wird zur Authentifizierung von Nachrichten verwendet, die zwischen der Managementstation (der SNMP-Manager) und einem Gerät (dem SNMP-Agenten) ausgetauscht werden. Der „Community String“ ist in jedem Paket enthalten, das zwischen diesen beiden Punkten übertragen wird.	
Rights	**Read-Only**	Wählen Sie im Auswahlfeld „Read-Only“, damit der SNMP-Manager diese Strings nutzen kann, um Informationen vom Switch zu erhalten.	
	Read/ Write	Wählen Sie im Auswahlfeld „Read/Write“, damit der SNMP-Manager diese Strings nutzen kann, um Einstellungen beim Switch zu konfigurieren.	
Network ID of Trusted Host		Geben Sie im Eingabefeld die IP-Adresse der dezentralen SNMP-Managementstation in Dezimalpunktschreibweise ein (z. B. 192.168.1.0).	
Number of Mask Bit (1-32)		Geben Sie im Eingabefeld die IP-Adresse der Subnetzmaske ein.	
Community Name List			
Parameter	**Standardwert**	**Beschreibung**	
No.		In dieser Spalte wird die Nummer der „Community“ angezeigt. Sie dient ausschließlich der Identifizierung. Klicken Sie auf eine Nummer, um die Einstellung einer spezifischen „Community“ zu modifizieren.	
Community String		In dieser Spalte wird der SNMP-„Community Strings“ angezeigt. Dies ist ein Textelement, das als Passwort fungiert.	
Rights	Read-Only, Read/ Write	In dieser Spalte werden die Berechtigungen für den „SNMP-Community-String“ angezeigt.	
Network ID of the Trusted Host		In dieser Spalte wird die IP-Adresse der dezentralen SNMP-Managementstation angezeigt, nachdem sie durch die Subnetzmaske modifiziert wurde.	
Number of Mask Bit		In dieser Spalte wird die Subnetzmaske für die IP-Adresse der dezentralen SNMP-Managementstation angezeigt.	
Action		Klicken Sie auf **[Clear]**, um einen spezifischen „Community String“ zu löschen.	

9.2.3.4 SNMP Trap

Hinweis

Trap-Empfänger-Einstellungen
In diesem Fenster können Sie IP-Adresse, Community und Version für den SNMP-Trap-Empfänger konfigurieren, um Events an den SNMP-Manager zu senden.

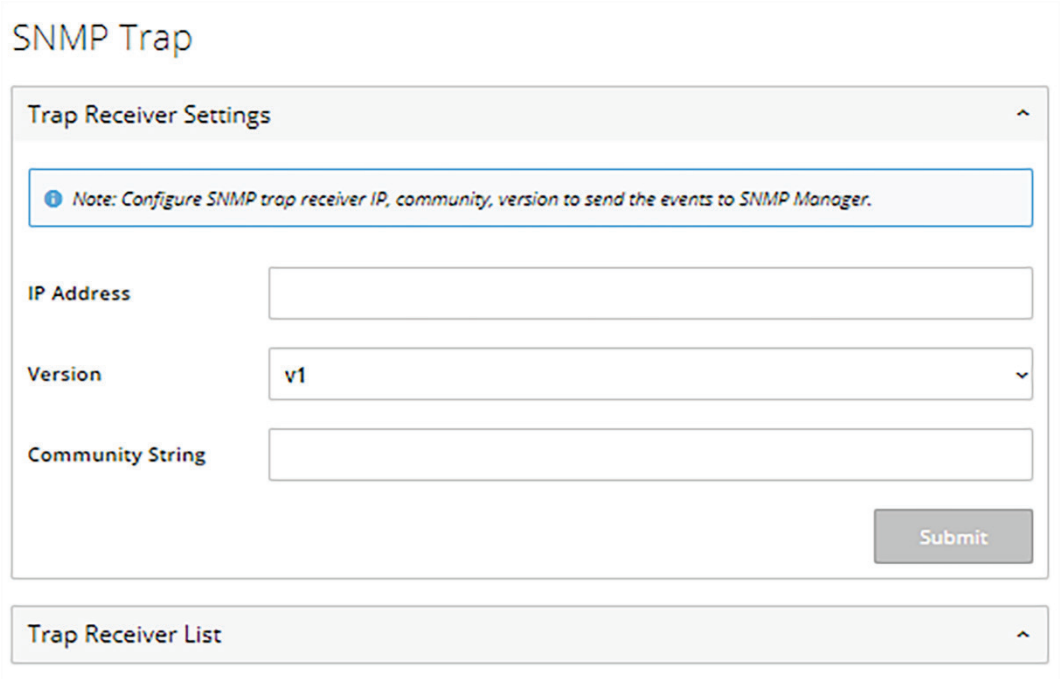


Abbildung 49: Register „Configuration“ – Menü „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“

Tabelle 38: Register „Configuration“ – Menü „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“

Trap Receiver Settings		
Parameter	**Standardwert**	**Beschreibung**
IP Address		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 List		
Parameter	**Standardwert**	**Beschreibung**
No.		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 Address		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.
Action		Klicken Sie auf die Schaltfläche **[Clear]**, um eine konfigurierte Trap-Empfängerstation zu löschen.

9.2.3.5 SNMPv3-Gruppe (SNMPv3 Group)

Hinweis

Möglichkeiten von SNMPv3-Gruppen
SNMPv3-Gruppen ermöglichen das Zusammenfassen von Benutzern in Gruppen mit unterschiedlicher Autorisierung und verschiedenen Zugriffsrechten.

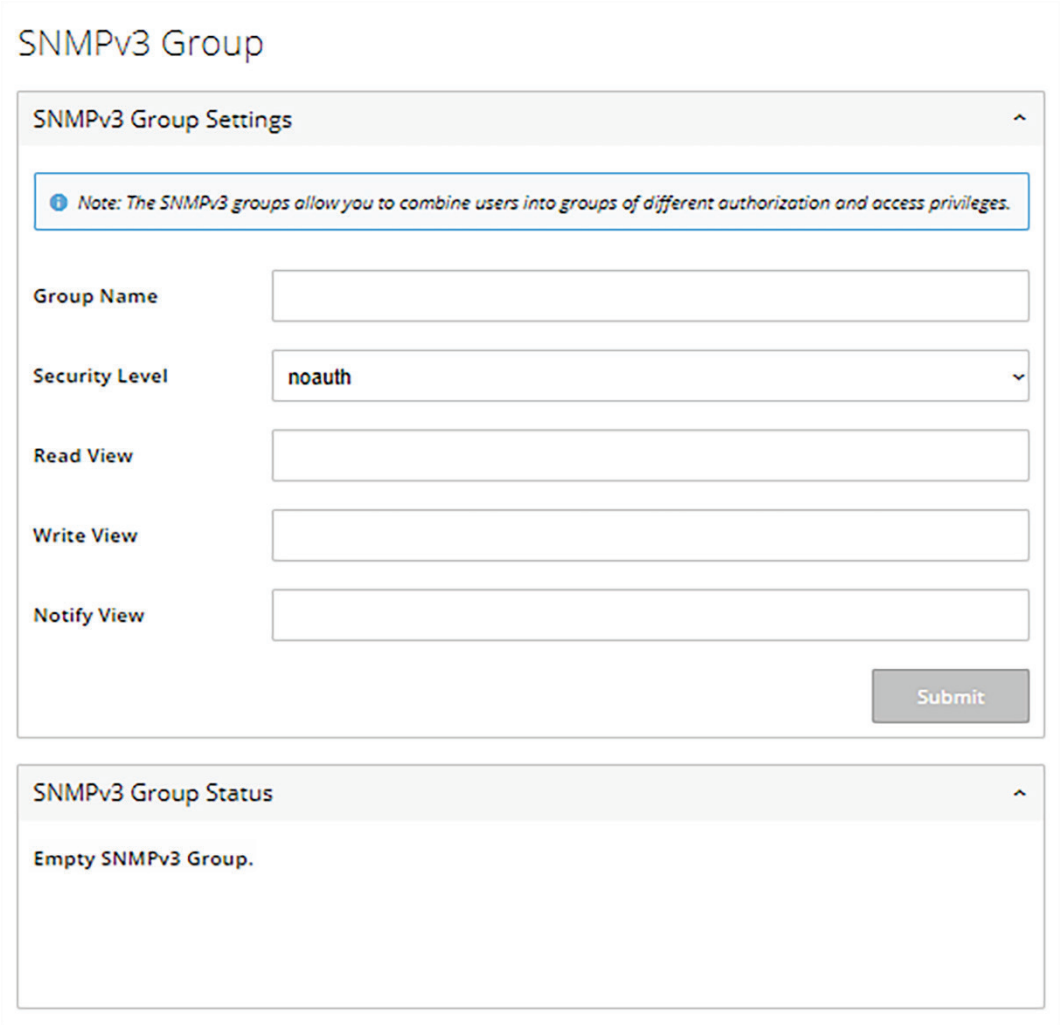


Abbildung 50: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 Group“

Tabelle 39: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 Group“

SNMPv3 Group Settings		
Parameter	**Standardwert**	**Beschreibung**
Group Name		Geben Sie im Eingabefeld den Gruppennamen für die SNMPv3 ein.
Security Level		In diesem Auswahlfeld wird der Sicherheitslevel ausgewählt.
	Noauth	Haben Sie im Auswahlfeld „noauth“ gewählt, dann können Sie den „Auth-Algorithmus“ und den „Priv-Algorithmus“ nicht ändern.
	auth	Haben Sie im Auswahlfeld „auth“ gewählt, dann können Sie den „Auth-Algorithmus“ und das „Auth-Password“ ändern.
	priv	Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie den „Auth-Algorithmus“, das „Auth-Password“, den „Priv-Algorithmus“ und das „Priv-Password“ ändern.
Read View	**None**	Geben Sie im Eingabefeld den Namen der Objekte ein, die in der Leseansicht verfügbar sein sollen. Geben Sie kein Objekt ein, sind alle Objekte lesbar.
Write View	**None**	Geben Sie im Eingabefeld den Namen der Objekte ein, auf die ein Schreibzugriff gewährt werden soll. Wurde keine Schreib- oder Benachrichtigungsansicht definiert, wird kein Schreibzugriff gewährt und es können keine Objekte Benachrichtigungen an die Mitglieder der Gruppe senden.
Notify View	**None**	Geben Sie im Eingabefeld den Namen des Objektes ein, das Benachrichtigungen der Benutzer empfangen kann. Durch die Verwendung einer Benachrichtigungsansicht bestimmt eine Gruppe die Liste von Benachrichtigungen, die ihre Benutzer empfangen können.
SNMPv3 Group Status		
Parameter	**Standardwert**	**Beschreibung**
Group Name		In dieser Spalte wird der Gruppenname angezeigt.
Security Model		In dieser Spalte wird der gewählte „Sicherheitslevel“ angezeigt. Wird immer v3 angezeigt: Nutzerbasiertes Sicherheitsmodell (User-based Security Model, USM)
Security Level		In dieser Spalte wird der gewählte „Sicherheitslevel“ angezeigt.
Read View		In dieser Spalte wird die „Read View“ angezeigt
Write View		In dieser Spalte wird die „Write View“ angezeigt
Notify View		In dieser Spalte wird die „Notify View“ angezeigt
Action		Klicken Sie auf **[Clear]**, um einen bestimmten Eintrag zu löschen.

9.2.3.6 SNMPv3-Nutzer (SNMPv3 User)

Hinweis

SNMPv3-Agent-Unterstützung
Der SNMPv3-Agent bietet Unterstützung für drei Benutzerlevel, die in einer Gruppe zusammengefasst werden können.

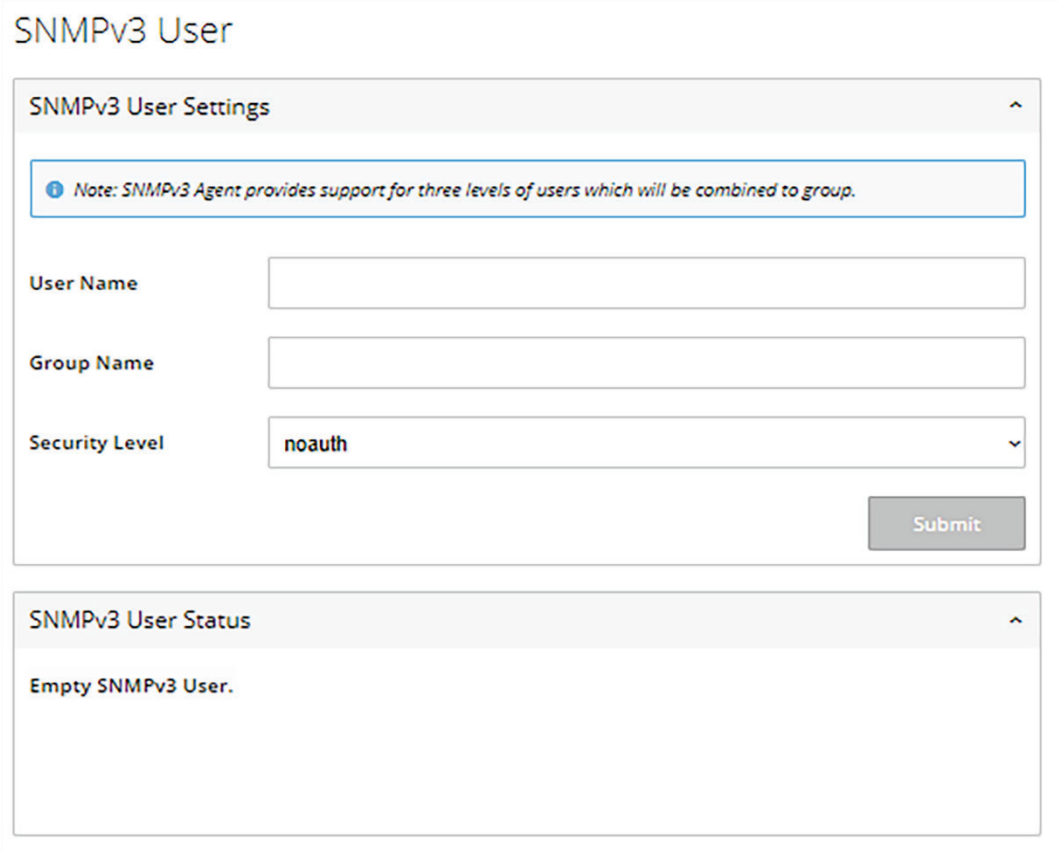


Abbildung 51: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 User“

Tabelle 40: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 User“

SNMPv3 User Settings		
Parameter	**Standardwert**	**Beschreibung**
User Name		Geben Sie im Eingabefeld einen neuen Benutzernamen ein oder modifizieren Sie einen bereits bestehenden Benutzernamen.
Group Name		Geben Sie im Eingabefeld den Gruppennamen für die SNMPv3 ein.
Security Level		In diesem Auswahlfeld wird der Sicherheitslevel ausgewählt.
	noauth	Haben Sie im Auswahlfeld „noauth“ gewählt, dann können Sie den „Auth-Algorithmus“ und den „Priv-Algorithmus“ nicht ändern.
	auth	Haben Sie im Auswahlfeld „auth“ gewählt, dann können Sie den „Auth-Algorithmus“ und das „Auth-Password“ ändern.
	priv	Haben Sie im Auswahlfeld „priv“ gewählt, dann können Sie den „Auth-Algorithmus“, den „Priv-Algorithmus“ und das „Priv-Password“ ändern.
SNMPv3 User Status		
Parameter	**Standardwert**	**Beschreibung**
User Name		In dieser Spalte wird der Benutzername angezeigt.
Group Name		In dieser Spalte wird der Gruppenname angezeigt.
Auth Protocol		In dieser Spalte wird der gewählte „Auth-Algorithmus“ angezeigt.
Priv Protocol		In dieser Spalte wird der gewählte „Priv-Algorithmus“ angezeigt
Action		Klicken Sie auf **[Clear]**, um einen bestimmten Eintrag zu löschen.

9.2.3.7 SNMPv3-Ansicht (SNMPv3 View)

Hinweis

Anzeige der SNMPv3-Konfiguration
In dieser Ansicht wird die SNMPv3-Konfiguration auf dem Gerät angezeigt.

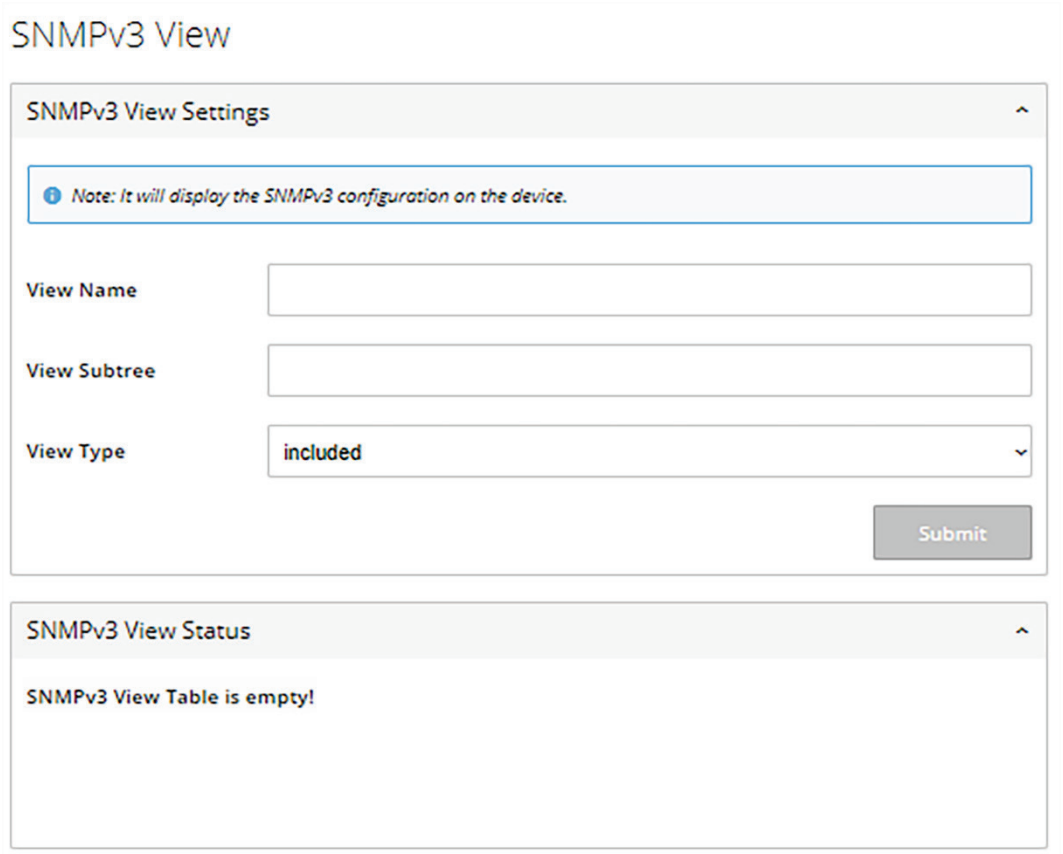


Abbildung 52: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 View“

Tabelle 41: Register „Configuration“ – Menü „SNMP“ – „SNMPv3 View“

SNMPv3 View Settings		
Parameter	**Standardwert**	**Beschreibung**
View Name		Geben Sie im Eingabefeld den Namen für die SNMPv3-View ein.
View Subtree		Geben Sie im Eingabefeld den Namen für den Subtree ein.
View Type	**included**	Haben Sie im Auswahlfeld „included“ gewählt, dann wird der Subtree eingefügt
	excluded	Haben Sie im Auswahlfeld „excluded“ gewählt, dann wird der Subtree nicht eingefügt.
SNMPv3 View Status		
Parameter	**Standardwert**	**Beschreibung**
View Name		In dieser Spalte wird der Name der SNMPv3-View angezeigt.
View Subtree		In dieser Spalte wird der Name des Subtree angezeigt.
View Type	Inserted Removed	In dieser Spalte wird der gewählte Typ angezeigt.
Action		Klicken Sie auf **[Clear]**, um einen bestimmten Eintrag zu löschen.

9.2.4 Systemmanagement (System Management)

9.2.4.1 Allgemeine Einstellung (General Setup)

Host Name
Der Hostname und der SNMP-Systemname sind identisch. Die maximale Zeichenlänge beträgt 64 Zeichen.

Hinweis **Konfiguration des Switch-Managements**
Konfigurieren Sie das Switch-Management (static/DHCP, IP-Adresse, VLAN etc.).

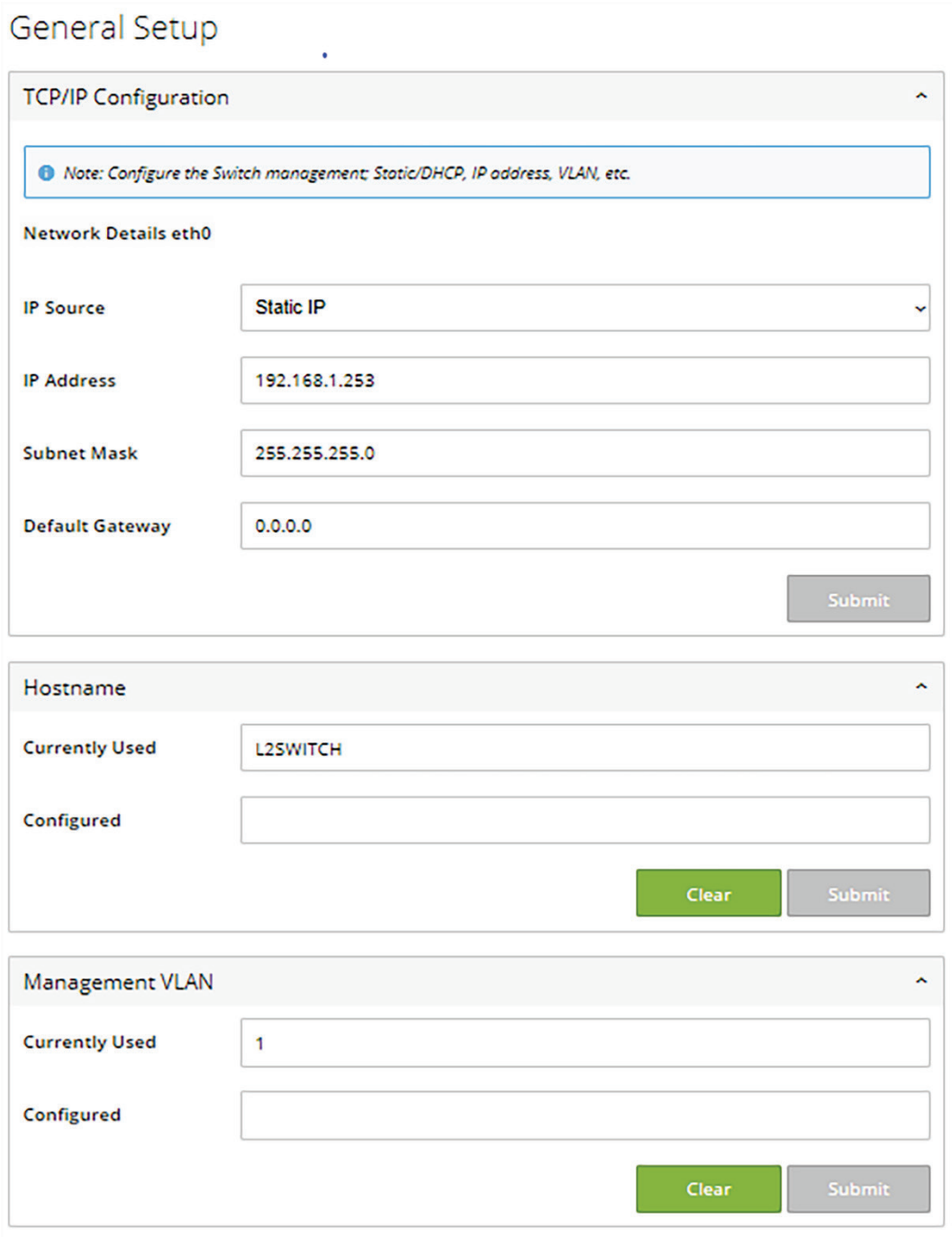


Abbildung 53: Register „Configuration“ – Menü „System Management“ – „General Setup“

Tabelle 42: Register „Configuration“ – Menü „System Management“ – „General Setup“

TCP/IP Configuration		
Parameter	**Standardwert**	**Beschreibung**
IP Source	**Static IP** DHCP	In diesem Auswahlfeld wählen Sie eine Option für die „IP Source“ (Quell-IP-Adresse) aus.
IP Address	**192.168.1.254**	Geben Sie die IP-Adresse des Switches in Dezimalpunktschreibweise ein.
Subnet Mask	**255.255.255.0**	Geben Sie im Eingabefeld die IP-Subnetzmaske des Switches in Dezimalpunktschreibweise ein.
Default Gateway	**0.0.0.0**	Geben Sie die IP-Adresse des ausgehenden Default-Gateways in Dezimalpunktschreibweise ein.
Hostname		
Parameter	**Standardwert**	**Beschreibung**
Currently Used	**L2SWITCH**	In dieser Spalte wird der Hostname angezeigt.
Configured		Geben Sie im Eingabefeld den Hostnamen ein.
Management VLAN		
Parameter	**Standardwert**	**Beschreibung**
Currently Used	**1**	In dieser Spalte wird das Management-VLAN angezeigt.
Configured		Geben Sie im Eingabefeld das Management-VLAN ein.

9.2.4.2 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.

Hinweis

Synchronisieren der Uhren in Computersystemen

Das SNTP („Simple Network Time Protocol“) ist ein Protokoll zur Synchronisierung von Uhren in Computersystemen über paketvermittelte Netzwerke mit variabler Paketlaufzeit.

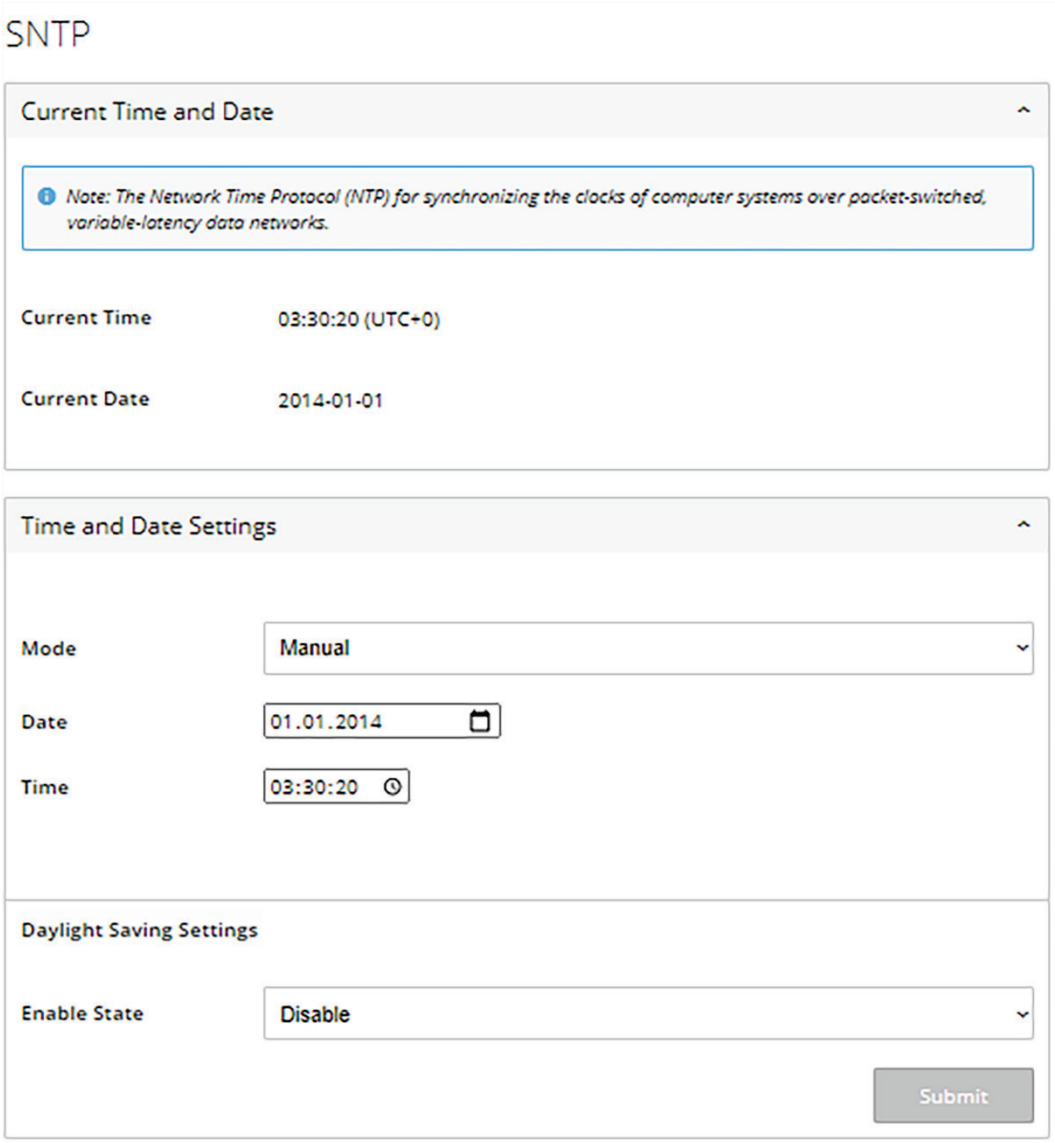


Abbildung 54: Register „Configuration“ – Menü „System Management“ – „SNTP“

Tabelle 43: Register „Configuration“ – Menü „System Management“ – „SNTP“

Current Time and Date				
Parameter	**Standardwert**	**Beschreibung**		
Current Time		In diesem Anzeigefeld wird die aktuelle Uhrzeit angezeigt, wenn Sie dieses Menü öffnen bzw. aktualisieren.		
Current Date		In diesem Anzeigefeld wird das aktuelle Datum angezeigt, wenn Sie dieses Menü öffnen bzw. aktualisieren.		
Time and Date Settings				
Parameter	**Standardwert**	**Beschreibung**		
Mode	Manual	Wählen Sie diese Option, wenn Sie Zeit und Datum für das System manuell einstellen möchten. Nachdem Sie auf **[Submit]** geklickt haben, erscheinen die neuen Angaben in den Anzeigefeldern „Aktuelle Uhrzeit“ und „Aktuelles Datum“.		
		Date	Geben Sie das neue Datum im Format Tag/Monat/Jahr ein. TT.MM.JJJJ	
		Time	Geben Sie die neue Zeit im Format Stunde/Minute/Sekunde ein. --:--:--	
	Network Time Protocol	Wählen Sie diese Option, wenn Sie das Network Time Protocol (NTP) für den Zeitdienst verwenden möchten.		
	NTP Server	Public	Wählen Sie diese Option, wenn Sie einen öffentlichen Server verwenden möchten.	
			ntp0.fau.de - Europe	
			ntps1-1.cs.tu-berlin.de - Europe	
	0.0.0.0	Manual	Wählen Sie diese Option, wenn Sie manuelle Einstellungen verwenden möchten.	
			IP	Geben Sie die IP-Adresse des NTP-Servers in Dezimalpunktschreibweise ein.
			Domain Name	Geben Sie die Domain-Adresse des Switches ein.
	Time Zone **+0000**	Geben Sie den Zeitunterschied zwischen UTC („Universal Time Coordinated“, ehemals GMT, „Greenwich Mean Time“) und der Zeitzone in hh:mm ein.		

Tabelle 43: Register „Configuration“ – Menü „System Management“ – „SNTP“

Daylight Saving Settings		
Parameter	**Standardwert**	**Beschreibung**
Enable State	**Disable**	Wählen Sie „Disable“, wenn Sie die Sommerzeit nicht verwenden möchten
	Enable	Wählen Sie „Enable“, wenn Sie die Sommerzeit verwenden möchten
Start Date[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.
End Date[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).	

9.2.4.3 Benutzerkonto (User Account)

Der Switch ermöglicht die Einrichtung von bis zu sechs Benutzerkonten. Der Benutzername sollte aus einer Kombination aus Zahlen oder Buchstaben bestehen. Das letzte Administratorkonto kann nicht gelöscht werden. Zur Nutzung der CLI oder des Web-Based- Managements muss sich ein Benutzer mit einem gültigen Benutzerkonto angemeldet haben.

Benutzerberechtigungen

Der Switch unterstützt zwei Arten von Benutzerkonten:

Die Default-Benutzerkonten haben folgende Anmeldeinformationen:
User Name = „admin“
User Password = „wago“

1.	Admin-Konten	Schreib-/Leseberechtigung
2.	normale Benutzerkonten	Nur Leseberechtigung - Die Nutzung des privilegierten Modus in der CLI ist nicht möglich. - Die Änderung von Konfigurationen im Web-Management ist nicht möglich.

Hinweis

Benutzerkonteneinstellungen

In den Benutzerkonteneinstellungen können die Zugangsberechtigungen zum Switch oder auf 802.1X-Netzwerke konfiguriert werden.

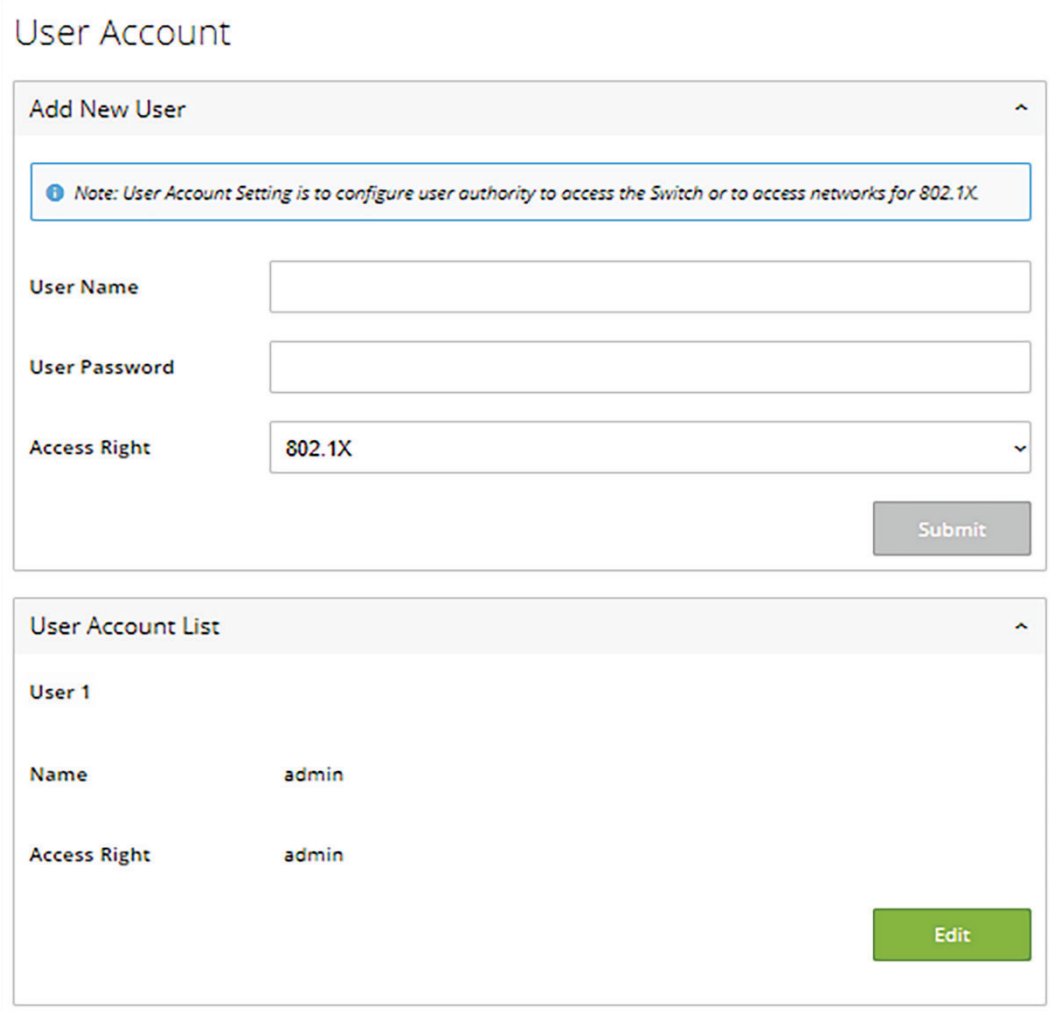


Abbildung 55: Register „Configuration“ – Menü „System Management“ – „User Account“

Tabelle 44: Register „Configuration“ – Menü „System Management“ – „User Account“

User Account Settings		
Parameter	**Standardwert**	**Beschreibung**
User Name		Geben Sie im Eingabefeld einen neuen Benutzernamen ein oder modifizieren Sie einen bereits bestehenden Benutzernamen.
User Password		Geben Sie im Eingabefeld ein neues Passwort ein oder modifizieren Sie ein bereits bestehendes Passwort. Sie können bis zu 32 alphanumerische Zeichen oder Zahlen eintragen.
User Authority		In diesem Auswahlfeld wählen Sie die Art des Benutzerkontos aus.
	802.1X	Wählen Sie im Auswahlfeld „802.1X“, wenn Sie diese Benutzer zur Authentifizierung benötigen.
	Normal (Read Only)	Wählen Sie im Auswahlfeld “Normal (Read Only“, 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.
User Account List		
Parameter	**Standardwert**	**Beschreibung**
No.		In dieser Spalte wird die Indexnummer eines Eintrags angezeigt.
Name		In dieser Spalte wird der Name des Benutzerkontos angezeigt.
Access Right		In dieser Spalte wird die Art des Benutzerkontos angezeigt.
Action		Klicken Sie auf die Schaltfläche **[Clear]**, um ein Benutzerkonto zu löschen.
		Hinweis  **Löschen Administratorkonto** Das letzte Administratorkonto kann nicht gelöscht werden.

9.2.5 Sturmkontrolle (Storm Control)

Wenn ein Broadcast-Sturm eintritt, wird das Netzwerk fortlaufend mit Broadcast- oder Multicast-Datenpaketen überhäuft. Broadcast-Stürme können mit zunehmender Anzahl dieser Datenpakete 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 Datenpakete 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) Datenpaketen, die vom Switch pro Sekunde an den Ports empfangen werden können. Ist die maximale Anzahl dieser Datenpakete pro Sekunde erreicht, werden alle nachfolgenden Datenpakete verworfen. Aktivieren Sie diese Funktion, wenn Sie die Anzahl dieser Datenpakete im Netzwerk verringern möchten.

Die Standardrate beträgt 300 Pakete pro Sekunde für Broadcast und DLF. Sie können eine maximale Rate von 5000 Pakete pro Sekunde für Multicast, Broadcast oder DLF einstellen.

Hinweis

Funktionsweise der Storm Control

Die Funktion „Storm Control“ verhindert, dass die Ports eines Switches in einem LAN an einer der Schnittstellen von Broadcast-, Multicast- oder unbekannten Unicast-Paketen beeinträchtigt werden.

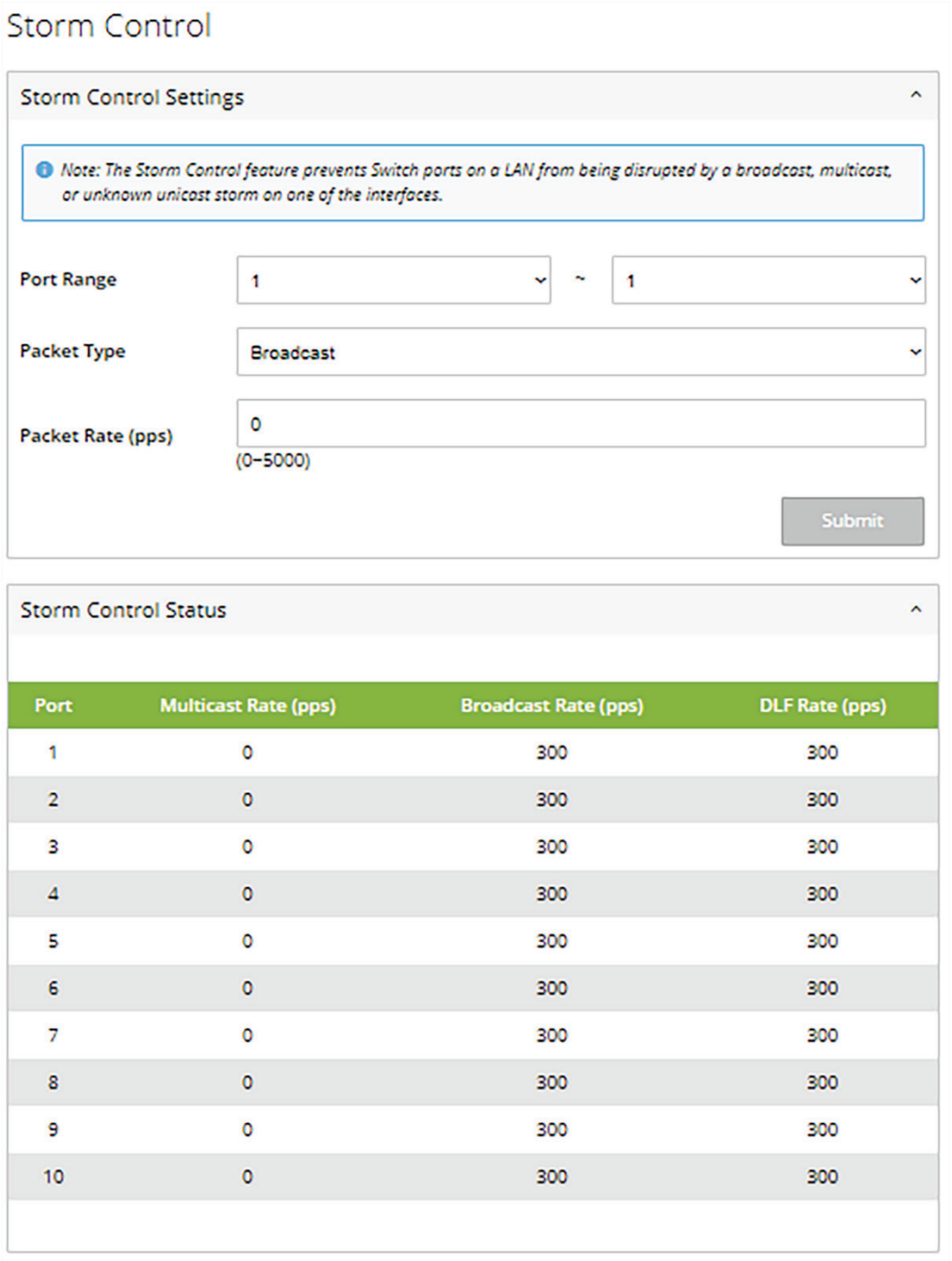


Abbildung 56: Register „Configuration“ – Menü „Storm Control“

Tabelle 45: Register „Configuration“ – Menü „Storm Control“

Storm Control Settings		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die Funktion „Storm Control“ zu konfigurieren.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die Funktion „Storm Control“ zu konfigurieren.
Packet Type	Broadcast	Wählen Sie im Auswahlfeld „Broadcast“, um einen Grenzwert für die Anzahl der pro Sekunde empfangenen Broadcast-Pakete festzulegen.
	Multicast	Wählen Sie im Auswahlfeld „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.
Packet Rate (0-5000)	300 = Broadcast/DLF Rate 0 = Multicast	Wählen Sie im Auswahlfeld die Anzahl der Datenpakete (des im Feld „Typ“ spezifizierten Typs) aus, die der Switch pro Sekunde empfangen kann.
Storm Control Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Multicast Rate (pps)		In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für „Multicast“ gibt.
Broadcast Rate (pps)		In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für „Broadcast“ gibt.
DLF Rate (pps)		In dieser Spalte wird angezeigt, ob es die Rate-Einstellung für „DLF“ gibt.

9.3 Sicherheit (Security)

9.3.1 802.1X

9.3.1.1 Kommunikationsstandard IEEE 802.1X

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

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

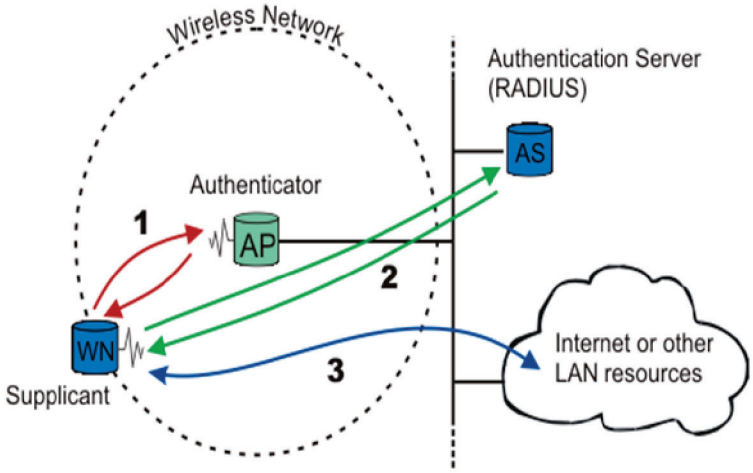


Abbildung 57: IEEE 802.1X

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

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

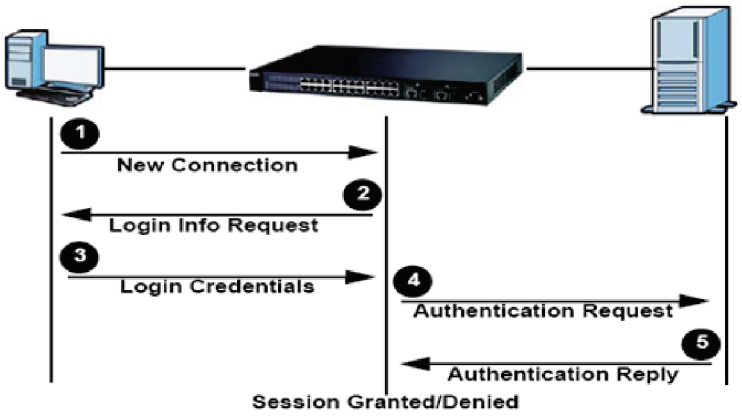


Abbildung 58: RADIUS-Server

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 Datenpakete am Port verworfen.

  Eingehend - Ist die 802.1X-Port-Authentifizierung für einen Benutzer fehlgeschlagen, werden nur am Port eingehende Datenpakete 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.

9.3.1.2 Globale Einstellungen (Global Setup)

Hinweis

Aktivieren der 802.1x-Authentifizierung
Aktivieren Sie aus Sicherheitsgründen die 802.1X-Authentifizierung für den Switch. Erst wenn Sie die 802.1X-Authentifizierung für den Switch aktiviert haben, können Sie diese Funktion auch für einzelne Ports konfigurieren.

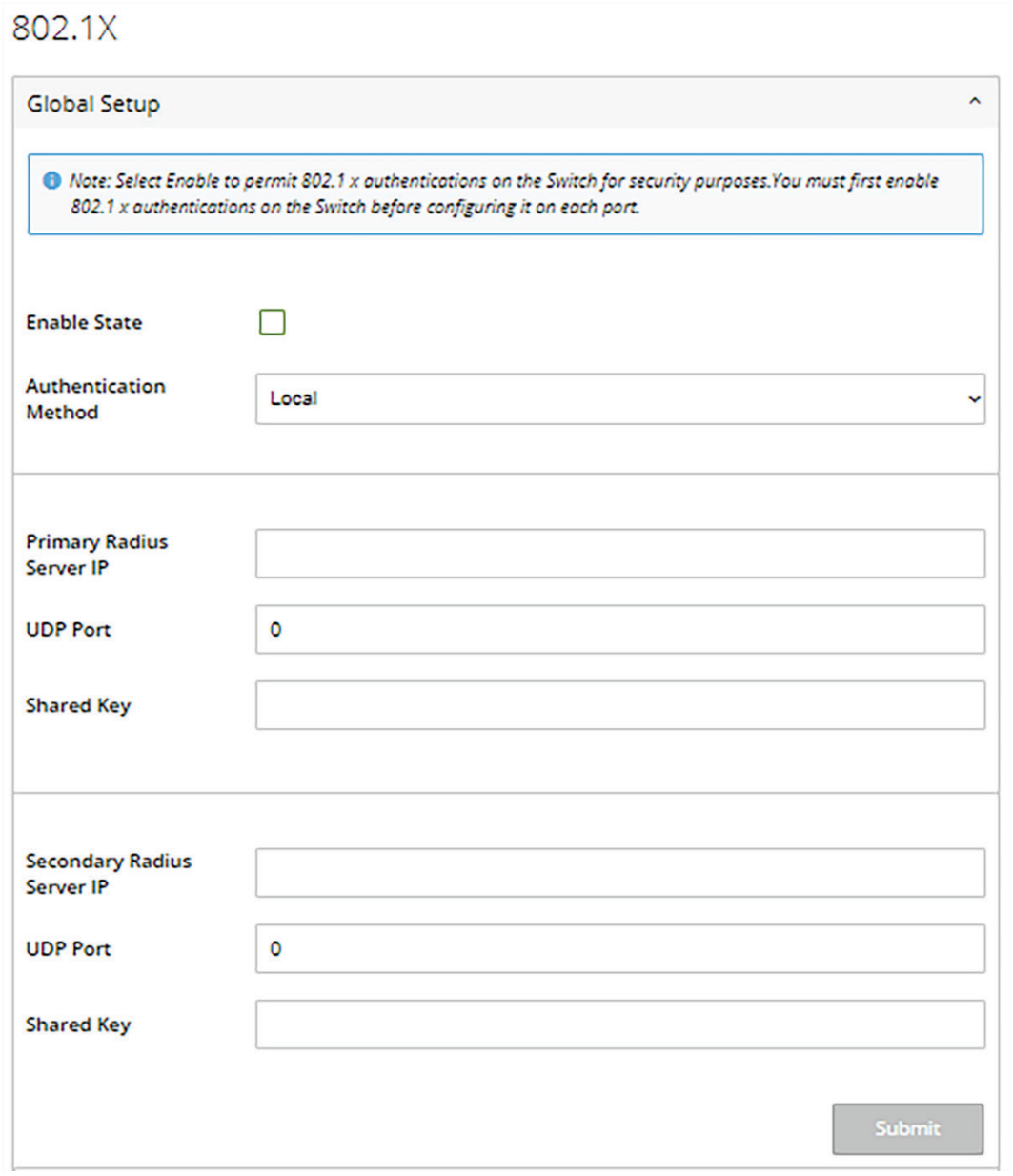


Abbildung 59: Register „Security“ – Menü „802.1X“ – „Global Setup“

Tabelle 46: Register „Security“ – Menü „802.1X“ – „Global Setup“

Global Setup		
Parameter	**Standardwert**	**Beschreibung**
Enable State	☐	☐ Die Funktion „802.1X“ ist für den Switch deaktiviert. ☑ Die Funktion „802.1X“ ist für den Switch aktiviert. **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.
Authentication Method	**Local**	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.
Primary Radius Server IP		Haben Sie beim Authentifizierungsverfahren „Radius“ ausgewählt, wird der primäre Radius-Server für alle Authentifizierungsanfragen verwendet. Geben Sie im Eingabefeld die IP-Adresse des externen Radius-Servers in Dezimalpunktschreibweise ein.
UDP Port	**0**	In diesem Anzeigefeld wird die VLAN-ID konfiguriert.
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.
Secondary RADIUS Server IP		Dies ist die IP für den sekundären Radius-Server, der nur als Back-up-Server zum Einsatz kommt, wenn der primäre Radius-Server ausfällt.

Tabelle 46: Register „Security“ – Menü „802.1X“ – „Global Setup“

Global Setup		
Parameter	**Standardwert**	**Beschreibung**
UDP Port	**0**	Geben Sie im Eingabefeld die IP-Adresse des externen Radius-Servers in Dezimalpunktschreibweise 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.

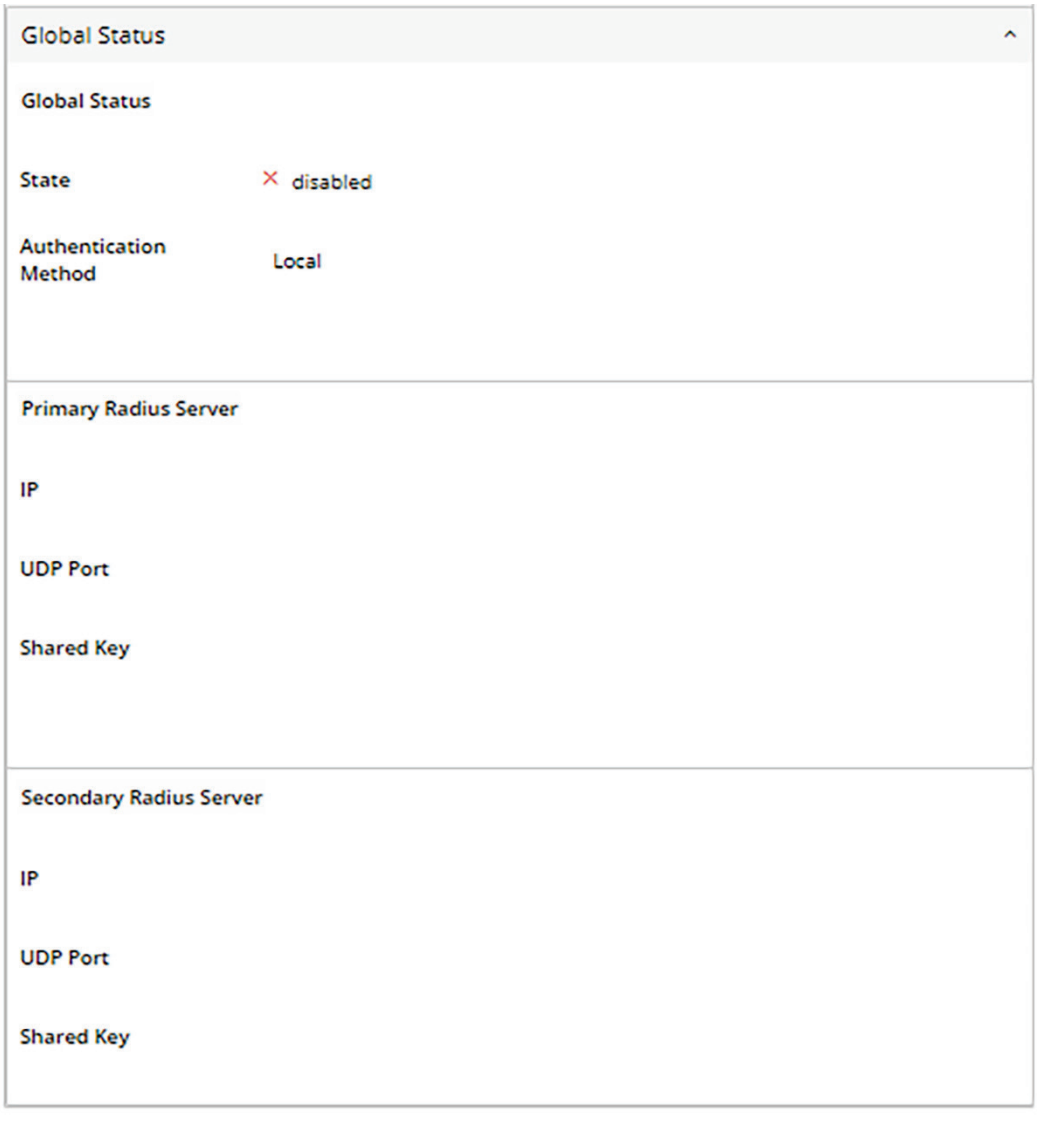


Abbildung 60: Register „Security“ – Menü „802.1X“ – „Global Status“

Tabelle 47: Register „Security“ – Menü „802.1X“ – „Global Status“

Global Status		
Parameter	**Standardwert**	**Beschreibung**
State	Disable Enable	In diesem Anzeigefeld wird angezeigt, ob die IEEE-802.1X-Authentifizierung aktiviert oder deaktiviert ist.
Authentication Method	Local Radius	In diesem Anzeigefeld wird das Authentifizierungsverfahren angezeigt.
Primary 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	
Secondary 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	

9.3.1.3 Port-Einstellungen (Port Setup)

Hinweis

802.1X-Authentifizierung
802.1X verwendet eine portbasierte Authentifizierung, bei der die Kommunikation zwischen einem sog. „Supplicant“ (Anfragesteller), einem „Authenticator“ (Authentikator) und einem Authentifizierungsserver verwendet wird.
Es gelten folgende Default-Werte: „Max-Req Times“ (Max. Anfragen): 2, „Quiet-Period“ (Passivitätszeitraum): 20 s, „Supp-Timeout“ (Anfragestellerzeitlimit): 30 s und „Server-Timeout“ (Serverzeitlimit): 16 s.

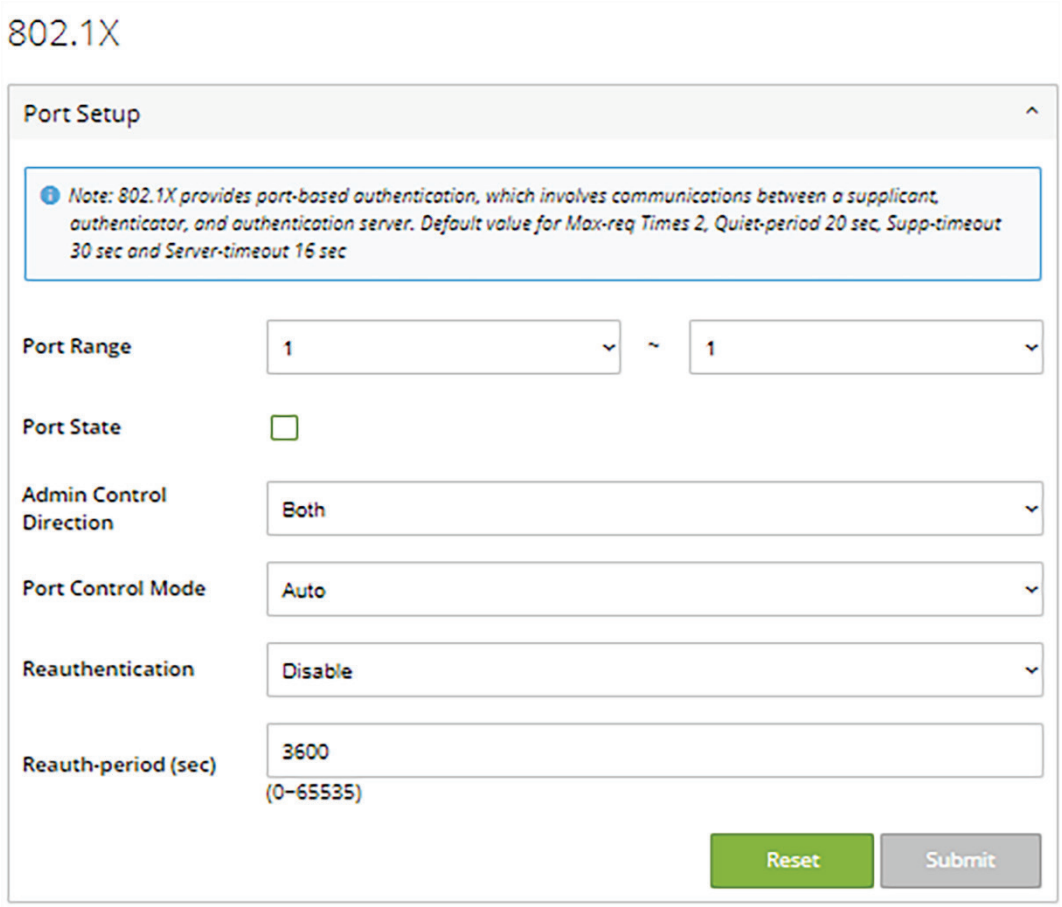
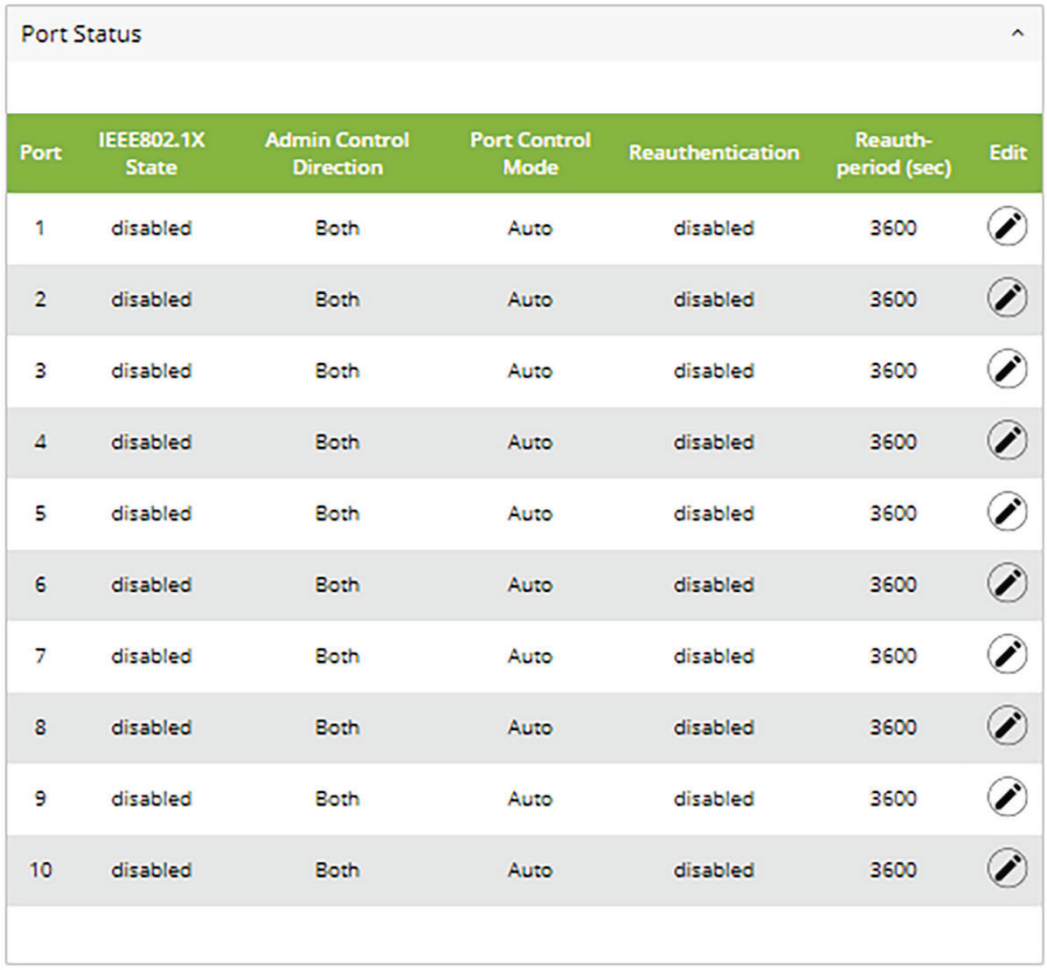


Abbildung 61: Register „Security“ – Menü „802.1X“ – „Port Setup“

Tabelle 48: Register „Security“ – Menü „802.1X“ – „Port Setup“

Port Setup		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die Funktion „Port Setup“ zu konfigurieren.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die Funktion „Port Setup“ zu konfigurieren.
Port State	☐	☐ Die Funktion „802.1X” ist für den Switch deaktiviert. ☑ Die Funktion „802.1X” ist für den Switch aktiviert. **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.
Admin Control Direction	**Both**	Wählen Sie im Auswahlfeld „Both“, wenn nach der fehlgeschlagenen IEEE-802.1X-Port-Authentifizierung eines Benutzers sowohl am Port eingehende als auch ausgehende Datenpakete verworfen werden sollen.
	In	Wählen Sie im Auswahlfeld „In“, wenn nach der fehlgeschlagenen IEEE-802.1X-Port-Authentifizierung eines Benutzers nur am Port eingehende Datenpakete verworfen werden sollen.
Reauthentication	**Disable**	Wählen Sie im Auswahlfeld „Disable“, wenn ein Teilnehmer den Benutzernamen und das Passwort nicht regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.
	Enable	Wählen Sie im Auswahlfeld „Enable“, 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.
	Force Authorized	Wählen Sie im Auswahlfeld „Force Authorized“, um eine permanente Authentifizierung für den Port zu aktivieren.
	Force Unauthorized	Wählen Sie im Auswahlfeld „Force Unauthorized“, um eine permanente Verweigerung der Authentifizierung für den Port zu aktivieren. Dadurch können an diesem Port keine Datenpakete weitergeleitet werden.
Reauth-period (sec) (0-65535)	**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.



Port Status

Port	IEEE802.1X State	Admin Control Direction	Port Control Mode	Reauthentication	Reauth-period (sec)	Edit
1	disabled	Both	Auto	disabled	3600	
2	disabled	Both	Auto	disabled	3600	
3	disabled	Both	Auto	disabled	3600	
4	disabled	Both	Auto	disabled	3600	
5	disabled	Both	Auto	disabled	3600	
6	disabled	Both	Auto	disabled	3600	
7	disabled	Both	Auto	disabled	3600	
8	disabled	Both	Auto	disabled	3600	
9	disabled	Both	Auto	disabled	3600	
10	disabled	Both	Auto	disabled	3600	

Abbildung 62: Register „Security“ – Menü „802.1X“ – „Port Status“

Tabelle 49: Register „Security“ – Menü „802.1X“ – „Port Status“

Port Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 **...** 10	In dieser Spalte werden die Port-Nummern angezeigt.
IEEE 802.1X State	Disable Enable	In dieser Spalte wird angezeigt, ob die IEEE-802.1X-Authentifizierung für einen Port aktiviert oder deaktiviert ist.
Admin Control Direction	Both In	In dieser Spalte wird die „Admin Control Direction“ angezeigt.
Port Control Mode	Automatic, Force Authorized, Force Unauthorized	In dieser Spalte wird der Port-Control-Mode angezeigt.
Reauthentication	Disable Enable	In dieser Spalte wird angezeigt, ob der Teilnehmer den Benutzernamen und das Passwort regelmäßig erneut eingeben muss, um mit dem Port verbunden zu bleiben.
Reauth Period (sec)	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.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.3.2 Access-Control-Liste (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 Datenpaketen festzulegen, die von spezifischen Eingangs-Ports oder allen Ports empfangen werden. Durch diese Regeln werden die MAC-Quell- und Zieladressen von Datenpaketen überprüft. Entsprechen die Datenpakete diesen Regeln, wird das System die Aktion „deny“ (verweigern) ausführen. Das heißt, dass die Datenpakete 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.

Hinweis

Berechtigungen der Access Control List (ACL)

Die „Access Control List“ (ACL, Zugriffssteuerungsliste) ist eine Liste mit Berechtigungen, die an ein Objekt angehängt ist und in der maximal 32 ACL-Einstellungen erlaubt sind. Mit dem „Drop State“ (Zugriffsverweigerung) wird spezifiziert, wem oder was der Zugriff auf das Objekt verweigert wird.

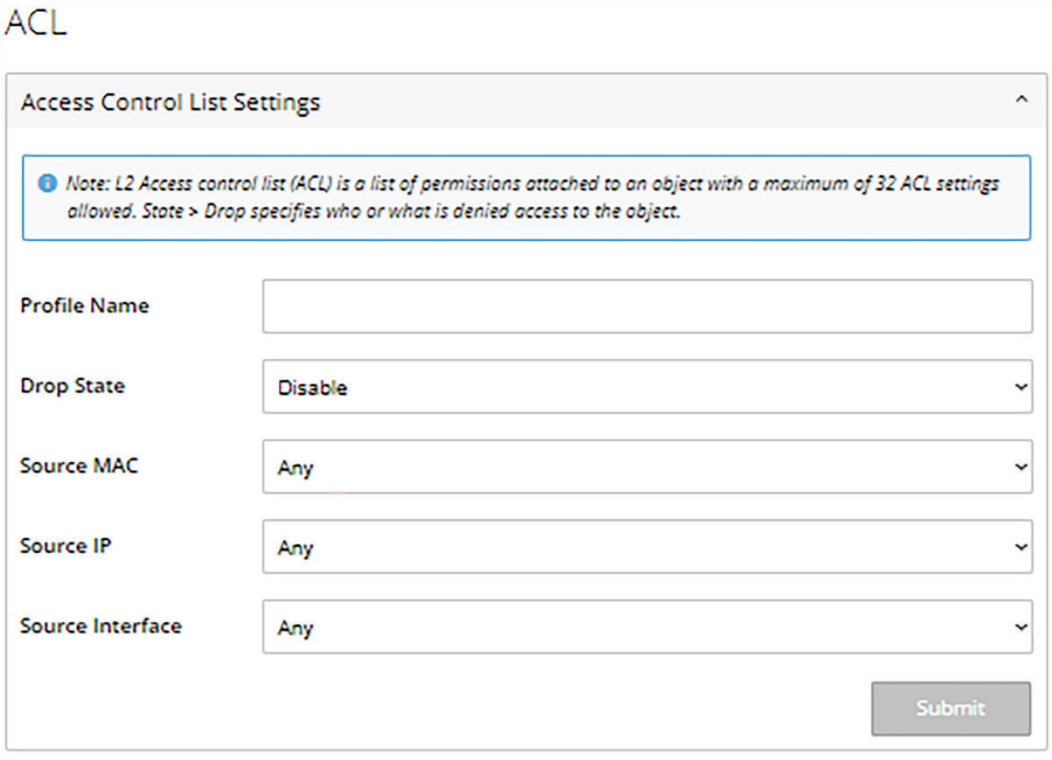


Abbildung 63: Register „Security“ – Menü „ACL“ – „Access Control List Settings“

Tabelle 50: Register „Security“ – Menü „ACL“ – „Access Control List Settings“

Access Control List Settings			
Parameter	**Standardwert**	**Beschreibung**	
Profile Name		Geben Sie im Eingabefeld den Namen des Profils ein.	
Drop State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, wenn die Datenpakete nicht verworfen werden sollen.	
	Enable	Wählen Sie im Auswahlfeld „Enable“, wenn die Datenpakete verworfen werden sollen.	
Source MAC	**Any**	Wählen Sie im Auswahlfeld „Any“, damit jede MAC-Adresse gültig ist.	
	Other	Wählen Sie im Auswahlfeld „Other“, um die MAC-Adresse für die Quelle in die Access-Control-Liste einzutragen.	
Source IP	**Any**	Wählen Sie im Auswahlfeld „Any“, damit jede IP-Adresse gültig ist.	
	Other	Wählen Sie im Auswahlfeld „Other“, um die Source-IP-Adresse in die Access-Control-Liste einzutragen.	
Source Interface	**Any**	Wählen Sie im Auswahlfeld „Any“, wenn jeder physikalische Port gültig ist.	
	Other	1 … 10	Geben Sie im Eingabefeld den physikalischen Port ein, für den dieser Eintrag in der Access-Control-Liste gültig ist.

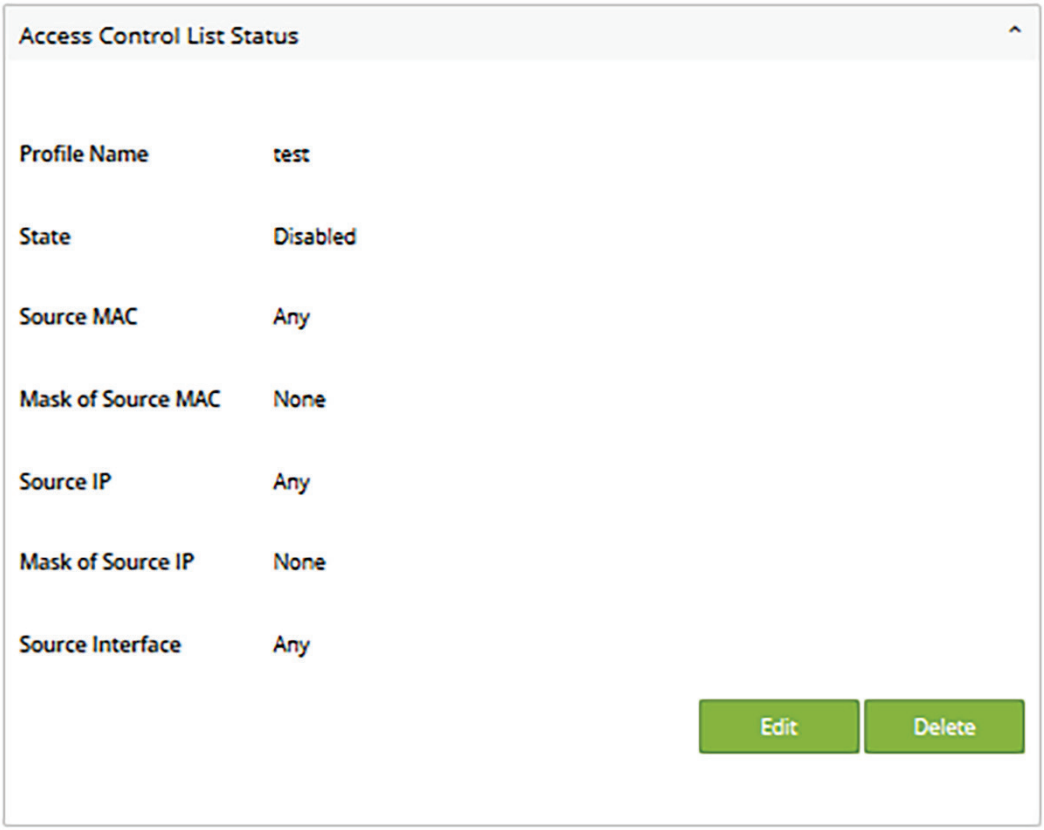


Abbildung 64: Register „Security“ – Menü „ACL“ – „Access Control List Status“

Tabelle 51: Register „Security“ – Menü „ACL“ – „Access Control List Status“

Access Control List Status		
Parameter	**Standardwert**	**Beschreibung**
Profile Name		In diesem Anzeigefeld wird der gewählte Name des Profils angezeigt.
Drop State	Disable Enable	In diesem Anzeigefeld wird der „Drop State“ angezeigt.
Source MAC Address	Any Other	In diesem Anzeigefeld wird die Source-Mac-Adresse angezeigt.
Source IP	Any Other	In diesem Anzeigefeld wird die Source-IP angezeigt.
Source Interface	Any Other	In diesem Anzeigefeld wird das Source-Interface angezeigt.

9.3.3 Port-Sicherheit (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 Datenpakete 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.

Hinweis

Konfiguration der Port-Sicherheitsfunktionen
In den Port-Sicherheitsfunktionen kann konfiguriert werden, welche Anzahl von MAC-Adressen an den Schnittstellen zulässig sind.

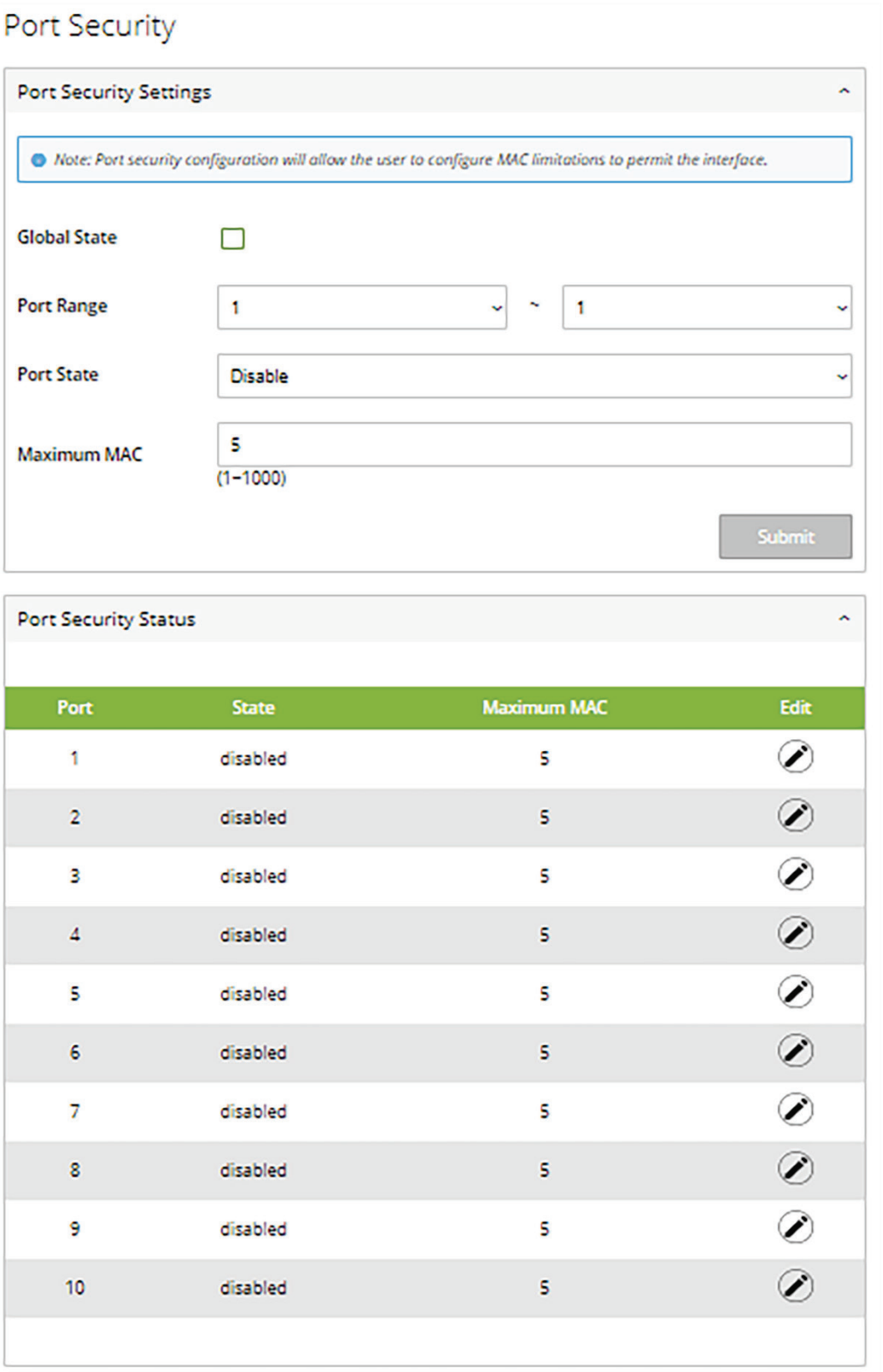


Abbildung 65: Register „Security“ – Menü „Port Security“

Tabelle 52: Register „Security“ – Menü „Port Security“

Port Security Settings			
Parameter	**Standardwert**	**Beschreibung**	
Global State	☐	☐	Die Funktion „Port Security“ ist für den Switch deaktiviert.
		☑	Die Funktion „Port Security“ ist für den Switch aktiviert.
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port Security“ zu konfigurieren.	
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „Port Security“ zu konfigurieren.	
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die Port-Sicherheit für einen Port bzw. Port-Bereich zu deaktivieren.	
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die Port-Sicherheit für einen Port bzw. Port-Bereich zu aktivieren.	
Maximum MAC (1–1000)	**5**	Geben Sie im Eingabefeld die maximale Anzahl der MAC-Adressen pro Schnittstelle ein.	
Port Security Status			
Parameter	**Standardwert**	**Beschreibung**	
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.	
State	Enable Disable	In dieser Spalte wird angezeigt, ob die Port-Sicherheit aktiviert oder deaktiviert ist.	
Maximum MAC Address	0 … 1000	In dieser Spalte wird die maximale Anzahl von MAC-Adressen angezeigt.	
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.	

9.3.4 Service Control

Mit der „Service Control“ können die Security-Dienste konfiguriert werden, die auf das Gerät zugreifen, wie etwa HTTP, HTTPS, SNMP v1/v2c, SNMP v3 oder SSH.

Hinweis

Funktion der Service Control

In der „Service Control“ werden Dienste, die auf das Gerät zugreifen, aktiviert bzw. deaktiviert.

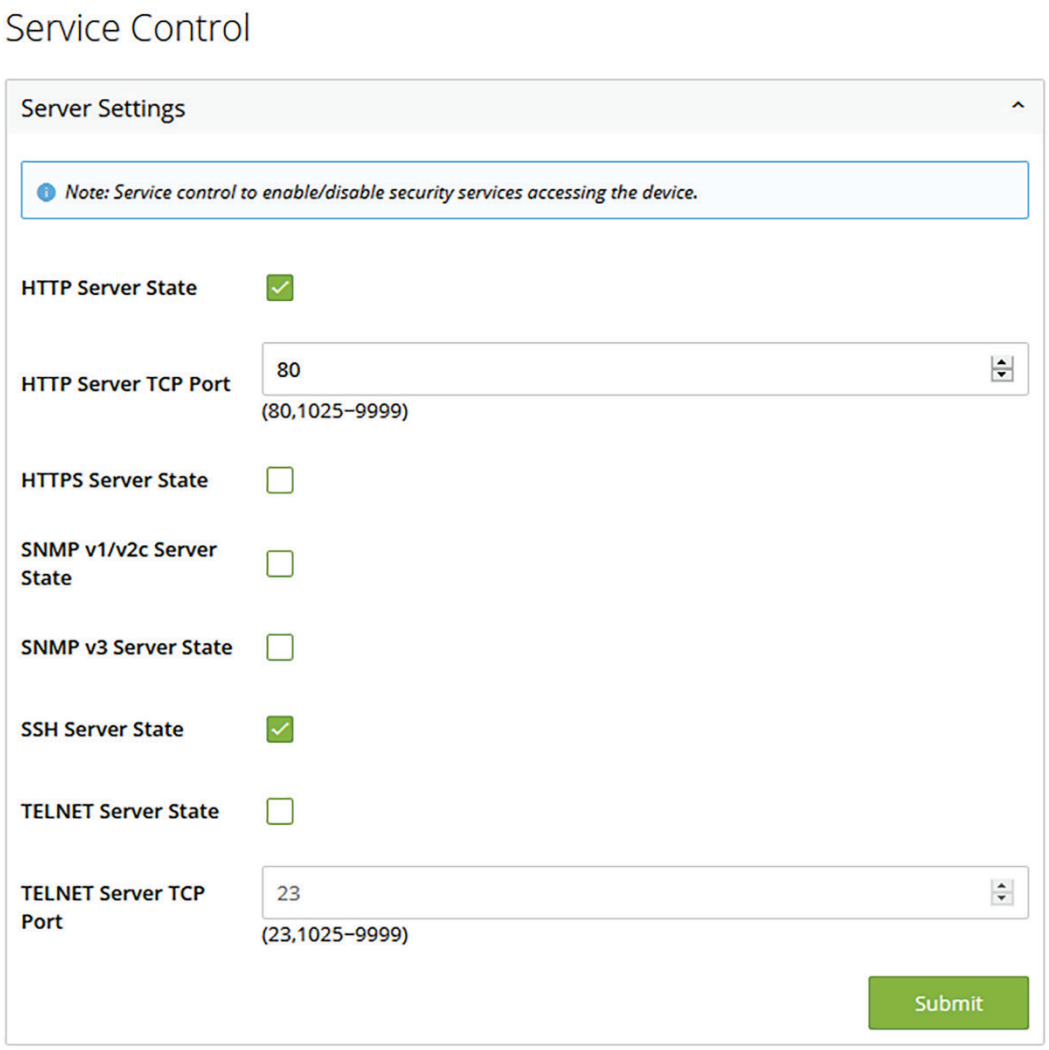


Abbildung 66: Register „Security“ – Menü „Service Control“

Tabelle 53: Register „Security“ – Menü „Service Control“

Server Settings		
Parameter	**Standardwert**	**Beschreibung**
HTTP Server State	☑	Aktiviert/deaktiviert den „HTTP-Server“.
HTTP Server TCP Port (80, 1025–9999)	**80** 1025 … 9999	Geben Sie im Eingabefeld den „HTTP-Server-TCP-Port“ ein.
HTTPS Server State	☐	Aktiviert/deaktiviert den „HTTPS-Server“.
SNMP v1/v2c Server State	☐	Aktiviert/deaktiviert de „SNMP-v1/v2c-Server“.
SNMP v3 Server State	☐	Aktiviert/deaktiviert den „SNMP-v3-Server“.
SSH Server State	☑	Aktiviert/deaktiviert den „SSH-Server“.
Telnet Server State	☐	Aktiviert/deaktiviert den „Telnet-Server“.
Telnet Server TCP Port (23, 1025~9999)	**23** 1025 … 9999	Geben Sie im Eingabefeld den TCP-Port für den Telnet-Server ein.
Server Status		
Parameter	**Standardwert**	**Beschreibung**
HTTP Server State	Enable Disable	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.
HTTP Server State	Enable Disable	In diesem Anzeigefeld wird der Status des HTTPS-Servers angezeigt.
SNMP v1/v2c Server State	Enable Disable	In diesem Anzeigefeld wird der Status des SNMP-v1/v2c-Servers angezeigt.
SNMP v3 Server State	Enable Disable	In diesem Anzeigefeld wird der Status des SNMP-v3-Servers angezeigt.
SSH Server State	Enable Disable	In diesem Anzeigefeld wird der Status des SSH-Servers angezeigt.
Telnet Server Status	Enable Disable	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.

9.3.5 VLAN

9.3.5.1 Port-Isolation (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 Datenpakete 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.

Hinweis

Konfigurieren der Ports

Es können Port-Bereiche konfiguriert werden. Dabei werden die vermittelnden Ports in virtuelle private Domänen partitioniert, die einzeln zugewiesen werden. Wenn z. B. die Kommunikation nur zwischen Port 1 und Port 2 erfolgen soll, dann kann die Port-Isolation genau so konfiguriert werden.

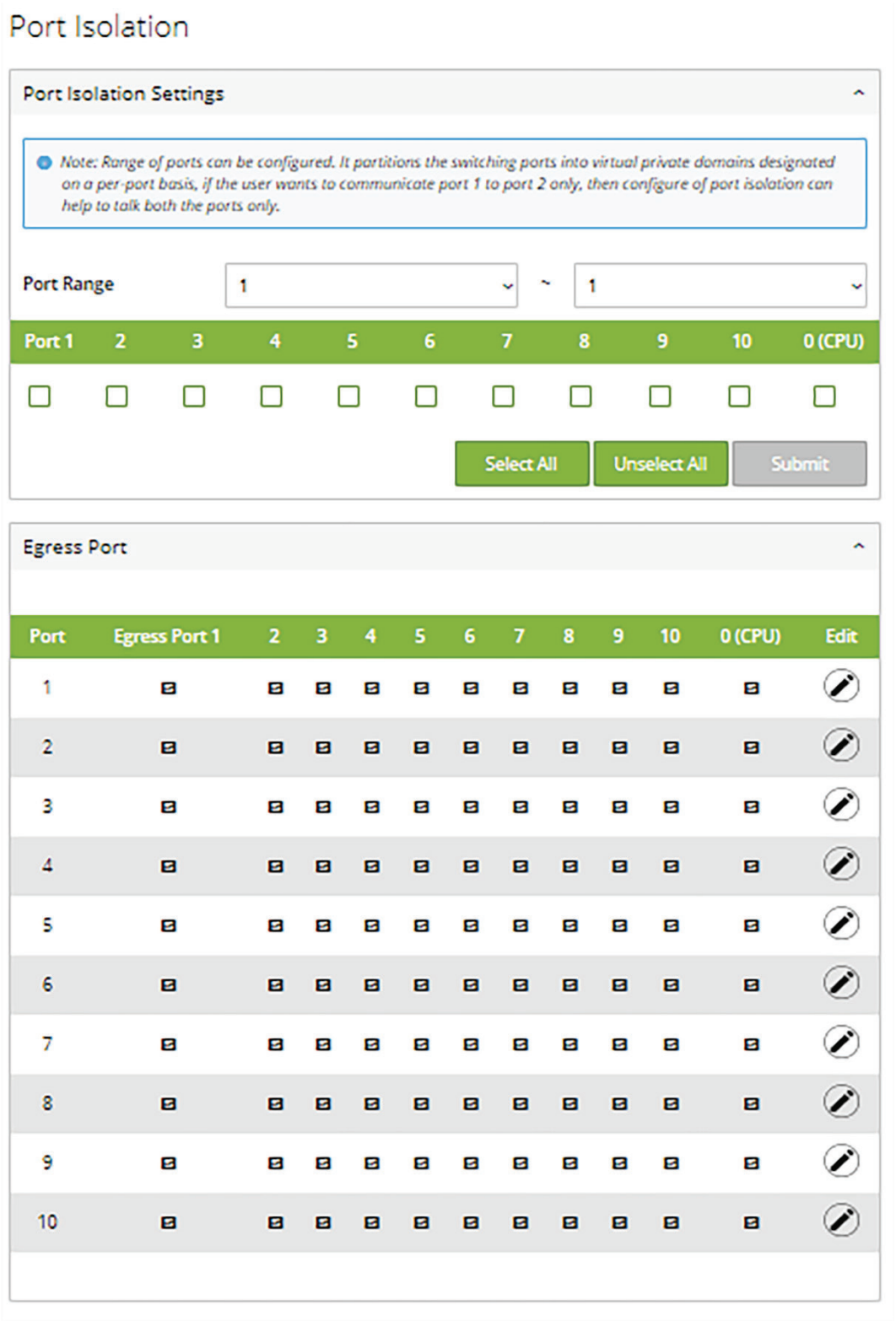


Abbildung 67: Register „Security“ – Menü „VLAN“ – „Port Isolation“

Tabelle 54: Register „Security“ – Menü „VLAN“ – „Port Isolation“

Port Isolation Settings				
Parameter		**Standardwert**	**Beschreibung**	
Port Range		**1** … 10 0 (CPU)	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Isolation“ konfigurieren möchten.	
		1 … 10 0 (CPU)	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, für den Sie die Einstellung der „Port Isolation“ konfigurieren möchten.	
Egress Port			Ein „Egress Port“ ist ein ausgehender Port, über den ein Datenpaket gesendet wird. Die Auswahl eines Ports als „Egress Port“ bedeutet, dass er mit dem Port, den Sie gerade konfigurieren, kommunizieren wird.	
	Select All	☐	☐	Es ist kein „Egress Port“ ausgewählt.
			☑	Es sind alle „Egress Ports“ ausgewählt.
	Disable All	☐	☐	Es ist kein „Egress Port“ deaktiviert.
			☑	Es sind alle „Egress Ports“ deaktiviert.
	☐ 0 (CPU) … ☐ 10	☐	☐	Der „Egress Port“ ist nicht aktiviert.
			☑	Der „Egress Port“ ist aktiviert.
Port Isolation Status				
Parameter		**Standardwert**	**Beschreibung**	
Port		**V**	V	„V“ zeigt an, dass die Datenpakete des Ports zu diesem Port gesendet werden können.
Egress Port			-	„-“ zeigt an, dass die Datenpakete des Ports nicht zu diesem Port gesendet werden können.
Edit			In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.	

9.3.5.2 VLAN-Einstellungen (VLAN Setup)

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 IEEE 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. Aber der Lean-Managed-Switch hat max. 5 VLANs zur Verfügung.

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.

Hinweis

Einrichtung von VLANs

Es können bis zu 5 VLANs eingerichtet werden. Es wird empfohlen, einen Trunk-Port mit Tag zu konfigurieren und alle Ports im VLAN beitreten zu lassen.

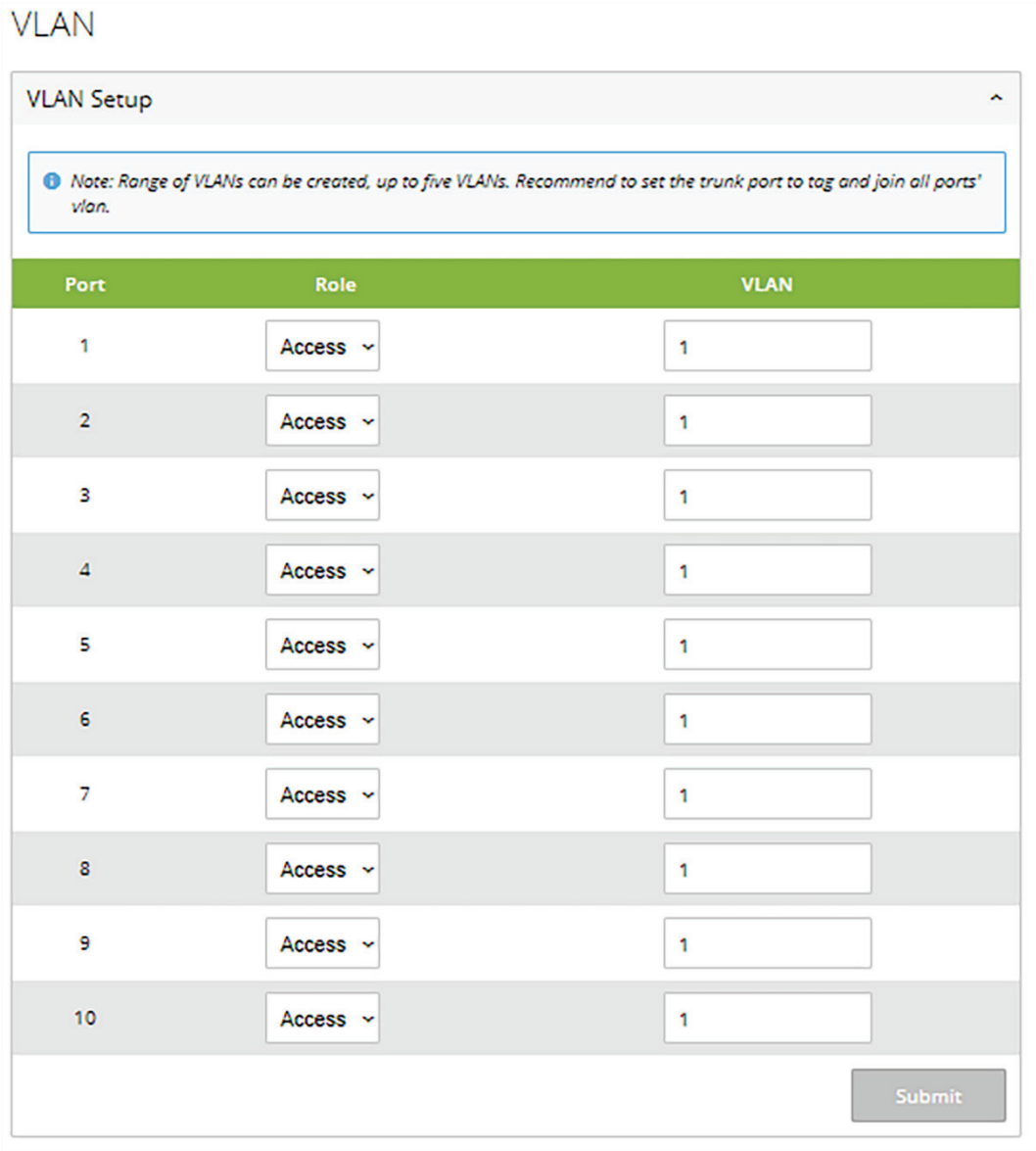


Abbildung 68: Register „Security“ – Menü „VLAN“ – „VLAN Setup“

Tabelle 55: Register „Security“ – Menü „VLAN“ – „VLAN Setup“

VLAN Setup		
Parameter	**Standardwert**	**Beschreibung**
Port		In dieser Spalte werden die Port-Nummern angezeigt.
Role	**Access**	Wählen Sie im Auswahlfeld „Access“, um diese „Role“ für den spezifischen Port auszuwählen.
	Trunk	Wählen Sie im Auswahlfeld „Trunk“, um diese „Role“ für den spezifischen Port auszuwählen.
VLAN		Geben Sie im Eingabefeld die „VLAN ID“ für diesen Eintrag ein. Gültiger Bereich: 1 … 4094
Tag	☐	☐ Der Port ist nicht aktiviert.
		☑ Der Port ist aktiviert.

Hinweis

Immer ein Port im Management-VLAN

Es muss immer ein Port im Management-VLAN sein.
Andernfalls kann der Switch nicht konfiguriert werden.
Eventuell ist dann ein Zurücksetzen des Switches auf die Werkseinstellungen notwendig sein. Dabei gehen die Konfigurationen verloren.

9.4 Redundanz (Redundancy)

9.4.1 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 800 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 zwei 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 Datenpakete 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 Datenpakete blockiert.

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

Hinweis

Funktion des Ethernet Ring Protection Switching (ERPS)

Die Funktion „Ethernet Ring Protection Switching“ (ERPS) implementiert einen Schutzschaltungsmechanismus für Ring-Topologien in der Ethernet-Schicht. Es sind nur zwei Ringeinstellungen mit einem standardmäßigen „WTR Timer“ von 300 s und einem „Guard Timer“ von 500 ms erlaubt. Global State aktiviert und deaktiviert die ERPS-Funktion (max. 2 Ringe pro Switch, max. 16 Switches pro Ring, Schaltzeit < 800 ms).
Über die Einstellung „Global State“ kann die ERPS-Funktion aktiviert bzw. deaktiviert werden.

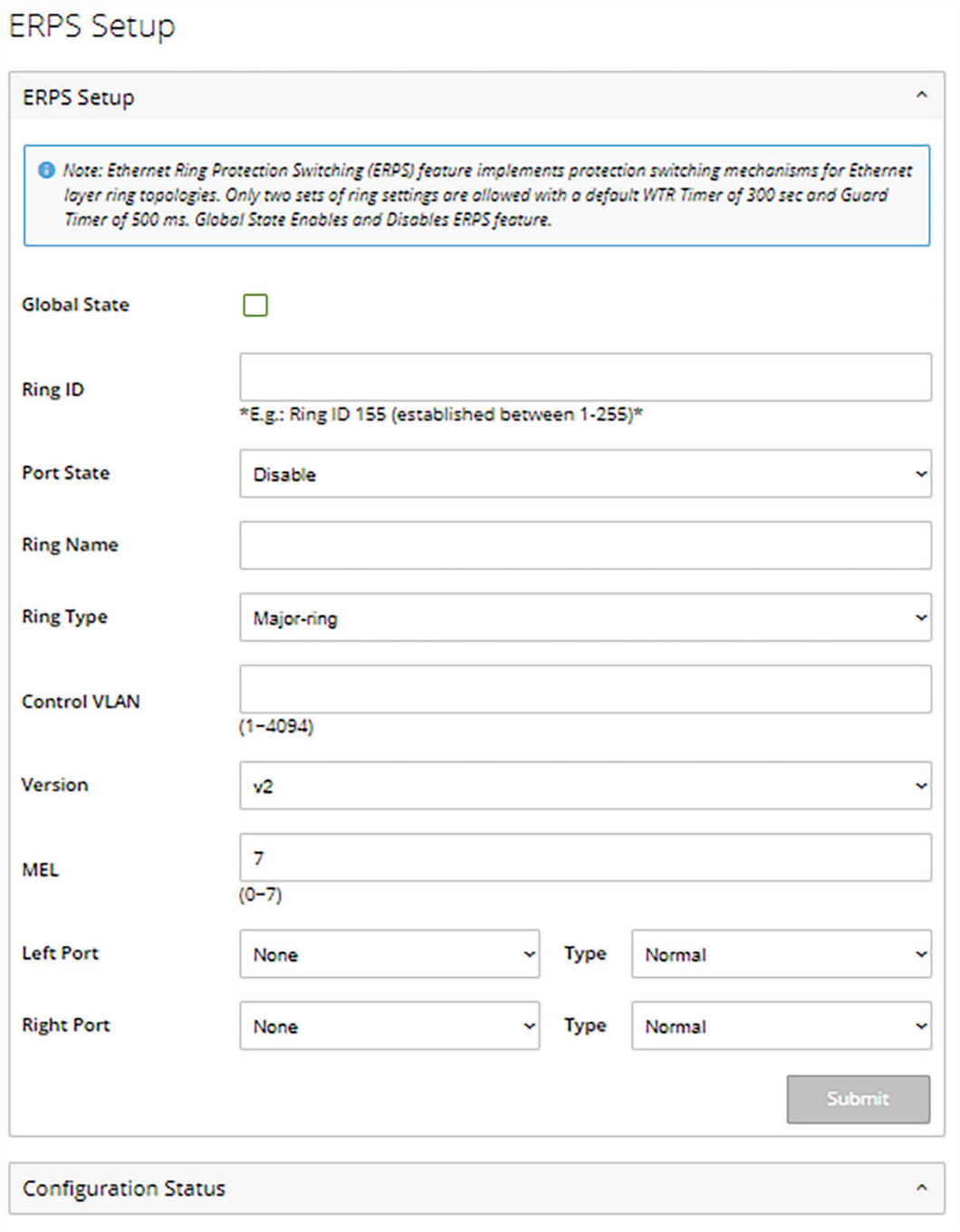


Abbildung 69: Register „Redundancy“ – Menü „ERPS“

Tabelle 56: Register „Redundancy“ – Menü „ERPS“

ERPS Setup		
Parameter	**Standardwert**	**Beschreibung**
Global State	☑	☐ Die Funktion „ERPS“ ist für den Switch deaktiviert. ☑ Die Funktion „ERPS“ ist für den Switch aktiviert.
Ring ID (*E.g.: Ring ID 155 (established between 1-255))		Geben Sie im Eingabefeld die Ring ID ein. Gültiger Bereich: 1 … 255 Aber der Lean-Managed-Switches unterstützt 2 Ringe.
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um den Zustand des Rings zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um den Zustand des Rings zu aktivieren.
Ring Name		Geben Sie im Eingabefeld den Namen des Rings ein (max. 32 Zeichen). (z. B. Major-Ring ID255)
Ring Type	**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.
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
Left Port		In diesem Auswahlfeld werden der linke Port und dessen Typ für den Ring konfiguriert.
	None	Wählen Sie im Auswahlfeld „None“, 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.
	Neighbor	Wählen Sie im Auswahlfeld „Neighbor“, 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.

Tabelle 56: Register „Redundancy“ – Menü „ERPS“

ERPS Setup		
Parameter	**Standardwert**	**Beschreibung**
Right Port		Wählen Sie im Auswahlfeld „v2“, wenn Sie die Version 2 der „ERPS“-Funktion nutzen möchten.
	None	Wählen Sie im Auswahlfeld „v1“, wenn Sie die Version 1 der „ERPS“-Funktion nutzen möchten.
	1 … 10	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
	Normal	In diesem Auswahlfeld werden der linke Port und dessen Typ für den Ring konfiguriert.
	Neighbor	Wählen Sie im Auswahlfeld „None“, wenn Sie keinen Port auswählen wollen.
	Owner	Wählen Sie im Auswahlfeld den entsprechenden Port aus.
ERPS Ring Status		
Parameter	**Standardwert**	**Beschreibung**
Ring ID	1 … 255	In diesem Anzeigefeld wird die Ring ID angezeigt.
Port State	Disable Enable	In diesem Anzeigefeld wird der Zustand des Ringes angezeigt.
Ring Name		In diesem Anzeigefeld wird der Name des Ringes angezeigt.
Ring Type	Major Ring Subring	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.
MEL	0 … 7	In diesem Anzeigefeld wird der Wert für das „Control MEL“ angezeigt.
Left Port	None 1 … 10 (12)	In diesem Anzeigefeld wird die Port-Nummer des linken Ports angezeigt.
Right Port	None 1 … 10 (12)	In diesem Anzeigefeld wird die Port-Nummer des rechten Ports angezeigt.
Left Port Type	Normal Neighbor Owner	In diesem Anzeigefeld wird der Typ des linken Ports angezeigt.
Right Port Type	Normal Neighbor Owner	In diesem Anzeigefeld wird der Typ des rechten Ports angezeigt.
Left Port Status	Forwarding Blocking	In diesem Anzeigefeld wird der aktuelle Status des linken Ports angezeigt.
Right Port Status	Forwarding Blocking	In diesem Anzeigefeld wird der aktuelle Status des rechten Ports angezeigt.
Ring Status	Protection Idle	In diesem Anzeigefeld wird der Ringstatus angezeigt.
Delete		Klicken Sie auf **[Clear]**, um diese Einstellung zu löschen.

9.4.2 STP/RSTP

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 57: 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.

9.4.2.1 STP/RSTP-Einstellung (STP/RSTP Setup)

Hinweis

Funktionen des STP/RSTP

Das STP/RSTP kann Netzwerkschleifen erkennen und aufbrechen sowie „Back-up Links“ (Ersatzverbindungen) zwischen Switches, Bridges oder Routern bereitstellen.

Default-Werte – „Forward Delay“: 15 s, „Mag Age“: 20 s und „Hello Time: 2 s.

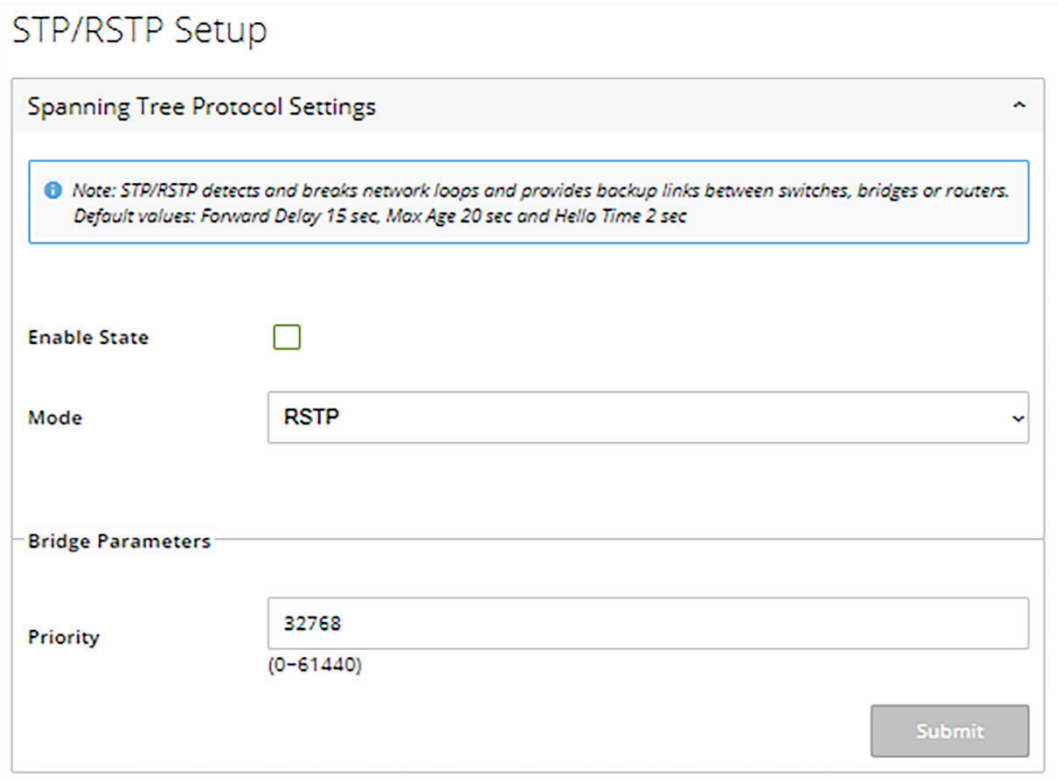


Abbildung 70: Register „Redundancy“ – Menü „STP/RSTP Setup“

Tabelle 58: Register „Redundancy“ – Menü „STP/RSTP Setup“

Spanning Tree Protocol Settings			
Parameter	**Standardwert**	**Beschreibung**	
Enable State	☐	☐	Die Funktion „STP/RSTP“ ist für den Switch deaktiviert.
		☑	Die Funktion „STP/RSTP“ ist für den Switch aktiviert.
Mode	**RSTP**	Wählen Sie im Auswahlfeld „RSTP“, wenn Sie das schnellere „Rapid Spanning Tree Protocol“ verwenden möchten.	
	STP	Wählen Sie im Auswahlfeld „STP“, wenn Sie das „Spanning Tree Protocol“ verwenden möchten.	
Bridge Parameters			
Parameter	**Standardwert**	**Beschreibung**	
Priority (Range: 0~61440)	**32768**	Geben Sie im Eingabefeld einen Wert für die Priorität ein. Je niedriger der von Ihnen zugewiesene numerische Wert ist, desto höher ist die Priorität dieser Bridge. Gültiger Bereich: 0 … 61440	

9.4.2.2 STP/RSTP-Port-Einstellung (STP/RSTP Port Setup)

Hinweis

Funktionen in den Port-Einstellungen
Die Port-Einstellungen ermöglichen die Konfiguration von Port-Bereich, „Edge Port“ und BDU-Filter sowie von „Guard“ und „Root Guard“ mit einem Default-Wert von 250 für die Pfadkosten und von 128 für die Priorität.

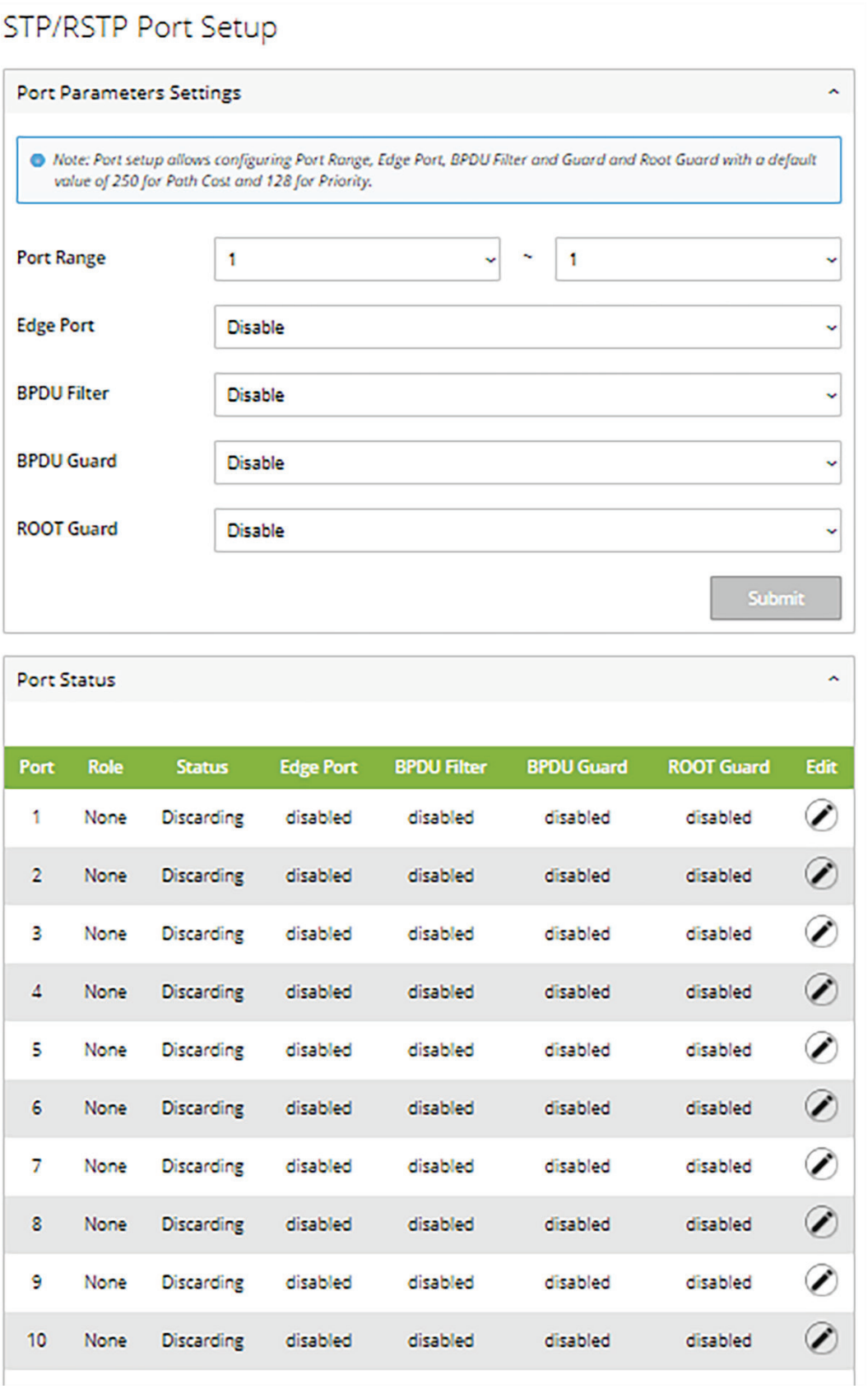


Abbildung 71: Register „Redundancy“ – Menü „STP/RSTP Port Setup“

Tabelle 59: Register „Redundancy“ – Menü „STP/RSTP Port Setup“

Port Parameter Settings		
Parameter	**Standardwert**	**Beschreibung**
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP/RSTP“-Funktion zu konfigurieren.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder einen Port-Bereich aus, um die „STP/RSTP“-Funktion zu konfigurieren.
Edge Port	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um den Port-Typ „Edge-Port“ für den spezifischen Port zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um den Port-Typ „Edge-Port“ für den spezifischen Port zu aktivieren.
BPDU Filter	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die BPDU-Filterfunktion für den spezifischen Port zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die BPDU-Filterfunktion für den spezifischen Port zu aktivieren.
BPDU Guard	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die Funktion „BPDU Guard“ für den spezifischen Port zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die Funktion „BPDU Guard“ für den spezifischen Port zu aktivieren.
ROOT Guard	**Disable**	Wählen Sie im Auswahlfeld „Disable“, um die Funktion „ROOT Guard“ für den spezifischen Port zu deaktivieren.
	Enable	Wählen Sie im Auswahlfeld „Enable“, um die Funktion „ROOT Guard“ für den spezifischen Port zu aktivieren.
Port Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
Role	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.
Edge Port	Disable Enable	In dieser Spalte wird der Zustand der Funktion „Edge Port“ angezeigt.

Tabelle 59: Register „Redundancy“ – Menü „STP/RSTP Port Setup“

Port Parameter Settings		
Parameter	**Standardwert**	**Beschreibung**
BPDU Filter	Disable Enable	In dieser Spalte wird der Zustand der BPDU-Filterfunktion angezeigt.
BPDU Guard	Disable Enable	In dieser Spalte wird der Zustand der Funktion „BPDU Guard“ angezeigt.
ROOT Guard	Disable Enable	In dieser Spalte wird der Zustand der Funktion „Root Guard“ angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.5 Diagnose (Diagnostic)

9.5.1 Alarm

9.5.1.1 Information

Hinweis

Aufgabe der Alarmfunktion
Die Alarmfunktion zeigt an, ob es Abweichungen gibt, die sofort korrigiert werden müssen.

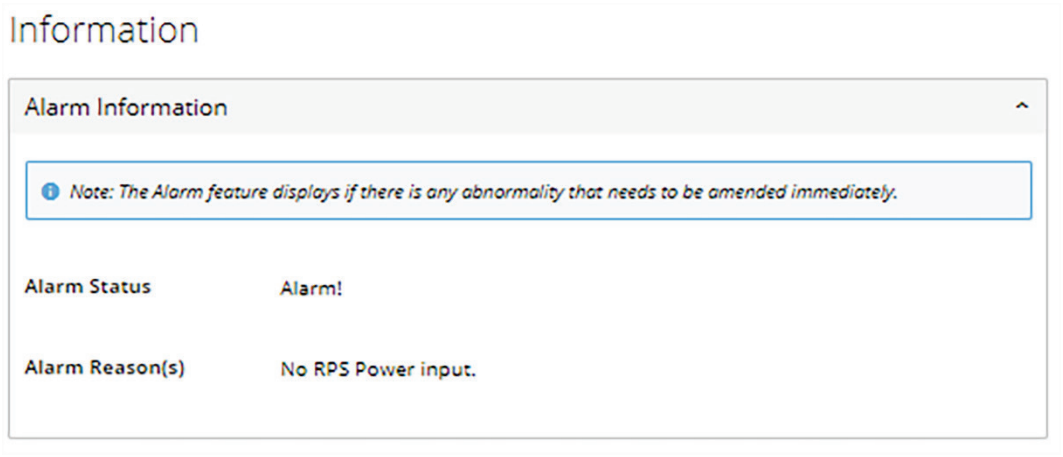


Abbildung 72: Register „Diagnostic“ – Menü „Information“

Tabelle 60: Register „Diagnostic“ – Menü „Information“

Alarm Information		
Parameter	**Standardwert**	**Beschreibung**
Alarm Status		In diesem Anzeigefeld wird angezeigt, ob Alarmereignisse stattgefunden haben.
Alarm Reason		In diesem Anzeigefeld werden die Details zu den Alarmereignissen angezeigt.

9.5.1.2 DIP Status

Hinweis

Anzeige des DIP-Status
Die Alarmfunktion zeigt an, ob es Abweichungen gibt, die sofort korrigiert werden müssen.

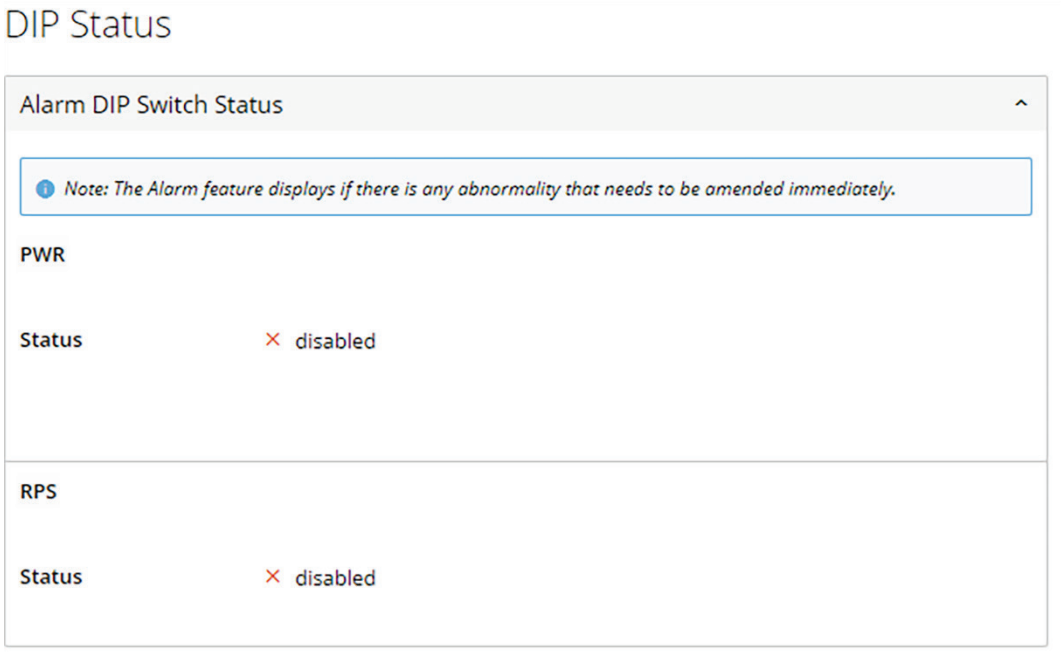


Abbildung 73: Register „Diagnostic“ – Menü „DIP Status“

Tabelle 61: Register „Diagnostic“ – Menü „DIP Status“

DIP switch Status		
Parameter	**Standardwert**	**Beschreibung**
PWR	**Disable** Enable	In diesem Feld wird angezeigt, ob „PWR“ aktiviert oder deaktiviert ist.
RPS	**Disable** Enable	In diesem Feld wird angezeigt, ob „RPS“ aktiviert oder deaktiviert ist.

9.5.1.3 Traffic Flooding

„Traffic Flooding“ bedeutet, dass Ihr Netzwerk fortlaufend mit Datenverkehr aus Broadcast- oder Multicast-Paketen „überflutet“ wird. „Broadcast Traffic Flooding“ kann mit zunehmender Anzahl dieser Pakete die Netzwerkkonnektivität vollständig lahmlegen.

Die „Traffic Flooding Control“ schützt die Switch-Bandbreite vor Paketüberflutungen, einschließlich Broadcast-Paketen, Multicast-Paketen und „Destination Lookup Failure“ (DLF, 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 Traffic Flooding 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 (pps) erreicht, werden alle nachfolgenden Pakete verworfen. Aktivieren Sie diese Funktion, wenn Sie die Anzahl dieser Pakete in Ihrem Netzwerk verringern möchten.

Obergrenze der „Traffic Flooding Control“: 3700 Pakete pro Sekunde (pps).

Default-Einstellungen

Broadcast Storm Control:	100 Pakete pro Sekunde (pps)
Multicast Storm Control	kein Wert
DLF Storm Control	100 Pakete pro Sekunde (pps)

Note

Einrichtung eines Alarm-Grenzwerts
Richten Sie einen Grenzwert für die Übertragung von Broadcast-, Multicast- und Broadcast-/Multicast-Pakettypen ein.

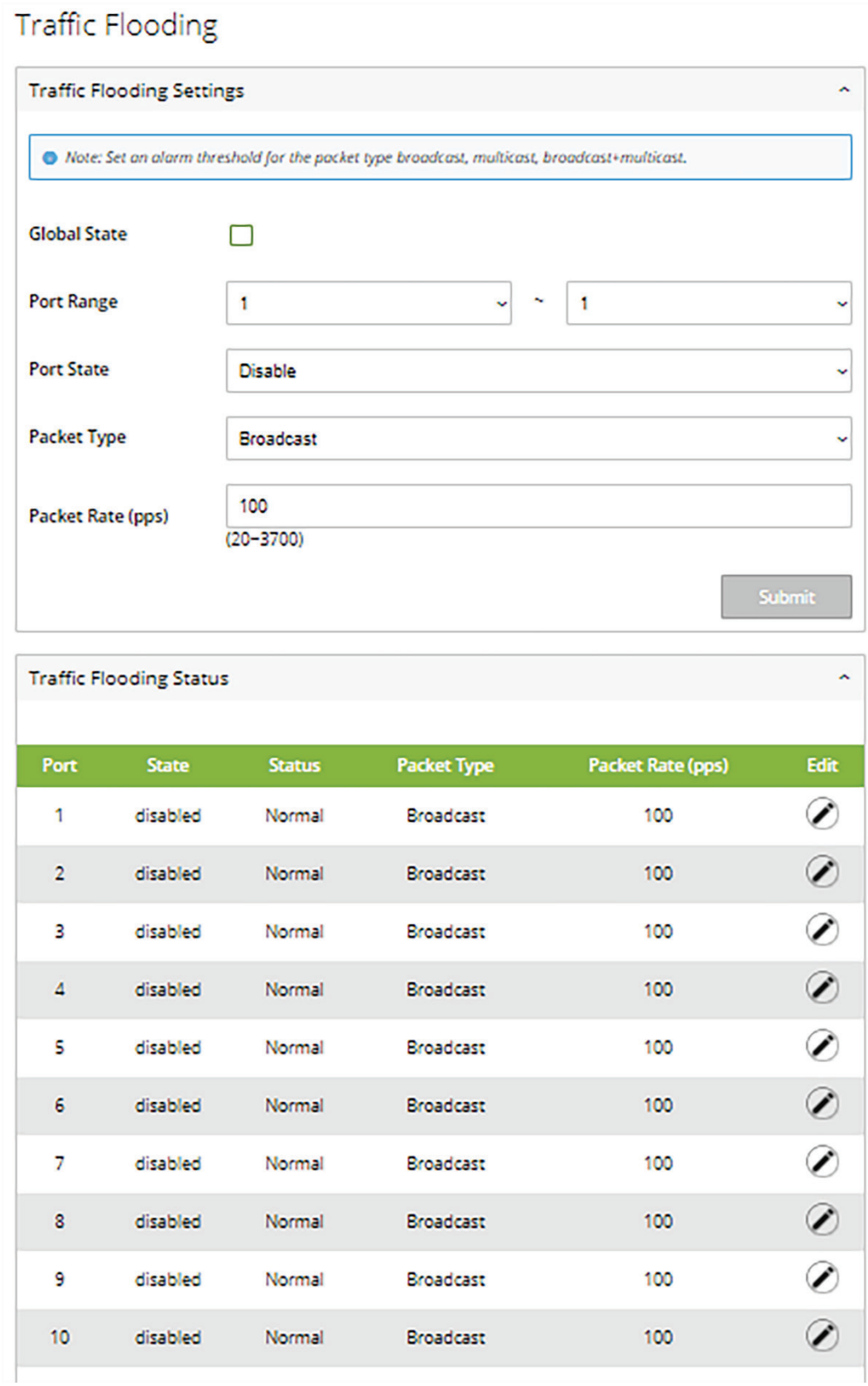


Abbildung 74: Register „Diagnostic“ – Menü „Traffic Flooding“

Tabelle 62: Register „Diagnostic“ – Menü „Traffic Flooding“

Traffic Flooding Settings		
Parameter	**Standardwert**	**Beschreibung**
Global State	☐	☐ Die Funktion „Global State“ ist für den Switch deaktiviert.
		☑ Die Funktion „Global State“ ist für den Switch aktiviert.
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie „Traffic Flooding“ konfigurieren möchten.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie „Traffic Flooding“ konfigurieren möchten.
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, wenn Sie die Funktion „Traffic Flooding“ für den Port oder Port-Bereich deaktivieren möchten.
	Enable	Wählen Sie im Auswahlfeld „Enable“, wenn Sie die Funktion „Traffic Flooding“ für den Port oder Port-Bereich aktivieren möchten.
Packet Type	**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.
Packet Rate (pps) (20-3700)		Geben Sie im Eingabefeld die Paketrate ein, die überwacht werden soll. Gültiger Bereich: 20 … 3700 Mbit/s
Traffic Flooding Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
State	Disable Enable	In dieser Spalte wird der Status des spezifischen Port angezeigt.
Status	Normal	In dieser Spalte wird der Status des Betriebszustandes angezeigt.
Packet Type	Broadcast Multicast Bcast+Mcast	In dieser Spalte wird der Typ des Datenpaketes angezeigt.
Packet Rate (pps)		In dieser Spalte wird die gewählte Paketrate angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.5.1.4 Port-Auslastung (Port Utilization)

Mit dieser Funktion kann ein Benutzer die Datenverkehrsauslastung eines Ports anzeigen und überwachen.

Note

Einstellungen für die Port-Auslastung
Stellen Sie die Port-Auslastung (begrenzt auf einem bestimmten Prozentsatz) über die „Rx packet rate %“ (Rx-Paketrate in Prozent) ein.

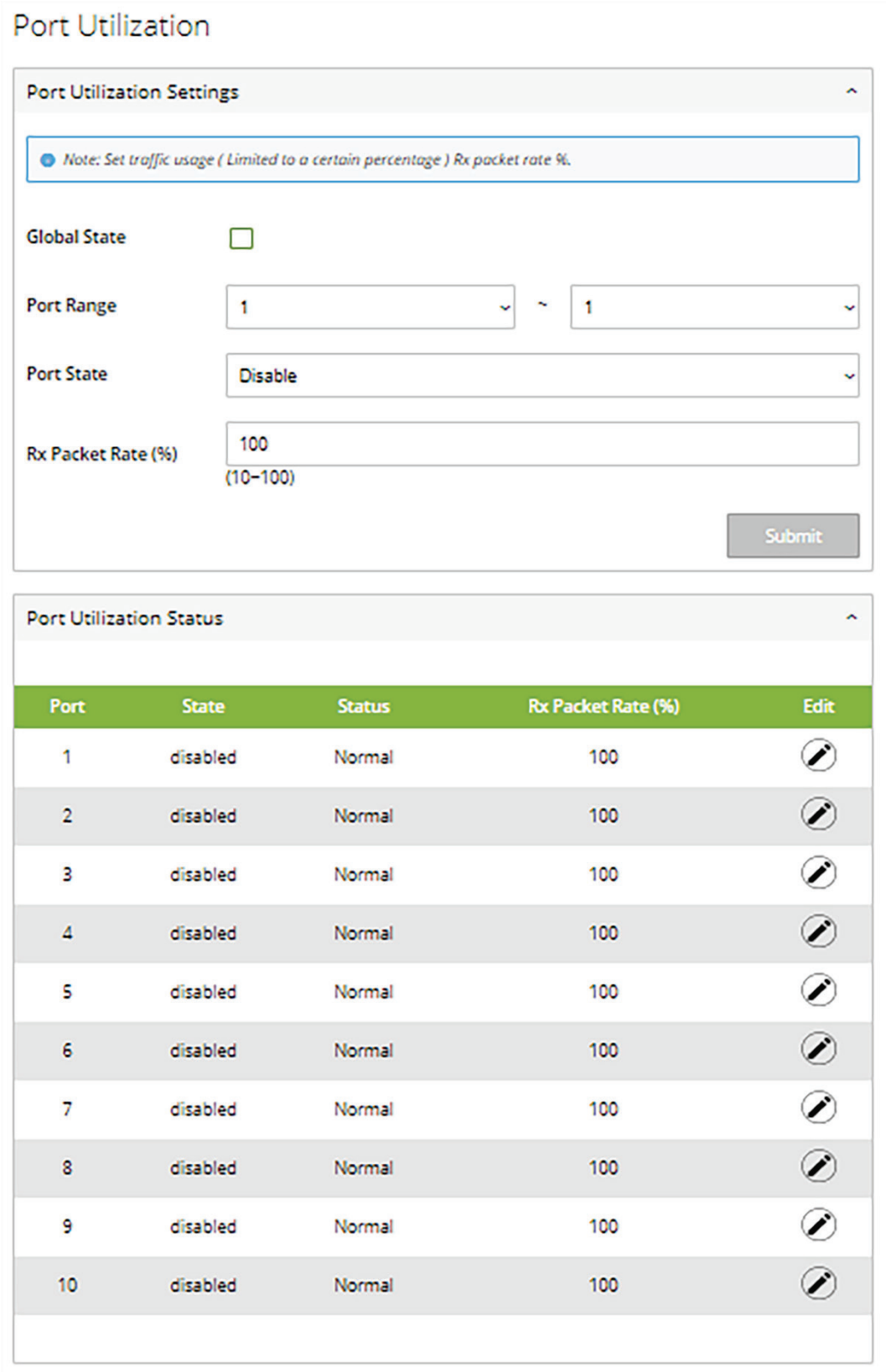


Abbildung 75: Register „Diagnostic“ – Menü „Port Utilization“

Tabelle 63: Register „Diagnostic“ – Menü „Port Utilization“

Port Utilization Settings		
Parameter	**Parameter**	**Parameter**
Global State	☐	☐ Die Funktion „Global State“ ist für den Switch deaktiviert.
		☑ Die Funktion „Global State“ ist für den Switch aktiviert.
Port Range	**1** … 10	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie „Port Utilization“ konfigurieren möchten.
	1 … 10	Wählen Sie im Auswahlfeld einen Port oder Port-Bereich aus, für den Sie „Port Utilization“ konfigurieren möchten.
Port State	**Disable**	Wählen Sie im Auswahlfeld „Disable“, wenn Sie die Funktion „Port Utilization“ für den Port oder Port-Bereich deaktivieren möchten.
	Enable	Wählen Sie im Auswahlfeld „Enable“, wenn Sie die Funktion „Port Utilization“ für den Port oder Port-Bereich deaktivieren möchten.
Rx Packet Rate (%) (10-100)	**100**	Geben Sie im Eingabefeld die Paketrate ein, die überwacht werden soll. Gültiger Bereich: 10 … 100 %.
Port Utilization Status		
Parameter	**Standardwert**	**Beschreibung**
Port	1 … 10	In dieser Spalte werden die Port-Nummern angezeigt.
State	Disable Enable	In dieser Spalte wird der Status des spezifischen Port angezeigt.
Status	Normal	In dieser Spalte wird der Status des Betriebszustandes angezeigt.
Rx Packet Rate (%)		In dieser Spalte wird die gewählte Paketrate angezeigt.
Edit		In dieser Spalte kann die Bearbeitungsfunktion aktiviert werden.

9.5.2 Dashboard Configuration

9.5.2.1 Quick Diagnosis Dashboard

9.5.2.1.1 Registrierung der Nachbargeräte des Switches (Port Registration Learn)

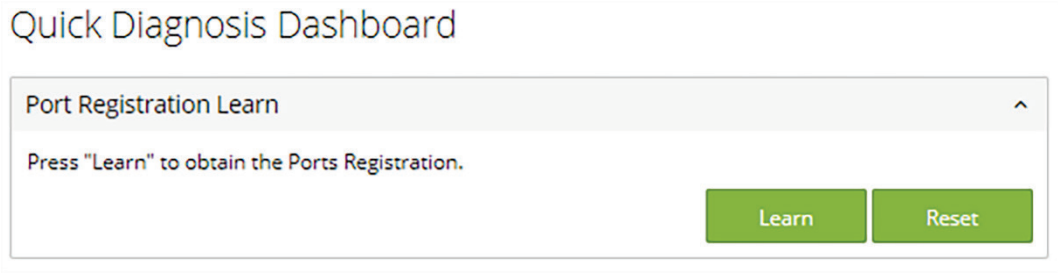


Abbildung 76: Register “Diagnostic” – Menu “Dashboard Configuration” – “Port Registration Learn”

Klicken Sie auf die Schaltfläche **[Learn]** (Erlernen), damit die Nachbargeräte im Switch gespeichert werden.
Wurde die Verbindung der einzelnen Teilnehmer zum Netzwerk korrekt eingerichtet, wird der aktuelle Verbindungszustand im Switch als Referenz gesichert. Abweichungen von diesem Zustand werden zukünftig als Fehler im Dashboard bzw. der Topology-Map angezeigt.

Klicken Sie auf die Schaltfläche **[Reset]**, um die Default-Konfiguration zurückzusetzen (erlernte Port-Anmeldungen werden verlernt).

Hinweis

Anlernen der Nachbargeräte
Aktivieren Sie LLDP bei den Nachbargeräten. Alternativ können Sie die Nachbargeräte über die MAC-Adresse anlernen. (siehe Kapitel „Konfiguration“ …> … „Manuelle Registration (Manual Registration“).

9.5.2.1.2 Port Link Down Statistics

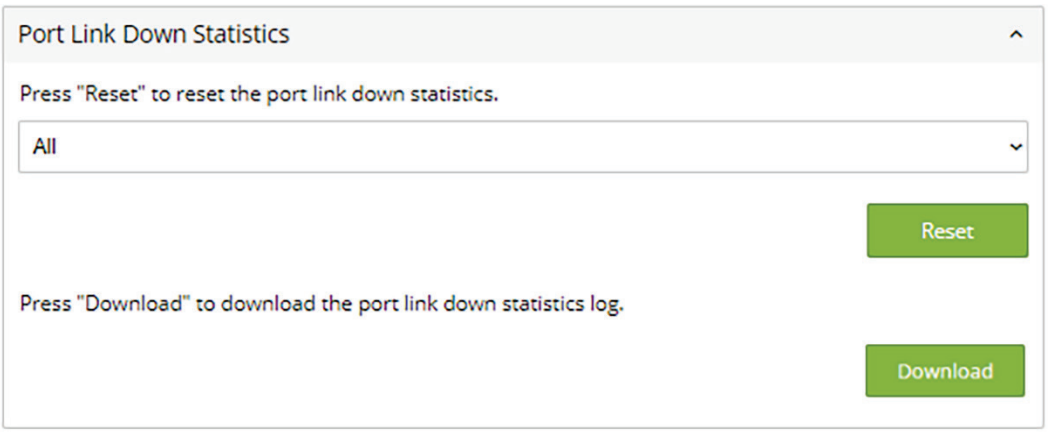


Abbildung 77: Register “Diagnostic” – Menu “Dashboard Configuration” – “Port Link Down Statistics”

In diesem Menü können Statistiken zu einzelnen oder allen Schnittstellen angezeigt, zurückgesetzt oder heruntergeladen werden.

Klicken Sie auf die Schaltfläche **[Reset]**, um die „Port Link Down Statistics“ (Port-Inaktivitätsstatistik) zurückzusetzen. Dadurch löschen sie die Werte aus dem Diagnose-Dashboard.

Klicken Sie auf die Schaltfläche **[Download]**, um die Log-Datei der Port-Inaktivitätsstatistik herunterzuladen.
Sie können diese Statistik entweder für alle oder für einzelne Ports herunterladen.
Mit Hilfe dieser Datei können Wackelkontakte in dem ETHERNET-Netzwerk lokalisiert werden.

9.5.2.1.3 Grenzwerte für kritische Fehler/Alarme (Critical/Alert Threshold)

Hier können Sie die Grenzwerte festlegen, bei denen sich die Farben der Anzeigen für „CPU Usage“ (CPU-Auslastung), „Memory Usage“ (Speicherauslastung), „Transmitting Port Usage“ (Sende-Port-Auslastung) und „Receiving Port Usage“(Empfangs-Port-Auslastung) im Dashboard ändern (siehe Kapitel „Diagnose (Diagnostic)“).

Note

Aufgabe der Grenzwerte

Der Grenzwert für Alarme bestimmt, wann sich eine Anzeige gelb färbt, und der für kritische Fehler, wann sie sich rot färbt. Diese Grenzwerte können einzeln für die Auslastung von CPU, Speicher und Sende-Ports (Tx) und Empfangs-Ports (Rx) konfiguriert werden.

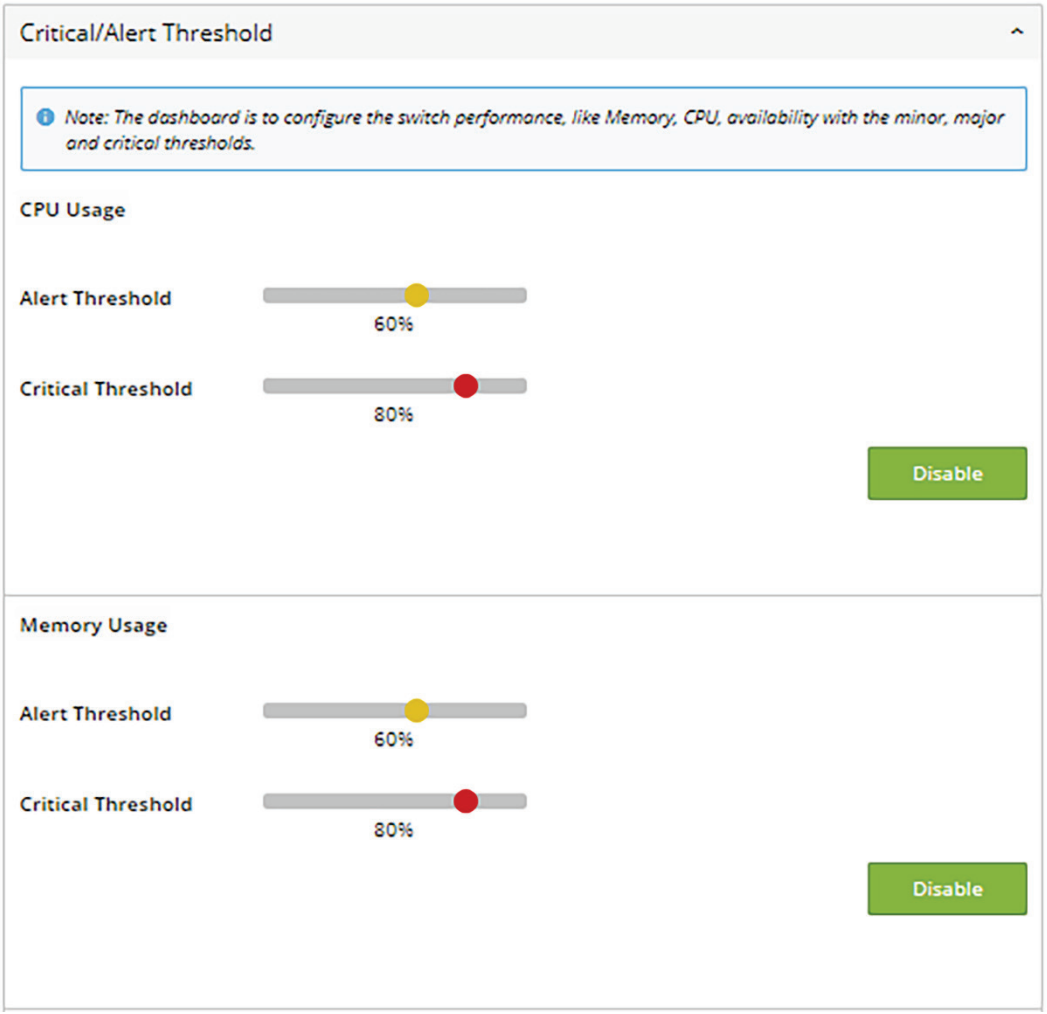


Abbildung 78: Register “Diagnostic” – Menu “Dashboard Configuration” – “Critical/Alert Threshold 01”

Klicken Sie auf die Schaltfläche **[Disable/Enable]**, um folgende Bereiche zu deaktivieren/aktivieren:

- CPU-Auslastung
- Speicherauslastung

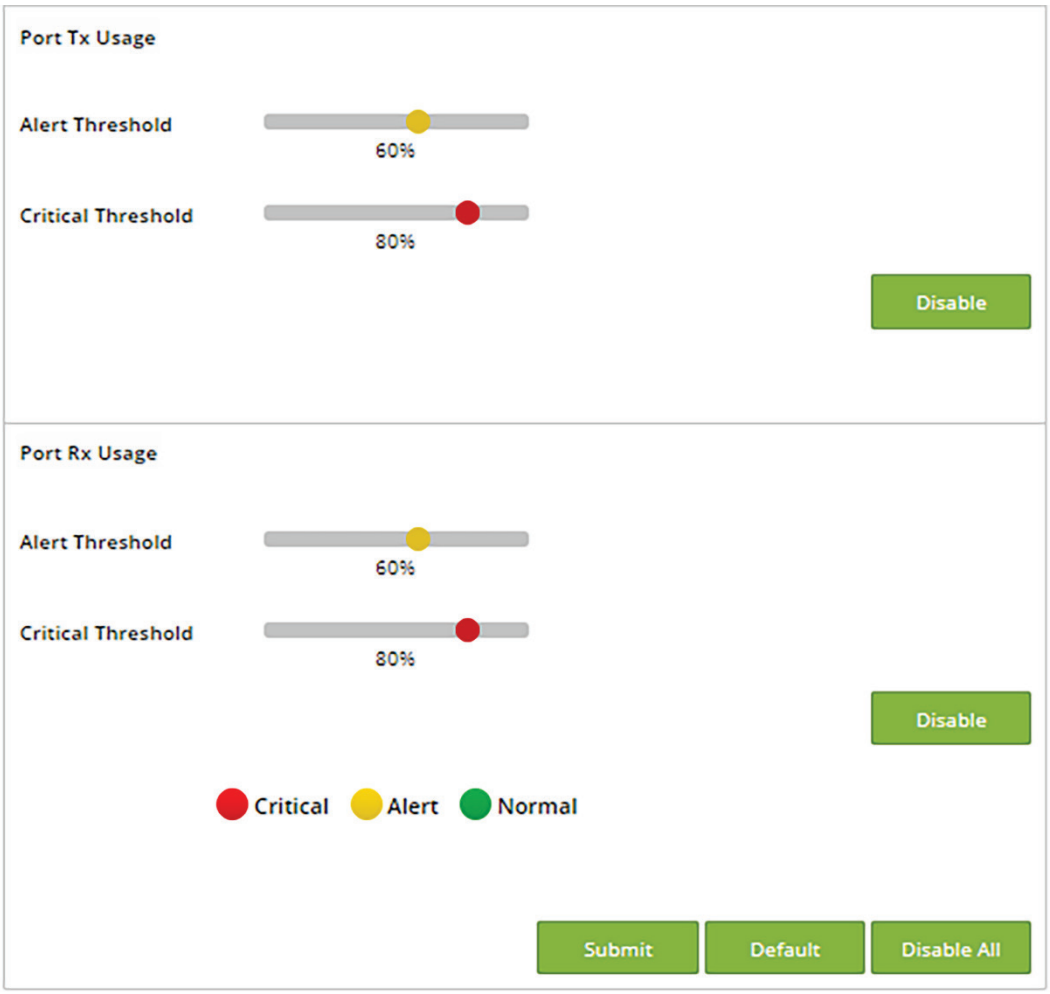


Abbildung 79: Register “Diagnostic” – Menu “Dashboard Configuration” – “Critical/Alert Threshold 02”

Klicken Sie auf die Schaltfläche **[Disable/Enable]**, um folgende Bereiche zu deaktivieren/aktivieren:

- Tx-Port-Auslastung
- Rx-Port-Auslastung

9.5.3 Modbus

9.5.3.1 Datenformat und Funktionscode

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

Tabelle 64: Datenformat und Funktionscode

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

9.5.3.2 Modbus-Register

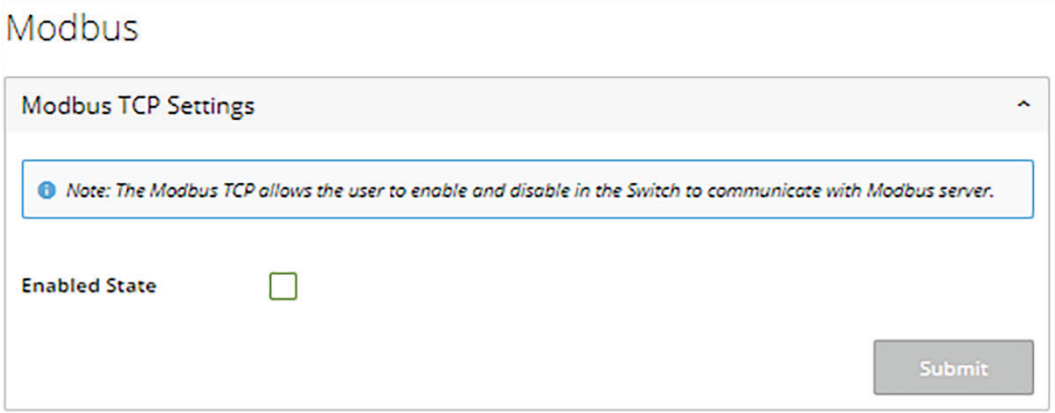


Abbildung 80: Register „Diagnostic“ – Menü „Modbus“

Tabelle 65: Modbus

Modbus TCP Settings			
Parameter	Standardwert	Beschreibung	
Enabled State	☐	☐	Die Funktion „Modbus“ ist für den Switch deaktiviert.
		☑	Die Funktion „Modbus“ ist für den Switch aktiviert.

Hinweis

Modbus-Register
Die Tabelle „Modbus-Register“ finden Sie im Kapitel „Anhang“ > … > „Modbus-Register“.
Die Modbus-Register werden auch im WBM angezeigt.

9.5.4 SNMP

Hinweis

Wechseln zum Konfigurationsmenü

Wenn Sie unter der Registerkarte „Diagnose (Diagnostic)“ auf das Menü „SNMP“ klicken, können Sie im Menü „SNMP“ auf die Registerkarte „Konfiguration (Configuration)“ zugreifen.

Eine ausführliche Beschreibung finden Sie im Kapitel „Konfiguration (Configuration)“ > „SNMP“.

9.5.5 System Log

9.5.5.1 Syslog-Servereinstellung (Syslog Server Setting)

Die Syslog-Funktion kann aktiviert oder deaktiviert werden. Die Default-Einstellung ist „deaktiviert“. Die Protokollnachricht wird im Dateisystem des Switches gespeichert. Wurde die IP-Adresse des Syslog-Servers konfiguriert, wird der Switch eine Kopie an ihn senden.

Hinweis

Größe der Protokollnachrichtendatei
Die Größe der Protokollnachrichtendatei ist auf 4 KB begrenzt. Ist die Datei voll, wird die jeweils älteste Nachricht ersetzt.

Hinweis

Syslog-Funktionsweise
Die Funktion „syslog“ (Systemprotokoll) zeichnet verschiedene Systeminformationen für das „Debugging“ (Fehlersuche) auf. Jeder Protokolleintrag zeichnet eine der folgenden Ebenen auf: Alert/Critical/Error/Warning/Notice/Information (Alarm/Kritischer Fehler/Fehler/Warnung/Hinweis/Information).

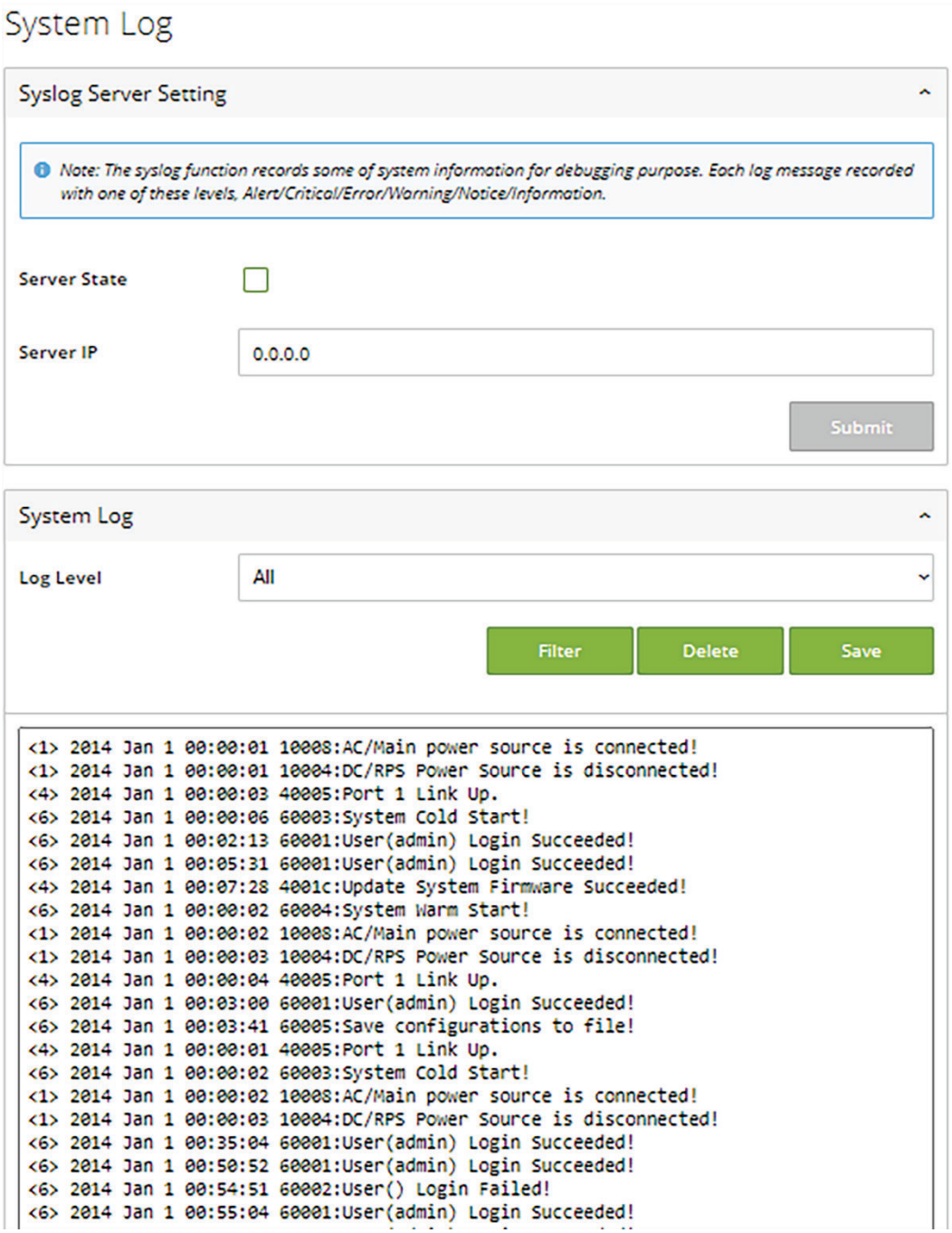


Abbildung 81: Register „Diagnostic“ – Menü „System Log“

Tabelle 66: Register „Diagnostic“ – Menü „System Log“

Syslog Server Settings		
Parameter	**Standardwert**	**Beschreibung**
Global State	☐	☐ Die Funktion „Global State“ ist für den Switch deaktiviert.
		☑ Die Funktion „Global State“ ist für den Switch aktiviert.
Server IP	**0.0.0.0**	Geben Sie im Eingabefeld die IP-Adresse in Dezimalpunktschreibweise ein (z. B.: 192.168.1.1).
System Log		
Parameter	**Standardwert**	**Beschreibung**
Log Level	**All**	Wählen Sie im Auswahlfeld „All“, wenn Sie alle Protokollnachrichten anzeigen wollen.
	1:Alarm	Wählen Sie im Auswahlfeld „Alarm“, wenn Sie die Log-Meldungen anzeigen wollen.
	2:Critical	Wählen Sie im Auswahlfeld „Critical“, wenn Sie die kritischen Protokollnachricht anzeigen wollen.
	3:Error	Wählen Sie im Auswahlfeld „Error“, wenn Sie die Fehler anzeigen wollen.
	4:Warning	Wählen Sie im Auswahlfeld „Warning“, wenn Sie die Warnungen anzeigen wollen.
	5:Notice	Wählen Sie im Auswahlfeld „Notice“, wenn Sie die Bekanntmachungen anzeigen wollen.
	6:Information	Wählen Sie im Auswahlfeld „Information“, wenn Sie alle Informationen anzeigen wollen.

9.6 Wartung (Maintenance)

9.6.1 Neustart (Reboot)

Hinweis

Aufgabe der Wartung
Der Bereich „Maintenance“ (Wartung) bietet Optionen für Neustart, Sichern/Wiederherstellen der Konfiguration, Firmware-Aktualisierung und Zurücksetzen des Switches auf die Werkseinstellungen.

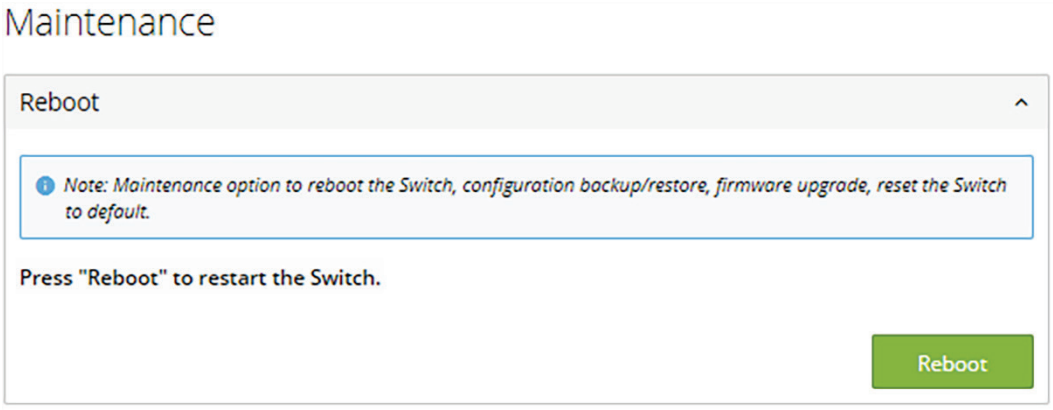


Abbildung 82: Register „Maintenance“ – Menü „Maintenance“ – „Reboot“

Die Funktion „Reboot“ 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 „Reboot“ auf die Schaltfläche **[Reboot]**.
   Daraufhin wird folgendes Fenster angezeigt:

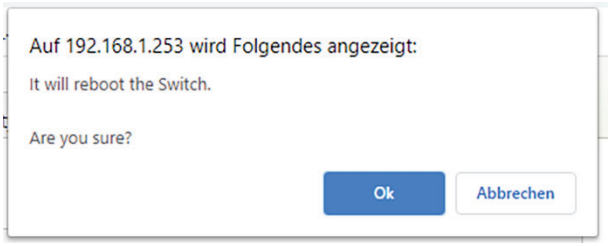


Abbildung 83: Register „Maintenance“ – „Reboot“ Register – Message

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.

9.6.2 Firmware-Aktualisierung (Upgrade Firmware)

Abbildung 84: Register „Maintenance“ – Menü „Maintenance“ – „Upgrade Firmware“

Führen Sie die nachfolgenden Schritte aus, um ein Update der Firmware des Switches durchzuführen.

1. Klicken Sie auf die Schaltfläche **[Choose file]**.
   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 Hochladen der Konfiguration (Upload Configuration)

Abbildung 85: Register „Maintenance“ – Menü „Maintenance“ – „Upload Configuration“

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 **[Choose file]**.
   Wählen Sie die Konfigurationsdatei mit Angabe des vollständigen Pfads aus.

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

Hinweis

Modifikation der Konfigurationsdatei
Durch Modifikationen der Konfigurationsdatei mit einem Texteditor kann eine höhere Anzahl von Switchen schnell konfiguriert werden.

9.6.4 Herunterladen der Konfiguration (Download Configuration)

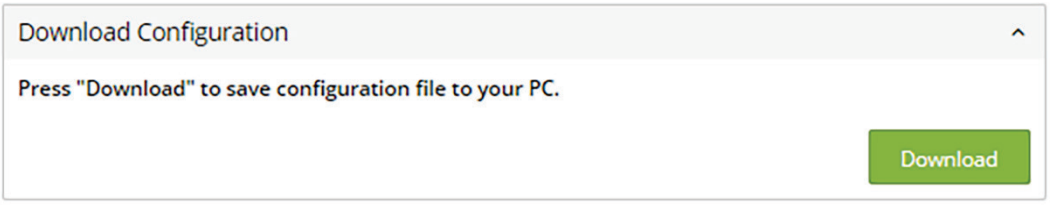


Abbildung 86: Register „Maintenance“ – Menü „Maintenance“ – „Download Configuration“

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

1. Wählen Sie „Press Download to save the configuration file to your PC“.
2. Klicken Sie auf die Schaltfläche **[Download]**, um den Download zu beginnen.

9.6.5 Zurücksetzen der Konfiguration (Reset Configuration)

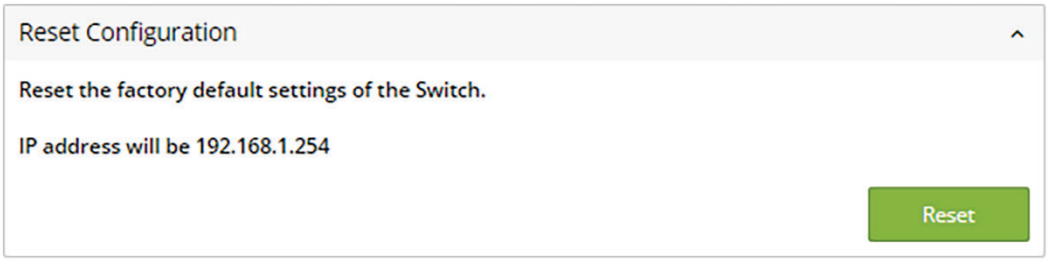


Abbildung 87: Register „Maintenance“ – Menü „Maintenance“ – „Reset Configuration“

Die Funktion „Reset Configuration“ setzt den Switch auf die Werkseinstellungen zurück.

Führen Sie die nachfolgenden Schritte aus, um den Switch zurückzusetzen.

1. Klicken Sie im Menü „Reset Configuration“ auf die Schaltfläche **[Reset]**. Daraufhin wird folgendes Fenster angezeigt:

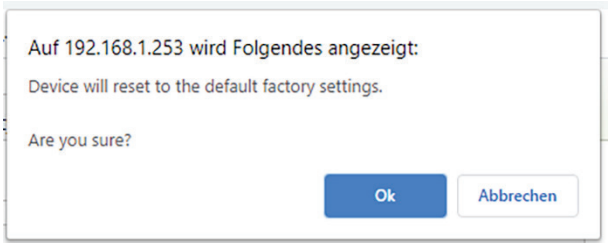


Abbildung 88: Register „Maintenance“ – „Reset“ Register – Message

2. Klicken Sie auf **[OK]** und warten Sie, bis der Switch neu gestartet ist. Dieser Vorgang kann bis zu zwei Minuten dauern. Die Systemkonfiguration wird auf die Default-Werte zurückgesetzt.

10 Anhang

10.1 RJ-45-Kabel

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

Tabelle 67: 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 Lean-Managed-Switch bietet die Funktionen Autocrossing und Autonegotiation am RJ-45-Anschluss.

10.2 Im Command Line Interface (CLI) konfigurieren

Um den Switch über CLI zu konfigurieren wird eine Telnet- oder SSH-Verbindung zum Switch benötigt.

Dieses Kapitel listet eine Auswahl der verfügbaren Befehle der Befehlszeilenschnittstellen auf.

10.2.1 System Status

10.2.1.1 System Information

Tabelle 68: CLI “System Information” Configuration

Node	Command	Description
enable	show hostname	This command displays the system’s network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures the static IP and subnet mask for the system.
interface	show	This command displays the current port configuration.
acl	show	This command displays the current access control list.
vlan	show	This command displays the current VLAN configuration.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system’s CPU utilization and memory information.
enable	show uptime	This command displays the system uptime.

10.2.2 Default Settings

10.2.2.1 System

Tabelle 69: CLI “System” Configuration

Node	Command	Description
enable	ping IPADDR [–c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR [–s SIZE]	This command sends an echo request to the destination host. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
enable	ping IPADDR [–c COUNT –s SIZE]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
enable	ping IPADDR [-s SIZE –c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
configure	Reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system’s network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	This command enter the configuration mode.
configure	interface eth0	This command enter the configuration mode of the interface.
eth0	Show	This command show information about eth0.
eth0	ip address A.B.C.D/M	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
eth0	ip address default-gateway A.B.C.D	This command configures the system’s default gateway.
eth0	ip dhcp client (disable|enable|renew)	This command configures a DHCP client function for the system. “Disable”: Use a static IP address for the switch. “Enable & Renew”: Use the DHCP client to get an IP address from the DHCP server.
eth0	management vlan VLAN_ID	This command configures the management VLAN.

10.2.2.2 Jumbo Frame

Tabelle 70: CLI “Jumbo Frame” Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240|1522|1536|1552|9216)	This command configures the maximum number of bytes for frame sizes.
configure	interface IFNAME	This command starts configuration mode.
interface	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes per frame.
configure	interface range gigabitethernet1/0/PORTLISTS	This command starts configuration mode.
if-range	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes per frame.

10.2.2.3 SNTP

Tabelle 71: CLI “SNTP” Configuration

Node	Command	Description
enable	show time	This command displays the current time and date configuration.
configure	time HOUR:MINUTE:SECOND	This command sets the current time of the switch. hour: 0 … 23 min: 0 … 59 sec: 0 … 59 Note: If you do not configure daylight saving time until after the date and time, the switch uses daylight saving time.
configure	time date YEAR/MONTH/DAY	This command sets the current date of the switch. year: 1970– month: 1 … 12 day: 1 … 31
configure	time daylight-saving-time	This command enables daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving time on the switch.
configure	time daylight-saving-time start-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the start date of daylight saving time.
configure	time daylight-saving-time end-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the end date of daylight saving time.
configure	time ntp-server (disable|enable)	This command disables/enables the NTP server settings.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of the time server.
configure	time ntp-server domain-name STRING	This command sets the domain names of the time server.
configure	time timezone STRING	This command sets the time difference between UTC (formerly GMT) and the time zone. Valid range: −1200 … +1200

Example

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

L2SWITCH(config)*#time timezone +0800*

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

L2SWITCH(config)*#time daylight-saving-time start-date first Monday 6 0*

L2SWITCH(config)*#time daylight-saving-time end-date last Saturday 10 0*

10.2.2.4 Management Host

Tabelle 72: CLI “Management Host” Configuration

Node	Command	Description
enable	show interface eth0	The command displays all eth0 interface configurations.
eth0	Show	The command displays all eth0 interface configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#interface eth0*

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

10.2.2.5 MAC Management

Tabelle 73: CLI “MAC Management” Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current “Age Time” for the MAC address table.
enable	show mac-address-table (static|dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information on a specific MAC address table.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries recognized by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLANID	This command deletes a static unicast entry from the address table.
configure	mac-address-table aging-time VALUE	This command configures the MAC table “Age Time.”
configure	clear mac address-table dynamic	This command deletes the dynamic address entries.

Example

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

10.2.2.6 Port Mirroring

Tabelle 74: CLI “Port Mirroring” Configuration

Node	Command	Description
enable	show mirror	This command displays the current “Port Mirroring” configurations.
configure	mirror (disable|enable)	This command disables/enables “Port Mirroring” on the switch.
configure	mirror destination port PORT_ID	This command specifies the monitor port for the “Port Mirroring.”
configure	mirror source ports PORT_LIST mode (both|ingress|egress)	This command adds a port or port range as the source port(s) for the “Port Mirroring.”
configure	no mirror source ports PORT_LIST	This command removes a port or port range as the source port(s) for the “Port Mirroring.”

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#mirror enable*

L2SWITCH(config)*#mirror destination port 2*

L2SWITCH(config)*#mirror source ports 3-11 mode both*

10.2.2.7 Port Settings

Tabelle 75: CLI “Port Settings” Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command is used to enter the “interface configure node.”
interface	Show	This command displays the current port configurations.
interface	flowcontrol (off | on)	This command disables/enables “Flow Control” for a port.
interface	speed (auto|10-full | 10-full-n | 10-half | 10-half-n | 100-full | 100-full -n | 100-half | 100-half-n | 1000-full | 1000-full-n)	This command configures the speed and duplex mode for a port.
interface	shutdown	This command disables a specific port.
interface	no shutdown	This command enables a specific port.
interface	description STRINGs	This command configures a description for the respective port.
interface	no description	This command is used to configure the standard description of the port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command is used to enter the interface configure node.
if-range	description STRINGs	This command configures a description for the specific port.
if-range	no description	This command is used to configure the standard port description for the individual ports.
if-range	shutdown	This command disables specific ports.
if-range	no shutdown	This command enables specific ports.
if-range	speed (auto|10-full | 10-full-n | 10-half | 10-half-n | 100-full | 100-full -n | 100-half | 100-half-n | 1000-full | 1000-full-n)	This command configures the speed and duplex for the port.

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config-if)#*speed auto*

10.2.3 Advanced Settings

10.2.3.1 Storm Control

Tabelle 76: CLI “Storm Control” Configuration

Node	Command	Description
enable	show storm-control	This command displays the current “Storm Control” configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables bandwidth limitation for broadcast, multicast or DLF packets and sets it for a specified type.
configure	no storm-control type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command disables bandwidth limitation for broadcast, multicast or DLF packets.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*storm-control rate 1 type broadcast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type multicast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type DLF ports 1-6*

10.2.3.2 VLAN

10.2.3.2.1 Port Isolation

Tabelle 77: CLI “Port Isolation” Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current “Port Isolation” configurations. “V” indicates that the port’s packets can be sent to this port. “-” indicates that the port’s packets cannot be sent to this port.
interface	port-isolation ports PORTLISTS	This command configures a port or port range to forward data packets from a specific port.
interface	no port-isolation	This command configures all ports to forward data packets from a specific port.

Example

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

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

10.2.3.2.2 VLAN Settings

Tabelle 78: CLI “VLAN Settings” Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1–4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1–4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name to the specific VLAN. The VLAN name should be a combination of numbers, letters, hyphens (-) and underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command resets the VLAN name to the default setting. Note: The default VLAN name comprises the following: : “VLAN”+VLAN_ID, VLAN1, VLAN2, …
vlan	fixed PORT_LIST	This command assigns ports to a VLAN group as fixed subscribers.
vlan	no fixed	This command deletes all fixed ports from a VLAN.
vlan	tagged PORT_LIST	This command assigns fixed ports to a VLAN group as tagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no tagged	This command deletes all tagged fixed ports from a VLAN.
vlan	untagged PORT_LIST	This command assigns fixed ports to a VLAN group as untagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no untagged	This command deletes all untagged ports from a VLAN.
vlan	acceptable frame type (all | tagged | untagged)	This command configures the permissible frame type.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*vlan 2*

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

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

10.2.3.3 LLDP

Tabelle 79: CLI “LLDP” Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all information of port neighbors.
configure	lldp (disable | enable)	This command globally enables/disables the LLDP function on the switch.
configure	lldp tx-hold <2-100>	This command configures the “tx-Hold Time” that determines the TTL of the switch message (TTL = tx-hold * tx-interval).
interface	lldp tx-interval <1-3600>	This command configures the interval to transmit the LLDP packets.

10.2.3.4 Loop Detection

Tabelle 80: CLI “Loop Detection” Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current configuration for “Loop Detection.”
configure	loop-detection (disable | enable)	This command disables/enables “Loop Detection” on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC address for special “Loop Detection” packets.
configure	no loop-detection address	This command resets the destination MAC address to the default setting (00:0b:04:AA:AA:AB).
interface	loop-detection (disable | enable)	This command disables/enables “Loop Detection” for a specific port.
interface	no shutdown	This command enables a specific port. The command can enable a port blocked by “Loop Detection.”
interface	loop-detection recovery (disable | enable)	This command enables/disables the “Recovery” function on a port.
interface	loop-detection recovery time VALUE	This command configures the “Recovery Time” period.

Example

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*

10.2.3.5 STP

Tabelle 81: CLI “STP” Configuration

Node	Command	Description
enable	show spanning-tree active	This command only displays STP information for active ports.
enable	show spanning-tree blockedports	This command only displays STP information for blocked ports.
enable	show spanning-tree port detail PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree summary	This command displays a summary of port states and configurations.
enable	clear spanning-tree counters	This command clears the STP statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears the STP statistics for a specific port.
configure	spanning-tree (disable | enable)	This command disables/enables the STP function in the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (“Forward Delay,” “Max Age” and “Hello Time”).
configure	no spanning-tree algorithm-timer	This command configures the default values for “Forward Delay,” “Max Age” and “Hello Time.”
configure	spanning-tree forward-time <4–30>	This command configures the “Forward Delay” period (in seconds) for the bridge.
configure	no spanning-tree forward-time	This command configures the default values for “Forward Delay.”
configure	spanning-tree hello-time <1–10>	This command configures the “Hello Time” period (in seconds) for the bridge.
configure	no spanning-tree hello-time	This command configures the default values for the “Hello Time.”
configure	spanning-tree max-age <6-40>	This command configures the “Max Age” period (in seconds) for bridge messages.
configure	no spanning-tree max-age	This command configures the default values for the “Max Age.”
configure	spanning-tree mode (rstp | stp)	This command configures the STP mode.
configure	spanning-tree pathcost method (short | long)	This command configures the path cost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree bpdufilter (disable | enable)	This command configures enables/disables the “BPDU Filter” function.
interface	spanning-tree bpduguard (disable | enable)	This command configures enables/disables the “BPDU Guard” function.
interface	spanning-tree edge-port (disable | enable)	This command enables/disables the “Edge Port” setting.

Tabelle 81: CLI “STP” Configuration

Node	Command	Description
interface	spanning-tree cost VALUE	This command configures the costs for the specific port. Cost range: 16-bit-based value range from 1 to 65,535, 32-bit-based value range from 1 to 200,000,000.
interface	no spanning-tree cost	This command sets the path cost of the specific port to the default value.
interface	spanning-tree port-priority <0-240>	This command configures the priority for the specific port (default value: 128).
interface	no spanning-tree port-priority	This command sets the priority of the specific port to the default value.

10.2.4 Security

10.2.4.1 Access Control List

Tabelle 82: CLI “Access Control List” Configuration

Node	Command	Description
enable	show access-list	This command displays all access control profiles.
configure	access-list STRING	This command creates a new access control profile, where “STRING” is the profile name.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable | drop | permit)	This command processes the profile. “disable”: The profile is disabled. “drop”: If packets match the profile, they are dropped. “permit”: If packets match the profile, they are forwarded.
acl	destination mac host MACADDR	This command configures the destination MAC address and the mask for the profile.
acl	destination mac MACADDR	This command configures the destination MAC address and the mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC address and the mask for the profile. The second “MACADDR” parameter is the mask (e.g., ffff.ffff.0000) for the profile.
acl	no destination mac	This command deletes the destination MAC address from the profile.
acl	ethertype STRING	This command configures the ETHERNET type for the profile, where the “STRING” is a hexadecimal value, e.g., 08AA.
acl	no ethertype	This command deletes the ETHERNET type limit from the profile.
acl	source mac host MACADDR	This command configures the source MAC address and the mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source MAC address and the mask for the profile.
acl	no source mac	This command deletes the source MAC and the mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and the mask for the profile.
acl	no source ip	This command deletes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and the mask for the profile.
acl	no destination ip	This command deletes the destination IP address from the profile.

10.2.5 Monitor

10.2.5.1 Alarm

Tabelle 83: CLI “Alarm” Configuration

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

10.2.5.2 Monitor Information

Tabelle 84: CLI “Monitor Information” Configuration

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

10.2.5.3 SFP Information

Tabelle 85: CLI “SFP Information” Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

10.2.6 Management

10.2.6.1 SNMP

Tabelle 86: CLI “SNMP” Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro | rw) trusted-host IPADDR	This command configures the “SNMP Community” name.
configure	snmp (disable | enable)	This command disables/enables SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command assigns a name to the system.
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command sets up the trap receiver’s configurations, including the IP address, version (v1 or v2c) and “Community.”

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*snmp enable*

L2SWITCH(config)#*snmp community public rw trusted-host 192.168.200.106/24*

L2SWITCH(config)#*snmp trap-receiver 192.168.200.106 v2c public*

L2SWITCH(config)#*snmp system-contact IT engineer*

L2SWITCH(config)#*snmp system-location Wago*

10.2.6.2 Maintenance

Tabelle 87: CLI “Maintenance” Configuration

Node	Command	Description
configure	reboot	This command reboots the system.
configure	reload default-config	This command resets the system configuration to the default settings. Note: The system automatically reboots to apply the configurations.
configure	write memory	This command writes the current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads an updated configuration file from the TFTP server, where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to the TFTP server.
configure	archive download-fw <URL PATH>	This command downloads an updated firmware file from the TFTP server, where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

10.2.6.3 System Log

Tabelle 88: CLI “System Log” Configuration

Node	Command	Description
enable	show syslog	The command displays all log messages recorded in the switch.
enable	show syslog level <1-6>	This command displays the log messages with the “LEVEL” recorded in the switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	syslog (disable | enable)	The command disables/enables the syslog function.
configure	clear syslog	The command clears the syslog message.

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config)#*syslog-server enable*

10.2.6.4 User Account

Tabelle 89: CLI “System Log” Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal | admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	The command deletes an existing user account.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*add user q admin*

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

10.3 Modbus/TCP-Tabellen

10.3.1 Datenformat und Funktionscode

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

Tabelle 90: Datenformat und Funktionscode

Datenzugriffstyp		Funktions-code	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 Modbus-Register

Der Modbus-Adressraum der Lean-Managed-Switches beginnt bei 1001 (dezimal) für den Funktionsblock 4.

Hinweis

Modbus-Adressraum

Der Modbus-Adressraum wird auch im Web-Based-Management angezeigt.

Tabelle 91: Modbus-Register

Read-Input-Register (Funktionscode 04) Registernummer 30001~39999						
Register Offset		Register Offset		Register Offset Dec	Register Offset Dec	Register Offset Dec
Dec	Dec	Dec	Dec			
System Information						
1001	3E9	1000	3E8	1	HEX	Vendor ID = 0x30DE
1002	3EA	1001	3E9	16	ASCII	Vendor Name = “WAGO” Word 0 Hi byte = ‘W’ Word 0 Lo byte = ‘A’ Word 1 Hi byte = ‘G’ Word 1 Lo byte = ‘O’ Word 2 Hi byte = ‘\0’

1033	409	1032	408	16	ASCII	**Product Name = “852-1813”**
						Word 0 Hi byte = ‘8’ Word 0 Lo byte = ‘5’ Word 1 Hi byte = ‘2’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘8’ Word 3 Hi byte = ‘1’ Word 3 Lo byte = ‘3’ Word 4 Hi byte = ‘\0’ Word 4 Lo byte = ‘\0
1065	429	1064	428	7	ASCII	**Product Serial Number**
						Ex: Serial No=A000000000001
1081	439	1080	438	12	ASCII	**Firmware Version=” V1.0.1.S0”**
						Word 0 Hi byte = ‘V’ Word 0 Lo byte = ‘1’ Word 1 Hi byte = ‘.’ Word 1 Lo byte = ‘0’ Word 2 Hi byte = ‘.’ Word 2 Lo byte = ‘1’ Word 3 Hi byte = ‘.’ Word 3 Lo byte = ‘S’ Word 4 Hi byte = ‘0’ Word 4 Lo byte = ‘\0’ Word 5 Hi byte = ‘\0’ Word 5 Lo byte = ‘\0’ Word 6 Hi byte = ‘\0’ Word 6 Lo byte = ‘\0’ Word 7 Hi byte = ‘\0’ Word 7 Lo byte = ‘\0’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0’
1097	449	1096	448	16	ASCII	Firmware Release Date="Mon Sep 30 18:51:45 2013"
1113	459	1112	458	3	HEX	**ETHERNET MAC Address**
						Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05

1129	469	1128	468	1	HEX	**Power 1 (PWR) Alarm, DIP switch 1 need ON**
						0x0000: no alarm 0x0003: No PWR input
1130	46A	1129	469	1	HEX	**Power 2(RPS) Alarm, DIP switch 1 need ON**
						0x0000: no alarm 0x0003: No RPS input
1145	479	1144	478	1	HEX	**Fault LED Status**
						0x0000: No 0x0001: Yes
Port Information						
				1	HEX	**1256 (Port 1) ... 1265 (Port 10) Port 1 to 10 Link Status**
1257	4E9	1256	4E8			0x0000: Link down
1258	4EA	1257	4E9			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1259	4EB	1258	4EA			0x0002: 10M-Full-FC_OFF
1260	4EC	1259	4EB			0x0003: 10M-Half-FC_ON
1261	4ED	1260	4EC			0x0004: 10M-Half-FC_OFF
1262	4EE	1261	4ED			0x0005: 100M-Full-FC_ON
1263	4EF	1262	4EE			0x0006: 100M-Full-FC_OFF
1264	4F0	1263	4EF			0x0007: 100M-Half-FC_ON
1265	4F1	1264	4F0			0x0008: 100M-Half-FC_OFF
1266	4F2	1265	4F1			0x0009: 1000M-Full-FC_ON
						0x000A: 1000M-Full-FC_OFF 0x000B: 1000M-Half-FC_ON 0x000C: 1000M-Half-FC_OFF 0xFFFF: No port
				32	ASCII	**Port 1 to 10 Medium**
1513	5E9	1512	5E8			Port Description = “100TX, RJ45.” Or “1000TX, SFP.”
1545	609	1544	608			Word 0 Hi byte = ‘1’
1577	629	1576	628			Word 0 Lo byte = ‘0’
1609	649	1608	648			Word 1 Hi byte = ‘0’
1641	669	1640	668			Word 1 Lo byte = ‘T’
1673	689	1672	688			…
1705	6A9	1704	6A8			Word 4 Hi byte = ‘4’
1737	6C9	1736	6C8			Word 4 Lo byte = ‘5’
1769	6E9	1768	6E8			Word 5 Hi byte = ‘.’
1801	709	1800	708			Word 5 Lo byte = ‘\0’

				2	HEX	**2024 (Port 1) ... 2042 (Port 10)** **Port 1 to 10 Tx Packets**
2025	7E9	2024	7E8			Ex: port 1 Tx Packet Amount = 0x87654321 Word 0 = 8765 Word 1 = 4321
2027	7EB	2026	7EA			
2029	7ED	2028	7EB			
2031	7EF	2030	7EE			
2033	7F1	2032	7F0			
2035	7F3	2034	7F2			
2037	7F5	2036	7F4			
2039	7F7	2038	7F6			
2041	7F9	2040	7F8			
2043	7FB	2042	7FA			
				2	HEX	**2088 (Port 1) ... 2106 (Port 10)** **Port 1 to 10 Rx Packets**
2089	829	2088	828			Ex: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2091	82B	2090	82A			
2093	82D	2092	82C			
2095	82F	2094	82E			
2097	831	2096	830			
2099	833	2098	832			
2101	835	2100	834			
2103	837	2102	836			
2105	839	2104	838			
2107	83B	2106	83A			
				2	HEX	**2152 (Port 1) ... 2170 (Port 10)** **Port 1 to 10 Tx Error Packets**
2153	869	2152	868			Ex: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
2155	86B	2154	86A			
2157	86D	2156	86C			
2159	86F	2158	86E			
2161	871	2160	870			
2163	873	2162	872			
2165	875	2164	874			
2167	877	2166	876			
2169	879	2168	878			
2171	87B	2170	87A			

				2	HEX	**2216 (Port 1) ... 2234 (Port 10)** **Port 1 to 10 Rx Error Packets**
2217	8A9	2216	8A8			Ex: port 1 Rx Error Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2219	8AB	2218	8AA			
2221	8AD	2220	8AC			
2223	8AF	2222	8AE			
2225	8B1	2224	8B0			
2227	8B3	2226	8B2			
2229	8B5	2228	8B4			
2231	8B7	2230	8B6			
2233	8B9	2232	8B8			
2235	8BB	2234	8BA			
Redundancy & Ring Information						
2281	8E9	2280	8E8	1	HEX	**STP Status** 0x0000 : STP is disabled 0x0001 : STP 0x0002 : RSTP
2285	8ED	2284	8EC	1	HEX	**ERPS Status** 0x0000 : Disabled 0x0001 : Enabled
ERPS Information						
3049	BE9	3048	BE8	1	HEX	**Ring ID for ERPSn (n=1)** Ex: 0x001 Ring ID=1
3050	BEB	3049	BE9	1	HEX	**State for ring of ERPS** 0x0000: Disabled. 0x0001: Enabled.
3051	C0B	3050	BEA	33	ASCII	**Name of Ring** Ring Name = “Ring1” Word 1 Lo byte = ‘R’ Word 2 Lo byte = ‘i’ Word 3 Lo byte = ‘n’ Word 4 Lo byte = ‘g’ Word 5 Lo byte = ‘1’ Word 6 Lo byte = ‘\0’
3084	C0C	3083	C0B	1	HEX	**Version & Ring Type** High byte – Version. Low byte – Ring Type. 0x01:Major-ring 0x02:Sub-ring Ex: 0x0201– Version2, Type: Major-ring
3085	C0D	3084	C0C	1	HEX	**Instance of Ring** Ex: 0x0001 Instance ID=1
3086	C0E	3085	C0D	1	HEX	**Control VLAN of Ring** E:0x000b Control VLAN=11

3087	C0F	3086	C0E	1	HEX	**Right Port of Ring**
						High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0502– Port 5, RPL Owner
3088	C10	3087	C0F	1	HEX	**Left Port of Ring**
						High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0303– Port 3, RPL Neighbour
3089	C11	3088	C10	1	HEX	**Ring port state**
						High byte –Left port state. Low byte – Right port state. 0x00: No connection 0x01: Forwarding 0x02: Blocking Ex: 0x0001– Left Port No connection Right Port Forwarding
3090	C12	3089	C11	1	HEX	**Ring ID for ERPSn (n=2)**
3091	C13	3090	C12	1		State of ERPS Ring
3124	C34	3091	C13	33	ASCII	Name of Ring
3125	C35	3124	C34	1	HEX	Version & Ring Type
3126	C36	3125	C35	1		Instance of Ring
3127	C37	3126	C36	1		Control VLAN of Ring
3128	C38	3127	C37	1		Right Port of Ring
3129	C39	3128	C38	1		Left Port of Ring
3130	C3A	3129	C39	1		Ring port state

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