TECHDOCS

Podręcznik

Switche przemysłowe WAGO



852-1813/000-001

Switch zarządzalny Lean

8Port 1000BASE-T; 2Slot 1000BASE-FX/TX; 8 x PoE

Wersja 1.1.0

© 2026 WAGO Kontakttechnik GmbH & Co. KG
Wszystkie prawa zastrzeżone.

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

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

e-mail: info@wago.com

Internet: www.wago.com

Wsparcie techniczne

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

e-mail: support@wago.com

Zostały podjęte wszelkie możliwe działania w celu zapewnienia prawidłowości i kompletności niniejszej dokumentacji. Pomimo zachowania najwyższej staranności nie jest możliwe wykluczenie błędów, dlatego autorzy będą wdzięczni za wszelkiego rodzaju wskazania i sugestie.

e-mail: documentation@wago.com

Należy zwrócić uwagę na fakt, że zastosowane w niniejszym podręczniku nazwy sprzętu i oprogramowania oraz nazwy marek poszczególnych firm podlegają ochronie znaków towarowych, marek lub ochronie patentowej.

Znak WAGO jest zarejestrowanym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.

Spis treści

1 Wskazówki dotyczące dokumentacji 8
1.1 Zakres obowiązywania 8
1.2 Prawa autorskie 8
1.3 Symbole 9
1.4 Zastosowane systemy liczbowe 10
1.5 Sposoby zapisu 10

2 Ważne objaśnienia 11
2.1 Podstawy prawne 11
2.1.1 Zastrzeżenie prawa do zmian technicznych 11
2.1.2 Kwalifikacje personelu 11
2.1.3 Użytkowanie switcha przemysłowego zgodne z przeznaczeniem 11
2.1.4 Stan techniczny urządzeń 12
2.1.5 Dyrektywy i wymagania dla zastosowania switcha przemysłowego 12
2.2 Wskazówki dotyczące bezpieczeństwa 13
2.3 Specjalne warunki zastosowania urządzeń ETHERNET 15

3 Wprowadzenie 16
3.1 Zakres dostawy 16
3.2 Technologia sieci Industrial ETHERNET 16
3.3 Technologia switchingu 17
3.4 PoE (Power over Ethernet) 17
3.5 Autonegocjacja 17
3.6 Autocrossing 18
3.7 Tryb Store and Forward Switching 18
3.8 Metody transmisji 18

4 Opis urządzenia 19
4.1 Widok 20
4.1.1 Widok z przodu 20
4.1.2 Widok z góry 22
4.2 Złącza 23
4.2.1 Śruba uziemienia 23
4.2.2 Zasilanie (PWR/RPS) 24
4.2.3 Złącza sieciowe 25
4.2.3.1 Złącze RJ-45 26
4.2.3.2 Złącza 10/100/1000BASE-T 26
4.2.3.3 Złącza 10/100/1000BASE-T z PoE+ 26
4.2.3.4 Złącza 1000BASE-SX/-LX/-ZX lub 100BASE-FX 26
4.3 Elementy sygnalizacyjne 27
4.3.1 LED urządzeń 27
4.3.2 LED złącz 28
4.4 Elementy obsługi 29
4.4.1 Mikroprzełączniki DIP 29
4.4.2 Przycisk resetu 30
4.5 Naklejka 31
4.5.1 Wersja sprzętu i oprogramowania 31
4.6 Parametry techniczne 32

4.6.1 Dane urządzenia 32
4.6.2 Dane systemowe 32
4.6.3 Zasilanie 32
4.6.4 Power over Ethernet (PoE) 32
4.6.5 Komunikacja 33
4.6.6 Warunki środowiskowe 34
4.7 Aprobaty 35

5 Montaż 36

5.1 Miejsce montażu 36
5.2 Montaż na szynie 36
5.3 Demontaż z szyny 36

6 Podłączanie urządzeń 37

6.1 Zasilanie 37
6.2 Złącze zewnętrznego styku alarmowego 38
6.3 Złącze 1000BASE-SX/-LX/-ZX, 100BASE-FX, światłowód 39
6.4 Porty 10/100/1000BASE-T 40
6.5 Połączenie danych między switchami PoE / PSE (Power Sourcing Equipment) 40

7 Konfiguracja 43

7.1 Przegląd opcji konfiguracji 43
7.1.1 Web-Based-Management 43
7.1.2 Połączenie Telnet lub SSH 43
7.1.3 Dostęp przez port konsolowy Command-Line-Interface (CLI) 44

8 Diagnostyka z panelem i mapą topologii 45

8.1 System zarządzania przez WWW (WBM) dla funkcji diagnostycznej 46
8.1.1 CPU Loading 46
8.1.2 Memory Information 47
8.1.3 Obciążenie portu nadawczego 47
8.1.4 Obciążenie portu odbiorczego 48
8.1.5 Szybkość broadcast portu nadawczego 48
8.1.6 Szybkość broadcast portu odbiorczego 49
8.1.7 Port PoE 49
8.1.8 Statystyka rozłączeń portu 50
8.2 Kursor myszy na pulpicie diagnostycznym 51
8.3 Collapse, User Login, Topology Map 52

9 Konfiguracja w systemie zarządzania przez WWW (WBM) 56

9.1 Information 62
9.1.1 Device Status 62
9.1.2 Legal Information 64
9.1.3 Port Counter 65
9.1.4 Utilization Information 66
9.2 Configuration 67
9.2.1 Device Discovery 67
9.2.1.1 LLDP 67
9.2.1.2 Manual Registration 69
9.2.2 Interface 71
9.2.2.1 Loop Detection 71

9.2.2.1.1 Loop Recovery 71
9.2.2.2 Port mirroring (Mirror) 75
9.2.2.3 Port Setup 77
9.2.2.3.1 Port Settings 77
9.2.2.4 Priorytetyzacja portów ETHERNET (Port Priority) 83
9.2.3 PoE Settings 85
9.2.3.1 Aktywacja PoE dla portu (Power ON) 85
9.2.3.2 PD Alive Check 87
9.2.4 SNMP 91
9.2.4.1 Event Settings 92
9.2.4.2 Port Event Settings 94
9.2.4.3 SNMP Setup 96
9.2.4.4 SNMP Trap 98
9.2.4.5 SNMPv3 Group 100
9.2.4.6 SNMPv3 User 102
9.2.4.7 SNMPv3 View 104
9.2.5 System Management 106
9.2.5.1 General Setup 106
9.2.5.2 SNTP 109
9.2.5.3 User Account 113
9.2.6 Storm Control 116
9.3 Security 119
9.3.1 802.1X 119
9.3.1.1 Standard komunikacyjny IEEE 802.1X 119
9.3.1.2 Global Setup 123
9.3.1.3 Port Setup 127
9.3.2 Access Control List (ACL) 131
9.3.3 Port Security 134
9.3.4 Service Control 137
9.3.5 VLAN 139
9.3.5.1 Port Isolation 139
9.3.5.2 VLAN Setup 142
9.4 Redundancy 145
9.4.1 ERPS 145
9.4.2 STP/RSTP 151
9.4.2.1 STP/RSTP Setup 156
9.4.2.2 STP/RSTP Port Setup 157
9.5 Diagnostic 161
9.5.1 Alarm 161
9.5.1.1 Information 161
9.5.1.2 DIP Status 162
9.5.1.3 Traffic Flooding 164
9.5.1.4 Port Utilization 167
9.5.2 Dashboard Configuration 170
9.5.2.1 Quick Diagnosis Dashboard 170
9.5.2.1.1 Port Registration Learn 170
9.5.2.1.2 Port Link Down Statistics 171
9.5.2.1.3 Critical/Alert Threshold 172
9.5.3 Modbus 174
9.5.3.1 Format danych i kod funkcji 174

9.5.3.2 Rejestry Modbus 174
9.5.4 SNMP 175
9.5.5 System Log 176
9.5.5.1 Syslog Server Setting 176
9.6 Maintenance 179
9.6.1 Reboot 179
9.6.2 Upgrade Firmware 180
9.6.3 Upload Configuration 181
9.6.4 Download Configuration 182
9.6.5 Reset Configuration 183

10 Załącznik 184

10.1 Przewód RJ-45 184
10.2 Konfiguracja w Command Line Interface (CLI) 185
10.2.1 System Status 185
10.2.1.1 System Information 185
10.2.2 Default Settings 186
10.2.2.1 System 186
10.2.2.2 Jumbo Frame 187
10.2.2.3 SNTP 188
10.2.2.4 Management Host 189
10.2.2.5 MAC Management 190
10.2.2.6 Port Mirroring 190
10.2.2.7 Port Settings 191
10.2.3 Advanced Settings 192
10.2.3.1 Power over Ethernet (PoE) 192
10.2.3.2 PD Alive Check 193
10.2.3.3 Storm Control 195
10.2.3.4 VLAN 196
10.2.3.4.1 Port Isolation 196
10.2.3.4.2 VLAN Settings 197
10.2.3.5 LLDP 198
10.2.3.6 Loop Detection 199
10.2.3.7 STP 200
10.2.4 Security 203
10.2.4.1 Access Control List 203
10.2.5 Monitor 204
10.2.5.1 Alarm 204
10.2.5.2 Monitor Information 204
10.2.5.3 SFP Information 204
10.2.6 Management 205
10.2.6.1 SNMP 205
10.2.6.2 Maintenance 206
10.2.6.3 System Log 206
10.2.6.4 User Account 207
10.3 Tabele Modbus/TCP 208
10.3.1 Format danych i kod funkcji 208
10.4 Rejestry Modbus 208

Spis ilustracji 214

Spis tabel 217

1 Wskazówki dotyczące dokumentacji

Wskazówka



Zachować dokumentację!
Niniejsza dokumentacja jest częścią produktu. Dlatego należy ją przechowywać przez cały czas użytkowania produktu. Dokumentację tę należy przekazać kolejnemu właścicielowi lub użytkownikowi produktu. Należy również zapewnić aktualizację dokumentacji o pojawiające się uzupełnienia.

1.1 Zakres obowiązywania

Niniejsza dokumentacja odnosi się do produktu należącego do akcesoriów WAGO ETHERNET „Lean-Managed-Switch“ (852-1813/000-001).

1.2 Prawa autorskie

Niniejsza dokumentacja, wraz ze wszystkimi zawartymi w niej ilustracjami, jest chroniona prawami autorskimi. Wszelkie zastosowanie niniejszej dokumentacji niezgodne z przepisami prawa autorskiego jest zabronione. Reprodukcja, tłumaczenie na inne języki, jak również archiwizacja elektroniczna i fototechniczna i modyfikacja wymagają pisemnej zgody ze strony firmy WAGO GmbH & Co. KG, Minden. Nieprzestrzeganie tego zalecenia upoważnia do wnoszenia roszczeń odszkodowawczych.

1.3 Symbole

NIEBEZPIE-CZEŃSTWO



Ostrzeżenie przed obrażeniami ciała!
Oznaczenie bezpośredniego zagrożenia o wysokim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

NIEBEZPIE-CZEŃSTWO



Ostrzeżenie przed obrażeniami ciała spowodowanymi przez prąd elektryczny!
Oznaczenie bezpośredniego zagrożenia o wysokim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

OSTRZEŻENIE



Ostrzeżenie przed obrażeniami ciała!
Oznaczenie możliwego zagrożenia o średnim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

PRZESTROGA



Ostrzeżenie przed obrażeniami ciała!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia o niskim poziomie ryzyka, które, jeśli nie zostanie wyeliminowane, może spowodować niewielkie lub umiarkowane obrażenia ciała.

UWAGA



Ostrzeżenie przed szkodami materialnymi!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia, które, jeśli nie zostanie wyeliminowane, może doprowadzić do powstania szkód materialnych.

ESD



Ostrzeżenie przed szkodami materialnymi w następstwie wyładowań elektrostatycznych!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia, które, jeśli nie zostanie wyeliminowane, może doprowadzić do powstania szkód materialnych.

Wskazówka



Ważna wskazówka!
Wskazuje na prawdopodobieństwo nieprawidłowego funkcjonowania, która jednak, jeśli nie zostanie wyeliminowane, nie prowadzi do szkód materialnych.

Informacja



Dodatkowa informacja
Odsyła do dalszych informacji, niestanowiących istotnej części dokumentacji (np. do informacji zawartych na stronie www).

1.4 Zastosowane systemy liczbowe

Tabela 1: Zastosowane systemy liczbowe

System liczbowy	Przykład	Uwaga
Dziesiętny	100	Zwykły zapis
Szesnastkowy	0x64	Notacja szesnastkowa
Binarny	'100' '0110.0100'	Zapis w apostrofach, półbajt oddzielony kropką

1.5 Sposoby zapisu

Tabela 2: Sposoby zapisu

Zapis	Znaczenie
kursywa	Nazwy ścieżek i plików są zapisywane kursywą, np.: *C:\Programy\Oprogramowanie WAGO*
Menu	Punkty menu są pogrubione, np.: **Zapisz**
>	Znak „większy od“ między dwiema nazwami oznacza wybór określonego punktu menu, np.: **Plik > Nowy**
Pole edycji	Nazwy pól do wprowadzania lub wyboru danych są przedstawiane pogrubioną czcionką, np.: **Początek zakresu pomiarowego**
„wartość“	Wartości wprowadzane lub wybierane są zapisywane w cudzysłowie, np.: w polu **Początek zakresu pomiarowego** wprowadź wartość „4 mA“.
[Przycisk]	Nazwy przycisków znajdujących się w polach dialogowych są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. **[Wprowadzanie]**
[Klawisz]	Nazwy klawiszy na klawiaturze są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. **[F5]**

2 Ważne objaśnienia

Rozdział ten zawiera wyłącznie zestawienie najważniejszych zasad bezpieczeństwa oraz wskazówek. Zostaną one także przedstawione w poszczególnych rozdziałach. W celu ochrony przed obrażeniami ciała oraz zapobiegania uszkodzeniom urządzeń, konieczne jest staranne zapoznanie się ze wskazówkami dotyczącymi bezpieczeństwa oraz ich przestrzeganie.

2.1 Podstawy prawne

2.1.1 Zastrzeżenie prawa do zmian technicznych

Firma WAGO Kontakttechnik GmbH & Co. KG zastrzega sobie prawo do zmian. W przypadku udzielania patentu lub ochrony wzoru użytkowego, wszystkie prawa są zastrzeżone dla WAGO Kontakttechnik GmbH & Co. KG. Produkty obce są wymieniane bez podawania informacji o prawach patentowych. Dlatego nie można wykluczyć istnienia tego rodzaju praw.

2.1.2 Kwalifikacje personelu

Wszystkie prace przy urządzeniach z serii 852 mogą być wykonywane wyłącznie przez wykwalifikowanych elektryków z odpowiednią wiedzą fachową w zakresie techniki automatyzacji. Osoby te muszą znać aktualne normy i wytyczne dotyczące AKPiA.

Wszelkie ingerencje w układ sterowania wolno wykonywać wyłącznie specjalistom, dysponującym odpowiednią wiedzą z zakresu programowania PLC.

2.1.3 Użytkowanie switcha przemysłowego zgodne z przeznaczeniem

Urządzenie posiada klasę ochronności IP30. Jest chronione przed wniknięciem ciał stałych o średnicy do 2,5 mm, jednak nie przed wnikaniem wody. Jeśli nie podano inaczej, urządzenie nie może być eksploatowane w środowisku charakteryzującym się wilgocią i występowaniem pyłów.

2.1.4 Stan techniczny urządzeń

Urządzenia są dostarczane na potrzeby danego zastosowania, w sprzętowej i programowej konfiguracji fabrycznej. Nie zawierają żadnych części, które wymagają od użytkownika konserwacji czy napraw. Następujące czynności powodują wyłączenie odpowiedzialności WAGO Kontakttechnik GmbH & Co. KG:

- naprawy
- wprowadzanie zmian w sprzęcie lub oprogramowaniu, które nie są opisane w instrukcji obsługi
- użycie komponentów niezgodnie z ich przeznaczeniem

Dalsze szczegóły podano w umowach kontraktowych. Prośby i zapytania dotyczące zmiany konfiguracji lub nowej konfiguracji osprzętu i oprogramowania należy kierować do firmy WAGO Kontakttechnik GmbH & Co. KG.

2.1.5 Dyrektywy i wymagania dla zastosowania switcha przemysłowego

Przy instalacji należy uwzględnić istotne dyrektywy i normy:

- W celu wyeliminowania błędów instalacyjnych i zagrożeń dla pracowników, przewody sieciowe i komunikacyjne muszą być podłączone i zainstalowane zgodnie z dyrektywami.

- Przy instalacji, uruchamianiu, konserwacji i naprawach urządzeń należy uwzględnić przepisy związane z zapobieganiem wypadkom (np. przepis 3 DGUV „Instalacje i urządzenia elektryczne“).

- Nie wolno dezaktywować funkcji i urządzeń awaryjnego wyłączania lub w jakichkolwiek inny sposób uniemożliwiać ich działanie. Patrz istotne dyrektywy (np. EN 418).

- Wyposażenie instalacyjne musi odpowiadać dyrektywom EMC, aby wykluczyć zakłócenia elektromagnetyczne.

- Należy stosować środki ochrony przed wyładowaniami elektrostatycznymi zgodnie z normą DIN EN 61340-5-1/-3. Przy zastosowaniu modułów należy upewnić się, że są uziemione odpowiednie elementy środowiska (osoby, miejsce pracy i opakowanie).

- Należy przestrzegać dyrektyw i przepisów dotyczących instalacji obudów switcha.

2.2 Wskazówki dotyczące bezpieczeństwa

Przy zabudowie urządzenia w instalacji oraz w trakcie jego instalacji należy przestrzegać następujących zasad bezpieczeństwa:

NIEBEZPIECZEŃSTWO



Nie pracować przy urządzeniach znajdujących się pod napięciem!
Przed rozpoczęciem montażu, usuwania usterek lub prac konserwacyjnych należy zawsze odłączyć urządzenie od zasilania.

NIEBEZPIECZEŃSTWO



Montaż wyłącznie w obudowach, szafach lub rozdzielniach elektrycznych!
Akcesoria WAGO ETHERNET z serii 852 są urządzeniami o konstrukcji otwartej. Wolno je zabudowywać wyłącznie w obudowach, szafach lub rozdzielniach elektrycznych. Dostęp do nich powinien być możliwy wyłącznie dla wykwalifikowanego personelu posiadającego odpowiedni kluczyk lub narzędzie.

NIEBEZPIECZEŃSTWO



Przestrzegać przepisów dotyczących zapobiegania wypadkom!
W trakcie montażu, uruchamiania, eksploatacji, konserwacji i usuwania usterek należy zawsze przestrzegać przepisów dotyczących zapobiegania wypadkom, właściwych dla danej maszyny/instalacji (np. przepis 3 DGUV „Instalacje i urządzenia elektryczne“).

NIEBEZPIECZEŃSTWO



Podłączać urządzenie zgodnie z przepisami!
W celu wyeliminowania zagrożeń personelu oraz usterek instalacji przewody transmisji danych i zasilające należy układać zgodnie z obowiązującymi normami, pamiętając o odpowiednim usytuowaniu przyłączy. Należy przestrzegać zasad kompatybilności elektromagnetycznej dla danego zastosowania.

UWAGA



Nie stosować w sieciach telekomunikacyjnych!
Urządzenia ze złączem ETHERNET/RJ-45 należy używać wyłącznie w sieciach LAN. Nie należy ich łączyć z sieciami telekomunikacyjnymi, jak np. z liniami telefonicznymi analogowymi lub cyfrowymi (ISDN).

UWAGA



Wymienić wadliwe lub uszkodzone urządzenia!
Wadliwe lub uszkodzone urządzenia (np. ze zdeformowanymi stykami) należy wymienić.

UWAGA



Chronić urządzenia przed materiałami o właściwościach pełzających i izolacyjnych!
Urządzenia nie są odporne na materiały o właściwościach pełzających i izolacyjnych, jak np. aerozole, silikony, trójglicerydy (składnik kremu do rąk). Jeżeli nie da się wykluczyć obecności tych substancji w pobliżu urządzeń, należy umieścić urządzenia w obudowie odpornej na działanie ww. środków. Generalnie do obsługi urządzeń należy używać czystych narzędzi i materiałów.

UWAGA



Czyścić wyłącznie przy użyciu dozwolonych materiałów!
Obudowę i zabrudzone styki wolno czyścić wyłącznie przy użyciu propanolu.

UWAGA



Nie stosować sprayu do styków!
Nie należy stosować sprayu do styków, gdyż w połączeniu z zanieczyszczeniami może on pogorszyć jakość miejsca styku.

UWAGA



Unikać zmian biegunowości!
Należy unikać zmiany biegunowości przewodów transmisji danych i zasilających, gdyż może to spowodować uszkodzenia urządzenia.

ESD



Unikać wyładowań elektrostatycznych!
W urządzeniu zintegrowane są komponenty elektroniczne, które mogą zostać zniszczone przez wyładowania elektrostatyczne w następstwie dotknięcia. Należy stosować środki ochrony przed wyładowaniami elektrostatycznymi zgodnie z normą DIN EN 61340-5-1/-3. Przy obsłudze urządzenia należy pamiętać o odpowiednim uziemieniu otoczenia (osoby, stanowisko pracy oraz opakowanie).

PRZESTROGA



Ostrzeżenie przed promieniami laserowymi
Nie należy zaglądać do otworów złącz, jeśli nie jest do nich podłączony przewód, aby nie narażać się na promieniowanie.
Emitowane promieniowanie może być niewidoczne.
Chodzi tu o laser klasy 1 zgodnie z EN 60825-1.

Wskazówka



Zakłócenia komunikacji radiowej w pomieszczeniach mieszkalnych
To urządzenie jest urządzeniem klasy A. W pomieszczeniach mieszkalnych może ono powodować zakłócenie komunikacji radiowej. W takiej sytuacji można wymagać od operatora podjęcia odpowiednich środków.

2.3 Specjalne warunki zastosowania urządzeń ETHERNET

Tam gdzie nie ma specjalnych uwarunkowań, urządzenia ETHERNET można stosować w sieciach lokalnych. Przy wykorzystaniu urządzeń ETHERNET należy przestrzegać następujących zasad bezpieczeństwa:

- Komponentów systemu sterowania oraz sieci sterowniczych nie należy łączyć bezpośrednio z otwartą siecią, na przykład Internetem lub siecią biurową. WAGO zaleca umieszczenie sieci sterowniczych za firewallem.
- Fizyczny i elektroniczny dostęp do wszystkich komponentów automatyki należy ograniczyć do kręgu osób upoważnionych.
- Przed pierwszym uruchomieniem należy koniecznie zmienić ustawione standardowo hasła! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- Używane hasła należy regularnie zmieniać! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- W przypadku konieczności zdalnego dostępu do komponentów systemu sterowania i sieci sterowniczej, należy korzystać z sieci „Virtual Private Network“ (VPN).
- Należy regularnie przeprowadzać analizę zagrożeń. Pozwala to na sprawdzenie, czy podjęte działania odpowiadają wymogom w zakresie ochrony.
- Przy projektowaniu instalacji należy zastosować mechanizmy „Defense-in-depth“ w celu ograniczenia dostępu do indywidualnych produktów i sieci oraz ich kontroli.

3 Wprowadzenie

3.1 Zakres dostawy

- 1 przemysłowy switch zarządzalny Lean z wielowtykiem z zaciskiem CAGE CLAMP® (nr kat. 2231-106/026-000)
- Zaślepki ochronne dla niewykorzystanych złącz
- Instrukcja użytkowania i montażu

3.2 Technologia sieci Industrial ETHERNET

Switche zarządzalne Lean wyposażone są w wytrzymałą obudowę, przystosowaną do warunków przemysłowych i są w pełni kompatybilne z następującymi standardami:

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

Switche umożliwiają zasilanie w zakresie napięcia 24 V ... 57 V.

Funkcjonalność Power over Ethernet (PoE+) jest obsługiwana na 8 portach. Inne funkcjonalności to autonegocjacja i Auto-MDI/MDIX (crossover) na wszystkich portach 10/100/1000 BASE-T.

3.3 Technologia switchingu

W sieci Industrial ETHERNET wykorzystywana jest głównie technologia switchingu. W tej technologii każde urządzenie w sieci może w dowolnym momencie wysyłać dane, gdyż zawsze posiada swobodne połączenie punkt-punkt z następnym switchem. Połączenie to jest dwukierunkowe, czyli urządzenia mogą równocześnie wysyłać i odbierać dane (full duplex).
Celowe zastosowanie technologii switchingu może zwiększyć zdolność sieci do pracy w czasie rzeczywistym, gdyż dzięki połączeniu punkt-punkt pozwala uniknąć kolizji w komunikacji.

3.4 PoE (Power over Ethernet)

W technologii „Power over Ethernet” (PoE) zasilanie i przesył danych odbywają się jednocześnie i bezpiecznie tym samym przewodem ETHERNET. Dzięki temu można zrezygnować z oddzielnego przewodu zasilającego.
„Power over Ethernet” (PoE) to technologia sieci ETHERNET zdefiniowana w standardach IEEE 802.3af (PoE) i IEEE 802.3at (PoE+).
Jeśli obsługiwany jest standard IEEE 802.3at, przez przewód ETHERNET można przesyłać wyższy prąd.

3.5 Autonegocjacja

Autonegocjacja umożliwia switchowi rozpoznanie oraz odpowiednio automatycznie ustawienie prędkości transmisji i trybu pracy dla każdego portu i podłączonego do niego urządzenia bądź urządzeń. Ustawiany jest przy tym możliwie najwyższy tryb (prędkość transmisji i tryb pracy).
Autonegocjacja dostępna jest dla urządzeń w sieci ETHERNET, które połączone są ze switchem miedzianym przewodem.
W ten sposób switch staje się urządzeniem plug-and-play.

3.6 Autocrossing

Autocrossing (MDI/MDI-X, „Medium Dependent Interface“) przeprowadza w razie potrzeby automatyczne krzyżowanie przewodów nadawczych i odbiorczych na złączach skrętki. Dzięki temu użytkownik może w równym stopniu wykorzystywać 1:1 podłączone i skrzyżowane przewody (przewody cross over).

3.7 Tryb Store and Forward Switching

W trybie „Store and Forward“ switch ETHERNET zapisuje tymczasowo cały telegram danych, sprawdza go pod kątem ewentualnych błędów (suma kontrolna CRC) i w przypadku ich niestwierdzenia ustawia go w kolejce oczekujących. Następnie telegram danych („MAC Table“) zostaje przekierowany selektywnie do tego portu, który ma dostęp do zaadresowanego węzła.

Czas opóźnienia, jakiego potrzebuje telegram danych, aby przejść przez switch store-and-forward, zależy od długości telegramu.

Zaleta trybu „Store and Forward": telegramy danych sprawdzane są pod kątem poprawności i ważności. W ten sposób unika się rozprzestrzenianiu w sieci błędnych lub uszkodzonych telegramów danych.

3.8 Metody transmisji

Transmisja danych w sieciach ETHERNET może odbywać się w dwóch trybach:

- Half duplex
  - Urządzenie ETHERNET może w jednej chwili bądź tylko odbierać, bądź tylko wysyłać dane.
  - Rozpoznawanie kolizji (CSMA/CD) jest aktywne.
  - Rozległość sieci ograniczona jest przez zwłoki w pracy urządzeń i mediów transmisji.

- Full duplex
  - Urządzenie ETHERNET może równocześnie wysyłać i odbierać dane.
  - Rozpoznawanie kolizji (CSMA/CD) jest wyłączone.
  - Rozległość sieci uzależniona jest tylko od ograniczeń wydajności zastosowanych komponentów wysyłających i odbierających dane.

4 Opis urządzenia

852-1813/000-001 to przemysłowy, konfigurowalny switch ETHERNET z 8 portami 10/100/1000BASE-T, obsługującymi wszystkie Power over Ethernet (PoE+) 30 W, i 2 portami SFP 100BASE-FX/1000BASE-LX/SX/ZX (moduły SFP są dostępne opcjonalnie).
Wszystkich 8 portów PoE+ można używać równolegle (moc PoE: 24 V DC = 120 W lub 48 V DC = 240 W).
Switch ma wytrzymałą obudowę, jest zasilany redundantnie i sygnalizuje status za pomocą przekaźnika. Switch pozwala na proste zarządzane siecią: uruchamianie i diagnostykę można realizować intuicyjnie bez zaawansowanej wiedzy informatycznej.
Mapa topologii (Topology Map) przestawia w czytelny sposób switch i urządzenia podłączone do sieci. Na pulpicie diagnostycznym wizualizowane są ważne informacje o funkcjach urządzenia.

Poniższe funkcje zwiększają wytrzymałość, niezawodność i bezpieczeństwo w sieci:

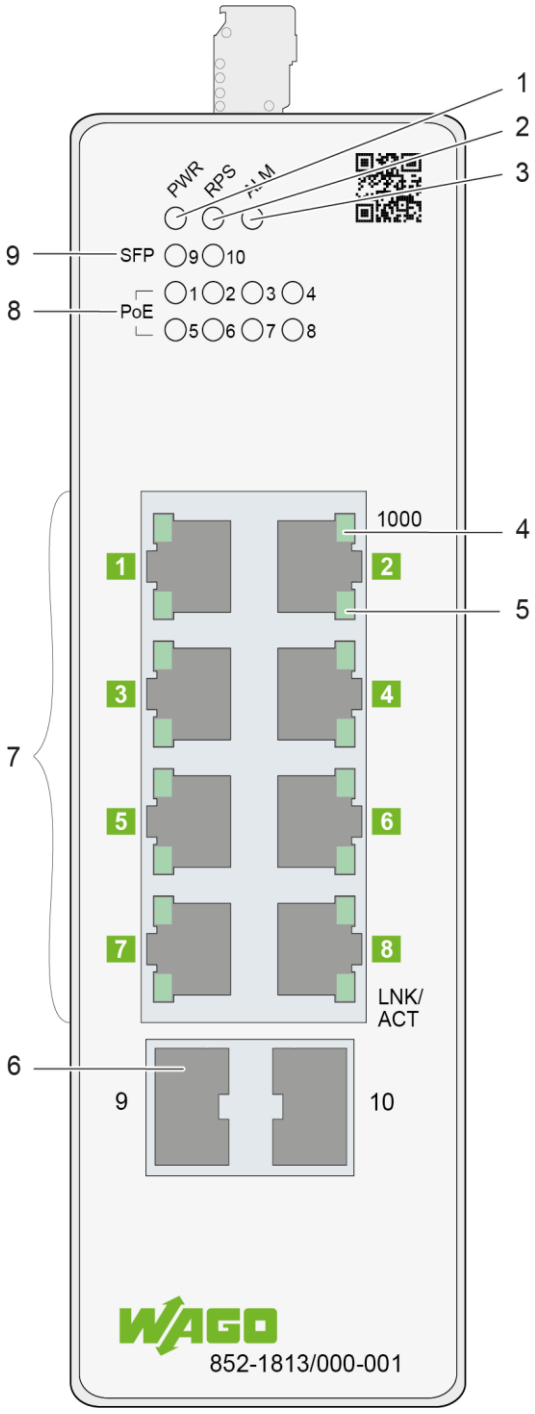
Bezpieczeństwo:
- Segmentacja sieci zgodnie z IEEE 802.1Q (maks. 5 VLAN),
- Uwierzytelnianie uczestników sieci zgodnie z IEEE 802.1X,
- Funkcje zapory sieciowej z Access-Control List (maks. 32 wpisy),
- Service Control,
- Port Security

Dostępność:
- Rapid Spanning Tree Protocol (RSTP) dla sieci kratowych i pierścieniowych
- ETHERNET Ring Protection Switching (ERPS) dla maksymalnie dwóch pierścieni na switch
- Loop Detection
- Storm Control na każdym porcie

Konfiguracja / diagnostyka / konserwacja:
- Port Mirroring,
- Rejestry Modbus®,
- SNMP v3,
- SNMP-Traps Events,
- Alarm Threshold,
- Port Statistic,
- Back-up and Restore,
- System Log,
- Syslog Server,
- Command Line Interface z SSH/Telnet,
- Topology Map
- Dashboard

4.1 Widok

4.1.1 Widok z przodu

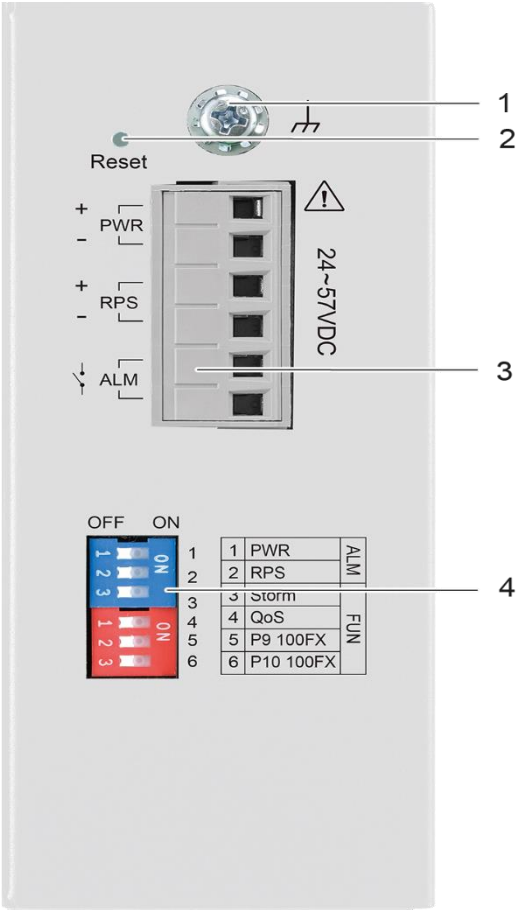


Ilustracja 1: Widok z przodu switcha zarządzalnego Lean

Tabela 3: Opis ilustracji „Widok z przodu switcha zarządzalnego Lean”

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
1	PWR	LED statusu napięcia zasilania	„Opis urządzenia“ > „Elementy sygnalizacyjne“
2	RPS	LED statusu redundantnego napięcia zasilania	„Opis urządzenia“ > „Elementy sygnalizacyjne“
3	ALM	LED statusu alarmu	„Opis urządzenia“ > „Elementy sygnalizacyjne“
4	-	LED statusu portu TX 1000 Mb/s (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
5	-	LED statusu portu TX LNK/ACT (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
6	-	Gniazdo SFP (1000BASE-SX/-LX/-ZX lub 100BASE-FX, światłowód) (2)	„Opis urządzenia“ > „Złącza“
7	-	Złącze RJ-45 (10/100M/1000BASE-T + PoE) (8)	„Opis urządzenia“ > „Złącza“
8	PoE	LED statusu PoE (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
9	SFP	LED statusu SFP (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“

4.1.2 Widok z góry



Ilustracja 2: Widok przemysłowego switcha zarządzalnego Lean z góry

Tabela 4: Opis ilustracji „Widok przemysłowego switcha zarządzalnego Lean z góry”

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
1	-	Śruba uziemienia	-
2	Reset	Przycisk resetu	„Opis urządzenia“ > „Elementy obsługi“
3	-	Wtyk (wielowtyk) do podłączenia zasilania (PWR/RPS/ALM) i bezpotencjałowego styku alarmowego	„Opis urządzenia“ > „Złącza“
4	-	Mikroprzełączniki DIP	„Opis urządzenia“ > „Elementy obsługi“

4.2 Złącza

4.2.1 Śruba uziemienia

Switch musi być uziemiony.
W tym celu należy połączyć śrubę uziemiającą z potencjałem uziemiania.
Nie należy dopuszczać do pracy switcha bez odpowiednio zainstalowanego przewodu PE.

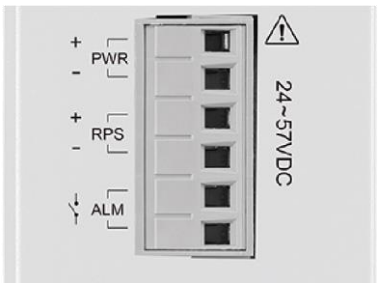


Ilustracja 3: Śruba uziemienia

4.2.2 Zasilanie (PWR/RPS)

Gniazdo (nr katalogowy 2231-106/026-000) można bez problemu połączyć z 6-biegunowym wtykiem, znajdującym się na górze switcha.

Wtyk składa się z następujących pinów:



Ilustracja 4: Złącze zasilające (PWR/RPS)

Tabela 5: Opis ilustracji „Złącze zasilające (PWR/RPS)”

Złącze	Nazwa	Opis
+	PWR	Podstawowe zasilanie prądem stałym
-	PWR	Podstawowe zasilanie prądem stałym
+	RPS	Rezerwowe zasilanie prądem stałym
-	RPS	Rezerwowe zasilanie prądem stałym
	ALM	Styk dla zewnętrznego alarmu
	ALM	Styk dla zewnętrznego alarmu

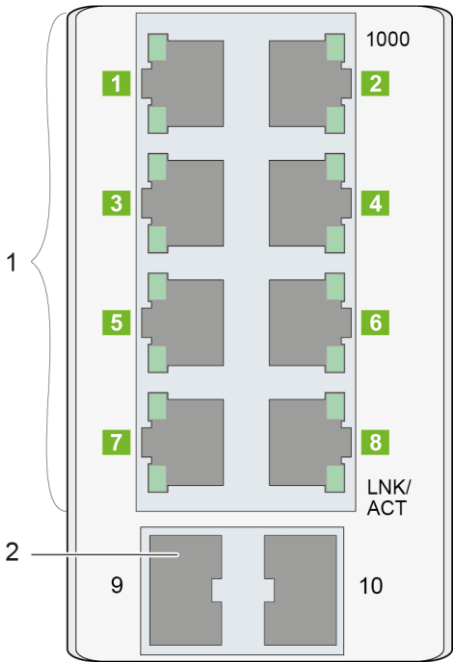
ESD



Ostrzeżenie przed szkodami materialnymi w następstwie wyładowań elektrostatycznych!
Praca switcha przy zasilaniu prądem stałym: zasilanie dostarczane jest z zewnętrznego źródła prądu stałego. Ponieważ switch nie ma wyłącznika sieciowego, włącza się natychmiast po wetknięciu zasilacza do gniazda zasilającego.

4.2.3 Złącza sieciowe

Switch zarządzalny Lean wykorzystuje złącza z wtykami światłowodowymi lub miedzianymi i wspiera ETHERNET, Fast-ETHERNET oraz Gigabit Ethernet.



Ilustracja 5: Złącza sieciowe

Tabela 6: Opis ilustracji „Złącza sieciowe”

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
1	-	Złącze RJ-45 (10/100/1000BASE-T) z PoE+ (8)	„Opis urządzenia“ > … „Złącza 10/100/1000BASE-T z PoE+”
2	-	Gniazda SFP (1000BASE-SX/-LX/-ZX lub 100BASE-FX, światłowód) (2)	„Opis urządzenia“ > … „Złącza 1000BASE-SX/-LX/-ZX lub 100BASE-FX”

4.2.3.1 Złącze RJ-45

Sieci obiektowe bazujące na sieci ETHERNET podłącza się za pomocą wtyków RJ-45.
Znaczenie pinów w wielowtykach RJ-45 do sieci ETHERNET określone zostało w dyrektywie EIA/TIA 568.
Kolory żył również są zgodne z tą dyrektywą. Znaczenie pinów i kolor żył są różne dla wykorzystanej liczby żył (4 lub 8 żył).

4.2.3.2 Złącza 10/100/1000BASE-T

Złącza 10/100/1000BASE-T wspierają prędkość sieci 10 Mbit/s, 100 Mbit/s i 1000 Mbit/s i mogą pracować w trybie transmisji half duplex i full duplex. Złącza te oferują ponadto automatyczne rozpoznawanie crossover (Auto-MDI/MDI-X) i mogą być wykorzystywane jako połączenia plug-and-play. Wystarczy po prostu wetknąć do złącz przewód zasilający, a one dopasowują się do urządzeń końcowego węzła. Dla złącz RJ-45 zalecane są następujące przewody:

- Kat. 5e lub lepsza z przewodem o długości maks. 100m

4.2.3.3 Złącza 10/100/1000BASE-T z PoE+

Złącza 10/100/1000BASE-T obsługują Power over Ethernet+ (PoE+) do 30 W na port.

Zalety:

- Brak konieczności oddzielnego zasilania urządzeń końcowych obsługujących PoE+
- Brak konieczności oddzielnych przewodów danych i zasilających

Wskazówka



Zwrócić uwagę na moc PoE.
Moc PoE dla ≥ 24 … < 48 V DC wynosi 120 W.
Moc PoE dla ≥ 48 … 57 V DC wynosi 240 W.

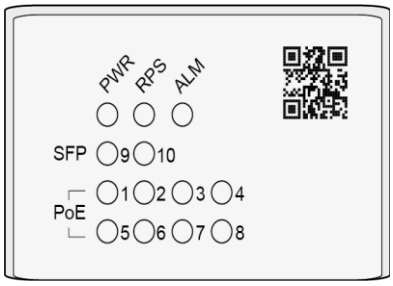
4.2.3.4 Złącza 1000BASE-SX/-LX/-ZX lub 100BASE-FX

Złącza 1000BASE-SX/-LX/-ZX domyślnie przeznaczone są do podłączania modułów Gigabit SFP.
Dodatkowo możliwe jest połączenie 100BASE-FX z prędkością sieci 100 Mb/s.
Wybór prędkości w gniazdach SFP realizuje się za pomocą mikroprzełączników DIP (zob. rozdział „Elementy sterujące“ > „Mikroprzełącznik DIP”).

4.3 Elementy sygnalizacyjne

Przemysłowy switch zarządzalny wyposażony jest we wskaźniki LED dla urządzeń i złącz. Na podstawie LED urządzeń można szybko rozpoznać status switcha, LED złącz natomiast informują o procesach łączeniowych.

4.3.1 LED urządzeń

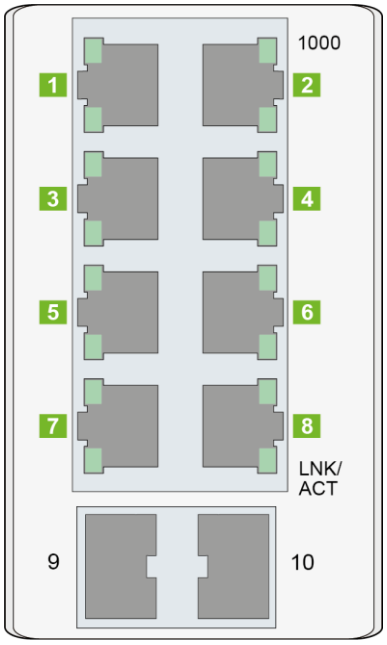


Ilustracja 6: LED urządzeń

Tabela 7: Opis ilustracjii „LED urządzeń“

LED		Nazwa	Status	Opis
PWR		Primary-Power-LED	zielony	Zastosowanie zasilacza podstawowego
			wył.	Zasilacz podstawowy wyłączony lub błąd
RPS		Redundant-Power-System-LED	zielony	Zastosowanie zasilacza rezerwowego
			wył.	Zasilacz rezerwowy wyłączony lub błąd
ALM		Alarm-LED	czerwony	Awaria połączenia z portem, inny alarm
			wył.	Nie zgłoszono alarmu
SFP	9, 10	SFP-Port-LED	zielony	Gniazdo SFP działa
			miga	Transmisja danych przez złącze
			wył.	Odłączenie złącza lub brak połączenia
PoE	1 … 8	LED portu PoE	zielony	Zasilanie przez złącze
			wył.	Brak zasilania

4.3.2 LED złącz



Ilustracja 7: LED złącz

Tabela 8: Opis ilustracji „LED złącz“

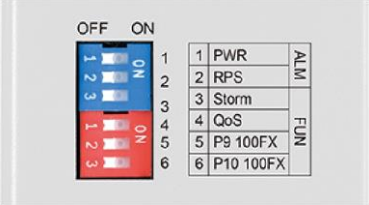
LED	Nazwa	Status	Opis
1000	LED złącza 1000BASE-T (1 LED dla każdego złącza)	zielony	Złącze działa z prędkością 1000 Mb/s
		wył.	Odłączenie złącza lub brak połączenia
LNK/ACT	LED złącza 10/100BASE-T (1 LED dla każdego złącza)	zielony	Złącze działa z prędkością 10/100/1000 Mb/s
		miga	Transmisja danych przez złącze
		wył.	Odłączenie złącza lub brak połączenia

4.4 Elementy obsługi

4.4.1 Mikroprzełączniki DIP

Na górze switcha zarządzalnego Lean znajdują się dwa mikroprzełączniki DIP, służące do konfiguracji alarmu. Przy aktywowanej funkcji zgłaszania alarmu przy wystąpieniu zdarzenia styk alarmowy zostaje załączony.

Znaczenie ustawień mikroprzełączników DIP objaśniono poniżej.



Ilustracja 8: Mikroprzełączniki DIP

Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“

Nr	Nazwa	Status	Opis
1	PWR	ON	Funkcja alarmu dla zasilacza podstawowego jest aktywowana
		OFF	Funkcja alarmu dla zasilacza podstawowego jest dezaktywowana.
2	RPS	ON	Funkcja alarmu dla zasilacza rezerwowego jest aktywowana
		OFF	Funkcja alarmu dla zasilacza rezerwowego jest dezaktywowana.
3	Storm	ON	Funkcja Storm Control jest aktywowana (300 pakietów na sekundę, Broadcast/DLF).
		OFF	Funkcja Storm Control jest sterowana przez oprogramowanie.
4	QoS	ON	QoS aktywny na porcie na porcie 1 ... 2.
		OFF	Funkcja Quality of Service jest sterowana przez oprogramowanie.
5	P9 100FX	ON	Złącze działa z prędkością 100 Mb/s.
		OFF	Złącze działa z prędkością 1000 Mb/s.
6	P10 100FX	ON	Złącze działa z prędkością 100 Mb/s.
		OFF	Złącze działa z prędkością 1000 Mb/s.

Użytkownik może ręcznie włączać i wyłączać funkcję alarmu dla zasilania podstawowego lub redundantnego przy użyciu mikroprzełączników DIP.

Aby móc aktywować funkcję alarmu dla złącza mikroprzełącznik DIP musi być ustawiony w pozycji „ON“. Ustawienie domyślne to pozycja „OFF“.

W celu konfiguracji i ustawienia mikroprzełączników DIP przy pierwszej instalacji zaleca się następujące działania:

1. Ustawić mikroprzełącznik DIP w pozycji „OFF“.
2. Zainstalować switch zarządzalny Lean w sieci.
3. Wybrać funkcję alarmu, która ma być aktywowana.
4. Ustawić mikroprzełącznik DIP danego złącza w pozycji „ON“.
5. Włączyć switch zarządzalny Lean.

4.4.2 Przycisk resetu



Ilustracja 2: Przycisk resetu

Tabela 2: Opis ilustracji „Przycisk resetu“

Nazwa	Status	Opis
Reset	Przycisk resetu należy nacisnąć na 2 sekundy, a następnie puścić.	System zostaje ponownie uruchomiony.
Stan fabryczny	Przycisk resetu należy nacisnąć na 10 sekund, a następnie puścić.	System zostanie przywrócony do ustawień fabrycznych.

Wskazówka

Ważna wskazówka!
Do naciśnięcia przycisku resetu można użyć odpowiedniego przyrządu (np. długopisu lub zagiętego spinacza).

4.5 Naklejka

4.5.1 Wersja sprzętu i oprogramowania

Z tyłu swicha zarządzalnego Lean znajduje się naklejka zawierająca dane: „MAC Address“ i „Serial NO“.



Ilustracja 9: Naklejka

Tabela 10: Opis ilustracji „Naklejka“

Nr	Opis „Serial NO“
01	Wersja firmware'u (lewy ciąg cyfr)
01	Wersja sprzętu (prawy ciąg cyfr)

4.6 Parametry techniczne

4.6.1 Dane urządzenia

Tabela 11: Dane techniczne – dane urządzenia

Szerokość	50 mm
Wysokość	120 mm (od górnej krawędzi szyny montażowej)
Głębokość	160 mm
Masa	560 g
Stopień ochrony	IP30

4.6.2 Dane systemowe

Tabela 12: Dane techniczne – dane systemowe

Tabela MAC	do 8000 adresów
VLAN	Port-based i Tag-based (maks. 5 VLAN)
Jumbo Frame Size	10 kB
Długość fali (światłowód)	zależnie od modułu SFP
Maksymalne długości	10/100/ 1000BASE-TX: 100 m; Światłowód: zależnie od modułu SFP

4.6.3 Zasilanie

Tabela 3: Dane techniczne – zasilanie

Napięcie zasilania	24 … 57 V DC
Maks. pobór mocy	13 W; 253 W przy 8 PoE+; 30 W na jedno złącze

4.6.4 Power over Ethernet (PoE)

Tabela 13: Dane techniczne – Power over Ethernet (PoE)

Dostępny przewód PD	25,50 W
Maks. moc dostarczana przez PSE	30 W
Napięcie (PD[1)])	50 … 57 V
Napięcie (PSE[2)])	24 … 57 V
Maks. prąd	600 mA
Maks. rezystancja	12,5 Ω (kategoria 5)
Moc PoE	120 W przy napięciu zasilania ≥24 … < 48 V DC 240 W przy napięciu zasilania 48 … 57 V DC
Tryb pracy obsługiwany przez PoE	Tryb A

[1)] PD = „Powered Device“

[2)] PSE = „Power Sourcing Equipment“

4.6.5 Komunikacja

Tabela 14: Dane techniczne – komunikacja

Porty (miedź; RJ-45)	8 x 10/100/1000BASE-T z PoE+
Porty (światłowód)	2 x 1000BASE-SX/-LX/-ZX lub 100BASE-FX (slot SFP)
Standardy	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/FX IEEE 802.3ab 1000BASE-T Ethernet IEEE 802.3z 1000BASE-SX/LX/ZX IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Prioritization IEEE 802.1x Port Authentication IEEE 802.1ab Link Layer Discovery Protocol (LLDP) IEEE 802.1AB LLDP-MED IEEE 802.3af Power over Ethernet (PoE) IEEE 802.3at High Power over Ethernet (PoE+) IEEE 802.3az Energy Efficient Ethernet (EEE) ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

4.6.6 Warunki środowiskowe

Tabela 15: Dane techniczne – Warunki środowiskowe

Temperatura otoczenia, praca	-40 … +60°C
Temperatura otoczenia, przechowywanie	-40 … +85°C
UL 61010 Użytkowanie Stopień zanieczyszczenia	 Wewnątrz pomieszczeń 2
Wilgotność względna (praca)	10 …95% (bez kondensacji)
Wilgotność względna (składowanie)	5 …95% (bez kondensacji)
Odporność na wibracje	zgodnie z IEC 60068-2-6
Odporność na wstrząsy	zgodnie z IEC 60068-2-27
EMC: odporność na zakłócenia	EN 55024 IEC 61000-4-2 IEC 61000-4-3 IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-6 IEC 61000-4-8 EN 61000-6-2
EMC: emisja zakłóceń	FCC Part 15 Subpart B klasa A EN 55011: klasa A EN 55032: klasa A EN 61000-6-4

4.7 Aprobaty

Aprobaty dla osprzętu WAGO-ETHERNET „Lean-Managed-Switch“ (852-1813/000-001):

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

5 Montaż

5.1 Miejsce montażu

Wybór miejsca montażu może mieć znaczny wpływ na wydajność switcha zarządzalnego Lean. Przy wyborze miejsca montażu zalecamy uwzględnienie następujących aspektów:

- Switch zarządzalny Lean należy instalować w odpowiednich warunkach. W rozdziale „Opis urządzenia“ > … > „Dane techniczne“ zamieszczono informacje o akceptowalnych zakresach roboczych temperatury i wilgotności powietrza.

Należy upewnić się, że zapewnione zostały odpowiednie warunki dla emisji ciepła przez swich zarządzalny Lean i odpowiednia wentylacja wokół niego. W pobliżu switcha zarządzalnego Lean nie należy umieszczać ciężkich obiektów.

5.2 Montaż na szynie

Szyna musi optymalnie wspierać zintegrowane w systemie środki EMC oraz ekranowanie przez styki modułu I/O.

Switch zarządzalny Lean należy zawiesić od góry na szynie i zamocować zatrzaskowo.

5.3 Demontaż z szyny

W celu demontażu z szyny należy wprowadzić odpowiedni przyrząd w znajdujący się pod switchem zarządzalnym Lean metalowy uchwyt i nacisnąć go do dołu.

Następnie można odczepić switch zarządzalny Lean od szyny i zdjąć go ruchem w górę.

6 Podłączanie urządzeń

6.1 Zasilanie

Switch wykorzystuje zasilanie prądem stałym w zakresie 24 …57 V.

Podstawowe i rezerwowe podłączenie do sieci realizowane jest przez 6-biegunowy wielowtyk, znajdujący się na górze switcha zarządzalnego Lean.

Gniazdo (nr katalogowy 2231-106/026-000) zawiera 6 zacisków przyłączeniowych i można je bez problemu połączyć ręcznie z 6-biegunowym wtykiem, znajdującym się na górze switcha, i równie łatwo rozłączyć.

Zasilacz switcha dopasowuje się automatycznie do lokalnego źródła napięcia i może włączyć się nawet wtedy, gdy nie są podłączone żadne lub nie wszystkie przewody.

1. Odpowiedni przewód uziemiający należy podłączyć do śruby uziemienia, znajdującej się na górze switcha.

2. Jeśli gniazdo nie zostało jeszcze wetknięte do wtyku, należy to uczynić teraz. Lekkim pociągnięciem należy sprawdzić czy gniazdo jest stabilnie zamocowane.

3. PWR +/-:
   W celu montażu lub demontażu przewodów, służących do zasilania podstawowego, należy wetknąć śrubokręt lub przyrząd montażowy bezpośrednio do zacisków gniazda i wprowadzić lub wyciągnąć przewód.

4. Gdy zasilacz podstawowy jest podłączony i aktywny, LED „PWR“ z przodu urządzenia świeci. Jeśli tak nie jest, należy upewnić się, że przewód zasilający jest właściwie podłączony i dobrze zamontowany.

5. RPS +/-:
   W celu montażu lub demontażu przewodów, służących do zasilania rezerwowego, należy wetknąć śrubokręt lub przyrząd montażowy bezpośrednio do zacisków gniazda i wprowadzić lub wyciągnąć przewód.

6. Gdy zasilacz rezerwowy jest podłączony i aktywny, LED „RPS” z przodu urządzenia świeci. Jeśli tak nie jest, należy upewnić się, że przewód zasilający jest właściwie podłączony i dobrze zamontowany.

6.2 Złącze zewnętrznego styku alarmowego

Switch zarządzalny Lean wyposażony jest w złącze styku alarmowego, znajdujące się na górze urządzenia. Szczegółowy sposób postępowania przy podłączaniu przewodu zasilającego do obu styków ALM 6-biegunowego gniazda można znaleźć w rozdziale „Zasilanie (PWR/RPS)“ (analogiczny sposób postępowania).

Bezpotencjałowy styk alarmowy można podłączyć do systemu diagnostycznego, zainstalowanego w dyspozytorni lub hali fabrycznej użytkownika. W przypadku wystąpienia awarii switch zarządzalny Lean poprzez styk alarmowy wysyła sygnał, aktywujący zewnętrzny alarm. Styk alarmowy ma dwa zaciski, służące jako obwód awaryjny do podłączania instalacji alarmowej.

Alarm zgłaszany jest w następujących przypadkach:

1 PWR/RPS:
   a Błąd zasilania (przerwanie przewodu zasilającego, awaria zasilania, itp.)
   b Wejściowe napięcie zasilające poza zakresem podanym w specyfikacji (24 … 57 V)

6.3 Złącze 1000BASE-SX/-LX/-ZX, 100BASE-FX, światłowód

Przy podłączaniu przewodu światłowodowego do złącza 1000BASE-SX/-LX lub 100BASE-FX przemysłowego switcha zarządzalnego należy zwrócić uwagę na prawidłowy typ wtyczki (LC) i modułu SFP.
Istnieją różne rodzaje modułów SFP: wielomodowe, jednomodowe lub WDM.
W celu poprawnego podłączenia przewodu światłowodowego należy wykonać opisane poniżej kroki:

Wskazówka

Gumowa pokrywa
Gumową pokrywę złącza 1000BASE-SX/LX lub 100BASE-FX należy zdjąć i zachować.
Jeśli moduł SFP nie jest podłączony, złącze powinno być dla ochrony zasłonięte gumową pokrywą.

1. Dany moduł SFP należy wetknąć i zablokować.

2. Należy upewnić się, że złącza światłowodowe są czyste. Wtyczki przewodów można czyścić, wycierając je czystą szmatką lub patyczkiem nasączonym etanolem. Zanieczyszczone końcówki światłowodu pogarszają jakość światła, transmitowanego przez przewód i obniżają wydajność złącza.

3. Wtyczkę LC należy połączyć z odpowiedni modułem SFP przemysłowego switcha zarządzalnego.

Wskazówka

Prawidłowe podłączenie przewodu światłowodowego do modułu SFP
Przy prawidłowym podłączeniu wtyczki przewodu światłowodowego do modułu SFP powinno być słyszalne zadziałanie zatrzasku.

4. Aby przekonać się, że połączenie zostało zrealizowane prawidłowo, należy sprawdzić, czy zaświeciła się odpowiednia LED złącza w przemysłowym switchu zarządzalnym (patrz rozdział „Opis urządzenia“> … > „Elementy sygnalizacyjne“).

6.4 Porty 10/100/1000BASE-T

Porty 10/100/1000BASE-T (złącza ETHERNET RJ-45) przemysłowego switcha zarządzalnego wspierają zarówno autosensing, jak i autonegocjację.

UWAGA



Unikać połączeń danych między portami PoE urządzeń zasilanych tym samym potencjałem!
Jeśli switche PoE korzystają z tego samego zasilania (tego samego potencjału), porty PoE nie mogą być bezpośrednio połączone ze sobą. Powstały w wyniku tego prąd zwarciowy uszkadza switche.

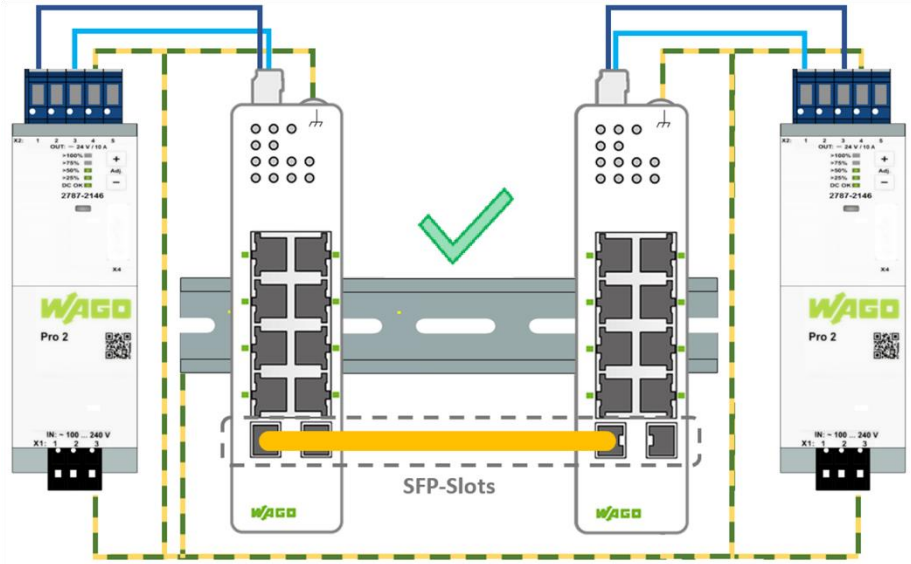
Więcej informacji można znaleźć w rozdziale „Połączenie danych między switchami PoE / PSE (Power Sourcing Equipment)“.

1. Wtyk przewodu skrętki kategorii 3/4/5/5e należy podłączyć do złącza RJ-45 przemysłowego switcha zarządzalnego, a drugi wtyk do wybranego węzła sieciowego.

2. Aby przekonać się, że połączenie zostało zrealizowane prawidłowo, należy sprawdzić, czy zaświeciła się odpowiednia LED złącza w przemysłowym switchu zarządzalnym.
(patrz rozdział „Elementy sygnalizacyjne“ > … > „LED złącz“).

6.5 Połączenie danych między switchami PoE / PSE (Power Sourcing Equipment)

Do utworzenia połączenia danych między dwoma switchami PoE należy użyć gniazd SFP.



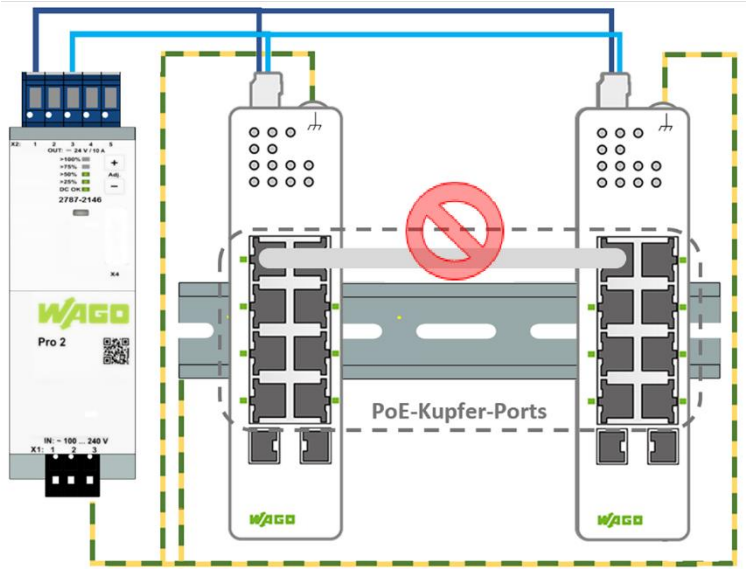
Ilustracja 10: Połączenie danych 01

Przy tworzeniu połączenia danych między dwoma swichami PoE przez porty PoE za pomocą przewodu miedzianego, do zasilania switchy należy użyć dwóch oddzielnych potencjałów.

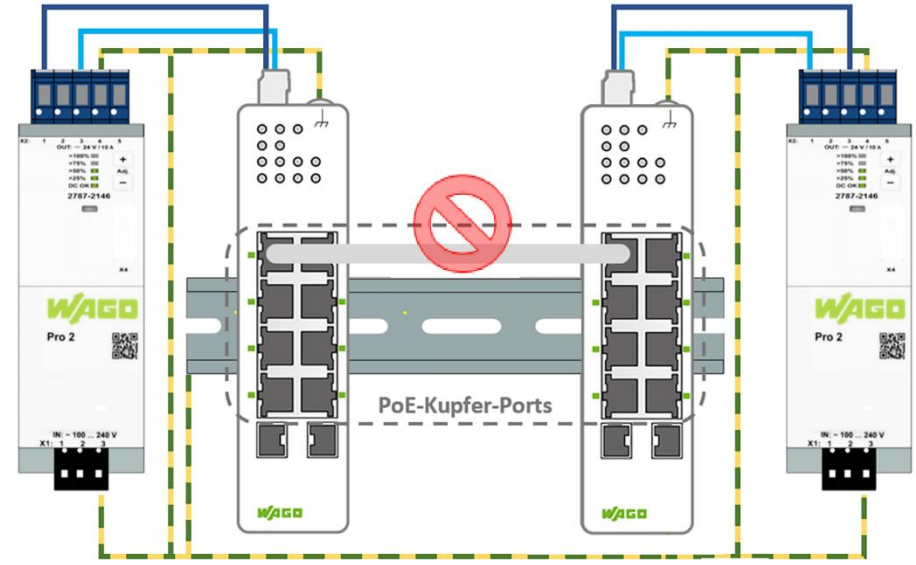
UWAGA



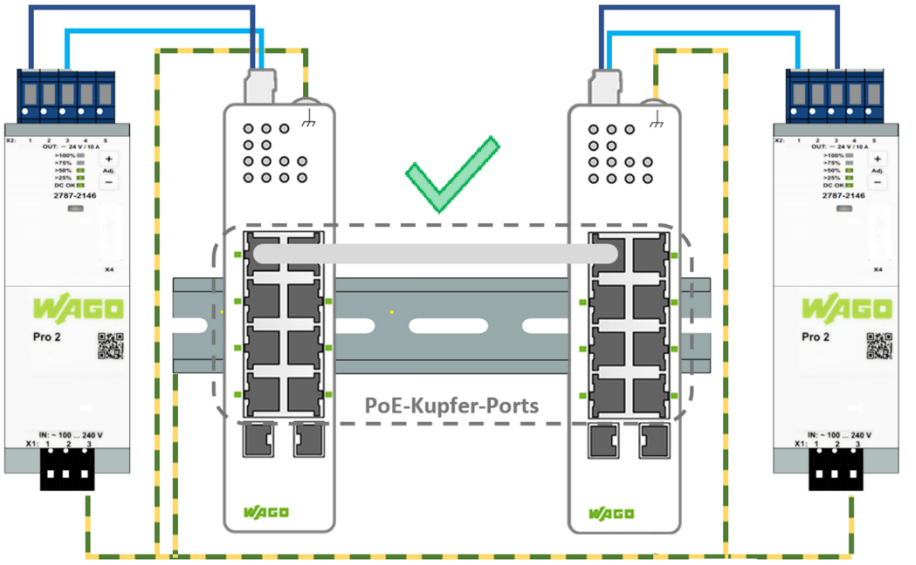
Użyć dwóch oddzielnych potencjałów!
Jeżeli zasilacze obu switchy PoE mają ten sam potencjał, może powstać zwarcie.
Powstały w wyniku tego prąd zwarciowy uszkadza switche.



Ilustracja 11: Połączenie danych 02

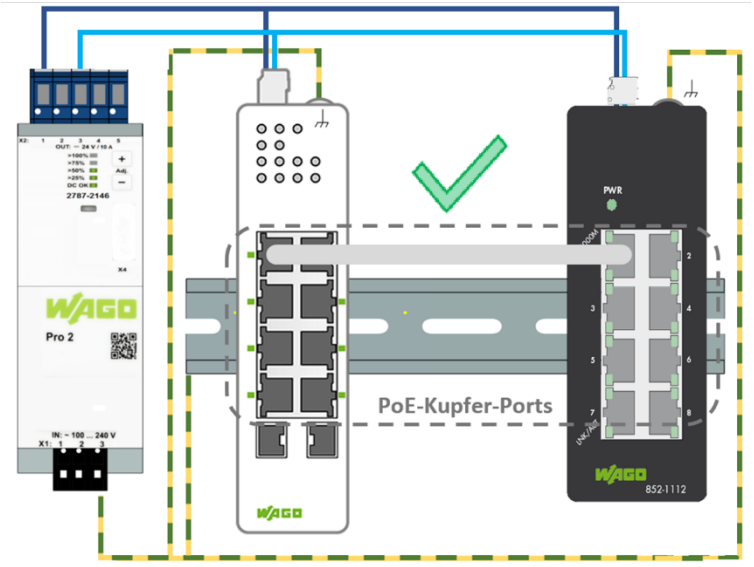


Ilustracja 12: Połączenie danych 03



Ilustracja 13: Połączenie danych 04

Nawiązanie połączenia danych między switchem nieobsługującym-PoE-a switchem obsługującym PoE nie podlega temu warunkowi.



Ilustracja 14: Połączenie danych 05

7 Konfiguracja

7.1 Przegląd opcji konfiguracji

Switch zarządzalny Lean oferuje trzy opcje zaawansowanych funkcji zarządzania:

7.1.1 Web-Based-Management

Interfejs użytkownika uruchamiany z menu można wywołać z WBM („Web Based Management“) za pomocą protokołów „http” lub „https”.

Wskazówka

Ustawienie standardowe
Standardowo switch zarządzalny Lean jest ustawiony na protokół „http”.

Wskazówka

Więcej informacji
Szczegółowy opis mona znaleźć w rozdziale „Konfiguracja w systemie zarządzania przez WWW (WBM)“.

7.1.2 Połączenie Telnet lub SSH

1. Komputer połącz z jednym z portów ETHERNET.

2. Otwórz sesję Telnet/SSH do adresu IP switcha. Gdy jest to pierwsze logowanie, zastosuj wartości domyślne.

Tabela 16: Domyślne ustawienia dla portu Telnet

Ustawienie	Wartość domyślna
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	wago

3. Upewnij się, że adres IP komputera znajduje się w tej samej podsieci – chyba że komunikujesz się ze switchem przez jeden lub kilka ruterów.

Wskazówka

Zastosowanie protokołu „Telnet“
Jeśli używany jest protokół „Telnet“, należy włączyć tę usługę (zobacz rozdział „Konfiguracja w systemie zarządzania przez WWW (WBM)“ > … > „Service Control“).

7.1.3 Dostęp przez port konsolowy Command-Line-Interface (CLI)

Poniżej opisano, jak wyświetlić konfigurację urządzenia przez port konsolowy (CLI).

1. Komputer połącz przez SSH lub Telnet z portem konsolowym (CLI) switcha.

2. Aby wywołać ekran logowania, kliknij [ENTER].

```
L2SWITCH login:
```

3. Wpisz **[admin]**, aby przejść do trybu CLI.

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

4. Wpisz **[enable]**, aby przejść do trybu uprzywilejowanego. Zastosuj następujące wartości standardowe dla nazwy użytkownika i hasła.

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

5. Wpisz **[show running config]**, aby zobaczyć aktualną konfigurację urządzenia.

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

Wskazówka



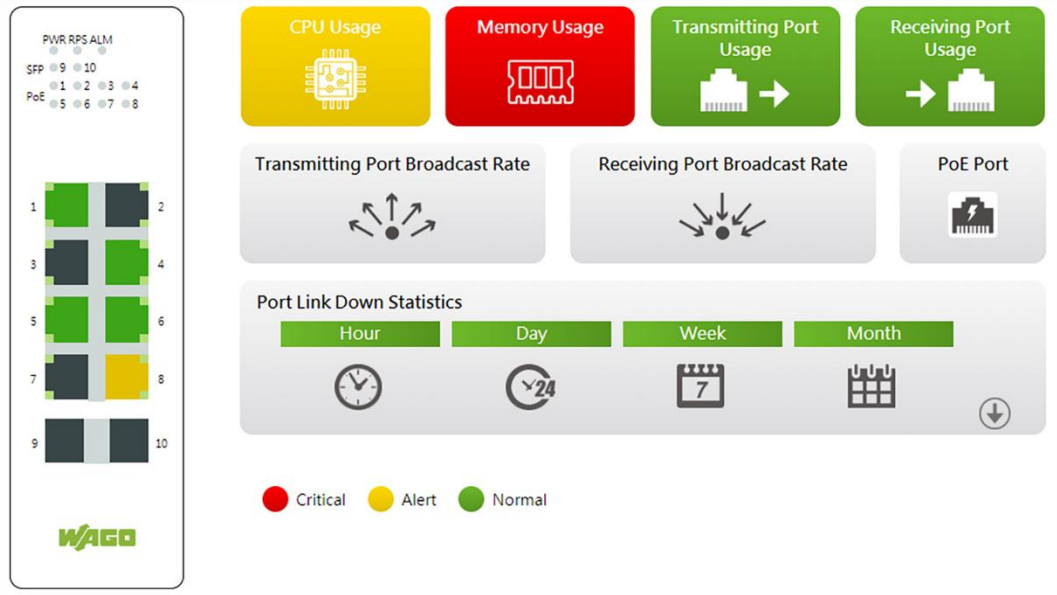
Więcej informacji
Szczegółowy opis można znaleźć w rozdziale „Załącznik“ > … > „Konfiguracja w Command Line Interface (CLI)“.

8 Diagnostyka z panelem i mapą topologii

Funkcja diagnostyczna może pomóc użytkownikom i administratorom sieci szybko zlokalizować, zdiagnozować i zidentyfikować problemy w systemie lub sieci. Jest to forma zarządzania siecią, która pomaga znaleźć problemy z łącznością, wydajnością i innymi obszarami sieci, a następnie mapuje je na panelu.

Wskazówka

Zmiana kolorów kafelków w przypadku przekroczenia progów
Dla uproszczenia diagnostyki można ustawić zmianę kolorów kafelków (czerwony, żółty i zielony) w przypadku przekroczenia lub spadku poniżej progu (zobacz rozdział „Dashboard Configuration“).

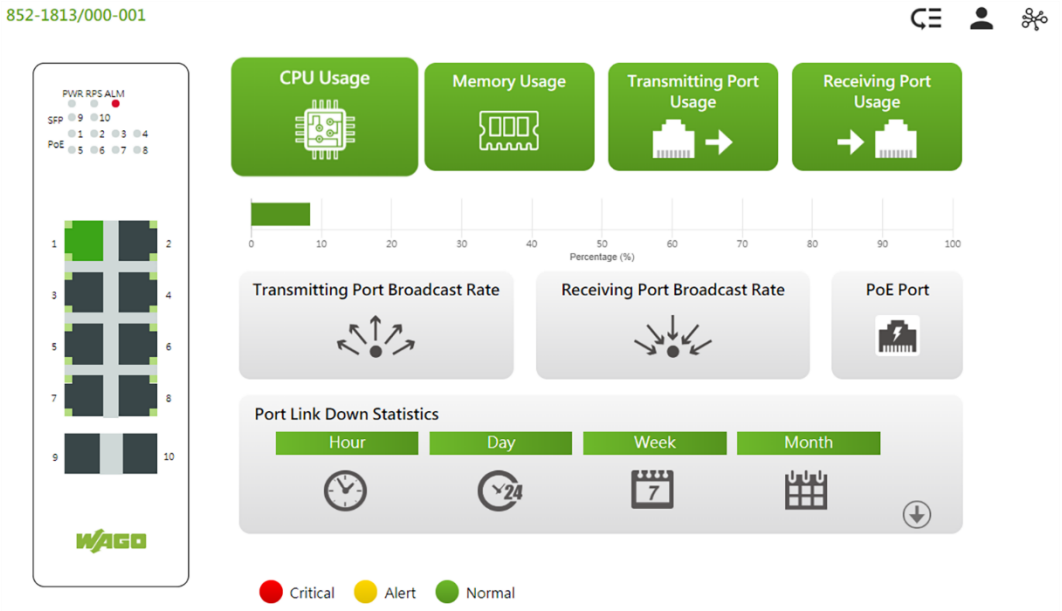


Ilustracja 15: Dashboard (przykład)

Wskazówka

Wyświetlanie LED „PWR” i „RPS” na panelu diagnostycznym
LED „PWR” i „RPS” nie są wyświetlane na panelu diagnostycznym.

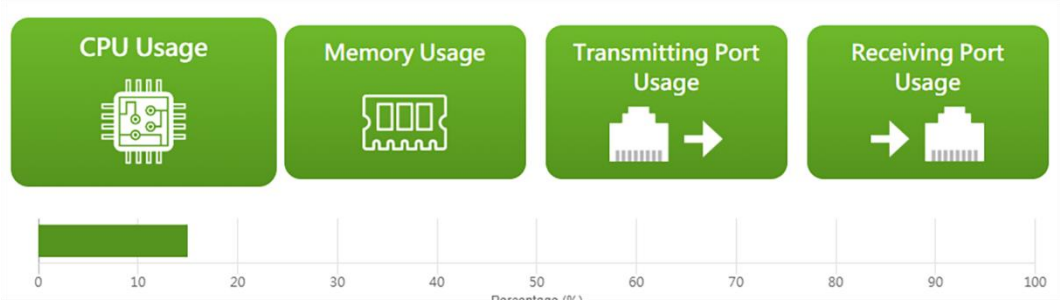
8.1 System zarządzania przez WWW (WBM) dla funkcji diagnostycznej



Ilustracja 16: Panel diagnostyczny

8.1.1 CPU Loading

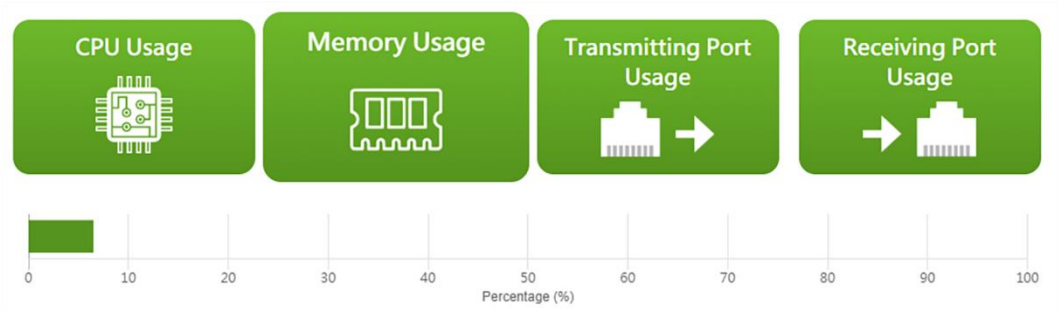
Użytkownicy mogą jednym kliknięciem wyświetlić obciążenie CPU switcha w procentach, jak pokazano poniżej.



Ilustracja 17: Obciążenie CPU

8.1.2 Memory Information

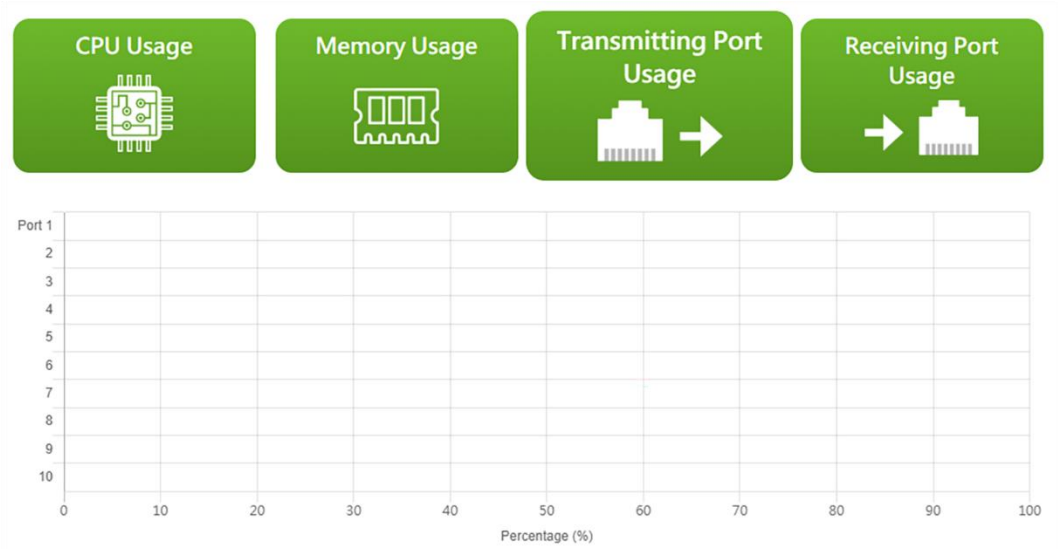
Użytkownicy mogą jednym kliknięciem wyświetlić obciążenie pamięci switcha w procentach, jak pokazano poniżej.



Ilustracja 18: Obciążenie pamięci

8.1.3 Obciążenie portu nadawczego

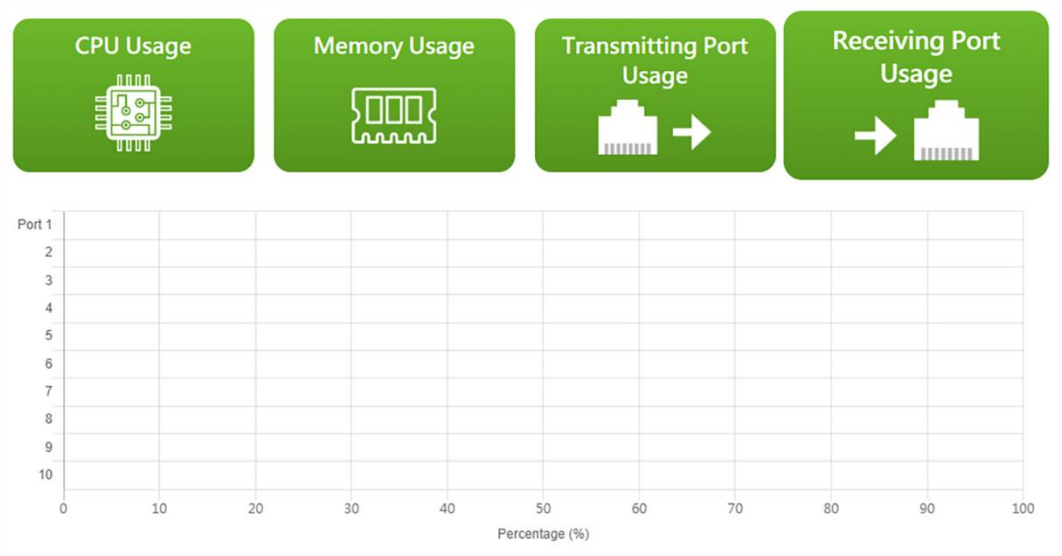
Użytkownicy mogą jednym kliknięciem wyświetlić obciążenie portu Tx switcha w procentach, jak pokazano poniżej.



Ilustracja 19: Obciążenie portu nadawczego (przykład)

8.1.4 Obciążenie portu odbiorczego

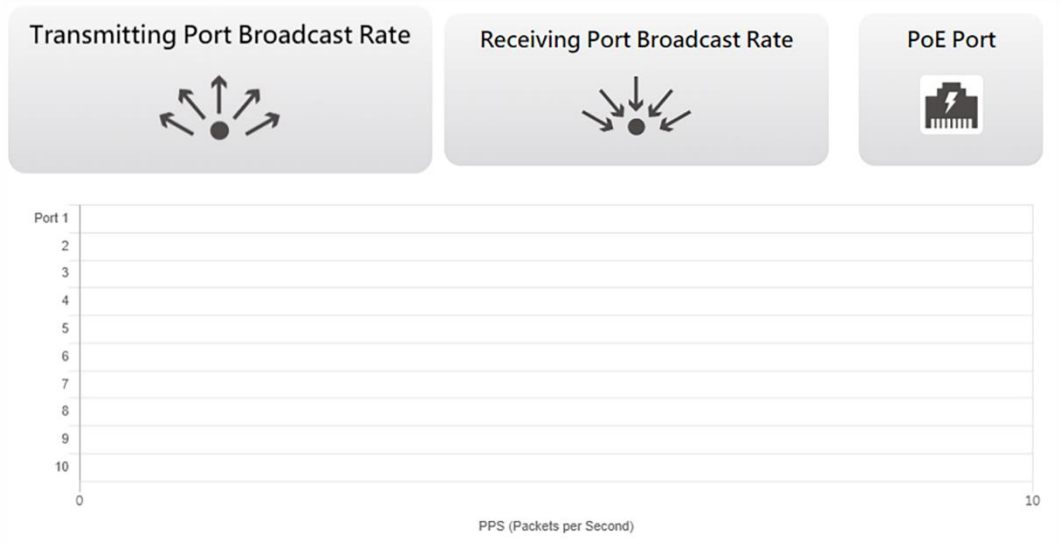
Użytkownicy mogą jednym kliknięciem wyświetlić obciążenie portu Rx switcha w procentach, jak pokazano poniżej.



Ilustracja 20: Obciążenie portu odbiorczego (przykład)

8.1.5 Szybkość broadcast portu nadawczego

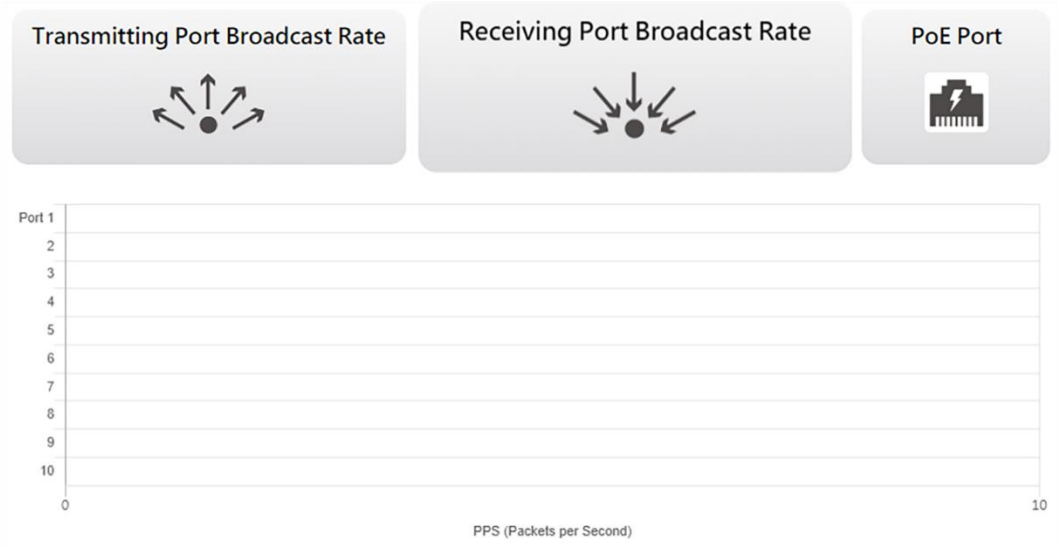
Użytkownicy mogą wyświetlić dla każdego portu szybkość transmisji portu nadawczego.



Ilustracja 21: Szybkość broadcastu portu nadawczego

8.1.6 Szybkość broadcast portu odbiorczego

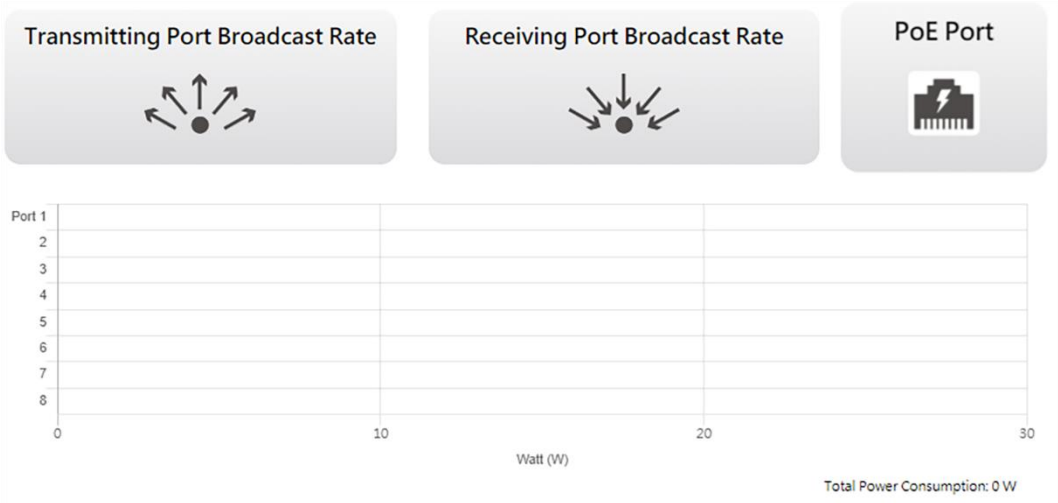
Użytkownicy mogą wyświetlić dla każdego portu szybkość transmisji portu odbiorczego.



Ilustracja 22: Szybkość broadcastu portu odbiorczego

8.1.7 Port PoE

Użytkownikowi wyświetlana jest wydajność PoE dostarczana na każdy port.

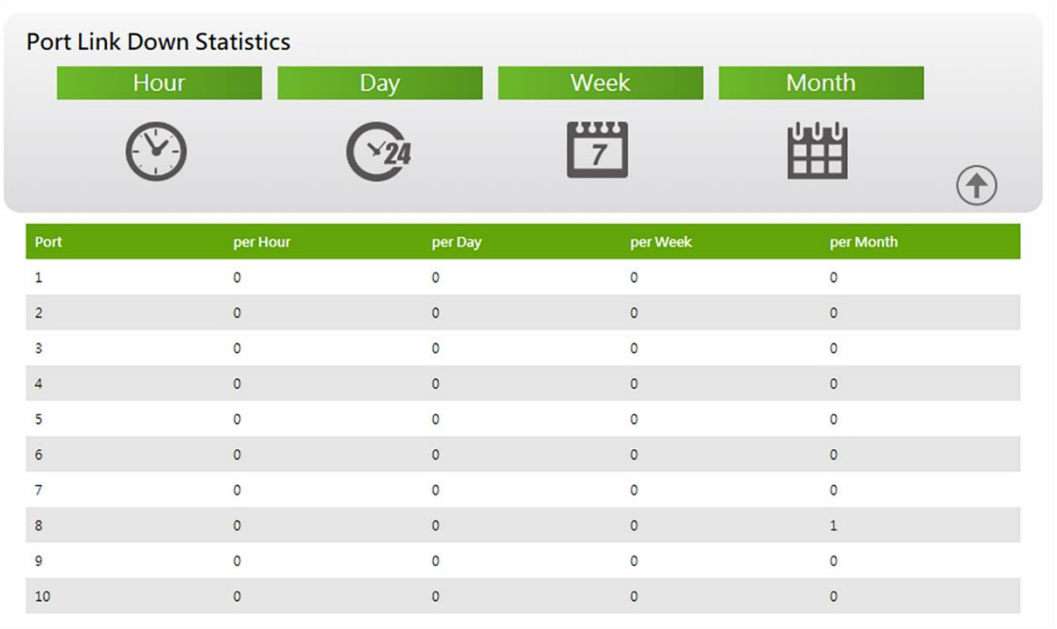


Ilustracja 23: Port PoE

8.1.8 Statystyka rozłączeń portu

Użytkownik może jednym kliknięciem zobaczyć przegląd, ile razy połączenie portu było nieaktywne („Link down”) w ciągu godziny, dnia, tygodnia i miesiąca.

Dzięki tej funkcji można szybko i łatwo zlokalizować luźne styki lub przerwanie przewodu sieciowego.

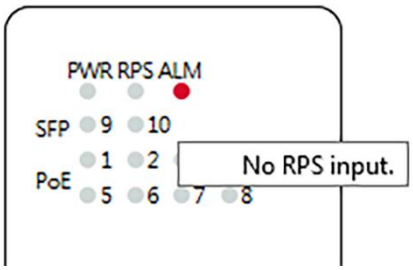


Port	per Hour	per Day	per Week	per Month
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	1
9	0	0	0	0
10	0	0	0	0

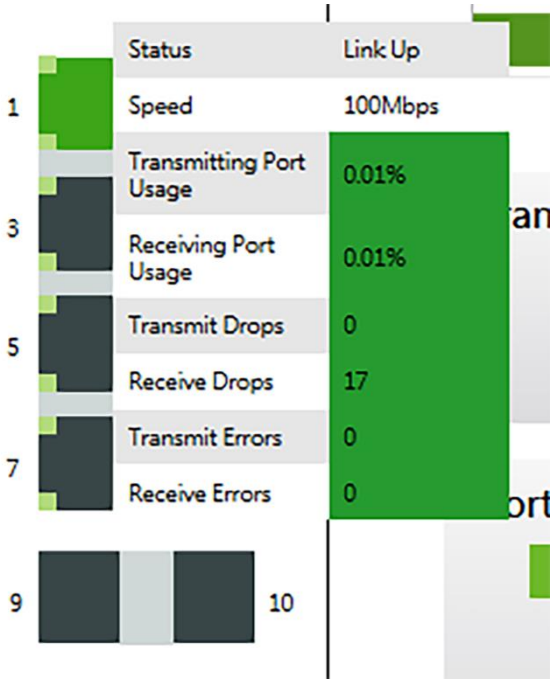
Ilustracja 24: Statystyka rozłączeń portu (przykład)

8.2 Kursor myszy na pulpicie diagnostycznym

Użytkownicy mogą uzyskać szczegółowe informacje o alarmach, ostrzeżeniach i obciążeniach, gdy po prostu najadą na nie kursorem myszy, jak pokazano poniżej.



Ilustracja 25: Informacje o LED



Ilustracja 26: Informacje o połączeniach dla każdego portu (przykład)

Analizując błędne pakiety danych (np. błędy transmisji), można wcześnie wykryć błędy w oprzewodowaniu.

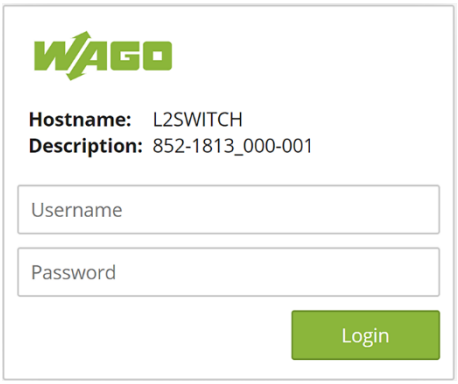
8.3 Collapse, User Login, Topology Map

Collapse option	Dzięki tej opcji użytkownik może powrócić do pulpitu.
User Login	Tutaj użytkownik loguje się do urządzenia, aby móc dokonać własnych ustawień konfiguracyjnych i serwisowych.
Topology Map	Ta mapa pokazuje użytkownikowi przegląd łączności.



Ilustracja 27: Collapse, User Login, Topology Map

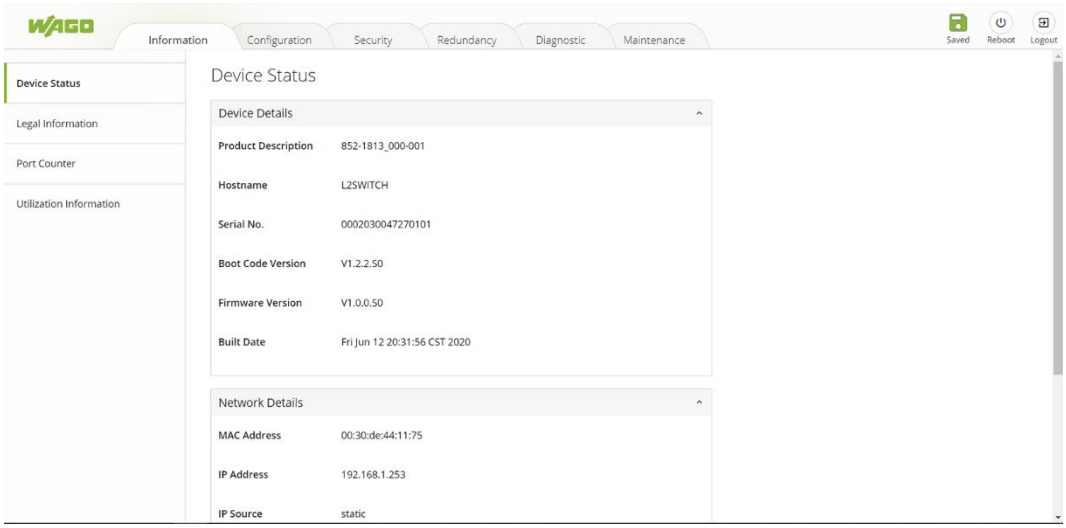
Jeśli użytkownik wybierze „User Login”, zostanie przekierowany do okna logowania switcha, jak pokazano poniżej.



Ilustracja 28: Logowanie

Tabela 17: Logowanie

Ustawienie	Domyślnie
Default Username	admin
Default Password	wago



Ilustracja 29: Tabela „Information” – menu „Device Status”

Wskazówka

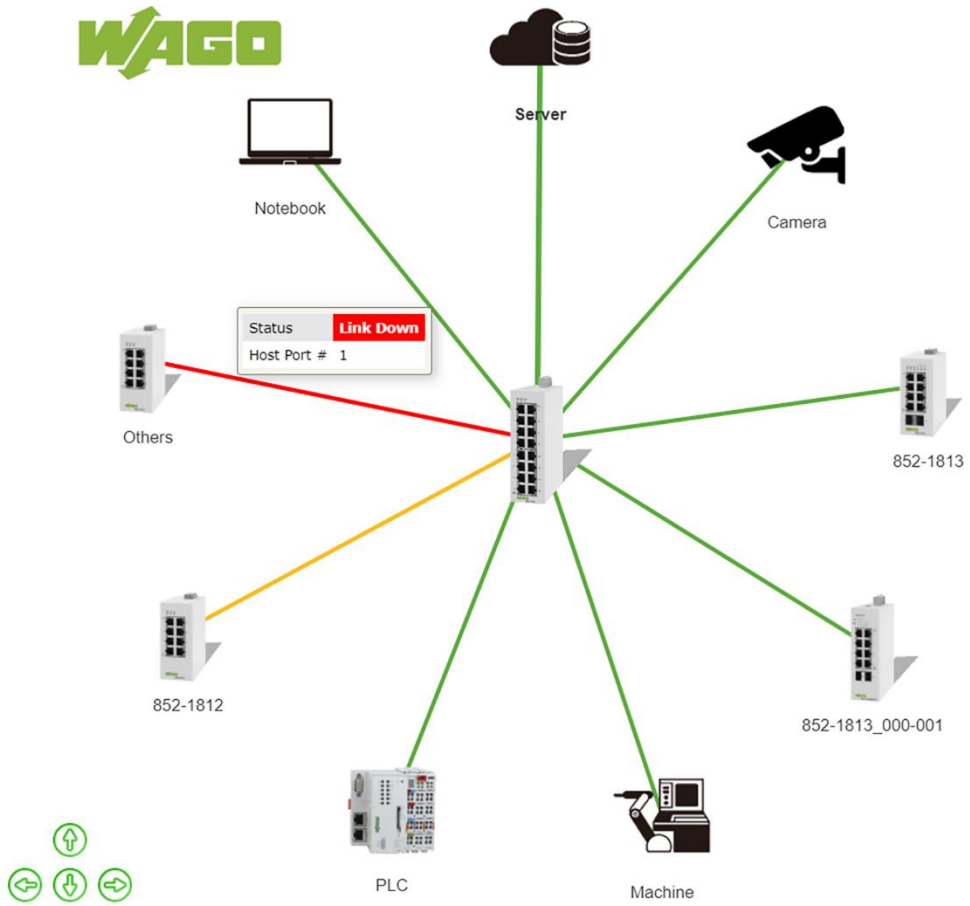
System zarządzania przez WWW (WBM)
Szczegółowy opis konfiguracji w systemie zarządzania przez WWW (WBM) można znaleźć w rozdziale „Konfiguracja w systemie zarządzania przez WWW (WBM)“.

Po wybraniu mapy topologii wyświetlany jest przegląd łączności sieciowej, jak pokazano poniżej.

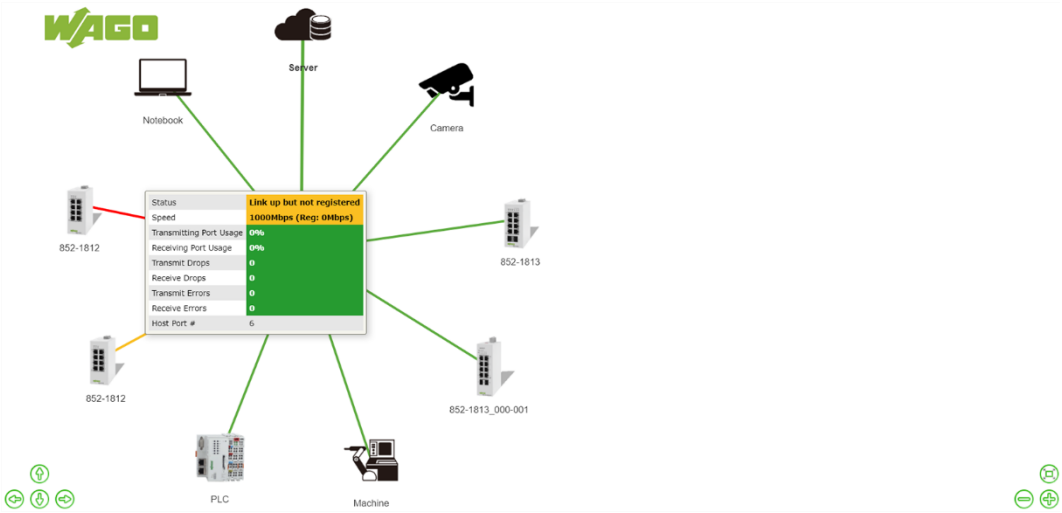
Switch pozwala na proste zarządzane siecią:

Diagnostykę można realizować intuicyjnie bez zaawansowanej wiedzy informatycznej. Mapa topologii przestawia w czytelny sposób switch i podłączone węzły. Ważne informacje diagnostyczne są wizualizowane.

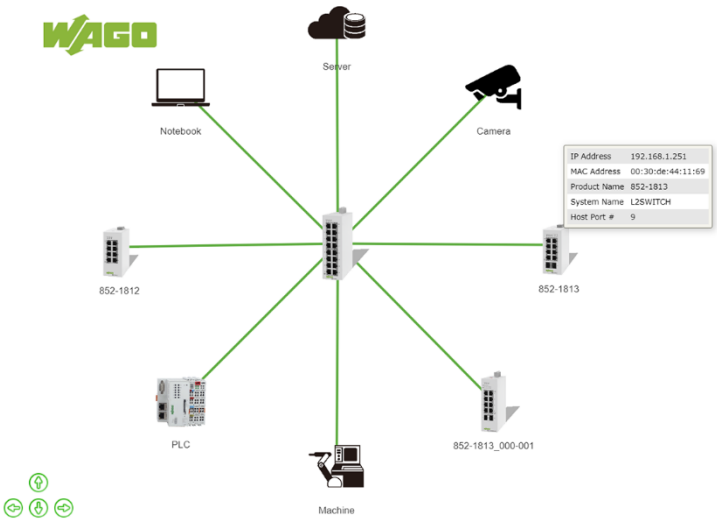
Gdy połączenie na porcie zostanie przerwane, linia połączenia zmienia kolor na czerwony.



Ilustracja 30: Mapa topologii – przerwane połączenie na porcie 1



Ilustracja 31: Mapa topologii – połączenie niezarejestrowane



Ilustracja 32: Mapa topologii – informacje o połączeniu

9 Konfiguracja w systemie zarządzania przez WWW (WBM)

W celu konfiguracji i zarządzania systemem do dyspozycji jest wewnętrzny system plików oraz zintegrowany serwer WWW, określany mianem systemu zarządzania przez WWW, w skrócie WBM.

Na zapisanych wewnętrznie stronach HTML otrzymuje się możliwe do odczytania informacje na temat konfiguracji i statusu węzła sieciowego. Dodatkowo można tutaj zmienić konfigurację urządzenia.
Ponadto za pomocą zaimplementowanego systemu plików można również przechowywać własne strony HTML.

Wskazówka



Po zmianach konfiguracji zawsze wykonać restart!
Aby zmienione ustawienia konfiguracyjne zostały zastosowane, po wprowadzeniu zmian należy zawsze restartować system.

1. Aby otworzyć WBM, uruchom przeglądarkę internetową (np. Google Chrome lub Mozilla Firefox).

Wskazówka



Ustawienie standardowe
Standardowo switch zarządzalny Lean jest ustawiony na protokół „http”.

Wskazówka



Korzystanie z protokołu „http”
Jeśli używany jest protokół „https“, należy aktywować tę usługę (zobacz rozdział „Service Control“).

2. Wpisz adres IP switcha.
3. Potwierdź przyciskiem **[Enter]**.
4. W oknie dialogowym wprowadź swój login oraz hasło:

   Użytkownik = „admin”
   Hasło = „wago”

5. Zostanie wyświetlona strona startowa WBM.
6. Wprowadź żądane ustawienia.
7. Wprowadzone zmiany potwierdź przyciskiem **[Submit]** lub porzuć zmiany przyciskiem **[Delete]**.
8. Aby przejąć ustawienia, potwierdź zmiany przyciskiem **[Save]**.

Przy pomocy linków na pasku nawigacji można otworzyć odpowiednie strony WBM:

Tabela 18: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM)

Linki do nawigacji i strony WBM
▶ **[Information]** **[Device Status]** • Device Details • Network Details • Operating Time **[Legal Information]** • WAGO Licenses • Open Source Licenses • WBM Licenses **[Port Counter]** • Port Counter **[Utilization Information]** • Utilization Information
▶ **[Configuration]** **[Device Discovery]** • LLDP • LLDP Settings • LLDP Neighbor Information • Manual Registration • Manual Registration Settings • Manual Registration Information **[Interface]** • Loop Detection • Configuration Settings • Configuration Status • Mirror • Port Mirror Settings • Port Setup • Port Setup • Port Status • Port Priority • Port Priority Settings • Port Priority Status **[PoE Settings]**
• PD Alive Check • PD Alive Check Settings • PD Alive Check Status

- Power ON/OFF
  - PoE Configuration Settings
  - PoE Configuration Status

[**SNMP**]

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

[System Management]

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

[Storm Control]

- Storm Control Settings
- Storm Control Status

▶ **[Security]**

[802.1X]

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

[ACL]

- Access Control List Settings
- Access Control List Status

[Port Security]

- Port Security Settings
- Port Security Status

[Service Control]

- Service Settings

[VLAN]

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

▶ **[Redundancy]**

[ERPS]

- ERPS Setup
- Configuration Status

[STP/RSTP]

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

▶ **[Diagnostic]**

[Alarm]

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

[Dashboard Configuration]

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

[Modbus]

- Modbus TCP Setting
- Modbus TCP Information

[**SNMP**]

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

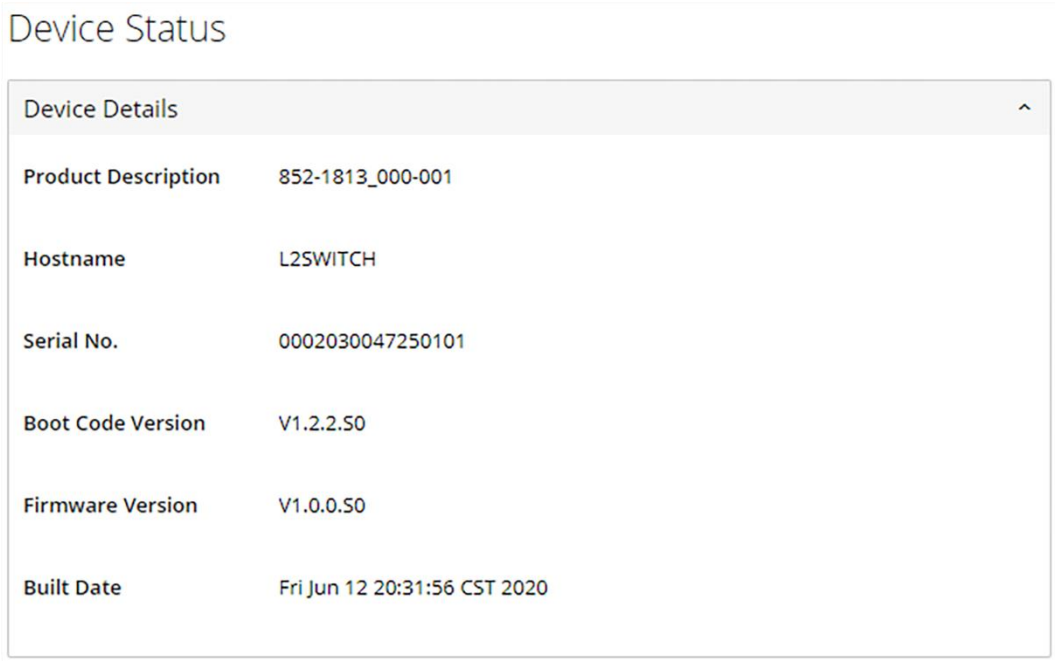
	• SNMPv3 View • SNMPv3 View Settings • SNMPv3 View Status **[System Log]** • Syslog Server Settings
	[Maintenace]
	• Reboot • Upgrade Firmware • Upload Configuration • Download Configuration • Reset Configuration

Na tych stronach WBM można wprowadzać ustawienia/konfiguracje dla przemysłowego switcha zarządzalnego.
Na niektórych stronach WBM istnieją zakładki, zawierające poszczególne strony do wprowadzania ustawień/konfiguracji.

Wartości domyślne przedstawiane są czcionką **pogrubioną.**

9.1 Information

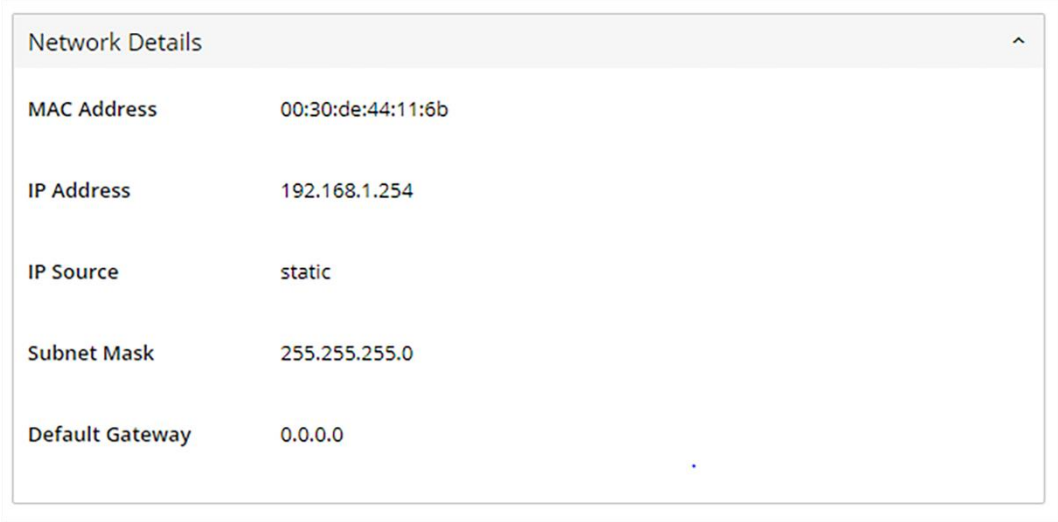
9.1.1 Device Status



Ilustracja 33: Zakładka „Information“ – menu „Device Status“ – „Device Details“

Tabela 19: Zakładka „Information“ – menu „Device Status“ – „Device Details"

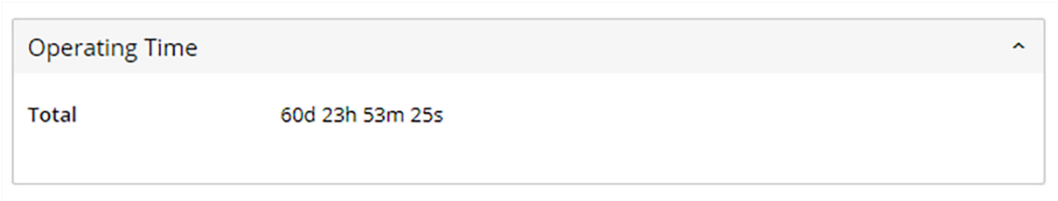
Parametr	Opis
Product Description	W tym polu wyświetlana jest nazwa modelu switcha.
Host Name	W tym polu wyświetlana jest nazwa hosta switcha.
Serial No.	W tym polu wyświetlany jest numer serii.
Boot Code Version	W tym polu wyświetlana jest wersja boot code.
Built Date	W tym polu wyświetlana jest data utworzenia aktualnie zainstalowanego firmware'u podstawowego.



Ilustracja 34: Zakładka „Information“ – menu „Device Status“ – „Network Details"

Tabela 20: Zakładka „Information“ – menu „Device Status“ – „Network Details"

Parametr	Opis
MAC Address	W tym polu wyświetlany jest adres MAC (Media Access Control) switcha.
IP Address	W tym polu wyświetlany jest adres IP switcha.
IP Source	W tym polu wyświetlany jest statyczny IP lub DHCP.
Subnet Mask	W tym polu wyświetlana jest maska podsieci.
Default Gateway	W tym polu wyświetlana jest domyślna brama switcha.



Ilustracja 35: Zakładka „Information“ – menu „Device Status“ – „Operating Time"

Tabela 21: Zakładka „Information“ – menu „Device Status“ – „Operating Time"

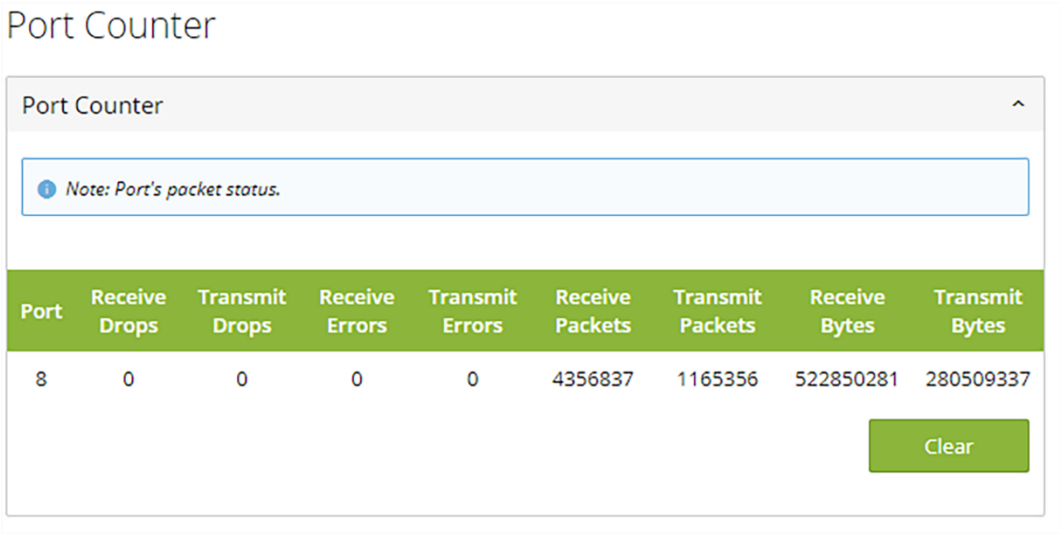
Parametr	Opis
Total	W tym polu wyświetlany jest czas pracy (dd:hh:mm:ss).

9.1.2 Legal Information

W tym menu znajdują się następujące informacje:

- WAGO Licenses
- Open Source Licenses
- WBM Licenses

9.1.3 Port Counter

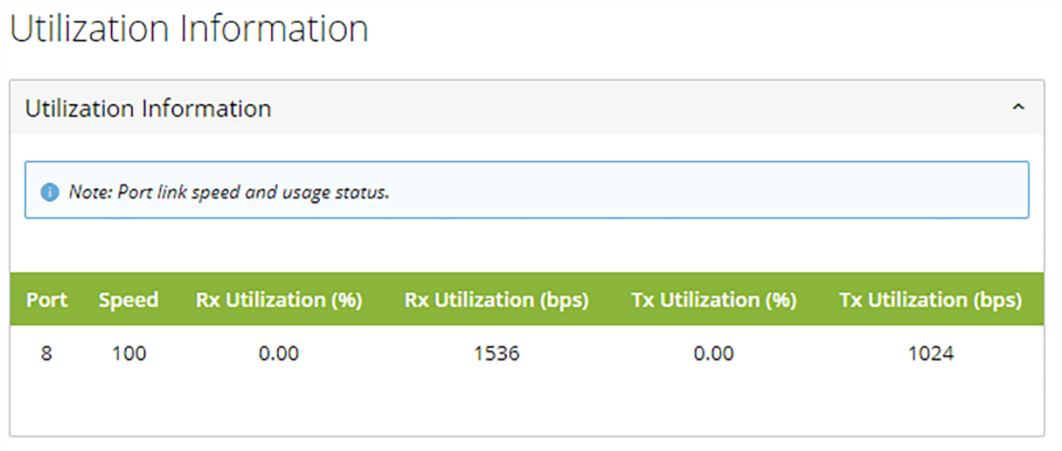


Ilustracja 36: Zakładka „Information“ – menu „Port Counter"

Tabela 22: Zakładka „Information“ – menu „Port Counter"

Port Statistics		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlane są numery portów.
Receive Drops		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych na linii odbiorczej.
Transmit Drops		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych na linii nadawczej.
Receive Errors		W tej kolumnie wyświetlana jest liczba błędów na linii odbiorczej.
Transmit Errors		W tej kolumnie wyświetlana jest liczba błędów na linii nadawczej.
Receive Packets		W tej kolumnie wyświetlana jest liczba odebranych pakietów danych od momentu włączenia.
Transmit Packets		W tej kolumnie wyświetlana jest liczba wysłanych pakietów danych od momentu włączenia.
Receive Bytes		W tej kolumnie wyświetlana jest liczba odebranych bajtów na porcie od momentu włączenia.
Transmit Byte		W tej kolumnie wyświetlana jest liczba wysłanych bajtów na porcie od momentu włączenia.

9.1.4 Utilization Information



Ilustracja 37: Zakładka „Information“ – menu „Utilization Information"

Tabela 23: Zakładka „Information“ – menu „Utilization Information"

Port Utilization Status		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlane są numery portów.
Speed		W tej kolumnie wyświetlana jest prędkość transferu.
RX Port Utilization (%)		W tej kolumnie wyświetlane jest procentowe obciążenie pasma RX.
RX Port Utilization (bps)		W tej kolumnie wyświetlane jest obciążenie pasma RX w bps.
TX Port Utilization (%)		W tej kolumnie wyświetlane jest obciążenie pasma TX.
RX Port Utilization (bps)		W tej kolumnie wyświetlane jest obciążenie pasma RX w bps.

9.2 Configuration

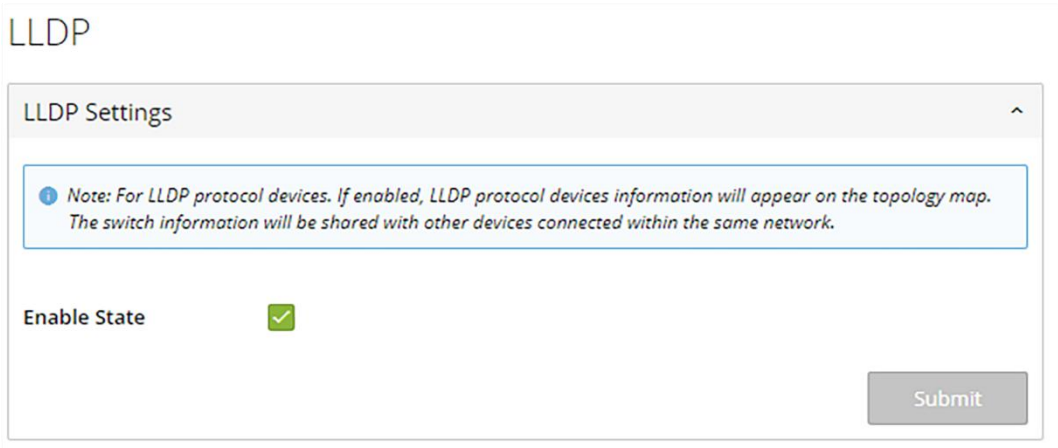
9.2.1 Device Discovery

9.2.1.1 LLDP

Opisany w tym standardzie LLDP („**L**ink **L**ayer **D**iscovery **P**rotocol“) umożliwia stacjom, połączonym siecią LAN zgodnie z IEEE 802®, wysyłanie informacji do innych stacji podłączonych do tej samej LAN. Informacje te obejmują podstawowe funkcje systemu tej stacji, włącznie z adresem zarządzającym lub adresami jednostki lub jednostek, umożliwiających zarządzanie tymi funkcjami, jak również identyfikację punktu dostępu stacji do LAN zgodnej z IEEE802, którego ta jednostka/te jednostki zarządzania potrzebuje/potrzebują.

Wskazówka

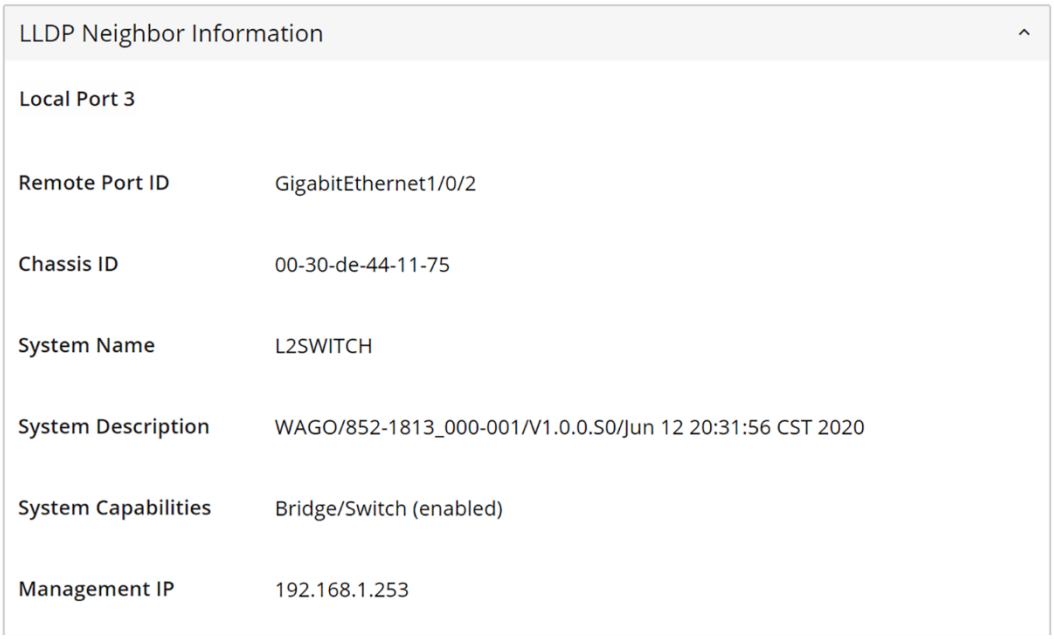
Dla urządzeń z protokołem LLDP:
Po aktywacji na mapie topologii pojawią się informacje o urządzeniach z protokołem LLDP. Informacje o switchu są udostępniane innym urządzeniom podłączonym do tej samej sieci.



Ilustracja 38: Zakładka „Configuration“ – menu „LLDP Settings“

Tabela 24: Zakładka „Configuration“ – menu „LLDP Settings“

LLDP Settings			
Parametr	**Domyślnie**	**Opis**	
State	☑	☐	Funkcja „LLDP“ dla switcha jest globalnie dezaktywowana.
		☑	Funkcja „LLDP“ dla switcha jest globalnie aktywowana.



Ilustracja 39: Zakładka „Configuration“ – menu „LLDP Neighbor Information“

Tabela 25: Zakładka „Configuration“ – menu „LLDP Neighbor Information“

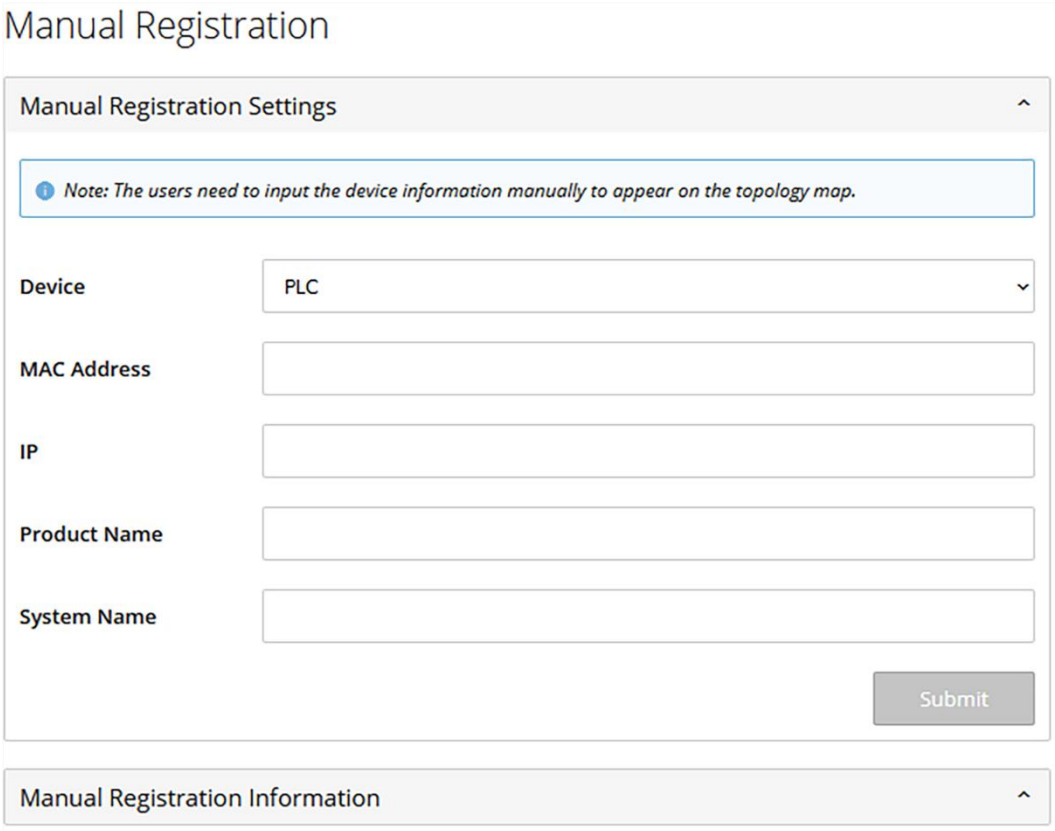
LLDP Neighbor Information		
Parametr	**Domyślnie**	**Opis**
Local Port X		W tym polu wyświetlane są numery portów.
Remote Port ID		W tym polu wyświetlany jest ID połączonego portu.
Chassis ID		W tym polu wyświetlany jest „Chassis ID“ sąsiedniego portu.
System Name		W tym polu wyświetlana jest nazwa systemowa sąsiedniego portu.
System Description		W tym polu wyświetlany jest opis systemowy sąsiedniego portu.
System Capabilities		W tym polu wyświetlane są możliwości systemowe sąsiedniego portu.
Management IP		W tym polu wyświetlany jest „adres zarządzający sąsiedniego portu.

9.2.1.2 Manual Registration

Jeśli urządzenie w sieci nie obsługuje LLDP, można je dodać do switcha za pomocą rejestracji ręcznej.

Wskazówka

Ręczne wprowadzanie informacji o urządzeniu
Użytkownik musi ręcznie wprowadzić informacje o urządzeniu, aby pojawiły się one na mapie topologii.



Ilustracja 40: Zakładka „Configuration“ – menu „Manual Registration“

Tabela 26: Zakładka „Configuration“ – menu „Manual Registration“

Manual Registration Settings		
Parametr	**Domyślnie**	**Opis**
Device	**PLC** Switch Camera Computer Display Machine Notebook Others Router Server Wireless	W polu wyboru należy wybrać odpowiednią nazwę urządzenia.
MAC Address		W polu edycji należy wpisać adres MAC urządzenia.
IP		W polu edycji należy wpisać adres IP urządzenia.
Product Name		W polu edycji należy wpisać nazwę produktu.
System Name		W polu edycji należy wpisać nazwę systemową urządzenia.

9.2.2 Interface

9.2.2.1 Loop Detection

„Loop Detection“ wykrywa problemy związane z tworzeniem się pętli w peryferiach sieci. Problemy te mogą pojawiać się, gdy port połączony jest ze switchem, znajdującym się w stanie pętli. Stan pętli powstaje w efekcie błędu użytkownika. Ma to miejsce, gdy dwa porty w jednym switchu połączone są tym samym przewodem. Gdy switch w stanie pętli wysyła wiadomości broadcast, są one zawracane do switcha i wysyłane ponownie co jakiś czas, tak że w efekcie powstaje tzw. „burza broadcastowa“.

„Loop Detection“ wysyła regularnie pakiety sondujące w celu wykrycia, czy port połączony jest z siecią w stanie pętli. Switch wyłącza port, gdy rozpozna, że pakiety sondujące zawracane są znowu do tego samego portu.

9.2.2.1.1 Loop Recovery

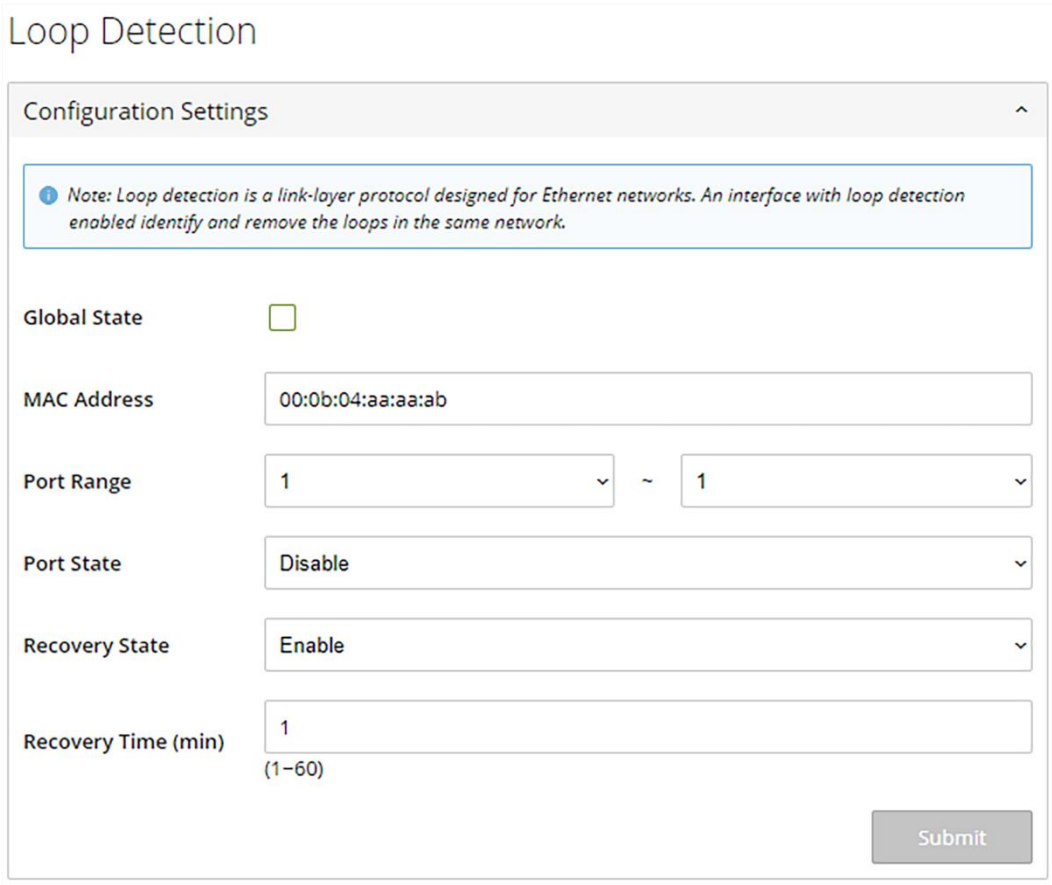
Przy aktywowanej funkcji „Loop Detection“ switch wysyła co dwie sekundy pakiet sondujący i czeka na jego odebranie. Gdy odbierze pakiet na tym samym porcie, dezaktywuje go. Po upływie określonego czasu, „Recovery Time“, znowu aktywuje port i ponownie przeprowadza „Loop Detection“.

Switch generuje „Syslog“, wewnętrzne wiadomości protokołu oraz „SNMP Traps“, gdy po „Loop Detection“ dezaktywował port.

Wskazówka



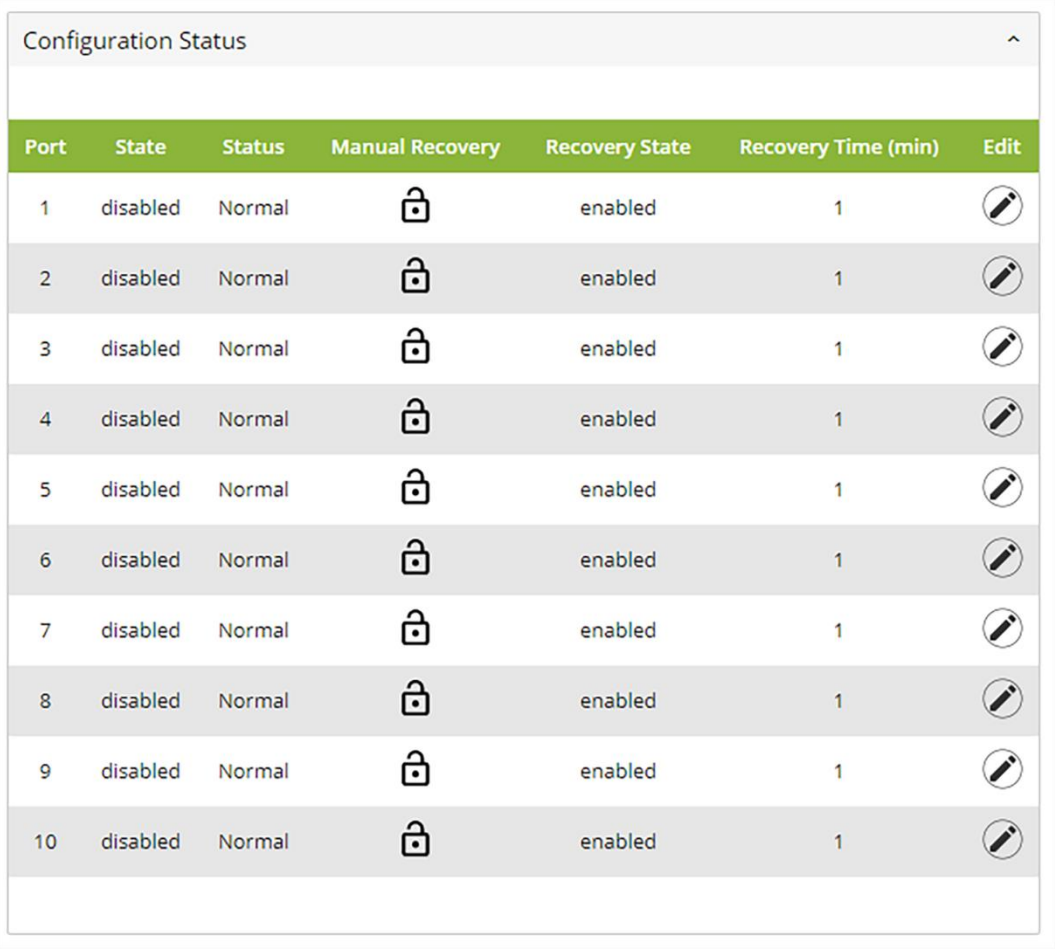
Loop Detection
Loop Detection to protokół warstwy łącza opracowany dla sieci ETHERNET. Interfejs z aktywną funkcją Loop Detection może w tej samej sieci wykrywać i usuwać pętle.



Ilustracja 41: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Settings“

Tabela 27: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Settings“

Configuration Settings			
Parametr	**Domyślnie**	**Opis**	
Global State	☑	☐	Funkcja „Loop Detection“ jest dla switcha dezaktywowana.
		☑	Funkcja „Loop Detection“ jest dla switcha aktywowana.
MAC Address		W polu edycji należy wybrać docelowy adres MAC, na który mają być wysyłane pakiety sondujące. Gdy port otrzyma te same pakiety danych, zostaje wyłączony.	
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „Loop Detection“.	
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „Loop Detection“.	
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować dla switcha funkcję „Loop Detection“.	
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować dla switcha funkcję „Loop Detection“.	
Recovery State	**Enable**	W polu wyboru należy wybrać „Enable“, aby port aktywował się automatycznie po upływie wyznaczonego czasu „Recovery Time“.	
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.	
Recovery Time (min) (Range: 1~60)	**1**	W polu edycji należy wpisać wartość „Recovery Time“ (w minutach), jaki switch musi odczekać, zanim reaktywuje port. Zakres czasowy: 1 … 60 min	



Ilustracja 42: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Status“

Tabela 28: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Status“

Status Loop Detection		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
State	Enable Disable	W tej kolumnie wyświetlana jest informacja, czy funkcja „Loop Detection“ jest aktywowana, czy dezaktywowana.
Status	None Normal	W tej kolumnie wyświetlana jest informacja, czy port jest zablokowany.
Manual Recovery		W tej kolumnie wyświetlana jest informacja, czy funkcja „Manual Recovery” została zakończona, czy nie.
Recovery State	Enable Disable	W tej kolumnie wyświetlana jest informacja, czy funkcja „Loop Recovery“ jest aktywowana, czy dezaktywowana.
Recovery Time (min)	1 … 60	W tej kolumnie wyświetlany jest „Recovery Time“ dla funkcji „Loop Detection“.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.2.2.2 Port mirroring (Mirror)

„Port Mirroring“ w przypadku switchy wykorzystywany jest do wysyłania kopii wysłanych/odebranych pakietów sieciowych z jednego lub kilku obszarów do monitoringu sieci lub innego portu switcha (Monitor Port).

„Port Mirroring“ wykorzystywany jest w systemach sieciowych, w których wymagane jest monitorowanie ruchu sieciowego, jak chociażby w systemie wykrywania i zapobiegania włamaniom IDS („**I**ntrusion **D**etection **S**ystem“).

„Port Mirroring“ wraz z programem do analizy ruchu sieciowego NTA („**N**etwork **T**raffic **A**nalyzer“) może być pomocny w monitorowaniu komunikacji sieciowej. Użytkownicy mogą w ten sposób monitorować na wybranych portach („Source Ports“) wchodzące/wychodzące pakiety danych.

Source Mode

- „Ingress” (wejście): Wchodzące pakiety danych są kopiowane i przekierowane do portu monitorującego.
- „Egress” (wyjście): Wychodzące pakiety danych są kopiowane i przekierowane do portu monitorującego.

Wskazówka



Wskazówka

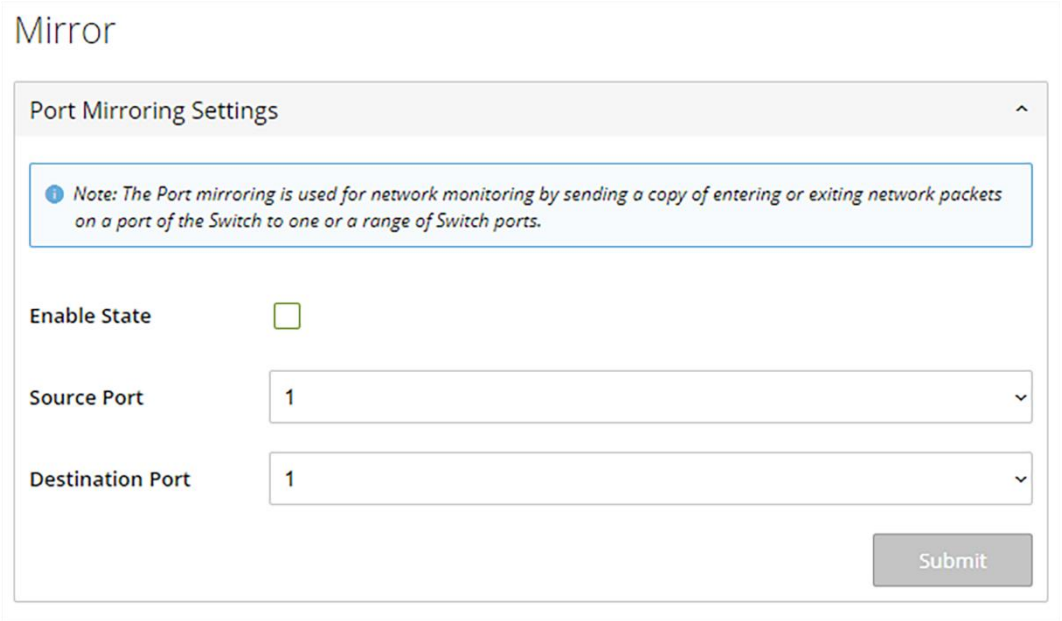
1. Port monitorujący nie może być członkiem grupy „Trunk Port".
2. Port monitorujący nie może być portem wejściowym ani wyjściowym.
3. Gdy port został skonfigurowany jako port źródłowy i użytkownik skonfigurował go następnie jako port docelowy, zostaje on automatycznie usunięty z portów źródłowych.

Wskazówka



Zastosowanie port mirroringu

Port mirroring jest używany do monitorowania sieci. Kopie pakietów sieciowych, które zostały wysłane/odebrane na porcie switcha, są wysyłane na jeden lub kilka innych portów switcha.



Ilustracja 43: Zakładka „Configuration“ – menu „Mirror“ – „Port Mirroring Settings“

Tabela 29: Zakładka „Configuration“ – menu „Mirror“ – „Port Mirroring Settings“

Port Mirror Settings			
Parametr	**Domyślnie**	**Opis**	
Enable State	☐	☐	Funkcja „Mirror” jest dla switcha dezaktywowana.
		☑	Funkcja „Mirror” jest dla switcha aktywowana.
Source Port	1 … 10	W polu wyboru należy wybrać port źródłowy dla funkcji „Mirror”.	
Destination Port	1 … 10	W polu wyboru należy wybrać port docelowy dla funkcji „Mirror”.	

9.2.2.3 Port Setup

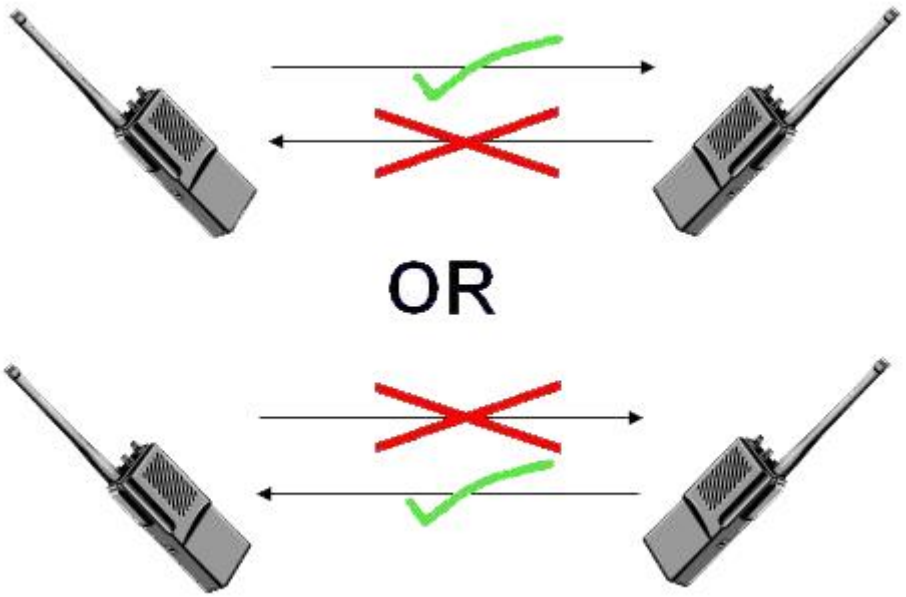
9.2.2.3.1 Port Settings

Tryb duplex

System komunikacyjny duplex jest systemem składającym się z dwóch połączonych ze sobą urządzeń, które mogą się ze sobą naprzemiennie komunikować.

Half duplex

W systemie half duplex komunikacja może przebiegać na tym samym porcie w obu kierunkach, ale zawsze tylko po kolei (nie równocześnie).
Oznacza to, że po odebraniu sygnału urządzenie, zanim odpowie, musi czekać, aż inne urządzenie zakończy nadawanie.



Ilustracja 44: Tryb half duplex

Full duplex

Tryb full duplex (zwany też podwójny duplex) pozwala na równoczesną komunikację w obu kierunkach.
Dla przykładu sieć telefoniczna jest systemem full duplex, gdyż obaj rozmówcy mogą równocześnie mówić i słuchać.



Ilustracja 45: Tryb full duplex

Auto MDI/MDIX

MDI („**M**edium-**D**ependent **I**nterface“) jest niezależnym od medium interfejsem w technice komunikacyjnej i częścią jednostki nadawczo-odbiorczej (transceiver) urządzenia sieciowego.

Auto-MDIX („**Aut**omatic **M**edium-**D**ependent **I**nterface **C**rossover“) jest technologią sieciową zintegrowaną w porcie, która automatycznie rozpoznaje rodzaj przewodu sieciowego (przewód prosty lub skrosowany) i konfiguruje odpowiednie połączenie.
Dzięki temu do połączenia urządzeń nie są potrzebne przewody skrosowane.
Interfejs automatycznie koryguje nieprawidłowe oprzewodowanie.
Aby funkcja Auto-MDIX działała prawidłowo, prędkość dla interfejsu i w ustawieniu duplexu musi być ustawiona na „Auto“.

Autonegocjacja

Autonegocjacja to proces, w którym dwa połączone ze sobą porty ETHERNET (np. port sieciowy komputera i port sieciowy rutera, hubu lub switcha, z którym jest on np. połączony), samodzielnie rozpoznają maksymalną największą prędkość transmisji oraz tryb duplex i automatycznie dokonują ustawień.
Autonegocjacja dotyczy tylko przewodów wielodrutowych (skrętka) – jednak nie przewodów WLAN, światłowodów lub kabli koncentrycznych.

Jeśli port nie wspiera autonegocjacji lub funkcja ta jest wyłączona, switch określa prędkość transmisji przez rozpoznanie sygnału na przewodzie i wykorzystuje tryb half duplex.
Gdy autonegocjacja jest w switchu wyłączona, port wykorzystuje przy nawiązywaniu połączenia skonfigurowane wstępnie ustawienia prędkości i trybu duplex.
Dlatego należy zapewnić, że dla portu wprowadzono takie same ustawienia, aby połączenie mogło zostać nawiązane.

Flow Control

„Flow Control“ reguluje transmisję sygnałów przez dostosowanie szerokości pasma do portu wejściowego.
Duży ruch danych na porcie redukuje szerokość pasma i może doprowadzić do przepełnienia bufora, czego skutkiem może być z kolei utrata pakietów i ramek.

Zgodnie z IEEE 802.3x switch stosuje kontrolę przepływu w trybie full duplex i „Backpressure Flow Control“ (wsteczna kontrola przepływu danych) w trybie half duplex.

Podczas „Flow Control“ switch wysyła w trybie full duplex do portu nadawczego sygnał przerwy, który ma tymczasowo wstrzymać wysyłanie sygnałów, gdy bufor portu odbiorczego grozi przepełnieniem.

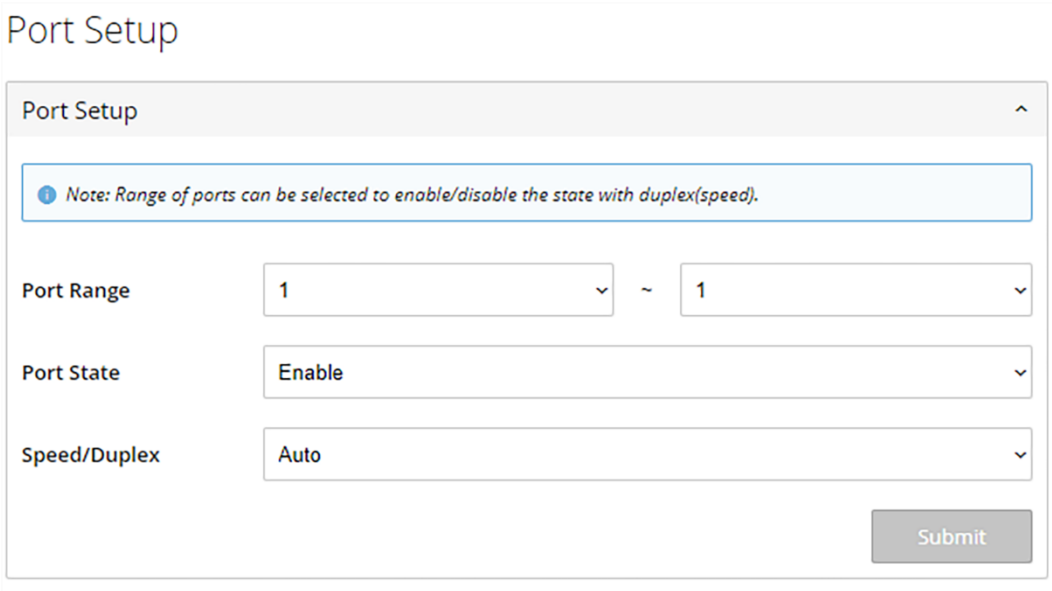
Przy „Backpressure Flow Control“ switch wysyła w trybie half duplex sygnał kolizji do portu nadawczego (imituje niejako status kolizji pakietów), który ma wstrzymać tymczasowo nadawanie i wznowić wysyłanie sygnałów dopiero po jakimś czasie.

Wskazówka

Wspieranie „Force Mode“
1000 BASE-T nie wspiera „Force Mode“.

Wskazówka

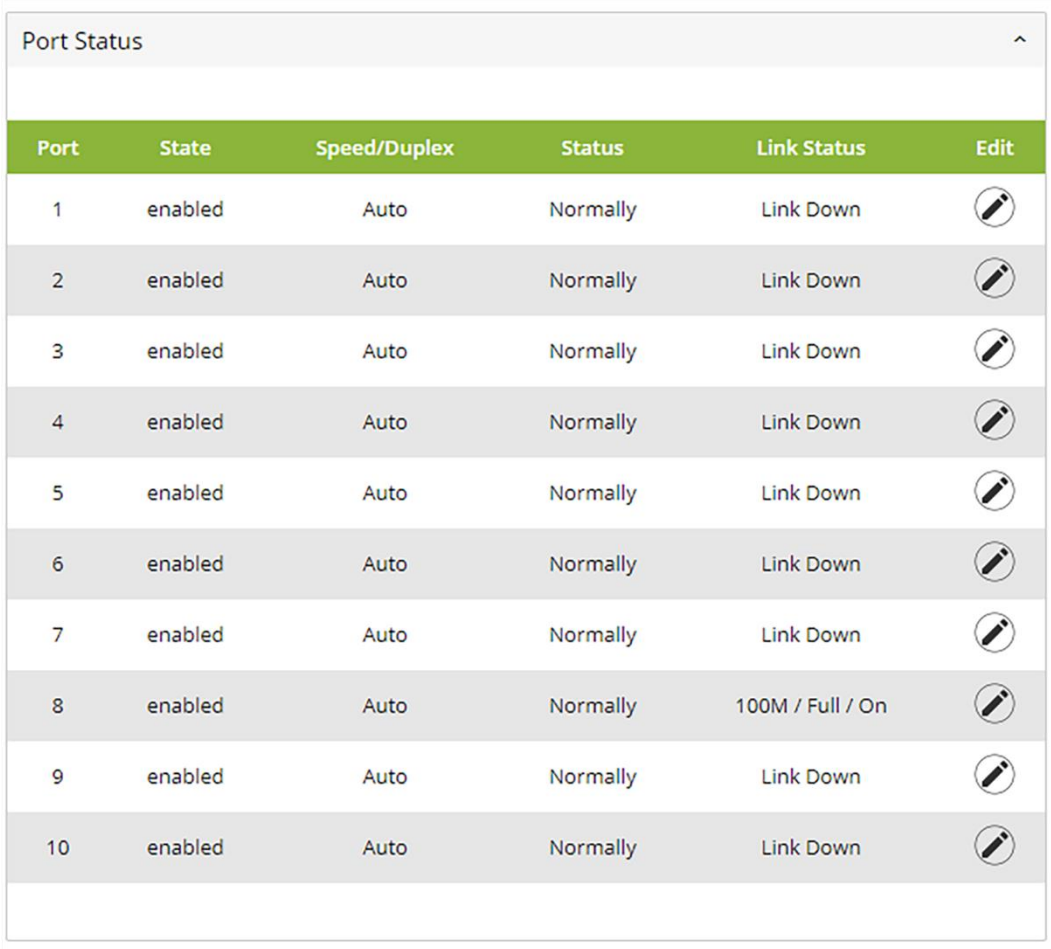
Wybór zakresu portów
Można wybrać cały zakres portów i dla nich aktywować lub dezaktywować stan duplex (prędkość).



Ilustracja 46: Zakładka „Configuration“ – menu „Port Setup“ – „Port Setup“

Tabela 30: Zakładka „Configuration“ – menu „Port Setup“ – „Port Setup“

Port Setup		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, w którym ma być skonfigurowany „Port Setup”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, w którym ma być skonfigurowany „Port Setup”.
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować port.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować port.
Speed/Duplex	**Auto**	W polu wyboru należy wybrać prędkość i tryb duplex dla portu. „Nway” oznacza autonegocjację w ETHERNET.
	10 Mbit/s / Full	
	10 Mbit/s / Full Nway	
	10 Mbit/s / Half	
	10 Mbit/s / Half Nway	
	100 Mbit/s / Full	
	100 Mbit/s / Full Nway	
	100 Mbit/s / Half	
	100 Mbit/s / Half Nway	
	1000 Mbit/s / Full	
	1000 Mbit/s / Full Nway	



Ilustracja 47: Zakładka „Configuration“– menu „Port Setup“ – „Port Status“

Tabela 31: Zakładka „Configuration“– menu „Port Setup“ – „Port Status“

Port Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
State		W tej kolumnie wyświetlana jest informacja, czy port jest aktywowany, czy dezaktywowany.
Speed/Duplex		W tej kolumnie wyświetlana jest informacja, dla jakiej prędkości (10 Mbit/s, 100 Mbit/s lub 1000 Mbit/s) i dla jakiego trybu duplex (full lub half) port został skonfigurowany.
Status		W tej kolumnie wyświetlane są odchylenia.
Link Status		W tej kolumnie wyświetlany jest „Link Status“ portu. Gdy port jest aktywny, wyświetlane są prędkość, tryb duplex i ustawienie kontroli przepływu. Komunikat „Link inaktiv” oznacza, że port bądź jest dezaktywowany, bądź nie jest podłączone żadne urządzenie.
Edit		W tej kolumnie można aktywować funkcję edycji.

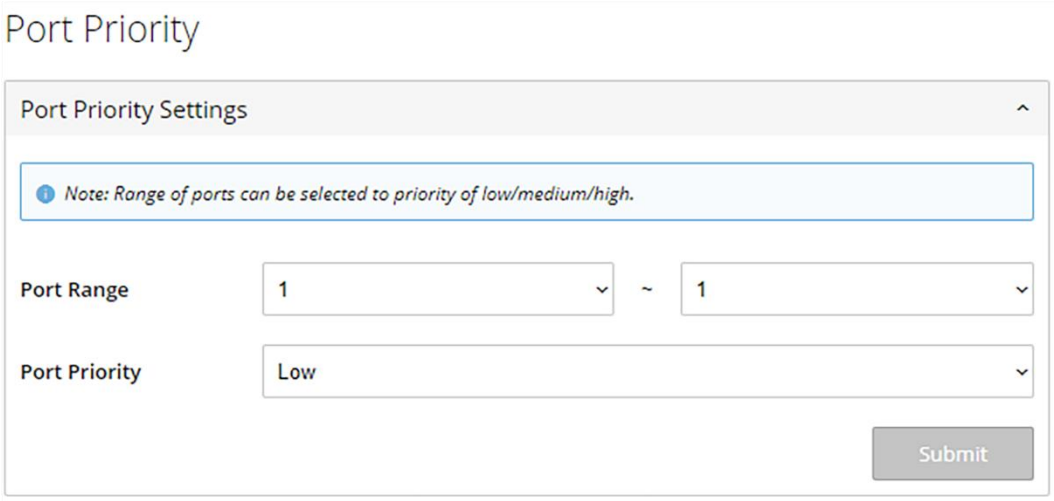
9.2.2.4 Priorytetyzacja portów ETHERNET (Port Priority)

Zazwyczaj sieci działają zgodnie z najlepszą możliwą metodą transmisji, co oznacza. że cały ruch danych na każdym porcie ma taki sam priorytet i taką samą szansę transmisji w stosownym czasie. Jeśli dochodzi do zatoru, każdy ruch danych ma taką samą szansę zostać odrzucony.

Za pomocą funkcji „Port Priority” można wybrać określony ruch danych i nadać mu priorytet zgodnie z jego relatywną ważnością. Implementacja priorytetyzacji portów w sieci poprawia przewidywalność wydajności sieci i zwiększa efektywność wykorzystania szerokości pasma.

Wskazówka

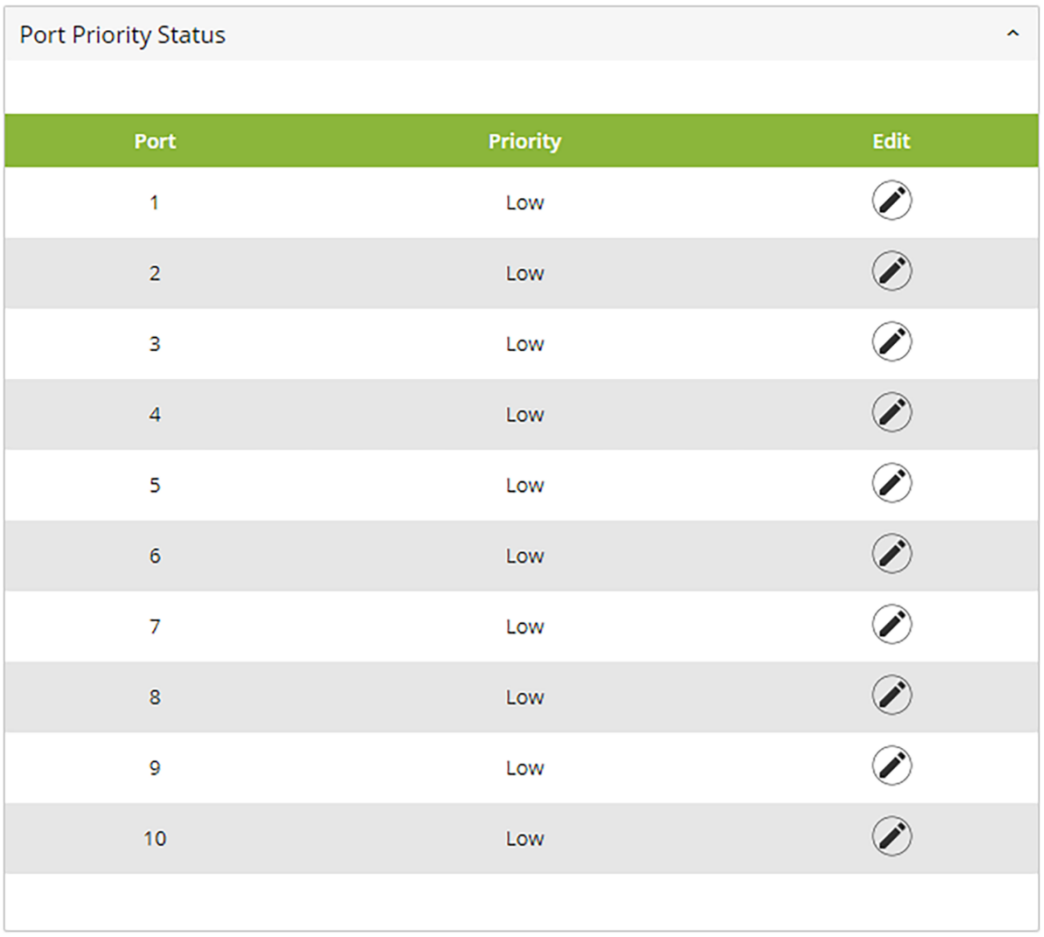
Wybór priorytetów portu
Można wybrać zakres portów i przypisać mu priorytet „Low”, „Medium” lub „High” (niski, średni lub wysoki).



Ilustracja 48: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Settings

Tabela 32: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Settings“

Port Priority Settings		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, w którym ma być skonfigurowany „Port Priority”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, w którym ma być skonfigurowany „Port Priority”.
Port Priority	Low	Dla aplikacji o dużym natężeniu ruchu należy w polu wyboru zaznaczyć opcję „Low”.
	Medium	Dla aplikacji o średnim natężeniu ruchu należy w polu wyboru zaznaczyć opcję „Medium”.
	High	Dla aplikacji o krytycznym czasowo natężeniu ruchu należy w polu wyboru zaznaczyć opcję „High”.



Ilustracja 49: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Status“

Tabela 33: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Status“

Port Priority Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
Priority	Low Medium High	W tej kolumnie wyświetlany jest priorytet portu.
Edit		W tej kolumnie można aktywować funkcję edycji.

Wskazówka

Priorytetyzacja urządzeń sieciowych

Preferowane jest, aby urządzenia sieciowe krytyczne czasowo (np. PLC, Remote-IO) otrzymały wysoki priorytet, a urządzenia niekrytyczne czasowo (np. kamera, drukarka) – niski priorytet.

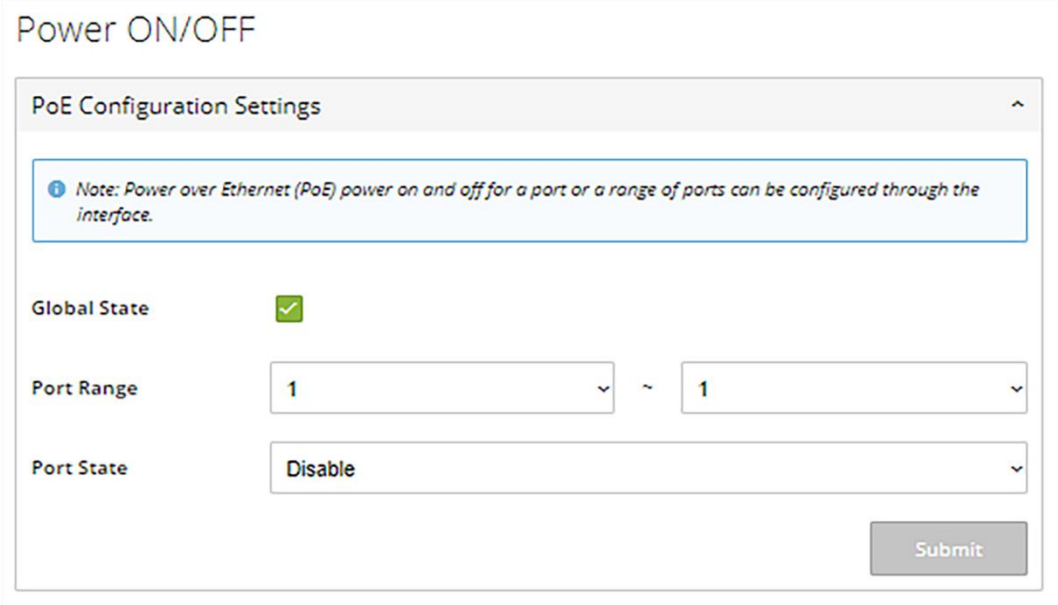
9.2.3 PoE Settings

9.2.3.1 Aktywacja PoE dla portu (Power ON)

Zasilanie PoE może być włączane lub wyłączane dla wybranych portów. Można wybrać pojedyncze porty lub całe zakresy portów.

Wskazówka

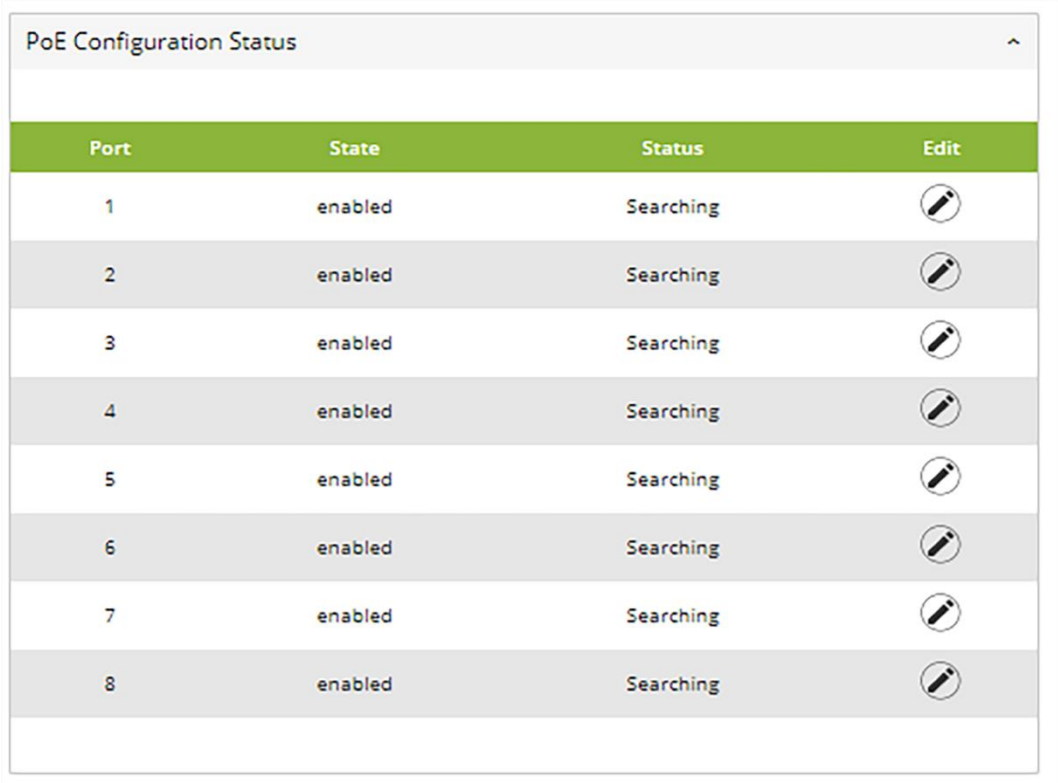
Włączanie/wyłączanie Power over Ethernet (PoE)
Zasilanie „Power over Ethernet” (PoE) można skonfigurować przez interfejs dla jednego lub kilku portów.



Ilustracja 50: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Settings“

Tabela 34: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Settings“

PoE Configuration Settings			
Parametr	**Domyślnie**	**Opis**	
Global State	☑	☐	Funkcja „Power ON” jest dla switcha dezaktywowana.
		☑	Funkcja „Power ON” jest dla switcha aktywowana.
Port Range	**1** … 8	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Power ON”.	
	1 … 8	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Power ON”.	
Port State	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Power ON” na wybranych portach.	
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Power ON” na wybranych portach.	



Ilustracja 51: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Status“

Tabela 35: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Status“

PoE Configuration Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 8	W tej kolumnie wyświetlany jest numer portu.
State	Enable Disable	W tej kolumnie wyświetlana jest informacja, czy PoE+ jest aktywowany, czy dezaktywowany.
Status		W tej kolumnie wyświetlana jest informacja, czy „Powered Device” jest zasilane.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.2.3.2 PD Alive Check

Ta funkcja pozwala na monitorowanie i resetowanie urządzeń PoE w sieci. Po aktywacji tej funkcji switch sprawdzi stany urządzeń w sieci.

Jeśli funkcja „Global state” jest aktywowana, switch po upływie interwału wyśle pakiet sprawdzający stan urządzeń („Alive Check”). Jeśli host nie odpowiada w momencie przekroczenia liczby powtórzeń („Retry Times“), switch wykonuje działanie skonfigurowane dla danego portu w „Action“ (reboot/alarm/all) dla PD.

Interval Time (sec)

To pole określa, z jakim interwałem wysyłane są komunikaty sprawdzające do PD („Powered Device”).

Action

W tym polu konfiguruje się działanie, które ma być wykonane w razie wykrycia błędu.

All:	Wysyła komunikat alarmowy do administratora i następnie restartuje PD.
Alarm:	Wysyła tylko komunikat alarmowy do administratora.
None:	Ciągle wysyła ping do zdalnego PD, nie podejmując żadnych dalszych działań.
Reboot:	Odłącza port PoE od zasilania i restartuje PD.

Power OFF Time (sec)

To pole określa, kiedy port PoE zostanie ponownie podłączony do zasilania po restarcie PD.

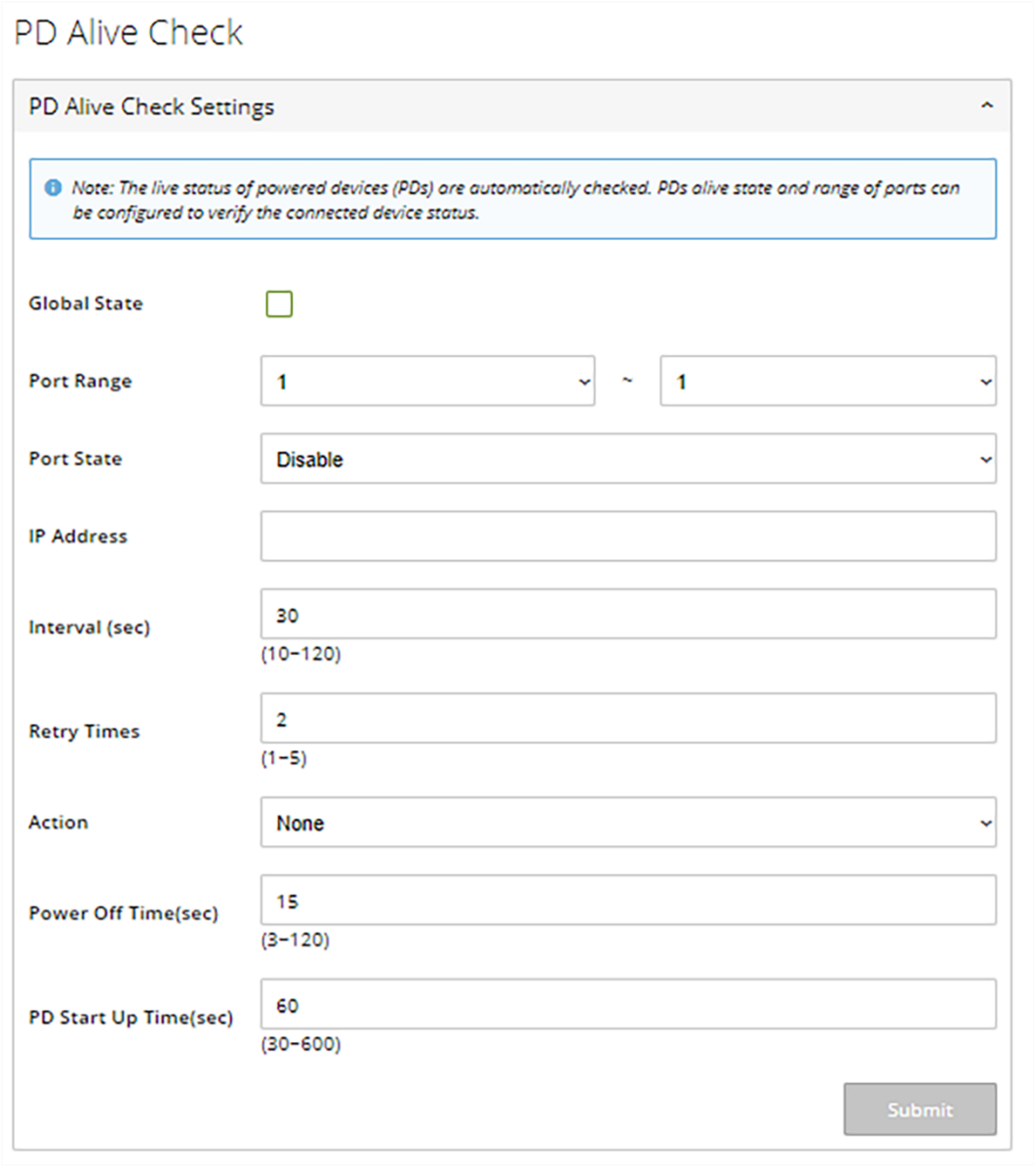
PD Startup Time (sec)

To pole określa, jak długo switch czeka po starcie PD, zanim przeprowadzi automatyczną kontrolę PoE.

Wskazówka

Automatyczna kontrola aktywności PD

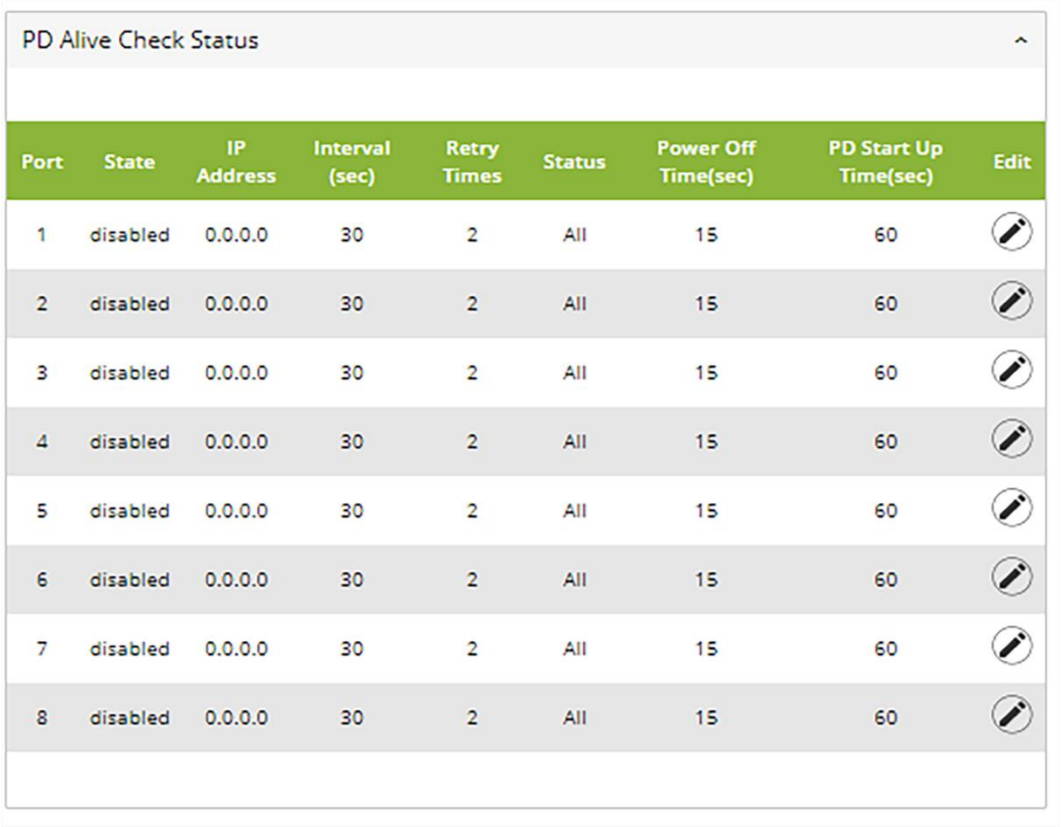
Status aktywności PD jest sprawdzany automatycznie. Status i zakres portów można skonfigurować, aby zweryfikować stan podłączonych urządzeń.



Ilustracja 52: Zakładka „Configuration” – menu „PoE Settings” – „PD Alive Check Settings”

Tabela 36: Zakładka „Configuration” – menu „PoE Settings” – „PD Alive Check Settings”

PD Alive Check Settings		
Parametr	**Domyślnie**	**Opis**
Global State	☐	☐ Funkcja „PD Alive Check” jest dla switcha dezaktywowana. ☑ Funkcja „PD Alive Check” jest dla switcha aktywowana.
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „PD Alive Check”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „PD Alive Check”.
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „PD Alive Check” na poszczególnych portach.
	Enable	W polu wyboru należy wybrać „Enable“, aby dezaktywować „PD Alive Check” na poszczególnych portach.
IP Address		W polu edycji należy wpisać „Host-IP Address“, który łączy się z portem.
Interval (sec) (10-120)	**30**	W polu wyboru należy określić interwał wysyłania pakietów sprawdzających stan urządzenia PoE.
Retry Times (1-5)	**2**	W polu wyboru należy określić liczbę powtórzeń dla wysyłania pakietów sprawdzających stan urządzenia PoE. Zakłada się przy tym, że host nie odpowiada.
Action	**None**	W polu wyboru należy wybrać „None“, jeśli uczestniczące PD ciągle „pinguje”, nie wykonując żadnych dodatkowych działań.
	Reboot	W polu wyboru należy wybrać „Reboot”, aby odłączyć port PoE od zasilacza i zrestartować uczestniczące PD.
	Alarm	W polu wyboru należy wybrać „Alarm”, aby wysłać komunikat alarmu do administratora.
	All	W polu wyboru należy wybrać „All”, aby wysłać komunikat alarmu do administratora i następnie zrestartować uczestniczące PD.
Power Off Time (sec) (3-120)	**15**	W polu wyboru należy wprowadzić czas, po którym port PoE zostanie ponownie podłączony do zasilania po restarcie uczestniczącego PD.
PD Startup Time (sec) (30 600)	**60**	W polu wyboru należy wprowadzić czas, przez jaki switch czeka po restarcie uczestniczącego PD, zanim przeprowadzi automatyczną kontrolę PoE.



Ilustracja 53: Zakładka „Configuration“ – menu „PoE Settings“ – „PD Alive Check Status“

Tabela 37: Zakładka „Configuration“ – menu „PoE Settings“ – „PD Alive Check Status“

PD Alive Check Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 8	W tej kolumnie wyświetlany jest numer portu.
State	Enable Disable	W tej kolumnie wyświetlany jest stan „PD Alive Check” dla danego portu.
IP Address		W tej kolumnie wyświetlany jest adres IP hosta dla danego portu.
Interval (sec)	10 … 120	W tej kolumnie wyświetlany jest interwał, z jakim wysyłane są komunikaty sprawdzające do uczestniczącego PD.
Retry Times	1 … 5	W tej kolumnie wyświetlana jest liczba powtórzeń wysyłania pakietów sprawdzających aktywność, gdy host dla danego portu nie odpowiedział na pakiet.
Status	None Reboot Alarm All	W tej kolumnie wyświetlana jest wybrana akcja.
Power Off Time (sec)	3 … 120	W tej kolumnie wyświetlany jest „Power Off Time”.
PD Startup Time (sec)	30 … 600	W tej kolumnie wyświetlany jest „PD Startup Time”.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.2.4 SNMP

„**S**imple **N**etwork **M**anagement **P**rotocol“ (SNMP) jest używany w systemach zarządzania siecią do monitorowania podłączonych urządzeń pod kątem stanów, które wymagają uwagi administratora. SNMP wchodzi w skład „Internet Protocol Suite“ zdefiniowanego przez Internet Engineering Task Force (IETF). Składa się z szeregu standardów do zarządzania siecią, włącznie z protokołem warstwy aplikacji, schematem bazy danych i szeregiem obiektów bazy danych.

SNMP przedstawia dane zarządzania w formie zmiennych zarządzanych systemów, opisujących konfigurację systemu. Zmienne mogą być potem odpytywane przez aplikacje zarządzania (i czasem również zmieniane).

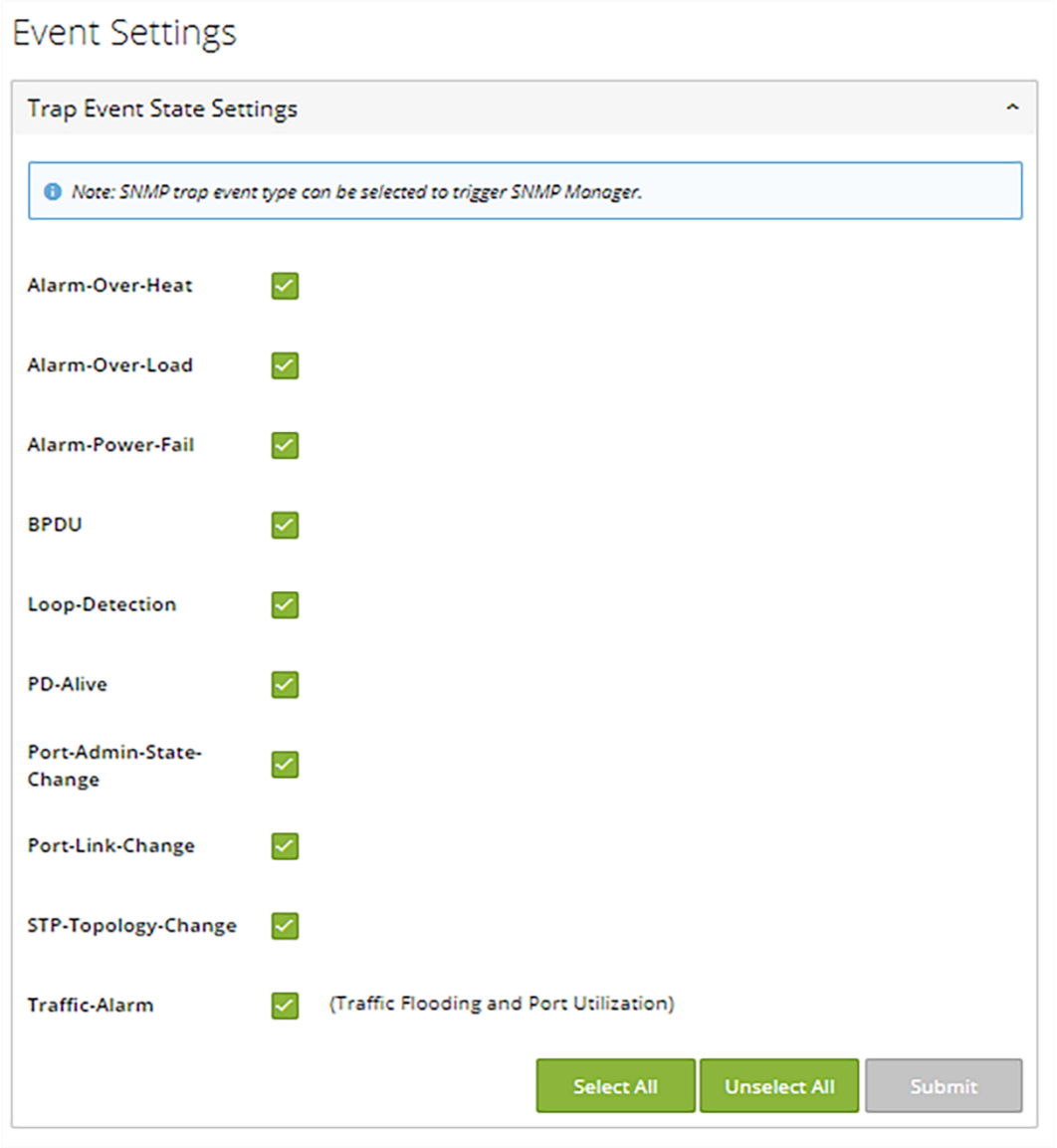
„SNMP Community String“ jest elementem tekstowym, funkcjonującym jako hasło. Funkcja ta wykorzystywana jest do uwierzytelniania wiadomości, wymienianych między stacja zarządzającą („SNMP Manager“) i urządzeniem („SNMP Agent“). Ten string zawarty jest w każdym pakiecie, transmitowanym między oboma tymi punktami.

„SNMP Community“ funkcjonuje jako hasło i wykorzystywane jest do definiowania parametrów bezpieczeństwa SNMP Clients w środowiskach SNMPv1 i SNMPv2c. Standardowe ustawienie „SNMP Community” dla SNMPv1 i SNMPv2c to „public”, dopóki SNMPv3 nie jest aktywowana. Jeśli SNMPv3 jest aktywowana, „Communities“ muszą być specyficzne dla SNMPv1 i v2c i nie mogą być używane razem.

9.2.4.1 Event Settings

Wskazówka

Wybór rodzaju zdarzenia trap SNMP
Można wybrać typy zdarzeń trap SNMP, które są wywoływane przez menedżera SNMP.



Ilustracja 54: Zakładka „Configuration“ – menu „SNMP“ – „Event Settings“ – „Trap Event State Settings“

Tabela 38: Zakładka „Configuration“ – menu „SNMP“ – „Event Settings“ – „Trap Event State Settings“

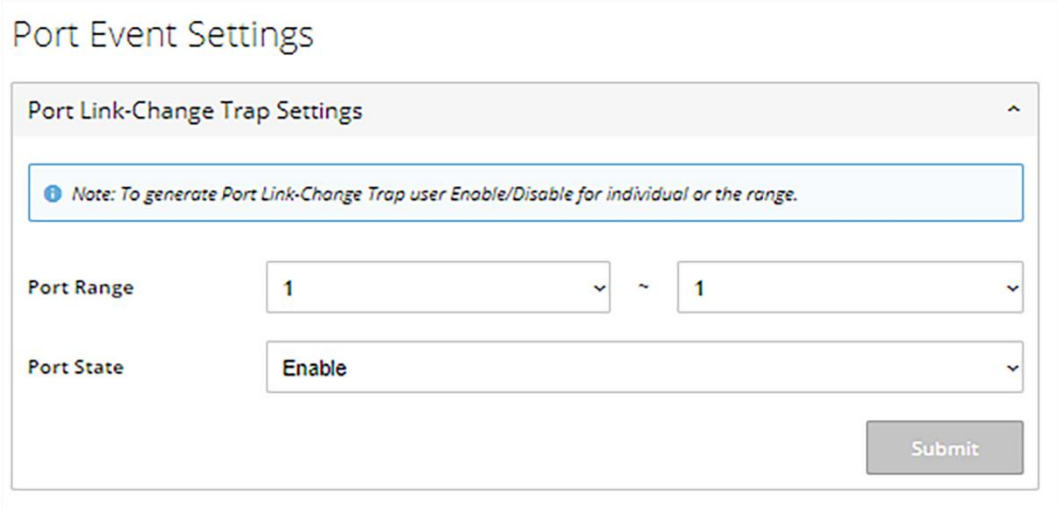
Trap Event State Settings		
Parametr	**Domyślnie**	**Opis**
Alarm-Over-Heat	☑	Aktywuje / dezaktywuje trap SNMP, gdy temperatura systemu jest zbyt wysoka.
Alarm-Over-Load	☑	Aktywuje / dezaktywuje trap SNMP, gdy system jest przeciążony.
Alarm-Power-Fail	☑	Aktywuje / dezaktywuje trap SNMP przy następujących stanach zasilania systemu: - przepięcie - spadek napięcia poniżej zakresu - przepięcie RPS - spadek napięcia poniżej zakresu RPS
BPDU	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest zablokowany z powodu: - BPDU Guard - BDPU Root - zmiana stanu portu BPDU
Loop Detection	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest zablokowany przez Loop Detection.
PD-Alive	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest aktywowany / dezaktywowany przez administratora.
Port-Admin-State-Change	☑	Aktywuje / dezaktywuje trap SNMP, gdy port wykazuje zmianę w górę/w dół.
Port-Link-Change	☑	Aktywuje / dezaktywuje trap SNMP, gdy zmienia się topologia STP.
STP-Topology-Change	☑	Aktywuje / dezaktywuje trap SNMP, gdy zmienia się topologia STP.
Traffic-Alarm (Traffic Flooding and Port Utilization)	☑	Aktywuje / dezaktywuje trap SNMP, gdy port zablokowany jest przez „Traffic Monitor”.

9.2.4.2 Port Event Settings

Wskazówka

Generowanie trapów Port-Link-Change

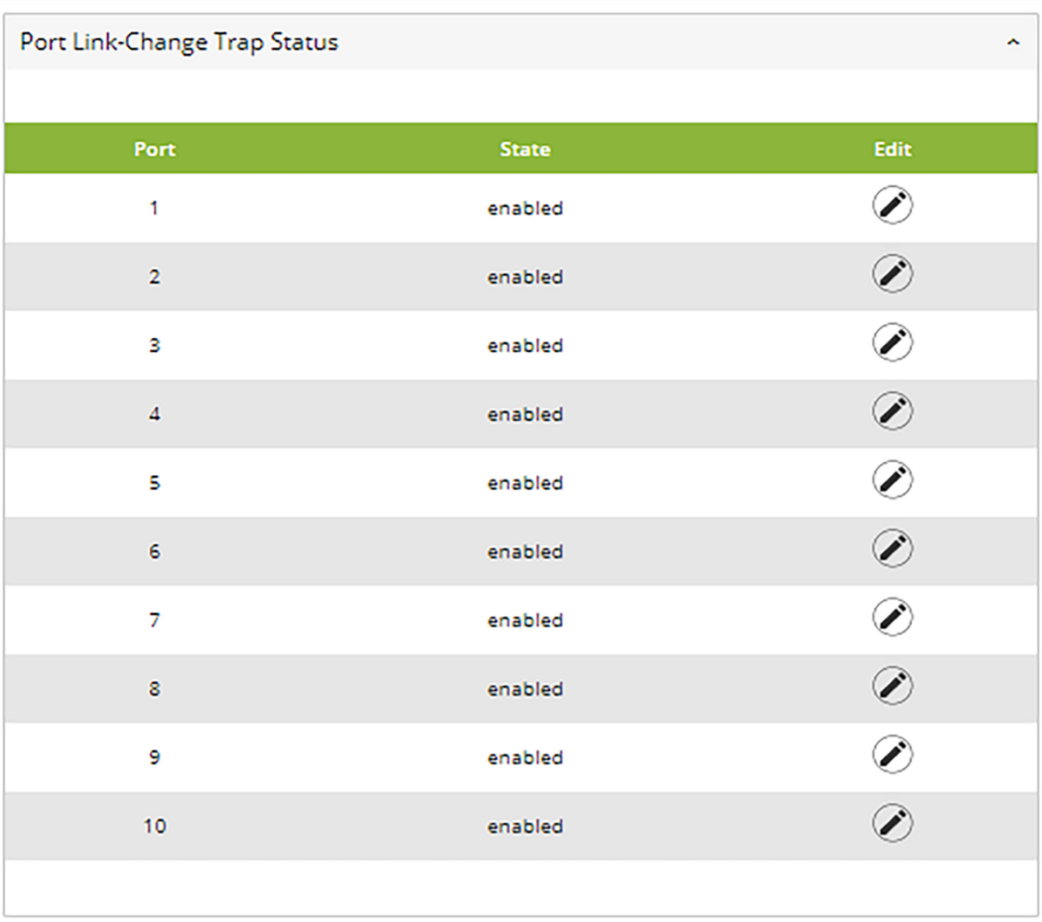
Użytkownicy mogą włączyć lub wyłączyć generowanie trapów dla pojedynczych lub wielu portów.



Ilustracja 55: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“

Tabela 39: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“

Port Link-Change Trap Settings		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Port Event Settings”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Port Event Settings”.
Port State	**Disable**	W polu wyboru należy wybrać „Disable”, aby dezaktywować funkcję „Port Event Settings” dla switcha.
	Enable	W polu wyboru należy wybrać „Enable”, aby aktywować funkcję „Port Event Settings” dla switcha.



Ilustracja 56: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“

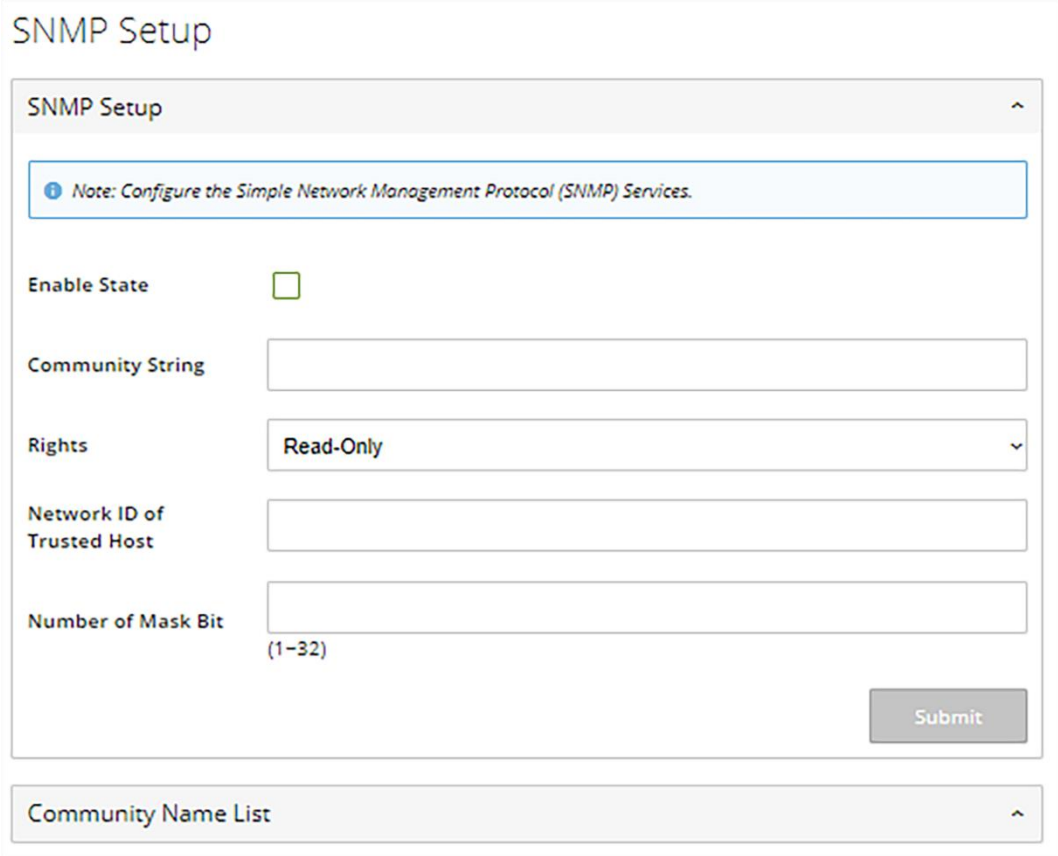
Tabela 40: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“

Port Link-Change Trap Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlany jest zakres portów.
State	Enable Disable	W tym polu wyświetlany jest status portu.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.2.4.3 SNMP Setup

Wskazówka

Simple Network Management Protocol (SNMP)
Tutaj można skonfigurować usługi „Simple Network Management Protocol” (SNMP).



Ilustracja 57: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Setup“ – „SNMP Setup“

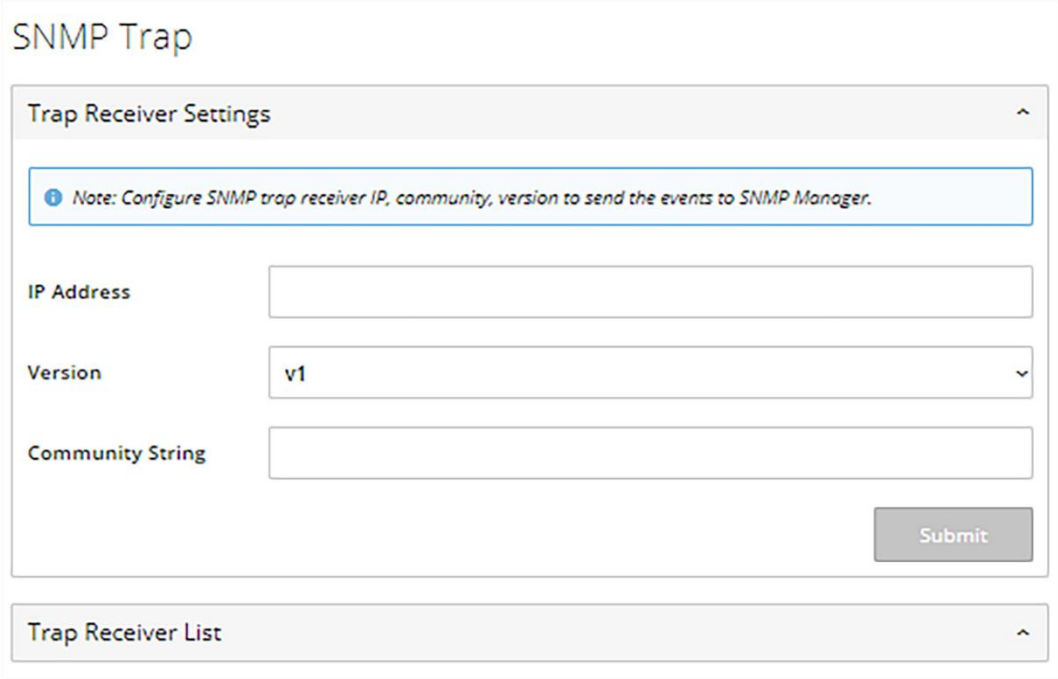
Tabela 41: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Setup“ – „SNMP Setup“

SNMP Setup			
Parametr	**Domyślnie**	**Opis**	
Enable State	☐	☐	Funkcja „SNMP Setup” nie jest dla switcha aktywowana.
		☑	Funkcja „SNMP Setup” jest dla switcha aktywowana.
Community String		W tym polu wpisuje się „Community String”, funkcjonujący jako hasło dla żądań stacji zarządzającej. Jest on elementem tekstowym, funkcjonującym jako hasło. Funkcja ta wykorzystywana jest do uwierzytelniania wiadomości, wymienianych między stacja zarządzającą („SNMP Manager“) i urządzeniem („SNMP Agent“). „Community String” zawarty jest w każdym pakiecie, transmitowanym między oboma tymi punktami.	
Rights	**Read-Only**	W polu wyboru należy wybrać „Read Only“, aby manager SNMP mógł wykorzystać te stringi w celu otrzymywania informacji od switcha.	
	Read/ Write	W polu wyboru należy wybrać „Read/Write“, aby manager SNMP mógł wykorzystać te stringi w celu skonfigurowania ustawień switcha.	
Network ID of Trusted Host		W polu edycji należy wpisać adres IP rozproszonej stacji zarządzającej SNMP, używając zapisu z kropkami (np. 192.168.1.0).	
Number of Mask Bit (1-32)		W polu edycji należy wpisać adres IP maski podsieci.	
Community Name List			
Parametr	**Domyślnie**	**Opis**	
No.		W tej kolumnie wyświetlany jest numer „Community“. Służy on wyłącznie do identyfikacji. Należy kliknąć ten numer, aby zmodyfikować ustawienie specyficznej „Community“.	
Community String		W tej kolumnie wyświetlany jest „Community String“ SNMP. Jest on elementem tekstowym, funkcjonującym jako hasło.	
Rights	Read-Only, Read/ Write	W tej kolumnie wyświetlane są uprawnienia dla „SNMP-Community-String”.	
Network ID of the Trusted Host		W tej kolumnie wyświetlany jest adres IP rozproszonej stacji zarządzającej SNMP po zmodyfikowaniu przez maskę podsieci.	
Number of Mask Bit		W tej kolumnie wyświetlana jest maska podsieci dla adresu IP rozproszonej stacji zarządzającej SNMP.	
Action		Należy kliknąć **[Clear]**, aby usunąć specyficzny „Community String”.	

9.2.4.4 SNMP Trap

Wskazówka

Ustawienia odbiorcy trap
W tym oknie można skonfigurować adres IP, Community i wersję dla odbiorcy trap SNMP, aby wysyłał on zdarzenia do managera SNMP.



Ilustracja 58: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“

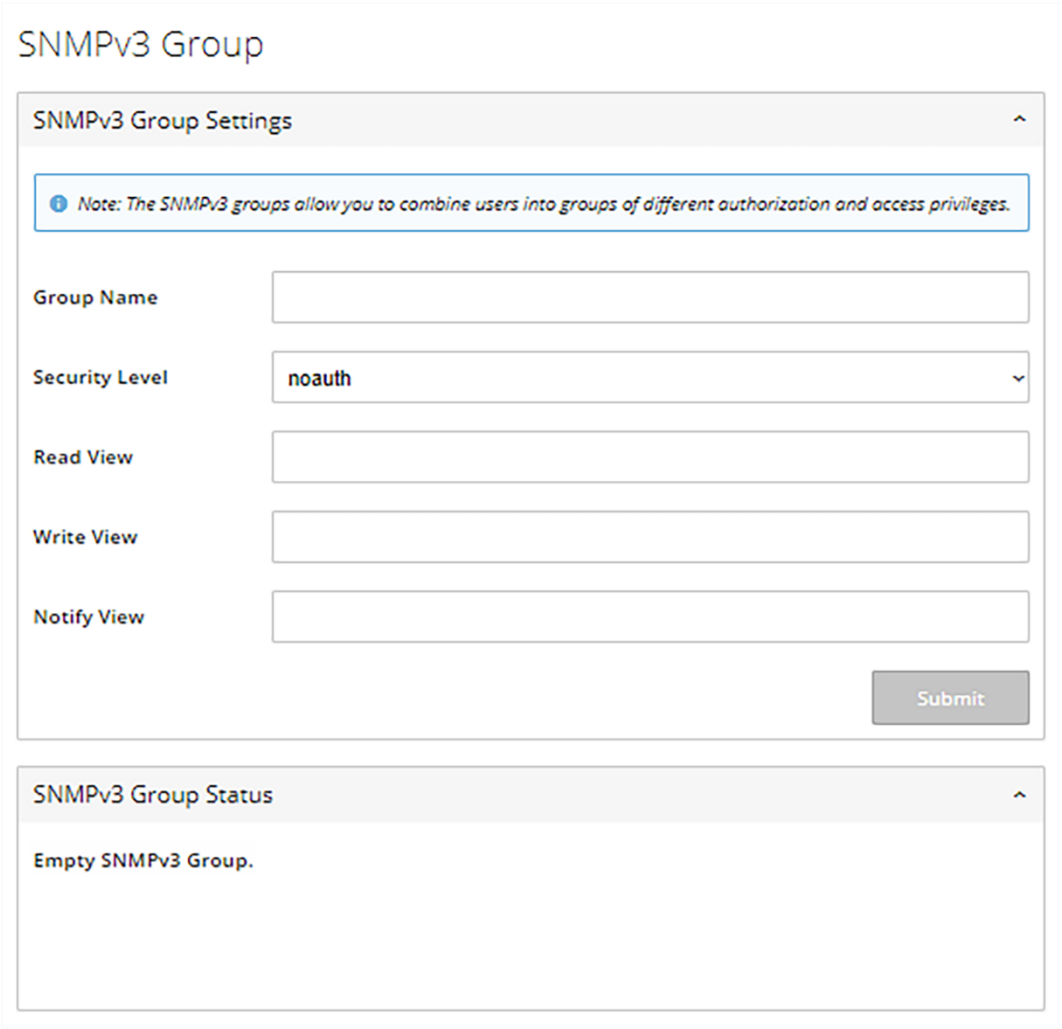
Tabela 42: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“

Trap Receiver Settings		
Parametr	**Domyślnie**	**Opis**
IP Address		W polu edycji należy wpisać adres IP rozproszonej stacji trap.
Version	**v1**	W polu wyboru należy wybrać „v1“, gdy ma być wykorzystana wersja 1 SNMP.
	v2c	W polu wyboru należy wybrać „v2c“, gdy ma być wykorzystana wersja v2c SNMP.
Community String		W polu edycji należy wpisać adres IP rozproszonej stacji zarządzającej SNMP, używając zapisu z kropkami (np. 192.168.1.0).
Trap Receiver List		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlany jest numer „Community“. Służy on wyłącznie do identyfikacji. Należy kliknąć ten numer, aby zmodyfikować ustawienie specyficznej „Community“.
IP Address		W tej kolumnie wyświetlany jest adres IP rozproszonej stacji trap.
Version	v1 v2c	W tej kolumnie wyświetlana jest zastosowana wersja SNMP.
Community String		W tej kolumnie wyświetlany jest zastosowany przez tę rozproszoną stację trap „Community String“.
Action		Aby usunąć skonfigurowaną stację odbiorczą trap, należy kliknąć przycisk **[Clear]**.

9.2.4.5 SNMPv3 Group

Wskazówka

Możliwości grup SNMPv3
Grupy SNMPv3 umożliwiają łączenie użytkowników w grupy o różnym poziomie autoryzacji i różnych uprawnieniach dostępu.



Ilustracja 59: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 Group“

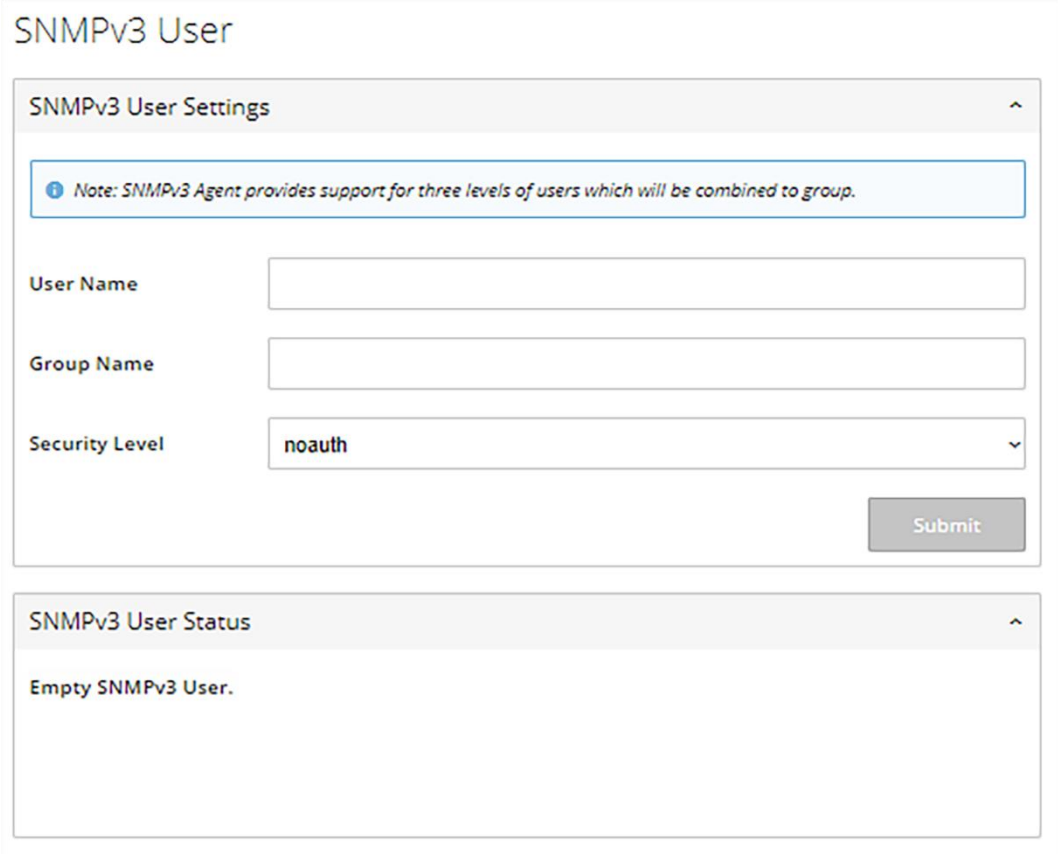
Tabela 43: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 Group“

SNMPv3 Group Settings		
Parametr	**Domyślnie**	**Opis**
Group Name		W polu edycji należy wpisać nazwę grupy dla SNMPv3.
Security Level		W polu wyboru można wybrać poziom bezpieczeństwa.
	Noauth	Gdy w polu wyboru wybrana jest opcja „noauth“, nie ma możliwości zmiany „Auth Algorithmus“ i „Priv-Algorithmus“.
	auth	Gdy w polu wyboru wybrana jest opcja „auth“, istnieje możliwość zmiany „Auth Algorithmus“ i „Auth Password“.
	priv	Gdy w polu wyboru wybrana jest opcja „priv“, istnieje możliwość zmiany „Auth Algorithmus“, „Auth Password“, „Priv Algorithmus“ i „Priv Password“.
Read View	**None**	W polu edycji należy wpisać nazwę obiektów, które mają być dostępne w widoku do odczytu. Jeśli nie jest wpisany żaden obiekt, wszystkie obiekty są do odczytu.
Write View	**None**	W polu edycji należy wpisać nazwę obiektów, do których ma być wybrany dostęp zapisu. Jeśli nie zdefiniowano widoku zapisu ani widoku powiadomień, nie jest przyznany dostęp do zapisu i obiekty nie mogą wysyłać powiadomień członkom grupy.
Notify View	**None**	W polu edycji należy wpisać nazwę obiektu, który może odbierać powiadomienia użytkowników. Poprzez użycie widoku powiadomień grupa określa listę powiadomień, które jej użytkownicy mogą otrzymywać.
SNMPv3 Group Status		
Parametr	**Domyślnie**	**Opis**
Group Name		W tej kolumnie wyświetlana jest nazwa grupy.
Security Model		W tej kolumnie wyświetlany jest wybrany poziom bezpieczeństwa. Zawsze wyświetlane v3: model zabezpieczeń oparty na użytkowniku (User-based Security Model, USM)
Security Level		W tej kolumnie wyświetlany jest wybrany poziom bezpieczeństwa.
Read View		W tej kolumnie wyświetlany jest „Read View“.
Write View		W tej kolumnie wyświetlany jest „Write View“.
Notify View		W tej kolumnie wyświetlany jest „Notify View“.
Action		Aby usunąć daną pozycję, należy kliknąć **[Clear]**.

9.2.4.6 SNMPv3 User

Wskazówka

Wsparcie agenta SNMPv3
Agent SNMPv3 zapewnia wsparcie dla trzech poziomów użytkowników, które można zebrać w grupę.



Ilustracja 60: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 User“

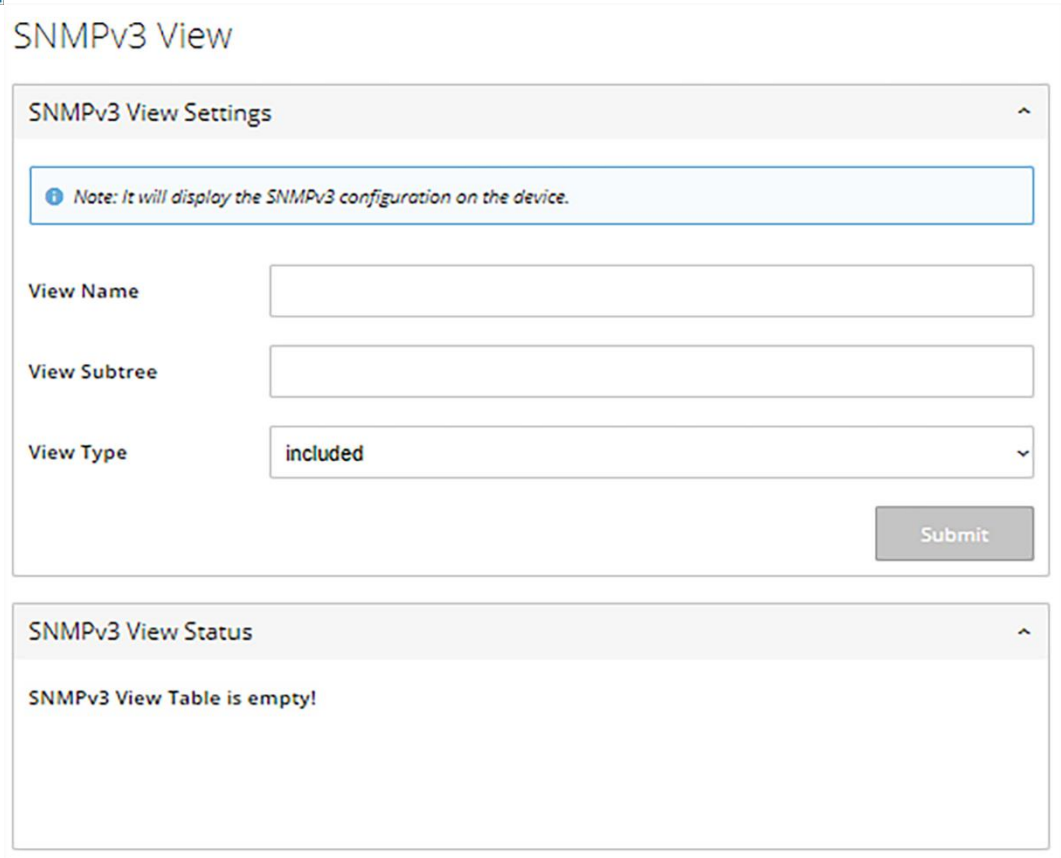
Tabela 44: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 User“

SNMPv3 User Settings		
Parametr	**Domyślnie**	**Opis**
User Name		W polu edycji należy wpisać nową nazwę użytkownika lub zmodyfikować już istniejącą.
Group Name		W polu edycji należy wpisać nazwę grupy dla SNMPv3.
Security Level		W polu wyboru można wybrać poziom bezpieczeństwa.
	noauth	Gdy w polu wyboru wybrana jest opcja „noauth“, nie ma możliwości zmiany „Auth Algorithmus“ i „Priv-Algorithmus“.
	auth	Gdy w polu wyboru wybrana jest opcja „auth“, istnieje możliwość zmiany „Auth Algorithmus“ i „Auth Password“.
	priv	Gdy w polu wyboru wybrana jest opcja „priv“, istnieje możliwość zmiany „Auth Algorithmus“, „Priv Algorithmus“ i „Priv Password“.
SNMPv3 User Status		
Parametr	**Domyślnie**	**Opis**
User Name		W tej kolumnie wyświetlana jest nazwa użytkownika.
Group Name		W tej kolumnie wyświetlana jest nazwa grupy.
Auth Protocol		W tej kolumnie wyświetlany jest wybrany „Auth Algorithmus“.
Priv Protocol		W tej kolumnie wyświetlany jest wybrany „Priv Algorithmus“.
Action		Aby usunąć daną pozycję, należy kliknąć **[Clear]**.

9.2.4.7 SNMPv3 View

Wskazówka

Wyświetlanie konfiguracji SNMPv3
W tym widoku wyświetlana jest konfiguracja SNMPv3 na urządzeniu.



Ilustracja 61: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 View“

Tabela 45: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 View“

SNMPv3 View Settings		
Parametr	**Domyślnie**	**Opis**
View Name		W polu edycji należy wpisać nazwę dla „SNMPv3 View“.
View Subtree		W polu edycji należy wpisać nazwę dla „Subtree“.
View Type	**included**	Gdy w polu wyboru wybrana jest opcja „included“, dodane zostaje „Subtree“.
	excluded	Gdy w polu wyboru wybrana jest opcja „excluded“, nie zostaje dodane „Subtree“.
SNMPv3 View Status		
Parametr	**Domyślnie**	**Opis**
View Name		W tej kolumnie wyświetlana jest nazwa „SNMPv3 View“.
View Subtree		W tej kolumnie wyświetlana jest nazwa „Subtree“.
View Type	Inserted Removed	W tej kolumnie wyświetlany jest wybrany typ.
Action		Aby usunąć daną pozycję, należy kliknąć **[Clear]**.

9.2.5 System Management

9.2.5.1 General Setup

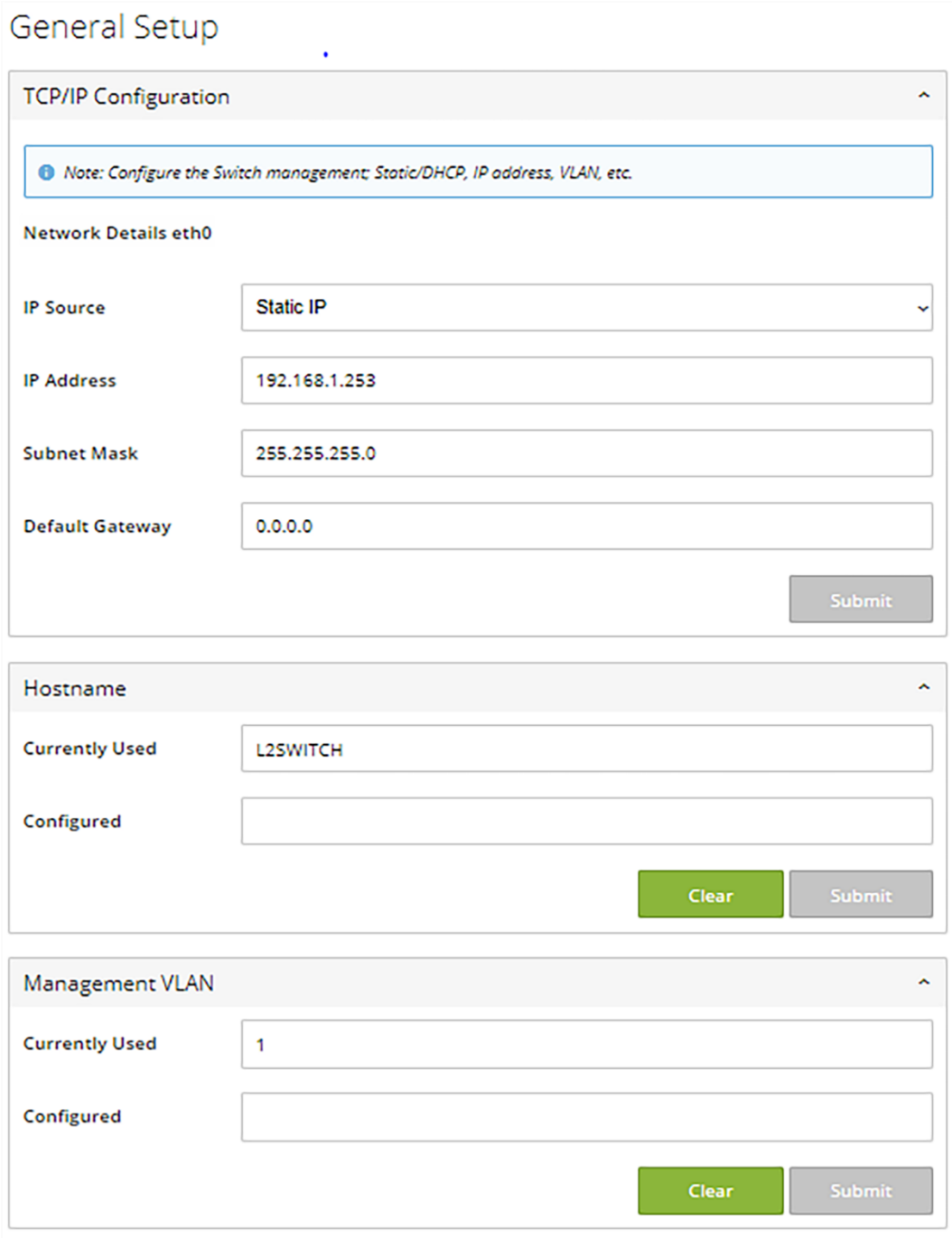
Host Name

Nazwa hosta i nazwa systemu SNMP są identyczne. Maksymalna długość wynosi 64 znaki.

Wskazówka



Konfiguracja zarządzania switchem
Należy skonfigurować zarządzanie switchem (static/DHCP, adres IP, VLAN itp.).



Ilustracja 62: Zakładka „Configuration“ – menu „System Management“ – „General Setup“

Tabela 46: Zakładka „Configuration“ – menu „System Management“ – „General Setup“

TCP/IP Configuration		
Parametr	**Domyślnie**	**Opis**
IP Source	**Static IP** DHCP	W polu wyboru należy wybrać opcję dla „IP Source“ (adres źródłowy IP).
IP Address	**192.168.1.254**	Należy wpisać adres IP switcha, używając zapisu z kropkami.
Subnet Mask	**255.255.255.0**	W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.
Default Gateway	**0.0.0.0**	Należy wpisać adres IP domyślnej bramy, używając zapisu z kropkami.
Hostname		
Parametr	**Domyślnie**	**Opis**
Currently Used	**L2SWITCH**	W tej kolumnie wyświetlana jest nazwa hosta.
Configured		W polu edycji należy wpisać nazwę hosta.
Management VLAN		
Parametr	**Domyślnie**	**Opis**
Currently Used	**1**	W tej kolumnie wyświetlany jest VLAN zarządzania.
Configured		W polu edycji należy wpisać VLAN zarządzania.

9.2.5.2 SNTP

SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) jest protokołem do synchronizacji zegarów w systemach komputerowych.
Jest to mniej złożona implementacja NTP („**N**etwork **T**ime **P**rotocol“).

SNTP wykorzystuje uniwersalny czas koordynowany UTC („**C**oordinated **U**niversal **T**ime“). Informacje o strefach czasowych i czasie letnim nie są transmitowane. Informacje te leżą poza zakresem protokołu i należy pobrać je osobno.

Port SNTP ma numer 123.

Wskazówka



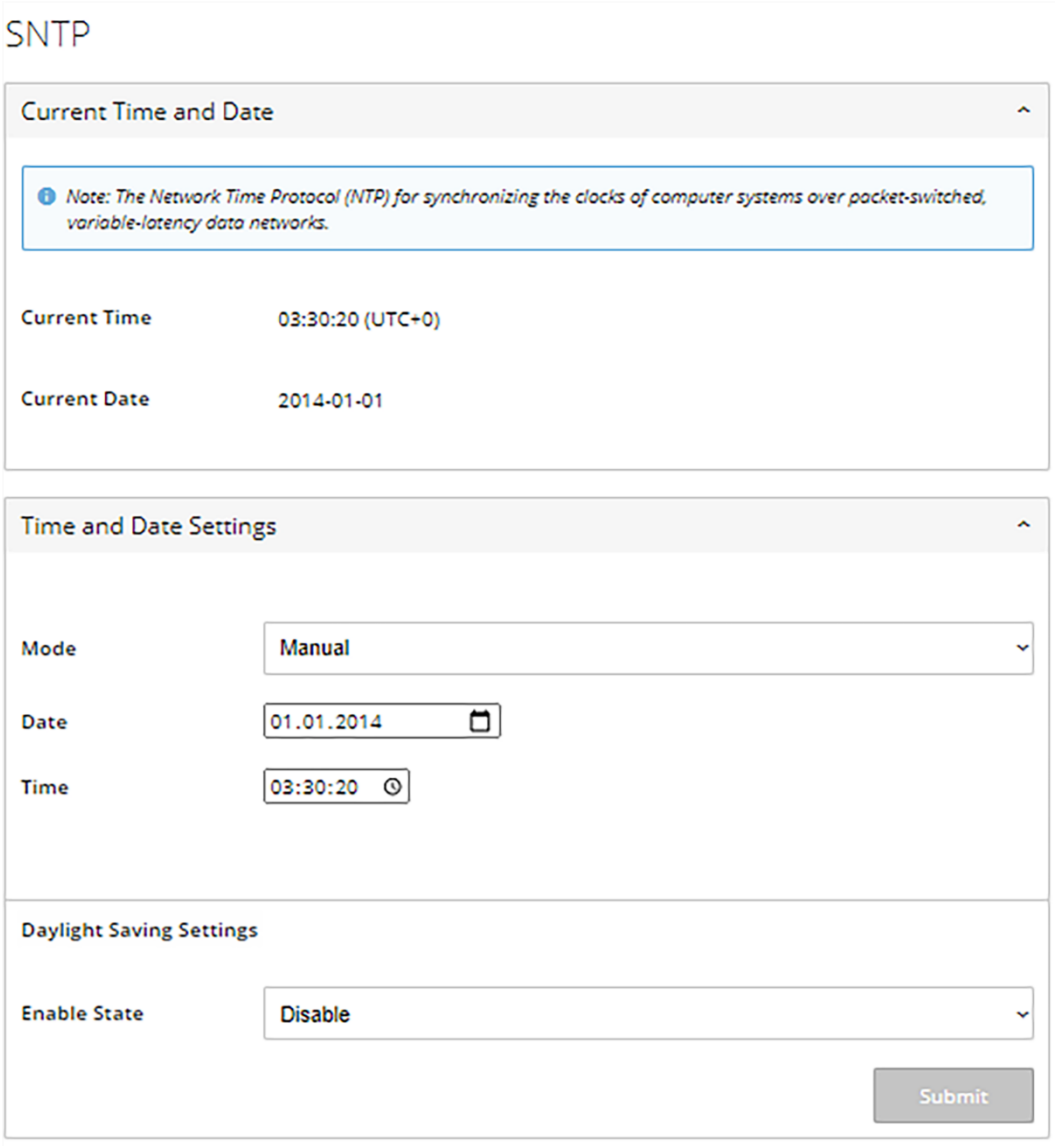
Wskazówka

1. Serwer SNTP odpowiada zawsze aktualnym uniwersalnym czasem koordynowanym UTC.
2. Gdy switch odbiera czas odpowiedzi SNTP, porównuje go z konfiguracją stref czasowych i odpowiednio konfiguruje czas dla switcha.
3. Jeśli nie skonfigurowano adresu IP serwera czasu, switch nie wysyła pakietów zapytań SNTP.
4. Jeśli switch nie odbiera pakietów odpowiedzi SNTP, powtarza zapytanie bez ograniczeń czasowych co dziesięć sekund.
5. Gdy switch otrzymuje odpowiedź SNTP, powtarza co godzinę zapytanie do serwera NTP.
6. Po zmianie strefy czasowej i serwera NTP switch powtarza proces zapytania.
7. Brak domyślnego serwera SNTP.

Wskazówka

Synchronizacja zegarów w systemach komputerowych

SNTP („Simple Network Time Protocol“) jest protokołem do synchronizacji zegarów w systemach komputerowych przez sieci pakietowe o zmiennym czasie przesyłu pakietów.



Ilustracja 63: Zakładka „Configuration“ – menu „System Management“ – „SNTP“

Tabela 47: Zakładka „Configuration“ – menu „System Management“ – „SNTP“

Current Time and Date				
Parametr	**Domyślnie**	**Opis**		
Current Time		W tym polu wyświetlana jest aktualna godzina otwarcia lub aktualizacji tego menu.		
Current Date		W tym polu wyświetlana jest aktualna data otwarcia lub aktualizacji tego menu.		
Time and Date Settings				
Parametr	**Domyślnie**	**Opis**		
Mode	Manual	Tę opcję należy wybrać, aby ręcznie ustawić w systemie czas i datę. Po kliknięciu **[Sumit]** pojawiają się nowe dane w polach „Current Time“ i „Current Date“.		
		Date	Należy wpisać nową datę w formacie dzień/miesiąc/rok. DD.MM.RRRR	
		Time	Należy wpisać nową datę w formacie godzina/minuta/sekunda. --:--:--	
	Network Time Protocol	Tę opcję należy wybrać, aby użyć Network Time Protocol (NTP) dla synchronizacji czasu.		
	NTP Server **0.0.0.0**	Public	W polu wyboru należy wybrać tę opcję, gdy ma być wykorzystany publiczny serwer.	
			ntp0.fau.de - Europa	
			ntps1-1.cs.tu-berlin.de - Europa	
		Manual	W polu wyboru należy wybrać tę opcję, gdy mają być zastosowane ręczne ustawienia.	
			IP	Należy wpisać adres IP serwera NTP, używając zapisu z kropkami.
			Domain Name	Należy wpisać adres domeny switcha.
	Time Zone **+0000**	Należy wpisać różnicę czasu między UTC („Universal Time Coordinated“, dawniej GMT, „Greenwich Mean Time“) a strefą czasową w formacie gg:mm.		

Tabela 47: Zakładka „Configuration“ – menu „System Management“ – „SNTP“

Daylight Saving Settings		
Parametr	**Domyślnie**	**Opis**
Enable State	**Disable**	Należy wybrać „Disable“, jeśli nie używamy czasu letniego.
	Enable	Należy wybrać „Enable“, jeśli nie używamy czasu letniego.
Start Date[1)]		Należy wpisać datę i godzinę początku czasu letniego, jeśli opcja ta została aktywowana. Czas wyświetlany jest w formacie 24-godzinnym.
End Date[2)]		Należy wpisać datę i godzinę końca czasu letniego, jeśli opcja ta została aktywowana. Czas wyświetlany jest w formacie 24-godzinnym.
1)	Na większości terytorium USA czas letni rozpoczyna się w drugą niedzielę marca. W każdej strefie czasowej USA czas letni rozpoczyna się o godzinie 02:00 czasu miejscowego. Zgodnie z tym należy wybrać „Second, Sunday, March“ i „2:00“. W Unii Europejskiej czas letni rozpoczyna się w ostatnią niedzielę marca. We wszystkich strefach czasowych Unii Europejskiej rozpoczyna się on w tym samym momencie (01:00 GMT lub UTC). Zgodnie z tym należy wybrać „Last, Sunday, March“ oraz w ostatnim polu wpisać godzinę w swojej strefie czasowej. Na przykład dla Niemiec należy wpisać „2:00“, gdyż czas letni w Niemczech jest o godzinę przed GMT lub UTC (GMT+1).	
2)	W USA czas letni kończy się w ostatnią niedzielę października. W każdej strefie czasowej USA czas letni kończy się o godzinie 02:00 czasu miejscowego. Zgodnie z tym należy wybrać „First, Sunday, November“ i „2:00“. W Unii Europejskiej czas letni kończy się w ostatnią niedzielę października. We wszystkich strefach czasowych Unii Europejskiej kończy się on w tym samym momencie (01:00 GMT lub UTC). Zgodnie z tym należy wybrać „Last, Sunday, November“ oraz w ostatnim polu wpisać godzinę w swojej strefie czasowej. Na przykład dla Niemiec należy wpisać „2:00“, gdyż czas letni w Niemczech jest o godzinę przed GMT lub UTC (GMT+1).	

9.2.5.3 User Account

Switch umożliwia utworzenie maksymalnie sześciu kont użytkownika. Nazwa użytkownika powinna składać się z kombinacji cyfr lub liter. Ostatniego konta administratora nie można usunąć. W celu wykorzystania CLI lub Web Based Management użytkownik musi zalogować się aktualnym kontem użytkownika.

Uprawnienia użytkowników

Switch wspiera dwa rodzaje kont użytkownika:

Domyślne konta użytkownika zawierają następujące informacje:
User Name = „admin“
User Password = „wago“

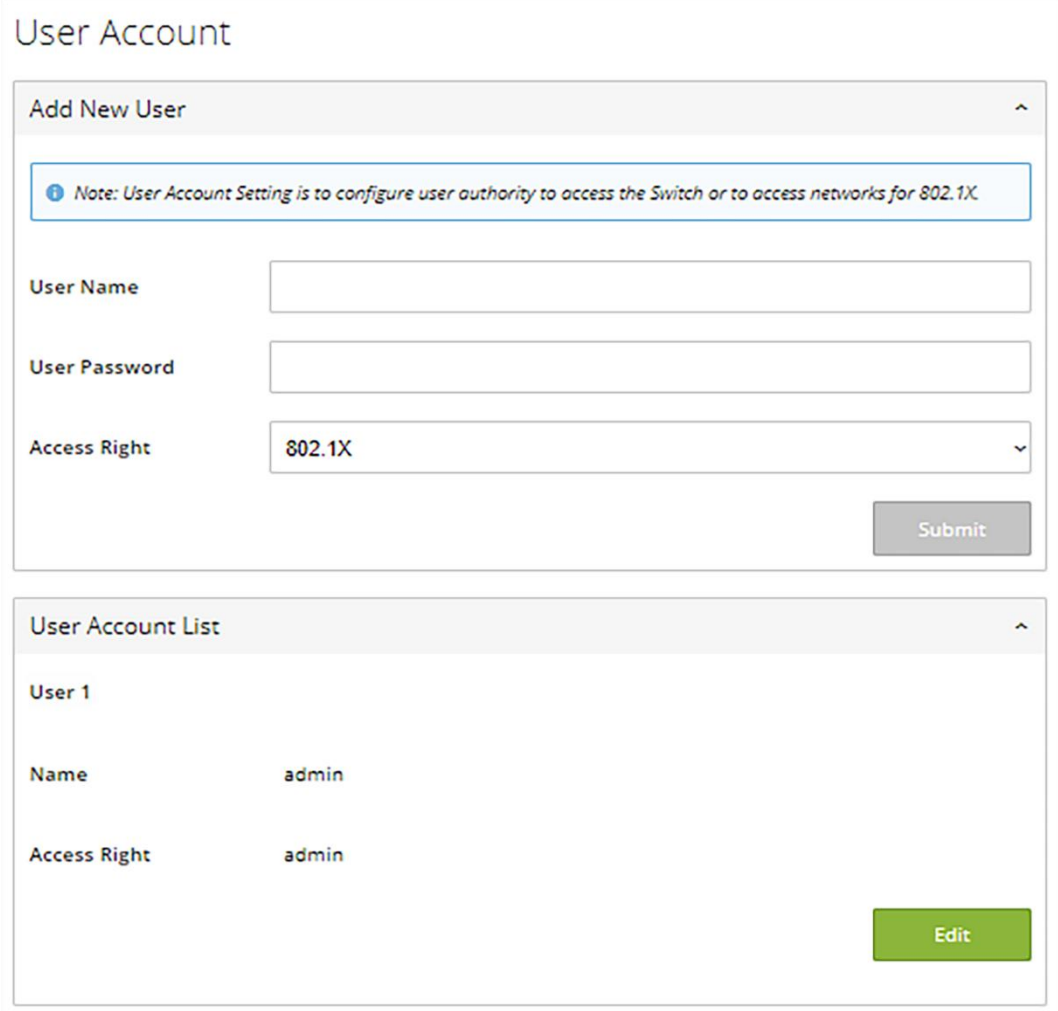
1. Konta administratora uprawnienia do zapisu/odczytu

2. Normalne konta użytkowników tylko uprawnienie do odczytu
   - Skorzystanie z uprzywilejowanego trybu w CLI nie jest możliwe.
   - Zmiana konfiguracji w Web-Management nie jest możliwa.

Wskazówka

Ustawienia kont użytkowników

W ustawieniach kont użytkowników można skonfigurować uprawnienia dostępu do switcha lub do sieci 802.1X.



Ilustracja 64: Zakładka „Configuration“ – Menu „System Management“ – „User Account“

Tabela 48: Zakładka „Configuration“ – Menu „System Management“ – „User Account“

User Account Settings		
Parametr	**Domyślnie**	**Opis**
User Name		W polu edycji należy wpisać nową nazwę użytkownika lub zmodyfikować już istniejącą.
User Password		W polu edycji należy wpisać nowe hasło lub zmodyfikować już istniejące. Można wpisać 32 znaki alfanumeryczne lub cyfry.
User Authority		W tym polu wyboru wybiera się rodzaj konta użytkownika.
	802.1X	W polu wyboru należy wybrać „802.1X“, jeśli ci użytkownicy mają być uwierzytelniani.
	Normal (Read Only)	W polu wyboru należy wybrać „Normal“, (Tylko do odczytu)“, dla tego konta użytkownika potrzebne jest tylko uprawnienie do odczytu.
	Admin	W polu wyboru należy wybrać „Admin“, jeśli dla tego konta użytkownika potrzebne jest uprawnienie do zapisu i odczytu.
User Account List		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlany jest numer indeksu wpisu.
Name		W tej kolumnie wyświetlana jest nazwa konta użytkownika.
Access Right		W tej kolumnie wyświetlany jest rodzaj konta użytkownika.
Action		Aby usunąć konto użytkownika, należy kliknąć przycisk **[Clear]**.
		Wskazówka  **Usuwanie konta administratora** Ostatniego konta administratora nie można usunąć.

9.2.6 Storm Control

Przy występowaniu burzy broadcastowej sieć przeciążona jest długotrwale pakietami transmitowanymi metodą broadcast lub mulicast. Burze broadcastowe mogą całkowicie sparaliżować łączność w sieci przez stale narastającą liczbę pakietów danych.

„Storm Control“ chroni szerokość pasma switcha przed zalewem pakietami, włącznie z pakietami broadcast, multicast i DLF („**D**estination **L**ookup **F**ailure“). Współczynnik jest progiem, który ogranicza całkowitą liczbę określonych typów pakietów. Na przykład, jeśli wybrano opcje broadcast i multicast, całkowita liczba pakietów danych przesyłanych na sekundę dla tych dwóch typów nie zostanie przekroczona.

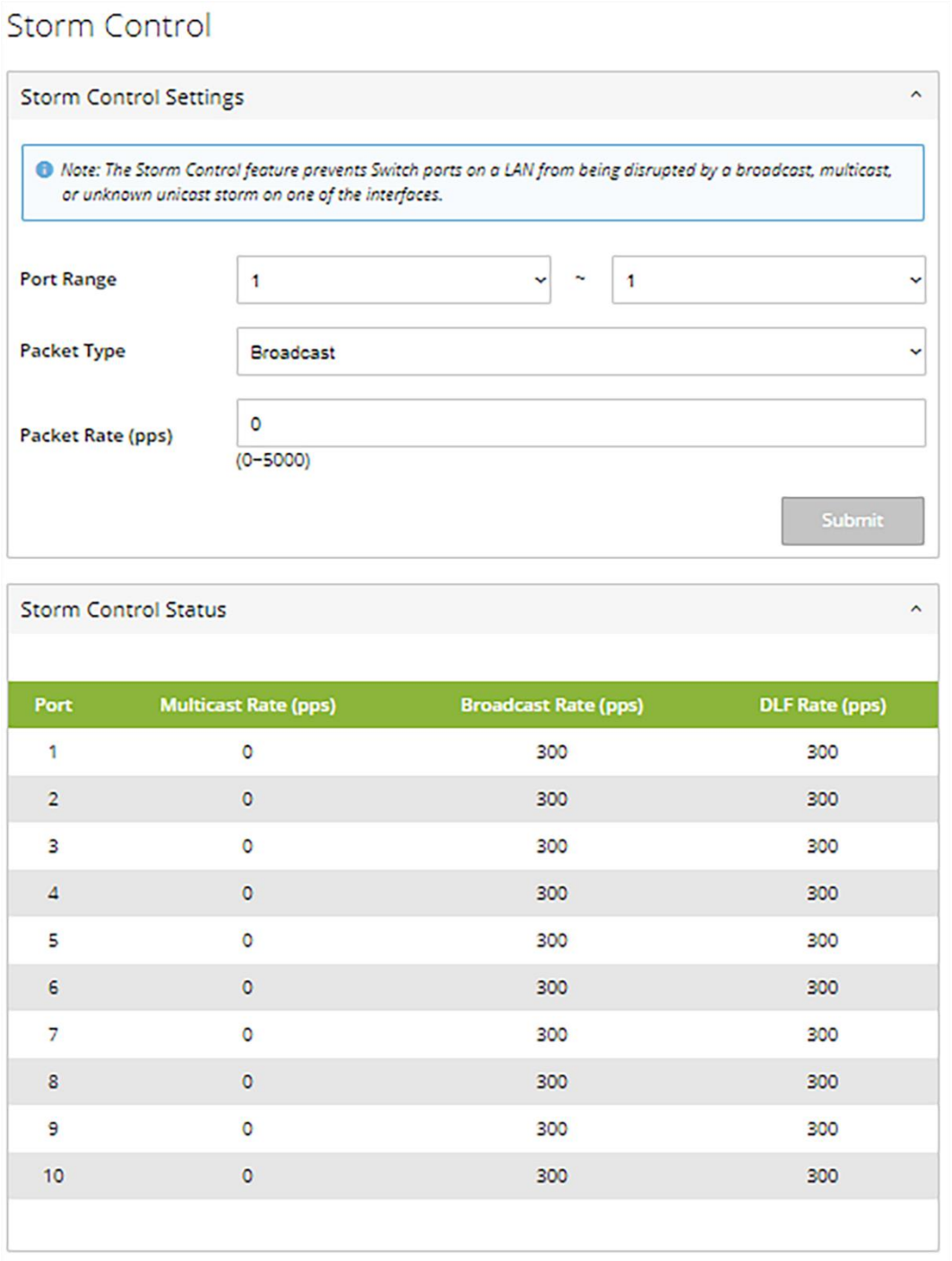
„Broadcast Storm Control“ ogranicza liczbę pakietów broadcast, multicast i nieznanych unicast (określanych też jako „Destination Lookup Failure“ lub DLF), które mogą być odbierane przez switch na portach w ciągu sekundy. Po osiągnięciu maksymalnej liczby tych pakietów danych na sekundę wszystkie pozostałe pakiety danych zostają odrzucone. Funkcję tę należy aktywować w celu ograniczenia liczby tych pakietów danych w sieci.

Domyślna wartość to 300 pakietów na sekundę dla Broadcast i DLF. Można ustawić maksymalną wartość 5000 pakietów na sekundę dla Multicast, Broadcast lub DLF.

Wskazówka

Działanie funkcji Storm Control

Funkcja „Storm Control” zapobiega zakłóceniom portów switcha w sieci LAN na jednym z interfejsów, spowodowanym przez pakiety broadcast, multicast lub unicast.



Ilustracja 65: Zakładka „Configuration“ – menu „Storm Control“

Tabela 49: Zakładka „Configuration“ – menu „Storm Control“

Storm Control Settings		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Storm Control“.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Storm Control“.
Packet Type	Broadcast	W polu wyboru należy wybrać „Broadcast“, aby ustawić wartość graniczną liczby odebranych pakietów broadcast w ciągu sekundy.
	Multicast	W polu wyboru należy wybrać „Multicast“, aby ustawić wartość graniczną liczby odebranych pakietów „Multicast“ w ciągu sekundy.
	DLF	W polu wyboru należy wybrać „DLF“, aby ustawić wartość graniczną liczby odebranych pakietów DLF w ciągu sekundy.
Packet Rate (0-5000)	300 = Broadcast/DLF Rate 0 = Multicast	W polu wyboru należy wybrać liczbę pakietów danych (rodzaju wyspecyfikowanego w polu „Typ“), jaką może odebrać switch w ciągu sekundy.
Storm Control Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
Multicast Rate (pps)		W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy multicast.
Broadcast Rate (pps)		W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy broadcast.
DLF Rate (pps)		W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy DLF.

9.3 Security

9.3.1 802.1X

9.3.1.1 Standard komunikacyjny IEEE 802.1X

IEEE 802.1X jest standardem IEEE dla sterowania dostępem do sieci na bazie portów (przy czym „port“ jest tu pojedynczym punktem dostępu do infrastruktury LAN). Standard ten wchodzi w skład grupy protokołów sieciowych IEEE 802.1. Udostępnia on mechanizm uwierzytelnienia dla urządzeń, chcących łączyć się z siecią LAN, i albo tworzy połącznie punkt-punkt, albo odmawia jego utworzenia, gdy uwierzytelnienie nie powiedzie się. Stosowany jest on dla większości bezprzewodowych punktów dostępu 802.11 i działa na bazie EAP („**E**xtensible **A**uthentication **P**rotocol“).

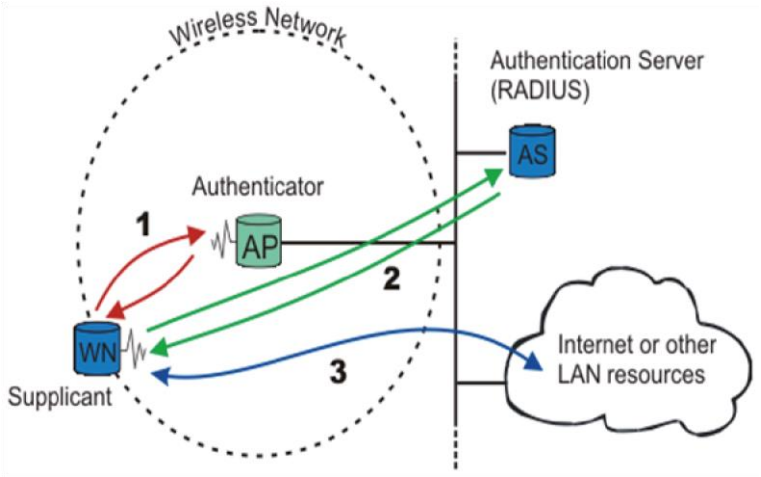
IEEE 802.1X wykorzystuje uwierzytelnienie na bazie portów, polegające na komunikacji między następującymi uczestnikami: tzw. „Supplicant“, „Authenticator“ i serwer uwierzytelniający. „Supplicant“ to najczęściej oprogramowanie na urządzeniu Client, przykładowo laptop, „Authenticator“ to połączony przewodem switch ETHERNET lub bezprzewodowy punkt dostępu, a serwer uwierzytelniający to zazwyczaj baza danych RADIUS („**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice“).

„Authenticator“ pełni funkcję swego rodzaju strażnika chronionej sieci. „Supplicant“ (np. urządzenie Client) dopóty nie uzyskuje od „Authenticator“ dostępu do chronionej strony sieci, dopóki jego tożsamość nie zostanie uwierzytelniona. Przy uwierzytelnieniu na bazie portów 802.1X „Supplicant“ musi udostępnić punktowi „Authentikator“ dane do logowania, takie jak nazwa użytkownika i hasło lub cyfrowy certyfikat, które następnie przekazywane są do serwera uwierzytelniającego w celu weryfikacji. Gdy dane do logowania są ważne (zgadzają się z wpisami w bazie danych serwera uwierzytelniającego), „Supplicant“ (urządzenie Client) uzyskuje dostęp do zasobów chronionej strony sieci.

Gdy zostaje rozpoznany nowy „Supplicant“, port switcha „Authenticator“ zostaje aktywowany i ustawiony jako „unauthorized“. W tym stanie mogą być wymieniane tylko dane 802.1X, a inny ruch danych, jak chociażby DHCP i HTTP, zostaje zablokowany na warstwie sieci (Layer 3). „Authenticator“ wysyła do „Supplicant“ zapytanie identyfikacyjne EAP, a ten odpowiada pakietem EAP, który „Authenticator“ przesyła do serwera uwierzytelniającego. Gdy serwer uwierzytelniający zaakceptuje żądanie, „Authenticator“ przełącza port do stanu „authorized“ i usuwa blokadę ruchu danych. Gdy „Supplicant“ wylogowuje się, wysyła do „Authenticator“ wiadomość wylogowania EAP. Ten znowu przełącza port do stanu „unauthorized“ i tym samym ponownie blokuje wszystkie dane nie-EAP.

Serwer RADIUS

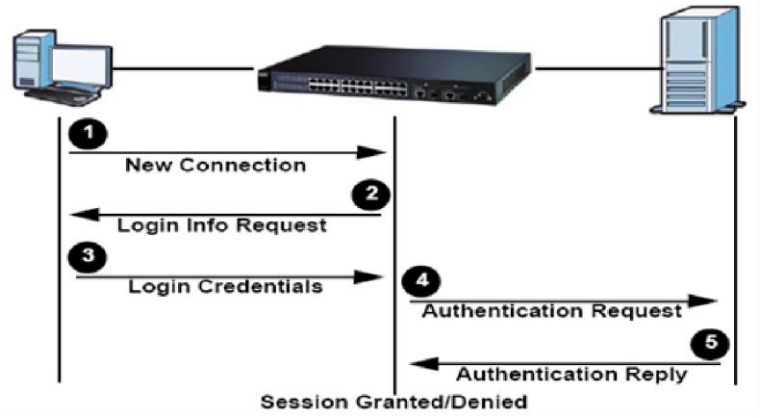
Serwer RADIUS („**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice“) jest protokołem bezpieczeństwa na bazie Client-Server do uwierzytelniania i kontroli uprawnień dostępu do sieci.
Serwer RADIUS wykorzystuje proces Challenge-Response i wspiera centralną administrację danymi użytkowników, takimi jak ID, hasła, numery telefonów, uprawnienia dostępu oraz danych account i składa się z protokołu księgowania i uwierzytelniania.
W połączeniu z DHCP i PPP może nastąpić automatyczna konfiguracja systemów dial-in z RADIUS.



Ilustracja 66: IEEE 802.1X

Na ilustracji poniżej przestawiono przebieg procesu uwierzytelniania dla portu z aktywowanym uwierzytelnieniem IEEE 802.1X. Switch wymaga od klienta danych do logowania w formie nazwy użytkownika i hasła.

Gdy Client prześle swoje dane do logowania, switch wysyła do serwera RADIUS żądanie uwierzytelnienia. Serwer RADIUS sprawdza następnie, czy Client uzyskał dostęp do portu.



Ilustracja 67: Serwer RADIUS

Lokalne konta użytkownika

Dzięki lokalnemu zapisowi profili użytkowników w switchu możliwe jest uwierzytelnianie przez niego użytkowników bez interakcji z serwerem uwierzytelniającym. Jednak liczba użytkowników, którzy mogą być w ten sposób uwierzytelnieni, jest ograniczona do 6.

Guest VLAN

Funkcja „Guest VLAN“ w uwierzytelnieniu IEEE 802.1X na bazie portów oferuje klientom ograniczone usługi, takie jak pobieranie klienta IEEE 802.1X. Klienci mogą aktualizować swój system za pomocą uwierzytelnienia IEEE 802.1X.

Gdy na porcie IEEE 802.1X aktywowana jest funkcja „Guest VLAN“, switch przydzieli do „Guest VLAN“ klientów, od których nie otrzymuje odpowiedzi na swoje żądanie EAP lub nie otrzymuje „Identity Frame“, bądź klientów, którzy nie wysyłają pakietów EAPOL (pakietów „EAP over LAN“).

Port Parameters

- **Admin Control Direction**

  Oba - Jeśli uwierzytelnianie portu 802.1X dla użytkownika nie powiedzie się, pakiety przychodzące i wychodzące na port zostaną odrzucone.

  Przychodzące - Jeśli uwierzytelnianie portu 802.1X dla użytkownika nie powiedzie się, odrzucone zostaną tylko pakiety przychodzące na port.

- **Re-Authentication**

  Funkcja ta pozwala zdefiniować, czy w celu utrzymania połączenia z portem uczestnik musi regularnie podawać na nowo nazwę użytkownika i hasło.

- **Okres reautentykacji**

  „Reauth Period“ pozwala zdefiniować, w jakich odstępach czasowych uczestnik musi podawać na nowo nazwę użytkownika i hasło w celu utrzymania połączenia z portem. Dopuszczalny zakres wartości w tym polu wynosi od 0 do 65535 sekund

- **Port Control Mode**

  „Auto“ Użytkownicy mają po uwierzytelnieniu dostęp do sieci.

  „Force-authorized“ Użytkownicy mają bez uwierzytelnienia dostęp do sieci.

  „Force-unauthorized“ Użytkownicy nie mają dostępu do sieci.

- **Quiet Period**
  „Quiet Period“ określa czas, jaki Client musi odczekać, zanim będzie mógł ponowić żądanie uwierzytelnienia. Zapobiega to przeciążeniu switcha przez powtarzające się żądania klienta. Dopuszczalny zakres wartości w tym polu wynosi od 0 do 65535 sekund.

- **Server-Timeout**
  Wartość „Server Timeout“ określa limit czasowy dla serwera uwierzytelniającego.

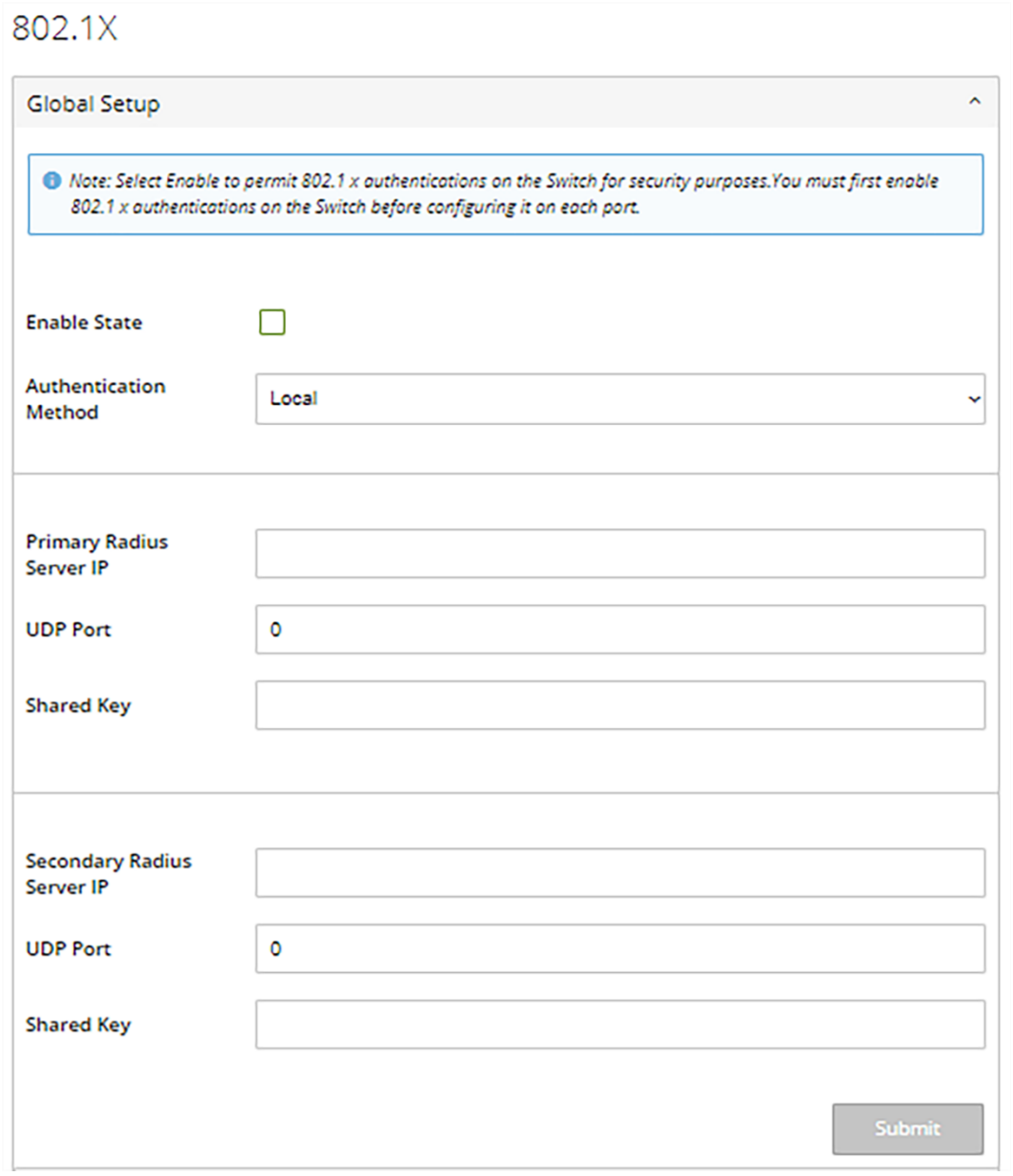
- **Supp-Timeout**
  „Supp Timeout“ jest wartością inicjalną limitu czasowego uczestnika „Supplicant“.

- **Max-req Time**
  „Max Req Time“ określa, jak często switch będzie próbował łączyć się z serwerem uwierzytelniającym, zanim uzna go za niepołączony. Dopuszczalny zakres w tym polu wynosi od 1 do 10 prób.

9.3.1.2 Global Setup

Wskazówka

Włączenie uwierzytelniania 802.1X
Ze względów bezpieczeństwa należy aktywować dla switcha uwierzytelnienie 802.1X. Najpierw należy aktywować dla switcha uwierzytelnienie 802.1X, a dopiero potem można konfigurować tę funkcję dla poszczególnych portów.



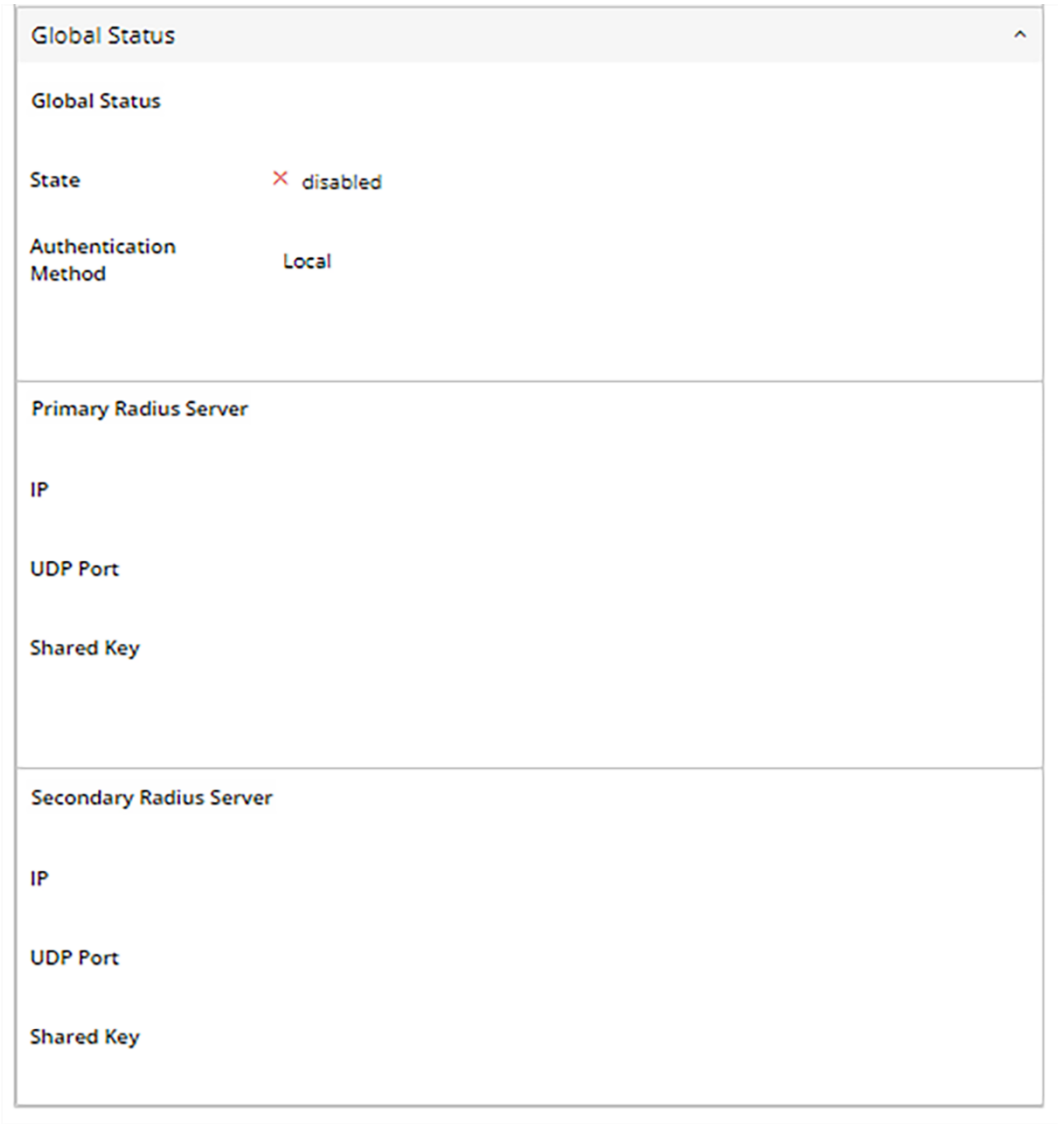
Ilustracja 68: Zakładka „Security“ – menu „802.1X“ – „Global Setup“

Tabela 50: Zakładka „Security“ – menu „802.1X“ – „Global Setup“

Global Setup			
Parametr	**Domyślnie**	**Opis**	
Enable State	☐	☐	Funkcja „802.1X“ jest dla switcha dezaktywowana.
		☑	Funkcja „802.1X“ jest dla switcha aktywowana.
		Wskazówka 	**Uwierzytelnienie IEEE 802.1X** Najpierw należy aktywować w switchu uwierzytelnienie IEEE 802.1X, a dopiero potem można konfigurować tę funkcję dla poszczególnych portów.
Authentication Method	**Local**	W polu wyboru należy wybrać „Lokal“, aby użyć do uwierzytelnienia grupy użytkowników „Guest“ i „User“ bazy danych kont użytkowników switcha. Liczba kont, które mogą równocześnie istnieć obok siebie, jest jednak ograniczona.	
	Radius	W polu wyboru należy wybrać „Radius“, aby aktywować protokół bezpieczeństwa, który w odróżnieniu do wewnętrznej bazy danych użytkowników w urządzeniach z ograniczoną pojemnością pamięci wykorzystuje do uwierzytelnienia użytkowników zewnętrzny serwer. Zasadniczo „Radius“ umożliwia walidację nieograniczonej liczby użytkowników z centralnej lokalizacji.	
Primary Radius Server IP		Jeśli wybrana została metoda uwierzytelnienia „Radius“, do wszystkich żądań uwierzytelnienia zostaje zastosowany podstawowy serwer „Radius“. W polu edycji należy wpisać adres IP zewnętrznego serwera „Radius“, używając zapisu z kropkami.	
UDP Port	**0**	Tu konfigurowany jest VLAN ID.	
Shared Key		W polu edycji należy wpisać hasło (32 znaki alfanumeryczne), które jest stosowane jako wspólny klucz dla połączenia między zewnętrznym serwerem „Radius“ i switchem. Klucz ten nie może być przesłany przez sieć. Klucze na zewnętrznym serwerze „Radius” i switchu muszą być identyczne.	
Secondary RADIUS Server IP		Jest to adres IP rezerwowego serwera RADIUS, wykorzystywanego tylko wtedy, gdy podstawowy serwer RADIUS ulegnie awarii.	

Tabela 50: Zakładka „Security“ – menu „802.1X“ – „Global Setup“

Global Setup		
Parametr	**Domyślnie**	**Opis**
UDP Port	**0**	W polu edycji należy wpisać adres IP zewnętrznego serwera „Radius“, używając zapisu z kropkami.
Shared Key		W polu edycji należy wpisać hasło (32 znaki alfanumeryczne), które jest stosowane jako wspólny klucz dla połączenia między zewnętrznym serwerem „Radius“ i switchem. Klucz ten nie może być przesłany przez sieć. Klucze na zewnętrznym serwerze „Radius” i switchu muszą być identyczne.



Ilustracja 69: Zakładka „Security“ – menu „802.1X“ – „Global Status“

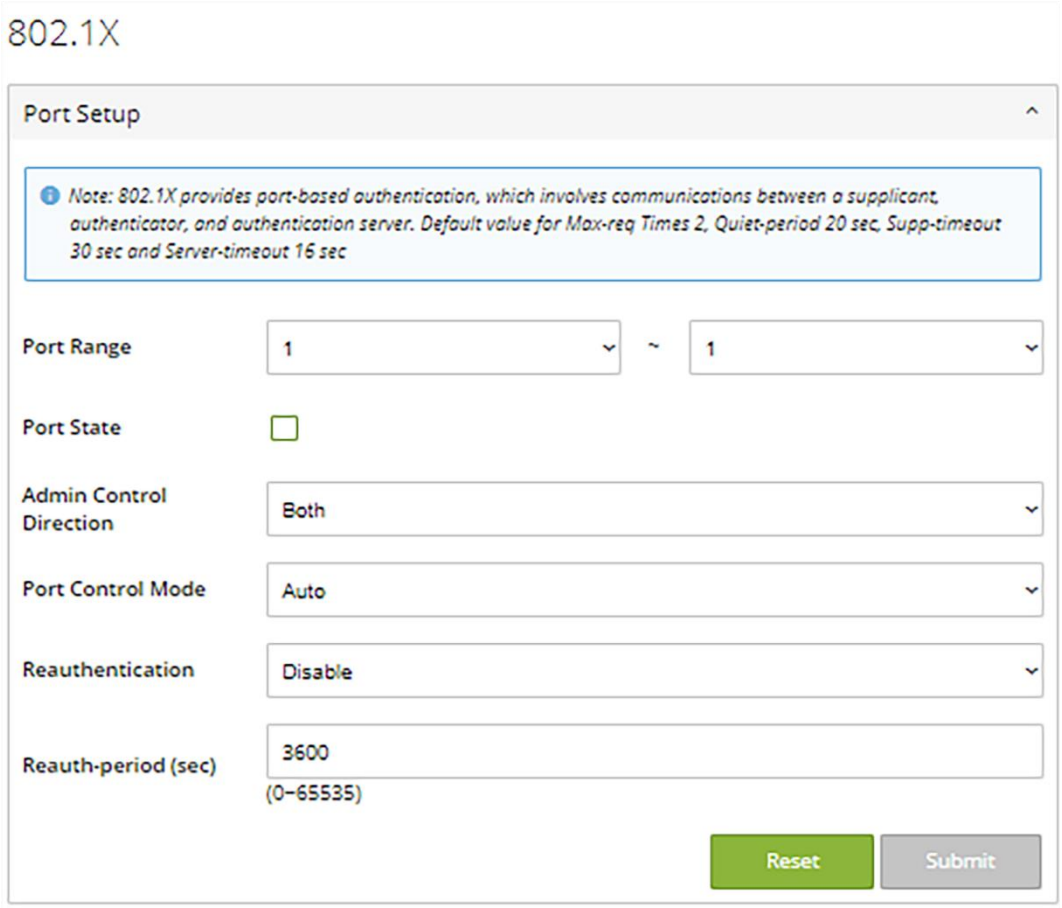
Tabela 51: Zakładka „Security“ – menu „802.1X“ – „Global Status“

Global Status		
Parametr	**Domyślnie**	**Opis**
State	Disable Enable	W tym polu wyświetlana jest informacja, czy uwierzytelnienie IEEE-802.1X jest aktywowane, czy dezaktywowane.
Authentication Method	Local Radius	W tym polu wyświetlana jest metoda uwierzytelniania.
Primary RADIUS Server	IP	W tym polu wyświetlane są adres IP, port dla UDP i wspólne klucze dla podstawowego serwera „Radius“. Pola są puste, jeśli nie wykonano konfiguracji.
	UDP Port	
	Shared Key	
Secondary RADIUS Server	IP	W tym polu wyświetlane są adres IP, port dla UDP i wspólne klucze dla rezerwowego serwera „Radius“. Pola są puste, jeśli nie wykonano konfiguracji.
	UDP Port	
	Shared Key	

9.3.1.3 Port Setup

Wskazówka

Uwierzytelnienie 802.1X
802.1X wykorzystuje uwierzytelnienie na bazie portów, polegające na komunikacji między następującymi uczestnikami: tzw. „Supplicant“, „Authenticator“ i serwer uwierzytelniający.
Obowiązują następujące wartości domyślne: „Max-Req Times” (maks. czas zapytań): 2, „Quiet-Period” (okres bezczynności): 20 s, „Supp-Timeout” (limit czasu żądającego): 30 s oraz „Server-Timeout” (limit czasu serwera): 16 s.



Ilustracja 70: Zakładka „Security“ – menu „802.1X“ – „Port Setup“

Tabela 52: Zakładka „Security“ – menu „802.1X“ – „Port Setup“

Port Setup		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Port Setup“.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Port Setup“.
Port State	☐	☐ Funkcja „802.1X” jest dla switcha dezaktywowana. ☑ Funkcja „802.1X” jest dla switcha aktywowana. **Wskazówka**  **Uwierzytelnienie IEEE 802.1X** Najpierw należy aktywować w switchu uwierzytelnienie IEEE 802.1X, a dopiero potem można konfigurować tę funkcję dla poszczególnych portów.
Admin Control Direction	**Both**	W polu wyboru należy wybrać „Both“, gdy po niepomyślnym uwierzytelnieniu IEEE 802.1X użytkownika zarówno pakiety danych, wchodzące na port, jak i wychodzące, zostają odrzucone.
	In	W polu wyboru należy wybrać „In“, gdy po niepomyślnym uwierzytelnieniu IEEE 802.1X użytkownika tylko pakiety danych, wchodzące na port, zostają odrzucone.
Reauthentication	**Disable**	W polu wyboru należy wybrać „Disable“, gdy w celu utrzymania połączenia z portem uczestnik nie musi regularnie podawać na nowo nazwę użytkownika i hasło.
	Enable	W polu wyboru należy wybrać „Enable“, gdy w celu utrzymania połączenia z portem uczestnik musi regularnie podawać na nowo nazwę użytkownika i hasło.
Port Control Mode	**Auto**	W polu wyboru należy wybrać „Auto“, aby aktywować dla portu uwierzytelnienie.
	Force Authorized	W polu wyboru należy wybrać „Force Authorized“, aby aktywować dla portu stałe uwierzytelnianie.
	Force Unauthorized	W polu wyboru należy wybrać „Force Unauthorized“, aby aktywować dla portu stałą odmowę uwierzytelniania. W efekcie na tym porcie nie mogą być przekazywane pakiety danych.
Reauth-period (sec) (0-65535)	**3600**	W polu edycji należy wybrać wartość interwału czasowego, w którym uczestnik musi podać ponownie nazwę użytkownika i hasło, w celu utrzymania połączenia z portem.

Port Status

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

Ilustracja 71: Zakładka „Security“ – menu „802.1X“ – „Port Status“

Tabela 53: Zakładka „Security“ – menu „802.1X“ – „Port Status“

Port Status		
Parametr	**Domyślnie**	**Opis**
Port	1 **…** 10	W tej kolumnie wyświetlane są numery portów.
IEEE 802.1X State	Disable Enable	W tej kolumnie wyświetlana jest informacja, czy uwierzytelnienie IEEE-802.1X jest dla portu aktywowane, czy dezaktywowane.
Admin Control Direction	Both In	W tej kolumnie wyświetlana jest „Admin Control Direction”.
Port Control Mode	Automatic, Force Authorized, Force Unauthorized	W tej kolumnie wyświetlany jest „Port Control Mode“.
Reauthentication	Disable Enable	W tej kolumnie wyświetlana jest informacja, czy w celu utrzymania połączenia z portem uczestnik musi regularnie podawać na nowo nazwę użytkownika i hasło w celu utrzymania połączenia z portem.
Reauth Period (sec)	0 … 65535	W tej kolumnie wyświetlana jest informacja, w jakich interwałach czasowych uczestnik musi podawać na nowo nazwę użytkownika i hasło w celu utrzymania połączenia z portem.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.3.2 Access Control List (ACL)

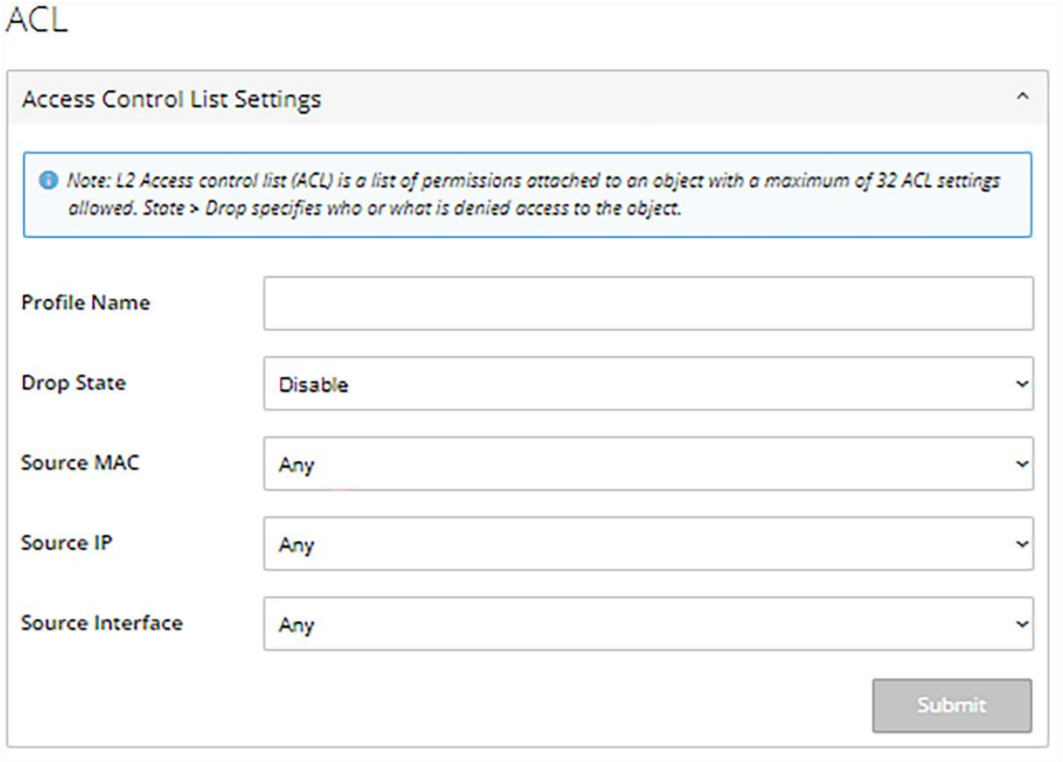
ACL („**A**ccess **C**ontrol List“) jest listą uprawień, przyporządkowanych do obiektu. Zawiera ona specyfikację, kto lub co otrzymuje dostęp do obiektu i jakie operacje mają być wykonywane z obiektem.

Funkcja ACL umożliwia użytkownikom ustalenie kilku reguł dotyczących odsyłania pakietów danych, odbieranych ze specyficznych portów wejściowych lub wszystkich portów. Dzięki tym regułom sprawdzane są źródłowe i docelowe adresy MAC pakietów danych. Jeśli pakiety danych odpowiadają tym regułom, system wykona akcję „deny” (odmowa). Oznacza to, że pakiety danych zostają odrzucone.

„Action Resolution Engine“ zbiera informacje (wyniki akcji i pomiarów) z trafień pod wpisami: jeśli dopasowano więcej niż jedną regułę, wykonywane są pomiary/liczniki z dyrektywy odpowiadającej regule o najwyższym priorytecie.

Wskazówka

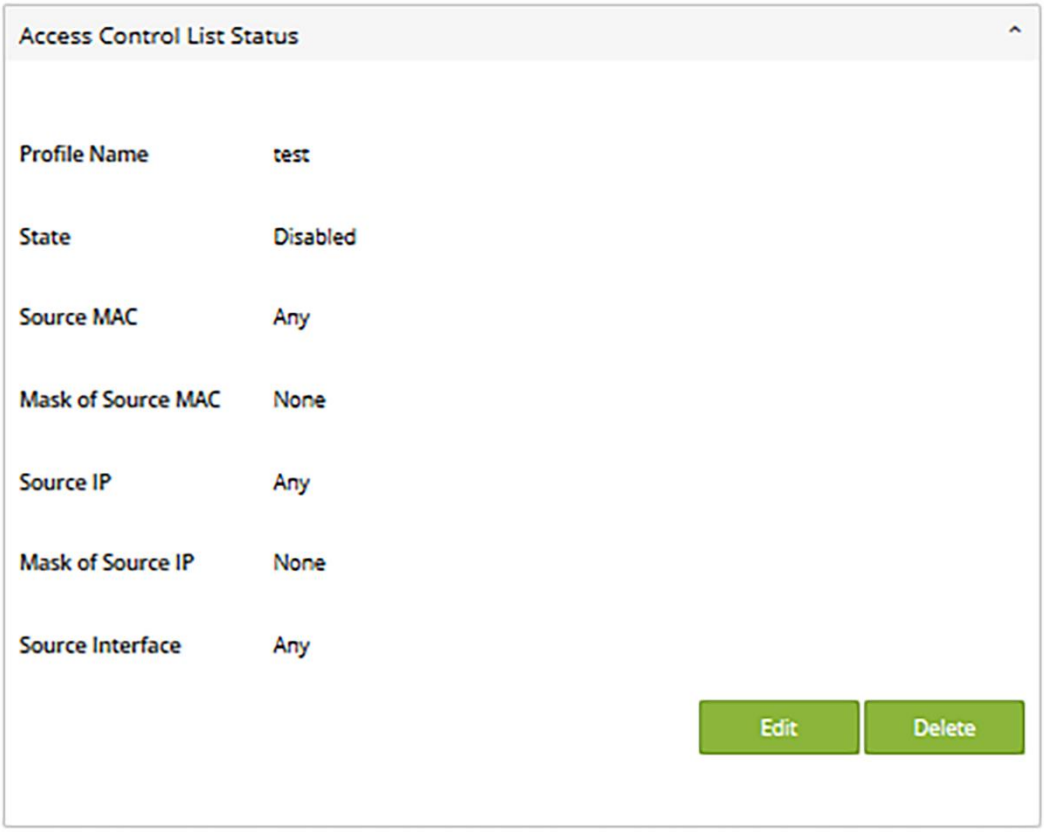
Uprawnienia listy Access Control List (ACL)
„Access Control List” (ACL, lista kontroli dostępu) jest listą uprawień, przyporządkowanych do obiektu, w której dozwolone są maksymalnie 32 ustawienia ACL. Przez „Drop State” (odmowa dostępu) określa się, komu lub czemu odmawia się dostępu do obiektu.



Ilustracja 72: Zakładka „Security” – menu „ACL” – „Access Control List Settings”

Tabela 54: Zakładka „Security” – menu „ACL” – „Access Control List Settings”

Access Control List Settings			
Parametr	**Domyślnie**	**Opis**	
Profile Name		W polu edycji należy wpisać nazwę profilu.	
Drop State	**Disable**	W polu wyboru należy wybrać „Disable“, jeśli pakiety danych nie mają być odrzucane.	
	Enable	W polu wyboru należy wybrać „Enable“, jeśli pakiety danych mają być odrzucane.	
Source MAC	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres MAC był ważny.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać adres MAC źródła do listy Access Control.	
Source IP	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres IP był ważny.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać adres IP źródła do listy Access Control.	
Source Interface	**Any**	W polu wyboru należy wybrać „Any“, gdy każdy fizyczny port jest ważny.	
	Other	1 … 10	W polu edycji należy wpisać fizyczny port, dla którego ten wpis w „Access Control List“ jest ważny.



Ilustracja 73: Zakładka „Security” – menu „ACL” – „Access Control List Status”

Tabela 55: Zakładka „Security” – menu „ACL” – „Access Control List Status”

Access Control List Status		
Parametr	**Domyślnie**	**Opis**
Profile Name		W tym polu wyświetlana jest wybrana nazwa profilu.
Drop State	Disable Enable	W tym polu wyświetlany jest „Drop State”.
Source MAC Address	Any Other	W tym polu wyświetlany jest „Source MAC Address“.
Source IP	Any Other	W tym polu wyświetlany jest źródłowy IP.
Source Interface	Any Other	W tym polu wyświetlany jest źródłowy interfejs.

9.3.3 Port Security

Switch odbiera adres MAC urządzenia, bezpośrednio połączonego z określonym portem, i pozwala na przesłanie danych. Funkcje switcha umożliwiają kontrolować, które urządzenia i w jakiej liczbie mogą łączyć się z portem switcha.

Za pomocą funkcji „Port Security“ można zdefiniować maksymalną liczbę adresów MAC przypadającą na interfejs. W razie przekroczenia tej liczby wchodzące pakiety danych z nowymi adresami MAC zostają odrzucone. Można to kontrolować za pomocą tabeli adresów MAC. Ograniczenie to obejmuje również statyczne adresy MAC.

Wskazówka

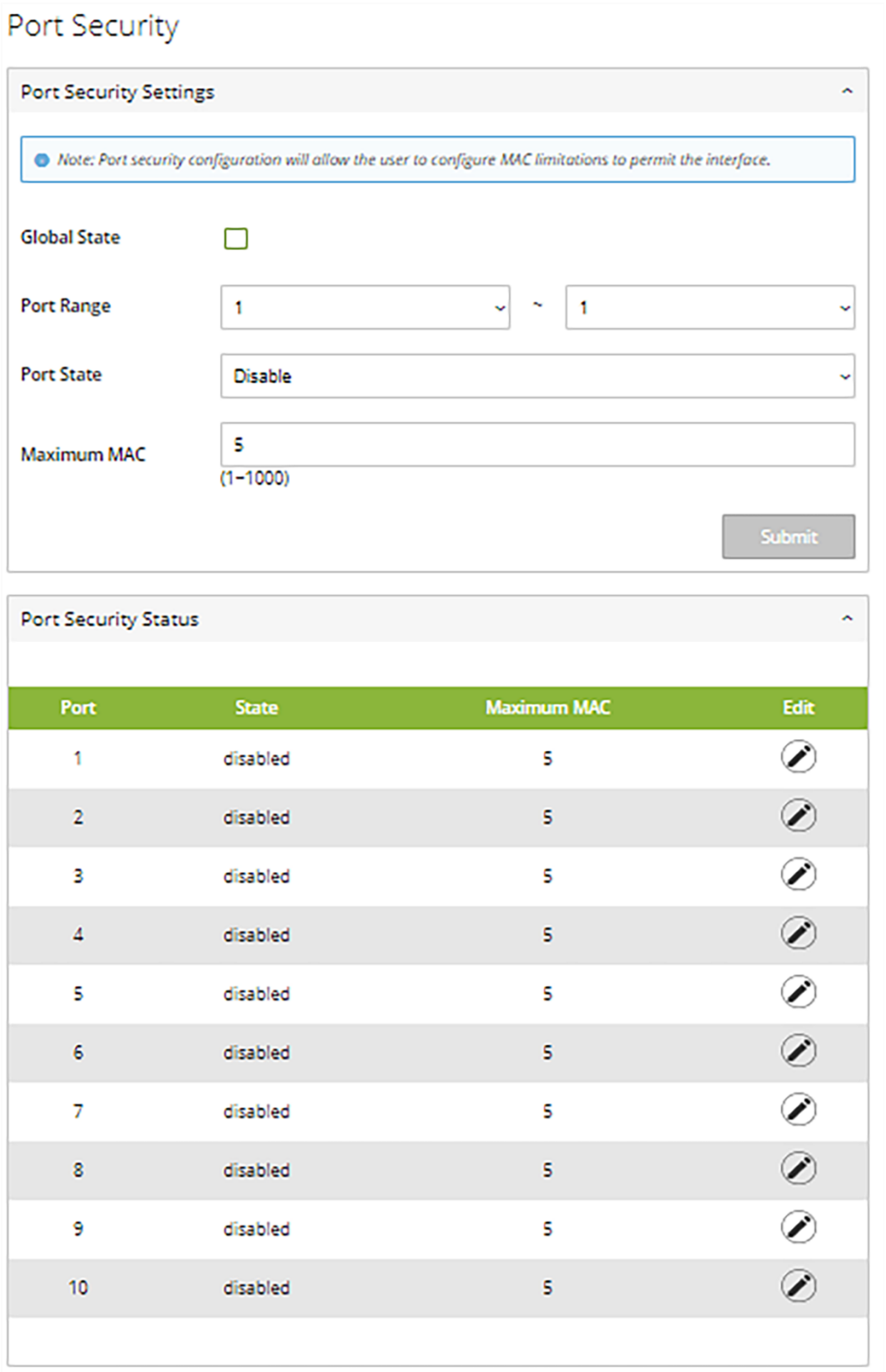


Zmiana stanu portu switcha
Gdy port switcha zmienia stan z dezaktywowanego na aktywowany, wszystkie adresy MAC zarejestrowane przez ten port zostały usunięte.

Wskazówka



Konfiguracja funkcji „Port Security”
W funkcjach „Port Security” można skonfigurować, jaka liczba adresów MAC jest dozwolona na interfejsach.



Ilustracja 74: Zakładka „Security” – menu „Port Security”

Tabela 56: Zakładka „Security” – menu „Port Security”

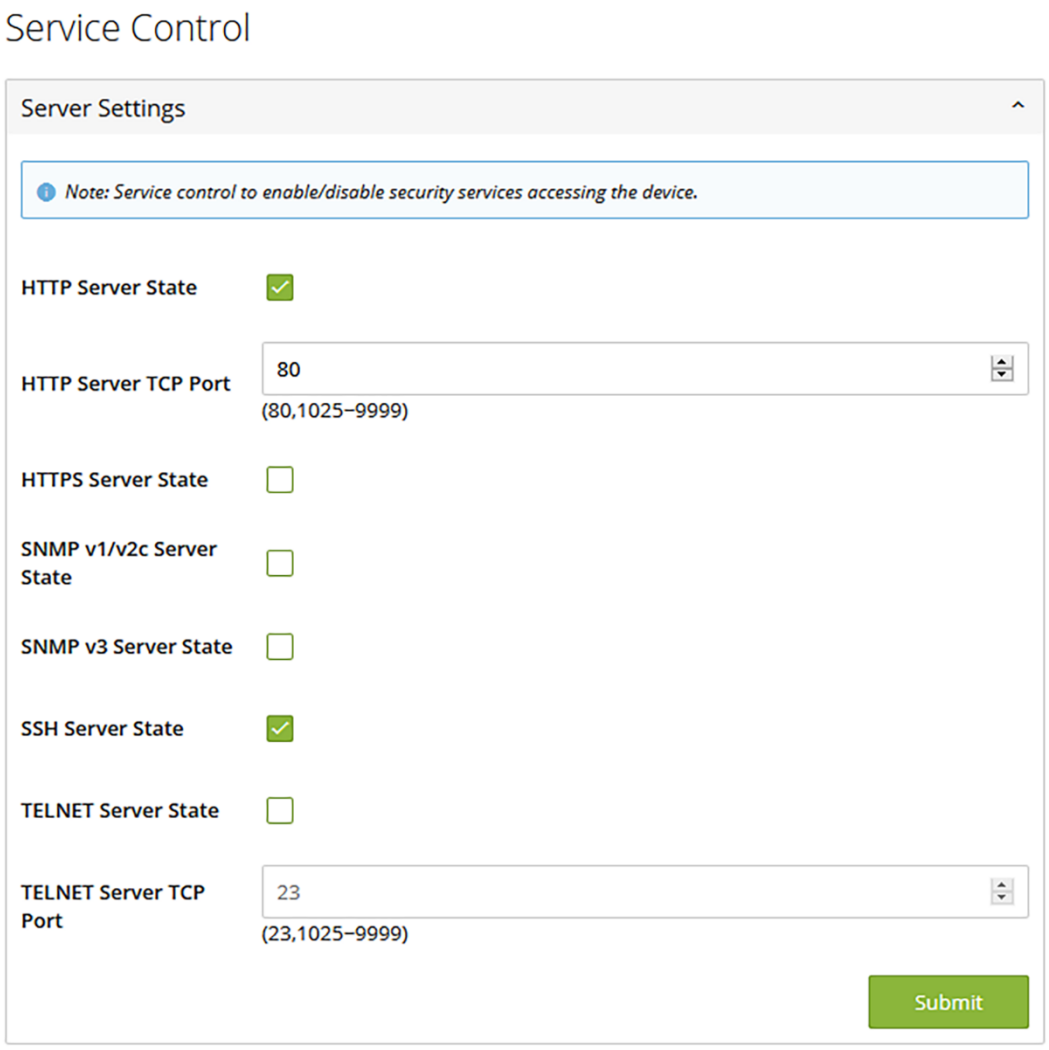
Port Security Settings			
Parametr	**Domyślnie**	**Opis**	
Global State	☐	☐	Funkcja „Port Security” jest dla switcha dezaktywowana.
		☑	Funkcja „Port Security” jest dla switcha aktywowana.
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Port Security”.	
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować funkcję „Port Security”.	
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Port Security“ dla portu lub zakresu portów.	
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Port Security“ dla portu lub zakresu portów.	
Maximum MAC (1–1000)	**5**	W polu edycji należy wpisać maksymalną liczbę adresów MAC na interfejs.	
Port Security Status			
Parametr	**Domyślnie**	**Opis**	
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.	
State	Enable Disable	W tej kolumnie wyświetlana jest informacja, czy „Port Security“ jest aktywowany, czy dezaktywowany.	
Maximum MAC Address	0 … 1000	W tej kolumnie wyświetlana jest maksymalna liczba adresów MAC.	
Edit		W tej kolumnie można aktywować funkcję edycji.	

9.3.4 Service Control

W „Service Control” można skonfigurować usługi bezpieczeństwa, które mają dostęp do urządzenia, takie jak HTTP, HTTPS, SNMP v1/v2c, SNMP v3 czy SSH.

Wskazówka

Funkcja „Service Control”
W „Service Control” aktywuje się lub deaktywuje usługi, które mają dostęp do urządzenia.



Ilustracja 75: Zakładka „Security” – menu „Service Control”

Tabela 57: Zakładka „Security” – menu „Service Control”

Server Settings		
Parametr	**Domyślnie**	**Opis**
HTTP Server State	☑	Aktywuje / dezaktywuje „HTTP Server”.
HTTP Server TCP Port (80, 1025–9999)	**80** 1025 … 9999	W polu edycji należy wpisać „HTTP Server TCP Port“.
HTTPS Server State	☐	Aktywuje / dezaktywuje „HTTPS Server”.
SNMP v1/v2c Server State	☐	Aktywuje / dezaktywuje „SNMP v1/v2c Server”.
SNMP v3 Server State	☐	Aktywuje / dezaktywuje „SNMP v3 Server”.
SSH Server State	☑	Aktywuje / dezaktywuje „SSH Server”.
Telnet Server State	☐	Aktywuje / dezaktywuje „Telnet Server”.
Telnet Server TCP Port (23, 1025~9999)	**23** 1025 … 9999	W polu edycji należy wpisać port TCP dla serwera Telnet.
Server Status		
Parametr	**Domyślnie**	**Opis**
HTTP Server State	Enable Disable	W tym polu wyświetlany jest status serwera HTTP.
HTTP Server TCP Port	80 1025 … 9999	W tym polu wyświetlany jest status „HTTP Server TCP Port“.
HTTP Server State	Enable Disable	W tym polu wyświetlany jest status serwera HTTPS.
SNMP v1/v2c Server State	Enable Disable	W tym polu wyświetlany jest status serwera SNMP v1/v2c.
SNMP v3 Server State	Enable Disable	W tym polu wyświetlany jest status serwera SNMP v3.
SSH Server State	Enable Disable	W tym polu wyświetlany jest status serwera SSH.
Telnet Server Status	Enable Disable	W tym polu wyświetlany jest status serwera Telnet.
Telnet Server TCP Port	23 1025 … 9999	Tu wyświetlany jest status „Telnet Server TCP Port“.

9.3.5 VLAN

9.3.5.1 Port Isolation

„Port Isolation“ to wirtualna funkcja LAN, bazująca na portach. Dzieli ona pośredniczące porty na indywidualne, prywatne domeny, które można osobno przydzielać. Przełączanie danych poza prywatną domeną switcha jest niedozwolone. Informacje ze znaczników VLAN pakietów danych są ignorowane.

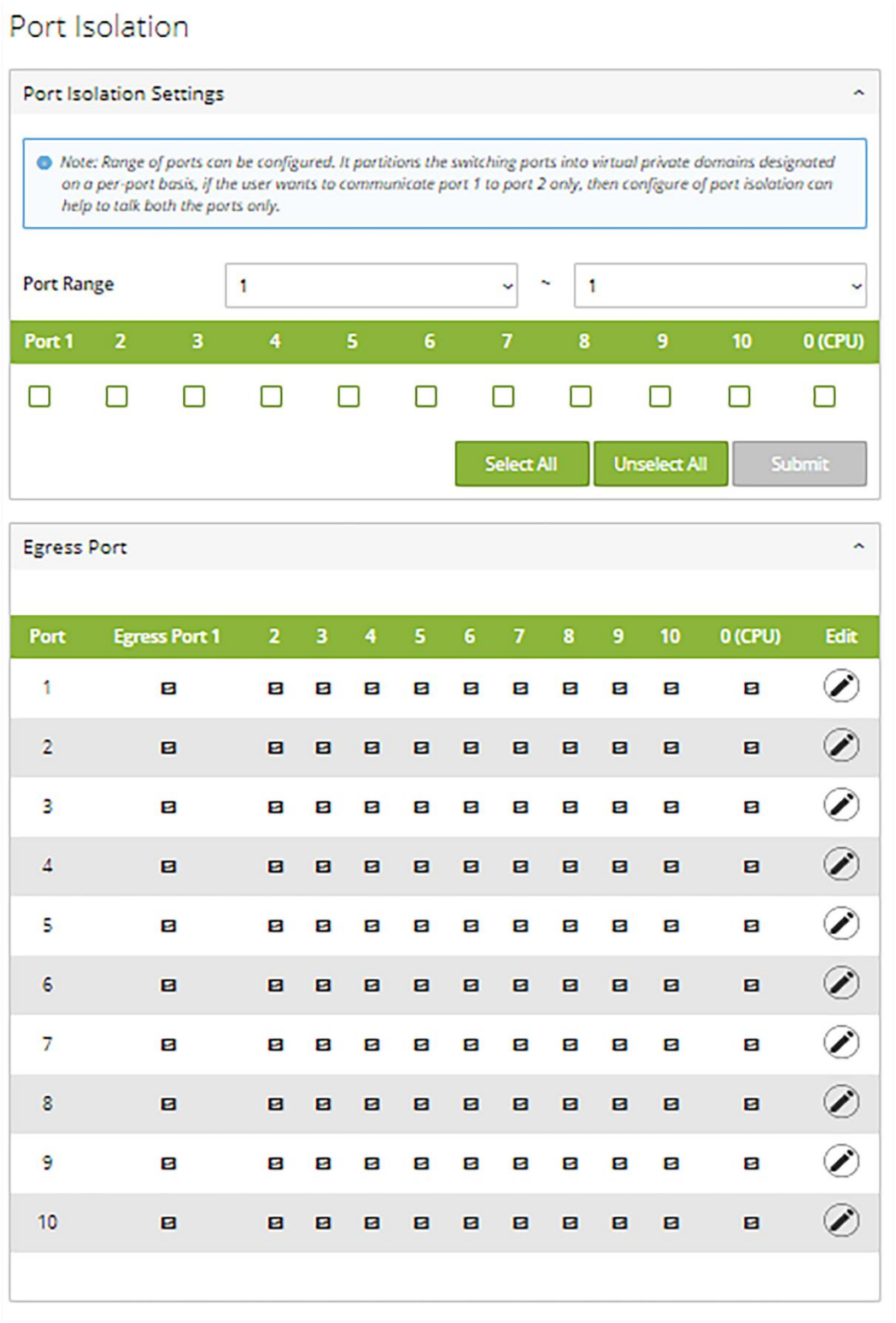
Za pomocą tej funkcji można dla każdego portu konfigurować jeden lub kilka portów wyjściowych, aby odebrane przez niego dane przesyłać do tego specyficznego portu. Gdy port CPU (port 0) nie jest portem wyjściowym dla specyficznego portu, host połączony ze specyficznym portem nie może zarządzać switchem.

Aby zezwolić na komunikację między dwoma portami uczestnika, należy zdefiniować port wyjściowy dla obu portów. CPU oznacza port zarządzający switcha. Standardowo tworzy on VLAN ze wszystkimi portami ETHERNET. Gdy nie tworzy VLAN ze specyficznym portem, switch nie może być zarządzany przez ten port.

Wskazówka



Konfiguracja portów
Można skonfigurować zakresy portów. W tym procesie pośredniczące porty zostają podzielone na indywidualne, prywatne domeny, które można osobno przydzielać. Jeżeli np. komunikacja ma się odbywać tylko między portem 1 a portem 2, izolację portów można skonfigurować w ten sam sposób.



Ilustracja 76: Zakładka „Security“ – menu „VLAN“ – „Port Isolation“

Tabela 58: Zakładka „Security“ – menu „VLAN“ – „Port Isolation“

Port Isolation Settings				
Parametr		**Domyślnie**	**Opis**	
Port Range		**1** … 10 0 (CPU)	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Port Isolation”.	
		1 … 10 0 (CPU)	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Port Isolation”.	
Egress Port			„Egress Port” to port wyjściowy, przez który wysyłany jest pakiet danych. Wyznaczenie któregoś portu jako „Egress Port“ oznacza, że będzie się on komunikował z aktualnie konfigurowanym portem.	
	Select All	☐	☐	Żaden „Egres Port“ nie jest wybrany.
			☑	Wszystkie „Egress Port“ są wybrane.
	Disable All	☐	☐	Żaden „Egres Port“ nie jest dezaktywowany.
			☑	Wszystkie „Egress Port“ są dezaktywowane.
	☐ 0 (CPU) … ☐ 10	☐	☐	„Egress Port” nie jest aktywowany.
			☑	„Egress Port” jest aktywowany.

Port Isolation Status			
Parametr	**Domyślnie**	**Opis**	
Port	**V**	V	„V“ oznacza, że pakiety portu mogą być do niego wysyłane.
Egress Port		-	„-“ oznacza, że pakiety portu nie mogą być do niego wysyłane.
Edit		W tej kolumnie można aktywować funkcję edycji.	

9.3.5.2 VLAN Setup

VLAN („**V**irtuelles **LAN**“) jest grupą hostów o jednolitych wymaganiach, które niezależnie od ich fizycznej lokalizacji komunikują się w taki sposób, jakby należały do jednej domeny broadcast. VLAN ma takie same atrybuty jak fizyczny LAN, ale umożliwia grupowanie stacji końcowych, nawet gdy nie znajdują się w tej samej sieci switcha. Nową konfigurację sieci można przeprowadzić w oprogramowaniu, zamiast w rozproszonych fizycznie urządzeniach.

VID („**V**LAN **ID**“) jest oznaczeniem sieci VLAN, stosowanym w standardzie IEEE 802.1Q. Składa się ono z 12 bitów i umożliwia oznaczenie 4096 (2^12) sieci VLAN. Z 4096 możliwych VID wartość VID 0 stosowana jest do oznaczenia „Priority Frames“, a wartość 4095 (FFF) jest zarezerwowana, tak więc możliwych jest maksymalnie 4094 konfiguracji VLAN. Jednak switch zarządzalny Lean ma maks. 5 VLAN do dyspozycji.

„Tagged VLAN“ wykorzystuje jednoznaczny znacznik (VLAN ID) w nagłówku MAC, aby jednoznacznie zidentyfikować przynależność ramki do VLAN, niezależnie od „Bridges“, wszystko jedno na którym switchu znacznik został wygenerowany. VLAN może być utworzony statycznie (ręcznie przez użytkownika) lub dynamicznie przez GVRP („GARP VLAN Registration Protocol“). VLAN ID przyporządkowuje ramkę do określonego VLAN i dostarcza informacje, potrzebne switchom do przetworzenia ramki wewnątrz sieci. Ramka z tagiem jest o cztery bajty dłuższa niż ramka bez tagu i zawiera dwa bajty dla TPID („Tag Protocol Identifier”, znajdującego się w polu typ/długość „ETHERNET Frames“) oraz dwa bajty dla TCI („Tag Control Information”, która zaczyna się po polu adresu źródłowego „ETHERNET Frames“).

CFI („Canonical Format Indicator“) jest 1-bitowym polem danych, którego wartość dla switcha ETHERNET zawsze wynosi 0. Jeśli ramka odebrana przez port ETHERNET ma wartość CFI wynoszącą 1, ramka nie powinna być wystawiona na port bez znacznika. Pozostałe 12 bitów definiują VLAN ID, co daje maksymalnie 4096 sieci VLAN. Należy pamiętać, że priorytet użytkownika i VLAN ID są niezależne od siebie. Ramka z VID (VLAN Identifier) o wartości null (0) określana jest jako „Priority Frame“, tzn. że istotny jest tylko poziom priorytetu, a domyślny VID portu wejściowego jako VID ramki zostaje odrzucony. Z 4096 możliwych VID wartość VID 0 stosowane jest do identyfikacji „Priority Frames“, a wartość 4095 (FFF) jest zarezerwowana, tak więc możliwych jest maksymalnie 4094 konfiguracji VLAN.

TPID	Priorytet użytkownika	CFI	VLAN ID
2 B	3 b	1 b	12 b

- **Przekierowane ramki ze znacznikiem i bez znacznika**

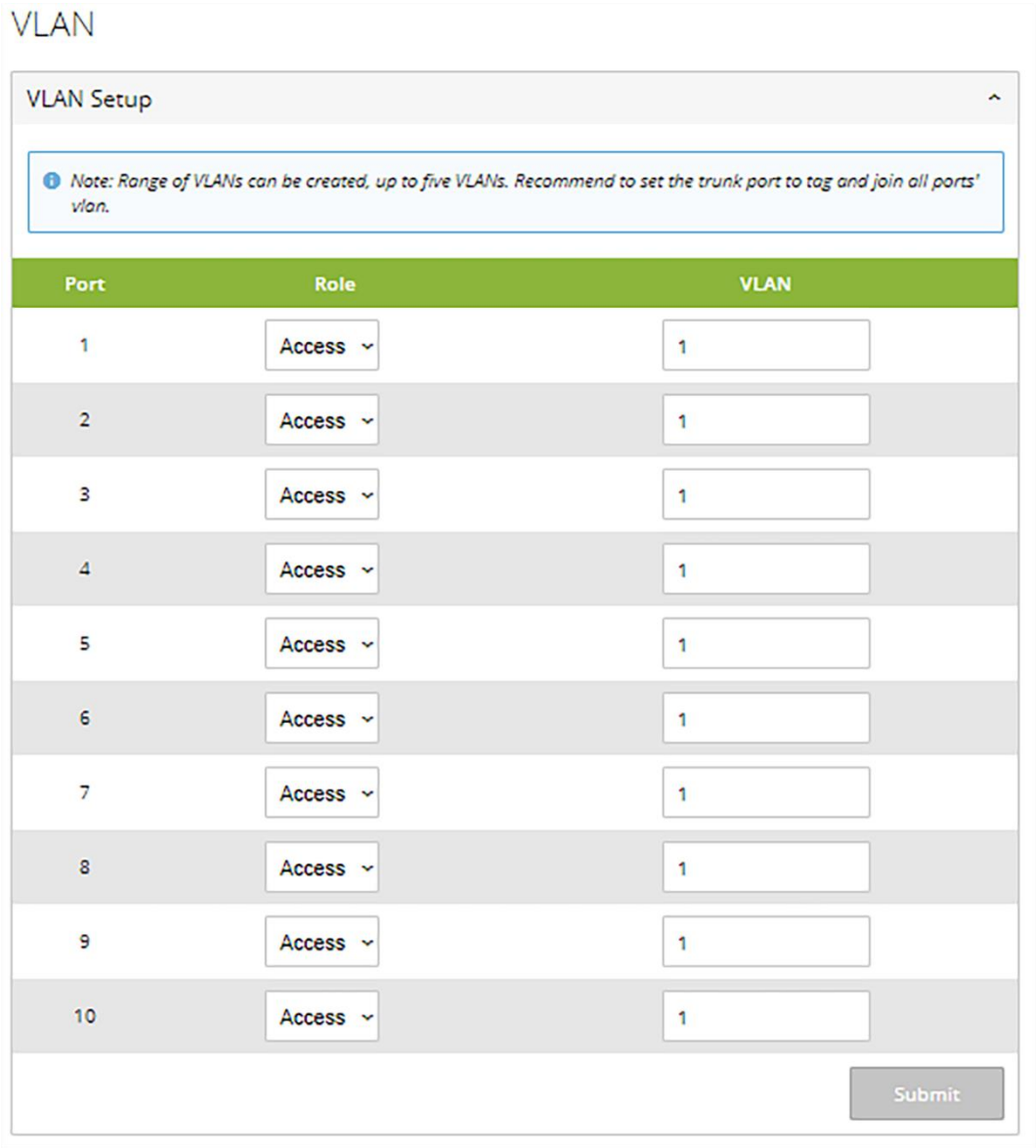
Każdy port switcha może przesyłać ramki ze znacznikiem i bez znacznika. Podczas przekierowania ramki przez switch wspierający VLAN 802.1Q do switcha bez tego wsparcia, switch musi najpierw zdecydować, dokąd wysyła ramkę i potem usunąć znacznik VLAN. W przeciwnym razie switch musi najpierw zdecydować, dokąd wysyła ramkę i następnie dodać znacznik VLAN, odpowiadający domyślnemu ID portu wejściowego. Domyślnym PVID dla wszystkich portów jest „VLAN 1“, co jednak można zmienić.

Ramka broadcast (lub multicast dla grupy multicast, znanej systemowi) dublowana jest tylko dla portów, będących uczestnikami VID (poza samym portem wejściowym) i tym samym zostaje ograniczona do specyficznej domeny.

Wskazówka

Konfiguracja VLAN

Można skonfigurować do 5 VLAN. Zalecane jest skonfigurowanie portu trunk z tagiem i dołączenie wszystkich portów do VLAN.



Ilustracja 77: Zakładka „Security“ – menu „VLAN“ – „VLAN Setup“

Tabela 59: Zakładka „Security“ – menu „VLAN“ – „VLAN Setup“

VLAN Setup		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlane są numery portów.
Role	**Access**	W polu wyboru należy wybrać „Access“, aby wybrać tę rolę dla specyficznego portu.
	Trunk	W polu wyboru należy wybrać „Trunk“, aby wybrać tę rolę dla specyficznego portu.
VLAN		W polu edycji należy wpisać „VLAN ID“ dla tego wpisu. Właściwy zakres: 1 … 4094
Tag	☐	☐ Port nie jest aktywowany.
		☑ Port jest aktywowany.

Wskazówka

Zawsze jeden port w Management VLAN

W Management VLAN musi zawsze być co najmniej jeden port.
W przeciwnym razie nie można skonfigurować switcha.
Ewentualnie może być konieczne zresetowanie switcha do ustawień fabrycznych. Wtedy konfiguracje zostaną utracone.

9.4 Redundancy

9.4.1 ERPS

Funkcja ERPS („**E**THERNET **R**ing **P**rotection **S**witching“) implementuje mechanizm łączeniowy dla topologii pierścienia w warstwie ETHERNET, zgodnie ze standardem ITU-T G.8032. Protokół ERP („**E**THERNET **R**ing **P**rotection“) chroni przy tym ruch danych ETHERNET w topologii pierścienia i zapewnia równocześnie, że w warstwie ETHERNET wewnątrz pierścienia nie mogą powstawać pętle. Tworzeniu pętli zapobiega blokada ruchu danych we wcześniej zdefiniowanym lub uszkodzonym linku.

Ochrona pierścieni ETHERNET zawiera następujące funkcje:

- Zapobieganie tworzeniu się pętli
- Zastosowanie mechanizmów rozpoznawania, przekierowania i bazy danych filtrowana (FDB)

Aby zapobiec powstawaniu pętli, należy zagwarantować, żeby ruch danych był zawsze prowadzony przez wszystkie linki pierścienia – poza jednym. Ten specjalny link pierścienia służy jako połączenie rezerwowe i określany jest jako RPL („**R**ing **P**rotection **L**ink“). Przy normalnej pracy jest on blokowany i nie jest wykorzystywany dla ruchu danych. Za blokowanie ruchu danych na końcu RPL odpowiedzialny jest specyficzny węzeł pierścienia ETHERNET „RPL Owner“. Gdy w pierścieniu ETHERNET dochodzi do awarii, węzeł „RPL Owner“ znosi blokadę na swoim końcu RPL, o ile RPL nie ma awarii, i otwiera drogę dla ruchu danych przez RPL. Także sąsiedni węzeł RPL pierścienia ETHERNET, zwany „RPL Neighbour“, może zablokować lub odblokować ruchu danych na swoim końcu RPL.

Pierścienie ETHERNET mogą wspierać sieć, składającą się z pierścieni ETHERNET, połączonych ze sobą przez jeden punkt lub kilka punktów. Protokół zdefiniowany w tym zaleceniu i mechanizmy ochrony połączeń mogą być zastosowane w sieci złożonej z pierścieni/łańcuchów w następujących warunkach:

- W połączeniach pierścieni ETHERNET nie są wspólnie użytkowane kanały R-APS.
- „ERP Control Process“ steruje w tylko jednym pierścieniu ETHERNET wszystkimi kanałami komunikacyjnymi i wszystkimi kanałami R-APS (np. blokowanie lub przepuszczanie) na wszystkich portach pierścienia.
- Każdy pierścień główny i podpierścień dysponują własnym RPL.

W nieprzeciążonym pierścieniu ETHERNET, w którym znajdują się wszystkie węzły pierścienia ETHERNET bez obciążenia (tzn. nie ma wykrytych awarii, aktywnych automatycznych lub zewnętrznych poleceń i odbierane są tylko wiadomości R-APS (NR, RB)), w którym długość światłowodu jest mniejsza niż 1200 km i który ma mniej niż 16 węzłów ETHERNET, czas przełączania (czas transferu, jak definiuje to ITU-T G.808.1) w przypadku awarii linku pierścienia nie powinien przekraczać 800 ms.

Architektura ochrony pierścienia bazuje na protokole APS do koordynacji funkcji ochrony pierścienia ETHERNET.

Switch wspiera maksymalnie dwa pierścienie.

Guard Timer

Wszystkie urządzenia w pierścieniu wykorzystują „Guard Timer“. Zapobiega on tworzeniu się zamkniętych pętli i wykorzystywaniu przez urządzenia przestarzałych komunikatów R-APS. „Guard Timer“ aktywowany jest, gdy urządzenia w pierścieniu odbierają informacje o lokalnym żądaniu przełączenia, jak chociażby po poleceniach SF („**S**witch **F**ail“), MS („**M**anual **S**witch“) czy FS („**F**orced **S**witch“). Po upływie czasu urządzenie w pierścieniu rozpoczyna wykonywanie działań, które odbiera od R-APS. Timera nie można zatrzymać.

WTR Timer

„WTR Timer“ („**W**ait **T**o **R**estore **Timer**“) wykorzystywany jest przez „RPL Owner“. „WTR Timer“ przechodzi w tryb rewertywny, aby zapobiec powtarzającemu się wyzwalaniu połączenia ochronnego przez fluktuację portów lub periodyczne błędy zaniku sygnału. Po upływie czasu „RPL Owner“ wysyła przez pierścień wiadomości R-APS (NR, RB).

WTB Timer

„WTB Timer“ („**W**ait **T**o **B**lock **Timer**“) aktywowany jest w „RPL Owner“. „RPL Owner“ wykorzystuje „WTB Timer“, zanim zainicjuje blokadę RPL, i wraca do stanu bez obciążenia, gdy użytkownik wpisał polecenia dla stanu FS lub MS. Ponieważ w pierścieniu może być aktywnych kilka poleceń FS równocześnie, „WTB Timer“ zapewnia, że usunięcie pojedynczego polecenia FS nie skutkuje od razu ponownym zablokowaniem RPL. „WTB Timer“ powinien działać 5 sekund dużej niż „Guard Timer“, aby urządzenie nadawcze miało wystarczająco dużo czasu na wysłanie dwóch wiadomości R-APS i aby pierścień mógł wykryć stan latencji. Przez kasowanie polecenia MS „WTB Timer“ zapobiega powstawaniu zamkniętej pętli, gdyż węzeł „RPL Owner“ podczas procesu przywracania nie reaguje na przedawnione rozproszone żądania MS.

Hold-off Timer

Każde urządzenie w pierścieniu wykorzystuje „Hold-off Timer“ do opóźnienia komunikatu o awarii portu. Po upływie czasu urządzenie w pierścieniu sprawdza status portu. Jeśli problem nadal istnieje, wysyłany jest komunikat. Jeśli problemu nie ma, komunikat nie jest wysyłany.

ERPS z trybem rewersji i bez

ERPS wykorzystuje tryby rewersji i nie-rewersji („revertive and non-revertive operation“). Jeśli w trybie rewersji warunki, wyzwalające przełączenie, już nie występują, funkcjonujący kanał transmisji zostaje ponownie utworzony, tzn. zablokowany na RPL. Po usunięciu stanu błędu kanał komunikacyjny zostaje przywrócony dopiero po upływie „WTR Timer“, aby zapobiec przełączaniu w tę

i we w tę stanów ochronnych w przypadku periodycznie występujących błędów. Bez trybu rewersji kanał komunikacyjny będzie po usunięciu warunków przełączania nadal wykorzystywał RPL, o ile RPL nie ma awarii.

Control VLAN

„Control VLAN" (VLAN sterowania) jest domeną, w której transmitowane są wyłącznie pakiety sterujące ERPS. Ponieważ w tej sieci VLAN nie są transmitowane inne pakiety danych, przy ERPS nie dochodzi do żadnej zwłoki. Dlatego przy konfiguracji Control VLAN dla pierścienia należy pamiętać, że jest nowa sieć VLAN. ERPS automatycznie tworzy Control VLAN i jej porty uczestników. Port uczestnika może mieć port lewy i port prawy.

W ERPS rozdzielane są pakiety do różnych sieci VLAN.
Pakiety sterowania transmitowane są w Control VLAN.

Instancja

W ERPS wersja 2 instancja jest profilem, specyfikującym jedną lub kilka sieci danych VLAN dla ERPS. I tak pakiety sterowania i danych są w ERPS rozdzielane do różnych sieci VLAN. Pakiety sterowania transmitowane są w control VLAN, a pakiety danych w jednej lub kilku Data VLAN. W ten sposób użytkownik może łatwo przydzielić instancję pierścieniowi ERPS.

Gdy w ERPS wersja 1 port blokowany jest przez ERPS, blokowane są wszystkie pakiety danych.

Gdy w ERPS wersja 2 port blokowany jest przez pierścień ERPS, blokowane są tylko pakiety danych należące do sieci VLAN, w tej instancji.

Wskazówka

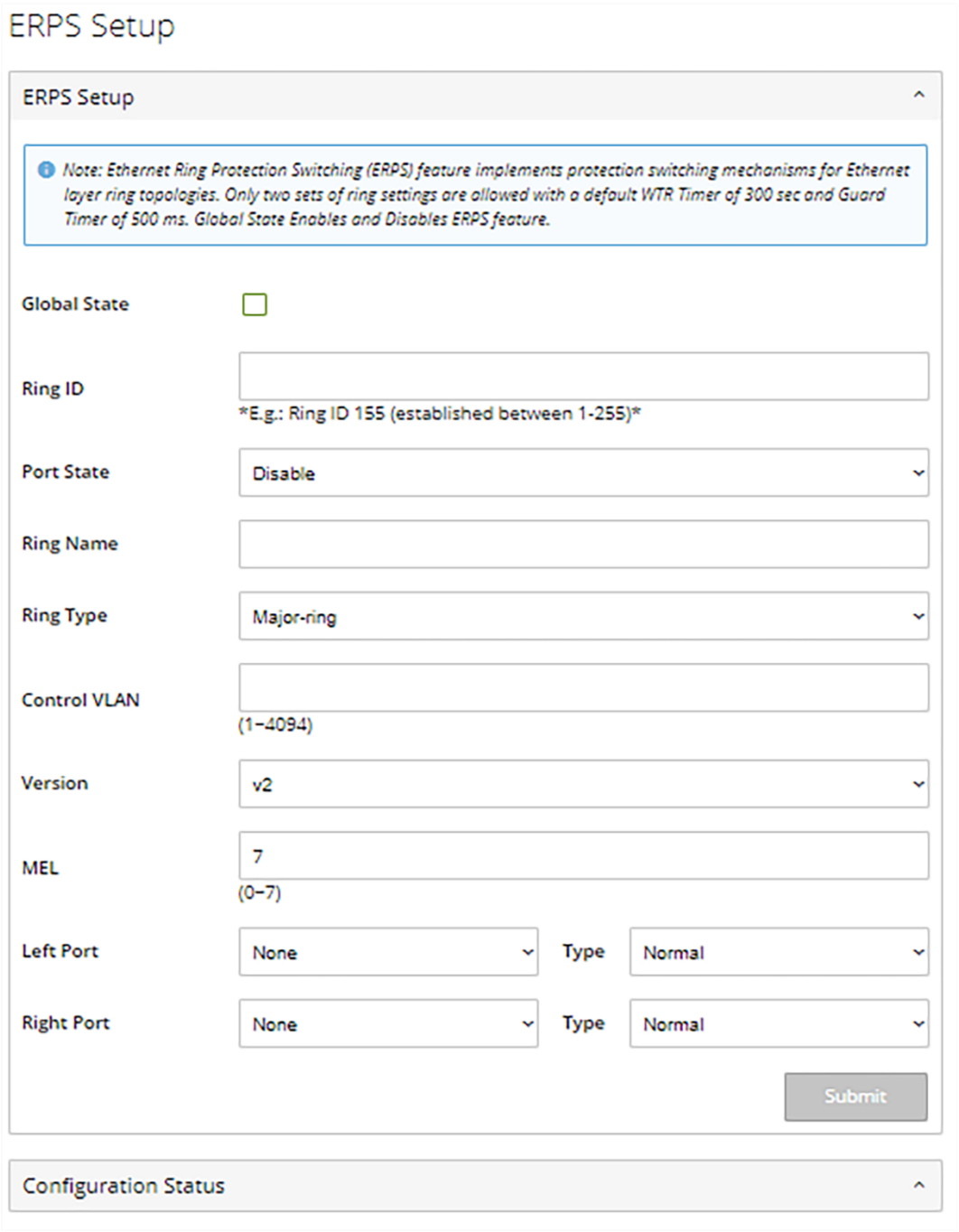


Control VLAN i instancja
W konfiguracjach CLI lub web istnieją ustawienia dla Control VLAN i dla instancji.
Jeśli Control VLAN została skonfigurowana dla pierścienia i powinna być skonfigurowana instancja dla tego pierścienia, Control VLAN dla instancji musi być ta sama jak dla pierścienia. W przeciwnym razie zgłaszany jest błąd. Aby móc mimo to zastosować tę instancję, można najpierw założyć Control VLAN tak, aby była taka sama jak dla instancji. Teraz można skonfigurować instancję.

Wskazówka



Funkcja Ethernet Ring Protection Switching (ERPS)
Funkcja „Ethernet Ring Protection Switching" (ERPS) implementuje mechanizm łączeniowy dla topologii pierścienia w warstwie Ethernet. Dozwolone są tylko dwa ustawienia pierścienia z domyślnym „WTR Timer" wynoszącym 300 s i „Guard Timer" wynoszącym 500 ms.
Global State aktywuje i dezaktywuje funkcję ERPS (maks. 2 pierścienie na switch, maks. 16 switchy na pierścień, czas przełączenia < 800 ms). Za pomocą ustawienia „Global State" funkcję ERPS można aktywować lub dezaktywować.



Ilustracja 78: Zakładka „Redundancy“ – menu „ERPS“

Tabela 60: Zakładka „Redundancy“ – menu „ERPS“

ERPS Setup		
Parametr	**Domyślnie**	**Opis**
Global State	☑	☐ Funkcja „ERPS“ jest dla switcha dezaktywowana. ☑ Funkcja „ERPS“ jest dla switcha aktywowana.
Ring ID (*E.g.: Ring ID 155 (established between 1-255))		W polu edycji należy wpisać „Ring ID“. Właściwy zakres: 1 … 255 Ale switch zarządzalny Lean wspiera 2 pierścienie.
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować stan pierścienia.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować stan pierścienia.
Ring Name		W polu edycji należy wpisać nazwę pierścienia (maks. 32 znaki). (np. Major Ring ID255)
Ring Type	**Major-Ring**	W polu wyboru należy wybrać „Major Ring“, gdy switch ma pracować w „Major Ring“.
	Subring	W polu wyboru należy wybrać „Subring“, gdy switch ma pracować w „Subring“.
Control VLAN (1-4094)	1 … 4094	W polu edycji należy wpisać VLAN ID, który ma służyć jako domena dla pakietów sterowania ERPS. Właściwy zakres: 1 … 4094
Version	**v2**	W polu wyboru należy wybrać „v2“, gdy ma być wykorzystana wersja 2 funkcji „ERPS“.
	v1	W polu wyboru należy wybrać „v1“, gdy ma być wykorzystana wersja 1 funkcji „ERPS“.
MEL (0~7)	**7**	W polu edycji należy wpisać wartość „Control MEL“ (**M**aintenance **E**ntity Group **L**evel) dla pierścienia. MEL określa priorytet. 0 = najniższy priorytet 7 = najwyższy priorytet
Left Port		W tym polu wyboru konfigurowany jest lewy port i jego typ dla pierścienia.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10	W polu wyboru należy wybrać odpowiedni port.
	Normal	W polu wyboru należy wybrać „Normal“, gdy dla portu nie została przydzielona specjalna funkcja w pierścieniu ERPS.
	Neighbor	W polu wyboru należy wybrać „Neightbor“, gdy sąsiedni port pełni funkcję „Neightbor“.
	Owner	W polu wyboru należy wybrać „Owner“, gdy port ma przejąć funkcję „Owner“ w pierścieniu ERPS.

Tabela 60: Zakładka „Redundancy“ – menu „ERPS“

ERPS Setup		
Parametr	**Domyślnie**	**Opis**
Right Port		W polu wyboru należy wybrać „v2“, gdy ma być wykorzystana wersja 2 funkcji „ERPS“.
	None	W polu wyboru należy wybrać „v1“, gdy ma być wykorzystana wersja 1 funkcji „ERPS“.
	1 … 10	W polu edycji należy wpisać wartość „Control MEL“ (**M**aintenance **E**ntity Group **L**evel) dla pierścienia. MEL określa priorytet. 0 = najniższy priorytet 7 = najwyższy priorytet
	Normal	W tym polu wyboru konfigurowany jest lewy port i jego typ dla pierścienia.
	Neighbor	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	Owner	W polu wyboru należy wybrać odpowiedni port.
ERPS Ring Status		
Parametr	**Domyślnie**	**Opis**
Ring ID	1 … 255	W tym polu wyświetlany jest „Ring ID“.
Port State	Disable Enable	W tym polu wyświetlany jest status pierścienia.
Ring Name		W tym polu wyświetlana jest nazwa pierścienia.
Ring Type	Major Ring Subring	W tym polu wyświetlany jest typ pierścienia.
Control VLAN	1 … 4084	W tym polu wyświetlana jest „Control VLAN“.
Version	v2 v1	W tym polu wyświetlana jest wersja funkcji „ERPS“.
MEL	0 … 7	W tym polu wyświetlana jest wartość dla „Control MEL.
Left Port	None 1 … 10 (12)	W tym polu wyświetlany jest numer lewego portu.
Right Port	None 1 … 10 (12)	W tym polu wyświetlany jest numer prawego portu.
Left Port Type	Normal Neighbor Owner	W tym polu wyświetlany jest typ lewego portu.
Right Port Type	Normal Neighbor Owner	W tym polu wyświetlany jest typ prawego portu.
Left Port Status	Forwarding Blocking	W tym polu wyświetlany jest aktualny status lewego portu.
Right Port Status	Forwarding Blocking	W tym polu wyświetlany jest aktualny status prawego portu.
Ring Status	Protection Idle	W tym polu wyświetlany jest status pierścienia.
Delete		Aby usunąć te ustawienia, należy kliknąć **[Clear]**.

9.4.2 STP/RSTP

(R)STP („(**R**apid) **S**panning **T**ree **P**rotocol)“) może wykryć pętle sieci i przerwać połączenia zapasowe („Backup Links“) między switchami, bridge'ami lub ruterami. Funkcja ta umożliwia switchowi interakcję w sieci z innymi switchami obsługującymi (R)STP, w celu zapewnienia , aby między dwoma danymi stacjami w sieci istniało tylko jedno połączenie.

Switch wspiera zarówno STP, jak i RSTP, zdefiniowane w wymienionych niżej standardach:

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

Switch wykorzystuje IEEE 802.1w RSTP, które umożliwia szybszą konwergencję „Spanning Tree“ (drzewa rozpinającego) niż STP (switch jest też kompatybilny wstecznie tylko z bridge'ami obsługującymi STP). Za pomocą RSTP propagowane są przez sieć informacje o zmianach topologii bezpośrednio przez urządzenie, które spowodowało zmianę topologii. W STP mają miejsce większe zwłoki, ponieważ urządzenie powodujące zmianę topologii, powiadamia najpierw „Root Bridge“, a dopiero potem sieć. Zarówno RSTP, jak i STP usuwają niechciane wyuczone adresy z bazy danych filtrów.

- W STP wyróżniane są stany portów „Blocking“, „Listening“, „Learning“ i „Forwarding“.
- W RSTP wyróżniane są stany portów „Discarding“, „Learning“ i „Forwarding“.

Stany portów przy switchach STP

- **„Blocking“**
  Gdy port tworzy „Switching Loop“ (pętlę między dwoma portami), dane użytkownika nie mogą być już wysyłane i odbierane. Port może jednak przejść do stanu „Forwarding“, gdy inne aktywne połączenia mają awarię i algorytm „Spanning Tree“ określa, że port może przejść w ten tryb.
  W stanie „Blocking“ mogą być jednak nadal odbierane i wysyłane dane BPDU.
- **„Listening“**
  Switch przetwarza dane BPDU i czeka na możliwe nowe informacje, przez które zostałby wprowadzony w stan „Blocking“.
- **„Learning“**
  Nawet jeśli port nie przekierował jeszcze żadnej ramki (pakietu), może nauczyć się adresów źródłowych odebranych ramek i dodać je do bazy danych filtrów („Switching Database“).
- **„Forwarding“**
  Port znajduje się w trybie roboczym i odbiera oraz wysyła dane. STP monitoruje potem wchodzące dane BPDU, czy wskazują, że port powinien przejść w stan „Blocking“, aby zapobiec powstaniu pętli.

- **„Disabled"**
  Nie jest to, dokładnie rzecz ujmując, część STP, gdyż administrator sieci może ręcznie dezaktywować port.

Role portów przy bridge'u RSTP

- **„Root"**
  „Root Port“ to przekierowujący port, który może transmitować dane z „Non-Root Bridge“ do „Root Bridge“.
- **„Designated”**
  Jest to przekierowujący port dla każdego segmentu LAN.
- **„Alternate“**
  Ten port jest alternatywną trasą do „Root Bridge“. Trasa przebiega jednak inaczej niż przy „Root Port“.
- **„Backup“**
  Ten port służy jako rezerwowa/redundantna trasa dla segmentu, z którym związany jest już inny „Bridge Port“.
- **„Disabled“**
  Nie jest to właściwie część STP, gdyż administrator sieci może ręcznie dezaktywować port.

Wskazówka



STP/RSTP
W tym dokumencie określnie „STP“ odnosi się zarówno STP, jak i RSTP.

Terminologia STP

Root Bridge

„Root Bridge“ to „Base“ (korzeń) drzewa rozpinającego.

Path Cost

„Path Cost“ to koszty transmisji ramki przez port do sieci LAN. Ta wartość zależy od prędkości transmisji.
Właściwy zakres wynosi od 1 do 200000000. Jest bardziej prawdopodobne, że trasa o większym koszcie jest blokowana przez STP, gdy zostanie wykryta pętla.

- „**Path Cost Short“** jest oryginalną wielkością o wartości 16-bitowej.
  Można tym samym brać pod uwagę tylko jedna prędkość do 10 Gbit.
- „**Path Cost Long“** jest wartością 32-bitową.
  Tym samym wspierana jest prędkość do 10 Tbit.

Tabela 61: Koszty trasy STP

Prędkość transmisji	Zalecana wartość	Zalecany zakres	Dopuszczalny zakres
4 Mb/s	250	100 … 1000	1 … 65535
10 Mb/s	100	50 … 600	1 … 65535
16 Mb/s	62	40 … 400	1 … 65535
100 Mb/s	19	10 … 60	1 … 65535
1 Gbit/s	4	3 … 10	1 … 65535
10 Gbit/s	2	1 … 5	1 … 65535

- Każdy „Bridge“ komunikuje się z „Root Bridge“ przez „Root Port“. „Root Port“ jest portem switcha o najniższych kosztach trasy do „Root Bridge“ (tj. „Root Path Cost“). Jeśli brak „Root Port“, switch staje się „Root Bridge“ dla sieci „Spanning Tree“.
- Dla każdego segmentu LAN wybierany jest „Designated Bridge“. Wśród wszystkich bridge'ów połączonych z LAN ma on najniższy koszt trasy do „Root Bridge“.

Forward Time (Forward Delay)

„Forward Time“ to maksymalny czas (w sekundach), jaki switch czeka, zanim zmieni stan. Zwłoka ta jest konieczna, gdyż każdy switch, zanim przekieruje ramkę, musi najpierw odebrać informacje o zmianach topologii. Poza tym każdy port potrzebuje czasu na odebranie informacji o konfliktach, które mogłyby go na powrót wprowadzić w stan zablokowania – w przeciwnym razie mogłoby dojść do powstania chwilowych pętli danych. Właściwy zakres wynosi od 4 do 30 sekund.

Max Age

„Max Age“ to maksymalny czas (w sekundach), przez jaki switch może czekać bez odbierania BPDU („**B**ridge **P**rotocol **D**ata **U**nit“), zanim spróbuje rozpocząć rekonfigurację. Wszystkie porty switcha (poza „Designated Ports“) odbierają BPDU w regularnych interwałach. Każdy port, który uczy się informacji STP (z ostatniej BPDU), staje się „Designated Port“ dla podłączonej sieci LAN. Gdy jest to „Root Port“, z portów switcha podłączonych do sieci wybrany zostaje nowy „Root Port“.

Hello Time

„Hello Time“ to interwał czasowy w sekundach między wiadomościami konfiguracyjnymi (BPDU „Bridge Protocol Data Unit“) wysyłanymi przez switch Root.

STP

Po tym jak bridge określi najbardziej korzystne cenowo „Spanning Tree“ z STP, aktywuje „Root Port“ i „Designated Ports“ dla podłączonych sieci LAN i dezaktywuje wszystkie inne porty uczestniczące w STP. Dlatego pakiety sieciowe przekierowywane są tylko między aktywowanymi portami i można uniknąć powstawaniu pętli.

Switche obsługujące STP wymieniają ze sobą regularnie dane BPDU. Gdy w sieci LAN powiązanej za pomocą bridge'a zmienia się topologia, rozpinane jest nowe drzewo. Gdy powstanie stabilna topologia sieci, wszystkie bridge'e czekają na „Hello BPDUs“, które są transmitowane przez „Root Bridge“. Gdy po zdefiniowanym wcześniej interwale („Max Age“) bridge nie odbierze „Hello BPDUs“, uznaje, że połączenie z „Root Bridge“ zostało przerwane. Potem rozpoczyna negocjacje z innymi bridge'ami, aby na nowo skonfigurować sieć i stworzyć aktualną topologię sieci.

Edge Port

„Edge Ports“ są połączone z siecią LAN, do której nie są podłączone inne bridge'e. Porty te mogą przechodzić bezpośrednio w stan „Forwarding“. Jednak RSTP monitoruje te porty pod kątem odbioru danych BPDU, gdy jest odłączony jeden bridge. RSTP można tak skonfigurować, aby automatycznie rozpoznawał „Edge Ports“. Gdy bridge rozpozna, że na „Edge Port“ przychodzą nowe dane BPDU, straci swój status jako „Edge Port“.

Forward Delay

„Forward Delay“ to maksymalny czas (w sekundach), jaki urządzenie root czeka, zanim zmieni stany (np. z „Listening“ na „Learning“ na „Forwarding“). Właściwy zakres wynosi od 4 do 30 s.

Transmission Limit

„Transmission Limit“ służy do konfiguracji minimalnego interwału między transmisjami następujących po sobie danych RSTP-BPDU. Tę funkcję można aktywować tylko w trybie RSTP. Właściwy zakres wynosi od 1 do 10 s.

Bridge Priority

Za pomocą „Bridge Priority“ definiowany jest wybór switcha root, portu root i „Designated Port“. Switch o najwyższym priorytecie zostaje switchem STA root. Jeśli jednak wszystkie switche mają ten sam priorytet, switchem root zostaje switch o najniższym adresie MAC.

Port Priority

Priorytet portu konfigurowany jest w switchu. Cyfra o niskiej wartości oznacza wysoki priorytet. Jest bardziej prawdopodobne, że port o mniejszym priorytecie jest blokowany przez STP, gdy zostanie wykryta pętla. Właściwy zakres wynosi od 0 do 240.

BPDU Guard

Ustawienia konfigurowane są dla każdego portu osobno. Gdy port jest aktywowany w „BDU Guard“ i odbiera BPDU, przechodzi w stan „Disabled“, aby uniknąć błędnego środowiska. Użytkownik musi aktywować port ręcznie.

BPDU Filter

Za pomocą tej funkcji w porcie switcha ustawiany jest filtr dla wysyłania lub odbierania danych BPDU. Gdy port odbiera dane BPDU, zostają one anulowane. Przy równoczesnej aktywacji „BPDU Filter“ i „BPDU Guard“ ten pierwszy ma najwyższy priorytet.

Wskazówka



BPDU Filter i BPDU Guard
Przy równoczesnej aktywacji „BPDU Filter“ i „BPDU Guard“ ten pierwszy ma najwyższy priorytet.

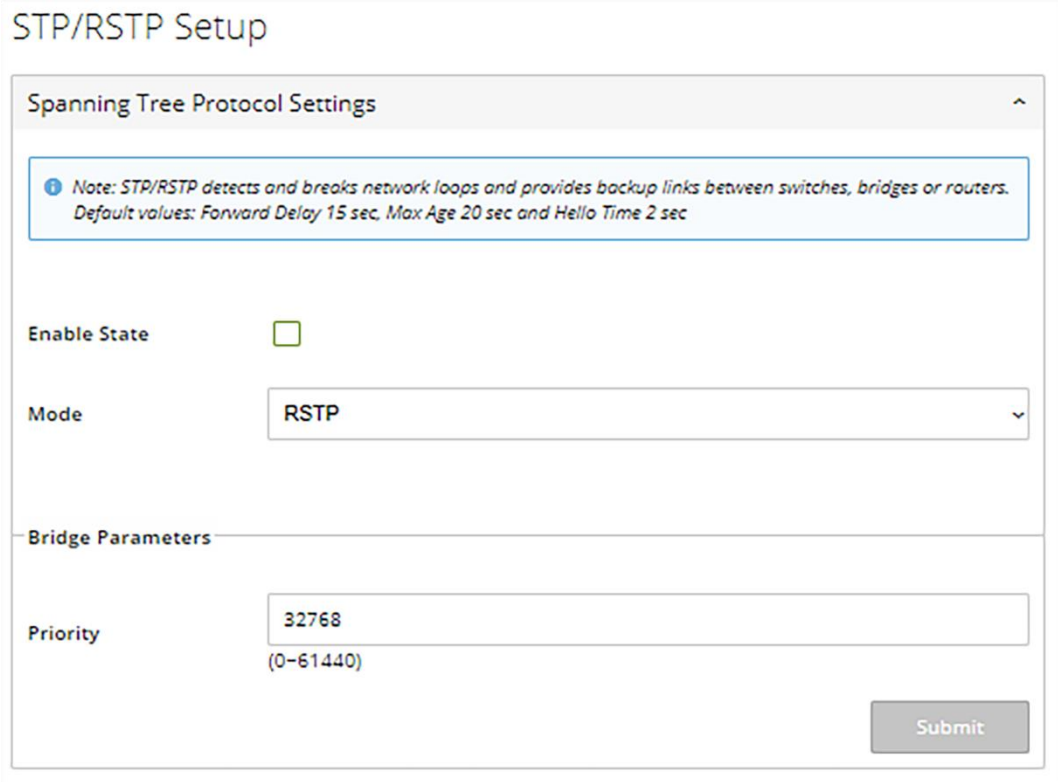
Root Guard

Funkcja „Root Guard“ zmusza interfejs do przyjęcia roli „Designated Port“, aby zapobiec sytuacji, że rolę switcha root będą pełnić sąsiadujące ze sobą switche. Funkcja ta daje możliwość ustalenia wyboru „Root Bridge“ w sieci. Zapobiega ona sytuacji, że „Designated Port“ mógłby stać się „Root Port“. Gdy port z funkcją „Root Guard“ odbiera BPDU o wyższej wartości, port przechodzi w stan niespójny z root (praktycznie równoważnym ze stanem „Listening“), aby utrzymać status aktualnego „Root Bridge“. Port może przejść w stan „Forwarding“, gdy w czasie trzech „Hello Times“ nie zostaną odebrane BPDU o wyższej wartości.

9.4.2.1 STP/RSTP Setup

Wskazówka

Funkcje STP/RSTP
STP/RSTP może wykryć pętle sieci i przerwać połączenia zapasowe („Back-up Links“) między switchami, bridge'ami lub ruterami.
Wartości domyślne – „Forward Delay“: 15 s, „Mag Age“: 20 s i „Hello Time: 2 s.



Ilustracja 79: Zakładka „Redundancy“ – menu „STP/RSTP Setup“

Tabela 62: Zakładka „Redundancy“ – menu „STP/RSTP Setup“

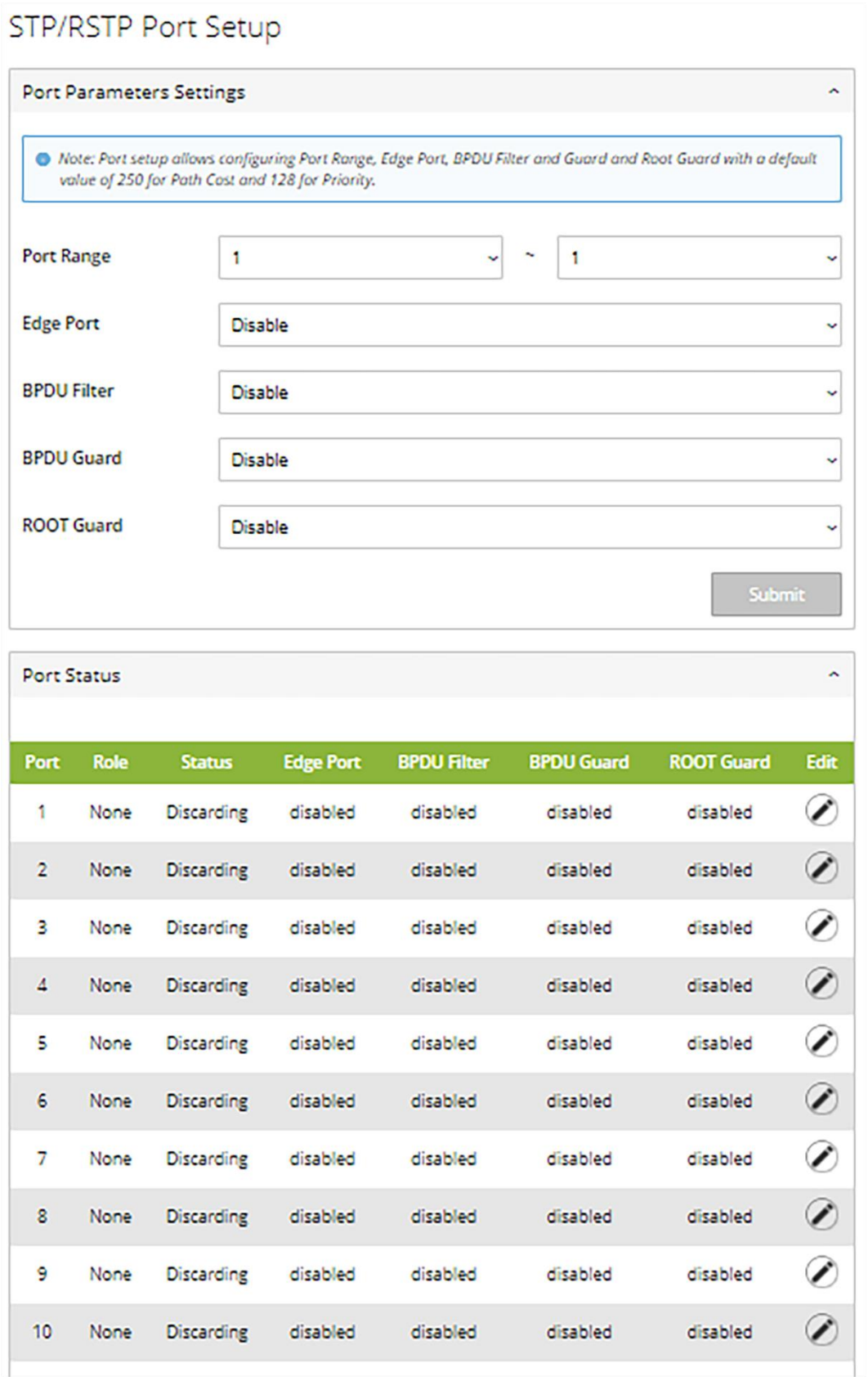
Spanning Tree Protocol Settings			
Parametr	**Domyślnie**	**Opis**	
Enable State	☐	☐	Funkcja „STP/RSTP“ jest dla switcha dezaktywowana.
		☑	Funkcja „STP/RSTP“ jest dla switcha aktywowana.
Mode	**RSTP**	W polu wyboru należy wybrać „RSTP“, gdy ma być zastosowany szybki „Rapid Spanning Tree Protocol“.	
	STP	W polu wyboru należy wybrać „STP“, gdy ma być zastosowany „Spanning Tree Protocol“.	
Bridge Parameters			
Parametr	**Domyślnie**	**Opis**	
Priority (Range: 0~61440)	**32768**	W polu edycji należy wpisać wartość priorytetu. Im niższa przypisana wartość numeryczna, tym wyższy priorytet bridge'a. Właściwy zakres: 0 … 61440	

9.4.2.2 STP/RSTP Port Setup

Wskazówka



Funkcje w ustawieniach portu
Ustawienia portu umożliwiają konfigurację zakresu portów, „Edge Port” i filtra BDU oraz funkcji „Guard” i „Root Guard” z wartością domyślną 250 dla kosztów trasy i 128 dla priorytetu.



Ilustracja 80: Zakładka „Redundancy“ – menu „STP/RSTP Port Setup“

Tabela 63: Zakładka „Redundancy“ – menu „STP/RSTP Port Setup“

Port Parameter Settings		
Parametr	**Domyślnie**	**Opis**
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „STP/RSTP Function“.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „STP/RSTP Function“.
Edge Port	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować typ „Edge Port“ dla specyficznego portu.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować typ „Edge Port“ dla specyficznego portu.
BPDU Filter	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję filtra BPDU dla specyficznego portu.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję filtra BPDU dla specyficznego portu.
BPDU Guard	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „BPDU Guard“ dla specyficznego portu.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „BPDU Guard“ dla specyficznego portu.
ROOT Guard	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „ROOT Guard“ dla specyficznego portu.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „BROOT Guard“ dla specyficznego portu.
Port Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
Role	Alternated Designated Root Backup None	W tej kolumnie wyświetlana jest rola portu.
Status	Discarding Blocking Listening Learning Forwarding Disabled	W tej kolumnie wyświetlany jest status portu.
Edge Port	Disable Enable	W tej kolumnie wyświetlany jest stan funkcji „Edge Port“.

Tabela 63: Zakładka „Redundancy“ – menu „STP/RSTP Port Setup“

Port Parameter Settings		
Parametr	**Domyślnie**	**Opis**
BPDU Filter	Disable Enable	W tej kolumnie wyświetlany jest stan funkcji „BPDU Filter“.
BPDU Guard	Disable Enable	W tej kolumnie wyświetlany jest stan funkcji „BPDU Guard“.
ROOT Guard	Disable Enable	W tej kolumnie wyświetlany jest stan funkcji „Root Guard“.
Edit		W tej kolumnie można aktywować funkcję edycji.

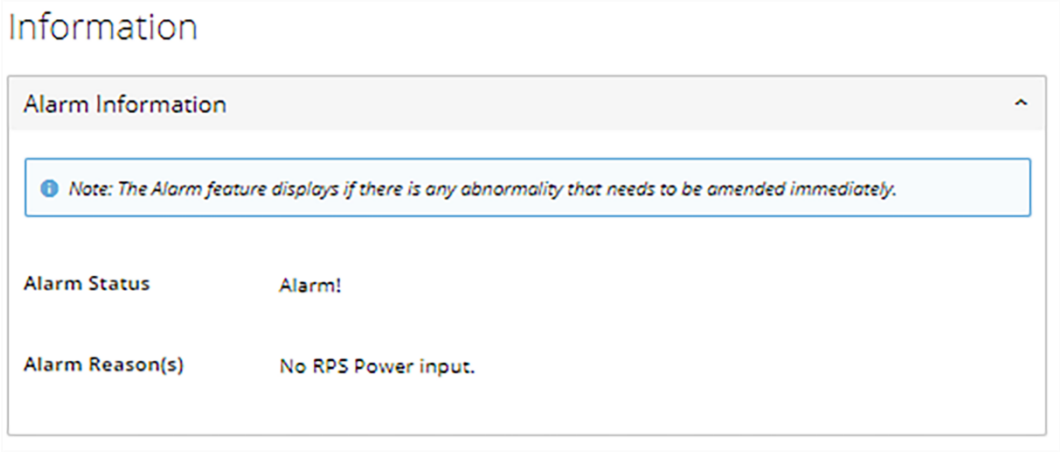
9.5 Diagnostic

9.5.1 Alarm

9.5.1.1 Information

Wskazówka

Zadanie funkcji alarmu
Funkcja alarmu wskazuje, czy występują błędy, które trzeba niezwłocznie usunąć.



Ilustracja 81: Zakładka „Diagnostic” – menu „Information”

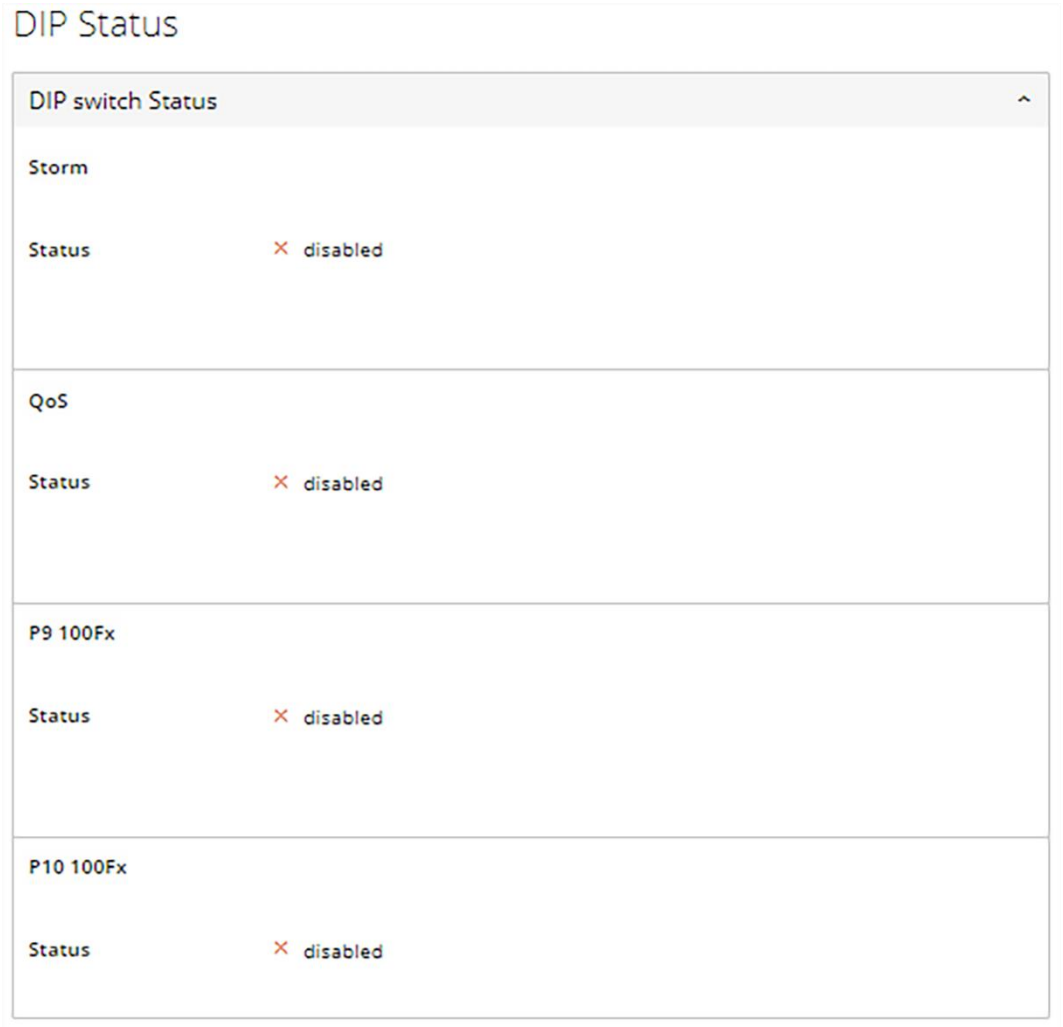
Tabela 64: Zakładka „Diagnostic” – menu „Information”

Alarm Information		
Parametr	**Domyślnie**	**Opis**
Alarm Status		W tym polu wyświetlana jest informacja, czy wystąpiły zdarzenia alarmu.
Alarm Reason		W tym polu wyświetlane są szczegóły dotyczące zdarzeń alarmu.

9.5.1.2 DIP Status

Wskazówka **Wyświetlanie statusu DIP**

Funkcja alarmu wskazuje, czy występują odstępstwa, które trzeba niezwłocznie skorygować.



Ilustracja 82: Zakładka „Diagnostic” – menu „DIP Status”

Tabela 65: Zakładka „Diagnostic” – menu „DIP Status”

DIP switch Status		
Parametr	**Parametr**	**Parametr**
Storm	**Disable** Enable	W tym polu wyświetlana jest informacja, czy „PWR” funkcja jest aktywowana czy dezaktywowana.
QoS	**Disable** Enable	W tym polu wyświetlana jest informacja, czy funkcja „RPS” jest aktywowana czy dezaktywowana.
P9 100Fx	**Disable** Enable	W tym polu wyświetlana jest informacja, czy funkcja „P9 100 Fx” jest aktywowana czy dezaktywowana.
P10 100Fx	**Disable** Enable	W tym polu wyświetlana jest informacja, czy funkcja „P10 100 Fx” jest aktywowana czy dezaktywowana.

9.5.1.3 Traffic Flooding

„Traffic Flooding” oznacza, że sieć jest nieustannie „zalewana” ruchem z pakietów broadcast lub multicast. „Broadcast Traffic Flooding” może całkowicie sparaliżować łączność w sieci przez stale narastającą liczbę pakietów.

„Traffic Flooding Control” chroni szerokość pasma switcha przed zalewem pakietami, włącznie z pakietami broadcast, multicast i „Destination Lookup Failure“ (DLF). Współczynnik jest progiem, który ogranicza całkowitą liczbę określonych typów pakietów. Na przykład, jeśli wybrano opcje broadcast i multicast, całkowita liczba pakietów przesyłanych na sekundę dla tych dwóch typów nie zostanie przekroczona.

„Broadcast Traffic Flooding Control” ogranicza liczbę pakietów broadcast, multicast i nieznanych unicast (określanych też jako „Destination Lookup Failure“ lub DLF), które mogą być odbierane przez switch na portach w ciągu sekundy. Po osiągnięciu maksymalnej liczby tych pakietów na sekundę wszystkie pozostałe pakiety zostają odrzucone. Funkcję tę należy aktywować w celu ograniczenia liczby tych pakietów w sieci.

Górna granica „Traffic Flooding Control”: 3700 pakietów na sekundę (pps).

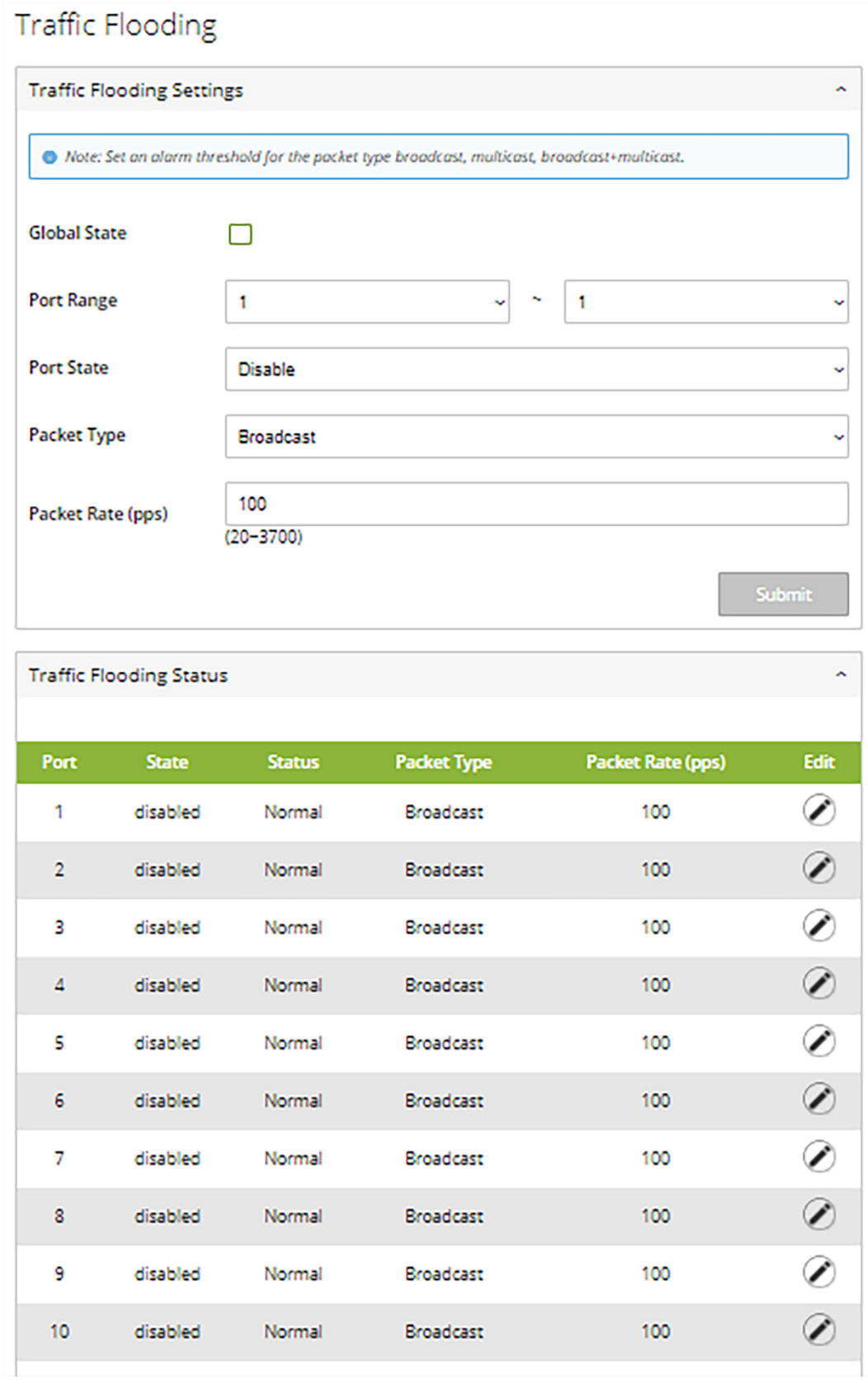
Ustawienia domyślne

Broadcast Storm Control:	100 pakietów na sekundę (pps)
Multicast Storm Control	brak wartości
DLF Storm Control	100 pakietów na sekundę (pps)

Wskazówka



Ustawienie wartości granicznej alarmu
Należy skonfigurować wartość graniczną dla przesyłu pakietów typu broadcast, multicast oraz broadcast/multicast.



Ilustracja 83: Zakładka „Diagnostic” – menu „Traffic Flooding”

Tabela 66: Zakładka „Diagnostic” – menu „Traffic Flooding”

Traffic Flooding Settings		
Parametr	**Parametr**	**Parametr**
Global State	☐	☐ Funkcja „Global State” jest dla switcha dezaktywowana.
		☑ Funkcja „Global State” jest dla switcha aktywowana.
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowany „Traffic Flooding”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowany „Traffic Flooding”.
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Traffic Floodingr“ dla portu lub zakresu portów.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Traffic Floodingr“ dla portu lub zakresu portów.
Packet Type	**Broadcast**	W polu wyboru należy wybrać „Broadcast“, gdy ma on być monitorowany jako typ pakietu.
	Multicast	W polu wyboru należy wybrać „Multicast“, gdy ma on być monitorowany jako typ pakietu.
	Bcast+Mcast	W polu wyboru należy wybrać „Bcast+Micast“, gdy oba mają być monitorowane jako typy pakietów.
Packet Rate (pps) (20-3700)		W polu edycji należy wpisać prędkość pakietu, która ma być monitorowana. Właściwy zakres: 20…3700 Mb/s
Traffic Flooding Status		
Parametr	**Parametr**	**Parametr**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
State	Disable Enable	W tej kolumnie wyświetlany jest status specyficznego portu.
Status	Normal	W tej kolumnie wyświetlany jest status stanu pracy.
Packet Type	Broadcast Multicast Bcast+Mcast	W tej kolumnie wyświetlany jest typ pakietu danych.
Packet Rate (pps)		W tej kolumnie wyświetlana jest wybrana prędkość pakietu.
Edit		W tej kolumnie można aktywować funkcję edycji.

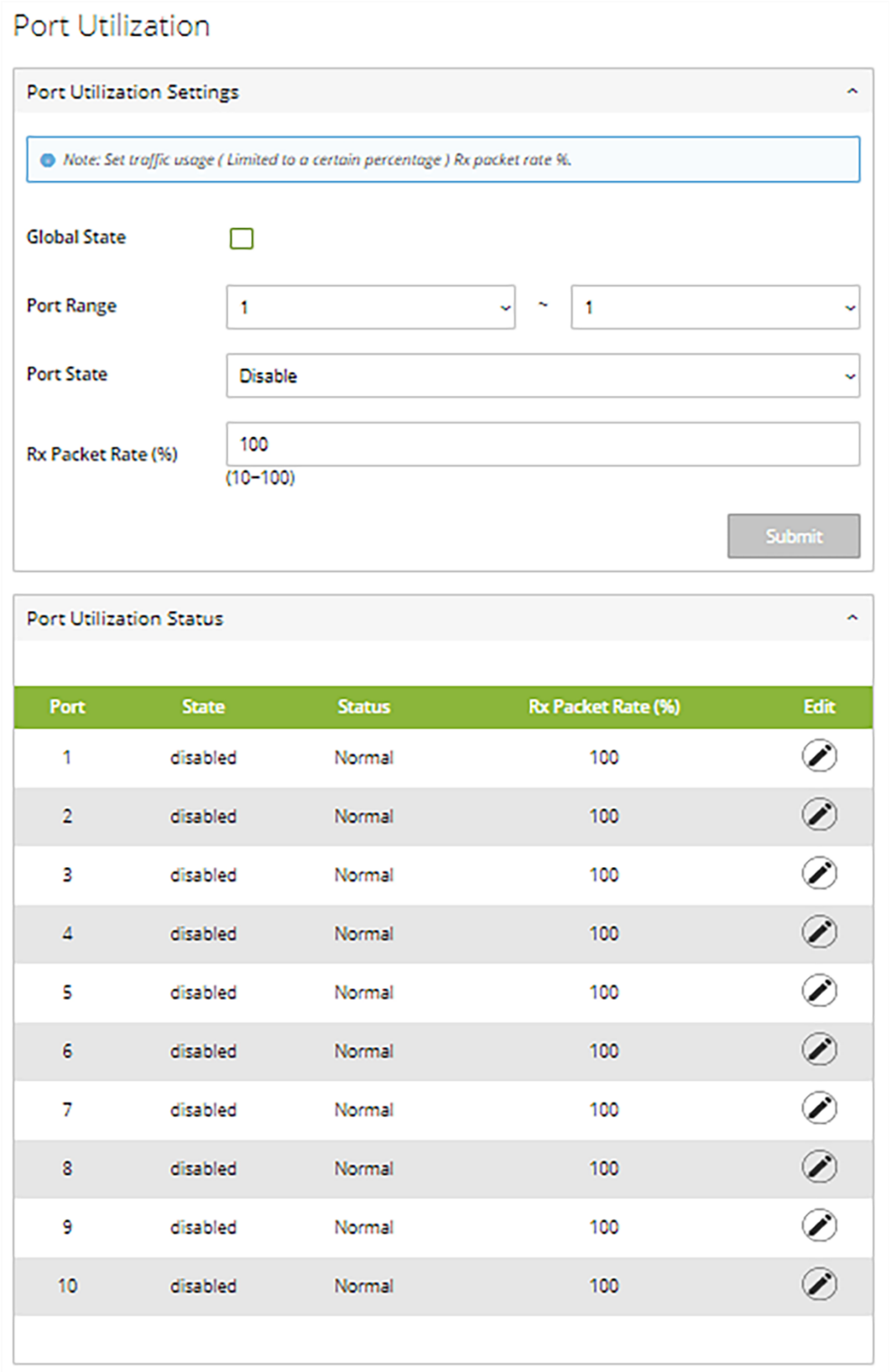
9.5.1.4 Port Utilization

Dzięki tej funkcji użytkownik może wyświetlać i monitorować obciążenie ruchu na porcie.

Wskazówka



Ustawienia dla Port Utilization
Port Utilization (ograniczone do określonego procentu) ustawia się za pomocą „Rx packet rate %” (szybkość pakietów Rx w procentach).



Ilustracja 84: Zakładka „Diagnostic” – menu „Port Utilization”

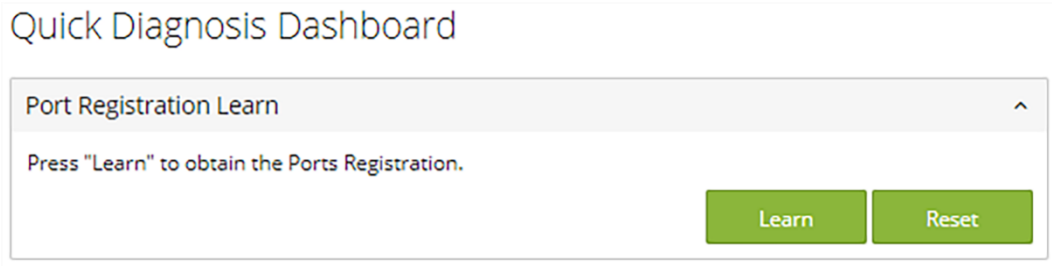
Tabela 67: Zakładka „Diagnostic” – menu „Port Utilization”

Port Utilization Settings		
Parametr	**Parametr**	**Parametr**
Global State	☐	☐ Funkcja „Global State” jest dla switcha dezaktywowana.
		☑ Funkcja „Global State” jest dla switcha aktywowana.
Port Range	**1** … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowana „Port Utilization”.
	1 … 10	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowana „Port Utilization”.
Port State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Traffic Utilization“ dla portu lub zakresu portów.
	Enable	W polu wyboru należy wybrać „Enable“, aby dezaktywować funkcję „Traffic Utilization“ dla portu lub zakresu portów.
Rx Packet Rate (%) (10-100)	**100**	W polu edycji należy wpisać prędkość pakietu, która ma być monitorowana. Właściwy zakres: 10 … 100 %.
Port Utilization Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10	W tej kolumnie wyświetlane są numery portów.
State	Disable Enable	W tej kolumnie wyświetlany jest status specyficznego portu.
Status	Normal	W tej kolumnie wyświetlany jest status stanu pracy.
Rx Packet Rate (%)		W tej kolumnie wyświetlana jest wybrana prędkość pakietu.
Edit		W tej kolumnie można aktywować funkcję edycji.

9.5.2 Dashboard Configuration

9.5.2.1 Quick Diagnosis Dashboard

9.5.2.1.1 Port Registration Learn



Ilustracja 85: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Port Registration Learn”

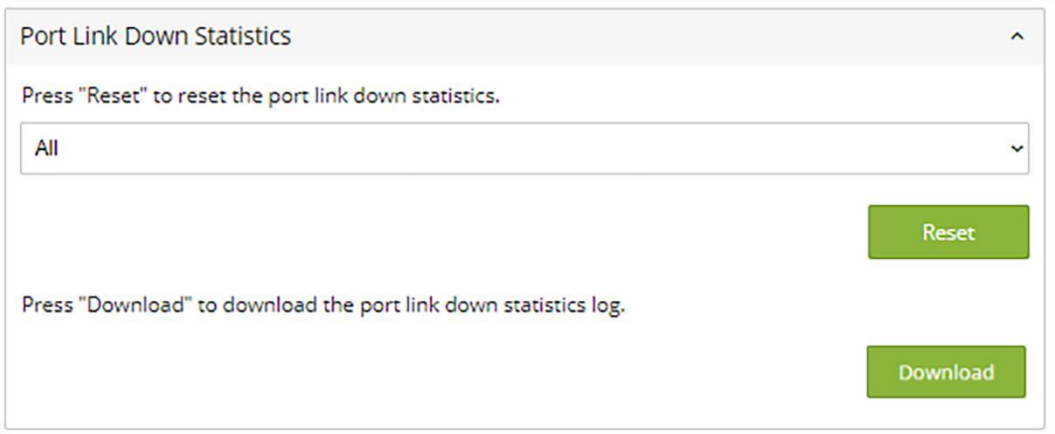
Należy kliknąć przycisk **[Learn]**, aby urządzenia sąsiednie zostały zapisane w switchu.
Jeżeli połączenie każdego z uczestników z siecią zostało poprawnie nawiązane, aktualny stan połączenia zostanie zapisany w switchu jako referencja.
Odchylenia od tego stanu będą w przyszłości wyświetlane jako błędy w panelu (dashboard) lub na mapie topologii.

Należy kliknąć przycisk **[Reset]**, aby przywrócić konfigurację domyślną (nauczone zgłoszenia portów zostaną zapomniane).

Wskazówka

Uczenie urządzeń sąsiednich
Należy aktywować LLDP na urządzeniach sąsiednich. Alternatywnie można uczyć urządzenia sąsiednie za pomocą adresu MAC (patrz rozdział „Konfiguracja“ …> … „Manual Registration“).

9.5.2.1.2 Port Link Down Statistics



Ilustracja 86: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Port Link Down Statistics”

W tym menu można wyświetlić, zresetować lub pobrać statystyki dotyczące pojedynczych lub wszystkich interfejsów.

Należy kliknąć przycisk **[Reset]**, aby zresetować „Port Link Down Statistics”. Dzięki temu wartości zostaną usunięte z panelu diagnostycznego.

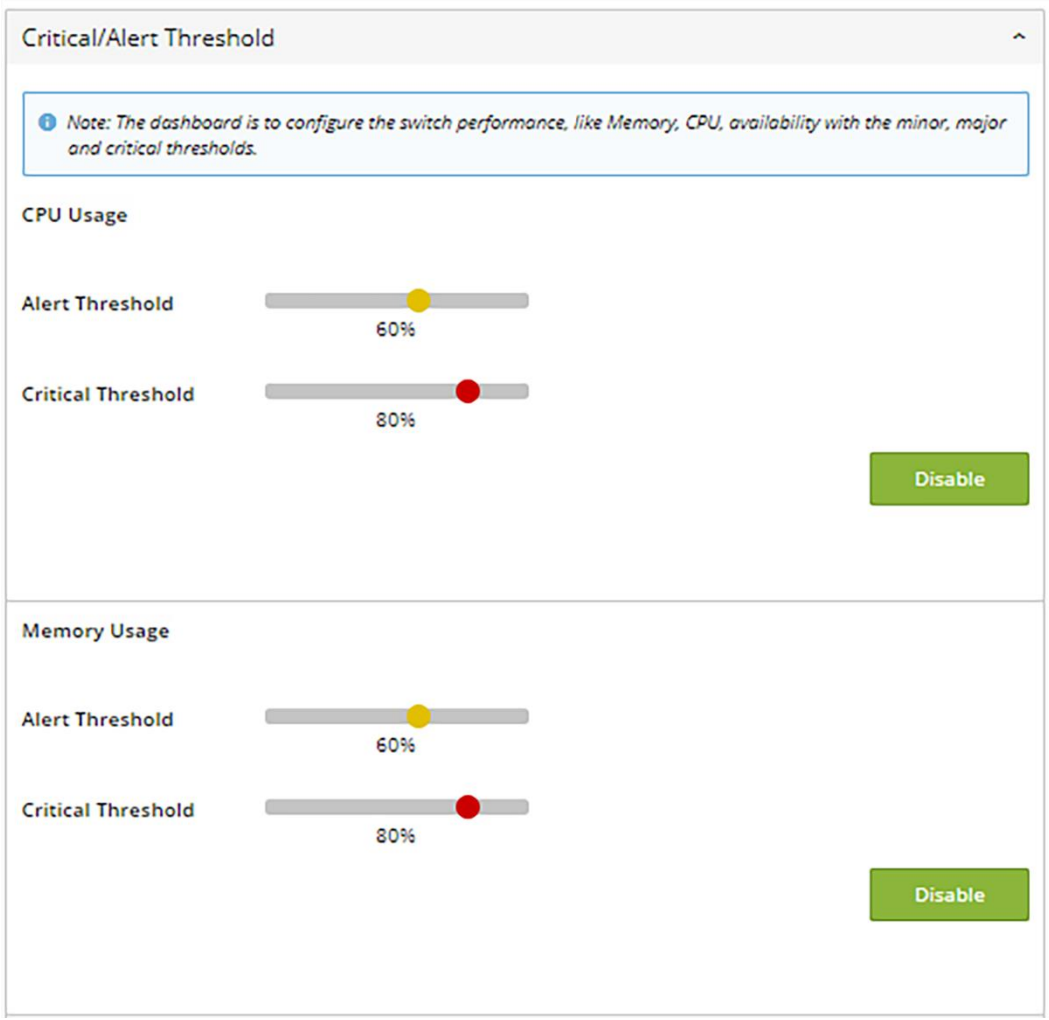
Należy kliknąć przycisk **[Download]**, aby pobrać plik dziennika statystyki nieaktywności portów.
Można pobrać tę statystykę albo dla wszystkich, albo dla pojedynczych portów. Za pomocą tego pliku można zlokalizować przerywane połączenia w sieci ETHERNET.

9.5.2.1.3 Critical/Alert Threshold

Tutaj można ustawić wartości graniczne, przy których zmieniają się kolory wskaźników dla „CPU Usage”, „Memory Usage”, „Transmitting Port Usage” i „Receiving Port Usage” w panelu (patrz rozdział „Diagnostic”).

Wskazówka **Określanie wartości granicznych**

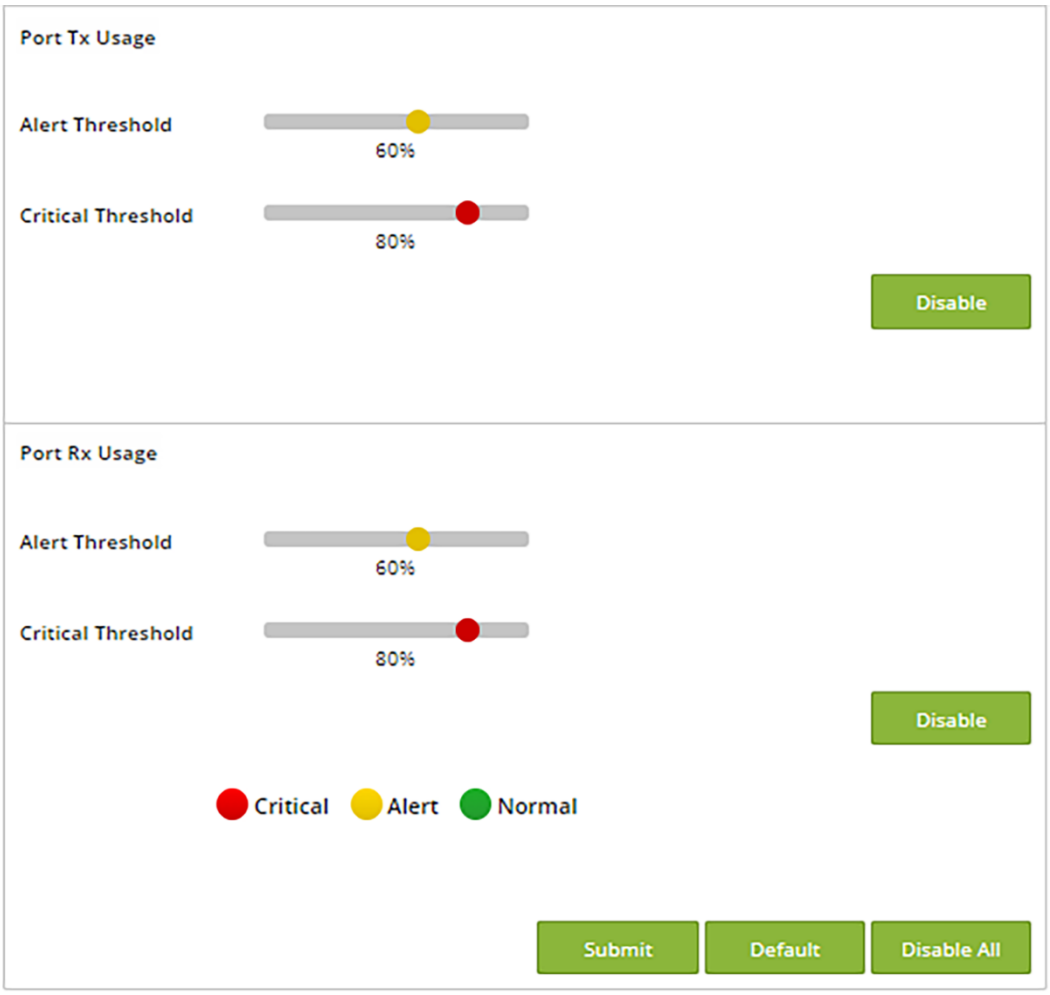
Wartość graniczna dla alarmów określa, kiedy wskaźnik zabarwi się na żółto, a dla krytycznych błędów — kiedy zabarwi się na czerwono. Te wartości graniczne można skonfigurować oddzielnie dla obciążenia CPU, pamięci oraz dla portów wysyłających (Tx) i odbierających (Rx).



Ilustracja 87: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Critical/Alert Threshold 01”

Należy kliknąć przycisk **[Disable/Enable]**, aby dezaktywować/aktywować następujące obszary:

- Obciążenie CPU
- Wykorzystanie pamięci



Ilustracja 88: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Critical/Alert Threshold 02”

Należy kliknąć przycisk **[Disable/Enable]**, aby dezaktywować/aktywować następujące obszary:

- Wykorzystanie portu Tx
- Wykorzystanie portu Rx

9.5.3 Modbus

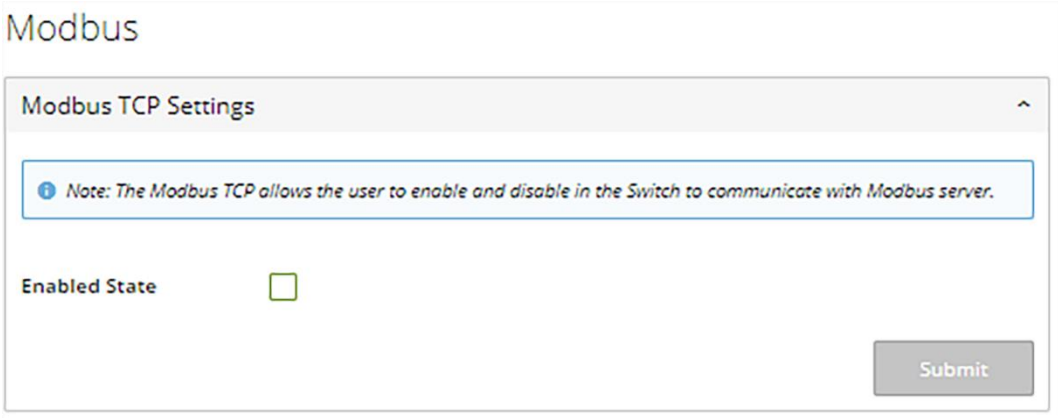
9.5.3.1 Format danych i kod funkcji

Modbus TCP wspiera różne typy formatów danych do odczytu.
Najważniejsze 4 typy to:

Tabela 68: Format danych i kod funkcji

Typ dostępu do danych		Kod funkcji	Nazwa funkcji	Wskazówka
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Nieobsługiwane
	Internal Bits or Physical Coils	1	Read Coils	Nieobsługiwane
Word access (dostęp 16-bitowy)	Physical Input Registers	4	Read Input Registers	
	Physical Output	3	Read Holding Registers	Nieobsługiwane

9.5.3.2 Rejestry Modbus



Ilustracja 89: Zakładka „Diagnostic” – menu „Modbus”

Tabela 69: Modbus

Modbus TCP Settings			
Parametr	**Domyślnie**	**Opis**	
Enabled State	☐	☐	Funkcja „Modbus” jest dla switcha dezaktywowana.
		☑	Funkcja „Modbus” jest dla switcha aktywowana.

Wskazówka

Rejestry Modbus
Tabelę „Rejestry Modbus” można znaleźć w rozdziale „Aneks” > … > „Rejestry Modbus”.
Rejestry Modbus są również wyświetlane w systemie zarządzania przez WWW (WBM).

9.5.4 SNMP

Wskazówka



Po kliknięciu na karcie „Diagnostic” menu „SNMP”, można uzyskać w menu „SNMP” dostęp do zakładki „Configuration”.
Szczegółowy opis mona znaleźć w rozdziale „Configuration” > „SNMP”.

9.5.5 System Log

9.5.5.1 Syslog Server Setting

Funkcję „syslog“ można aktywować lub dezaktywować. Ustawienie domyślne to „disabled”. Wiadomość protokołu zapisywana jest w systemie plików switcha. Jeśli skonfigurowany został adres IP serwera „syslog“, switch będzie wysyłał do niego kopię.

Wskazówka

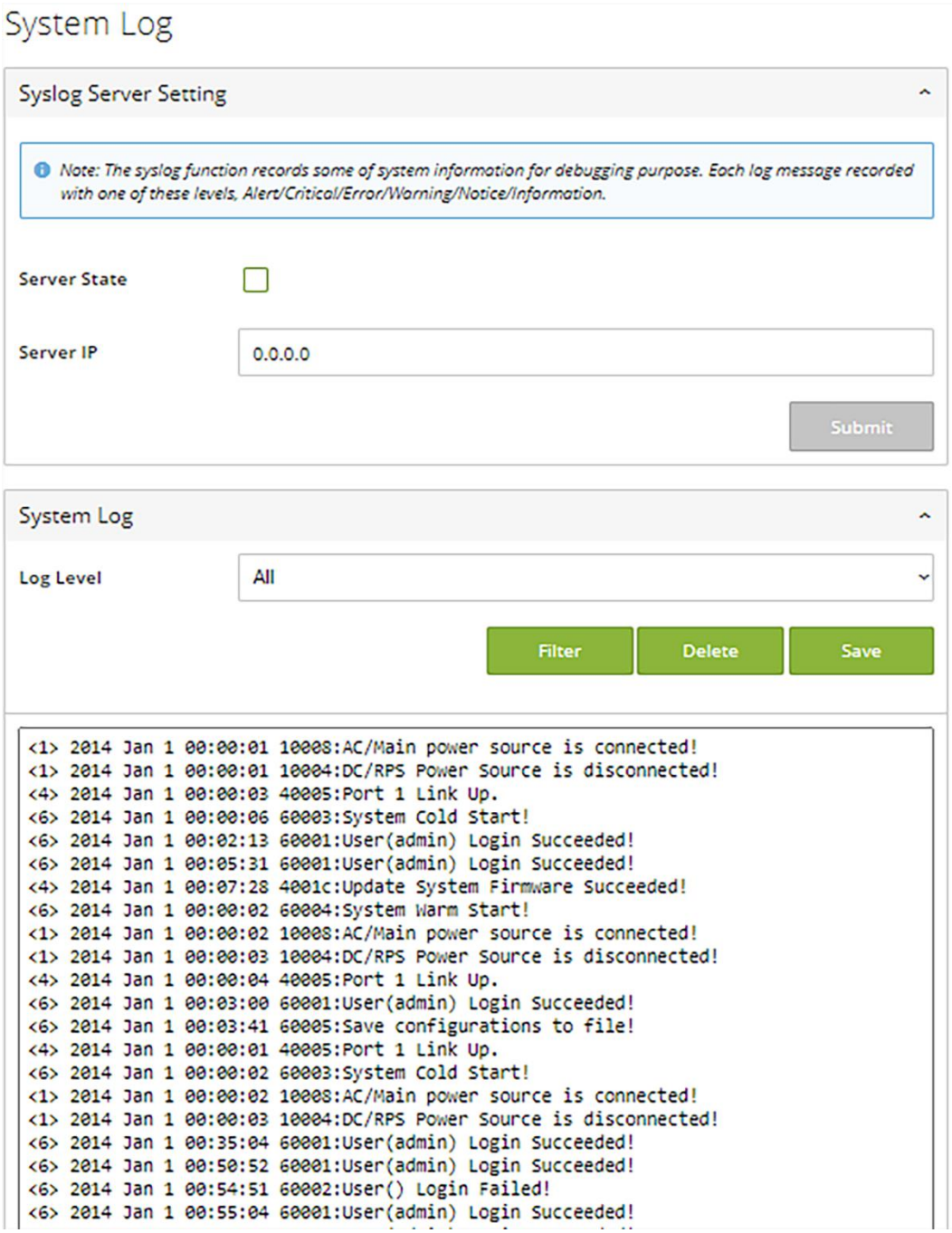


Wielkość „Log Message File“
Wielkość „Log Message File“ ograniczona jest do 4 KB. Jeśli plik jest pełny, najstarsza wiadomość zostaje zastąpiona nowszą.

Wskazówka



Sposób działania syslog
Funkcja „syslog“ zapisuje różne informacje systemowe dla funkcji „Debugging“. Każdy wpis w protokole rejestruje jeden z następujących poziomów: Alert/Critical/Error/Warning/Notice/Information.



Ilustracja 90: Zakładka „Diagnostic” – menu „System Log”

Tabela 70: Zakładka „Diagnostic” – menu „System Log”

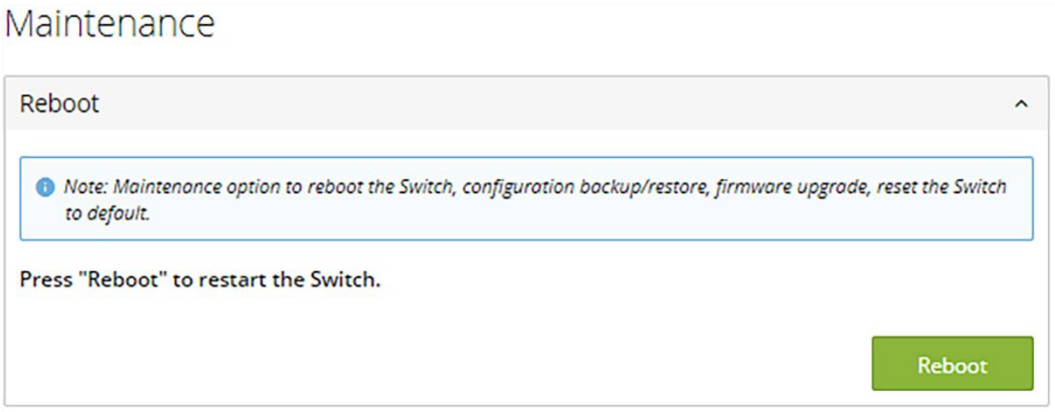
Syslog Server Settings		
Parametr	**Parametr**	**Parametr**
Global State	☐	☐ Funkcja „Global State” jest dla switcha dezaktywowana.
		☑ Funkcja „Global State” jest dla switcha aktywowana.
Server IP	**0.0.0.0**	W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami (np.: 192.168.1.1).
System Log		
Parametr	**Domyślnie**	**Opis**
Log Level	**All**	W polu wyboru należy wybrać „All“, jeśli mają być wyświetlone wszystkie wiadomości protokołów.
	1:Alarm	W polu wyboru należy wybrać „Alarm“, aby wyświetlić komunikaty dziennika zdarzeń.
	2:Critical	W polu wyboru należy wybrać „Critical“, jeśli mają być wyświetlone krytyczne wiadomości protokołów.
	3:Error	W polu wyboru należy wybrać „Error“, jeśli mają być wyświetlone błędy.
	4:Warning	W polu wyboru należy wybrać „Warning“, jeśli mają być wyświetlone ostrzeżenia.
	5:Notice	W polu wyboru należy wybrać „Notice“, jeśli mają być wyświetlone powiadomienia.
	6:Information	W polu wyboru należy wybrać „Information“, jeśli mają być wyświetlone wszystkie informacje.

9.6 Maintenance

9.6.1 Reboot

Wskazówka

Zakres konserwacji
Sekcja „Maintenance” oferuje opcje ponownego uruchomienia, zapisu/przywrócenia konfiguracji, aktualizacji firmware'u oraz zresetowania switcha do ustawień fabrycznych.

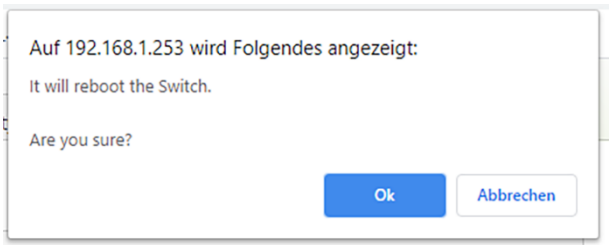


Ilustracja 91: Zakładka „Maintenance” – menu „Maintenance” – „Reboot”

Funkcja „Reboot“ umożliwia restart switcha bez fizycznego odłączenia napięcia zasilającego.

W celu przeprowadzenia restartu switcha należy wykonać następujące kroki:

1. Kliknij przycisk **[Reboot]** w menu „Reboot”.
   Pojawi się widoczne niżej okno.



Ilustracja 92: Zakładka „Maintenance” – zakładka „Reboot” – Message

2. Kliknij **[OK]** i poczekaj, aż switch ponownie się uruchomi. Proces może trwać do dwóch minut. Konfiguracji switcha nie zostaje w efekcie tego procesu zmieniona.

9.6.2 Upgrade Firmware



Ilustracja 93: Zakładka „Maintenance” – menu „Maintenance” – „Upgrade Firmware”

W celu przeprowadzenia aktualizacji firmware'u switcha należy wykonać następujące kroki:

1. Kliknij przycisk **[Choose file]**.
   Zostanie otwarte okno dialogowe dotyczące wyboru pliku. Wybierz w nim odpowiedni plik firmware'u.

2. Kliknij przycisk **[Upgrade]**, aby załadować nowy firmware.

9.6.3 Upload Configuration



Ilustracja 94: Zakładka „Maintenance” – menu „Maintenance” – „Upload Configuration”

W celu pobrania pliku konfiguracyjnego z PC do switcha należy wykonać następujące kroki:

1. Wybierz „Upload the configuration file to the Switch“.

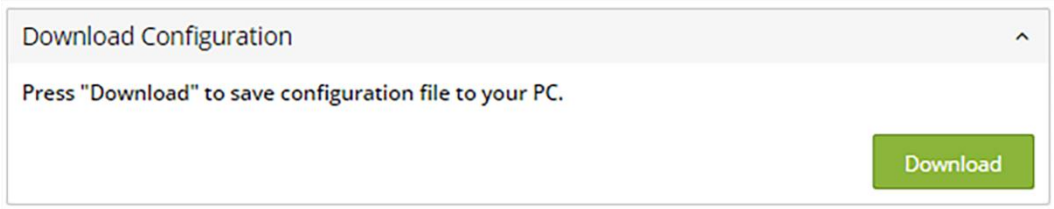
2. Kliknij przycisk **[Choose file]**.
   Wybierz plik konfiguracyjny, podając pełną ścieżkę.

3. Kliknij przycisk **[Upload]**, aby rozpocząć pobieranie.

Wskazówka

Modyfikacja pliku konfiguracyjnego
Dzięki modyfikacji pliku konfiguracyjnego za pomocą edytora tekstu można szybko skonfigurować większą liczbę switchy.

9.6.4 Download Configuration



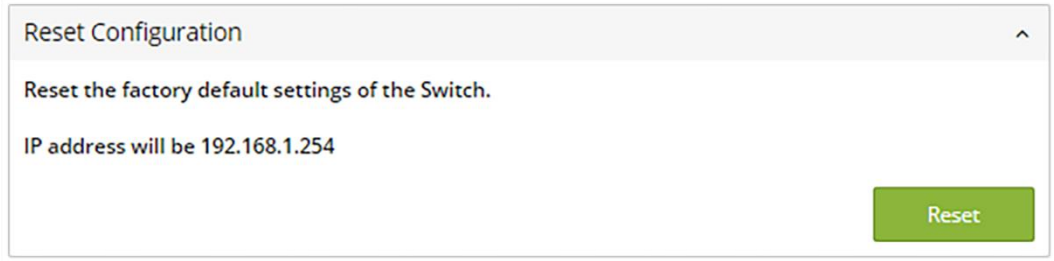
Ilustracja 95: Zakładka „Maintenance” – menu „Maintenance” – „Download Configuration”

W celu zapisania pliku konfiguracyjnego na swoim PC należy wykonać następujące kroki:

1. Wybierz „Presss Download, aby zapisać plik konfiguracyjny na komputerze”.

2. Kliknij przycisk **[Download]**, aby rozpocząć pobieranie.

9.6.5 Reset Configuration

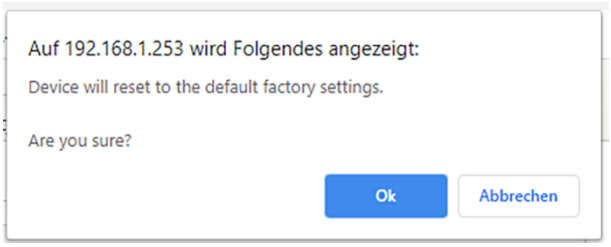


Ilustracja 96: Zakładka „Maintenance” – menu „Maintenance” – „Reset Configuration”

Funkcja „Reset Configuration“ przywraca switch do ustawień fabrycznych.

W celu przeprowadzenia restartu switcha należy wykonać następujące kroki:

1. W menu „Reset Configuration“ kliknij przycisk **[Reset]**. Pojawi się widoczne niżej okno.



Ilustracja 97: Zakładka „Maintenance“ – „Reset“ – Message

2. Kliknij **[OK]** i poczekaj, aż switch ponownie się uruchomi. Proces może trwać do dwóch minut. Konfiguracja systemu zostanie zresetowana do wartości domyślnych.

10 Załącznik

10.1 Przewód RJ-45

Do podłączania urządzeń sieciowych należy używać standaryzowanych przewodów ETHERNET. Obłożenie zacisków jest następujące:

Tabela 71: Przewód RJ-45

Styk	Nazwa		Para	Kolor (zgodnie z EIA/TIA 568B)
	4-żyłowy	8-żyłowy		
1	TD+	D1+	2	biały/pomarańczowy
2	TD−	D1−	2	pomarańczowy
3	RX+	D2+	3	biały/zielony
4	niewykorzystany	D3+	1	niebieski
5	niewykorzystany	D3−	1	biały/niebieski
6	RX−	D2−	3	zielony
7	niewykorzystany	D4+	4	biały/brązowy
8	niewykorzystany	D4−	4	brązowy

Wskazówka



Funkcje na złączu RJ-45
Switch zarządzający Lean oferuje na złączu RJ-45 takie funkcje jak „Autocrossing“ i „Autonegotiation“.

10.2 Konfiguracja w Command Line Interface (CLI)

Do skonfigurowania switcha przez CLI wymagane jest połączenie Telnet lub SSH.

Ten rozdział zawiera wybór dostępnych poleceń interfejsu wiersza poleceń.

10.2.1 System Status

10.2.1.1 System Information

Table 72: CLI “System Information” Configuration

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

10.2.2 Default Settings

10.2.2.1 System

Table 73: CLI “System” Configuration

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

10.2.2.2 Jumbo Frame

Table 74: CLI “Jumbo Frame” Configuration

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

10.2.2.3 SNTP

Table 75: CLI “SNTP” Configuration

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

Example

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

L2SWITCH(config)*#time timezone +0800*

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

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

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

10.2.2.4 Management Host

Table 76: CLI “Management Host” Configuration

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

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#interface eth0*

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

10.2.2.5 MAC Management

Table 77: CLI “MAC Management” Configuration

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

Example

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

10.2.2.6 Port Mirroring

Table 78: CLI “Port Mirroring” Configuration

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

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#mirror enable*

L2SWITCH(config)*#mirror destination port 2*

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

10.2.2.7 Port Settings

Table 79: CLI “Port Settings” Configuration

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

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config-if)#*speed auto*

10.2.3 Advanced Settings

10.2.3.1 Power over Ethernet (PoE)

Table 80: CLI “PoE Settings” Configuration

Node	Command	Description
enable	show poe	This command displays the PoE configurations and status.
configure	poe (disable | enable)	This command disables or enables the global PoE for the Switch.
configure	poe total-power	This command configures the total power which the Switch can support.
interface	poe(disable|enable)	This command enables or disables the PoE function on the specific port.
if-range	poe (disable | enable)	This command disables / enables the PoE on a port or a range of ports.

10.2.3.2 PD Alive Check

Table 81: CLI “PD Alive Check” Configuration

Node	Command	Description
enable	show pd-alive	This command displays the configuration of the PD Alive Check.
configure	pd-alive (disable|enable)	This command disables or enables the global PD Alive Check on the Switch.
Interface	pd-alive (disable|enable)	This command disables or enables the PD Alive Check on the interface.
Interface	pd-alive action (all|alarm|none|reboot)	This command configures the action when the system detects that the host cannot respond the keep-a-live probe packet. **All:** Send an alarm message to inform the administrator and then reboot the PD. **Alarm:** Send an alarm message to inform the administrator. **None:** Keep Ping the remote PD but does nothing further. **Reboot:** Cut off the power of the PoE port, make the PD rebooted..
Interface	pd-alive interval VALUE	This command configures the interval to send the keep-a-live probe packets to check if the host is still alive for the specific port.
Interface	pd-alive ip IP_ADDR	This command configures the Host IP address which connects to the specific port.
Interface	pd-alive power-off-time VALUE startup-time VALUE	This command configures the power-off time and startup time.
Interface	pd-alive retry-time VALUE	This command configures the retry times when no response from the host for the keep-a-live probe packet for the specific port.
enable	show snmp	This command displays the SNMP configurations.
configure	snmp (disable|enable)	This command disables/enables the SNMP on the switch.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	no snmp community	This command restores the snmp community to default.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	no snmp system-contact STRING	This command restores the system contact to default.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	no snmp system-location STRING	This command restores the system location to default.
configure	snmp system-name STRING	This command configures a name for the system. (The System Name is same as the host name, (up to 64 characters)
configure	no snmp system-name STRING	This command restores the system name string to default.
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver’s configurations, including the IP address, version (v1 or v2c) and community.

Table 81: CLI “PD Alive Check” Configuration

Node	Command	Description
configure	no snmp trap-receiver IPADDR	This command deletes the trap receiver’s configurations.

10.2.3.3 Storm Control

Table 82: CLI “Storm Control” Configuration

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

Example

L2SWITCH#*configure terminal*

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

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

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

10.2.3.4 VLAN

10.2.3.4.1 Port Isolation

Table 83: CLI “Port Isolation” Configuration

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

Example

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

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

10.2.3.4.2 VLAN Settings

Table 84: CLI “VLAN Settings” Configuration

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

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*vlan 2*

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

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

10.2.3.5 LLDP

Table 85: CLI “LLDP” Configuration

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

10.2.3.6 Loop Detection

Table 86: CLI “Loop Detection” Configuration

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

Example

L2SWITCH(config)#*loop-detection enable*

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

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

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

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

10.2.3.7 STP

Table 87: CLI “STP” Configuration

Node	Command	Description
enable	show spanning-tree active	This command only displays STP information for active ports.
enable	show spanning-tree blockedports	This command only displays STP information for blocked ports.
enable	show spanning-tree port detail PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree summary	This command displays a summary of port states and configurations.
enable	clear spanning-tree counters	This command clears the STP statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears the STP statistics for a specific port.
configure	spanning-tree (disable | enable)	This command disables/enables the STP function in the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (“Forward Delay,” “Max Age” and “Hello Time”).
configure	no spanning-tree algorithm-timer	This command configures the default values for “Forward Delay,” “Max Age” and “Hello Time.”
configure	spanning-tree forward-time <4–30>	This command configures the “Forward Delay” period (in seconds) for the bridge.
configure	no spanning-tree forward-time	This command configures the default values for “Forward Delay.”
configure	spanning-tree hello-time <1–10>	This command configures the “Hello Time” period (in seconds) for the bridge.
configure	no spanning-tree hello-time	This command configures the default values for the “Hello Time.”
configure	spanning-tree max-age <6-40>	This command configures the “Max Age” period (in seconds) for bridge messages.
configure	no spanning-tree max-age	This command configures the default values for the “Max Age.”
configure	spanning-tree mode (rstp | stp)	This command configures the STP mode.
configure	spanning-tree pathcost method (short | long)	This command configures the path cost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree bpdufilter (disable | enable)	This command configures enables/disables the “BPDU Filter” function.
interface	spanning-tree bpduguard (disable | enable)	This command configures enables/disables the “BPDU Guard” function.
interface	spanning-tree edge-port (disable | enable)	This command enables/disables the “Edge Port” setting.
interface	spanning-tree cost VALUE	This command configures the costs for the specific port. Cost range: 16-bit-based value range from 1 to 65,535, 32-bit-based value range from 1 to 200,000,000.
interface	no spanning-tree cost	This command sets the path cost of the specific port to the default value.

Table 87: CLI “STP” Configuration

Node	Command	Description
interface	spanning-tree port-priority <0-240>	This command configures the priority for the specific port (default value: 128).
interface	no spanning-tree port-priority	This command sets the priority of the specific port to the default value.

10.2.4 Security

10.2.4.1 Access Control List

Table 88: CLI “Access Control List” Configuration

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

10.2.5 Monitor

10.2.5.1 Alarm

Table 89: CLI “Alarm” Configuration

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

10.2.5.2 Monitor Information

Table 90: CLI “Monitor Information” Configuration

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

10.2.5.3 SFP Information

Table 91: CLI “SFP Information” Configuration

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

10.2.6 Management

10.2.6.1 SNMP

Table 92: CLI “SNMP” Configuration

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

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*snmp enable*

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

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

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

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

10.2.6.2 Maintenance

Table 93: CLI “Maintenance” Configuration

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

10.2.6.3 System Log

Table 94: CLI “System Log” Configuration

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

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config)#*syslog-server enable*

10.2.6.4 User Account

Table 95: CLI “System Log” Configuration

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

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*add user q admin*

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

10.3 Tabele Modbus/TCP

10.3.1 Format danych i kod funkcji

Modbus/TCP wspiera różne typy formatów danych do odczytu.
Najważniejsze 4 typy to:

Tabela 96: Format danych i kod funkcji

Typ dostępu do danych		Kod funkcji	Nazwa funkcji	Wskazówka
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Nieobsługiwane
	Internal Bits or Physical Coils	1	Read Coils	Nieobsługiwane
Word access (dostęp 16-bitowy)	Physical Input Registers	4	Read Input Registers	
	Physical Output	3	Read Holding Registers	Nieobsługiwane

10.4 Rejestry Modbus

Przestrzeń adresowa Modbus switcha zarządzalnego Lean rozpoczyna się od 1001 (dziesiętne) dla kodu funkcji 4.

Wskazówka

Przestrzeń adresowa Modbus®
Przestrzeń adresowa Modbus jest również wyświetlana w Web-Based-Management.

Tabela 97: Rejestry Modbus

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

1033	409	1032	408	16	ASCII	**Product Name = “852-1813_000-001”**
						Word 0 Hi byte = ‘8’ Word 0 Lo byte = ‘5’ Word 1 Hi byte = ‘2’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘8’ Word 3 Hi byte = ‘1’ Word 3 Lo byte = ‘3’ Word 4 Hi byte = ‘_’ Word 4 Lo byte = ‘0’ Word 5 Hi byte = ‘0’ Word 5 Lo byte = ‘0’ Word 6 Hi byte = ‘-’ Word 6 Lo byte = ‘0’ Word 7 Hi byte = ‘0’ Word 7 Lo byte = ‘1’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0
1065	429	1064	428	7	ASCII	**Product Serial Number**
						Ex: Serial No=A000000000001
1081	439	1080	438	12	ASCII	**Firmware Version=” V1.0.1.S0”**
						Word 0 Hi byte = ‘V’ Word 0 Lo byte = ‘1’ Word 1 Hi byte = ‘.’ Word 1 Lo byte = ‘0’ Word 2 Hi byte = ‘.’ Word 2 Lo byte = ‘1’ Word 3 Hi byte = ‘.’ Word 3 Lo byte = ‘S’ Word 4 Hi byte = ‘0’ Word 4 Lo byte = ‘\0’ Word 5 Hi byte = ‘\0’ Word 5 Lo byte = ‘\0’ Word 6 Hi byte = ‘\0’ Word 6 Lo byte = ‘\0’ Word 7 Hi byte = ‘\0’ Word 7 Lo byte = ‘\0’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0’
1097	449	1096	448	16	ASCII	Firmware Release Date="Mon Sep 30 18:51:45 2013"
1113	459	1112	458	3	HEX	**ETHERNET MAC Address**
						Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05

1129	469	1128	468	1	HEX	**Power 1 (PWR) Alarm**
						0x0000: no alarm 0x0003: No PWR input
1130	46A	1129	469	1	HEX	**Power 2(RPS) Alarm**
						0x0000: no alarm 0x0003: No RPS input
1145	479	1144	478	1	HEX	**Fault LED Status**
						0x0000: No 0x0001: Yes
Port Information						
				1	HEX	**Port 1 to 10 Link Status**
1257	4E9	1256	4E8			0x0000: Link down
1258	4EA	1257	4E9			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1259	4EB	1258	4EA			0x0002: 10M-Full-FC_OFF
1260	4EC	1259	4EB			0x0003: 10M-Half-FC_ON
1261	4ED	1260	4EC			0x0004: 10M-Half-FC_OFF
1262	4EE	1261	4ED			0x0005: 100M-Full-FC_ON
1263	4EF	1262	4EE			0x0006: 100M-Full-FC_OFF
1264	4F0	1263	4EF			0x0007: 100M-Half-FC_ON
1265	4F1	1264	4F0			0x0008: 100M-Half-FC_OFF
1266	4F2	1265	4F1			0x0009: 1000M-Full-FC_ON
						0x000A: 1000M-Full-FC_OFF 0x000B: 1000M-Half-FC_ON 0x000C: 1000M-Half-FC_OFF 0xFFFF: No port
				32	ASCII	**Port 1 to 12 Medium**
1513	5E9	1512	5E8			Port Description = “100TX, RJ45.” Or “1000TX, SFP.”
1545	609	1544	608			Word 0 Hi byte = ‘1’
1577	629	1576	628			Word 0 Lo byte = ‘0’
1609	649	1608	648			Word 1 Hi byte = ‘0’
1641	669	1640	668			Word 1 Lo byte = ‘T’
1673	689	1672	688			…
1705	6A9	1704	6A8			Word 4 Hi byte = ‘4’
1737	6C9	1736	6C8			Word 4 Lo byte = ‘5’
1769	6E9	1768	6E8			Word 5 Hi byte = ‘.’
1801	709	1800	708			Word 5 Lo byte = ‘\0’

				2	HEX	**Port 1 to 12 Tx Packets**
2025	7E9	2024	7E8			Ex: port 1 Tx Packet Amount = 0x87654321 Word 0 = 8765 Word 1 = 4321
2027	7EB	2026	7EA			
2029	7ED	2028	7EB			
2031	7EF	2030	7EE			
2033	7F1	2032	7F0			
2035	7F3	2034	7F2			
2037	7F5	2036	7F4			
2039	7F7	2038	7F6			
2041	7F9	2040	7F8			
2043	7FB	2042	7FA			
				2	HEX	**Port 1 to 12 Rx Packets**
2089	829	2088	828			Ex: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2091	82B	2090	82A			
2093	82D	2092	82C			
2095	82F	2094	82E			
2097	831	2096	830			
2099	833	2098	832			
2101	835	2100	834			
2103	837	2102	836			
2105	839	2104	838			
2107	83B	2106	83A			
				2	HEX	**Port 1 to 12 Tx Error Packets**
2153	869	2152	868			Ex: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
2155	86B	2154	86A			
2157	86D	2156	86C			
2159	86F	2158	86E			
2161	871	2160	870			
2163	873	2162	872			
2165	875	2164	874			
2167	877	2166	876			
2169	879	2168	878			
2171	87B	2170	87A			

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

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

Spis ilustracji

Ilustracja 1: Widok z przodu switcha zarządzalnego Lean 20
Ilustracja 2: Widok przemysłowego switcha zarządzalnego Lean z góry 22
Ilustracja 3: Śruba uziemienia 23
Ilustracja 4: Złącze zasilające (PWR/RPS) 24
Ilustracja 5: Złącza sieciowe 25
Ilustracja 6: LED urządzeń 27
Ilustracja 7: LED złącz 28
Ilustracja 8: Mikroprzełączniki DIP 29
Ilustracja 9: Naklejka 31
Ilustracja 10: Połączenie danych 01 40
Ilustracja 11: Połączenie danych 02 41
Ilustracja 12: Połączenie danych 03 41
Ilustracja 13: Połączenie danych 04 42
Ilustracja 14: Połączenie danych 05 42
Ilustracja 15: Dashboard (przykład) 45
Ilustracja 16: Panel diagnostyczny 46
Ilustracja 17: Obciążenie CPU 46
Ilustracja 18: Obciążenie pamięci 47
Ilustracja 19: Obciążenie portu nadawczego (przykład) 47
Ilustracja 20: Obciążenie portu odbiorczego (przykład) 48
Ilustracja 21: Szybkość broadcastu portu nadawczego 48
Ilustracja 22: Szybkość broadcastu portu odbiorczego 49
Ilustracja 23: Port PoE 49
Ilustracja 24: Statystyka rozłączeń portu (przykład) 50
Ilustracja 25: Informacje o LED 51
Ilustracja 26: Informacje o połączeniach dla każdego portu (przykład) 51
Ilustracja 27: Collapse, User Login, Topology Map 52
Ilustracja 28: Logowanie 52
Ilustracja 29: Tabela „Information” – menu „Device Status” 53
Ilustracja 30: Mapa topologii – przerwane połączenie na porcie 1 54
Ilustracja 31: Mapa topologii – połączenie niezarejestrowane 54
Ilustracja 32: Mapa topologii – informacje o połączeniu 55
Ilustracja 33: Zakładka „Information“ – menu „Device Status“ – „Device Details“ 62
Ilustracja 34: Zakładka „Information“ – menu „Device Status“ – „Network Details" 63
Ilustracja 35: Zakładka „Information“ – menu „Device Status“ – „Operating Time" 63
Ilustracja 36: Zakładka „Information“ – menu „Port Counter" 65
Ilustracja 37: Zakładka „Information“ – menu „Utilization Information" 66
Ilustracja 38: Zakładka „Configuration“ – menu „LLDP Settings“ 67
Ilustracja 39: Zakładka „Configuration“ – menu „LLDP Neighbor Information“ 68
Ilustracja 40: Zakładka „Configuration“ – menu „Manual Registration“ 69
Ilustracja 41: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Settings“ 72
Ilustracja 42: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Status“ 74

Ilustracja 43: Zakładka „Configuration“ – menu „Mirror“ – „Port Mirroring Settings“ 76
Ilustracja 44: Tryb half duplex....77
Ilustracja 45: Tryb full duplex....78
Ilustracja 46: Zakładka „Configuration“ – menu „Port Setup“ – „Port Setup“ 79
Ilustracja 47: Zakładka „Configuration“– menu „Port Setup“ – „Port Status“....81
Ilustracja 48: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Settings....83
Ilustracja 49: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Status“ 84
Ilustracja 50: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Settings“....85
Ilustracja 51: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Status“....86
Ilustracja 52: Zakładka „Configuration” – menu „PoE Settings” – „PD Alive Check Settings”....88
Ilustracja 53: Zakładka „Configuration“ – menu „PoE Settings“ – „PD Alive Check Status“ 90
Ilustracja 54: Zakładka „Configuration“ – menu „SNMP“ – „Event Settings“ – „Trap Event State Settings“ 92
Ilustracja 55: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“....94
Ilustracja 56: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“....95
Ilustracja 57: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Setup“ – „SNMP Setup“....96
Ilustracja 58: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“....98
Ilustracja 59: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 Group“....100
Ilustracja 60: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 User“ 102
Ilustracja 61: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 View“ 104
Ilustracja 62: Zakładka „Configuration“ – menu „System Management“ – „General Setup“ 107
Ilustracja 63: Zakładka „Configuration“ – menu „System Management“ – „SNTP“ 110
Ilustracja 64: Zakładka „Configuration“ – Menu „System Management“ – „User Account“....114
Ilustracja 65: Zakładka „Configuration“ – menu „Storm Control“ 117
Ilustracja 66: IEEE 802.1X 120
Ilustracja 67: Serwer RADIUS 120
Ilustracja 68: Zakładka „Security“ – menu „802.1X“ – „Global Setup“ 123
Ilustracja 69: Zakładka „Security“ – menu „802.1X“ – „Global Status“....126
Ilustracja 70: Zakładka „Security“ – menu „802.1X“ – „Port Setup“ 127
Ilustracja 71: Zakładka „Security“ – menu „802.1X“ – „Port Status“ 129
Ilustracja 72: Zakładka „Security” – menu „ACL” – „Access Control List Settings” 131
Ilustracja 73: Zakładka „Security” – menu „ACL” – „Access Control List Status” 133
Ilustracja 74: Zakładka „Security” – menu „Port Security” 135
Ilustracja 75: Zakładka „Security” – menu „Service Control” 137

Ilustracja 76: Zakładka „Security“ – menu „VLAN“ – „Port Isolation“ 140
Ilustracja 77: Zakładka „Security“ – menu „VLAN“ – „VLAN Setup“ 143
Ilustracja 78: Zakładka „Redundancy“ – menu „ERPS“.....148
Ilustracja 79: Zakładka „Redundancy“ – menu „STP/RSTP Setup“.....156
Ilustracja 80: Zakładka „Redundancy“ – menu „STP/RSTP Port Setup“ 158
Ilustracja 81: Zakładka „Diagnostic” – menu „Information”.....161
Ilustracja 82: Zakładka „Diagnostic” – menu „DIP Status”.....162
Ilustracja 83: Zakładka „Diagnostic” – menu „Traffic Flooding” 165
Ilustracja 84: Zakładka „Diagnostic” – menu „Port Utilization”.....168
Ilustracja 85: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Port Registration Learn”.....170
Ilustracja 86: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Port Link Down Statistics”.....171
Ilustracja 87: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Critical/Alert Threshold 01”.....172
Ilustracja 88: Zakładka „Diagnostic” – menu „Dashboard Configuration” – „Critical/Alert Threshold 02”.....173
Ilustracja 89: Zakładka „Diagnostic” – menu „Modbus” 174
Ilustracja 90: Zakładka „Diagnostic” – menu „System Log” 177
Ilustracja 91: Zakładka „Maintenance” – menu „Maintenance” – „Reboot” 179
Ilustracja 92: Zakładka „Maintenance” – zakładka „Reboot” – Message 179
Ilustracja 93: Zakładka „Maintenance” – menu „Maintenance” – „Upgrade Firmware”.....180
Ilustracja 94: Zakładka „Maintenance” – menu „Maintenance” – „Upload Configuration” 181
Ilustracja 95: Zakładka „Maintenance” – menu „Maintenance” – „Download Configuration” 182
Ilustracja 96: Zakładka „Maintenance” – menu „Maintenance” – „Reset Configuration” 183
Ilustracja 97: Zakładka „Maintenance“ – „Reset“ – Message 183

Spis tabel

Tabela 1: Zastosowane systemy liczbowe....10
Tabela 2: Sposoby zapisu....10
Tabela 3: Opis ilustracji „Widok z przodu switcha zarządzalnego Lean”....21
Tabela 4: Opis ilustracji „Widok przemysłowego switcha zarządzalnego Lean z góry”....22
Tabela 5: Opis ilustracji „Złącze zasilające (PWR/RPS)”....24
Tabela 6: Opis ilustracji „Złącza sieciowe”....25
Tabela 7: Opis ilustracjii „LED urządzeń“....27
Tabela 8: Opis ilustracji „LED złącz“....28
Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“....29
Tabela 10: Opis ilustracji „Naklejka“....31
Tabela 11: Dane techniczne – dane urządzenia....32
Tabela 12: Dane techniczne – dane systemowe....32
Tabela 13: Dane techniczne – Power over Ethernet (PoE)....32
Tabela 14: Dane techniczne – komunikacja....33
Tabela 15: Dane techniczne – Warunki środowiskowe....34
Tabela 16: Domyślne ustawienia dla portu Telnet....43
Tabela 17: Logowanie....52
Tabela 18: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM)....57
Tabela 19: Zakładka „Information“ – menu „Device Status“ – „Device Details"....62
Tabela 20: Zakładka „Information“ – menu „Device Status“ – „Network Details"....63
Tabela 21: Zakładka „Information“ – menu „Device Status“ – „Operating Time"....63
Tabela 22: Zakładka „Information“ – menu „Port Counter"....65
Tabela 23: Zakładka „Information“ – menu „Utilization Information"....66
Tabela 24: Zakładka „Configuration“ – menu „LLDP Settings“....67
Tabela 25: Zakładka „Configuration“ – menu „LLDP Neighbor Information“....68
Tabela 26: Zakładka „Configuration“ – menu „Manual Registration“....70
Tabela 27: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Settings“....73
Tabela 28: Zakładka „Configuration“ – menu „Loop Detection“ – „Configuration Status“....74
Tabela 29: Zakładka „Configuration“ – menu „Mirror“ – „Port Mirroring Settings“76
Tabela 30: Zakładka „Configuration“ – menu „Port Setup“ – „Port Setup“....80
Tabela 31: Zakładka „Configuration“– menu „Port Setup“ – „Port Status“....82
Tabela 32: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Settings“....83
Tabela 33: Zakładka „Configuration“ – menu „Port Priority“ – „Port Priority Status“....84
Tabela 34: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Settings“....85
Tabela 35: Zakładka „Configuration“ – menu „PoE Settings“ – „Power ON/OFF“ – „PoE Configuration Status“....86
Tabela 36: Zakładka „Configuration” – menu „PoE Settings” – „PD Alive Check Settings”....89
Tabela 37: Zakładka „Configuration“ – menu „PoE Settings“ – „PD Alive Check Status“....90

Tabela 38: Zakładka „Configuration“ – menu „SNMP“ – „Event Settings“ – „Trap Event State Settings“ 93
Tabela 39: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Settings“.....94
Tabela 40: Zakładka „Configuration“ – menu „SNMP“ – „Port Event Settings“ – „Port Link-Change Trap Status“.....95
Tabela 41: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Setup“ – „SNMP Setup“ 97
Tabela 42: Zakładka „Configuration“ – menu „SNMP“ – „SNMP Trap“ – „Trap Receiver Settings“.....99
Tabela 43: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 Group“ 101
Tabela 44: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 User“.....103
Tabela 45: Zakładka „Configuration“ – menu „SNMP“ – „SNMPv3 View“ 105
Tabela 46: Zakładka „Configuration“ – menu „System Management“ – „General Setup“ 108
Tabela 47: Zakładka „Configuration“ – menu „System Management“ – „SNTP“111
Tabela 48: Zakładka „Configuration“ – Menu „System Management“ – „User Account“.....115
Tabela 49: Zakładka „Configuration“ – menu „Storm Control“.....118
Tabela 50: Zakładka „Security“ – menu „802.1X“ – „Global Setup“.....124
Tabela 51: Zakładka „Security“ – menu „802.1X“ – „Global Status“.....126
Tabela 52: Zakładka „Security“ – menu „802.1X“ – „Port Setup“ 128
Tabela 53: Zakładka „Security“ – menu „802.1X“ – „Port Status“.....130
Tabela 54: Zakładka „Security” – menu „ACL” – „Access Control List Settings”132
Tabela 55: Zakładka „Security” – menu „ACL” – „Access Control List Status” ..133
Tabela 56: Zakładka „Security” – menu „Port Security” 136
Tabela 57: Zakładka „Security” – menu „Service Control” 138
Tabela 58: Zakładka „Security“ – menu „VLAN“ – „Port Isolation“ 141
Tabela 59: Zakładka „Security“ – menu „VLAN“ – „VLAN Setup“.....144
Tabela 60: Zakładka „Redundancy“ – menu „ERPS“.....149
Tabela 61: Koszty trasy STP.....153
Tabela 62: Zakładka „Redundancy“ – menu „STP/RSTP Setup“.....156
Tabela 63: Zakładka „Redundancy“ – menu „STP/RSTP Port Setup“.....159
Tabela 64: Zakładka „Diagnostic” – menu „Information” 161
Tabela 65: Zakładka „Diagnostic” – menu „DIP Status” 163
Tabela 66: Zakładka „Diagnostic” – menu „Traffic Flooding”.....166
Tabela 67: Zakładka „Diagnostic” – menu „Port Utilization” 169
Tabela 68: Format danych i kod funkcji 174
Tabela 69: Modbus 174
Tabela 70: Zakładka „Diagnostic” – menu „System Log” 178
Tabela 71: Przewód RJ-45.....184
Table 72: CLI “System Information” Configuration.....185
Table 73: CLI “System” Configuration 186
Table 74: CLI “Jumbo Frame” Configuration 187
Table 75: CLI “SNTP” Configuration.....188
Table 76: CLI “Management Host” Configuration 189
Table 77: CLI “MAC Management” Configuration.....190
Table 78: CLI “Port Mirroring” Configuration.....190
Table 79: CLI “Port Settings” Configuration 191
Table 80: CLI “PoE Settings” Configuration.....192

Table 81: CLI “PD Alive Check” Configuration....194
Table 82: CLI “Storm Control” Configuration....195
Table 83: CLI “Port Isolation” Configuration....196
Table 84: CLI “VLAN Settings” Configuration....197
Table 85: CLI “LLDP” Configuration....198
Table 86: CLI “Loop Detection” Configuration....199
Table 87: CLI “STP” Configuration....201
Table 88: CLI “Access Control List” Configuration....203
Table 89: CLI “Alarm” Configuration....204
Table 90: CLI “Monitor Information” Configuration....204
Table 91: CLI “SFP Information” Configuration....204
Table 92: CLI “SNMP” Configuration....205
Table 93: CLI “Maintenance” Configuration....206
Table 94: CLI “System Log” Configuration....206
Table 95: CLI “System Log” Configuration....207
Tabela 96: Format danych i kod funkcji....208
Tabela 97: Rejestry Modbus....208

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Faks: 0571/887 – 844169
e-mail: info@wago.com
Internet: www.wago.com