TECHDOCS

Podręcznik

Akcesoria WAGO ETHERNET 852



852-1605

Industrial-Managed-Switch

8 Ports 1000BASE-T, 4 x 1000BASE-SX/LX, PROFINET; EXT

Wersja 1.0.0

© 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 10
1.1 Zakres obowiązywania 10
1.2 Prawa autorskie 10
1.3 Symbole 11
1.4 Zastosowane systemy liczbowe 12
1.5 Sposoby zapisu 12

2 Ważne objaśnienia 13
2.1 Podstawy prawne 13
2.1.1 Zastrzeżenie prawa do zmian technicznych 13
2.1.2 Kwalifikacje personelu 13
2.1.3 Użytkowanie switcha przemysłowego zgodne z przeznaczeniem 13
2.1.4 Stan techniczny urządzeń 14
2.1.5 Dyrektywy i wymagania dla zastosowania switcha przemysłowego 14
2.2 Wskazówki dotyczące bezpieczeństwa 15
2.3 Specjalne warunki zastosowania urządzeń ETHERNET 17

3 Wprowadzenie 18
3.1 Zakres dostawy 18
3.2 Technologia sieci Industrial ETHERNET 18
3.3 PROFINET 19
3.4 Technologia switchingu 21
3.5 Autonegocjacja 21
3.6 Autocrossing 22
3.7 Tryb Store and Forward Switching 22
3.8 Metody transmisji 22

4 Opis urządzenia 23
4.1 Widok 24
4.1.1 Widok z przodu 24
4.1.2 Widok z góry 26
4.2 Złącza 27
4.2.1 Zasilanie (PWR/RPS) 27
4.2.2 Złącza sieciowe 28
4.2.2.1 Złącze RJ-45 29
4.2.2.2 Złącza 10/100/1000BASE-T 29
4.2.2.3 Złącza 1000BASE-SX/LX 29
4.3 Elementy sygnalizacyjne 30
4.3.1 LED urządzeń 30
4.3.2 LED złącz 31
4.4 Elementy obsługi 32
4.4.1 Mikroprzełączniki DIP 32
4.4.2 Przycisk resetu 33
4.5 Naklejka 34
4.6 Parametry techniczne 35
4.6.1 Dane urządzenia 35
4.6.2 Dane systemowe 35
4.6.3 Zasilanie 35

4.6.4 Komunikacja ..... **Błąd! Nie zdefiniowano zakładki.**
4.6.5 Warunki środowiskowe 37
4.7 Aprobaty 38

5 PROFINET 39

5.1 Przegląd systemu 39
5.1.1 Budowa 39
5.1.1.1 Klasy urządzeń 39
5.1.1.2 Model urządzenia dla I/O devices 40
5.2 Komunikacja 43
5.3 Transmisja danych 45
5.3.1 Komunikacja w czasie rzeczywistym 45
5.3.2 Metody transmisji 45
5.3.3 Rodzaje transmisji 45
5.3.4 Budowa telegramu 47
5.4 Adresowanie 48
5.4.1 Nazwa urządzenia 48
5.5 Klasy zgodności („Conformance Classes“) 49
5.6 Redundancja mediów 52
5.7 Protocols 54
5.8 Switch zarządzalny PROFINET 56
5.9 Plik GSDML 57
5.9.1 Wprowadzenie 57
5.9.2 Budowa pliku GSDML 58
5.9.3 Jednoznaczna identyfikacja IO devices 60
5.10 Projektowanie za pomocą pliku GSDML 61
5.10.1 Konfiguracja 61
5.10.1.1 Narzędzia projektowe (przegląd) 62
5.10.1.2 Ogólne podejście do projektowania systemu PROFINET 62
5.10.1.3 Załadowanie projektu do IO controllera. 65
5.10.2 Parametr 66
5.10.2.1 Obszar „General” 66
5.10.2.2 Obszar „PROFINET interface [X1]” 67
5.10.2.3 Obszar „Advanced options” 68
5.10.2.4 Obszar „Port 1” 70
5.10.2.5 Obszar „Port options” 71
5.10.2.6 Sekcja „Identification & Maintenance“ 72
5.10.2.7 Obszar „Process alarms“ 73
5.10.2.8 Obszar „Assembly parameters“ 74
5.10.2.9 Obszar „IO adresses“ 76
5.11 Cykliczne dane I/O 77
5.11.1 Przykład cyklicznych danych I/O 78
5.12 Parametry DAP 81
5.13 Dostęp przez port konsolowy (CLI) 85
5.13.1 Nadawanie adresu IP za pomocą portu konsolowego 85
5.14 Parametryzacja przez WBM w trybie PROFINET 89
5.14.1 System Status 92
5.14.1.1 System Information 92
5.14.2 General Settings 94
5.14.2.1 General Settings 94

5.14.2.1.1 System ... 94
5.14.2.2 Port Mirroring ... 96
5.14.2.3 Port Settings ... 98
5.14.3 PROFINET ... 99
5.14.3.1 PROFINET Setting ... 99
5.14.3.2 Information ... 100
5.14.3.3 Diagnostics List ... 101
5.14.4 Advanced Settings ... 102
5.14.4.1 MRP ... 102
5.14.5 Management ... 105
5.14.5.1 Upload File ... 105
5.14.5.1.1 User Account ... 105

6 Montaż ... 106

6.1 Miejsce montażu ... 106
6.2 Montaż na szynie ... 106
6.3 Demontaż z szyny ... 106

7 Podłączanie urządzeń ... 107

7.1 Zasilanie ... 107
7.2 Złącze zewnętrznego styku alarmowego ... 108
7.3 Złącze przewodu konsolowego ... 108
7.4 Porty 1000BASE-SX/LX, światłowód ... 109
7.5 Porty 10/100/1000BASE-T ... 110

8 Opis funkcji ... 111

8.1 General Settings ... 111
8.1.1 Jumbo Frame ... 111
8.1.2 SNTP ... 111
8.1.3 Management Host ... 112
8.1.4 MAC Management ... 112
8.1.4.1 Static MAC ... 113
8.1.5 Port Mirroring ... 114
8.1.6 Port Settings ... 114
8.2 Advanced Settings ... 118
8.2.1 Bandwidth Control ... 118
8.2.1.1 QoS ... 118
8.2.1.2 Rate Limitation ... 125
8.2.1.2.1 Storm Control ... 125
8.2.1.2.2 Rate Limitation ... 125
8.2.2 IGMP Snooping ... 126
8.2.2.1 Multicast Address ... 129
8.2.3 VLAN ... 132
8.2.3.1 Port Isolation ... 133
8.2.4 LLDP ... 135
8.2.5 MAC based VLAN ... 135
8.2.6 Loop Detection ... 136
8.2.7 STP ... 137
8.3 Security ... 143
8.3.1 Access Control List ... 143
8.4 Monitor ... 144

8.4.1 Alarm 144
8.4.2 Monitor Informations 144
8.4.3 RMON Statistics 144
8.4.4 SFP 144
8.4.4.1 SFP Information 145
8.4.5 Traffic Monitor 145
8.5 Management 146
8.5.1 SNMP 146
8.5.1.1 SNMP Trap 147

9 Konfiguracja 148

9.1 Przegląd opcji konfiguracji 148
9.1.1 Port Telnet 149
9.2 Port konsolowy 150

10 System Web Based Management (WBM) 151

10.1 System Status 154
10.1.1 System Information 154
10.2 General Settings 156
10.2.1 General Settings 156
10.2.1.1 System 156
10.2.1.2 Jumbo Frame 158
10.2.1.3 SNTP 159
10.2.1.4 Management Host 162
10.2.2 MAC Management 163
10.2.2.1 Static MAC Settings 163
10.2.2.2 MAC Table 165
10.2.2.3 Age Time Setting 166
10.2.2.4 Blacklisting 167
10.2.3 Port Mirroring 168
10.2.4 Port Settings 170
10.2.4.1 General Settings 170
10.2.4.2 Information 172
10.3 PROFINET 172
10.4 Advanced Settings 173
10.4.1 Bandwidth Control 173
10.4.1.1 QoS 173
10.4.1.1.1 Port Priority 173
10.4.1.1.2 IP DiffServ (DSCP) 174
10.4.1.1.3 Priority/Queue Mapping 175
10.4.1.1.4 Schedule Mode 176
10.4.1.2 Bandwidth Limitation 178
10.4.1.2.1 Storm Control 178
10.4.1.2.2 Bandwidth Limitation 180
10.4.2 IGMP-Snooping 181
10.4.2.1 IGMP-Snooping 181
10.4.2.1.1 General Settings 181
10.4.2.1.2 Port Settings 183
10.4.2.1.3 Querier Settings 185
10.4.2.2 IGMP Filtering 186
10.4.2.2.1 General Settings 186

10.4.2.2.2 Multicast Groups 187
10.4.2.2.3 Port Settings 188
10.4.2.3 Static Multicast 189
10.4.2.4 Multicast Statistics 190
10.4.3 VLAN 191
10.4.3.1 Port Isolation 191
10.4.3.2 VLAN 193
10.4.3.2.1 VLAN Settings 193
10.4.3.2.2 Tag Settings 195
10.4.3.2.3 Port Settings 196
10.4.3.3 MAC VLAN 198
10.4.4 LLDP 199
10.4.4.1 Settings 199
10.4.4.2 Neighboring Detection 201
10.4.5 Loop Detection 202
10.4.6 MRP 204
10.4.7 Spanning Tree Protocol 207
10.4.7.1 General Settings 207
10.4.7.2 Port Parameters 209
10.4.7.3 STP Status 212
10.5 Security 213
10.5.1 Access Control List 213
10.6 Monitor 217
10.6.1 Alarm Information 217
10.6.2 System Information 218
10.6.3 Port Statistics 220
10.6.4 Port Utilization 221
10.6.5 RMON Statistics 222
10.6.6 SFP Information 225
10.6.7 Traffic Monitor 228
10.7 Management 230
10.7.1 SNMP 230
10.7.1.1 SNMP 230
10.7.1.1.1 SNMP Settings 230
10.7.1.1.2 Community Name 231
10.7.1.2 SNMP Trap 233
10.7.1.2.1 Trap Receiver Settings 233
10.7.1.2.2 Trap Event State 234
10.7.1.2.3 Port Trap Settings 235
10.7.1.3 SNMPv3 Configuration 236
10.7.1.3.1 SNMPv3 User 236
10.7.1.3.2 SNMPv3 Group 238
10.7.1.3.3 SNMPv3 View 239
10.7.2 Maintenance 240
10.7.2.1 Configuration 240
10.7.2.2 Firmware 242
10.7.2.3 Reboot 243
10.7.2.4 Protocols 244
10.7.3 System Log 246
10.7.4 Upload File 248

10.7.5 Ping 249
10.7.6 User Account 250

11 Załącznik 252

11.1 Przewód konsolowy (RJ-45 do DB9) 252
11.2 Przewód RJ-45 253
11.3 Configuring in the Command Line Interface (CLI) (dostęp przez konsolę (CLI)) 254
11.3.1 System Status 254
11.3.1.1 System Information 254
11.3.2 Basic Settings 255
11.3.2.1 System 255
11.3.2.1.1 Jumbo Frame 256
11.3.2.1.2 SNTP 256
11.3.2.1.3 Management Host 257
11.3.2.2 MAC Management 258
11.3.2.3 Port Mirroring 258
11.3.2.4 Port Settings 259
11.3.3 Advanced Settings 260
11.3.3.1 Bandwidth Control 260
11.3.3.1.1 QoS 260
11.3.3.1.2 Rate Limitation 261
11.3.3.1.2.1 Storm Control 261
11.3.3.2 IGMP Snooping 262
11.3.3.2.1 IGMP Snooping Querier♠ 265
11.3.3.2.2 IGMP Snooping Filtering 265
11.3.3.3 Multicast Address 266
11.3.3.4 VLAN 266
11.3.3.4.1 Port Isolation 266
11.3.3.4.2 VLAN Settings 267
11.3.3.4.3 MAC VLAN 269
11.3.3.5 LLDP 270
11.3.3.6 Loop Detection 271
11.3.3.7 MRP 272
11.3.3.8 STP 273
11.3.4 Security 276
11.3.4.1 Access Control List 276
11.3.5 Monitor 279
11.3.5.1 Alarm 279
11.3.5.2 Monitor Information 279
11.3.5.3 Port Statistics 279
11.3.5.4 Port Utilization 279
11.3.5.5 RMON Statistics 279
11.3.5.6 SFP Information 279
11.3.5.7 Traffic Monitor 280
11.3.6 Management 281
11.3.6.1 SNMP 281
11.3.6.1.1 SNMP 281
11.3.6.1.2 SNMP Trap 282
11.3.6.1.2.1 Port Trap Settings 282

11.3.6.1.3 SNMPv3 283
11.3.6.2 Maintenance 284
11.3.6.2.1 Reboot 284
11.3.6.3 System Log 285
11.3.6.4 User Account 285

Spis ilustracji 286

Spis tabel 289

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 „Industrial-Managed-Switch“ (852-1605).

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 danego urządzenia/układu.

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.
- Aby zredukować niebezpieczeństwo cyberataku i tym samym zwiększyć cyberbezpieczeństwo, wszystkie porty i usługi w komponentach systemu sterowania, które nie są wykorzystywane przez aplikację (np. dla WAGO-I/O-CHECK i CODESYS) należy zamykać. Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.
- 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 z gniazdem
- Zaślepki ochronne dla niewykorzystanych złącz
- Przewód danych RS-232 dla CLI

3.2 Technologia sieci Industrial ETHERNET

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

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3z
- IEEE 802.3x
- IEEE 802.1d
- IEEE 802.1w
- IEEE 802.1s
- IEEE 802.1Q
- IEEE 802.1p
- IEEE 802.1ab
- PROFINET®

Switche umożliwiają zasilanie w zakresie napięcia 12 V ... 60 V.

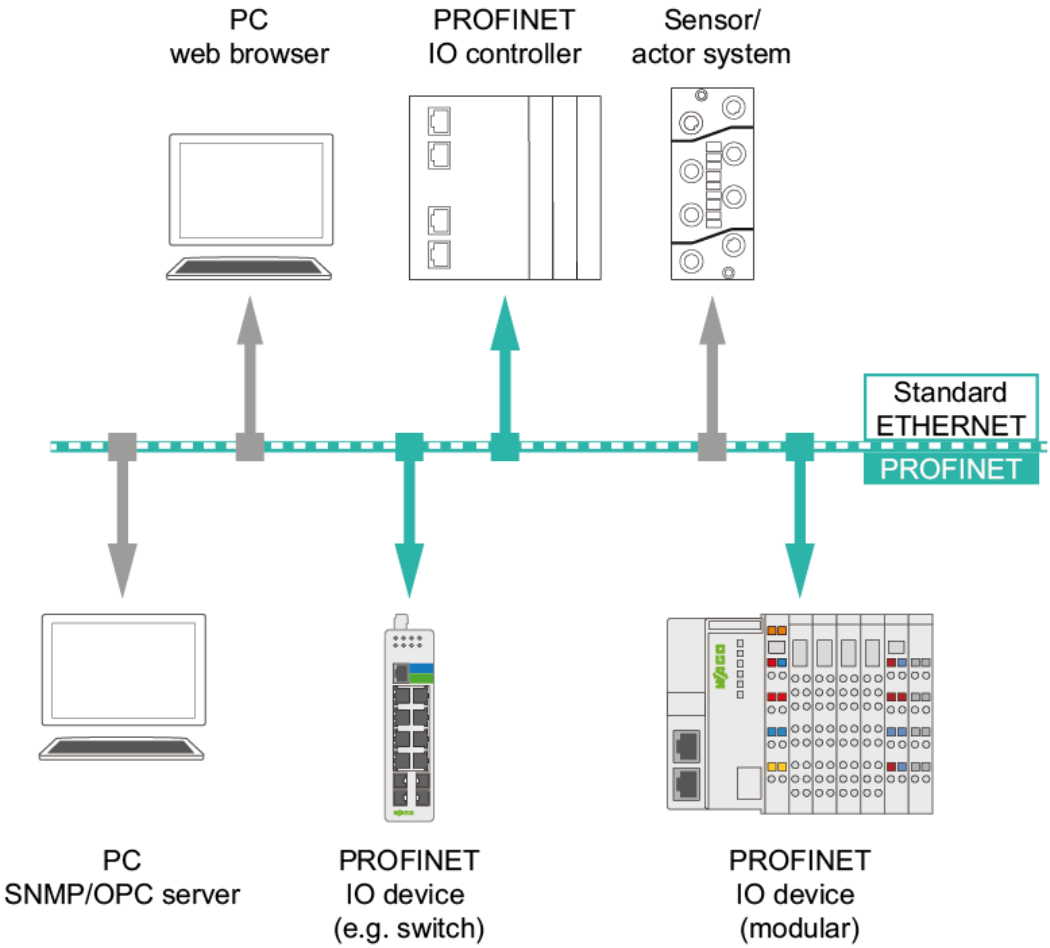
Inne funkcjonalności to autonegocjacja i Auto-MDI/MDIX (crossover) na wszystkich portach 10/100/1000 BASE-T.

3.3 PROFINET

System komunikacji ETHERNET czasu rzeczywistego PROFINET jest jednym z najbardziej elastycznych i rozpowszechnionych systemów sieci obiektowej w technice automatyki. Dzięki globalnej obecności rynkowej PROFINET jest w wielu branżach znany i akceptowany. Producenci i użytkownicy są zrzeszeni na całym świecie w organizacji PROFIBUS & PROFINET International (PI).

PROFINET jest uważany za następcę konwencjonalnej sieci obiektowej PROFIBUS i dlatego jest często wybierany, gdy komunikacja przełączana jest z konwencjonalnych sieci obiektowych na system sieci obiektowej na bazie ETHERNET. Pod względem technicznym PROFINET oferuje szereg zalet, które w zależności od wymagań środowiska aplikacyjnego mogą przesądzać o wyborze tego systemu sieci obiektowej. Również z powodu tych zalet PROFINET może być stosowany w najróżniejszych branżach.

PROFINET umożliwia łączenie standardowych urządzeń sieci ETHERNET i urządzeń pracujących w czasie rzeczywistym w jednej sieci. Dzięki funkcjonalności PROFINET komunikacja w sieci obiektowej nie koliduje ze standardową komunikację na bazie TCP/IP. Ta elastyczność stanowi ogromną przewagę nad innymi systemami czasu rzeczywistego ETHERNET, w których standardowe urządzenia IT mogą nie być zintegrowane z siecią w ogóle lub tylko w wyznaczonych punktach, albo są uwzględniane w komunikacji tylko podczas bieżącej pracy sterownika. Na ilustracji „Równoległe korzystanie ze standardu ETHERNET i PROFINET” przedstawiono schematycznie to równoległe wykorzystanie tego samego fizycznego połączenia.



Ilustracja 1: Równoległe korzystanie ze standardu ETHERNET i PROFINET

W PROFINET następuje rozdzielenie urządzeń z funkcjonalnością czasu rzeczywistego i bez tej funkcjonalności. To rozdzielenie przebiega różnie w zależności od klasy czasu rzeczywistego (RT_Class):

- Przy RT_Class_1 rozdzielenie odbywa się poprzez priorytetyzację telegramów czasu rzeczywistego za pomocą VLAN.
- Przy RT_Class_3 rozdzielenie odbywa się za pomocą specjalnych switchy PROFINET, które dokonują rezerwacji przepustowości dla telegramów czasu rzeczywistego.

Takie rozdzielenie urządzeń z funkcjonalnością czasu rzeczywistego i bez niej zapewnia, że każde standardowe urządzenie IT może być używane w dowolnym miejscu sieci PROFINET bez konieczności stosowania specjalnych środków do fizycznego podłączania.

Do każdego interfejsu w sieci automatyki można podłączyć dowolne urządzenie obsługujące ETHERNET. W przypadku RT_Class_1 należy przy tym uwzględnić dopuszczalne obciążenie sieci wynikające ze standardowego ruchu danych.

Z dowolnego interfejsu w sieci automatyki można przeprowadzić diagnostykę za pomocą komputera PC, bez względu na stan pracy systemu automatyki. Funkcja

ta umożliwia optymalne fizyczne dostosowanie struktury sieci do istniejących warunków oraz funkcjonowanie bez ograniczeń wynikających z topologii:

- topologia pierścienia (tylko w przypadku korzystania z protokołu redundancji mediów, np. MRP)
- topologia liniowa
- topologia gwiazdy
- sieć kratowa

W wielu przypadkach możliwe jest również przyłączenie wcześniej wyodrębnionych sieci, o ile uwzględni się dopuszczalne obciążenie sieci.

3.4 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.

3.5 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 rozprzestrzeniania 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

852-1605 to przemysłowy, konfigurowalny switch ETHERNET z 8 miedzianymi portami 10/100/1000BASE-T i 4 slotami SFP-1000BASE-SX/LX. Odpowiednie moduły SFP są dostępne opcjonalnie.

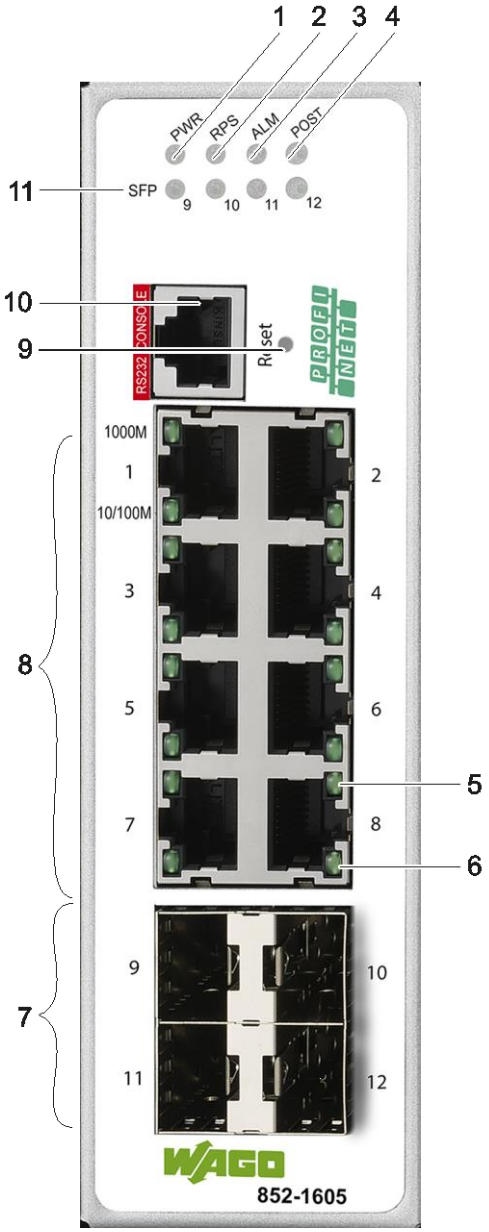
Switch posiada m.in. następujące cechy:

- odporna obudowa
- redundantne zasilanie
- monitorowanie funkcji za pomocą przekaźnika

Łatwa integracja z systemem automatyki odbywa się za pomocą pliku opisu urządzenia PROFINET (GSD).

4.1 Widok

4.1.1 Widok z przodu



Ilustracja 2: Widok przemysłowego switcha zarządzalnego z przodu

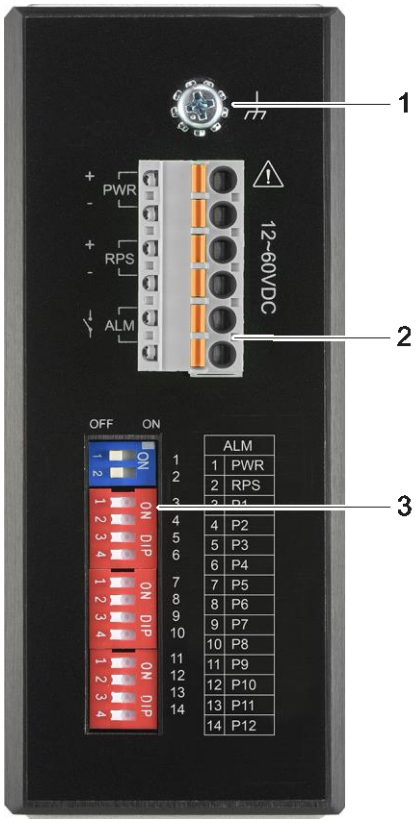
Tabela 3: Opis do ilustracji „Widok przemysłowego switcha zarządzalnego z przodu”

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
1	PWR	LED statusu napięcia zasilania	„Opis urządzenia“ > „Elementy sygnalizacyjne“
2	RPS	LED statusu zasilania redundantnego	„Opis urządzenia“ > „Elementy sygnalizacyjne“
3	ALM	LED statusu alarmu	„Opis urządzenia“ > „Elementy sygnalizacyjne“
4	POST	LED statusu POST	„Opis urządzenia“ > „Elementy sygnalizacyjne“

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

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
5	-	LED statusu T-Port – 1000-Mb/s (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
6	-	LED statusu T-Port – 10/100-Mb/s (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
7	-	Złącze 4 x SFP (1000BASE-SX/LX, światłowód)	„Opis urządzenia“ > „Złącza“
8	-	Złącze 8 x RJ-45 (10/100/1000BASE-T)	„Opis urządzenia“ > „Złącza“
9	Reset	Przycisk resetu	„Opis urządzenia“ > „Elementy obsługi“
10	-	Złącze 1 x RJ-45 (RS-232)	„Opis urządzenia“ > „Złącza“
11	SFP	LED statusu portu SFP LNK/ACT (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“

4.1.2 Widok z góry



Ilustracja 3: Widok przemysłowego switcha zarządzalnego z góry

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

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

4.2 Złącza

4.2.1 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	Objaśnienie	Opis
+	PWR	Podstawowe zasilanie prądem stałym
-	PWR	Podstawowe zasilanie prądem stałym
+	RPS	Rezerwowe zasilanie prądem stałym
-	RPS	Rezerwowe zasilanie prądem stałym
	HW ALM	Styk dla zewnętrznego alarmu
	HW ALM	Styk dla zewnętrznego alarmu

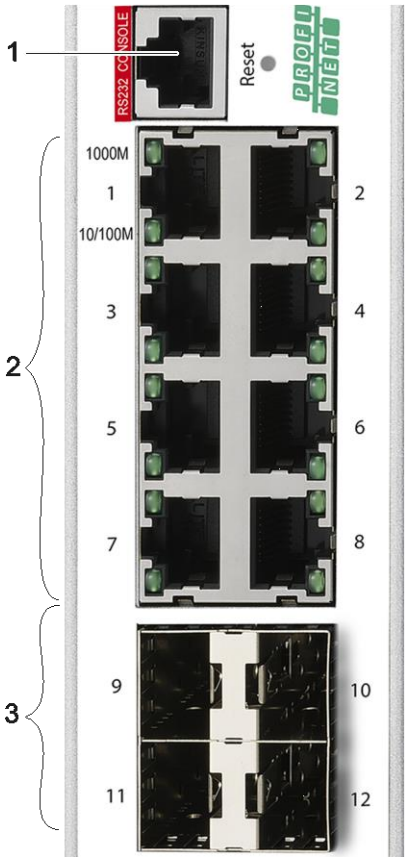
ESD



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.

4.2.2 Złącza sieciowe

Przemysłowy switch zarządzalny wykorzystuje złącza z wtykami światłowodowymi lub miedzianymi i obsługuje ETHERNET, Fast-ETHERNET oraz Gigabit Ethernet.



Ilustracja 5: Złącza sieciowe

Tabela 6: Opis ilustracji „Złącza sieciowe”

Poz.	Nazwa	Znaczenie	Szczegóły – patrz rozdział
1	-	Złącze 1 x RJ-45 (port RS-232)	„Opis urządzenia“ > … > „Złącze RJ-45“
2	-	Złącze 8 x RJ-45 (10/100/1000BASE-T)	„Opis urządzenia“ > … „Złącza 10/100/1000BASE-T“
3	-	Złącze 4 x SFP (1000BASE-SX/LX, światłowód)	„Opis urządzenia“ > … „Złącza 1000BASE-SX/-LX“

4.2.2.1 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).

4.2.2.2 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

4.2.2.3 Złącza 1000BASE-SX/LX

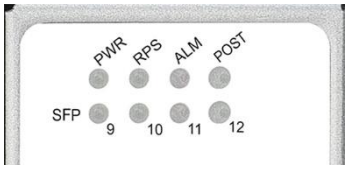
Złącza 1000BASE-SX/-LX przeznaczone są do podłączania modułów Gigabit SFP, wspierających prędkość transmisji 1000 Mbit/s.

4.3 Elementy sygnalizacyjne

Przemysłowy switch zarządzalny wyposażony jest we wskaźniki LED dla urządzeń i złącz.

4.3.1 LED urządzeń

Na podstawie LED urządzenia można szybko rozpoznać status switcha.



Ilustracja 6: LED urządzeń

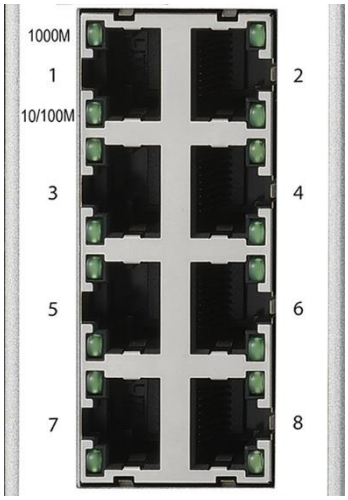
Tabela 7: Opis ilustracji „LED urządzeń“

LED		Nazwa	Status	Opis
PWR		Primary-Power-LED	zielony	Przemysłowy switch zarządzalny wykorzystuje zasilacz podstawowy.
			Off	Zasilacz podstawowy jest wyłączony lub wykazuje błąd.
RPS		Redundant-Power-System-LED	zielony	Przemysłowy switch zarządzalny wykorzystuje zasilacz rezerwowy.
			Off	Zasilacz rezerwowy jest wyłączony lub wykazuje błąd.
ALM [1)]		Alarm-LED	czerwony	Awaria połączenia, inny alarm; styk alarmowy zostaje aktywowany.
			Off	Alarm nie jest zgłaszany.
ALM [2)]		Alarm-LED	czerwony	Wystąpił błąd PROFINET.
			miga	Brak „Application Relation”
			Off	Alarm nie jest zgłaszany.
POST		Power-On-Self-Test-LED	zielony	Switch jest gotowy do pracy lub pracuje.
			Off	Switch nie jest gotowy do pracy.
SFP	9 … 12	SFP-Port-LED	zielony	Świeci, gdy złącze jest połączone.
			miga	Przez złącze transmitowane są dane.
			Off	Brak nawiązanego ważnego połączenia ze złączem

[1)] Tryb PROFINET nieaktywny
[2)] Tryb PROFINET aktywny; styk alarmowy nie jest sterowany przez diagnostykę PROFINET.

4.3.2 LED złącz

LED złącz natomiast informują o procesach łączeniowych.



Ilustracja 7: LED dla złącz RJ-45

Tabela 8: Opis ilustracji „LED dla złącz RJ-45”

LED	Nazwa	Status	Opis
1000M	LED portów 1000BASE-T (1 LED dla każdego złącza)	zielony	Złącze pracuje z prędkością 1000 Mbit/s.
		miga	Przez złącze transmitowane są dane.
		Off	Brak nawiązanego ważnego połączenia ze złączem
10/100M	LED portów 10/100BASE-T (1 LED dla każdego złącza)	zielony	Złącze pracuje z prędkością 10/100 Mbit/s.
		miga	Przez złącze transmitowane są dane.
		Off	Brak nawiązanego ważnego połączenia ze złączem

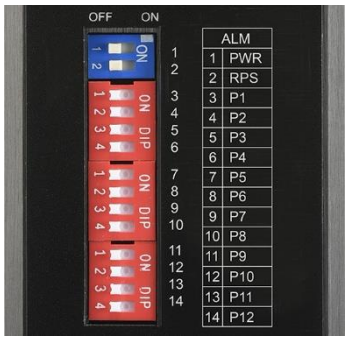
4.4 Elementy obsługi

4.4.1 Mikroprzełączniki DIP

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

Jeśli tryb PROFINET nie jest aktywny, po włączeniu funkcji alarmu dodatkowo wyświetlana jest informacja przez LED urządzenia „ALM” (zob. rozdział „Elementy sygnalizacyjne”).

Znaczenie ustawień mikroprzełączników DIP objaśniono poniżej.



Ilustracja 8: Mikroprzełączniki DIP

Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“

No.	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	P1	ON	Funkcja alarmu przy błędzie połączenia dla portu 1 jest aktywowana.
		OFF	Funkcja alarmu przy błędzie połączenia dla portu 1 jest dezaktywowana.
...			
10	P8	ON	Funkcja alarmu przy błędzie połączenia dla portu 8 jest aktywowana.
		OFF	Funkcja alarmu przy błędzie połączenia dla portu 8 jest dezaktywowana.
11	P9	ON	Funkcja alarmu przy błędzie połączenia dla portu 9 (SFP) jest aktywowana.
		OFF	Funkcja alarmu przy błędzie połączenia dla portu 9 (SFP) jest dezaktywowana.

Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“

No.	Nazwa	Status	Opis
…			
14	P12	ON	Funkcja alarmu przy błędzie połączenia dla portu 12 (SFP) jest aktywowana.
		OFF	Funkcja alarmu przy błędzie połączenia dla portu 12 (SFP) jest dezaktywowana.

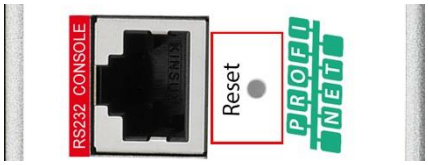
Użytkownik może ręcznie włączać i wyłączać funkcję alarmu zarówno dla każdego złącza, jak i dla zasilania podstawowego lub redundantnego przy użyciu mikroprzełączników DIP.

Aby móc aktywować odpowiednią 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. Ustaw mikroprzełącznik DIP w pozycji „OFF“.
2. Zainstaluj przemysłowy switch zarządzalny w sieci.
3. Wybierz port, który ma być monitorowany lub który ma aktywować alarm. Możliwy jest wybór wielokrotny.
4. Ustaw mikroprzełącznik DIP danego złącza w pozycji „ON“.
5. Włącz przemysłowy switch zarządzalny.

4.4.2 Przycisk resetu



Ilustracja 9: Przycisk resetu

Tabela 10: Opis ilustracji „Przycisk resetu“

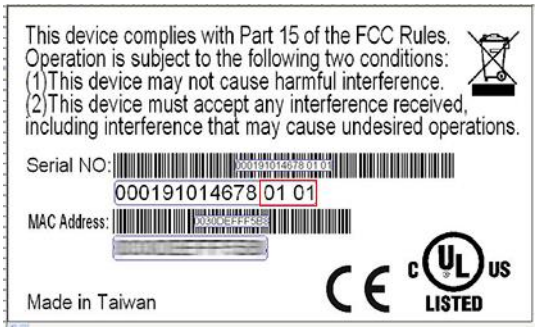
Nazwa	Status	Opis
Reset	Przycisk resetu należy nacisnąć na 2 sekundy, a następnie puścić.	System zostaje ponownie uruchomiony.

Wskazówka

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

4.5 Naklejka

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



Ilustracja 10: Naklejka (przykład)

Tabela 11: Opis ilustracji „Naklejka (przykład)“

No.	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 12: Dane techniczne – dane urządzenia

szerokość	50 mm
wysokość	162 mm (od górnej krawędzi szyny montażowej)
głębokość	120 mm
masa	945 g
stopień ochrony	IP30

4.6.2 Dane systemowe

Tabela 13: Dane techniczne – dane systemowe

Tabela MAC	do 16000 adresów
VLAN	Port-based i Tag-based (4094 VIDs)
Jumbo Frame Size	10240 B
Długość fali (światłowód)	zależnie od modułu SFP
Maksymalne odległości	10/100/ 1000BASE-T: 100 m; Włókno szklane: 2 … 80 km RS-232: 15 m

4.6.3 Zasilanie

Tabela 14: Dane techniczne – zasilanie

Napięcie zasilania	12 … 60 V DC
Maks. pobór mocy	18 W

4.6.4 Komunikacja

Tabela 15: Dane techniczne – komunikacja

Konfiguracja i update	1 x host USB 2.0
Porty (miedź; RJ-45)	8 x 10/100/1000BASE-T 1 x RS-232
Porty (światłowód)	4 x 1000BASE-SX/-LX
Standardy	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/-FX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Class of Service IEEE 802.1ab Link Layer Discovery Protocol (LLDP) PROFINET CC-B
Zarządzanie siecią	• CLI przez port konsoli, Telnet i SSH • Port RJ-45 do lokalnego zarządzania • Zarządzanie przez stronę WWW • Wyświetlanie stanu i raportowanie zdarzeń przez stronę WWW • Zarządzanie portami • Autonegocjacja • Tryb dupleks • 802.3x Flow Control • Obsługa Jumbo Frame • Zarządzanie SNMP v1 i v2c • SNMP Trap • Link UP/Down • Zmiana konfiguracji • Zimny start • Gorący start • Wysyłanie trapów: 5 celów • Zapewnienie zarządzania błędami, wydajnością, konfiguracją i bezpieczeństwem • RMON: 4 grupy RMON 1, 2, 3, 9 (przebieg, statystyka, alarmy i zdarzenia) dla ulepszenia zarządzania ruchem, monitorowania i analizy

Bezpieczeństwo sieci	• ACL
	  • Uwierzytelnianie dostępu do sieci na bazie portu
	  • Uwierzytelnienie dostępu do sieci na bazie adresu MAC
	• Bezpieczeństwo SNMP v3
	• SSH
	• Uwierzytelnienie przez stronę WWW

4.6.5 Warunki środowiskowe

Tabela 16: Dane techniczne – Warunki środowiskowe

Temperatura otoczenia, praca	-40 … +70°C
Temperatura otoczenia, przechowywanie	-40 … +80 °C
Wilgotność względna (bez kondensacji)	10 … 95%
Odporność na wibracje zgodnie z	EN 60068-2-6
Odporność na wstrząsy zgodnie z	EN 60068-2-27
EMC: odporność na zakłócenia zgodnie z	EN 55024 EN 61000-6-2 EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8
EMC: norma emisji zgodnie z	FCC Part 15 EN 55022: klasa A EN 55011: klasa A EN 61000-6-4

4.7 Aprobaty

Aprobaty dla osprzętu WAGO-ETHERNET „Industrial-Managed-Switch“ (852-1605):

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

5 PROFINET

5.1 Przegląd systemu

5.1.1 Budowa

5.1.1.1 Klasy urządzeń

Wymiana danych procesowych w PROFINET IO odbywa się zgodnie z modelem Provider–Consumer:

- „Provider“ tworzą dane i wysyłają je w telegramach danych bez konkretnego żądania.
- „Consumer“ odbierają dane i je przetwarzają.

Tabela 17: Przykłady Provider i Consumer

Dane	Provider	Consumer
Dane procesowe (wejścia)	IO devices	IO controller
Dane procesowe (wyjścia)	IO controller	IO devices
Dane parametryczne	IO controller	IO devices

PROFINET IO definiuje następujące klasy urządzeń (zobacz także ilustrację „Klasy urządzeń w PROFINET IO”):

- **IO controller**:
  IO controller jest częścią nadrzędnego PLC („**P**rogrammable **L**ogic **C**ontroller“), w którym działa program automatyki i który przetwarza przychodzące dane procesowe i diagnostyczne. IO controller jest dostawcą (Provider) danych wyjściowych i danych parametrycznych oraz odbiorcą (Consumer) danych wejściowych urządzeń I/O.

- **IO device:**
  I/O device to rozproszone urządzenie obiektowe, które przez PROFINET IO jest podłączane do jednego lub kilku IO controller. I/O device jest dostawcą (Provider) danych wejściowych i odbiorcą (Consumer) danych wyjściowych oraz danych parametrycznych.
  Switche PROFINET firmy WAGO są I/O devices.

- **I device:**
  I device to inteligentne urządzenie I/O z zintegrowaną jednostką sterującą (np. zintegrowany PLC), które może przejmować funkcje wstępnego przetwarzania (np. systemy I/O). I device jest dostawcą (Provider) danych wejściowych i odbiorcą (Consumer) danych wyjściowych oraz danych parametrycznych.

- **IO supervisor:**
  IO supervisor (np. stacja inżynierska) jest PD („**P**rogramming **D**evice“), komputerem PC lub HMI („**H**uman **M**achine **I**nterface“) do uruchamiania lub

diagnostyki. IO supervisor jest często używany tylko tymczasowo do projektowania sieci i do konfiguracji IO controller.

W systemie PROFINET IO zawsze znajdują się co najmniej 1 IO controller i 1 lub kilka I/O devices. IO supervisor jest zazwyczaj angażowany tylko tymczasowo podczas uruchomienia i diagnostyki.

5.1.1.2 Model urządzenia dla I/O devices

PROFINET obsługuje I/O devices w następujących wariantach:

- Kompaktowe urządzenia obiektowe:
  Stopień rozbudowy jest w stanie dostawy już ustalony i nie może być zmieniony przez użytkownika.

- Modularne urządzenia obiektowe:
  Stopień rozbudowy może być podczas projektowania instalacji dostosowany indywidualnie do zastosowania.

Do opisu technicznych i funkcjonalnych możliwości I/O devices służy model urządzenia. Ten model urządzenia określony jest w pliku GSDML przez DAP („**D**evice **A**ccess **P**oint“) dla danej rodziny urządzeń. DAP jest punktem dostępu dla komunikacji urządzenia obiektowego z interfejsem ETHERNET i programem automatyki.

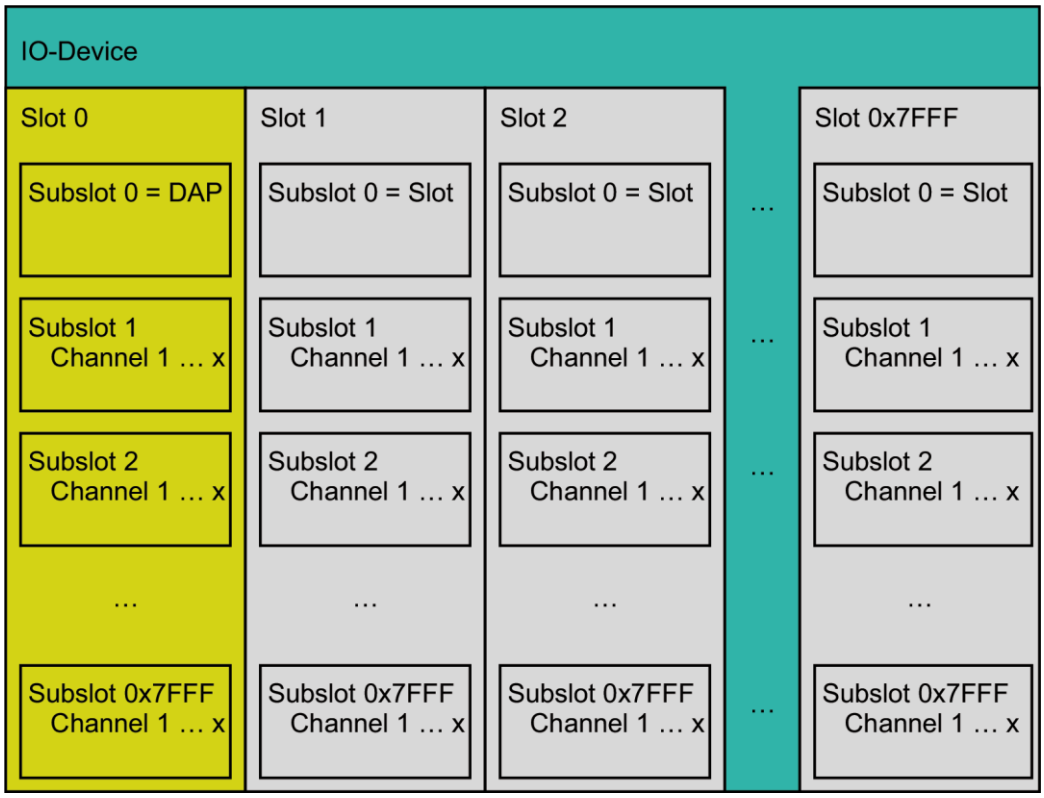
Dla modelu urządzenia I/O device znormalizowane są następujące struktury:

- **DAP** oznacza I/O device jako jednostkę.

- **Slot** oznacza fizyczne gniazdo modułu I/O w modularnym I/O device. Sloty służą do adresowania projektowanych modułów. Te moduły zawierają z kolei 1 lub kilka subslotów do wymiany danych.

- **Subsloty** w obrębie slotu tworzą właściwy interfejs do wejść i wyjść i tym samym do procesu. Granularność subslota, a tym samym podział danych I/O, jest specyficzna dla producenta. Zawartość danych subslota jest zawsze opatrzona informacją statusową, która określa ważność danych. Każdy slot musi zawierać co najmniej 1 subslot.

- **Index** dotyczy tylko wymiany danych acyklicznych. Indeks określa dane, które można zapisywać lub odczytywać w obrębie slotu lub subslotu. Określone indeksy są zdefiniowane przez normy. Pozostałe indeksy mogą być definiowane przez producenta.



Ilustracja 11: Adresowanie danych I/O device przez sloty i subsloty

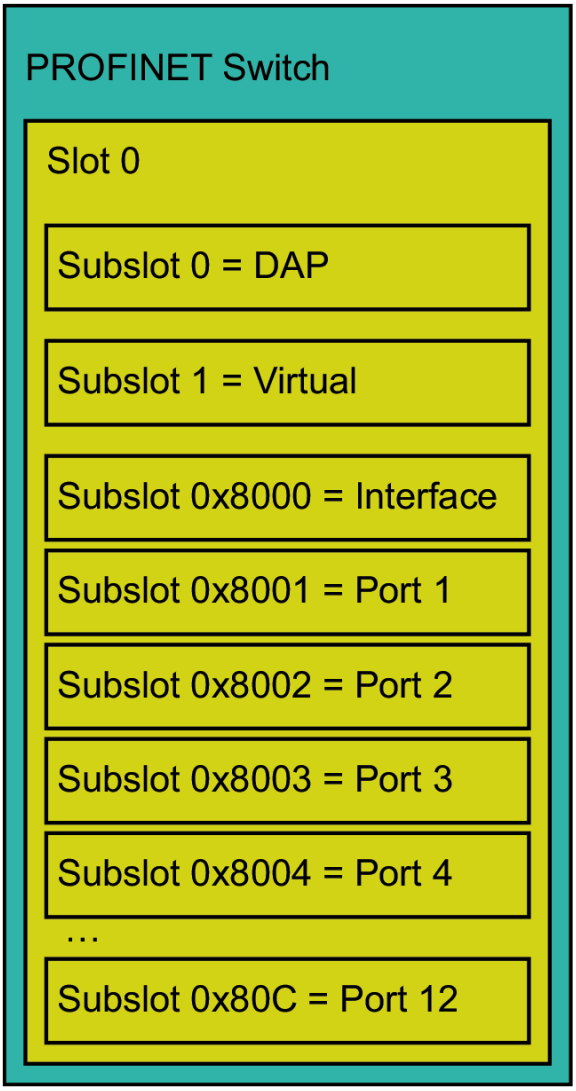
Adresowanie danych odbywa się w zależności od typu transmisji:

Tabela 18: Adresowanie danych w zależności od typu transmisji

Typ transmisji	**Adresowanie przez kombinację**		
	Slot	**Subslot**	**Indeks**
Cykliczna	X	X	–
Acykliczna	X	X	X

Określenie kombinacji slot/subslot może być ustalone przez producenta.

Switch zarządzalny PROFINET WAGO zawiera tylko slot 0. Przyporządkowanie subslotów jest przedstawione na poniższym rysunku. Każdy port switcha odpowiada jednemu subslotowi.



Ilustracja 12: Mapowanie subslotów w switchu zarządzalnym PROFINET WAGO

5.2 Komunikacja

W sieciach PROFINET komunikacja odbywa się przez Industrial ETHERNET.

Aby nawiązać komunikację między IO controller a IO device (np. switchem zarządzalnym PROFINET WAGO), należy ustalić ścieżki komunikacyjne. Te ścieżki komunikacyjne są podczas uruchamiania systemu konfigurowane przez IO controller na podstawie danych projektowych. W ten sposób relacja komunikacyjna dla wymiany danych jest jednoznacznie określona.

Każda wymiana danych jest osadzona w AR („**A**pplication **R**elation“). Przez AR ładowane są ogólne parametry komunikacyjne oraz parametry specyficzne dla producenta.

W PROFINET zdefiniowano następujące AR:

- Implicit AR
  Ta AR definiuje relację aplikacji między IO controller lub IO supervisor a IO device w celu acyklicznego odczytu danych z IO device. Przy implicit AR zapis nie jest dozwolony.
  Ta AR nie musi być jawnie ustanawiana, lecz jest standardowo zawsze w dostępie IO device.

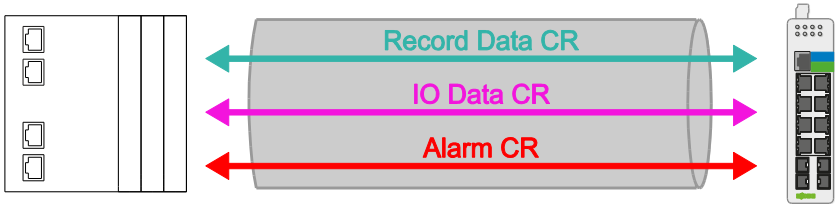
- IOCAR („**IO**-**C**ontroller **A**pplication **R**elation“)
  Ta AR służy do wymiany cyklicznych danych wejściowych i wyjściowych, danych acyklicznych oraz dwukierunkowych alarmów.

- IOSAR („**IO**-**S**upervisor **A**pplication **R**elation“)
  Ta AR służy do wymiany danych między IO supervisor a IO device oraz do przejęcia jednego lub kilku podmodułów IO device, które są przyporządkowane do odpowiednich IO controller. Wymiana danych może odpowiadać wymianie IOCAR.

W obrębie AR dane jednoznacznie określają tak zwane CR („**C**ommunication **R**elation“):

- Record Data CR (R-CR):
  Kanał komunikacyjny dla acyklicznej wymiany danych
- IO Data CR (IO-CR):
  Kanały komunikacyjne dla cyklicznej wymiany danych (dane wejściowe i wyjściowe)

- Alarm CR (A-CR):
  Kanał komunikacyjny dla alarmów



Ilustracja 13: Relacje komunikacyjne w PROFINET

W systemie PROFINET ze switchami zarządzalnymi WAGO można używać wielu IO controller. Każdy IO controller może nawiązać jedno połączenie AR z każdym z wielu IO devices.

5.3 Transmisja danych

Przesyłanie danych procesowych w sieciach PROFINET odbywa się zasadniczo w czasie rzeczywistym (RT = „**R**eal **T**ime“). Dodatkowo telegramy danych mogą być również przesyłane w trybie NRT („**N**on-**R**eal **T**ime“) przez standardowy ETHERNET. PROFINET wykorzystuje następujące możliwości:

- Komunikacja NRT w ramach sieci i między sieciami:
  Ta komunikacja odpowiada „zwykłej” komunikacji w sieciach ETHERNET. Warunki czasu rzeczywistego nie są spełniane. Taka komunikacja może być nawiązywana np. z urządzeniami HMI.

- Komunikacja RT w obrębie sieci:
  Ta komunikacja ma na celu wysoki poziom determinizmu. Wykorzystuje ona kanał RT. UDP/IP nie jest w tej konfiguracji używany.

- Komunikacja RT między sieciami:
  Ta komunikacja odbywa się z wykorzystaniem dodatkowego protokołowania. Wykorzystuje ona kanał RT. Dodatkowo używany jest UDP/IP.

5.3.1 Komunikacja w czasie rzeczywistym

Telegramy danych w formacie PROFINET są priorytetyzowane w stosunku do standardowych telegramów danych zgodnie z IEEE 802.1Q. Dzięki temu zagwarantowany jest wymagany w systemach automatyki determinizm. W tym procesie dane są przesyłane za pomocą priorytetowych telegramów ETHERNET.

5.3.2 Metody transmisji

Transmisja danych w sieciach PROFINET odbywa się w trybie full duplex:

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

5.3.3 Rodzaje transmisji

PROFINET obsługuje następujące tryby transmisji:

Transmisja acykliczna

Acyklicznie odbywa się transmisja danych dla następujących procesów:

- Ustanowienie połączenia czasu rzeczywistego (nawiązywanie połączenia)
- Parametryzacja switcha zarządzalnego PROFINET oraz jego podmodułów
- Odczyt informacji diagnostycznych
- Odczyt informacji identyfikacyjnych, serwisowych lub konserwacyjnych
- Odczyt danych I/O
- Odczyt informacji alarmowych

- inne

Transmisja cykliczna

Cyklicznie odbywa się przesyłanie danych procesowych i innych danych użytkowych.

Cykliczne dane I/O są przesyłane jako dane czasu rzeczywistego bez potwierdzenia. Czas trwania cyklu można parametryzować indywidualnie.

Monitorowanie połączenia danych odbywa się na podstawie monitorowania czasu, które jest wyprowadzone z wielokrotności parametryzowanego czasu cyklu wysyłania.

Podczas transmisji w telegramie czasu rzeczywistego dane subslotu są uzupełniane przez dane użytkowe urządzenia towarzyszącego (status Providera). Te informacje o statusie są analizowane przez odbiorcę (Consumer) danych I/O. W ten sposób Consumer może ocenić ważność danych wyłącznie na podstawie cyklicznej wymiany danych. W przeciwnym kierunku informacje o statusie odbiorcy (Consumer) są przekazywane do nadawcy (Provider). Zależnie od typu I/O podmodułu statusy dla Provider i Consumer mogą być również przesyłane w obu kierunkach.

Telegramy danych zawierają po danych dodatkowe informacje o statusie (APDU-Status). Brak cyklicznych danych jest monitorowany przez danego odbiorcę (Consumer) relacji komunikacyjnej. Jeśli odbiór danych nie nastąpi w zaprogramowanym czasie monitorowania, Consumer rozłącza połączenie.

5.3.4 Budowa telegramu

Telegram danych w PROFINET ma następującą strukturę:

Dest. addr.	Source addr.	VLAN tag	Ether type	FrameID	Application data	Cycle counter	Data status	Transfer status	FCS

Tabela 19: Obszary w telegramie PROFINET

Obszar	Zakres	Opis
Dest. addr.	6 B	Adres docelowy (adres MAC)
Source addr.	6 B	Adres źródłowy (adres MAC)
VLAN tag	4 B	Służy do przesyłania priorytetu.
Ether type	2 B	0x8892 → Typ telegramu PROFINET RT
FrameID	2 B	Zawiera wymieniony FrameID (zob. też tabela „Przykłady dla ‚FrameID‘“).
Application data	0 B … 1440 B	Dane użytkownika
Cycle counter	2 B	Zawiera numer cyklu w wielokrotnościach 31,25 µs. Przykład: czas cyklu = 4 ms: Cycle counter = 128 (128 × 31,25 µs = 4 ms)
Data status	1 B	Zawiera informacje o statusie danych (zob. tabela „Przykład dla ‚Data status‘“).
Transfer status	1 B	RT_Class_1: 0 RT_Class_3: 0/1 (1 = ramka zastępcza)
FCS	4 B	Suma kontrolna do wykrywania błędów transmisji.

5.4 Adresowanie

Adresowanie urządzenia w sieci PROFINET składa się z następujących składników:

- Nazwa urządzenia
- Adres MAC
- Adres IP (adres IP, maska podsieci i adres bramy)

W ustawieniu fabrycznym switch zarządzalny PROFINET ma następujący adres IP: **0.0.0.0**

Switchowi PROFINET adres IP jest przydzielany przez protokół DCP. To przypisanie może np. zostać wykonane przez I/O controller.

5.4.1 Nazwa urządzenia

Zanim I/O device zostanie przez I/O controller zaadresowane, oba urządzenia muszą otrzymać nazwy. W PROFINET wybrano takie podejście, gdyż nazwy są łatwiejsze w obsłudze niż adresy IP.

Wskazówka

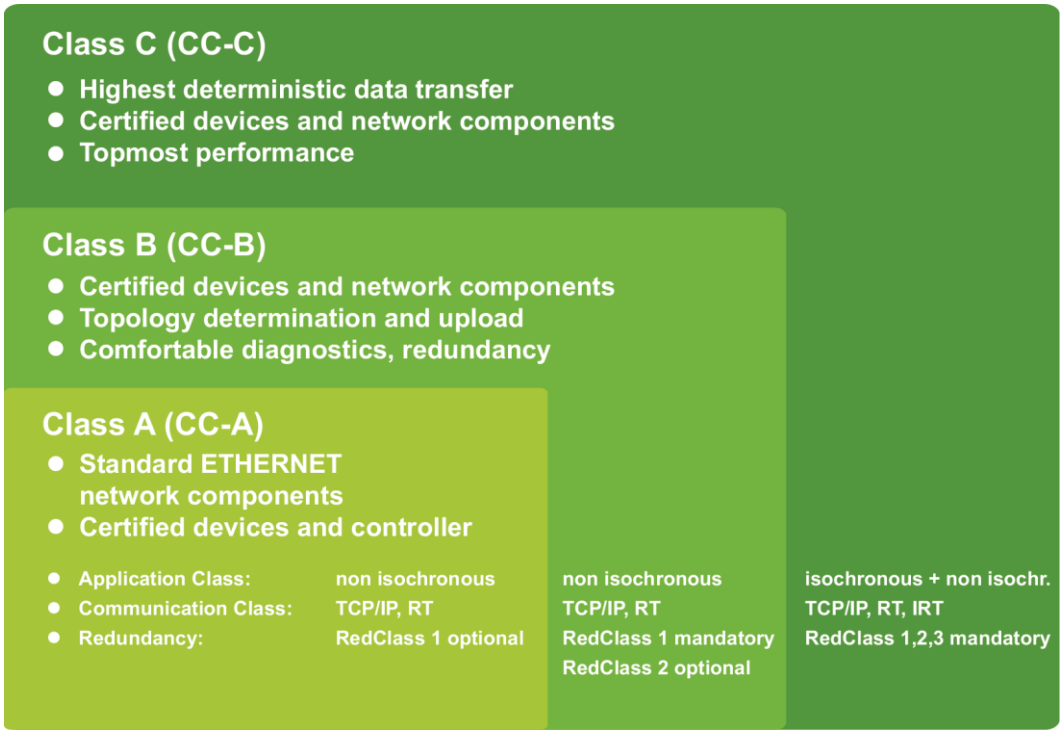


Użycie znaków jest ograniczone!
Przy nadawaniu nazw PROFINET obsługuje tylko wybrane znaki. Do tych znaków należą cyfry 0 … 9, małe litery a … z, znak łącznika „-” oraz kropka „.”.
Nazwa urządzenia może zawierać maksymalnie 127 znaków, przy czym między myślnikami i kropkami może być użytych do 63 liter lub cyfr. Spacje nie są dozwolone!

W ustawieniu fabrycznym switch zarządzalny PROFINET nie ma jeszcze przypisanej nazwy urządzenia. Jednak switch zarządzalny PROFINET jest rozpoznawalny w sieci przez IO controller dopiero, gdy przy IO supervisor (PD lub PC) przydzieli mu nazwę. Po przydzieleniu ustawień IP połączenie można ustanowić na podstawie danych projektowych.

5.5 Klasy zgodności („Conformance Classes“)

Wymagania dotyczące aplikacji z wykorzystaniem PROFINET IO można podzielić na 3 klasy zgodności („CC“ = „**C**onformance **C**lasses“). W normie IEC 61784-2 zdefiniowano dla PROFINET 3 klasy zgodności **CC-A**, **CC-B** i **CC-C**.



Ilustracja 14: Przegląd klas zgodności od A do C

Do tych 3 klas zgodności można przypisać konkretne zastosowania:

CC-A: Automatyzacja instalacji („Plant Control“)

- Spełnia wymagania podstawowej automatyzacji instalacji.
- Wykorzystywane urządzenia PROFINET są certyfikowane.
- Zapewnia podstawowe funkcje PROFINET IO z komunikacją RT.
- Wszystkie usługi IT można wykorzystywać bez ograniczeń.
- Dla czasów cyklu do 100 ms (np. w automatyce instalacji)
- Możliwe jest wykorzystanie istniejącego oprzewodowania budynku.
- Definicja integracji systemów bezprzewodowych, takich jak *Bluetooth*® lub WLAN
- Określenie integracji istniejących sieci obiektowych, takich jak PROFIBUS, INTERBUS lub DeviceNet (niezależnie od producenta)
- Koncepcje bezpieczeństwa dostępu z Internetu do diagnostyki zdalnej, bez możliwości ingerencji osób nieuprawnionych

CC-B: Automatyzacja maszyn („Machine Control“)

- Spełnia wymagania dla automatyzacji maszyn.
- Urządzenia i infrastruktura sieciowa muszą być certyfikowane.
- Rozszerza koncepcję o diagnostykę sieci opartą na mechanizmach IT oraz o informacje o topologii.
- Funkcja „system redundancy“ (np. w automatyce procesowej) jest zawarta w rozszerzeniu CC-B do CC-B(PA).
- Dla czasów cyklu transmisji danych do 10 ms (np. sterownik PLC jako typowy sterownik maszyny)
- Infrastruktura musi podlegać jasno określonym wytycznym.
- Dozwolone są tylko komponenty PROFINET. Również switche i przewody muszą spełniać minimalne wymagania PROFINET.
- Przewody muszą mieć ekranowanie, aby zapewnić kompatybilność elektromagnetyczną.

CC-C: Automatyka ruchu („Motion Control“)

- Spełnia wymagania automatyki ruchu.
- Urządzenia i infrastruktura sieciowa muszą być certyfikowane.
- Opisuje podstawowe funkcje dla urządzeń z rezerwacją przepustowości na bazie sprzętu i synchronizacją (komunikacja IRT).
- Stanowi podstawę dla aplikacji taktowo-synchronicznych.
- Dla czasów cyklu poniżej 1 ms (np. do sterowania ruchami)
- Wszystkie komponenty muszą być urządzeniami klasy C i mogą być synchronizowane czasowo.
- Komunikacja izochronna jest warunkiem osiągnięcia wymaganych czasów cyklu. Uczestnicy są izochroniczni, gdy wszyscy mają ten sam czas („clock synchronization“).

Poszczególne klasy zgodności można łączyć ze sobą. System wykorzystujący PROFINET IO może obejmować różne klasy zgodności. Możliwe jest także utworzenie kilku stref tej samej klasy zgodności.

Aby taki podział mógł zostać zrealizowany, urządzenia danej klasy zgodności muszą spełniać określone minimalne wymagania dotyczące implementowanych funkcji i protokołów.

Tabela 20: Porównanie klas zgodności

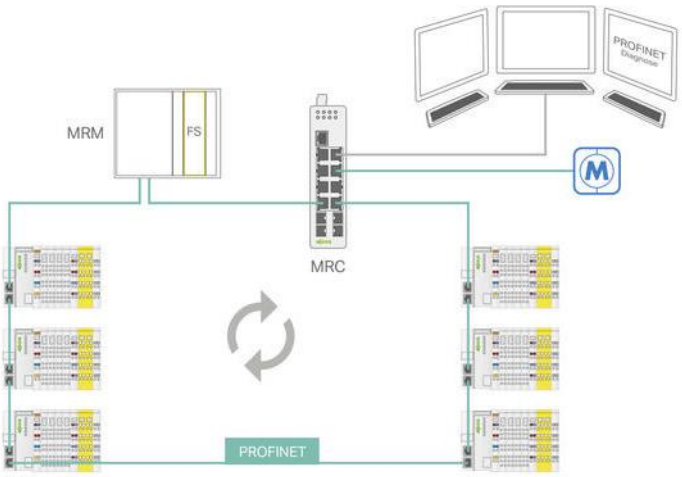
Wymaganie	Klasa A (CC-A)	Klasa B (CC-B)	Klasa C (CC-C)
Funkcje bazowe	• Komunikacja RT • Cykliczne I/O • Parametry • Alarmy	• Komunikacja RT • Cykliczne I/O • Parametry • Alarmy • Diagnostyka sieci • Informacje o topologii • Redundancja systemu	• Komunikacja RT • Cykliczne I/O • Parametry • Alarmy • Diagnostyka sieci • Informacje o topologii • Zarezerwowana szerokość pasma (IRT) • Synchronizacja
Oprzewodowanie	Zgodnie z IEC 61784-5-3 i IEC 24702 • Miedź • Światłowód • Bezprzewodowe	Zgodnie z IEC 61784-5-3 • Miedź • Światłowód	Zgodnie z IEC 61784-5-3 • Miedź • Światłowód
Typowe zastosowanie	• Obiekty infrastrukturalne • Automatyka budynkowa	• Automatyka przemysłowa • Automatyka procesowa	• Motion Control

W praktyce urządzenia, które odpowiadają klasie zgodności CC-A, mogą zawierać pojedyncze funkcje z CC-B lub CC-C.

5.6 Redundancja mediów

PROFINET realizuje redundancję mediów za pomocą protokołu MRP. W tym celu urządzenia PROFINET są rozmieszczone w topologii pierścieniowej.

W topologii pierścieniowej 1 urządzenie pełni rolę menedżera redundancji (Redundancy manager). Wszystkie pozostałe urządzenia w pierścieniu są klientami redundancji (Redundancy client).



Ilustracja 15: Redundancja mediów w PROFINET (topologia pierścienia)

Tabela 21: Opis ilustracji „Redundancja mediów w PROFINET (topologia pierścienia)“

Skrót	Znaczenie
MRM	Redundancy manager
MRC	Redundancy client

Wybór i określenie portów pierścieniowych odbywa się podczas projektowania. Każdy port produktu może pełnić rolę menedżera redundancji lub klienta redundancji.

Funkcja redundancji mediów

Przy prawidłowej komunikacji menedżer redundancji blokuje jeden z dwóch portów pierścieniowych. Dzięki temu zapewnione jest, że żadne telegramy danych nie krążą. Z punktu widzenia komunikacji danych pierścień staje się topologią liniową.

Menedżer redundancji monitoruje topologię pierścienia pod kątem przerw, wysyłając telegramy testowe z obu portów pierścieniowych. Telegramy testowe krążą w topologii pierścienia w obu kierunkach, aż dotrą do innego portu pierścieniowego menedżera redundancji. Jeśli odbiór jednego z telegramów testowych nie zostanie potwierdzony, następuje przerwanie komunikacji. To przerwanie może mieć różne przyczyny:

- Utrata połączenia między 2 urządzeniami
- Awaria urządzenia w topologii pierścienia

W przypadku wystąpienia przerwy menedżer redundancji przełącza oba swoje porty pierścieniowe. Przez tę ścieżkę zastępczą zostaje przywrócone działające połączenie między wszystkimi pozostałymi urządzeniami w formie topologii liniowej.

Czas między przerwaniem pierścienia a przywróceniem działającej topologii liniowej nazywany jest czasem rekonfiguracji.

Po usunięciu przerwy przywracane są pierwotne ścieżki transmisji, oba porty pierścieniowe w menedżerze redundancji zostają od siebie oddzielone, a klienci redundancji są informowani o zmianie. Klienci redundancji wykorzystują następnie znane ścieżki do innych urządzeń.

Wszystkie urządzenia (I/O controller, I/O devices, switche itp.), które są połączone w topologii pierścienia, muszą obsługiwać funkcję redundancji mediów. Te urządzenia tworzą tak zwaną domenę redundancji.

Funkcja redundancji mediów jest w switchu zarządzalnym PROFINET realizowana za pomocą następującej procedury:

MRP („Media Redundancy Protocol“)

Ta metoda redundancji jest metodą standardową i opiera się na normie IEC 61158, typ 10 „PROFINET“. W tej metodzie maksymalnie 50 urządzeń może być połączonych w topologii pierścienia. Typowy czas rekonfiguracji wynosi 200 ms.

Poniższe warunki muszą być spełnione, aby zapewnić bezawaryjną pracę z MRP:

- Wszystkie urządzenia, połączone w topologii pierścienia, muszą obsługiwać MRP.
- Funkcja „MRP“ musi być aktywowana we wszystkich urządzeniach.
- Wszystkie urządzenia muszą być ze sobą połączone za pomocą swoich portów pierścieniowych.
- Topologia pierścienia może składać się maksymalnie z 50 urządzeń.
- W urządzeniach nie jest ustawiona funkcja IRT.

5.7 Protokoły

W tym rozdziale wymieniono protokoły PROFINET, które są wykorzystywane w switchu zarządzalnym PROFINET.

DCP

Za pomocą DCP („**D**ynamic **C**onfiguration **P**rotocol“) zgodnie z IEC 61158 można konfigurować urządzenia w systemie ETHERNET. Na przykład można przydzielać nieadresowanym urządzeniom nazwy oraz ustawienia IP, aby urządzenia te były dostępne w sieci przez protokół IP.

Aby odpytywać i przydzielać informacje adresowe, DCP udostępnia różne usługi, np.:

- DCP_Identify queries
- DCP_Get services
- DCP_Set services

Urządzenie ETHERNET jest przy pierwszym uruchomieniu w ustawieniach fabrycznych. Nazwa urządzenia nie istnieje (pusty ciąg, NIL), a ustawienia IP **adres**, **maska podsieci** oraz **brama domyślna** mają wartość 0.0.0.0.

Urządzenie ETHERNET jest dostępne przez ICMP dopiero po przypisaniu mu nazwy oraz prawidłowych ustawień IP za pomocą odpowiednich usług DCP_Set.

LLDP

LLDP („**L**ink **L**ayer **D**iscovery **P**rotocol“) jest protokołem warstwy 2 modelu odniesienia ISO/OSI.

LLDP umożliwia urządzeniu ETHERNET w sieci LAN („**L**ocal Area **N**etwork“) wysyłanie informacji o sobie i odbieranie informacji od sąsiednich urządzeń. Urządzenie przechowuje odebrane informacje w swojej LLDP-MIB („**M**anagement **I**nformation **B**ase“), którą można odczytać za pomocą systemu zarządzania siecią przez SNMP.

Telegramy LLDP są wysyłane z EtherType 0x88CC zarówno w stałych odstępach czasu, jak i przy zmianach LLDP-MIB na adres multicast-MAC **01:80:C2:00:00:0E**. Telegramy są odbierane i przetwarzane tylko przez bezpośredniego sąsiada w sieci.

MRP

MRP („**M**edia **R**edundancy **P**rotocol“) jest określony zgodnie z IEC 62439 i w przypadku awarii umożliwia przełączenie ścieżek komunikacyjnych dla ruchu TCP/IP i RT_Class_1 w ciągu 200 ms. Do zastosowania tej metody wymagany jest 1 MRM („**M**edia **R**edundancy **M**anager“) oraz 1 lub więcej MRC („**M**edia-**R**edundancy **C**lients“), rozmieszczonych w topologii pierścienia. W związku z tym zainstalowane urządzenia muszą mieć co najmniej 2 porty ETHERNET.

MRM jest zwykle zrealizowany w IO controller lub w switchu PROFINET. MRM kieruje ruch telegramów do urządzeń znajdujących się w topologii pierścienia w niezakłóconym trybie pracy tylko przez 1 z obu portów pierścieniowych. W ten sposób dzieli topologię pierścienia na wirtualną topologię liniową. MRM dodatkowo sprawdza zaprojektowaną topologię pierścienia pod kątem ewentualnych przerw za pomocą cyklicznie rotujących telegramów testowych. Te telegramy testowe są przez MRC przekazywane tylko do następnego uczestnika. Jeśli MRM nie otrzyma zwrotnie testowych telegramów wysłanych przez jego pierwszy port pierścieniowy na drugim porcie, sprawdza, w którym miejscu topologia pierścienia została przerwana. Następnie przełącza ruch telegramów dla uczestników, którzy nie są już osiągalni przez pierwszy port pierścieniowy, na drugi port pierścieniowy.

RTC

RTC („**R**eal **T**ime **C**yclic“) jest cyklicznym protokołem PROFINET.

Dzięki technologii czasu rzeczywistego omijane są warstwy TCP/IP, dzięki czemu deterministyczne działanie aplikacji osiąga szybkość od 1 do 10 milisekund. Dzięki temu PROFINET RT jest idealny dla zastosowań, w których sterowanie dwustanowymi i analogowymi wejściami/wyjściami jest kluczowe dla cykli produkcyjnych. Poprzez pominięcie TCP/IP i przesyłanie komunikatów danych z fizycznej warstwy ETHERNET do warstwy aplikacji, „PROFINET Real Time“ zapewnia wysoki stopień determinizmu.

5.8 Switch zarządzalny PROFINET

Switch zarządzalny PROFINET posiada następujące właściwości PROFINET:

Funkcje cykliczne (PROFINET RT):

- Minimalny interwał: 32 ms
- Rozszerzony i tryb startowy Legacy
- Nawiązywanie połączeń
  - 1x IOC_AR, 1x DA_AR
  - 1x Input CR
  - 1x Output CR
  - 1x Alarm CR

Funkcje niecykliczne:

- Tryb połączony:
  - Odczyt informacji diagnostycznych IO device (Record)
  - Zapisywanie różnych parametrów konfiguracji
  - Wysyłanie alarmów do I/O controller
- Tryb niepołączony:
  - Odczyt informacji diagnostycznych IO device (Record)

Funkcje ogólne:

- Klient/menedżer MRP, pojedyncza instancja (konfigurowalna niezależnie dla każdego portu)
- LLDP & LLDP MIB
- Łatwa wymiana urządzeń
- Netload II certyfikowany

Następujące funkcje nie są obsługiwane:

- DHCP
- FSU
- Shared Input
- Shared Device
- IOS_AR
- IOS_AR TakeOver
- IRT, RT_CLASS_3 Data Exchange
- PROFIenergy
- Precision Transparent Clock Protocol (PTCP)

5.9 Plik GSDML

5.9.1 Wprowadzenie

Wszystkie I/O devices są opisane w pliku specyficznym dla producenta pod względem ich właściwości technicznych i funkcjonalnych. Ten plik GSDML („**G**eneral **S**tation **D**escription **M**arkup **L**anguage“) bazuje na XML. Zawiera wszystkie dane potrzebne do inżynierii oraz do wymiany danych z I/O controller. Należą do nich między innymi:

- Opis poszczególnych I/O devices (urządzeń wejściowe i wyjściowe)
- Możliwości zastosowania urządzeń I/O w slotach
- Parametry wymagane do prawidłowego działania I/O devices
- Diagnostyka i związane z nią znaczenia, dostarczane przez I/O devices
- Opis wielu urządzeń należących do jednej rodziny w jednym pliku

Plik GSD jest wielojęzyczny.

Nazwa pliku GSD odpowiada następującemu schematowi:

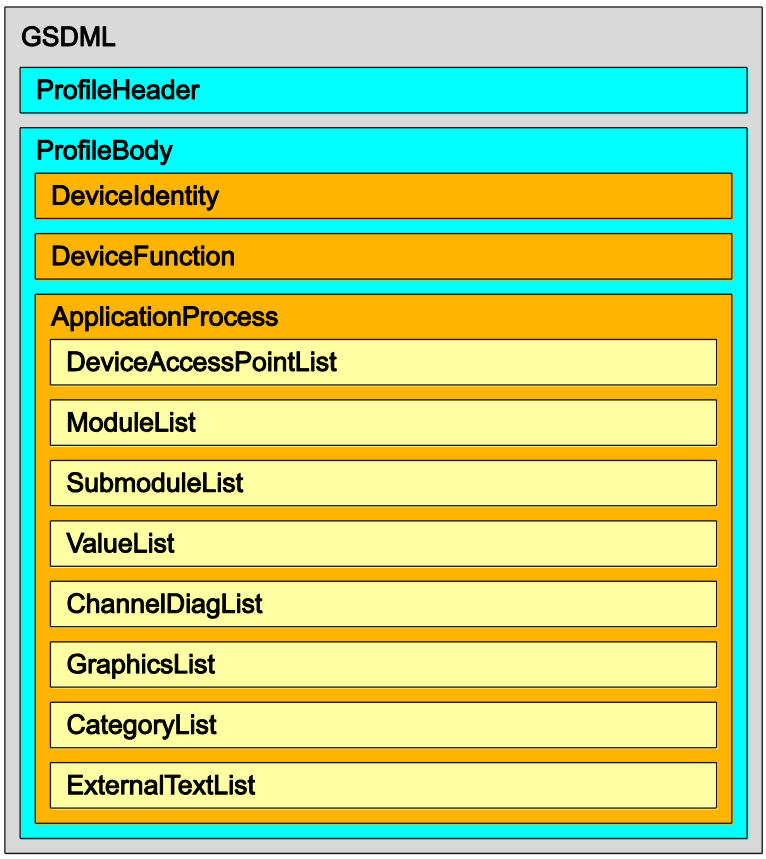
GSDML-<version>-<Manufacturer>-<Devicename>-<Date>.xml

Przykład nazwy pliku GSD:

GSDML-V2.33-WAGO-852-20190213.xml

5.9.2 Budowa pliku GSDML

Zawartość pliku GSDML jest zorganizowana zgodnie z normą ISO 15745.



Ilustracja 16: Ogólna budowa pliku GSDML

ProfileHeader

Struktura i zawartość są określone przez standard.
Zawiera następujące informacje:

- ProfileIdentification
- ProfileRevision
- ProfileName
- ProfileSource
- ProfileClassID
- ISO15745Reference

ProfileBody

Zawiera wszystkie dane specyficzne dla I/O device lub rodziny urządzeń.
Sekcja ProfileBody dzieli się na:

- DeviceIdentity
- DeviceFunction
- ApplicationProcess

DeviceIdentity

Zawiera informacje dotyczące identyfikacji I/O device.
Składa się z:

- Vendor_ID
  (Ta ID jest przydzielana przez PNO i zawiera identyfikator firmy. Jest ona unikatowa dla każdego producenta.)
- Device_ID
  (Device_ID może być zdefiniowany specyficznie przez producenta.)
- InfoText (opis rodziny urządzeń) oraz
- VendorName.

DeviceFunction

Informacje dotyczące funkcji rodziny urządzeń

ApplicationProcess

Zawiera rzeczywiste dane dotyczące I/O device
Sekcja dzieli się na:

- DeviceAccessPointList
- ModuleList
- SubmoduleList
- ValueList
- ChannelDiagList
- GraphicsList
- CategoryList
- ExternalTextList

DeviceAccessPointList

Zawiera opisy wszystkich dostępnych w rodzinie urządzeń połączeń magistralowych (DAP = „**D**evice **A**ccess **P**oint“).
Obejmuje m.in.:

- ModuleInfo (nazwa, opis, numer katalogowy, stan wersji itp.)
- CertificationInfo (Conformance, Application i NetLoad Class)
- SubslotList
- IOConfigData (maksymalna długość przesyłanych danych)
- UseableModules (tylko w przypadku modularnie skonstruowanych IO devices)
- VirtualSubmoduleList
- SystemDefinedSubmoduleList
- Graphics (ilustracja systemowa IO device)

ModuleList

Zawiera opisy poszczególnych modułów IO devices.

SubmoduleList

Zawiera opisy poszczególnych podmodułów IO device.

ValueList

Zawiera parametry, które można ustawić dla IO device oraz przyporządkowanie między wartością a oznaczeniem.
Oznaczenie jest określane przez **TextID** w **ExternalTextList**.

ChannelDiagList

Zawiera przyporządkowanie błędu do odpowiedniego tekstu.
Odpowiedni tekst jest określany przez ID w **ExternalTextList**.

GraphicsList

Zawiera odwołania do symboli graficznych wszystkich IO devices w rodzinie urządzeń.

CategoryList

Zawiera przyporządkowanie modułów do określonej kategorii.
To przyporządkowanie służy do strukturyzacji katalogu modułów dla tego IO device w odpowiednim oprogramowaniu inżynierskim.

ExternalTextList

Zawiera wszystkie teksty, do których można znaleźć odniesienia w innych obszarach pliku GSDM za pomocą odpowiedniego **TextID**.
Ta lista może być przygotowana w różnych wersjach językowych.

5.9.3 Jednoznaczna identyfikacja IO devices

Jednoznaczną identyfikację IO devices w pliku GSDML określają następujące identyfikatory:

- Vendor_ID (identyfikator producenta; zob. **DeviceIdentity**)
- Device_ID (jednoznaczny identyfikator urządzenia; zob. **DeviceIdentity**)
- Modul-ID (jednoznaczny identyfikator wszystkich modułów, które mogą być używane w ramach danego IO device; zob. **ModuleList**)
- Submodul-ID (jednoznaczny identyfikator wszystkich submodułów, które mogą być używane w ramach danego modułu; zob. **SubmoduleList**)

5.10 Projektowanie za pomocą pliku GSDML

W tym rozdziale opisano ogólny sposób postępowania, bez uwzględnienia specyficznych dla producentów narzędzi konfiguracyjnych. Opisy tych narzędzi konfiguracyjnych można znaleźć u danego producenta.

Konfigurowanie switcha zarządzalnego PROFINET zasadniczo obejmuje następujące fazy:

1 Planowanie (włączenie w topologię itp.)
2 Parametryzacja/konfiguracja za pomocą narzędzia projektowego
3 Budowa sieci
4 Test
5 Uruchamianie

5.10.1 Konfiguracja

Właściwe konfigurowanie switcha zarządzalnego PROFINET przy użyciu narzędzia projektowego może się rozpocząć, gdy spełnione są następujące warunki:

- Faza wyboru urządzeń i topologii sieci została zakończona.
- Wszystkie pozostałe kwestie związane z ogólnym projektowaniem również zostały wyjaśnione.

Wskazówka



Uwzględnić dokumentację narzędzia projektowego!
Ten rozdział zawiera ogólne wskazówki dotyczące konfigurowania systemu PROFINET.
Przy obsłudze stosowanego narzędzia projektowego należy korzystać z dokumentacji danego producenta.

Zasadniczo konfigurowanie może odbywać się na 2 różne sposoby:

- **Offline**
  Do narzędzia projektowego początkowo nie jest podłączony żaden rzeczywisty system PROFINET. Projekt jest tworzony i konfigurowany z planowanymi urządzeniami i planowaną topologią. Następnie rzeczywisty system PROFINET zostaje podłączony do narzędzia projektowego, a utworzony projekt jest załadowany do rzeczywistego IO controllera.
- **Online**
  Do narzędzia projektowego podłączony jest rzeczywisty system PROFINET. Projekt jest tworzony z rzeczywistą konfiguracją i ładowany do IO controllera.

Zasadnicze postępowanie jest podobne w obu przypadkach. Procedurę konfiguracji offline opisano w dalszej części dokumentu.

5.10.1.1 Narzędzia projektowe (przegląd)

Do planowania, projektowania i konfigurowania systemu PROFINET dostępne są różne narzędzia projektowe, specyficzne dla poszczególnych producentów.

Poniższa tabela zawiera wybór narzędzi projektowych PROFINET różnych producentów. Lista jest uporządkowana alfabetycznie. Nie jest ona pełna i nie zawiera jakiejkolwiek oceny.

Tabela 22: Przegląd narzędzi projektowych

Producent	Narzędzie projektowe
3S	CODESYS
Beckhoff	TwinCAT
Hilscher	SYCON.net
Phoenix Contact	PCWorx
Siemens	STEP 7 (TIA Portal)

Ogólne podejście do projektowania jest we wszystkich narzędziach projektowych w zasadzie identyczne.

Używane narzędzie projektowe powinno spełniać co najmniej następujące zadania:

- Zarządzanie urządzeniami PROFINET w katalogu sprzętu
- Łączenie urządzeń w (graficznym) widoku sieci i/lub w widoku konfiguracji sprzętu
- Przydzielanie nazw i adresów urządzeń
- Monitorowanie i sterowanie zmiennymi online
- Dostęp online do danych procesowych
- Diagnostyka urządzeń PROFINET
- Diagnostyka urządzeń sieciowych (np. switchy)
- Przedstawienie projektu w strukturze hierarchicznej (np. strukturze drzewa)
- Sprawdzenie projektu pod kątem spójności, poprawności i zgodności z zestawieniem ilościowym
- Wsparcie użytkownika przy tworzeniu dokumentacji instalacji

W poniższych opisach przykładowo użyto narzędzia „TIA” firmy Siemens.

Wskazówka



Przestrzegać instrukcji użytkowania!
Szczegółową instrukcję konfiguracji switcha zarządzalnego PROFINET przy użyciu narzędzia projektowego „TIA” firmy Siemens można znaleźć w instrukcji użytkowania „TIA Portal – WAGO PROFINET Managed Switches”. Ten dokument można pobrać ze strony www.wago.com.

5.10.1.2 Ogólne podejście do projektowania systemu PROFINET

Poniżej wymienione kroki mogą się różnić w zależności od używanego narzędzia projektowego. Zasadniczo opisane podejście jest jednak identyczne.

1. Zaimportuj w razie potrzeby odpowiednie pliki GSD dla nowych urządzeń PROFINET.
   W istniejącym projekcie ponowny import pliku GSD zwykle jest konieczny tylko wtedy, gdy I/O device zostanie rozszerzone o typy modułów I/O, które nie są jeszcze zawarte w danym I/O device.

2. Dla nowego systemu PROFINET utwórz nowy projekt w narzędziu projektowym.
   Aby rozbudować istniejący system PROFINET, otwórz istniejący projekt.

3. Dodaj nowe urządzenia PROFINET jako instancje urządzeń z katalogu sprzętu do otwartego projektu.

4. Przypisz nowym urządzeniom PROFINET nazwy urządzeń i/lub adresy IP (jeśli wymagane) zgodnie z projektem.
   Od Conformance Class B każdy uczestnik sieci PROFINET musi mieć nadaną nazwę urządzenia i adres IP.
   Nadaj możliwie „opisowe” nazwy urządzeń, aby ułatwić ich szybsze rozpoznawanie (np. w komunikatach diagnostycznych).
   W zależności od używanego narzędzia projektowego i zastosowanej struktury danych przypisywanie nazw urządzeń i/lub adresów IP może odbywać się automatycznie.

5. Jeżeli urządzeniem PROFINET jest modularny I/O device (np. WAGO-I/O-SYSTEM), wybierz z katalogu sprzętu moduły, które będą użyte, i dodaj je do projektu. Dostosuj strukturę danych wejściowych i wyjściowych na podstawie odpowiednich podmodułów.
   Dzięki temu m.in. określana jest struktura obrazów procesu dla danych wejściowych i wyjściowych.

Informacja



Zwrócić uwagę na wielkość obrazów procesu!
Wielkość obrazów procesu oblicza się jako sumę danych wejściowych i wyjściowych wszystkich modułów i podmodułów skonfigurowanych w węźle PROFINET. Dzięki celowemu doborowi odpowiednich typów podmodułów dla modułów dwustanowych można, zależnie od urządzenia, zoptymalizowania struktury obrazów procesu dla danych wejściowych i wyjściowych.
Zawartość obrazów procesu jest wymieniana z I/O controllerem podczas ruchu danych w czasie rzeczywistym.

6. Połącz nowe urządzenia PROFINET zgodnie z zaplanowaną topologią.
   Wizualizacja topologii zależy od używanego narzędzia projektowego i może różnić się od rzeczywistej topologii.

7. W razie potrzeby dostosuj ustawienia wspólne dla różnych stacji w odpowiednim podmodule IO device.

8. W razie potrzeby dostosuj parametryzację zaprojektowanych modułów i podmodułów w IO devices.

9. Wybierz klasę komunikacji (NRT lub RT) w odpowiednim podmodule IO device.

10. Sprawdź czas odświeżania, cykl wysyłania oraz monitorowanie połączenia z IO controllerem i w razie potrzeby dostosuj te ustawienia.

11. Jeśli chcesz użyć stacji w sieci redundantnej (topologia pierścieniowa), przypisz IO device rolę klienta MRP i w razie potrzeby dostosuj nazwę domeny MRP.

12. Sprawdź ustawienia połączeń w podmodułach portów IO device i w razie potrzeby je dostosuj.

13. Przeprowadź kontrolę zaprojektowanego systemu PROFINET i następnie zapisz go.
    Narzędzie projektowe sprawdza np. logiczną poprawność zaprojektowanego systemu oraz zgodność z określonym zestawem ilościowym.

14. Utwórz dokumentację zaprojektowanego systemu PROFINET.
    W zależności od używanego narzędzia projektowego tworzenie dokumentacji może odbyć się automatycznie.

15. W razie potrzeby utwórz odpowiednie programy użytkowe lub dostosuj je i przetestuj wprowadzone zmiany.
    Zakres tego kroku zależy w zasadzie od tego, czy tworzony jest zupełnie nowy system PROFINET, czy rozszerzany istniejący.

16. W razie potrzeby dostosuj zarządzanie kontami użytkowników:
    - Tworzenie nowych ról użytkowników
    - Zakładanie użytkowników
    - Przydzielenie odpowiednich uprawnień

Wskazówka



Dezaktywować nieużywane porty!
Zgodnie z wytyczną PNO „PROFINET Security” nieużywane porty muszą być dezaktywowane.

Na tym konfiguracja offline zostaje na razie zakończona.

5.10.1.3 Załadowanie projektu do IO controllera.

Aby móc załadować projekt do IO controllera, należy zrealizować zaplanowaną konfigurację systemu PROFINET i zbudować topologię.

Następnie można zakończyć fazę projektową w następujący sposób:

1. W razie potrzeby utwórz za pomocą dostępnych narzędzi projektowych docelową konfigurację sieci PROFINET.
   Docelowa konfiguracja jest niezbędna do integracji IO device w domenie IRT.
   Udostępnienie konfiguracji docelowej jest wymagane również przy zamiarze wymiany urządzeń bez nadawania nazwy stacji za pomocą narzędzia.
   Jeżeli konfiguracja docelowa i rzeczywista są zgodne, można w razie potrzeby przy pierwszym uruchomieniu zrezygnować z nadawania nazwy stacji za pomocą narzędzia.

2. Następnie włącz zasilanie interfejsu sieciowego.

3. Alternatywnie do nadawania nazwy stacji za pomocą topologii możesz przypisać nazwę urządzenia za pomocą narzędzia DCP.
   W razie możliwości można również zdefiniować nazwę urządzenia za pomocą mikroprzełączników DIP.

4. Załaduj dane systemowe do IO controllera.

Po pomyślnym załadowaniu danych systemowych może nastąpić wymiana danych między IO controllerem a IO device.

5.10.2 Parametry

Parametry switcha zarządzalnego PROFINET można konfigurować za pomocą wybranego oprogrammowania narzędziowego.

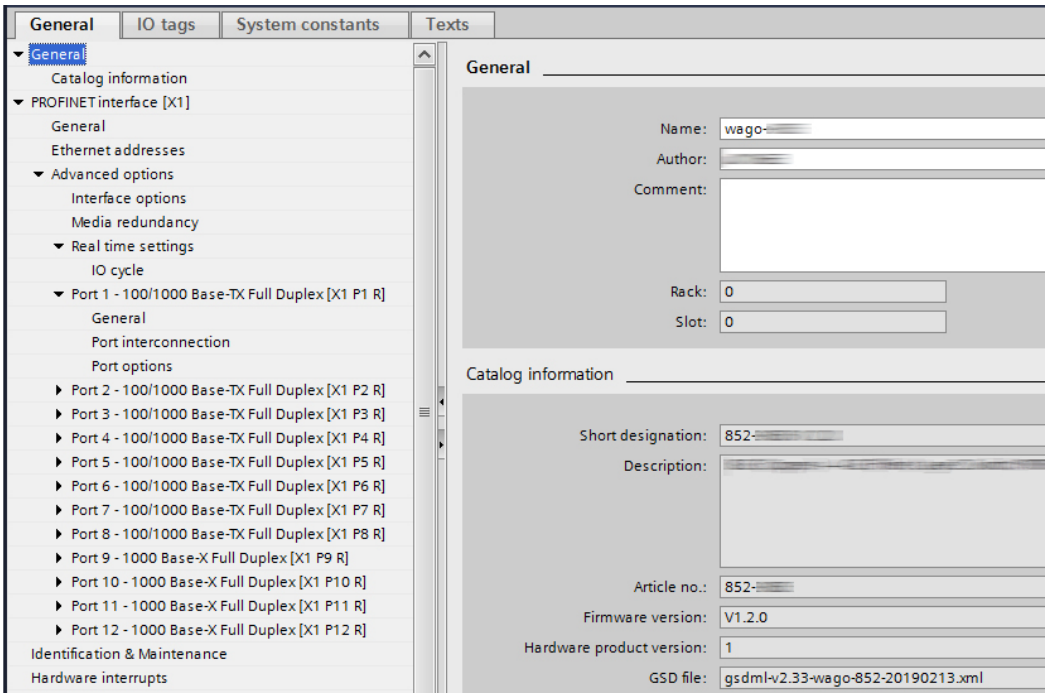
Na ilustracjach są objaśnione poszczególne parametry i podane odniesienia do pliku GSDML.

W poniższych opisach przykładowo użyto narzędzia „TIA” firmy Siemens.

Wskazówka

Przestrzegać instrukcji użytkowania!
Szczegółową instrukcję konfiguracji switcha zarządzalnego PROFINET przy użyciu narzędzia projektowego „TIA” firmy Siemens można znaleźć w instrukcji użytkowania „TIA Portal – WAGO PROFINET Managed Switches”. Ten dokument można pobrać ze strony www.wago.com.

5.10.2.1 Obszar „General”

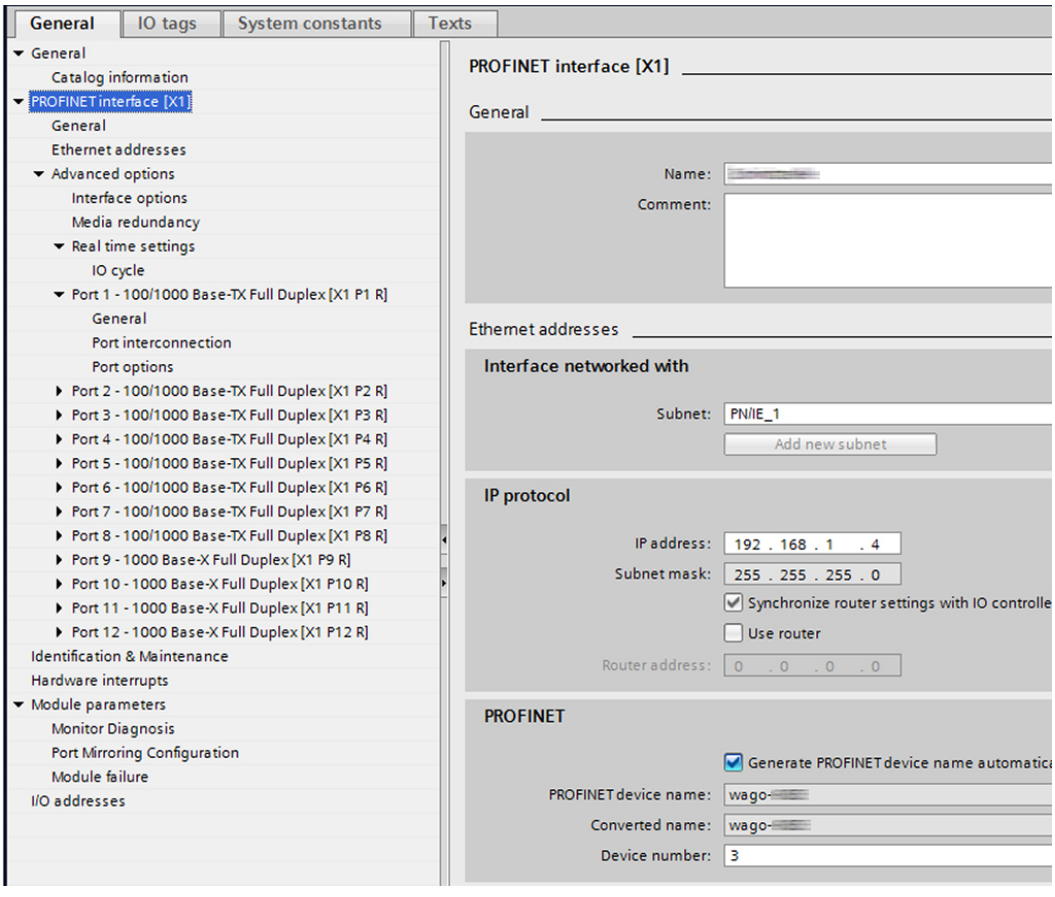


Ilustracja 17: Parametry PROFINET – obszar „General”

Tabela 23: Parametry PROFINET dla obszaru „General”

Parametr	Opis	Znacznik w GSDML
Name	Nazwa DAP	DeviceAccessPointItem [DNS_CompatibleName]
Author	Osoba zajmująca się urządzeniem w narzędziu projektowym	–
Comment	Pole komentarza	–
Rack	Dokładny opis miejsca montażu	–
Slot	Dokładny opis miejsca montażu	–
Short designation	Nazwa modułu	ModuleInfo/Name
Description	Opis modułu	ModuleInfo/InfoText
Article no.	Numer katalogowy modułu	ModuleInfo/OrderNumber
Firmware version	Wersja firmware'u	ModuleInfo/SoftwareRelease
Hardware product version	Wersja sprzętu	ModuleInfo/HardwareRelease
GDS file	Nazwa pliku GSDML	–

5.10.2.2 Obszar „PROFINET interface [X1]”

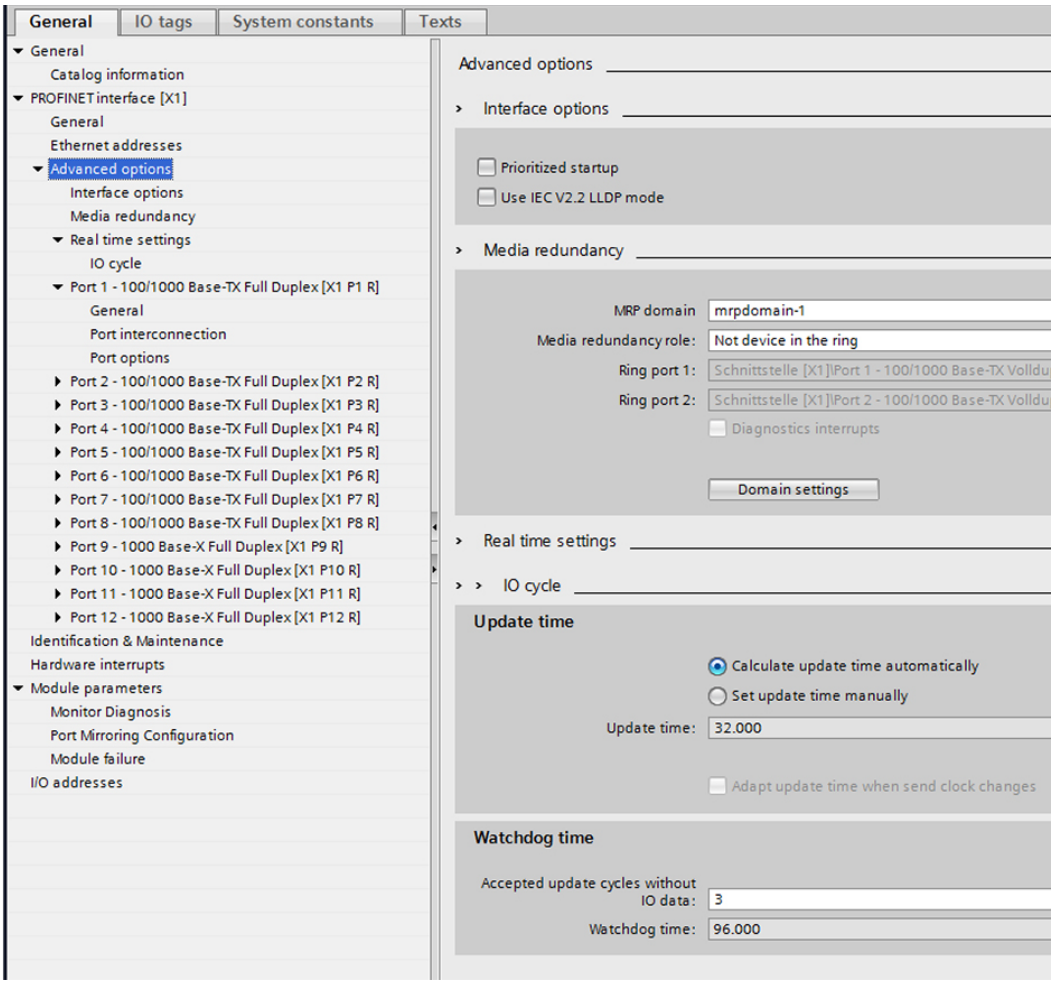


Ilustracja 18: Parametry PROFINET – obszar „PROFINET interface [X1]”

Tabela 24: Parametry PROFINET dla obszaru „PROFINET interface [X1]”

Parametr	Opis	Znacznik w GSDML
Name	Nazwa interfejsu	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem
Comment	Pole komentarza	–
Subnet	Nazwa podsieci	–
IP Address	Adres IP (domyślnie: 0.0.0.0)	–
Subnet mask	Maska podsieci	–
PROFINET device name	Nazwa urządzenia; może być automatycznie pobrana z pliku GSDML.	DeviceAccessPointItem [DNS_CompatibleName]
Converted name	Nazwa urządzenia; jest automatycznie pobierana z pliku GSDML.	DeviceAccessPointItem [DNS_CompatibleName]
Device number	Numer urządzenia w sieci	–

5.10.2.3 Obszar „Advanced options”



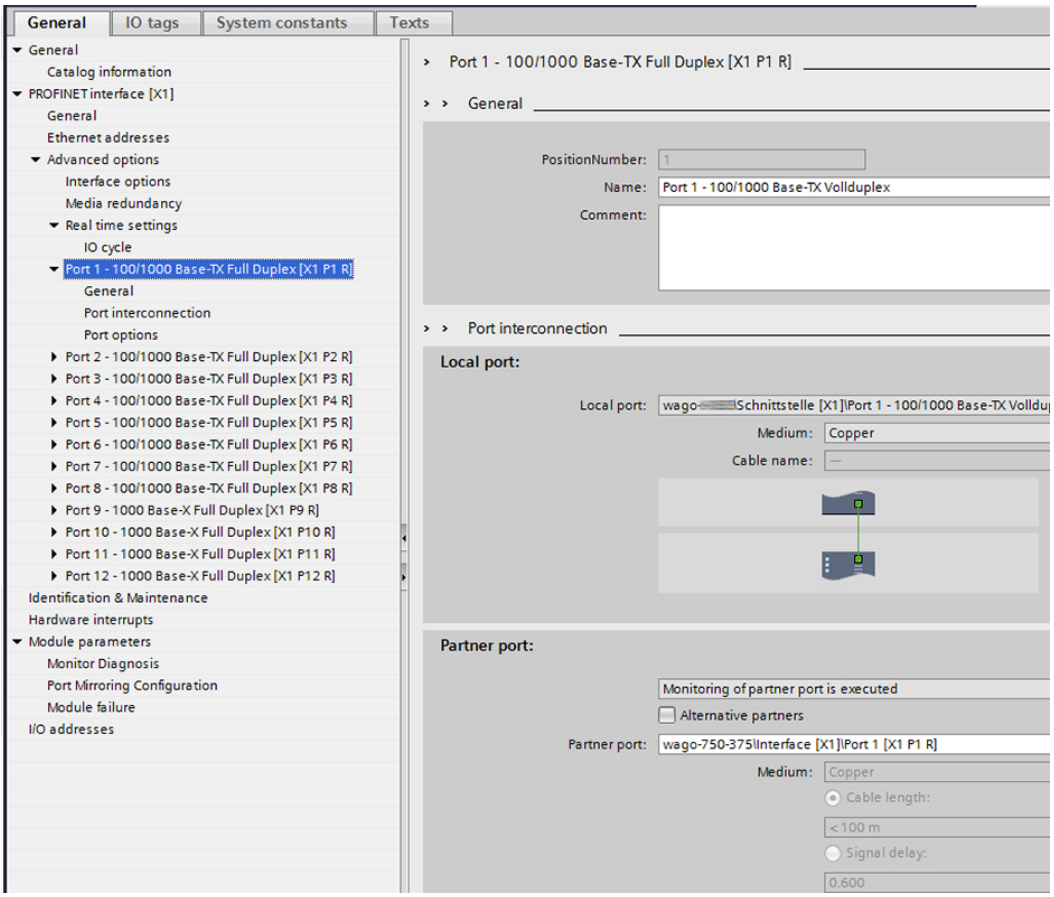
Ilustracja 19: Parametry PROFINET – obszar „Advanced options”

Tabela 25: Parametry PROFINET dla obszaru „Advanced options”

Parametr	Opis	Znacznik w GSDML
MRP domain	Nazwa MRP	–
Media redundancy role	Klient (MRC) lub Manager (MRM) w pierścieniu	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ MediaRedundancy
Ring port 1	Wskazanie 1. portu przypisanego do pierścienia MRP	–
Ring port 2	Wskazanie 2. portu przypisanego do pierścienia MRP	–
Update time	Czas trwania cyklu dla danych I/O	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ ApplicationRelations
Accepted update cycles without IO data	Współczynnik czasu aktualizacji, po przekroczeniu którego zostanie wygenerowany błąd.	–
Watchdog time	Iloczyn czasu aktualizacji i współczynnika	–

5.10.2.4 Obszar „Port 1”

Poniższe opisy przedstawiono przykładowo dla portu 1. Dotyczy to odpowiednio także portów od 2 do 12.



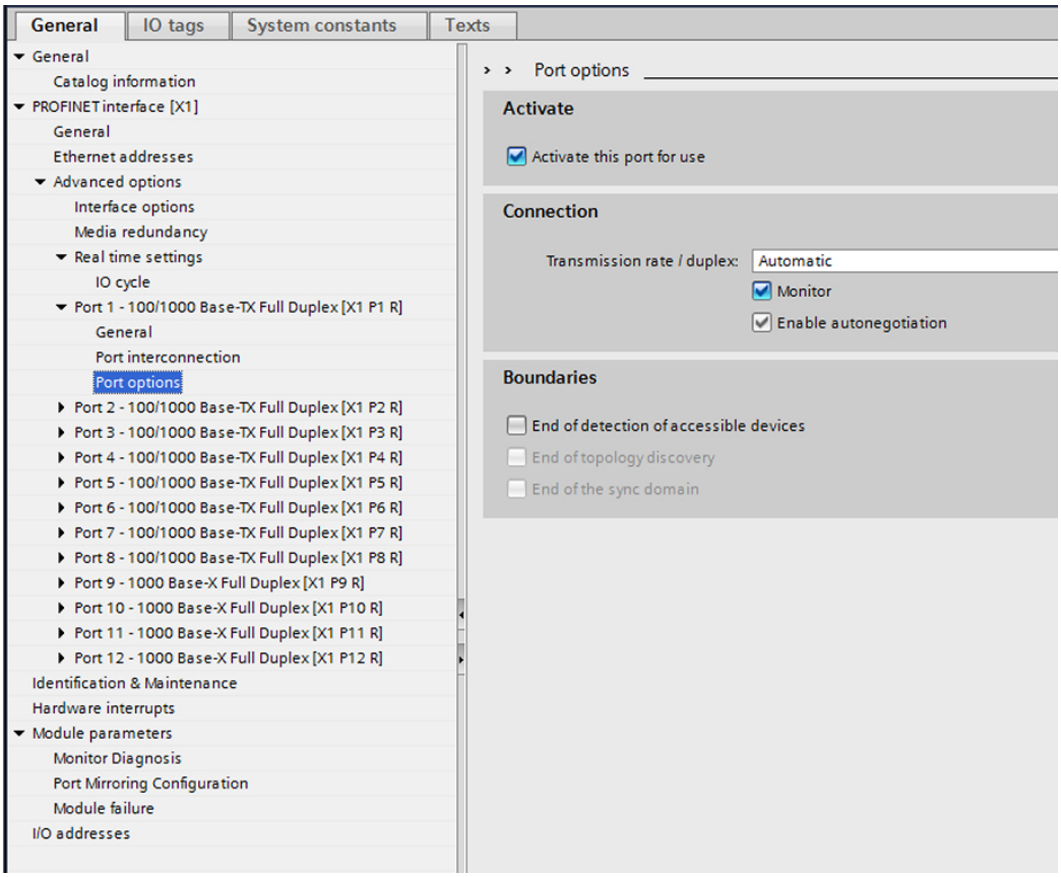
Ilustracja 20: Parametry PROFINET – obszar „Port 1”

Tabela 26: Parametry PROFINET® dla obszaru „Port 1”

Parametr	Opis	Znacznik w GSDML
Name	Nazwa portu	SystemDefinedSubmoduleList/ PortSubmoduleItem
Comment	Pole komentarza	–
Local Port	Wskazanie lokalnego portu	–
Medium	Medium transmisji	–
Partner port	Podłączony port	–

5.10.2.5 Obszar „Port options”

Poniższe opisy przedstawiono przykładowo dla portu 1. Dotyczy to odpowiednio także portów od 2 do 12.

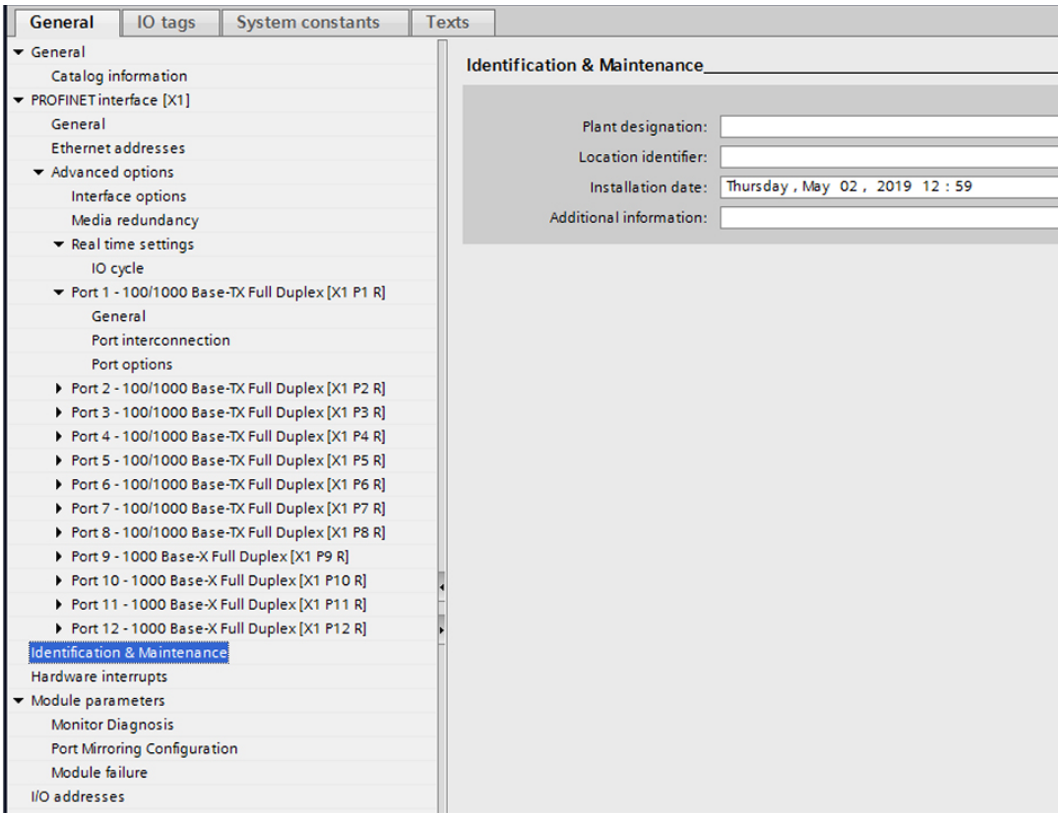


Ilustracja 21: Parametry PROFINET – obszar „General”

Tabela 27: Parametry PROFINET dla obszaru „Advanced options”

Parametr	Opis	Znacznik w GSDML
Activate	Aktywacja/dezaktywacja portu	–
Transmission rate/duplex	Ustawienie prędkości transmisji i trybu duplex	ValueList/ ValueItem[ID=“ID_RV_PORT_RATE”]
Monitor	Aktywacja/dezaktywacja monitorowania	–
Enable autonegotiation	Aktywacja/dezaktywacja autonegocjacji	–

5.10.2.6 Obszar „Identification & Maintenance“

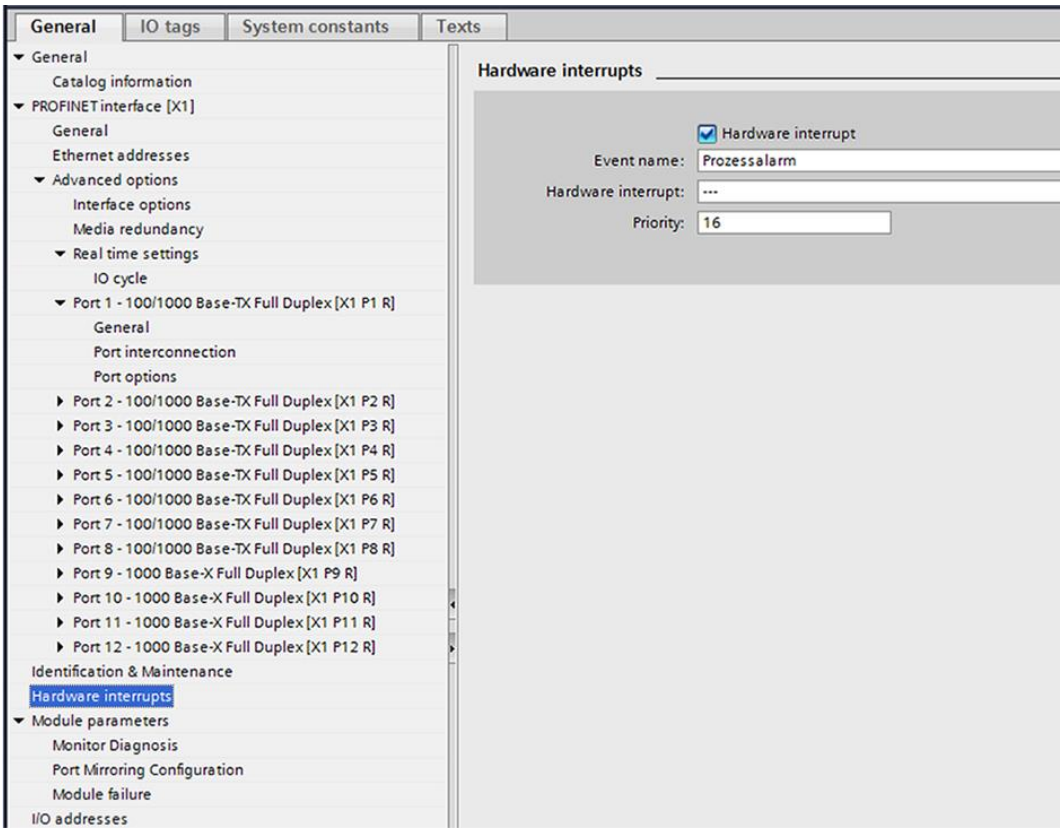


Ilustracja 22: Parametry PROFINET – obszar „Identification & Maintenance“

Tabela 28: Parametry PROFINET dla obszaru „Identification & Maintenance“

Parametr	Opis	Znacznik w GSDML
Plant designation	Oznaczenie instalacji	–
Location identifer	Oznaczenie miejsca montażu	–
Installation date	Data montażu	–
Additional information	Pole komentarza	–

5.10.2.7 Obszar „Process alarms“

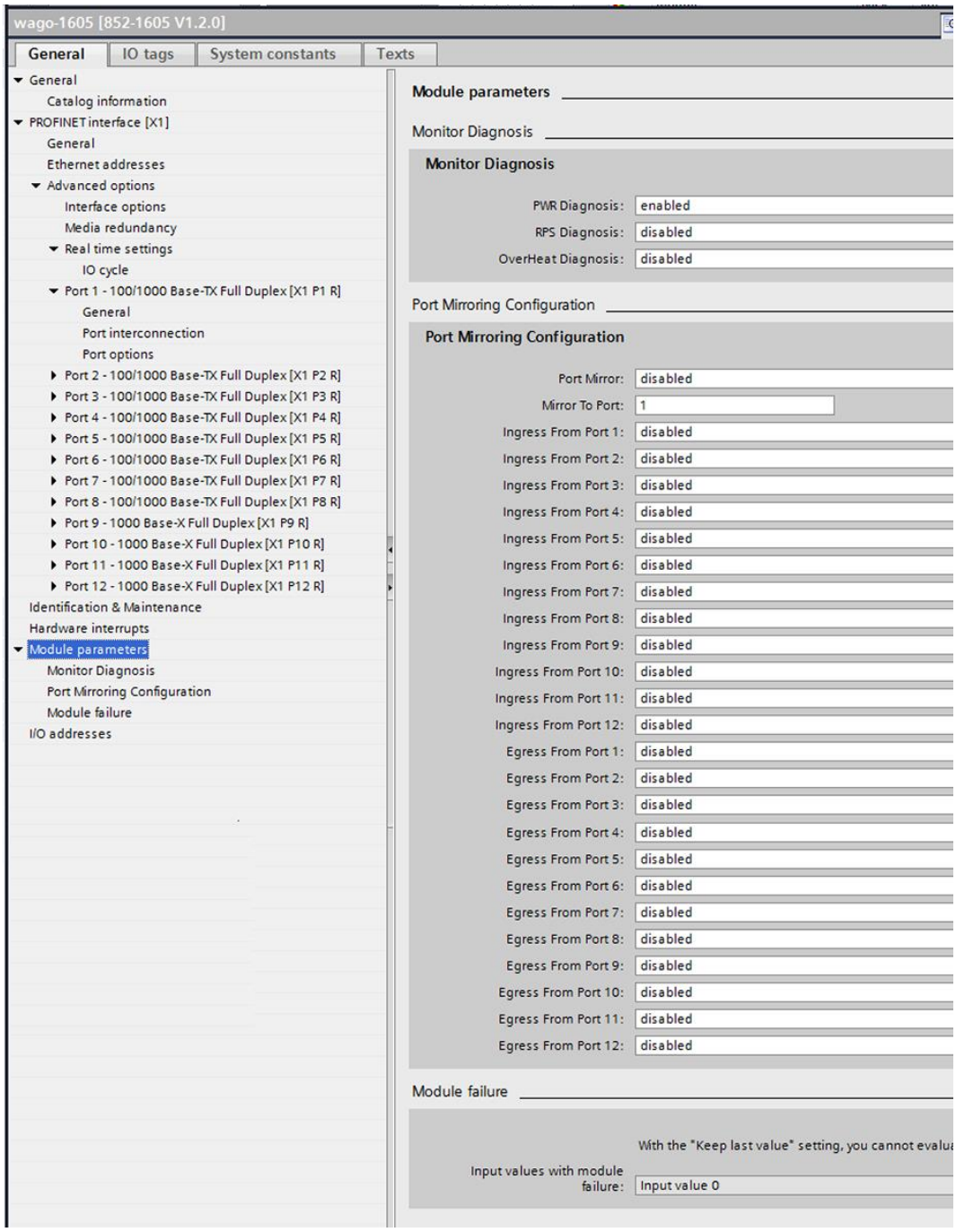


Ilustracja 23: Parametry PROFINET – obszar „Process alarms“

Tabela 29: Parametry PROFINET dla obszaru „Process alarms“

Parametr	Opis	Znacznik w GSDML
Event name	Nazwa alarmu	–
Hardware interrupt	Aktywacja/dezaktywacja monitorowania alarmów procesowych	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem
Priority	Priorytet przesyłania danych	–

5.10.2.8 Obszar „Assembly parameters“

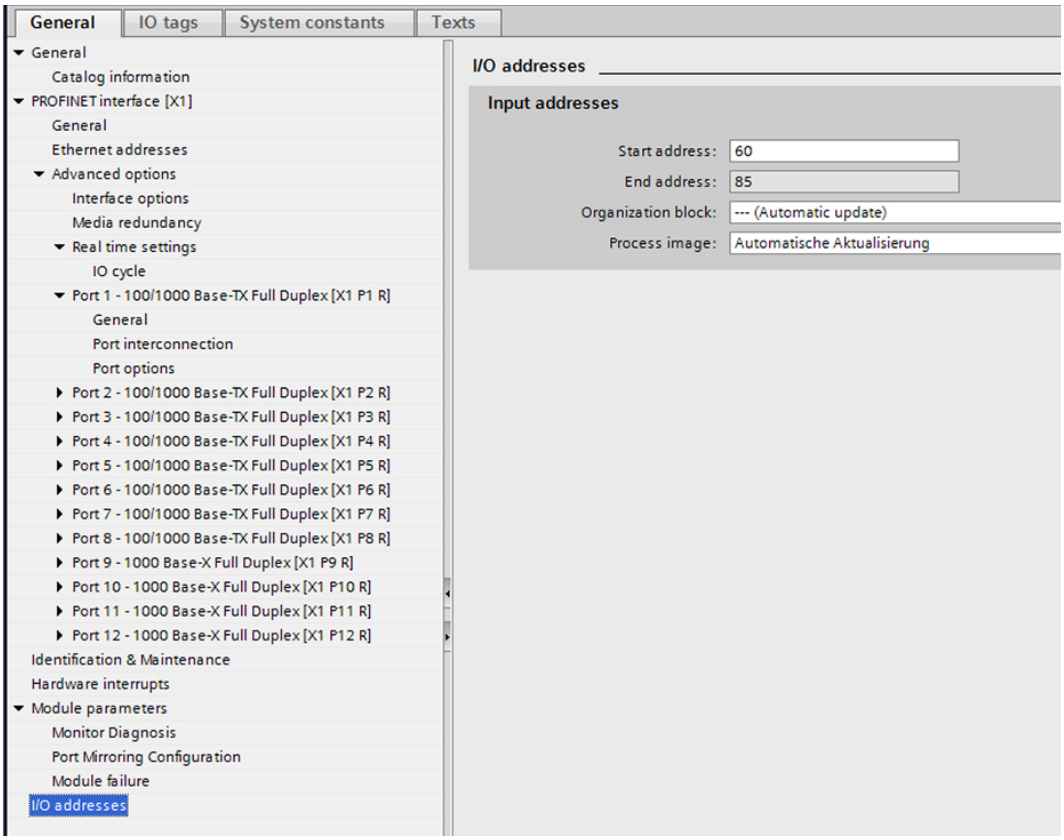


Ilustracja 24: Parametry PROFINET – obszar „Assembly parameters“

Tabela 30: Parametry PROFINET dla obszaru „Assembly parameters“

Parametr	Opis	Znacznik w GSDML
PWR Diagnosis	Diagnostyka „Zasilanie podstawowe“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “2”]
RPS Diagnosis	Diagnostyka „Zasilanie rezerwowe“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “3”]
OverHeat Diagnosis	Diagnostyka „Przegrzanie“	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “5”]
Port Mirror	Mirroring portu aktywowany/dezaktywowany	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Mirror To Port	Wskazanie, do którego portu ma być wykonywany mirroring.	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Ingress From Port (x)	Mirroring portu „Wejście“ dla portu (x) aktywowane/dezaktywowane	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Egress From Port (x)	Mirroring portu „Wyjście“ dla portu (x) aktywowane/dezaktywowane	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Input values with module failure	Wskazanie, jaka wartość ma być użyta w przypadku awarii podzespołu.	–

5.10.2.9 Obszar „IO adresses“



Ilustracja 25: Parametry PROFINET – obszar „IO adresses“

Tabela 31: Parametry PROFINET dla obszaru „IO adresses“

Parametr	Opis	Znacznik w GSDML
Start adress	Adres początkowy cyklicznego odwzorowania adresów	–
End Address	Generowany automatycznie	–
Organization block	Aktualizacja bloku organizacyjnego	–
Prozess image	Aktualizacja obrazu procesu danych I/O	–

5.11 Cykliczne dane I/O

Cykliczne dane I/O są przesyłane pomiędzy PLC a switchami w określonych odstępach czasu. Te dane są przesyłane niemal w czasie rzeczywistym. Na przykład informacje o statusie switchów oraz zmienne, które mają zostać zapisane w switchu, zazwyczaj są częścią danych cyklicznych.

Cykliczne dane I/O są powiązane z podmodułami.

Subslot 0 nie jest domyślnie używany dla podmodułów I/O.

PROFINET rozróżnia 3 typy podmodułów:

- Wirtualne podmoduły
- Podmoduły interfejsowe oraz
- Podmoduły portów.

Wszystkie te podmoduły mogą być powiązane z danymi I/O.

Podmoduł wirtualny jest zawsze zawarty w subslocie 1.

Switch zarządzalny PROFINET definiuje wszystkie cykliczne dane I/O tylko w wirtualnym podmodule. Ten wirtualny podmoduł jest przypisany do slotu 0/subslotu 1.

Cykliczne dane I/O obejmują 26 bajtów. Pierwsze 2 bajty danych zawierają informacje diagnostyczne urządzenia. Kolejne 24 bajty oznaczają informacje o statusie portów (2 bajty danych na informację o porcie).

Cykliczne dane I/O są generowane tylko wtedy, gdy zostały odpowiednio skonfigurowane w używanym oprogramowaniu narzędziowym.

Format cyklicznych danych I/O przedstawiono w poniższym zestawieniu.

Tabela 32: Format cyklicznych danych I/O – PROFINET

Offset bajtów	Zakres	Opis
0	16 b	Stan diagnostyczny switcha zarządzalnego PROFINET
2	16 b	Status PORT 1
4	16 b	Status PORT 2
6	16 b	Status PORT 3
8	16 b	Status PORT 4
10	16 b	Status PORT 5
12	16 b	Status PORT 6
14	16 b	Status PORT 7
16	16 b	Status PORT 8
18	16 b	Status PORT 9
20	16 b	Status PORT 10
22	16 b	Status PORT 11
24	16 b	Status PORT 12

5.11.1 Przykład cyklicznych danych I/O

Następujący przykład oparty jest na narzędziu projektowym „TIA” firmy Siemens.

Dla cyklicznych danych I/O, które są adresowane za pomocą slotu 0/subslotu 1, TIA Portal automatycznie generuje adres mapowania po tym, jak zostały przeciągnięte metodą drag & drop z katalogu sprzętu do widoku sieci.

Użytkownik może użyć adresu mapowania, aby uzyskać dostęp do każdego bitu danych za pomocą znaczników PLC.

Dane są przedstawione w formacie WORD (16 b).

W poniższym zestawieniu znajduje się szczegółowa struktura danych:

Tabela 33: Cykliczne wejście dla diagnostyki urządzenia

Znacznik	Bit	Opis	Wartość	Uwaga
DIAG.%X0	0	pn_diagcode_board_temp	0 = NO 1 = YES	Przegrzanie płyty głównej
DIAG.%X1	1	pn_diagcode_cpu_temp	0 = NO 1 = YES	Przegrzanie CPU
DIAG.%X2	2	pn_diagcode_phy_temp	0 = NO 1 = YES	Przegrzanie PHY
DIAG.%X3	3	pn_diagcode_pwr_ovolt	0 = NO 1 = YES	Przepięcie w zasilaniu podstawowym
DIAG.%X4	4	pn_diagcode_rps_ovolt	0 = NO 1 = YES	Przepięcie w zasilaniu rezerwowym

Tabela 33: Cykliczne wejście dla diagnostyki urządzenia

Znacznik	Bit	Opis	Wartość	Uwaga
DIAG.%X5	5	pn_diagcode_pwr_uvolt	0 = NO 1 = YES	Spadek napięcia poniżej zakresu w zasilaniu podstawowym
DIAG.%X6	6	pn_diagcode_rps_uvolt	0 = NO 1 = YES	Spadek napięcia poniżej zakresu w zasilaniu rezerwowym
DIAG.%X7	7	pn_diagcode_pwr_nopwr	0 = NO 1 = YES	Brak zasilania podstawowego
DIAG.%X8	8	pn_diagcode_rps_nopwr	0 = NO 1 = YES	Brak zasilania rezerwowego
DIAG.%X9	9	MRP Ring State	0 = inaktive 1 = aktive	
DIAG.%X10	10	MRP Ring Running Status	0 = closed 1 = open	Wskazówka: Ma sens tylko przy DIAG.%X9 = 1
DIAG.%X11 … DIAG.%X14	11 … 14	Zarezerwowane		
DIAG.%X15	15	Device Status	0 = OK 1 = error	Stos PROFINET nie generuje alarmu przy: DIAG.%X15 = 0

Tabela 34: Cykliczne wejście dla stanu portu Pn (n = 1 … 12)

Znacznik	Bit	Opis	Wartość	Uwaga
Pn.%X0	0	Port Power Status	0 = off 1 = on	
Pn.%X1	1	Port Duplex Mode	0 = full duplex 1 = half duplex	
Pn.%X2	2	Port Link Status	0 = link off 1 = link on	
Pn.%X3	3	Port Speed	0b000 = 10M 0b001 = 100M 0b010 = 1000M 0b111 = Auto	Ten bit jest łączony z Pn.%X4 i Pn.%X5.
Pn.%X4	4			
Pn.%X5	5			
Pn.%X6	6	Port Current Link Activity	1 = disable 2 = block 3 = listen 4 = learn 5 = foward	Ten bit jest łączony z Pn.%X7 i Pn.%X8.
Pn.%X7	7			
Pn.%X8	8			
Pn.%X9	9	Port LLDP Admin Status	0 = disabled 1 = Txonly 2 = Rxonly 3 = TxRx	Ten bit jest łączony z Pn.%X10.
Pn.%X10	10			
Pn.%X11 … Pn.%X15	11 … 15	Zarezerwowane		

5.12 Parametry DAP

Parametry DAP są używane do konfiguracji IO device. Po uruchomieniu IO device przesyłane są te parametry:

- IO controller odczytuje te parametry z IO device, aby rozpoznać funkcje IO device.
- IO controller zapisuje te parametry w IO device, aby skonfigurować funkcje IO device.

Dla swicha zarządzalnego PROFINET udostępniane są następujące parametry DAP:

Tabela 35: Parametry DAP dla switcha PROFINET WAGO

Indeks	Subslot	Dostęp	Długość	Opis
1	0x1	R/W	3	Aktywacja/dezaktywacja komunikatów diagnostycznych
2	0x8001 … 0x800C	R	6	Odczyt statusu portu (na port)
3	0x1	R	12	Odczyt diagnostyki urządzenia
4	0x1	R/W	10	Konfigurowanie funkcji mirroringu portu

Poniżej przedstawiono szczegółową strukturę danych poszczególnych indeksów parametrów.

INDEKS=1

Tabela 36: Aktywacja/dezaktywacja komunikatów diagnostycznych

Offset	Wartość	Opis	Wartość domyślna
0	0	Aktywacja alarmu „PWR Diagnose”	0
	1	Dezaktywacja alarmu „PWR Diagnose”	
1	0	Aktywacja alarmu „RPS Diagnose”	0
	1	Dezaktywacja alarmu „RPS Diagnose”	
2	0	Aktywacja diagnostyki temperatury	0
	1	Dezaktywacja diagnostyki temperatury	

INDEKS=2

Tabela 37: Odczyt statusu portu (dla każdego portu)

Offset	Wartość	Opis	Wartość domyślna
0	0	Port wyłączony	0
	1	Port włączony	
1	0	Port: tryb – full duplex	0
	1	Port: tryb – half duplex	
2	0	Port: łącze – wyłączone	0
	1	Port: łącze – włączone	
3	0	Port: prędkość transmisji – 10 Mbit/s	0
	1	Port: prędkość transmisji – 100 Mbit/s	
	2	Port: prędkość transmisji – 1 Gb/s	
	7	Port: prędkość transmisji – automatyczna	
4	1	Port: aktywność łącza – disabled	5
	2	Port: aktywność łącza – blocked	
	3	Port: aktywność łącza – listen	
	4	Port: aktywność łącza – learn	
	5	Port: aktywność łącza – forward	
5	0	Port: status LLDP Admin – disabled	0
	1	Port: status LLDP Admin – Tx only	
	2	Port: status LLDP Admin – Rx only	
	3	Port: status LLDP Admin – Tx/Rx	

INDEKS=3

Tabela 38: Odczyt diagnostyki urządzenia

Offset	Wartość	Opis	Wartość domyślna
0	0	Płyta główna – brak przegrzania	0
	1	Płyta główna – przegrzanie	
1	0	CPU – brak przegrzania	0
	1	CPU – przegrzanie	
2	0	ETHERNET PHY – brak przegrzania	0
	1	ETHERNET PHY – przegrzanie	
3	0	PWR – brak przepięcia	0
	1	PWR – przepięcie	
4	0	RPS – brak przepięcia	0
	1	RPS – przepięcie	
5	0	PWR – brak spadku napięcia poniżej zakresu	0
	1	PWR – spadek napięcia poniżej zakresu	
6	0	RPS – brak spadku napięcia poniżej zakresu	0
	1	RPS – spadek napięcia poniżej zakresu	
7	0	PWR ma napięcie.	0
	1	PWR nie ma napięcia.	
8	0	RPS ma napięcie.	0
	1	RPS nie ma napięcia.	
9	0	MRP ring dezaktywowany	0
	1	MRP ring aktywowany	
10	0	MRP ring otwarty (sensowne, gdy bajt 9 = 1)	0
	1	MRP ring zamknięty (sensowne, gdy bajt 9 = 1)	
11	0	Urządzenie zgłasza błąd (alarm).	0
	1	Urządzenie działa prawidłowo, brak alarmu.	

INDEX=4, Configure Port Mirror

Tabela 39: Konfiguracja funkcji mirroringu portu

Offset bajtów	Offset bitów	Wartość	Opis	Wartość domyślna
0	–	0	Dezaktywacja mirroringu portu	0
		1	Aktywacja mirroringu portu	
1	–	0 … 255	Port docelowy do mirroringu	0
2	0	0	Dezaktywacja mirroringu dla wejścia portu 1.	0
		1	Aktywacja mirroringu dla wejścia portu 1.	
	1	0	Dezaktywacja mirroringu dla wejścia portu 2.	0
		1	Aktywacja mirroringu dla wejścia portu 2.	
…				
3	3	0	Dezaktywacja mirroringu dla wejścia portu 12.	0
		1	Aktywacja mirroringu dla wejścia portu 12.	
…				
6	0	0	Dezaktywacja mirroringu dla wyjścia portu 1.	0
		1	Aktywacja mirroringu dla wyjścia portu 1.	
…				
9	7	0	Dezaktywacja mirroringu dla wyjścia portu 12.	0
		1	Aktywacja mirroringu dla wyjścia portu 12.	

W przeciwieństwie do cyklicznych danych I/O dostęp do parametrów DAP odbywa się za pomocą bloków funkcyjnych RDREC/WRRREC (np. w TIA; patrz także informację aplikacyjną dotyczącą switcha zarządzalnego PROFINET WAGO).

5.13 Dostęp przez port konsolowy (CLI)

5.13.1 Nadawanie adresu IP za pomocą portu konsolowego

Switch zarządzalny PROFINET jest dostarczany z następującymi ustawieniami IPv4.

- Adres IP 0.0.0.0
- Maska podsieci 0.0.0.0
- Brama domyślna 0.0.0.0

W trybie PROFINET parametry sieciowe mogą być przypisywane wyłącznie przez narzędzie inżynieryjne lub sterownik PROFINET.

Poniżej opisano, jak za pomocą portu konsolowego można skonfigurować adres IP switcha zarządzalnego PROFINET.

1. Połącz komputer z portem konsolowym switcha za pomocą odpowiedniego przewodu.

2. Użyj następujących ustawień portu konsolowego:

Tabela 40: Domyślne ustawienia dla portu konsolowego

Ustawienie	Wartość domyślna
Baud Rate (prędkość transmisji)	38400
Parity (parzystość)	None
Number of Data Bits (liczba bitów danych)	8
Number of Stop Bits	1
Flow Control	None

3. Naciśnij **[ENTER]**, aby wywołać ekran logowania.

```
L2SWITCH login:
```

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

```
PN-SWITCH login: admin
PN-SWITCH>
```

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

```
PN-SWITCH>enable
user:admin
password: wago
```

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

```
PN-SWITCH#show running-config
Current configuration:
vlan 1
name VLAN1
fixed 1-12
!
interface gigabitethernet1/0/1
!
interface gigabitethernet1/0/2
!
interface gigabitethernet1/0/3
!
interface gigabitethernet1/0/4
!
interface gigabitethernet1/0/5
!
interface gigabitethernet1/0/6
!
interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
interface gigabitethernet1/0/10
!
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 0.0.0.0/0
ip address default-gateway 0.0.0.0
!
profinet enable
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-1605
```

7. Wpisz **[configure terminal]**, aby skonfigurować urządzenie.

```
PN-SWITCH#configure terminal
PN-SWITCH(config)#
```

8. Wpisz **[profinet disable]**, aby dezaktywować PROFINET w urządzeniu.

```
PN-SWITCH(config)#profinet disable
Sukces!
```

9. Wpisz **[interface eth0]**, aby skonfigurować parametry sieciowe switcha.

```
PN-SWITCH(config)#interface eth0
PN-SWITCH(config-if)#
```

10. Wpisz **[ip address 192.168.1.254/24]**, aby skonfigurować nowy adres IP (np. 192.168.1.254) lub maskę podsieci (np. 255.255.255.0).

```
PN-SWITCH(config-if)#ip 192.168.1.254/24
Uwaga: brama domyślna znajduje się w innej podsieci niż
adres IP.
```

11. Wpisz **[exit]**, aby opuścić menu konfiguracji parametrów sieci.

```
PN-SWITCH(config-if)#exit
PN-SWITCH(config)#
```

12. Wpisz **[exit]**, aby opuścić menu konfiguracji urządzenia.

```
PN-SWITCH(config)#exit
PN-SWITCH#
```

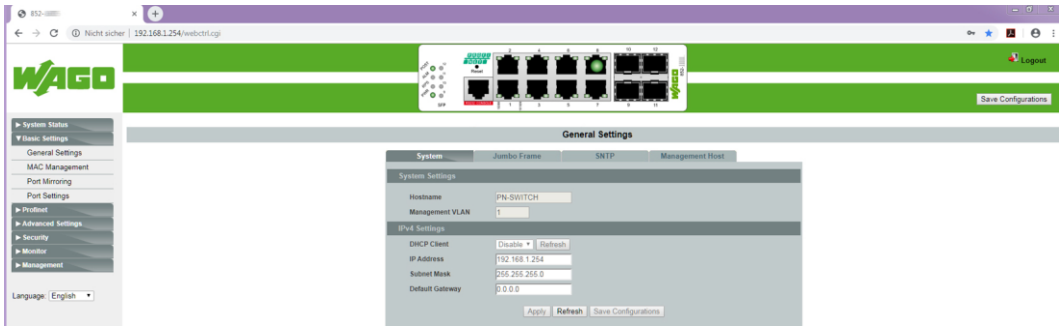
13. Wpisz **[show running config]**, aby zobaczyć aktualną konfigurację urządzenia.

```
PN-SWITCH#show running-config
Current configuration:
vlan 1
name VLAN1
fixed 1-12
!
interface gigabitethernet1/0/1
!
interface gigabitethernet1/0/2
!
interface gigabitethernet1/0/3
!
interface gigabitethernet1/0/4
!
interface gigabitethernet1/0/5
!
interface gigabitethernet1/0/6
!
interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
```

```
interface gigabitethernet1/0/10
!
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 192.168.1.254/24
ip address default-gateway 0.0.0.0
!
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-1605
```

Teraz można uzyskać dostęp do switcha zarządzalnego PROFINET pod adresem IP 192.168.1.254 za pomocą przeglądarki internetowej.



Ilustracja 26: Dostęp do switcha zarządzalnego PROFINET przez WBM

5.14 Parametryzacja przez WBM w trybie PROFINET

W celu konfiguracji i zarządzania switchem zarządzalnym PROFINET do dyspozycji jest wewnętrzny system plików oraz zintegrowany serwer WWW, określany mianem systemu zarządzania przez WWW, w skrócie WBM („**W**eb **B**ased-**M**anagement system”).

Switch zarządzalny PROFINET jest dostarczany z aktywowanym trybem PROFINET. Fabrycznie zadane są następujące ustawienia:

- Adres IP: 0.0.0.0
- Maska podsieci: 0.0.0.0

Aby korzystać z WBM, należy najpierw przydzielić adres IP. Istnieje tu wiele możliwości:

- przez odpowiednie narzędzie do projektowania (patrz rozdział „Projektowanie”)
- przez port konsolowy (patrz także rozdział „Dostęp przez port konsolowy (CLI)”)
- przez DCP za pomocą zewnętrznego narzędzia (np. PRONETA firmy Siemens lub PROFINET Commander)

W trybie PROFINET funkcjonalność WBM jest ograniczona.

Wskazówka



Więcej informacji o WBM
W tym rozdziale znajdują się opisy funkcji, które można zrealizować w aktywowanym trybie PROFINET za pomocą WBM.
Szczegółowe informacje o WBM można znaleźć w rozdziale „Konfiguracja w systemie zarządzania przez WWW (WBM)“.

Jeśli tryb PROFINET jest aktywny, wiele parametrów konfiguruje IO controller. Jeżeli konfiguracja w WBM nie jest możliwa, w systemie WBM pojawia się komunikat „**Konfiguracja odbywa się w trybie PROFINET przez sterownik PNIO**”.

WBM jest dostępny pod skonfigurowanym adresem IP.

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 zrestartować system.

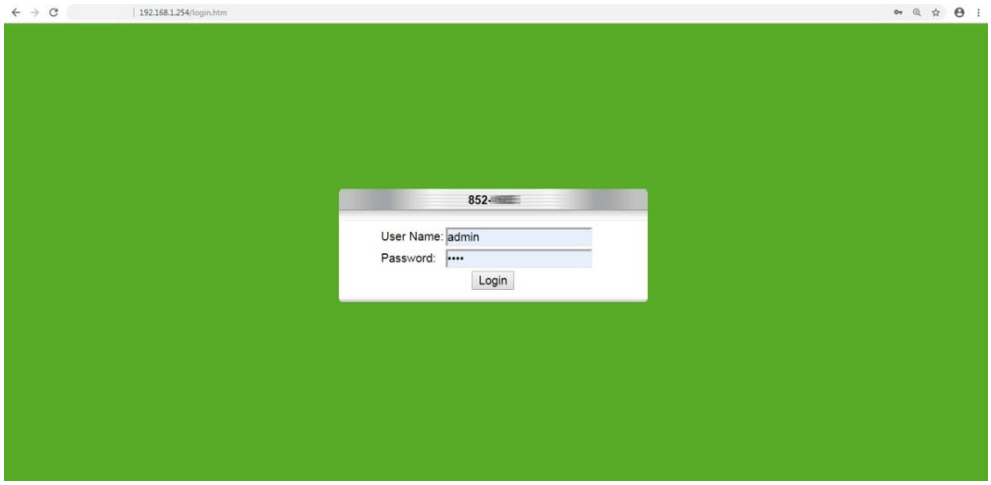
1. Aby otworzyć WBM, uruchom przeglądarkę internetową. Do korzystania z WBM zaleca się używanie aktualnej przeglądarki Google Chrome lub Firefox.

2. W pasku adresu wpisz adres IP switcha zarządzalnego PROFINET.

3. Potwierdź przyciskiem **[Enter]**.

4. W oknie logowania wprowadź swoją nazwę użytkownika oraz hasło:

   Default-User = „admin“
   Default-Passwort = „wago“



Ilustracja 27: Okno logowania do WBM

   WAGO zaleca zmianę nazwy użytkownika i hasła po 1. logowaniu. Te ustawienia znajdziesz w menu **Management** > **SNMP** > **User Account**.

5. Zostanie wyświetlona strona startowa WBM.

6. Wprowadź żądane ustawienia.

7. Wprowadzone zmiany potwierdź przyciskiem **[Apply]** lub **[Update]** albo porzuć przyciskiem **[Delete]** lub **[Discard]**.

8. Aby przejąć ustawienia, potwierdź zmiany przyciskiem **[Save configuration]**.

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

Tabela 41: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM)

Linki do nawigacji i strony WBM
▶ **[Systemstatus]**
• System Information
▶ **[Basic Settings]**
• General Settings • Port Mirroring • Port Settings
▶ **[PROFINET]**
• Configuration • Information • Diagnostics
▶ **[Advanced Settings]**
• MRP
▶ **[Security]**
▶ **[Monitor]**
▶ **[Management]**
[SNMP] • Upload File • User Account

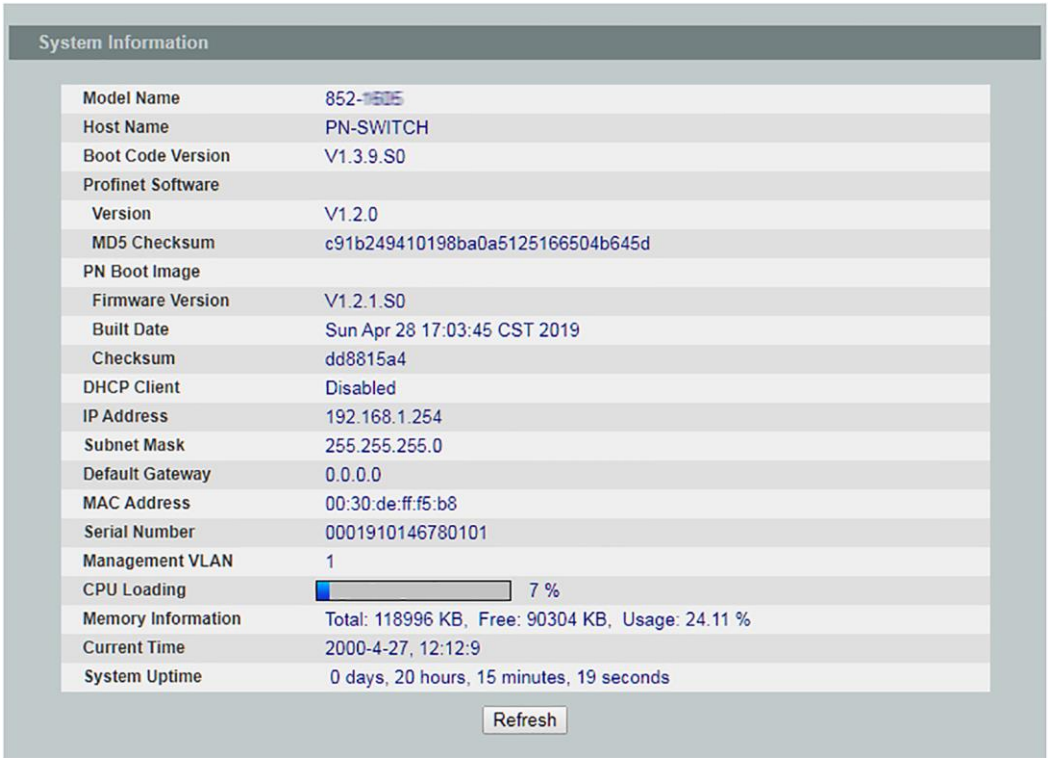
Na tych stronach WBM można wprowadzać ustawienia/konfiguracje dla switcha zarządzalnego PROFINET.

Na niektórych stronach WBM istnieją zakładki, zawierające poszczególne strony do wprowadzania ustawień/konfiguracji.

Wartości domyślne przedstawiane są czcionką **pogrubioną.**

5.14.1 System Status

5.14.1.1 System Information



Ilustracja 28: Strona WBM „System Information”

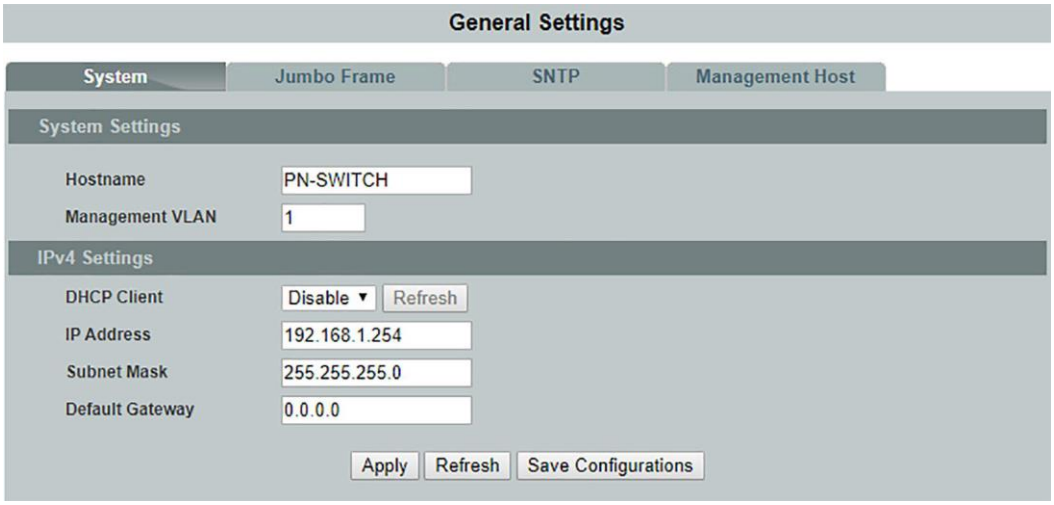
Tabela 42: Strona WBM „System Information” (przykład 852-1605 możliwy do przeniesienia na 852-0602, -0603).

Parametr	Opis
Model Name	W tym polu wyświetlana jest nazwa modelu switcha.
Host Name	W tym polu wyświetlana jest nazwa hosta switcha.
Boot Code Version	W tym polu wyświetlana jest wersja boot code.
Profinet Software Version	Numer identyfikacyjny wersji oprogramowania PROFINET
Profinet Software MD5 Checksum	Suma kontrolna wersji oprogramowania PROFINET
PN Boot Image Firmware Version	W tym polu wyświetlana jest wersja „PN Boot Image”.
PN Boot Image Build Date	W tym polu wyświetlana jest data wygenerowania firmware'u.
PN Boot Image Checksum	W tym polu wyświetlana jest suma kontrolna „PN Boot Image”.
DHCP Client	W tym polu wyświetlana jest informacja, czy aktywowana jest funkcja „DHCP Client“.
IP Address	W tym polu wyświetlany jest adres IP switcha.
Subnet Mask	W tym polu wyświetlana jest maska podsieci switcha.
Default Gateway	W tym polu wyświetlana jest domyślna brama switcha.
MAC Address	W tym polu wyświetlany jest adres MAC (Media Access Control) switcha.
Serial Number	W tym polu wyświetlany jest numer serii.
Management VLAN	W tym polu wyświetlany jest VLAN ID, potrzebny do realizacji procesów zarządzania switchem.
CPU Loading	W tym polu wyświetlane jest obłożenie switcha w procentach.
Memory Information	W tym polu wyświetlana jest całkowita („Total”) oraz aktualnie dostępna („Free”) i używana („Usage”) pamięć switcha.
Current Time	W tym polu wyświetlana jest aktualna data (yyyy-mm-dd) i godzina (hh:mm:ss).
System Uptime	W tym polu wyświetlany jest czas, przez który działa switch od momentu włączenia: dni, godziny, minuty i sekundy.

5.14.2 General Settings

5.14.2.1 General Settings

5.14.2.1.1 System



Ilustracja 29: Strona WBM „General Settings“ – zakładka „System“

Tabela 43: Strona WBM „General Settings“ – zakładka „System“

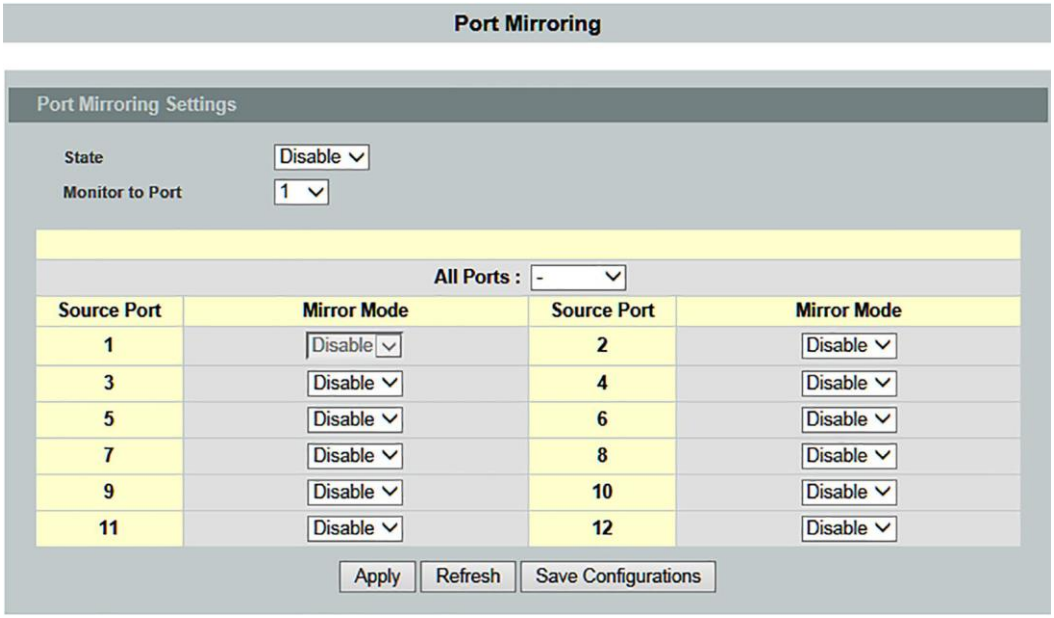
System Settings		
Parametr	**Domyślnie**	**Opis**
Hostname	**PN-SWITCH**	Należy wpisać nazwę switcha, składającą się z maksymalnie 64 liter/cyfr. Nazwa hosta powinna składać się z kombinacji cyfr, liter, łączników (-) lub podkreśleń (_).
Management VLAN	**1**	Należy wpisać grupę VLAN, która ma uzyskać dostęp do switcha. Właściwy zakres VLAN: 1 … 4094.
		Wskazówka  **Konfiguracja Management VLAN** Przed konfiguracją Management VLAN należy najpierw utworzyć Management VLAN i przypisać co najmniej jeden port.
IPv4 Settings		
Parametr	**Domyślnie**	**Opis**
DHCP Client	**Disable**	W polu wyboru należy wybrać „Disable“, gdy adres IP switcha ma być skonfigurowany ręcznie.
	Enable	W polu wyboru należy wybrać „Enable“, aby switch przyjął adres IP wygenerowany automatycznie przez serwer DHCP. Należy kliknąć **[Renew]**, aby switch ponownie przyjął adres IP z serwera DHCP.
IP Address	**0.0.0.0**	W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami.
Subnet Mask	**0.0.0.0**	W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.
Default Gateway	0.0.0.0	W polu edycji należy wpisać adres IP domyślnej bramy, używając zapisu z kropkami.

5.14.2.2 Port Mirroring

UWAGA



Błędny mirroring może zakłócić działanie aplikacji!
Z powodu błędnego mirroringu portów aplikacja może ulec zakłóceniu lub stać się niestabilna. W takim przypadku switch w trybie PROFINET można po prostu ponownie uruchomić. Dzięki temu IO controller nadpisze błędne ustawienia aktualną konfiguracją.



Ilustracja 30: Strona WBM „Port Mirroring“

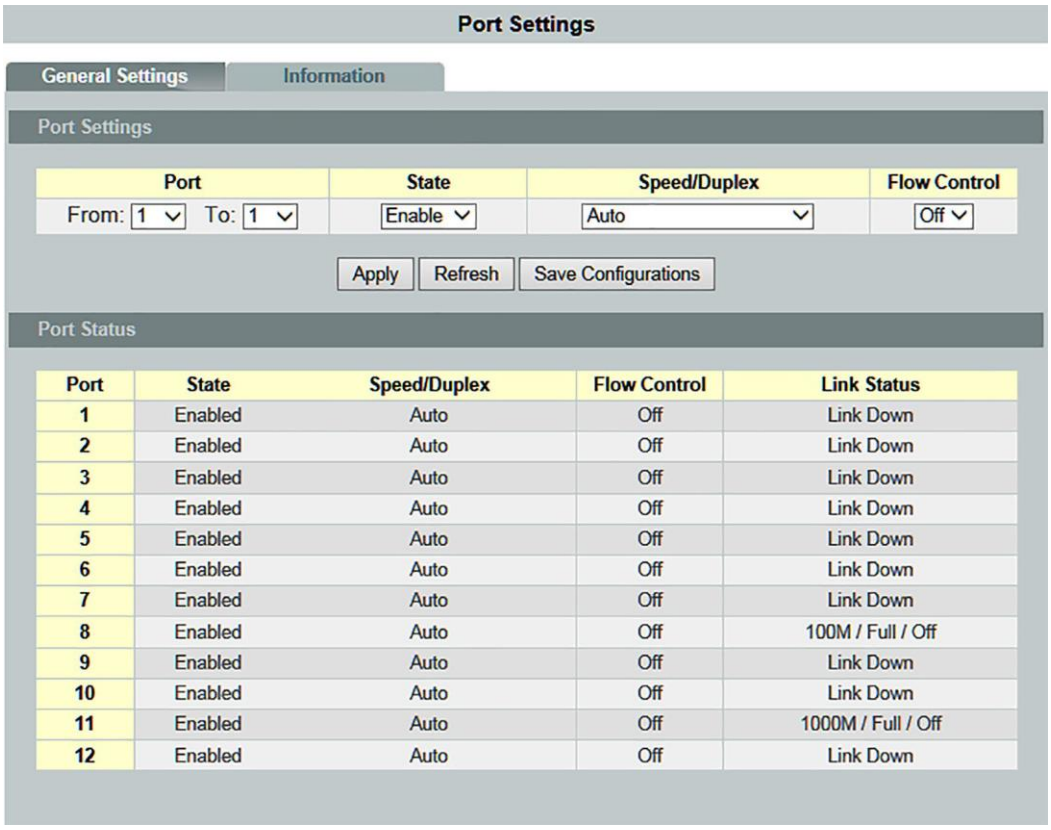
Tabela 44: Strona WBM „Port Mirroring“

Parametr	Domyślnie	Opis
Status	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Port Mirroring”.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Port Mirroring”.
Monitor to Port	**1** … 10 (12)	W polu wyboru należy wybrać port, który ma być połączony z „Network Traffic Analyzer“.
All Ports	**–**	Ustawienia w tym polu wyboru oddziałują na wszystkie porty. Należy tu wprowadzać tylko takie ustawienia, które mają dotyczyć wszystkich portów. Należy rozpocząć od ustawień ogólnych, a następnie wprowadzać ustawienia dla poszczególnych portów.
	Disable	
	Ingress	
	Egress	
	Both	
Source Port	**1** … 10 (12)	W tej kolumnie wyświetlany jest numer poszczególnych „Source Ports”.
Mirror Mode	**Disable**	W polu wyboru należy wybrać „Disable“, gdy ruch danych nie ma być skopiowany z wyspecyfikowanych „Source Ports“ do „Monitor Port“.
	Ingress	W polu wyboru należy wybrać „Ingress“, aby skopiować tylko dane wchodzące wyspecyfikowanych „Source Ports” do „Monitor Port”.
	Egress	W polu wyboru należy wybrać „Egress“, aby skopiować tylko dane wychodzące wyspecyfikowanych „Source Ports” do „Monitor Port”.
	Both	W polu wyboru należy wybrać „Both“, aby skopiować dane wchodzące i wychodzące z wyspecyfikowanych „Source Ports“ do „Monitor Port“.

Switch zarządzalny PROFINET umożliwia mirroring wielu portów. Oznacza to, że kilka portów może być mirrorowanych na jeden port docelowy.

Reset tych ustawień można przeprowadzić przez reset lub ponowne uruchomienie switcha.

5.14.2.3 Port Settings



Ilustracja 31: Strona WBM „Port Settings“ – zakładka „General Settings“

W trybie PROFINET ta strona służy wyłącznie do celów informacyjnych. Zmiana ustawień nie jest możliwa.

5.14.3 PROFINET

5.14.3.1 PROFINET Setting



Ilustracja 32: Strona WBM „PROFINET Setting“

W ustawieniach fabrycznych aktywowany jest tryb PROFINET.

UWAGA

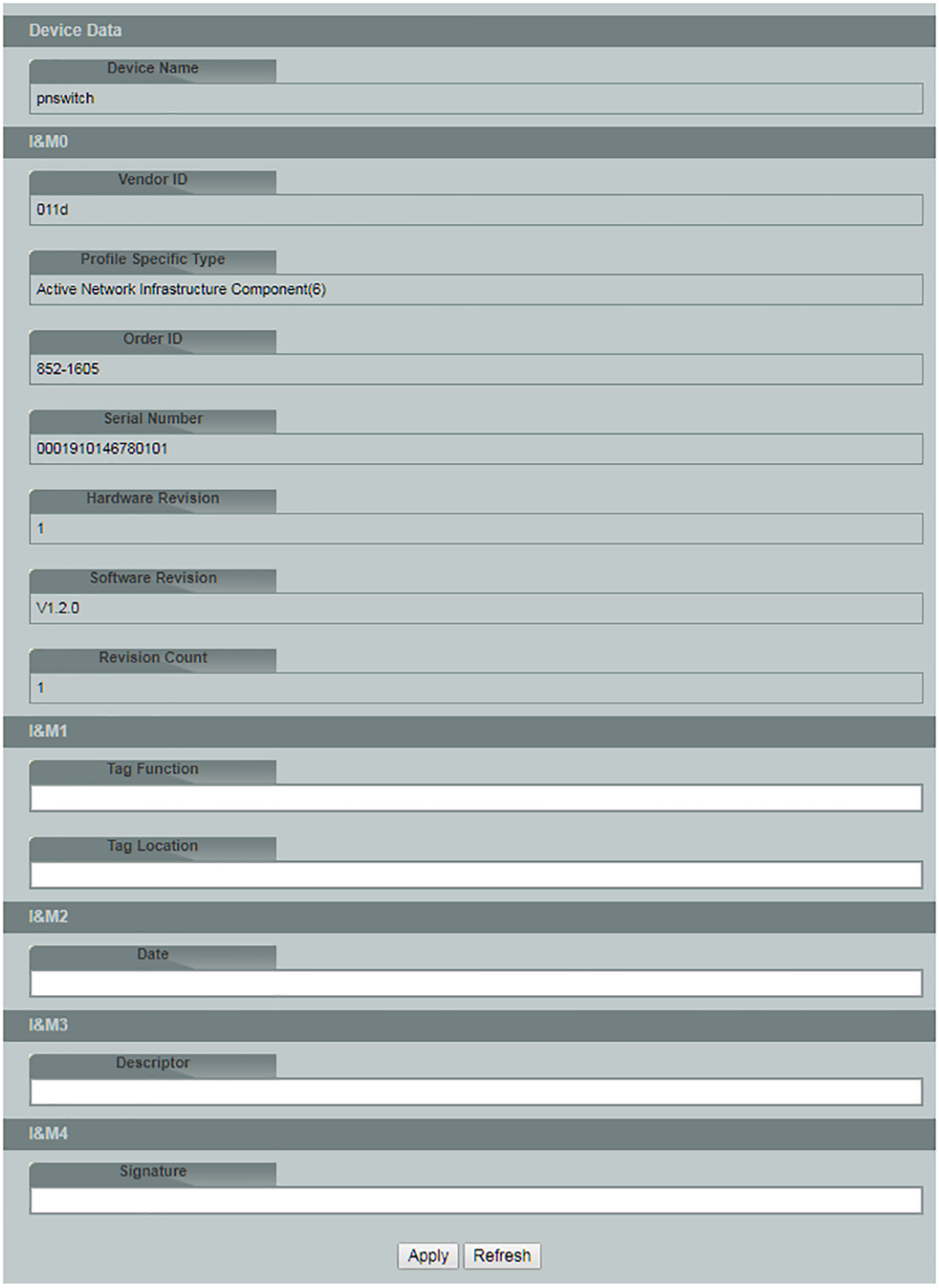


Ustawienia WBM w trybie PROFINET mogą powodować nieprawidłowe działanie!
Jeśli switch zarządzalny PROFINET jest w trybie PROFINET, jest on konfigurowany przez IO controllera. Zmiany ustawień w WBM mogą spowodować nieprawidłowe działanie switcha w sieci PROFINET.
Reset switcha spowoduje ponowne wgranie konfiguracji przez IO controllera do urządzenia. W ten sposób błędne konfiguracje zostaną nadpisane.

Tabela 45: Strona WBM „PROFINET Setting“

Parametr	Domyślnie	Opis
Status	**Enable**	W polu wyboru należy wybrać „Enable“, aby włączyć „PROFINET Setting”.
	Disable	W polu wyboru należy wybrać „Disable“, aby wyłączyć „PROFINET Setting”.

5.14.3.2 Information



Ilustracja 33: Strona WBM „Information“

5.14.3.3 Diagnosis List

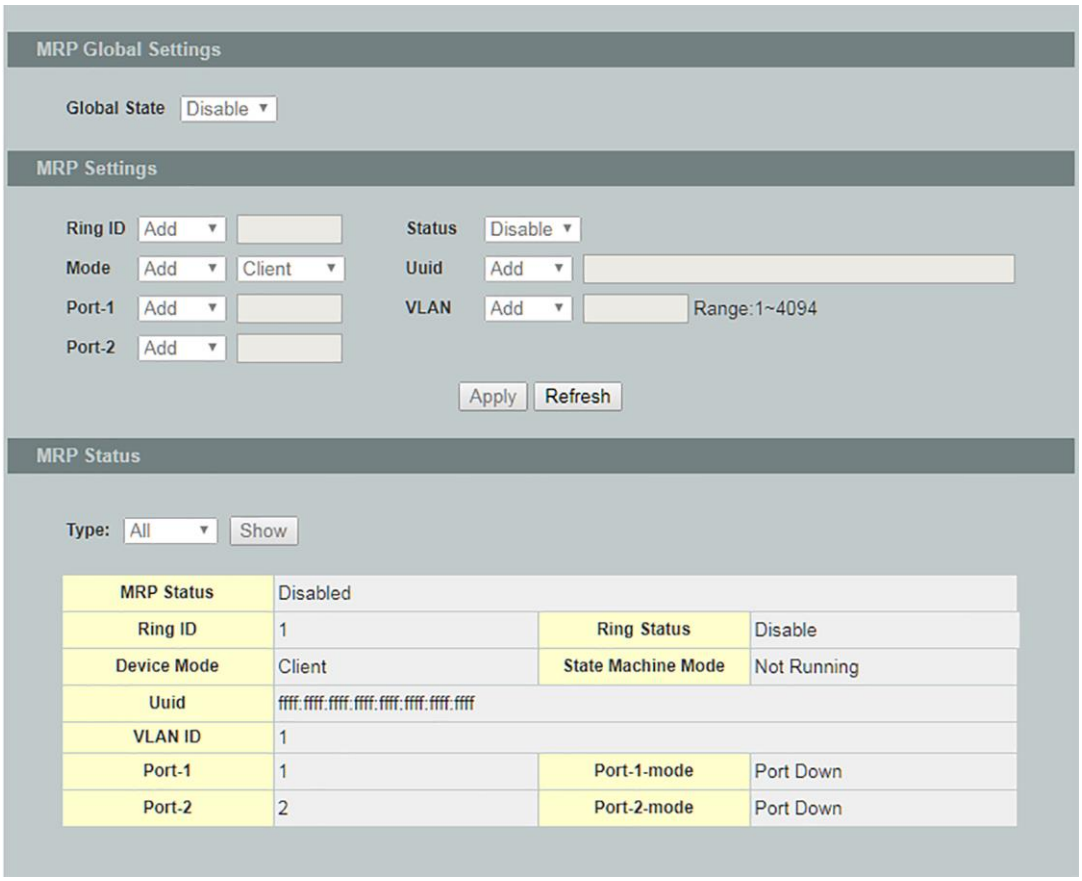


Ilustracja 34: Strona WBM „Diagnosis List”

Ta strona służy do wyświetlania dostępnych diagnostyk.

5.14.4 Advanced Settings

5.14.4.1 MRP



Ilustracja 35: Strona WBM „MRP”

Tabela 46: Strona WBM „MRP”

MRP Global Settings		
Parametr	**Domyślnie**	**Opis**
Global Settings	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję globalnego MRP.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję. globalnego MRP.
MRP Settings		
Parametr	**Domyślnie**	**Opis**
Ring ID	**Add**	W polu wyboru należy wybrać „Add“, aby wpisać ID nowego pierścienia.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć ID pierścienia.
Mode	**Add**	W polu wyboru należy wybrać „Add”, aby skonfigurować switch jako klienta (MRC) lub menedżera (MRM).
	Remove	W polu wyboru należy wybrać „Remove”, aby usunąć switch jako klienta (MRC) lub menedżera (MRM).
Port 1	**Add**	W polu wyboru należy wybrać „Add“, aby dodać podstawowe złącze dla pierścienia MRP.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć podstawowe złącze dla pierścienia MRP.
Port 2	**Add**	W polu wyboru należy wybrać „Add“, aby dodać rezerwowe złącze dla pierścienia MRP.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć rezerwowe złącze dla pierścienia MRP.
Status	**Disable**	W polu wyboru należy wybrać „Disable“, aby włączyć dany pierścień.
	Enable	W polu wyboru należy wybrać „Disable“, aby włączyć dany pierścień.
Uuid	**Add**	Konfiguruje "Universal Unique Identifier" (UUID) dla pierścienia MRP. Jest to ciąg znaków w formacie szesnastkowym, przestawiający pierścień, do którego należy ten switch. **Przykład:** 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Remove	
VLAN	**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, dla których ten pierścień ma być aktywowany. Właściwy zakres VLAN ID: 1 … 4094 Przy podawaniu zakresu dla poszczególnych sieci VLAN należy użyć przecinka (,) lub łącznika (-).
	Remove	W polu wyboru należy wybrać „Remove“ i podać sieci VLAN, dla których ten switch nie ma być aktywowany.

Tabela 46: Strona WBM „MRP”

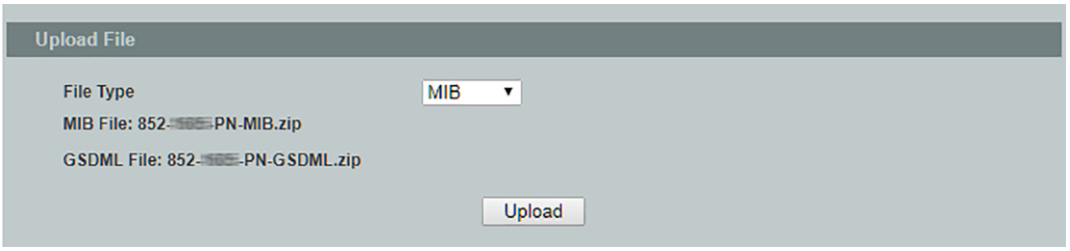
MRP Status		
Parametr	**Domyślnie**	**Opis**
Type	**All**	W polu wyboru należy wybrać „All“, gdy mają być wyświetlone wszystkie statusy MRP.
	Ring ID	W polu wyboru należy wybrać ID pierścienia, dla którego ma być wyświetlany status MRP.
MRP Status	–	W tym polu wyświetlany jest aktualny stan danego pierścienia MRP.
Ring ID	–	W tym polu wyświetlany jest ID pierścienia MRP.
Device Mode	–	W tym polu wyświetlany jest tryb switcha: Client (CRM)/Manager (MRM)
Uuid	–	W tym polu wyświetlany jest przydzielony UUID.
Vlan ID	–	W tym polu wyświetlana jest informacja, do której sieci VLAN należy pierścień.
Port-1	–	W tym polu wyświetlany jest przyporządkowany port switcha.
Port-2	–	W tym polu wyświetlany jest przyporządkowany port switcha.
Ring Status	–	W tym polu wyświetlany jest aktualny status pierścienia MRP.
State Machine Mode	–	W tym polu wyświetlana jest informacja, czy maszyna stanów MRP jest uruchomiona, czy nie.
Port-1-mode	–	W tym polu wyświetlany jest status portu: (port down/port up).
Port-2-mode	–	W tym polu wyświetlany jest status portu: (port down/port up).

5.14.5 Management

5.14.5.1 Upload File

Do switcha zarządzalnego PROFINET wgrywa się pliki GSDML i MIB.

Pliki te można załadować przez przeglądarkę do WBM.

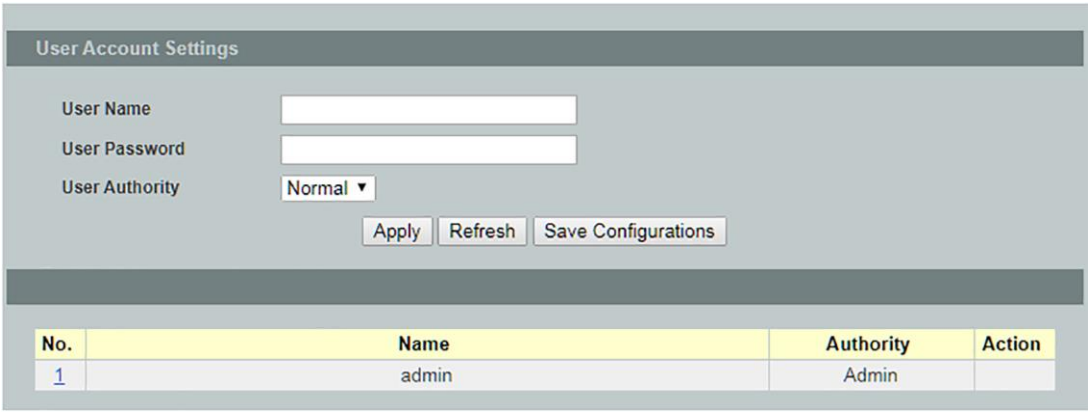


Ilustracja 36: Strona WBM „Upload File”

Tabela 47: Strona WBM „Upload File”

Parametr	Domyślnie	Opis
File Type	**MIB**	Wybór, czy do WMB ma być załadowany plik MIB czy GSDML

5.14.5.1.1 User Account



Ilustracja 37: Strona WBM „User Account”

Tabela 48: Strona WBM „User Account”

Parametr	Domyślnie	Opis
User Name	**admin**	Nazwa użytkownika
User Password	**wago**	Hasło
User Authority	**Admin**	Grupa uprawnień aktualnego użytkownika

6 Montaż

6.1 Miejsce montażu

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

- Przemysłowy switch zarządzalny 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 przemysłowy swich zarządzalny i odpowiednia wentylacja wokół niego. W pobliżu przemysłowego switch zarządzalnego nie należy umieszczać ciężkich obiektów.

6.2 Montaż na szynie

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

Przemysłowy switch zarządzalny należy zawiesić od góry na szynie i zamocować zatrzaskowo.

6.3 Demontaż z szyny

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

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

7 Podłączanie urządzeń

7.1 Zasilanie

Przemysłowy switch zarządzalny wykorzystuje zasilanie prądem stałym w zakresie 12 … 60 V.

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

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 przemysłowego switcha zarządzalnego 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.

Wskazówka



Uziemienie switcha
Uziemienie switcha pozwala uniknąć zakłóceń elektromagnetycznych na skutek promieniowania elektromagnetycznego.
Należy przy tym uwzględnić odpowiednie normy dla instalacji zgodnych z EMC.

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.

7.2 Złącze zewnętrznego styku alarmowego

Przemysłowy switch zarządzalny 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 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 Błąd połączenia (np. przerwanie przewodu, awaria urządzenia itp.)

2 PWR/RPS:
   a Błąd zasilania (przerwanie przewodu zasilającego, awaria zasilania, itp.)
   b Wejściowe napięcie zasilające poza zakresem podanym w specyfikacji (12 … 60 V)

7.3 Złącze przewodu konsolowego

Złącze konsolowe (RJ-45) umożliwia lokalne zastosowanie.

1. Stronę RJ-45 przewodu (składającego się z 8-pinowej wtyczki RJ-45 i DB9) należy wetknąć do złącza konsolowego RJ-45 w przemysłowym switchu zarządzalnym, a drugi koniec przewodu do złącza COM komputera.

2. Ustawienia HyperTerminal należy skonfigurować zgodnie z opisem zawartym w rozdziale „Konfiguracja“ > … > „Port konsolowy“.

Informacje dotyczące znaczenia pinów złącza konsoli (8-pinowy wtyk RJ-45) można znaleźć w rozdziale „Załącznik“ > … > „Złącze konsolowe (RJ-45 do DB9)“.

7.4 Porty 1000BASE-SX/LX, światłowód

Przy podłączaniu przewodu światłowodowego do złącza 1000BASE-SX/LX 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 należy zdjąć i zachować. Jeśli moduł SFP nie jest podłączony, złącze powinno być dla ochrony zasłonięte gumową pokrywą.

1. Dany moduł SFP wetknij i zablokuj.

2. Upewnij 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 połącz 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, sprawdź, czy zaświeciła się odpowiednia LED złącza w przemysłowym switchu zarządzalnym (patrz rozdział „Opis urządzenia“> … > „Elementy sygnalizacyjne“).

7.5 Porty 10/100/1000BASE-T

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

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

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

8 Opis funkcji

8.1 General Settings

8.1.1 Jumbo Frame

„Jumbo Frames“ to ramki ETHERNET o rozmiarze większym niż 1518 bajtów. Mogą one zwiększyć efektywność transmisji danych w sieci. Im większe „Jumbo Frames“, tym większa wydajność sieci.

Wskazówka



Ustawienia „Jumbo Frames“
Ustawienie rozmiaru „Jumbo Frames“ dotyczy każdego portu switcha.

Wszystkie podłączone urządzenia sieciowe muszą wspierać tę samą wielkość „Jumbo Frames“.
Pakiety danych większe niż ustawiona „Jumbo Frame“ zostają przed dane urządzenie sieciowe odrzucone.

8.1.2 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.

8.1.3 Management Host

Funkcja „Management Host“ ogranicza liczbę hostów, które mogą zarządzać switchem. W ustawieniach domyślnych nie ma funkcji „Management Host“. Wynika to z tego, że każdy host może zarządzać switchem przez Telnet lub przeglądarkę internetową. Gdy użytkownik skonfigurował jeden lub więcej hostów, switch może być zarządzany tylko przed te hosty. Funkcja ta umożliwia użytkownikom konfigurację maksymalnie trzech wpisów dla management IP.

8.1.4 MAC Management

Adres MAC („**M**edia **A**ccess **C**ontrol **Adresse**“, adres sprzętowy do kontroli dostępu) to unikalny numer urządzenia w sieci.

Adres dynamiczny

Przy odbiorze ramki switch odbiera źródłowy adres MAC w tabeli adresów wraz z odebranym portem, VLAN i „Age Time“ (żywotność). Po upływie „Age Time“ wpis zostaje usunięty z tabeli adresów.

Adres statyczny

Ustawiony przez użytkownika adres statyczny nie ma „Age Time“ i dlatego nie jest usuwany ze switcha. Adres statyczny może zostać usunięty wyłącznie przez użytkownika. Switch wspiera tabelę adresów o wielkości do 16 K.

Adresy statyczne i dynamiczne znajdują się w tej samej tabeli.

MAC Table

„MAC Table“ (tabela adresów MAC, określana także jako filtr bazy danych) pokazuje, które ramki przekierowane są do portów switcha lub są odfiltrowywane. Jeśli urządzenie, mogące należeć do grupy VLAN, wysyła pakiet danych, który przekierowany jest do portu w switchu, adres MAC urządzenia odczytywany jest z tabeli adresów MAC.
Wyświetlana jest też informacja, czy chodzi o adres MAC dynamiczny (nadany przez switch) czy statyczny (ustawiony ręcznie).

Tabela adresów MAC

Switch wykorzystuje tabelę adresów MAC, aby określić, gdzie przesłać ramki.

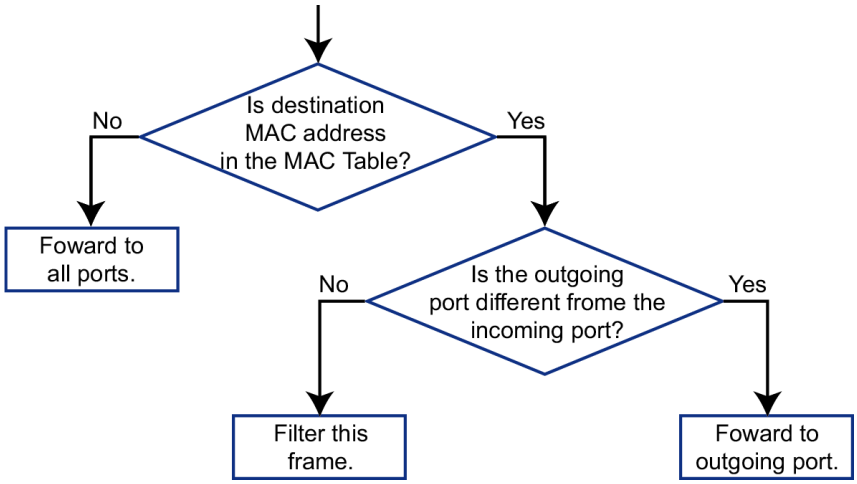
1. Switch sprawdza odebraną ramkę i rozpoznaje port, z którego pochodzi źródłowy adres MAC.

2. Switch sprawdza, czy docelowy adres MAC ramki i rozpoznany już źródłowy adres MAC są w tabeli adresów MAC zgodne.

   - Jeśli switch zna już port dla tego adresu MAC, przesyła ramkę do tego portu.

- Jeśli switch nie zna jeszcze portu dla tego adresu MAC, przesyła ramkę do wszystkich portów. „Port Flooding“ (za częste przekazywanie do wszystkich portów) może prowadzić do zatorów w sieci.

- Jeśli switch zna już port dla tego adresu MAC, a port docelowy i wejściowy są identyczne, ramka jest filtrowana.



Ilustracja 38: Diagram przebiegu tabeli adresów MAC

8.1.4.1 Static MAC

Statyczne adresy MAC

Statyczny adres MAC to adres, który został ręcznie wpisany do tabeli adresów MAC. Statyczne adresy MAC nie mają „Age Time“. Po stworzeniu reguły dla statycznych adresów MAC można tworzyć te adresy dla portu. Może to ograniczyć potrzebę transmisji danych.

8.1.5 Port Mirroring

„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.

Tryb źródłowy

- „Ingress” (wejście): Wchodzące pakiety danych są kopiowane i przekierowane do portu monitorującego.
- „Egress” (wyjście): Wychodzące pakiety danych są kopiowane i przekierowane do portu monitorującego.
- Oba: Zarówno wchodzące. jak i wychodzące pakiety danych są kopiowane i przekierowane do „Monitor Port“.

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.

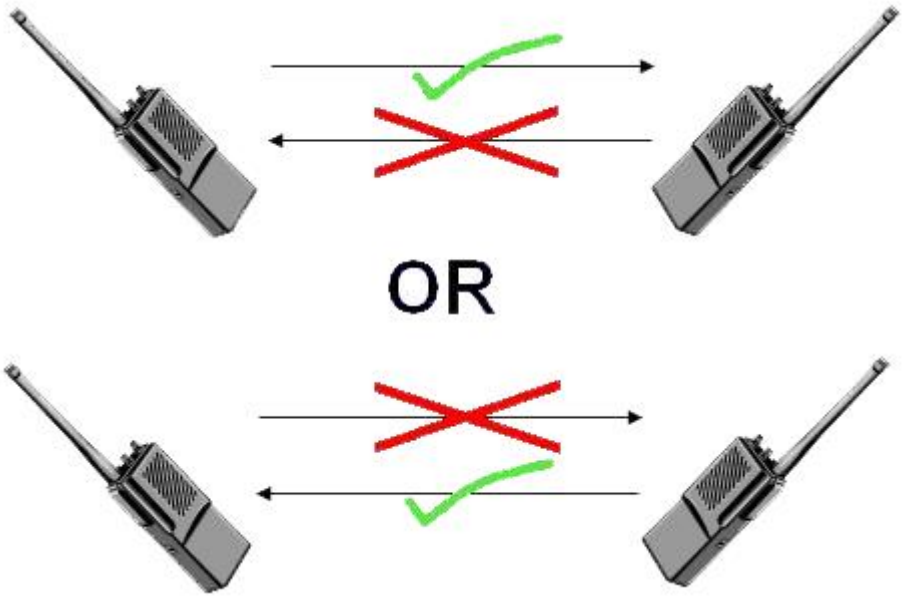
8.1.6 Port Settings

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 39: 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 40: 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 sieciowe ETHERNET (np. port sieciowy komputera i port sieciowy rutera, hubu lub switcha, z którym jest on np. połączony), samodzielnie uzgadniają i konfigurują maksymalną największą prędkość transmisji oraz tryb duplex.
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“ (sterowanie przepływem danych) 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 „Flow Control“ w trybie full duplex i „Back Pressure Flow Control“ (wsteczna kontrola przepływu danych) w trybie half duplex.

Przy „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 „Back Pressure 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“.

8.2 Advanced Settings

8.2.1 Bandwidth Control

8.2.1.1 QoS

Każdy port wyjściowy wspiera maksymalnie osiem „Transmit Queues“ (kolejki wartości wyjściowych). Każda „Transmit Queue“ zawiera przy tym listę, na której wyspecyfikowana jest kolejność transmisji pakietów. Każda wchodząca ramka zostaje przekierowana do jednej z ośmiu „Transmit Queues“ przydzielonego portu wyjściowego na podstawie swojego priorytetu. Port wyjściowy przesyła pakiety z każdej z ośmiu „Transmit Queues“ według konfigurowalnego algorytmu kolejności, który może składać się z kombinacji SP („**S**trict **P**riority“, regulacja priorytetu) i/lub WRR („**W**eighted **R**ound **R**obin“, algorytm szeregowania).

Zazwyczaj sieci działają zgodnie z najlepszą możliwą metodą transmisji, tzn. że cały ruch danych 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.

Przy konfiguracji funkcji QoS („**Q**uality **o**f **S**ervice“, jakość usługi) można wybrać specyficzny ruch danych, przydzielić mu priorytet odpowiednio do jego relatywnej ważności i zastosować zarządzanie zatorem i techniki mające mu zapobiec. Implementacja QoS w sieci poprawia przewidywalność wydajności sieci i zwiększa efektywność wykorzystania szerokości pasma.

Przemysłowy switch zarządzalny wspiera „802.1p Priority Queuing“ (rodzaj kolejki priorytetowej zgodnie ze standardem 802.1p).
Switch dysponuje ośmioma „Priority Queues“. Są one podzielone na klasy, przy czym klasa 7 oznacza najwyższy priorytet, a klasa 0 najniższy. Te osiem klas priorytetów wyspecyfikowanych w standardzie IEEE 802.1p (p0 do p7) przyporządkowane są „Priority Queues“ switcha w następujący sposób:

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

„Priority Scheduling“ implementowana jest przez wymienione wyżej „Priority Queues“. Switch przetwarza cztery „Hardware Priority Queues“ w kolejności, przy czym rozpoczyna od najwyższego „Priority Queue” (3) i kończąc na najniższej (0). Każda „Hardware Queue“ transmituje wszystkie swoje pakiety do bufora switcha i dopiero potem niższy priorytet uzyskuje zgodę na transmisję swoich pakietów. Gdy niższy „Hardware Priority Queue“ prześle swoje pakiety, najwyższy ponownie rozpoczyna transmisję swoich pakietów, które w międzyczasie odebrał.

Rozszerzenie QoS

Switch można tak skonfigurować, aby priorytetować ruch danych, nawet gdy wchodzące pakiety nie mają „IEEE 802.1p Priority Tags“ (znaczników priorytetu IEEE 802.1p) lub aby zmieniał istniejące „Priority Tags“ zgodnie z własnymi ustawieniami. Switch umożliwia zastosowanie jednej z niżej wymienionych metod nadawania priorytetów wchodzącym pakietom:

- 802.1p Tag Priority
- Priorytety dla pakietów przydziela się na podstawie ich „802.1p Tag Priority“.

- QoS na bazie portu
- Priorytety dla pakietów przydziela się na bazie portu wejściowego switcha.

- QoS na bazie DSCP
- Priorytety dla pakietów przydziela się na bazie ich DSCP („**D**ifferentiated **S**ervices **C**ode **P**oints“, wartości typu usługi).

Wskazówka

Rozszerzone metody QoS
Rozszerzone metody QoS dotyczą tylko wewnętrznego przyporządkowania w „Priority Queue“ dla switcha. Switch nie przeprowadza zmian wartości IEEE 802.1p dla ramki wyjściowej.

W celu zmiany priorytetu wchodzących pakietów można bądź skorzystać z jednej z wyżej wymienionych metod, bądź nie stosować w ogóle żadnych ustawień dla rozszerzenia QoS switcha.

Priorytet 802.1p

Przy zastosowaniu mechanizmu priorytetowania sprawdzane jest, czy pakiet ma ustawiony „802.1p Priority Tag“. Jeśli priorytet istnieje, pakiet zostaje przydzielony na podstawie swojej wartości priorytetu programowalnej „Egress Queue“. „Tag Priority“ może być przydzielony do każdej dostępnej „Queue“.

Pakiet ETHERNET

6	6	2	42-1496	4
DA	SA	Typ/długość	Dane	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q-Rag	Typ/długość	Dane	FCS

802.1Q-Tag

2 B	2 B		
Tag Protocol Identifier (TPID)	Tag Control Information (TCI)		
16 b	3 b	1 b	12 b
TPID (0x8100)	Priority	CFI	VID

- TPID („**T**ag **P**rotocol **Id**entifier“)
  Pole 16-bitowe ustawiane jest na wartość 0x8100, aby rozpoznać ramkę jako „IEEE 802.1Q Tag Frame“.

- TCI („**T**ag **C**ontrol **I**nformation“)

- PCP („**P**riority **C**ode **P**oint“)
  To pole zajmuje 3 bity i odnosi się do priorytetu IEEE 802.1p. Wyświetla poziom priorytetu ramki w skali od 0 (najniższy) do 7 (najwyższy), przez który można przydzielać priorytet różnym klasom ruchu danych (język, wideo, dane itd.).

- CFI („**C**anonical **F**ormat **I**ndicator“)
  Pole to zajmuje 1 bit. Jeśli pole to ma wartość 1, adres MAC nie ma kanonicznego formatu. Jeśli pole to ma wartość 0, adres MAC ma kanoniczny format. W przypadku switchy ETHERNET wartość ta zawsze wynosi 0. CFI wykorzystywany jest dla zapewnienia kompatybilności między sieciami ETHERNET i „Token Ring“. Jeśli ramka odebrana przez port ETHERNET ma wartość CFI wynoszącą 1, ramka nie powinna być wystawiona na port bez znacznika.

- VID („**V**LAN **Id**entifier“)
  Pole to zajmuje 12 bitów i podaje VLAN, do którego należy ramka. Wartość 0 oznacza, że ramka nie należy do VLAN i „802.1Q Tag“ podaje tu tylko priorytet i służy jako „Priority Tag“. Wartość szesnastkowa 0xFFF jest zarezerwowana do celów implementacji. Wszystkie inne wartości mogą być użyte jako „VLAN Identifier”, a więc wspieranych jest 4094 wirtualnych sieci lokalnych VLAN. W „Bridges“ VLAN 1 jest często zarezerwowany dla zarządzania.

Poziomy priorytetu

PCP („**P**riority **C**ode **P**oint“):

Tabela 49: Poziomy priorytetu

PCP	Priorytet sieci	Cechy ruchu danych
1	0 (najniższy)	„Background“
0	1	„Best Effort“
2	2	„Excellent Effort“
3	3	„Critical Applications“
4	4	Wideo, latencja <100 ms
5	5	Wideo, latencja < 10 ms
6	6	Sterowanie siecią złożoną
7	7 (najwyższy)	Sterowanie siecią

DiffServ (DSCP)

DiffServ („**Diff**erentiated **Serv**ices“) jest architekturą sieci komputerowej, specyfikującą prosty, skalowalny mechanizm o dużej ziarnistości, służący do klasyfikowania, zarządzania ruchem sieci i przygotowywania gwarancji QoS („Quality of Service“) w nowoczesnych sieciach IP. DiffServ może być wykorzystywany na przykład w celu GS („**G**uaranteed **S**ervice“) o niewielkiej latencji dla krytycznego ruchu sieci, jak chociażby dane dotyczące języka, wideo, podczas gdy niekrytyczny ruch danych, jak na przykład dane internetowe lub transfer danych otrzymują proste gwarancje „Best Effort“.

DSCP („**D**ifferentiated **S**ervices **C**ode **P**oint“) jest polem 6-bitowym w nagłówku pakietów IP, które służy do klasyfikacji pakietów. DSCP zastępuje przestarzały precedens IP – pole 3-bitowe w bajcie „Type of Service“ nagłówka IP, które pierwotnie wykorzystywane było dla klasyfikacji i priorytetowania rodzajów ruchów danych.

Przy zastosowaniu mechanizmu priorytetowania DiffServ pakiet klasyfikowany jest na podstawie pola DSCP w nagłówku IP. Jeśli znacznik istnieje, pakiet zostaje przekierowany dalej zgodnie ze swoją wartością „Tag Priority“ do programowalnego „Egress Queue“. „Tag Priority“ może być przydzielony każdej dostępnej „Queue“.

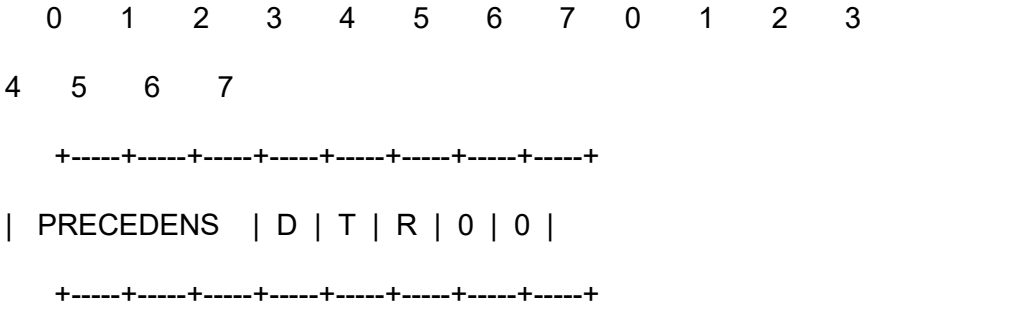
<table>
<tr><th>Version</th><th>IHL</th><th>Type of Service</th><th colspan="2">Total Length</th></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Haeder checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
</table>

Przykład nagłówka pakietu danych internetowych

„Type of Service“ w nagłówku IP: 8 b

Pole „Type of Service“ zawiera dane dotyczące abstrakcyjnych parametrów żądanej „Quality of Service“. Parametry te wykorzystywane są do ręcznego wyboru właściwych parametrów usługi, gdy pakiet danych ma być przesłany dalej przez określoną sieć. Niektóre sieci oferują precedens usługi, która traktuje ruch danych z wyższym precedensem w sposób uprzywilejowany w stosunku do innych (przy wysokim obciążeniu sieci na ogół akceptują tylko dane o odpowiednio wysokiego poziomu precedensu). Najbardziej korzystny wybór jest kompromisem pomiędzy niewielką zwłoką, wysoką niezawodnością i wysoką przepustowością.

Bit 0 … 2	Precedens	
Bit 3	0 = normalna zwłoka	1 = nieznaczna zwłoka
Bit 4	0 = normalna przepustowość	1 = wysoka przepustowość
Bit 5	0 = normalna niezawodność	1 = wysoka niezawodność
Bit 6 … 7	Zarezerwowane do wykorzystania w przyszłości.	



Precedens

111 – Network Control
110 – Internetwork Control
101 – CRITIC/ECP
100 – Flash Override
011 – Flash
010 – Immediate
001 – Priority
000 – Routine

Specyfikacja parametrów dla zwłoki, przepustowości i niezawodności może podnieść koszty serwisu. W wielu sieciach preferowanie jednego z tych parametrów oznacza dyskryminację innego. Abstrahując od bardzo szczególnych przypadków, przeważnie powinny być wyspecyfikowane co najwyżej dwa z tych trzech parametrów.

Parametr „Type of Service“ wykorzystywany jest w celu specyfikacji rodzaju przetwarzania pakietu danych w trakcie przesyłania przez sieć. Przykładowe przyporządkowanie „Internet Type of Service“ do rzeczywiście oferowanej usługi w sieciach, jak na przykład AUTODIN II, ARPANET, SATNET i PRNET wymieniono w punkcie „Service Mappings“.

Przyporządkowanie precedensu sterowania siecią powinno być stosowane tylko wewnątrz sieci. Rzeczywiste zastosowanie tego przyporządkowania i sterownie nim zależy od danej sieci. Przyporządkowanie sterowania siecią złożoną powinno być przeprowadzone tylko przez inicjatorów sterownia bramami.

Jeśli przyporządkowania te mają dotyczyć określonej sieci, jest ona odpowiedzialna za kontrolę dostępu i zastosowanie tego przyporządkowania.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
…					
60	0	61	0	62	0
62	0				

Przykład:

Nagłówek IP

DSCP=50 -> 45 C8 …

Queuing Algorithms

Za pomocą funkcji „Queuing Algorithms“ switche mogą tworzyć osobne „Queues“ dla pakietów, mogących pochodzić z każdego pojedynczego źródła lub każdego strumienia danych, i w ten sposób zapobiegać opanowaniu całej szerokości pasma przez jedno źródło.

SPQ

W SPQ („**S**trict **P**riority **Q**ueuing“) przetwarzane są cztery „Hardware Priority Queues“ po kolei – najpierw ta z najwyższym priorytetem (3), a na końcu ta z najniższym (0). Każda „Hardware Queue“ transmituje wszystkie swoje pakiety do bufora i dopiero potem niższy priorytet uzyskuje zgodę na transmisję swoich pakietów. Gdy niższy „Hardware Priority Queue“ prześle swoje pakiet, najwyższy ponownie rozpoczyna transmisję swoich pakietów, które w międzyczasie odebrał.

WRR

RR („**R**ound **R**obin“) jest procesem, który aktywuje się dopiero wtedy, gdy na porcie jest większy ruch danych, niż może on przetworzyć. „Queue“ niezależnie od wchodzącego ruchu danych udostępniana jest na porcie ograniczona szerokość pasma. Następnie taka „Queue“ jest ustawiana na końcu listy. Potem następna „Queue“ otrzymuje taką samą szerokość pasma, jest ustawiana na końcu listy i tak dalej, aż do momentu, gdy wszystkie „Queues“ zostają przetworzone. Cały proces odbywa się w pętli, aż w „Queue” nie będzie już ruchu danych.

WRR („**W**eighted **R**ound **R**obin“) wykorzystuje te same algorytmy co proces „Round Robin“, tylko tutaj „Queues“ zostają podzielone na podstawie swojego priorytetu i wagi (wartość wprowadzonej w polu „Weight Value“), zamiast przydzielania im stałej szerokości pasma. WRR aktywuje się tylko wtedy, gdy na porcie jest większy ruch danych, niż może on przetworzyć. „Queues“ o wyższej wadze są bardziej faworyzowane niż te o mniejszej wadze. Mechanizm ten jest bardzo efektywny, gdyż dzieli całą dostępną szerokość pasma na mniejsze „Traffic Queues“ i przydziela ją tym, które jeszcze nie były przetwarzane.

Wskazówka



Funkcja DiffServ
DiffServ jest w przemysłowym switchu zarządzalnym nieaktywna.
Przy dezaktywacji DiffServ używany jest „802.1p Tag Priority“.

8.2.1.2 Rate Limitation

8.2.1.2.1 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.

„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 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 na sekundę wszystkie pozostałe pakiety zostają odrzucone. Funkcję tę należy aktywować w celu ograniczenia liczby tych pakietów w sieci.

Jednostka „Storm Control“ to 625 pps (pakietów na sekundę).

8.2.1.2.2 Rate Limitation

„Rate Limitation“ służy do sterowania prędkością danych, odbieranych przez interfejs sieciowych lub transmitowanych przez niego.

8.2.2 IGMP Snooping

Proces „IGMP Snooping“ („**I**nternet **G**roup **M**anagement **P**rotocol **Snooping**“) stosowany jest przy ruchu danych typu multicast. Switch może wtedy pasywnie „podsłuchiwać“ pakiety IGMP, transmitowane między ruterami lub switchami IP multicast i hostami IP multicast, w celu rozpoznania, do jakiej grupy IP multicast należą. „IGMP Snooping“ umożliwia switchowi rozpoznanie grup multicast bez wcześniejszego ich ręcznego skonfigurowania przez użytkownika.

Sprawdza on przechodzące przez niego pakiety IGMP, odczytuje informacje o rejestracji grup i odpowiednio konfiguruje multicasting.

Switch kieruje ruch danych multicast do swoich grup docelowych multicast (które rozpoznał za pomocą „IGMP Snooping“ lub po ręcznej konfiguracji) dalej do portów, które są członkami grupy. „IGMP Snooping“ nie generuje dodatkowego ruchu w sieci, więc ruch danych multicast kierowany przez switch może zostać wyraźnie zredukowany.

Switch może realizować „IGMP Snooping“ przy maksymalnie 4094 wirtualnych sieci lokalnych VLAN. Switch można skonfigurować tak, aby automatycznie rozpoznawał przynależność do grup multicast we wszystkich sieciach VLAN. Switch wykonuje wtedy „IGMP Snooping“ w pierwszych wirtualnych sieciach lokalnych VLAN, wysyłających pakiety IGMP.

Ten tryb nazywany jest „Auto Mode“. Alternatywnie można także samodzielnie wyspecyfikować wirtualne sieci lokalne VLAN, w których ma być realizowany „IGMP Snooping“. Ten tryb nazywany jest „Fixed Mode“. W trybie „Fixed Mode“ switch rozpoznaje przynależności do grupy tylko w tych wirtualnych sieciach lokalnych VLAN , które zostały wcześniej jednoznacznie dodane jako VLAN „IGMP Snooping“.

Immediate Leave

Przy aktywowaniu polecenia „IGMP Immediate Leave“ switch natychmiast usuwa jeden port, gdy tylko odbierze na tym porcie „Leave Message“ z wersją 2 IGMP. Z funkcji „Immediate Leave“ należy korzystać tylko wtedy, gdy na każdym porcie w sieci VLAN jest tylko jeden odbiorca („Immediate Leave“ jest wspierana tylko przez hosty w wersji 2 IGMP).

Switch korzysta z funkcji „Immediate Leave“ przy „IGMP Snooping“, aby usunąć z tabeli przekierowania interfejs, który wysyła „Leave Message“ bez konieczności wysyłania przez switch do interfejsu specyficznych dla grupy żądań. Interfejs VLAN zostaje usunięty z katalogu multicast grupy multicast, wyspecyfikowanej w pierwotnej „Leave Message“. Funkcja „Immediate Leave“ gwarantuje optymalne wykorzystanie szerokości pasma dla wszystkich hostów w sieci, nawet gdy w użyciu jest kilka grup multicast równocześnie.

Fast Leave

Switch umożliwia konfigurację czasu zwłoki. Po upływie tego czasu switch usuwa interfejs z grupy multicast.

Last Member Query Interval

„Last Member Query Interval“ jest maksymalnym czasem odpowiedzi, który przesyłany jest w specyficznych dla grupy zapytaniach jako odpowiedź na wiadomości „Leave Group“, oraz wskazuje na interwał między specyficznymi dla grupy komunikatami zapytań.

Gdy switch bez aktywowanej funkcji „Immediate Leave“ odbiera na porcie odbiorczym „IGMP Leave Message“ od urządzenia sieci, wysyła na ten port specyficzne dla IGMP zapytanie i czeka na komunikaty członkostwa grupy IGMP. Jeśli w trakcie skonfigurowanego czasu nie otrzyma komunikatu, port odbiorczy zostaje wykluczony z grupy multicast.

IGMP Querier

Dla sieci fizycznej istnieje zazwyczaj tylko jeden „Querier“. Wszystkie rutery multicast rozpoczynają pracę jako „Querier“ dla każdej podłączonej sieci. Gdy ruter multicast odbierze „Query Message“ od rutera o niższym adresie IP, MUSI przyjąć rolę jako nie-„Querier“ w tej sieci. Gdy ruter przez określony czas [„Other Querier Present Interval“] nie otrzymuje „Query Message“ od innego rutera, sam przejmuje rolę jako „Querier“. Ruter wysyła regularnie [„Query Interval“] „General Query“ do wszystkich podłączonych sieci, dla których pełni funkcję „Querier“ w celu zebrania informacji. Przy rozruchu ruter POWINIEN wysłać „General Queries“ [„Startup Query Count“] w niewielkim odstępie czasowym [„Startup Query Interval“], aby szybko i niezawodnie zebrać informacje o członkostwie. „General Query“ skierowane jest do grupy All-Systems Multicast (224.0.0.1), ma wartość pola adresu grupowego 0 i maksymalny czas odpowiedzi [„Query Response Interval“].

Port IGMP Querier Mode

- Auto
  - Switch wykorzystuje ten port jako „IGMP Query Port”, gdy port odbiera pakiety „IGMP Query”.

- Fixed
  - Switch wykorzysta ten port/te porty jako „IGMP Query Port(s)“. Ten tryb wykorzystywany jest, gdy serwer IGMP multicast połączony jest z portem/portami.
  - Switch przekazuje pakiety „Report/Leave“ klienta zawsze na ten port. Standardowo port połączony jest z serwerem IGMP.
- Edge
- Switch nie będzie używać tego portu jako „IGMP Query Port”.
  - Odebrane na tym porcie pakiety „IGMP Query“ zostają odrzucone. Standardowo port połączony jest z klientem IGMP.

Wskazówka



Przekazywanie pakietów „IGMP Join/Leave“
Przemysłowy switch zarządzalny przekazuje pakiety „IGMP Joint/Leave“ na port Query.

IGMP Proxy Snooping

Przez „IGMP Proxy Snooping“ można zredukować liczbę wysyłanych przez ruter IGMP „Reports“ i „Leaves“.

Konfiguracje

Użytkownik może aktywować lub dezaktywować w switchu „IGMP Snooping“. Dotyczy to także specyficznych wirtualnych sieci lokalnych. Gdy „IGMP Snooping“ zostaje w switchu dezaktywowany, dezaktywowany zostaje dla wszystkich wirtualnych sieci lokalnych, nawet jeśli w niektórych VLAN „IGMP Snooping” jest aktywowany.

Wskazówka



Stany VLAN
Istnieje stan globalny i poszczególne stany VLAN.
Gdy stan globalny zostaje dezaktywowany, dezaktywowany zostaje „IGMP Snooping“ w switchu, nawet jeśli poszczególne stany VLAN zostały aktywowane.
Gdy dla „IGMP Snooping“ aktywowany jest stan globalny, funkcja ta musi być dla specyficznych VLAN pojedynczo aktywowana przez użytkownika.

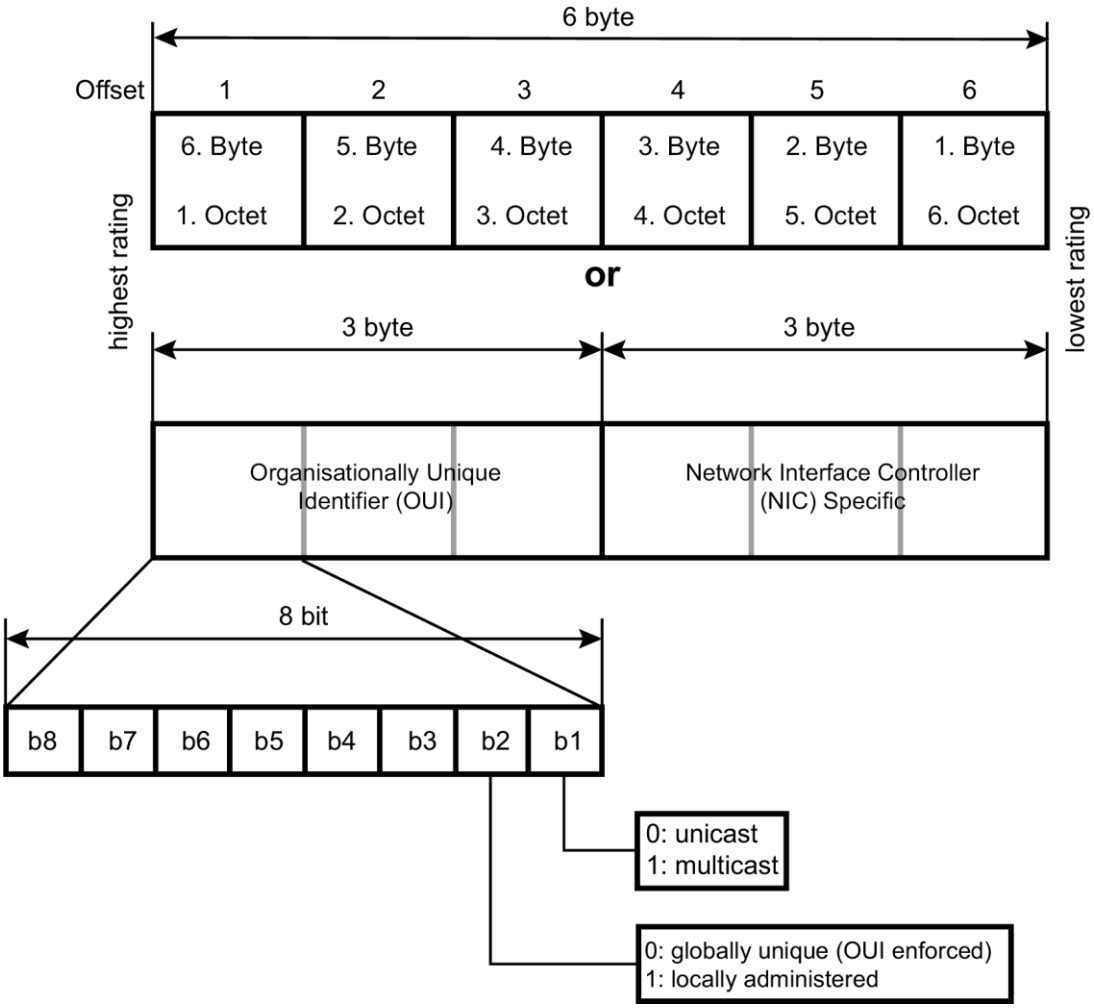
8.2.2.1 Multicast Address

Adres multicast odnosi się do grupy zainteresowanych odbiorców. Zgodnie ze standardem RFC 3171 adresy od 224.0.0.0 do 239.255.255.255 (dawniej adresy klasy D) w IPv4 są zarezerwowane jako adresy multicast.

Pierwszy oktet (01) zawiera bit broadcast/multicast. Dolne 23 bity 28-bitowego adresu IP multicast zostają przyporządkowane do 23 bitów dostępnej przestrzeni adresowej ETHERNET. Tworzy to wieloznaczność przy transmisji pakietów. Gdy w tej samej podsieci zgłaszają się dwa hosty przy różnych grupach multicast, których adresy różnią się tylko w pierwszych 5 bitach, oba pakiety ETHERNET wysyłane są do obu grup multicast przy obu hostach. Oprogramowanie sieciowe w hostach musi każdorazowo odrzucić niepotrzebne pakiety.

Tabela 50: Klasy multicast i zakresy adresów

Klasa	Zakres adresów	Wsparcie
Klasa A	1.0.0.1 do 126.255.255.254	Wsparcie 16 milionów hostów w każdej z 127 sieci
Klasa B	128.1.0.1 do 191.255.255.254	Wsparcie 65 000 hostów w każdej z 16 000 sieci
Klasa C	192.0.1.1 do 223.255.254.254	Wsparcie 254 hostów w każdej z 2 milionów sieci
Klasa D	224.0.0.0 do 239.255.255.255	Zarezerwowana dla grup multicast
Klasa E	240.0.0.0 do 254.255.255.254	Zarezerwowana do wykorzystania w przyszłości lub dla celów badawczych i rozwojowych



Ilustracja 41: Adres multicast

Tabela 51: Adres IP multicast

Adres IP multicast	Opis
224.0.0.0	Adres bazowy (zarezerwowany)
224.0.0.1	Grupa „All Hosts Multicast“, zawierająca wszystkie systemy w tym samym segmencie sieci
224.0.0.2	Grupa „All Router Multicast“, zawierająca wszystkie rutery w tym samym segmencie sieci
224.0.0.5	„Open Shortest Path First” (protokół OSPF), adres „AllSPFRouters” Ten adres jest wykorzystywany do wysyłania „Hello-Paketen” do wszystkich routerów OSPF w segmencie sieci.
224.0.0.6	Adres „OSPF AllDRouters” Ten adres wykorzystywany jest do wysyłania informacji o rutingu OSPF do „OSPF Designated Router“ w segmencie sieci.

Tabela 51: Adres IP multicast

Adres IP multicast	Opis
224.0.0.9	RIP („Routing Information Protocol”) wersja 2 adresu grupowego Ten protokół wykorzystywany jest do wysyłania informacji o rutingu do wszystkich ruterów kompatybilnych z RIPv2 w segmencie sieci.
224.0.0.10	Adres grupy EIGRP Adres ten wykorzystywany jest do wysyłania informacji o rutingu EIGRP do wszystkich ruterów EIGRP w segmencie sieci.
224.0.0.13	PIM wersja 2 („Protocol Independent Multicast“)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP wersja 3 („Internet Group Management Protocol“)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Adres multicast DNS
224.0.0.252	Adres „Link-local Multicast Name Resolution“
224.0.1.1	Adres „Network Time Protocol“
224.0.1.39	Adres „Cisco Auto-RP-Announce“
224.0.1.40	Adres „Cisco Auto-RP-Discovery“
224.0.1.41	Adres „H.323 Gatekeeper Discovery“

8.2.3 VLAN

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 możliwe są maksymalnie 4094 konfiguracje VLAN.

„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 przekazana 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 możliwe są maksymalnie 4094 konfiguracej 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.

- **802.1Q-VLAN na bazie portów**

Jako uczestnik VLAN na bazie portów port zostaje przydzielony do specyficznej sieci VLAN, niezależnie od tego, który użytkownik lub które urządzenie są połączone z tym portem. Oznacza to, że wszyscy połączeni z tym portem użytkownicy są uczestnikami tej samej sieci VLAN. Standardowo przyporządkowania do VLAN dokonuje administrator. Konfiguracja portu jest statyczna i nie można jej zmienić automatycznie na inną sieć VLAN bez przeprowadzenia ponownej ręcznej konfiguracji.

Tak jak przy innych procesach VLAN pakiety przekierowane tą metodą nie mogą być transmitowane do innych domen VLAN lub sieci. Po przypisaniu portu do sieci VLAN nie może on odbierać ani wysyłać danych do urządzeń w innej sieci VLAN bez użycia urządzenia warstwy 3.

Urządzenie podłączone do portu nie może rozpoznać, że istnieje VLAN. Urządzenie rozpoznaje jedynie, że jest częścią podsieci i może się komunikować z innymi uczestnikami sieci, wysyłając po prostu informacje przez połączenie przewodowe. Switch odpowiedzialny jest za identyfikację informacji, pochodzących ze specyficznej sieci VLAN, i musi zapewnić przesłanie tych informacji do wszystkich uczestników VLAN. Poza tym switch musi zapewnić, żeby informacje te nie mogły zostać odebrane przez porty z innej sieci VLAN.

Tym procesem można prosto, szybko i łatwo zarządzać, gdyż nie wymaga on rozbudowanych tabel przyporządkowań do segmentacji VLAN. Jeśli połączenie „Port-to-VLAN” realizowane jest za pomocą „**A**pplication-**S**pecific **I**ntegrated **C**ircuit” (ASIC), pozwala to uzyskać dużą wydajność. ASIC umożliwia przyporządkowanie „Port-to-VLAN“ na poziomie sprzętu.

8.2.3.1 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 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 2 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.

8.2.4 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 IEEE 802, którego ta jednostka/te jednostki zarządzania potrzebuje/potrzebują.

Informacje dystrybuowane przez ten protokół zapisywane są przez odbiorców w zwykłej MIB („**M**anagement **I**nformation Base“). W ten sposób umożliwione jest NMS („**N**etwork **M**anagement **S**ystem“), za pośrednictwem protokołów zarządzających, jak na przykład SNTP („**S**imple **N**etwork **M**anagement **P**rotocol“), uzyskanie dostępu do tych informacji.

8.2.5 MAC based VLAN

VLAN na bazie MAC umożliwia użytkownikom priorytetowe przypisywanie pojedynczych pakietów danych do VLAN na podstawie adresu MAC.

8.2.6 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 specjalne pakiety multicast, w celu wykrycia, czy port połączony jest z siecią w stanie pętli. Switch wyłącza port, gdy rozpozna, że specjalne pakiety multicast zawracane są znowu do tego samego portu.

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.

8.2.7 STP

(R)STP („(**R**apid) **S**panning **T**ree **P**rotocol)“) może wykryć pętle sieci i przerwać połączenia zapasowe („Back-up 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 52: Koszty trasy STP

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

- 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 negocjację 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 Ports“. 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.

MSTP

MSTP („**M**ultiple **S**panning **T**ree **P**rotocol“) jest rozszerzeniem RSTP. Umożliwia różne instancje „Spanning Trees“ w związku z siecią VLAN („Virtual Local Area Networks“).
Dla sieci VLAN lub grupy sieci VLAN mogą więc tworzone być niezależne od siebie instancje STP, które wykorzystują wewnątrz sieci LAN kilka drzew rozpinających.
Podczas procesu MSTP określany jest bridge root i najniższe koszty odcinków między bridgem root i oferowanymi portami root poszczególnych bridge'ów.
Bridge root wysyła Bridge Protocol Data Units (BPDU) do wszystkich bridge'ów i przez dane konfiguracyjne zawarte w pakietach BPDU ustala konfigurację sieci.

8.3 Security

8.3.1 Access Control List

ACL („**A**ccess **C**ontrol **L**ist“) jest listą uprawnień przyporządkowaną 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, odbieranych ze specyficznych portów wejściowych lub wszystkich portów. Dzięki tym regułom sprawdzane są źródłowe i docelowe adresy MAC pakietów. Jeśli pakiety odpowiadają tym regułom, system wykona akcję „deny“. Oznacza to, że pakiety zostają odrzucone.

Filtrowanie pakietów może odbywać się według:

- adresu MAC lub IP źródła
- adresu MAC lub IP docelowego
- zakresu adresów MAC lub IP
- wybieralnych portów źródłowych lub docelowych (np. UDP lub TCP)

„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.

8.4 Monitor

8.4.1 Alarm

Funkcja ta powiadamia administratora sieci o określonych zdarzeniach i sytuacjach wewnątrz sieci.

Przykład

P1: ON – Połączenie na porcie 1 jest przerwane.

PWR: ON – Zasilanie podstawowe jest przerwane.

RPS: ON – Zasilanie rezerwowe jest przerwane.

8.4.2 Monitor Informations

Za pomocą tej funkcji wyświetlane są niektóre informacje o sprzęcie, służące do monitorowania systemu i zapewnienia prawidłowej pracy sieci.

8.4.3 RMON Statistics

Za pomocą tej funkcji można monitorować i usuwać statystyki RMON.

Jabber

Jako „Jabber“ określa się uczestników sieci takich jak ETHERNET, którzy posiadają pakiety danych większe niż dozwolony MTU („**M**aximum **T**ransmission **U**nit“).

8.4.4 SFP

SFP („**S**mall **F**orm-factor **P**luggable“) to małe standaryzowane moduły dla połączeń sieciowych.
SFP oznacza modularny interfejs wspierający różne media transmisji i stosowany jest w technice sieciowej do uelastyczniania interfejsów.

8.4.4.1 SFP Information

DDMI („**D**igital **D**iagnostics **M**onitoring **I**nterface“) to technologia, umożliwiająca użytkownikom monitorowanie następujących parametrów czasu rzeczywistego w modułach SFP:

- Napięcie
- Prąd Bias
- Moc wejściowa
- Moc wyjściowa
- Temperatura
- Światłowód
- Łącznik
- Długość fali
- Długość transmisji
- Obsługa DDM
- Handler: Nazwa
- Handler: Numer katalogowy
- Handler: Rewizja
- Handler: Numer klucza
- Data (zakodowana)

8.4.5 Traffic Monitor

Funkcję „Traffic Monitor“ można aktywować i dezaktywować zarówno dla specyficznego portu, jak i dla całego switcha. Za pomocą tej funkcji można monitorować prędkość danych pakietów broadcast, multicast lub broadcast i multicast. Gdy pakiety przekraczają specyfikację dla jednego użytkownika, port zostaje zablokowany. Gdy aktywowana jest funkcja „Recovery“, po upływie „Recovery Time“ port zostaje reaktywowany.

8.5 Management

8.5.1 SNMP

SNMP („**S**imple **N**etwork **M**anagement **P**rotocol“) jest standardem do zarządzania urządzeniami ETHERNET w sieciach TCP/IP. Służy on do transportu danych kontrolnych, umożliwiających wymianę informacji o zarządzaniu, statusie i statystycznych pomiędzy poszczególnymi komponentami sieci a systemem zarządzania.

SNMP wchodzi w skład „Internet Protocol Suite“ zdefiniowanego przez IETF („**I**nternet **E**ngineering **T**ask **F**orce“). 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).

Wsparcie MIB

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 ETHERNET Interface MIB
- RFC 1757 RMON Group 1,2,3,9

„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 SNMP v1 i SNMP v2c to „public“, dopóki SNMP v3 nie jest aktywowana. Jeśli SNMP v3 jest aktywowana, „Communities“ muszą być specyficzne dla SNMP v1 i v2c i nie mogą być używane razem.

ID sieci „Trusted Host“:

Adres IP jest kombinacją ID sieci i ID hosta.

- Network-ID = (Host-IP i maska).
- Użytkownik musi tylko ID sieci i ID hosta zostawić jako „0“. Gdy użytkownik wpisze ID hosta, np. 192.168.1.102, system cofnie ID hosta do 192.168.1.0.

Wskazówka



Community String
Użytkownicy powinni móc konfigurować tylko „Community String“ i uprawnienia.

Gdy użytkownik konfiguruje „Community String“ i uprawnienia z ID sieci „Trusted Host“ = 0.0.0.0 i maską podsieci = 0.0.0.0, oznacza to, że wszystkie hosty z tym „Community String“ mają dostęp do switcha.

8.5.1.1 SNMP Trap

Trap to dobrowolna wiadomość, wysyłana od urządzenia „Agent“ do „Manager“, że miało miejsce zdarzenie. „SNMP Manager“, odbierający trap, może wysyłać zapytania o więcej informacji.

9 Konfiguracja

9.1 Przegląd opcji konfiguracji

Przemysłowy switch zarządzalny oferuje 2 rozszerzone funkcje konfiguracji:

Port Telnet/SSH
Przez port Telnet można wywołać z WBM („Web Based Management“) uruchamiany z menu interfejs użytkownika.

Wskazówka



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

Port konsolowy
Przez port konsolowy z przodu przemysłowego switcha zarządzalnego (lokalnie) można przez zintegrowanego agenta zarządzającego wywołać CLI („Command Line Interface“).

Agent zarządzający bazuje na SNMP (Simple Network Management Protocol). Z pomocą tego agenta SNMP przemysłowym switchem zarządzalnym można zarządzać z każdego PC w sieci poprzez odpowiednie oprogramowanie.

Agent zarządzający obejmuje również agenta internetowego HTTP. Do agenta internetowego można uzyskać dostęp przez standardową przeglądarkę internetową z każdego PD podłączonego do sieci.

Wskazówka



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

9.1.1 Port Telnet

1. Połącz komputer z jednym z portów ETHERNET.

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

Tabela 53: Domyślne ustawienia dla portu Telnet

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

Wskazówka



Zwrócić uwagę na wskazówki dotyczące nadawania adresu IP!
W ustawieniu fabrycznym urządzenie ma adres IP 0.0.0.0 i i można się z nim bezpośrednio połączyć przez port Telnet.
Nadanie adresu IP musi zostać wykonane przez DCP lub przez CLI. Szczegółowe informacje dotyczące sposobu postępowania można znaleźć w rozdziale „PROFINET“.

9.2 Port konsolowy

Przed uzyskaniem dostępu do zintegrowanego agenta zarządzającego przemysłowego switcha zarządzalnego za pośrednictwem połączenia sieciowego należy najpierw skonfigurować urządzenie lokalne – przez port konsolowy lub protokół BOOTP – korzystając z domyślnego adresu IP, maski podsieci i standardowej bramy.

Po zakończeniu konfiguracji parametrów IP przemysłowego switcha zarządzalnego dostęp do integrowanego programu konfiguracyjnego można uzyskać z dowolnego miejsca w obrębie podłączonej sieci lub przez Internet. Zintegrowany program konfiguracyjny można uruchomić za pomocą Telnetu z dowolnego komputera w sieci. Ponadto z każdego komputera można zarządzać nim przez przeglądarkę internetową.

Wskazówka



Warunek utworzenia połączenia
Należy upewnić się, że w celu nawiązania połączenia terminal lub PC skonfigurowany jest przy użyciu wymienionych wyżej ustawień.
W przeciwnym razie połączenie nie zostanie nawiązane.

1. Połącz komputer z portem konsolowym switcha za pomocą odpowiedniego przewodu.

   Szczegóły dotyczące połączenia przewodów we wtyczce można znaleźć w rozdziale „Załącznik“ > … > „Przewód RJ-45“.

2. Użyj emulatora terminala (PuTTY) z następującymi ustawieniami:

Tabela 54: Domyślne ustawienia dla portu konsolowego

Ustawienie	Wartość domyślna
Baud Rate	38400
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3. Naciśnij **[ENTER]**, aby wywołać ekran logowania.

Tabela 55: Ekran logowania

Ustawienie	Wartość domyślna
Default Username	admin
Default Password	wago

Wskazówka



Przestrzegać sposobu postępowania!
Szczegółową informację dotyczącą sposobu postępowania przy nawiązywaniu połączenia i przypisaniu adresu IP przez CLI można znaleźć w rozdziale „PROFINET“ > „Dostęp przez port konsolowy (CLI)“.

10 System Web Based Management (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.

Wskazówka



W ustawieniu fabrycznym WBM jest tylko częściowo użyteczny!
W ustawieniu fabrycznym switch znajduje się w trybie PROFINET. W tym trybie WBM jest tylko częściowo użyteczny (zob. rozdział „PROFINET“). Aby korzystać z pełnego zakresu funkcji WBM, należy wyłączyć tryb PROFINET switcha.

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, otwórz najpierw przeglądarkę internetową (np. Microsoft Internet-Explorer lub Mozilla Firefox).
2. W pasku adresu wpisz adres IP produktu.
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 **[Apply]** lub **[Update]** albo porzuć przyciskiem **[Delete]** lub **[Discard]**.
8. Aby przejąć ustawienia, potwierdź zmiany przyciskiem **[Save configuration]**.

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

Tabela 56: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM)

Linki do nawigacji i strony WBM
▶ **[Systemstatus]**
• System Information
▶ **[Basic Settings]**
• General Settings • MAC Management • Port Mirroring • Port Settings
▶ **[PROFINET]**
• Configuration • Information • Diagnostics
▶ **[Advanced Settings]**
[Bandwidth Control] • QoS • Bandwidth Limitation **[IGMP-Snooping]** • IGMP-Snooping • IGMP Filtering • Multicast Address • Multicast IP Statistics **[VLAN]** • Port Isolation • VLAN • MAC VLAN • LLDP • Loop Detection • MRP • STP (RSTP/MSTP)
▶ **[Security]**
• Access Control List
▶ **[Monitor]**
• Alarm • System Information • Port Statistics • Port Utilization

- RMON Statistics
- SFP Information
- Traffic Monitor

▶ **[Management]**

[SNMP]

- SNMP
- SNMP Trap
- SNMPv3

- Maintenance
- System Log
- Upload File
- Ping
- User Account
- Open source License
- Wago Licenses

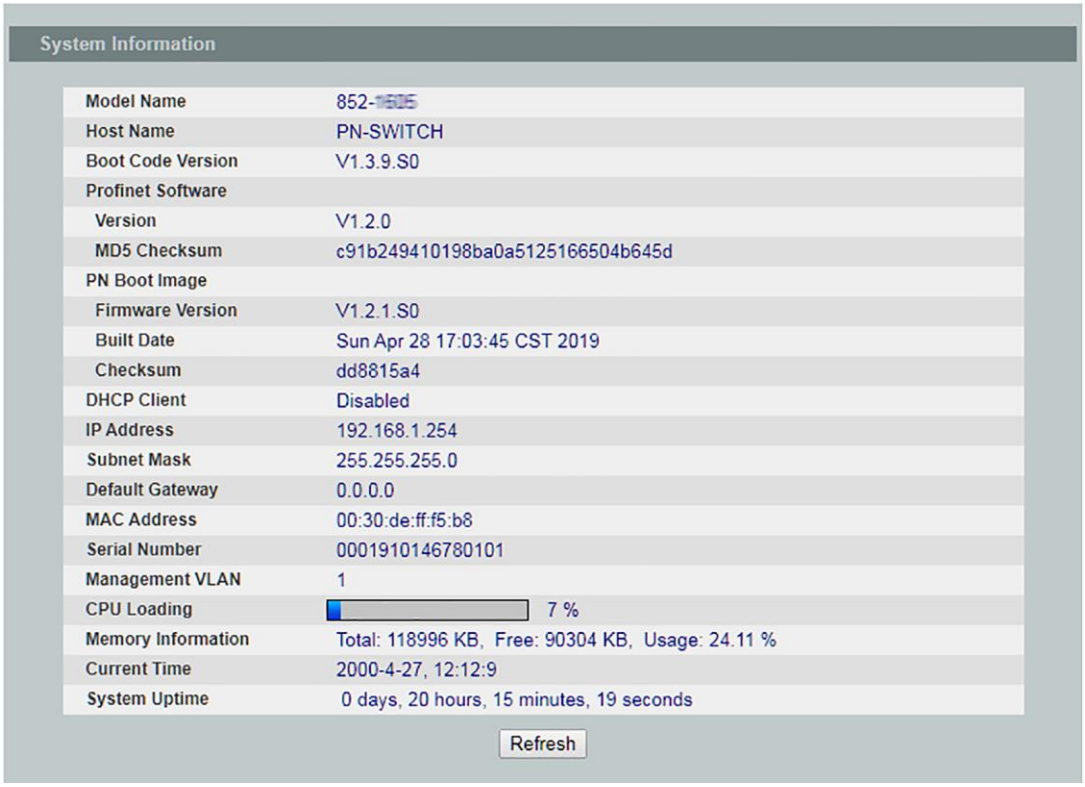
Na tych stronach WBM można wprowadzać ustawienia/konfiguracje dla przemysłowego switcha zarządzalnego.

Na niektórych stronach WBM istnieją zakładki, zawierające poszczególne strony do wprowadzania ustawień/konfiguracji.

Wartości domyślne przedstawiane są czcionką **pogrubioną.**

10.1 System Status

10.1.1 System Information



Ilustracja 42: Strona WBM „System Information“

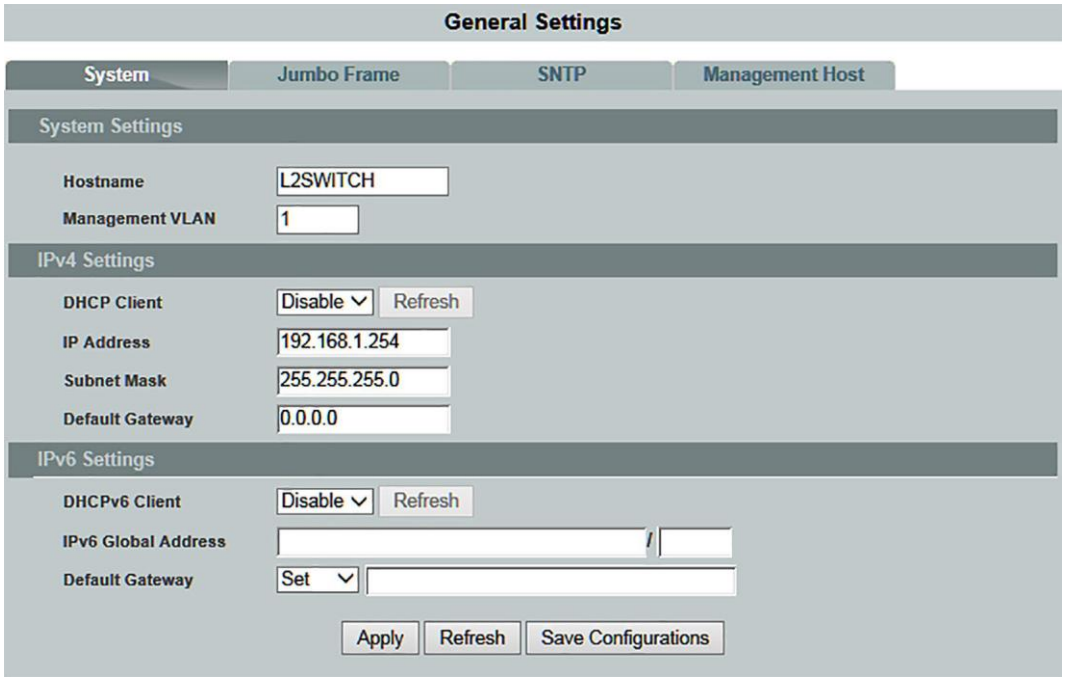
Tabela 57: Strona WBM „System Information“

Parametr	Opis
Model Name	W tym polu wyświetlana jest nazwa modelu switcha.
Host Name	W tym polu wyświetlana jest nazwa hosta switcha.
Boot Code Version	W tym polu wyświetlana jest wersja boot code.
Profinet Software Version	Numer identyfikacyjny wersji oprogramowania PROFINET
Profinet Software MD5 Checksum	Suma kontrolna wersji oprogramowania PROFINET
PN Boot Image Firmware Version	W tym polu wyświetlana jest wersja „PN Boot Image”.
PN Boot Image Build Date	W tym polu wyświetlana jest data wygenerowania firmware'u.
PN Boot Image Checksum	W tym polu wyświetlana jest suma kontrolna „PN Boot Image”.
DHCP Client	W tym polu wyświetlana jest informacja, czy aktywowana jest funkcja „DHCP Client“.
IP Address	W tym polu wyświetlany jest adres IP switcha.
Subnet Mask	W tym polu wyświetlana jest maska podsieci switcha.
Default Gateway	W tym polu wyświetlana jest domyślna brama switcha.
MAC Address	W tym polu wyświetlany jest adres MAC (Media Access Control) switcha.
Serial Number	W tym polu wyświetlany jest numer serii.
Management VLAN	W tym polu wyświetlany jest VLAN ID, potrzebny do realizacji procesów zarządzania switchem.
CPU Loading	W tym polu wyświetlane jest obłożenie switcha w procentach.
Memory Information	W tym polu wyświetlana jest całkowita („Total”) oraz aktualnie dostępna („Free”) i używana („Usage”) pamięć switcha.
Current Time	W tym polu wyświetlana jest aktualna data (yyyy-mm-dd) i godzina (hh:mm:ss).
System Uptime	W tym polu wyświetlany jest czas, przez który działa switch od momentu włączenia: dni, godziny, minuty i sekundy.

10.2 General Settings

10.2.1 General Settings

10.2.1.1 System



Ilustracja 43: Strona WBM „General Settings“ – zakładka „System“

Tabela 58: Strona WBM „General Settings“ – zakładka „System“

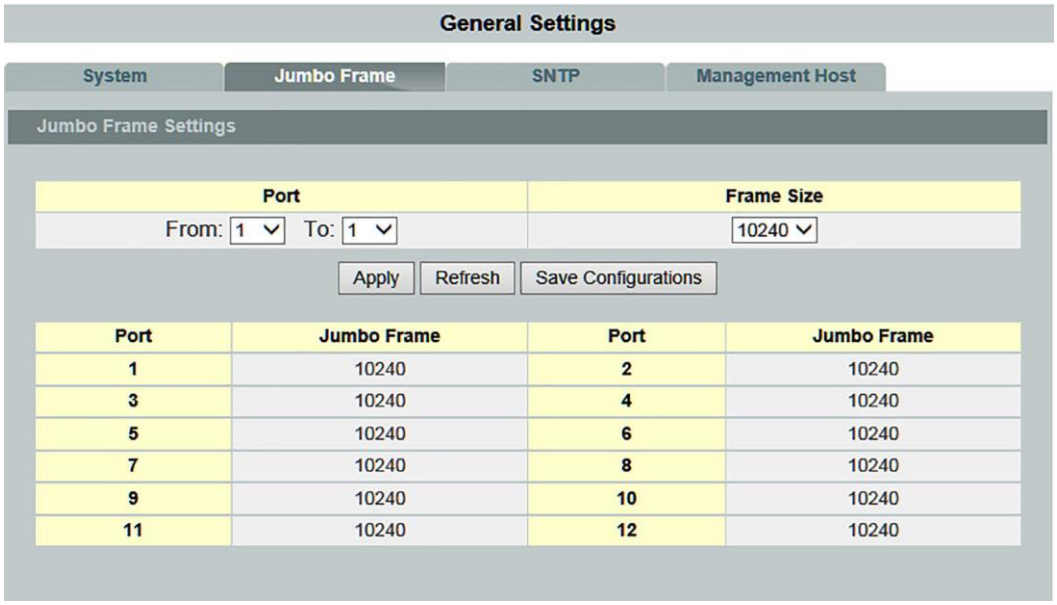
System Settings		
Parametr	**Domyślnie**	**Opis**
Hostname	**L2SWITCH**	Należy wpisać nazwę switcha, składającą się z maksymalnie 64 liter/cyfr. Nazwa hosta powinna składać się z kombinacji cyfr, liter, łączników (-) lub podkreśleń (_).
Management VLAN	**1**	Należy wpisać grupę VLAN, która ma uzyskać dostęp do switcha. Właściwy zakres VLAN: 1 … 4094.
		Wskazówka  **Konfiguracja Management-VLAN** Przed konfiguracją Management VLAN należy najpierw utworzyć Management VLAN i przypisać co najmniej jeden port.
IPv4 Settings		
Parametr	**Domyślnie**	**Opis**
DHCP Client	**Disable**	W polu wyboru należy wybrać „Disable“, gdy adres IP switcha ma być skonfigurowany ręcznie.
	Enable	W polu wyboru należy wybrać „Enable“, aby switch przyjął adres IP wygenerowany automatycznie przez serwer DHCP. Należy kliknąć **[Renew]**, aby switch ponownie przyjął adres IP z serwera DHCP.
IP Address	**0.0.0.0**	W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami.
Subnet Mask	**0.0.0.0**	W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.
Default Gateway	0.0.0.0	W polu edycji należy wpisać adres IP domyślnej bramy, używając zapisu z kropkami.
IPv6 Settings		
Parametr	**Domyślnie**	**Opis**
DHCPv6 Client	**Disable**	W polu wyboru należy wybrać „Disable“, gdy adres IP switcha ma być skonfigurowany ręcznie.
	Enable	W polu wyboru należy wybrać „Enable“, aby switch przyjął adres IP wygenerowany automatycznie przez DHCP. Należy kliknąć **[Renew]**, aby switch aktualizował wartości**.**
IPv6 Global Address		W tym polu wyświetlany jest globalny adres IPv6.
Default Gateway	**Set**	W polu wyboru należy wybrać „Set“, jeśli adres IP ma być wpisany. Należy wpisać adres IP domyślnej bramy, używając zapisu z kropkami.
	Unset	W polu wyboru należy wybrać „Unset“, jeśli adres IP nie ma być wpisany.

10.2.1.2 Jumbo Frame

Wskazówka

Dodatkowa informacja

Więcej informacji o „Jumbo Frame“ można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 44: Strona WBM – zakładka „Jumbo Frame”

Tabela 59: Strona WBM – zakładka „Jumbo Frame”

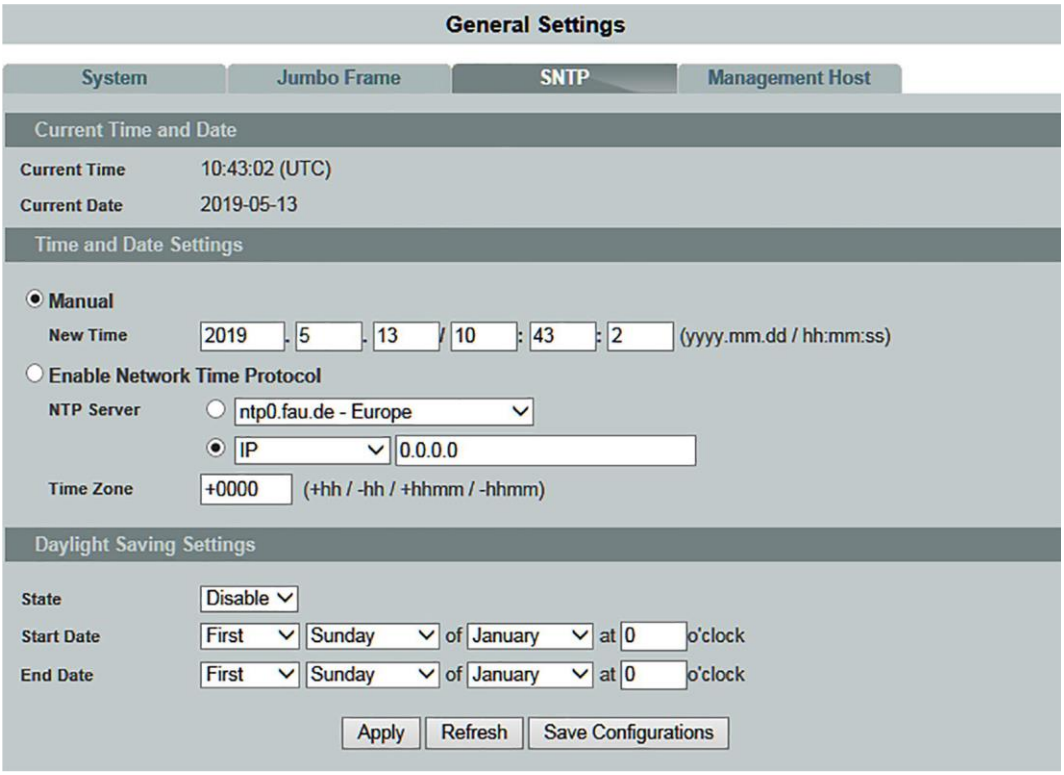
Jumbo Frame Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Jumbo Frame“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Jumbo Frame“.
Jumbo Frame		**10240**	W polu wyboru należy dla wszystkich portów wybrać maksymalną liczbę bajtów dla „Jumbo Frame“. Im większa wielkość „Jumbo Frames“, tym większa wydajność sieci.
		1522	
		1536	
		1552	
		9010	
		9216	
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Jumbo Frame		1522	W tej kolumnie wyświetlana jest maksymalna liczba bajtów dla „Jumbo Frame“.
		1536	
		1552	
		9010	
		9216	
		10240	

10.2.1.3 SNTP

Wskazówka

Dodatkowa informacja

Więcej informacji o „SNTP“ (**S**imple **N**etwork **T**ime **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 45: Strona WBM – zakładka „SNTP”

Tabela 60: Strona WBM – zakładka „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**		
Manual	New Time ○	Tę opcję należy wybrać, aby ręcznie ustawić w systemie czas i datę. Należy wpisać nową datę w formacie rok/miesiąc/dzień oraz aktualny czas w formacie godzina/minuta/sekunda. Po kliknięciu [Apply] pojawiają się nowe dane w polach „Current Time“ i „Current Date“.		
Enable Network Time Protocol		Tę opcję należy wybrać, aby użyć Network Time Protocol (NTP) dla synchronizacji czasu.		
	NTP-Server ◉	◉	Tę opcję należy wybrać, aby użyć zdefiniowanego wcześniej serwera czasu. Switch będzie przez 60 sekund szukał serwera czasu.	
		○	Tę opcję należy wybrać, aby wpisać adres IP serwera czasu. Switch będzie przez 60 sekund szukał serwera czasu.	
	0.0.0.0	◉	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 60: Strona WBM – zakładka „SNTP”

Daylight Saving Settings		
Parametr	**Domyślnie**	**Opis**
Status	**Disable**	Należy wybrać „Disable“, jeśli nie używamy czasu letniego.
	Enable	Należy wybrać „Enable“, jeśli ma być zastosowany czas letni.
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.

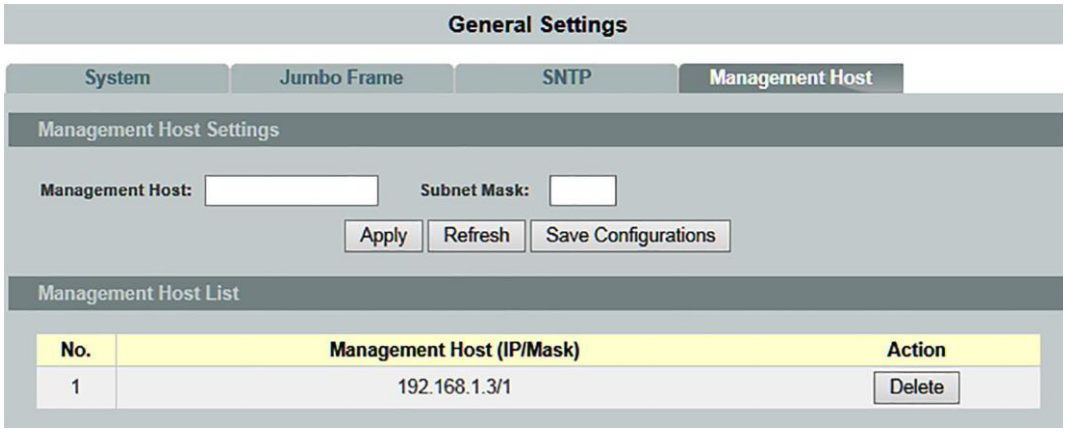
1)	Na większości terytorium USA czas letni rozpoczyna się w drugą niedzielę marca. W każdej strefie czasowej USA czas letni rozpoczyna się o godzinie 02:00 czasu miejscowego. Zgodnie z tym należy wybrać „Second, Sunday, March“ i „2:00“. W Unii Europejskiej czas letni rozpoczyna się w ostatnią niedzielę 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).

10.2.1.4 Management Host

Wskazówka

Dodatkowa informacja

Więcej informacji o „Management Host” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 46: Strona WBM – zakładka „Management Host”

Tabela 61: Strona WBM – zakładka „Management Host”

Management Host Settings		
Parametr	**Domyślnie**	**Opis**
Management Host		W polu edycji należy wpisać adres IP „Management Host“, używając zapisu z kropkami.
Subnet Mask		W polu edycji należy wpisać numer adresu maski podsieci „Management Host“, używając zapisu z kropkami.
Management Host List		
Parametr	**Domyślnie**	**Opis**
No.	1 … 3	W tej kolumnie wyświetlane są kolejne numery każdego „Management Host“.
Management Host (IP/Mask)		W tej kolumnie wyświetlane są adresy IP „Management Host”.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

10.2.2 MAC Management

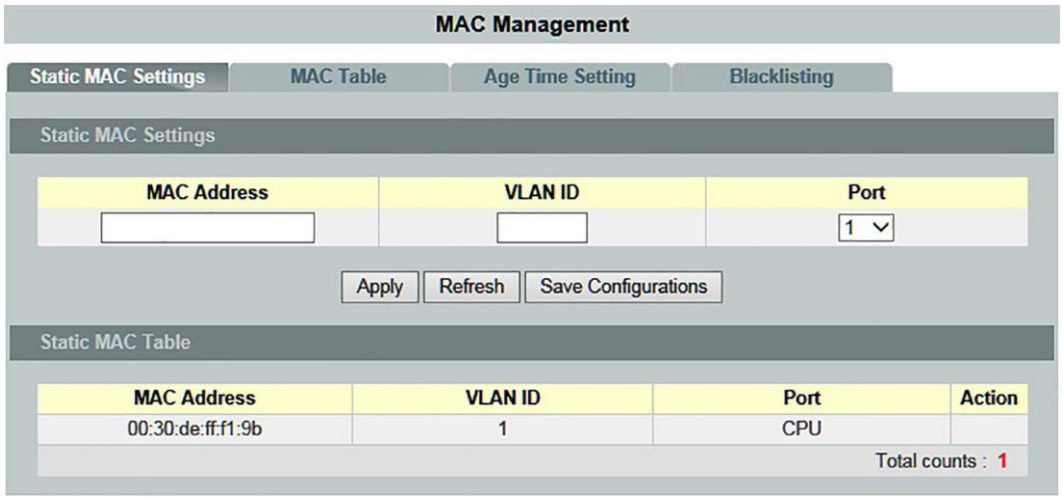
Wskazówka

Dodatkowa informacja
Więcej informacji o „MAC Management” można znaleźć w rozdziale „Opis funkcji”.

10.2.2.1 Static MAC Settings

Wskazówka

Dodatkowa informacja
Więcej informacji o „SNTP“ (Static MAC Settings) można znaleźć w rozdziale „Opis funkcji“.

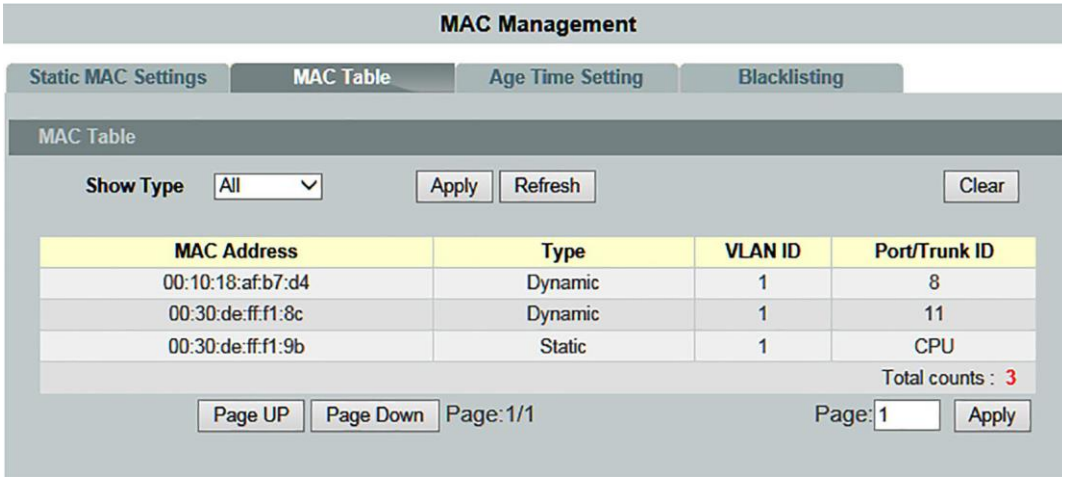


Ilustracja 47: Strona WBM – zakładka „Static MAC Settings”

Tabela 62: Strona WBM – zakładka „Static MAC Settings”

Static MAC Settings		
Parametr	**Domyślnie**	**Opis**
MAC Address		W polu edycji należy wpisać adres MAC komputera lub urządzenia, który ma być przejęty do tabeli adresów MAC. Właściwy format to: hh:hh:hh:hh:hh:hh.
VLAN ID		W polu edycji należy wpisać „VLAN ID“, który ma być przydzielony komputerowi lub urządzeniu.
Port	**1**	W polu wyboru należy wybrać port, na którym podłączony jest komputer lub port.
Static MAC Table		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tej kolumnie wyświetlane są wpisane ręcznie adresy MAC.
VLAN ID		W tej kolumnie wyświetlany jest „VLAN ID“ wpisanych ręcznie adresów MAC.
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów wpisanych ręcznie adresów MAC. Adres MAC „CPU” jest adresem MAC switcha.
Action		Należy kliknąć **[Delete]**, aby usnąć wpisany ręcznie adres MAC z tabeli adresów MAC. Adresu MAC switcha nie można usunąć z tabeli statycznych adresów MAC.
Total counts		W tym polu wyświetlana jest zbiorcza liczba wpisów w tabeli statycznych adresów MAC.

10.2.2.2 MAC Table

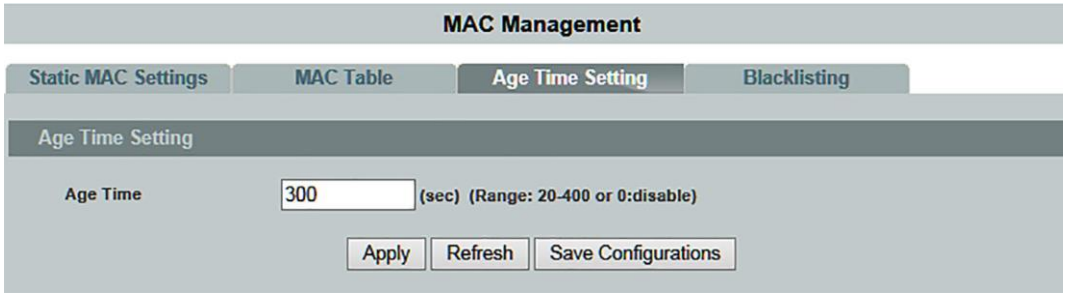


Ilustracja 48: Strona WBM – zakładka „MAC Table”

Tabela 63: Strona WBM – zakładka „MAC Table”

MAC Table		
Parametr	**Domyślnie**	**Opis**
Show Type	**[All]**	W polu wyboru należy wybrać „All“, aby wyświetlić wszystkie adresy MAC.
	Static	W polu wyboru należy wybrać „Static“, aby wyświetlić statyczne adresy MAC.
	Dynamic	W polu wyboru należy wybrać „Dynamic“, aby wyświetlić dynamiczne adresy MAC.
	Port	W polu wyboru należy wybrać „Port“, aby wyświetlić odpowiednie adresy MAC.
	MAC	W polu wyboru należy wybrać „MAC“, aby wyświetlić odpowiednie adresy MAC.
MAC Address		W tej kolumnie wyświetlane są adresy MAC.
Type		W tej kolumnie wyświetlana jest informacja, czy wpis został wprowadzony ręcznie (Static), czy nadany przez switch (Dynamic).
VLAN ID		W tej kolumnie wyświetlany jest „VLAN ID“ adresu MAC.
Port/Trunk ID		W tej kolumnie wyświetlany jest numer portu, z którym połączony jest adres MAC. „CPU“ oznacza tu wpis adresu MAC switcha.
Total counts		W tym polu wyświetlana jest zbiorcza liczba wpisów w tabeli adresów MAC.
Page Up		Przy dużej liczbie adresów MAC można tym przyciskiem przewinąć ekran w górę.
Page Down		Przy dużej liczbie adresów MAC można tym przyciskiem przewinąć ekran w dół.
Page		W tym polu wyświetlana jest aktualna strona tabeli adresów MAC.

10.2.2.3 Age Time Setting



Ilustracja 49: Strona WBM – zakładka „Age Time Setting”

Tabela 64: Strona WBM „MAC Management” – zakładka „Age Time Setting”

Age Time Setting		
Parametr	**Domyślnie**	**Opis**
Age Time (sec) (Range: 20-400 or 0:disable)	**300**	W polu edycji należy wpisać „Age Time“. Właściwy zakres: 0 lub 20 … 400 s

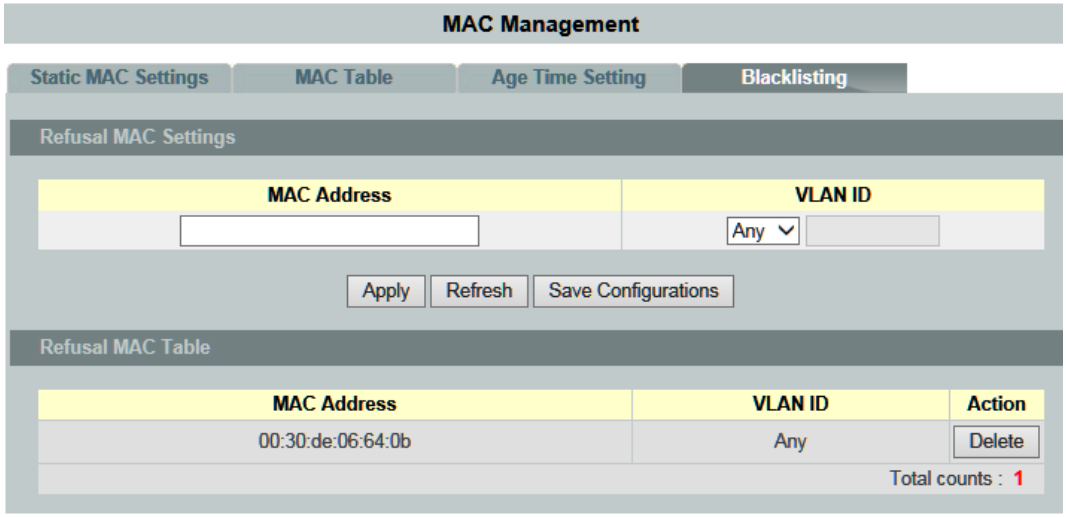
10.2.2.4 Blacklisting

Wskazówka

Dodatkowa informacja
Więcej informacji o „Blacklisting” można znaleźć w rozdziale „Opis funkcji”.

Wskazówka

Maksymalna liczba wpisów MAC na „Blacklist“
Można skonfigurować maksymalnie 20 wpisów.



Ilustracja 50: Strona WBM – zakładka „Blacklisting”

Tabela 65: Strona WBM – zakładka „Blacklisting”

Blacklisting		
Parametr	**Domyślnie**	**Opis**
MAC Address		W polu edycji należy wpisać adres MAC komputera lub urządzenia, który/które ma być odrzucony/odrzucone. Właściwy format to: hh:hh:hh:hh:hh:hh.
VLAN ID	**Any**	Switch otrzymuje dowolny „VLAN ID“.
	VLAN	W polu edycji należy wpisać „VLAN ID“, który ma być przydzielony komputerowi lub urządzeniu.
Refusal MAC Settings		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tej kolumnie wyświetlane są adresy MAC.
VLAN ID		W tej kolumnie wyświetlany jest „VLAN ID“ wpisanych adresów MAC.
Action		Kliknij **[Delete]**, aby usunąć ręcznie wpisany adres MAC z tabeli „Blacklist”.
Total counts		W tym polu wyświetlana jest zbiorcza liczba wpisów w tabeli „Blacklist“.

10.2.3 Port Mirroring

Wskazówka

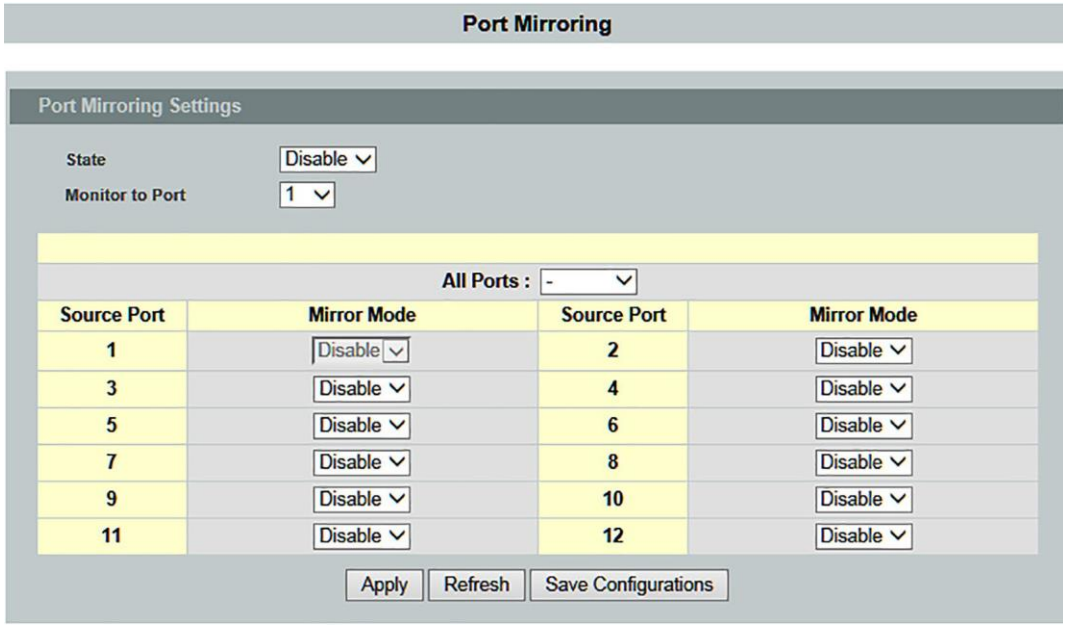
Dodatkowa informacja

Więcej informacji o „Port Mirroring” można znaleźć w rozdziale „Opis funkcji”.

Wskazówka

Monitor Port

„Monitor Port“ nie może być członkiem grupy „Trunk Port“.
„Monitor Port“ nie może być portem wejściowym lub wyjściowym.
Gdy port został skonfigurowany jako port źródłowy i użytkownik skonfigurował go następnie jako port docelowy, zostaje on automatycznie usunięty z portów źródłowych.



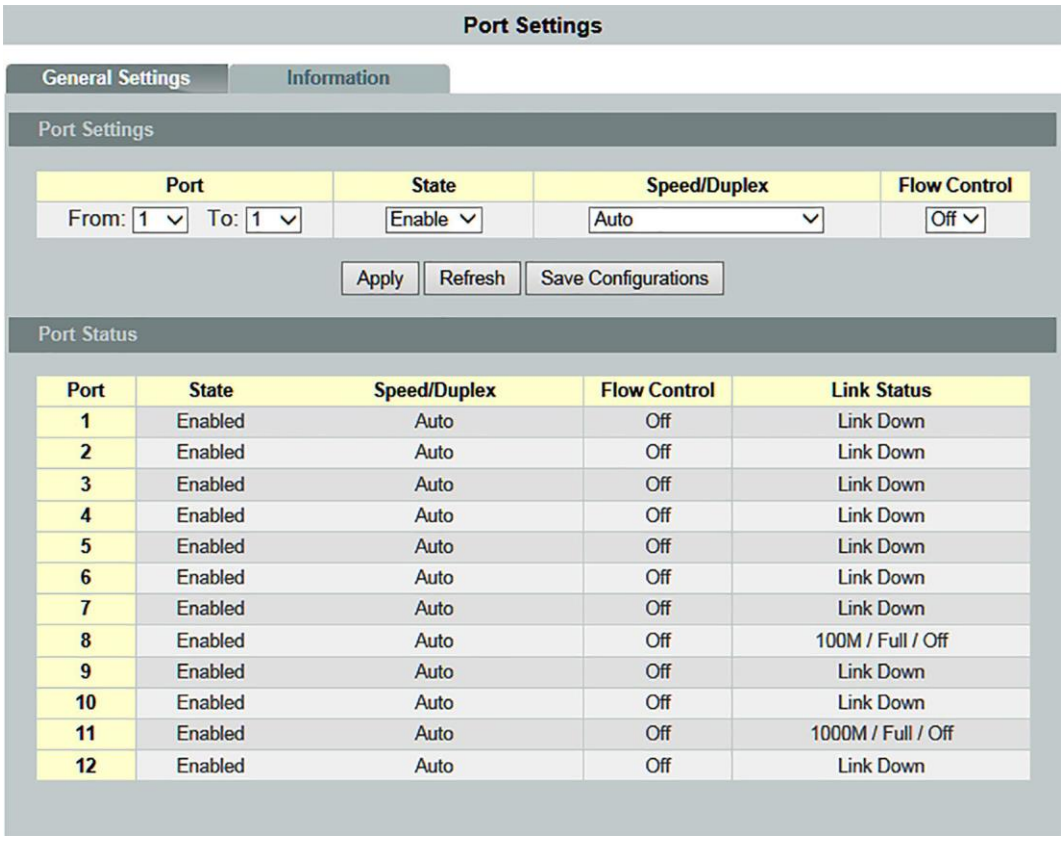
Ilustracja 51: Strona WBM – „Port Mirroring”

Tabela 66: Strona WBM – „Port Mirroring”

Port Mirroring Settings		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Port Mirroring”.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Port Mirroring”.
Monitor to Port	**1** … 10 (12)	W polu wyboru należy wybrać port, który ma być połączony z „Network Traffic Analyzer“.
All Ports	-	Ustawienia w tym polu wyboru oddziałują na wszystkie porty. Należy tu wprowadzać tylko takie ustawienia, które mają dotyczyć wszystkich portów. Należy rozpocząć od ustawień ogólnych, a następnie wprowadzać ustawienia dla poszczególnych portów.
	Disable	
	Ingress	
	Egress	
	Both	
Source Port	1 … 10 (12)	W tej kolumnie wyświetlany jest numer poszczególnych „Source Ports”.
Mirror Mode	Disable	W polu wyboru należy wybrać „Disable“, gdy ruch danych nie ma być skopiowany z wyspecyfikowanych „Source Ports“ do „Monitor Port“.
	Ingress	W polu wyboru należy wybrać „Ingress“, aby skopiować tylko dane wchodzące wyspecyfikowanych „Source Ports” do „Monitor Port”.
	Egress	W polu wyboru należy wybrać „Egress“, aby skopiować tylko dane wychodzące wyspecyfikowanych „Source Ports” do „Monitor Port”.
	Both	W polu wyboru należy wybrać „Both“, aby skopiować dane wchodzące i wychodzące z wyspecyfikowanych „Source Ports“ do „Monitor Port“.

10.2.4 Port Settings

10.2.4.1 General Settings

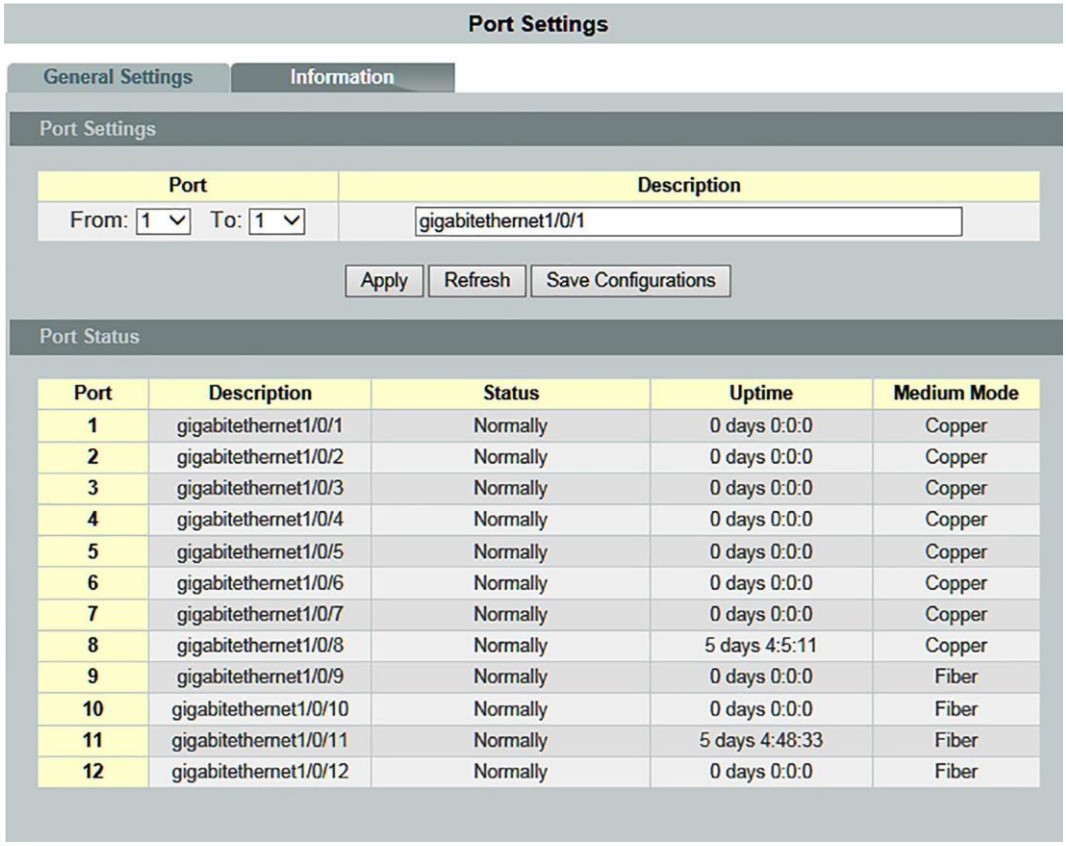


Ilustracja 52: Strona WBM „Port Settings“ – zakładka „General Settings“

Tabela 67: Strona WBM – zakładka „Port Settings” – zakładka „General Settings”

Port Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
State		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować port.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować port.
Speed/Duplex		**Auto**	W polu wyboru należy wybrać prędkość i tryb duplex dla portu.
		10 Mb/s / full dupleks	
		10 Mb/s / half duplex	
		100 Mb/s / full dupleks	
		100 Mb/s / half duplex	
		1000 Mb/s / full dupleks	
Flow control		**Off**	W polu wyboru należy wybrać „Off“, aby przerwać dostęp do zasobów buforów portów i przerwać pracę switcha w sieci.
		On	W polu wyboru należy wybrać „On“, aby otrzymać dostęp do zasobów buforów portów i zapewnić bezprzerwową pracę switcha w sieci.
Port Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	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.
Flow control			W tej kolumnie wyświetlana jest informacja, czy „Flow Control“ dla portu ustawiona jest na „On“, czy na „Off“.
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.

10.2.4.2 Information



Ilustracja 53: Strona WBM „Port Settings” – zakładka „Information”

Tabela 68: Strona WBM „Port Settings” – zakładka „Information”

Port Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być wyświetlony.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być wyświetlony.
Opis			W polu edycji należy wpisać nazwę portu.
Port Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Opis			W tej kolumnie wyświetlana jest nazwa portu.
Status			W tej kolumnie wyświetlany jest status portu.
Uptime			W tej kolumnie wyświetlany jest czas pracy portu.
Medium Mode		Copper Fiber	W tej kolumnie wyświetlany jest rodzaj połączenia. Copper wire Fiber optic cable

10.3 PROFINET

Opisy interfejsu WBM w obszarze PROFINET można znaleźć w rozdziale „PROFINET”.

10.4 Advanced Settings

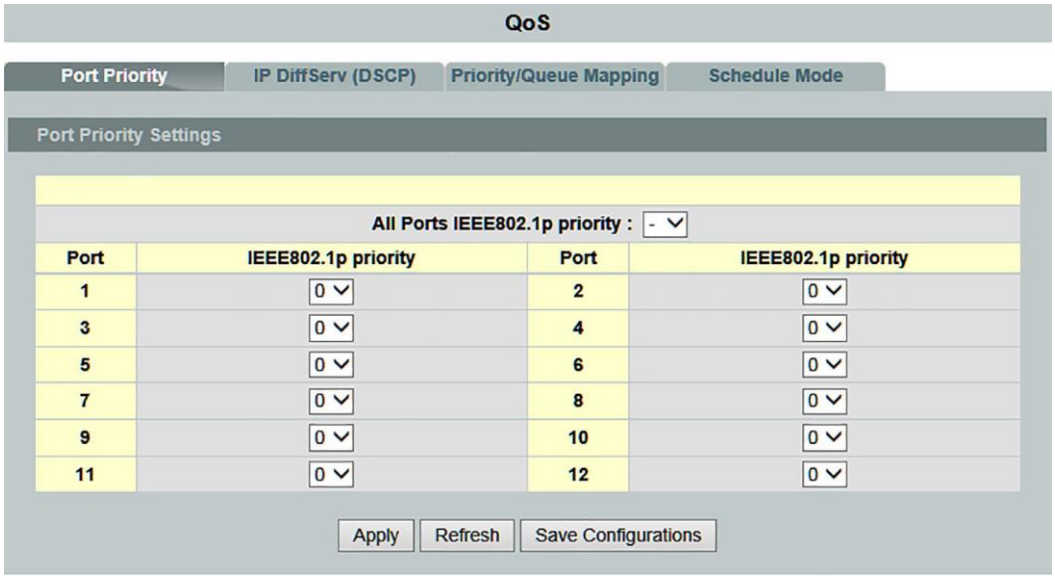
10.4.1 Bandwidth Control

10.4.1.1 QoS

Wskazówka

Dodatkowa informacja
Więcej informacji o „QoS” (Quality of Service) można znaleźć w rozdziale „Opis funkcji”.

10.4.1.1.1 Port Priority

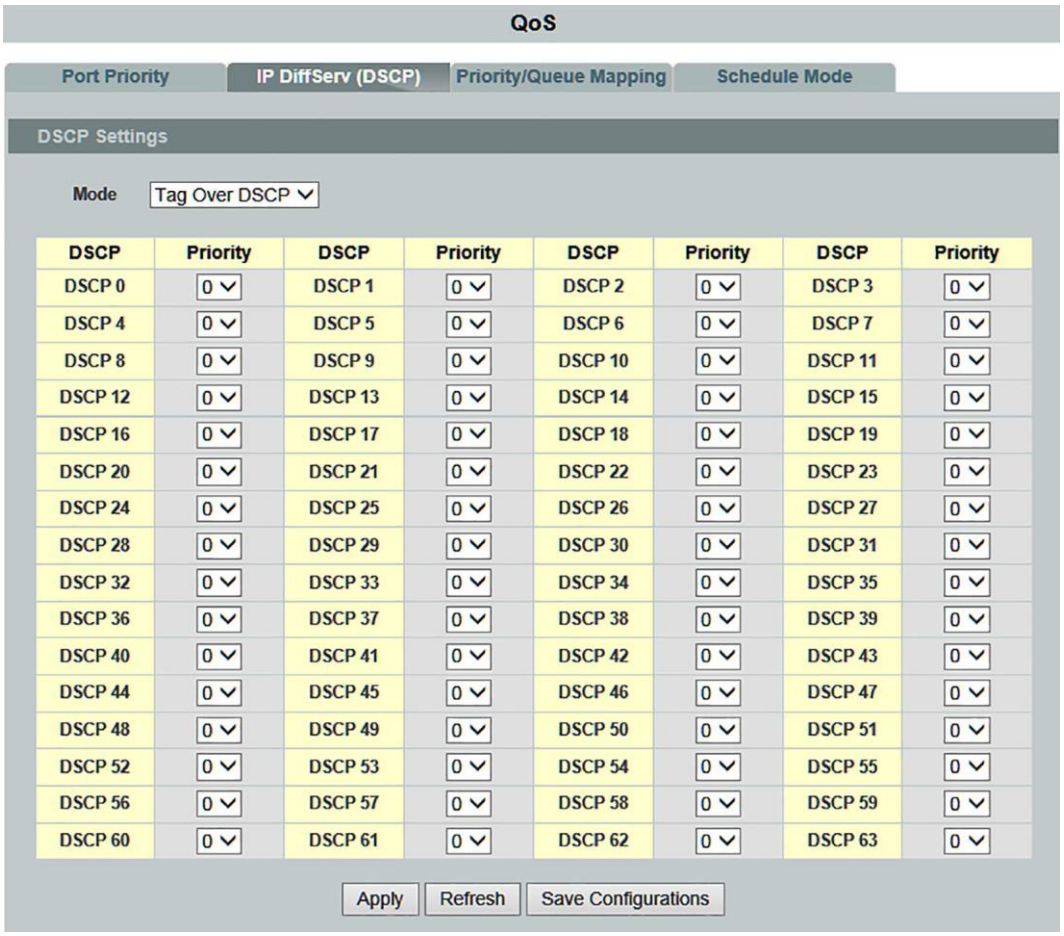


Ilustracja 54: Strona WBM „QoS” – zakładka „Port Priority”

Tabela 69: Strona WBM „QoS” – zakładka „Port Priority”

Port Priority Settings		
Parametr	**Domyślnie**	**Opis**
All Ports have IEEE 802.1p priority.	-	W polu wyboru należy wybrać wartość priorytetu dla wszystkich portów. Wartość ta określa priorytet pakietu i dołączana jest do pola „Priority Tag“ wchodzących pakietów.
	0 … 7	0 = najniższy priorytet 7 = najwyższy priorytet
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
IEEE 802.1p Priority	**0** … 7	W polu wyboru należy wybrać priorytet dla pakietów, odbieranych na tym porcie. Tylko pakietowi bez „802.1p Tag Priority“ przydzielany jest tu podany priorytet.

10.4.1.1.2 IP DiffServ (DSCP)

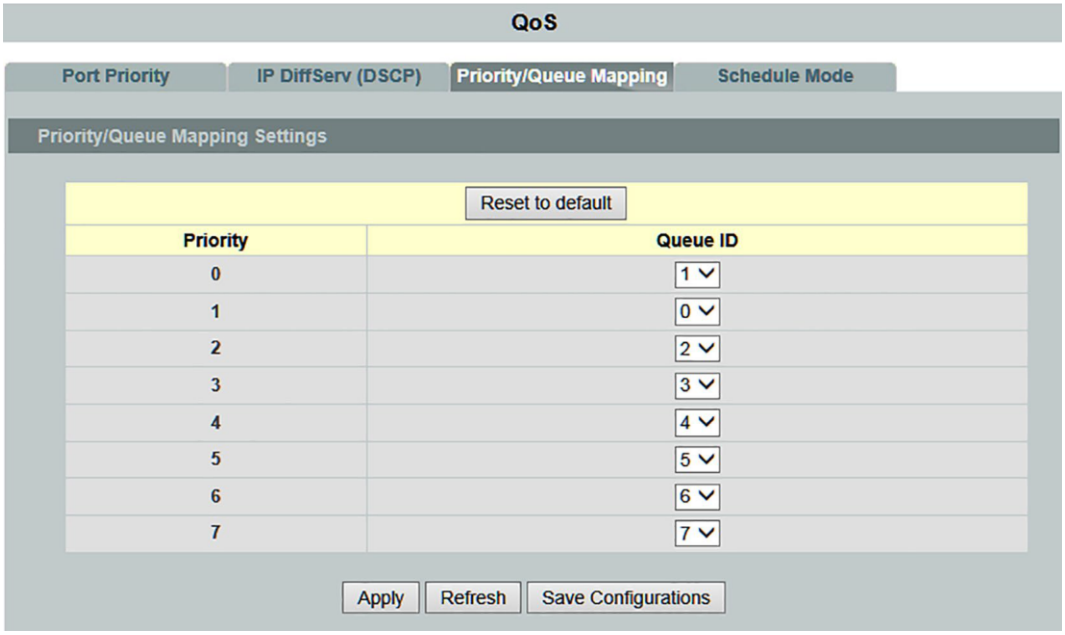


Ilustracja 55: Strona WBM) „QoS” – zakładka „IP DiffServ (DSCP)”

Tabela 70: Strona WBM „QoS” – zakładka „IP DiffServ (DSCP)”

DSCP Settings		
Parametr	**Domyślnie**	**Opis**
Mode	**Tag Over DSCP**	W polu wyboru należy wybrać „Tag Over DSCP“, gdy znacznik 802.1p otrzymuje wyższy priorytet niż priorytet DSCP.
	DSCP Over Tag	W polu wyboru należy wybrać „DSCP Over Tag“, gdy znacznik 802.1p otrzymuje niższy priorytet niż priorytet DSCP.
DSCP	DSCP 0 … DSCP 63	W tej kolumnie wyświetlane są pola DHCP.
Priority	**0** … 7	W polu wyboru należy wybrać poziom priorytetu. 0 = najniższy priorytet 7 = najwyższy priorytet

10.4.1.1.3 Priority/Queue Mapping



Ilustracja 56: Strona WBM „QoS" – zakładka „Priority/Queue Mapping"

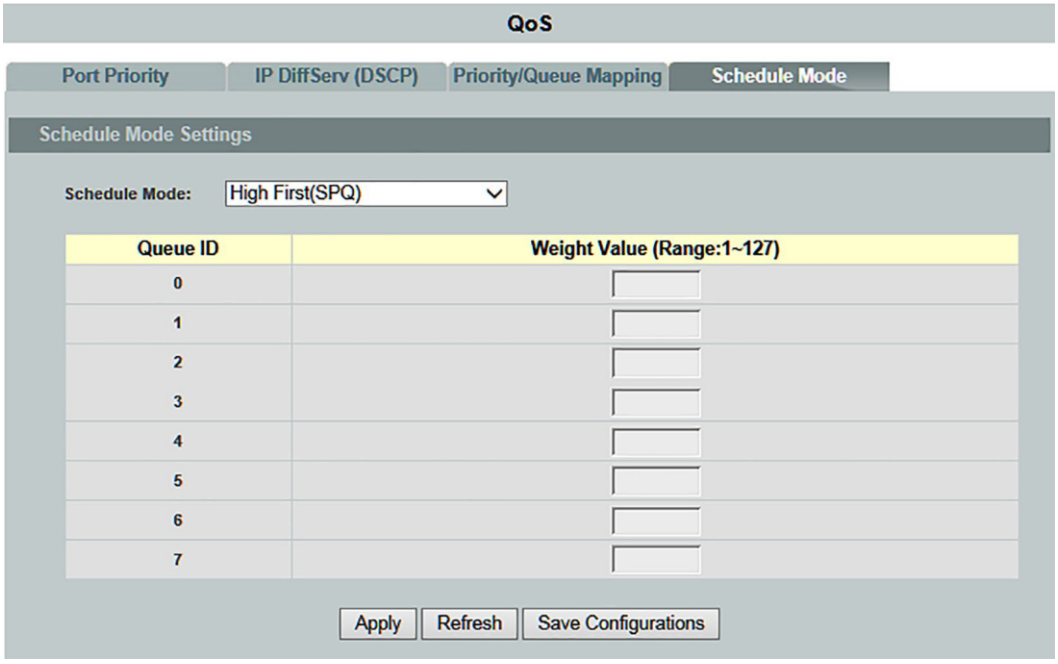
Tabela 71: Strona WBM „QoS" – zakładka „Priority/Queue Mapping"

Priority/Queue Mapping Settings		
Parametr	**Domyślnie**	**Opis**
Reset to defauli		Przycisk ten należy kliknąć, aby zresetować priorytet „Queues" do wartości domyślnych.
Priority	0 … 7	W tej kolumnie wyświetlany jest poziom priorytetu. 0 = najniższy priorytet 7 = najwyższy priorytet
Queue ID	0 … 7	W polu wyboru należy wybrać numer „Queue" dla pakietów z poziomem priorytetu.

Tabela 72: Default Settings

Priority	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

10.4.1.1.4 Schedule Mode



Ilustracja 57: Strona systemu zarządzania przez WWW (WBM) „QoS” – zakładka „Schedule Mode”

Tabela 73: Strona WBM „QoS“ – zakładka „Schedule Mode“

Schedule Mode Settings			
Parametr	**Domyślnie**	**Opis**	
Schedule Mode	**Strict Priority Queuing (SPQ)**	W polu wyboru należy wybrać „Strict Priority Queuing (SPQ)“, gdy „Hardware Priority Queues)“ mają być wykonywane po kolei.	
	Weighted Round Robin (WRR)	W polu wyboru należy wybrać „Weighted Round Robin (WRR)“, gdy ma być wykorzystany algorytm na bazie wagi Queue (wartość wprowadzana w polu Weight Value (Range: 1~127)). „Queues“ o wyższej wadze są bardziej faworyzowane niż te o mniejszej wadze.	
Queue ID	0 … 7	W tej kolumnie wyświetlana jest informacja, która „Queue“ jest konfigurowana. 0 = najniższy priorytet 7 = najwyższy priorytet	
Weight Value (Range: 1~127)	**1** … 127	„Weight Value“ może być konfigurowana, gdy zostanie wybrana „Weighted Round Robin (WRR)“. Szerokość pasma dzielona jest między różne „Traffic Queues“ odpowiednio do ich wagi. 0 = najniższy priorytet 127 = najwyższy priorytet	
		Wskazówka 	**Zmiana „Weight Value (Range: 1~127)“** Przy wyborze „Strict Priority Queuing (SPQ)“ nie można zmienić „Weight Value“. Aby było to możliwe, należy najpierw wybrać „Weighted Round Robin (WRR)“. Potem można zmienić „Strict Priority Queuing (SPQ)“.

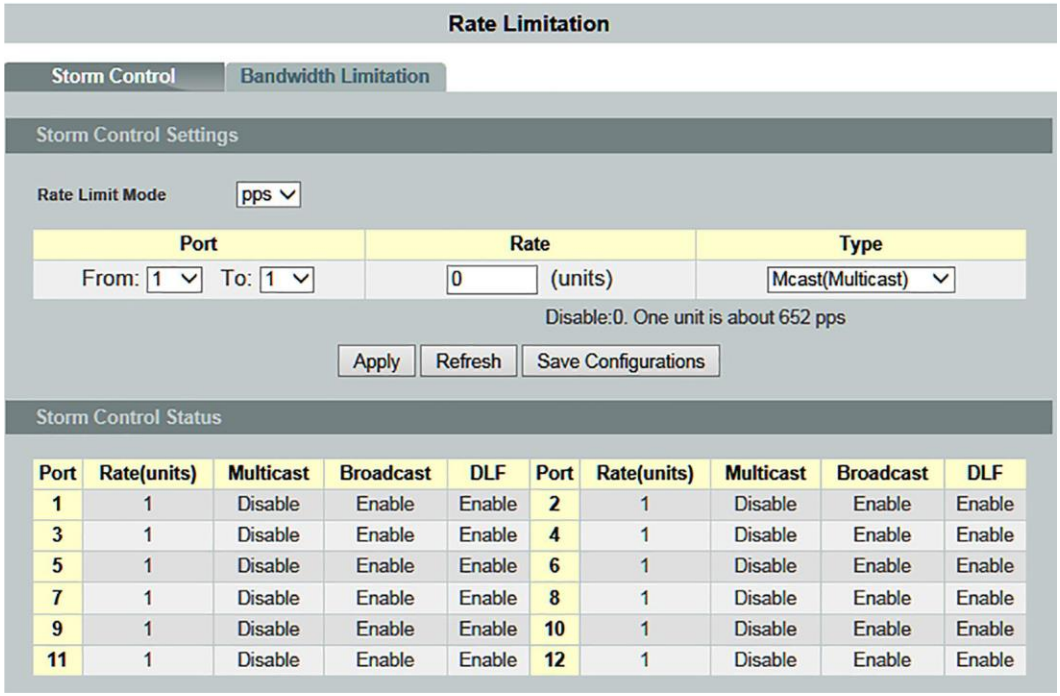
10.4.1.2 Rate Limitation

10.4.1.2.1 Storm Control

Wskazówka

Dodatkowa informacja

Więcej informacji o „Storm Control” można znaleźć w rozdziale „Opis funkcji”.



Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable
7	1	Disable	Enable	Enable	8	1	Disable	Enable	Enable
9	1	Disable	Enable	Enable	10	1	Disable	Enable	Enable
11	1	Disable	Enable	Enable	12	1	Disable	Enable	Enable

Ilustracja 58: Strona WBM „Rate Limitation“ – zakładka „Strom Control“

Tabela 74: Strona WBM „Rate Limitation“ – zakładka „Storm Control“

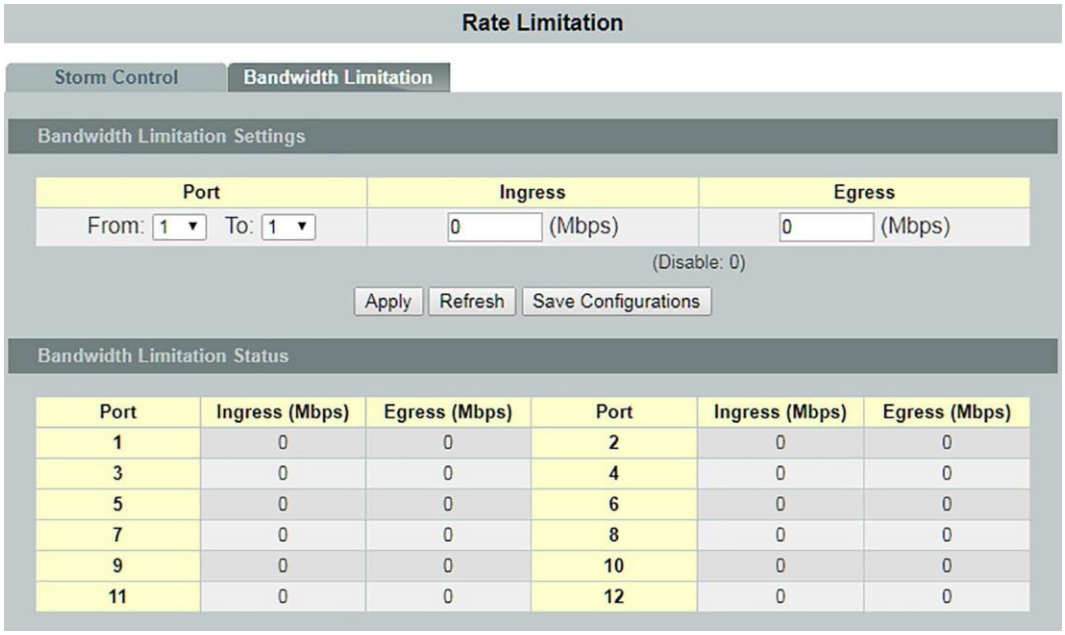
Storm Control Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Storm Control”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Storm Control”.
Number (units)		**0**	W polu wyboru należy wybrać liczbę pakietów (rodzaju wyspecyfikowanego w polu „Typ“), jaką może odebrać switch w ciągu sekundy.
Type		Bcast (Broadcast)	W polu wyboru należy wybrać „Bcast (Broadcast)“, aby ustawić wartość graniczną liczby odebranych pakietów broadcast w ciągu sekundy.
		Mcast (Multicast)	W polu wyboru należy wybrać „Mcast (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.
		Mcast+Bcast	W polu wyboru należy wybrać „Mcast+Bcast“, aby ustawić wartość graniczną liczby odebranych pakietów multicast i broadcast w ciągu sekundy.
		Mcast+DLF	W polu wyboru należy wybrać „Mcast+DLF“, aby ustawić wartość graniczną liczby odebranych pakietów multicast i broadcast w ciągu sekundy.
		Bcast+DLF	W polu wyboru należy wybrać „Bcast+DLF“, aby ustawić wartość graniczną liczby odebranych pakietów broadcast i DLF w ciągu sekundy.
		Mcast+Bcast+ DLF	W polu wyboru należy wybrać „Mcast+Bcast+DLF“, aby ustawić wartość graniczną liczby odebranych pakietów multicast, broadcast i DLF w ciągu sekundy.
Storm Control Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Number (units)			W tej kolumnie wyświetlana jest liczba pakietów, jaką może odebrać switch w ciągu sekundy.
Multicast		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy multicast.
Broadcast		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy broadcast.
DLF		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy ustawienie w kolumnie „Rate“ dotyczy DLF.

10.4.1.2.2 Bandwidth Limitation

Wskazówka

Dodatkowa informacja

Więcej informacji o „Bandwidth Limitation“ można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 59: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“

Tabela 75: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“

Bandwidth Limitation Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Bandwidth Limitation Settings“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Bandwidth Limitation Settings“.
Ingress (Mbs)		**0**	W polu edycji należy wpisać „Bandwidth Limitation“ dla wchodzących pakietów. Port 1 … 8 0 … 100 Port 9 … 10(12) 0 … 1000
Egress (Mbs)		**0**	W polu edycji należy wpisać „Bandwidth Limitation“ dla wychodzących pakietów.
Bandwidth Limitation Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Ingress (Mbs)			W tej kolumnie wyświetlane są ustawiona wartość „Bandwidth“ dla Ingress.
Egress (Mbs)			W tej kolumnie wyświetlane są ustawiona wartość „Bandwidth“ dla Egress.

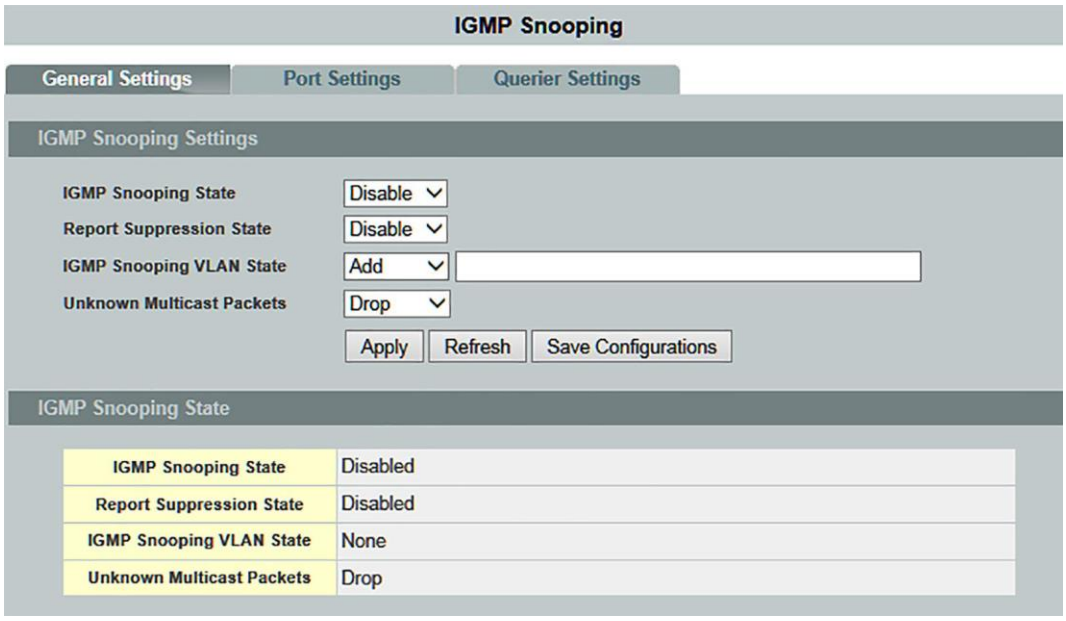
10.4.2 IGMP-Snooping

Wskazówka

Dodatkowa informacja
Więcej informacji o „IGMP-Snooping“ (**I**nternet **G**roup **M**anagement **P**rotocol Snooping) można znaleźć w rozdziale „Opis funkcji“.

10.4.2.1 IGMP-Snooping

10.4.2.1.1 General Settings

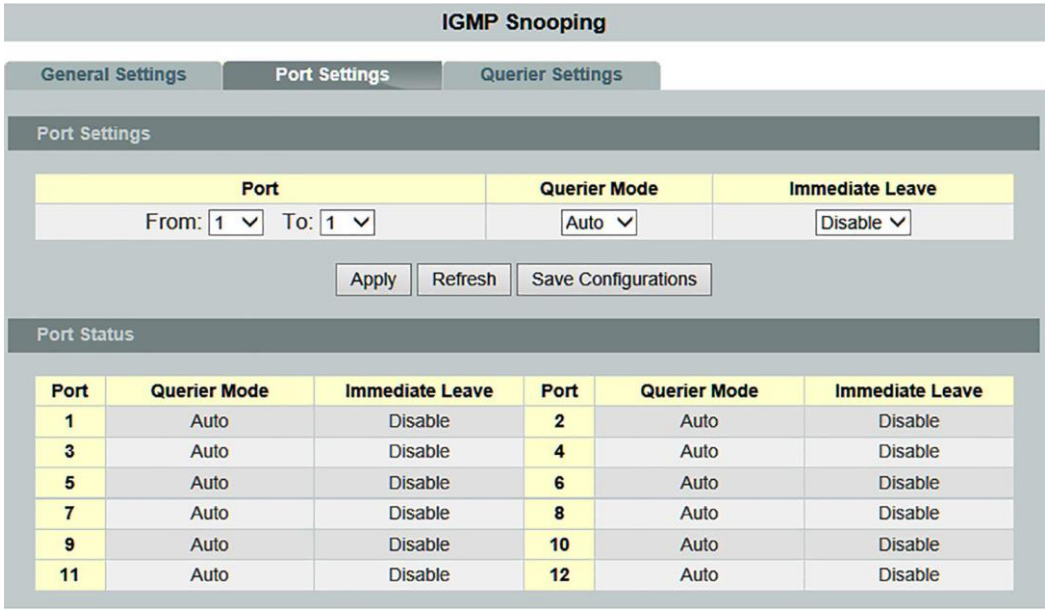


Ilustracja 60: Strona WBM „IGMP Snooping“ – zakładka „General Settings“

Tabela 76: Strona WBM „IGMP Snooping“ – zakładka „General Settings“

IGMP Snooping Settings		
Parametr	**Domyślnie**	**Opis**
IGMP Snooping State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „IGMP Snooping“ i przesłać dane grupowe multicast tylko do tych portów, które są członkami grupy.
Report Suppression State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Reportu Suppression“ przy aktywnym „IGMP Snooping“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Reportu Suppression“ przy aktywnym „IGMP Snooping“.
IGMP Snooping VLAN State	**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, w których switch ma wykonywać „IGMP Snooping“. Właściwy zakres VLAN ID: 1 … 4094 Przy podawaniu zakresu dla poszczególnych sieci VLAN należy użyć przecinka (,) lub łącznika (-).
	Delete	W polu wyboru należy wybrać „Delete“ i wpisać sieci VLAN, w których switch ma wykonywać „IGMP Snooping“.
Unknown Multicast Packets		W tym polu wyboru można wybrać reakcję swicha przy odbiorze nieznanych ramek multicast.
	Drop	Należy wybrać „Drop“, gdy ramki te mają być odrzucone.
	Flooding	Należy wybrać „Flooding“, gdy ramki te mają być przesłane do wszystkich portów.
IGMP Snooping State		
Parametr	**Domyślnie**	**Opis**
IGMP Snooping State	Disable Enable	W tym polu wyświetlana jest informacja, czy funkcja „IGMP Snooping“ jest globalne aktywowana, czy dezaktywowana.
Report Suppression State	Disable Enable	W tym polu wyświetlana jest informacja, czy funkcja „Report Suppression“ przy „IGMP-Snooping” jest aktywowana, czy dezaktywowana.
IGMP Snooping VLAN State	None 1 … 4094	W tym polu wyświetlane są VLAN, w których switch wykonuje „IGMP Snooping“. Wartość „None“ wyświetlana jest, gdy dla żadnego portu IGMP Snooping“.
Unknown Multicast Packets	Drop Flooding	W tym polu wyświetlana jest informacja, czy switch odrzuca nieznane pakiety multicast, czy przesyła je do wszystkich portów.

10.4.2.1.2 Port Settings



Ilustracja 61: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“

Tabela 77: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“

Port Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Settings“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Settings“.
Querier Mode		**Auto**	W polu wyboru należy wybrać ustawienie „Auto“, gdy switch ma wykorzystać ten port jako „IGMP Query Port“, gdy „IGMP Query“ odbierze pakiety.
		Fix	W polu wyboru należy wybrać ustawienie „Fix“, gdy switch zawsze wykorzystuje port lub porty jako „IGMP Query Ports”. To ustawienie wykorzystywane jest, gdy serwer IGMP multicast połączony jest z portem/portami.
		Edge	W polu wyboru należy wybrać ustawienie „Edge“, gdy switch nie ma wykorzystać tego portu jako „IGMP Query Port“. W tym przypadku switch nie protokołuje, że ruter IGMP jest połączony z portem i nie przekazuje też do tego portu pakietów „IGMP Join/Leave“.
Immediate Leave		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję. „Immediate Leave” na poszczególnych portach.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję. „Immediate Leave” na poszczególnych portach.
Port Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Querier Mode		Auto Fix Edge	W tej kolumnie wyświetlany jest tryb „Querier“ dla specyficznego portu.
Immediate Leave		Disable Enable	W tej kolumnie wyświetlane jest ustawienie „Immediate Leave“ dla specyficznego portu.

10.4.2.1.3 Querier Settings



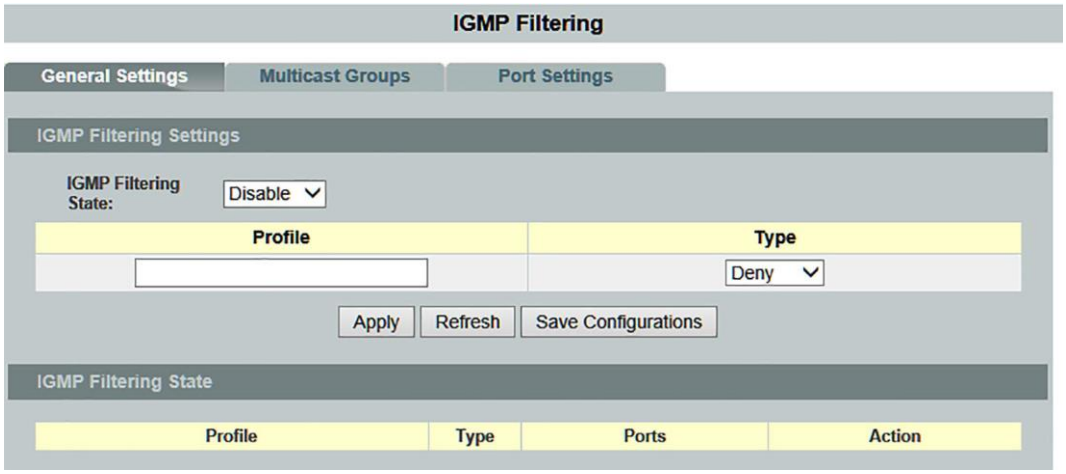
Ilustracja 62: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings“

Tabela 78: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings

Querier Settings		
Parametr	**Domyślnie**	**Opis**
Querier Status	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
Querier VLAN State	**Add**	W polu wyboru należy wybrać „Add“, aby wpisać VLAN ID.
	Delete	W polu wyboru należy wybrać „Delete“, aby usunąć VLAN ID.
Querier Status		
Parametr	**Domyślnie**	**Opis**
Querier Status	Disable Enable	W tym polu wyświetlany jest status „Querier“.
Querier VLAN State	None 0 … 4094	W tym polu wyświetlany jest VLAN ID.

10.4.2.2 IGMP Filtering

10.4.2.2.1 General Settings

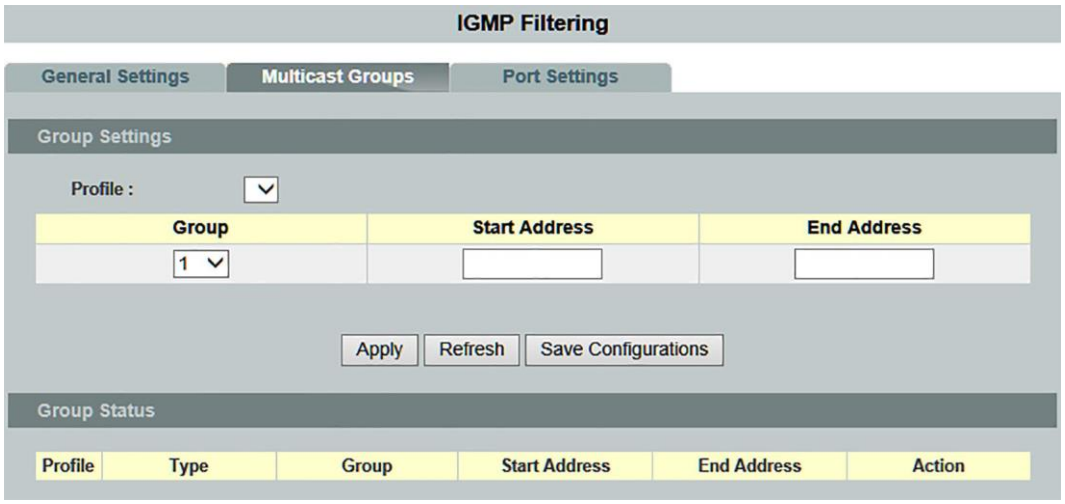


Ilustracja 63: Strona WBM „IGMP Filtering“ – zakładka „General Settings“

Tabela 79: Strona WBM „IGMP Filtering“ – zakładka „General Settings“

IGMP Filtering Settings		
Parametr	**Domyślnie**	**Opis**
IGMP Filtering State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
Profile		W polu edycji należy wpisać filtr IGMP.
Type	**Deny**	W polu wyboru należy wybrać „Deny“, aby nie zezwolić na dostęp do grupy.
	Permit	W polu wyboru należy wybrać „Permit“, aby zezwolić na dostęp do grupy.
IGMP Filtering State		
Parametr	**Domyślnie**	**Opis**
Profile		W tej kolumnie wyświetlana jest nazwa profilu. Aby modyfikować profil, należy kliknąć na tę nazwę.
Type	Deny Permit	W tej kolumnie wyświetlany jest wariant działania.
Ports	1 … 10 (12)	W tej kolumnie wyświetlane są porty, dla których aktywowany jest profil filtra IGMP.
Action	Delete	Aby usunąć adresy multicast, należy kliknąć **[Delete]**.

10.4.2.2.2 Multicast Groups

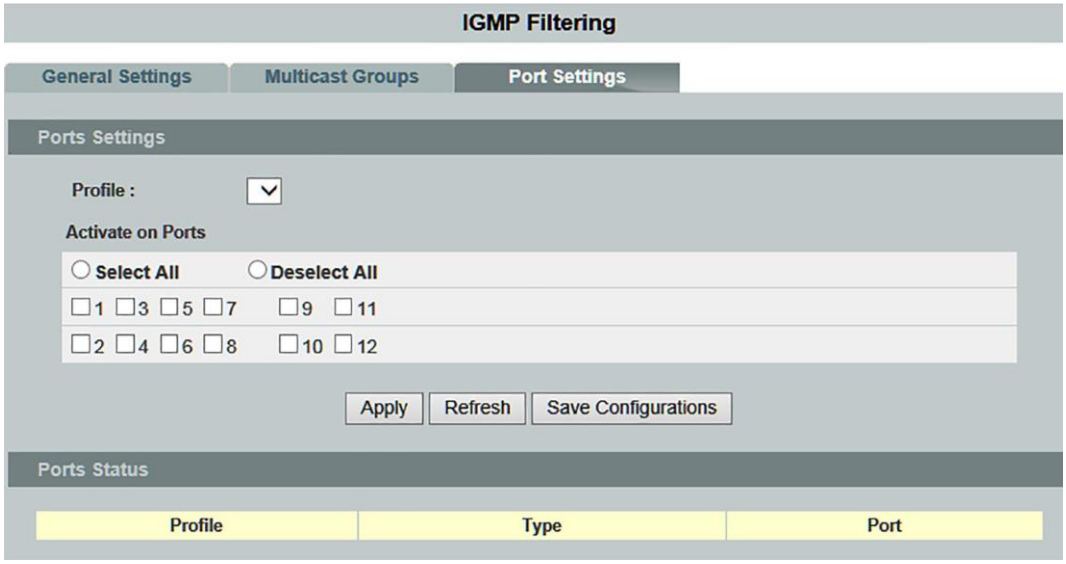


Ilustracja 64: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“

Tabela 80: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“

Group Status		
Parametr	**Domyślnie**	**Opis**
Profile		W polu wyboru należy wybrać profil, który ma być skonfigurowany dla grupy.
Group	**1** … 10	W polu wyboru należy wybrać grupę multicast.
Start Address		W polu edycji należy wpisać pierwszy adres multicast konfigurowanej grupy.
End Address		W polu edycji należy wpisać ostatni adres multicast konfigurowanej grupy.
Group Status		
Parametr	**Domyślnie**	**Opis**
Profile		W tej kolumnie wyświetlana jest nazwa profilu.
Type	Deny Permit	W tej kolumnie wyświetlany jest wariant działania.
Group	1 … 10	W tej kolumnie wyświetlana jest grupa.
Start Address		W tej kolumnie wyświetlany jest pierwszy adres multicast.
End Address		W tej kolumnie wyświetlany jest ostatni adres multicast.
Action	Delete	Aby usunąć adresy multicast, należy kliknąć **[Delete]**.

10.4.2.2.3 Port Settings



Ilustracja 65: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“

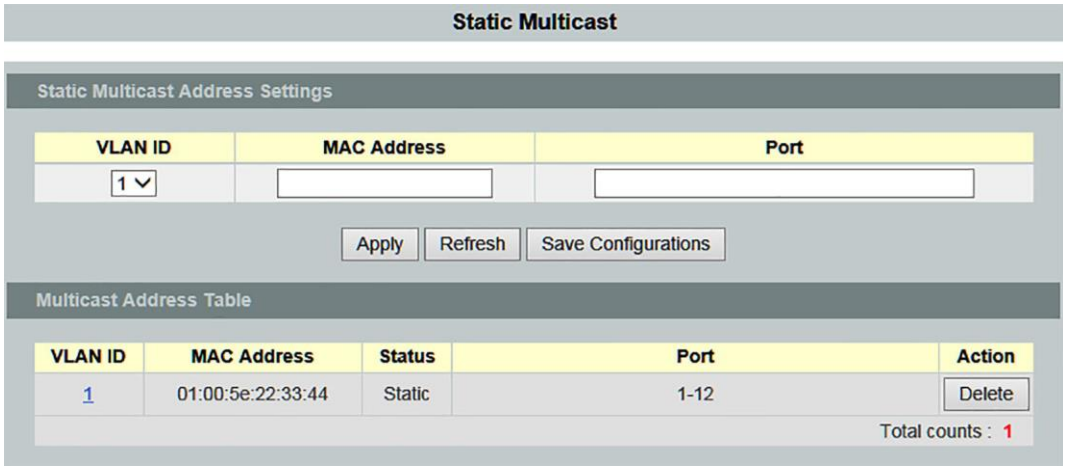
Tabela 81: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“

Port Settings				
Parametr		**Domyślnie**	**Opis**	
Profile			W polu wyboru należy wybrać profil, który ma być skonfigurowany dla grupy.	
Port	Select All	○	○	Żaden port nie jest wybrany.
			◉	Wybrane są wszystkie porty.
	Disable All	○	○	Żaden port nie jest dezaktywowany.
			◉	Wszystkie porty są dezaktywowane.
	☐ 1 … ☐ 10 (12)	☐	☐	Port nie jest aktywowany.
			☑	Port jest aktywowany.
Port Status				
Parametr		**Domyślnie**	**Opis**	
Profile			W tej kolumnie wyświetlana jest nazwa profilu.	
Type		Deny Permit	W tej kolumnie wyświetlany jest wariant działania.	
Ports		1 … 10 (12)	W tej kolumnie wyświetlane są porty, dla których aktywowany jest profil filtra IGMP.	

10.4.2.3 Static Multicast

Wskazówka

Dodatkowa informacja
Więcej informacji o „Static Multicast” można znaleźć w rozdziale „Opis funkcji”.

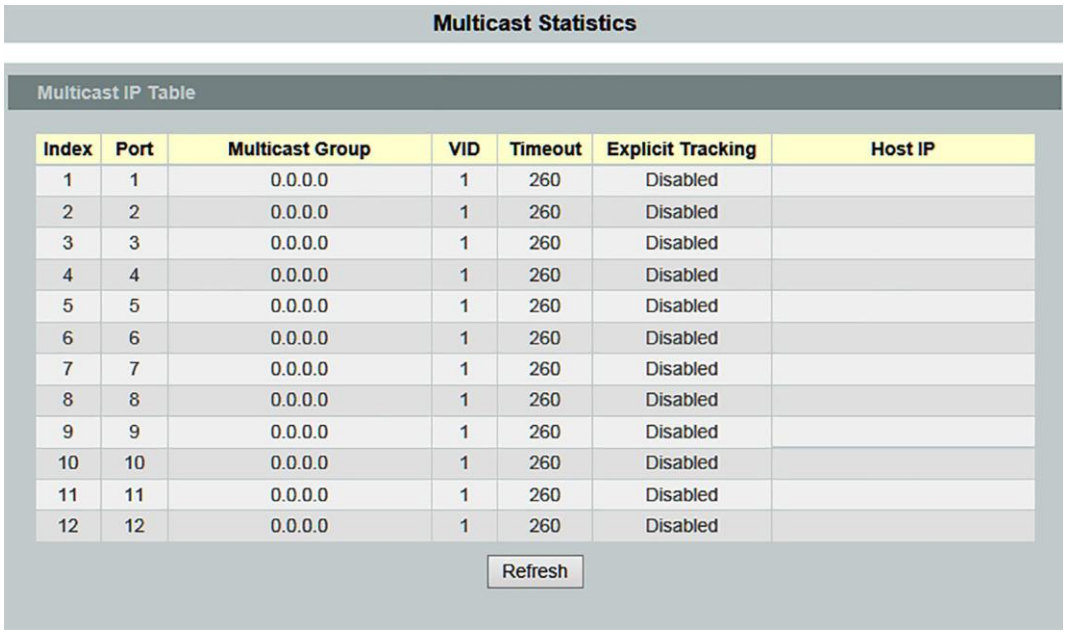


Ilustracja 66: Strona WBM „Static Multicast“

Tabela 82: Strona WBM „Static Multicast“

Static Multicast Address Settings		
Parametr	**Domyślnie**	**Opis**
VLAN ID	**1**	W polu wyboru należy wybrać VLAN ID, która ma być skonfigurowana.
MAC Address		W polu edycji należy wpisać adres MAC multicast dla danego pierścienia. Należy skonfigurować adres MAC multicast, który nie otrzyma „Age Time“. Właściwy format to: 0x:0x:0x:0x:0x:0x.
Port		W polu edycji należy wpisać port dla adresu MAC multicast.
Multicast Address Table		
Parametr	**Domyślnie**	**Opis**
VLAN ID	0 … 4094	W tej kolumnie wyświetlane są wybrane VLAN ID.
MAC Address		W tej kolumnie wyświetlane są adresy multicast.
Status		W tej kolumnie wyświetlany jest status adresów multicast.
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Action		Aby usunąć adresy multicast, należy kliknąć **[Delete]**.
Total counts		W tym polu wyświetlana jest zbiorcza liczba wpisów w tabeli adresów multicast.

10.4.2.4 Multicast Statistics



Ilustracja 67: Strona WBM „Multicast Statistics“

Tabela 83: Strona WBM „Multicast Statistics“

Multicast IP Table		
Parametr	**Domyślnie**	**Opis**
Index	1 … 10 (12)	W tej kolumnie wyświetlana jest liczba wpisów.
Port	1 … 10 (12)	W tej kolumnie wyświetlany jest numer portu.
Multicast Group		W tej kolumnie wyświetlany jest adres IP grupy multicast.
VLAN ID		W tej kolumnie wyświetlany jest VLAN ID.
Timeout		W tej kolumnie wyświetlany jest czas „Timeout“.
Explicit Tracking		W tej kolumnie wyświetlana jest informacja, czy ustawiony jest „Explicit Tracking“.
Host IP		W tej kolumnie wyświetlane jest IP hosta.

10.4.3 VLAN

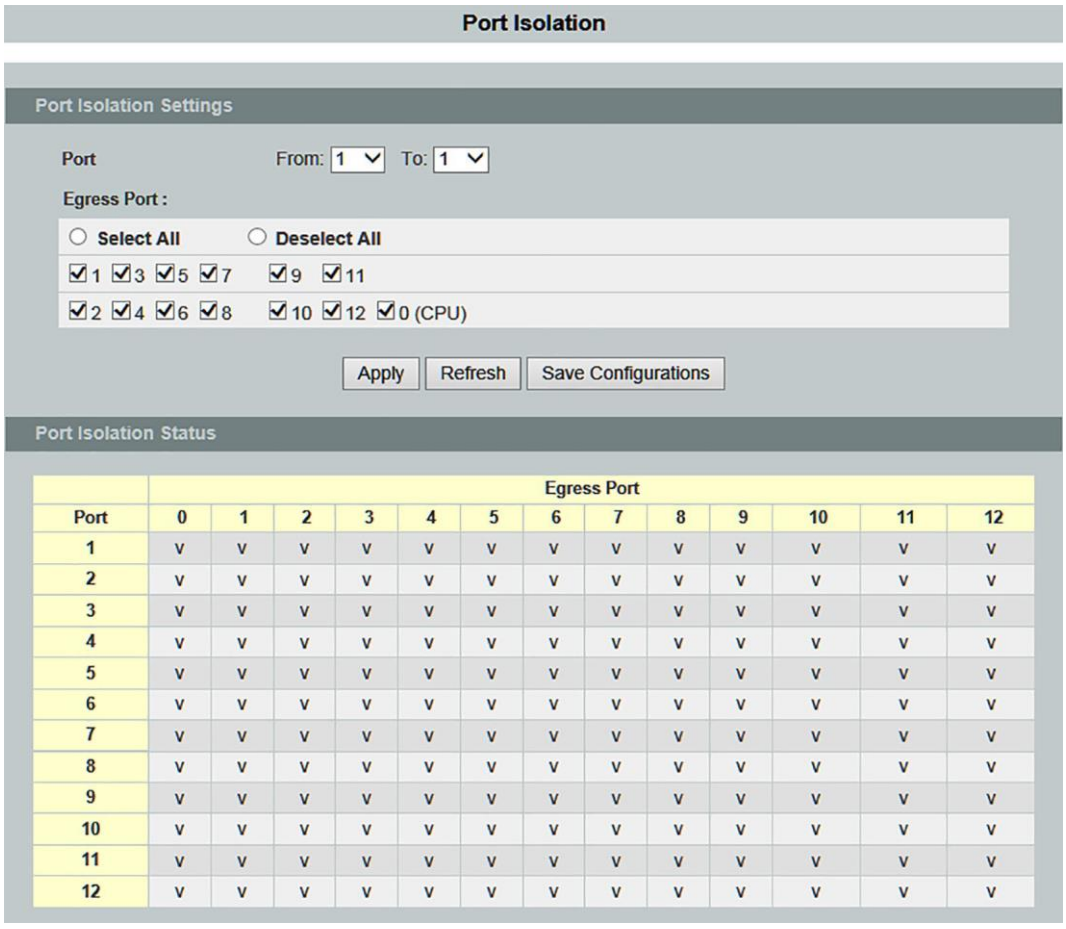
Wskazówka

Dodatkowa informacja
Więcej informacji o „VLAN“ (**V**irtual **L**ocal **A**rea **N**etwork) można znaleźć w rozdziale „Opis funkcji“.

10.4.3.1 Port Isolation

Wskazówka

Dodatkowa informacja
Więcej informacji o „Port Isolation” można znaleźć w rozdziale „Opis funkcji”.



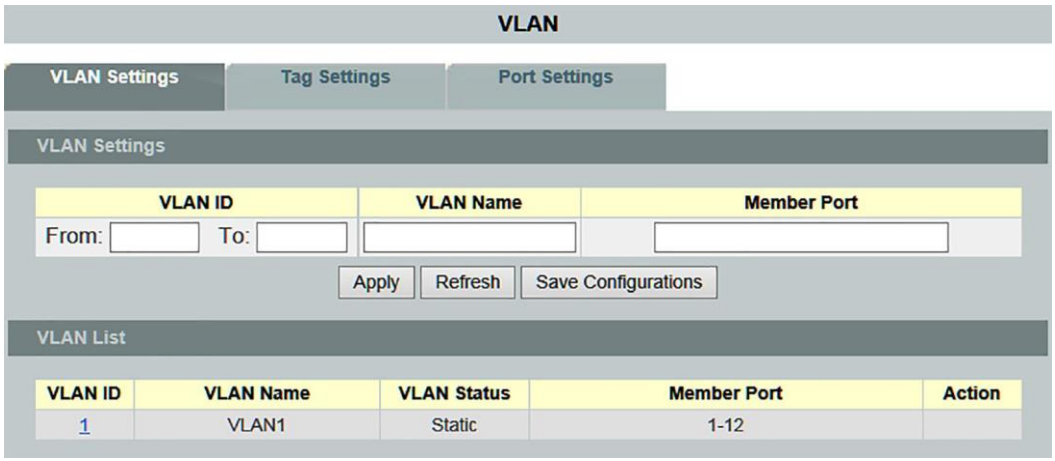
Ilustracja 68: Strona WBM „Port Isolation“

Tabela 84: Strona WBM „Port Isolation“

Port Isolation Settings				
Parametr		**Domyślnie**	**Opis**	
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Port Isolation”.	
	To:	**1**	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 port wyjściowy nie jest wybrany.
			◉	Wybrane są wszystkie porty wyjściowe.
	Disable All	○	○	Żaden port wyjściowy nie jest dezaktywowany.
			◉	Wszystkie porty wyjściowe są wdezaktywowane.
	☐ 0 (CPU) … ☐ 10 (12)	☐	☐	Port wyjściowy nie jest aktywowany.
			☑	Port wyjściowy 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.

10.4.3.2 VLAN

10.4.3.2.1 VLAN Settings

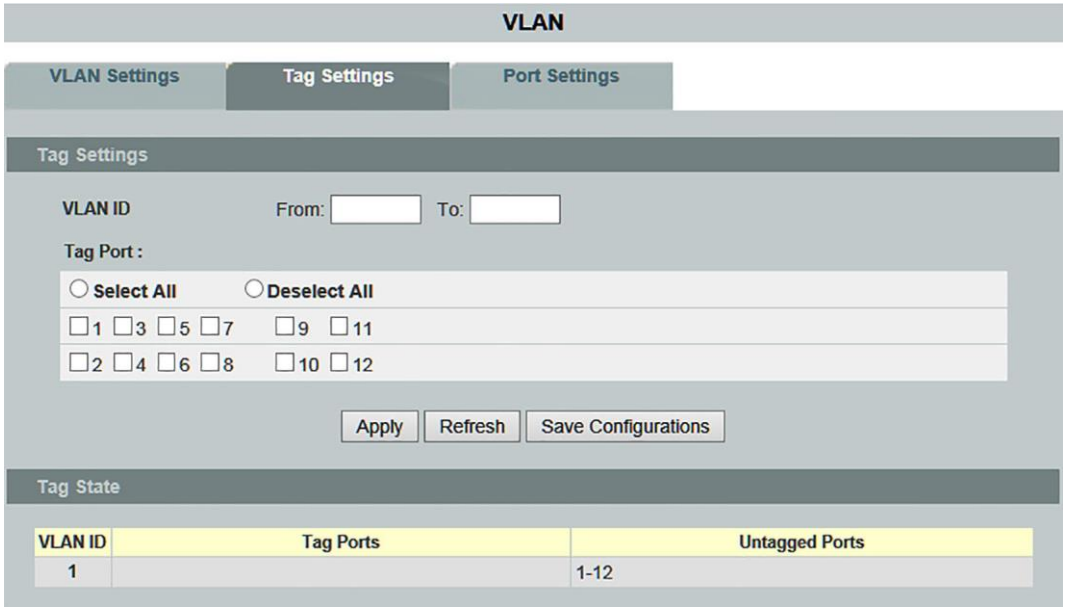


Ilustracja 69: Strona WBM „VLAN“ – zakładka „VLAN Settings“

Tabela 85: Strona WBM „VLAN“ – zakładka „VLAN Settings“

VLAN Settings			
Parametr		**Domyślnie**	**Opis**
VLAN ID	From:		W polu edycji należy wpisać „VLAN ID“ dla tego wpisu. Właściwy zakres: 1 … 4094
	To:		W polu edycji należy wpisać „VLAN ID“ dla tego wpisu. Właściwy zakres: 1 … 4094
VLAN Name			W polu edycji, w celu jednoznacznej identyfikacji, należy wpisać wybraną nazwę VLAN. Nazwa hosta powinna składać się z kombinacji cyfr, liter, łączników (-) lub podkreśleń (_).
Member Port			W polu edycji należy wpisać numer portu, który switch ma przyporządkować do VLAN jako uczestnika. Można podać kilka numerów portów lub zakresów portów, rozdzielając poszczególne porty przecinkiem (,) lub stosując przy zakresach portów łącznika (-).
VLAN List			
Parametr		**Domyślnie**	**Opis**
VLAN ID		1 … 4094	W tej kolumnie wyświetlany jest numer indeksu wpisu VLAN. Należy kliknąć ten numer, aby zmodyfikować wpis VLAN.
VLAN Name			W tej kolumnie wyświetlana jest nazwa VLAN.
VLAN Status		Static Dynamic 802.1Q-VLAN	W tej kolumnie wyświetlany jest status VLAN.
Member Port		1-10 (12)	W tej kolumnie wyświetlana jest informacja, które porty przyporządkowane są do VLAN jako uczestnicy.
Action			Aby usunąć VLAN, należy kliknąć **[Delete]**.
		Wskazówka 	**Usuwanie VLAN1** Usunięcie VLAN1 nie jest możliwe.

10.4.3.2.2 Tag Settings

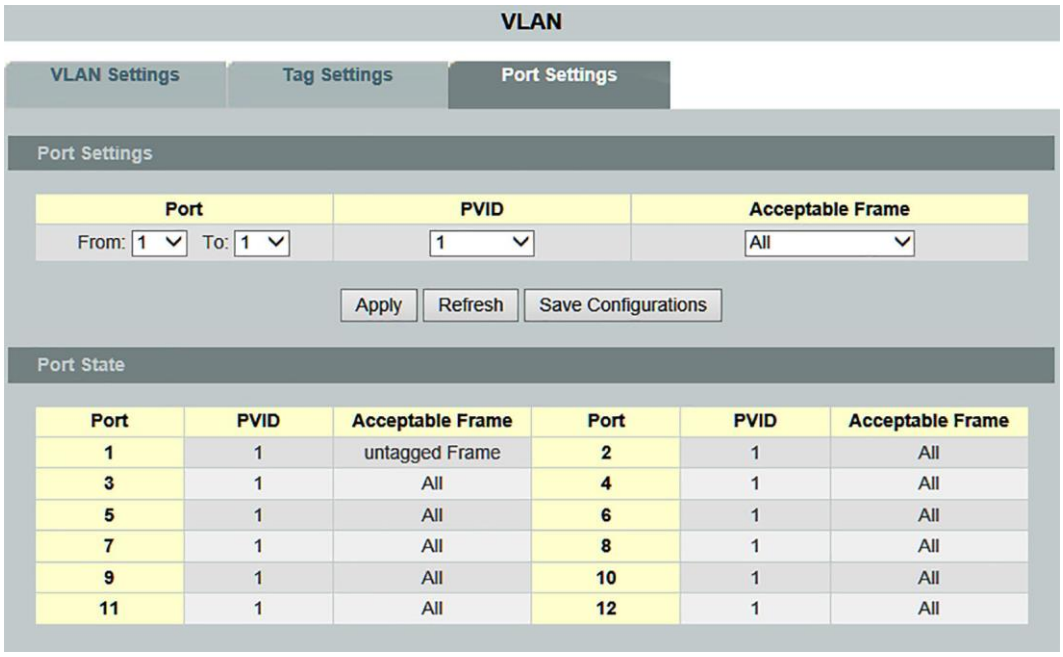


Ilustracja 70: Strona WBM „VLAN“ – zakładka „Tag Settings“

Tabela 86: Strona WBM „VLAN“ – zakładka „Tag Settings“

Tag Settings				
Parametr		**Domyślnie**	**Opis**	
VLAN ID	From:		W polu edycji należy wpisać „VLAN ID“ dla tego wpisu. Właściwy zakres: 1 … 4094	
	To:		W polu edycji należy wpisać „VLAN ID“ dla tego wpisu. Właściwy zakres: 1 … 4094	
Tag Port	Select All	○	○	Żaden port nie jest wybrany jako port ze znacznikiem.
			◉	Wszystkie porty są wybrane jako port ze znacznikiem.
	Disable All	○	○	Żaden port ze znacznikiem nie jest aktywowany.
			◉	Wszystkie porty ze znacznikiem są dezaktywowane.
	☐ 1 … ☐ 10 (12)	☐	☐	Port nie jest aktywowany.
			☑	Port jest aktywowany.
Tag State				
Parametr		**Domyślnie**	**Opis**	
VLAN ID		1 … 4094	W tej kolumnie wyświetlany jest VLAN ID.	
Tag Ports		1 … 7	W tej kolumnie wyświetlane są porty, które przyporządkowane są jako porty ze znacznikiem.	
Untagged Ports		1 … 7	W tej kolumnie wyświetlane są porty, które przyporządkowane są jako porty bez znacznika.	

10.4.3.2.3 Port Settings



Ilustracja 71: Strona WBM „VLAN“ – zakładka „Port Settings“

Tabela 87: Strona WBM „VLAN“ – zakładka „Port Settings“

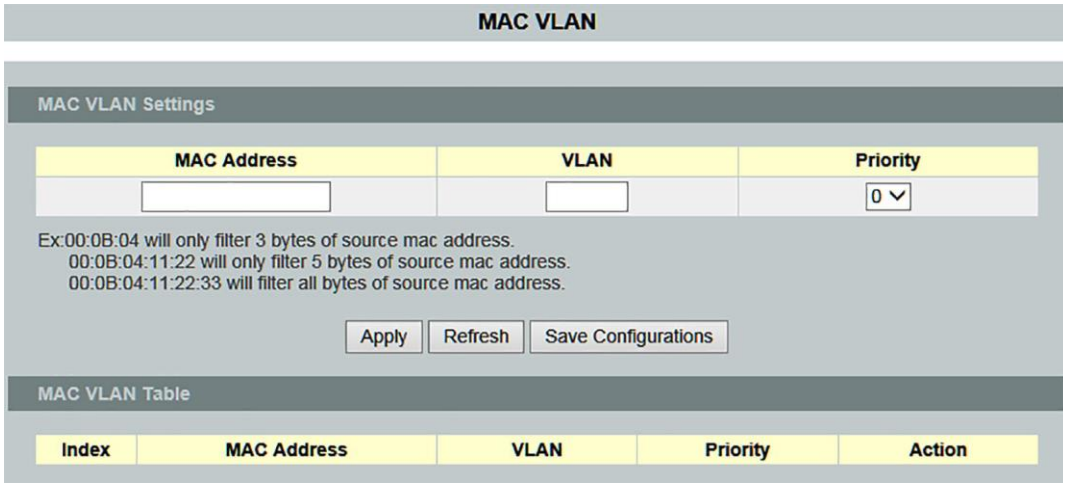
Port Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Settings“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Settings“.
PVID		**1**	W polu wyboru należy wybrać numer PVID (Port VLAN ID).
Acceptable Frame			W tym polu wyboru można wybrać rodzaje ramek dopuszczalne do portu.
		All	Należy wybrać „All“, gdy na tym porcie mają być akceptowane wszystkie ramki (ze znacznikiem i bez).
		Only untagged VLANs	Należy wybrać „Only untagged VLANs, gdy na tym porcie mają być akceptowane tylko ramki bez znacznika. Wszystkie ramki ze znacznikiem zostają odrzucone.
		only tagged VLANs	Należy wybrać „tagged Frame“, gdy na tym porcie mają być akceptowane tylko ramki ze znacznikiem. Wszystkie ramki bez znacznika zostają odrzucone.
Port Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
PVID			W tej kolumnie wyświetlane są numery VLAN ID.
Acceptable Frame		All only untagged VLANs only tagged VLANs	W tej kolumnie wyświetlane są rodzaje ramek dopuszczalnych dla tego portu.

10.4.3.3 MAC VLAN

Wskazówka

Dodatkowa informacja

Więcej informacji o „MAC-VLAN” (**M**edia **A**ccess **C**ontrol-**V**irtual **L**ocal **A**rea **N**etwork) można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 72: Strona WBM „MAC VLAN“

Tabela 88: Strona WBM „MAC VLAN“

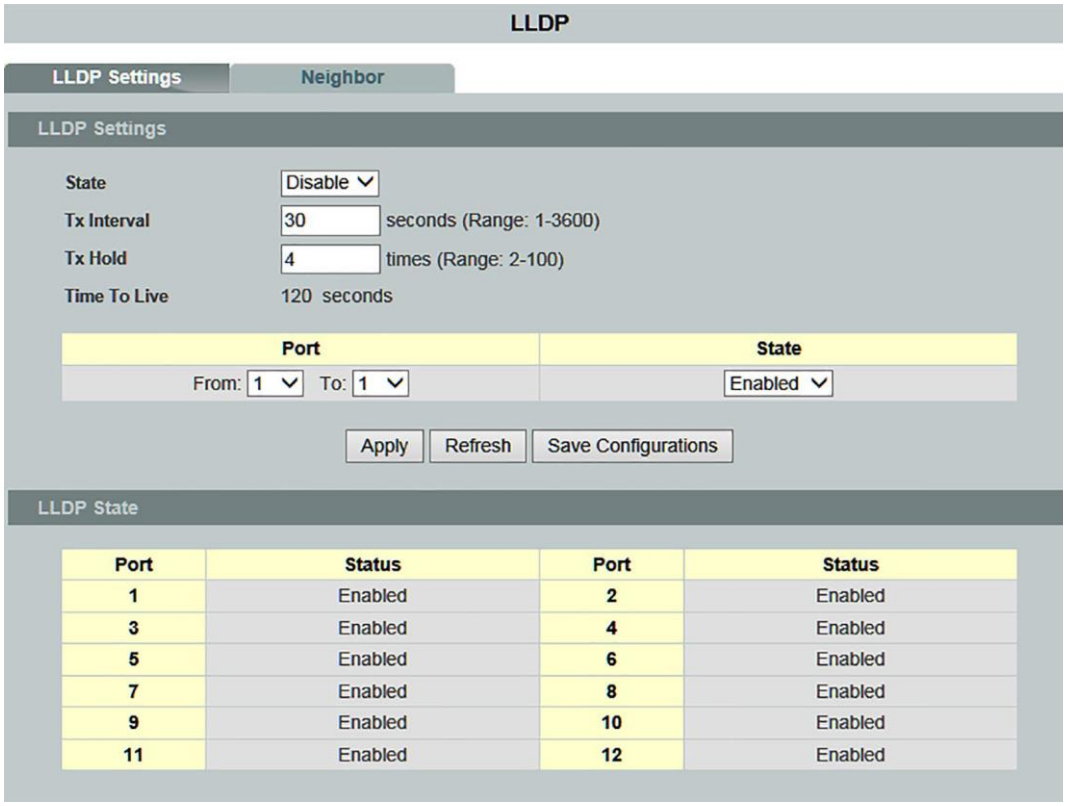
MAC VLAN Settings		
Parametr	**Domyślnie**	**Opis**
MAC Address		W polu edycji należy wpisać pierwsze trzy lub więcej bajtów adresu MAC.
VLAN		W polu edycji należy wpisać wartość dla MAC VLAN dla instancji. Właściwy zakres: 1 … 4094 Można skonfigurować jedną lub więcej „Data VLAN“.
Priority	**0** … 7	W polu wyboru należy wybrać priorytet dla specyficznego portu. 0 = najniższy priorytet 7 = najwyższy priorytet
MAC VLAN Table		
Parametr	**Domyślnie**	**Opis**
Index	1 … 10	W tej kolumnie wyświetlana jest liczba wpisów.
MAC Address		W tej kolumnie wyświetlany jest adres MAC.
VLAN		W tej kolumnie wyświetlany jest VLAN ID dla specyficznego portu.
Priority	0 … 7	W tej kolumnie wyświetlany jest priorytet dla specyficznego portu.
Action		Aby usunąć adresy multicast, należy kliknąć **[Delete]**.

10.4.4 LLDP

Wskazówka

Dodatkowa informacja
Więcej informacji o „LLDP“ (**L**ink **L**ayer **D**iscovery **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.

10.4.4.1 Settings

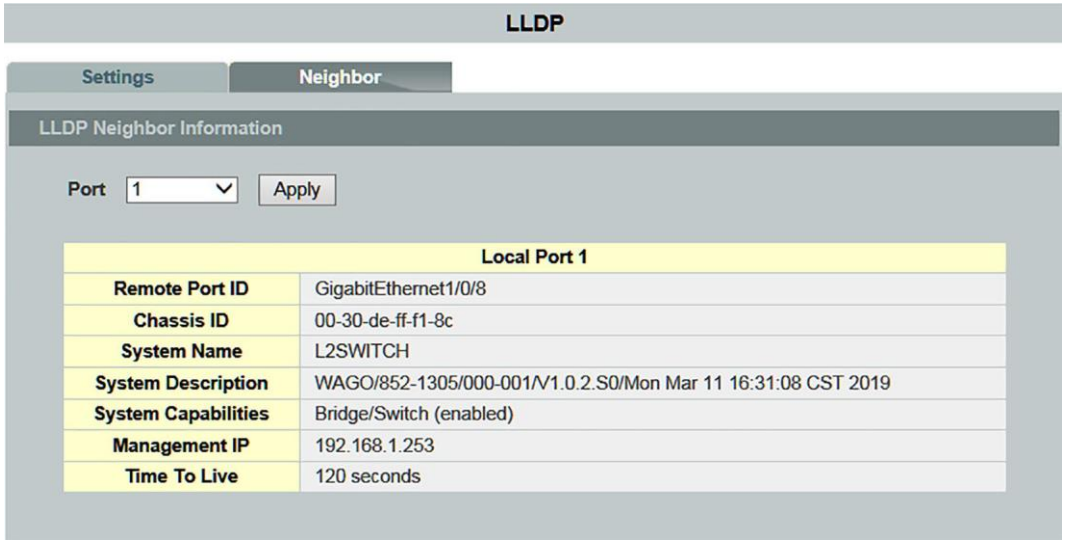


Ilustracja 73: Strona WBM „LLDP“ – zakładka „LLDP Settings“

Tabela 89: Strona WBM „LLDP“ – zakładka „LLDP Settings“

LLDP Settings			
Parametr		**Domyślnie**	**Opis**
Status		**Disable**	W polu wyboru należy wybrać „Disable“, aby globalnie dezaktywować dla switcha funkcję LLDP.
		Enable	W polu wyboru należy wybrać „Enable“, aby globalnie aktywować funkcję „LLDP” dla switcha.
TX Interval		**30**	W polu edycji należy wpisać wartość „Tx Interval“ dla pakietów „LLDP“.
TX Hold		**4**	W polu edycji należy wpisać wartość „Tx Hold-Time“, która określa TTL wiadomości switcha. (TTL = tx-hold * tx-interval)
Time To Live		**120**	W tym polu wyświetlana jest żywotność informacji switcha.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „LLDP”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „LLDP”.
Status		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „LLDP” na poszczególnych portach.
		Rx Only	W polu wyboru należy wybrać ustawienie „Rx Only“, jeśli dla switcha lub portów zawsze używany jest „Rx Interval“ jako interwał transmisji.
		Tx Only	W polu wyboru należy wybrać ustawienie „Tx Only“, jeśli dla switcha lub portów zawsze używany jest „Tx Interval“ jako interwał transmisji.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować „LLDP” na poszczególnych portach.
LLDP State			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Status		Disable Enable	W tej kolumnie wyświetlana jest informacja, czy funkcja „LLDP“ jest aktywowana, czy dezaktywowana.

10.4.4.2 Neighboring Detection



Ilustracja 74: Strona WBM „LLDP“ – zakładka „Neighboring Detection“

Tabela 90: Strona WBM „LLDP“ – zakładka „Neighboring Detection“

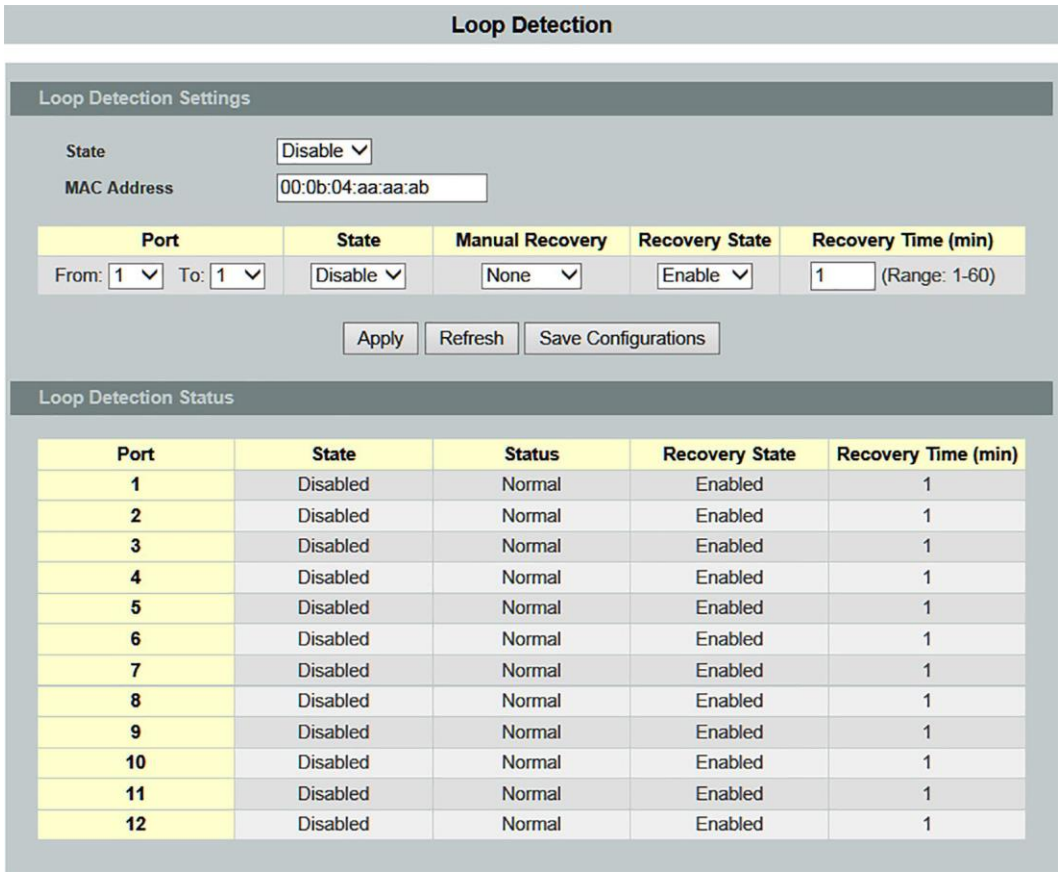
LLDP Neighbor Information		
Parametr	**Domyślnie**	**Opis**
Port	**All**	W polu wyboru należy wybrać „All“, gdy mają być wyświetlane informacje od wszystkich sąsiednich portów.
	1 … 10 (12)	W polu wyboru należy wybrać port, którego sąsiadującego portu mają być wyświetlane informacje.
Local Port	1 … 10 (12)	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.
Time To Live		W tym polu wyświetlany jest czas ważności informacji sąsiedniego portu.

10.4.5 Loop Detection

Wskazówka

Dodatkowa informacja

Więcej informacji o „Loop Detection” można znaleźć w rozdziale „Opis funkcji”.

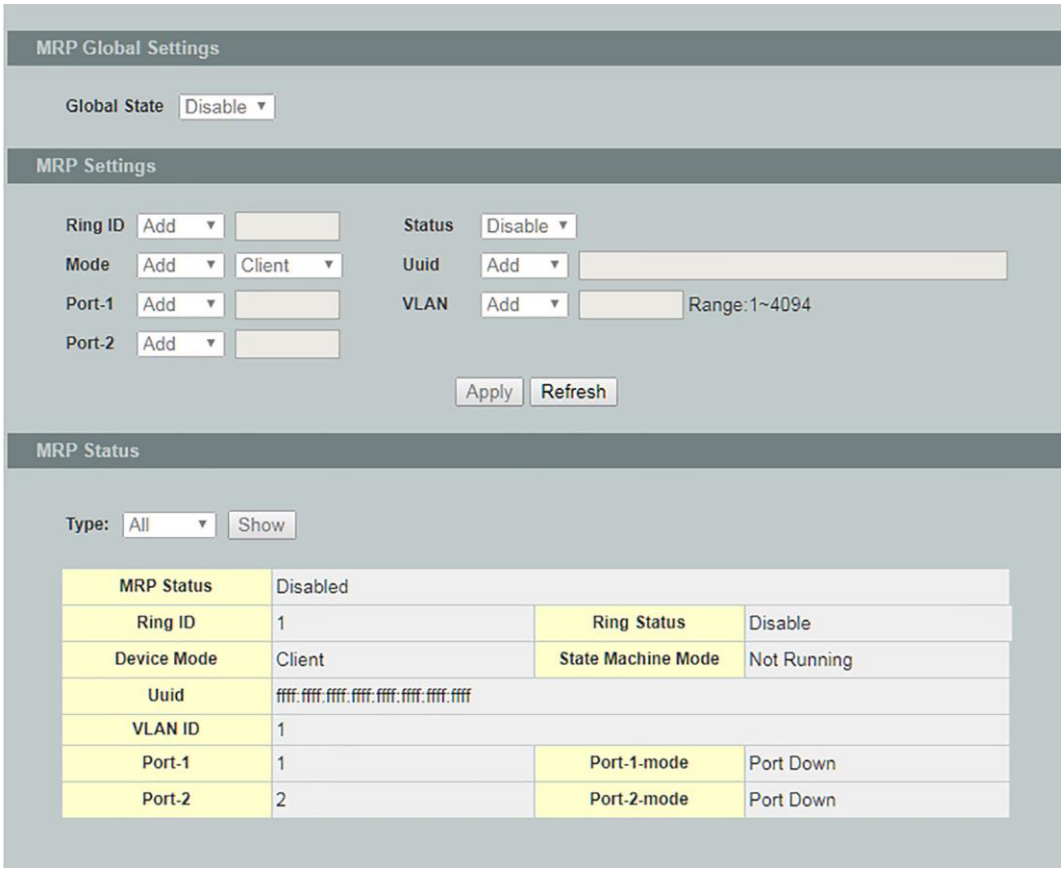


Ilustracja 75: Strona WBM „Loop Detection”

Tabela 91: Strona WBM „Loop Detection”

Loop Detection Settings			
Parametr		**Domyślnie**	**Opis**
Status		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
MAC Address			W polu edycji należy wybrać docelowy adres MAC, na który mają być wysyłane pakiety sondujące. Gdy port otrzyma te same pakiety, zostaje wyłączony.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „Loop Guard Protection“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „Loop Guard Protection“.
Status		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować dla switcha funkcję „Loop Guard“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować dla switcha funkcję „Loop Guard“.
Action		**None**	W polu wyboru należy wybrać „None“, aby wyłączyć dla portu funkcję „Loop Detection“.
		Activate	W polu wyboru należy wybrać „Activate“, jeśli nie mają być zmienione funkcje „Status“ i „Loop Correction“.
Loop Recovery		**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
Loop Detection Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
State		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy funkcja „Loop Guard“ jest aktywowana, czy dezaktywowana.
Status		None Normal	W tej kolumnie wyświetlana jest informacja, czy port jest zablokowany.
Loop Recovery		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy funkcja „Loop Recovery“ jest aktywowana, czy dezaktywowana.
Recovery Time (min)		1 … 50	W tej kolumnie wyświetlany jest „Loop Recovery“ dla funkcji „Recovery Status“.

10.4.6 MRP



Ilustracja 76: Strona WBM „MRP Global Settings“

Tabela 92: Strona WBM „MRP”

MRP Global Settings		
Parametr	**Domyślnie**	**Opis**
Global State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję globalnego MRP.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję. globalnego MRP.
MRP Settings		
Parametr	**Domyślnie**	**Opis**
Ring ID	**Add**	W polu wyboru należy wybrać „Add“, aby wpisać ID nowego pierścienia.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć ID pierścienia.
Mode	**Add**	W polu wyboru należy wybrać „Add”, aby skonfigurować switch jako klienta (MRC) lub menedżera (MRM).
	Remove	W polu wyboru należy wybrać „Remove”, aby usunąć switch jako klienta (MRC) lub menedżera (MRM).
Port 1	**Add**	W polu wyboru należy wybrać „Add“, aby dodać podstawowe złącze dla pierścienia MRP.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć podstawowe złącze dla pierścienia MRP.
Port 2	**Add**	W polu wyboru należy wybrać „Add“, aby dodać rezerwowe złącze dla pierścienia MRP.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć rezerwowe złącze dla pierścienia MRP.
Status	**Disable**	W polu wyboru należy wybrać „Disable“, aby włączyć dany pierścień.
	Enable	W polu wyboru należy wybrać „Disable“, aby włączyć dany pierścień.
UUID	**Add**	Konfiguruje "Universal Unique Identifier" (UUID) dla pierścienia MRP. Jest to ciąg znaków w formacie szesnastkowym, przestawiający pierścień, do którego należy ten switch. **Przykład:** 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Remove	
VLAN	**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, dla których ten pierścień ma być aktywowany. Właściwy zakres VLAN ID: 1 … 4094 Przy podawaniu zakresu dla poszczególnych sieci VLAN należy użyć przecinka (,) lub łącznika (-).
	Remove	W polu wyboru należy wybrać „Remove“ i podać sieci VLAN, dla których ten switch nie ma być aktywowany.

Tabela 92: Strona WBM „MRP”

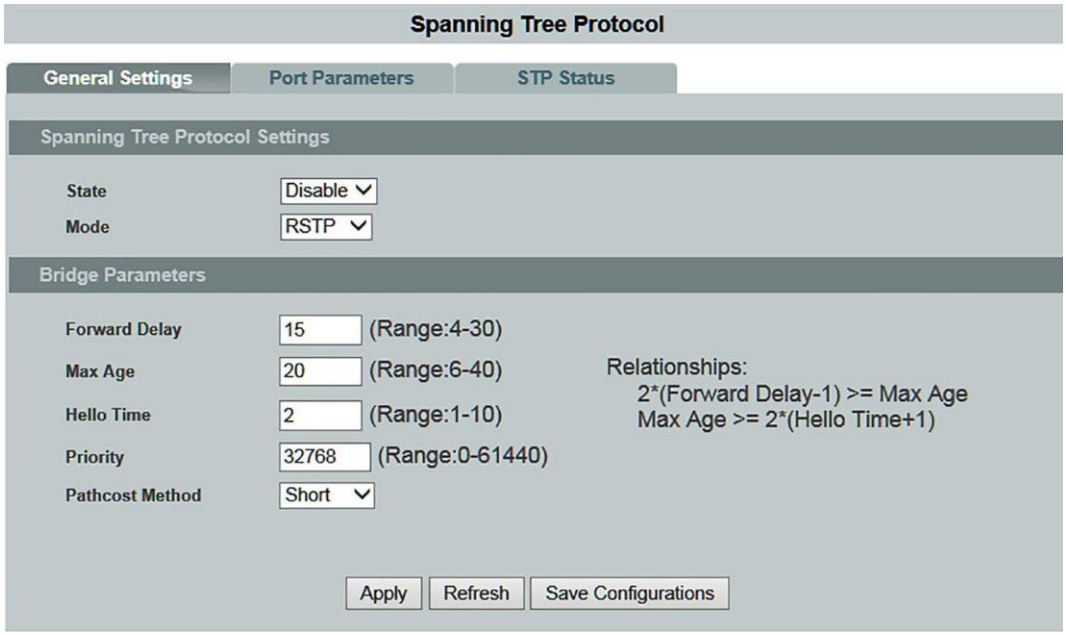
MRP Status (aktualny stan danego pierścienia MRP)		
Parametr	**Domyślnie**	**Opis**
Type	**All**	W polu wyboru należy wybrać „All“, gdy mają być wyświetlone wszystkie statusy MRP.
	Ring_1 … Ring_4	W polu wyboru należy wybrać ID pierścienia, dla którego ma być wyświetlany status MRP.
MRP Status	–	W tym polu wyświetlany jest aktualny stan danego pierścienia MRP.
Ring ID	–	W tym polu wyświetlany jest ID pierścienia MRP.
Device Mode	–	W tym polu wyświetlany jest tryb switcha: Client (CRM)/Manager (MRM)
Uuid	–	W tym polu wyświetlany jest przydzielony UUID.
VLAN ID	–	W tym polu wyświetlana jest informacja, do której sieci VLAN należy pierścień.
Port-1	–	W tym polu wyświetlany jest przyporządokowany port switcha.
Port-2	–	W tym polu wyświetlany jest przyporządokowany port switcha.
Ring Status	–	W tym polu wyświetlany jest aktualny status pierścienia MRP.
State Machine Mode	–	W tym polu wyświetlana jest informacja, czy maszyna stanów MRP jest uruchomiona, czy nie.
Port-1 Mode	–	W tym polu wyświetlany jest status portu: (port down/port up).
Port-2 Mode	–	W tym polu wyświetlany jest status portu: (port down/port up).

10.4.7 Spanning Tree Protocol

Wskazówka

Dodatkowa informacja
Więcej informacji o „**S**panning **T**ree **P**rotocol“ (STP) można znaleźć w rozdziale „Opis funkcji“.

10.4.7.1 General Settings

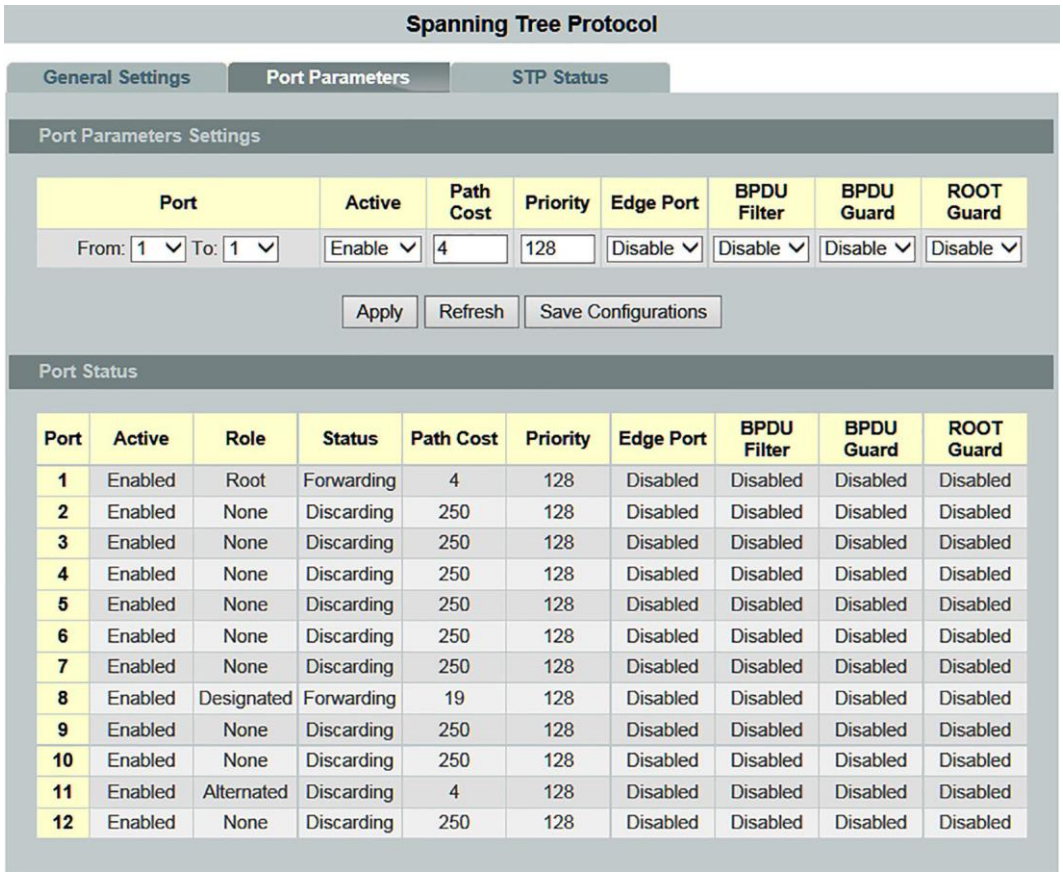


Ilustracja 77: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“

Tabela 93: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“

Spanning Tree Protocol Settings		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby zastosować „Spanning Tree Protocol“ (STP) lub „Rapid Spanning Tree Protocol” (RSTP).
Mode	**RSTP**	W polu wyboru należy wybrać „RSTP“, gdy ma być zastosowany szybki „Rapid Spanning Tree Protocol“.
	MSTP	W polu wyboru należy wybrać „MSTP“, gdy ma być zastosowany „Multiple Spanning Tree Protocol“.
	STP	W polu wyboru należy wybrać „STP“, gdy ma być zastosowany „Spanning Tree Protocol“.
Bridge Parameters		
Parametr	**Domyślnie**	**Opis**
Forward Delay	**15**	W polu edycji należy wpisać czas „Forward Delay“. Właściwy zakres: 4 … 30 s
Max Age	**20**	W polu edycji należy wpisać czas „Max Age“. Właściwy zakres: 6 … 40 s
Hello Time	**2**	W polu edycji należy wpisać czas „Hello Time“. Właściwy zakres: 1 … 10 s
Priority	**32768**	W polu edycji należy wpisać wartość priorytetu. Im niższa przypisana wartość numeryczna, tym wyższy priorytet bridge'a. Właściwy zakres: 0 … 61440
Path Cost Method	**Short**	W polu wyboru należy wybrać „Short“, gdy ma być wybrana wielkość 16 bitów i prędkość transmisji do 10 Gbit. 10 Mbit = 100 100 Mbit = 19 1 Gbit = 4 10 Gbit = 2
	Long	W polu wyboru należy wybrać „Long“, gdy ma być wybrana wielkość 32 bity i prędkość transmisji do 10 Tbit. 10 Mbit = 2000000 100 Mbit = 200000 1 Gbit = 20000 10 Gbit = 2000 100 Gbit = 200 1 Tbit = 20

10.4.7.2 Port Parameters



Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	Root	Forwarding	4	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
7	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
8	Enabled	Designated	Forwarding	19	128	Disabled	Disabled	Disabled	Disabled
9	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
10	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
11	Enabled	Alternated	Discarding	4	128	Disabled	Disabled	Disabled	Disabled
12	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Ilustracja 78: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“

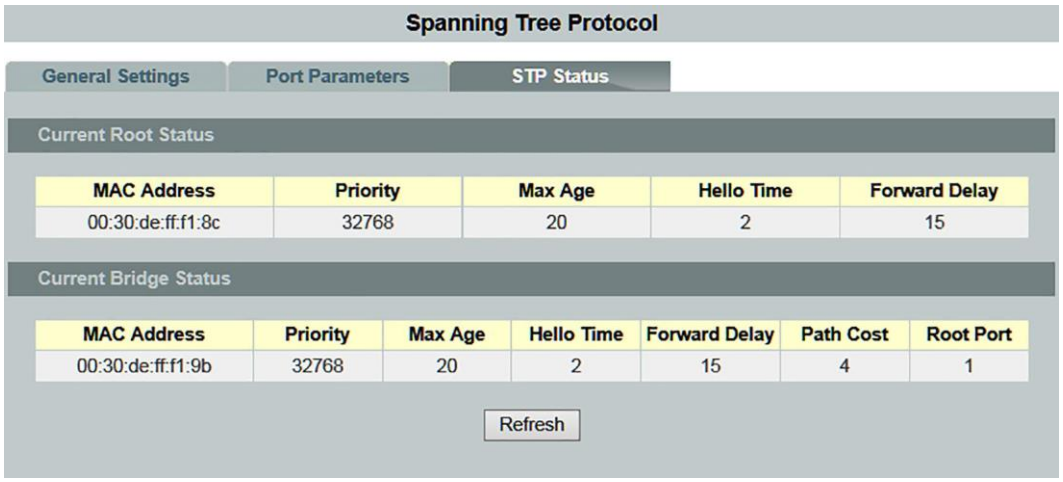
Tabela 94: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“

Port Parameter Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „STP Function“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „STP Function“.
Active		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „STP Funkction“ dla specyficznego portu.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować „STP Funkction“ dla specyficznego portu.
Path Costs		**250**	W polu edycji należy wpisać wartość „Path Cost“ dla specyficznego portu.
Priority		**128**	W polu edycji należy wpisać wartość priorytetu dla specyficznego portu.
Edge Port		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować typ portu „Edge Port“ dla specyficznego portu.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować typ portu „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 „BPDU Filter“ 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 „ROOT Guard“ dla specyficznego portu.

Tabela 94: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“

Port Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Active	**Enable** Disable	W tej kolumnie wyświetlany jest stan „STP Function“.
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.
Path Costs	0 … 65535	W tej kolumnie wyświetlana jest wartość „Path Cost“ portu.
Priority	0 … 61440	W tej kolumnie wyświetlany jest priorytet portu.
Edge Port	Disable Enable	W tej kolumnie wyświetlany jest stan funkcji „Edge Port“.
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“.

10.4.7.3 STP Status



Ilustracja 79: Strona WBM „Spanning Tree Protocol“ – zakładka „STP Status“

Tabela 95: Strona WBM „STP“ – zakładka „STP-Status“

Current Root Status		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tym polu wyświetlany jest adres MAC dla „Root Bridge“.
Priority		W tym polu wyświetlany jest priorytet dla „Root Bridge“. Również ten switch może być „Root Bridge“.
Max Age		W tym polu wyświetlany jest „Max Age“ dla „Root Bridge“.
Hello Time		W tym polu wyświetlany jest „Hello Time“ dla „Root Bridge“. „Root-Bridge“ określa „Hello-Time“, „Max-Age“ i „Forwarding-Delay“.
Forward Delay		W tym polu wyświetlany jest maksymalny czas (w sekundach), jaki switch „Root“ czeka, zanim zmieni stan.
Current Bridge Status		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tym polu wyświetlany jest lokalny adres MAC aktualnego bridge'a.
Priority		W tym polu wyświetlany jest priorytet.
Max Age		W tym polu wyświetlany jest „Max Age“.
Hello Time		W tym polu wyświetlany jest „Hello Time“.
Forward Delay		W tym polu wyświetlany jest „Forward Time“.
Path Costs		W tym polu wyświetlana jest wartość „Path Cost“.
Port ROOT		W tym polu wyświetlany jest numer portu switcha, przez który switch musi komunikować się z „Root“ „Spanning Tree“.

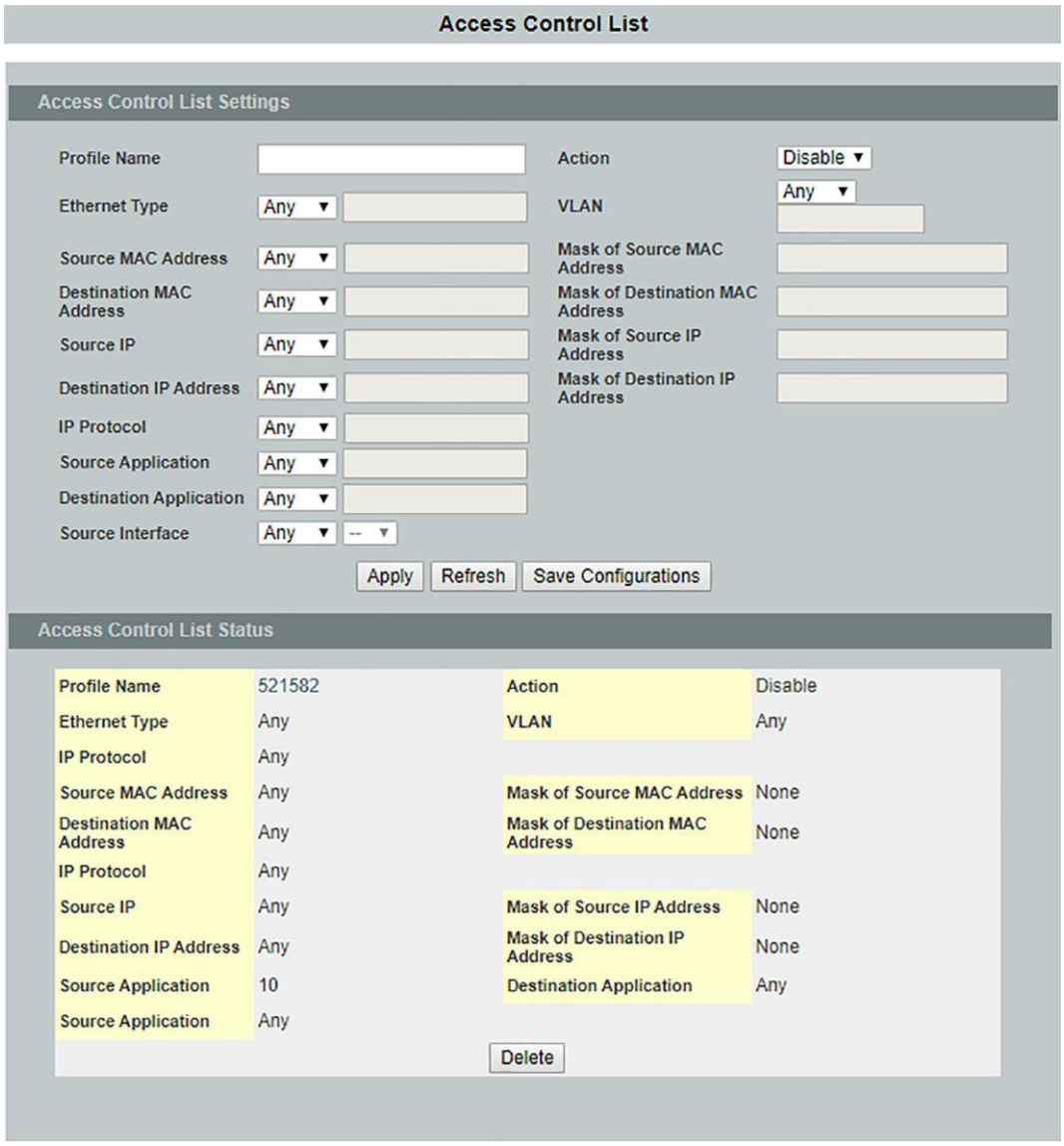
10.5 Security

10.5.1 Access Control List

Wskazówka

Dodatkowa informacja

Więcej informacji o „Access Control List” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 80: Strona WBM „Access Control List“

Tabela 96: Strona WBM „Access Control List“

Access Control List Settings		
Parametr	**Domyślnie**	**Opis**
Profile Name		W polu edycji należy wpisać nazwę profilu.
Action	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować sterowanie dostępem.
	Permission	W polu wyboru należy wybrać „Permission“, aby przesłać dalej pakiety danych, odpowiadające informacjom.
	Drop	W polu wyboru należy wybrać „Drop“, aby odrzuci pakiety danych, odpowiadające informacjom.
ETHERNET Type	**Any**	W polu wyboru należy wybrać „Any“, aby każdy typ ETHERNET był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wyspecyfikować typ ETHERNET, dla którego ma być ważne sterowanie dostępem.
VLAN	**Any**	W polu wyboru należy wybrać „Any“, aby każdy VLAN ID był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Access Controll List“ określony VLAN ID.
Source MAC Address	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres MAC był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Access Controll List“ adres MAC dla źródła.
Mask of Source MAC Address		W polu edycji należy wpisać źródłowy adres MAC maski bitowej dla źródłowych adresów MAC pakietów, które mają być filtrowane. Gdy w polu wyboru „Source MAC Address“ została wybrana opcja „Any“, pole to pozostaje puste. Wtedy profil wyfiltruje tylko adres MAC, wpisany w polu „Source MAC Address“.
Destination MAC Address	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres MAC był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Access Controll List“ docelowy adres MAC.
Mask of Destination MAC Address		W polu edycji należy wpisać docelowy adres MAC maski bitowej dla docelowych adresów MAC pakietów, które mają być filtrowane. Gdy w polu wyboru „Destination MAC Address“ została wybrana opcja „Any“, pole to pozostaje puste. Wtedy profil wyfiltruje tylko adres MAC, wpisany w polu „Destination MAC Address“.
Source IP	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres IP był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Source IP“ docelowy adres IP.
Mask of Source IP Address		W polu edycji należy wpisać źródłowy adres IP maski bitowej dla źródłowych adresów IP pakietów, które mają być filtrowane. Gdy w polu wyboru „Source IP“ została wybrana opcja „Any“, pole to pozostaje puste. Wtedy profil wyfiltruje tylko adres IP, wpisany w polu „Source IP Address“.
Destination IP Address	**Any**	W polu wyboru należy wybrać „Any“, aby każdy adres IP był ważny.
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Access Control List“ docelowy adres IP.

Tabela 96: Strona WBM „Access Control List“

Mask of Destination IP Address		W polu edycji należy wpisać docelowy adres IP maski bitowej dla docelowych adresów IP pakietów, które mają być filtrowane. Gdy w polu wyboru „Destination IP Address“ została wybrana opcja „Any“, pole to pozostaje puste. Wtedy profil wyfiltruje tylko adres IP, wpisany w polu „Destination IP Address“.	
IP Protokol	**Any**	W polu wyboru należy wybrać „Any“, aby każdy protokół IP dla „Access Control List“ był ważny.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać protokół.	
Source Application	**Any**	W polu wyboru należy wybrać „Any“, aby każda aplikacja była ważna.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać port źródłowy (np. 2234).	
Destination Applikation	**Any**	W polu wyboru należy wybrać „Any“, aby każda docelowa aplikacja była ważna.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać do „Access Control List“ port docelowy (np. 502).	
Source Interface	**Any**	W polu wyboru należy wybrać „Any“, gdy każdy fizyczny port jest ważny.	
	Other	1 … 10 (12)	W polu edycji należy wpisać fizyczny port, dla którego ten wpis w „Access Control List“ jest ważny.

Tabela 96: Strona WBM „Access Control List“

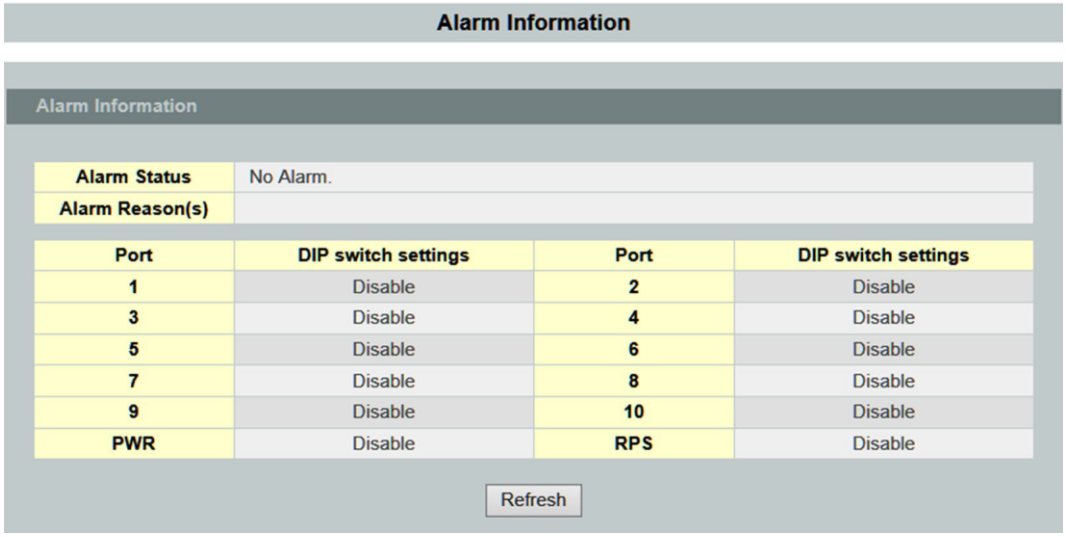
Access Control List Status		
Parametr	**DomyślnIe**	**Opis**
Profile Name		W tym polu wyświetlana jest wybrana nazwa profilu.
Action	Disable Permission Discard DSCP	W tym polu wyświetlany jest status sterowania dostępem. (DSCP tylko przy IPv4)
ETHERNET Type	Any Other	W tym polu wyświetlany jest typ ETHERNET.
VLAN	Any Other	W tym polu wyświetlany jest VLAN ID.
IP Protokol	Any Other	W tym polu wyświetlany jest IP protokołu.
Source MAC Address	Any Other	W tym polu wyświetlany jest „Source MAC Address“.
Mask of Source MAC Address		W tym polu wyświetlany jest źródłowy adres MAC maski bitowej.
Destination MAC Address	Any Other	W tym polu wyświetlany jest docelowy adres MAC.
Mask of Destination MAC Address		W tym polu wyświetlany jest docelowy adres MAC maski bitowej.
IP Protokol	Any Other	W tym polu wyświetlany jest IP protokołu.
Source IP	Any Other	W tym polu wyświetlany jest źródłowy IP.
Mask of Source IP Address		W tym polu wyświetlany jest źródłowy adres MAC maski bitowej.
Destination IP Address	Any Other	W tym polu wyświetlany jest docelowy adres IP.
Mask of Destination IP Address		W tym polu wyświetlany jest docelowy adres IP maski bitowej.
Source Application	Any Other	W tym polu wyświetlana jest źródłowa aplikacja.
Destination Applikation	Any Other	W tym polu wyświetlana jest docelowa aplikacja.
Source Interface	1 … 10 (12)	W tym polu wyświetlany jest źródłowy interfejs.

10.6 Monitor

10.6.1 Alarm Information

Wskazówka

Dodatkowa informacja
Więcej informacji o „Alarm” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 81: Strona WBM „Alarm Information“

Tabela 97: Strona WBM „Alarm Information“

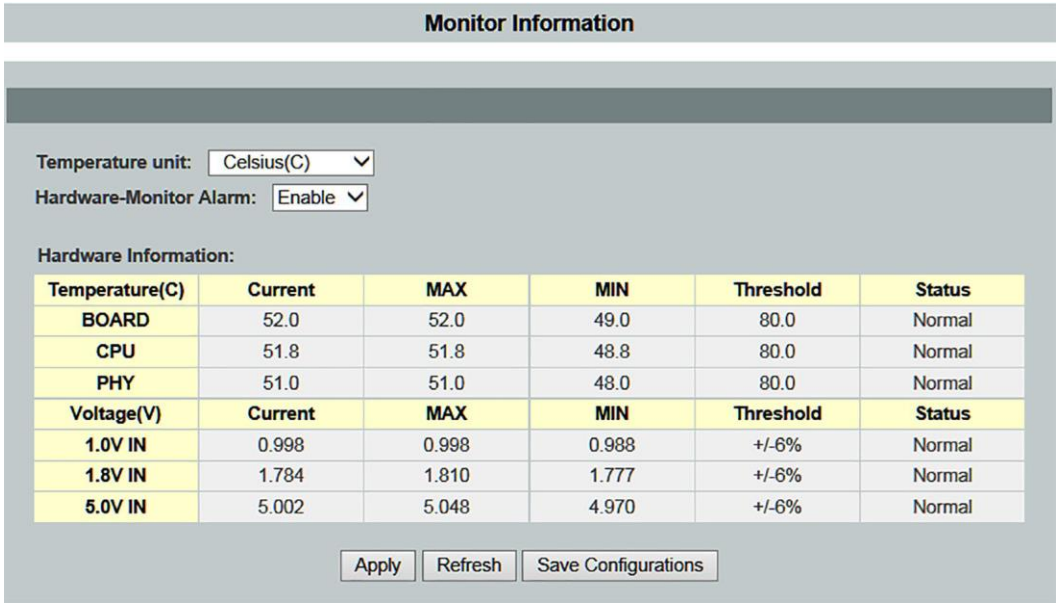
Alarm Information		
Parametr	**Domyślnie**	**Opis**
Alarm Status		W tym polu wyświetlana jest informacja, czy wystąpiły zdarzenia alarmu.
Alarm Reason(s)		W tym polu wyświetlane są szczegóły dotyczące zdarzeń alarmu.
Port	0 … 10 PWR RPS	W tej kolumnie wyświetlana jest nazwa mikroprzełącznika DIP.
DIP switch Settings	Enable Disable	W tej kolumnie wyświetlany jest aktualny status mikroprzełącznika DIP.

10.6.2 Monitor Information

Wskazówka

Dodatkowa informacja

Więcej informacji o „Monitor Information” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 82: Strona WBM „Monitor Information”

Tabela 98: Strona WBM „Monitor Information“

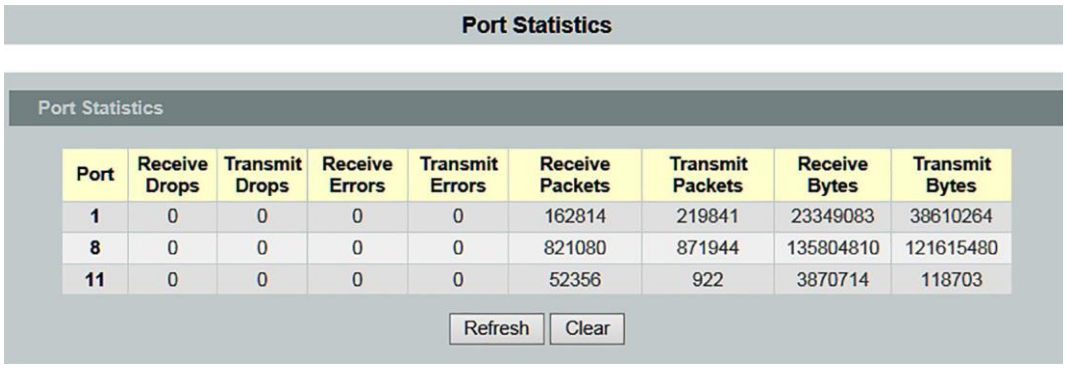
Hardware Information		
Parametr	**Domyślnie**	**Opis**
Temperature unit	**Celsius (C)**	W polu wyboru należy wybrać „Celsius (C)“, jeśli temperatura ma być wskazywana w skali Celsiusa.
	Fahrenheit (F)	W polu wyboru należy wybrać „Fahrenheit (C)“, jeśli temperatura ma być wskazywana w skali Fahrenheita.
Hardware Information		
Parametr	**Domyślnie**	**Opis**
Temperature (C)		
Current		W tej kolumnie wyświetlana jest aktualna temperatura głównej płytki drukowanej „BOARD“, „CPU“ i chipu MAC „PHY“.
MAX		W tej kolumnie wyświetlana jest maksymalna temperatura głównej płytki drukowanej „BOARD“, „CPU“ i chipu MAC „PHY“.
MIN		W tej kolumnie wyświetlana jest minimalna temperatura głównej płytki drukowanej „BOARD“, „CPU“ i chipu MAC „PHY“.
Threshold		W tej kolumnie wyświetlany jest ustawiony próg.
Status		W tej kolumnie wyświetlany jest status.
Voltage (V)		
Current		W tej kolumnie wyświetlane jest aktualne napięcie dla wejść „1,0 V IN“, „2,5 V IN“ i „3,3 V IN“.
MAX		W tej kolumnie wyświetlane jest maksymalne napięcie dla wejść „1,0 V IN“, „2,5 V IN“ i „3,3 V IN“.
MIN		W tej kolumnie wyświetlane jest minimalne napięcie dla wejść „1,0 V IN“, „2,5 V IN“ i „3,3 V IN“.
Threshold		W tej kolumnie wyświetlany jest ustawiony próg.
Status		W tej kolumnie wyświetlany jest status.

10.6.3 Port Statistics

Wskazówka

Dodatkowa informacja

Więcej informacji o „Port Statystic” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 83: Strona WBM „Port Statistics“

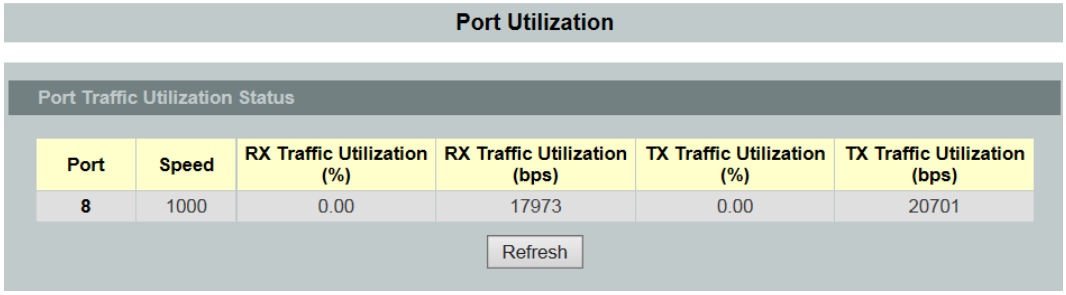
Tabela 99: Strona WBM „Port Statistics“

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

10.6.4 Port Utilization

Wskazówka

Dodatkowa informacja
Więcej informacji o „Port Utilization” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 84: Strona WBM „Port Utilization“

Tabela 100: Strona WBM „Port Utilization“

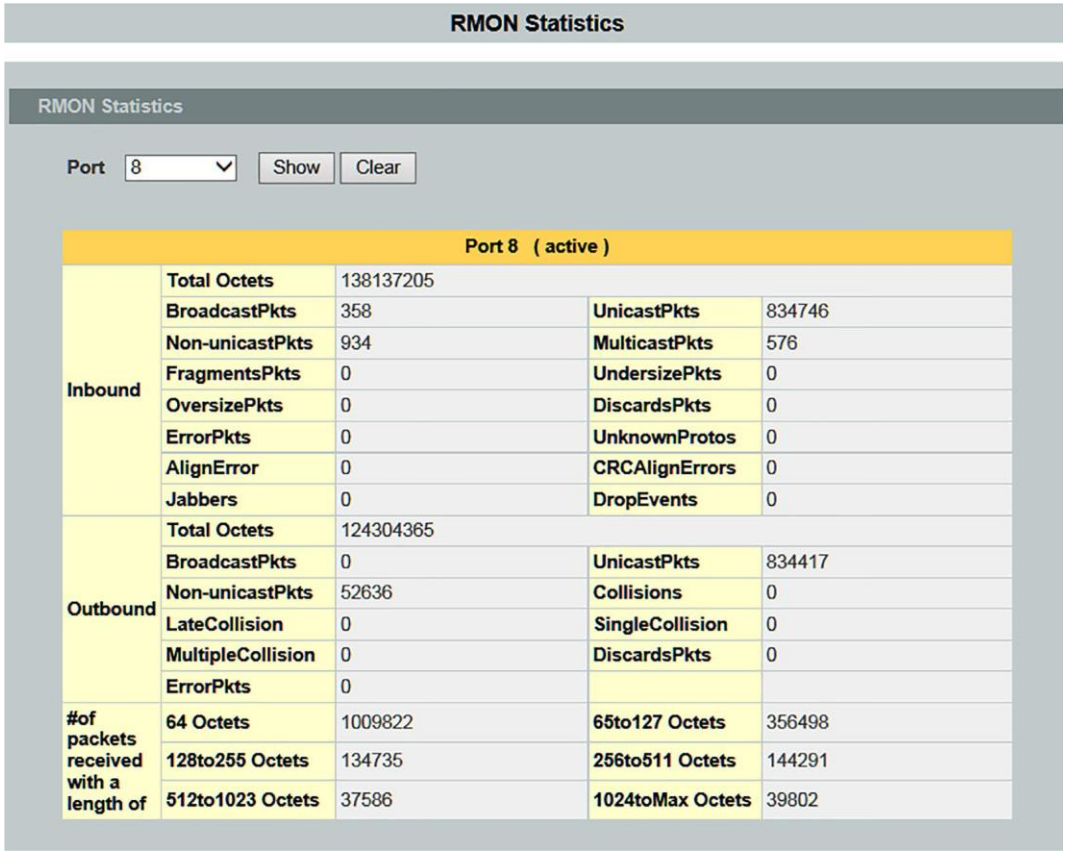
Port Utilization Status		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlane są numery portów.
Speed		W tej kolumnie wyświetlana jest prędkość transferu.
RX Traffic Utilization (%)		W tej kolumnie wyświetlane jest procentowe obciążenie pasma RX.
RX Traffic Utilization (bps)		W tej kolumnie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

10.6.5 RMON Statistics

Wskazówka

Dodatkowa informacja

Więcej informacji o „RMON Statistic” można znaleźć w rozdziale „Opis funkcji”.



Port 8 (active)				
Inbound	Total Octets	138137205		
	BroadcastPkts	358	UnicastPkts	834746
	Non-unicastPkts	934	MulticastPkts	576
	FragmentsPkts	0	UndersizePkts	0
	OversizePkts	0	DiscardsPkts	0
	ErrorPkts	0	UnknownProtos	0
	AlignError	0	CRCAlignErrors	0
	Jabbers	0	DropEvents	0
Outbound	Total Octets	124304365		
	BroadcastPkts	0	UnicastPkts	834417
	Non-unicastPkts	52636	Collisions	0
	LateCollision	0	SingleCollision	0
	MultipleCollision	0	DiscardsPkts	0
	ErrorPkts	0		
#of packets received with a length of	64 Octets	1009822	65to127 Octets	356498
	128to255 Octets	134735	256to511 Octets	144291
	512to1023 Octets	37586	1024toMax Octets	39802

Ilustracja 85: Strona WBM „RMON Statistics“

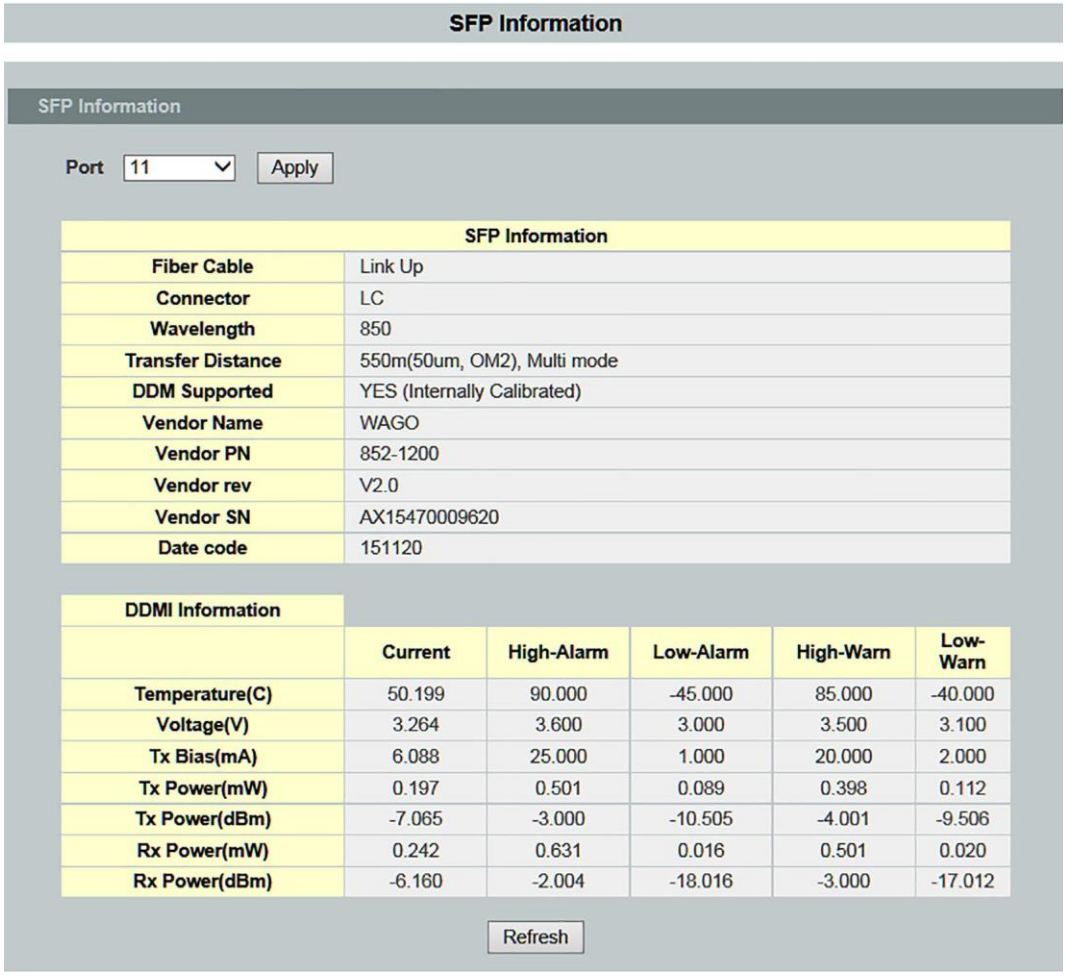
Tabela 101: Strona WBM „RMON Statistics“

RMON Statistics			
Parametr		**Domyślnie**	**Opis**
Port		**-**	W polu wyboru należy wybrać „-“, jeśli statystyka nie ma być wyświetlona.
		1 … 10 All	W polu wyboru należy wybrać port lub zakres portów, dla którego/których mają być wyświetlone statystyki RMON.
Selected Port x (active)			
Parametr		**Domyślnie**	**Opis**
Incoming	Total Octets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych.
	Broadcast Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów broadcast.
	Unicast Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów unicast.
	No Unicast Packets		W tej kolumnie wyświetlana jest liczba odebranej przez port sumy pakietów broadcast i multicast.
	Multicast Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów multicast.
	Fragmented Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port fragmentarycznych pakietów danych.
	Undersized Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port zbyt małych pakietów danych.
	Oversized Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port zbyt dużych pakietów danych.
	Discards Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych, które zostały odrzucone.
	Error Packets		W tej kolumnie wyświetlana jest liczba odebranych przez port błędnych pakietów danych.
	Unknown Protos		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów, które zawierały jako cel nieznany lub nieobsługiwany protokół.
	Align Error		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych, przy których zbiorcza liczba bitów odebranej ramki nie jest podzielna przez 8.
	CRC Align Errors		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych z błędem sumy kontrolnej.
	Jabbers		W tej kolumnie wyświetlana jest liczba odebranych przez port „Jabber“.
	Drop Events		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych.

Tabela 101: Strona WBM „RMON Statistics“

Outgoing	Total Octets		W tej kolumnie wyświetlana jest liczba wysłanych przez port pakietów danych.
	Broadcast Packets		W tej kolumnie wyświetlana jest liczba wysyłanych przez port pakietów broadcast.
	Unicast Packets		W tej kolumnie wyświetlana jest liczba wysyłanych przez port pakietów unicast.
	No Unicast Packets		W tej kolumnie wyświetlana jest liczba wysyłanych przez port pakietów unicast.
	Collisions		W tej kolumnie wyświetlana jest liczba pakietów danych, które mają być wysłane, miały kolizję lub zostały odrzucone.
	Late Collision		W tej kolumnie wyświetlana jest liczba pakietów danych, które mają być wysłane, miały kolizję lub zostały odrzucone.
	Single Collisions		W tym polu wyświetlana jest liczba pojedynczych kolizji wysłanych pakietów danych.
	Multiple Collisions		W tym polu wyświetlana jest liczba wielokrotnych kolizji wysłanych pakietów danych.
	Discards Packets		W tej kolumnie wyświetlana jest liczba wysłanych przez port pakietów danych, które zostały odrzucone.
	Error Packets		W tej kolumnie wyświetlana jest liczba wysłanych przez port pakietów danych, które był błędne.
#(number) of packets receives with a lengh of	64 Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość 64 oktetów.
	65 to 127 Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość od 65 do 127 oktetów.
	128 to 255 Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość od 128 do 255 oktetów.
	256 to 511 Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość od 256 do 511 oktetów.
	512 to 1023 Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość od 512 do 1023 oktetów.
	1024 to Max. Octets		W tym polu wyświetlana jest liczba odebranych przez port pakietów danych, które miały długość większą niż 1024 oktety.

10.6.6 SFP Information



Ilustracja 86: Strona WBM „SPF Information“

Tabela 102: Strona WBM „SPF Information“

SFP Information		
Parametr	**Domyślnie**	**Opis**
Port	**-**	W polu wyboru należy wybrać „-“, gdy nie jest wetknięty moduł SFP.
	9, 10	W polu wyboru należy wybrać port, do którego jest wetknięty moduł SFP.
SFP Information		
Parametr	**Domyślnie**	**Opis**
Fiber Cable		W tym polu wyświetlana jest informacja, czy podłączony jest światłowód.
Connector		W tym polu wyświetlany jest kod typu wtyczki światłowodu.
Wavelength		W tym polu wyświetlana jest długość fali.
Transfer Distance		W tym polu wyświetlana jest odległość, na jaką wykonany ma być transfer.
DDM Support		W tym polu wyświetlana jest informacja, czy moduł SFP wspiera DDM („Dynamic Device Mapping“).
Vendor Name		W tym polu wyświetlana jest nazwa producenta SFP.
Vendor PN		W tym polu wyświetlany jest numer części.
Vendor rev		W tym polu wyświetlana jest wersja numeru części.
Vendor SN		W tym polu wyświetlany jest numer serii (ASCII).
Date code		W tym polu wyświetlana jest data wersji.

Tabela 102: Strona WBM „SPF Information“

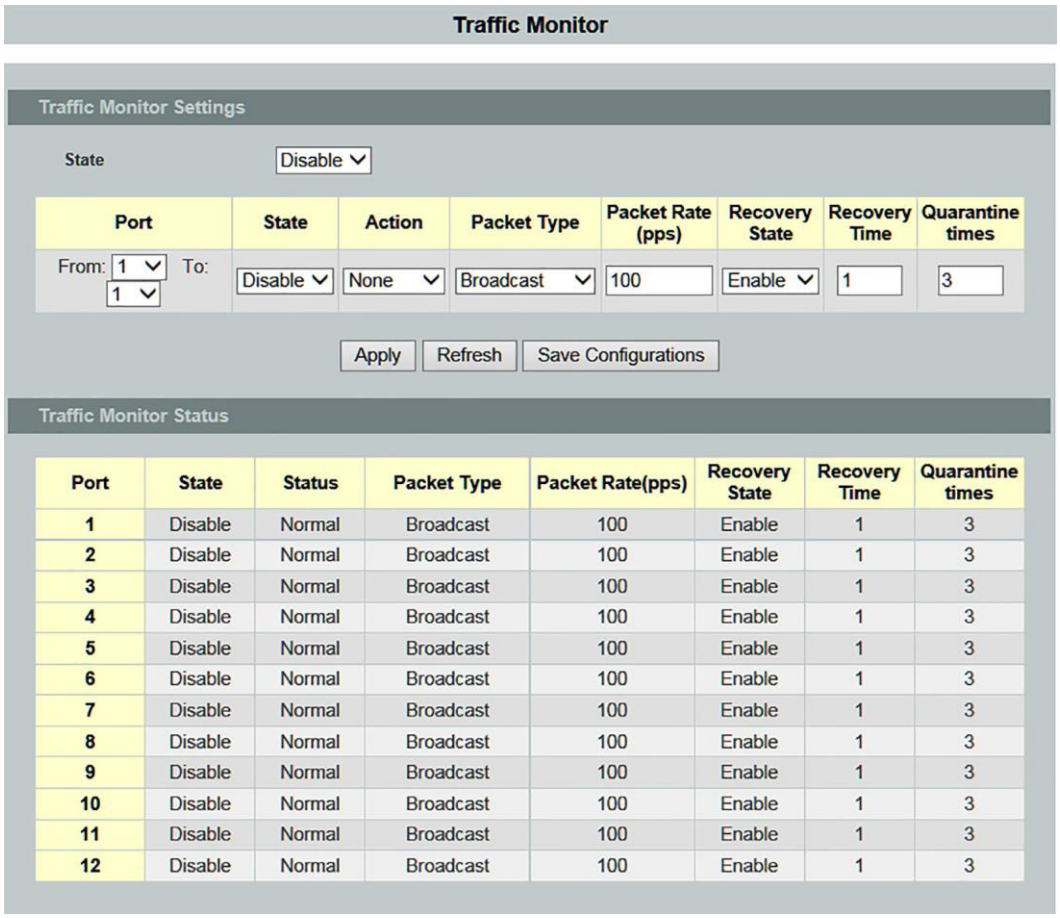
DDMI Information		
Parametr	**Domyślnie**	**Opis**
Current		W tej kolumnie wyświetlane są następujące aktualne wartości: - Temperature (C) - Voltage (V) - Tx Bias (mA) - Tx Power (mW) - Tx Power (dBm) - Rx Power (mW) - Rx Power (dBm)
High-Alarm		W tej kolumnie wyświetlane są wartości „High-Alarm“ dla następujących parametrów: - Temperature(C) - Voltage (V) - Tx Bias (mA) - Tx Power (mW) - Tx Power (dBm) - Rx Power (mW) - Rx Power (dBm)
Low-Alarm		W tej kolumnie wyświetlane są wartości „Low-Alarm“ dla następujących parametrów: - Temperature (C) - Voltage (V) - Tx Bias (mA) - Tx Power (mW) - Tx Power (dBm) - Rx Power (mW) - Rx Power (dBm)
High-Warn		W tej kolumnie wyświetlane są wartości „High-Warn“ dla następujących parametrów: - Temperature (C) - Voltage (V) - Tx Bias (mA) - Tx Power (mW) - Tx Power (dBm) - Rx Power (mW) - Rx Power (dBm)
Low-Warn		W tej kolumnie wyświetlane są wartości „Low-Warn“ dla następujących parametrów: - Temperature (C) - Voltage (V) - Tx Bias (mA) - Tx Power (mW) - Tx Power (dBm) - Rx Power (mW) - Rx Power (dBm)

10.6.7 Traffic Monitor

Wskazówka

Dodatkowa informacja

Więcej informacji o „Traffic Monitor” można znaleźć w rozdziale „Opis funkcji”.



Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time	Quarantine times
1	Disable	Normal	Broadcast	100	Enable	1	3
2	Disable	Normal	Broadcast	100	Enable	1	3
3	Disable	Normal	Broadcast	100	Enable	1	3
4	Disable	Normal	Broadcast	100	Enable	1	3
5	Disable	Normal	Broadcast	100	Enable	1	3
6	Disable	Normal	Broadcast	100	Enable	1	3
7	Disable	Normal	Broadcast	100	Enable	1	3
8	Disable	Normal	Broadcast	100	Enable	1	3
9	Disable	Normal	Broadcast	100	Enable	1	3
10	Disable	Normal	Broadcast	100	Enable	1	3
11	Disable	Normal	Broadcast	100	Enable	1	3
12	Disable	Normal	Broadcast	100	Enable	1	3

Ilustracja 87: Strona WBM „Traffic Monitor“

Tabela 103: Strona WBM „Traffic Monitor”

Traffic Monitor Settings			
Parametr		**Domyślnie**	**Opis**
Status		**Disable**	W polu wyboru należy wybrać „Disable“, aby globalnie dezaktywować funkcję „Traffic Monitor“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Traffic Monitor“.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Traffic Monitor“ dla portu lub zakresu portów.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Traffic Monitor“ dla portu lub zakresu portów.
Action		**None**	W polu wyboru należy wybrać „None“, jeśli blokada portów nie ma być zniesiona.
		Unblock	W polu wyboru należy wybrać „Unblock“, jeśli blokada portów nie ma być zniesiona.
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)			W polu edycji należy wpisać prędkość pakietu, która ma być monitorowana.
Recovery State		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Recovery“ w „Traffic Monitor“ dla portu lub zakresu portów.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Recovery“ w „Traffic Monitor“ dla portu lub zakresu portów.
Recovery Time		**1**	W tej kolumnie należy wpisać „Recovery Time“, który ma być monitorowany.
Quarantime Times		**3**	W polu edycji należy wpisać wartość „Quarantine Times” dla „Traffic-Monitor”.
Traffic Monitor 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.
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.
Recovery State		Enable Disable	W tej kolumnie wyświetlany jest status wybranej funkcji „Recovery“.
Recovery Time (min)		1 … 60	W tej kolumnie wyświetlany jest wybrany „Recovery Time“.
Quarantime Times		3	W tej kolumnie wyświetlany jest wybrany czas kwarantanny.

10.7 Management

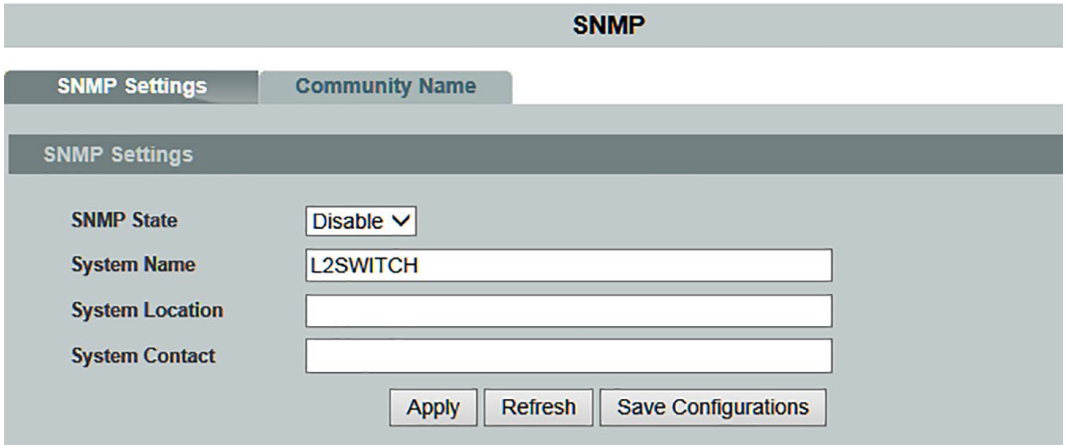
10.7.1 SNMP

10.7.1.1 SNMP

10.7.1.1.1 SNMP Settings

Wskazówka **Dodatkowa informacja**

Więcej informacji o „SNMP“ (**S**imple **N**etwork **M**anagement **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.

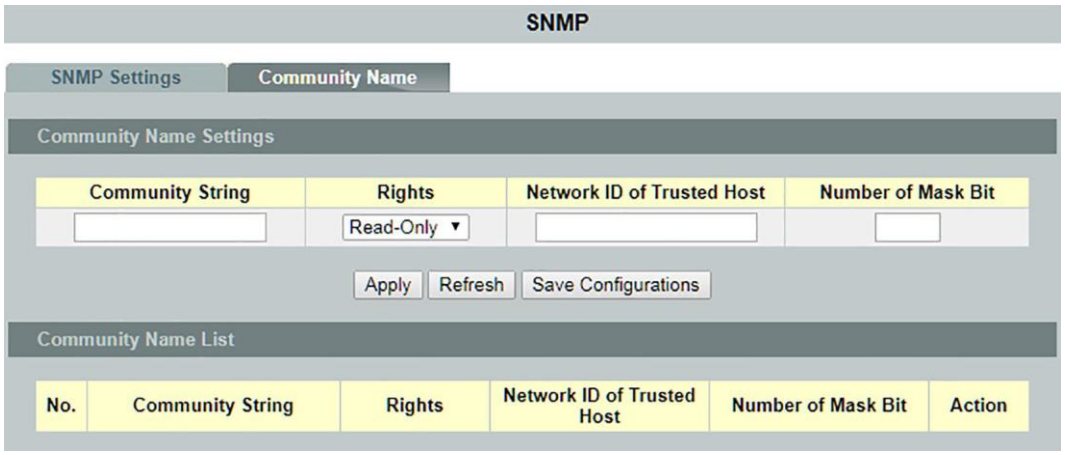


Ilustracja 88: Strona WBM „SNMP“ – zakładka „SNMP Settings“

Tabela 104: Strona WBM „SNMP“ – zakładka „SNMP Settings“

SNMP Settings		
Parametr	**Domyślnie**	**Opis**
SNMP State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować w switchu SNMP.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować w switchu SNMP.
System Name	**L2SWITCH**	W polu edycji należy wpisać nazwę systemową switcha. (nazwa systemowa i nazwa hosta są identyczne).
System Location	**–**	W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami.
System Contact	**–**	W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.

10.7.1.1.2 Community Name



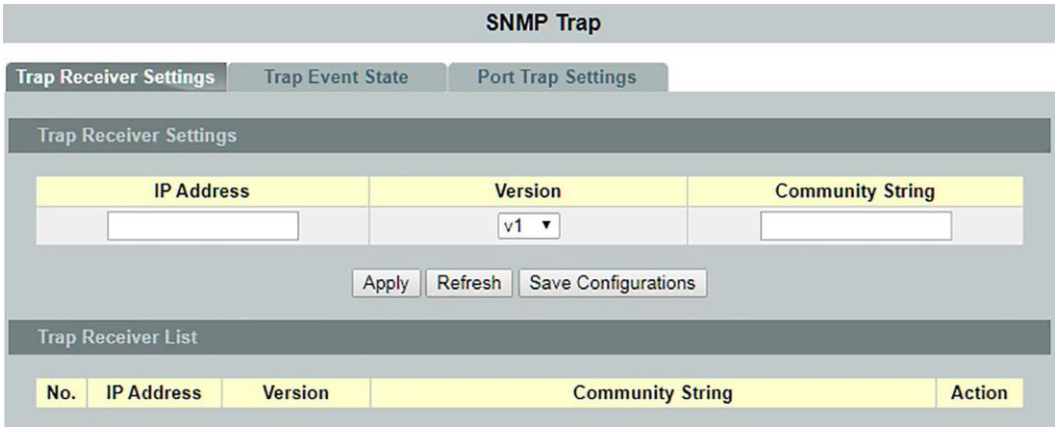
Ilustracja 89: Strona WBM „SNMP“ – zakładka „Community Name“

Tabela 105: Strona WBM „SNMP“ – zakładka „Community Name“

Community Name Settings		
Parametr	**Domyślnie**	**Opis**
Community String		W polu edycji należy wpisać „Community String“, funkcjonujący jako hasło dla żądań stacji zarządzającej.
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 the 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		W polu edycji należy wpisać adres IP maski podsieci rozproszonej stacji zarządzającej SNMP, używając zapisu z kropkami (np. 255.255.255.0).
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 „CNTP Community String“. 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 **[Delete]**, aby usunąć specyficzny „Community String”.

10.7.1.2 SNMP Trap

10.7.1.2.1 Trap Receiver Settings

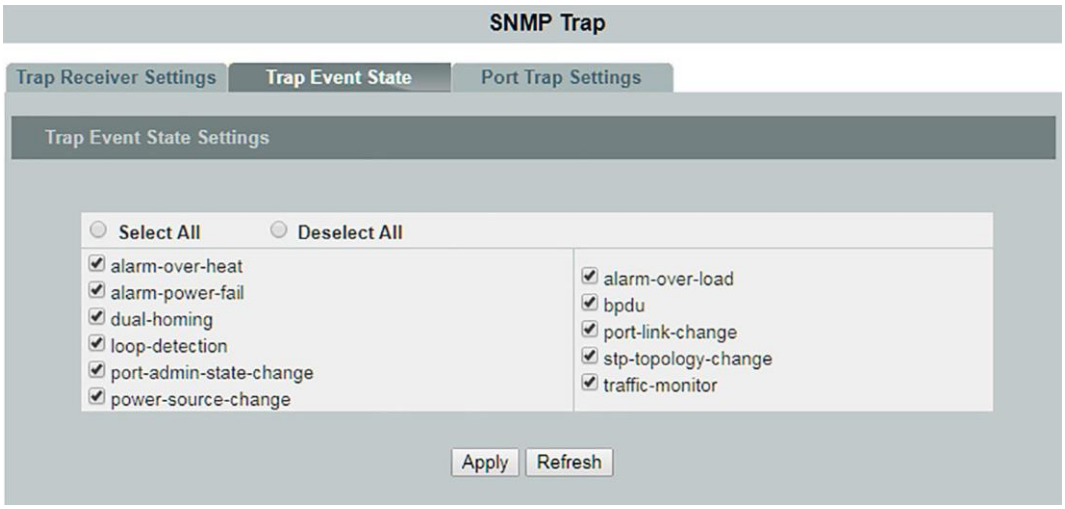


Ilustracja 90: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“

Tabela 106: Strona WBM „SNMP Trap“ – zakładka „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 **[Delete]**.

10.7.1.2.2 Trap Event State

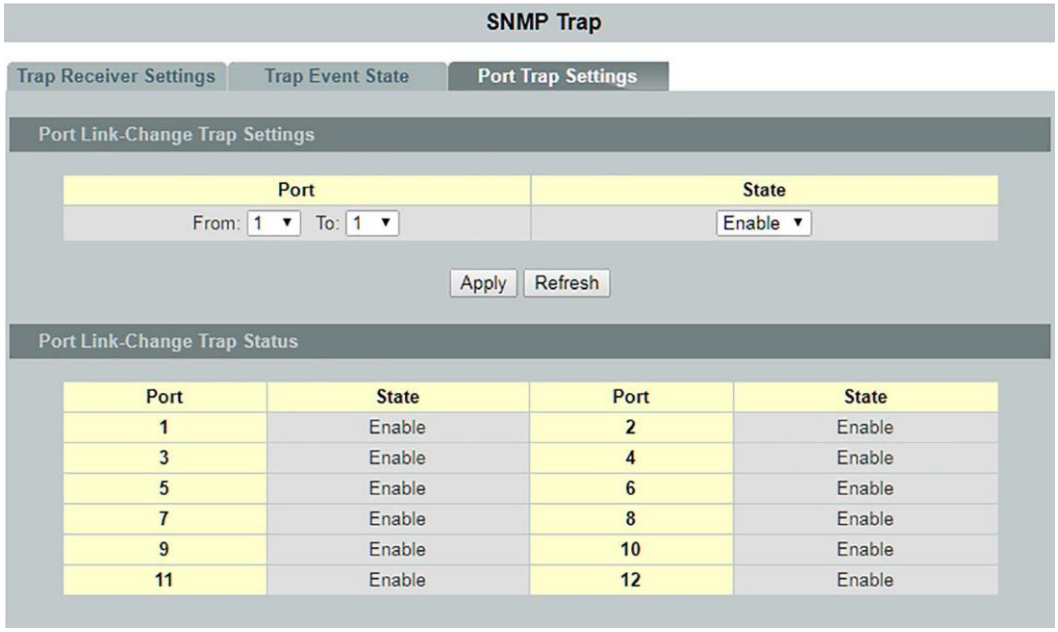


Ilustracja 91: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“

Tabela 107: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“

Trap Event State Settings		
Parametr	**Domyślnie**	**Opis**
alarm-over-heat	☑	Aktywuje / dezaktywuje trap SNMP, gdy temperatura systemu jest zbyt wysoka.
alarm-power-fail	☑	Aktywuje / dezaktywuje trap SNMP, gdy wydajność systemu przekracza poziom / spada poniżej poziomu napięcia. Nadnapięcie RPS / Napięcie RPS
dual-homing	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest zablokowany przez „Dual Homing“.
loop-detection	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest zablokowany przez Loop Detection.
port-admin-state-change	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest aktywowany / dezaktywowany przez administratora.
power-source-change	☑	Aktywuje / dezaktywuje trap SNMP, gdy źródło prądu zostało zmienione. (AC na DC lub DC na AC)
alarm-over-load	☑	Aktywuje / dezaktywuje trap SNMP, gdy system jest przeciążony.
bpdu	☑	Aktywuje / dezaktywuje trap SNMP, gdy port jest zablokowany przez „BPDU Guard/BDPU Root”. Status złącza „Guard/BPDU” jest zmieniony.
port-link-change	☑	Aktywuje / dezaktywuje trap SNMP, Aktywuje / dezaktywuje trap SNMP, gdy port wykazuje zmianę w górę/w dół.
stp-topology-change	☑	Aktywuje / dezaktywuje trap SNMP, gdy zmienia się topologia STP.
traffic-monitor	☑	Aktywuje / dezaktywuje trap SNMP, gdy port zablokowany jest przez „Traffic Monitor“.

10.7.1.2.3 Port Trap Settings



Ilustracja 92: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“

Tabela 108: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“

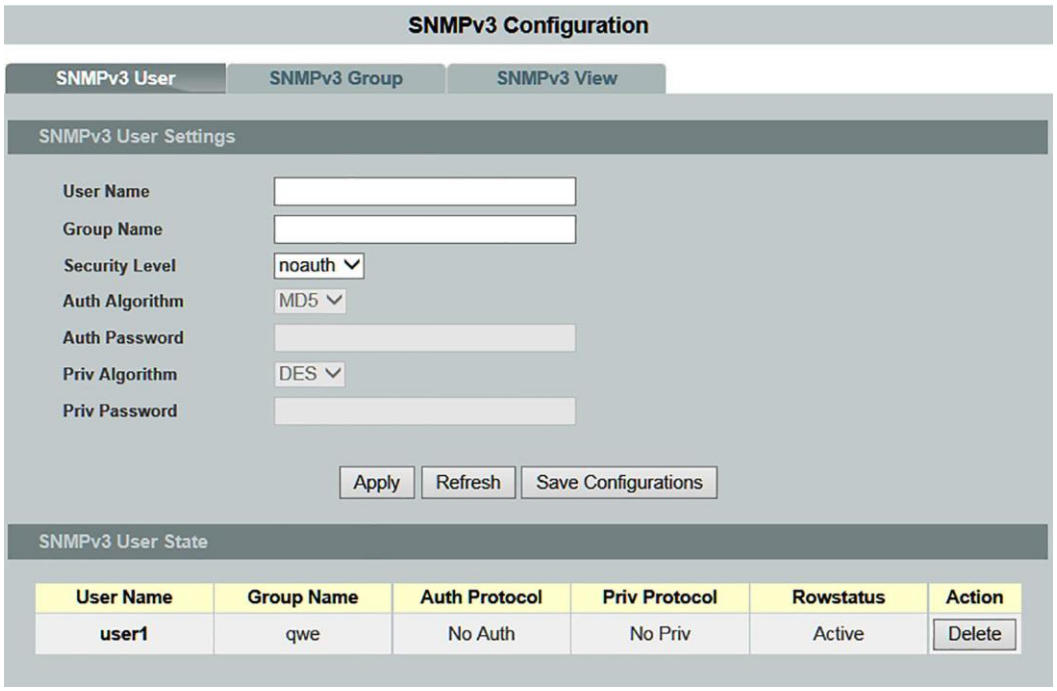
Port Link-Change Trap Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
State		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować status portu.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować status portu.
Port Link-Change Trap Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlany jest zakres portów.
State		Enable Disable	W tym polu wyświetlany jest status portu.

10.7.1.3 SNMPv3 Configuration

10.7.1.3.1 SNMPv3 User

Wskazówka

Dodatkowa informacja
Więcej informacji o „SNMPv3” znajdą Państwo w rozdziale „Opis funkcji”.

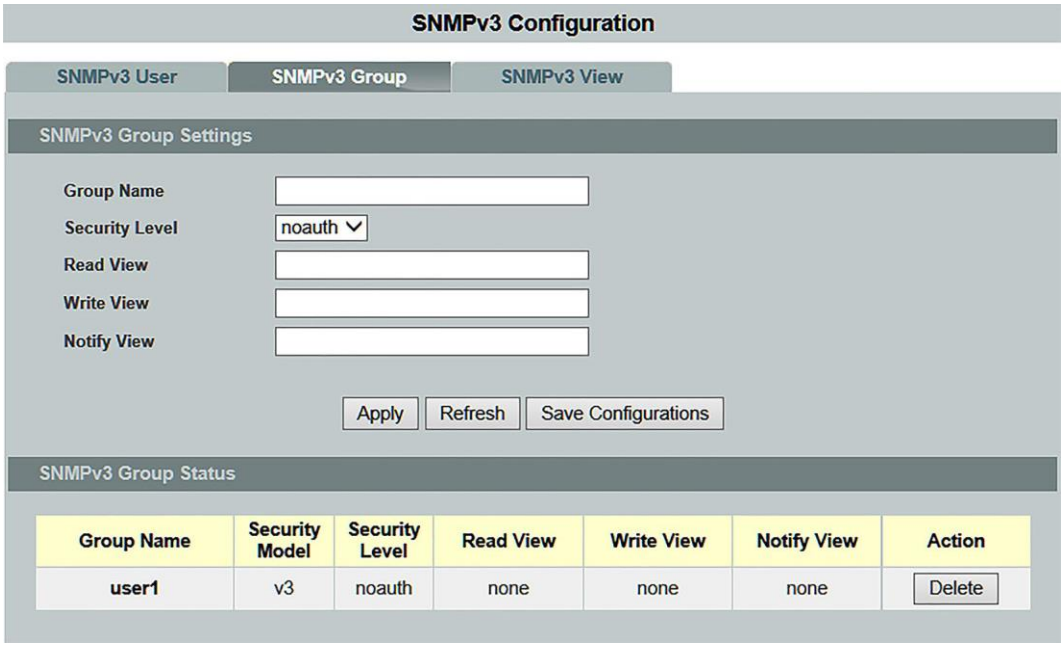


Ilustracja 93: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“

Tabela 109: Strona WBM „SNMPv3 Configuration“ – zakładka „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 Algorithm“ i „Priv Algorithm“.
	auth	Gdy w polu wyboru wybrana jest opcja „auth“, istnieje możliwość zmiany „Auth Algorithm“ i „Auth Password“.
	priv	Gdy w polu wyboru wybrana jest opcja „priv“, istnieje możliwość zmiany „Auth Algorithm“, „Auth Password“, „Priv Algorithm“ i „Priv Password“.
Auth Algorithm	**MD5**	Gdy w polu wyboru wybrana jest opcja „auth“ lub „priv“, istnieje możliwość wyboru „Auth Algorithm“ „MD5“.
	SHA	Gdy w polu wyboru wybrana jest opcja „auth“ lub „priv“, istnieje możliwość wyboru „Auth Algorithm“ „SHA“.
Auth Password		Gdy w polu wyboru wybrana jest opcja „auth“, można w polu edycji wpisać hasło (co najmniej 8 znaków alfanumerycznych).
Priv Algorithm	**DES**	Gdy w polu wyboru wybrana jest opcja „priv“, w polu wyboru można wybrać „DES“.
	AES	Gdy w polu wyboru wybrana jest opcja „priv“, w polu wyboru można wybrać „AES“.
Priv Password		Gdy w polu wyboru wybrana jest opcja „priv“, można w polu edycji wpisać hasło (co najmniej 8 znaków alfanumerycznych).
SNMPv3 User State		
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 Algorithm“.
Priv Protocol		W tej kolumnie wyświetlany jest wybrany „Priv Algorithm“.
Rowstatus		W tej kolumnie wyświetlany jest „Rowstatus“.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

10.7.1.3.2 SNMPv3 Group

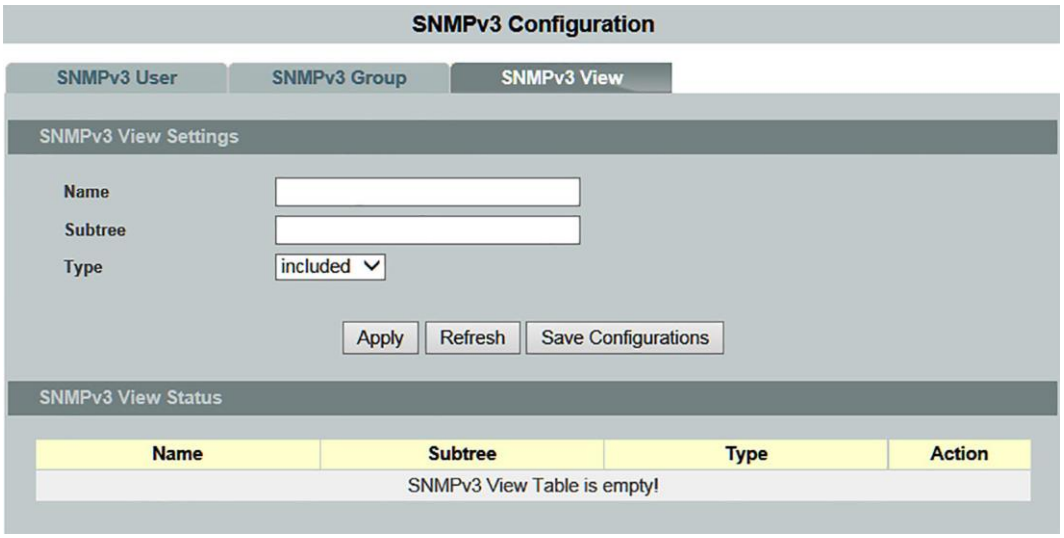


Ilustracja 94: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“

Tabela 110: Strona WBM „SNMPv3 Configuration“ – zakładka „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 auth priv	W polu wyboru należy wybrać odpowiedni poziom bezpieczeństwa.
Read View		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		W polu edycji należy wpisać nazwę obiektów, do których ma być wybrany dostęp zapisu.
Notify View		W polu edycji należy wpisać nazwę obiektu, który może odbierać powiadomienia użytkowników.
SNMPv3 Group Status		
Parametr	**Domyślnie**	**Opis**
Group Name		W tej kolumnie wyświetlana jest nazwa grupy.
Security Model		W tej kolumnie wyświetlany jest wybrany model bezpieczeństwa.
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 **[Delete]**.

10.7.1.3.3 SNMPv3 View



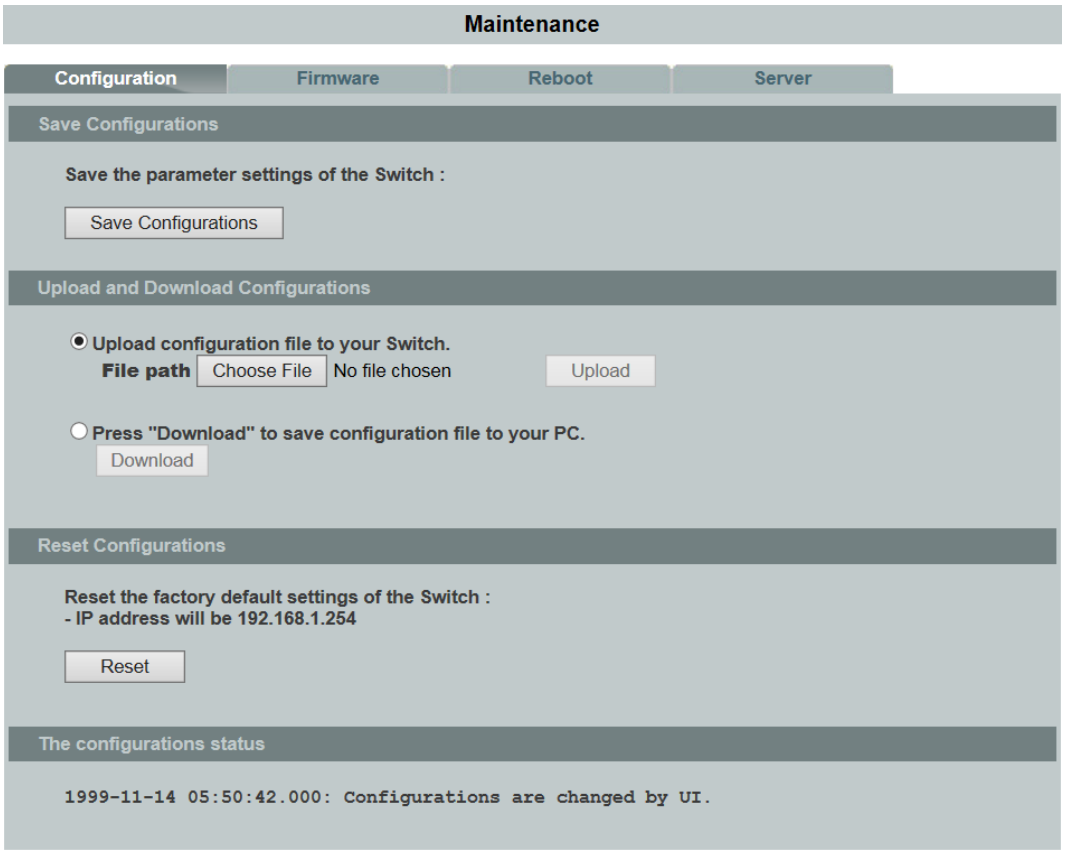
Ilustracja 95: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“

Tabela 111: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“

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

10.7.2 Maintenance

10.7.2.1 Configuration



Ilustracja 96: Strona WBM „Maintenance“ – zakładka „Configuration“

Save Configurations

- Należy kliknąć przycisk **[Save Configuration]**, aby zapisać aktualne ustawienia w NV-RAM (Flash).

Upload and Download Configurations

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

1. Zaznacz „Press Download to save the configuration file to your PC“.
2. Kliknij przycisk **[Download]**, aby rozpocząć pobieranie.

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

1. Zaznacz „Upload the configuration file to the Switch“.
2. Kliknij przycisk **[Select file]**.
   Wybierz plik konfiguracyjny, podając pełną ścieżkę.
3. Kliknij przycisk **[Upload]**, aby rozpocząć pobieranie.

Reset Configurations

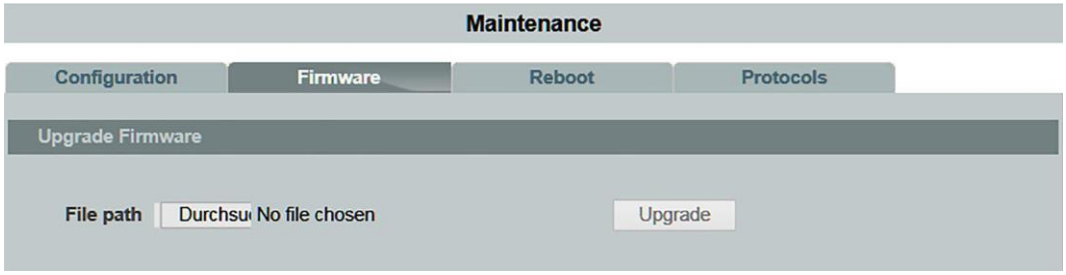
- Kliknij przycisk **[Reset]**, aby cofnąć konfigurację switcha do ustawień fabrycznych.

The configuration status

Jeśli konfiguracje zostały zmienione, pojawi się informacja „The configurations have been changed“.

Jeśli konfiguracje nie zostały zmienione, pojawi się informacja „The user configurations file is the default“. The configurations are default values.“.

10.7.2.2 Firmware



Ilustracja 97: Strona WBM „Maintenance“ – zakładka „Firmware“

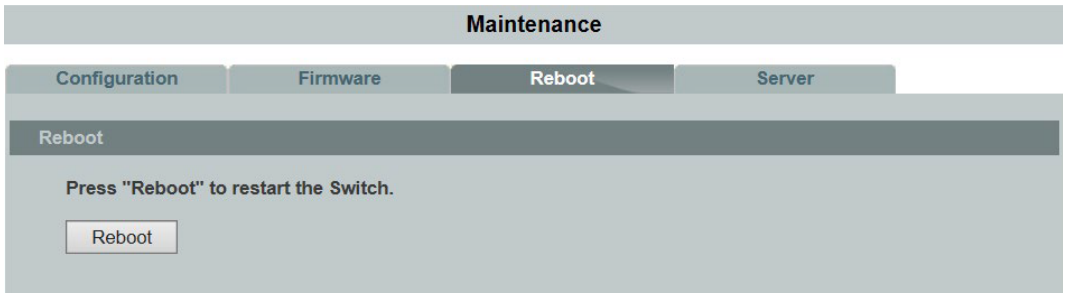
Upgrade Firmware

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

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

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

10.7.2.3 Reboot



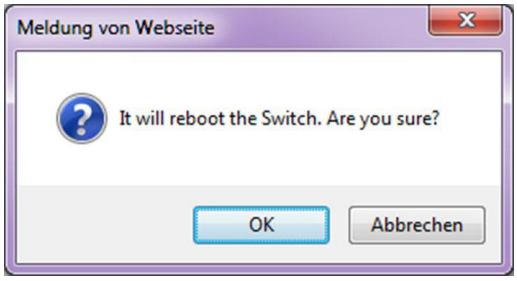
Ilustracja 98: Strona WBM „Maintenance“ – zakładka „Reboot“

Reboot

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

W celu przeprowadzenia restartu switcha należy wykonać następujące kroki:

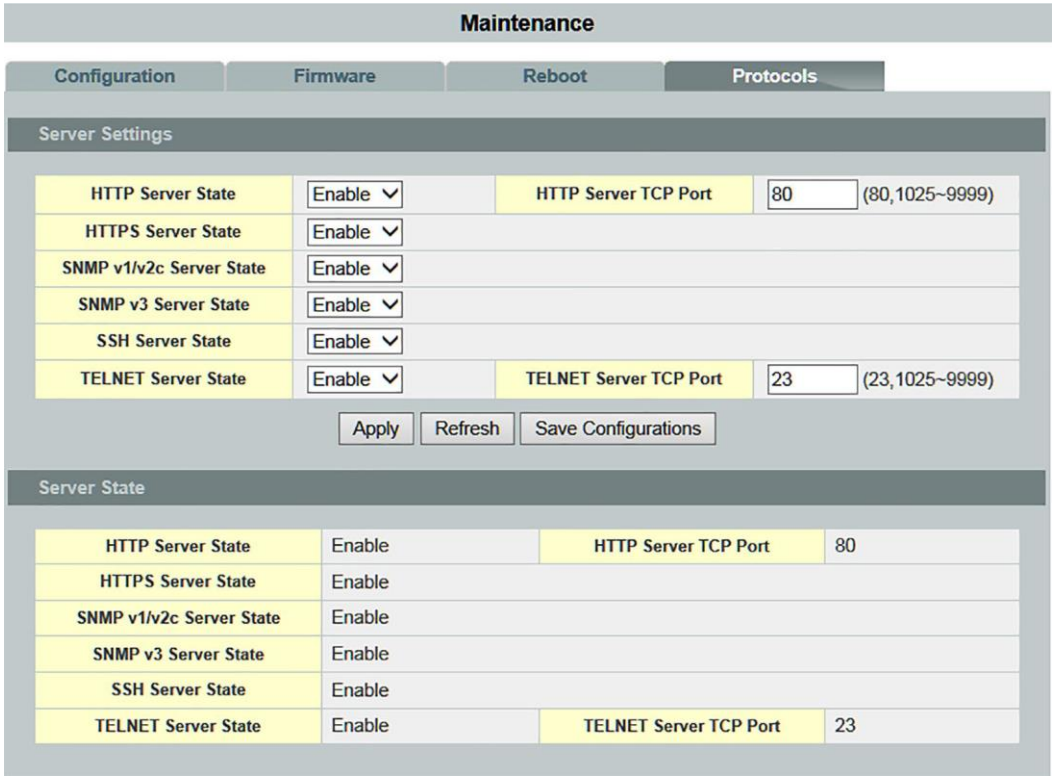
1. W menu „Reboot“ kliknij przycisk **[Reboot]**. Pojawi się widoczne niżej okno.



Ilustracja 99: Strona WBM „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.

10.7.2.4 Protocols



Ilustracja 100: Strona WBM „Maintenance“ – zakładka „Protocols“

Tabela 112: Strona WBM „Maintenance“ – zakładka „Protocols“

Server Settings		
Parametr	**Domyślnie**	**Opis**
HTTP Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „HTTP Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „HTTP Server“.
HTTP Server TCP Port (80, 1025~9999)	**80** 1025 … 9999	W polu edycji należy wpisać „HTTP Server TCP Port“.
HTTPS Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „HTTPS Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „HTTPS Server“.
SNMP v1/v2c Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „SNMP v1/v2c Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „SNMP v1/v2c Server“.
SNMP v3 Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „SNMP v3 Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „SNMP v3 Server“.
SSH Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „SSH Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „SSH Server“.
Telnet Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „Telnet Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „Telnet Server“.
Telnet Server TCP Port (23, 1025~9999)	**23** 1025 … 9999	W polu edycji należy wpisać „Telnet Server TCP Port“.
Server State		
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“.
HTTPS 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 State	Enable Disable	W tym polu wyświetlany jest status serwera Telnet.
Telnet Server TCP Port	23 1025 … 9999	W tym polu wyświetlany jest status „Telnet Server TCP Port“.

10.7.3 System Log

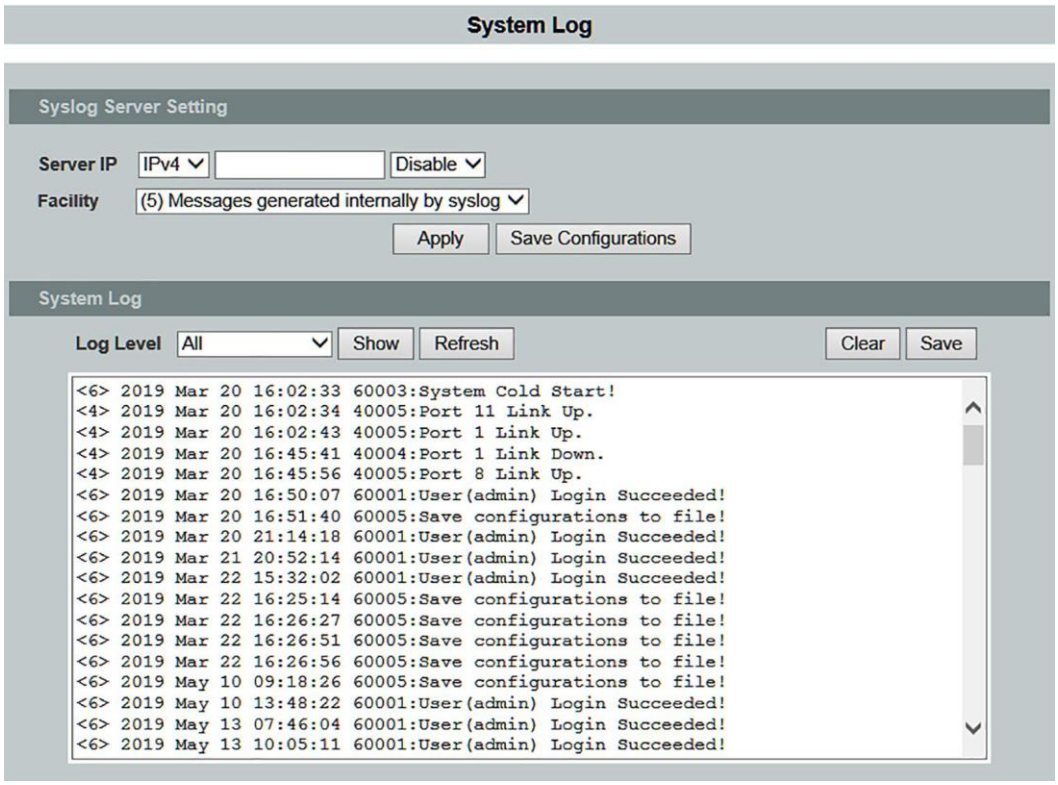
Funkcja „syslog“ zapisuje różne informacje systemowe dla funkcji „Debugging“. Każdy wpis w protokole rejestruje jeden z następujących poziomów:
- Alert
- Critical
- Error
- Warning
- Notice
- Information

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.

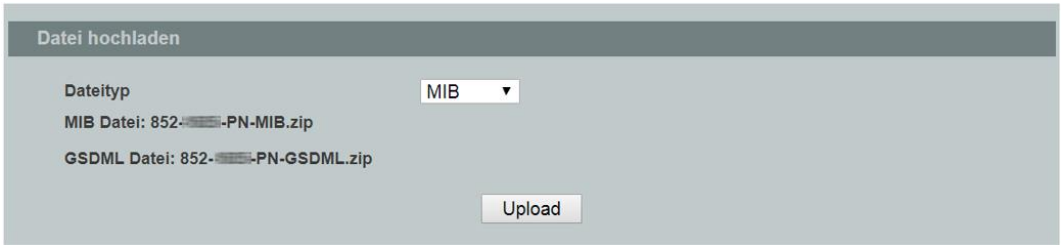


Ilustracja 101: Strona WBM „System Log“

Tabela 113: Strona WBM „System Log“

Syslog Server Settings		
Parametr	**Domyślnie**	**Opis**
Server IP Address	**IPv4**	W polu wyboru należy wybrać „IPv4“, gdy ma być wykorzystana ta wersja protokołu internetowego.
	IPv6	W polu wyboru należy wybrać „IPv6“, gdy ma być wykorzystana ta wersja protokołu internetowego.
		W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami (np.: 192.168.1.1).
	Disable	W polu wyboru należy wybrać „Disable“, aby switch nie wysyłał wszystkich nowych komunikatów dziennika zdarzeń do serwera „syslog“.
	Enable	W polu wyboru należy wybrać „Einable“, aby switch wysyłał wszystkie nowe komunikaty dziennika zdarzeń do serwera „syslog“.
Ustawienie	(1) User-level messages	W polu wyboru należy wybrać „(1) User-level messages“, aby wyświetlić komunikaty dziennika zdarzeń.
	(5) Messages generated internally by syslogd	W polu wyboru należy wybrać „(5) Messages generated internally by syslogd“, by wyświetlić wygenerowane wewnętrznie komunikaty „syslog“.
	(14) Log alert	
	(16) Local use 0	
	(17) Local use 1	
	(18) Local use 2	
	(19) Local use 3	
	(20) Local use 4	
	(21) Local use 5	
	(22) Local use 6	
	(23) Local use 7	
System Log		
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.

10.7.4 Upload File

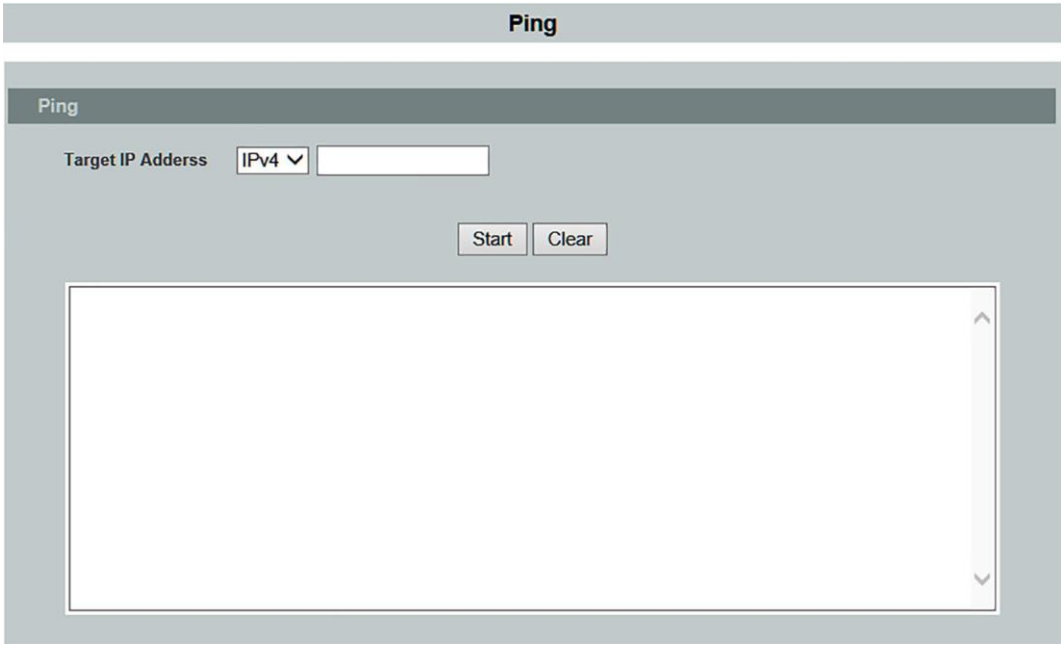


Ilustracja 102: Strona WBM „Upload File”

Tabela 114: Strona WBM „Upload File”

Parametr	Domyślnie	Opis
File Type	**MIB**	Wybór, czy do WMB ma być załadowany plik MIB czy GSDML

10.7.5 Ping



Ilustracja 103: Strona WBM „Ping“

Tabela 115: Strona WBM „Ping“

Parametr	Domyślnie	Opis
Target IP Address	–	Wpisanie adresu docelowego

10.7.6 User Account

Switch umożliwia utworzenie maksymalnie sześciu kont użytkownika. Nazwa użytkownika i hasło muszą 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.

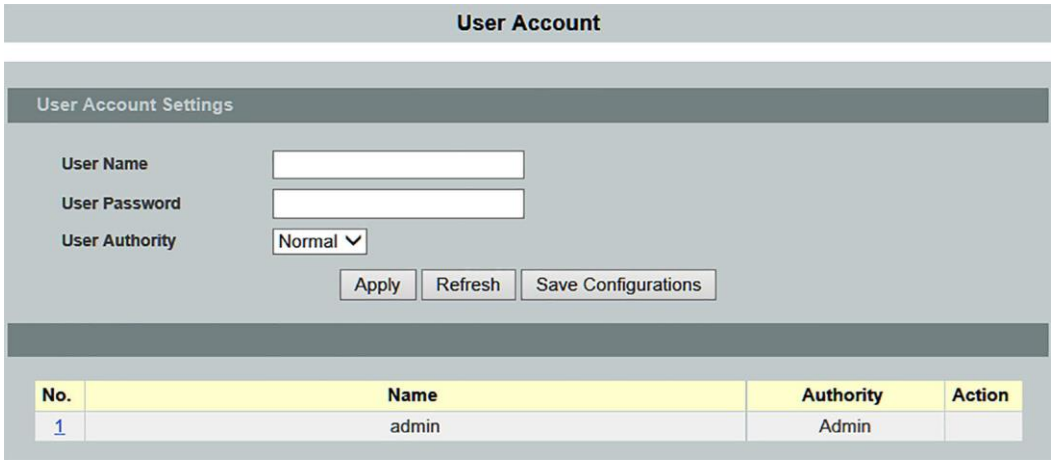
Uprawnienia użytkowników

Switch wspiera dwa rodzaje kont użytkownika:

Domyślne konta użytkownika zawierają następujące informacje:
Wersja firmware'u 01: 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.

Ponadto switch wspiera konto użytkownika „Backdoor“. Jeśli użytkownik zapomniał swoją nazwę użytkownika lub swoje hasło, switch może utworzyć konto „Backdoor“ z adresem MAC systemu. Dzięki temu użytkownik może się zalogować i utworzyć nowe konto.



Ilustracja 104: Strona WBM „User Account”

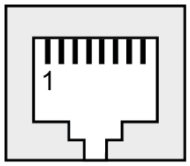
Tabela 116: Strona WBM „User Account”

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.
	Normal	W polu wyboru należy wybrać „Normal“, jeśli 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.
No.		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlany jest numer indeksu wpisu.
Name		W tej kolumnie wyświetlana jest nazwa konta użytkownika.
User Authority		W tej kolumnie wyświetlany jest rodzaj konta użytkownika.
Action		Aby usunąć konto użytkownika, należy kliknąć przycisk **[Delete]**.
		Wskazówka  **Usuwanie konta administratora** Ostatniego konta administratora nie można usunąć.

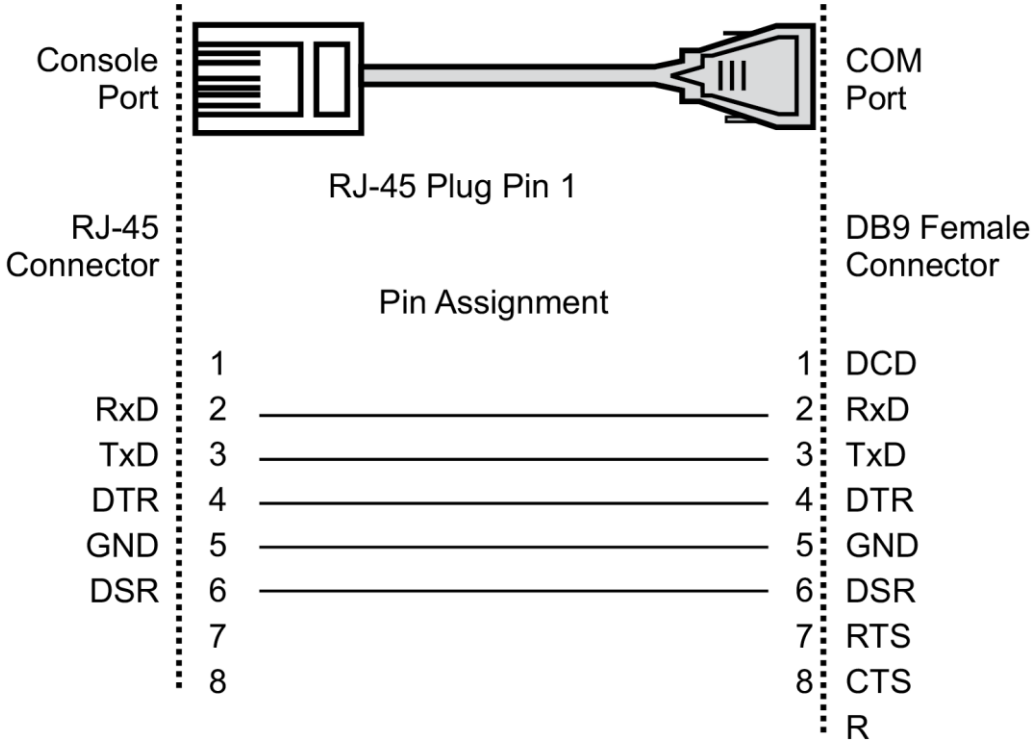
11 Załącznik

11.1 Przewód konsolowy (RJ-45 do DB9)

Do połączenia złącza konsolowego przemysłowego switcha zarządzalnego ze złączem COM należy użyć załączonego przewodu konsolowego. Obłożenie zacisków jest następujące:



Ilustracja 105: Obłożenie zacisków RJ-45



Ilustracja 106: Obłożenie zacisków RJ-45 do DB9

11.2 Przewód RJ-45

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

Tabela 117: Przewód RJ-45

Styk	Objaśnienie		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
Przemysłowy switch zarządzający oferuje na złączu RJ-45 takie funkcje jak „Autocrossing“ i „Autonegotiation“.

11.3 Configuring in the Command Line Interface (CLI) (dostęp przez konsolę (CLI))

11.3.1 System Status

11.3.1.1 System Information

Table 118: 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 addressA.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
acl	show	This command displays the current access control profile.
vlan	show	This command displays the current VLAN configurations.
enable	show hostname	This command displays the system’s network name.
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 loading and memory information.
enable	show uptime	This command displays the system uptime.

11.3.2 Basic Settings

11.3.2.1 System

Table 119: CLI “System” Configuration

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

11.3.2.1.1 Jumbo Frame

Table 120: CLI “Jumbo Frame” Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240|1522|1536|1552|9216)	This command configures the maximum number of bytes of frame size for all ports.

11.3.2.1.2 SNTP

Table 121: CLI “SNTP” Configuration

Node	Command	Description
enable	show time	This command displays the current time and date configuration.
configure	time HOUR:MINUTE:SECOND	This command sets the current time of the switch. hour: 0-23 min: 0-59 sec: 0-59 Note: If you configure daylight saving time after you configure the date and time, the switch uses daylight saving time.
configure	time date YEAR/MONTH/DAY	This command sets the current date of the switch. year: 1970– month: 1–12 day: 1–31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving time on the switch.
configure	time daylight-saving-time start-date (first|second|third|fourth|last) (Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday) MONTH HOUR	This command sets the start date of daylight saving time.
configure	time daylight-saving-time end-date (first|second|third|fourth|last) (Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday) MONTH HOUR	This command sets the end date of daylight saving time.
configure	time ntp-server (disable|enable)	This command disables/enables the NTP server settings.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of the time server.
configure	time 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*

11.3.2.1.3 Management Host

Table 122: 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*

11.3.2.2 MAC Management

Table 123: CLI “MAC Management” Configuration

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

Example

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

11.3.2.3 Port Mirroring

Table 124: CLI “Port Mirroring” Configuration

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

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#mirror enable*

L2SWITCH(config)*#mirror destination port 2*

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

11.3.2.4 Port Settings

Table 125: CLI “Port Settings” Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none|mac)	This command tests the loopback mode of operation for the specific port.
interface	Flow control (off|on)	This command disables/enables the flow control for the port.
interface	speed (auto|10-full||10-half100-full|100-half)	This command configures the speed and duplex mode for a port.
interface	shutdown	This command disables a specific port.
interface	no shutdown	This command enables a specific port.
interface	description STRINGs	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
interface	cable test start	This command starts to diagnostics the Ethernet cable.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto|10-full||10-half|100-full|100-half|1000-full)	This command configures the speed and duplex for the port.

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config-if)#*speed auto*

11.3.3 Advanced Settings

11.3.3.1 Bandwidth Control

11.3.3.1.1 QoS

Table 126: CLI “QoS” Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the “Service Queue”.
enable	show qos mode	This command displays the current IEEE 802.1p QoS mode.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping of the “Service Queue”.
configure	no queue cos-map	This command configures the default settings for the 802.1p priority mapping of the “Service Queue”.
configure	qos mode high-first	This command sets the QoS mode to “high_first” so every “Hardware Queue” transmits all packets in its buffer before permitting the next lower priority queue to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command sets the QoS mode to “Weighted Round Robin”.
interface	default-priority	This command allows the user to specify which priority is assigned by default to the untagged packets received by the switch. The priority value entered with this command is used to determine which of the “Hardware Priority Queues” the packet is forwarded to. Default: 0.
interface	no default-priority	This command sets the default priority for the specific port to 0.
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable|enable)	This command disables/enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

11.3.3.1.2 Rate Limitation

Table 127: CLI “Rate Limitation” Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current “Rate Limitation” configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the rate limitation for outgoing packets and sets the limit.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the rate limitation for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the rate limitation for incoming packets and sets the limit.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the rate limitation for incoming packets.

Example

L2SWITCH#*configure terminal*

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

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

11.3.3.1.2.1 Storm Control

Table 128: CLI “Storm Control” Configuration

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

Example

L2SWITCH#*configure terminal*

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

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

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

11.3.3.2 IGMP Snooping

Table 129: CLI “IGMP Snooping” Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current “IGMP Snooping” configurations.
enable	show igmp-snooping counters	This command displays the current IGMP snooping counters.
enable	show igmp-snooping querier	This command displays the current IGMP Queriers.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears all of the IGMP snooping counters.
configure	igmp-snooping (disable|enable)	This command disables/enables “IGMP Snooping” on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables “IGMP Snooping” on a VLAN or VLAN range.
configure	no igmp-snooping vlan VLAN_ID	This command disables “IGMP Snooping” on a VLAN or VLAN range.
configure	igmp-snooping unknown-multicast(drop|flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled.
configure	igmp-snooping report-suppression (disable|enable)	This command disables/enables the “IGMP Snooping Report Suppression” function on the switch.
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port|vlan)	This command clears the IGMP snooping counters for port or vlan.
interface	igmp-querier-mode (auto|fixed|edge)	This command specifies if and under what conditions the ports are “IGMP Query Ports”. The switch forwards the “IGMP Join/Leave” packets to an “IGMP Query Port,” treating the port as if it were connected to an IGMP multicast router (or server). “IGMP Snooping” must also be enabled (default: “Auto”).
interface	igmp-immediate-leave	The command enables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.
interface	no igmp-immediate-leave	The command disables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.
interface	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific interface.
interface	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific interface.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific ports.
if-range	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific ports.

Table 129: CLI “IGMP Snooping” Configuration

Node	Command	Description
if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the ports are IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Domyślnie:auto)

Example

L2SWITCH(config)#*igmp-snooping enable*

L2SWITCH(config)#*igmp-snooping vlan 1*

L2SWITCH(config)#*igmp-snooping querier enable*

L2SWITCH(config)#*igmp-snooping querier vlan 1*

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

L2SWITCH(config-if)#*igmp-immediate-leave*

L2SWITCH(config-if)# *igmp-querier-mode fixed*

L2SWITCH(config-if)# *igmp-snooping group-limit 20*

11.3.3.2.1 IGMP Snooping Querier♠

Table 130: CLI “IGMP Snooping Querier” Configuration

Node	Command	Description
configure	igmp-snooping querier (disable|enable)	This command disables/enables the IGMP snooping querier on the Switch.
configure	igmp-snooping querier vlan VLANIDs	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANIDs	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.

11.3.3.2.2 IGMP Snooping Filtering

Table 131: CLI “IGMP Snooping Filtering” Configuration

Node	Command	Description
enable	show igmp-snooping filtering	This command displays the IGMP snooping filtering configurations.
configure	igmp-snooping filtering (enable|disable)	This command enables/disables the IGMP snooping filtering profiles on the Switch.
configure	igmp-snooping filtering profile	This command enters the IGMP snooping filtering profiles configuration node.
configure	no igmp-snooping filtering all	This command removes all of the IGMP snooping filtering profiles from the Switch.
configure	no igmp-snooping filtering STRINGS	This command removes the IGMP snooping filtering profiles by name from the Switch.
config-igmp	Group GROUP_ID start-address START-ADDR end-address END-ADDR	This command configures the group configurations, including group index and start multicast address and end multicast address.
config-igmp	type (deny|permit)	This command configures the type of deny or permit for the group.
config-igmp	no group GROUP-ID	This command removes the group configurations.
config-igmp	no group all	This command removes all of the group configurations.
config-igmp	type (deny|permit)	This command configures the type of deny or permit for the group.
interface	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the specific port.
interface	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-config	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the range of ports.
if-config	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the range of ports.

11.3.3.3 Multicast Address

Table 132: CLI “Multicast Address” Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan VLANID	This command displays the current static/dynamic multicast address entries with a specific vlan.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command deletes a static multicast entry from the address table.

11.3.3.4 VLAN

11.3.3.4.1 Port Isolation

Table 133: CLI “Port Isolation” Configuration

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

Example

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

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

11.3.3.4.2 VLAN Settings

Table 134: CLI “VLAN Settings” Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1–4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1–4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be a combination of numbers, letters, hyphens (-) and underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command resets the VLAN name to the default setting. Note: The default VLAN name is comprised as follows: “VLAN”+VLAN_ID, VLAN1, VLAN2, …
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORT_LIST	This command assigns ports to a VLAN group as fixed subscribers.
vlan	no fixed PORTLISTS	This command deletes all fixed ports from a VLAN.
vlan	tagged PORT_LIST	This command assigns fixed ports to a VLAN group as tagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no tagged PORTLISTS	This command deletes all permanently assigned tagged ports from a VLAN.
vlan	untagged PORT_LIST	This command assigns fixed ports to a VLAN group as untagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no untagged PORTLISTS	This command deletes all untagged ports from a VLAN.
interface	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. All – acceptable all frame types. tagged – acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.

Table 134: CLI “VLAN Settings” Configuration

Node	Command	Description
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*vlan 2*

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

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

11.3.3.4.3 MAC VLAN

Table 135: CLI “MAC VLAN” Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Example

L2SWITCH(config)# *mac-vlan 00:01:02:03:04vlan 111 priority 1*

L2SWITCH(config)# *mac-vlan 00:01:02:22:04vlan 121 priority 1*

L2SWITCH(config)# *mac-vlan 00:01:22:22:04:05 vlan 221 priority 1*

11.3.3.5 LLDP

Table 136: CLI “LLDP” Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all the information of the port neighbors.
configure	lldp (disable|enable)	This command globally enables/disables the LLDP function on the switch.
configure	lldp tx-interval	This command configures the transmission interval for LLDP packets.
configure	lldp tx-hold	This command configures the “tx-Hold Time” that determines the TTL of the switch message. (TTL = tx-hold * tx-interval)
interface	lldp-agent (disable|enable|rx-only|tx-only)	This command configures the Agent function for LLDP. “disable”: LLDP is disabled for a specific port. “enable”: The LLDP packet is transmitted on a specific port and received. “tx-only”: The LLDP packet is only transmitted on a specific port. “rx-only”: The LLDP packet is only received on a specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	lldp-agent (disable|enable|rx-only|tx-only)	This command configures the LLDP agent function. “disable”: Disable the LLDP on the specific port. “enable” Transmit and Receive the LLDP packet on the specific port. “tx-only” Transmit the LLDP packet on the specific port only. “rx-only” Receive the LLDP packet on the specific port.

11.3.3.6 Loop Detection

Table 137: CLI “Loop Detection” Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable|enable)	This command disables/enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default. (00:0b:04:AA:AA:AB)
interface	loop-detection (disable|enable)	This command disables/enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable|enable)	This command enables/disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable|enable)	This command disables/enables the loop detection on the ports.
if-range	loop-detection recovery (disable enable)	This command enables/disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example

L2SWITCH(config)#*loop-detection enable*

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

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

11.3.3.7 MRP

Table 138: CLI “MRP” Configuration

Node	Command	Description
enable	show mrp information	This command displays the overall mrp’s configured information and also global mrp settings
enable	show mrp ring-id [RING_ID]	This command displays the mrp information of the specific
configure	mrp enable	This command enables the media redundancy protocol on the switch.
configure	no mrp enable	This command disables media redundancy protocol on the switch.
configure	Mrp ring-id <1-4>	This command creates the particular ring with mentioned ID
enable	show mrp information	This command displays the overall mrp’s configured information and also global mrp settings
enable	show mrp ring-id [RING_ID]	This command displays the mrp information of the specific
configure	mrp enable	This command enables the media redundancy protocol on the switch.
configure	no mrp enable	This command disables media redundancy protocol on the switch.
configure	Mrp ring-id <1-4>	This command creates the particular ring with mentioned ID
configure-mrp	ring uuid	This command configures the universal unique identifier (UUID) for the ring. It’s a string in hexadecimal format representing the ring to which this switch belongs to. ex: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
configure-mrp	no ring enable	This command disables the particular ring
configure-mrp	no ring mode	This command removes the node mode.
configure-mrp	no ring port-1	This command removes the port-1 for the ring on the Switch.
configure-mrp	no ring port-2	This command removes the port-2 for the ring on the Switch.
configure-mrp	no ring vlan	This command removes the ring on that VLAN.
configure-mrp	no ring uuid	This command removes the universal unique identifier (UUID) for the ring.

11.3.3.8 STP

Table 139: CLI “STP” Configuration

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

Table 139: CLI “STP” Configuration

Node	Command	Description
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	spanning-tree(disable|enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdufilter(disable|enable)	This command configures enables/disables the bpdu filter function for the specific port.
if-range	spanning-tree bpduguard(disable|enable)	This command configures enables/disables the bpdu guard function for the specific port.
if-range	spanning-tree rootguard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port(disable|enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
if-range	no spanning-tree cost	This command configures the path cost to default for the specific port.
if-range	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

11.3.4 Security

11.3.4.1 Access Control List

Table 140: 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.
configure	no access-list STRING	This command deletes an access control profile.
acl	Show	This command displays the current access control profile.
acl	action (disable|drop|permit)	This command processes this profile. “disable”: The profile is disabled. “drop”: If packets match the profile, they are dropped. “permit”: If packets match the profile, they are forwarded.
acl	destination mac hostMACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source AMC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.

Table 140: CLI “Access Control List” Configuration

Node	Command	Description
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Example:

L2SWITCH#*configure terminal*

L2SWITCH(config)#*access-list 111*

L2SWITCH(config-acl)#*vlan 2*

L2SWITCH(config-acl)#*source interface 1*

L2SWITCH(config-acl)#*show*

11.3.5 Monitor

11.3.5.1 Alarm

Table 141: CLI “Alarm” Configuration

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

11.3.5.2 Monitor Information

Table 142: CLI “Monitor Information” Configuration

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

11.3.5.3 Port Statistics

Table 143: CLI “Port Statistics” Configuration

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

11.3.5.4 Port Utilization

Table 144: CLI “Port Statistics” Configuration

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

11.3.5.5 RMON Statistics

Table 145: CLI “RMON Statistics” Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears the RMON statistics for one or all ports.

11.3.5.6 SFP Information

Table 146: 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.

11.3.5.7 Traffic Monitor

Table 147: CLI “Traffic Monitor” Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the “Traffic Monitor” configurations and current status.
configure	traffic-monitor (disable|enable)	This command enables/disables the “Traffic Monitor” on the switch.
interface	traffic-monitor (disable|enable)	This command enables/disables the “Traffic Monitor” on a specific port.
interface	traffic-monitor rate RATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and type for the “Traffic Monitor” on a specific port. mcast: broadcast packet mcast: multicast packet The rate should be greater than 50 pps.
interface	traffic-monitor recovery (disable|enable)	This command enables/disables the “Recover” function for the “Traffic Monitor” on a specific port.
interface	traffic-monitor recovery time VALUE	This command configures the “Recovery Time” for the “Traffic Monitor” on a specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	traffic-monitor (disable|enable)	This command enables/disables the traffic monitor on the port.
if-range	traffic-monitor rateRATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.
if-range	traffic-monitor recovery (disable|enable)	This command enables/disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.

11.3.6 Management

11.3.6.1 SNMP

11.3.6.1.1 SNMP

Table 148: CLI “SNMP” Configuration

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

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*snmp enable*

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

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

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

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

11.3.6.1.2 SNMP Trap

Table 149: CLI “SNMP Trap” Configuration

Node	Command	Description
enable	show snmp trap-event	This command displays the SNMP configurations.
configure	snmp trap-event alarm-over-heat (disable/enable)	This command enables/disables the alarm-over-heat trap.
configure	snmp trap-event alarm-over-load (disable/enable)	This command enables/disables the alarm-over-load trap.
configure	snmp trap-event alarm-power-fail (enable/enable)	This command enables/disables the alarm-power-fail trap.
configure	snmp trap-event bpdu (disable/enable)	This command enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap.
configure	snmp trap-event dual-homing (disable/enable)	This command enables/disables the dual-homing trap.
configure	snmp trap-event dying-gasp (disable/enable)	This command enables/disables the dying-gasp trap.
configure	snmp trap-event loop-detection (disable/enable)	This command enables/disables the loop-detection trap.
configure	snmp trap-event pd-alive (disable/enable)	This command enables/disables the pd-alive trap.
configure	snmp trap-event port-admin-state-change (disable/enable)	This command enables/disables the port-admin-state-change trap.
configure	snmp trap-event port-link-change (disable/enable)	This command enables/disables the port-link-change trap.
configure	snmp trap-event power-source-change (disable/enable)	This command enables/disables the power-source-change trap.
configure	snmp trap-event stp-topology-change (disable/enable)	This command enables/disables the stp-topology-change trap.
configure	snmp trap-event traffic-monitor (disable/enable)	This command enables/disables thetraffic-monitor trap.
configure	snmp trap-event xpress-ring (disable/enable)	This command enables/disables the xpress-ring trap.

11.3.6.1.2.1 Port Trap Settings

Table 150: CLI “Port Trap Settings” Configuration

Node	Command	Description
enable	show snmp port-link-change-trap	This command displays the SNMP port link-change trap configurations.
interface	snmp port-link-change-trap	This command enables the link change trap on the specific port.
interface	no snmp port-link-change-trap	This command disables the link change trap on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	snmp port-link-change-trap	This command enables the link change trap on the specific ports.
if-range	no snmp port-link-change-trap	This command disables the link change trap on the specific ports.

11.3.6.1.3 SNMPv3

Table 151: CLI “SNMPv3” Configuration

Node	Command	Description
enable	show snmp user	This command displays all snmp v3 users.
enable	show snmp group	This command displays all snmp v3 groups.
enable	show snmp view	This command displays all snmp v3 view.
configure	snmp user USERNAME GROUPNAME noauth	Configures v3 user of non- authentication.
configure	snmp user USERNAME GROUPNAME auth (MD5|SHA) STRINGS	Configures v3 user of authentication.
configure	snmp user USERNAME GROUPNAME priv (MD5|SHA) STRINGS des STRINGS	Configures v3 user osnmf authentication and encryption.
configure	snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non- authentication.
configure	snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication.
configure	snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	snmp view VIEWNAME STRINGS (included|excluded)	To identify the subtree.
configure	no snmp user USERNAME GROUPNAME	This command removes a v3 user from switch.
configure	no snmp group GROUPNAME	This command removes a v3 group from switch.
configure	no snmp view VIEWNAME STRINGS	This command removes a v3 view from switch.

11.3.6.2 Maintenance

Table 152: CLI “Maintenance” Configuration

Node	Command	Description
enable	show config-change-status	This command displays the configurations status if there are default values.
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. Note: The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw<URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface eth0*

L2SWITCH(config-if)#*ip address 172.20.1.101/24*

L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*

L2SWITCH(config-if)#*management vlan 1*

11.3.6.2.1 Reboot

Table 153: CLI “Reboot” Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	serwer WWW	This command enables the web on the Switch.
configure	brak web servera	This command disables the web on the Switch.

11.3.6.3 System Log

Table 154: CLI “System Log” Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	clear syslog	The command clears the syslog message.
configure	syslog-server (disable|enable)	The command disables/enables the syslog server function.
configure	syslog-server ipv4-ip IPADDR	The command configures the syslog server’s IP address in IPv4 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example

L2SWITCH#*configure terminal*

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

L2SWITCH(config)#*syslog-server enable*

11.3.6.4 User Account

Table 155: CLI “USB Flash” 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	This command deletes a present user account.

Example

L2SWITCH#*configure terminal*

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

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

Spis ilustracji

Ilustracja 1: Równoległe korzystanie ze standardu ETHERNET i PROFINET 20
Ilustracja 2: Widok przemysłowego switcha zarządzalnego z przodu 24
Ilustracja 3: Widok przemysłowego switcha zarządzalnego z góry 26
Ilustracja 4: Złącze zasilające (PWR/RPS).....27
Ilustracja 5: Złącza sieciowe.....28
Ilustracja 6: LED urządzeń 30
Ilustracja 7: LED dla złącz RJ-45.....31
Ilustracja 8: Mikroprzełączniki DIP.....32
Ilustracja 9: Przycisk resetu.....33
Ilustracja 10: Naklejka (przykład).....34
Ilustracja 11: Adresowanie danych I/O device przez sloty i subsloty.....41
Ilustracja 12: Mapowanie subslotów w switchu zarządzalnym PROFINET WAGO 42
Ilustracja 13: Relacje komunikacyjne w PROFINET 44
Ilustracja 14: Przegląd klas zgodności od A do C.....49
Ilustracja 15: Redundancja mediów w PROFINET (topologia pierścienia).....52
Ilustracja 16: Ogólna budowa pliku GSDML 58
Ilustracja 17: Parametry PROFINET – obszar „General” 66
Ilustracja 18: Parametry PROFINET – obszar „PROFINET interface [X1]” 67
Ilustracja 19: Parametry PROFINET – obszar „Advanced options”.....68
Ilustracja 20: Parametry PROFINET – obszar „Port 1” 70
Ilustracja 21: Parametry PROFINET – obszar „General” 71
Ilustracja 22: Parametry PROFINET – obszar „Identification & Maintenance“ 72
Ilustracja 23: Parametry PROFINET – obszar „Process alarms“ 73
Ilustracja 24: Parametry PROFINET – obszar „Assembly parameters“.....74
Ilustracja 25: Parametry PROFINET – obszar „IO adresses“.....76
Ilustracja 26: Dostęp do switcha zarządzalnego PROFINET przez WBM.....88
Ilustracja 27: Okno logowania do WBM.....90
Ilustracja 28: Strona WBM „System Information” 92
Ilustracja 29: Strona WBM „General Settings“ – zakładka „System“ 94
Ilustracja 30: Strona WBM „Port Mirroring“ 96
Ilustracja 31: Strona WBM „Port Settings“ – zakładka „General Settings“.....98
Ilustracja 32: Strona WBM „PROFINET Setting“.....99
Ilustracja 33: Strona WBM „Information“.....100
Ilustracja 34: Strona WBM „Diagnosis List” 101
Ilustracja 35: Strona WBM „MRP”.....102
Ilustracja 36: Strona WBM „Upload File”.....105
Ilustracja 37: Strona WBM „User Account” 105
Ilustracja 38: Diagram przebiegu tabeli adresów MAC 113
Ilustracja 39: Tryb half duplex.....115
Ilustracja 40: Tryb full duplex.....115
Ilustracja 41: Adres multicast.....130
Ilustracja 42: Strona WBM „System Information“.....154
Ilustracja 43: Strona WBM „General Settings“ – zakładka „System“ 156
Ilustracja 44: Strona WBM – zakładka „Jumbo Frame”.....158
Ilustracja 45: Strona WBM – zakładka „SNTP” 159
Ilustracja 46: Strona WBM – zakładka „Management Host”.....162

Ilustracja 47: Strona WBM – zakładka „Static MAC Settings” 163
Ilustracja 48: Strona WBM – zakładka „MAC Table” 165
Ilustracja 49: Strona WBM – zakładka „Age Time Setting” 166
Ilustracja 50: Strona WBM – zakładka „Blacklisting” 167
Ilustracja 51: Strona WBM – „Port Mirroring” 168
Ilustracja 52: Strona WBM „Port Settings“ – zakładka „General Settings“ 170
Ilustracja 53: Strona WBM „Port Settings” – zakładka „Information” 172
Ilustracja 54: Strona WBM „QoS” – zakładka „Port Priority” 173
Ilustracja 55: Strona WBM) „QoS” – zakładka „IP DiffServ (DSCP)” 174
Ilustracja 56: Strona WBM „QoS” – zakładka „Priority/Queue Mapping“ 175
Ilustracja 57: Strona systemu zarządzania przez WWW (WBM) „QoS” – zakładka „Schedule Mode” 176
Ilustracja 58: Strona WBM „Rate Limitation“ – zakładka „Strom Control“ 178
Ilustracja 59: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“ 180
Ilustracja 60: Strona WBM „IGMP Snooping“ – zakładka „General Settings“ 181
Ilustracja 61: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“ 183
Ilustracja 62: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings“ 185
Ilustracja 63: Strona WBM „IGMP Filtering“ – zakładka „General Settings“ 186
Ilustracja 64: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“ 187
Ilustracja 65: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“ 188
Ilustracja 66: Strona WBM „Static Multicast“ 189
Ilustracja 67: Strona WBM „Multicast Statistics“ 190
Ilustracja 68: Strona WBM „Port Isolation“ 191
Ilustracja 69: Strona WBM „VLAN“ – zakładka „VLAN Settings“ 193
Ilustracja 70: Strona WBM „VLAN“ – zakładka „Tag Settings“ 195
Ilustracja 71: Strona WBM „VLAN“ – zakładka „Port Settings“ 196
Ilustracja 72: Strona WBM „MAC VLAN“ 198
Ilustracja 73: Strona WBM „LLDP“ – zakładka „LLDP Settings“ 199
Ilustracja 74: Strona WBM „LLDP“ – zakładka „Neighboring Detection“ 201
Ilustracja 75: Strona WBM „Loop Detection” 202
Ilustracja 76: Strona WBM „MRP Global Settings“ 204
Ilustracja 77: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“ 207
Ilustracja 78: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“ 209
Ilustracja 79: Strona WBM „Spanning Tree Protocol“ – zakładka „STP Status“ 212
Ilustracja 80: Strona WBM „Access Control List“ 213
Ilustracja 81: Strona WBM „Alarm Information“ 217
Ilustracja 82: Strona WBM „Monitor Information” 218
Ilustracja 83: Strona WBM „Port Statistics“ 220
Ilustracja 84: Strona WBM „Port Utilization“ 221
Ilustracja 85: Strona WBM „RMON Statistics“ 222
Ilustracja 86: Strona WBM „SPF Information“ 225
Ilustracja 87: Strona WBM „Traffic Monitor“ 228
Ilustracja 88: Strona WBM „SNMP“ – zakładka „SNMP Settings“ 230
Ilustracja 89: Strona WBM „SNMP“ – zakładka „Community Name“ 231
Ilustracja 90: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“ .233
Ilustracja 91: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“ 234
Ilustracja 92: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“ 235

Ilustracja 93: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“ 236
Ilustracja 94: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“ 238
Ilustracja 95: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“ 239
Ilustracja 96: Strona WBM „Maintenance“ – zakładka „Configuration“ 240
Ilustracja 97: Strona WBM „Maintenance“ – zakładka „Firmware“ 242
Ilustracja 98: Strona WBM „Maintenance“ – zakładka „Reboot“.....243
Ilustracja 99: Strona WBM „Maintenance“ – zakładka „Reboot“ – Message 243
Ilustracja 100: Strona WBM „Maintenance“ – zakładka „Protocols“ 244
Ilustracja 101: Strona WBM „System Log“.....246
Ilustracja 102: Strona WBM „Upload File”.....248
Ilustracja 103: Strona WBM „Ping“ 249
Ilustracja 104: Strona WBM „User Account” 250
Ilustracja 105: Obłożenie zacisków RJ-45 252
Ilustracja 106: Obłożenie zacisków RJ-45 do DB9 252

Spis tabel

Tabela 1: Zastosowane systemy liczbowe....12
Tabela 2: Sposoby zapisu....12
Tabela 3: Opis do ilustracji „Widok przemysłowego switcha zarządzalnego z przodu”....24
Tabela 4: Opis do ilustracji „Widok przemysłowego switcha zarządzalnego z góry” 26
Tabela 5: Opis ilustracji „Złącze zasilające (PWR/RPS)” 27
Tabela 6: Opis ilustracji „Złącza sieciowe”....28
Tabela 7: Opis ilustracji „LED urządzeń“ 30
Tabela 8: Opis ilustracji „LED dla złącz RJ-45”....31
Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“....32
Tabela 10: Opis ilustracji „Przycisk resetu“....33
Tabela 11: Opis ilustracji „Naklejka (przykład)“....34
Tabela 12: Dane techniczne – dane urządzenia....35
Tabela 13: Dane techniczne – dane systemowe 35
Tabela 14: Dane techniczne – zasilanie 35
Tabela 15: Dane techniczne – komunikacja 36
Tabela 16: Dane techniczne – Warunki środowiskowe....37
Tabela 17: Przykłady Provider i Consumer....39
Tabela 18: Adresowanie danych w zależności od typu transmisji....41
Tabela 19: Obszary w telegramie PROFINET 47
Tabela 20: Porównanie klas zgodności 51
Tabela 21: Opis ilustracji „Redundancja mediów w PROFINET (topologia pierścienia)“ 52
Tabela 22: Przegląd narzędzi projektowych 62
Tabela 23: Parametry PROFINET dla obszaru „General”....67
Tabela 24: Parametry PROFINET dla obszaru „PROFINET interface [X1]”....68
Tabela 25: Parametry PROFINET dla obszaru „Advanced options” 69
Tabela 26: Parametry PROFINET® dla obszaru „Port 1” 70
Tabela 27: Parametry PROFINET dla obszaru „Advanced options” 71
Tabela 28: Parametry PROFINET dla obszaru „Identification & Maintenance“ ...72
Tabela 29: Parametry PROFINET dla obszaru „Process alarms“ 73
Tabela 30: Parametry PROFINET dla obszaru „Assembly parameters“ 75
Tabela 31: Parametry PROFINET dla obszaru „IO adresses“ 76
Tabela 32: Format cyklicznych danych I/O – PROFINET 78
Tabela 33: Cykliczne wejście dla diagnostyki urządzenia....78
Tabela 34: Cykliczne wejście dla stanu portu Pn (n = 1 … 12)....80
Tabela 35: Parametry DAP dla switcha PROFINET WAGO 81
Tabela 36: Aktywacja/dezaktywacja komunikatów diagnostycznych 81
Tabela 37: Odczyt statusu portu (dla każdego portu) 82
Tabela 38: Odczyt diagnostyki urządzenia 83
Tabela 39: Konfiguracja funkcji mirroringu portu....84
Tabela 40: Domyślne ustawienia dla portu konsolowego 85
Tabela 41: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM)....91
Tabela 42: Strona WBM „System Information” (przykład 852-1605 możliwy do przeniesienia na 852-0602, -0603). 93

Tabela 43: Strona WBM „General Settings“ – zakładka „System“ 95
Tabela 44: Strona WBM „Port Mirroring“ 97
Tabela 45: Strona WBM „PROFINET Setting“.....99
Tabela 46: Strona WBM „MRP”.....103
Tabela 47: Strona WBM „Upload File”.....105
Tabela 48: Strona WBM „User Account”.....105
Tabela 49: Poziomy priorytetu.....121
Tabela 50: Klasy multicast i zakresy adresów 129
Tabela 51: Adres IP multicast.....130
Tabela 52: Koszty trasy STP 139
Tabela 53: Domyślne ustawienia dla portu Telnet 149
Tabela 54: Domyślne ustawienia dla portu konsolowego 150
Tabela 55: Ekran logowania 150
Tabela 56: Przegląd – linki do nawigacji i strony systemu zarządzania przez WWW (WBM).....152
Tabela 57: Strona WBM „System Information“ 155
Tabela 58: Strona WBM „General Settings“ – zakładka „System“ 157
Tabela 59: Strona WBM – zakładka „Jumbo Frame” 158
Tabela 60: Strona WBM – zakładka „SNTP” 160
Tabela 61: Strona WBM – zakładka „Management Host” 162
Tabela 62: Strona WBM – zakładka „Static MAC Settings” 164
Tabela 63: Strona WBM – zakładka „MAC Table” 165
Tabela 64: Strona WBM „MAC Management” – zakładka „Age Time Setting” ..166
Tabela 65: Strona WBM – zakładka „Blacklisting” 167
Tabela 66: Strona WBM – „Port Mirroring” 169
Tabela 67: Strona WBM – zakładka „Port Settings” – zakładka „General Settings” 171
Tabela 68: Strona WBM „Port Settings” – zakładka „Information”.....172
Tabela 69: Strona WBM „QoS” – zakładka „Port Priority” 173
Tabela 70: Strona WBM „QoS” – zakładka „IP DiffServ (DSCP)” 174
Tabela 71: Strona WBM „QoS“ – zakładka „Priority/Queue Mapping“ 175
Tabela 72: Default Settings 175
Tabela 73: Strona WBM „QoS“ – zakładka „Schedule Mode“.....177
Tabela 74: Strona WBM „Rate Limitation“ – zakładka „Storm Control“ 179
Tabela 75: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“ ..180
Tabela 76: Strona WBM „IGMP Snooping“ – zakładka „General Settings“ 182
Tabela 77: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“ 184
Tabela 78: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings 185
Tabela 79: Strona WBM „IGMP Filtering“ – zakładka „General Settings“.....186
Tabela 80: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“.....187
Tabela 81: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“.....188
Tabela 82: Strona WBM „Static Multicast“ 189
Tabela 83: Strona WBM „Multicast Statistics“.....190
Tabela 84: Strona WBM „Port Isolation“ 192
Tabela 85: Strona WBM „VLAN“ – zakładka „VLAN Settings“ 194
Tabela 86: Strona WBM „VLAN“ – zakładka „Tag Settings“ 195
Tabela 87: Strona WBM „VLAN“ – zakładka „Port Settings“ 197
Tabela 88: Strona WBM „MAC VLAN“.....198
Tabela 89: Strona WBM „LLDP“ – zakładka „LLDP Settings“ 200
Tabela 90: Strona WBM „LLDP“ – zakładka „Neighboring Detection“.....201

Tabela 91: Strona WBM „Loop Detection” 203
Tabela 92: Strona WBM „MRP” 205
Tabela 93: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“ 208
Tabela 94: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“ 210
Tabela 95: Strona WBM „STP“ – zakładka „STP-Status“ 212
Tabela 96: Strona WBM „Access Control List“ 214
Tabela 97: Strona WBM „Alarm Information“ 217
Tabela 98: Strona WBM „Monitor Information“ 219
Tabela 99: Strona WBM „Port Statistics“ 220
Tabela 100: Strona WBM „Port Utilization“ 221
Tabela 101: Strona WBM „RMON Statistics“ 223
Tabela 102: Strona WBM „SPF Information“ 226
Tabela 103: Strona WBM „Traffic Monitor” 229
Tabela 104: Strona WBM „SNMP“ – zakładka „SNMP Settings“ 230
Tabela 105: Strona WBM „SNMP“ – zakładka „Community Name“ 232
Tabela 106: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“ ..233
Tabela 107: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“ 234
Tabela 108: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“ 235
Tabela 109: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“ 237
Tabela 110: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“ 238
Tabela 111: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“ 239
Tabela 112: Strona WBM „Maintenance“ – zakładka „Protocols“ 245
Tabela 113: Strona WBM „System Log“ 247
Tabela 114: Strona WBM „Upload File” 248
Tabela 115: Strona WBM „Ping“ 249
Tabela 116: Strona WBM „User Account” 251
Tabela 117: Przewód RJ-45 253
Table 118: CLI “System Information” Configuration 254
Table 119: CLI “System” Configuration 255
Table 120: CLI “Jumbo Frame” Configuration 256
Table 121: CLI “SNTP” Configuration 256
Table 122: CLI “Management Host” Configuration 257
Table 123: CLI “MAC Management” Configuration 258
Table 124: CLI “Port Mirroring” Configuration 258
Table 125: CLI “Port Settings” Configuration 259
Table 126: CLI “QoS” Configuration 260
Table 127: CLI “Rate Limitation” Configuration 261
Table 128: CLI “Storm Control” Configuration 261
Table 129: CLI “IGMP Snooping” Configuration 263
Table 130: CLI “IGMP Snooping Querier” Configuration 265
Table 131: CLI “IGMP Snooping Filtering” Configuration 265
Table 132: CLI “Multicast Address” Configuration 266
Table 133: CLI “Port Isolation” Configuration 266
Table 134: CLI “VLAN Settings” Configuration 268
Table 135: CLI “MAC VLAN” Configuration 269

Table 136: CLI “LLDP” Configuration 270
Table 137: CLI “Loop Detection” Configuration....271
Table 138: CLI “MRP” Configuration 272
Table 139: CLI “STP” Configuration 274
Table 140: CLI “Access Control List” Configuration 277
Table 141: CLI “Alarm” Configuration 279
Table 142: CLI “Monitor Information” Configuration 279
Table 143: CLI “Port Statistics” Configuration....279
Table 144: CLI “Port Statistics” Configuration....279
Table 145: CLI “RMON Statistics” Configuration 279
Table 146: CLI “SFP Information” Configuration....279
Table 147: CLI “Traffic Monitor” Configuration....280
Table 148: CLI “SNMP” Configuration 281
Table 149: CLI “SNMP Trap” Configuration....282
Table 150: CLI “Port Trap Settings” Configuration....282
Table 151: CLI “SNMPv3” Configuration 283
Table 152: CLI “Maintenance” Configuration 284
Table 153: CLI “Reboot” Configuration....284
Table 154: CLI “System Log” Configuration....285
Table 155: CLI “USB Flash” Configuration 285

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