WAGO Lean-Managed-Switches

Funktionshandbuch

852-181x
852-181x/xxx-xxx
852-1832



© 2026 WAGO GmbH & Co. KG
Alle Rechte vorbehalten.

WAGO GmbH & Co. KG
Hansastraße 27 D-32423 Minden

Tel: +49 (0) 571/887 – 0

Fax: +49 (0) 571/887 – 844 169

E-Mail: ✉ **info@wago.com**

Web: 🌐 **http:/www.wago.com**

Technischer Support

Tel: +49 (0) 571/887 – 44555

Fax: +49 (0) 571/887 – 844555

E-Mail: ✉ **support@wago.com**

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

E-Mail: ✉ **documentation@wago.com**

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

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.

Inhaltsverzeichnis

Inhaltsverzeichnis ... 3

1 Bestimmungen ... 6

1.1 Gültigkeitsbereich ... 6
1.1.1 Mitgeltende Dokumente ... 7
1.1.2 Information ... 7

2 Überblick ... 8

3 Funktionen ... 9

3.1 Netzwerkdiagnose mit dem Browser ... 9
3.1.1 Diagnose mit dem Dashboard ... 9
3.1.2 Darstellung des Gerätestandorts und eines Ansprechpartners ... 10
3.1.3 Topologie-Map zur Erkennung der Nachbargeräte ... 10
3.2 Konfigurationsfunktionen ... 10
3.3 Tab-Information im WBM ... 12
3.3.1 Device-Status ... 12
3.3.2 Legal Information ... 12
3.3.3 Port Counter ... 12
3.3.4 Running Configuration ... 13
3.3.5 Utilization-Information ... 13
3.4 Tab-Configuration im WBM ... 13
3.4.1 Device-Discovery ... 13
3.4.1.1 LLDP ... 13
3.4.1.2 Manual-Registration ... 15
3.4.2 Fieldbus-Priority ... 15
3.4.3 Interface ... 17
3.4.3.1 Loop-Detection ... 17
3.4.3.2 Mirror ... 18
3.4.3.3 Port-Set-up ... 19
3.4.3.4 Port-Priority ... 21
3.4.4 PoE-Settings ... 22
3.4.4.1 PD-Alive-Check ... 22
3.4.4.2 Power ON/OFF ... 24
3.4.5 SNMP ... 25
3.4.5.1 SNMP Set-up ... 26
3.4.5.2 SNMP v1/2c ... 27
3.4.5.3 SMNP Trap ... 28
3.4.5.4 SMNP Event Settings ... 29
3.4.5.5 SMNPv3-View ... 30
3.4.5.6 SMNPv3-Group ... 31
3.4.5.7 SMNPv3-User ... 32
3.4.6 Systemmanagement ... 34
3.4.6.1 General Set-up ... 34
3.4.6.2 SNTP ... 35
3.4.6.3 User Account ... 37
3.4.6.1 Reset-Button ... 38
3.4.7 Storm Control ... 39
3.4.8 Wizard ... 40
3.5 Tab Security im WBM ... 40

3.5.1 802.1X ... 40
3.5.1.1 Global Set-up ... 41
3.5.1.2 Port-Set-up ... 42
3.5.1.3 Port-Status ... 43
3.5.2 ACL ... 44
3.5.3 Port-Security ... 46
3.5.4 Port-Security Advanced ... 47
3.5.5 Sticky MAC Whitelisting ... 49
3.5.6 Service-Control ... 51
3.5.7 VLAN ... 53
3.5.7.1 Port-Isolation ... 53
3.5.7.2 VLAN-Set-up ... 53
3.6 Tab-Redundancy im WBM ... 55
3.6.1 ERPS ... 55
3.6.2 STP/RSTP ... 58
3.6.2.1 STP/RSTP Einstellungen ... 59
3.6.2.2 STP/RSTP-Port-Einstellungen ... 60
3.7 Tab-Diagnostic im WBM ... 62
3.7.1 Alarm ... 62
3.7.1.1 Information ... 62
3.7.1.2 ALM-Output ... 62
3.7.1.3 DIP-Status ... 63
3.7.1.4 Traffic-Flooding ... 64
3.7.1.5 Port-Auslastung (Port Utilization) ... 65
3.7.2 Dashboard-Configuration ... 65
3.7.3 Modbus TCP ... 67
3.7.4 SNMP ... 68
3.7.5 Syslog ... 68
3.7.6 SSL-Certificate ... 69
3.8 Tab Maintenance im WBM ... 71
3.8.1 Maintenance ... 71
3.9 Erweiterte Konfiguration per CLI ... 72
4 In Betrieb nehmen ... 73
4.1 Einschalten des Switches ... 73
4.2 Werksseitige Zugangsdaten ... 73
4.3 Konfigurieren einer IP-Adresse ... 73
4.3.1 Konfigurieren einer IP-Adresse über das CLI ... 73
4.3.2 Konfigurieren des Switches als DHCP-Client über das CLI ... 74
4.3.3 Konfigurieren einer IP-Adresse über das WBM ... 74
4.4 Testen der Netzwerkverbindung ... 74
4.5 Passwörter ändern ... 75
4.5.1 Passwortänderung per Konfigurationsdatei ... 76
4.6 Ausschalten/Neustart ... 76
5 Konfigurieren ... 77
5.1 Konfigurieren im WBM ... 77
5.1.1 Aufbau des WBM ... 77
5.1.2 Arbeiten im WBM ... 79
5.2 Konfigurieren mit dem CLI ... 80
5.2.1 Verbindungsaufbau zum CLI ... 80
5.2.2 Konfigurationsebenen im CLI ... 80
5.2.3 Beispiel zur Navigation durch die CLI-Hierarchieebenen und Nutzung des CLI ... 81

5.2.4 Verwendung der Hilfsfunktionen im CLI ... 82
5.3 Konfigurieren mit Netzwerkmanagement-Software ... 84
6 Service ... 85
6.1 Firmwareänderungen ... 85
6.1.1 Firmware-Update mit dem WBM durchführen ... 85
6.1.2 Firmware-Update per CLI durchführen ... 86
6.2 Zurücksetzen auf Werkseinstellungen ... 86
7 Tabellenverzeichnis ... 88
8 Abbildungsverzeichnis ... 90

1 Bestimmungen

1.1 Gültigkeitsbereich

Das vorliegende Dokument gilt für folgende Produkte:

852-1812

Lean-Managed-Switch; 8 Ports, 1000BASE-T

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1812

852-1812/010-000

Lean-Managed-Switch; 8 Ports, 1000BASE-T

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1812/010-000

852-1813

Lean-Managed-Switch; 8 Ports, 1000BASE-T; 2 Slots 1000BASE-SX/LX

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1813

852-1813/010-000

Lean-Managed-Switch; 8 Ports, 1000BASE-T; 2 Slots 1000BASE-SX/LX

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1813/010-000

852-1813/000-001

Lean-Managed-Switch; 8 Ports, 1000BASE-T; 2 Slots 1000BASE-SX/LX; 8 × Power over Ethernet

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1813/000-001

852-1813/010-001

Lean-Managed-Switch; 8 Ports, 1000BASE-T; 2 Slots 1000BASE-SX/LX; 8 × Power over Ethernet

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1813/010-001

852-1816

Lean-Managed-Switch; 16 Ports, 1000BASE-T

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1816

852-1816/010-000

Lean-Managed-Switch; 16 Ports, 1000BASE-T; lichtgrau

Firmwareversion	1.3.0 (S0)
Produktdetailseite	http://www.wago.com/852-1816/010-000

852-1832

Lean-Managed-Switch; 8 Ports, 1000BASE-T; IP67

Firmwareversion	1.0.0 (S0)
Produktdetailseite	http://www.wago.com/852-1832

Die vollständige Gebrauchsanleitung für die Produkte besteht aus mehreren, mitgeltenden Dokumenten. Die Produkte dürfen nur gemäß Anweisungen der vollständigen Gebrauchsanleitung installiert und betrieben werden. Kenntnis aller mitgeltenden Dokumente ist Voraussetzung für die bestimmungsgemäße Verwendung. Alle Dokumente und Informationen finden Sie auf den Produktdetailseiten.

1.1.1 Mitgeltende Dokumente

Produkthandbuch des verwendeten Produktes.

Alle Dokumente und Informationen finden Sie unter:

www.wago.com/....

1.1.2 Information

Das vorliegende Dokument beschreibt den vollständigen Umfang von Funktionen. Nicht alle beschriebenen Funktionen werden von jedem Produkt unterstützt.

2 Überblick

Die Lean-Managed-Switches sind konfigurierbare ETHERNET-Switches mit unterschiedlicher Anzahl von ETHERNET-Ports mit Übertragungsraten von bis zu einem Gigabit. Einige Modelle unterstützen zusätzlich „Power over Ethernet“ (PoE+) mit bis zu 30 W und verfügen über 2 SFP-Ports (SFP-Module sind optional erhältlich).

Die Switches besitzen ein robustes Gehäuse, eine redundante Spannungsversorgung und eine Funktionsüberwachung, teilweise mit konfigurierbarem Alarmrelais. Die Switches bieten 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.

Folgende Funktionen steigern die Robustheit, Verfügbarkeit und Sicherheit im Netzwerk:

Sicherheit:

Netzwerksegmentierung gemäß IEEE802.1Q (max. 5 VLAN), 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 Netzwerke und Ringtopologien, „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, Alarm-Thresholds, Port-Statistic, Back-up and Restore, System-Log, Syslog-Server, Command-Line-Interface mit SSH/Telnet, Topology-Map und Diagnose-Dashboard.

3 Funktionen

HINWEIS

Die in den nachfolgenden Abschnitten beschriebenen Funktionen sind nicht in allen Produkten enthalten, für die dieses Handbuch gültig ist. Abweichungen ergeben sich insbesondere aus den unterschiedlichen Hardware-Fähigkeiten.

3.1 Netzwerkdiagnose mit dem Browser

3.1.1 Diagnose mit dem Dashboard

Die Diagnosefunktion dient der schnellen Identifikation, Analyse und Lokalisierung von Netzwerkproblemen. Sie unterstützt bei der Fehlererkennung in Bereichen wie Konnektivität, Performance und Systemverhalten. Diagnosedaten werden zentral im Dashboard visualisiert und stehen für weitere Auswertungen bereit.

Der Status wird in Ampelfarben angezeigt:

- Grün: normaler Betrieb
- Gelb: Warnung (z. B. erhöhte Speicherauslastung)
- Rot: kritischer Fehler (z. B. Speicher nahezu vollständig belegt)

HINWEIS

Das Dashboard wird vor dem Login im WBM und nach dem Logout angezeigt.

Beispielansicht (WBM)

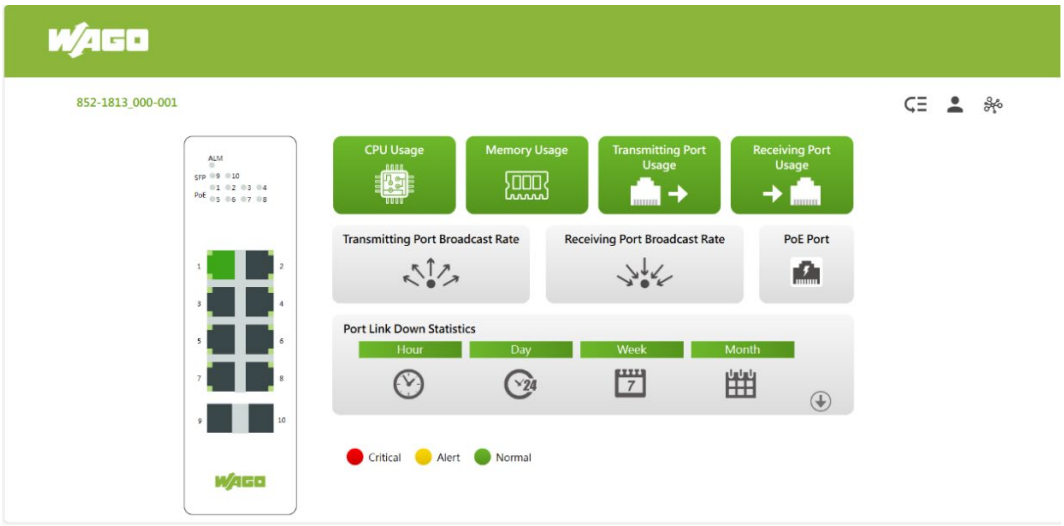


Abbildung 1: Dashboard (Beispiel)

3.1.2 Darstellung des Gerätestandorts und eines Ansprechpartners

Wenn in den SNMP-Einstellungen ein physischer Standort und Kontakt konfiguriert sind, werden diese Informationen im Dashboard oberhalb der schematischen Darstellung des Switches dargestellt. Weitere Informationen unter: **SNMP**

3.1.3 Topologie-Map zur Erkennung der Nachbargeräte

Die Topologie-Map stellt direkt angeschlossene Nachbargeräte grafisch dar. Geräteinformationen werden bei Mauszeigerkontakt eingeblendet; der Umfang der zur Verfügung stehenden Informationen hängt vom Gerätetyp sowie den per LLDP bereitgestellten Informationen ab.

HINWEIS

Darstellung wird in Google Chrome, Microsoft Edge und Firefox unterstützt. Internet Explorer ist nicht kompatibel.

Beispielansicht (WBM)

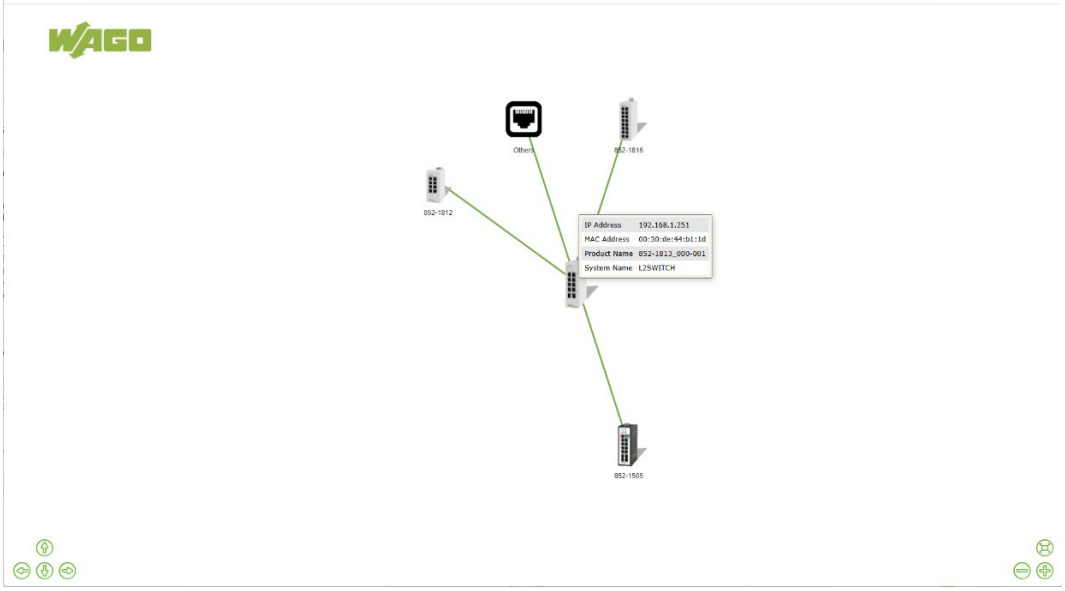


Abbildung 2: Topologie-Map – Anzeige mit Mouse-over (Beispiel)

- Die Topologie-Map kann durch Doppelklick auf den Switch verlassen werden.

3.2 Konfigurationsfunktionen

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

Web-Based Management (WBM)

Das Web-Based Management (WBM) ist eine menügesteuerte Benutzeroberfläche. Aufgerufen wird das WBM über die Protokolle „http“ (Standardeinstellung) oder „https“.

Das WBM zeigt Informationen über die Konfiguration und den Status des Switches und die Konfiguration des Gerätes kann geändert werden. Weitere Informationen unter: **Konfigurieren im WBM**

Beispielansicht (WBM)

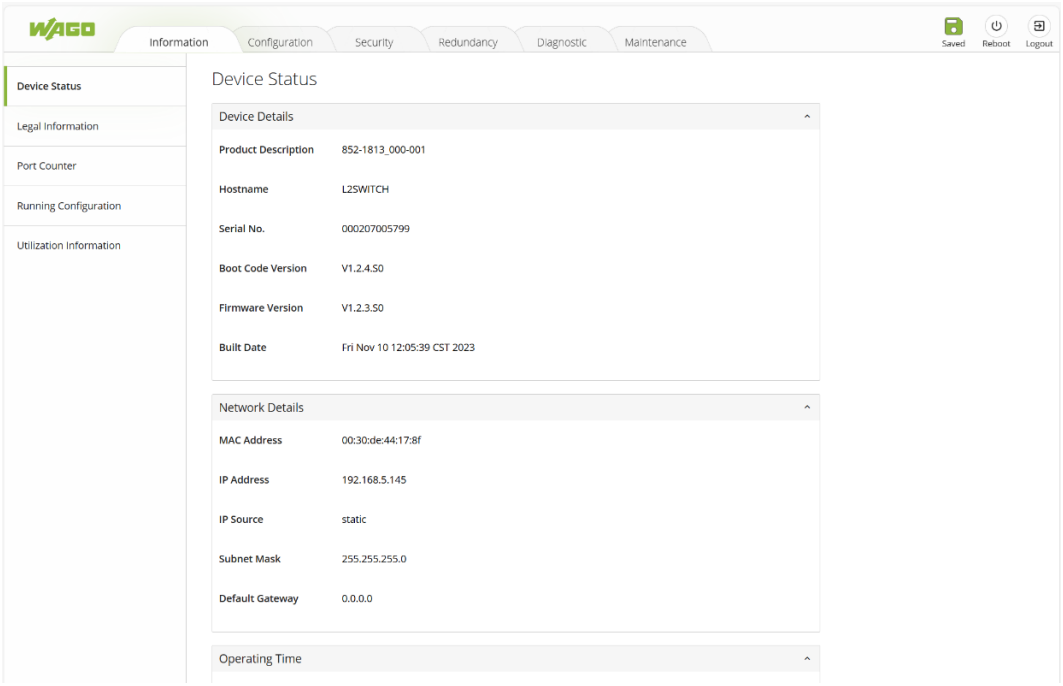


Abbildung 3: Aufbau einer WBM-Seite (Beispiel)

Command Line Interface (CLI)

Um den Switch per CLI zu konfigurieren, wird eine Telnet- oder SSH-Verbindung zum Switch benötigt. Weitere Informationen unter: **Konfigurieren mit dem CLI**

Simple Network Management Protocol (SNMP)

SNMP ist ein IETF-standardisiertes Protokoll zur Überwachung und Steuerung netzwerkfähiger Geräte. Es umfasst ein Protokoll, ein Datenbankschema (MIB) und zugehörige Objektdefinitionen.

Verwaltungsinformationen werden in Form von MIB-Variablen bereitgestellt und können per SNMP-Manager abgefragt oder modifiziert werden. Weitere Informationen unter: **Konfigurieren mit Netzwerkmanagement-Software**

3.3 Tab-Information im WBM

3.3.1 Device-Status

Nach dem Log-in werden hier Informationen über das Gerät angezeigt.

Beispielansicht (WBM)

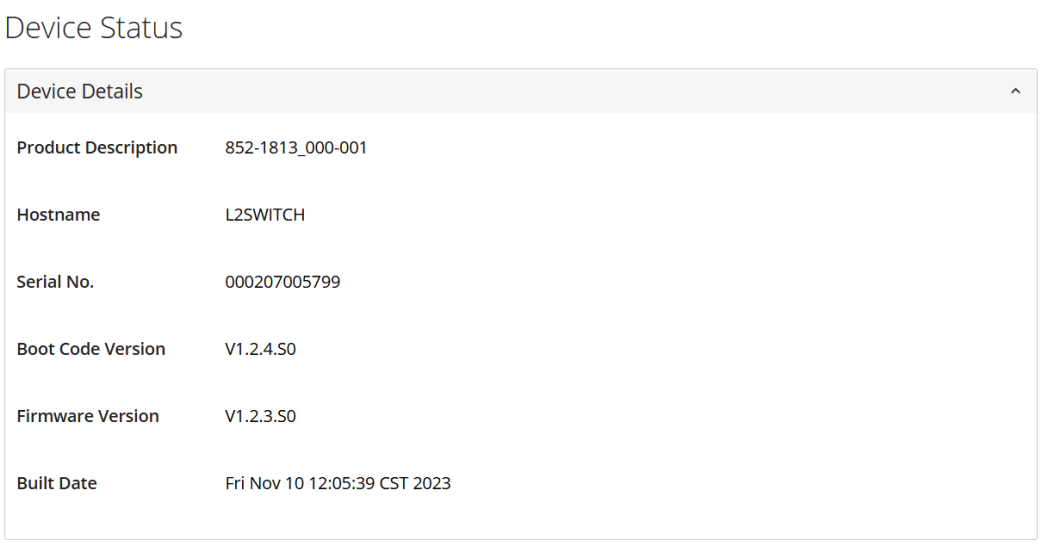


Abbildung 4: Device-Status

- Dargestellt werden Informationen wie Softwareversionsstände, eine Übersicht zur Netzwerkkonfiguration und die Betriebszeit seit dem letzten Neustart.

3.3.2 Legal Information

In diesem Menü finden Sie Lizenzinformationen untergliedert in:

- WAGO Lizenzen
- Open-Source-Lizenzen
- WBM-Lizenzen

3.3.3 Port Counter

Zeigt portbasiert eine Statistik zur Datenübertragung an. Die Counter werden automatisch bei einem Neustart des Switches zurückgesetzt; ein manuelles Zurücksetzen ist über die entsprechende Schaltfläche möglich.

Tabelle 1: Übersicht über die Port Counter

Parameter	Beschreibung
Receive/Transmit Drops	Anzahl empfangener/zu sendender Pakete die verworfen wurden, z. B. aufgrund einer ACL-Regel; weitere Informationen zu ACL-Regeln unter: ACL
Receive/Transmit Errors	Anzahl empfangener/zu sendender Pakete die Fehler enthielten, z. B. aufgrund einer fehlerhaften Prüfsumme
Receive/Transmit Packets	Anzahl empfangener/gesendeter Pakete
Receive/Transmit Bytes	Anzahl empfangener/gesendeter Bytes

CLI-Befehle

Tabelle 2: Port-Counter CLI

Befehl	Node
`show port-statistics`	enable
`clear port-statistics`	configure

3.3.4 Running Configuration

Dargestellt wird die aktuelle Konfiguration in Form von CLI-Befehlen. Die Darstellung ermöglicht einen schnellen Gesamtüberblick über die Gerätekonfiguration. Bei Bedarf können die Befehle in die Zwischenablage kopiert werden.

CLI-Befehle

Tabelle 3: Running-Configuration CLI

Befehl	Node
`show running-config`	enable

3.3.5 Utilization-Information

Informationen zur Leistung der einzelnen Ports werden angezeigt.

Tabelle 4: Übersicht über die Utilization-Information

Parameter	Beschreibung
Speed	Konfigurierte bzw. automatisch ausgehandelte Übertragungsrate in Mbit/s
Rx Utilization %/bps	Auslastung der Bandbreite in Empfangsrichtung in Prozent und Bits per second
Tx Utilization %/bps	Auslastung der Bandbreite in Ausgangsrichtung in Prozent und Bits per second

CLI-Befehle

Tabelle 5: Port-Utilization CLI

Befehl	Node
`show port-utilization`	enable

3.4 Tab-Configuration im WBM

3.4.1 Device-Discovery

3.4.1.1 LLDP

Das „Link Layer Discovery Protocol“ (LLDP) gemäß IEEE 802 ermöglicht die Übertragung von Systeminformationen zwischen direkt verbundenen Stationen innerhalb eines LAN. Über LLDP werden u. a. Managementadressen, Systemfunktionen und Informationen zur eindeutigen Identifikation eines Gerätes an benachbarte Geräte übermittelt. Diese Informationen dienen der Netzwerkverwaltung und Topologieerkennung.

Informationen zu weiteren Geräten im Netzwerk werden unter „LLDP Neighbor Information“ angezeigt, sobald diese erkannt wurden. Der Umfang der gezeigten Informationen ist abhängig von den Fähigkeiten des jeweiligen Remote-Gerätes.

Beispielansicht (WBM)

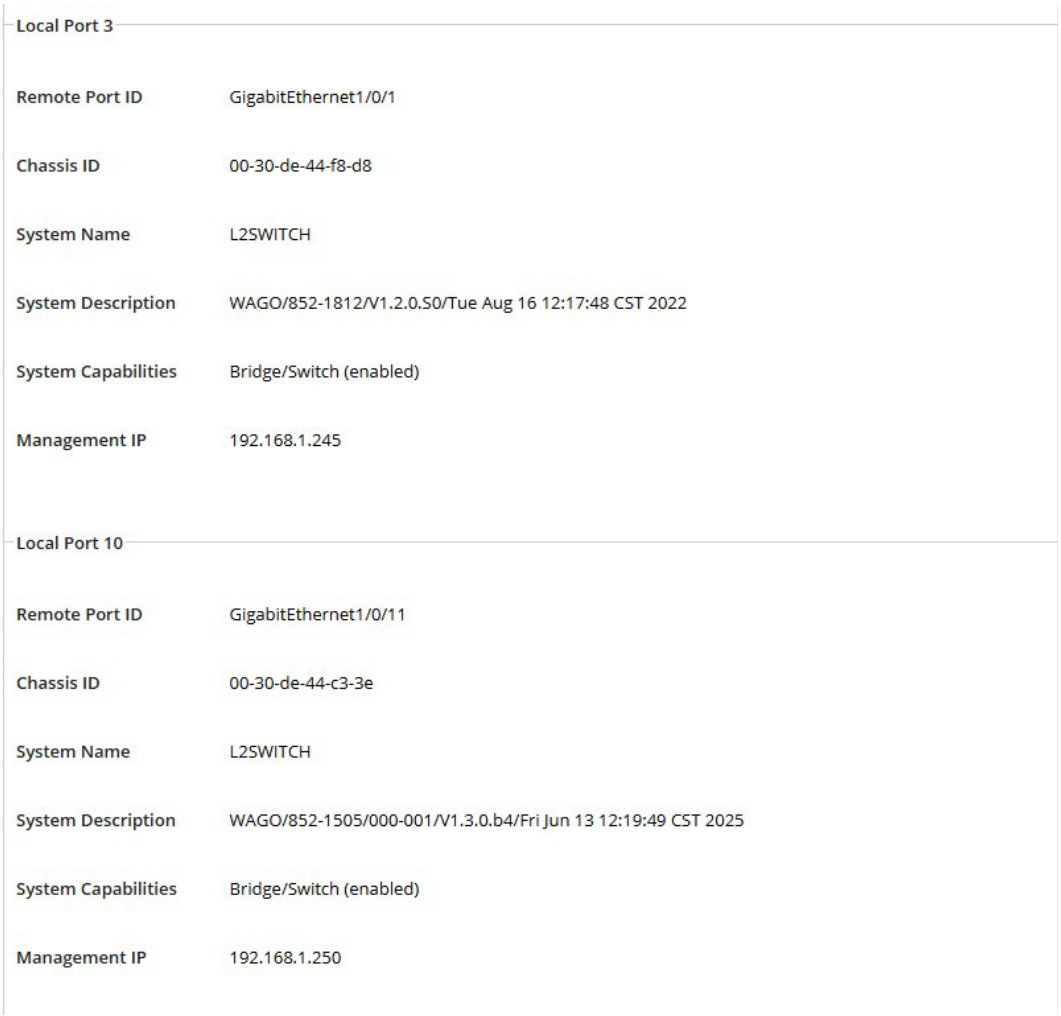


Abbildung 5: LLDP Settings + LLDP Neighbor Information

Tabelle 6: Übersicht zu den LLDP-Nachbarschaftsinformationen an den jeweiligen Ports

Parameter	Beschreibung
Remote Port ID	Hier wird die Kennung des Ports angezeigt, über den das benachbarte Gerät mit dem lokalen Switch-Port verbunden ist. Kann zur Identifizierung von Fehlern oder zum Mapping physischer Verbindung genutzt werden.
Chassis ID	Die angezeigte Chassis-ID dient zur eindeutigen Identifizierung des benachbarten Geräts. Standardmäßig wird für WAGO Switches die MAC-Adresse verwendet.
System Name/ System Description/ System Capabilities	Name, Beschreibung und Fähigkeiten des benachbarten Geräts werden hier angezeigt und helfen bei der Identifikation des jeweiligen Geräts. Einige Geräte bieten die Möglichkeit diese Informationen benutzerdefiniert anzupassen.
Management IP	Es wird die Managementadresse angezeigt, die zur Verwaltung des benachbarten Gerätes verwendet werden kann.

CLI-Befehle

Tabelle 7: LLDP CLI

Befehl	Node
`show lldp`	enable
`show lldp neighbor`	enable
`lldp ...`	configure
`lldp-agent ...`	interface
`lldp-agent ...`	if-range

3.4.1.2 Manual-Registration

Wenn ein Gerät im Netzwerk LLDP nicht unterstützt, dann kann dieses Gerät dem Switch über die manuelle Registrierung bekannt gemacht werden. Diese Informationen werden anschließend in der Topologie-Map angezeigt.

Das Feature benötigt zur manuellen Registrierung eines Geräts dessen MAC-Adresse. Da jedoch häufig nur die IP-Adresse eines Geräts bekannt ist, versucht der Switch, die MAC-Adresse automatisch zu ermitteln, wenn diese nicht angegeben wird. Hierzu wird die IP-Adresse verwendet.

CLI-Befehle

Tabelle 8: Manual-Registration CLI

Befehl	Node
`show manual-registration-device`	enable
`manual-registration-device`	configure

3.4.2 Fieldbus-Priority

In ETHERNET-Netzwerken konkurrieren besonders zeitkritische Informationen von Feldbusprotokollen mit weniger zeitkritischen Daten, wie z. B. denen für den Zugriff auf das WBM. Fieldbus-Priority wirkt sich insbesondere in Zeiträumen mit besonders hoher Netzwerkauslastung aus, die zum Teil durch zeitunkritischen (unpriorisierten) Datenverkehr hervorgerufen wird. In diesem Fall ermöglicht das Feature die priorisierte Datenübertragung eines ausgewählten Feldbusprotokolls, sodass dessen Informationen mit kleinstmöglicher Verzögerung weitergeleitet werden. Daten des priorisierten Feldbusprotokolls werden mit Priorität 6 verarbeitet. Für weitere Details hierzu beachten Sie den folgenden Hinweis.

Die Identifizierung von PROFINET- und GOOSE-Daten erfolgt anhand des Ethertype 0x8892 bzw. 0x88b8, EtherNet/IP™-Pakete werden anhand des UDP-Quell-/Zielports 2222 bzw. des TCP-Quell-/Zielports 44818 erkannt.

Durch die Priorisierung wird u. a. ein zuverlässiger Echtzeit-Datenaustausch innerhalb des PROFINET®-Systems ermöglicht. Die Geräte erfüllen die Anforderungen der Conformance-Class A.

Eine GSDML-Datei ist nicht vorhanden; eine Konfiguration über das TIA Portal oder einen PROFINET®-Controller ist nicht möglich.

HINWEIS

Priorisierung gemäß IEEE802.1Q und Prioritäts-Warteschlangen

WAGO Lean-Managed-Switches beachten bei der Paketweiterleitung auch Priorisierungsinformationen im Feld „Priority Code Point“ (PCP) (Wertebereich 0 … 7) gemäß IEEE 802.1Q. Für jede Prioritätsstufe hält der Switch eine eigene Warteschlange zur Abarbeitung vor. Pakete, die keine Priorisierungsinformation nach IEEE 802.1Q enthalten, werden priorisiert wie Pakete mit PCP = 0. PROFINET®-, EtherNet/IP™- bzw. Goose-Daten werden mit Priorität 6 verarbeitet, wenn Fieldbus-Priority für das jeweilige Protokoll aktiviert ist. Die höchste Prioritätsstufe (7) wird für die Verarbeitung von Daten der Redundanzprotokolle verwendet (siehe **Tab-Redundancy im WBM**).

Beispielansicht (WBM)

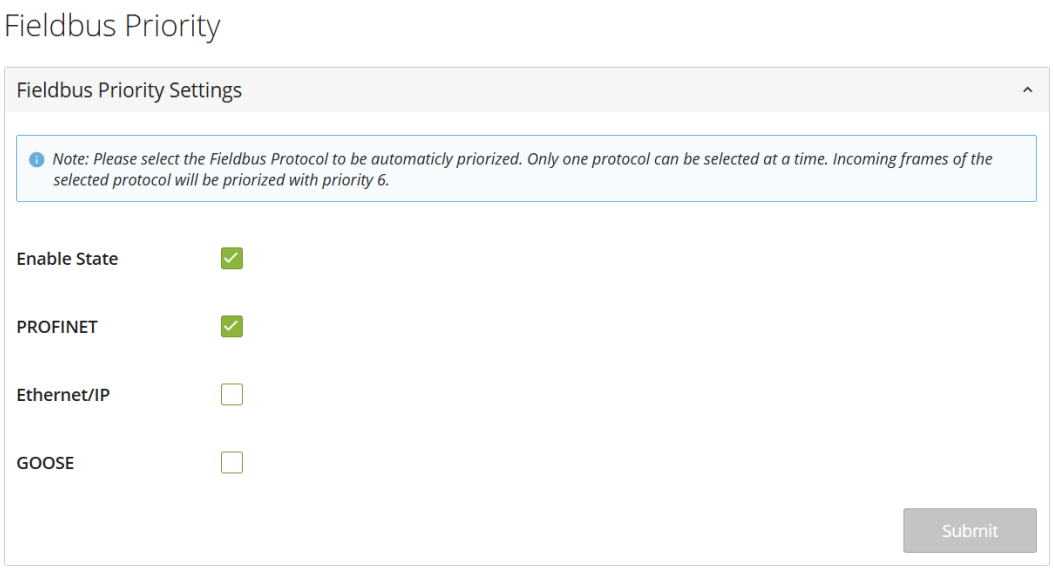


Abbildung 6: Fieldbus-Priority

CLI-Befehle

Tabelle 9: Fieldbus-Priority CLI

Befehl	Node
`show fieldbus-priority`	enable
`fieldbus-priority ...`	configure
`fieldbus-priority type ...`	configure

3.4.3 Interface

3.4.3.1 Loop-Detection

Die Funktion Loop-Detection dient der Erkennung von Schleifen im Netzwerk, insbesondere infolge fehlerhafter physikalischer Verkabelung.

Ein Schleifenzustand entsteht typischerweise durch direkte Verbindung zweier Ports eines Switches, was zu Broadcast-Storms führen kann. Loop-Detection erkennt solche Zustände durch den Versand von Prüfpaketen alle 2 Sekunden an eine im Netzwerk nicht vorhandene MAC-Adresse. Werden diese über denselben Port zurückempfangen, deaktiviert der Switch den betroffenen Port, um Netzwerkausfälle zu verhindern.

Bei aktiviertem Recovery-State werden die entsprechenden Ports nach Ablauf der eingestellten Recovery-Time automatisch wieder aktiviert und der Switch arbeitet normal weiter. Loop-Detection prüft weiterhin, ob Schleifen im Netzwerk auftreten.

Im Ereignisfall erzeugt der Switch Syslog-Einträge, interne Log-Meldungen sowie SNMP-Traps.

Beispielansicht (WBM)

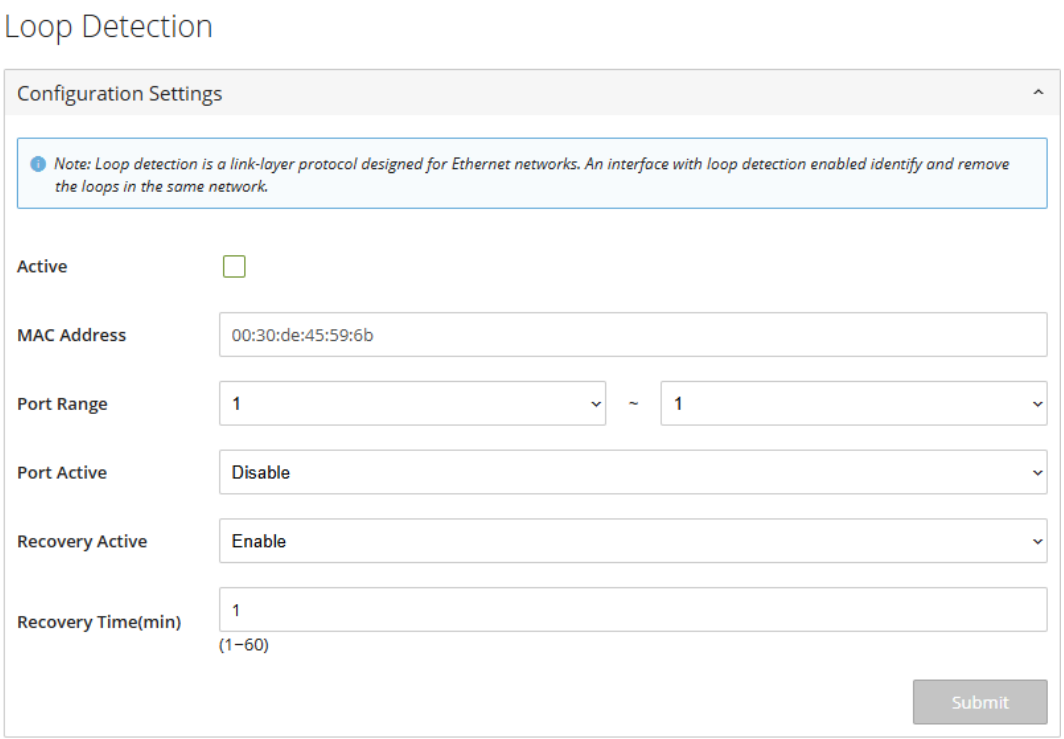


Abbildung 7: Loop-Detection – Configuration-Settings

Tabelle 10: Übersicht über die Konfigurationseinstellungen für die Loop-Detection

Parameter	Beschreibung
State	Anzeige, ob die Loop-Detection für den jeweiligen Port ein- oder ausgeschaltet ist.
Status	Anzeige, ob der jeweilige Port geblockt ist; sofern die Recovery-Funktion eingeschaltet ist, sollte sich dieser Status nach der konfigurierten Zeitspanne normalisieren – andernfalls wurde die Schleife noch nicht beseitigt.
Manual Recovery	Über diese Schaltfläche kann ein deaktivierter Port manuell wieder freigegeben werden. Wenn die Recovery-Funktion aktiviert wurde, ist ein manuelles Freigeben nicht erforderlich.
Recovery State/Time(min)	Angabe, ob die Recovery-Funktion ein- oder ausgeschaltet ist und welche Zeitspanne konfiguriert wurde, die der Switch wartet, bis er den Port wieder frei gibt.

CLI-Befehle

Tabelle 11: Loop-Detection CLI

Befehl	Node
`show loop-detection`	enable
`loop-detection ...`	configure
`interface range gigabitethernet1/0/...`	configure
`loop-detection ...`	interface
`no shutdown`	interface
`loop-detection recovery ...`	interface
`loop-detection recovery time ...`	interface
`loop-detection ...`	if-range
`loop-detection recovery ...`	if-range
`loop-detection recovery time ...`	if-range

3.4.3.2 Mirror

Port-Mirroring ermöglicht das Kopieren von eingehendem und/oder ausgehendem Datenverkehr eines oder mehrerer Source Ports auf einen weiteren Port zur Analyse.

Diese Funktion wird zur passiven Überwachung des Netzwerkverkehrs eingesetzt, z. B. in Verbindung mit „Intrusion Detection Systems“ (IDS) oder „Network Traffic Analyzers“ (NTA). Sie dient der Protokollierung und Auswertung sicherheitsrelevanter oder leistungsbezogener Informationen.

HINWEIS

Über das CLI können mehrere Source-Ports für das Port-Mirroring definiert werden. Zusätzlich lässt sich konfigurieren, ob der gespiegelte Datenstrom den Ingress-, Egress- oder bidirektionalen Datenverkehr umfasst.

Beispielansicht (WBM)

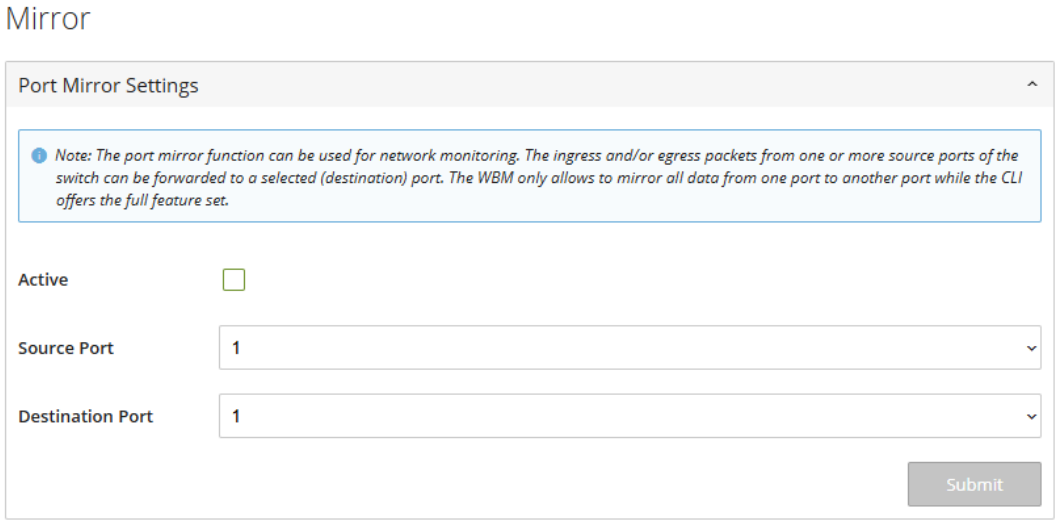


Abbildung 8: Port Mirror Settings

CLI-Befehle

Tabelle 12: Port-Mirror CLI

Befehl	Node
`show mirror`	enable
`mirror ...`	configure
`mirror destination port ...`	configure
`mirror source ports ... mode ...`	Configure
`no mirror source ports …`	Configure

3.4.3.3 Port-Set-up

Port-Set-up ermöglicht die Konfiguration grundlegender Eigenschaften einzelner Ports wie das (De-)Aktivieren von Ports und die Auswahl des Duplex-Modus, Nway (Autonegotiation zur automatischen Aushandlung des Duplex-Modus und der Geschwindigkeit), Auto MDI/MDIX (benötigt Nway) und Flow-Control.

Das Produkt 852-1813/xxx-001 erlaubt, die Geschwindigkeit der SFP-Module über DIP-Schalter fest auf „100 Mbps/Full“ einzustellen. Die im WBM getroffene Einstellung wird hierbei überschrieben. Weitere Informationen dazu finden Sie im Abschnitt **DIP-Status** und im jeweiligen Produkthandbuch.

ⓘ HINWEIS

Behandlung von Kompatibilitätsproblemen

Wenn ein Port trotz korrekter Verkabelung nicht aktiviert wird, kann dies auf Kompatibilitäts-probleme beim Feature „Auto MDI/MDIX“ hindeuten. In diesem Fall sollte eine manuelle Konfiguration der Port-Geschwindigkeit und der Duplex-Einstellung vorgenommen werden. Es sollte bei beiden Kommunikationsendgeräten (Ports) dieselbe Einstellung vorgenommen werden.

WAGO Lean-Managed Switches ermöglichen neben dem Einsatz von 1Gbit/s-SFP-Modulen auch den Einsatz von 100Mbit/s-SFP-Modulen. Dabei ist zu beachten, dass Nway (Autonegotiation) für Verbindungen spezifiziert wurde, die auf Kupferkabeln basieren. Bei der Verwendung von SFP-Modulen für Glasfaserverbindungen (nur Produkte mit den Artikelnummern 852-1813 und 852-1813/xxx-xxx) sollte die Datenübertragungsrate manuell konfiguriert werden. Nicht jede der verfügbaren Geschwindigkeitsoptionen wird von jedem SFP-Modul unterstützt. Abhängig von der maximalen Geschwindigkeit des verwendeten SFP-Moduls werden die Einstellungen „100 Mbps/Full“ bzw. „1000 Mbps/Full“ von nahezu allen SFP-Modulen zuverlässig unterstützt.

Beispielansicht (WBM)

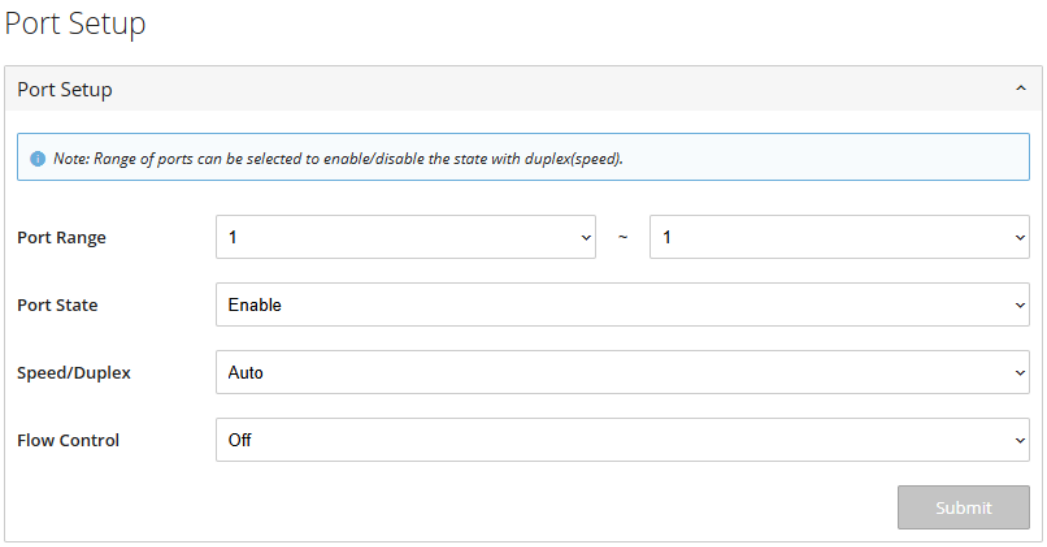


Abbildung 9: Port-Set-up

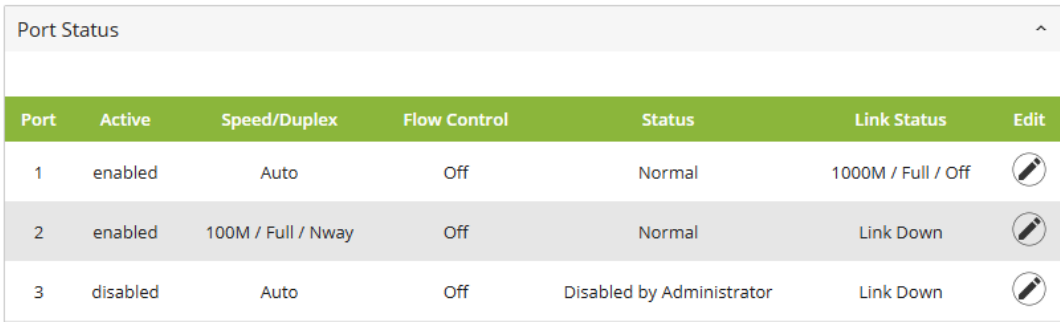


Abbildung 10: Port Status

- Im Port-Status wird die vorgenommene Konfiguration tabellarisch dargestellt und um aktuelle Informationen zur Verbindung ergänzt.
- Wenn der Port eine Verbindung aufbauen konnte, wird in der Spalte Link-Status ausgegeben, mit welchen Parametern die Verbindung aktiv ist:
- Datenübertragungsrate
- Duplex-Modus
- Flow-Control

CLI-Befehle

Tabelle 13: Port-Set-up CLI

Befehl	Node
`show interface ...`	enable
`interface ...`	configure
`interface range gigabitethernet1/0/ ...`	configure
`flowcontrol ...`	interface
`speed ...`	interface
`shutdown`	interface

`description ...`	interface
`cable test`	interface
`clean cable-test result`	interface
`show cable-test result`	interface
`description ...`	if-range
`shutdown`	if-range
`speed ...`	if-range

3.4.3.4 Port-Priority

Netzwerke übertragen Daten standardmäßig ohne Priorisierung; alle Frames werden gleichbehandelt. Bei Überlast besteht für alle Datenpakete die gleiche Verwerfungswahrscheinlichkeit.

Mit Port-Priority lässt sich der ausgehende Datenverkehr eines Ports priorisieren. Höher priorisierte Frames werden bei Bandbreitenengpässen bevorzugt übertragen. Dies verbessert die Übertragungsqualität für kritische Dienste und optimiert die Ressourcennutzung.

Bevorzugt sollten zeitkritische Netzwerkgeräte (z. B. SPS, Remote-IO) eine hohe und zeitunkritische Netzwerkgeräte (z. B. Kameras, Drucker) eine niedrige Priorität erhalten. Pakete der Prioritätsstufen High, Medium bzw. Low werden den Warteschlangen 6, 4 bzw. 0 zugeordnet. Beachten Sie den Hinweis im Abschnitt **Fieldbus-Priority**.

Beim Switch 852-1813/xxx-001 können die Ports 1 … 2 über den DIP-Schalter „QoS“ priorisiert werden. Dies überschreibt die unter Port-Priority vorgenommenen Einstellungen, siehe **DIP-Status**.

HINWEIS

Priorisierung der Daten im Netzwerk

Port-Priority hilft, insbesondere während einer zeitweise hohen Netzwerkauslastung die Übertragungsqualität zu verbessern. Eine dauerhaft sehr hohe Netzwerkauslastung an der Grenze der maximalen Übertragungskapazität sollte jedoch durch eine optimierte Netzwerktopologie bzw. Anwendungskonfiguration oder einer Erhöhung der Bandbreite vermieden werden.

Beispielansicht (WBM)

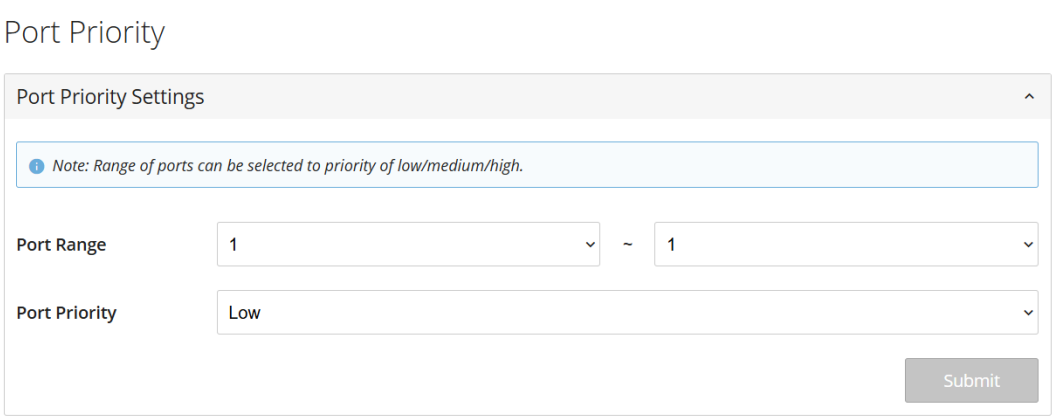


Abbildung 11: Port-Priority-Settings

CLI-Befehle

Tabelle 14: Port-Priority CLI

Befehl	Node
`show queue cos-map`	enable
`show qos mode`	enable
`show diffserv`	enable
`queue cos-map ...`	configure
`qos mode high-first`	configure
`qos mode wrr-queue weights ...`	configure
`diffserv ...`	configure
`diffserv dscp ... priority ...`	configure
`default-priority`	interface

3.4.4 PoE-Settings

HINWEIS

PoE Funktion

Diese Funktion ist nur bei den WAGO Lean-Managed-Switches mit den Artikelnummern 852-1813/000-001 und 852-1813/010-001 vorhanden. Bei Überschreitung der verfügbaren PoE-Leistung wird die Spannungsversorgung mittels PoE zum Schutz des Switches abgeschaltet.

3.4.4.1 PD-Alive-Check

Bei aktiviertem PD-Alive-Check (PD = Powered Device) überprüft der Switch die Erreichbarkeit der mit Spannung versorgten Geräte. Ist die Funktion für einen Port aktiv, sendet der Switch in jedem Prüfintervall ein Prüfpaket. Erfolgt keine Antwort innerhalb der konfigurierten Anzahl von Wiederholversuchen, wird die unter „Action“ definierte Maßnahme angewendet.

Beispielansicht (WBM)

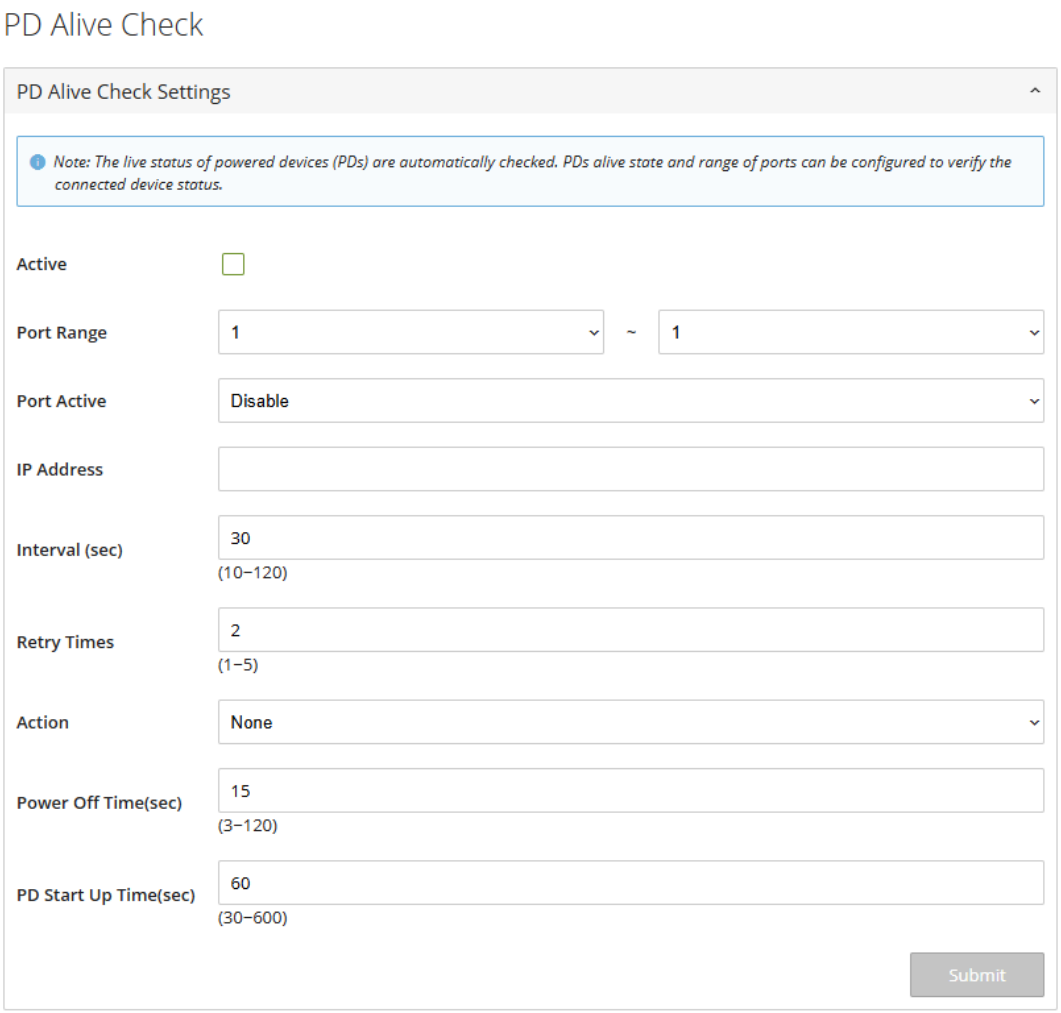


Abbildung 12: PD Alive Check Settings

- Für einzelne Ports oder Port-Bereiche kann über Port Active die Funktion ein- bzw. ausgeschaltet werden. Bei aktiviertem PD-Alive-Check können die IP-Adresse des Hosts sowie Intervall und Wiederholungsrate für das Versenden der Prüfpakete konfiguriert werden.
- Für den Fall, dass ein Prüfpaket vom Endgerät nicht beantwortet wird, kann der Switch verschiedene Aktionen ausführen. Hierzu gehören das Generieren eines Alarms und der Neustart des PD durch kurzzeitiges Unterbrechen der Spannungsversorgung. Beide Aktionen können auch in Kombination ausgeführt werden (Option „All“).
- Sofern „All“ oder „Reboot“ als Aktion konfiguriert wurde, kann über die Werte „Power Off Time“ und „PD Start Up Time“ definiert werden, wie lange gewartet wird, bis der Port nach dem Abschalten des Endgeräts wieder mit Strom versorgt wird und nach welcher Zeitspanne der Switch wieder mit dem Versenden vom Prüfpaketen beginnt.

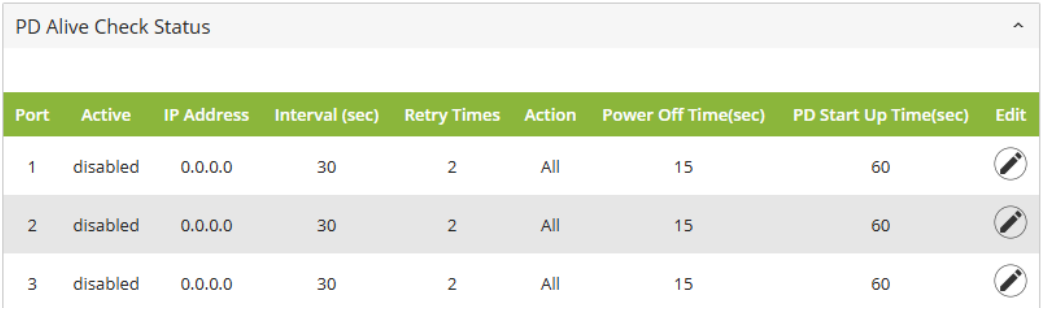


Abbildung 13: PD-Alive-Check Status

CLI-Befehle

Tabelle 15: PD-Alive-Check CLI

Befehl	Node
`show pd-alive`	enable
`pd-alive ...`	configure
`pd-alive ...`	interface
`pd-alive action ...`	interface
`pd-alive interval ...`	interface
`pd-alive ip ... pd-alive power-off-time ... startup-time ...`	interface
`pd-alive retry-time ...`	interface

3.4.4.2 Power ON/OFF

Diese Konfigurationsseite ermöglicht es die Spannungsversorgung mittels „Power over Ethernet“ (PoE) global sowie für einzelne Ports ein- und auszuschalten.

Beispielansicht (WBM)

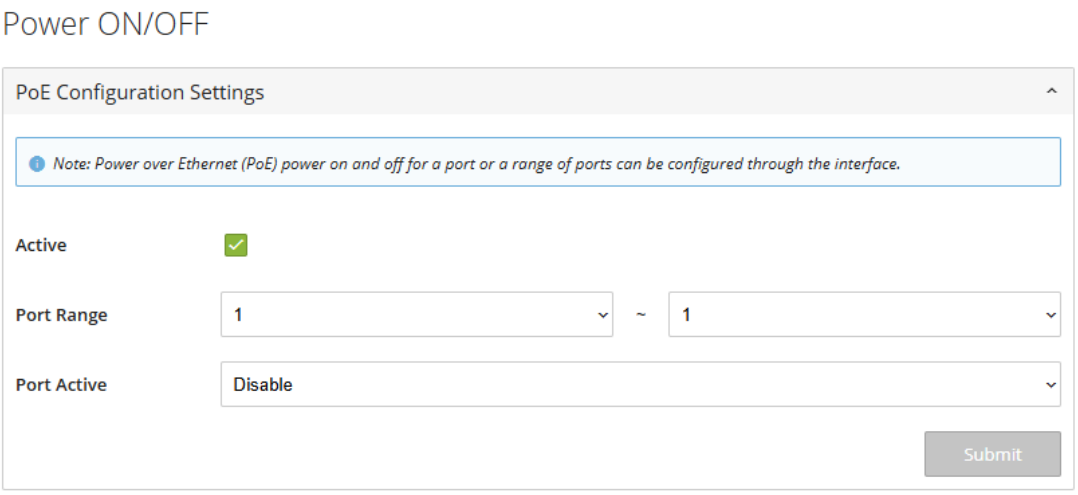


Abbildung 14: PoE-Configuration-Settings

Tabelle 16: Übersicht über den PoE-Configuration-Status an den jeweiligen Ports

Parameter	Beschreibung
Active	Darstellung, für welche Ports PoE aktiviert oder deaktiviert wurde; wenn ein Endgerät nicht mit Strom versorgt werden kann, kann hier kontrolliert werden, ob die PoE-Einstellungen am entsprechenden Port korrekt sind.
Status	Hier kann abgelesen werden, ob ein Endgerät tatsächlich mit Strom versorgt wird. Wenn trotz eingeschalteter PoE-Funktion kein Strom an das Endgerät geliefert wird, sollte geprüft werden, ob die Verkabelung korrekt ist, das Endgerät kompatibel zum IEEE-PoE-Standard ist oder, bei mehreren Endgeräten, das Leistungsbudget des Switches überschritten wurde.

CLI-Befehle

Tabelle 17: PoE-Configuration CLI

Befehl	Node
`show poe`	enable
`poe ...`	configure
`poe total-power`	configure
`poe ...`	interface
`poe ...`	if-range

3.4.5 SNMP

„Simple Network Management Protocol“ (SNMP) ist Bestandteil der IETF-spezifizierten „Internet Protocol Suite“. Es umfasst ein Anwendungsschichtprotokoll, ein MIB-Datenmodell und standardisierte Managementobjekte zur Überwachung und Steuerung netzwerkbasierter Geräte.

Managementdaten werden über MIB-Variablen bereitgestellt und können von der SNMP-Verwaltungssoftware (SNMP-Manager) abgefragt oder geändert werden.

WAGO Lean-Managed-Switches unterstützen SNMP in der Version 1/2c und die Version 3 mit umfangreicherer Rechteverwaltung und Authentifizierung.

3.4.5.1 SNMP Set-up

Dienste des „Simple Network Management Protocol“ (SNMP) und generelle SNMP-Informationen können hier konfiguriert werden.

Beispielansicht (WBM)

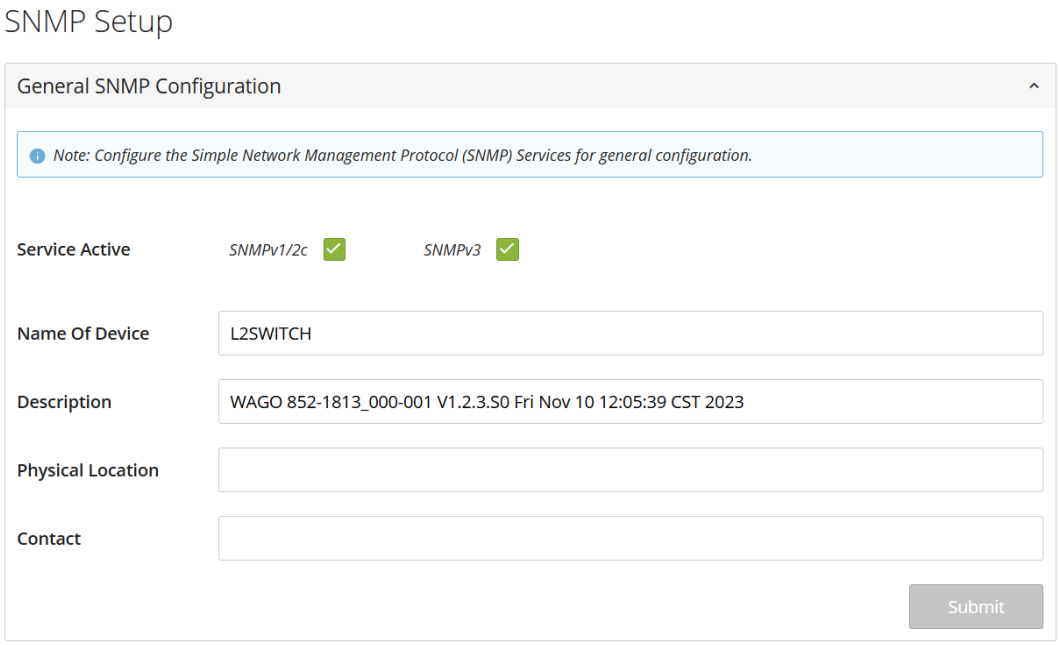


Abbildung 15: General SNMP-Configuration

HINWEIS

Gerätename: Anzeige in Topologie-Map

Der hier hinterlegte Gerätename wird auch beim Austausch von Geräteinformationen per LLDP verwendet. Er wird auf diesem Wege u. a.in der Topologie-Map angezeigt.

Physischer Standort und Kontakt: Anzeige im Dashboard

Der hier hinterlegte physische Standort und Kontakt werden im Dashboard des Gerätes angezeigt. Hierdurch ist eine einfache Zuordnung des Geräts möglich.

Hinterlegen Sie keine sensiblen Informationen, da diese ggf. auch von Unbefugten eingesehen werden können.

CLI-Befehle

Tabelle 18: SNMP CLI

Befehl	Node
`show snmp`	enable
`snmp ...`	configure
`snmp system-name ...`	configure
`snmp system-description ...`	configure
`snmp system-location ...`	configure
`snmp system-contact ...`	configure

3.4.5.2 SNMP v1/2c

Hinter dem Menü SNMP v1/2c verbergen sich die Einstellungen zur Konfiguration der Zugriffsrechte und des Community-Strings.

In SNMPv1 und SNMPv2c erfolgt die Authentifizierung und Rechtevergabe über Community-Strings, die im Klartext zwischen SNMP-Manager und SNMP-Agent übertragen werden. In vielen Fällen wird standardmäßig der Community-String „public“ verwendet. Bei den WAGO Lean-Managed-Switches ist in den Werkseinstellungen kein Community-String voreingestellt. Bei aktivierter SNMPv3-Funktionalität müssen v1/v2c-Communities separat konfiguriert werden; eine gemeinsame Nutzung ist nicht zulässig.

Beispielansicht (WBM)

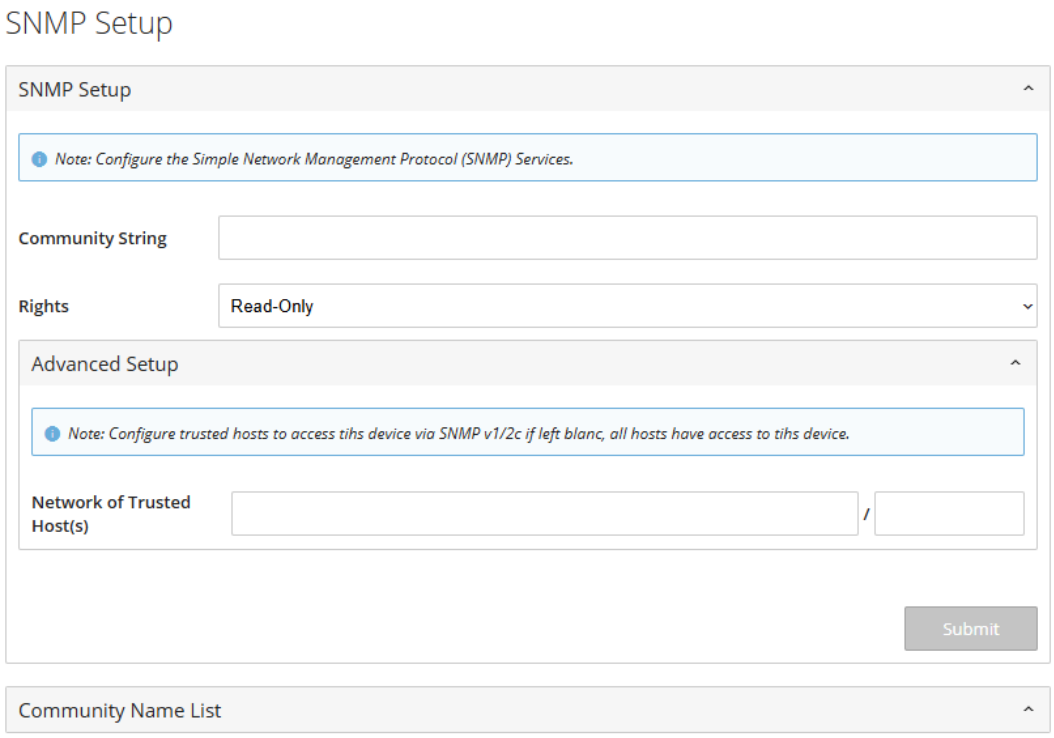


Abbildung 16: SNMP v1/2c

- Zu jedem Community-String können über das Drop-Down-Menü Rechte (Read-Only oder Read/Write) vergeben werden.
- In den Advanced Settings lässt sich optional ein vertrauenswürdiges IP-Netzwerk definieren. Wenn ein solches Netzwerk definiert ist, können nur Hosts in diesem Netzwerk den Switch

per SNMP verwalten. Die Definition des vertrauenswürdigen Netzwerks erfolgt durch die Angabe einer Netzwerkadresse und einer Subnetzmaske (CIDR-Notation).

Tabelle 19: Übersicht über die konfigurierten Communities und die zugehörigen Einstellungen

Parameter	Beschreibung
No./Community-String	Nummer der Community und der zugehörige String
Rights	In dieser Zeile werden die Berechtigungen für den „SNMP-Community-String“ angezeigt. Sollte ein Community-String falsch konfiguriert sein, kann der Status der Rechte hier abgelesen werden.
Network ID of the Trusted Host/Number of Mask Bit	Die IP-Adresse und die Anzahl der Subnet-Mask-Bits können hier abgelesen werden. Die SNMP-Manager, die auf den Switch via SNMP zugreifen wollen, müssen aus dem hier konfigurierten IP-Subnetz stammen. Andernfalls wird der Zugriff per SNMP vom Switch verweigert. Sollte eine Community nicht ordnungsgemäß funktionieren, können diese Informationen bei der Fehleridentifikation helfen.

CLI-Befehle

Tabelle 20: SNMP v1/2c CLI

Befehl	Node
`snmp community ... ... trusted-host ...`	configure

3.4.5.3 SMNP Trap

SNMP-Traps ermöglichen es dem Switch den SNMP-Manager bei Auftreten bestimmter Ereignisse selbstständig zu informieren. In diesem Menü wird das Ziel für SNMP-Traps konfiguriert.

Beispielansicht (WBM)

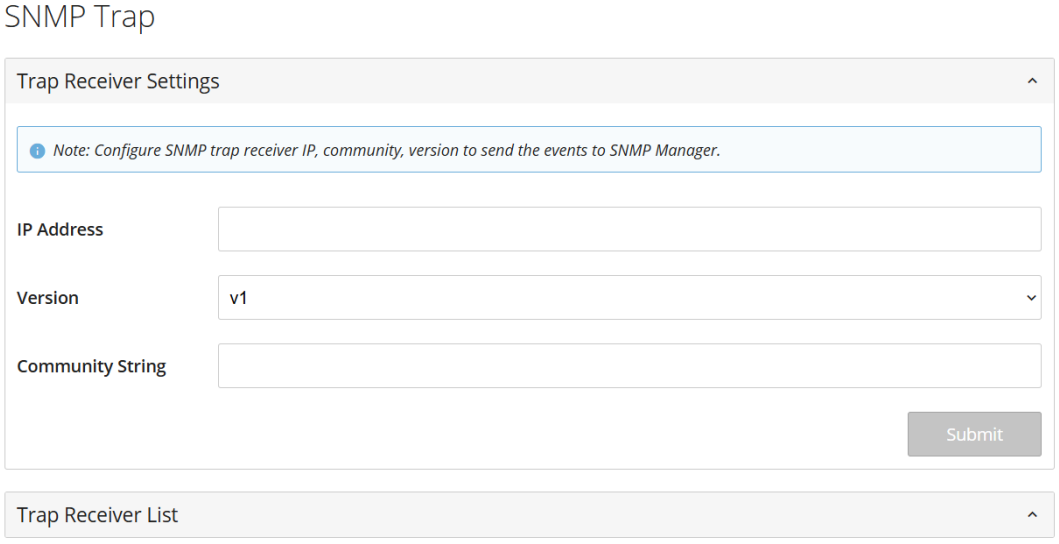


Abbildung 17: SNMP-Trap

Tabelle 21: Übersicht über die Parameter der Trap-Receiver

Parameter	Beschreibung
No/IP Address/Version	Nummer der Community, IP-Adresse des dezentralen Trap-Receivers und die SNMP-Version können hier abgelesen werden und helfen bei der Identifizierung eines Fehlers.

Community String	Der Community-String für den Trap-Receiver ist hier einsehbar. Stimmt er nicht mit dem erwarteten Wert überein, wird der Trap vom Receiver ignoriert. In diesem Fall muss der Community-String auf Sender und Receiver identisch konfiguriert werden.

CLI-Befehle

Tabelle 22: SNMP-Trap CLI

Befehl	Node
`snmp trap-receiver ...`	configure

3.4.5.4 SMNP Event Settings

Es können SNMP-Trap-Eventtypen ausgewählt werden, bei deren Auftreten der konfigurierte SNMP-Trap-Receiver informiert wird. Solche Events sind u. a. Übertemperatur, Überlastung, Stromausfall, Blockierung des Ports, Loop-Detection, Topologieänderungen.

Trap Event State Settings

Die zur Verfügung stehenden SNMP-Traps sind in zwei Kategorien unterteilt. Zum einen können unter „Trap Event State Settings“ SNMP-Traps aktiviert werden, die sich auf den Betriebsstatus und wesentliche Features des Switches beziehen. Zum anderen kann unter „Port Link-Change Trap Settings“ für jeden physischen Netzwerk-Port des Switches ein Trap aktiviert werden, der den SNMP-Manager bei einer Änderung des Link-Status informiert.

Beispielansicht (WBM)

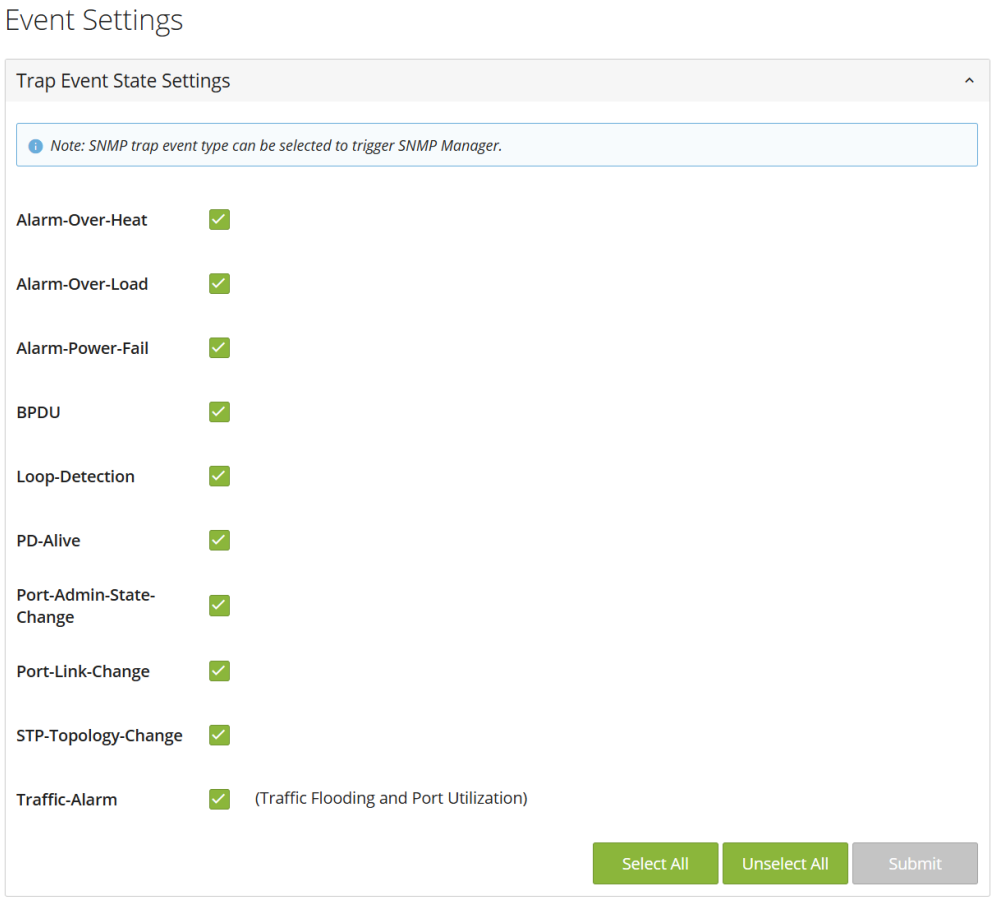


Abbildung 18: SNMP – Trap Event State Settings

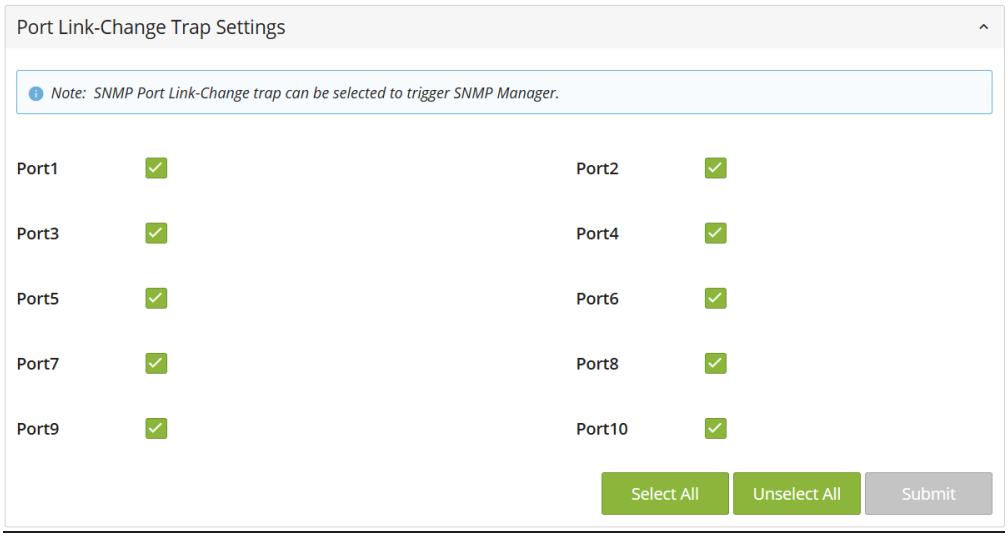


Abbildung 19: SNMP – Port Link-Change Trap Settings

CLI-Befehle

Tabelle 23: SNMP Event CLI

Befehl	Node
`show snmp trap-event`	enable
`snmp trap-event alarm-over-heat ...`	configure
`snmp trap-event alarm-over-load ...`	configure
`snmp trap-event alarm-power-fail ...`	configure
`snmp trap-event bpdu ...`	configure
`snmp trap-event loop-detection ...`	configure
`snmp trap-event port-admin-state-change ...`	configure
`snmp trap-event port-link-change ...`	configure
`snmp trap-event power-source-change ...`	configure
`snmp trap-event stp-topology-change ...`	configure
`snmp trap-event traffic-monitor ...`	Configure
`show snmp port-link-change-trap`	enable
`snmp port-link-change-trap`	interface
`interface range ...`	configure
`snmp port-link-change-trap`	if-range

3.4.5.5 SMNPv3-View

Der Bereich „SNMPv3 View“ ermöglicht die Definition von SNMPv3-Views. In einer View werden Objekte der MIB zusammengefasst. Nutzer einer SNMP-Gruppe erhalten Zugriff auf die in einer View definierten MIB-Objekte, indem die View in den Gruppeneinstellungen angegeben wird; siehe hierzu auch **SMNPv3-Group**. Wenn eine View für die Gruppe als „Read View“ konfiguriert wird, erhalten die Nutzer lediglich lesenden Zugriff.

Beispielansicht (WBM)

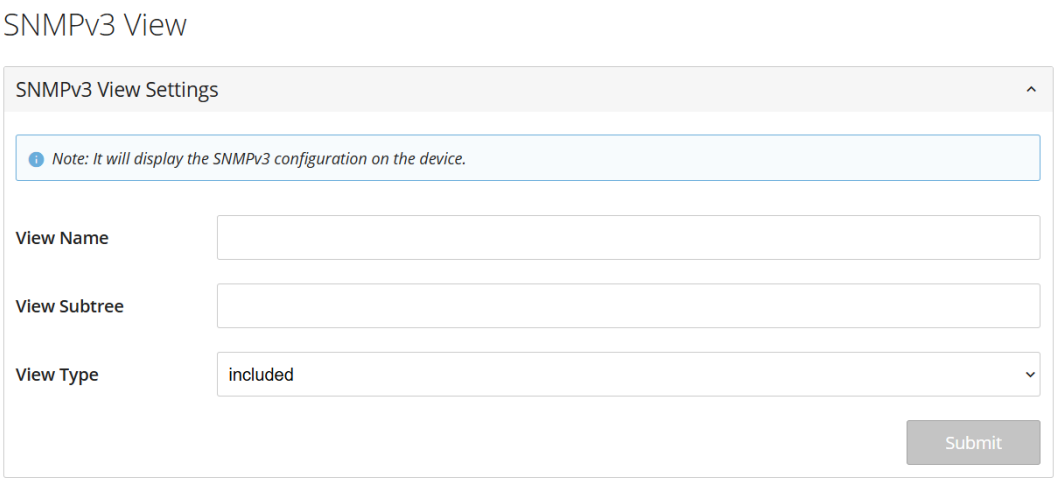


Abbildung 20: SNMP – SNMPv3-View-Settings

CLI-Befehle

Tabelle 24: SNMPv3 View CLI

Befehl	Node
`show snmp view`	enable
`snmp view ...`	configure
`no snmp view ...`	configure

3.4.5.6 SMNPv3-Group

SNMPv3-Gruppen ermöglichen, den Zugriff auf die SNMP-Informationen feingranular zu steuern.

Beachten Sie bei der Konfiguration einer SNMPv3-Gruppe folgendes:

- Der Gruppenname kann frei gewählt werden.
- Geben Sie vorab definierte Views (siehe Abschnitt **SMNPv3-View**) an, auf die Gruppenmitglieder Zugriff erhalten sollen. Indem Sie die Views unter „Read View“, „Write View“ oder „Notify View“ eintragen, können Sie steuern, welche Art von Zugriff auf die in der SNMP-View definierten SNMP-Objekte gewährt wird.
- Vergeben Sie ein Security-Level, das die Mindestanforderung an die Benutzerauthentifizierung definiert. Das für einen User definierte Security-Level muss gleich oder höher liegen als das Security-Level der Gruppe; anderenfalls werden SNMP-Anfragen abgelehnt. Die verschiedenen Level sind im Abschnitt **SMNPv3-User** in **Tabelle 26** beschrieben.

Beispielansicht (WBM)

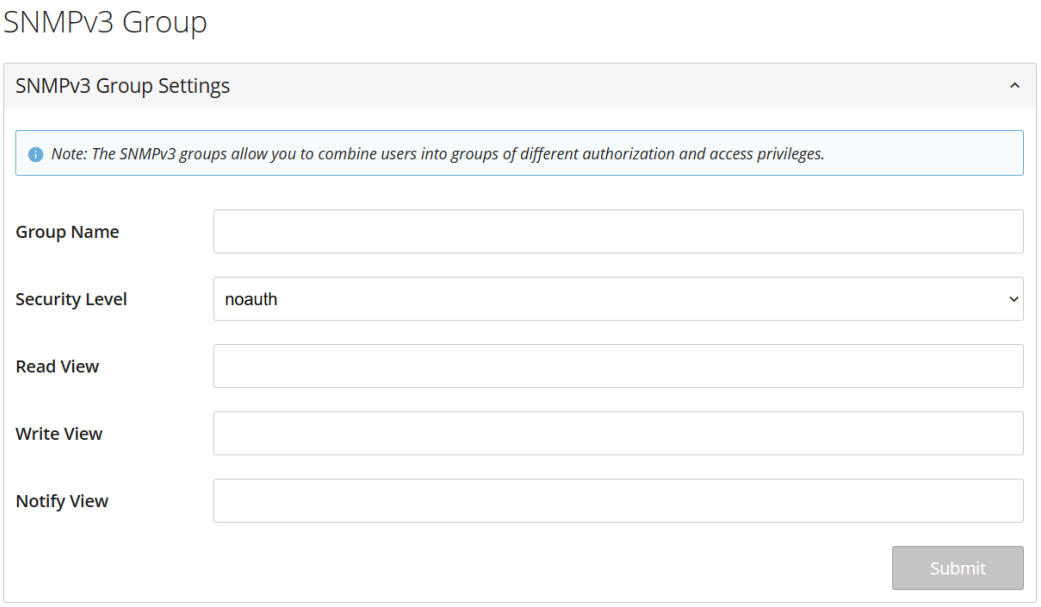


Abbildung 21: SNMP – SNMPv3-Group

HINWEIS

Sollte eine Gruppe mit falscher Berechtigung angelegt worden sein, muss die Gruppe gelöscht und neu angelegt werden.

CLI-Befehle

Tabelle 25: SNMPv3 Group CLI

Befehl	Node
`show snmp group`	enable
`snmp group ... noauth ...`	configure
`snmp group ... auth ...`	configure
`snmp group ... priv ...`	configure

3.4.5.7 SMNPv3-User

Hier können SNMPv3-Benutzer angelegt und bereits angelegten Gruppen zugeordnet werden. Für anzulegende Benutzer kann zwischen drei Sicherheitsstufen (noauth, auth und priv) gewählt werden.

Tabelle 26: Übersicht über die für Benutzer einstellbaren Sicherheitsstufen

Parameter	Beschreibung
noauth	Keine Authentifizierung, keine Verschlüsselung
auth	Authentifizierung, aber keine Verschlüsselung
priv	Authentifizierung und Verschlüsselung

Beispielansicht (WBM)

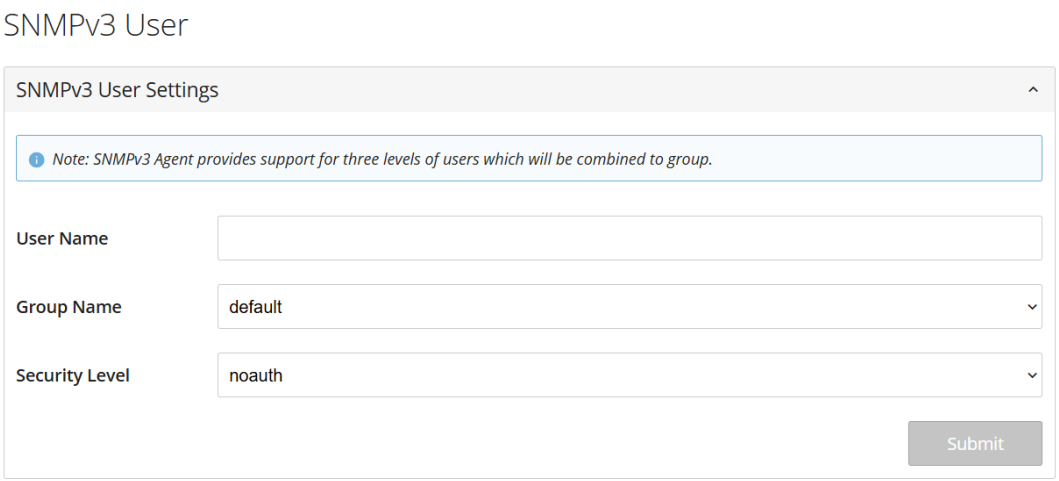


Abbildung 22: SNMP – SNMPv3-User

- Um einen Benutzer anlegen zu können, müssen entsprechende Vorbedingungen geschaffen werden.

  Daher ist es empfehlenswert, zunächst eine View einzurichten, dann eine Gruppe zu erstellen, der die View zugeordnet wird und erst dann den Benutzer einzurichten, dem eine Gruppe zugeordnet werden kann.

Tabelle 27: Übersicht über die angelegten User und zugehörige Einstellungen

Parameter	Beschreibung
User Name	Bezeichnung des Benutzers
Group Name	zugewiesene Benutzergruppe
Auth Protocol	gewählter Authentifizierungsalgorithmus
Priv Protocol	gewählter Verschlüsselungsalgorithmus
Row Status	Hier kann der aktuelle Status des Benutzers abgelesen werden. Sollte hier nicht „Active“ stehen, kann der angezeigt Status bei der Fehleranalyse helfen.

CLI-Befehle

Tabelle 28: SNMPv3 CLI

Befehl	Node
`show snmp user`	enable
`snmp user ... noauth`	configure
`snmp user ... auth ...`	configure
`snmp user ... priv ...`	configure

3.4.6 Systemmanagement

Im Systemmanagement werden, neben allgemeinen Einstellungen zur Verwaltung des Switches, auch die Uhrzeitsynchronisation und Nutzeraccounts konfiguriert.

3.4.6.1 General Set-up

Konfiguration des Switch-Managements.

TCP/IP Configuration

Beispielansicht (WBM)

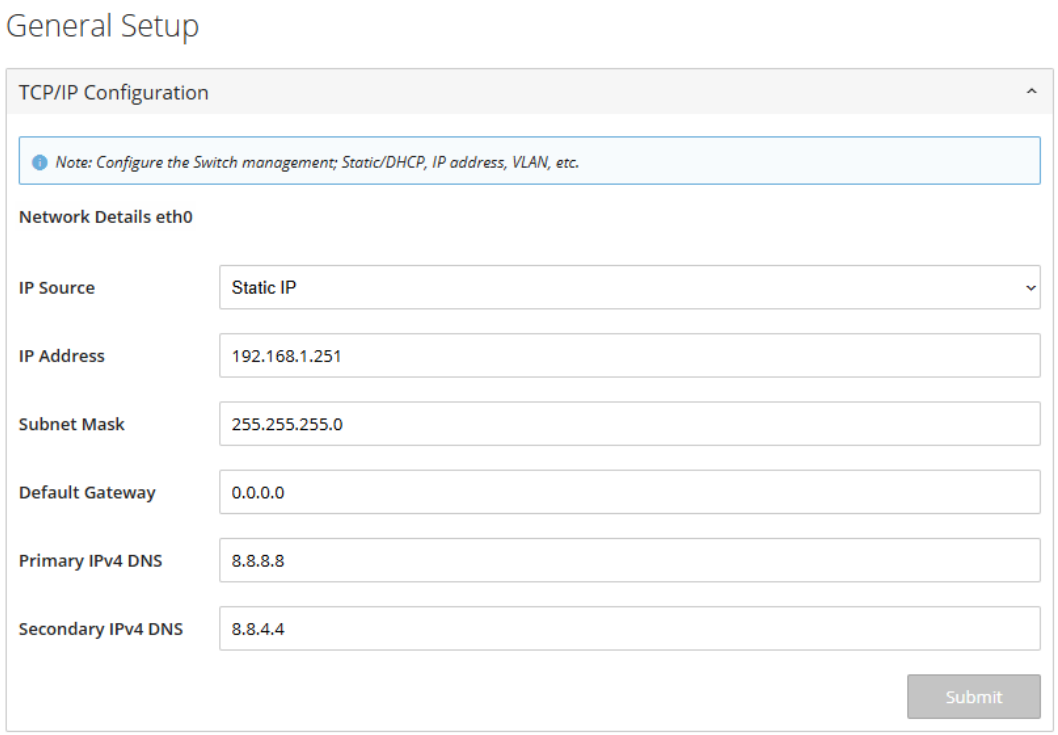


Abbildung 23: General Set-up – TCP-IP-Configuration

Hostname

Beispielansicht (WBM)

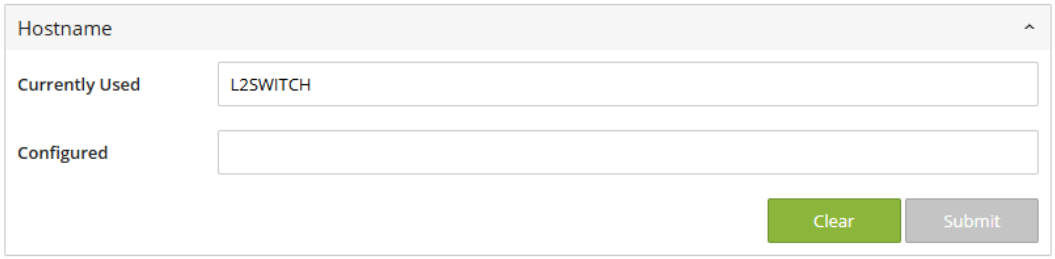


Abbildung 24: General Set-up – Hostname

Management-VLAN

Ein Management-VLAN definiert das VLAN, über das die Managementschnittstellen des Switches (z. B. WBM, CLI, SNMP) erreichbar sind. Dadurch wird der Management-Traffic von regulärem Datenverkehr logisch getrennt. Die Isolation verbessert die Zugriffskontrolle, reduziert potenzielle Störungen durch Nutzlastverkehr und ermöglicht eine gezielte Absicherung des Managementzugangs, z. B. durch ACLs oder dedizierte Layer-3-Segmente.

Beispielansicht (WBM)



Abbildung 25: General Set-up – Managed VLAN

3.4.6.2 SNTP

Neben der manuellen Konfiguration der Uhrzeit kann der Switch seine Systemzeit auch über SNTP mit der koordinierten Weltzeit (UTC) synchronisieren. Die empfangene Zeitinformation wird gemäß der konfigurierten Zeitzone angepasst. Bei ausbleibender Antwort sendet der Switch ohne zeitliche Begrenzung alle 10 Sekunden eine erneute Anfrage an den Zeitserver. Nach erfolgreichem Empfang einer SNTP-Antwort erfolgt die erneute Zeitsynchronisation im Stundenintervall. Änderungen an Zeitzone oder SNTP-Server initiieren eine sofortige Wiederholung des Abfrageprozesses. Werkseitig ist kein SNTP-Server voreingestellt.

Der Standard-Port ist UDP/123.

Beispielansicht (WBM)

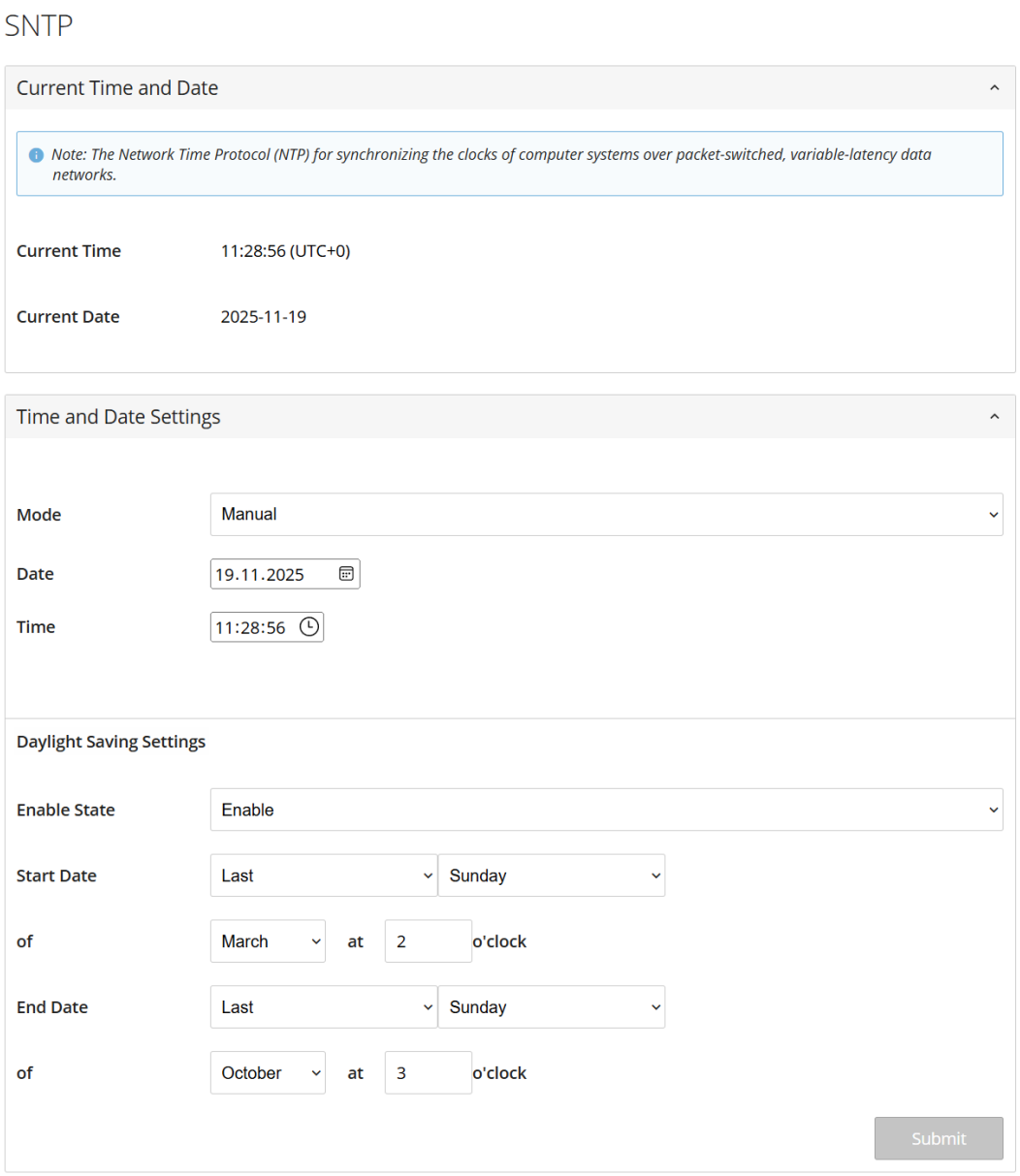


Abbildung 26: SNTP

- Im Beispiel sind Datum und Uhrzeit manuell konfiguriert worden.
- Wird der Modus auf „Network Time Protocol“ konfiguriert, kann ein öffentlicher Server ausgewählt werden, von dem die Zeit bezogen werden. Alternativ können die Servereinstellungen auch manuell eingegeben werden. Unter „Time Zone“ muss im Format hh:mm der Zeitunterschied zwischen UTC und der eigenen Zeitzone eingestellt werden.
- Bei aktivierten Daylight-Saving-Settings können Start und Ende der Sommerzeit über entsprechende Datums- und Uhrzeitangaben konfiguriert werden.

CLI-Befehle

Tabelle 29: SNTP CLI

Befehl	Node
`show time`	enable
`time …`	configure
`time date …`	configure
`time daylight-saving-time`	configure
`time daylight-saving-time start-date ... ... ... ...`	configure
`time daylight-saving-time end-date ... ... ... ...`	configure
`time ntp-server ...`	configure
`time ntp-server ...`	configure
`time timezone ...`	configure

3.4.6.3 User Account

Der Switch unterstützt die Konfiguration von bis zu sechs Benutzerkonten. Benutzernamen müssen alphanumerisch sein. Das letzte verbleibende Administratorkonto ist nicht löschbar. Der Zugriff auf CLI oder Web-Based-Management erfordert eine Authentifizierung über ein gültiges Benutzerkonto.

Beispielansicht (WBM)

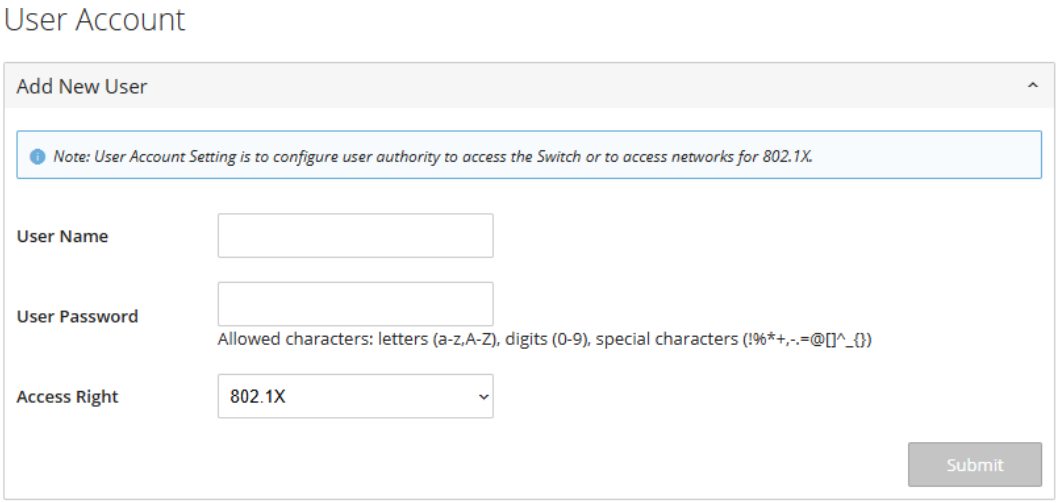


Abbildung 27: User Account – Add New User

Tabelle 30: Übersicht über die angelegten User und zugehörige Berechtigungen

Parameter	Beschreibung
User x/Name	User-Nummer und Username (bestehend aus bis zu 32 alphanumerischen Zeichen)
Access Right	Hier kann die Art des jeweiligen Benutzerkontos abgelesen werden. Sollten dem Benutzer die falschen Berechtigungen zugewiesen worden sein, kann dies über die Schaltfläche „Edit“ aktualisiert werden. • Normal (Read Only): Benutzer können Einstellungen des Switches überprüfen, jedoch keine Änderungen vornehmen. • Admin: Der Benutzer erhält einen Vollzugriff auf sämtliche Einstellungs-möglichkeiten des Switches. • 802.1x: Benutzerkonto, das Konfigurationseinstellungen weder einsehen noch ändern kann. Wenn IEEE802.1X (siehe **802.1X**) mit lokaler Authentifzierung konfiguriert ist, kann ein Supplicant die Zugangsdaten verwenden, um Netzwerkzugang zu erhalten. Wenn bei einem bestehenden Benutzerkonto die Schaltfläche „Edit“ betätigt wird, werden die Felder im Bereich „Add New User“ vorausgefüllt und die Rechte können entsprechend angepasst werden. Wenn lediglich das Passwort geändert wird, bleibt der aktuelle User bestehen und wird mit dem eingegebenen Passwort gespeichert. Für den Fall, dass Benutzername und/oder Rechte geändert wurden, bleibt der ursprüngliche Benutzer bestehen und es wird zusätzlich ein neues Konto angelegt. Der ursprüngliche Benutzer sollte dann gelöscht werden.

CLI-Befehle

Tabelle 31: User Account CLI

Befehl	Node
`show user account`	enable
`add user ...`	configure
`delete user ...`	configure

3.4.6.1 Reset-Button

Über diese Einstellmöglichkeit lässt sich der Reset-Taster des Switches deaktivieren, um eine ungewollte Betätigung zu verhindern.

Weitere Informationen zum Zurücksetzen des Switches finden Sie im Abschnitt **Zurücksetzen auf Werkseinstellungen**.

HINWEIS

Das Menü „Reset Button“ ist nur beim Lean-Managed-Switch mit der Artikelnummer 852-1832 vorhanden. Beachten Sie, dass der Switch bei einer Deaktivierung des Reset-Tasters und verlorenen Zugangsdaten nicht mehr auf die Werkseinstellungen zurückgesetzt werden kann.

CLI-Befehle

Tabelle 32: Reset-Button CLI

Befehl	Node
`show reset-button`	enable
`reset-button ...`	configure

3.4.7 Storm Control

Durch versehentliche oder böswillige Handlungen kann es zum massenhaften Versand verschiedener Pakettypen im Netzwerk kommen. Storm-Control kann dabei helfen, die negativen Auswirkungen eines massenhaften Versands von Broadcast-, Multicast- und Destination-Look-up-Failure-Paketen (DLF) zu begrenzen, indem es Pakete dieser Typen oberhalb eines festgelegten Grenzwertes pro Sekunde verwirft. Dies hilft dabei, die Ressourcen der Netzwerkperipherie zu schützen.

Die Standardgrenze beträgt 300 Pakete/s für DLF und 1000 Pakete/s für Broadcast. Multicast-Pakete werden unbegrenzt übertragen. Der maximal konfigurierbare Grenzwertwert liegt jeweils bei 5000 Paketen pro Sekunde. Das Feature lässt sich für bestimmte Ports bzw. Pakettypen deaktivieren, indem als Grenzwert 0 konfiguriert wird.

HINWEIS

Einstellungen ändern bei Fehlverhalten

Wenn im Netzwerk ein Fehlverhalten von Diensten festgestellt wird, kontrollieren Sie, ob die Einstellung für die jeweilige Art von Datenstrom ggf. zu konservativ gewählt wurde. Einige Dienste nutzen beispielsweise Broadcast-Pakete exzessiv, sodass der Default-Grenzwert bereits im Normalbetrieb überschritten wird.

Beispielansicht (WBM)

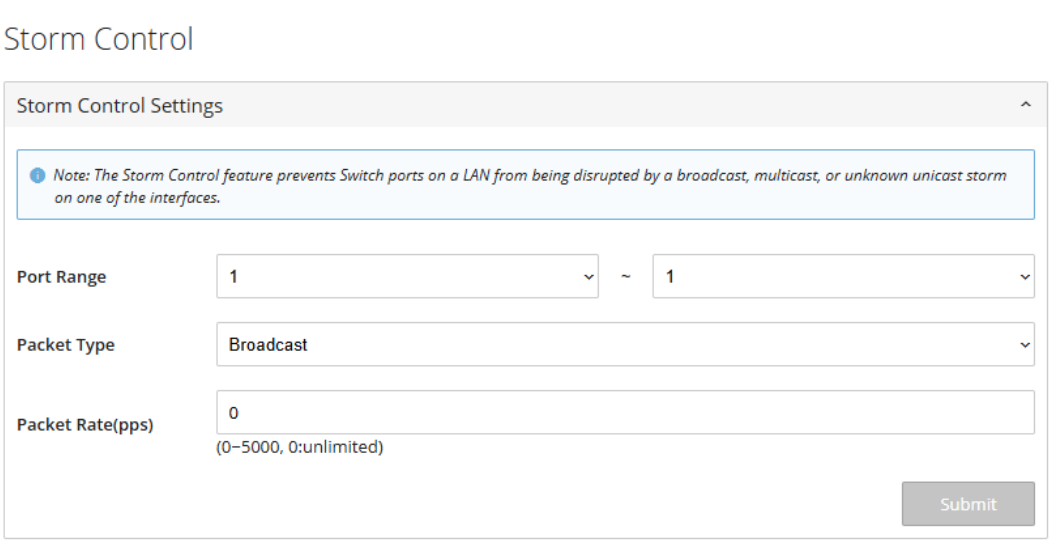


Abbildung 28: Storm-Control – Settings

CLI-Befehle

Tabelle 33: Storm-Control CLI

Befehl	Node
`show storm-control`	enable
`storm-control rate ... type ... ports ...`	configure
`no storm-control type ... ports ...`	configure
`deny ...`	configure

3.4.8 Wizard

Der Wizard stellt eine Assistenzfunktion für die Ersteinrichtung des Switches dar.

Weitere Informationen dazu finden Sie im Abschnitt **In Betrieb nehmen**.

Beispielansicht (WBM)

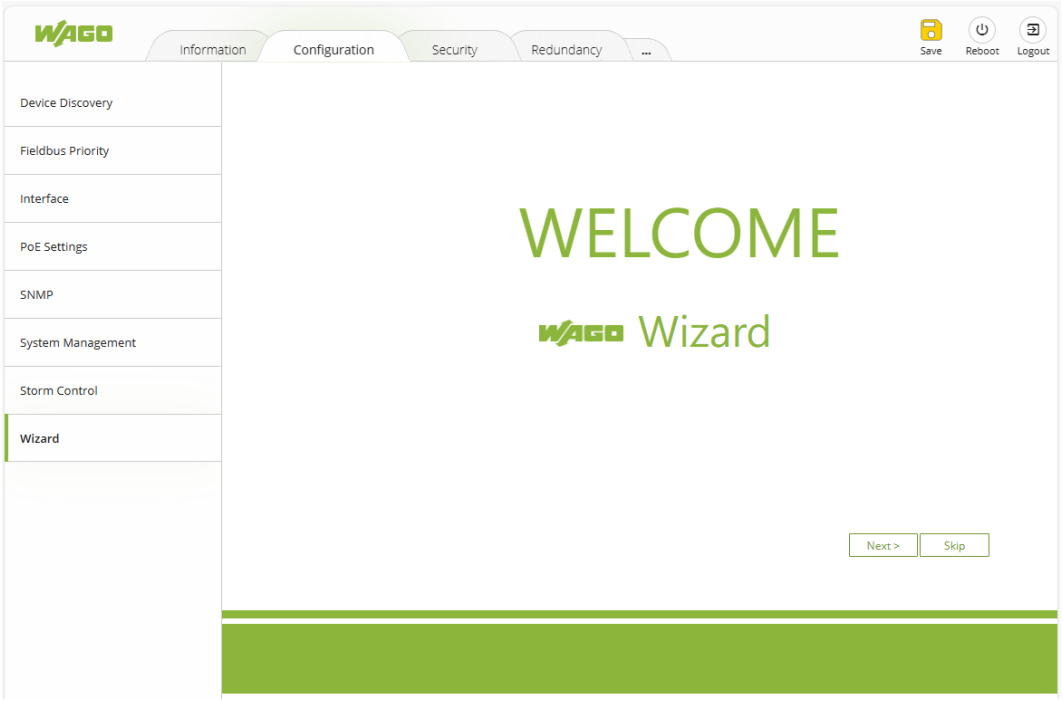


Abbildung 29: Wizard

3.5 Tab Security im WBM

3.5.1 802.1X

Das Netzwerkprotokoll IEEE 802.1X kann die Sicherheit im Netzwerk erhöhen, indem Geräte, die über den Switch kommunizieren möchten, sich zuvor authentifizieren müssen. Die Authentifizierung erfolgt über die Interaktion zwischen Supplicant (Client), Authenticator (Switch) und Authentication Server (Switch bzw. RADIUS-Server). Der physische Port eines Switches wird bis zum erfolgreichen Abschluss der Authentifizierung nur für den Austausch von Authentifizierungsinformationen freigegeben. Es gibt zwei Authentifizierungsverfahren, die sich bezüglich des Speicherorts der Authentifizierungsinformationen unterscheiden:

- Bei lokaler Speicherung werden die Benutzer mit dem Zugriffrecht 802.1X in der lokalen Benutzerkontendatenbank des Switches (weitere Informationen dazu im Abschnitt: **User Account**) zur Authentifizierung von verbundenen Netzwerkgeräten genutzt. Die Anzahl der Konten, die gleichzeitig nebeneinander bestehen können, ist hierbei auf 6 begrenzt. Der Switch unterstützt das MD5-Challenge-Verfahren als Methode für die Netzwerk-authentifizierung.
- Alternativ kann ein im Netzwerk erreichbarer RADIUS-Server zur Authentifizierung von Netzwerkgeräten verwendet werden. Bei RADIUS-Servern ist die Anzahl der Konten, die zur Authentifizierung erstellt werden können, prinzipiell unbegrenzt. Zudem bieten RADIUS-Server erweiterte Möglichkeiten, etwa in Bezug auf Protokollierungsfunktionen oder bei der Definition von Eigenschaften, die ein Netzwerkteilnehmer erfüllen muss. Ebenfalls besteht die

Möglichkeit komplexere Netzwerkauthentifizierungsverfahren als MD5 zu verwenden.

3.5.1.1 Global Set-up

- Im Menü „Global Setup“ wird das Authentifizierungsverfahren konfiguriert. Bei Verwendung des Verfahrens „RADIUS“ sind Verbindungsinformationen der Server anzugeben. Beim Authentifizierungsverfahren RADIUS wird der primäre RADIUS-Server für alle Authentifizierungsanfragen verwendet. Der sekundäre RADIUS-Server (Back-up-Server) kommt nur zum Einsatz, wenn der primäre RADIUS-Server ausfällt.

ⓘ HINWEIS

Shared Keys

Die Passwörter für die Verbindung zum jeweiligen RADIUS-Server (Shared Key) können aus bis zu 32 alphanumerischen Zeichen bestehen und sind vor unberechtigtem Zugriff zu schützen. Der Shared Key auf dem jeweiligen externen RADIUS-Server und dem Switch müssen identisch sein.

Beispielansicht (WBM)

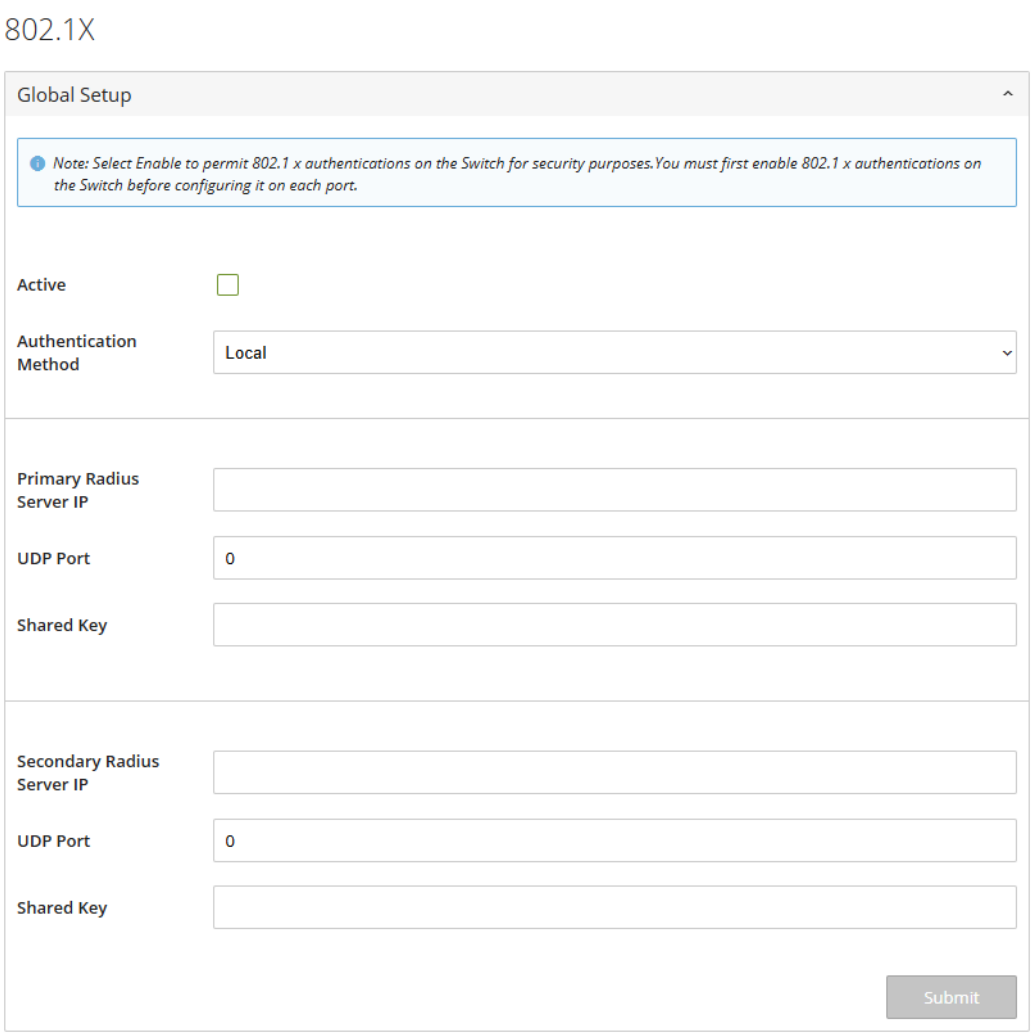


Abbildung 30: 802.1X – Global Set-up

3.5.1.2 Port-Set-up

In diesem Menü lassen sich portspezifische Einstellungen für die 802.1X-Authentifizierung vornehmen.

Beispielansicht (WBM)

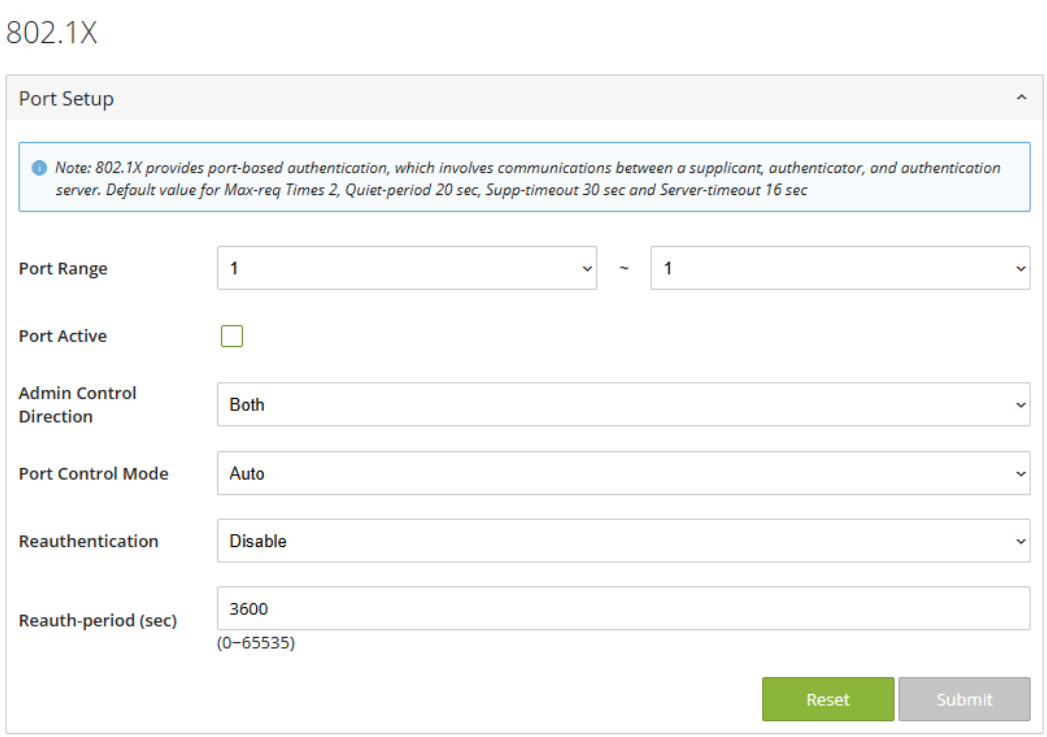


Abbildung 31: 802.1X – Port-Set-up

Tabelle 34: Übersicht über die konfigurierten Authentifizierungsmethoden an den jeweiligen Ports

Parameter	Beschreibung
Admin Control Direction	Angabe, ob nach einer fehlgeschlagenen Authentifizierung eines Nutzers Daten in beide Kommunikationsrichtungen (am Port eingehende und ausgehende Datenpakete) verworfen werden sollen oder nur eingehende Datenpakete.
Port-Control-Mode	Angaben zum Modus der Portkontrolle „Force Unauthorized“ sollte gewählt werden, wenn eine permanente Verweigerung der Authentifizierung für den Port erzwungen werden soll. Dadurch können an diesem Port keine Pakete weitergeleitet werden. Wird „Force Authorized“ gewählt, wird der Port dauerhaft in den autorisierten Zustand versetzt. Dadurch wird die Authentifizierung umgangen und der Port verhält sich wie ein regulärer Access-Port.
Reauthentication	Angabe, ob der Supplicant (Client) regelmäßig erneut den Benutzernamen und das Passwort übermitteln muss, um über den Port Daten austauschen zu können
Reauth-period (sec)	Angabe des Zeitintervalls, nach dem der Supplicant den Benutzernamen und das Passwort erneut übermitteln muss, um weiterhin über den Port Daten austauschen zu können

HINWEIS

Gast-VLANs können nur via CLI konfiguriert werden.

Für die Einbindung nicht authentifizierter Geräte kann ein Gast-VLAN eingerichtet werden.

Clients, deren Authentifizierung scheitert, werden diesem Gast-VLAN zugewiesen. Die Möglichkeiten im Gast-VLAN können bspw. derart eingeschränkt werden, dass nur ein Client für die 802.1X-Authentifizierung heruntergeladen werden kann oder es wird lediglich ein Zugriff auf öffentlich verfügbare Ressourcen gewährt.

- Wenn die Authentifizierung fehlschlägt, kann ein Problem mit der Konfiguration der kryptografischen Protokolle vorliegen. In diesem Fall sollte kontrolliert werden, ob die vom Supplicant (Client) und dem Authentication-Server (RADIUS) unterstützten Protokolle kompatibel sind. Mögliche Protokolle sind:

CLI-Befehle

Tabelle 35: 802.1X CLI

Befehl	Node
`show dot1x`	enable
`show dot1x username`	enable
`show dot1x accounting-record`	enable
`dot1x authentication ...`	configure
`dot1x authentic-method ...`	configure
`no dot1x authentic-method`	configure
`dot1x radius primary-server-ip ... port ...`	configure
`dot1x radius primary-server-ip ... port ... key ...`	configure
`dot1x radius secondary-server-ip ... port ...`	configure
`dot1x radius secondary-server-ip ... port ... key ...`	configure
`no dot1x radius secondary-server-ip`	configure
`dot1x username ... passwd ...`	configure
`no dot1x username ...`	configure
`dot1x accounting ...`	configure
`dot1x guest-vlan ...`	configure
`no dot1x guest-vlan`	configure
`dot1x admin-control-direction ...`	interface
`dot1x default`	interface
`dot1x max-req ...`	interface
`dot1x port-control ...`	interface
`dot1x authentication ...`	interface
`dot1x reauthentication ...`	interface
`dot1x timeout quiet-period`	interface
`dot1x timeout server-timeout`	interface
`dot1x timeout reauth-period`	interface
`dot1x timeout supp-timeout`	interface
`dot1x guest-vlan ...`	interface

3.5.1.3 Port-Status

Der Port-Status gibt einen Überblick über den IEEE 802.1X-Authentifizierungszustand jedes einzelnen Ports.

3.5.2 ACL

Häufig ist es gewünscht den Zugang zum Netzwerk auf bestimmte Teilnehmer oder Dienste zu begrenzen. Hierbei hilft eine ACL (Access Control List), indem diese die Möglichkeit bereitstellt, die Übertragung definierter Pakete im Netzwerk zu kontrollieren. Die Zugriffkontrolle über ACL ermöglicht es, Datenpakete anhand definierter Bedingungen (Filter) entweder zu verwerfen (Blacklist) oder für die Datenübertragung zuzulassen (Whitelist). Bedingungen können im WBM z. B. für die IP- und/oder MAC-Adresse erstellt werden; erweiterte Filtermöglichkeiten stehen im CLI bereit. Die Bedingungen einer ACL-Regel werden logisch verundet, müssen also alle erfüllt sein, damit die definierte Aktion auf ein Datenpaket angewendet wird. Treffen die Filter mehrerer ACL-Regeln auf ein Datenpaket zu, wird die Aktion (verwerfen/weiterleiten) der Regel ausgeführt, die zuletzt hinzugefügt wurde (in der Liste der ACL-Regeln am weitesten unten).

Sind Whitelist-ACLs definiert und es trifft keine der Regeln zu, wird das Paket nicht weitergeleitet. Sind lediglich Blacklist-Regeln erstellt worden und es trifft keine der Regeln zu, wird das Datenpaket weitergeleitet. Bis zu 32 Regeln können definiert werden.

ⓘ HINWEIS

Gefahr des Zugangsverlusts zur Verwaltungsoberfläche des Switches

Insbesondere bei der Erstellung von Whitelist-Regeln kann es schnell passieren den Zugang zum WBM zu verlieren. Wenn beispielsweise eine erste Whitelist-Regel erstellt wird, die auf eine bestimmte IP-Adresse und Eingangsschnittstelle (Switch-Port) filtert, kann sofort nach dem Erstellen der Regel nur noch über den definierten Port in Kombination mit der definierten IP-Adresse kommuniziert werden, da keine weitere Regel existiert, die einen anderen Datenverkehr zulässt. Aus diesem Grund sollten Sie die Erstellung von ACL-Regeln sorgfältig planen und dokumentieren.

Wenn es dennoch einmal zu der Situation kommt, dass Sie bei der Konfiguration der ACL-Regeln den Zugang zum WBM verlieren, hilft es, den Switch neu zu starten, da hierdurch alle ungespeicherten Einstellungen verloren gehen.

Beispielansicht (WBM)

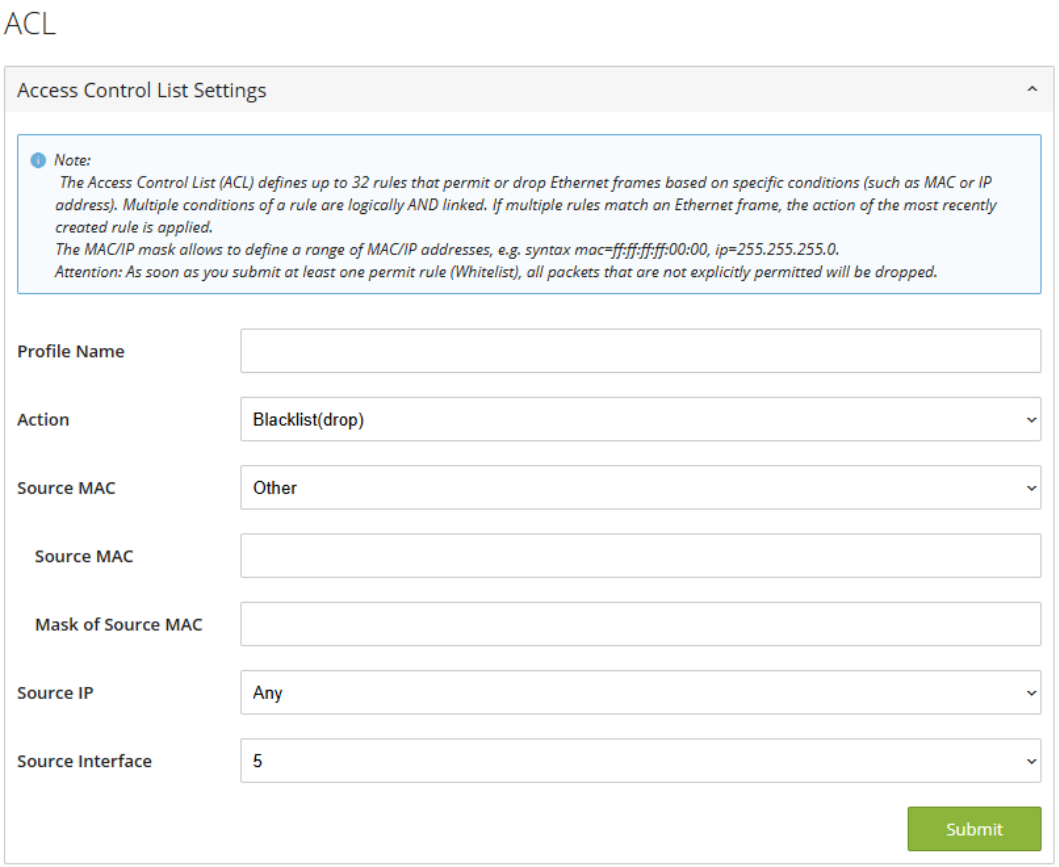


Abbildung 32: Access-Control-List-Settings

- Als Profilname ist ein beliebiger Name zur Identifikation der ACL-Regeln anzugeben.
- Unter „Action“ ist anzugeben, ob die Datenpakete bei einem Zutreffen der Filterregeln verworfen (Blacklist) oder weitergeleitet (Whitelist) werden.
- Als Filterregeln können im WBM die Quell-MAC-Adresse des Absenders, die Quell-IP-Adresse des Absenders und die Schnittstelle (Switch-Port) definiert werden.
- Damit die definierte Action angewendet wird, müssen alle definierten Filterregeln zutreffen.
- Im CLI stehen weitere Filtermöglichkeiten zur Verfügung.

CLI-Befehle

Tabelle 36: ACL CLI

Befehl	Node
`show access-list`	enable
`access-list ...`	configure
`show`	acl
`action ...`	acl
`action dscp remarking ...`	acl
`action 802.1p remarking ...`	acl
`802.1p ...`	acl
`dscp ...`	acl
`destination mac host ...`	acl

`destination mac ...`	acl
`destination mac ...`	acl
`ethertype ...`	acl
`source mac host ...`	acl
`source mac ...`	acl
`source ip host ...`	acl
`source ip ...`	acl
`destination ip host ...`	acl
`destination ip ...`	acl
`l4-source-port ...`	acl
`L4-destination-port ...`	acl
`vlan ...`	acl
`source interface ...`	acl

3.5.3 Port-Security

Unberechtigte Erweiterungen eines Netzwerkes können ein Security-Problem darstellen. Beispielsweise ist es denkbar, dass ein mit dem Switch verbundenes Endgerät unbefugt durch einen weiteren Switch ersetzt wird, um weitere Endgeräte zum Netzwerk hinzuzufügen oder es werden an einem vorhandenen Unmanaged Switch unbefugt weitere Endgeräte angeschlossen. Port-Security wirkt diesem Problem entgegen, indem es die maximale Anzahl an erlaubten (dynamisch gelernten) MAC-Adressen an einem Switch-Port überwacht und begrenzt. Das führt dazu, dass keine zusätzlichen Geräte über den Switch-Port kommunizieren können. Jedes Gerät im Netzwerk besitzt eine individuelle MAC-Adresse.

Port Security ist jedoch anfällig, wenn gezielt ein vorübergehender Link-Down provoziert wird. Nach dem Wiederaufbau des Links muss Port Security die dynamischen MAC-Adressen neu lernen. Es werden immer die MAC-Adressen gelernt, welche zuerst am Port des Switches gesehen wurden, bis die erlaubte Anzahl pro Port erreicht ist. Unter den neu gelernten MAC-Adressen könnte sich jedoch auch die Adresse eines unauthorisierten Gerätes befinden. Sie können dieses Problem durch den zusätzlichen Einsatz von **Port-Security Advanced** umgehen. Alternativ zu Port Security ist der Einsatz von **Sticky MAC Whitelisting** denkbar.

ⓘ HINWEIS

Überprüfung der Adressen

Zur Überprüfung der Anzahl der aktiven MAC-Adressen pro Port kann die MAC-Adress-Tabelle genutzt werden. Diese kann im CLI eingesehen werden:

```
L2SWITCH(config)# show mac-address-table
```

Beispielansicht (WBM)

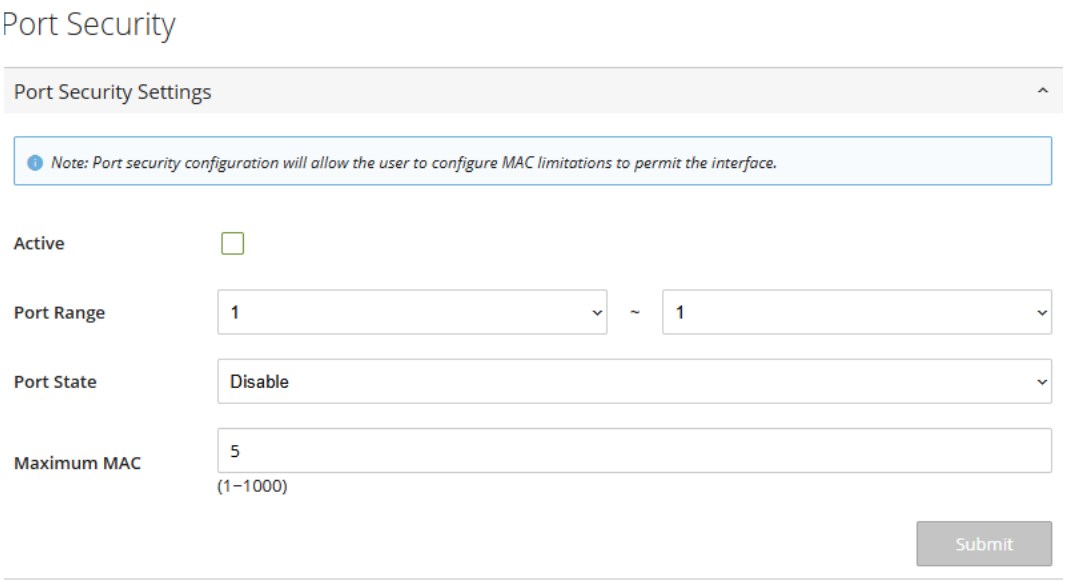


Abbildung 33: Port-Security

- Wenn das konfigurierte MAC-Adressen-Limit erreicht ist, werden Pakete von neuen MAC-Adressen verworfen.
- Statische MAC-Adressen werden berücksichtigt. Bei Aktivierung eines zuvor deaktivierten Ports werden alle gelernten MAC-Adressen dieses Ports gelöscht.

CLI-Befehle

Tabelle 37: Port Security CLI

Befehl	Node
`show port-security`	enable
`port-security ...`	configure
`interface range gigabitethernet1/0/ ...`	configure
`port-security ...`	interface
`port-security limit ...`	interface
`port-security ...`	if-range
`port-security limit ...`	if-range

3.5.4 Port-Security Advanced

Port-Security Advanced ist eine einfach zu verwendende, erweiterte Form der Port-Security. Nach einem Linkdown (z. B. durch ein gezogenes Kabel oder einen Geräteausfall) wird der betreffende Port gesperrt. Die Funktion kann unter anderem dabei helfen, Sicherheitsrisiken zu vermeiden, wenn eine unberechtigte Person versucht, ein vorhandenes Netzwerkgerät durch ein anderes zu ersetzen.

- Wenn ein Port wegen Port-Security Advanced gesperrt wurde, muss er via CLI oder WBM manuell vom Administrator wieder aktiviert werden. Der Administrator sollte vor der Reaktivierung eine Ports die Integrität des Netzwerks überprüfen.
- Port-Security Advanced basiert auf der Lernfunktion des Dashboards. Damit Port-Security Advanced abgezogene Netzwerkkabel erkennt, müssen die Ports angelernt werden. Dies erfolgt durch einen Klick auf die Schaltfläche „Learn“ im Menü „Dashboard Configuration“, siehe **Dashboard-Configuration**. Hierbei merkt sich der Switch, welche Ports aktiv sind.

HINWEIS

Mögliche Beeinträchtigung der Systemverfügbarkeit

Port-Security Advanced erhöht die Netzwerksicherheit, kann aber die Systemverfügbarkeit beeinträchtigen. Beachten Sie daher folgende Hinweise:

- Port-Security Advanced sollte nicht auf Ports aktiviert werden, die zum Aufbau von Netzwerkredundanz (ERPS oder RSTP) verwendet werden.
- Um einen dauerhaften Zugriff auf das Gerät zu ermöglichen, sollte Port-Security Advanced nicht auf Uplink-Ports aktiviert werden.
- Gesperrte Ports können nur vom Administrator freigegeben werden. Hierzu ist eine Anmeldung am Gerät erforderlich.

Beispielansicht (WBM)

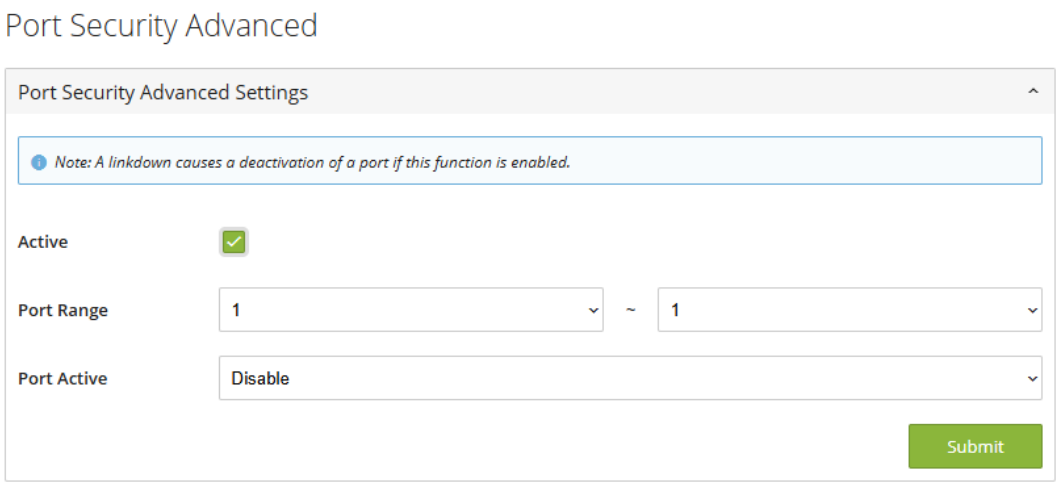


Abbildung 34: Port-Security Advanced

Tabelle 38: Port-Security Advanced Status

Parameter	Beschreibung
Active	Angabe, ob Port-Security Advanced am entsprechenden Port eingeschaltet ist
Monitor	Wenn Port-Security Advanced eine Verbindungsunterbrechung erkannt und den Port deaktiviert hat, wird „Shutdown“ angezeigt, ansonsten „Normal“.
Manual Recovery	Im Falle einer Port-Abschaltung durch Port-Security Advanced kann ein Adminitrator über diese Schaltfläche den Port manuell wieder freigeben.

CLI-Befehle

Tabelle 39: Port Security Advanced CLI

Befehl	Node
`show port-security-adv`	enable
`port-security-adv ...`	configure
`port-security-adv ...`	if-range
`port-registration reset`	if-range
`port-registration learn`	if-range

3.5.5 Sticky MAC Whitelisting

Sticky-MAC-Whitelisting ist ein Verfahren, das Eigenschaften von **Port-Security** mit Filterregeln, vergleichbar mit einer **ACL**, kombiniert. Nur Netzwerkgeräte, deren MAC-Adressen in der Sticky-MAC-Tabelle eingetragen sind, können über den Switch kommunizieren. Das manuelle Erstellen der Sticky-MAC-Tabelle kann durch einen automatisierten Lernmechanismus vereinfacht werden.

Die gleichzeitige Verwendung von Port Security und Sticky MAC Whitelisting ist nicht vorgesehen. Bei aktiviertem Sticky MAC Whitelisting werden ausschließlich Pakete von den in der Sticky MAC Tabelle hinterlegten MAC-Adressen akzeptiert. Dadurch hat Port Security, welches mit dynamischen MAC-Adressen arbeitet, faktisch keine zusätzliche Wirkung mehr.

HINWEIS

Gefahr des Zugangsverlusts zur Verwaltungsoberfläche des Switches

Die MAC-Adresse des zur Konfiguration des Switches verwendeten Endgerätes muss in der Sticky-MAC-Tabelle enthalten sein. Wenn dies zum Zeitpunkt der Aktivierung des Features Sticky-MAC-Whitelisting nicht der Fall ist, geht der Zugriff zum WBM unmittelbar verloren.

Wenn es dennoch einmal zu der Situation kommt, dass Sie den Zugang zum WBM verlieren, hilft es, den Switch neu zu starten, da hierdurch alle ungespeicherten Einstellungen verloren gehen.

Beispielansicht (WBM)

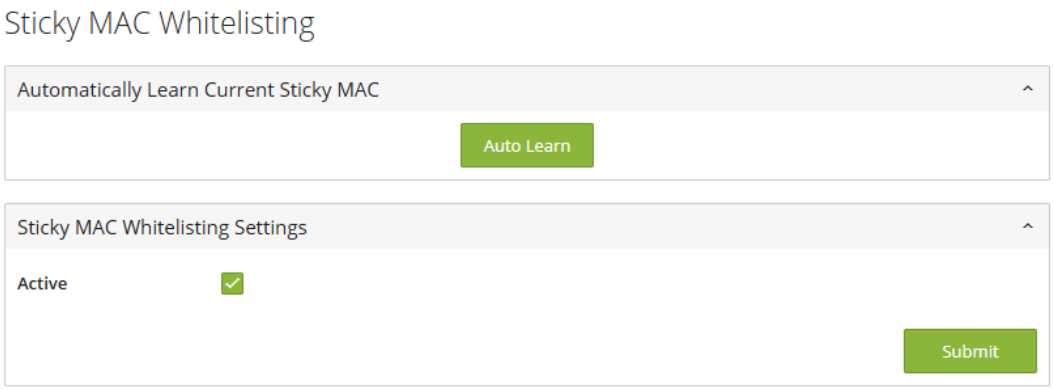


Abbildung 35: Auto-Learn und Aktivierung von Sticky-MAC-Whitelisting

- Die Funktion „Auto Learn“ aktiviert das Sticky-MAC-Whitelisting und fügt alle dem Switch bekannten MAC-Adressen der Sticky-MAC-Tabelle hinzu. Der Switch berücksichtigt hierbei dynamisch gelernte MAC-Adressen in der MAC-Adresstabelle.
- Nach der Ausführung von „Auto Learn“ sollten die Einträge in der Sticky-MAC-Tabelle überprüft werden.

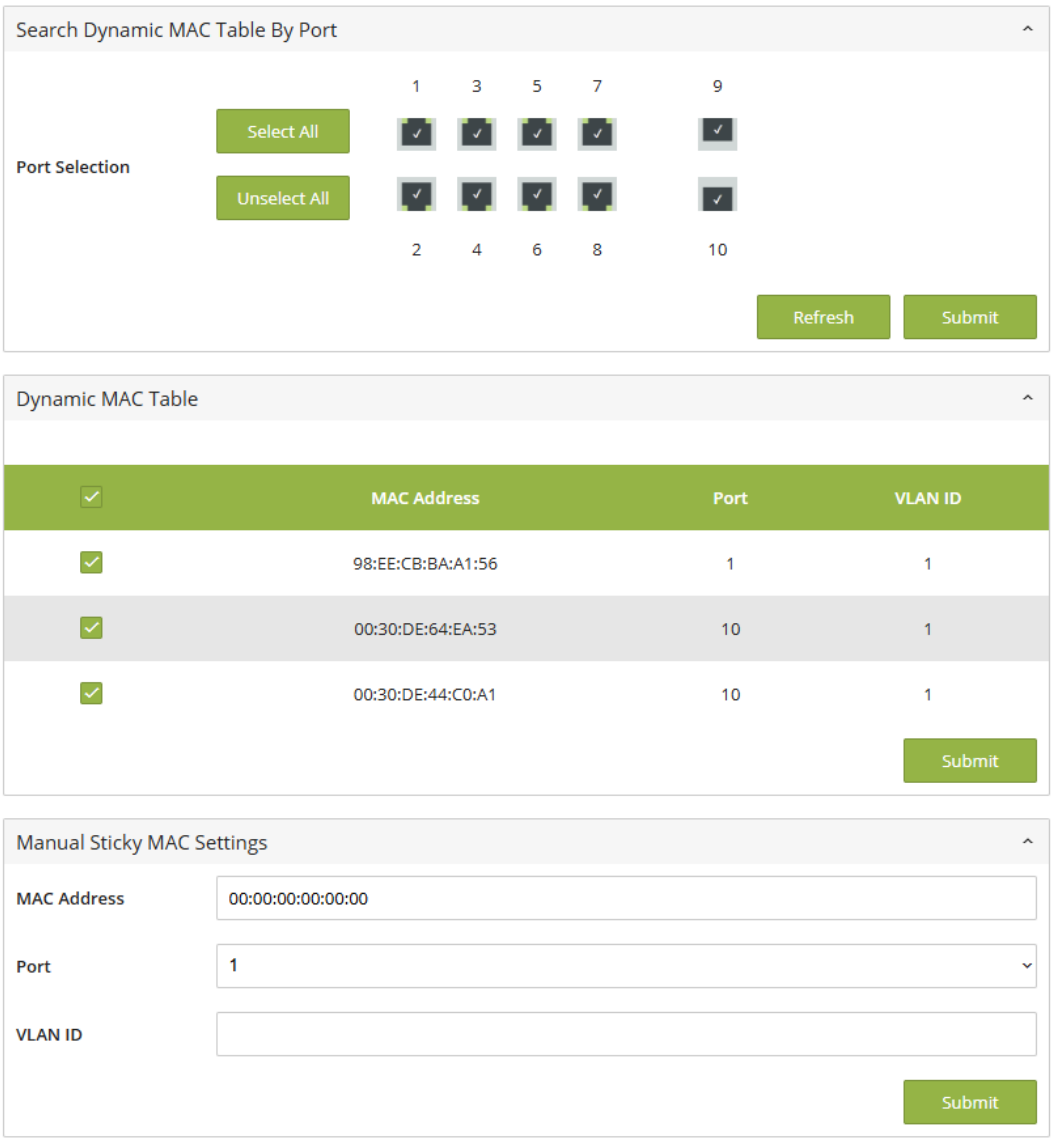


Abbildung 36: Manuelles Hinzufügen von Adressen zur Sticky-MAC-Tabelle

- Eine größere Kontrolle beim Anlegen der Sticky-MAC-Tabelle ist durch die selektive Auswahl von MAC-Adressen aus der Dynamic-MAC-Tabelle möglich. Eine Vorfilterung ist möglich, indem einzelne oder mehrere Ports in der Suchmaske ausgewählt und mit einem Klick auf „Submit“ bestätigt werden. Möchten Sie die vorherige Auswahl wiederverwenden, genügt ein Klick auf „Refresh“.
- Nach der Aktivierung von Sticky-MAC-Whitelisting können weitere MAC-Adressen jederzeit manuell hinzugefügt werden.

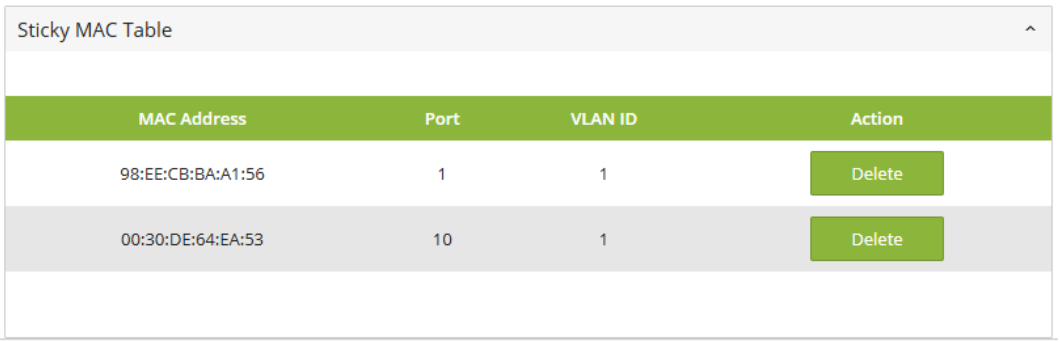


Abbildung 37: Sticky-MAC-Tabelle

- Die Sticky-MAC-Tabelle gibt einen Überblick über alle MAC-Adressen von Geräten, die über den Switch kommunizieren dürfen. Bei Bedarf können einzelne Einträge entfernt werden.

CLI-Befehle

Tabelle 40: Sticky-MAC-Whitelisting CLI

Befehl	Node
`show sticky-mac-whitelisting`	enable
`sticky-mac-whitelisting ...`	configure
`sticky-mac-whitelisting auto-learn`	configure

3.5.6 Service-Control

Die vom Switch bereitgestellten Dienste wie etwa HTTP, HTTPS, SNMP v1/v2c, SNMP v3 oder SSH können hier konfiguriert werden.

Beispielansicht (WBM)

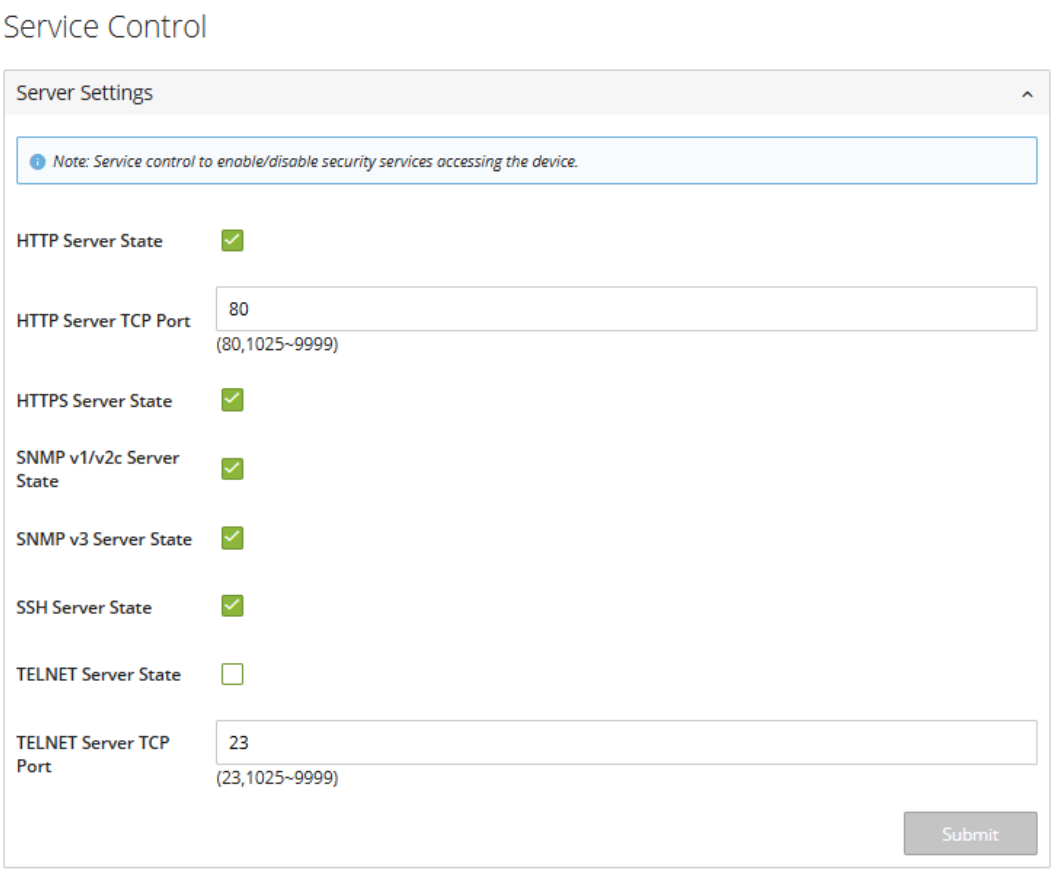


Abbildung 38: Service-Control

CLI-Befehle

Tabelle 41: Service-Control CLI

Befehl	Node
`show server status`	enable
`ssh server`	configure
`telnet server`	configure
`SNMPv1/v2c`	configure
`SNMPv1/v2c`	configure
`SNMPv3`	configure
`SNMPv3`	configure
`web server`	configure

3.5.7 VLAN

3.5.7.1 Port-Isolation

Port-Isolation ermöglicht, die Switch-Ports virtuell in Domänen zu unterteilen. Eine Datenvermittlung zu einem Port, der nicht derselben Domäne angehört, wird unterbunden. Möglicherweise vorhandene VLAN-Tags der Datenpakete werden ignoriert.

Die Konfiguration der Port-Isolation erfolgt, indem für jeden Port individuell festgelegt wird, an welche der weiteren Ports empfangene Daten weitergeleitet werden können. Ein Port, der als Weiterleitungsziel konfiguriert werden kann, wird als Egress-Port bezeichnet. Der Port 0 (CPU) nimmt hierbei eine Sonderrolle ein und repräsentiert die Managementschnittstelle des Switches. Damit ein Endgerät, das mit einem spezifischen Port des Switches verbunden ist, den Switch verwalten kann (WBM, CLI, SNMP), muss für diesen Port der Egress-Port 0 (CPU) aktiviert sein.

Beispielansicht (WBM)

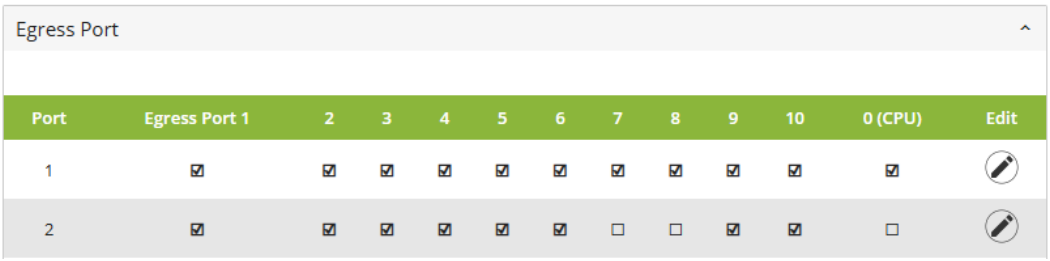


Abbildung 39: Port-Isolation

- Im oben gezeigten Beispiel ist eine Weiterleitung der an Port 1 eingehenden Daten an alle anderen Ports des Switches möglich.
- Eine Weiterleitung der an Port 2 eingehenden Daten ist an Port 7 und 8 nicht möglich. Darüber hinaus kann ein Endgerät an Port 2 den Switch nicht verwalten.

CLI-Befehle

Tabelle 42: Port-Isolation CLI

Befehl	Node
`show port isolation`	enable
`port-isolation ...`	interface
`no port-isolation`	interface

3.5.7.2 VLAN-Set-up

Der Switch erlaubt eine Unterteilung des physischen Netzwerks in virtuelle Netzwerke gemäß Standard IEEE 802.1Q. Ohne Erweiterung der physischen Verkabelung und Anschaffung weiterer Netzwerkinfrastruktur-Hardware können so mehrere Netzwerke geschaffen werden, die sich verhalten wie physikalisch vollkommen getrennte Netzwerke. Durch die Konfiguration in Software ist zudem eine Anpassung des Netzwerks aus der Ferne möglich. Die Zuordnung eines Endgerätes zu einem virtuellen Netzwerk erfolgt über die Konfiguration einer Virtual-LAN-ID (VID) für den Switch-Port, mit dem das Endgerät verbunden ist. Ports, an denen ein Endgerät angeschlossen ist, sind hierzu der Rolle „Access“ hinzuzufügen. Werksseitig ist allen Switch-Ports die VID 1 zugeordnet.

Damit Endgeräte miteinander kommunizieren können, müssen diese generell demselben VLAN

zugeordnet sein. Wenn im Einzelfall Verbindungen über die Grenzen eines VLAN hinweg dennoch ermöglicht werden sollen, dann müssen hierzu leistungsfähigere Netzwerkgeräte wie L3-Switche, Router oder Firewalls eingesetzt werden. Lean-Managed-Switches unterstützen diese Funktion nicht, können jedoch mit leistungsfähigeren Netzwerkgeräten kombiniert werden.

Ein virtuelles Netzwerk ist nicht auf einen einzelnen Netzwerk-Switch beschränkt. Eine effiziente Übertragung der Daten aus mehreren VLAN erfolgt zwischen Netzwerkgeräten, die gemäß Standard IEEE 802.1Q arbeiten, durch die Zuordnung einzelner Ports zur Rolle „Trunk“. Damit das empfangende Netzwerkgerät die Daten eines Trunk-Ports einem VLAN eindeutig zuordnen kann, wird vom absendenden Netzwerkgerät jedem Datenpaket ein VLAN-Tag hinzugefügt. Das VLAN-Tag enthält unter anderem die VID.

Daten der Switch-Ports mit der Rolle „Access“ erhalten kein Tag. Aus diesem Grund kann ein Access-Port nur einem VLAN zugeordnet werden. Endgeräte, die mit einem Access-Port verbunden sind, müssen den Standard IEEE 802.1Q nicht unterstützen. Allen Daten, die der Switch über einen Tag-Port empfängt, fügt der Switch automatisch ein Tag hinzu. Vor der Datenübertragung an einem Access-Port wird das Tag entfernt.

WAGO Lean-Managed-Switches können bis zu 5 unterschiedliche VLAN verarbeiten. Als VLAN-ID können Werte zwischen 1 und 4094 definiert werden.

Beispielansicht (WBM)

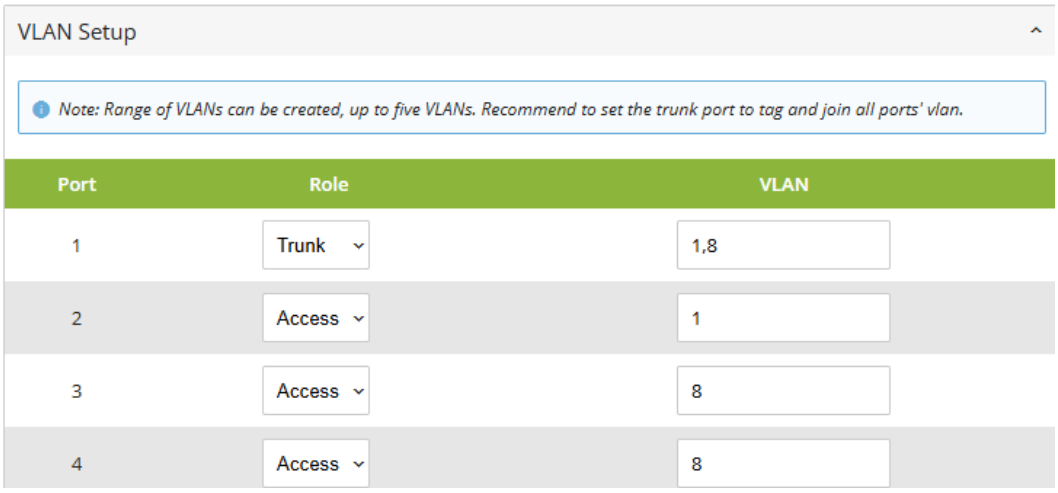


Abbildung 40: VLAN-Set-up

- Ports 2 bis 4 sind mit Endgeräten verbunden.
- Port 1 ist mit einem Netzwerkgerät verbunden (z. B. ein weiterer Switch), der den Standard IEEE 802.1Q unterstützt. Es werden Daten der VLAN 1 und 8 übertragen.
- Die Endgeräte an Port 3 und 4 können untereinander kommunizieren; eine Kommunikation mit dem Endgerät an Port 2 ist aufgrund des abweichenden VLANs nicht möglich.

CLI-Befehle

Tabelle 43: VLAN-Set-up CLI

Befehl	Node
`show vlan ...`	enable
`vlan ...`	configure
`interface range ...`	configure
`vlan range ...`	configure
`acceptable frame type ...`	interface
`pvid ...`	interface
`pvid ...`	if-range
`show`	vlan
`name ...`	vlan
`add ...`	vlan
`fixed ...`	vlan
`tagged ...`	vlan
`untagged ...`	vlan
`...`	vlan-range
`add ...`	vlan-range
`fixed ...`	vlan-range
`tagged ...`	vlan-range
`untagged ...`	vlan-range

3.6 Tab-Redundancy im WBM

Der Ausfall eines Netzwerkes kann zu hohen Ausfallzeiten und Kosten führen. Durch das Hinzufügen von Redundanz kann dieses Risiko verringert werden. Eine redundant ausgeführte Verkabelung kann jedoch schnell zu einer Überlastung des Netzwerkes führen, wenn Datenpakete im Kreis oder einer Netzwerkschleife wiederholt versandt werden. Diesem Problem begegnen die im folgenden vorgestellten Protokolle dadurch, dass Sie redundante Verbindungen verwalten und den Datenübertragungsweg bei Ausfall einer Verbindung automatisch umkonfigurieren.

3.6.1 ERPS

ERPS gemäß ITU-T G.8032 implementiert einen Layer-2-Schutzmechanismus für ETHERNET-Ringtopologien. Schleifen werden durch Blockierung eines definierten Ringabschnittes verhindert, welcher als „Ring Protection Link“ (RPL) bezeichnet wird. Jeweils einer der Switches am Ende des RPL muss als RPL-Owner oder RPL-Neighbor definiert werden.

Der RPL wird im Normalbetrieb für den Datenverkehr blockiert und nur im Fehlerfall durch den RPL-Owner freigegeben. Zu diesem Zweck tauschen sich RPL-Owner und RPL-Neighbor über das Automatic „Protection Switching-Protokoll“ (APS) aus. Jeder Ring – sei es der Hauptring als zentraler Ring oder ein Subring als sekundärer, an den Hauptring angeschlossener Ring – besitzt einen eigenen RPL. Eine gemeinsame Nutzung von R-APS-Kanälen zwischen Ringen ist ausgeschlossen.

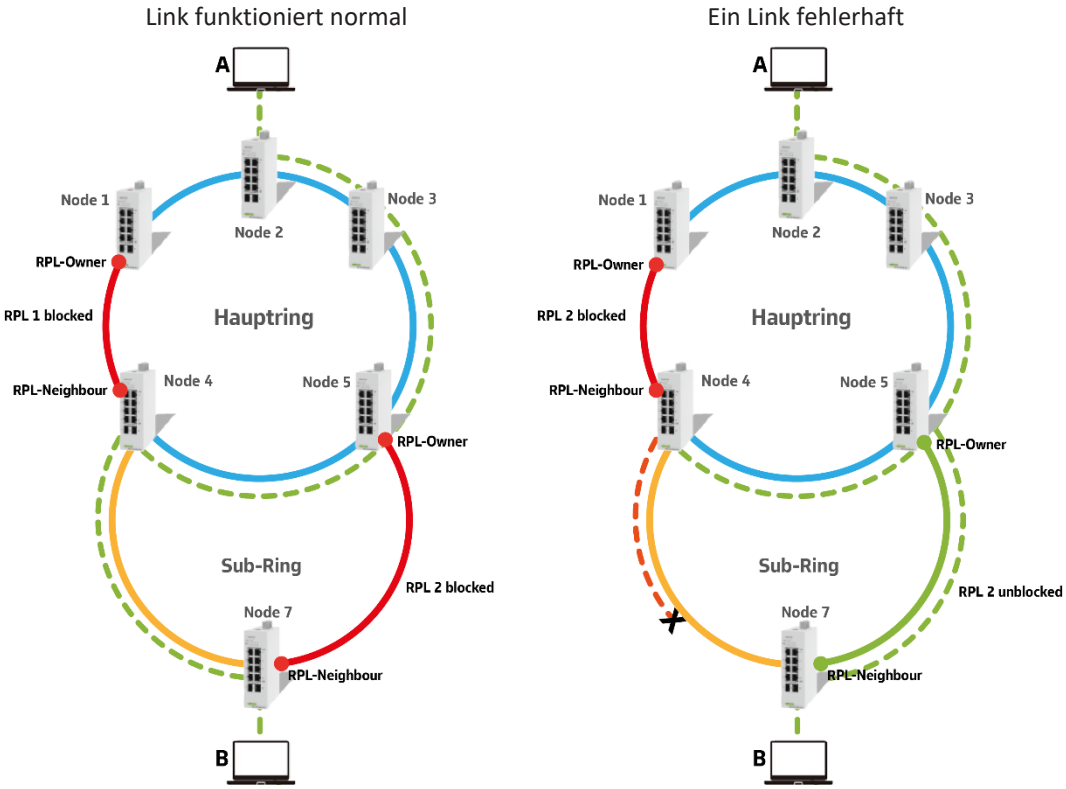


Abbildung 41: ERPS-Funktionsschema

Ein WAGO Lean-Managed-Switch unterstützt bis zu zwei Ringe. Bestandteil eines Rings sollten maximal 16 Nodes (Switche) sein, um Probleme bei der Erkennung des Netzwerkstatus zu vermeiden. Bei einer Gesamtlänge des Rings unter 1200 km können so Umschaltzeiten von < 800 ms (gemäß ITU-T G.808.1) erreicht werden.

VLAN-Struktur

Control-VLAN: Es handelt sich hierbei um ein dediziertes VLAN für ERPS-Steuerdaten. Das im ERPS-Set-up konfigurierte Control-VLAN wird automatisch erstellt. Es sollten dem VLAN keine anderen Ports hinzugefügt werden als die Switch-Ports, die zur Kommunikation im Ring dienen (bezeichnet als Left/Right-Port).

Beispielansicht (WBM)

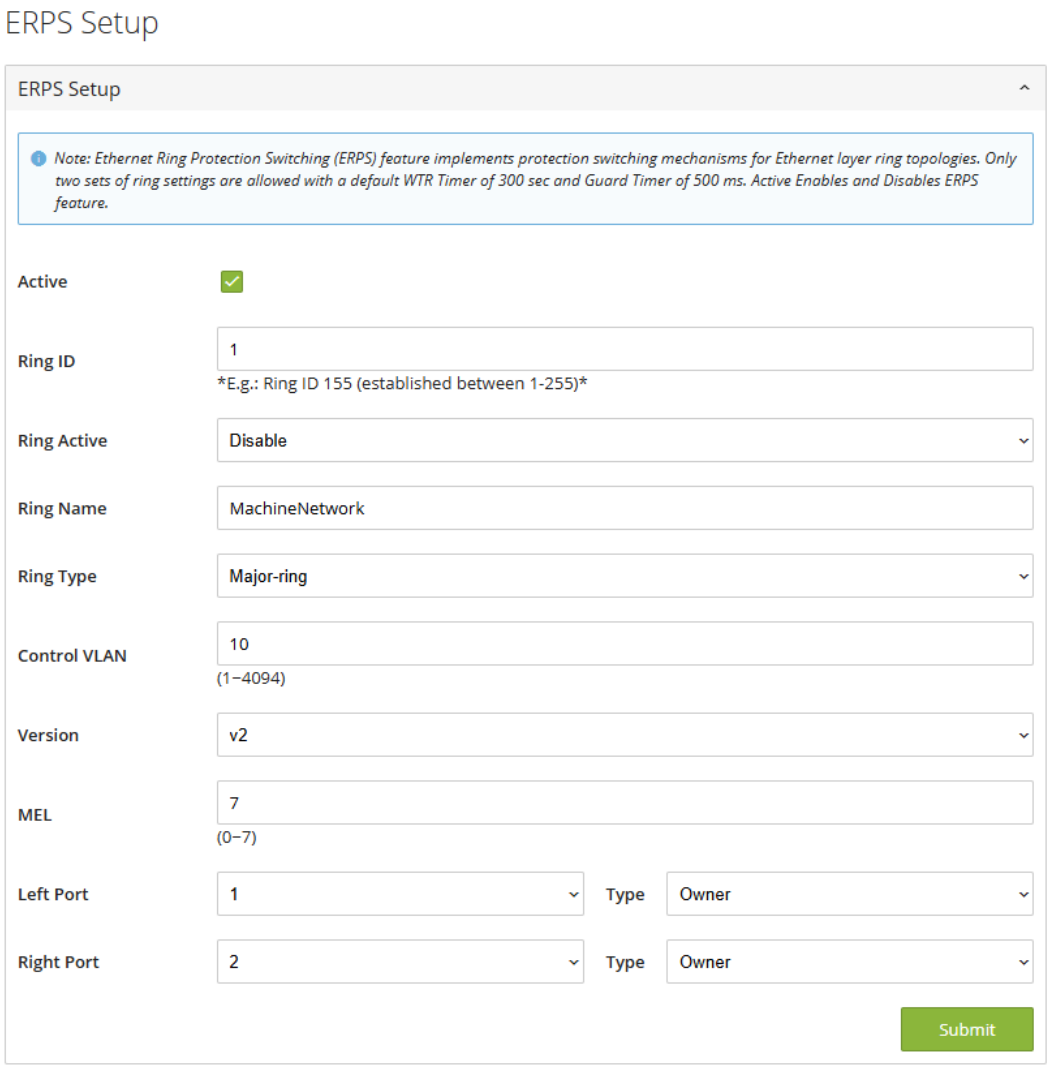


Abbildung 42: ERPS-Set-up

- Die Ring-ID muss auf allen Switches eines Rings identisch sein. Nur so können die Knoten dieselbe ERPS-Domain erkennen, R-APS-Messages korrekt zuordnen und gemeinsam eine konsistente Ringprotektion aufbauen.
- Der Ringname ist ein lokaler, administrativer Bezeichner. Er dient der Identifikation im Management, hat jedoch keine funktionale Relevanz für das ERPS-Protokoll. Eine einheitliche Vergabe ist sinnvoll, aber nicht zwingend erforderlich.
- Es muss ein dediziertes Control VLAN definiert sein, das für die ERPS-Verwaltungs-informationen vorgesehen ist. Dieses Control-VLAN muss auf allen Switches im Ring identisch sein.
- MEL (Maintenance Entity Level) definiert die Hierarchie der OAM-Messages für die Fehler-erkennung und das Monitoring innerhalb eines Rings.
  Möglich sind Werte von 0 bis 7. Höhere Werte kennzeichnen Maintenance-Domains mit höherer Priorität und ermöglichen eine klare Trennung zwischen Customer-, Service-Provider- und Operator-Ebene. So können OAM-Funktionen unterschiedlicher Ebenen unabhängig voneinander ausgeführt werden. Die Werte müssen auf allen Ringteilnehmern abgestimmt sein.
- Den beiden Ports (Links und Rechts), die Mitglieder des ERPS-Rings sind, muss ein Typ

zugewiesen werden: Ein Port im Ring muss als Owner definiert werden, der Port am anderen Ende des Links als Neighbour. Der Link zwischen Owner und Neighbour ist der RPL. Alle anderen Ports des Rings sind als Normal zu konfigurieren.

CLI-Befehle

Tabelle 44: ERPS CLI

Befehl	Node
`show erps`	enable
`show erps instance`	enable
`show erps instance ...`	enable
`erps enable`	configure
`erps ring-id ...`	configure
`erps instance`	configure
`show`	erps-ring
`control-vlan`	erps-ring
`guard-timer`	erps-ring
`holdoff-timer`	erps-ring
`left-port ...type ...`	erps-ring
`mel ...`	erps-ring
`name ...`	erps-ring
`revertive`	erps-ring
`right-port ...type ...`	erps-ring
`ring enable`	erps-ring
`version`	erps-ring
`wtr-timer`	erps-ring
`instance ... control-vlan ...`	config-erps-inst
`show`	config-erps-inst

3.6.2 STP/RSTP

Mit STP (Spanning Tree Protocol)/RSTP (Rapid Spanning Tree Protocol) werden Schutzmechanismen ähnlich wie bei ERPS konfiguriert. STP/RSTP sind jedoch neben der Ringtopologie auch für allgemeiner vermaschte Topologien wie z. B. einer vermaschten Sterntopologie einsetzbar. Topologieänderungen werden erkannt und Pfade dynamisch angepasst. Die Konvergenzzeit ist jedoch langsamer als bei ERPS (typisch sind 20 bis 50 Sekunden bei STP und 1 bis 10 Sekunden bei RSTP).

Die Schaffung eines schleifenfreien Netzwerks erfolgt durch das selektive Blockieren von redundanten Links. Die Entscheidung zum Aktivieren bzw. Deaktivieren eines Links wird anhand von Pfadkosten getroffen, die für die Übertragung von Daten im Netzwerk für jeden Switch-Port festgelegt sind. Üblicherweise gilt: je geringer die Datenübertragungsrate eines Links, desto höher die definierten Pfadkosten. Der Algorithmus ermittelt und aktiviert automatisch die Links mit den in Summe geringsten Pfadkosten, um eine schleifenfreie Verbindung zwischen allen Netzwerkteilnehmern zu ermöglichen.

In jedem Spanning-Tree-Netzwerk wird das Gerät mit dem kleinsten Priority-Wert als Root-Bridge festgelegt. Wenn mehrere Geräte die gleiche Priority haben, wird das Gerät mit der kleinsten MAC-Adresse als Root-Bridge definiert. Konfigurieren Sie die Priority-Werte so, dass ein leistungsstarker, zentral in der Netzwerktopologie eingebundener Switch zur Root-Bridge wird.

Im Spanning-Tree-Netzwerk tauschen alle Switches sogenannte BPDU-Frames (Bridge Protocol Data Unit) mit der Root-Bridge aus, die Verwaltungsdaten enthalten.

3.6.2.1 STP/RSTP Einstellungen

Beispielansicht (WBM)

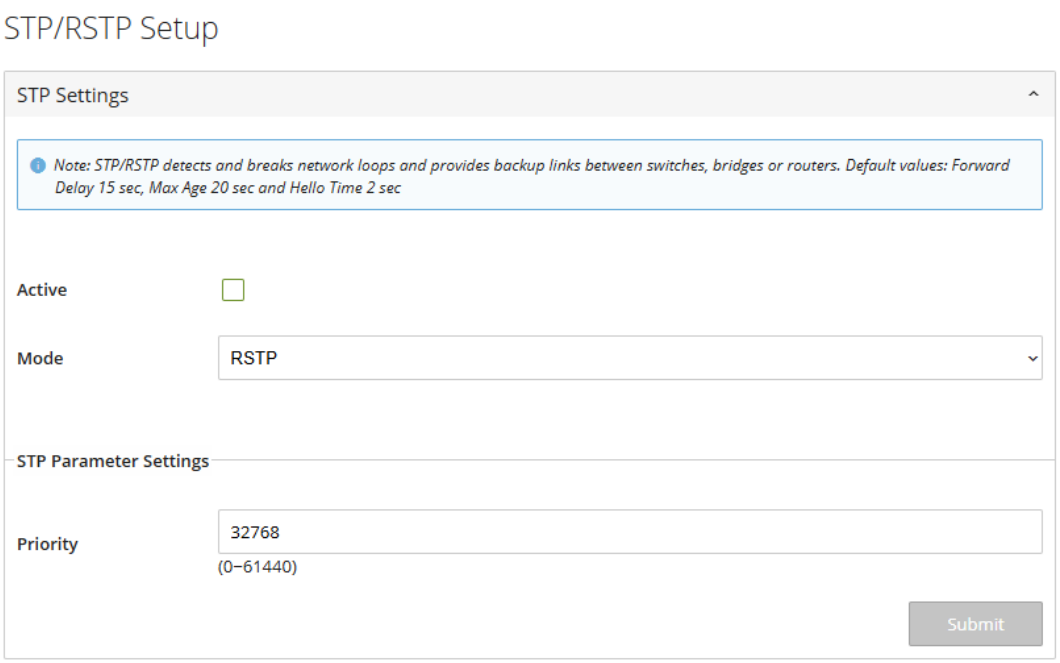


Abbildung 43: STP/RSTP-Set-up

3.6.2.2 STP/RSTP-Port-Einstellungen

Beispielansicht (WBM)

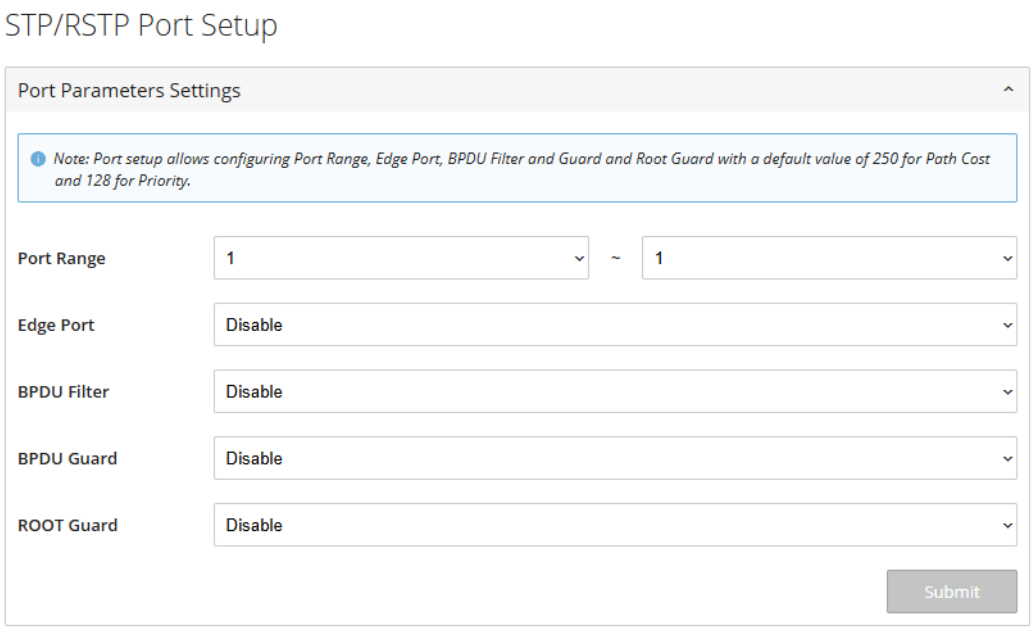


Abbildung 44: STR/RSTP Port-Set-up

- Edge-Ports sind speziell für Endgeräte wie PCs oder Drucker gedacht. Sie dienen dazu, die langsamen Übergangsphasen (Listening/Learning) zu überspringen und sofort in den Forwarding-State zu wechseln, damit Endgeräte direkt und ohne Verzögerung kommunizieren können. Ohne das Festlegen von Edge-Ports kann die Konvergenzzeit in großen Netzwerken derart stark ansteigen, dass festgelegte Timeouts überschritten werden und kein konvergenter Zustand erreicht wird. In diesem Fall kann es aufgrund von Loops zu Netzwerkproblemen wie Broadcast-Stürmen kommen.
- Die Funktion „BPDU-Filter“ sorgt dafür, dass über den Port keine BPDU-Nachrichten ausgetauscht werden. Dadurch wird verhindert, dass ein Port am Spanning-Tree teilnimmt. Das schützt die STP-Topologie vor unbeabsichtigten Einflüssen und sorgt für eine schnellere Port-Aktivierung bei reinen Endgeräte-Ports. Wenn jedoch ein Switch an einem Port mit aktiviertem BPDU-Filter angeschlossen wird, können mögliche Schleifen im Netzwerk nicht korrekt erkannt werden. In der Regel sollte daher bevorzugt die Funktion „BPDU-Guard“ verwendet werden.
- Die Funktion „BPDU-Guard“ deaktiviert einen Port, an dem eine BPDU-Konfigurations-nachricht empfangen wird. Dadurch wird sichergestellt, dass ausschließlich Endgeräte am so konfigurierten Port betrieben werden und das Gesamtnetz vor unbeabsichtigten STP-Topologieänderungen geschützt ist.
- Die Funktion „ROOT-Guard“ blockiert temporär einen so geschützten Port, wenn ein verbundener Switch versucht, zur Root-Bridge zu werden. Dadurch werden die Stabilität und Integrität der STP-Topologie geschützt, auch gegenüber unberechtigten Manipulations-versuchen.

HINWEIS

BPDU-Filter und BPDU-Guard

Bei gleichzeitiger Aktivierung der beiden Funktionen „BPDU-Filter“ und „BPDU-Guard“ hat ersterer die höhere Priorität.

CLI-Befehle

Tabelle 45: STP/RSTP CLI

Befehl	Node
`show spanning-tree active`	enable
`show spanning-tree blockedports`	enable
`show spanning-tree port detail ...`	enable
`show spanning-tree statistics ...`	enable
`show spanning-tree summary`	enable
`clear spanning-tree counters`	enable
`clear spanning-tree counters ...`	enable
`spanning-tree ...`	configure
`spanning-tree algorithm-timer forward-time ... max-age ... hello-time ...`	configure
`spanning-tree forward-time ...`	configure
`spanning-tree hello-time ...`	configure
`spanning-tree max-age ...`	configure
`spanning-tree mode ...`	configure
`spanning-tree pathcost method ...`	configure
`spanning-tree priority ...`	configure
`interface range gigabitethernet1/0/ ...`	configure
`spanning-tree ...`	interface
`spanning-tree bpdufilter ...`	interface
`spanning-tree bpduguard ...`	interface
`spanning-tree rootguard ...`	interface
`spanning-tree edge-port ...`	interface
`spanning-tree cost ...`	interface
`spanning-tree port-priority ...`	interface
`spanning-tree ...`	if-range
`spanning-tree bpdufilter ...`	if-range
`spanning-tree bpduguard ...`	if-range
`spanning-tree rootguard ...`	if-range
`spanning-tree edge-port ...`	if-range
`spanning-tree cost ...`	if-range
`spanning-tree port-priority ...`	if-range

Tabelle 46: Übersicht über die STR/RSTP Port Parameter im CLI

Parameter	Beschreibung
Forward Time	Die „Forward Time“ (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.
Max Age	Das „Max Age“ (Maximales Alter) ist die maximale Zeit (in Sekunden), die der Switch ohne eine BPDU (Bridge Protocol Data Unit, Konfigurationsnachricht) zu empfangen warten kann, bevor er versucht, mit der Rekonfiguration zu beginnen. Alle Switch-Ports (außer „Designated Ports“) empfangen in regelmäßigen Abständen BPDU. Jeder Port, der STP-Informationen (aus der letzten BPDU) verlernt, wird zum „Designated Port“ für das angeschlossene LAN. Wenn dies ein „Root Port“ ist, wird aus den an das Netzwerk angeschlossenen Switch-Ports ein neuer „Root Port“ gewählt.
Hello Time	Die „Hello Time“ ist das Zeitintervall (in Sekunden) zwischen den vom Root-Switch versendeten Konfigurationsnachrichten (BPDU, Bridge Protocol Data Unit).
Transmission Limit	Mit dem „Transmission Limit“ (Übertragungsgrenze) wird das minimale Intervall zwischen der Übertragung aufeinanderfolgender RSTP-BPDU konfiguriert. Diese Funktion kann nur im RSTP-Modus aktiviert werden. Der gültige Bereich liegt bei 1 bis 10 Sekunden.

3.7 Tab-Diagnostic im WBM

3.7.1 Alarm

In den Unterabschnitten des Menüpunktes „Alarm“ lassen sich aktive Alarme einsehen und Konfigurationseinstellungen zu Alarmen vornehmen.

3.7.1.1 Information

In diesem Untermenü werden aktive Alarmmeldungen angezeigt.

CLI-Befehle

Tabelle 47: ALM-Output

Befehl	Node
`show alarm-info`	enable

3.7.1.2 ALM-Output

Hier kann das Verhalten des Alarmrelais des Switches konfiguriert werden. Das Relais dient als potentialfreier Meldekontakt zur Weiterleitung von Geräte- oder Port-Fehlern an übergeordnete Systeme. Für jedes überwachte Ereignis kann festgelegt werden, ob es den Alarmkontakt auslösen soll.

Über die Einstellung „Relay Direction“ lässt sich konfigurieren, ob das Relais im fehlerfreien Zustand geöffnet („Normal Open“) oder geschlossen („Normal Close“) ist.

Alarmmeldungen für die primäre und sekundäre Spannungsversorgung (PWR bzw. RPS) können über die DIP-Schalter des Switches konfiguriert werden. Weitere Informationen zu den DIP-Schaltern finden Sie im Produkthandbuch.

HINWEIS

Bei den WAGO Lean-Managed-Switches mit den Artikelnummern 852-1816 und 852-1816/010-000 kann die Relay-Direction aufgrund von Hardwareeinschränkungen nicht verändert werden.

Der Lean-Managed-Switch mit der Artikelnummer 852-1832 besitzt kein Alarmrelais. Die Einstellmöglichkeiten sind bei diesem Produkt daher nicht vorhanden. Ebenfalls sind keine DIP-Schalter vorhanden.

Tabelle 48: Übersicht über die Konfiguration für ALM-Output

Parameter	Beschreibung
ERPS	Signalisierung von Fehlern im Zusammenhang mit dem ERPS-Redundanzprotokoll
Port 1 … 10	Signalisierung von Verbindungsunterbrechungen am jeweiligen Port
Relay Direction	Angabe, wie das Relayverhalten im Ruhezustand sein soll (NO oder NC).

CLI-Befehle

Tabelle 49: ALM-Output

Befehl	Node
`show alarm-relay`	enable
`alarm-relay ...`	configure

3.7.1.3 DIP-Status

Angezeigt wird der Status der DIP-Schalter auf der Gehäuseoberseite zu verschiedenen Features. Weitere Informationen zu den DIP-Schaltern finden Sie im Produkthandbuch.

HINWEIS

Der Lean-Managed-Switch mit der Artikelnummer 852-1832 besitzt keine DIP-Schalter. Der Menüpunkt „DIP Status“ ist bei diesem Produkt daher nicht vorhanden.

HINWEIS

Die folgenden DIP-Schalter stehen nur bei den WAGO Lean-Managed-Switches mit den Artikelnummern 852-1813/000-001 und 852-1813/010-001 zur Verfügung.

Tabelle 50: Übersicht über zusätzliche DIP-Schalter bei 852-1813/000-001 und 852-1813/010-001

Feature	Beschreibung
Storm	Konfiguriert **Storm Control** für alle Ports mit den Grenzwerten 300 Pakete/s für DLF und 1000 Pakete/s für Broadcast.
QoS	Priorisiert den Datenverkehr der Ports 1 und 2 höher gegenüber allen anderen Ports; durch die Aktivierung werden die Einstellungen überschrieben.
P9 100Fx	Konfiguriert den jeweiligen SFP-Port auf die Geschwindigkeitseinstellung „100 Mbps/Full“; dies ermöglicht die Nutzung von SFP-Modulen mit einer maximalen Datenübertragungsrate von 100 Mbit/s ohne Konfiguration im WBM.
P10 100Fx	

CLI-Befehle

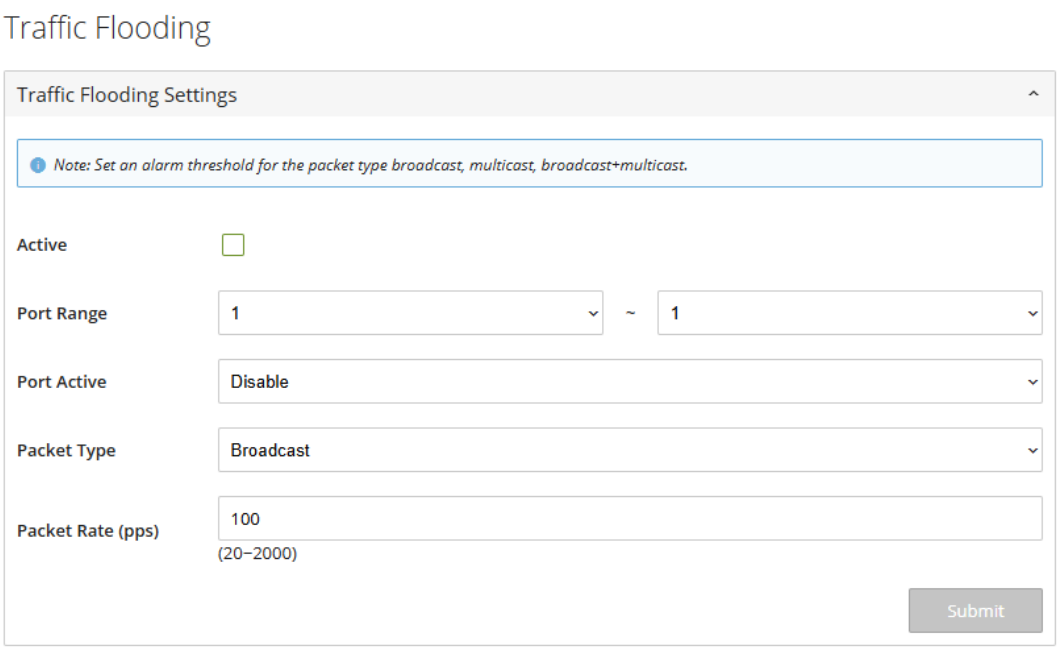
Tabelle 51: DIP Status

Befehl	Node
`show alarm-info`	enable

3.7.1.4 Traffic-Flooding

Hier wird ein Grenzwert für Mulitcast- und/oder Broadcast-Pakete in Paketen pro Sekunde festgelegt, ab dem der Switch einen Alarm generiert.

Beispielansicht (WBM)



HINWEIS

Konfiguration der Alarmwerte für Traffic-Flooding

Es wird empfohlen, die Werte für den jeweils vorliegenden Anwendungsfall anzupassen.

- Die Standardwerte (100 pps für Broadcast, kein Wert für Mulicast) gelten für typische Anwendungen in Büroumgebungen und kleineren Unternehmen.

3.7.1.5 Port-Auslastung (Port Utilization)

Hier wird die Alarmschwelle für die Port-Auslastung konfiguriert. Bei Überschreitung des Schwellwertes generiert der Switch einen Alarm.

Beispielansicht (WBM)

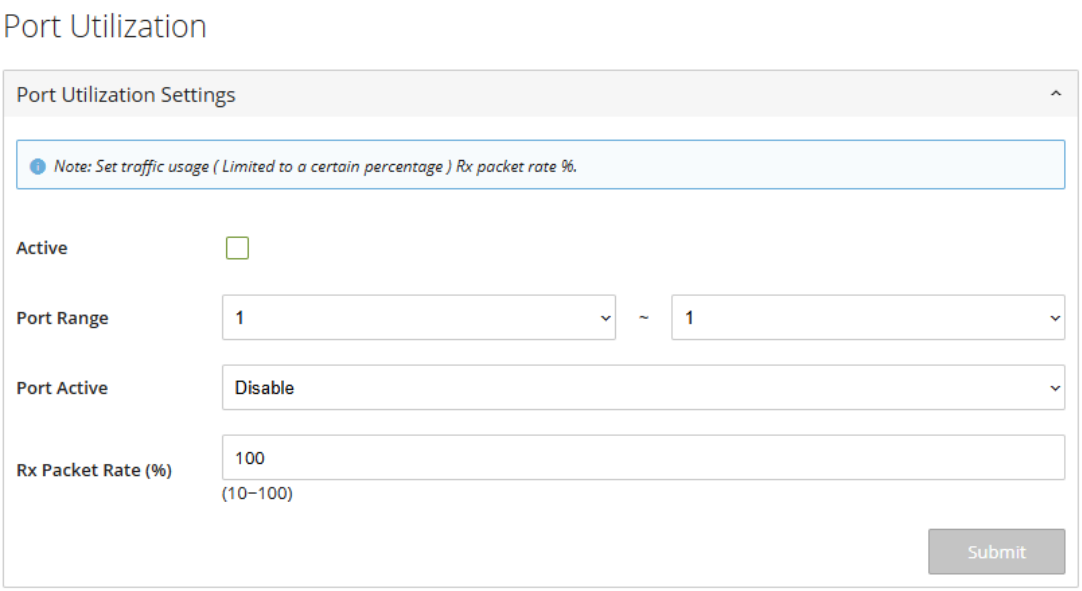


Abbildung 45: Port-Utilization

- Die maximale Rx-Paketrate (Paketempfangsrate in Prozent) wird entweder für alle oder für ausgewählte Ports definiert.

CLI-Befehle

Tabelle 52: Utilization-Tthreshold CLI

Befehl	Node
`port-utilization threshold ...`	configure
`port-utilization threshold rate ...`	interface
`port-utilization threshold state ...`	interface

3.7.2 Dashboard-Configuration

Hier finden sich verschiedene Optionen zur Anpassung des Dashboard-Verhaltens (für weitere Informationen zu den Informationen im Dashboard siehe Abschnitt **Diagnose mit dem Dashboard**):

- Anlernen und Zurücksetzen angelernter Nachbargeräte: Über das Anlernen kann ermittelt werden, welche Switch-Ports für die Verwendung vorgesehen sind. Wenn z. B. ein Link ausfällt (z. B. Kabel defekt oder gelöst), wird dies im Dashboard dargestellt.
- Zurücksetzen aller Statistiken und Bereitstellen einer downloadbaren Log-Datei der Port-Link-Down-Statistik
- Konfiguration von Grenzwerten für Alarme

Beispielansicht (WBM)

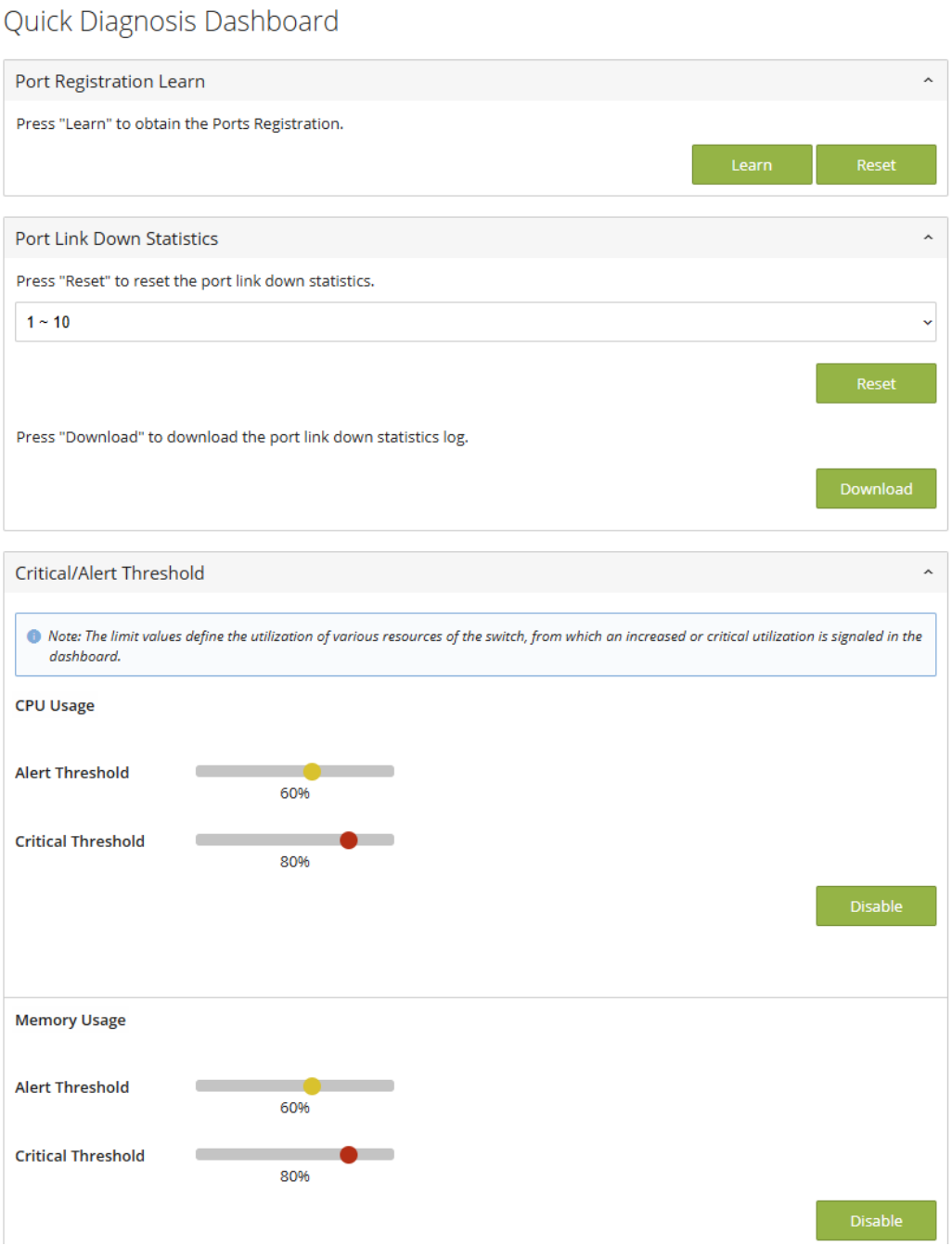


Abbildung 46: Quick Diagnosis Dashboard

HINWEIS

Anlernen der Nachbargeräte, die mit dem Switch in Verbindung stehen

Beim Anlernen müssen die Nachbargeräte bereits verbunden und aktiv sein. Wenn ein Nachbargerät LLDP unterstützt, sollte dieses ebenfalls aktiviert sein, um Geräteinformationen zu übermitteln. Ansonsten wird nur die MAC-Adresse gelernt.

Konfiguration von Grenzwerten für kritische Fehler und Alarme

Grenzwerte sollten anhand des Normalbetriebs und der geplanten Nutzung definiert werden. Dadurch können Überlastungen frühzeitig erkannt und Fehlfunktionen vermieden werden. Zu niedrige Schwellenwerte führen zu unnötigen Alarmen, zu hohe Schwellenwerte können kritische Zustände zu spät melden.

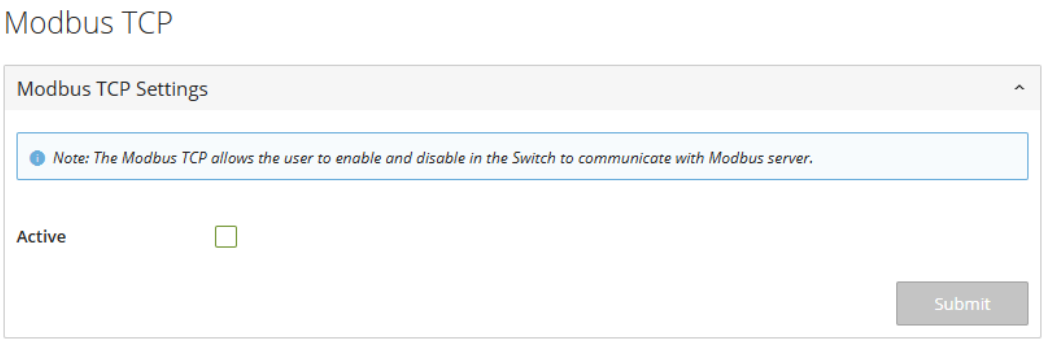
Grenzwerte für CPU-Usage, Memory-Usage, Port-Tx-Usage und Port-Rx-Usage

Für die Auslastung von CPU, Arbeitsspeicher sowie die Sende- und Empfangsrichtung der Netzwerk-Ports können Alarmgrenzwerte definiert werden.

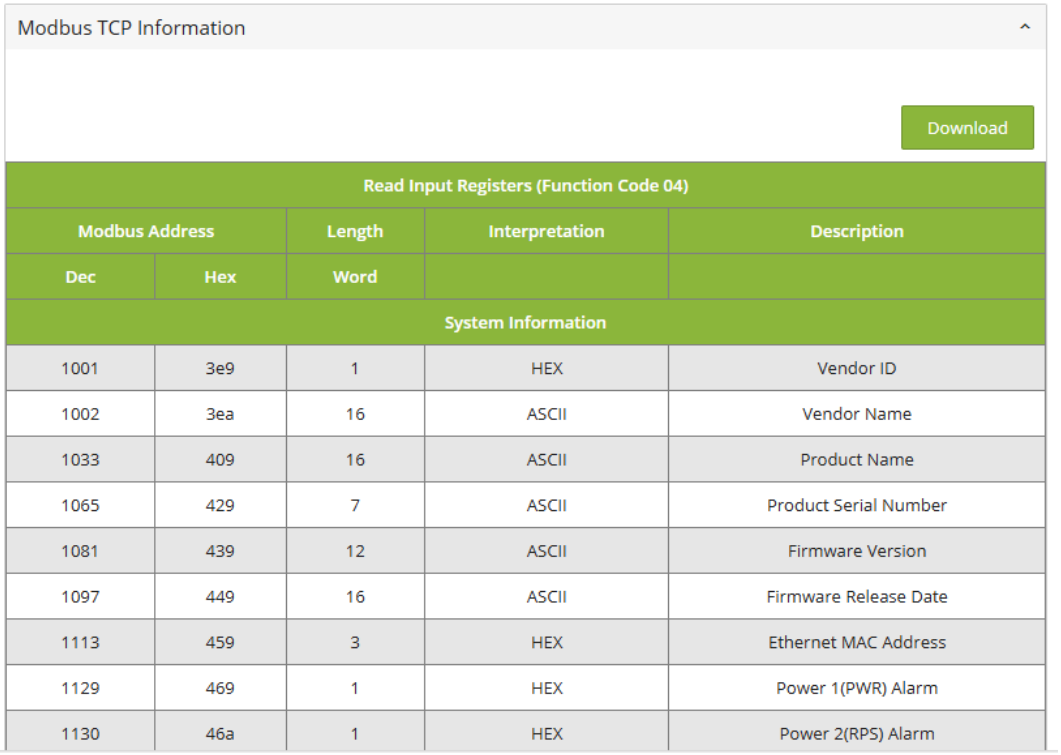
- Alert: Ab diesem Grenzwert wird im Dashboard eine Vorwarnung in gelber Farbe ausgegeben. Der Alarm kann möglicherweise frühzeitig (vor dem Auftreten von Verbindungsfehlern) auf eine Fehlkonfiguration (z. B. Loop, Broadcast-Sturm) oder einen atypischen Traffic hinweisen. Der Standardwert liegt bei 60 % der Auslastung.
- Critical: Ab diesem Grenzwert wird im Dashboard vor einer kritischen Ressourcenauslastung in roter Farbe gewarnt.
  Der Standardwert liegt bei 80 % der Auslastung.

3.7.3 Modbus TCP

Im Menü „Modbus TCP“ kann der Modbus®-Server des Switches aktiviert werden, um wesentliche Systemstatus per Modbus® auslesen zu können. Die verfügbaren Modbus®-Register werden tabellarisch aufgelistet und lassen sich herunterladen.



Beispielansicht (WBM)



Read Input Registers (Function Code 04)				
Modbus Address		Length	Interpretation	Description
Dec	Hex	Word		
System Information				
1001	3e9	1	HEX	Vendor ID
1002	3ea	16	ASCII	Vendor Name
1033	409	16	ASCII	Product Name
1065	429	7	ASCII	Product Serial Number
1081	439	12	ASCII	Firmware Version
1097	449	16	ASCII	Firmware Release Date
1113	459	3	HEX	Ethernet MAC Address
1129	469	1	HEX	Power 1(PWR) Alarm
1130	46a	1	HEX	Power 2(RPS) Alarm

Abbildung 47: Modbus TCP

CLI-Befehle

Tabelle 53: Modbus TCP CLI

Befehl	Node
`show modbus`	enable
`modbus …`	configure

3.7.4 SNMP

Informationen finden Sie im Abschnitt **SNMP**.

3.7.5 Syslog

Das Systemprotokoll zeichnet verschiedene Systeminformationen für die Fehlersuche mit Angabe der Priorität (Warnstufen 1 bis 6) auf.

Zusätzlich besteht die Möglichkeit, Logs an einen Syslog-Server zu senden.

HINWEIS

Größe der Protokollnachrichtendatei im Switch

Die Größe der Protokollnachrichtendatei im Switch ist auf 4 kB begrenzt. Wenn die Datei voll ist, wird die jeweils älteste Nachricht ersetzt.

Beispielansicht (WBM)

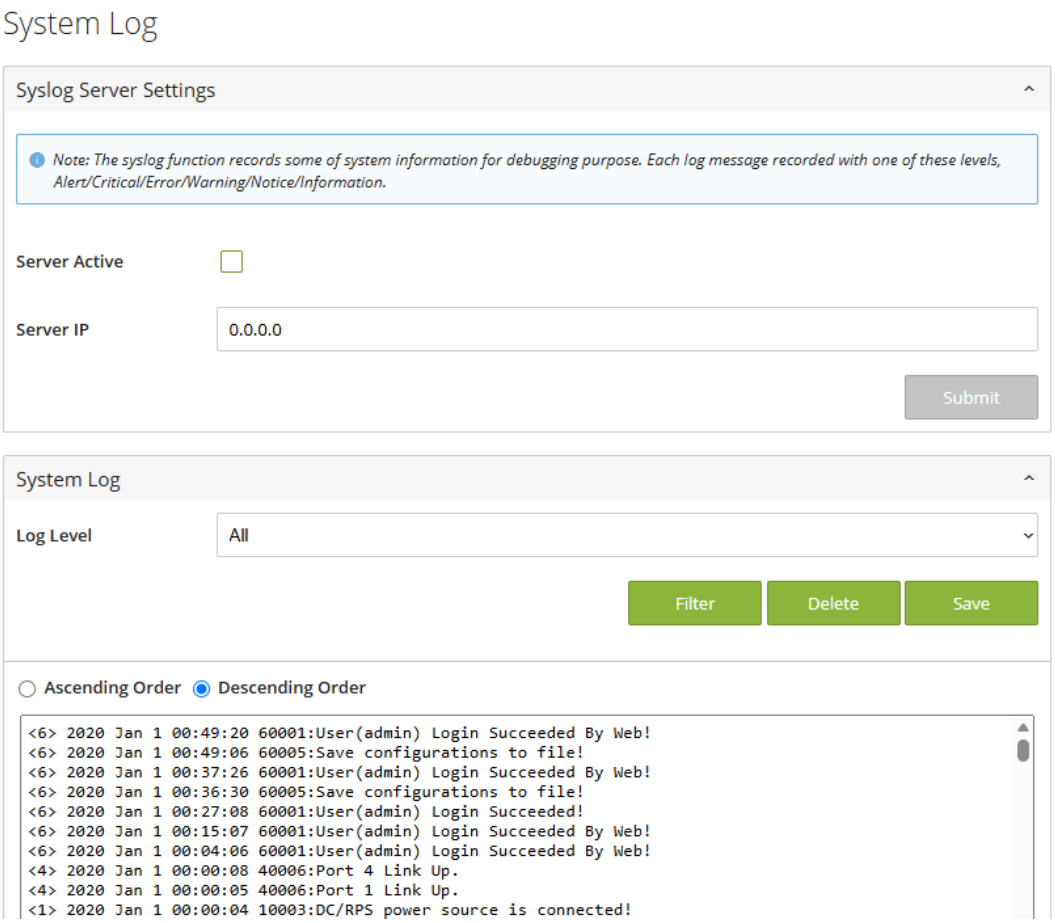


Abbildung 48: System Log

CLI-Befehle

Tabelle 54: Syslog CLI

Befehl	Node
`show syslog`	enable
`clear syslog`	configure
`show syslog level …`	enable
`show syslog server`	enable
`syslog-server ...`	configure
`syslog-server ip ...`	configure

3.7.6 SSL-Certificate

Der Switch erlaubt, das werksseitig installierte SSL-Zertifikat, das für die verschlüsselte Übertragung der WBM-Daten (https) benötigt wird, zu ersetzen. Dadurch kann die Sicherheit weiter erhöht werden. Außerdem können bei der Installation eines Zertifikats von einer vertrauenswürdigen Zertifizierungsstelle Sicherheitswarnungen im Webbrowser vermieden werden. Das Zertifikat muss als *.pfx-Datei vorliegen. Ein gegebenenfalls verwendetes Passwort zum Schutz der Zertifikatsdaten ist anzugeben.

Beispielansicht (WBM)

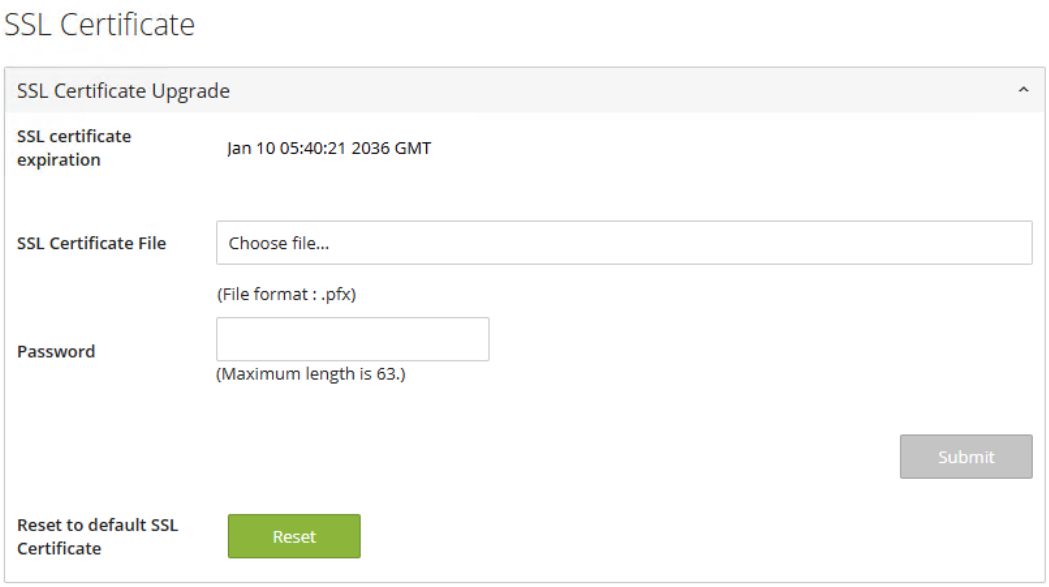


Abbildung 49: SSL-Certificate

3.8 Tab Maintenance im WBM

3.8.1 Maintenance

Unter „Maintenance“ können folgende Funktionen aufgerufen werden:

Tabelle 55: Übersicht über die Funktionen im Menü „Maintenance“

Befehl	Erläuterung
Reboot	Ermöglicht, den Switch ohne Trennen der Spannungsversorgung neu zu starten; siehe **Ausschalten/Neustart**.
Upgrade firmware	Führt ein Update der Firmware des Switches durch; siehe **Firmware-Update mit dem WBM durchführen**.
Upload configuration	Lädt eine Konfigurationsdatei vom PC auf den Switch.[1]
Download configuration	Speichert die aktuelle Konfiguration des Switches in einer Datei auf Ihrem PC.
Reset configuration	Der Switch wird auf die Werkseinstellungen zurückgesetzt. Optional können die Netzwerkeinstellungen und/oder Benutzerkonten beibehalten werden. Siehe auch **Zurücksetzen auf Werkseinstellungen**.

1) **Modifikation der Konfigurationsdatei**:
Durch Modifikationen der Konfigurationsdatei mit einem Texteditor kann eine größere Anzahl von Switches schnell konfiguriert werden.

Beispielansicht (WBM)

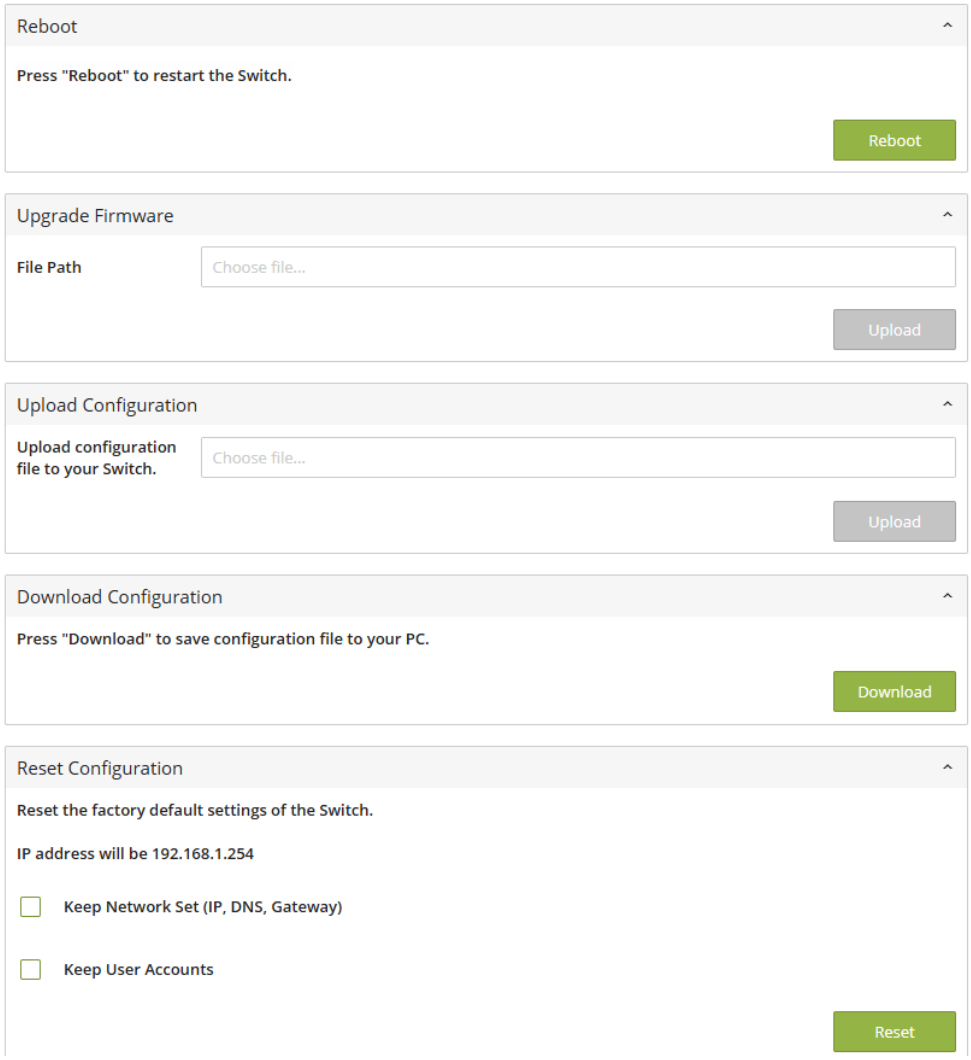


Abbildung 50: Maintenance

CLI-Befehle

Tabelle 56: Maintenance – Upload and Download Configuration CLI

Befehl	Node
`write memory`	configure
`archive download-config ...`	configure
`archive upload-config ...`	configure
`reload default-config`	configure

3.9 Erweiterte Konfiguration per CLI

Für Fälle, in denen Spezialparameter angepasst werden müssen oder erweiterte Features benötigt werden, die im WBM nicht vorhanden sind, steht das textbasierte CLI (Command Line Interface) bereit. Darüber hinaus stellt es die Basis für eine automatisierte Konfiguration bei Massenrollouts dar. Das WBM konzentriert sich hingegen auf eine benutzerfreundliche Darstellung der meistverwendeten Funktionen im Webbrowser, die auch für Einsteiger leicht konfigurierbar sind. Weitere Informationen finden Sie im Abschnitt **Konfigurieren mit dem CLI**.

Die folgende Tabelle gibt einen Überblick über häufig verwendete Funktionen, die exklusiv im CLI zur Verfügung stehen:

Tabelle 57: Beschreibung erweiterter Funktionen im CLI

Befehl	Kurzbeschreibung
`cli ...`	Konfiguration eines Auto-Logout bei Zeitüberschreitung (gültig für WBM und CLI)
`copy ...`	Kopieren von Konfigurationen.
`gateway-keep-alive ...`	Konfiguration des Keepalive-Mechanismus für ein Gateway
`igmp-snooping ...`	Dient der Optimierung der Netzwerkleistung bei der Übertragung von Multicast-Paketen.
`ip-multicast ...`	Konfiguration einer IP-Multicast Verbindung
`mac-address-table ...`	Konfiguration des Verhaltens der MAC-Address-Tabelle
`onvif ...`	Konfiguration von onvif, einem offenen Standard für IP-basierte Sicherheitsprodukte, z. B. Überwachungskameras

4 In Betrieb nehmen

4.1 Einschalten des Switches

Es werden folgende Hilfsmittel und Informationen benötigt:

- Netzwerkkabel (Cat5e oder besser)
- Stromversorgung für den Switch
- PC oder Laptop
- ggf. Terminalsoftware (z. B. PuTTY, Tera Term)
- Informationen: gewünschte IP-Adresse, Subnetzmaske, Gateway (bei statischer Konfiguration) oder DHCP-Server-Adresse

Um den Switch in Betrieb zu nehmen, müssen folgende Schritte ausgeführt werden:

1 Der Switch wird durch das Verbinden mit der Stromversorgung „eingeschaltet“.

2 Danach wird die Status-LED überprüft (Power-LED sollte leuchten).

3 Dann wird das Netzwerkkabel zwischen Switch und PC/Laptop angeschlossen.

Bootvorgang abwarten, bis LEDs das Erreichen des Betriebsstatus anzeigen. (Dieser Vorgang kann bis zu zwei Minuten dauern.)

4.2 Werksseitige Zugangsdaten

Tabelle 58: Werksseitige Zugangsdaten

IP-Adresse	192.168.1.254
Benutzername	admin
Passwort	wago

4.3 Konfigurieren einer IP-Adresse

Es kann auf verschiedenen Wegen die IP-Adresse für den Switch vergeben werden. Sofern die IP-Adresse nicht via DHCP zugewiesen werden soll, muss eine statische IP-Adresse konfiguriert werden. Bis zu diesem Punkt wird die Standard-IP-Adresse 192.168.1.254 mit der Subnetzmaske 255.255.255.0 verwendet.

In den folgenden Beispielen ist der Name des Switches (Hostname) im Netzwerk L2SWITCH. Als beispielhaft konfigurierte IP-Adresse wird die 192.168.1.100 verwendet.

4.3.1 Konfigurieren einer IP-Adresse über das CLI

1 Bauen Sie eine Terminalverbindung auf und wechseln Sie in den Configuration-Modus (siehe **Konfigurieren mit dem CLI**).

2 Anschließend kann die IP-Konfiguration vorgenommen werden. Beispielkonfiguration: IP-Adresse: 192.168.1.100, Subnetzmaske: 255.255.255.0 (24 Subnetzmasken-Bits), Gateway: 192.168.1.1.

```
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#ip address 192.168.1.100/24 default-gateway
192.168.1.1
```

3 Bei einer Änderung der IP-Konfiguration kann die Terminalverbindung abbrechen. Bauen Sie in diesem Fall die Verbindung unter Angabe der zugewiesenen IP-Adresse neu auf. Denken Sie daran, ggf. auch die IP-Adresse Ihres PC anzupassen.

4 Speichern Sie die geänderte Konfiguration persistent ab:

```
L2SWITCH(config)#write memory
```

4.3.2 Konfigurieren des Switches als DHCP-Client über das CLI

Damit DHCP verwendet werden kann, muss ein DHCP-Server im Netzwerk verfügbar sein. Dieser weist dem Switch eine IP-Konfiguration zu.

1 Bauen Sie eine Terminalverbindung auf und wechseln Sie in den Configuration-Modus (siehe **Konfigurieren mit dem CLI**).

2 Aktivieren Sie den DHCP-Client:

```
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#ip dhcp client enable
```

3 Bei einer Änderung der IP-Konfiguration kann die Terminalverbindung abbrechen. Bauen Sie in diesem Fall die Verbindung unter Angabe der zugewiesenen IP-Adresse neu auf. Denken Sie daran, ggf. auch die IP-Adresse Ihres PCs anzupassen.

4 Speichern Sie die geänderte Konfiguration persistent ab:

```
L2SWITCH(config)#write memory
```

4.3.3 Konfigurieren einer IP-Adresse über das WBM

1 Verbinden Sie den PC per LAN-Kabel mit dem Switch und geben Sie die IP-Adresse im Webbrowser ein (Standard-IP-Adresse: 192.168.1.254).

2 Melden Sie sich mit dem administrativen Benutzer an. Sofern nicht anders konfiguriert, gelten die ab Werk vorgegebenen Daten (Benutzername: admin, Passwort: wago).

3 Wechseln Sie zum Tab „Configuration“ und wählen Sie im Menü „System Management“ > „General Setup“ aus. Im Bereich „TCP/IP Configuration“ kann die IP-Konfiguration vorgenommen werden. Weitere Informationen zum Thema finden Sie im Abschnitt **General** .

4 Übernehmen Sie die Änderungen mit einem Klick auf die Schaltfläche „Submit“.

5 Der Webbrowser wechselt automatisch zur neu zugewiesenen IP-Adresse. Rufen Sie im Falle eines Verbindungsabbruchs die neue IP-Adresse manuell auf und denken Sie daran, ggf. auch die IP-Adresse Ihres PC anzupassen.

6 Speichern Sie die geänderte Konfiguration persistent ab, indem Sie im WBM auf die Schaltfläche „Save“ klicken.

4.4 Testen der Netzwerkverbindung

Die Erreichbarkeit eines Gerätes im IP-Netzwerk kann mit Hilfe des Ping-Befehls überprüft werden. Dieser Befehl sendet ICMP-Echo-Requests an die angegebene IP-Adresse oder den Hostnamen und liefert Informationen zur Round-Trip-Time oder ggf. einen Paketverlust als Antwort zurück.

Vom PC aus den Switch anpingen:

1 Öffnen Sie einen Terminalemulator(z. B. die Eingabeaufforderung von Windows) und geben Sie den Ping-Befehl für die entsprechende IP-Adresse ein; in diesem Beispiel 192.168.1.254:
`ping 192.168.1.254`

Vom Switch aus ins Netzwerk pingen (z. B. um ein Gateway zu testen):

1 Greifen Sie über eine Terminalsoftware auf den Switch zu (siehe **Konfigurieren mit dem CLI**). Nach dem Login und dem Wechsel in den Privileged-Modus kann der Ping-Befehl abgesetzt werden. In diesem Beispiel wird über den Switch die IP 192.168.10.1 des PCs angepingt:
`L2SWITCH# ping 192.168.10.1`

Wenn bei der Antwort ein Fehler auftritt, z. B. durch Paketverlust oder wenn die Antwortzeiten hoch ausfallen, prüfen Sie folgende Punkte:

- Verkabelung
- IP/Subnetzmaske
- Gateway-Einstellungen
- Erreichbarkeit des DHCP-Servers
- Firewall-Konfiguration

4.5 Passwörter ändern

Hinweise zum Ändern von Passwörtern finden Sie im Abschnitt **User Account**.

HINWEIS

Passwörter ändern

Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten keinen hinreichenden Schutz.

- Ändern Sie die Passwörter entsprechend Ihren Erfordernissen.

4.5.1 Passwortänderung per Konfigurationsdatei

Es ist möglich, ein oder mehrere Benutzerpasswörter über die Konfigurationsdatei des Switches zu ändern. Gehen Sie dazu wie folgt vor:

1 Laden Sie die Konfigurationsdatei herunter, siehe **Maintenance**.

2 Fügen Sie über dem Eintrag „model-name …“ folgenden Inhalt hinzu und ersetzen Sie dabei die Parameter <username> sowie <password> durch einen bereits vorhandenen Benutzernamen sowie das neue Passwort:

```
change-password <username> <password>
```

Beachten Sie, dass keine Passwortänderung erfolgt, wenn das Passwort ungültige Zeichen enthält. Gültige Zeichen sind: Buchstaben (a-z,A-Z), Zahlen (0-9), Sonderzeichen (!%*+,-.=@[]^_{})

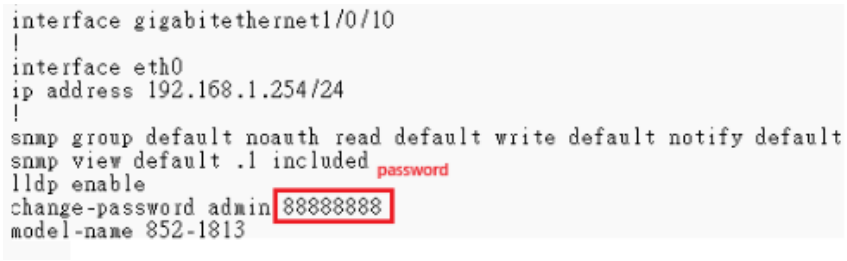


Abbildung 51: Passwortänderung per Konfigurationsdatei

3 Laden Sie die angepasste Konfigurationsdatei in das Gerät, siehe **Maintenance**.

4.6 Ausschalten/Neustart

Ein Neustart kann durch die Funktion „Reboot“ auf der WBM-Seite „Maintenance“ ausgeführt werden. Dieser Vorgang kann bis zu zwei Minuten dauern.

Zusätzlich dazu gibt es in der Kopfzeile jeder WBM-Seite einen Reboot-Schaltfläche.

Um per CLI einen Neustart auszuführen, kann auf der Configuration-Ebene folgender Befehl verwendet werden:

```
L2SWITCH(config)#reboot
```

Wenn der Switch über WBM oder CLI nicht erreichbar ist, kann ein Reset auch durch kurzzeitiges Trennen der Stromversorgung ausgelöst werden. Nach dem Trennen sollte das Gerät einige Sekunden ausgeschaltet bleiben, bevor die Stromversorgung wiederhergestellt wird.

Reset-Verfahren:

1 Informieren Sie vor dem Reset ggf. betroffene Nutzer.

2 Nutzen Sie eine der oben beschriebenen Methoden, um einen Reset des Switches durchzuführen.

3 Der Neustart erfolgt automatisch durch den Switch.

5 Konfigurieren

5.1 Konfigurieren im WBM

Das „Web-Based-Management“ (WBM) ist eine über einen Webbrowser erreichbare Konfigurations- und Verwaltungsschnittstelle des Switches.

5.1.1 Aufbau des WBM

Rechts in der Kopfzeile befinden sich Schaltflächen zum Speichern der vorgenommenen Einstellungen (3), zum Neustarten des Switches (4) und zum Abmelden vom WBM (5). Mittig sind Registerreiter (2) angeordnet, die die jeweiligen Hauptbereiche des WBM zugänglich machen:

- Information (siehe **Tab-Information im WBM**)
- Configuration (siehe **Tab-Configuration im WBM**)
- Security (siehe **Tab Security im WBM**)
- Redundancy (siehe **Tab-Redundancy im WBM**)
- Diagnostic (siehe **Tab-Diagnostic im WBM**)
- Maintenance (siehe **Tab Maintenance im WBM**)

Nach Auswahl eines der Hauptbereiche wird links zu dem jeweiligen Bereich eine Navigationsleiste (1) angezeigt, die die jeweiligen Menüpunkte und ggf. Untermenüs zur Verfügung stellt. Über dieses Menü wird die entsprechende Seite im WBM aufgerufen, die im Konfigurationsbereich (6) dargestellt wird.

Auf den aufgerufenen Seiten kann im Allgemeinen in diesem Bereich eine Konfiguration über Eingabefelder, Auswahllisten, Check-Boxen und weitere Elemente vorgenommen werden.

Im Anzeigebereich (8) werden (in der Regel tabellarisch oder in Listenform) die getroffenen Einstellungen dargestellt.

Bei einigen Seiten kann über die Bleistift-Schaltfläche (9) rechts in der Tabelle z. B. ein Port direkt für die Konfiguration ausgewählt werden.

Zur besseren Übersicht können sowohl der Konfigurations- als auch der Anzeigebereich über den Pfeil (7) zu- bzw. aufgeklappt werden.

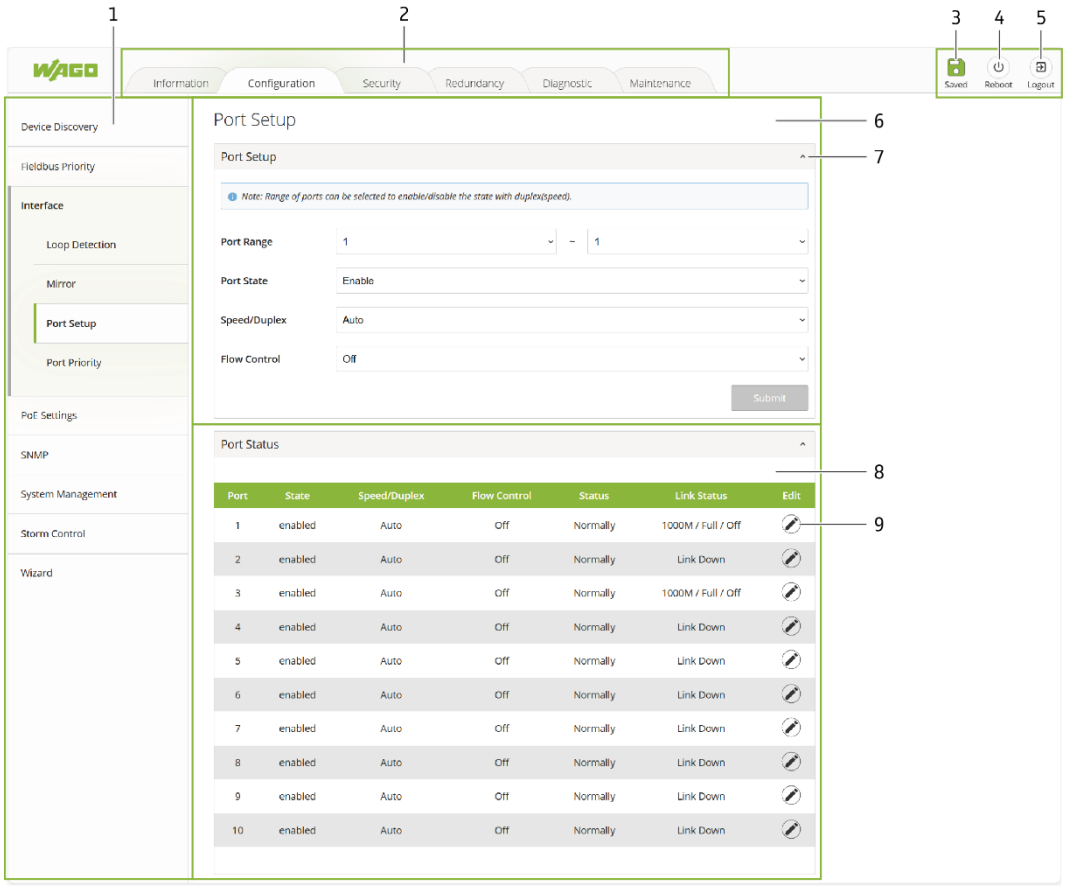


Abbildung 52: Aufbau des WBM

Einige Steuerungselemente werden im WBM auf zahlreichen Seiten eingesetzt. Im Folgenden wird deren Verwendung erläutert:

- **Active (1):** Mit dieser Check-Box lässt sich die jeweilige Funktion generell aktivieren und deaktivieren. Sie arbeitet wie ein Hauptschalter für die Funktion. In früheren Firmware-Versionsständen wurde teilweise „Global State“ zur Beschreibung der Check-Box verwendet.
- **Port Range (2):** Über die beiden Drop-Down-Listen kann ein Bereich ausgewählt werden. Dadurch können Änderungen für mehrere Ports gleichzeitig vorgenommen werden.

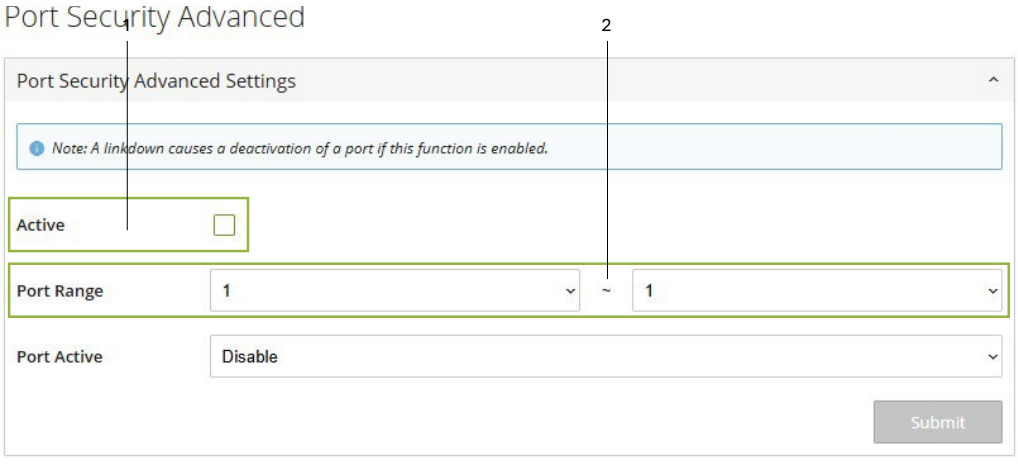


Abbildung 53: Wiederkehrende Einstellungsmöglichkeiten

5.1.2 Arbeiten im WBM

HINWEIS

Temporäre oder permanente Konfigurationsänderungen

Um Änderungen dauerhaft in die Konfiguration zu übernehmen, müssen diese über die Schaltfläche „Save“ (3) in die „startup-config“ übernommen werden.

Bei der Arbeit im WBM muss unterschieden werden zwischen der aktuellen Konfiguration, der „runnig-config“ und der Konfiguration, die der Switch nach einem Neustart automatisch lädt, der „startup-config“. Konfigurationsänderungen werden zunächst in der „running-config“ im Arbeitsspeicher abgelegt und sind sofort wirksam. Erst durch Klicken der Save-Schaltfläche in der Kopfzeile wird die „running-config“ als „startup-config“ in den persistenten Speicher übernommen. Ohne diesen Schritt gehen vorgenommene Änderungen bei einem Neustart verloren.

Der Vorteil einer „running-config“ liegt in der Möglichkeit, Konfigurationsänderungen ohne großes Risiko vornehmen zu können. Wenn anschließend etwas nicht mehr korrekt arbeitet oder der Zugriff auf das WBM nicht mehr möglich ist, genügt ein Neustart, um die zuvor verwendete Konfiguration zu laden. Beim Start des Switches wird die „startup-config“ kopiert und als „running-config“ verwendet.

Tabelle 59: Unterschiede zwischen „running-config“ und „startup-config“

Funktion	Definition	Erläuterung
running-config	aktuell im Arbeitsspeicher (RAM) aktive Konfiguration des Switches	Die Änderungen wirken sofort, nachdem sie eingegeben und übermittelt wurden. Die Konfiguration geht verloren, wenn der Switch neu gestartet oder ausgeschaltet wird. Anzeige durch den CLI-Befehl „show running-config“
startup-config	dauerhaft gespeicherte Konfiguration im nichtflüchtigen Speicher (NVRAM) des Switches	Die Konfiguration wird beim Starten des Switches automatisch geladen. Sie ist auch nach Neustart oder Stromausfall verfügbar.

Um mit dem WBM-Einstellungen vorzunehmen, sind folgende Arbeitsschritte nötig:

1 Öffnen Sie einen Webbrowser.

2 Geben Sie die IP-Adresse des Switches ein (Werkseinstellung: 192.168.1.254).

3 Bei Verwendung des Protokolls https wird ihr Webbrowser unter Umständen eine Sicherheitswarnungen anzeigen. Dies hängt damit zusammen, dass das hinterlegte Zertifikat selbstsigniert und allgemeingültig ist. Das Hinterlegen eines Zertifikates einer anerkannten Zertifizierungsstelle würde diese Warnung vermeiden. Hierzu müsste jedoch die individuell konfigurierbare Adresse des Switches bereits bei der Produktion bekannt sein. Aus diesem Grund ist es für WAGO nicht möglich, die Meldung zu verhindern. Die Kommunikation erfolgt dennoch verschlüsselt.

4 Um bestmöglich gegen Angriffe geschützt zu sein, können Sie das bereitgestellte Zertifikat bei der Ersteinrichtung in ihrem Webbrowser als vertrauenswürdig hinterlegen. Bei nachfolgenden Zugriffen auf das WBM sollten Sie keine Warnmeldung mehr erhalten. Wenn dennoch eine Warnung angezeigt wird, prüfen Sie, dass Sie mit dem korrekten Gerät verbunden sind.

5 Nach dem Klicken auf das Log-in-Icon können im Anmeldedialog der Username und das Passwort eingegeben werden (bei Erstanmeldung: „admin“ und „wago“).

6 Die Startseite wird angezeigt. Fenster und Register können ausgewählt und Einstellungen vorgenommen werden.

5.2 Konfigurieren mit dem CLI

HINWEIS

Temporäre oder permanente Konfigurationsänderungen

Um Änderungen dauerhaft in die Konfiguration zu übernehmen, müssen diese über `write memory` (auf der „config“-Ebene) in die „startup-config“ übernommen werden.

Auf die Kommandozeilenoberfläche (CLI, Command Line Interface) kann über Telnet und SSH zugegriffen werden:

- Telnet stellt einen Remote-Zugriff über eine IP-Verbindung mit geringen Sicherheitsanforderungen dar und muss im WBM aktiviert werden (WBM-Registerreiter „Security“ – „Service Control“)
- SSH gewährleistet einen sicheren Remote-Zugriff über eine verschlüsselte IP-Verbindung.

5.2.1 Verbindungsaufbau zum CLI

Um via CLI-Einstellungen vorzunehmen, muss zunächst eine Verbindung aufgebaut werden. Hierzu sind folgende Arbeitsschritte nötig, die beispielhaft unter Verwendung der Software PuTTY dargestellt werden:

1 Starten Sie das Programm PuTTY.

2 Geben Sie die IP-Adresse des Switches ein (Werkseinstellung: 192.168.1.254).

3 Wählen Sie die gewünschte Zugriffsart aus, z. B. SSH oder Telnet.

4 Bauen Sie mit einem Klick auf die Schaltfläche „Open“ die Verbindung zum Switch auf.

5 Geben Sie nach dem erfolgreichen Verbindungsaufbau „admin“ ein (dies ist auch dann erforderlich, wenn Sie die Benutzerkonten des Switches an Ihre Bedürfnisse angepasst haben). Dadurch gelangen Sie in den „User Mode“, der als Ausgangsbasis für die weiteren Schritte dient.

```
Login as: admin
```

5.2.2 Konfigurationsebenen im CLI

Das CLI ist hierarchisch aufgebaut. In welchem Modus ein Befehl zur Verfügung steht, ist im Abschnitt **Funktionen** in den Tabellen mit den CLI-Befehlen, jeweils in der Spalte „Node“, differenziert.

Tabelle 60: Übersicht über die CLI-Ebenen

Ebene/Modus	Beschreibung und hierarchischer Aufruf des Modus
User Mode/View Mode	Basisebene, die nach dem Verbindungsaufbau betreten wird (siehe **Verbindungsaufbau zum CLI**; ermöglicht den Wechsel in den Privileged-Modus.

Privileged/Enable Mode (Node: enable)	Wird durch Eingabe des Befehls `enable` betreten und erfordert die Eingabe von Zugangsdaten mit Berechtigung „Normal (read only)“ oder „Admin“; siehe **User Account**. Dieser Modus dient vor allem dazu, die Konfiguration mit den Befehlen `show ...` einzusehen.
Configuration-Modus (Node: configure)	Wird durch Eingabe von `configure terminal` im Privileged-Modus betreten; Änderungen an systemweiten Einstellungen (z. B. Hostname, Management-IP, VLANs).
Configuration Sub-Modes (Node: interface) (Node: if-range) (Node:acl) (Node: vlan) usw.	Es existieren weitere Modi, die aus dem Configuration-Modus heraus aufgerufen werden können. Die Auflistung an dieser Stelle ist nicht abschließend, sondern soll das Prinzip verdeutlichen. Der Interface-Modus wird durch Eingabe des Befehls `interface`, gefolgt vom Schnittstellennamen, betreten, z. B. mit `interface eth0`. In diesem Modus stehen sämtliche Befehle zur Konfiguration der Schnittstelle zur Verfügung, z. B. um diese zu deaktivieren oder um die Geschwindigkeit anzupassen. Wenn mehrere Schnittstellen parallel konfiguriert werden sollen, bietet sich stattdessen der Befehl `interface range` an, z. B. `interface range gigabitethernet1/0/ 5-8`. Neben den Submodi für die Schnittstellenkonfiguration existieren weitere Modi, z. B. für die Konfiguration von ACLs oder VLANs. Sie erkennen einen Submodus jeweils am angepassten Prompt innerhalb des CLI. Beispiel-Prompt zur VLAN-Konfiguration: `WAGO1812(config-vlan)#`

Mit der Eingabe des Befehls `exit` wird der aktuelle Modus verlassen und zum vorherigen Modus gewechselt. Befindet man sich bereits im User-Modus, wird die Verbindung zum Switch geschlossen.

5.2.3 Beispiel zur Navigation durch die CLI-Hierarchieebenen und Nutzung des CLI

HINWEIS

Umkehren der Verhaltensweise von CLI-Kommandos mit dem Zusatz `no`

Viele CLI-Kommandos können durch Voranstellen des Befehls `no` in ihrer Bedeutung umgekehrt werden.

Beispiele:

- Aktivieren eines deaktivierten Ports: `L2Switch(config-if)# no shutdown`
- Löschen des VLAN 33: `L2Switch(config-if)# no vlan 33`

Die folgende Sequenz soll beispielhaft das Wechseln zwischen verschiedenen Hierarchieebenen und das Ausführen von Befehlen verdeutlichen. Es wird davon ausgegangen, dass eine Verbindung zum User-Modus des CLI aufgebaut wurde (siehe Abschnitt **Verbindungsaufbau zum CLI**):

1 Aufrufen des Privileged-Modus; hierzu ist es erforderlich, Zugangsdaten mit den Benutzerrechten „Normal (read only)“ oder „Admin“ zu verwenden:

```
L2Switch>enable
user:admin
password:
L2Switch#
```

2 Ausführen des Befehls `show hostname`, um den Namen des Switches anzuzeigen:

```
L2Switch#show hostname
The system's network name is "L2Switch".
```

3 Ändern des Switch-Namens in „NewName“ mit dem Befehl `hostname NewName;` der Befehl schlägt fehl, da der Befehl nur im Configuration-Modus ausgeführt werden darf:

```
L2Switch#hostname NewName
% Command incomplete.
```

4 Aufrufen des Configuration-Modus; diese Ebene kann nur aufgerufen werden, wenn das verwendete Benutzerkonto der Berechtigungsstufe „Admin“ angehört:

```
L2Switch#configure terminal
L2Switch(config)#
```

5 Ändern des Switch-Namens in „NewName“ mit dem Befehl `hostname NewName`:

```
L2Switch(config)#hostname NewName
Success!

NewName(config)#
```

6 Konfiguration der ETHERNET-Schnittstelle 5 auf 100 Mbit/s Vollduplex:

```
NewName(config)#interface gigabitethernet1/0/5
NewName(config-if)#speed 100-full
Success!

NewName(config-if)#
```

7 Verlassen des Interface-Modus:

```
NewName(config-if)#exit
NewName(config)#
```

8 Persistentes Speichern der Änderungen als „startup-config“:

```
L2Switch(config)#write memory
Success!
```

9 Verlassen des Configuration-Modus:

```
NewName(config)#exit
NewName#
```

10 Anzeigen des in Schritt 5 neu vergebenen Switch-Namens:

```
NewName#show hostname
The system's network name is "NewName".
```

5.2.4 Verwendung der Hilfsfunktionen im CLI

Integrierte Hilfe

Im CLI steht eine Hilfefunktion zur Verfügung, die durch die Eingabe von **?** aufgerufen wird.

Durch die Eingabe eines einzelnen **?** im CLI werden die zur Verfügung stehenden Befehle der jeweiligen Konfigurationsebene aufgelistet, z. B. für den VLAN-Sub-Modus:

```
L2Switch(config-vlan)# ?
  add             Adds Ports to be a permanent member of the VLAN group.
  end             End current mode and down to previous mode.
  exit            Exit current mode and down to previous mode.
  fixed           Assigns Ports to be a permanent member of the VLAN group.
  list            Prints command list.
  name            Assigns a name to the vlan.
  no              Negate a command or set its defaults.
  show            Display the vlan configurations.
  tagged          Assigns Ports for taged member of the VLAN group.
  untagged        Assigns Ports for untaged member of the VLAN group.
```

Die Parameter zu einem Befehl werden angezeigt, indem nach dem Befehlsnamen ein Leerzeichen gefolgt vom **?** eingegeben wird, z. B. für die Parameter des `time` Befehls:

```
L2Switch(config)#time ?
  TIME              Format: hour:minute:second.
  date              Sets the date on the Switch.
  daylight-saving-time  Configures the daylight saving time.
  ntp-server        The NTP server.
  timezone          Sets the timezone on the Switch.
```

Die Eingabe des **?** nach einem Parameter stellt die Syntax für Parameterwerte dar, z. B. beim Konfigurieren der Zeitzone:

```
L2Switch(config)#time timezone ?
  STRINGS           Sets the time difference between UTC and your time zone.
                    +hh / -hh / +hhmm / -hhmm
```

Vervollständigung von CLI-Kommandos

Durch die Verwendung der Tabulator-Taste können Befehle vervollständigt werden.

Wenn ein Befehl beim Drücken der Tabulator-Taste nicht eindeutig vervollständigt werden kann, werden die verfügbaren Befehle aufgelistet:

```
L2Switch(config)#d <Tab>
delete                deny                  diffserv              dot1x
```

Abkürzen von CLI-Kommandos

Wenn nach der Eingabe der ersten Buchstaben eindeutig auf ein Kommando geschlossen werden kann, muss das Kommando nicht ausgeschrieben werden. Zum Beispiel kann im User-Modus der Befehl `enable` zu `en` abgekürzt werden:

```
L2Switch>en
user:
```

Navigieren durch die Befehlshistorie

Mit den Steuerungstasten „↑“ und „↓“ kann durch den Verlauf der letzten Eingaben navigiert werden.

ⓘ HINWEIS

Einstellungen negieren

Für viele Befehle gibt es die Möglichkeit über das Voranstellen von `no` die gemachten Einstellungen zu negieren, z. B. `L2SWITCH(config-if-range)#no shutdown`, wodurch zuvor deaktivierte Ports wieder aktiviert werden.

5.3 Konfigurieren mit Netzwerkmanagement-Software

Eine Netzwerkmanagement-Software dient zur zentralen Überwachung und Konfiguration von Switches, Routern und weiteren Netzwerkkomponenten. Sie ermöglicht den Zugriff auf Geräteparameter, die Verwaltung von Firmware-Updates sowie die Analyse von Performance- und Fehlerzuständen. Über Funktionen wie eine Topologieübersicht, Syslog-Integration und proaktive Benachrichtigungen kann sie den effizienten Betrieb und die Fehlersuche im Netzwerk unterstützen.

Die WAGO Lean-Managed-Switches sind SNMP-fähig und ermöglichen so eine Integration in Netzwerkmanagement-Software.

Informationen zum Hinzufügen eines SNMP-fähiges Gerätes finden Sie in der Dokumentation Ihrer Netzwerkmanagement-Software. Der generelle Ablauf ist jedoch in der Regel folgender:

1 Aktivieren Sie SNMP auf dem Switch und konfigurieren Sie die Zugangsrechte, siehe Abschnitt **SNMP**.

2 Richten Sie die Management-Software ein. Geben Sie dazu folgende Daten ein: IP-Adresse, SNMP-Version und Zugangsdaten (bei SNMPv1/v2c: Community-String, bei SNMPv3: Benutzer/Passwort) des Switches. Führen Sie einen Verbindungstest durch.

3 Importieren Sie die von WAGO bereitgestellte MIB-Datei für den Switch in die Netzwerkmanagement-Software, um Zugriff auf WAGO-spezifische Parameter zu erhalten.

4 Konfigurieren Sie die Abfrageintervalle und die zu überwachenden Parameter.

5 Werten Sie die Ergebnisse aus und protokollieren Sie sie.

6 Service

6.1 Firmwareänderungen

HINWEIS

Verwenden Sie nur aktuelle Firmware

Die aktuelle Firmwareversion finden Sie im Internet unter **https://downloadcenter.wago.com/**.

HINWEIS

Während des Updatevorgangs dürfen keine produktiven Netzwerkverbindungen über den Switch laufen. Die neue Firmware ist nach einem Neustart des Geräts aktiv.

- Die vom Switch verwendete Firmware kann im WBM ermittelt werden. Die **aktuell verwendete** Firmwareversion (Zeile „Firmware Version“) wird im WBM auf der Seite „Informationen“ – „Device Status“ angezeigt.
- Um die vom Switch verwendete Firmware über das CLI zu ermitteln, kann folgender Befehl verwendet werden: `L2SWITCH# show model`

6.1.1 Firmware-Update mit dem WBM durchführen

Bei WAGO Switches können Firmware-Upgrades durchgeführt werden, um Fehler zu beheben und neue Funktionen bereitzustellen.

Prüfen Sie im WAGO Download Center (**https://downloadcenter.wago.com**), ob eine neue Firmware für Ihren Switch zur Verfügung steht. Wenn dies der Fall ist, laden Sie die Firmware herunter und überprüfen Sie die Release-Note und weitere mitgelieferte Dokumente auf Hinweise zum Firmware-Update. Der Firmware-Update-Prozess kann anschließend wie folgt ausgeführt werden:

1 Starten Sie einen Browser und rufen Sie das WBM des Switches auf. Weitere Informationen zum Login im WBM finden Sie im Abschnitt **Arbeiten im WBM**.

2 Klicken Sie im Reiter „Maintenance“ im Bereich „Upgrade Firmware“ auf das Feld „Choose file“ und wählen Sie die heruntergeladene *.fw-Datei aus.

3 Übertragen Sie durch Klick auf die Upload-Schaltfläche die Firmware auf den Switch.

4 Warten Sie, bis der Update-Prozess beendet und der Switch wieder erreichbar ist. **Die Verbindung zwischen PC und Gerät und die Spannungsversorgungdürfen während des gesamten Aktualisierungsprozesses nicht unterbrochen werden!**

5 Führen Sie einen Funktionstest in Ihrer Anwendungsumgebung durch.

6.1.2 Firmware-Update per CLI durchführen

Bei WAGO Switches können Firmware-Upgrades durchgeführt werden, um Fehler zu beheben und neue Funktionen bereitzustellen.

Prüfen Sie im WAGO Download Center (**https://downloadcenter.wago.com**), ob eine neue Firmware für Ihren Switch zur Verfügung steht. Wenn dies der Fall ist, laden Sie die Firmware herunter und überprüfen Sie die Release-Note und weitere mitgelieferte Dokumente auf Hinweise zum Firmware-Update. Der Firmware-Update-Prozess kann anschließend wie folgt ausgeführt werden:

1 Bauen Sie eine Terminalverbindung auf und wechseln Sie in den Configuration-Modus, siehe **Konfigurieren mit dem CLI**.

2 Starten Sie das Firmware-Update mit dem Befehl

```
archive download-fw ...
```

Geben Sie statt `...` den Server-Speicherort der neuen Firmware an, z. B. „http://192.168.1.1/newFirmware.fw“. Der Switch lädt die Firmware anschließend vom Server herunter und installiert sie im Gerät.

3 Warten Sie, bis der Update-Prozess beendet und der Switch wieder erreichbar ist. **Die Verbindung zwischen PC und Gerät und die Spannungsversorgungdürfen während des gesamten Aktualisierungsprozesses nicht unterbrochen werden!**

4 Führen Sie einen Funktionstest in Ihrer Anwendungsumgebung durch.

6.2 Zurücksetzen auf Werkseinstellungen

Ein Zurücksetzen auf die Werkseinstellungen kann erforderlich werden, wenn z. B. fehlerhafte Konfigurationen in die „startup config“ übernommen wurden, Zugriffsparameter nicht mehr bekannt sind oder das Gerät aufgrund inkonsistenter Einstellungen nicht mehr vollständig erreichbar ist. Das Zurücksetzen auf die Werkseinstellungen kann bis zu zwei Minuten dauern; hierbei wird ein Neustart durchgeführt.

Zurücksetzen via Hardware-Taster

Das Gerät kann durch Drücken des Reset-Tasters am Produkt (siehe Produkthandbuch) zurückgesetzt werden. Der Taster muss min. 10 Sekunden dauerhaft gedrückt werden. Andernfalls wird das Gerät lediglich neu gestartet.

Einige Produkte ermöglichen, den Reset-Taster softwareseitig zu deaktivieren, siehe **Reset-Button**.

Zurücksetzen via WBM

Rufen Sie das WBM auf (siehe **Arbeiten im WBM**) und klicken Sie im Register „Maintenance“, im Bereich „Reset Configuration“ auf die Schaltfläche „Reset“.

Zurücksetzen via CLI

Bauen Sie eine Verbindung zum CLI auf (siehe **Konfigurieren mit dem CLI**) und wechseln Sie in den Configuration-Modus. Das Wiederherstellen der Werksgrundeinstellungen erfolgt durch Ausführung des folgenden Befehls:

```
L2SWITCH(config)#reload default-config
```

7 Tabellenverzeichnis

Tabelle 1: Übersicht über die Port Counter 12
Tabelle 2: Port-Counter CLI 13
Tabelle 3: Running-Configuration CLI 13
Tabelle 4: Übersicht über die Utilization-Information 13
Tabelle 5: Port-Utilization CLI 13
Tabelle 6: Übersicht zu den LLDP-Nachbarschaftsinformationen an den jeweiligen Ports 14
Tabelle 7: LLDP CLI 15
Tabelle 8: Manual-Registration CLI 15
Tabelle 9: Fieldbus-Priority CLI 16
Tabelle 10: Übersicht über die Konfigurationseinstellungen für die Loop-Detection 17
Tabelle 11: Loop-Detection CLI 18
Tabelle 12: Port-Mirror CLI 19
Tabelle 13: Port-Set-up CLI 20
Tabelle 14: Port-Priority CLI 22
Tabelle 15: PD-Alive-Check CLI 24
Tabelle 16: Übersicht über den PoE-Configuration-Status an den jeweiligen Ports 25
Tabelle 17: PoE-Configuration CLI 25
Tabelle 18: SNMP CLI 27
Tabelle 19: Übersicht über die konfigurierten Communities und die zugehörigen Einstellungen 28
Tabelle 20: SNMP v1/2c CLI 28
Tabelle 21: Übersicht über die Parameter der Trap-Receiver 28
Tabelle 22: SNMP-Trap CLI 29
Tabelle 23: SNMP Event CLI 30
Tabelle 24: SNMPv3 View CLI 31
Tabelle 25: SNMPv3 Group CLI 32
Tabelle 26: Übersicht über die für Benutzer einstellbaren Sicherheitsstufen 32
Tabelle 27: Übersicht über die angelegten User und zugehörige Einstellungen 33
Tabelle 28: SNMPv3 CLI 33
Tabelle 29: SNTP CLI 37
Tabelle 30: Übersicht über die angelegten User und zugehörige Berechtigungen 38
Tabelle 31: User Account CLI 38
Tabelle 32: Reset-Button CLI 38
Tabelle 33: Storm-Control CLI 39
Tabelle 34: Übersicht über die konfigurierten Authentifizierungsmethoden an den jeweiligen Ports 42
Tabelle 35: 802.1X CLI 43
Tabelle 36: ACL CLI 45
Tabelle 37: Port Security CLI 47
Tabelle 38: Port-Security Advanced Status 48
Tabelle 39: Port Security Advanced CLI 48
Tabelle 40: Sticky-MAC-Whitelisting CLI 51
Tabelle 41: Service-Control CLI 52
Tabelle 42: Port-Isolation CLI 53

Tabelle 43: VLAN-Set-up CLI 55
Tabelle 44: ERPS CLI 58
Tabelle 45: STP/RSTP CLI 61
Tabelle 46: Übersicht über die STR/RSTP Port Parameter im CLI 62
Tabelle 47: ALM-Output 62
Tabelle 48: Übersicht über die Konfiguration für ALM-Output 63
Tabelle 49: ALM-Output 63
Tabelle 50: Übersicht über zusätzliche DIP-Schalter bei 852-1813/000-001 und 852-1813/010-001 63
Tabelle 51: DIP Status 64
Tabelle 52: Utilization-Tthreshold CLI 65
Tabelle 53: Modbus TCP CLI 68
Tabelle 54: Syslog CLI 69
Tabelle 55: Übersicht über die Funktionen im Menü „Maintenance“ 71
Tabelle 56: Maintenance – Upload and Download Configuration CLI 72
Tabelle 57: Beschreibung erweiterter Funktionen im CLI 72
Tabelle 58: Werksseitige Zugangsdaten 73
Tabelle 59: Unterschiede zwischen „running-config“ und „startup-config“ 79
Tabelle 60: Übersicht über die CLI-Ebenen 80

8 Abbildungsverzeichnis

Abbildung 1: Dashboard (Beispiel) 9
Abbildung 2: Topologie-Map – Anzeige mit Mouse-over (Beispiel) 10
Abbildung 3: Aufbau einer WBM-Seite (Beispiel) 11
Abbildung 4: Device-Status 12
Abbildung 5: LLDP Settings + LLDP Neighbor Information 14
Abbildung 6: Fieldbus-Priority 16
Abbildung 7: Loop-Detection – Configuration-Settings 17
Abbildung 8: Port Mirror Settings 18
Abbildung 9: Port-Set-up 20
Abbildung 10: Port Status 20
Abbildung 11: Port-Priority-Settings 21
Abbildung 12: PD Alive Check Settings 23
Abbildung 13: PD-Alive-Check Status 24
Abbildung 14: PoE-Configuration-Settings 24
Abbildung 15: General SNMP-Configuration 26
Abbildung 16: SNMP v1/2c 27
Abbildung 17: SNMP-Trap 28
Abbildung 18: SNMP – Trap Event State Settings 29
Abbildung 19: SNMP – Port Link-Change Trap Settings 30
Abbildung 20: SNMP – SNMPv3-View-Settings 31
Abbildung 21: SNMP – SNMPv3-Group 32
Abbildung 22: SNMP – SNMPv3-User 33
Abbildung 23: General Set-up – TCP-IP-Configuration 34
Abbildung 24: General Set-up – Hostname 34
Abbildung 25: General Set-up – Managed VLAN 35
Abbildung 26: SNTP 36
Abbildung 27: User Account – Add New User 37
Abbildung 28: Storm-Control – Settings 39
Abbildung 29: Wizard 40
Abbildung 30: 802.1X – Global Set-up 41
Abbildung 31: 802.1X – Port-Set-up 42
Abbildung 32: Access-Control-List-Settings 45
Abbildung 33: Port-Security 47
Abbildung 34: Port-Security Advanced 48
Abbildung 35: Auto-Learn und Aktivierung von Sticky-MAC-Whitelisting 49
Abbildung 36: Manuelles Hinzufügen von Adressen zur Sticky-MAC-Tabelle 50
Abbildung 37: Sticky-MAC-Tabelle 51
Abbildung 38: Service-Control 52
Abbildung 39: Port-Isolation 53
Abbildung 40: VLAN-Set-up 54
Abbildung 41: ERPS-Funktionsschema 56
Abbildung 42: ERPS-Set-up 57
Abbildung 43: STP/RSTP-Set-up 59

Abbildung 44: STR/RSTP Port-Set-up 60
Abbildung 45: Port-Utilization 65
Abbildung 46: Quick Diagnosis Dashboard 66
Abbildung 47: Modbus TCP 68
Abbildung 48: System Log 69
Abbildung 49: SSL-Certificate 70
Abbildung 50: Maintenance 71
Abbildung 51: Passwortänderung per Konfigurationsdatei 76
Abbildung 52: Aufbau des WBM 78
Abbildung 53: Wiederkehrende Einstellungsmöglichkeiten 78

WAGO GmbH & Co. KG
Postfach 2880 · 32385 Minden
Hansastraße 27 · D-32423 Minden
info@wago.com
www.wago.com

Zentrale	+49 (0) 571/887 – 0
Vert rieb	+49 (0) 571/887 – 44 222
Auftragsservice	+49 (0) 571/887 – 44 333
Fax	+49 (0) 571/887 – 844 169

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.
Copyright – WAGO GmbH & Co. KG – Alle Rechte vorbehalten. Inhalt und Struktur der WAGO Websites, Kataloge, Videos und andere WAGO Medien unterliegen dem Urheberrecht. Die Verbreitung oder Veränderung des Inhalts dieser Seiten und Videos ist nicht gestattet. Des Weiteren darf der Inhalt weder zu kommerziellen Zwecken kopiert, noch Dritten zugänglich gemacht werden. Dem Urheberrecht unterliegen auch die Bilder und Videos, die der WAGO GmbH & Co. KG von Dritten zur Verfügung gestellt wurden.