TECHDOCS

Podręcznik

WAGO-Industrial-Switches



852-1505/000-001

Industrial-Managed-Switch

8 Ports 1000BASE-T; 4 Slots 1000BASE-SX/LX; EXT; 8 x PoE; USB

Wersja 1.1.0

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

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

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

e-mail: info@wago.com

Internet: www.wago.com

Wsparcie techniczne

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

e-mail: support@wago.com

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

e-mail: documentation@wago.com

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

Znak WAGO jest zastrzeżonym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.

Spis treści

1 Wskazówki dotyczące dokumentacji 11
1.1 Zakres obowiązywania 11
1.2 Prawa autorskie 11
1.3 Symbol 12
1.4 Zastosowane systemy liczbowe 13
1.5 Sposoby zapisu 13

2 Ważne objaśnienia 14
2.1 Podstawy prawne 14
2.1.1 Zastrzeżenie prawa do zmian technicznych 14
2.1.2 Kwalifikacje personelu 14
2.1.3 Użytkowanie switcha przemysłowego zgodne z przeznaczeniem 14
2.1.4 Stan techniczny urządzeń 15
2.1.5 Dyrektywy i wymagania dla zastosowania switcha przemysłowego 15
2.2 Wskazówki dotyczące bezpieczeństwa 16
2.3 Specjalne warunki zastosowania urządzeń ETHERNET 18

3 Wprowadzenie 19
3.1 Zakres dostawy 19
3.2 Technologia sieci Industrial ETHERNET 19
3.3 Technologia switchingu 20
3.4 PoE (Power over Ethernet) 20
3.5 Autonegocjacja 20
3.6 Autocrossing 21
3.7 Tryb Store and Forward Switching 21
3.8 Metody transmisji 21

4 Opis urządzenia 22
4.1 Widok 23
4.1.1 Widok z przodu 23
4.1.2 Widok z góry 25
4.2 Złącza 26
4.2.1 Śruba uziemienia 26
4.2.2 Zasilanie (PWR/RPS) 27
4.2.3 Złącza sieciowe 28
4.2.3.1 Złącze RJ-45 29
4.2.3.2 Złącze USB 29
4.2.3.3 Złącza 10/100/1000BASE-T 29
4.2.3.4 Złącza 10/100/1000BASE-T z PoE+ 29
4.2.3.5 Złącza 1000BASE-SX/LX 30
4.3 Elementy sygnalizacyjne 31
4.3.1 LED urządzeń 31
4.3.2 LED złącz 32
4.4 Elementy obsługi 33
4.4.1 Mikroprzełączniki DIP 33
4.4.2 Przycisk resetu 34
4.5 Naklejka 35
4.5.1 Wersja sprzętu i oprogramowania 35

4.6 Parametry techniczne ... 36
4.6.1 Dane urządzenia ... 36
4.6.2 Dane systemowe ... 36
4.6.3 Zasilanie ... 36
4.6.4 Power over Ethernet (PoE) ... 36
4.6.5 Komunikacja ... 37
4.6.6 Warunki środowiskowe ... 38
4.7 Normy i dyrektywy ... 39
4.8 Aprobaty ... 40

5 Montaż ... 41

5.1 Miejsce montażu ... 41
5.2 Montaż na szynie ... 41
5.3 Demontaż z szyny ... 41

6 Podłączanie urządzeń ... 42

6.1 Zasilanie ... 42
6.2 Złącze zewnętrznego styku alarmowego ... 44
6.3 Złącze przewodu konsolowego ... 44
6.4 Porty 1000BASE-SX/LX, światłowód ... 45
6.5 Porty 10/100/1000BASE-T ... 46

7 Opis funkcji ... 47

7.1 Ustawienia podstawowe ... 47
7.1.1 Jumbo Frame ... 47
7.1.2 SNTP ... 47
7.1.3 Management Host ... 49
7.1.4 MAC Management ... 49
7.1.4.1 Static MAC ... 50
7.1.4.2 Blacklisting (MAC Blacklist) ... 50
7.1.5 Port Mirroring ... 51
7.1.6 Port Settings ... 51
7.2 Advanced Settings ... 55
7.2.1 Bandwidth Control ... 55
7.2.1.1 QoS („Quality of Service“) ... 55
7.2.1.2 Rate Limitation ... 62
7.2.1.2.1 Storm Control ... 62
7.2.1.2.2 Rate Limitation ... 62
7.2.2 IGMP Snooping ... 63
7.2.3 Multicast VLAN Registration (MVR) ... 66
7.2.3.1 Static Multicast ... 69
7.2.3.2 VLAN ... 72
7.2.3.3 Port Isolation ... 73
7.2.4 GARP/GVRP ... 75
7.2.4.1 Q-in-Q ... 77
7.2.4.2 Port-based Q-in-Q ... 80
7.2.4.3 Selektywne Q-in-Q ... 81
7.2.4.3.1 DHCP Relay ... 82
7.2.4.3.2 DHCP Options ... 84
7.2.5 DHCP Server ... 85
7.2.6 Dual Homing ... 87

7.2.7 Dual Ring ... 88
7.2.8 ERPS ... 89
7.2.9 Link Aggregation ... 92
7.2.9.1 Static Trunk ... 92
7.2.9.2 LACP ... 92
7.2.10 LLDP ... 94
7.2.11 Loop Detection ... 95
7.2.12 Jet Ring ... 96
7.2.13 PoE (Power over Ethernet) ... 97
7.2.14 Static Route ... 98
7.2.15 STP ... 99
7.2.16 Xpress Ring ... 105
7.3 Security ... 106
7.3.1 IP Source Guard ... 106
7.3.1.1 DHCP Snooping ... 107
7.3.1.1.1 Server Screening ... 109
7.3.1.2 Binding Table ... 109
7.3.1.3 ARP Inspection ... 110
7.3.1.3.1 Filter Table ... 111
7.3.2 Access Control List (ACL) ... 112
7.3.3 Standard komunikacyjny IEEE 802.1X ... 113
7.3.4 Port Security ... 117
7.3.4.1 Sticky MAC Settings ... 117
7.4 Monitor ... 118
7.4.1 Alarm ... 118
7.4.2 System Information ... 118
7.4.3 Port Statistics ... 118
7.4.4 Port Utilization ... 118
7.4.5 RMON Statistics ... 118
7.4.6 SFP ... 119
7.4.6.1 DDMI ... 119
7.4.7 Traffic Monitor ... 119
7.5 Management ... 120
7.5.1 SNMP ... 120
7.5.1.1 SNMP Trap ... 121
7.5.1.2 SNMPv3 ... 121
7.5.2 Auto Provision ... 121
7.5.3 Mail Alarm ... 123
7.5.4 Ping ... 123
7.5.5 USB Funktions ... 124
7.5.5.1 Ładowanie firmware'u ... 124
7.5.5.2 Zapisywanie pliku konfiguracyjnego ... 125
7.5.5.3 Zapisywanie pliku syslog ... 125
7.5.5.4 Ładowanie pliku konfiguracyjnego ... 125

8 Konfiguracja ... 127

8.1 Przegląd opcji konfiguracji ... 127
8.1.1 Port Telnet ... 128
8.2 Port konsolowy ... 129

9 System Web Based Management (WBM) ... 130

9.1 System Status 134
9.1.1 System Information 134
9.2 General Settings 136
9.2.1 General Settings 136
9.2.1.1 System 136
9.2.1.2 Jumbo Frame 138
9.2.1.3 SNTP 139
9.2.1.4 Management Host 142
9.2.2 MAC Management 143
9.2.2.1 Static MAC Settings 143
9.2.2.2 MAC Table 145
9.2.2.3 Age Time Setting 146
9.2.2.4 Blacklisting 147
9.2.3 Port Mirroring 148
9.2.4 Port Settings 150
9.2.4.1 General Settings 150
9.2.4.2 Information 152
9.3 Advanced Settings 153
9.3.1 Bandwidth Control 153
9.3.1.1 QoS 153
9.3.1.1.1 Port Priority 153
9.3.1.1.2 IP DiffServ (DSCP) 154
9.3.1.1.3 Priority/Queue Mapping 155
9.3.1.1.4 Schedule Mode 156
9.3.1.2 Rate Limitation 158
9.3.1.2.1 Storm Control 158
9.3.1.2.2 Bandwidt Limitation 160
9.3.2 IGMP Snooping 162
9.3.2.1 IGMP Snooping 162
9.3.2.1.1 General Settings 162
9.3.2.1.2 Port Settings 164
9.3.2.1.3 Querier Settings 166
9.3.2.2 IGMP Filtering 167
9.3.2.2.1 General Settings 167
9.3.2.2.2 Multicast Groups 168
9.3.2.2.3 Port Settings 169
9.3.2.3 Multicast VLAN Registration 170
9.3.2.3.1 MVR Settings 170
9.3.2.3.2 Group Settings 172
9.3.2.4 Static Multicast 173
9.3.2.5 Multicast Statistics 174
9.3.3 VLAN 175
9.3.3.1 Port Isolation 175
9.3.3.2 VLAN 177
9.3.3.2.1 VLAN Settings 177
9.3.3.2.2 Tag Settings 179
9.3.3.2.3 Port Settings 180
9.3.3.3 GARP VLAN Registration Protocol 182
9.3.3.3.1 GVRP 182
9.3.3.3.2 GARP Timer 184

9.3.3.4 IP Subnet VLAN 186
9.3.3.5 MAC VLAN 187
9.3.3.6 Protocol VLAN 188
9.3.3.7 Q-in-Q 189
9.3.3.7.1 VLAN Stacking 189
9.3.3.7.2 Port-based Q-in-Q 191
9.3.3.7.3 Selective Q-in-Q 192
9.3.4 DHCP Relay 194
9.3.5 DHCP Options 195
9.3.6 DHCP Server 197
9.3.6.1 General Settings 197
9.3.6.2 Pool Settings 199
9.3.6.3 Binding Information 203
9.3.6.4 Statistics 204
9.3.7 Dual Homing 205
9.3.8 Dual Ring 207
9.3.9 ERPS 209
9.3.9.1 Ring Settings 209
9.3.9.2 Instance Settings 213
9.3.10 Link Aggregation 214
9.3.10.1 Static Trunk 214
9.3.10.2 LACP 216
9.3.10.3 LACP info. 218
9.3.11 LLDP 220
9.3.11.1 LLDP Settings 220
9.3.11.2 Neighboring Detection 222
9.3.12 Loop Detection 223
9.3.13 Jet Ring 225
9.3.14 Modbus 227
9.3.15 PoE 228
9.3.15.1 Configuration 228
9.3.15.2 Schedule 230
9.3.15.3 PD Alive Check 233
9.3.15.4 Power Delay 236
9.3.16 Static Route 238
9.3.17 Spanning Tree Protocol (STP) 240
9.3.17.1 General Settings 240
9.3.17.2 Port Parameters 242
9.3.17.3 STP Status 245
9.3.18 Xpress Ring 246
9.4 Security 248
9.4.1 IP Source Guard 248
9.4.1.1 DHCP Snooping 248
9.4.1.1.1 DHCP Snooping 248
9.4.1.1.2 Port Settings 250
9.4.1.1.3 Server Screening 251
9.4.1.2 DHCP Snooping Binding Table 252
9.4.1.2.1 Static Entry Settings 252
9.4.1.2.2 Binding Table 254
9.4.1.3 ARP Inspection 255

9.4.1.3.1 ARP Inspection 255
9.4.1.3.2 Filter Table 257
9.4.2 Access Control List (ACL) 258
9.4.3 IEEE 802.1X 262
9.4.3.1 Global Settings 262
9.4.3.2 Port Settings 265
9.4.4 Port Security 269
9.4.4.1 Port Security 269
9.4.4.2 Sticky MAC Settings 271
9.5 Monitor 272
9.5.1 Alarm Information 272
9.5.2 System Information 273
9.5.3 Port Statistics 275
9.5.4 Port Utilization 276
9.5.5 RMON Statistics 277
9.5.6 SFP Information 280
9.5.7 Traffic Monitor 283
9.6 Management 286
9.6.1 SNMP 286
9.6.1.1 SNMP 286
9.6.1.1.1 SNMP Settings 286
9.6.1.1.2 Community Name 287
9.6.1.2 SNMP Trap 289
9.6.1.2.1 Trap Receiver Settings 289
9.6.1.2.2 Trap Event State 291
9.6.1.2.3 Port Trap Settings 292
9.6.1.3 SNMPv3 Configuration 293
9.6.1.3.1 SNMPv3 User 293
9.6.1.3.2 SNMPv3 Group 295
9.6.1.3.3 SNMPv3 View 296
9.6.2 Auto Provision 297
9.6.3 Mail Alarm 298
9.6.4 Maintenance 300
9.6.4.1 Configuration 300
9.6.4.2 Firmware 302
9.6.4.3 Reboot 303
9.6.4.4 Protocols 304
9.6.5 System Log 306
9.6.6 Ping 308
9.6.7 USB Funktions 309
9.6.8 User Account 310

10 Załącznik 312

10.1 Przewód konsolowy (RJ-45 do DB9) 312
10.2 Przewód RJ-45 313
10.3 Configuring in the Command Line Interface (CLI) 314
10.3.1 System Status 314
10.3.1.1 System Information 314
10.3.2 Basic Settings 315
10.3.2.1 System 315

10.3.2.1.1 Jumbo Frame....316
10.3.2.1.2 SNTP....317
10.3.2.1.3 Management Host....318
10.3.2.2 MAC Management....319
10.3.2.2.1 Blackhole MAC....319
10.3.2.3 Port Mirroring....320
10.3.2.4 Port Settings:....321
10.3.3 Advanced Settings....322
10.3.3.1 Bandwidth Control....322
10.3.3.1.1 QoS....322
10.3.3.1.2 Rate Limitation....323
10.3.3.1.2.1 Storm Control....323
10.3.3.2 IGMP Snooping....324
10.3.3.2.1 IGMP Snooping Querier♠....326
10.3.3.2.2 IGMP Snooping Filtering....326
10.3.3.2.3 MVR....327
10.3.3.2.4 Multicast Address....328
10.3.3.3 VLAN....328
10.3.3.3.1 Port Isolation....328
10.3.3.3.2 VLAN Settings....329
10.3.3.3.3 GARP/GVRP....331
10.3.3.3.4 IP Subnet VLAN....332
10.3.3.3.5 MAC VLAN....332
10.3.3.3.6 Protocol VLAN....333
10.3.3.3.7 Q-in-Q....334
10.3.3.3.7.1 VLAN Stacking....334
10.3.3.4 DHCP Relay....336
10.3.3.5 DHCP Options....337
10.3.3.6 Dual Homing....337
10.3.3.7 ERPS....338
10.3.3.8 Link Aggregation....339
10.3.3.8.1 LACP....340
10.3.3.9 LLDP....341
10.3.3.10 Loop Detection....342
10.3.3.11 Modbus....343
10.3.3.12 PoE....343
10.3.3.12.1 PoE Schedule....343
10.3.3.12.2 PD Alive Check....344
10.3.3.12.3 Power Delay....344
10.3.3.13 Static Route....345
10.3.3.14 STP....348
10.3.3.14.1 MSTP....351
10.3.3.15 Xpress Ring....353
10.3.4 Security....354
10.3.4.1 IP Source Guard....354
10.3.4.1.1 DHCP Snooping....354
10.3.4.1.1.1 Server Screening....355
10.3.4.1.2 Binding Table....355
10.3.4.1.3 ARP Inspection....356
10.3.4.1.3.1 Filter Table....356

10.3.4.2 Access Control List 357
10.3.4.3 802.1X 360
10.3.4.4 Port Security 362
10.3.5 Monitor 363
10.3.5.1 Alarm 363
10.3.5.2 Monitor Information 363
10.3.5.3 Port Statistics 363
10.3.5.4 Port Utilization 363
10.3.5.5 RMON Statistics 363
10.3.5.6 SFP Information 363
10.3.5.7 Traffic Monitor 364
10.3.6 Management 365
10.3.6.1 SNMP 365
10.3.6.1.1 SNMP 365
10.3.6.1.2 SNMP Trap 366
10.3.6.1.2.1 Port Trap Settings 366
10.3.6.1.3 SNMPv3 367
10.3.6.2 Auto Provision 368
10.3.6.3 Mail Alarm 368
10.3.6.4 Maintenance 369
10.3.6.4.1 Reboot 370
10.3.6.5 System Log 370
10.3.6.6 USB Flash 371
10.3.6.7 User Account 372
10.4 Tabele MODBUS/TCP 373
10.4.1 Format danych i kod funkcji 373
10.4.2 Rejestry MODBUS 374

Spis ilustracji 407

Spis tabel 411

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“ (852-1505/000-001).

1.2 Prawa autorskie

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

1.3 Symbol

NIEBEZPIECZEŃSTWO



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

NIEBEZPIECZEŃSTWO



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 802.3ad
- IEEE 802.3x
- IEEE 802.1D
- IEEE 802.1w
- IEEE 802.1s
- IEEE 802.1Q
- IEEE 802.1p
- IEEE 802.1X
- IEEE 802.1AB
- IEEE 1588v2
- IEEE 802.3af
- IEEE 802.3at
- ITU-T G8032v1/v2

Switche mają zasilanie w zakresie napięcia 24 … 57 V.
Power over Ethernet (PoE+) jest obsługiwany na 8 portach.
Inne funkcjonalności to autonegocjacja i Auto-MDI/MDIX (crossover) na wszystkich portach 10/100/1000 BASE-T.

3.3 Technologia switchingu

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

3.4 PoE (Power over Ethernet)

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

3.5 Autonegocjacja

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

3.6 Autocrossing

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

3.7 Tryb Store and Forward Switching

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

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

Zaleta trybu „Store and Forward":
Telegramy danych sprawdzane są pod kątem poprawności i ważności. W ten sposób unika się 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.

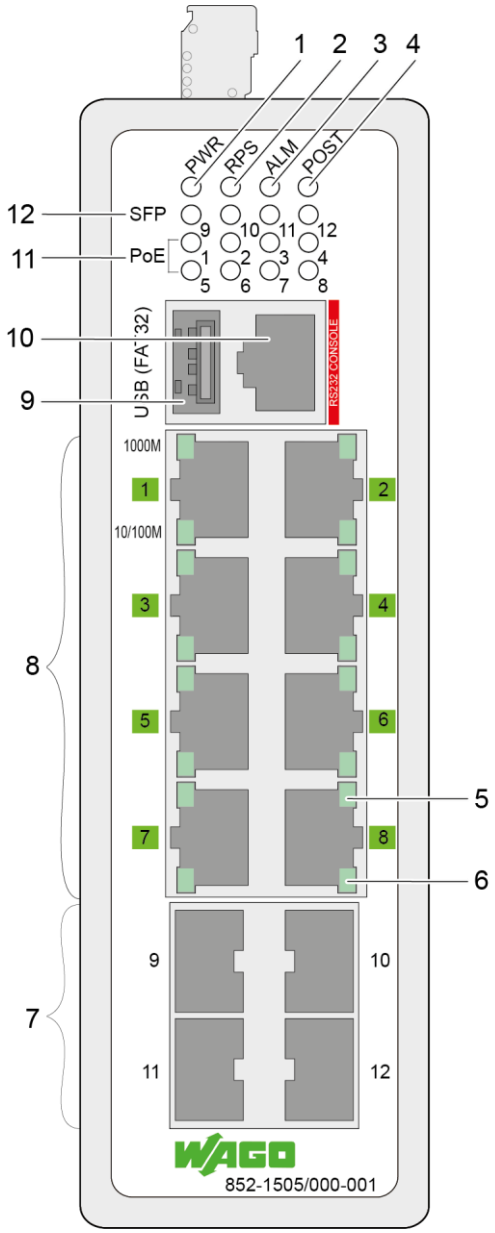
- Full duplex
  - Urządzenie ETHERNET może równocześnie wysyłać i odbierać dane.
  - Rozpoznawanie kolizji (CSMA/CD) jest wyłączone.
  - Rozległość sieci uzależniona jest tylko od ograniczeń wydajności zastosowanych komponentów wysyłających i odbierających dane.

4 Opis urządzenia

852-1505/000-001 to przemysłowy, konfigurowalny switch ETHERNET z 8 portami 10/100/1000BASE-T, które wszystkie obsługują Power over Ethernet (PoE+) o mocy do 30 W. Te 8 portów można wykorzystywać jednocześnie do zasilania i transmisji danych.
Pozwala to nie tylko ograniczyć nakłady związane z oprzewodowaniem, lecz także zrezygnować z osobnego zasilacza dla czujników.
Przemysłowy switch zarządzalny można łatwo konfigurować i instalować i dzięki temu wykorzystywać w różnorakich aplikacjach.
4 sloty SFP pozwalają na zastosowanie przemysłowego switcha zarządzalnego w rozległych sieciach.
Zintegrowane złącze USB umożliwia aktualizację firmware'u i konfigurację switcha za pomocą pamięci USB.

4.1 Widok

4.1.1 Widok z przodu



Ilustracja 1: 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 redundantnego napięcia zasilania	„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 slotu SFP (1000BASE-SX/LX, światłowód) (4)	„Opis urządzenia“ > „Złącza“
8	-	Złącze RJ-45 (10/100/1000BASE-T) z PoE+ (8)	„Opis urządzenia“ > „Złącza“
9	-	Złącze USB	„Opis urządzenia“ > … > „Złącza sieciowe“
10	-	Złącze 1 x RJ-45 (RS-232)	„Opis urządzenia“ > „Złącza“
11	PoE	LED statusu Power over Ethernet (8) (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“
12	SFP	LED statusu portu SFP LNK/ACT (4) (1 LED dla każdego złącza)	„Opis urządzenia“ > „Elementy sygnalizacyjne“

4.1.2 Widok z góry



Ilustracja 2: 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	Reset	Przycisk resetu	„Opis urządzenia“ > „Elementy obsługi“

4.2 Złącza

4.2.1 Śruba uziemienia

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



Ilustracja 3: Śruba uziemienia

UWAGA



Instrukcja sposobu uziemienia!
Nie należy łączyć za pomocą przewodów PWR - ani PWR + z potencjałem uziemienia.

4.2.2 Zasilanie (PWR/RPS)

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

Wtyk składa się z następujących pinów:



Ilustracja 4: Złącze zasilające (PWR/RPS)

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

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

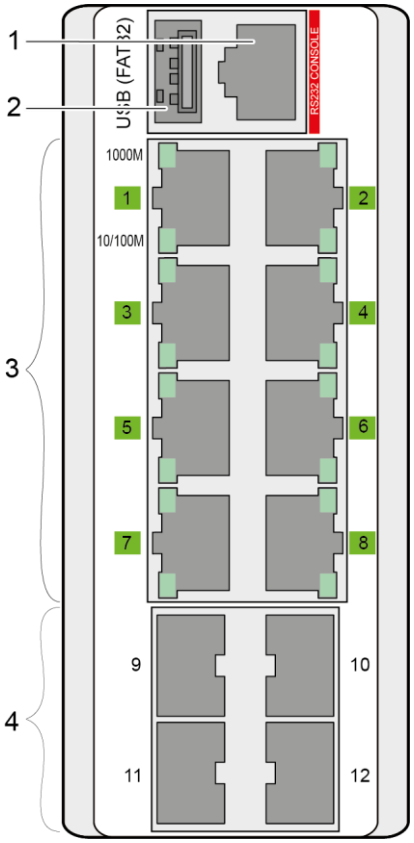
ESD



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

4.2.3 Złącza sieciowe

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 USB	„Opis urządzenia“ > … > „Złącze USB“
3	-	Złącze 8 x RJ-45 (10/100/1000BASE-T) z PoE+	„Opis urządzenia“ > … „Złącza 10/100/1000BASE-T z PoE+“
4	-	Złącze 4 x SFP (1000BASE-SX/LX, światłowód)	„Opis urządzenia“ > … „Złącza 1000BASE-SX/-LX“

4.2.3.1 Złącze RJ-45

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

4.2.3.2 Złącze USB

Złącze USB switcha może służyć do realizacji następujących funkcji:

- ładowanie oprogramowania firmware
- zapisywanie pliku konfiguracyjnego
- zapisywanie pliku syslog
- ładowanie pliku konfiguracyjnego

4.2.3.3 Złącza 10/100/1000BASE-T

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

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

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

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

Zalety:

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

Wskazówka



Zwrócić uwagę na moc PoE.
Moc PoE przy 24V DC wynosi 120 W.
Jeśli wszystkie 8 portów są podłączone, moc dostarczana przez PSE (**P**ower **S**ourcing **E**quipment) wynosi maksymalnie 15 W.
Jeśli podłączone są tylko 4 porty, moc dostarczana przez PSE wynosi 30 W.

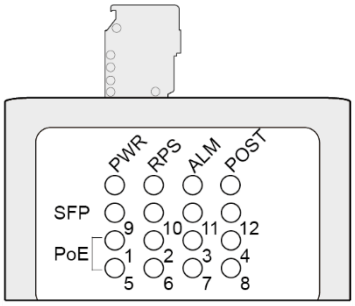
4.2.3.5 Złącza 1000BASE-SX/LX

Złącza 1000BASE-SX/-LX przeznaczone są do podłączania modułów Gigabit SFP, wspierających prędkość transmisji 100/1000 Mbit/s.

4.3 Elementy sygnalizacyjne

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

4.3.1 LED urządzeń

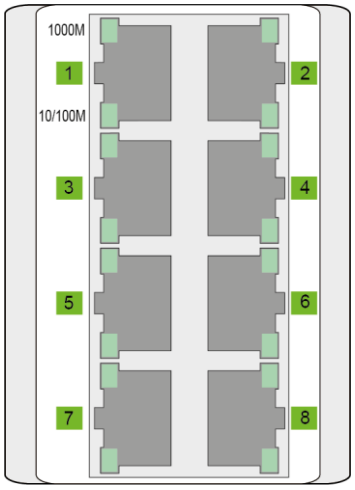


Ilustracja 6: LED urządzeń

Tabela 7: Opis ilustracjii „LED urządzeń“

LED		Nazwa	Status	Opis
PWR		Primary-Power-LED	zielony	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		Alarm-LED	czerwony	Awaria połączenia, inny alarm
			Off	Alarm nie jest zgłaszany.
POST		Power-On-Self-Test-LED	miga	Przeprowadzany jest autotest.
			zielony	Autotest został zakończony.
			Off	Brak napięcia roboczego lub błąd podczas wykonywania autotestu.
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
PoE	1 … 8	LED portu PoE	zielony	Zasilanie PoE jest obecne.
			Off	Nie ma zasilania PoE.

4.3.2 LED złącz



Ilustracja 7: LED złącz

Tabela 8: Opis ilustracji „LED złącz“

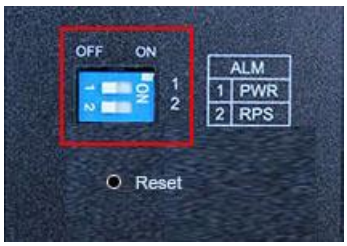
LED	Nazwa	Status	Opis
1000M	LED portów 1000BASE-T (1 LED dla każdego złącza)	zielony	Złącze pracuje z prędkością 1000 Mbit/s.
		miga	Przez złącze transmitowane są dane.
		Off	Brak nawiązanego ważnego połączenia ze złączem
10/100M	LED portów 10/100BASE-T (1 LED dla każdego złącza)	zielony	Złącze pracuje 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 dwa mikroprzełączniki DIP, służące do konfiguracji alarmu. Przy aktywowanej funkcji zgłaszania alarmu przy wystąpieniu zdarzenia styk alarmowy zostaje załączony.

Znaczenie ustawień mikroprzełączników DIP objaśniono poniżej.



Ilustracja 8: Mikroprzełączniki DIP

Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“

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.

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

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

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

1. Ustaw mikroprzełącznik DIP w pozycji „OFF“.
2. Zainstaluj przemysłowy switch zarządzalny w swojej sieci.
3. Wybierz funkcję alarmu, która ma być aktywowana.
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.

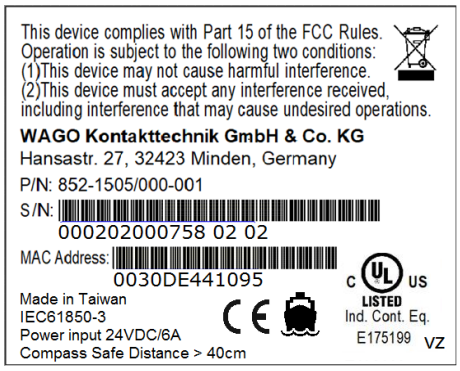
Wskazówka

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

4.5 Naklejka

4.5.1 Wersja sprzętu i oprogramowania

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



Ilustracja 10: Naklejka

Tabela 11: Opis ilustracji „Naklejka“

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

4.6 Parametry techniczne

4.6.1 Dane urządzenia

Tabela 12: Dane techniczne – dane urządzenia

Szerokość	50 mm
Wysokość	120 mm (od górnej krawędzi szyny montażowej)
Głębokość	162 mm
Masa	955 g
Stopień ochrony	IP30

4.6.2 Dane systemowe

Tabela 13: Dane techniczne – dane systemowe

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

4.6.3 Zasilanie

Tabela 14: Dane techniczne – zasilanie

Napięcie zasilania	24 … 57 V DC (CE, UL) 24 V DC (DNV GL) 24/48 V DC (LR)
Maks. pobór mocy	18 W; 258 W z 8 PoE+ (48 V DC)

4.6.4 Power over Ethernet (PoE)

Tabela 15: Dane techniczne – Power over Ethernet (PoE)

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

[1)] PD = „Powered Device“

[2)] PSE = „Power Sourcing Equipment“

4.6.5 Komunikacja

Tabela 16: Dane techniczne – komunikacja

Konfiguracja i update	1 x host USB 2.0
Porty (miedź; RJ-45)	8 x 10/100/1000BASE-T z PoE+ 1 x RS-232
Porty (światłowód)	4 x 1000BASE-SX/-LX
Standardy	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX 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 Prioritization IEEE 802.1x Port Authentication IEEE 802.1ab Link Layer Discovery Protocol (LLDP) IEEE 802.3ad Link Aggregation IEEE 1588v2 Precision Time Protocol (PTP) IEEE 802.3af Power over Ethernet (PoE) IEEE 802.3at High Power over Ethernet (PoE+) ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

4.6.6 Warunki środowiskowe

Tabela 17: Dane techniczne – warunki środowiskowe

Temperatura otoczenia, praca	-40 … +70°C (CE) -10 … +60°C (UL) -25 … +70°C (DNV GL) +5 … +70°C (LR)
Temperatura otoczenia, przechowywanie	-40 …+85°C
UL 61010 Użytkowanie Stopień zanieczyszczenia	Wewnątrz pomieszczeń 2
Wilgotność względna (bez kondensacji)	10 … 95%
Odporność na wibracje	zgodnie z IEC 60068-2-6
Odporność na wstrząsy	zgodnie z IEC 60068-2-27
EMC: odporność na zakłócenia	EN 55024 EN 61000-6-2 IEC 61000-4-2 IEC 61000-4-3 IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-6 IEC 61000-4-8
EMC: emisja zakłóceń	FCC Part 15 EN 55011: Klasa A EN 55032: Klasa A EN 61000-6-4
Bezpieczna odległość od kompasu	> 40 cm

4.7 Normy i dyrektywy

Zasilanie	zgodnie z IEC 61850-3:2013

4.8 Aprobaty

Aprobaty dla osprzętu WAGO-ETHERNET „Industrial-Managed-Switch“ (852-1505/000-001):

Znak zgodności

Aprobaty dla osprzętu WAGO-ETHERNET „Industrial-Managed-Switch“ (852-1505/000-001):

Ordinary Locations		UL61010-2-201 (E175199)

Aprobaty morskie dla osprzętu WAGO-ETHERNET „Industrial-Managed-Switch“ (852-1505/000-001):

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

LR (Lloyd’s Register)	Env. 1, 2, 3

Wskazówka

Ważne od wersji firmware'u 02!
Te aprobaty morskie są ważne tylko od wersji hardware'u 02.
Switche o wersji hardware'u 01 nie mają aprobat morskich!

Wersje hardware'u 01 i 02 są z technicznego punktu widzenia identyczne. Dla wersji hardware'u 02 naklejka i ulotka do opakowania zostały dostosowane do wymogów aprobat morskich.

5 Montaż

5.1 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.

5.2 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.

5.3 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.

6 Podłączanie urządzeń

6.1 Zasilanie

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

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

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

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

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

Wskazówka



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

UWAGA



Instrukcja sposobu uziemienia!
Nie należy łączyć za pomocą przewodów PWR - ani PWR + z potencjałem uziemienia.

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

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

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

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

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

6.2 Złącze zewnętrznego styku alarmowego

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

2 Błąd w Jet Ring lub ERPS-Ring

6.3 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 konsolowego (8-stykowy RJ-45) można znaleźć w rozdziale „Załącznik“ > … > „Złącze konsolowe (RJ-45 do DB9)“.

6.4 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“).

6.5 Porty 10/100/1000BASE-T

Porty 10/100/1000Base-T (złącza RJ-45 Ethernet) switcha przemysłowego 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“).

7 Opis funkcji

7.1 Ustawienia podstawowe

7.1.1 Jumbo Frame

„Jumbo Frames“ to ramki ETHERNET o rozmiarze większym niż 1518 Byte. 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 przez dane urządzenie sieciowe odrzucone.

7.1.2 SNTP

SNTP („**S**imple **N**etwork **T**ime **P**rotocol“) jest protokołem służącym do synchronizacji czasu między serwerem czasu (serwer NTP („**N**etwork **T**ime **P**rotocol“) i serwer SNTP) i czasem systemowym w urządzeniu ETHERNET. Protokół jest obsługiwany przez port UDP. Wspierane jest wyłącznie adresowanie unicast.

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

7.1.3 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.

7.1.4 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.

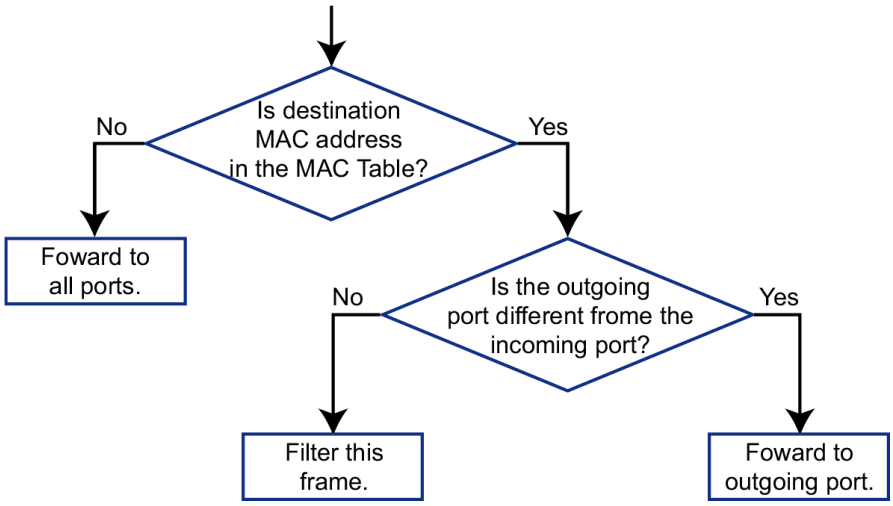
1. Switch sprawdza odebraną ramkę i rozpoznaje port, z którego pochodzi źródłowy adres MAC.

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 11: Diagram przebiegu tabeli adresów MAC

7.1.4.1 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.

7.1.4.2 Blacklisting (MAC Blacklist)

Ten rodzaj adresów MAC wpisywany jest ręcznie. Switch odrzuca pakiety danych, które mają te adresy MAC jako źródłowe lub docelowe i które są zawarte we wpisach adresów MAC „Blackhole“. Wpisy „Blackhole“ konfigurowane są w celu odfiltrowania specyficznych źródłowych lub docelowych adresów MAC.

7.1.5 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.

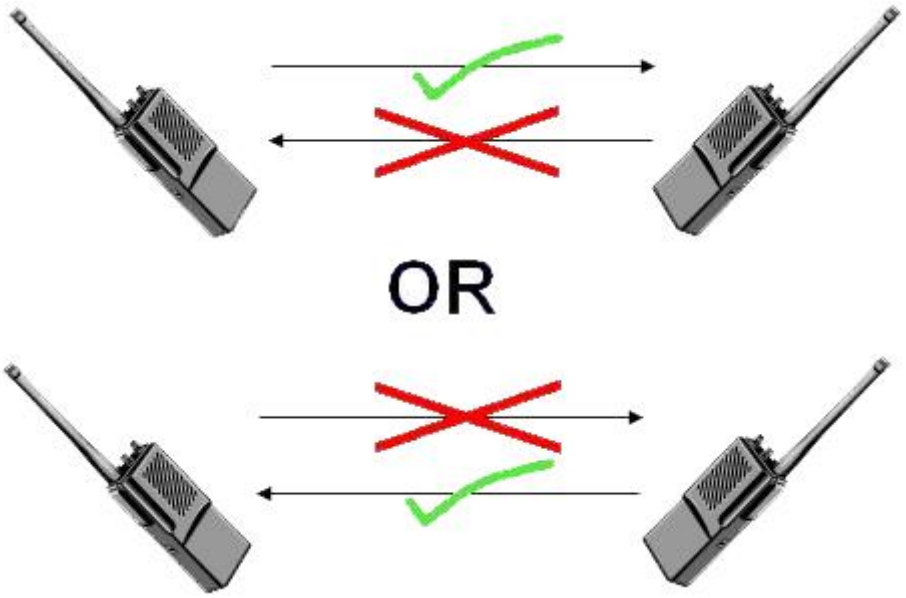
7.1.6 Port Settings

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 12: 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 13: Tryb full duplex

Test Loopback

W teście „Loopback“ sygnał wysyłany jest z jednego urządzenia komunikacyjnego i zaraz potem znowu do niego przesłany („looped back“).
W ten sposób sprawdzane jest prawidłowe działanie urządzenia i wyszukiwane są uszkodzone węzły sieciowe.
W teście „Loopback“ używa się specjalnej wtyczki, tzw. „wrap plug“, którą wtyka się do portu urządzenia komunikacyjnego. Wtyczka powoduje, że przesyłane dane (z wyjścia) powracają jako dane odbiorcze (do wejścia) i w ten sposób symulowany jest zamknięty obieg komunikacji w pojedynczym komputerze.

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 VLAN, 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“.

7.2 Advanced Settings

7.2.1 Bandwidth Control

7.2.1.1 QoS („Quality of Service“)

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 danych. Każda wchodząca ramka zostaje przekierowana do jednej z ośmiu „Transmit Queues“ przydzielonego portu wyjściowego na podstawie swojego priorytetu. Port wyjściowy przesyła pakiety danych 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 kończy 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 pakiet, najwyższy ponownie rozpoczyna transmisję swoich pakietów, które w międzyczasie odebrał.

Rozszerzenie QoS

Switch można tak skonfigurować, aby priorytetować ruch danych, nawet gdy wchodzące pakiety danych 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 danych:

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

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

- QoS na bazie DSCP
  - Priorytety dla pakietów danych 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 danych 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 Tag	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 18: 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“.

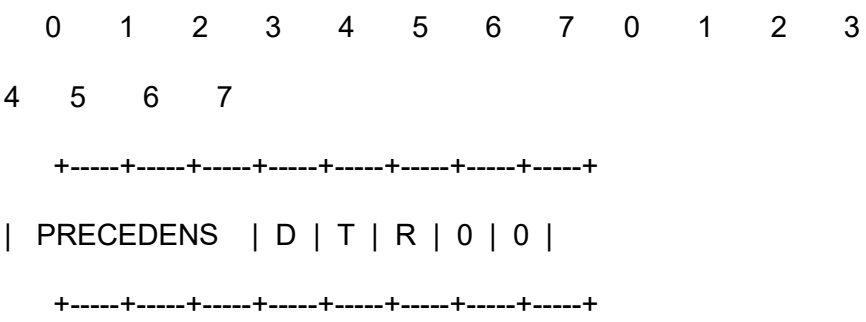
<table>
<tr><th>Version</th><th>IHL</th><th>Type of Service</th><th colspan="2">Total Length</th></tr>
<tr><td colspan="3">Oznaczanie</td><td>Flagi</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source 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 danych, 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 danych do bufora i dopiero potem niższy priorytet uzyskuje zgodę na transmisję swoich pakietów danych. Gdy niższy „Hardware Priority Queue“ prześle swoje pakiety danych, najwyższy ponownie rozpoczyna transmisję swoich pakietów danych, 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. Dla „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“.

7.2.1.2 Rate Limitation

7.2.1.2.1 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 danych.

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

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

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

7.2.1.2.2 Rate Limitation

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

7.2.2 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.

7.2.3 Multicast VLAN Registration (MVR)

MVR („**M**ulticast **V**LAN **R**egistration“), przez który Media Server może transmitować strumień multicast do własnej lokalnej sieci multicast i przy czym klienci odbierający strumień VLAN mogą znajdować się w różnych sieciach VLAN. Klienci w różnych sieciach VLAN mogą dołączyć do grupy multicast lub ją opuścić, wysyłając „IGMP Join Message“ lub „IGMP Leave Message“ do portu odbiorczego. Port odbiorczy należący do grup multicast może odbierać strumień multicast z Media Servera. Bez wsparcia MVR strumień multicast z Media Servera i uczestnicy powinni znajdować się w tej samej sieci VLAN.

- Porty źródłowe: Porty źródłowe strumienia.
- Porty odbiorcze: Porty klientów.
- Porty ze znacznikiem: Porty ze znacznikiem należy skonfigurować w celu przyporządkowania ich jako porty źródłowe lub odbiorcze.

Tryb MVR

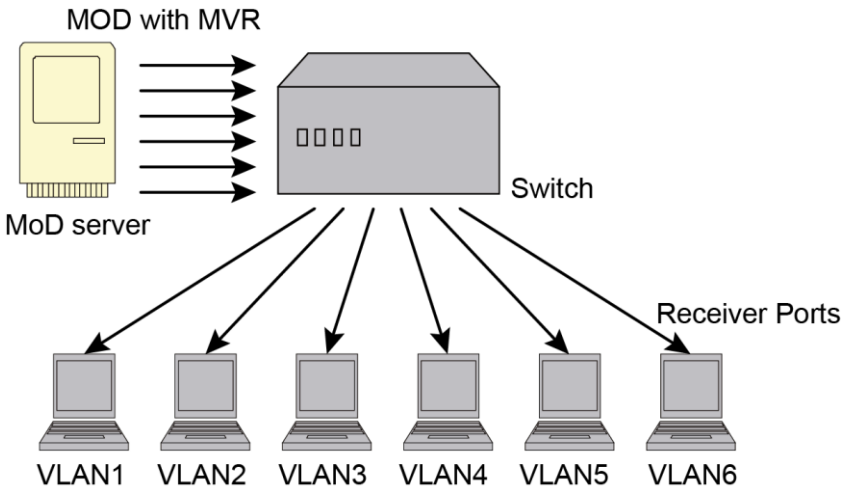
- **Tryb dynamiczny**
  Gdy w „MVR Settings“ aktywowany jest tryb dynamiczny, „IGMP Report Message“ z portu odbiorczego przesyłany jest do portów źródłowych rutera multicast. Ruter multicast może dynamicznie rozpoznawać, które grupy multicast znajdują się na których interfejsach.

- **Tryb kompatybilności**
  Gdy w „MVR Settings“ aktywowany jest tryb kompatybilności, „IGMP Report Message“ wysyłany z portu odbiorczego nie jest przesyłany do portów źródłowych rutera multicast. Ruter multicast musi być skonfigurowany statycznie.

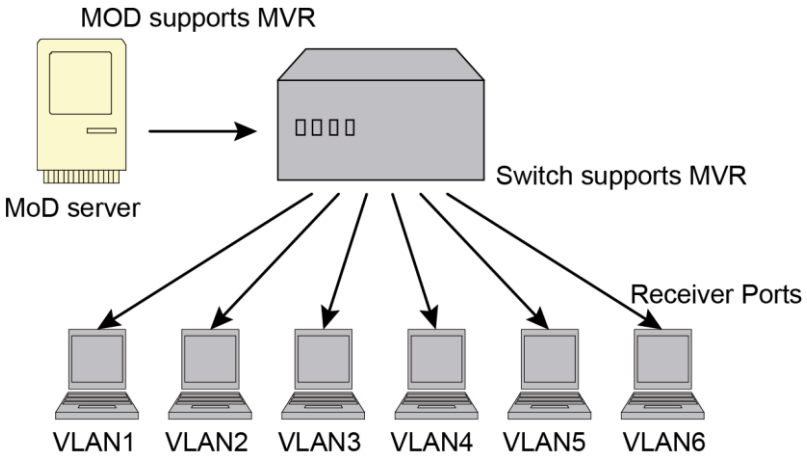
- **Tryb pracy**
  Join Operation
  Uczestnik wysyła do switcha „IGMP Report Message“, aby dołączyć do odpowiedniej grupy multicast. Następny krok zależy od tego, czy „IGMP Report Message“ pasuje do skonfigurowanego w switchu adresu MAC multicast czy nie. Jeśli pasuje, CPU switcha modyfikuje tabelę adresów sprzętu, aby dołączyć ten port odbiorczy i VLAN jako cel przekierowania danych dla MVLAN.

- **Leave Operation**
  Uczestnik wysyła do switcha „IGMP Leave Message“, aby opuścić multicast. CPU switcha wyśle specyficzne dla grupy „IGMP Query“ do portu odbiorczego sieci VLAN. Gdy w sieci VLAN jest inny uczestnik, musi on odpowiedzieć w maksymalnym czasie odpowiedzi. Jeśli nie ma uczestnika, switch usunie ten port odbiorczy.

- **Immediate Leave Operation**
  Uczestnik wysyła do switcha „IGMP Leave Message“, aby opuścić multicast. Uczestnicy nie muszą czekać, aż CPU switcha wyśle specyficzne dla grupy „IGMP Query“ do portu odbiorczego sieci VLAN. Switch natychmiast usunie ten port odbiorczy.



Ilustracja 14: MOD bez MVR



Ilustracja 15: MOD wspiera MVR

Domyślna konfiguracja dla nowej MVR:

Informacje MVR VLAN

VLAN ID:	2
Name:	MVR2
Active:	Enabled
Modus:	Dynamic
Source-port(s):	None
Receiver port(s):	None
Port(s) with tag:	None

Switch umożliwia użytkownikowi utworzenie maksymalnie 250 grup.
Switch umożliwia użytkownikowi utworzenie maksymalnie 16 MVR.

Wskazówka



Wskazówki

- IGMP Snooping“ i MVR można aktywować niezależnie od siebie.
- „IGMP Snooping“ i MVR wykorzystują ten sam „Timer IGMP“.
- MVR może rozpoznać komunikaty IGMPv3.
- Wpisy grup, jak komunikat IGMPv3, podobnie jak poniższe typy wpisów grup, nie są traktowane przez switch jako komunikaty członkostwa. Te typy wpisów grup to „MODE_IS_INCLUDE“, „CHANGE_TO_INCLUDE_MODE“, „ALLOW_NEW_SOURCES“ i „BLOCK_OLD_SOURCES“.
- Nie należy wykorzystywać adresu grupowego X.0.0.1 dla strumienia multicast. System rozpoznaje i protokółuje adres 224.0.0.1 dla dynamicznego „Querier Port”. Adres grupowy X.0.0.1 mógłby spowodować konflikt z 224.0.0.1.
- Dolne 23 bity 28-bitowego adresu IP multicast zostają przyporządkowane do 23 bitów dostępnej przestrzeni adresowej ETHERNET. Przy konfiguracji adresu grupowego switch porównuje tylko dolne 23 bity.
- Polecenie CLI „group 1 start-address 224.1.1.1 6“ tworzy 6 grup. Oznacza to, że jeden IP odpowiada jednej grupie.
- Nazwa MVR powinna składać się z kombinacji cyfr lub liter.
- Nazwa grupy powinna składać się z kombinacji cyfr lub liter.

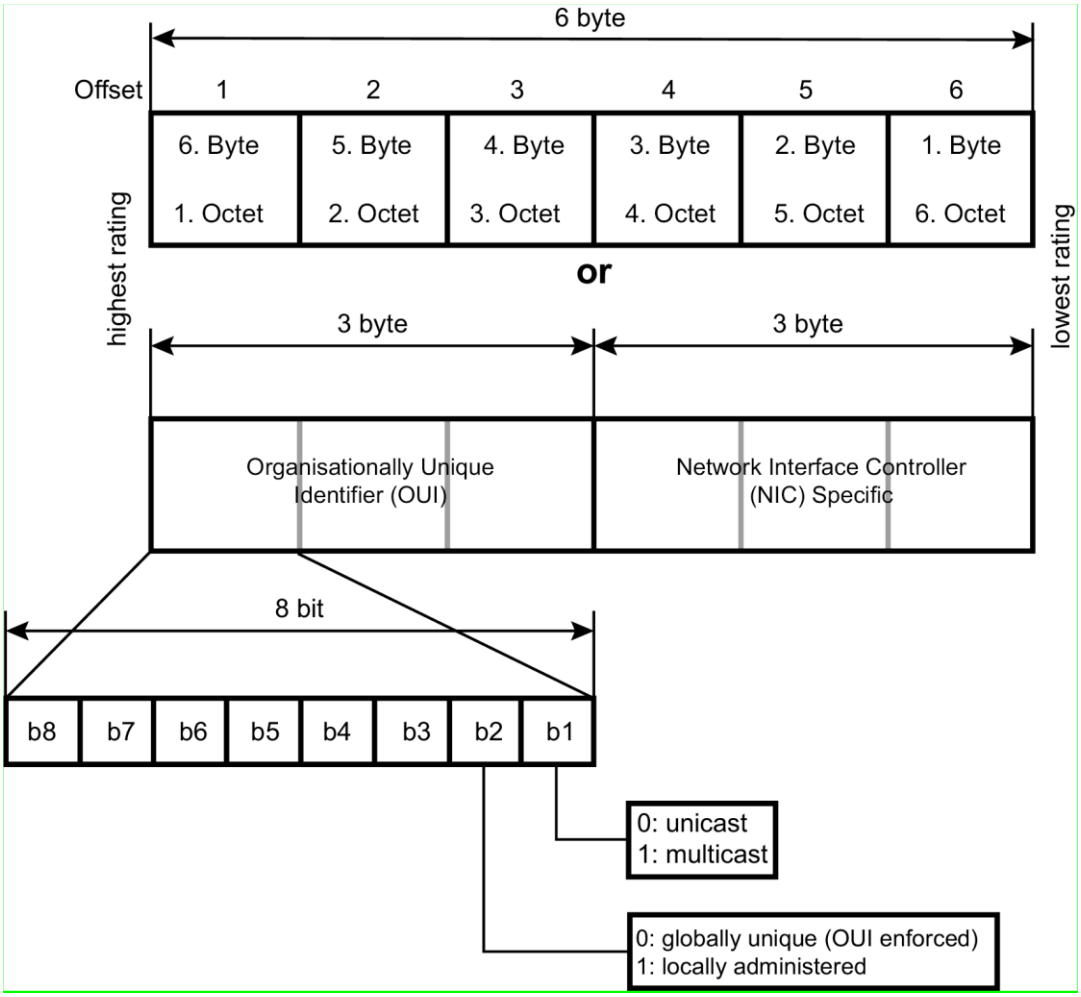
7.2.3.1 Static Multicast

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 19: 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	Zarezerwowane do wykorzystania w przyszłości lub dla celów badawczych i rozwojowych



Ilustracja 16: Adres multicast

Tabela 20: 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 Packets” 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 20: 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“

7.2.3.2 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 możliwych jest maksymalnie 4094 konfiguracji 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 ze znacznikiem jest o cztery bajty dłuższa niż ramka bez znacznika 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 możliwych jest maksymalnie 4094 konfiguracji VLAN.

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

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

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

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

- **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 danych 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.

7.2.3.3 Port Isolation

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

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

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

7.2.4 GARP/GVRP

GARP („**G**eneric **A**ttribute **R**egistration **P**rotocol“) i GVRP („GARP VLAN Registration Protocol lub Generic VLAN Registration Protocol“) to standardowe protokoły branżowe, opisane w IEEE 802.1p. GVRP jest aplikacją GARP, umożliwiającą zgodną z 802.1Q „VLAN Pruning“ oraz dynamiczne tworzenie VLAN na „802.1Q Trunk Ports“.

Za pomocą GVRP switch może wymieniać informacje dotyczące konfiguracji sieci VLAN z innymi switchami GVRP, usuwać niepotrzebne dane broadcast i nieznane dane unicast („Pruning“) oraz tworzyć dynamicznie sieci VLAN, które połączone są ze sobą przez „802.1Q Trunk Ports“.

GVRP wykorzystuje GID („**G**roup **Id**entification“) i GIP, wspólne opisy automatów stanów („State Machine Descriptions“) i wspólne mechanizmy transmisji informacji, zdefiniowane do zastosowania w aplikacjach bazujących na GARP. GVRP można uruchomić tylko przez „802.1Q Trunk Links“. GVRP koryguje „Trunk Links“, aby przez połączenia Trunk transmitowane były tylko aktywne sieci VLAN. Przed dołączeniem VLAN do Trunk GVRP czeka na żądania połączenia od switchy. Aktualizacje GVRP i timery można zmieniać. Porty GVRP mogą pracować w różnych trybach w celu sterowania korekcją sieci VLAN. Konfiguracja GVRP umożliwia dynamiczne dodawanie i zarządzanie sieciami VLAN w bazie danych w celu wsparcia procesów „Trunking“.

Można powiedzieć, że GVPR umożliwia propagowanie informacji VLAN z urządzenia do urządzenia. Za pomocą GVRP można ręcznie konfigurować pojedynczy switch dla wszystkich sieci VLAN potrzebnych do sieci, po czym wszystkie inne switche w sieci mogą dynamicznie rozpoznać te sieci VLAN. Końcowe węzły można podłączyć do każdego switcha i połączyć się z dowolną siecią VLAN. Dla końcowych węzłów, które GVRP chce wykorzystać, potrzebne są karty sieciowe obsługujące GVRP (NIC). Karta sieciowa obsługująca GVRP zostaje skonfigurowana z żądaną siecią lub sieciami VLAN i następnie połączona z aktywowanym w GVRP switchem. Karta sieciowa komunikuje się ze switchem, gdy tylko powstanie połączenie między kartą sieciową i switchem.

Registration Mode:

- **Normal**
  Tryb rejestracji „normal“ pozwala na dynamiczne tworzenie (gdy tylko aktywowane jest dynamiczne tworzenie VLAN), rejestrowanie i wyrejestrowanie sieci VLAN na porcie „Trunk“. Tryb „normal“ jest ustawieniem domyślnym.

- **Forbidden**
  Tryb rejestracji „forbidden“ wyrejestrowuje wszystkie sieci VLAN (poza VLAN 1) i zapobiega dalszemu tworzeniu lub rejestracji sieci VLAN na porcie „Trunk“.

- **Fixed**
  Tryb rejestracji „fixed“ pozwala na ręczne tworzenie i rejestrację sieci VLAN, zapobiega wyrejestrowaniu sieci VLAN i rejestruje wszystkie znane sieci VLAN na innych portach na porcie „Trunk“. (To samo dotyczy statycznej sieci VLAN)

GVRP Timer:

- **Join Timer**
  „Join Timer“ specyfikuje maksymalny czas w milisekundach, przez który interfejs czeka, zanim rozpocznie wysyłanie komunikatów VLAN.

- **Leave Timer**
  „Leave Timer“ specyfikuje maksymalny czas w milisekundach, przez który interfejs czeka po odebraniu „Leave Message“, zanim opuści wyspecyfikowaną we wiadomości sieć VLAN.

- **Leaveall Timer**
  „Leaveall Timer“ specyfikuje interwał czasowy w milisekundach, po którym „Leaveall Messages“ wysyłany jest do interfejsów. „Leaveall Messages“ mogą przy tym pomóc w aktualizacji informacji o aktualnym członkostwie GVRP i VLAN w sieci.

7.2.4.1 Q-in-Q

„Q-in-Q Tunneling“ określany jest również jako „VLAN Stacking“. Wykorzystywana jest przy tym technologia 802.1Q double tagging. Q-in-Q wykorzystywana jest przez ISP (Internet Service Provider), którzy wykorzystują TLS („**T**ransparent **L**AN **S**ervices“) i którzy mają swoje własne sieci VLAN niezależnie od VLAN klienta. Standardowo każda sieć VLAN dostawcy usług łączy ze sobą grupę lokalizacji klienta. VLAN dostawcy usług może jednak być użytkowana wspólnie przez kilku klientów, wykazujących te same punkty końcowe i wymagania QoS sieci VLAN. Tak zwane „Double Tagging“ przedstawia stosunkowo prostą metodę implementacji transparentnej sieci LAN. Osiągane jest to przez enkapsulację „ETHERNET Frames“. W procesie tym w „ETHERNET Frames“, które wysyłane są przez wejściowy PE („Provider Edge“), zostaje zagnieżdżony drugi lub zewnętrzny znacznik VLAN. Ten znacznik VLAN odpowiada VLAN dostawcy usług. Gdy ramka osiągnie docelowy PE, zostaje otwarta sieć VLAN dostawcy usług. Adres docelowy hermetyzowanej ramki i VLAN ID zostają zastosowane do kolejnych decyzji L2, podobnie jak „ETHERNET Frame“, przychodząca z fizycznego portu ETHERNET. Znacznik VLAN dostawcy usług określa członkostwo w VPLS („**V**irtual **P**rivate **L**AN **S**ervice“). Double Tagging łączy kilka sieci VLAN wewnątrz innej sieci VLAN i umożliwia prywatne, dedykowane połączenie ETHERNET między klientami, którzy chcą w sposób transparentny dotrzeć do swojej podsieci przez kilka sieci. Dostawcy usług mogą tworzyć swoje własne sieci VLAN bez kontaktowania się przez „Double Tagging“ z sieciami VLAN klientów. Umożliwia to połączenie klientów z ISP i ASP („**A**pplication **S**ervice **P**roviders“).

Porty połączone z sieciami VLAN dostawców usług określane są jako „Tunnel Ports“, a porty połączone z sieciami VLAN klientów określane są jako „Access Ports“. Gdy port skonfigurowany jest jako „Tunnel Port“, wszystkie wychodzące pakiety danych na tym porcie są transmitowane ze znacznikiem SPVLAN (SPVID i priorytet 1p). Wchodzący pakiet może mieć dwa znaczniki (SPVLAN + CVLAN), jeden znacznik (SPVLAN lub CVLAN) lub nie mieć żadnego znacznika.
W każdym przypadku pakiet wysyłany jest ze znacznikiem SPVLAN. Gdy port skonfigurowany jest jako „Access Port“, wchodzące pakiety danych mogą mieć tylko jeden znacznik CVLAN (CVID i priorytet 1p) lub nie mieć żadnego znacznika. Tym samym wszystkie pakiety danych wysyłane z „Access Ports“ albo nie mają znacznika, albo mają pojedynczy znacznik (CVLAN). Gdy port skonfigurowany jest jako zwykły port, „Double Tagging Frames“ zostają zignorowane.

Double Tagging Format

Tag VLAN („VLAN Stacking“ dostawcy usług lub IEEE 802.1Q klienta) składa się z następujących trzech pól:

TPID	Priority	VID

TPID

TPID („**T**ag **P**rotocol **I**dentifier“) jest standardowym kodem ETHERNET, identyfikującym ramkę i wskazującym, czy zawiera ona informację o znaczniku IEEE 802.1Q. Wartość w tym polu wynosi 0x8100 jak opisano w IEEE 802.1Q. Inni dostawcy mogą też stosować inną wartość, jak chociażby 0x9100.

„Tunnel TPID“ jest typem znacznika „VLAN Stacking“, który switch dodaje do wychodzących ramek, wysyłanych przez „Tunnel Port“ urządzeń PE dostawcy usług.

Priority

Priorytet dotyczy standardu IEEE 802.1p, który pozwala dostawcy usług na nadawanie priorytetów pakietom danych na podstawie ich CoS („Class of Service“), za które klient zapłacił. „0“ oznacza tu najniższy poziom priorytetu, a „7“ najwyższy.

VID

VID („**V**LAN **ID**“). SP VID jest VID dla drugiego lub zewnętrznego znacznika VLAN (dostawcy usług). CVID jest VID dla pierwszego lub wewnętrznego znacznika VLAN (klienta).

Poniżej przedstawiono formaty ramek dla „ETHERNET Frame“ bez znacznika, ramki 802.1Q z pojedynczym znacznikiem (klient) i ramki 802.1Q z podwójnym znacznikiem (dostawca usług).

Ramka bez znacznika	DA		Len lub Etype	Dane	FCS						
Ramka z pojedynczym znacznikiem	DA	SA	TPID	P	VID	Len lub Etype	Dane	FCS			
Ramka z podwójnym znacznikiem	DA	SA	Tunnel TPID	P	VID	TPID	P	VID	Len lub Etype	Dane	FCS

DA	Adres docelowy
SA	Adres źródłowy
Tunnel TPID	„Tag Protocol Identifier“ dodany na „Tunnel Port“
VID	VLAN ID
Len lub Etype	Długość lub typ ramki ETHERNET
Dane	Dane ramki
FCS	Frame Check Sequence (pole sumy kontrolnej)

Role portów przy VLAN Stacking

Przy „VLAN Stacking“ każdy port może mieć przydzieloną jedną z trzech „ról“: „normal“, „Access Port“ lub „Tunnel Port“.

- Dla normalnego przełączania ramki IEEE 802.1Q należy wybrać „normal“ (brak „VLAN Stacking“).
- Dla portów wejściowych na urządzeniach PE dostawcy usług należy wybrać „Access Port“. Wchodząca ramka traktowana jest jako ramka bez znacznika, więc może być dołączony drugi znacznik VLAN (zewnętrzny znacznik VLAN).
- Dla portów wyjściowych w obszarze PE dostawcy usług należy wybrać „Tunnel Port“. Wszystkie sieci VLAN należące do klienta mogą być łączone w pojedynczej sieci VLAN dostawcy usług (przy zastosowaniu zewnętrznego znacznika VLAN, zdefiniowanego przez SP VID).

Wskazówka



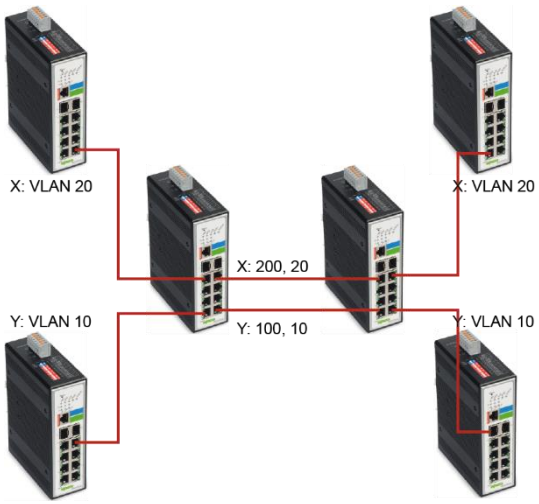
Konfiguracja Q-in-Q

Aby ramki z podwójnym znacznikiem mogły być przełączane poprawnie, użytkownicy muszą skonfigurować w switchu Q-in-Q sieć VLAN dostawcy usług (SPVLAN). Wtedy znaczniki te mogą być przełączane poprawnie zgodnie z SP VID. W SPVLAN powinny być zawarte wszystkie przynależne „Tunnel Ports“ i „Access Ports”. Poza tym „Tunnel Ports“ powinny być skonfigurowane jako porty ze znacznikiem, a „Access Port“ jako porty bez znacznika.

7.2.4.2 Port-based Q-in-Q

Enkapsulacja Q-in-Q może być używana do konwersji pakietu 802.1Q z pojedynczym znacznikiem na pakiet Q-in-Q z podwójnym znacznikiem. Enkapsulacja Q-in-Q może być oparta na portach lub ruchu. Oparta na porcie enkapsulacja Q-in-Q może być używana do enkapsulacji wszystkich przychodzących pakietów danych w porcie z tym samym znacznikiem zewnętrznym SPVID. Tryb ten jest mniej elastyczny.

Na poniższej ilustracji X i Y są klientami sieci dostawcy usług (SPN) z tunelami VPN między ich odpowiednimi głównym i lokalnym miejscem prowadzenia biznesu. Obie grupy mają dla swojej grupy VLAN identyczny znacznik VLAN. Dostawca usługi może obie te sieci VLAN rozróżnić wewnątrz swojej sieci przez dodanie na swoim urządzeniu PE A klientowi X znacznika 100, a klientowi Y znacznika 200, a następnie usunięcie tych znaczników na urządzeniu PE B, gdy ramka danych znów opuści sieć.



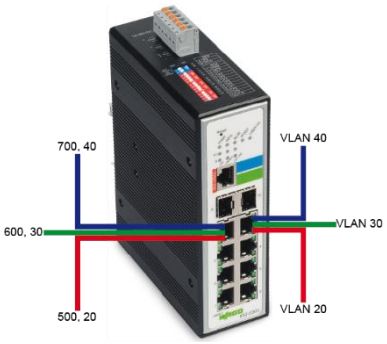
Ilustracja 17: Q-in-Q na bazie portów

Ten przykład pokazuje, jak switch A skonfigurowany jest z portem 1 na switchu w celu oznaczenia wchodzących ramek z VID dostawcy usługi wynoszącym 200 (porty połączone z siecią klienta X) i jak skonfigurowany jest port 7 w celu oznaczenia wchodzących ramek z VID dostawcy usługi wynoszącym 100 (porty połączone z siecią klienta Y). Ponadto pokazuje, jak przyporządkowane są priorytety dla portów od 1 do 3 i portów od 7 do 4.

7.2.4.3 Selektywne Q-in-Q

Q-in-Q na bazie ruchu danych określane jest również jako selektywne Q-in-Q. Umożliwia switchowi dodawanie do ramek wchodzących na porcie odpowiednio do ich wewnętrznych znaczników VLAN różnych zewnętrznych znaczników VLAN. W selektywnym trybie Q-in-Q switch przeprowadza klasyfikację ruchu danych odbywającego się na porcie na podstawie VLAN ID. Gdy użytkownik stosuje dla różnych usług różne VLAN ID, ruch danych może być klasyfikowany na podstawie VLAN ID. Przykład: VLAN ID 100 nadawany jest dla serfowania w Internecie na komputerze, VLAN ID 200 dla IPTV, a VLAN ID 300 dla klientów VIP. Po odebraniu danych użytkownika switch oznacza ruch danych przez serfowanie w Internecie na PC wartością 500 jako zewnętrzny znacznik SPVID, dane IPTV wartością 600 i dane klientów VIP wartością 700.

Poniższy przykład pokazuje konfigurację portu 3 na switchu w celu nadania wchodzącym ramkom znaczników dla różnych VID i priorytetów dostawcy usług.



Ilustracja 18: Przykład konfiguracji

7.2.4.3.1 DHCP Relay

Ponieważ wiadomość „DHCPDISCOVER“ („**D**ynamic **H**ost **C**onfiguration Protocol“) jest wiadomością broadcast i broadcasty przechodzą tylko przez inne segmenty, gdy są wyraźnie rutowane, należy w interfejsie rutera skonfigurować „DHCP Relay Agent“, aby wszystkie wiadomości „DHCPDISCOVER“ mogły być przekierowane do serwera DHCP. Alternatywnie ruter można skonfigurować również tak, aby przesyłał wiadomości DHCP i BOOTP. W sieci rutingu „DHCP Relay Agents“ potrzebne byłyby, gdy ma być zaimplementowany tylko jeden serwer DHCP.

„DHCP Relay“, który jest albo hostem, albo ruterem IP, czeka na wiadomości „DHCP Client“, dochodzące przez podsieć, i przekazuje je bezpośrednio do skonfigurowanego serwera DHCP. Serwer DHCP odsyła wiadomości odpowiedzi DHCP z powrotem bezpośrednio do „DHCP Relay Agent“, który następnie przekazuje je dalej do „DHCP Client“. Administrator DHCP używa „DHCP Relay Agents“ do scentralizowania serwerów DHCP, aby serwer DHCP nie musiał znajdować się w każdej podsieci.

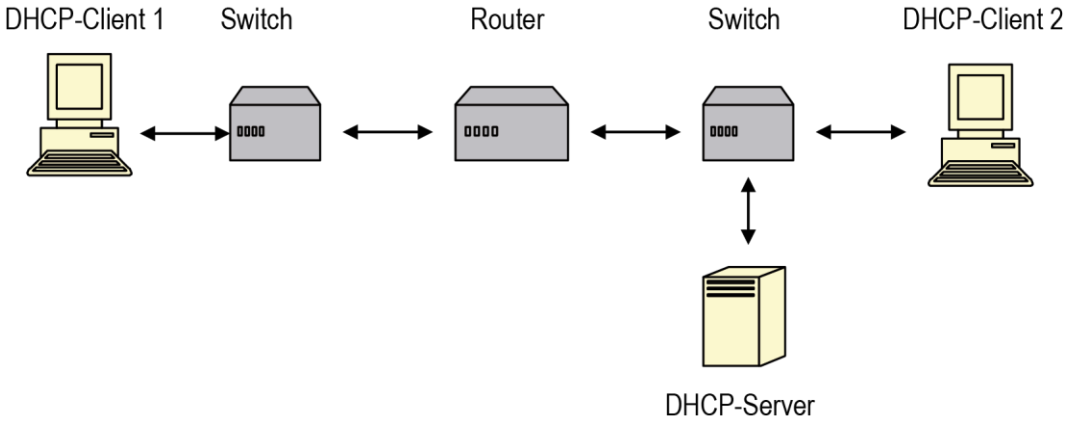
W mniejszych sieciach DHCP zazwyczaj wykorzystuje broadcasty, jednak w określonych okolicznościach wykorzystywane są także adresy unicast. Może to być sytuacja, gdy sieci mają pojedynczy serwer DHCP, udostępniający adresy IP dla kilku podsieci. Ruter dla takiej podsieci odbiera broadcasty DHCP i konwertuje je na unicasty (z docelowym adresem MAC/IP skonfigurowanego serwera DHCP, źródłowym adresem MAC/IP rutera). Pole GIADDR na stronie głównej DHCP zawiera adres IP interfejsu w ruterze, przez który odebrał on żądanie DHCP. Serwer DHCP wykorzystuje pole GIADDR do identyfikacji podsieci dla urządzenia i wybiera adres IP z właściwej „Pool“. Potem serwer DHCP przesyła „DHCP OFFER“ przez unicast z powrotem do rutera, który konwertuje ją z powrotem na broadcast i wysyła do właściwej podsieci, w której znajduje się urządzenie, żądające adresu.

Konfiguracje

Użytkownik może aktywować lub dezaktywować w switchu „DHCP Relay“. Może to wymagać również specyficznej sieci VLAN. Gdy funkcja „DHCP Relay“ jest w switchu dezaktywowana, dezaktywowana jest dla wszystkich wirtualnych sieci lokalnych, nawet jeśli była aktywowana dla pojedynczych VLAN.

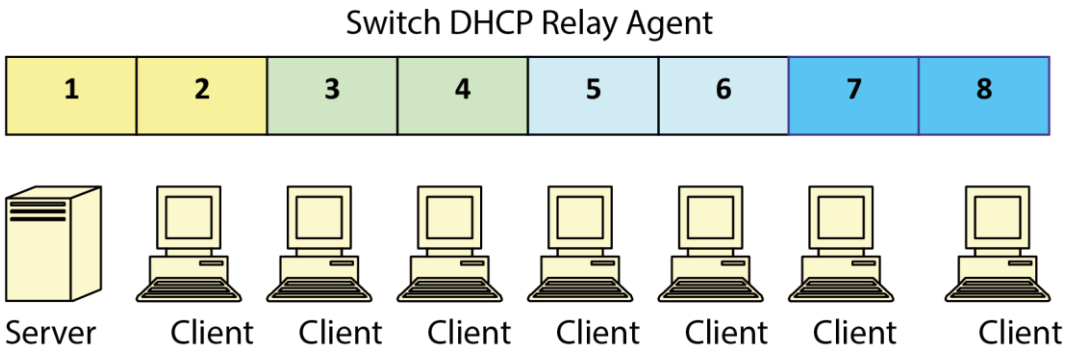
Zastosowania

- **Zastosowanie 1 (przez ruter**)
  „DHCP Client“ 1 i „DHCP Client“ 2 znajdują się w różnych segmentach IP. Adres IP otrzymują oni jednak z tego samego serwera DHCP.



Ilustracja 19: Zastosowanie 1 (przez ruter)

- **Zastosowanie 2 (lokalnie w różnych sieciach VLAN)**
  „DHCP Client“ 1 i „DHCP Client“ 2 znajdują się w różnych sieciach VLAN. Adres IP otrzymują oni jednak z tego samego serwera DHCP.



Ilustracja 20: Zastosowanie 2 (lokalnie w różnych sieciach VLAN)

VLAN 1: Port 1, 2 (Management VLAN)
VLAN 2: Port 3, 4
VLAN 3: Port 5, 6
VLAN 4: Port 7, 8

Serwer DHCP -> Port 1.
Klient DHCP -> Port 2, 3, 4, 5, 6, 7, 8.

Rezultat: Porty 2, 3, 4, 5, 6, 7 i 8 połączone z hostami mogą otrzymać IP od serwera DHCP.

Wskazówka

Połączenie serwera DHCP
Serwer DHCP musi być połączony z portami uczestników zarządzającej sieci VLAN.
W „Management VLAN“ musi być aktywowana funkcja „DHCP Relay“.

7.2.4.3.2 DHCP Options

DHCP (Dynamic Host Configuration Protocol) to bardziej zaawansowana wersja BootP, kompatybilna z tym protokołem.
„DHCP Option 82“ to „**DHCP** Relay Agent Information **Option**“.
Option 82 została opracowana, aby umożliwić „DHCP Relay Agent“ dołączenie do żądania specyficznych dla połączenia informacji, która przesyłana jest dalej do serwera DHCP. Opcja ta wykorzystuje w szczególności dwie podopcje: „Circuit ID“ i „Remote ID“.

„DHCP Option 82“ działa na bazie „DHCP Snooping“ i/lub „DHCP Relay”.

Switch monitoruje pakiety DHCP i dołącza do pakietów „DHCPDISCOVER“ i „DHCPREQUEST“ kilka informacji. Następnie switch usuwa „DHCP Option 82“ z pakietów „DHCPOFFER“ i „DHCPACK“. Serwer DHCP przydziela potem klientowi, zgodnie z tymi informacjami, domenę IP.

Maksymalna długość tych informacji wynosi 32 znaki.

W dużych miastach i na terenach gęsto zaludnionych z dostępem do sieci ETHERNET DHCP może centralnie zarządzać przydzielaniem adresów IP dla dużej liczby użytkowników. Gdy funkcja „DHCP Option 82“ jest w switchu aktywowana, urządzenie użytkownika można zidentyfikować na podstawie portu switcha, przez który łączy się ono z siecią (dodatkowo do jego adresu MAC). Nawet jeśli wiele hostów łączy się w sieci użytkowników LAN przez ten sam port switcha, każdy jeden host można jednoznacznie zidentyfikować.

Gdy „DHCP Snooping Information Option 82“ jest w switchu aktywowany, następuje taka sekwencja zdarzeń:

- Host („DHCP Client“) generuje żądanie DHCP i wysyła je do sieci.
- Gdy switch odbierze żądanie DHCP, dołącza do pakietu informacje „Option 82”. Informacje te zawierają adres MAC switcha (podopcja „Remote ID“), „Port Identifier“ i „VLAN-Mod-Port“, z którego odebrany został pakiet (podopcja „Circuit ID“).
- Gdy dla „Relay Agent“ został skonfigurowany adres IP, switch dołącza go do pakietu DHCP.
- Switch przekazuje żądanie DHCP z polem Option 82 do serwera DHCP.
- Serwer DHCP odbiera pakiet. Gdy serwer obsługuje Option 82, może użyć „Remote ID“, „Circuit ID“ lub obie funkcje do przydzielenia adresów IP i implementacji dyrektyw, jak na przykład ograniczenie liczby adresów IP, która może być przydzielona pojedynczemu „Remote ID“ lub „Circuit ID“. Następnie serwer DHCP transmituje pole Option 82 do odpowiedzi DHCP.
- Gdy żądanie zostało przesłane ze switcha do serwera, serwer DHCP przekazuje odpowiedź do switcha jako unicast. Gdy klient i serwer znajdują się w tej samej podsieci, serwer przekazuje odpowiedź jako broadcast. Switch weryfikuje potem pierwotnie wprowadzone dane Option 82, sprawdzając pole „Remote ID“ i w niektórych warunkach także „Circuit ID“. Switch usuwa pole Option 82 i przekazuje pakiet dalej do portu switcha, który połączony jest z „DHCP Client“ i wysłał żądanie DHCP.

Option Frame Format

Tabela 21: Option Frame Format

Kod	Len	Agent Information Field					
82	N	i1	i2	i3	i4	…	iN

„Agent Information Field“ składa się z sekwencji krotek (podopcja/długość/wartość) dla każdej podopcji, które kodowane są w następujący sposób:

Tabela 22: Option Frame Format

Podopcja	Len	Wartość podopcji					
1	N	s1	s2	s3	s4	…	sN

Agent DHCP Kod podopcji	Opis podopcji
1	Podopcja „Agent Circuit ID”
2	Podopcja „Agent Remote ID”

Tabela 23: Frame Format podopcji „Circuit ID“

Typ podopcji	Długość	Typ „Circuit ID”	Długość	VLAN	Moduł	Port
1	6	0	4	2	1	1

Tabela 24: Frame Format podopcji „Remote ID“

Typ podopcji	Długość	Typ „Circuit ID”	Długość	Adres MAC
2	8	0	6	6

Tabela 25: Format podopcji „Circuit ID“

Kod	Len	Typ podopcji	Długość	ID slota	ID portu	VLAN ID	Informacja
0x52	0x0c	0x01	0x0a	0x01	0x01	0x0002	justin

7.2.5 DHCP Server

Przy konfiguracji parametrów sieci przez DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) urządzenie ETHERNET po inicjalizacji przesyła samodzielnie żądanie klienta do serwera DHCP. To żądanie jest telegramem broadcast, zawierającym adres sprzętu (MAC ID, adres MAC) urządzenia ETHERNET.

Serwer DHCP otrzymuje żądanie. Serwer ten zarządza pulą adresów IP i dla każdego adresu IP zapisuje należny mu adres MAC oraz inne parametry. Jeśli żądany adres MAC jest już w „Pool“, serwer odpowiada przechowywanym już adresem IP. Ale serwer DHCP odpowiada również na odpowiedzi od dotychczas nieznanych adresów MAC: jeśli ma jeszcze w swoim zakresie wolne adresy IP,

przydziela jednemu z tych wolnych adresów nowy adres MAC i wysyła odpowiedź.

Urządzenie ETHERNET czeka na odpowiedź serwera DHCP. Nadchodzące pakiety danych zawierają między innymi adres IP i adres MAC urządzenia ETHERNET. Po adresie MAC urządzenie ETHERNET rozpoznaje, czy wiadomość jest przeznaczona dla niego i w razie zgodności przejmuje przesłany adres IP i stosuje go w swoim interfejsie sieciowym.

W razie braku odpowiedzi po 4 sekundach wysyłane jest powtórne żądanie, potem po 8 i ostatnie po 16 sekundach.

Gdy żądania pozostają bez odpowiedzi, generowany jest komunikat o błędzie.

Wskazówka

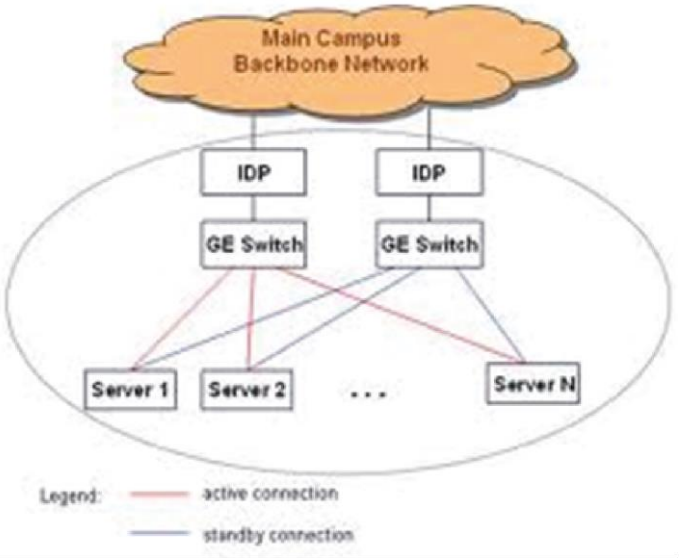


Konfiguracja DHCP nie jest zapisywana!
Należy pamiętać, że przy zastosowaniu DHCP, odmiennie, niż w przypadku konfiguracji BootP, konfiguracja sieci nie jest zapisywana. Urządzenie przy następnym starcie systemu otrzymuje nowy adres IP.

Różnica pomiędzy BooP a DHCP polega na tym, że te dwa protokoły stosują różne metody przyporządkowywania.

7.2.6 Dual Homing

Za pomocą „Dual Homing“ opisywana jest topologia sieci, w której urządzenie połączone jest z siecią przez dwa niezależne punkty dostępu do sieci („Points of Attachment“). Jeden punkt dostępu tworzy połączenie podstawowe, a drugi służy jako rezerwa, na wypadek awarii połączenia podstawowego.

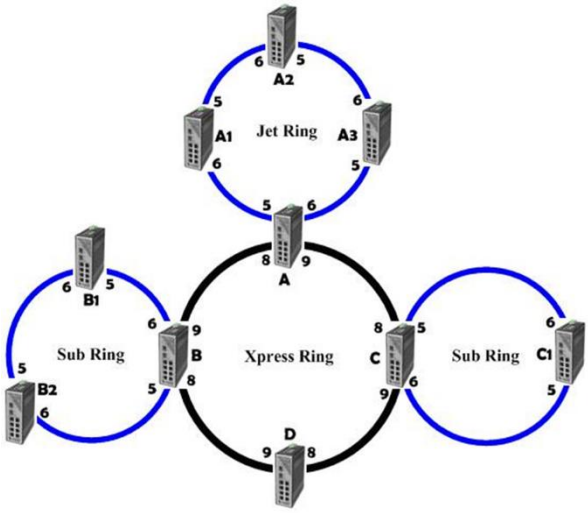


Ilustracja 21: Dual Homing

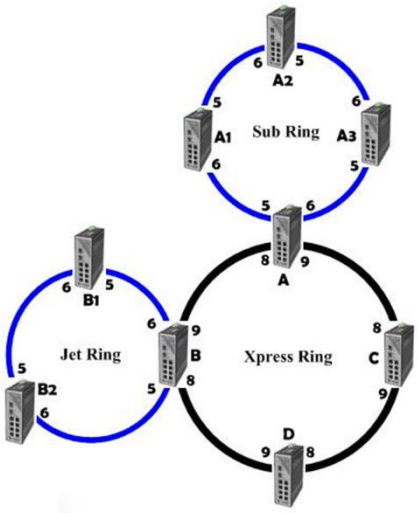
Na przykład połączenia podstawowe i rezerwowe mogłyby być w różny sposób połączone z Internetem. Połączenie podstawowe mogłoby być połączone przez fizyczną sieć, a rezerwowe przez sieć bezprzewodową. Przy aktywowanej funkcji „Dual Homing“ urządzenie łączy się standardowo przez połączenie podstawowe, podczas gdy połączenie rezerwowe pozostaje przerwane. Gdy port lub wszystkie porty mają awarię, urządzenie wybiera połączenie rezerwowe. Gdy w tej sytuacji również połączenie rezerwowe ma awarię, urządzenie pozostaje nieaktywne. Połączenie rezerwowe działa tylko wtedy, gdy podstawowe jest przerwane.

7.2.7 Dual Ring

Za pomocą funkcji „Dual Ring“ można przy użyciu switcha połączyć 2 sąsiadujące ze sobą ringi, bez konieczności użycia dodatkowych portów lub przewodów. Taka konfiguracja pozwala zredukować liczbę potrzebnych portów i obniżyć koszty oprzewodowania, gdyż nie są potrzebne dodatkowe przewody.



Ilustracja 22: Dual Ring Switch ABC



Ilustracja 23: Dual Ring switch AB

Dodatkowo można również zintegrować inne urządzenia końcowe ETHERNET WAGO w Jet Ring. Należy przy tym aktywować w urządzeniach mechanizm Fast Aging.

Wskazówka

Więcej informacji
Więcej informacji można znaleźć w podręcznikach do urządzeń końcowych ETHERNET WAGO.
Podręczniki te są dostępne do pobrania na stronie www.wago.com.

7.2.8 ERPS

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

Ochrona pierścieni ETHERNET zawiera następujące funkcje:

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

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

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

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

W nieprzeciążonym pierścieniu ETHERNET, w którym znajdują się wszystkie węzły pierścienia ETHERNET bez obciążenia (tzn. nie ma wykrytych awarii, aktywnych automatycznych lub zewnętrznych poleceń i odbierane są tylko wiadomości R-APS (NR, RB)), w którym długość światłowodu jest mniejsza niż 1200 km i który ma mniej niż 16 węzłów ETHERNET, czas przełączania (czas transferu, jak definiuje to ITU-T G.808.1) w przypadku awarii linku pierścienia nie powinien przekraczać 50 ms.

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

Switch wspiera maksymalnie sześć pierścieni.

Guard Timer

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

WTR Timer

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

WTB Timer

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

Hold-off Timer

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

ERPS z trybem rewersji i bez

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

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

Control VLAN

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

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

Instancja

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

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

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

Wskazówka



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

7.2.9 Link Aggregation

7.2.9.1 Static Trunk

„Link Aggregation“ (zwana też „Trunking“) jest grupowaniem fizycznych portów w jeden logiczny link o większej pojemności. Przy łączeniu portów korzystne cenowo może być zastosowanie większej liczby mniej szybkich linków, niż nie wykorzystanie w pełni jednego szybkiego, ale drogiego „Port Link“.

Jednak im więcej portów zostanie powiązanych, tym mniej jest ich dostępnych. „Trunk Group“ jest logicznym linkiem, zawierającym kilka portów. Switch wspiera zarówno statyczne, jak i dynamiczne „Link Aggregation“.

Wskazówka



„Link Aggregation“
W dobrze zaprojektowanej sieci zaleca się stosowanie tylko statycznej „Link Aggregation”. Zapewnia to większą stabilność sieci i kontrolę dla switcha przez „Trunk Groups“.

7.2.9.2 LACP

Zgodnie ze standardem IEEE 802.3ad switch wspiera statyczny i dynamiczny (LACP) „Port Trunking“. W standardzie IEEE 802.3ad opisany został LACP („**L**ink **A**ggregation **C**ontrol **P**rotocol“) dla dynamicznego tworzenia i zarządzania „Trunk Groups“.

Przy aktywacji na porcie „LACP Link Aggregation“ może on automatycznie łączyć się z portami na innym końcu połączenia, w celu utworzenia „Trunk Groups”. Ponadto LACP na redundancję portów, tzn. że gdy aktywny port ma awarię, inny port aktywuje się jako „zapasowy“ bez potrzeby ingerencji użytkownika.
Należy przy tym zwrócić uwagę na następujące kwestie:

- Wszystkie porty muszą być połączone peer-to-peer z tym samym switchem ETHERNET i skonfigurowane na „LACP Trunking“.
- LACP działa tylko przez połączenia full duplex.
- Wszystkie porty w tej samej „Trunk Group“ muszą być zgodne pod względem typu, medium, prędkości, trybu duplex i ustawień dla „Flow Control“.
- „Trunk Groups“ lub LACP należy skonfigurować, zanim zostanie nawiązane połączenie ze switchem ETHERNET, aby uniknąć pętli w topologii sieci.

System Priority

Za pomocą „System Priority LACP“ określana jest przynależność do LAG („**L**ink **A**ggregation **G**roup“) i identyfikowane jest urządzenie dla innych switchy podczas negocjacji LAG.
Switch o najniższym priorytecie systemowym (i najniższym numerze portu, gdy priorytet systemowy jest ten sam) staje się „serwerem“ LACP. Serwer ten steruje pracą ustawień LACP. Im niższy numer, tym wyższy poziom priorytetu.

System ID

„LACP System ID“ jest kombinacją wartości priorytetu systemowego LACP i adresu MAC rutera.

Administrative Key

„Administrative Key“ definiuje zdolność portu do łączenia się z innymi portami. Zdolność ta określana jest przez następujące czynniki:

- Fizyczne właściwości portu, jak na przykład prędkość danych, zdolność do pracy duplex i peer-to-peer lub podzielone medium transmisji
- Ograniczenia konfiguracyjne wprowadzone przez użytkownika

Port Priority

„Port Priority“ definiuje, które porty przechodzą w tryb stand by, gdy istnieją ograniczenia sprzętowe, uniemożliwiające wiązanie wszystkich kompatybilnych portów.

7.2.10 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.

7.2.11 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.

7.2.12 Jet Ring

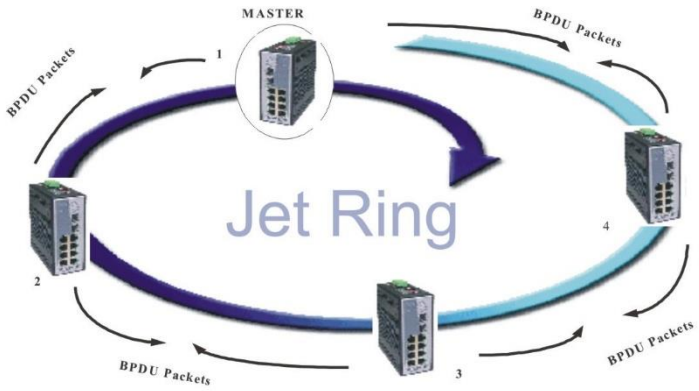
Przez ustawienie w sieci funkcji Jet Ring (połączenie redundantne) krytyczne połączenia są lepiej chronione przed wystąpieniem błędów i pętli. Dodatkowo czas awarii sieci spada poniżej 300 ms.

Za pomocą funkcji Jet Ring użytkownicy mogą stworzyć rezerwową trasę do sieci. Dzięki temu w przypadku, gdy połączenie zostanie nagle przerwane lub zerwane, udostępniana jest zapasowa trasa transmisji danych. Funkcja ta jest niezmiernie ważna w aplikacjach przemysłowych, gdyż na skutek awarii połączenia bez zabezpieczenia czas zatrzymania sieci może sięgnąć nawet kliku minut, co wiąże się ze znacznymi stratami.

Protokół Jet Ring służy do optymalizacji rezerwowych połączeń komunikacyjnych oraz umożliwienia ponownego nawiązania połączenia w krótkim czasie. Funkcja Jet Ring powoduje automatyczne wyznaczenie switcha jako „mastera“ sieci i automatyczną blokadę złącz. Zapobiega to temu, że pakiety danych wysyłane są przez wszystkie rezerwowe segmenty pętli sieć. Gdy segment pierścienia, w którym wystąpił błąd, zostaje oddzielony od reszty sieci, protokół Jet Ring automatycznie ponownie dostosowuje pierścień tak, że część sieci, która została oddzielona, ponownie nawiązuje kontakt z resztą sieci.

Krok 1

Funkcję Jet Ring na poniższej ilustracji można zastosować dla połączenia czterech jednostek przemysłowego switcha zarządzalnego.



Ilustracja 24: Jet Ring

Krok 2

Przez funkcję Jet Ring zostaje wtedy automatycznie wybrany switch Arbiter, potem sieć jest gotowa do pracy.

7.2.13 PoE (Power over Ethernet)

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

Tabela 26: Porównanie PoE i PoE+

Cecha	PoE	PoE+
Standard	IEEE 802.3af	IEEE 802.3at
Moc PSE	15,4 W	25,4 W
Maks. moc PD	12,95 W	21,90 W
Maks. prąd na parę żył	350 mA	600 mA
Standard transmisji	10BASE-T 100BASE-TX	10BASE-T 100BASE-TX 1000BASE-T

Przykład obliczeń dla PoE+:

Tabela 27: Przykład obliczeń dla PoE+

Pobór mocy	Wartość
4 porty po 30 W	120 W
Maks. pobór mocy	18 W
Łącznie	**<138 W**

Dla PoE wymagane są specjalne urządzenia zasilające (PSE = „**P**ower **S**ourcing **E**quipment“) i urządzenia końcowe (PD = „**P**owered **D**evice“).

Opis klas mocy PoE można znaleźć w załączniku (patrz rozdział „Załącznik” > „Klasy mocy PoE”).

PoE w tym produkcie można zrealizować w następującym trybie pracy.

Tryb pracy A

W tym trybie zasilanie jest modulowane na przewodach danych („zasilanie fantomowe”).

Tryb pracy A może być stosowany w następujących standardach transmisji:
- 10BASE-T
- 100BASE-TX
- 1000BASE-T

W tym trybie pary żył 1 i 2 (+) oraz 3 i 6 (−) są wykorzystywane do zasilania. Do tego można użyć 4-żyłowego lub 8-żyłowego przewodu ETHERNET, który odpowiada co najmniej kategorii 5 lub 5e (patrz rozdział „Załącznik” > „Przewód RJ-45”).

7.2.14 Static Route

Trasy statyczne definiują wyraźne ścieżki między dwoma systemami końcowymi. Trasy te definiowane są przy instalacji sieci i z reguły zapisywane są w ruterze jako stała tabela routingu. Urządzenia końcowe są przyporządkowane do rutera, przez który są dostępne i mogą osiągać inne cele. Tras statycznych nie można automatycznie aktualizować. W przypadku zmian sieci trasy statyczne należy ręcznie skonfigurować na nowo. Trasy statyczne potrzebują mniejszej szerokości pasma niż trasy dynamiczne. W celu wyliczenia i analizy aktualizacji routingu nie są wykorzystywane cykle CPU.

IP Forwarding

IP Forwarding umożliwia przesyłanie pakietów IP między hostami poza granice sieci. Jeśli dwa hosty znajdują się w różnych sieciach, dane muszą być przesyłane przez router łączący obie sieci. W przypadku dużych sieci jak np. Internet, ruterów może być wiele. Podczas tworzenia tras podawany jest tylko następny host w drodze do hosta docelowego, a nie cała trasa. Jeśli dane są transportowane przez kilka ruterów, trasy do następnego rutera muszą być również utworzone na pośrednich ruterach.

IP Forwarding funkcjonuje zarówno jako ruter, jak również jako routing Inter VLAN z trunk stick.

Baza danych routingu odgrywa ważną rolę przy kierowaniu pakietów danych. Rutery zapełniają bazę danych routingu bądź przez ręczne konfiguracje, bądź za pomocą dynamicznych protokołów routingu.

Ręczne konfiguracje routingu obliczane są jako trasy statyczne. Zawsze gdy ruter odbierze pakiet IP, wywoływany jest docelowy adres IP i w tabeli routingu wyszukiwana jest trasa zgodności o najdłuższym prefiksie. Pakiet zostaje przekierowany do przydzielonego następnego hosta.

7.2.15 STP

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

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

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

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

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

Stany portów przy switchach STP

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

- **„Forwarding“**
  Port znajduje się w trybie roboczym i odbiera oraz wysyła dane. STP monitoruje potem wchodzące dane BPDU, czy wskazują, że port powinien przejść w stan „Blocking“, aby zapobiec powstaniu pętli.
- **„Disabled"**
  Nie jest to, dokładnie rzecz ujmując, część STP, gdyż administrator sieci może ręcznie dezaktywować port.

Role portów przy bridge'u RSTP

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

Wskazówka



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

Terminologia STP

Root Bridge

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

Path Cost

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

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

Tabela 28: Koszty trasy STP

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

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

Forward Time (Forward Delay)

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

Max Age

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

Hello Time

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

STP

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

Switche obsługujące STP wymieniają ze sobą regularnie dane BPDU. Gdy w sieci LAN powiązanej za pomocą bridge'a zmienia się topologia, rozpinane jest nowe drzewo. Gdy powstanie stabilna topologia sieci, wszystkie bridge'e czekają na „Hello BPDUs“, które są transmitowane przez „Root Bridge“. Gdy po zdefiniowanym wcześniej interwale („Max Age“) bridge nie odbierze „Hello BPDUs“, uznaje, że połączenie z „Root Bridge“ zostało przerwane. Potem rozpoczyna 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 „**B**ridge **P**rotocol **D**ata **U**nits“ (BPDU) do wszystkich bridge'ów i przez dane konfiguracyjne zawarte w pakietach BPDU ustala konfigurację sieci.

7.2.16 Xpress Ring

Xpress Ring reprezentuje technologię pierścienia o szybkim czasie reakcji z funkcją samoregeneracji, umożliwiającą przywracanie przerwanych połączeń w sieci w ciągu 50 ms.

Szybkie przywracanie połączeń i redundancja są ważnymi funkcjami zwiększającymi niezawodność w systemach pracujących non stop.

W przypadku awarii segmentu dobrze zaprojektowana sieć ze switchem „Arbiter“. i portami pierścienia może zostać naprawiona w bardzo krótkim czasie.

Switch w Xpress Ring może odgrywać tylko dwie role: „Forwarder“ lub „Arbiter“. Zawsze może być tylko jeden „Arbiter“, podczas gdy wszystkie inne switche pełnią rolę „Forwarder“.

Jeden z portów switcha „Arbiter“ wprowadzany jest w stan zablokowania. Gdy jedno z połączeń pierścienia ma awarię, zablokowany port zostaje przywrócony do stanu przesyłania.

7.3 Security

7.3.1 IP Source Guard

„IP Source Guard“ jest funkcją zabezpieczającą, filtrującą ruch danych IP na niezabezpieczonych portach layer2 na podstawie podłączenia do bazy danych „DHCP Snooping“ lub ręcznie skonfigurowanego połączenia źródłowego IP. Za pomocą tej funkcji można zapobiegać atakom takim jak „IP Spoofing“ (wysyłanie pakietów IP z fałszywym adresem IP nadawcy), gdy host próbuje zafałszować adres IP innego hosta. Każdy ruch danych IP, wchodzący do interfejsu z innym adresem źródłowym IP niż ten przydzielony (przez DHCP lub statyczną konfigurację), zostaje wyfiltrowany na niezabezpieczonych portach Layer2.

Funkcja ta stosowana jest na niezabezpieczonych interfejsach Layer2 w kombinacji z „DHCP Snooping”. Tabela połączeń źródłowych IP konfigurowana jest ręcznie (statyczne połączenie źródłowe IP) lub tworzona i zarządzana jest z informacji funkcji „DHCP Snooping“. Każdy wpis w tej tabeli zawiera adres IP oraz przynależne adresy MAC i VLAN. „IP Source Guard“ wspiera tylko porty layer2, włącznie z „Access Ports“ i „Trunk Ports“.

„IP Source Guard“ obejmuje następujące funkcje:
1. DHCP Snooping
2. DHCP Binding Table
3. ARP Inspection
4. Blacklist Filter (ARP Inspection za pomocą tabeli adresów MAC)

7.3.1.1 DHCP Snooping

„DHCP Snooping“ jest funkcją DHCP zwiększającą bezpieczeństwo sieci poprzez filtrowanie niezabezpieczonych wiadomości DHCP oraz tworzenie i wykorzystanie podłączenia do bazy danych „DHCP Snooping“ (zwanego również tabelą połączeń „DHCP Snooping“).

„DHCP Snooping“ działa jako zapora sieciowa między niezabezpieczonymi hostami i serwerem DHCP. Może być wykorzystywana do rozróżnienia między interfejsami niezabezpieczonymi, połączonymi z końcowymi użytkownikami, i interfejsami zabezpieczonymi, połączonymi z serwerem DHCP lub innym switchem.

Tabela połączeń „DHCP Snooping“ zawiera adres MAC, adres IP, „Lease Time” (czas dzierżawy), rodzaj połączenia, numer VLAN i informacje o lokalnych niezabezpieczonych interfejsach switcha.

Gdy switch odbiera pakiet od niezabezpieczonego interfejsu, a interfejs należy do sieci VLAN, w której aktywowany jest „DHCP Snooping“, switch porównuje adresy źródłowe MAC z adresem sprzętowym „DHCP Client“. Jeśli adresy zgadzają się (normalny przypadek), switch przekierowuje pakiet dalej. Jeśli nie, odrzuca go.

Switch odrzuca pakiet DHCP w następujących sytuacjach:
- Pakiet z serwera DHCP, jak chociażby DHCPOFFER, DHCPACK, DHCPNAK lub DHCPLEASEQUERY, odbierany jest przez niezabezpieczony port.
- Pakiet zostaje odebrany przez niezabezpieczony interfejs, a adres źródłowy MAC i adres sprzętowy „DHCP Client“ nie zgadzają się z żadnym z aktualnych połączeń.

Za pomocą „DHCP Snooping“ nie można wyfiltrować w sieci autoryzowanych pakietów DHCP i dynamicznie tworzyć tabeli połączeń. Zapobiega to otrzymywaniu przez klientów adresów IP od nieautoryzowanych serwerów DHCP.

Trusted vs. Untrusted Ports

Dla „DHCP Snooping“ każdy port jest bądź portem zabezpieczonym („Trusted Port“) lub niezabezpieczonym („Untrusted Port“). Ustawienie to jest niezależne od ustawienia „Trusted/Untrusted“ dla „ARP Inspection“. Można wyspecyfikować maksymalną liczbę pakietów DHCP, jakie może odebrać każdy port („trusted“ lub „untrusted“) na sekundę.

„Trusted Ports“ połączone są z serwerami DHCP lub switchami. Switch odrzuci pakiety DHCP z „Trusted Ports“ tylko wtedy, gdy prędkość transmisji odebranych pakietów jest za wysoka. Switch uczy się od „Trusted Ports“ połączeń dynamicznych.

Wskazówka

Żądania DHCP

Switch odrzuca wszystkie żądania DHCP, gdy aktywowany jest „DHCP Snooping“, ale nie ma „Trusted Ports“.

„Untrusted Ports“ połączone są z uczestnikami. Switch odrzuca pakiety DHCP z tych portów w następujących sytuacjach:

- Pakiet jest pakietem serwera DHCP (np. „OFFER“, „ACK“ lub „NACK“).
- Adres źródłowy MAC i adres źródłowy IP w pakiecie nie zgadzają się z żadnym z aktualnych połączeń.
- Adres źródłowy MAC i port źródłowy w pakiecie „RELEASE” lub „DECLINE” nie zgadzają się z żadnym z aktualnych połączeń.
- Prędkość transmisji odebranych pakietów DHCP jest za wysoka.

Baza danych dla DHCP Snooping

Switch zapisuje tabelę połączeń w pamięci nieulotnej. Switch zostaje ponownie uruchomiony, ładuje statyczne połączenia z pamięci permanentnej, traci przy tym jednak połączenia dynamiczne, więc urządzenia w sieci muszą na nowo wysyłać żądania.

Konfiguracja DHCP Snooping

W celu skonfigurowania „DHCP Snooping“ w switchu należy wykonać następujące działania:

1. Aktywuj „DHCP Snooping” w switchu.
2. Aktywuj „DHCP Snooping” dla każdej sieci VLAN.
3. Skonfiguruj „Trusted Ports” i „Untrusted Ports”.
4. Skonfiguruj statyczne połączenia.

Wskazówka

DHCP Snooping

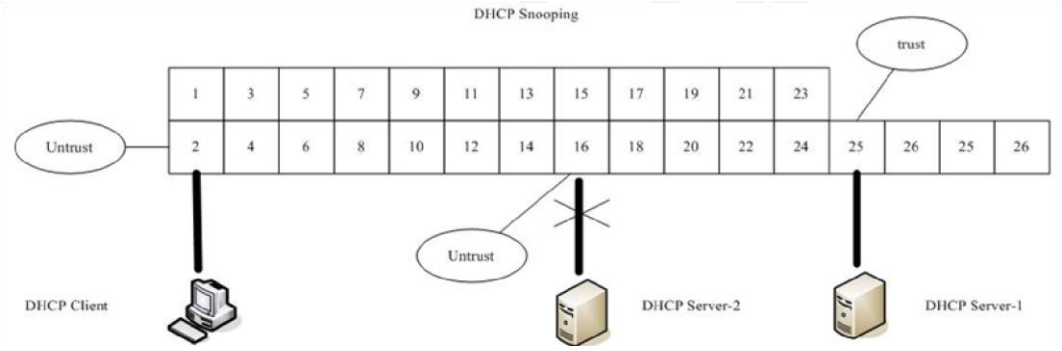
Switch odrzuca wszystkie żądania DHCP, gdy aktywowany jest „DHCP Snooping“, ale nie ma „Trusted Ports“.

Gdy połączenie z tym portem ma usterkę, wyuczone przez ten port wpisy zostają usunięte z tabeli połączeń „DHCP Snooping“.

Należy najpierw aktywować globalny „DHCP Snooping“ i „DHCP Snooping“ dla sieci VLAN.

Do ważnych zadań „DHCP Snooping“ należy:

1 Tworzenie i zarządzanie tabelą połączeń dla funkcji „ARP Inspection“.
2 Filtrowanie pakietów danych z serwerów DHCP, połączonych z „Untrusted Port“.



Ilustracja 25: DHCP Snooping

Pakiety danych z serwerów DHCP, połączonych z „Untrusted Port“, zostają wyfiltrowane.

7.3.1.1.1 Server Screening

Switch wspiera „Server Screening“ – funkcję, która zapobiega dostępowi „Rogue DHCP Servers“ (nieautoryzowane, nieważne serwery DHCP). Oznacza to, że gdy w sieci istnieje jeden lub kilka serwerów DHCP i oferowane są usługi DHCP dla różnych, osobnych grup klientów, pakiety danych z ważnego serwera DHCP przekierowywane są do klienta.

Gdy funkcja ta jest aktywowana, należy najpierw aktywować funkcję „DHCP Snooping“. Switch umożliwia konfigurację maksymalnie trzech ważnych serwerów DHCP.

Gdy nie ma skonfigurowanych serwerów DHCP, oznacza to, że wszystkie serwery DHCP są ważne.

7.3.1.2 Binding Table

W tabeli połączeń „DHCP Snooping“ ujęte są wszystkie informacje hosta, które zostały wprowadzone za pomocą „DHCP Snooping“ (dynamiczne) lub przez użytkowników (statyczne). „ARP Inspection“ wykorzystuje tę tabelę, aby rozstrzygać, czy pakiety ARP mają być przekazywane dalej czy odrzucone. Pakiety ARP wysyłane przez nieważne hosty zostają odrzucone. Po upływie czasu „Lease Time“ wpis zostaje z tabeli usunięty.

Połączenia statyczne są jednoznacznie rozpoznane przez adresy MAC i VLAN ID. Każdy adres MAC i VLAN ID może należeć do jednego statycznego połączenia. Przy tworzeniu połączenia statycznego z adresem MAC i VLAN ID istniejącego już połączenia, nowe połączenie statyczne zastępuje stare.

Połączenia są stosowane przy „DHCP Snooping“ i „ARP Inspection“ do rozróżniania autoryzowanych i nieautoryzowanych pakietów danych w sieci.

Switch rozpoznaje połączenia dynamiczne przez „Snooping“ w pakietach DHCP, a statyczne informacje przez ręczne wpisy z menu „Static Entry Settings“.

7.3.1.3 ARP Inspection

Dynamiczny tryb „ARP Inspection“ („**A**ddress **R**esolution **P**rotocol **Inspection**“) jest funkcją bezpieczeństwa, przy której sprawdzane są pakiety ARP w sieci. Przy dynamicznym trybie „ARP Inspection“ połączenia adresów IP z MAC porównywane są z wpisami z zabezpieczonej bazy danych (baza danych „DHCP Snooping“), zanim pakiet zostanie przekierowany. Dynamiczny tryb „ARP Inspection“ odpytuje pakiety ARP z nieważnym połączeniem adresów IP i MAC, protokołuje je i następnie odrzuca. Funkcja ta oferuje ochronę przed określonymi atakami „man in the middle“.

Dynamiczny tryb „ARP Inspection“ zapewnia, że przekierowane będą tylko ważne zapytania i odpowiedzi ARP.

Switch wykonuje następujące procesy:

- Przechwycenie wszystkich zapytań i odpowiedzi na niezabezpieczonych portach
- Kontrola wszystkich odpytanych pakietów danych o ważne połączenia adresowe IP i MAC przed aktualizacją lokalnej pamięci podręcznej ARP lub przed przekazaniem pakietu danych do odpowiedniego celu

Trusted Port i Untrusted Port

- Ustawienie to jest niezależne od ustawienia „Trusted/Untrusted“ dla „DHCP Snooping“.
- Switch w żadnym razie nie odrzuci pakietów ARP z „Trusted Ports“.
- Switch odrzuci pakiety ARP z „Untrusted Ports“, gdy informacje nadawcy w pakietach ARP nie będą zgodne z żadnym z aktualnych połączeń.
- Standardowo „Trusted Ports“ są „Uplink Ports“, a „Untrusted Ports“ połączone są z uczestnikami.

Konfiguracje

Funkcja „ARP Inspection“ może być w switchu przez użytkowników aktywowana lub dezaktywowana. Może to wymagać również specyficznej sieci VLAN. Gdy funkcja „ARP Inspection“ jest w switchu dezaktywowana, dezaktywowana jest we wszystkich wirtualnych sieciach lokalnych, nawet jeśli była aktywowana dla pojedynczych VLAN.

Wskazówka



Stan globalny/Stan VLAN
Istnieje stan globalny i poszczególne stany VLAN.

Gdy stan globalny zostaje dezaktywowany, dezaktywowana zostaje funkcja „IGMP Inspection“ w switchu, nawet jeśli poszczególne stany VLAN zostały aktywowane.

Gdy dla „IGMP Inspection“ aktywowany jest stan globalny, funkcja ta musi być dla specyficznych VLAN pojedynczo aktywowana przez użytkownika.

7.3.1.3.1 Filter Table

Przy dynamicznym trybie „ARP Inspection“ połączenia adresów IP z MAC porównywane są z wpisami z zabezpieczonej bazy danych (baza danych „DHCP Snooping“), zanim pakiet zostanie przekierowany. Gdy switch rozpozna nieautoryzowany pakiet ARP, automatycznie utworzy filtr adresu MAC w celu zablokowania ruchu danych z adresu źródłowego MAC i źródłowego VLAN ID tego pakietu danych. Ponadto switch będzie regularnie usuwał wpisy, których „Age Time“ upłynął.

- Gdy przy aktywowanej funkcji „ARP Inspection“ system rozpozna nieważne hosty, utworzy wpis filtra w tabeli adresów MAC.
- Gdy przy dezaktywowanej funkcji „ARP Inspection“ połączenie na porcie ma awarię, switch będzie usuwał wpisy filtra MAC dla tego portu.
- Gdy przy aktywowanej funkcji „ARP Inspection“ połączenie na porcie ma awarię, switch będzie usuwał wpisy filtra MAC dla tego portu.
- Maksymalna liczba wpisów w tabeli filtrów adresów MAC wynosi 256.
- Gdy tabela filtrów adresów MAC dla „ARP Inspection“ jest pełna i switch odbierze nieautoryzowany pakiet ARP, automatycznie utworzy protokół „SYSLOG“ i odrzuci pakiet ARP. Protokół „SYSLOG“ tworzony jest tylko raz.

7.3.2 Access Control List (ACL)

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

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

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

7.3.3 Standard komunikacyjny IEEE 802.1X

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

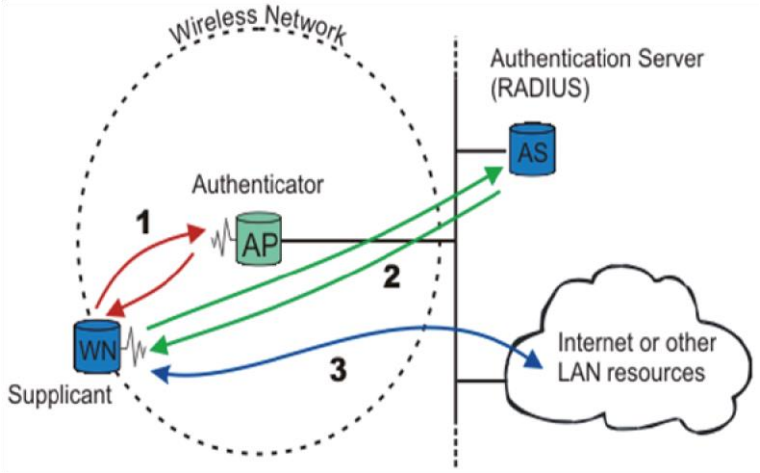
IEEE 802.1X wykorzystuje uwierzytelnienie na bazie portów, polegające na komunikacji między następującymi uczestnikami: tzw. „Supplicant“, „Authenticator“ i serwer uwierzytelniający. „Supplicant“ to najczęściej oprogramowanie na urządzeniu Client, przykładowo laptop, „Authenticator“ to połączony przewodem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

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

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

Serwer RADIUS

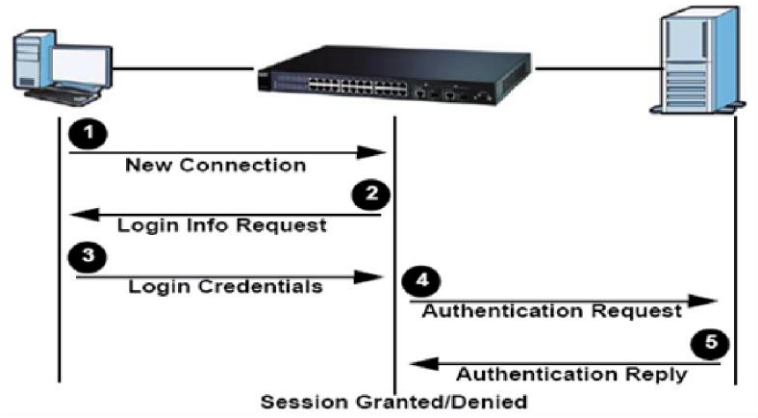
Serwer RADIUS („**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice“) jest protokołem bezpieczeństwa na bazie Client-Server do uwierzytelniania i kontroli uprawnień dostępu do sieci.
Serwer RADIUS wykorzystuje proces Challenge-Response i wspiera centralną administrację danymi użytkowników,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



Ilustracja 26: IEEE 802.1X

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

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



Ilustracja 27: Serwer RADIUS

Lokalne konta użytkownika

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

Guest VLAN

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

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

Port Parameters

- **Admin Control Direction**

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

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

- **Re-Authentication**

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

- **Reauth-Period**

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

- **Port Control Mode**

  „Auto“ Użytkownicy mają po uwierzytelnieniu dostęp do sieci.

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

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

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

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

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

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

7.3.4 Port Security

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

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

Wskazówka



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

7.3.4.1 Sticky MAC Settings

„Port Security“ za pomocą funkcji „Sticky MAC“ oferuje wiele podobnych zalet jak „Port Security“ za pomocą statycznych adresów MAC, ale „Sticky MAC“ mogą być uczone dynamicznie. „Port Security“ za pomocą „Sticky MAC“ zawiera dynamicznie nauczone adresy MAC podczas warunku link-down.

7.4 Monitor

7.4.1 Alarm

Funkcja ta powiadamia administratora sieci o wszystkich anormalnych sytuacjach wewnątrz sieci.

Wskazówka



Mikroprzełącznik DIP alarmu
Za pomocą mikroprzełącznika DIP alarmu użytkownik może skonfigurować, czy przy wystąpieniu określonego zdarzenia ma być wysyłany komunikat o alarmie.

Przykład

P1:	ON	– Switch wysyła komunikat o alarmie, gdy połączenie na porcie 1 ma awarię.
PWR:	ON	– Switch wysyła komunikat o alarmie, gdy zasilanie podstawowe zostaje przerwane.
RPS:	ON	– Switch wysyła komunikat o alarmie, gdy zasilanie redundantne zostaje przerwane.

7.4.2 System Information

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

7.4.3 Port Statistics

Za pomocą tej funkcji monitorowane są statystyki portów i wyświetlana jest np. liczba odebranych i wysłanych pakietów danych.

7.4.4 Port Utilization

Za pomocą tej funkcji wyświetlane jest obłożenie portów.

7.4.5 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“).

7.4.6 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.

7.4.6.1 DDMI

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

7.4.7 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.

7.5 Management

7.5.1 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 wpisać 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.

7.5.1.1 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.

7.5.1.2 SNMPv3

W wersji 3 SNMP wymiana wiadomości jest powiązana z kontami użytkowników. Każde urządzenie znające ustawione hasła może odczytywać lub zapisywać wartości z urządzenia ETHERNET. W SNMPv3 dane użytkowe wiadomości SNMP mogą być szyfrowane w czasie transferu. W ten sposób wartości adresowane i zapisywane nie mogą być podsłuchiwane przez ETHERNET, przez co SNMPv3 jest często stosowany w sieciach wymagających wysokiego stopnia zabezpieczenia.

7.5.2 Auto Provision

Funkcja „Auto Provision“ to usługa oferowana przez usługodawców, umożliwiająca szybką, prostą i automatyczną konfigurację urządzeń zdalnych z rozproszonej lokalizacji lub aktualizację za pomocą firmware'u.

1. Gdy funkcja ta jest aktywowana, switch pobierze najpierw plik informacyjny z serwera usługodawcy.

   Nazwa pliku tworzona jest według następującej reguły:
   Seria_Model_Autoprovision.txt

   Przykład: 852_1505_Autoprovision.txt

   Plik składa się z następującej zawartości:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=5228-000-1.0.0.b1
Firmware_Image_File=5228-000-1.0.0.b1.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=5228-000-1.0.0.b1.save
Global_Configuration_Reboot=0
Specific_Configuration_State=0
Specific_Configuration_Reboot=0
```

2. Gdy wartość „AUTO_PROVISION_VER“ jest wyższa niż wartość aktualnej wersji „Auto Provision“, przejdź do kroku 3 – jeśli nie, odczekaj 24 godziny i ponownie zacznij od kroku 1.

3. Jeśli „Firmware_Upgrade_State =1“, przejdź do kroku 4 – jeśli nie, przejdź do kroku 6.

4. Jeśli „Firmware_Version“ różni się od aktualnej wersji firmware'u, pobierz „Firmware_Image_File“ i zaktualizuj firmware.

5. Jeśli aktualizacja firmware' powiodła się i „Firmware_Reboot=1“, wykonywany jest „reboot_flag=1“.

6. Jeśli „Global_Configuration_State =1“, pobierz „Global_Configuration_File“ i zaktualizuj konfigurację – jeśli nie, przejdź do kroku 8.

7. Jeśli aktualizacja konfiguracji powiodła się i „Global_Configuration_Reboot =1“, wykonywany jest „reboot_flag=1“.

8. Jeśli „Global_Configuration_State =1“, pobierz specyficzny plik konfiguracyjny i zaktualizuj konfigurację – jeśli nie, przejdź do kroku 10. Nazwa brzmi: „Serie_Modell_“ z 12-bitowymi cyframi MAC, np. „852_1505_00e04c8196b9.txt“.

9. Jeśli aktualizacja konfiguracji powiodła się i „Specific_Configuration_Reboot =1“, wykonywany jest „reboot_flag=1“.

10. Jeśli „reboot_flag=1“, zapisz wykonaną konfigurację i restartuj switch – jeśli nie, odczekaj 24 godziny i ponownie zacznij od kroku 1.

7.5.3 Mail Alarm

„Mail Alarm“ wysyła e-mail trap do zdefiniowanego wcześniej administratora, gdy mają miejsce określone zdarzenia. Zdarzenia te wymienione są poniżej:

System Reboot:	System wykonuje gorący lub zimny start.
Port Link Change:	Połączenie na porcie jest tworzone lub przerwane.
Configuration Change:	Konfiguracje systemu w NV-RAM zostały zaktualizowane.
Firmware Upgrade:	Firmware systemu został zaktualizowany.
User Login:	Użytkownik zalogował się w systemie.
Port Blocked:	Port zostaje zablokowany przez „Loop Detection“ lub „BPDU Guard“.

7.5.4 Ping

Polecenie „Ping“ służy do sprawdzania dostępności urządzenia ETHERNET. „Ping“ bazuje na tym, że urządzenie programujące wysyła „ICMP Echo Request“ i czeka na „ICMP Echo Response“ odpytywanego urządzenia ETHERNET.

7.5.5 USB Funktions

Złącze USB switcha może służyć do realizacji następujących funkcji:

- ładowanie oprogramowania firmware
- zapisywanie pliku konfiguracyjnego
- zapisywanie pliku syslog
- ładowanie pliku konfiguracyjnego

W ustawieniach fabrycznych funkcje te są dezaktywowane. Funkcje można aktywować za pomocą Web-Based-Management lub komend CLI. Przy pierwszym wetknięciu pendrive'a USB automatycznie tworzona jest na nim konieczna struktura katalogów.

7.5.5.1 Ładowanie firmware'u

Plik firmware'u należy załadować do switcha w następujący sposób:

1. Utwórz na pendrive'ie USB (system plików FAT32) katalog z nazwą switcha (np. 852-1505_000-001).



Ilustracja 28: Funkcje USB, zakładanie katalogu

Wskazówka

Nazwa katalogu
Nazwa katalogu nie powinna zawierać znaków specjalnych! Przy zakładaniu katalogu ukośnik w nazwie produktu należy zastąpić podkreślnikiem.

2. Skopiuj nowy plik firmware'u do tego katalogu.



Ilustracja 29: Funkcje USB, plik firmware'u w katalogu

Wskazówka

Zawartość katalogu
W tym katalogu może znajdować się tylko plik firmware'u. Jeśli będzie tam coś więcej niż tylko plik firmware'u, ładowanie firmware'u zostaje przerwane.

3. Wetknij pendrive USB do złącza USB switcha.

4. Nowa wersja firmware'u zostaje automatycznie przesłana do switcha.
Podczas procesu ładowania LED POST miga na zielono.
Po zakończeniu procesu ładowania LED POST świeci na zielono.

Wskazówka

Nie wyciągać pendrive'a USB!
Podczas procesu ładowania firmware'u nie wolno wyciągać pendrive'a USB.

Wskazówka

Podczas ładowania nie odłączać zasilania!
Podczas ładowania firmware'u nie wolno odłączać zasilania.

7.5.5.2 Zapisywanie pliku konfiguracyjnego

1. Wetknij pendrive USB (system plików FAT32) do złącza USB switcha.

2. Plik konfiguracyjny zostaje automatycznie przesłany na pendrive.
Podczas zapisywania LED statusu POST miga na zielono.
Po zakończeniu zapisywania LED statusu POST świeci na zielono.

   Format nazwy pliku konfiguracyjnego:
   config_YYYYMMDDhhmmss.cfg

7.5.5.3 Zapisywanie pliku syslog

1. Wetknij pendrive USB (system plików FAT32) do złącza USB switcha.

2. Plik syslog zostaje automatycznie przesłany na pendrive.

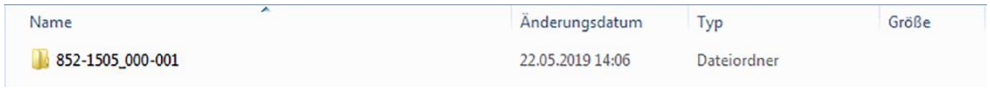
   Format nazwy pliku SYSLOG: flash_YYYYMMDDhhmmss.log

   Podczas zapisywania LED statusu POST miga na zielono.
   Po zakończeniu zapisywania LED statusu POST świeci na zielono.

7.5.5.4 Ładowanie pliku konfiguracyjnego

Plik konfiguracyjny należy załadować do switcha w następujący sposób:

1. Utwórz na pendrive'ie USB (system plików FAT32) katalog z nazwą switcha (np. 852-1505_000-001).

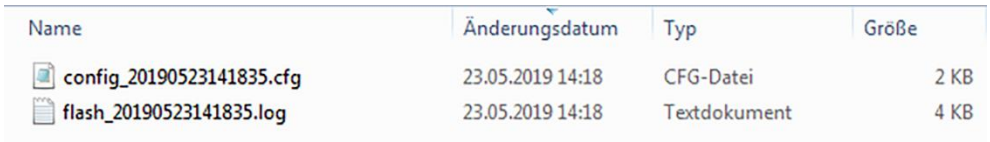


Ilustracja 30: Funkcje USB, zakładanie katalogu

Wskazówka

Nazwa katalogu
Nazwa katalogu nie powinna zawierać znaków specjalnych!
Przy zakładaniu katalogu ukośnik w nazwie produktu należy zastąpić podkreślnikiem.

2. Skopiuj plik konfiguracyjny do tego katalogu.



Ilustracja 31: Funkcje USB, plik konfiguracyjny w katalogu

3. Wetknij pendrive USB do złącza USB switcha.

4. Nowa wersja pliku konfiguracyjnego zostaje automatycznie przesłana do switcha.
Podczas procesu ładowania LED statusu POST miga na zielono.
Po zakończeniu procesu ładowania LED statusu POST świeci na zielono.

8 Konfiguracja

8.1 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 („**C**ommand **L**ine **I**nterface“).

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)“.

8.1.1 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 29: Domyślne ustawienia dla portu Telnet

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

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

8.2 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. Telnet należy używać z następującymi ustawieniami:

Tabela 30: 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 31: Ekran logowania

Ustawienie	Wartość domyślna
Default Username	admin
Default Password	wago

9 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.

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 wprowadź adres IP interfejsu sieciowego/sterownika.
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 32: Przegląd – linki nawigacyjne 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

▶ **[Advanced Settings]**

[Bandwidth Control]

- QoS
- Rate Limitation

[IMGP Snooping]

- IGMP Snooping
- IGMP Filtering
- MVR
- Static Multicast
- Multicast Statistics

[VLAN]

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

- DHCP Relay
- DHCP Options
- DHCP Server
- Dual Homing
- Dual Ring
- ERPS
- Link Aggregation
- LLDP
- Loop Detection
- Jet Ring
- Modbus
- PoE
- Static Route
- STP
- Xpress Ring

▶ **[Security]**

[IP Source Guard]

- DHCP Snooping
- Binding Table
- ARP Inspection

- Access Control List
- IEEE 802.1X
- Port Security

▶ **[Monitor]**

- Alarm
- System Information
- Port Statistics
- Port Utilization
- RMON Statistics
- SFP Information
- Traffic Monitor

▶ **[Management]**

[SNMP]

- SNMP
- SNMP Trap
- SNMPv3

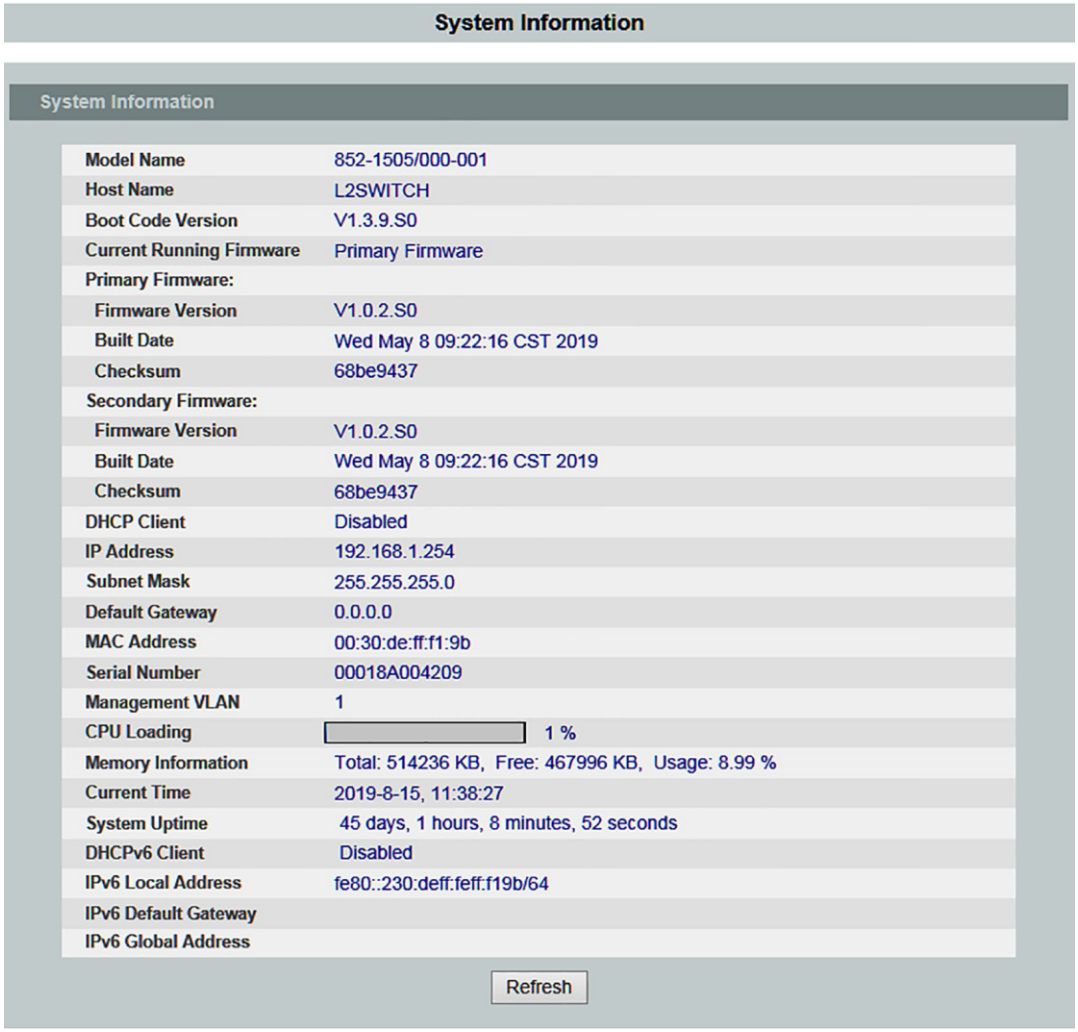
- Auto Provision
- Mail Alarm
- Maintenance
- System Log
- Ping
- USB Funktions
- User Account
- Open source License
- Wago Licenses

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.**

9.1 System Status

9.1.1 System Information



Ilustracja 32: Strona WBM „System Information“

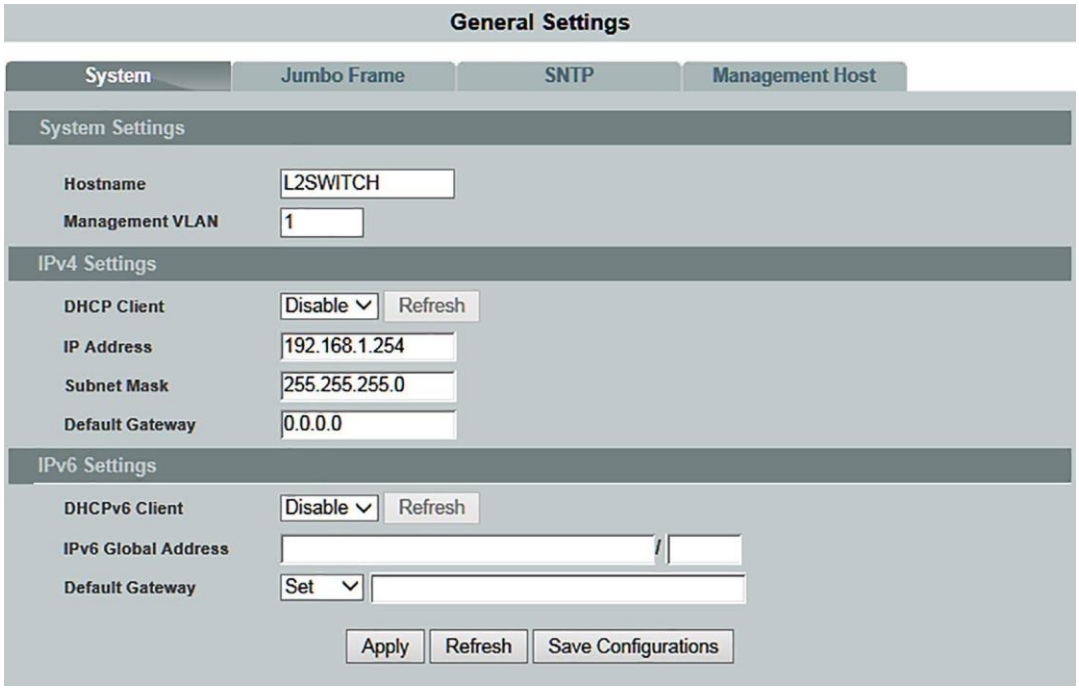
Tabela 33: Strona WBM „System Information“

Parametr	Opis
Modell 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.
Current Running Firmware	Aktualne zastosowany firmware
Primary Firmware	
Firmware Version	W tym polu wyświetlany jest numer wersji aktualnie zainstalowanego firmware'u podstawowego.
Built Date	W tym polu wyświetlana jest data utworzenia aktualnie zainstalowanego firmware'u podstawowego.
Checksum	W tym polu wyświetlana jest suma kontrolna aktualnie zainstalowanego firmware'u podstawowego.
Secondary Firmware	
Firmware Version	W tym polu wyświetlany jest numer wersji aktualnie zainstalowanego firmware'u zapasowego.
Built Date	W tym polu wyświetlana jest data utworzenia aktualnie zainstalowanego firmware'u zapasowego.
Checksum	W tym polu wyświetlana jest suma kontrolna aktualnie zainstalowanego firmware'u zapasowego.
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.
DHCPv6 Client	W tym polu wyświetlana jest informacja, czy DHCPv6 Client jest włączony/wyłączony.
IPv6 Local Address	W tym polu wyświetlany jest lokalny adres IPv6.
IPv6 Default Gateway	W tym polu wyświetlana jest domyślna brama switcha.
IPv6 Global Address	W tym polu wyświetlana jest informacja, czy został wpisany również globalny adres IPv6.
Refresh	Aby zaktualizować informacje na stronie, należy kliknąć ten przycisk.

9.2 General Settings

9.2.1 General Settings

9.2.1.1 System



Ilustracja 33: Strona WBM „General Settings“ – zakładka „System“

Tabela 34: Strona WBM „General Settings“ – zakładka „System“

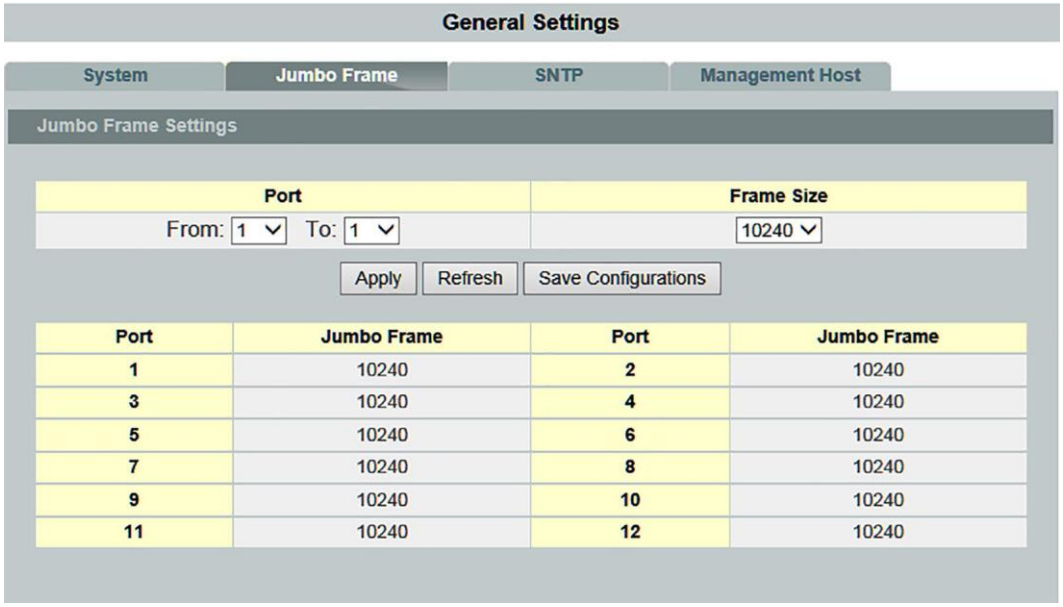
System Settings		
Parametr	**Domyślnie**	**Opis**
Hostname	**L2SWITCH**	Należy wpisać nazwę switcha, składającą się z maksymalnie 64 liter/cyfr. Nazwa hosta powinna składać się z kombinacji cyfr, liter, łączników (-) lub podkreśleń (_).
Management VLAN	**1**	Należy wpisać grupę VLAN, która ma uzyskać 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	**192.168.1.254**	W polu edycji należy wpisać adres IP switcha, używając zapisu z kropkami.
Subnet Mask	**255.255.255.0**	W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.
Default Gateway	0.0.0.0	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.

9.2.1.2 Jumbo Frame

Wskazówka

Dodatkowa informacja

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



Ilustracja 34: Strona WBM „General Settings“ – zakładka „Jumbo Frame”

Tabela 35: Strona WBM „General Settings“ – zakładka „Jumbo Frame”

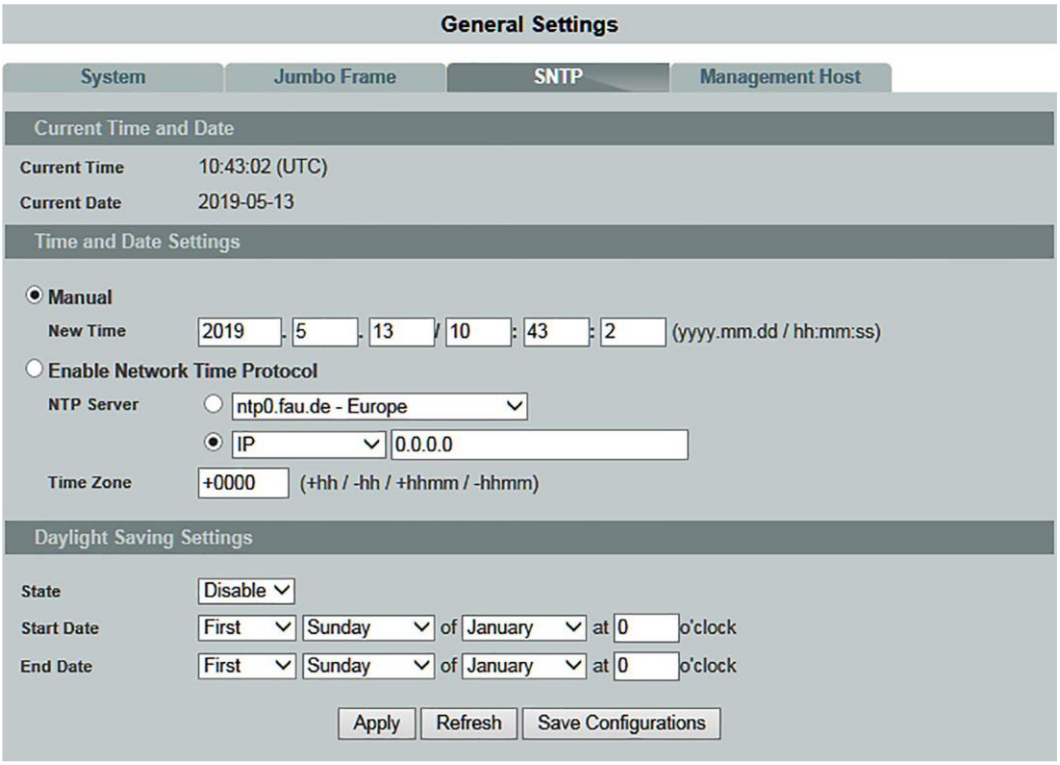
Jumbo Frame Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Jumbo Frame“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Jumbo Frame“.
Jumbo Frame		**10240**	W polu wyboru należy dla 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	

9.2.1.3 SNTP

Wskazówka

Dodatkowa informacja

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



Ilustracja 35: Strona WBM „General Settings“ – zakładka „SNTP”

Tabela 36: Strona WBM „General Settings“ – 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]** pojawią 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 36: Strona WBM „General Settings“ – zakładka „SNTP”

Daylight Saving Settings		
Parametr	**Domyślnie**	**Opis**
State	**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.

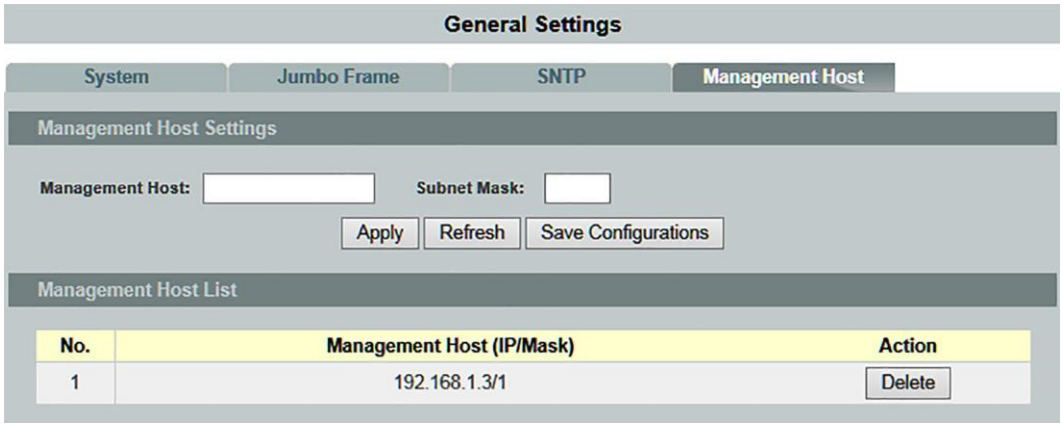
1)	Na większości terytorium USA czas letni rozpoczyna się w drugą niedzielę marca. W każdej strefie czasowej USA czas letni rozpoczyna się o godzinie 02:00 czasu miejscowego. Zgodnie z tym należy wybrać „Second, Sunday, March“ i „2:00“. W Unii Europejskiej czas letni rozpoczyna się w ostatnią niedzielę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

9.2.1.4 Management Host

Wskazówka

Dodatkowa informacja

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



Ilustracja 36: Strona WBM „General Settings“ – zakładka „Management Host“

Tabela 37: Strona WBM „General Settings“ – 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]**.

9.2.2 MAC Management

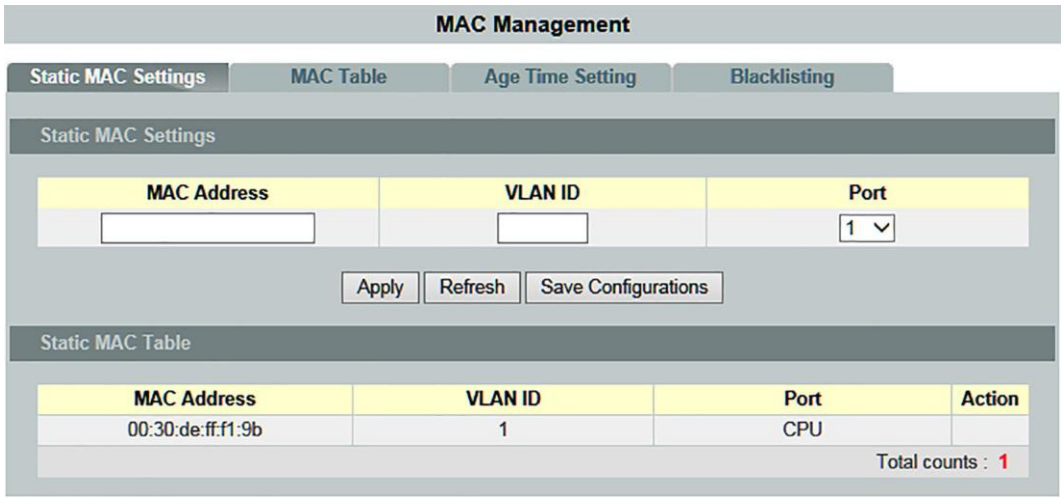
Wskazówka

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

9.2.2.1 Static MAC Settings

Wskazówka

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

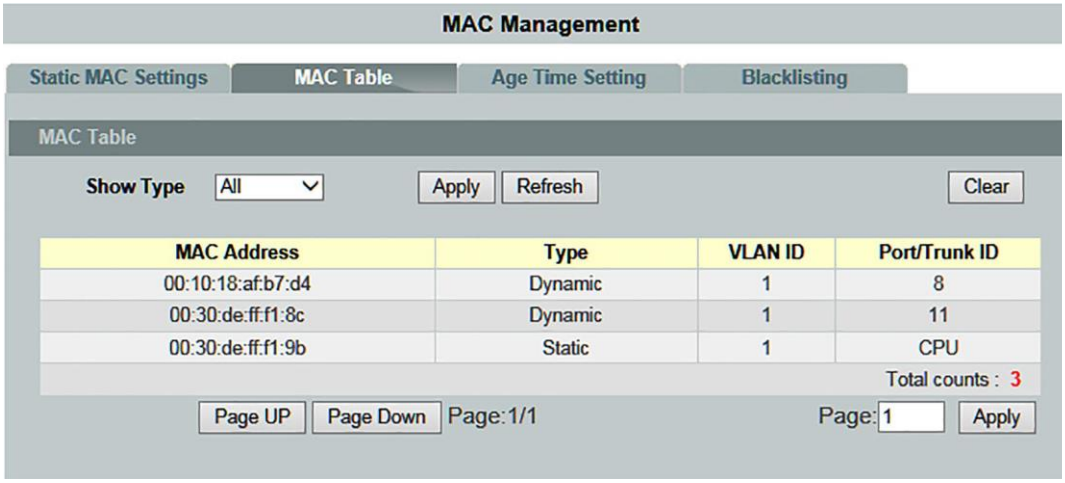


Ilustracja 37: Strona WBM „MAC Management“ – zakładka „Static MAC Settings”

Tabela 38: Strona WBM „MAC Management“ – 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.

9.2.2.2 MAC Table

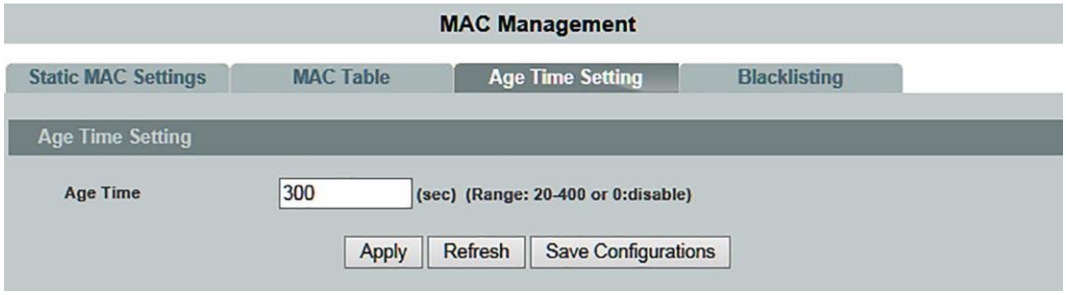


Ilustracja 38: Strona WBM „MAC Management“ – zakładka „MAC Table”

Tabela 39: Strona WBM „MAC Management“ – 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 wyświetlana jest „VLAN ID” wpisu 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.

9.2.2.3 Age Time Setting



Ilustracja 39: Strona WBM „MAC Management“ – zakładka „Age Time Setting”

Tabela 40: 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

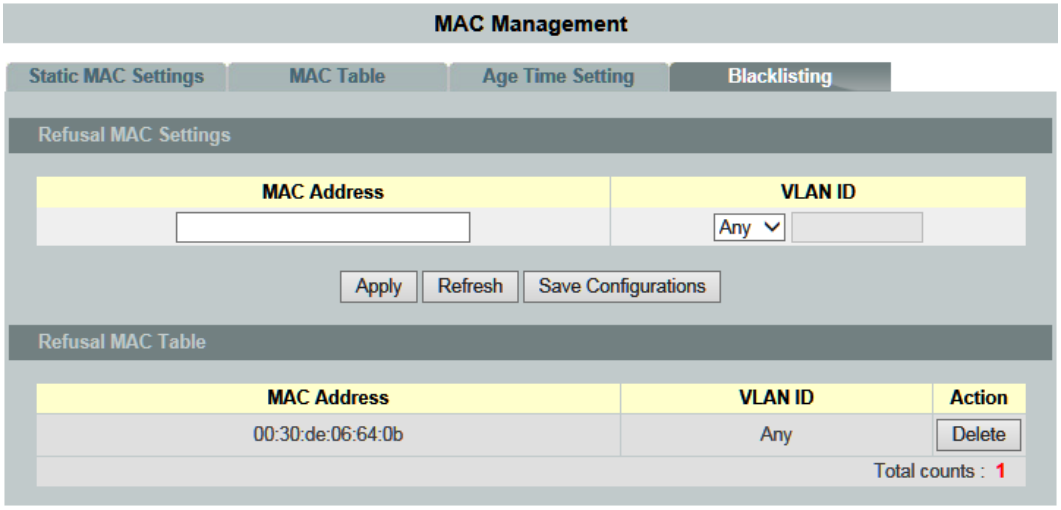
9.2.2.4 Blacklisting

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 40: Strona WBM „MAC Management“ – zakładka „Blacklisting”

Tabela 41: Strona WBM „MAC Management“ – 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“.

9.2.3 Port Mirroring

Wskazówka

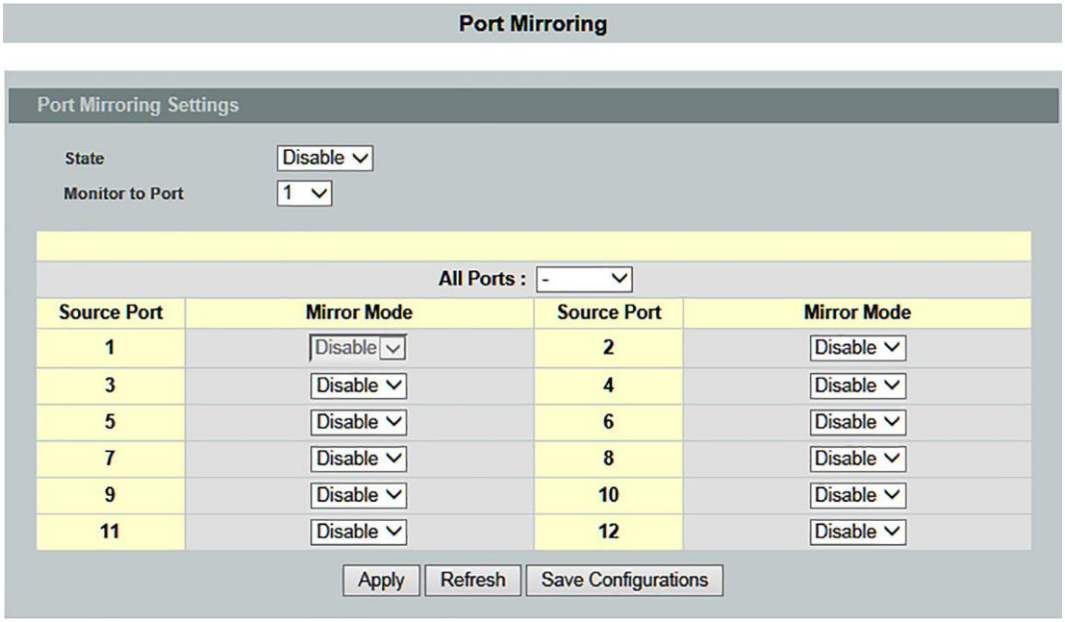
Dodatkowa informacja

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

Wskazówka

Monitor Port

„Monitor Port“ nie może być członkiem grupy „Trunk Port“.
Port monitorujący 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.



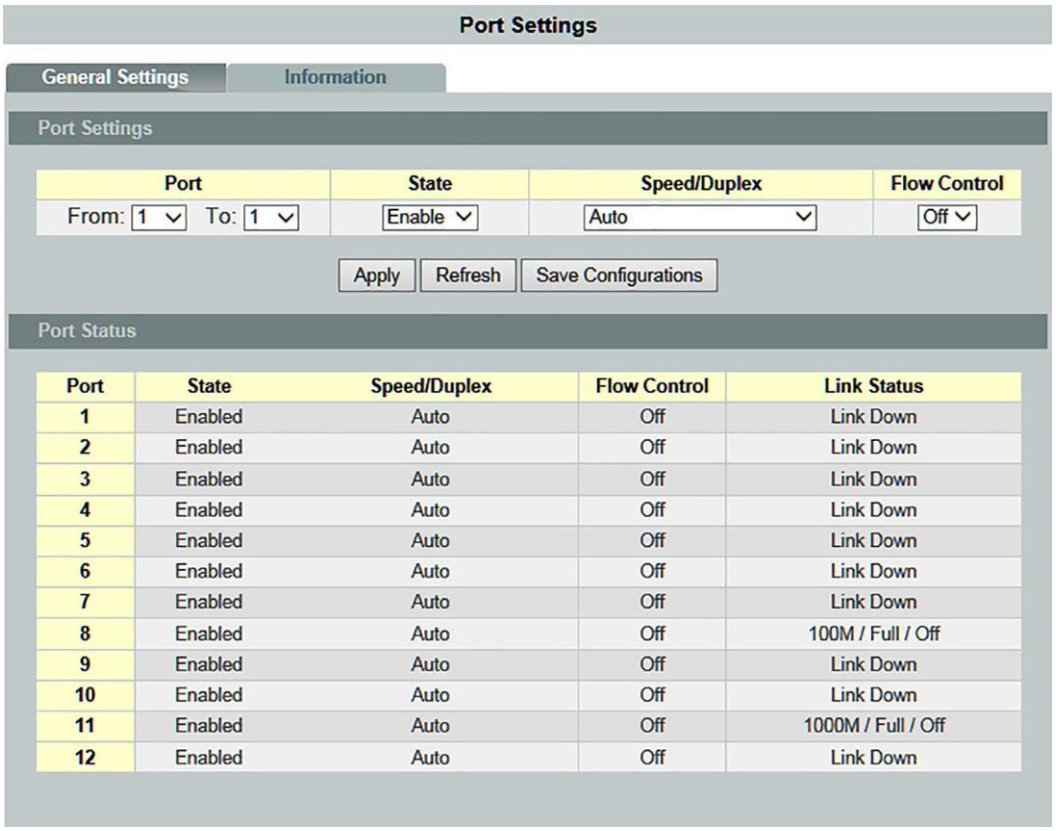
Ilustracja 41: Strona WBM „Port Mirroring”

Tabela 42: 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 Port“ 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 Port“ do „Monitor Port“.

9.2.4 Port Settings

9.2.4.1 General Settings

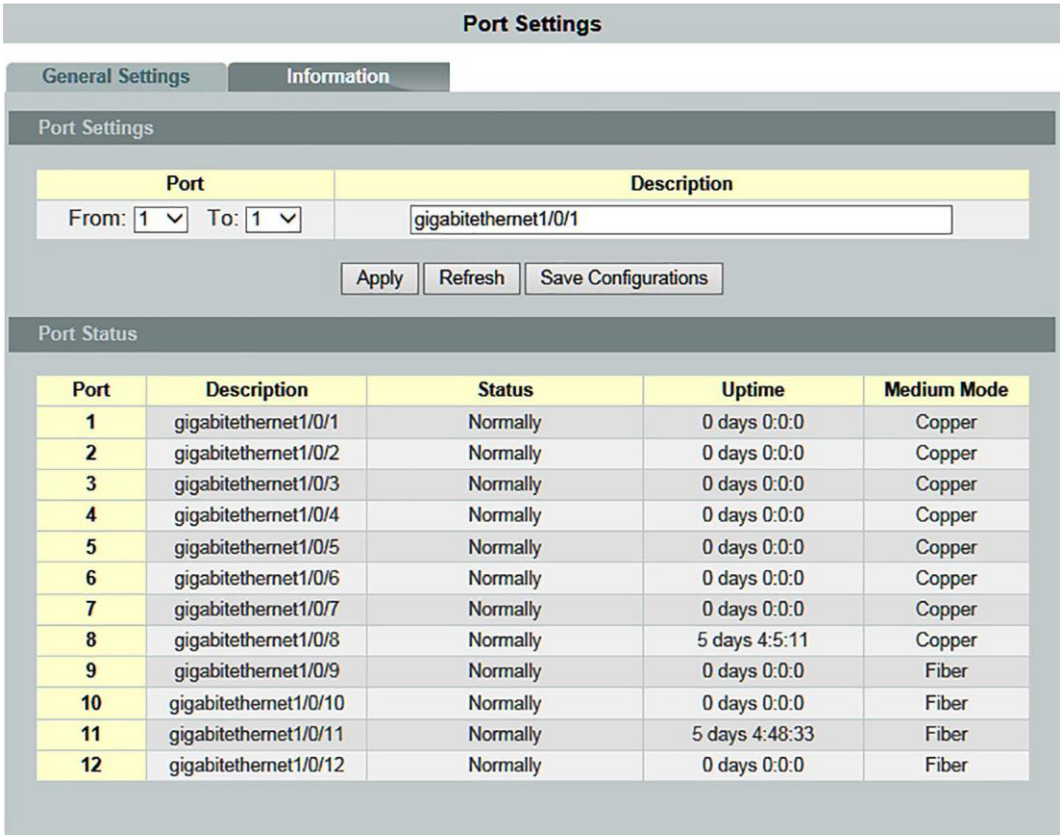


Ilustracja 42: Strona WBM „Port Settings“ – zakładka „General Settings“

Tabela 43: Strona WBM „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.
Status		**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.

9.2.4.2 Information



Ilustracja 43: Strona WBM „Port Settings” – zakładka „Information”

Tabela 44: 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.
Description			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

9.3 Advanced Settings

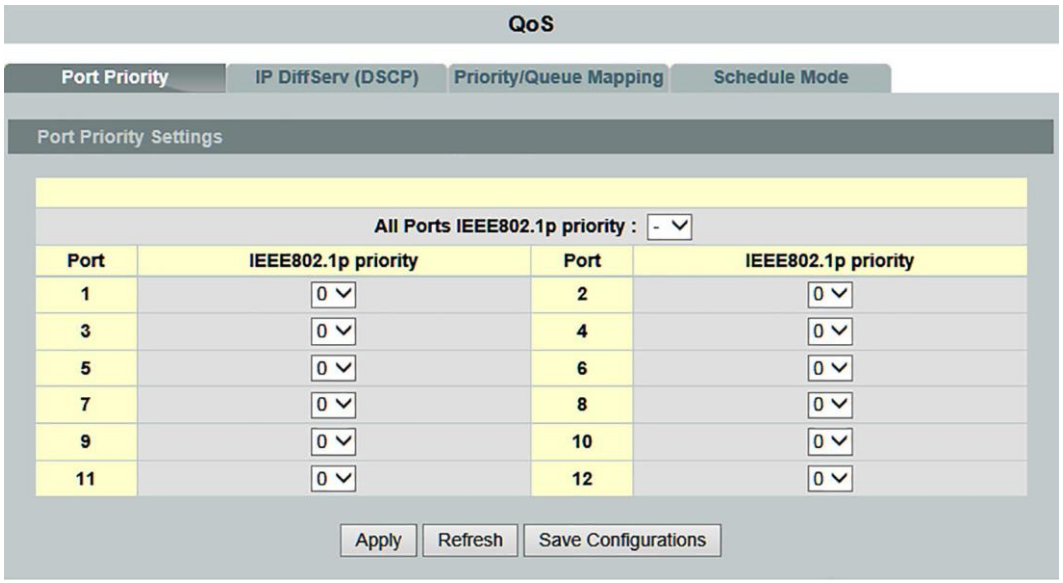
9.3.1 Bandwidth Control

9.3.1.1 QoS

Wskazówka

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

9.3.1.1.1 Port Priority

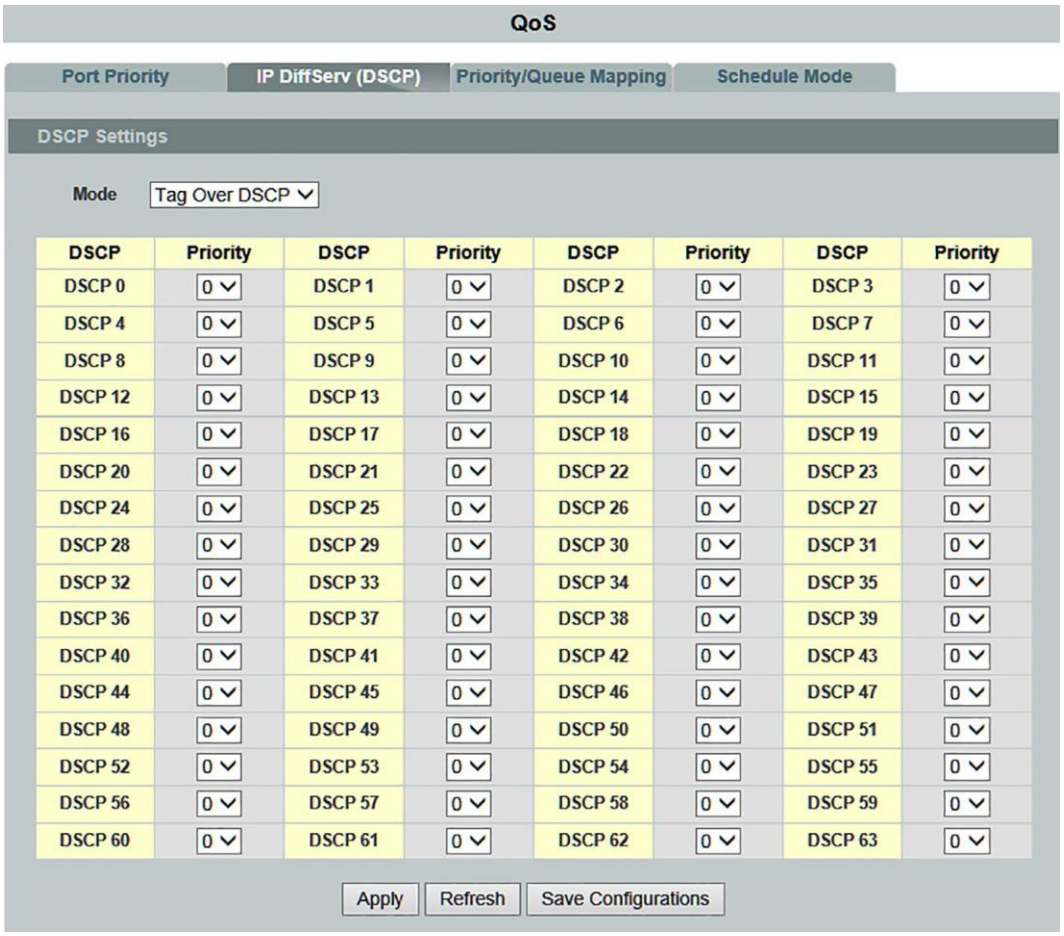


Ilustracja 44: Strona WBM „QoS” – zakładka „Port Priority”

Tabela 45: 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 danych.
	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 danych, odbieranych na tym porcie. Tylko pakietowi bez „802.1p Tag Priority“ przydzielany jest tu podany priorytet.

9.3.1.1.2 IP DiffServ (DSCP)

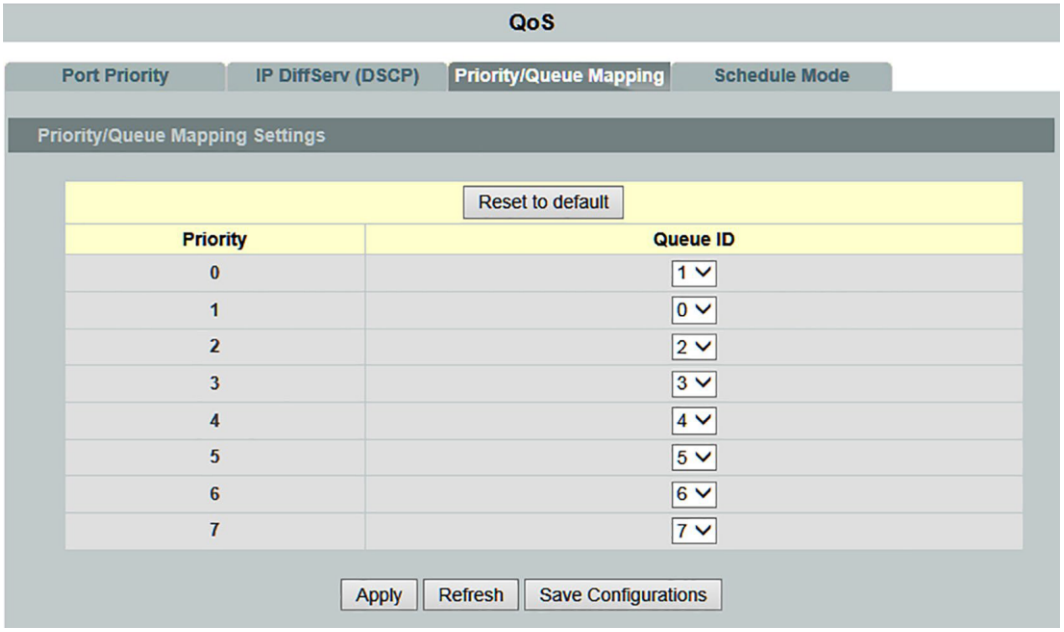


Ilustracja 45: Strona WBM „QoS” – zakładka „IP DiffServ (DSCP)”

Tabela 46: 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

9.3.1.1.3 Priority/Queue Mapping



Ilustracja 46: Strona WBM „QoS" – zakładka „Priority/Queue Mapping"

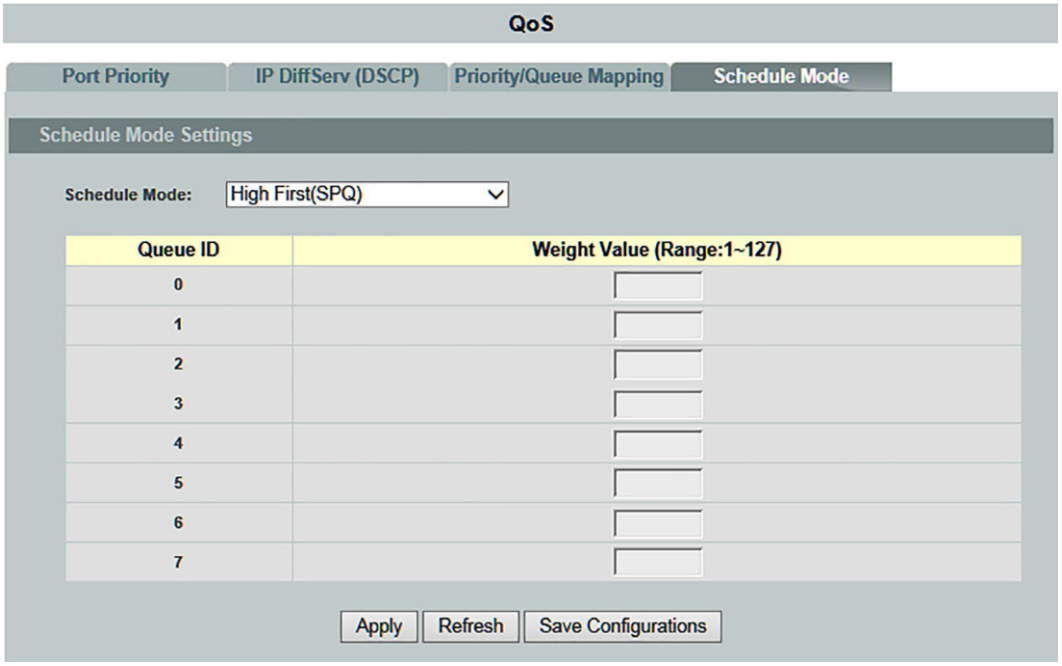
Tabela 47: Strona WBM „QoS" – zakładka „Priority/Queue Mapping"

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 danych z poziomem priorytetu.

Tabela 48: Default Settings

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

9.3.1.1.4 Schedule Mode



Ilustracja 47:: Strona WBM „QoS“ – zakładka „Schedule Mode“

Tabela 49: Strona WBM „QoS“ – zakładka „Schedule Mode“

Schedule Mode Settings		
Parametr	**Domyślnie**	**Opis**
Schedule Mode	**Strict Priority Queuing (SPQ)**	W polu wyboru wybierz „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“. W tym celu należy najpierw wybrać „Weighted Round Robin (WRR)”. Potem można zmienić „Strict Priority Queuing (SPQ)“.

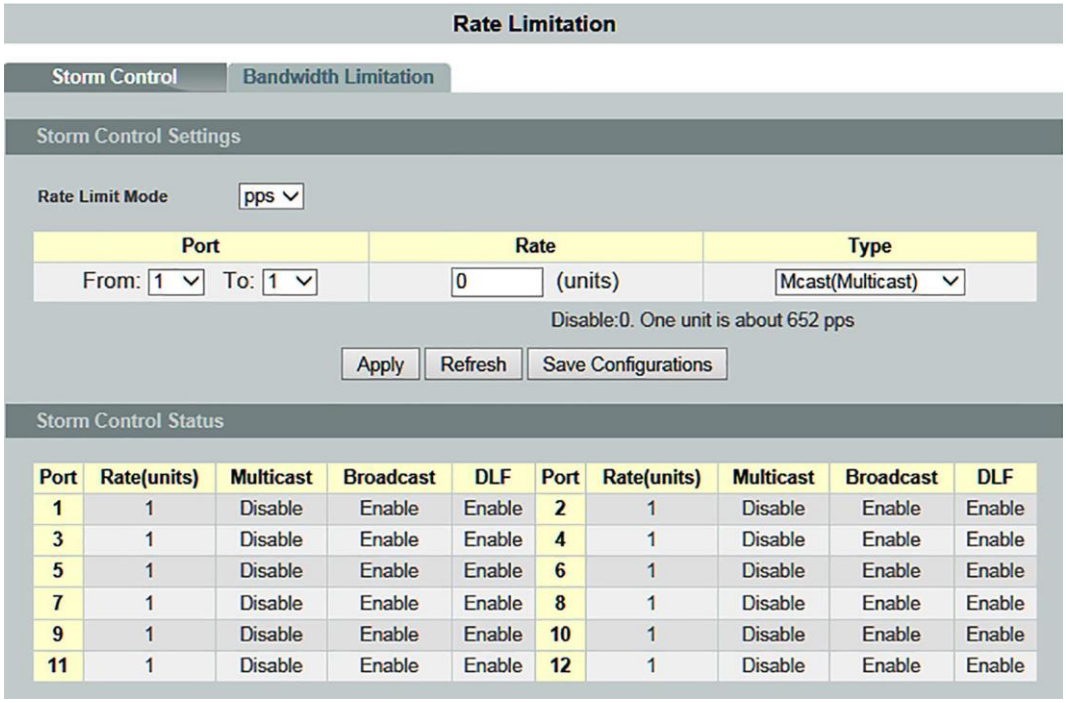
9.3.1.2 Rate Limitation

9.3.1.2.1 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 48: Strona WBM „Rate Limitation“ – zakładka „Strom Control“

Tabela 50: Strona WBM „Rate Limitation“ – zakładka „Storm Control“

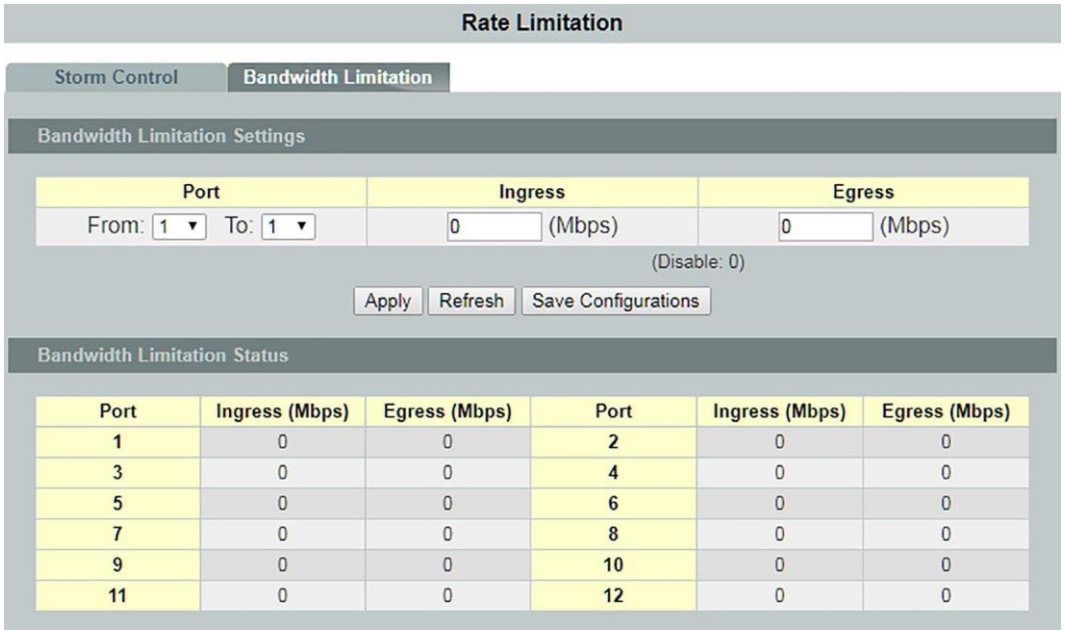
Storm Control Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Storm Control”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Storm Control”.
Number (units)		**0**	W polu wyboru należy wybrać liczbę pakietów danych (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 danych, 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.

9.3.1.2.2 Bandwidt Limitation

Wskazówka

Dodatkowa informacja

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



Ilustracja 49: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“

Tabela 51: 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 (Mbps)		**0**	W polu edycji należy wpisać „Bandwidth Limitation“ dla wchodzących pakietów danych. Port 1 … 8 0 … 100 Port 9 … 10(12) 0 … 1000
Egress (Mbps)		**0**	W polu edycji należy wpisać „Bandwidth Limitation“ dla wychodzących pakietów danych.
Bandwidth Limitation Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Ingress (Mbps)			W tej kolumnie wyświetlane są ustawiona wartość „Bandwidth“ dla Ingress.
Egress (Mbps)			W tej kolumnie wyświetlane są ustawiona wartość „Bandwidth“ dla Egress.

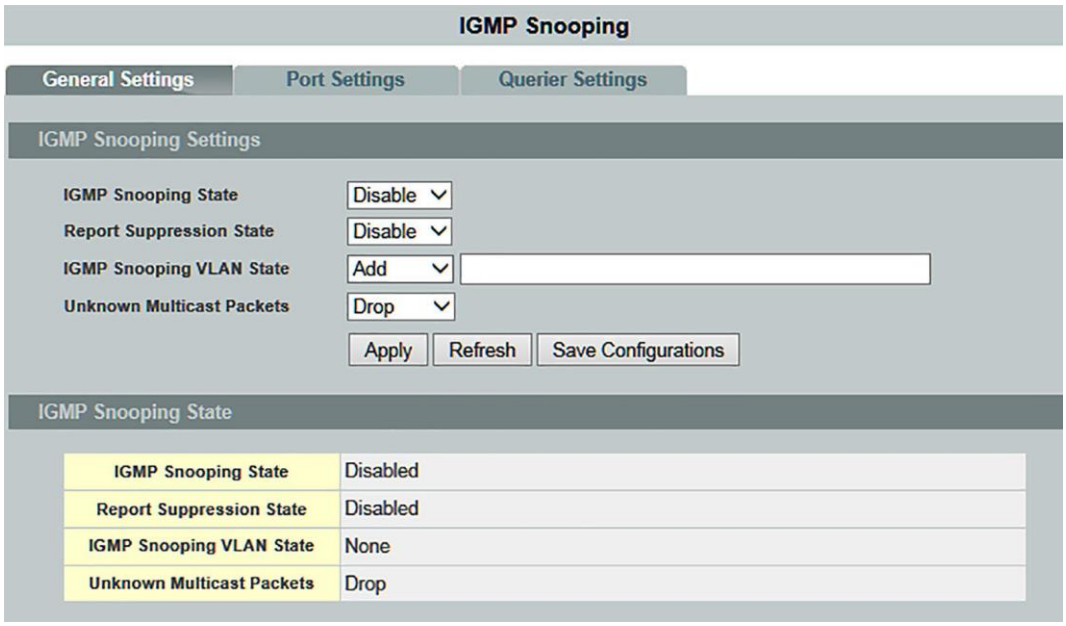
9.3.2 IGMP Snooping

Wskazówka

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

9.3.2.1 IGMP Snooping

9.3.2.1.1 General Settings

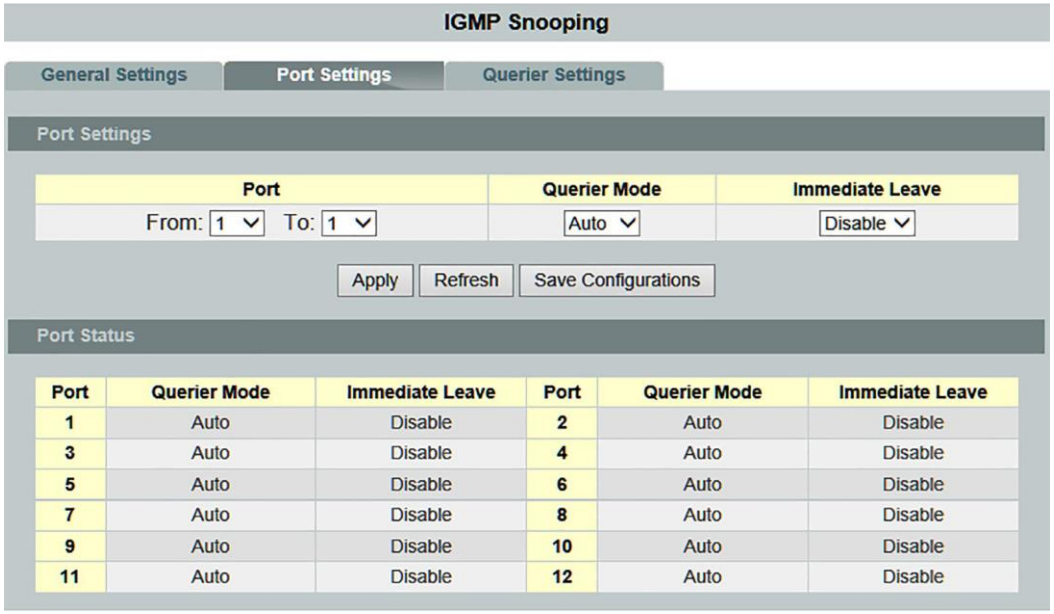


Ilustracja 50: Strona WBM „IGMP Snooping“ – zakładka „General Settings“

Tabela 52: 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.
Repport Suppression State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Status Report Suppression“ przy „IGMP Snooping”.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Status Report Suppression“ przy „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.
Repport Suppression State	Disable Enable	W tym polu wyświetlana jest informacja, czy funkcja „Repport Suppression State“ 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.

9.3.2.1.2 Port Settings

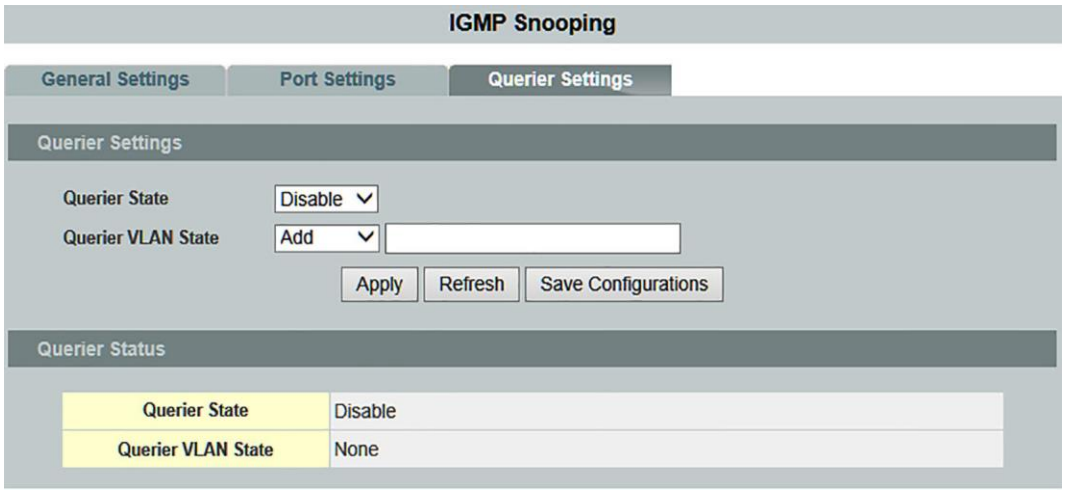


Ilustracja 51: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“

Tabela 53: 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 port „IGMP Query“, gdy „IGMP Query“ odbierze pakiety.
		Fix	W polu wyboru wybierz ustawienie „Fix”, gdy switch ma zawsze traktować port lub porty jako porty „IGMP Query”. 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 port „IGMP Query“. W tym przypadku switch nie protokołuje, że ruter IGMP jest połączony z portem i nie przekazuje też do tego portu pakietów danych „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 konkretnego portu.

9.3.2.1.3 Querier Settings



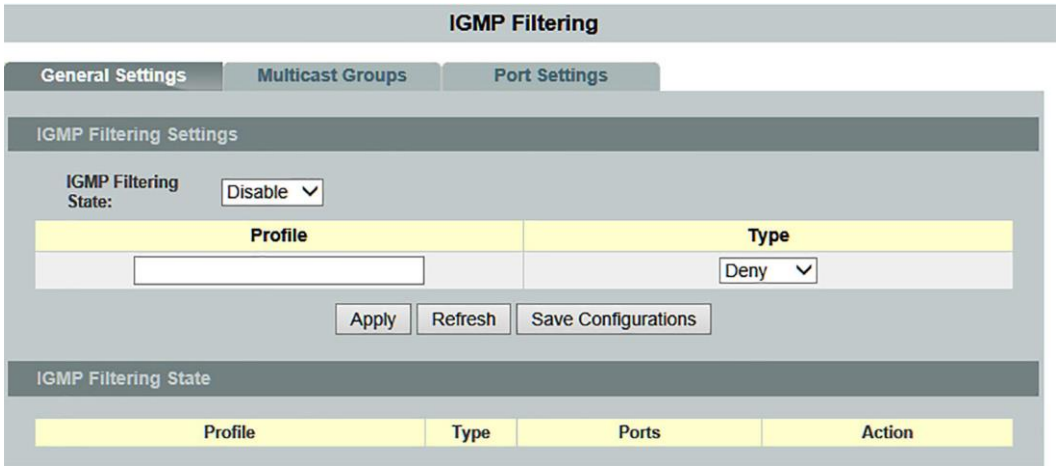
Ilustracja 52: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings“

Tabela 54: 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.

9.3.2.2 IGMP Filtering

9.3.2.2.1 General Settings

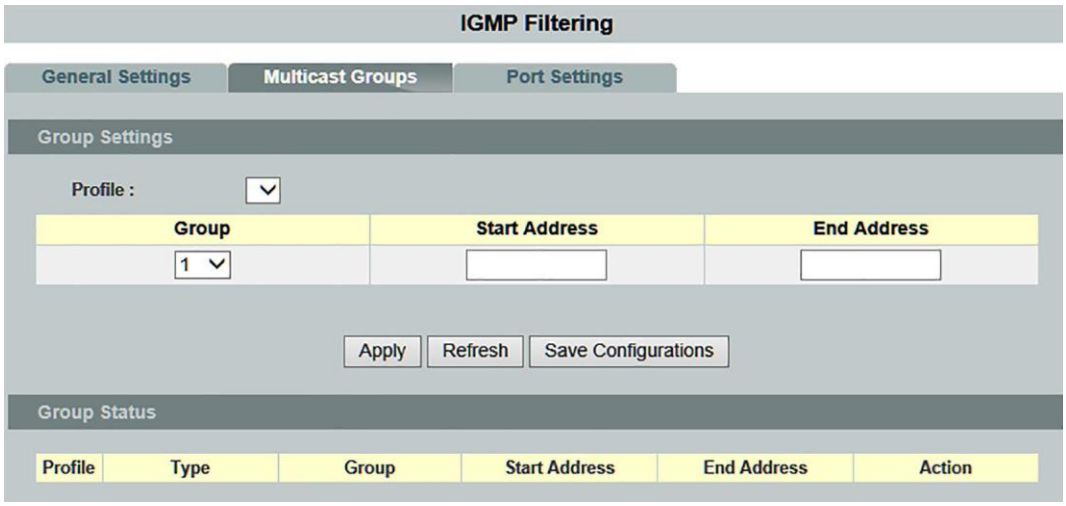


Ilustracja 53: Strona WBM „IGMP Filtering“ – zakładka „General Settings“

Tabela 55: 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]**.

9.3.2.2.2 Multicast Groups

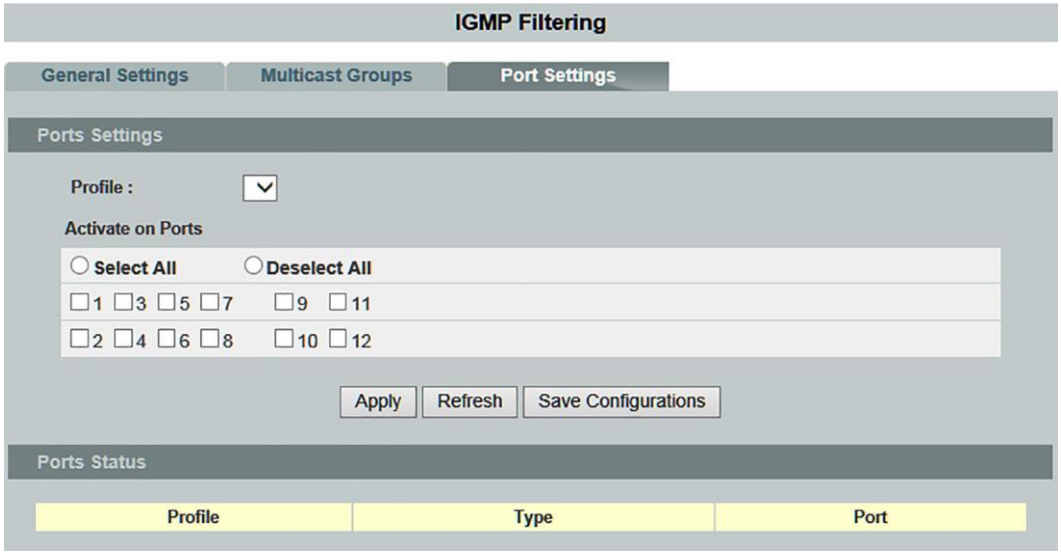


Ilustracja 54: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“

Tabela 56: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“

Group Settings		
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]**.

9.3.2.2.3 Port Settings



Ilustracja 55: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“

Tabela 57: 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“.	

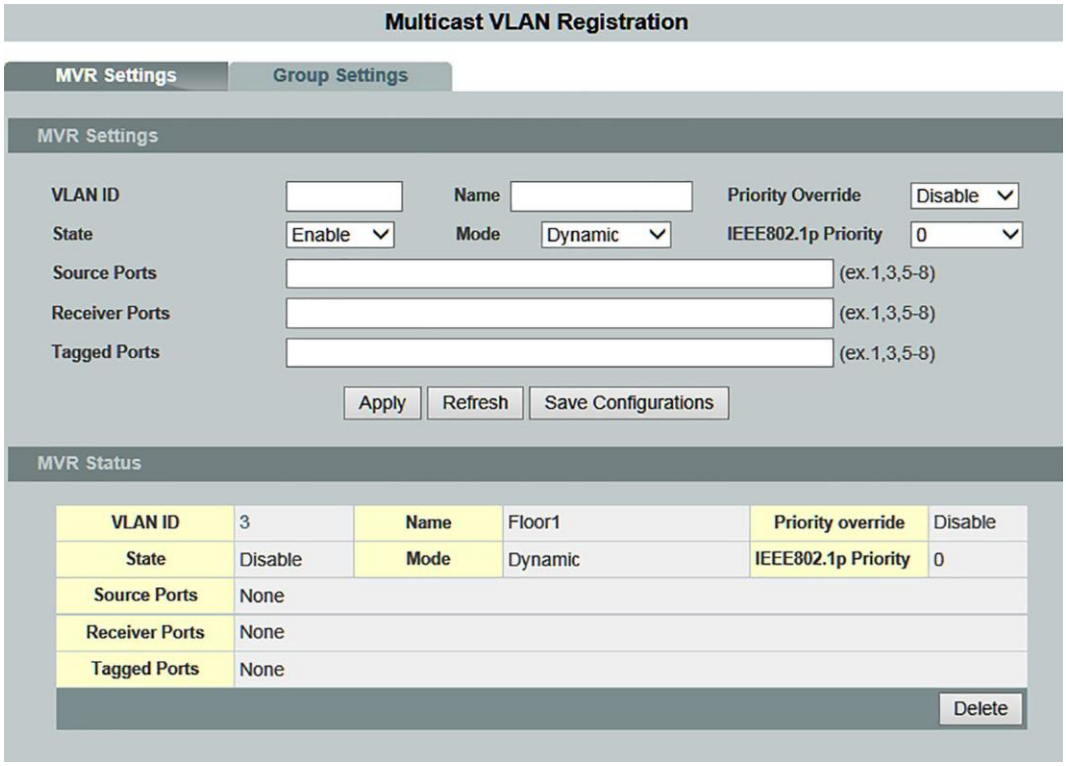
9.3.2.3 Multicast VLAN Registration

Wskazówka

Dodatkowa informacja

Więcej informacji o „**M**ulticast **V**LAN **R**egistration“ (MVR) można znaleźć w rozdziale „Opis funkcji“.

9.3.2.3.1 MVR Settings

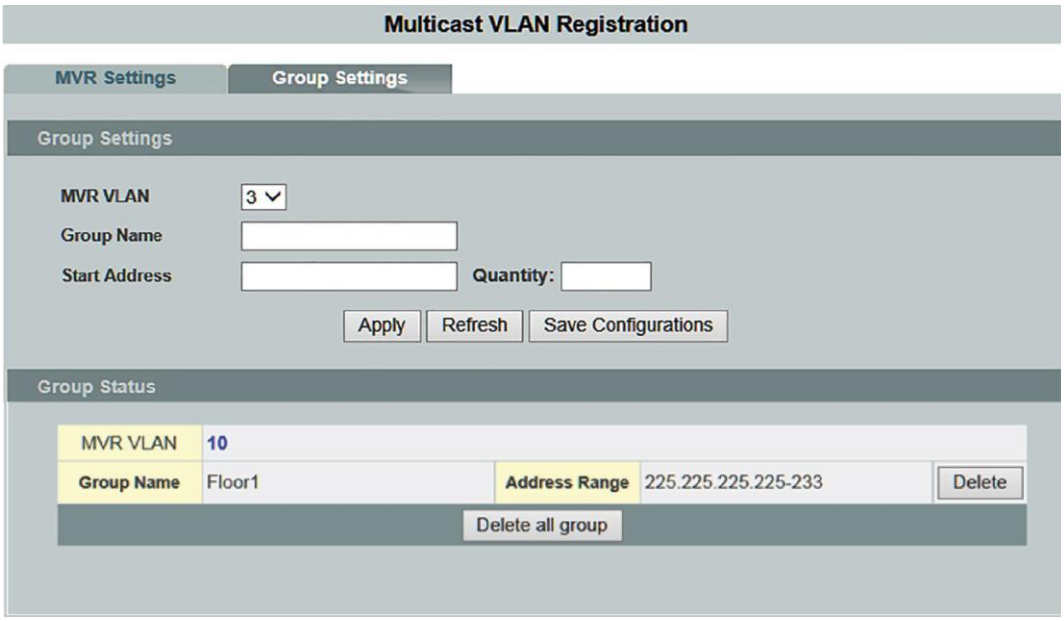


Ilustracja 56: Strona WBM „Multicast VLAN Registration“ – zakładka „MVR Settings“

Tabela 58: Strona WBM „Multicast VLAN Registration“ – zakładka „MVR Settings“

MVR Settings		
Parametr	**Domyślnie**	**Opis**
VLAN ID		W polu edycji należy wpisać VLAN ID.
Nazwa		W polu edycji należy wpisać nazwę MVR.
Priority override	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
State	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „MVR“.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować „MVR“.
Mode	**Dynamic**	W polu wyboru należy wybrać „Dynamic“, aby skonfigurować tryb dynamiczny dla „MVR“.
	Compatible	W polu wyboru należy wybrać „Compatible“, aby skonfigurować tryb kompatybilny dla „MVR“.
IEEE 802.1p Priority	**0** … 7	W polu wyboru należy wybrać priorytet dla pakietów danych, odbieranych na tym porcie. Tylko pakietowi bez „802.1p Tag Priority“ przydzielany jest tu podany priorytet.
Source Ports	1 … 8	W polu edycji należy wpisać „Source Port“ lub zakres „Source Port“ dla MVR. Standardowo „Source Ports“ są połączone z „Streaming Server“.
Receiver Ports	1 … 8	W polu edycji należy wpisać „Receiver Port“ lub zakres „Receiver Port“ dla MVR. Standardowo „Receiver Ports“ są połączone z „Streaming Client“.
Tagged Ports	1 … 8	W polu edycji należy wpisać port ze znacznikiem lub zakres dla „MVR“. To samo dotyczy portów VLAN ze znacznikiem.
MVR Status		
Parametr	**Domyślnie**	**Opis**
VLAN ID		W tym polu wyświetlany jest VLAN ID.
Name		W tym polu wyświetlana jest wybrana przez użytkownika nazwa.
Priority override	Disable Enable	W tym polu wyświetlany jest status.
State	Disable Enable	W tym polu wyświetlany jest status „MVR“.
Mode	Dynamic Compatible	W tym polu wyświetlany jest tryb „MVR“.
IEEE 802.1p Priority	0 … 7	W tym polu wyświetlana jest wybrany przez użytkownika priorytet dla pakietów danych.
Source Ports	1 … 8	W tym polu wyświetlany jest „Source Port” lub zakres „Source Port” dla „MVR“.
Receiver Ports	1 … 8	W tym polu wyświetlany jest „Receiver Port” lub zakres „Receiver Port” dla „MVR“.
Tagged Ports	1 … 8	W tym polu wyświetlany jest port ze znacznikiem lub zakres portów ze znacznikami dla „MVR“.

9.3.2.3.2 Group Settings



Ilustracja 57: Strona WBM „Multicast VLAN Registration“ – zakładka „Group Settings“

Tabela 59: Strona WBM „Multicast VLAN Registration“ – zakładka „Group Settings“

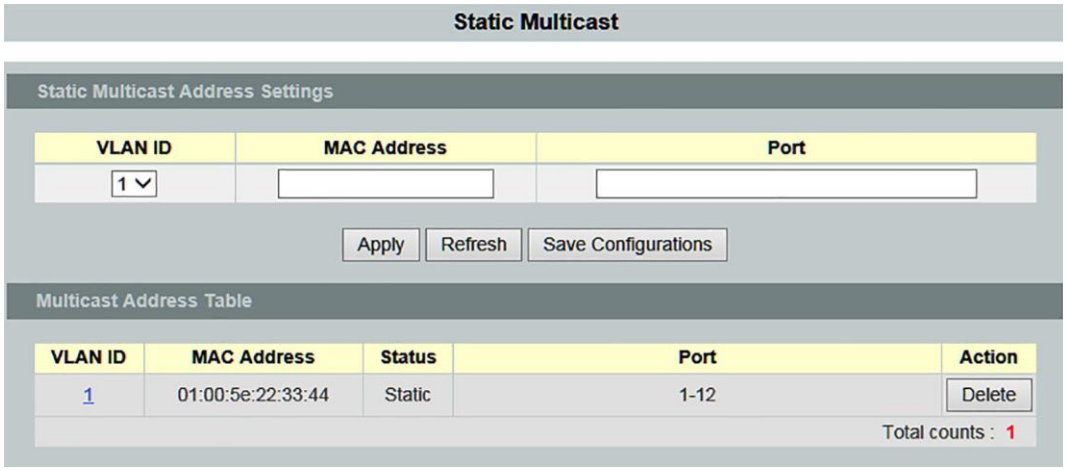
Group Settings		
Parametr	**Domyślnie**	**Opis**
MRV VLAN		W polu wyboru należy wybrać liczbę „MVR VLAN“.
Group Name		W polu edycji należy wpisać nazwę grupy „MVR“.
Start Address		W polu edycji należy wpisać początkowy adres „Multicast“.
Quantity		W polu edycji należy wpisać liczbę początkowych adresów „Multicast“.
Group Status		
Parametr	**Domyślnie**	**Opis**
MRV VLAN		W tym polu wyświetlana jest liczba MVR VLAN.
Group Name		W tym polu wyświetlana jest wybrana przez użytkownika nazwa grupy.
Address Range		W tym polu wyświetlany jest adres początkowy „Multicast“.
Delete		Aby usunąć te ustawienia, należy kliknąć **[Delete]**.
Delete all group		Aby usunąć ustawienia dla całej grupy, należy kliknąć **[Delete all group]**.

9.3.2.4 Static Multicast

Wskazówka

Dodatkowa informacja

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

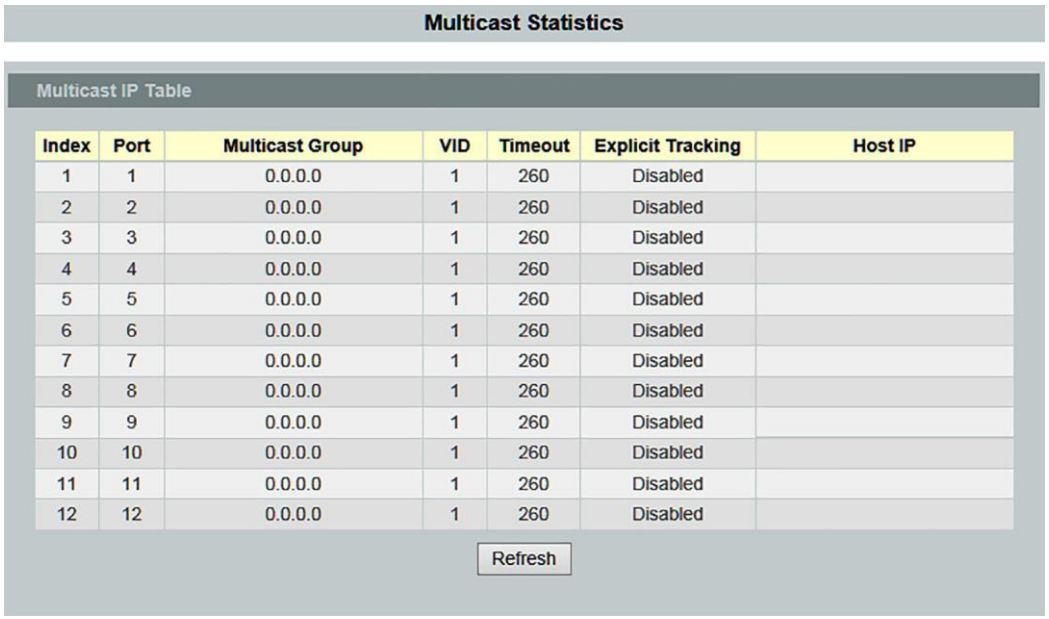


Ilustracja 58: Strona WBM „Static Multicast“

Tabela 60: 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“.

9.3.2.5 Multicast Statistics



Ilustracja 59: Strona WBM „Multicast Statistics“

Tabela 61: 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“.
VID		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 wyświetlany jest „Host IP“.

9.3.3 VLAN

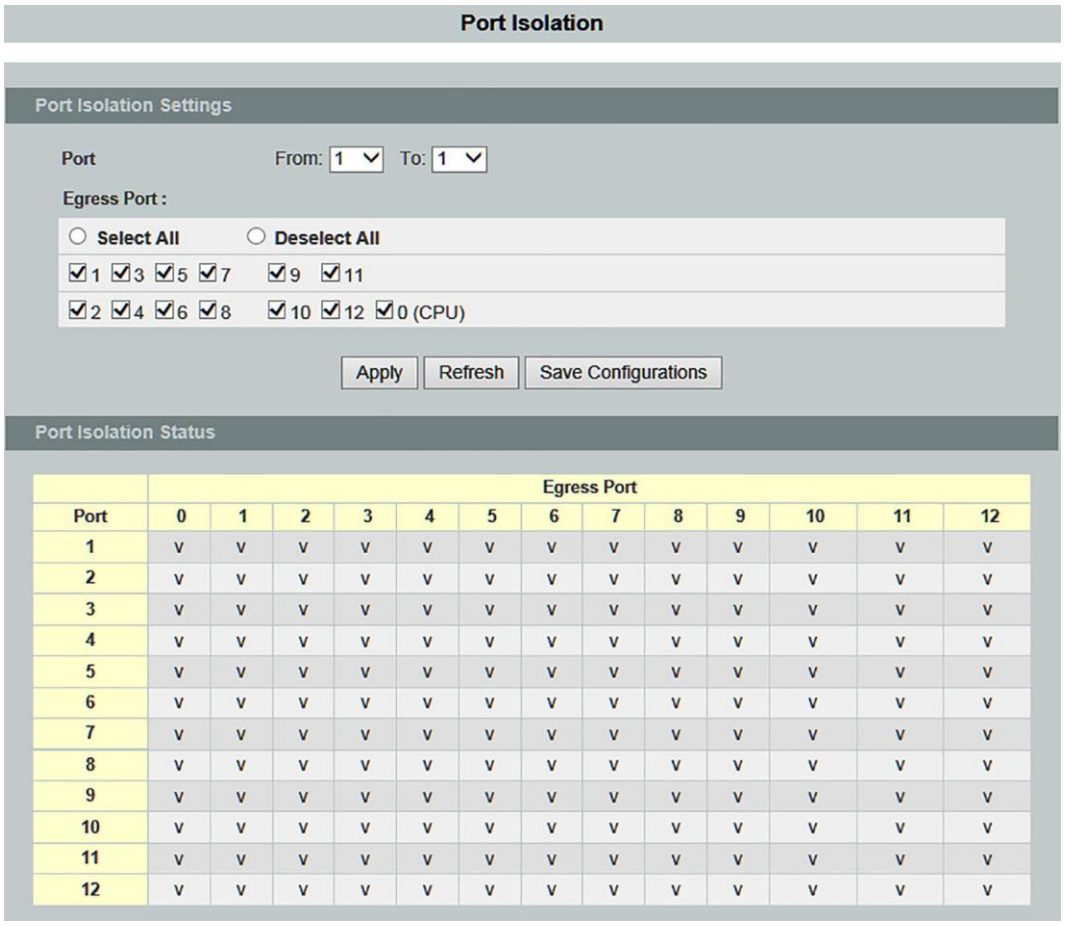
Wskazówka **Dodatkowa informacja**

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

9.3.3.1 Port Isolation

Wskazówka **Dodatkowa informacja**

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



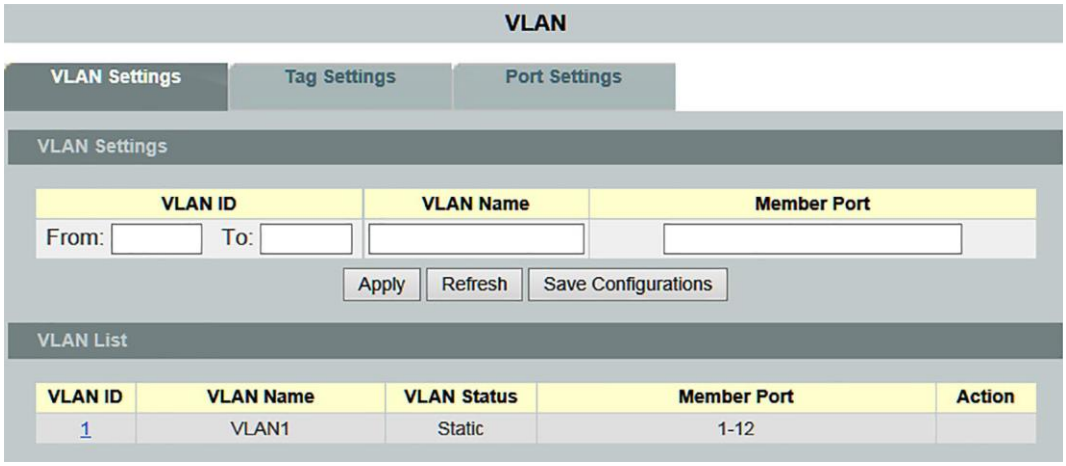
Ilustracja 60: Strona WBM „Port Isolation“

Tabela 62: 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 „Egres Port“ nie jest wybrany.
			◉	Wszystkie „Egress Port“ są wybrane.
	Disable All	○	○	Żaden „Egres Port“ nie jest dezaktywowany.
			◉	Wszystkie „Egress Port“ są dezaktywowane.
	☐ 0 (CPU) … ☐ 10 (12)	☐	☐	„Egress Port” nie jest aktywowany.
			☑	„Egress Port” jest aktywowany.
Port Isolation Status				
Parametr		**Domyślnie**	**Opis**	
Port		**V**	V	„V“ oznacza, że pakiety portu mogą być do niego wysyłane.
Egress Port			-	„-“ oznacza, że pakiety portu nie mogą być do niego wysyłane.

9.3.3.2 VLAN

9.3.3.2.1 VLAN Settings

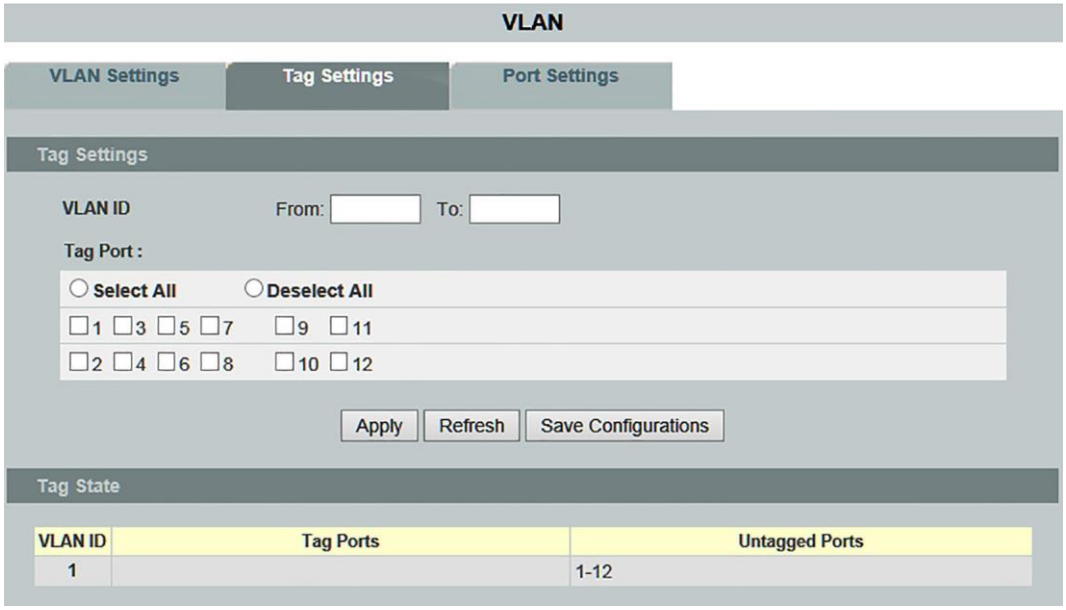


Ilustracja 61: Strona WBM „VLAN“ – zakładka „VLAN Settings“

Tabela 63: 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 VLAN 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.

9.3.3.2.2 Tag Settings

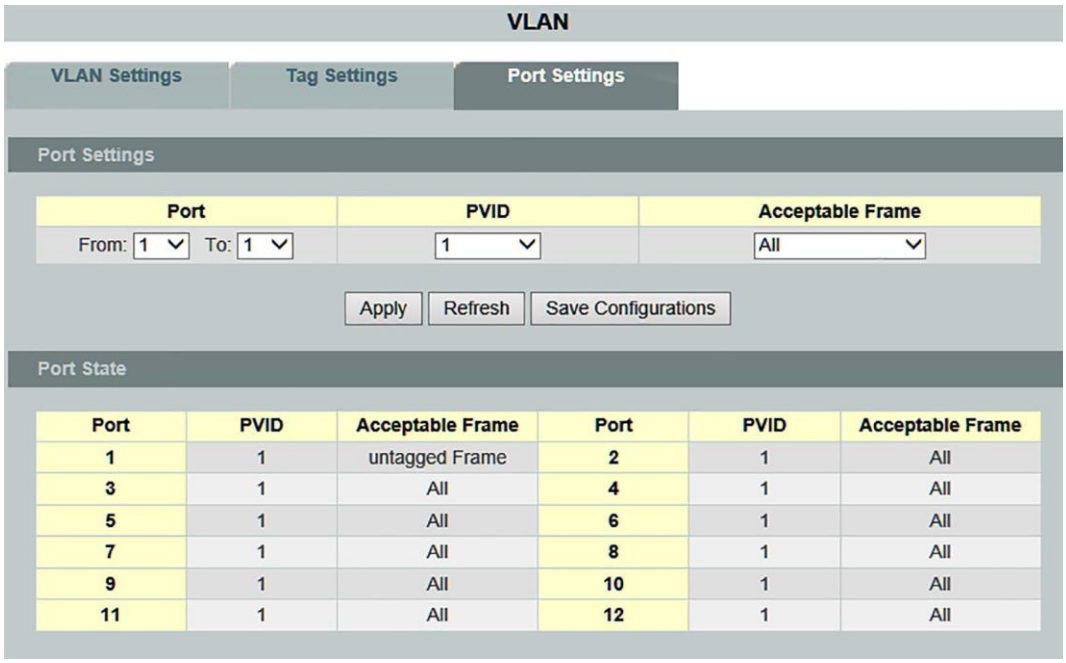


Ilustracja 62: Strona WBM „VLAN“ – zakładka „Tag Settings“

Tabela 64: 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.	

9.3.3.2.3 Port Settings



Ilustracja 63: Strona WBM „VLAN“ – zakładka „Port Settings“

Tabela 65: 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).
		untagged Frame	Należy wybrać „untagged Frame“, gdy na tym porcie mają być akceptowane tylko ramki bez znacznika. Wszystkie ramki ze znacznikiem zostają odrzucone.
		tagged Frame	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 untagged Frame tagged Frame	W tej kolumnie wyświetlane są rodzaje ramek dopuszczalnych dla tego portu.

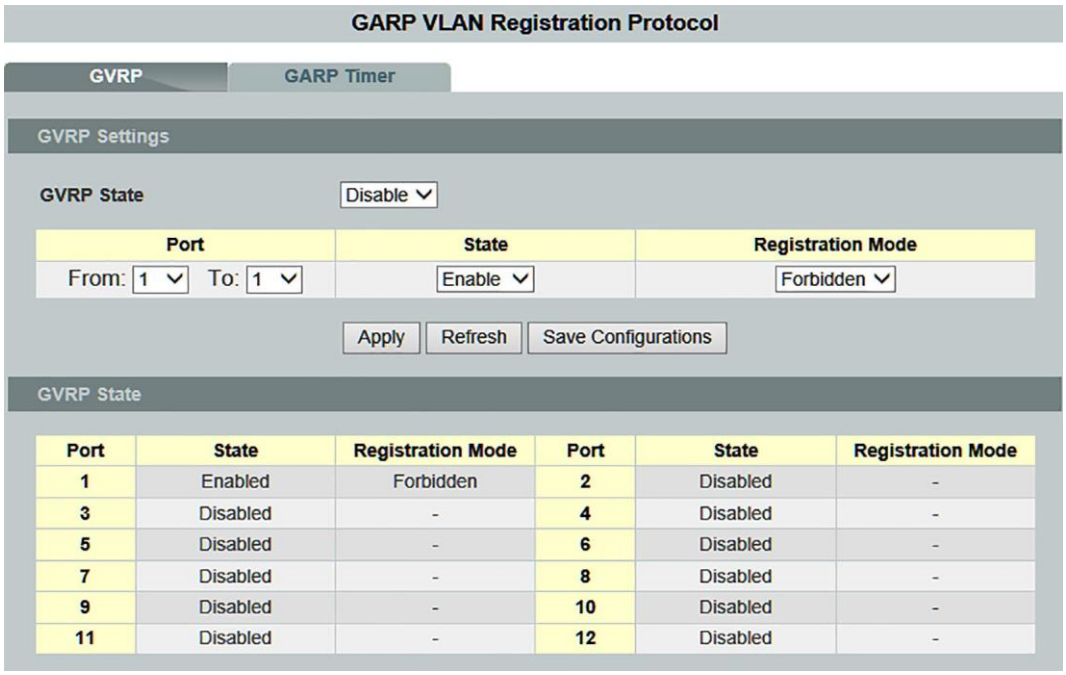
9.3.3.3 GARP VLAN Registration Protocol

Wskazówka

Dodatkowa informacja

Więcej informacji o „GARP/GVRP“ (**G**eneric **A**ttribute **R**egistration **P**rotocol/**G**ARP **V**LAN **R**egistration **P**rotocol lub **G**eneric **V**LAN **R**egistration **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.

9.3.3.3.1 GVRP



Ilustracja 64: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP“

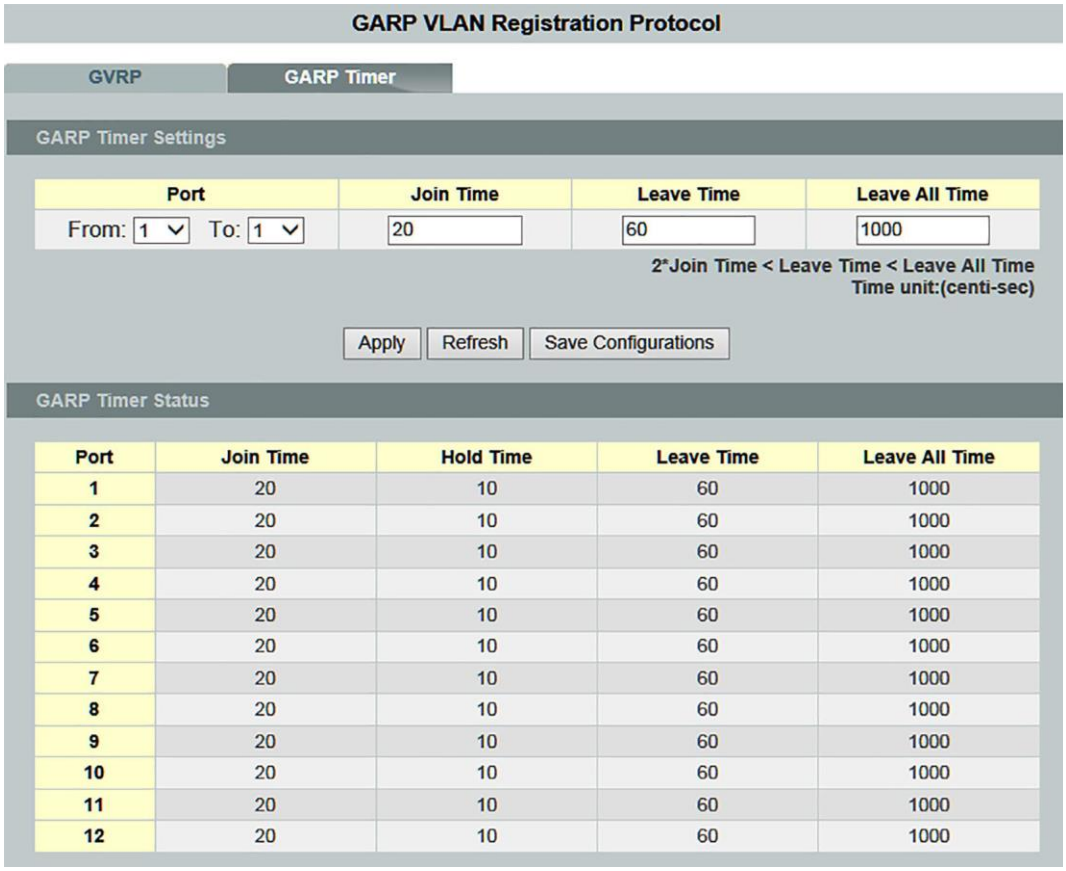
Tabela 66: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP“

GVRP Settings			
Parametr		**Domyślnie**	**Opis**
GVRP State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „GVRP”.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „GVRP“ i wymieniać informacje o konfiguracji VLAN z innymi switchami GVRP.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, przy którym mają być skonfigurowane ustawienia „GVRP”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, przy którym mają być skonfigurowane ustawienia „GVRP”.
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować dla portu funkcję „GVRP“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować dla portu funkcję „GVRP“.
Registration Mode		**Normal**	W polu wyboru należy wybrać „Normal“, aby pozwolić na dynamiczne tworzenie (gdy tylko aktywowane jest dynamiczne tworzenie VLAN), rejestrowanie i wyrejestrowanie sieci VLAN na porcie „Trunk“.
		Forbidden	W polu wyboru należy wybrać „Forbidden“, aby wyrejestrować wszystkie sieci VLAN (poza VLAN 1) i zapobiec dalszemu tworzeniu lub rejestracji sieci VLAN na porcie „Trunk“.
GVRP State			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
State		Disable Enable	W tej kolumnie wyświetlany jest ustawiony status.
Registration Mode		Normal Forbidden	W tej kolumnie wyświetlany jest wybrany „Registration Mode“.

9.3.3.3.2 GARP Timer

Wskazówka

Większe wartości dla „join“, „leave“ i „leave all“
Wartość dla „leave“ musi być większa niż trzykrotna wartość dla „join“ (leave >= join x 3).
Wartość dla „leave all“ musi być większa niż wartość dla „leave“ (leave all > leave).



Port	Join Time	Hold Time	Leave Time	Leave All Time
1	20	10	60	1000
2	20	10	60	1000
3	20	10	60	1000
4	20	10	60	1000
5	20	10	60	1000
6	20	10	60	1000
7	20	10	60	1000
8	20	10	60	1000
9	20	10	60	1000
10	20	10	60	1000
11	20	10	60	1000
12	20	10	60	1000

Ilustracja 65: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP Timer“

Tabela 67: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP Timer“

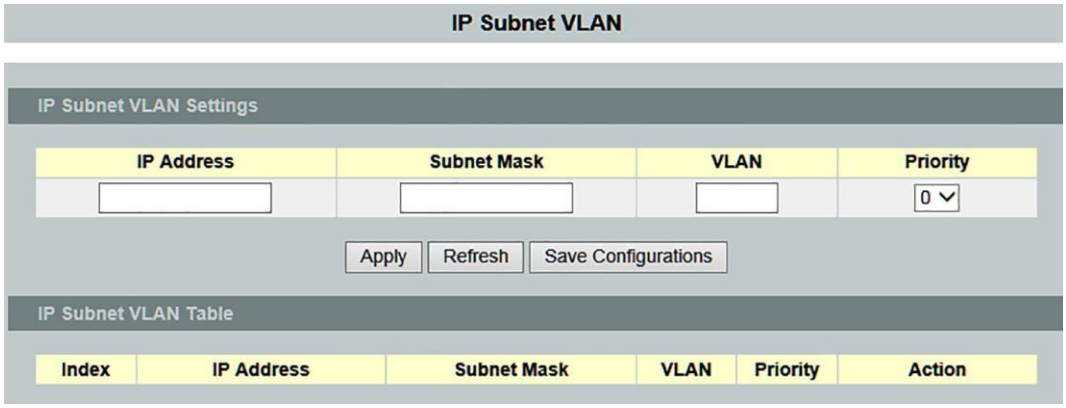
GARP Timer			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „GARP Timer“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „GARP Timer“.
Join Time		**20**	W polu edycji należy wpisać maksymalny czas w milisekundach, przez który interfejs czeka, zanim rozpocznie wysyłanie komunikatów VLAN.
Leave Time		**60**	W polu edycji należy wpisać maksymalny czas w milisekundach, przez który interfejs czeka po odebraniu „Leave Message“, zanim opuści wyspecyfikowaną we wiadomości sieć VLAN.
Leave All Time		**1000**	W polu edycji należy wpisać interwał czasowy w milisekundach, po którym „Leavealll Messages“ wysyłane są do interfejsów. „Leaveall Messages“ mogą przy tym pomóc w aktualizacji informacji o aktualnym członkostwie „GVRP“ i „VLAN“ w sieci.
GARP Timer Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Join Time			W tej kolumnie wyświetlany jest „Join Time“.
Hold Time			W tej kolumnie wyświetlany jest „Hold Time“.
Leave Time			W tej kolumnie wyświetlany jest „Leave Time“.
Leave All Time			W tej kolumnie wyświetlany jest „Leave All Time“.

9.3.3.4 IP Subnet VLAN

Wskazówka

Dodatkowa informacja

Więcej informacji o „IP Subnet VLAN” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 66: Strona WBM „IP Subnet VLAN“

Tabela 68: Strona WBM „IP Subnet VLAN“

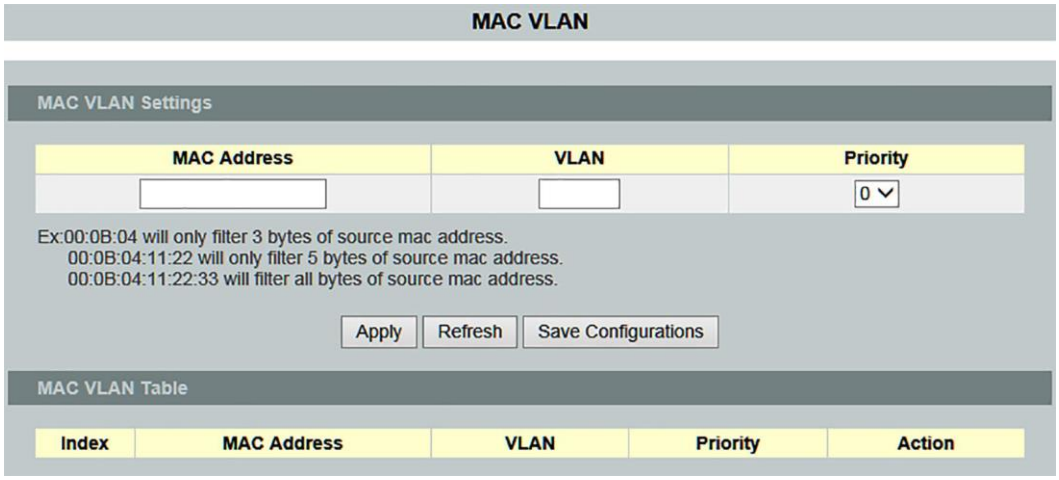
IP Subnet VLAN Settings		
Parametr	**Domyślnie**	**Opis**
IP Address		W polu edycji należy wpisać adres IP podsieci VLAN.
Subnet Mask		W polu edycji należy wpisać maskę podsieci switcha, używając zapisu z kropkami.
VLAN		W polu edycji należy wpisać wartość „IP Subnet VLAN“ dla instancji. Właściwy zakres: 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
IP Subnet VLAN Table		
Parametr	**Domyślnie**	**Opis**
Index	1 … 10	W tej kolumnie wyświetlana jest liczba wpisów.
IP Address		W tej kolumnie wyświetlany jest adres IP „IP Subnet VLAN”.
Subnet Mask		W tej kolumnie wyświetlana jest maska podsieci switcha.
VLAN		W tej kolumnie wyświetlana jest ID „IP Subnet VLAN” dla określonego portu.
Priority	0 … 7	W tej kolumnie wyświetlany jest priorytet dla specyficznego portu.
Action		Aby usunąć adresy „IP Subnet VLAN“, należy kliknąć **[Delete]**.
Total counts		W tym polu wyświetlana jest zbiorcza liczba wpisów w tabeli „IP Subnet VLAN”.

9.3.3.5 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“.

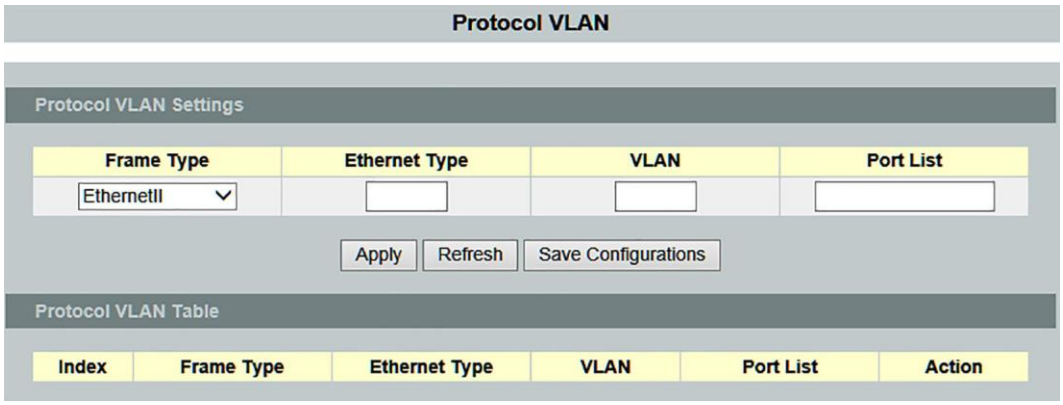


Ilustracja 67: Strona WBM „MAC VLAN“

Tabela 69: 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]**.

9.3.3.6 Protocol VLAN



Ilustracja 68: Strona WBM „Protocol VLAN“

Tabela 70: Strona WBM „Protocol VLAN“

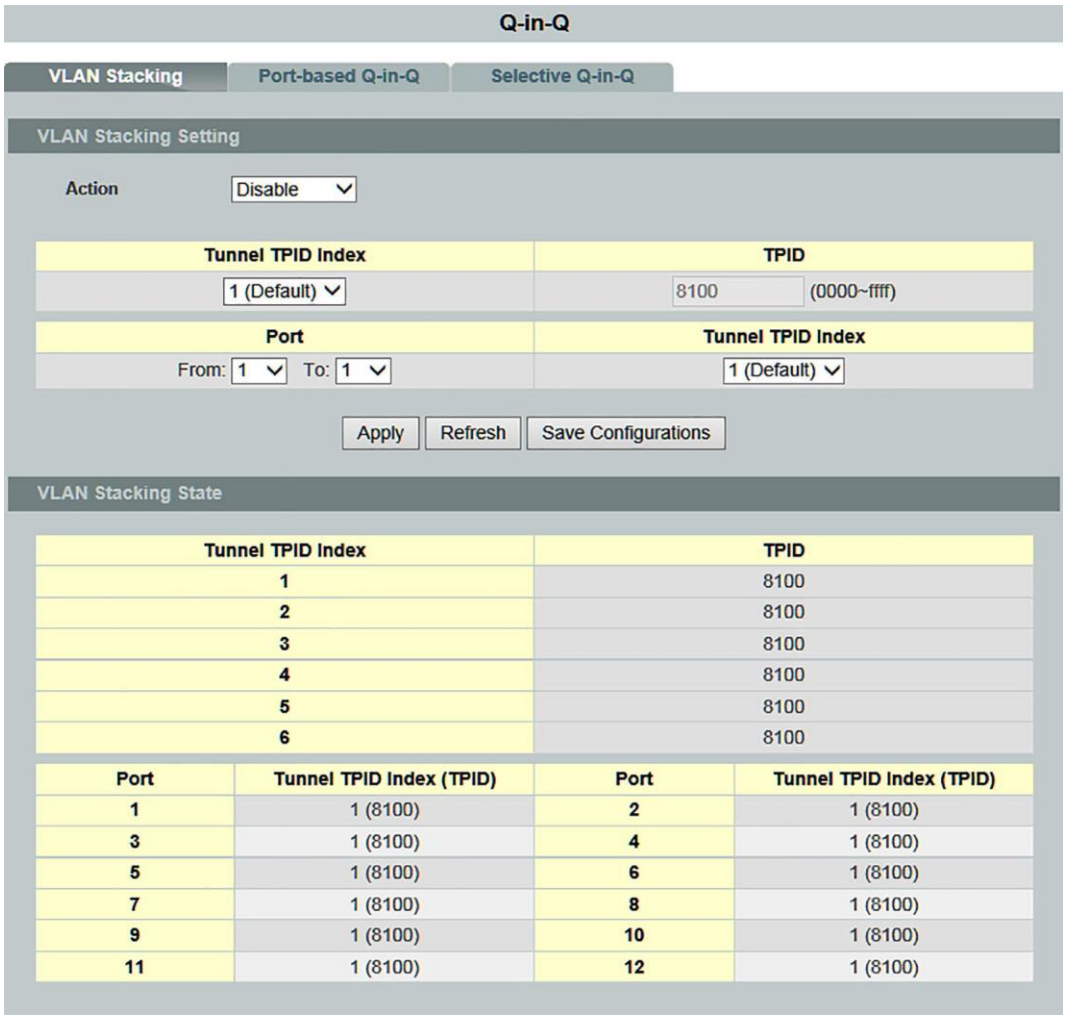
MAC VLAN Settings		
Parametr	**Domyślnie**	**Opis**
Frame Type	**EthernetII**	W polu wyboru należy wybrać „EthernetII“, gdy ma być skonfigurowany ten typ ramki.
	Non-LLC SNAP	W polu wyboru należy wybrać „Non-LLC SNAP“, gdy ma być skonfigurowany ten typ ramki.
	LLC SNAP	W polu wyboru należy wybrać „LLC SNAP“, gdy ma być skonfigurowany ten typ ramki.
Ethernet Type		W polu edycji należy wpisać typ ETHERNET. (np. 0800)
VLAN	1 … 4094	W polu edycji należy wpisać VLAN ID. Właściwy zakres: 1 … 4094
Port List	1 … 10 (12)	W polu edycji należy wpisać port lub grupę portów (np. 1 – 3) dla „Protocol VLAN“.
Protokol VLAN Table		
Parametr	**Domyślnie**	**Opis**
Index		W tej kolumnie wyświetlana jest liczba wpisów.
Frame Type		W tej kolumnie wyświetlany jest typ ramki.
ETHERNET Type		W tej kolumnie wyświetlany jest typ ETHERNET.
VLAN		W tej kolumnie wyświetlany jest VLAN ID.
Port List		W tej kolumnie wyświetlana jest „Port List“.
Action		Aby usunąć adresy multicast, należy kliknąć **[Delete]**.

9.3.3.7 Q-in-Q

Wskazówka

Dodatkowa informacja
Więcej informacji o „Q-in-Q” można znaleźć w rozdziale „Opis funkcji”.

9.3.3.7.1 VLAN Stacking

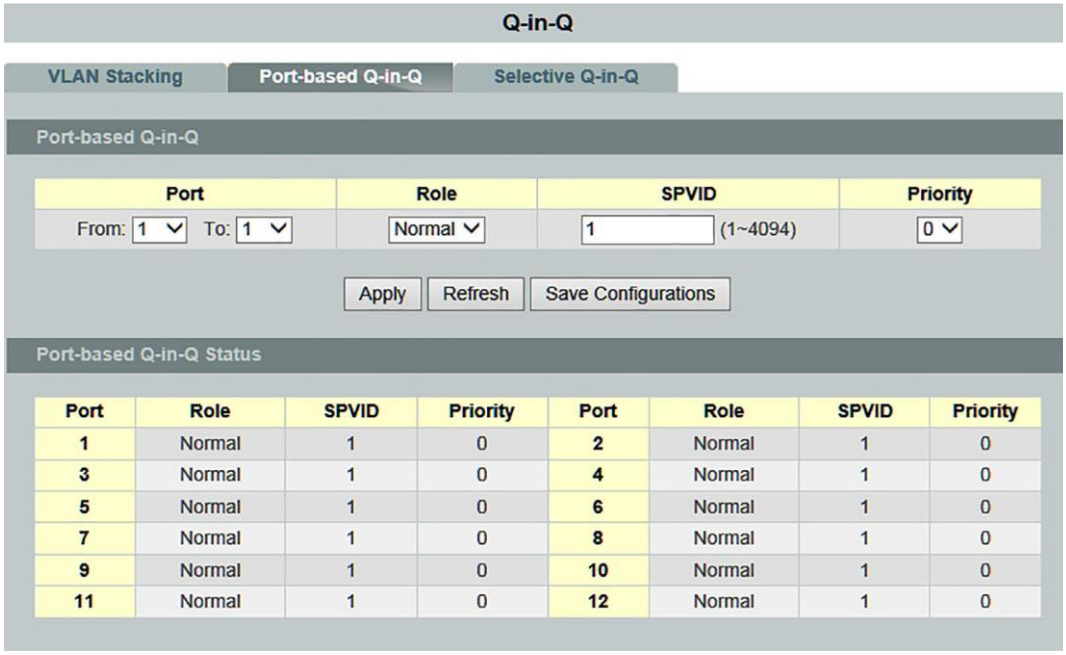


Ilustracja 69: Strona WBM „Q-in-Q“ – zakładka „VLAN Stacking“

Tabela 71: Strona WBM „Q-in-Q“ – zakładka „VLAN Stacking“

VLAN Stacking Setting			
Parametr		**Domyślnie**	**Opis**
Action		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „VLAN Stacking“.
		Port-Based	W polu wyboru należy wybrać „Port-Based“, aby realizować funkcję „VLAN Stacking“ na bazie portów.
		Selective	W polu wyboru należy wybrać „Selective“, aby realizować funkcję „VLAN Stacking“ selektywnie.
Tunnel TPID Index		1 (Default) … 6	W polu wyboru należy wybrać numer indeksu tabeli.
TPID (0000~ffff)			W polu edycji należy wpisać wartość dla TRIP. Właściwy zakres: 0000 … ffff
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „VLAN Stacking“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „VLAN Stacking“.
Tunnel TPID Index		1 (Default) … 6	W polu wyboru należy wybrać „Tunnel TPID Index“.
VLAN Stacking State			
Parametr		**Domyślnie**	**Opis**
Tunnel TPID Index		1 … 6	W tej kolumnie wyświetlany jest numer indeksu tabeli.
TPID		0000 … ffff	W tej kolumnie wyświetlany jest TRIP.
Port		1 … 10 (12)	W tej kolumnie wyświetlany jest numer portu.
Tunnel TPID Index (TPID)			W tej kolumnie wyświetlany jest numer indeksu tabeli dla specyficznego portu.

9.3.3.7.2 Port-based Q-in-Q

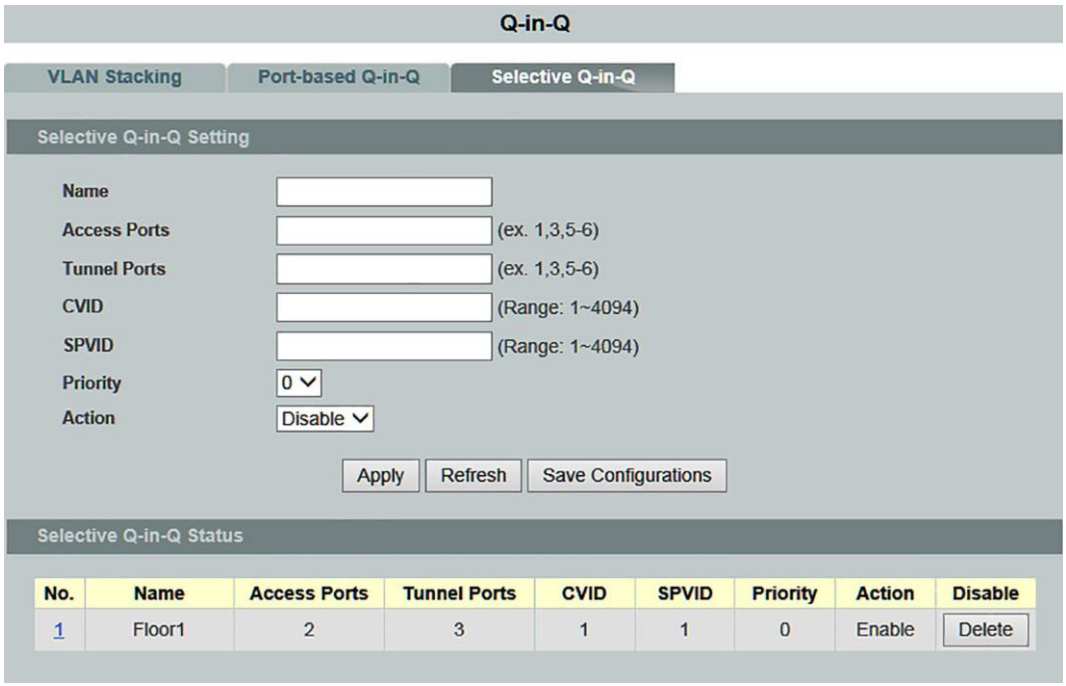


Ilustracja 70: Strona WBM „Q-in-Q“ – zakładka „Port-based Q-in-Q“

Tabela 72: Strona WBM „Q-in-Q“ – zakładka „Port-based Q-in-Q“

Port-based Q-in-Q			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Q-in-Q“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Q-in-Q“.
Role		**Normal**	W polu wyboru należy wybrać „Normal“, aby wybrać tę rolę dla specyficznego portu.
		Access	W polu wyboru należy wybrać „Access“, aby wybrać tę rolę dla specyficznego portu.
		Tunnel	W polu wyboru należy wybrać „Tunnel“, aby wybrać tę rolę dla specyficznego portu.
SPVID (1~4094)		**1**	W polu edycji należy wpisać VLAN dostawcy usługi „SPVID”. Właściwy zakres: 1 … 4094
Priority		**0** … 7	W polu wyboru należy wybrać priorytet dla specyficznego portu. 0 = najniższy priorytet 7 = najwyższy priorytet
Port-based Q-in-Q Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlany jest numer portu.
Role			W tej kolumnie wyświetlana jest rola specyficznego portu.
SPVID			W tej kolumnie wyświetlana jest SPVID.
Priority			W tej kolumnie wyświetlany jest priorytet dla specyficznego portu.

9.3.3.7.3 Selective Q-in-Q



Ilustracja 71: Strona WBM „Q-in-Q“ – zakładka „Selective Q-in-Q“

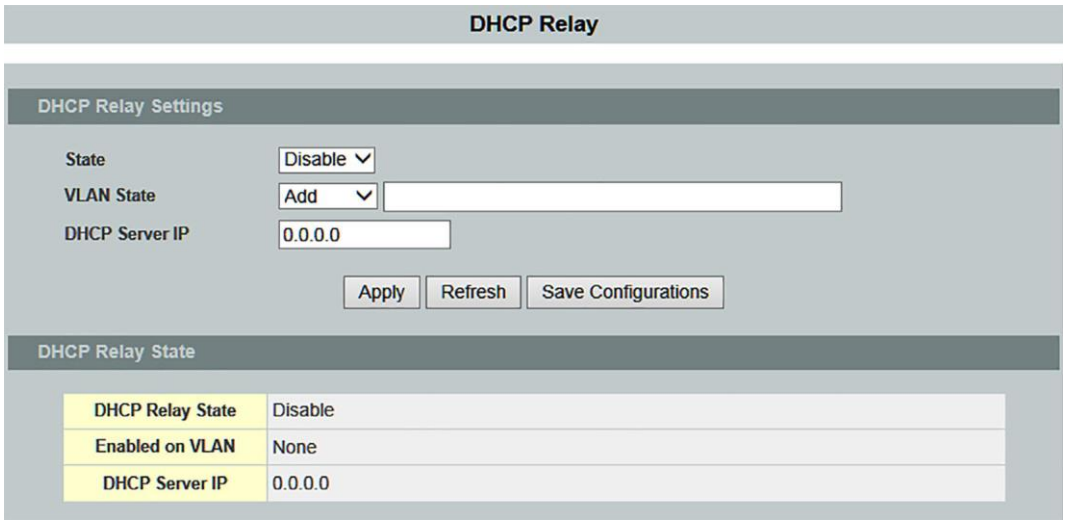
Tabela 73: Strona WBM „Q-in-Q“ – zakładka „Selective Q-in-Q“

Selective Q-in-Q Setting		
Parametr	**Domyślnie**	**Opis**
Name		W polu edycji należy wpisać nazwę dla selektywnego profilu „Q-in-Q”.
Access Ports (ex. 1,3,5-6)		W polu edycji należy wpisać „Access Port“ lub zakres.
Tunnel Ports (ex. 1,3,5-6)		W polu edycji należy wpisać „Tunnel Port“ lub zakres.
CVID (Range: 1~4094)		W polu edycji należy wpisać VLAN klienta „CVID“. Właściwy zakres: 1 … 4094
SPVID (Range: 1~4094)		W polu edycji należy wpisać VLAN dostawcy usługi „SPVID”. Właściwy zakres: 1 … 4094
Priority	**0** … 7	W polu wyboru należy wybrać poziom priorytetu. 0 = najniższy priorytet 7 = najwyższy priorytet
Action	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
Selektiver Q-in-Q Status		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlany jest numer indeksu.
Name		W tej kolumnie wyświetlana jest nazwa selektywnego profilu „Q-in-Q”.
Access Ports		W tej kolumnie wyświetlany jest „Access Port“.
Tunnel Ports		W tej kolumnie wyświetlany jest „Tunnel Port“.
CVID		W tej kolumnie wyświetlany jest VLAN klienta „CVID“.
SPVID		W tej kolumnie wyświetlany jest VLAN dostawcy usługi „SPVID”.
Priority	0 … 7	W tej kolumnie wyświetlany jest poziom priorytetu. 0 = najniższy priorytet 7 = najwyższy priorytet
Action	Disable Enable	W tej kolumnie wyświetlana jest wybrana akcja.
Disable		Aby usunąć ustawienia dla selektywnej „Q-in-Q“, należy kliknąć **[Delete]**.

9.3.4 DHCP Relay

Wskazówka

Dodatkowa informacja
Więcej informacji o „DHCP Relay“ (**D**ynamic **H**ost **C**onfiguration **P**rotocol **Relay**) można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 72: Strona WBM „DHCP Relay“

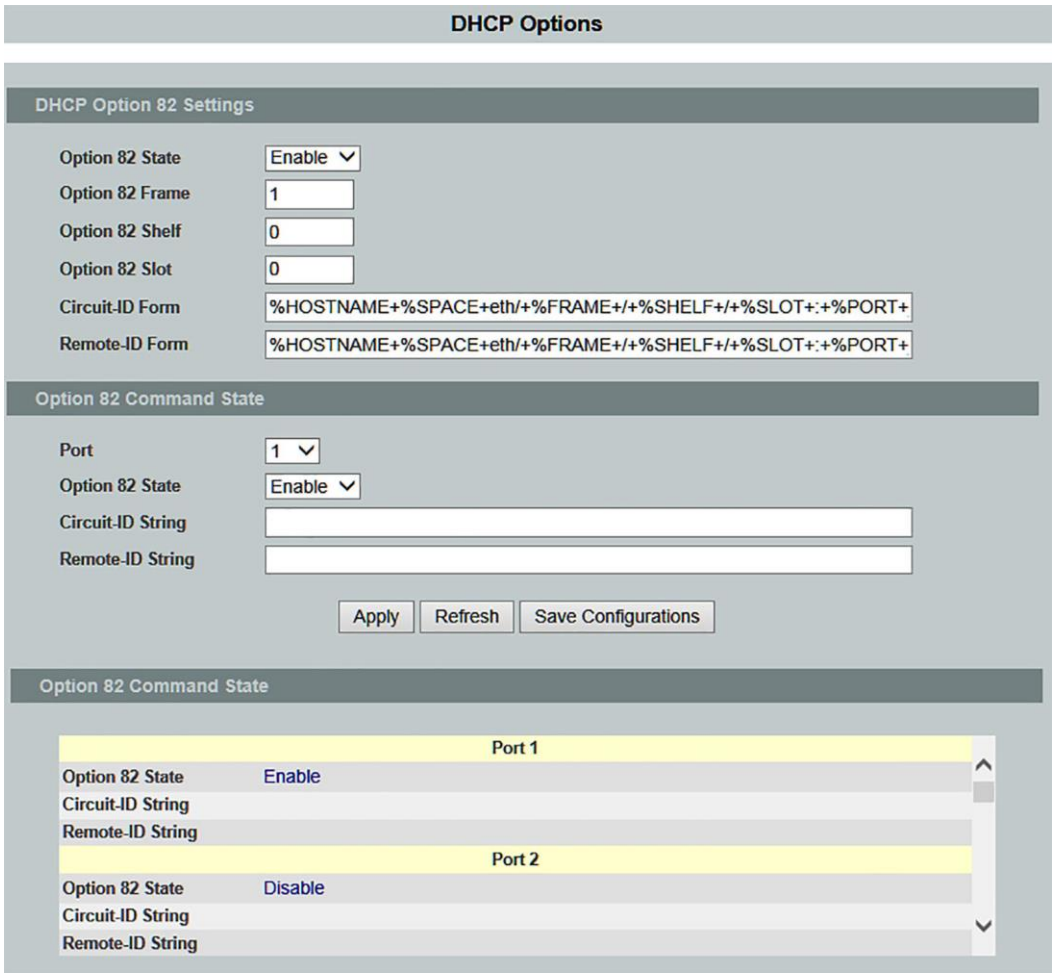
Tabela 74: Strona WBM „DHCP Relay“

DHCP Relay Settings		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „DHCP Relay”.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „DHCP Relay“.
VLAN State	**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, w których switch ma wykonywać „DHCP Relay“. 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 nie ma wykonywać „DHCP Relay“.
DHCP Server IP	**0.0.0.0**	W polu edycji należy wpisać adres IP serwera DHCP.
DHCP Relay State		
Parametr	**Domyślnie**	**Opis**
DHCP Relay State	Disable Enable	W tym polu wyświetlana jest informacja, czy funkcja „DHCP Relay“ jest aktywowana, czy dezaktywowana.
Enabled on VLAN	None 0 … 4094	W tym polu wyświetlana jest informacja, czy używana jest sieć VLAN.
DHCP Server IP		W tym polu wyświetlany jest adres IP serwera DHCP.

9.3.5 DHCP Options

Wskazówka

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



Ilustracja 73: Strona WBM „DHCP Options“

Tabela 75: Strona WBM „DHCP Options“

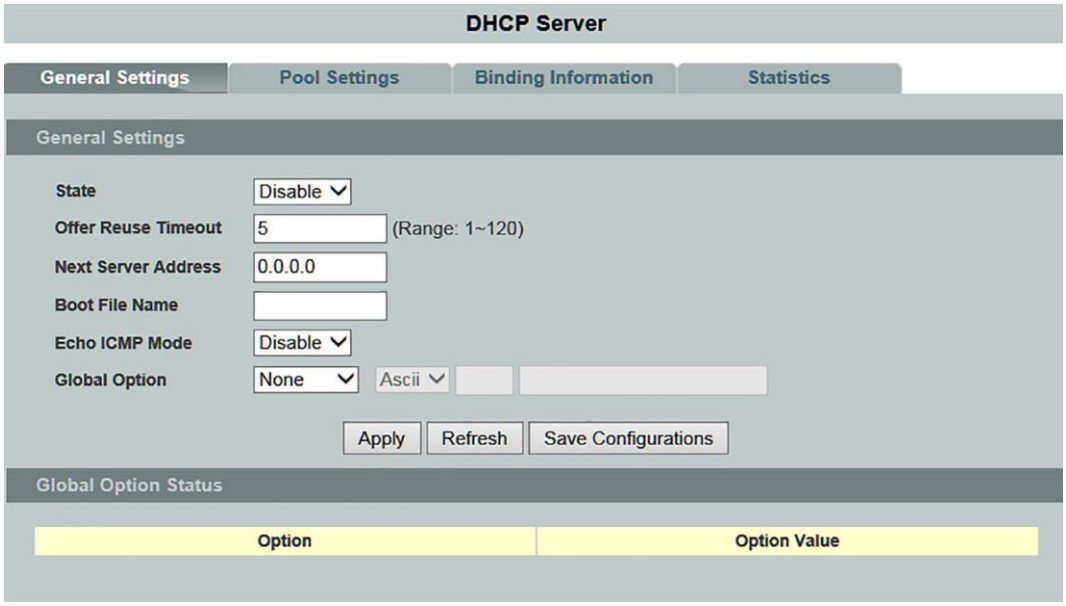
DHCP Option 82 Settings		
Parametr	**Domyślnie**	**Opis**
Option 82 State	**Enable**	W polu wyboru należy wybrać „Enable“, aby dezaktywować w switchu „DHCP Option 82“.
	Disable	W polu wyboru należy wybrać „Disable“, aby aktywować w switchu „DHCP Option 82”.
Option 82 Frame	**1**	W polu edycji należy wpisać żądany numer ramki.
Option 82 Shelf	**0**	W polu edycji należy wpisać żądany numer „Shelf”, aby jednoznacznie zidentyfikować switch.
Option 82 Slot	**0**	W polu edycji należy wpisać żądany numer „Slot”, aby jednoznacznie zidentyfikować switch.
Circuit-ID String	**%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN**	W polu edycji można zmodyfikować dodany string.
Remote-ID Form	**%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN**	W polu edycji można zmodyfikować dodany string.
Option 82 Command State		
Parametr	**Domyślnie**	**Opis**
Port	**1** … 10 (12)	W polu wyboru należy wybrać port.
Option 82 State	**Enable**	W polu wyboru należy wybrać „Enable“, aby dezaktywować w switchu „Option 82 Command State”.
	Disable	W polu wyboru należy wybrać „Disable“, aby aktywować w switchu „Option 82 Command State”.
Circuit-ID String		W polu edycji należy wpisać „Circuit-ID String“.
Remote-ID String		W polu edycji należy wpisać „Remote-ID String“.
Option 82 Command State		
Parametr	**Domyślnie**	**Opis**
Port	**1** … 10 (12)	W tym polu wyświetlane są numery portów.
Option 82 State		W tym polu wyświetlany jest „Option-82-Status“.
Circuit-ID String		W tym polu wyświetlany jest „Circuit-ID String“.
Remote-ID String		W tym polu wyświetlany jest „Remote-ID String“.

9.3.6 DHCP Server

Wskazówka

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

9.3.6.1 General Settings

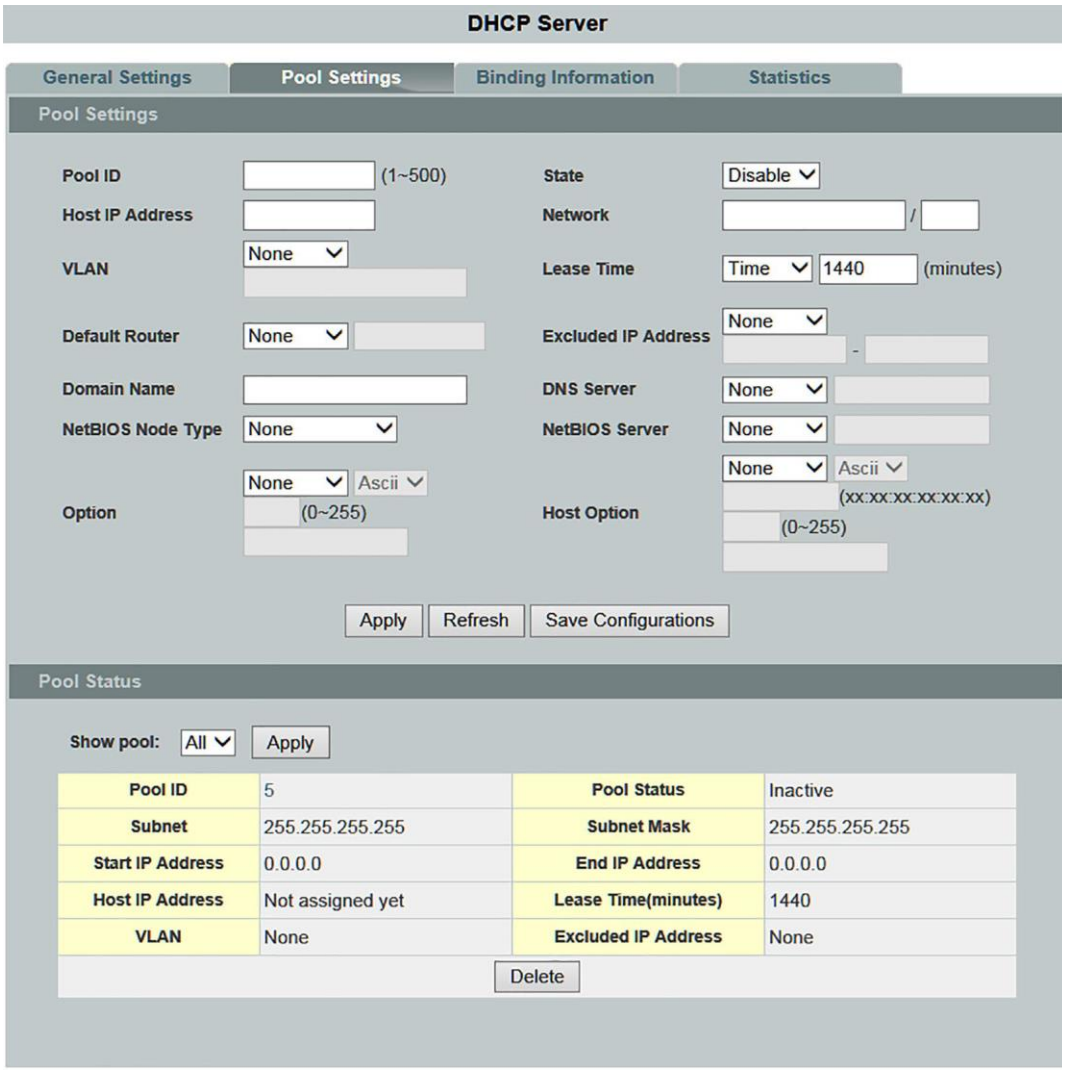


Ilustracja 74: Strona WBM „DHCP Server“ – zakładka „General Settings“

Tabela 76: Strona WBM „DHCP Server“ – zakładka „General Settings“

General Settings		
Parametr	**Domyślnie**	**Opis**
State	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „DHCP Server“.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję „DHCP Server“.
Offer Reuse Timeout (Range: 1~120)		W polu edycji należy wprowadzić maksymalny czas, po którym oferowany adres IP może zostać zwrócony do puli wolnych adresów. Właściwy zakres: 1 … 120
Next Server Address	0.0.0.0	W polu edycji należy wpisać adres IP dla następnego serwera.
Boot File Name		W polu edycji należy wpisać nazwę pliku boot, który jest stosowany do zidentyfikowania obrazu boot.
Echo ICMP Mode	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „Echo ICMP Mode“. Zanim serwer zaproponuje klientowi określony adres IP, tworzone jest żądanie ICMP w celu zapewnienia, że adres, który ma być zaproponowany, który ma być zaproponowany, nie jest używany przez żaden host w sieci.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Echo ICMP Mode“.
Global Option		W tym polu wyboru konfigurowane są globalne opcje i ich format. „Global Option“ dostępne są dla „DHCP Clients“ tylko wtedy, gdy nie ma opcji specyficznej dla hosta i opcji specyficznej dla „Pool“.
	None	W polu wyboru należy wybrać „None“, gdy nie ma być skonfigurowana „Global Option“.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „Global Option“.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „Global Option“.
	Ascii	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć globalną opcję w kodzie Ascii.
	IP	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć adres IP dla „Global Option“.
Global Option Status		
Parametr	**Domyślnie**	**Opis**
Option		W tej kolumnie wyświetlany jest numer indeksu tabeli.
Option Value		W tej kolumnie wyświetlany jest TRIP.

9.3.6.2 Pool Settings



Ilustracja 75: Strona WBM „DHCP Server“ – zakładka „Pool Settings“

Tabela 77: Strona WBM „DHCP Server“ – zakładka „Pool Settings“

General Settings		
Parametr	**Domyślnie**	**Opis**
Pool ID (1~8)		W polu edycji należy wpisać „Pool ID”. Właściwy zakres: 1 … 8
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować ustawienia „Pool“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować ustawienia „Pool“.
Host IP Address		W polu edycji należy wpisać „Host IP Address“, który będzie zastosowany przy wysyłaniu pakietów danych jako źródłowy adres IP.
Network		W polu edycji należy wpisać adres sieci.
VLAN		W polu wyboru można wybrać VLAN.
	None	W polu wyboru należy wybrać „None“, gdy nie ma być podana sieć VLAN.
	Add	W polu wyboru należy wybrać „Add“, aby dodać sieć VLAN.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć sieć VLAN.
Lease Time (minutes)	**Time**	W polu wyboru należy wybrać „Time“, aby podać czas, przez który klient może korzystać z adresu IP, przydzielonego przez serwer.
	Infinite	W polu wyboru należy wybrać „Infinite“, jeśli czas ma być nieograniczony.
Default Router		W polu wyboru można wybrać „Default Router“.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden „Default Router”.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „Default Router”.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „Default Router”.
Excluded IP Address		W polu wyboru można wybrać wyłączony adres IP.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden „Default Router”.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „Default Router”.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „Default Router”.
Domain Name		W polu edycji należy wpisać nazwę domeny.
DNS Server		W polu wyboru można wybrać „DNS Server“.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden „DNS Server”.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „DNS Server”.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „DNS Server”.

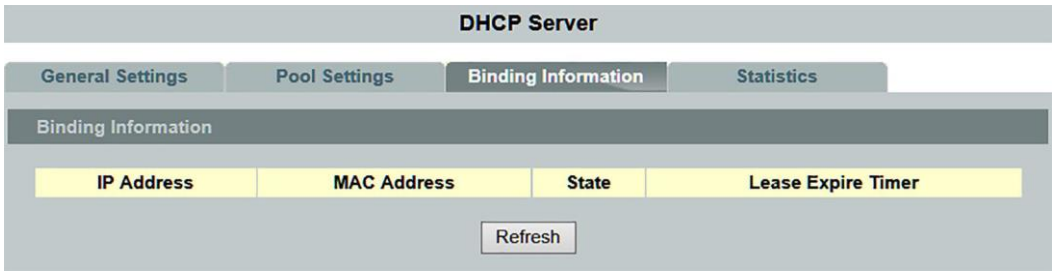
Tabela 77: Strona WBM „DHCP Server“ – zakładka „Pool Settings“

NetBIOS Node Type	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden „NetBios Node Type”.
	B-Node	W polu wyboru należy wybrać „B-Node“, aby wybrać ten „NetBios Node Type“.
	H-Node	W polu wyboru należy wybrać „H-Node“, aby wybrać ten „NetBios Node Type“.
	M-Node	W polu wyboru należy wybrać „M-Node“, aby wybrać ten „NetBios Node Type“.
	P-Node	W polu wyboru należy wybrać „P-Node“, aby wybrać ten „NetBios Node Type“.
	Remove Node	W polu wyboru należy wybrać „Remove-Node“, aby wybrać ten „NetBios Node Type“.
NetBIOS Server		W polu wyboru można wybrać „NetBIOS Server“.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden.„NetBios Server”.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „NetBios Server”.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „NetBios Server”.
Option (0~255)		W tym polu wyboru konfigurowane są opcje i ich format. Właściwy zakres: 0 … 255
	None	W polu wyboru należy wybrać „None“, jeśli „Option“ nie ma być wybrana.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „Option“.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „Option“.
	Ascii	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć „Option“ w kodzie Ascii.
	IP	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć adres IP dla „Option“.
Host Option xx:xx:xx:xx:xx:xx (0~255)		W tym polu wyboru konfigurowane są „Host Option“ i ich format. Właściwy zakres: 0 … 255
	None	W polu wyboru należy wybrać „None“, jeśli „Option“ nie ma być wybrana.
	Add	W polu wyboru należy wybrać „Add“, aby dodać „Option“.
	Remove	W polu wyboru należy wybrać „Remove“, aby usunąć „Option“.
	Ascii	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć „Option“ w kodzie Ascii.
	IP	Jeśli została wybrana funkcja „Add“ lub „Remove“, w tym polu edycji można wpisać lub usunąć adres IP dla „Option“.

Tabela 77: Strona WBM „DHCP Server“ – zakładka „Pool Settings“

Global Option Status		
Parametr	**Domyślnie**	**Opis**
Show Pool	All 1 … 8	W polu wyboru należy wybrać odpowiedni „Pool“.
Pool ID		W tym polu wyświetlany jest „Pool ID“.
Pool Status		W tym polu wyświetlana jest informacja, czy funkcja „Pool“ jest aktywowana, czy dezaktywowana.
Subnet		W tym polu wyświetlana jest „Subnet“.
Subnet Mask		W tym polu wyświetlana jest „Subnet Mask“.
Start IP Address		W tym polu wyświetlany jest „Start IP Address“.
End IP Address		W tym polu wyświetlany jest „End IP Address“.
Host IP Address		W tym polu wyświetlany jest „Host IP Address“.
Lease Time		W tym polu wyświetlany jest „Lease Time“ w minutach.
VLAN		W tym polu wyświetlana jest sieć VLAN.
Excluded IP Address		W tym polu wyświetlany jest wyłączony adres IP.

9.3.6.3 Binding Information

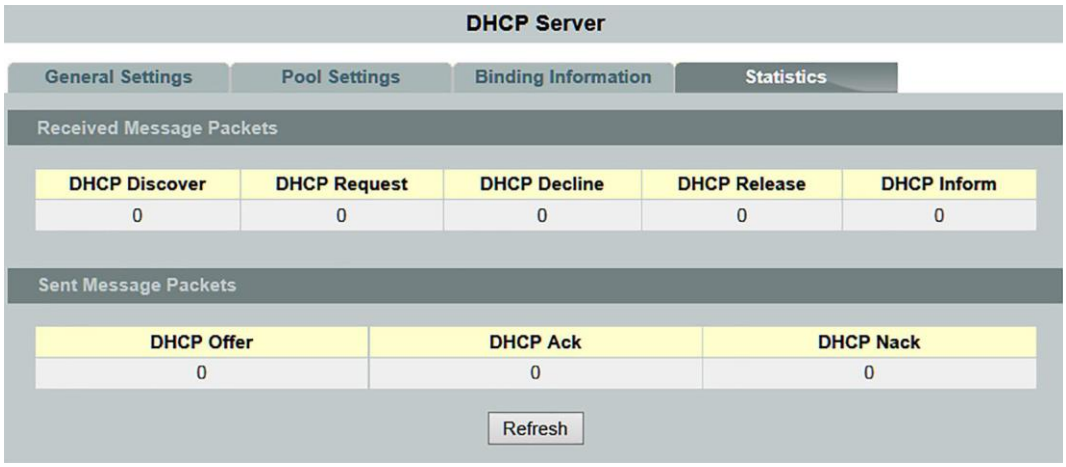


Ilustracja 76: Strona WBM „DHCP Server“ – zakładka „Binding Information“

Tabela 78: Strona WBM „DHCP Server“ – zakładka „Binding Information“

Binding Information		
Parametr	**Domyślnie**	**Opis**
IP Address		W tej kolumnie wyświetlany jest adres IP.
MAC Address		W tej kolumnie wyświetlany jest adres MAC.
State		W tej kolumnie wyświetlany jest status.
Lease Expire Timer		W tej kolumnie wyświetlany jest „Lease Expire Timer“.

9.3.6.4 Statistics



Ilustracja 77: Strona WBM „DHCP Server“ – zakładka „Statistics“

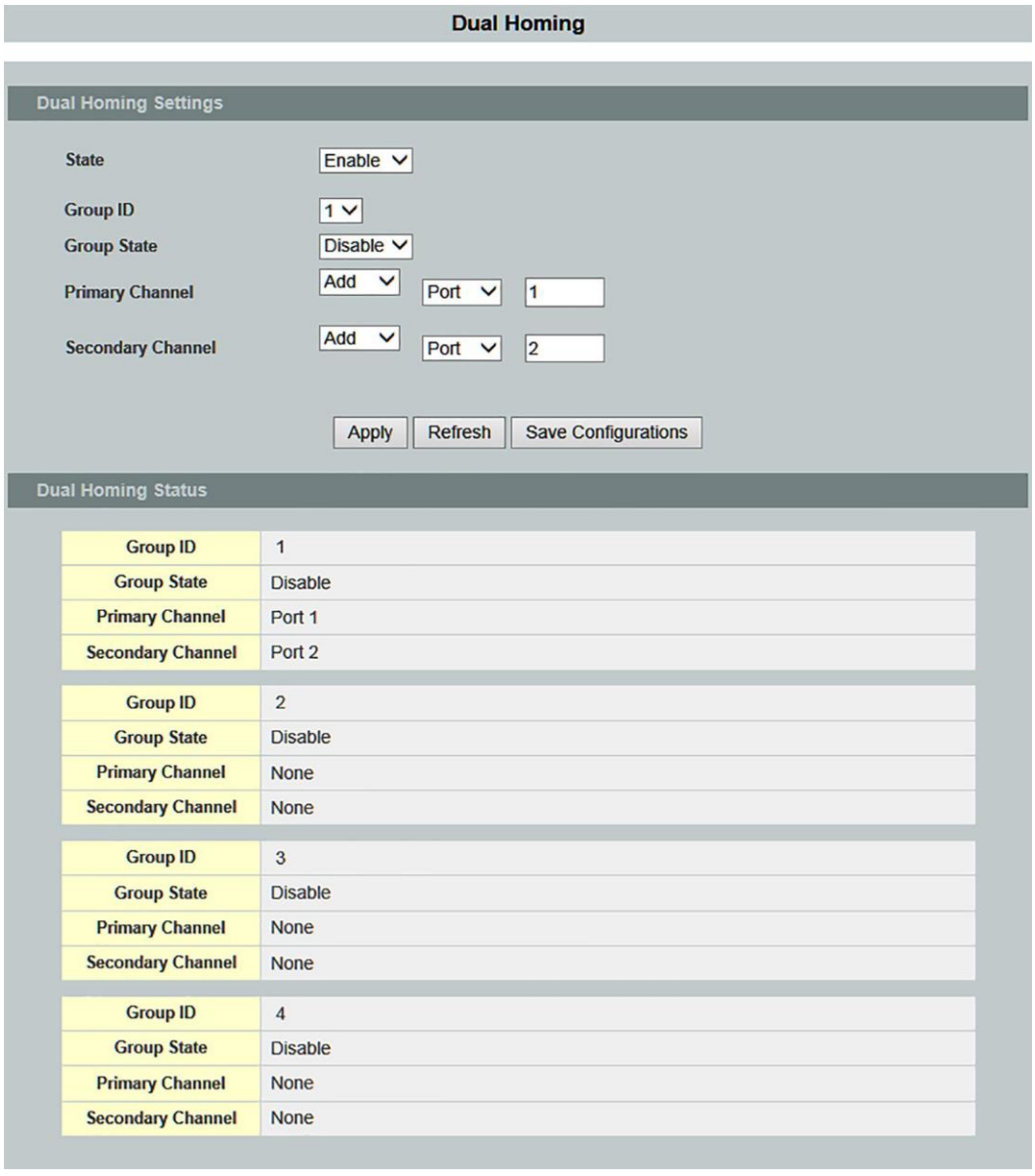
Tabela 79: Strona WBM „DHCP Server“ – zakładka „Statistics“

Received Message Packets		
Parametr	**Domyślnie**	**Opis**
DHCP Discover		W tej kolumnie wyświetlana jest wartość dla „DHCP Discover“.
DHCP Request		W tej kolumnie wyświetlana jest wartość dla „DHCP Request“.
DHCP Decline		W tej kolumnie wyświetlana jest wartość dla „DHCP Decline“.
DHCP Release		W tej kolumnie wyświetlana jest wartość dla „DHCP Release“.
Sent Message Packets		
Parametr	**Domyślnie**	**Opis**
DHCP Offer		W tej kolumnie wyświetlana jest wartość dla „DHCP Offer“.
DHCP Ack		W tej kolumnie wyświetlana jest wartość dla „DHCP Ack“.
DHCP Nack		W tej kolumnie wyświetlana jest wartość dla „DHCP Nack“.

9.3.7 Dual Homing

Wskazówka

Dodatkowa informacja
Więcej informacji o „Dual Homing“ można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 78: Strona WBM „Dual Homing“

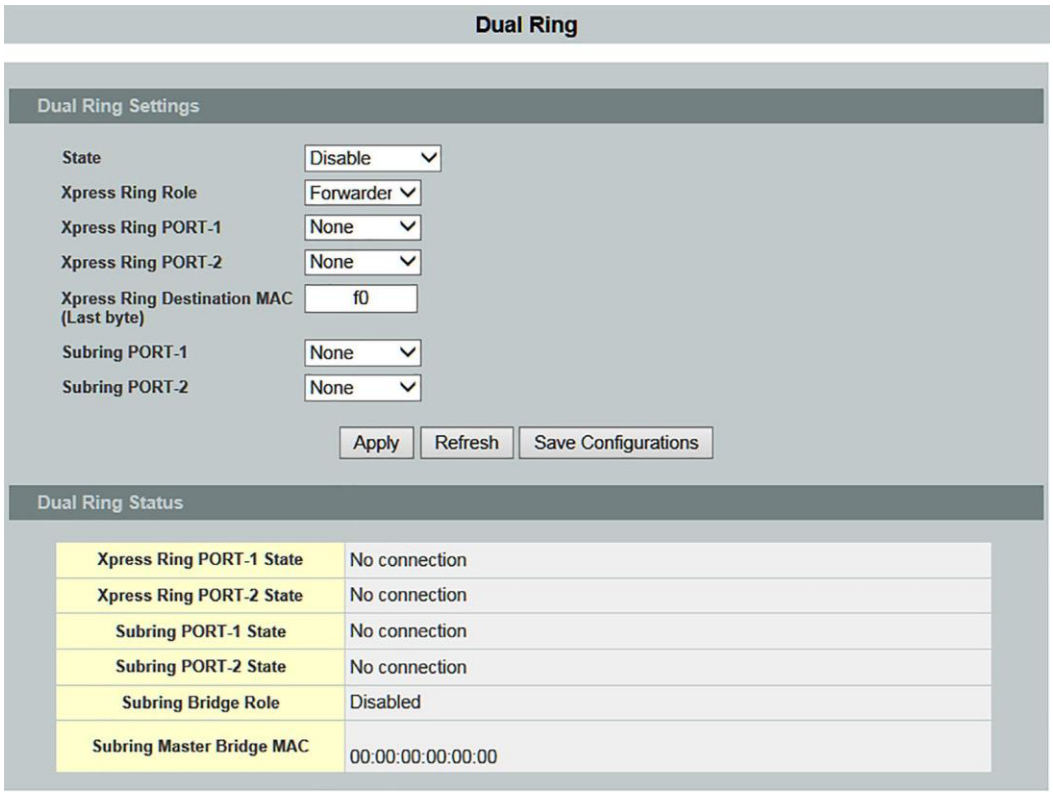
Tabela 80: Strona WBM „Dual Homing“

Dual Homing Settings		
Parametr	**Domyślnie**	**Opis**
State	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „Dual Homing“.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Dual Homing“.
Group ID	**1** … 4	W polu wyboru należy wybrać grupę „Dual Homing“, która ma być wyświetlona.
Group State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
Primary Channel	**Add**	W polu wyboru należy wybrać „Add“, aby dodać „Primary Channel“.
	Reset	W polu wyboru należy wybrać „Reset“, aby zresetować „Primary Channel“.
	Port	W tym polu konfiguruje się „Primary Channel“. W polu wyboru należy wybrać „Port“, aby skonfigurować tylko jeden port.
	Trunk	W tym polu konfiguruje się „Secondary Channel“. W polu wyboru należy wybrać Trunk“, aby skonfigurować tylko jedną „Trunk Group“.
		W polu edycji należy wpisać numer „Primary Channel“.
Sekundary Channel	**Add**	W polu wyboru należy wybrać „Add“, aby dodać „Secondary Channel“.
	Reset	W polu wyboru należy wybrać „Reset“, aby zresetować „Secondary Channel“.
	Port	W tym polu konfiguruje się „Secondary Channel“. W polu wyboru należy wybrać „Port“, aby skonfigurować tylko jeden port.
	Trunk	W tym polu konfiguruje się „Secondary Channel“. W polu wyboru należy wybrać Trunk“, aby skonfigurować tylko jedną „Trunk Group“.
		W polu edycji należy wpisać numer „Secondary Channel“.
Dual Homing Status		
Parametr	**Domyślnie**	**Opis**
Group ID	1 … 4	W tym polu wyświetlany jest „Group ID“ dla „Dual Homing“.
Group State	Disable Enable	W tym polu wyświetlany jest status „Dual Homing“.
Primary Channel	None Port 1 … 10 (12)	W tym polu wyświetlany jest wybrany „Primary Channel“.
Sekundary Channel	None Port 1 … 10 (12)	W tym polu wyświetlany jest wybrany „Secondary Channel“.

9.3.8 Dual Ring

Wskazówka

Dodatkowa informacja
Więcej informacji o „Dual Ring“ można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 79: Strona WBM „Dual Ring“

Tabela 81: Strona WBM „Dual Ring“

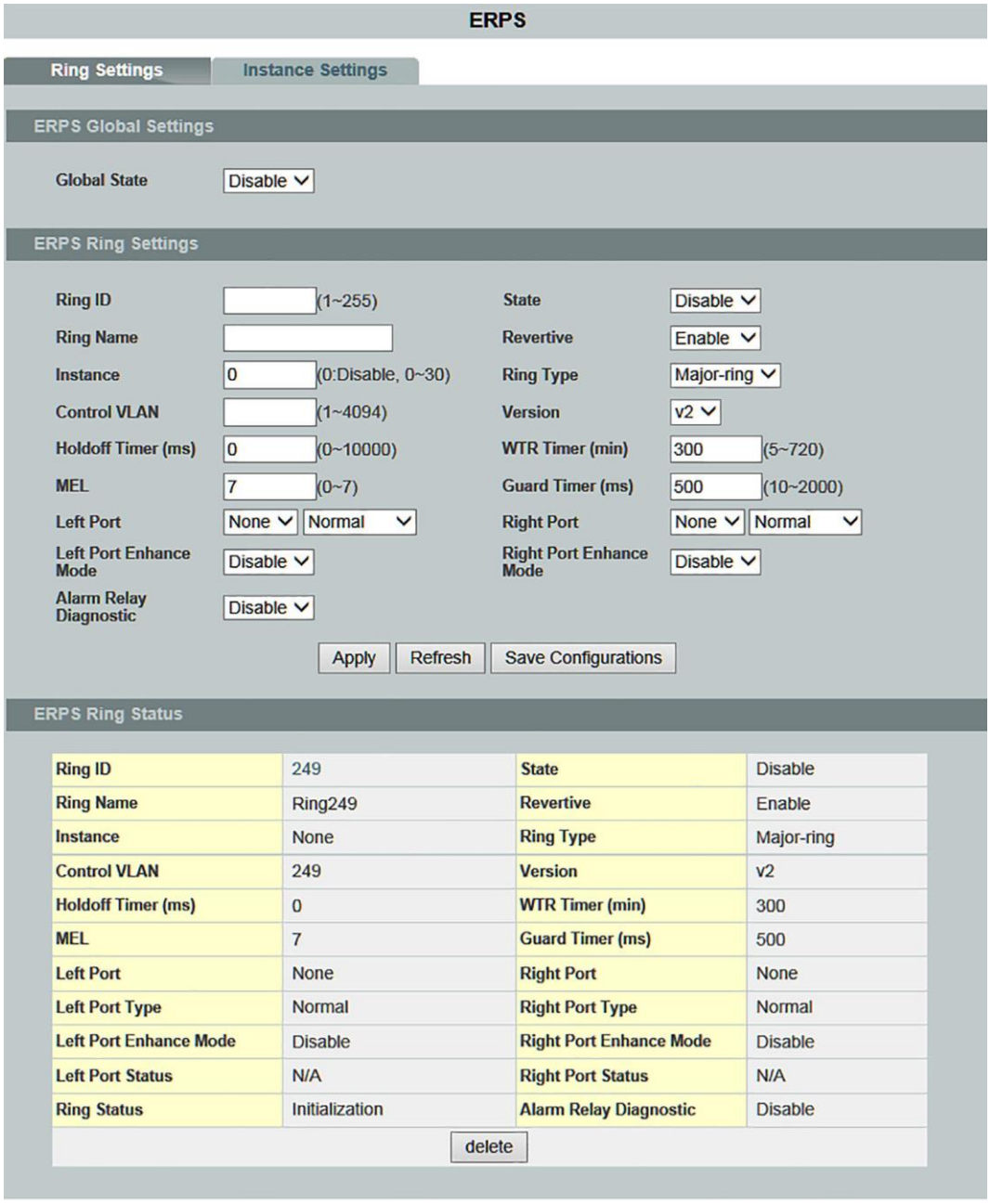
Dual Ring Settings		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Dual Ring“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Dual Ring“.
Xpress Ring Role	**Forwarder**	W polu wyboru należy wybrać „Forwarder“, gdy switch ma pracować w „Xpress Ring“ jako „Forwarder“.
	Arbiter	W polu wyboru należy wybrać „Arbiter“, gdy switch ma pracować w „Xpress Ring“ jako „Arbiter“.
Xpress Ring PORT 1	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać „Port 1“ w „Xpress Ring“.
Xpress Ring PORT 2	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać „Port 2“ w „Xpress Ring“.
Xpress Ring Destination MAC (Last Byte)	**f0**	W polu edycji należy wpisać ID „Xpress Ring“.
Subring PORT 1	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać „Port 1“ w „Jet Ring“.
Subring PORT-2	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać „Port 2“ w „Jet Ring“.
Dual Ring Status		
Parametr	**Domyślnie**	**Opis**
Status Xpress-Ring PORT-1	Forwarding Blocking	W tym polu wyświetlana jest informacja, jaki status ma port 1 „Xpress Ring“.
Status Xpress-Ring PORT-2	Forwarding Blocking	W tym polu wyświetlana jest informacja, jaki status ma port 2 „Xpress Ring“.
Subring PORT-1 State	Forwarding Blocking	W tym polu wyświetlana jest informacja, jaki status ma port 1 Jet Ring“.
Subring PORT-2 State	Forwarding Blocking	W tym polu wyświetlana jest informacja, jaki status ma port 2 Jet Ring“.
Subring Bridge Role	Forwarder master	W tym polu wyświetlana jest „informacja, jaką rolę odgrywa switch w Xpress Ring“.
Subring-master-Bridge-MAC		W tym polu wyświetlany jest MAC ID dla „Jet Ring“.

9.3.9 ERPS

Wskazówka

Dodatkowa informacja
Więcej informacji o „ERPS“ (**E**THERNET **R**ing **P**rotection **S**witching) można znaleźć w rozdziale „Opis funkcji“.

9.3.9.1 Ring Settings



Ilustracja 80: Strona WBM „ERPS“ – zakładka „Ring Settings“

Tabela 82: Strona WBM „ERPS“ – zakładka „Ring Settings“

ERPS Global Settings		
Parametr	**Domyślnie**	**Opis**
Global State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „ERPS“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „ERPS“.
ERPS Ring Settings		
Parametr	**Domyślnie**	**Opis**
Ring ID (1~255)		W polu edycji należy wpisać „Ring ID“. Właściwy zakres: 1 … 255
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować stan pierścienia.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować stan pierścienia.
Ring Name		W polu edycji należy wpisać nazwę pierścienia (maks. 32 znaki). (np. Major Ring ID255)
Revertive	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować tryb „Revertive“.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować tryb „Revertive“.
Instance (0:Disable, 0~30)		W polu edycji należy wpisać instancję dla pierścienia. Prawidłowy zakres: 0 … 30 0 („Disable“) oznacza, że wykorzystywana jest wersja 1 ERPS. „Control VLAN“ instancji powinna być taka sama jak „Control VLAN“ pod nią.
Ring Type	**Major Ring**	W polu wyboru należy wybrać „Major Ring“, gdy switch ma pracować w „Major Ring“.
	Subring	W polu wyboru należy wybrać „Subring“, gdy switch ma pracować w „Subring“.
Control VLAN (1~4094)	1 … 4094	W polu edycji należy wpisać VLAN ID, który ma służyć jako domena dla pakietów sterowania ERPS. Właściwy zakres: 1 … 4094
Version	**v2**	W polu wyboru należy wybrać „v2“, gdy ma być wykorzystana wersja 2 funkcji „ERPS“.
	v1	W polu wyboru należy wybrać „v1“, gdy ma być wykorzystana wersja 1 funkcji „ERPS“.
Holdoff Timer (ms) (0~10000)	**0**	W polu edycji należy wpisać wartość „Holdoff Timer“ dla pierścienia. Zakres czasowy: 0 … 10000 ms
WTR Timer (min) (5~720)	**300**	W polu edycji należy wpisać wartość „WTR Timer“ dla pierścienia. Zakres czasowy: 5 … 720 min
MEL (0~7)	**7**	W polu edycji należy wpisać wartość „Control MEL“ (**M**aintenance **E**ntity Group **L**evel) dla pierścienia. MEL określa priorytet. 0 = najniższy priorytet 7 = najwyższy priorytet

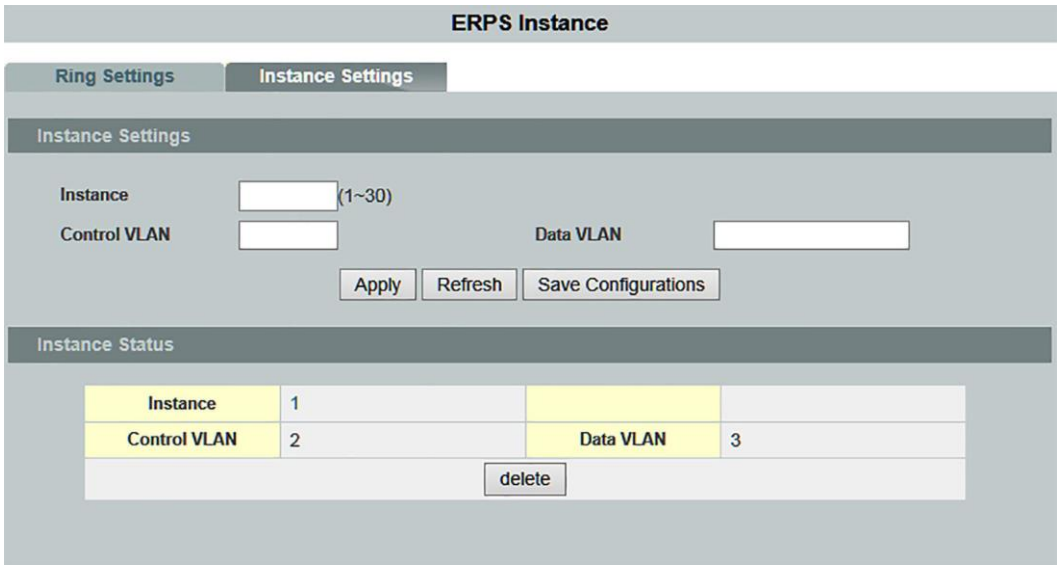
Tabela 82: Strona WBM „ERPS“ – zakładka „Ring Settings“

Guard Timer (ms) (10~2000)	**500**	W polu edycji należy wpisać wartość „Guard Timer“ dla pierścienia. Zakres czasowy: 10 … 2000 ms
Left Port		W tym polu wyboru konfigurowany jest lewy port i jego typ dla pierścienia.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać odpowiedni port.
	Normal	W polu wyboru należy wybrać „Normal“, gdy dla portu nie została przydzielona specjalna funkcja w pierścieniu ERPS.
	Neightbor	W polu wyboru należy wybrać „Neightbor“, gdy sąsiedni port pełni funkcję „Neightbor“.
	Owner	W polu wyboru należy wybrać „Owner“, gdy port ma przejąć funkcję „Owner“ w pierścieniu ERPS.
Right Port		W tym polu wyboru konfigurowany jest prawy port i jego typ dla pierścienia.
	None	W polu wyboru należy wybrać „None“, jeśli nie ma być wybrany żaden port.
	1 … 10 (12)	W polu wyboru należy wybrać odpowiedni port.
	Normal	W polu wyboru należy wybrać „Normal“, gdy dla portu nie została przydzielona specjalna funkcja w pierścieniu ERPS.
	Neightbor	W polu wyboru należy wybrać „Neightbor“, gdy sąsiedni port pełni funkcję „Neightbor“.
	Owner	W polu wyboru należy wybrać „Owner“, gdy port ma przejąć funkcję „Owner“ w pierścieniu ERPS.
Left Port Enhance Mode	**Disable**	W polu wyboru należy wybrać „Disable“, gdy na tym porcie podłączone jest urządzenie wspierające ERPS.
	Enable	W polu wyboru należy wybrać „Enable“, gdy na tym porcie podłączone jest urządzenie niewspierające ERPS. Należy przy tym uwzględnić „Aging Time” podłączonego urządzenia.
Right Port Enhance Mode	**Disable**	W polu wyboru należy wybrać „Disable“, gdy na tym porcie podłączone jest urządzenie wspierające ERPS.
	Enable	W polu wyboru należy wybrać „Enable“, gdy na tym porcie podłączone jest urządzenie niewspierające ERPS. Należy przy tym uwzględnić „Aging Time” podłączonego urządzenia.
Alarm Relay	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Alarm Relay“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Alarm Relay“.

Tabela 82: Strona WBM „ERPS“ – zakładka „Ring Settings“

ERPS Ring Status		
Parametr	**Domyślnie**	**Opis**
Ring ID	1 … 255	W tym polu wyświetlany jest „Ring ID“.
State	Disable Enable	W tym polu wyświetlany jest status pierścienia.
Ring Name		W tym polu wyświetlana jest nazwa pierścienia.
Revertive	Enable Disable	W tym polu wyświetlany jest status trybu „Revertive“.
Instance		W tym polu wyświetlana jest instancja dla pierścienia.
Ring Type	Major Ring Subring	W tym polu wyświetlany jest typ pierścienia.
Control VLAN	1 … 4084	W tym polu wyświetlana jest „Control VLAN“.
Version	v2 v1	W tym polu wyświetlana jest wersja funkcji „ERPS“.
Holdoff Timer (ms)	0 … 10000	W tym polu wyświetlany jest czas dla „Holdoff Timer“.
WTR Timer (min)	5 … 12	W tym polu wyświetlany jest czas dla „WTR Timer“.
MEL	0 … 7	W tym polu wyświetlana jest wartość dla „Control MEL.
Guard Timer (ms)	10 …2000	W tym polu wyświetlany jest czas dla „Guard Timer“.
Left Port	None 1 … 10 (12)	W tym polu wyświetlany jest numer lewego portu.
Right Port	None 1 … 10 (12)	W tym polu wyświetlany jest numer prawego portu.
Left Port Type	Normal Neighbor Owner	W tym polu wyświetlany jest typ lewego portu.
Right Port Type	Normal Neighbor Owner	W tym polu wyświetlany jest typ prawego portu.
Left Port Enhance Mode	Enable Disable	W tym polu wyświetlany jest status lewego portu.
Right Port Enhance Mode	Enable Disable	W tym polu wyświetlany jest status prawego portu.
Left Port Status	Forwarding Blocking	W tym polu wyświetlany jest aktualny status lewego portu.
Right Port Status	Forwarding Blocking	W tym polu wyświetlany jest aktualny status prawego portu.
Ring Status	Protection Idle	W tym polu wyświetlany jest status pierścienia.
Alarm Relay	Enable Disable	W tym polu wyświetlany jest status „Alarm Relay“.
Delete		Aby usunąć te ustawienia, należy kliknąć **[Delete]**.

9.3.9.2 Instance Settings



Ilustracja 81: Strona WBM „ERPS“ – zakładka „Instance Settings“

Tabela 83: Strona WBM „ERPS“ – zakładka „Instance Settings“

Instance Settings		
Parametr	**Domyślnie**	**Opis**
Instance (1~30)		W polu edycji należy wpisać „Instance ID“. Właściwy zakres: 1 … 30
Control VLAN		W polu edycji należy wpisać „Control VLAN“ dla instancji. Właściwy zakres: 1 … 4094
Data VLAN		W polu edycji należy wpisać „Data VLAN“ dla instancji. Właściwy zakres: 1 … 4094 Można skonfigurować jedną lub więcej „Data VLAN“.
Instance Status		
Parametr	**Domyślnie**	**Opis**
Instance	1 … 31	W tym polu wyświetlany jest „Instance ID“.
Control VLAN	1 … 4094	W tym polu wyświetlana jest „Control VLAN“ instancji.
Data VLAN	1 … 4094	W tym polu wyświetlana jest „Data VLAN“ instancji.
Delete		Aby usunąć te ustawienia, należy kliknąć **[Delete]**.

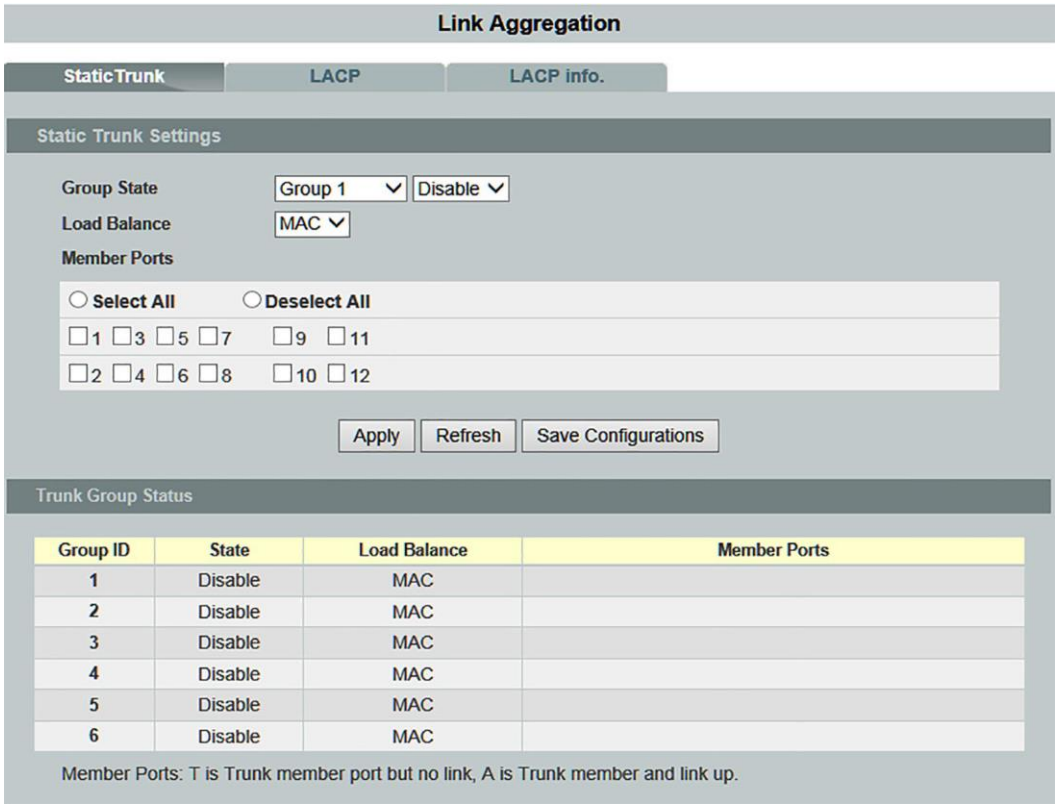
9.3.10 Link Aggregation

Wskazówka

Dodatkowa informacja

Więcej informacji o „Link Aggregation” można znaleźć w rozdziale „Opis funkcji”.

9.3.10.1 Static Trunk



Ilustracja 82: Strona WBM „Link Aggregation“ – zakładka „Static Trunk“

Tabela 84: Strona WBM „Link Aggregation“ – zakładka „Static Trunk“

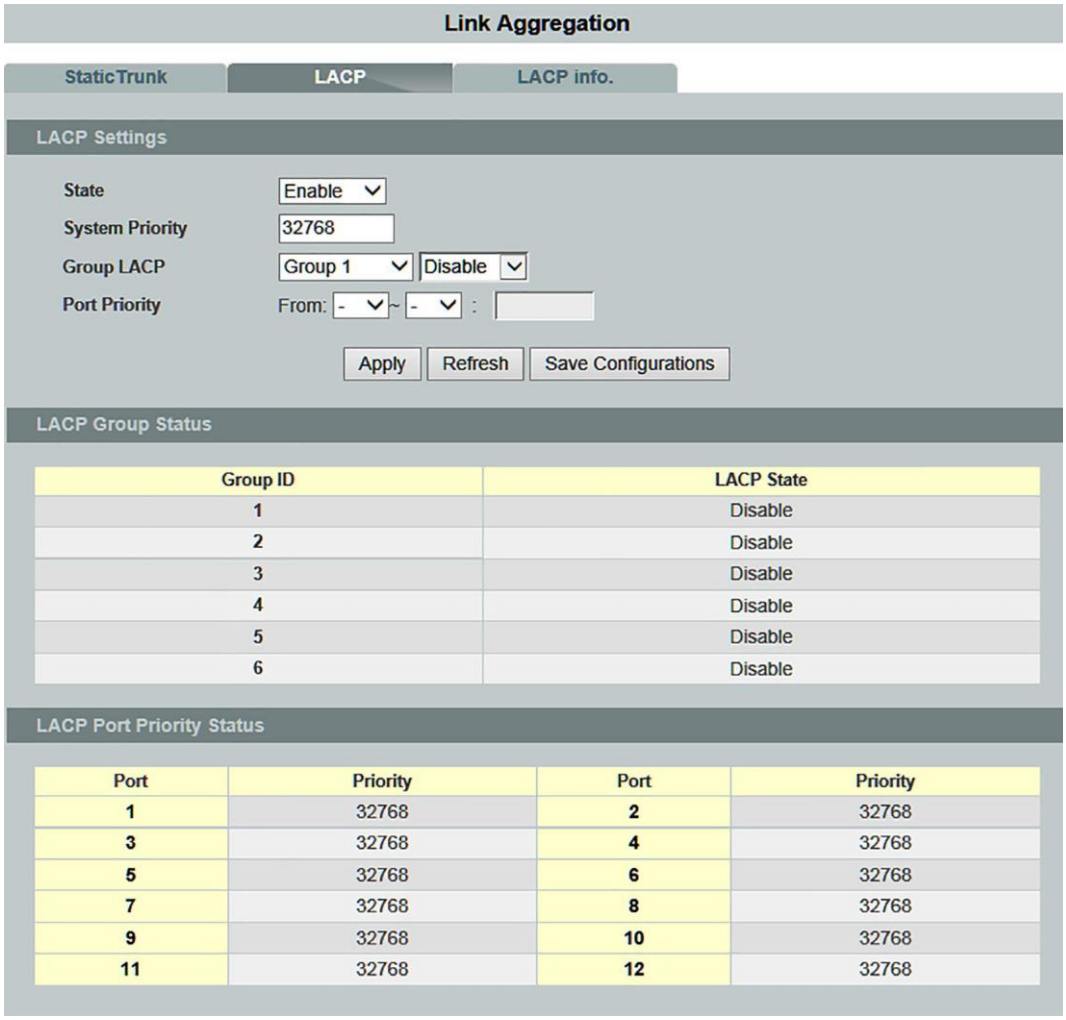
Static Trunk Settings				
Parametr		**Domyślnie**	**Opis**	
Group State		**Group 1** … Group 6	W polu wyboru należy wybrać oznaczenie dla „Trunk Group“ (logiczny link, zawierający kilka portów).	
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować statyczną „Trunk Group“.	
		Enable	W polu wyboru należy wybrać „Enable“, aby zastosować statyczną „Trunk Group“.	
Load Balance		**MAC**	W polu wyboru należy wybrać „MAC“, aby skonfigurować algorytm wyrównywania obciążeń dla specyficznej Trunk Group“.	
		IP	W polu wyboru należy wybrać „IP“, aby skonfigurować algorytm wyrównywania obciążeń dla specyficznej Trunk Group“.	
Member Ports	Select All	○	○	Nie wybrano portu, który ma być dołączony do statycznej „Trunk Group“.
			◉	Wybrano wszystkie porty, które mają być dołączone do statycznej „Trunk Group“.
	Disable All	○	○	Żaden port nie jest dezaktywowany.
			◉	Wszystkie porty są dezaktywowane.
	☐ 1 … ☐ 10 (12)	☐	☐	Port nie jest aktywowany.
			☑	Port jest aktywowany.
Trunk Group Status				
Parametr		**Domyślnie**	**Opis**	
Group ID		1 … 6	W tej kolumnie wyświetlany jest „Group ID“ dla „Trunk Group“ (logiczny link, zawierający kilka portów).	
State		Disable Enable	W tej kolumnie wyświetlana jest informacja, czy „Trunk Group“ jest aktywowana, czy dezaktywowana.	
Load Balance		1 … 6	W tej kolumnie wyświetlane są dyrektywy dla wyrównywania obciążeń „Trunk Group“.	
Member Ports			W tej kolumnie wyświetlane są porty, przyporządkowane do statycznej „Trunk Group“.	

9.3.10.2 LACP

Wskazówka

Dodatkowa informacja

Więcej informacji o „LACP“ (**L**ink **A**ggregation **C**ontrol **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.

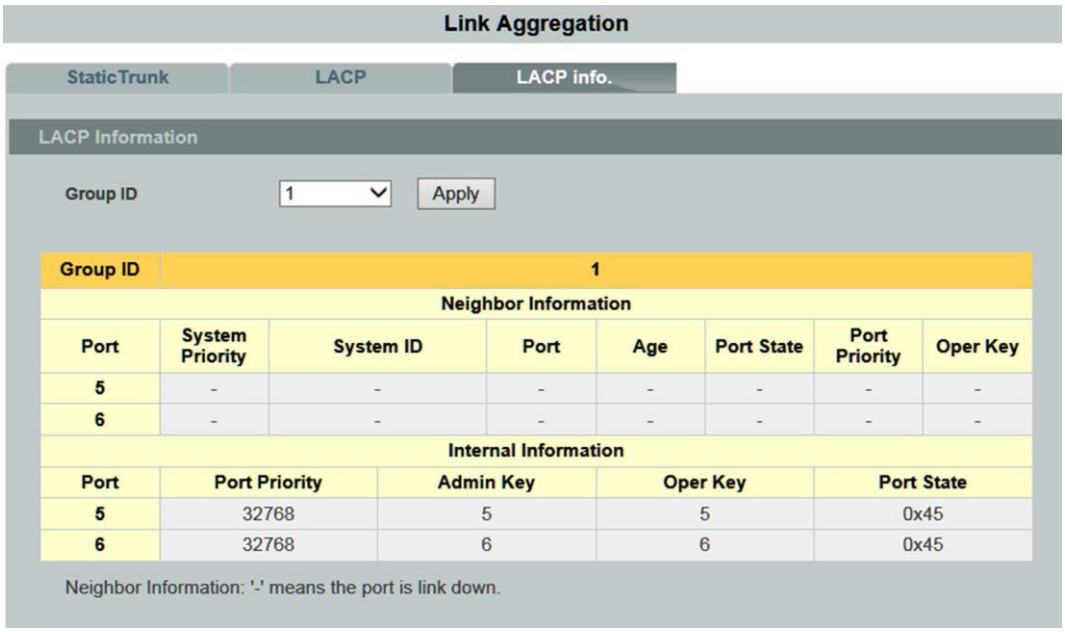


Ilustracja 83: Strona WBM „Link Aggregation“ – zakładka „LACP“

Tabela 85: Strona WBM „Link Aggregation“ – zakładka „LACP“

LACP Settings			
Parametr		**Domyślnie**	**Opis**
State		**Disable**	W polu wyboru należy wybrać „Disable“, jeśli nie ma być zastosowany „Link Aggregation Control Protocol“ (LACP).
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Link Aggregation Control Protocol” (LACP).
System Priority		1 … 65535	W polu wyboru należy wybrać „LACP System Priority“. Należy wpisać cyfrę, określającą priorytet aktywnego portu z „Link Aggregation Control Protocol“ (LACP). Im niższa liczba, tym wyższy poziom priorytetu.
Group LACP		**Group 1** … Group 6	W polu wyboru należy wybrać „Trunk Group ID“.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować LACP dla „Trunk Group ID“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować LACP dla „Trunk Group“.
Port Priority	From:	-	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowany priorytet LACP.
	To:	-	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowany priorytet LACP.
		32768	Domyślna wartość priorytetu wynosi 32768.
LACP Group Status			
Parametr		**Domyślnie**	**Opis**
Group ID		1 … 6	W tej kolumnie wyświetlany jest „LACP Group ID“.
LACP State		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy LACP jest dla grupy aktywowany, czy dezaktywowany.
LACP Port Prioriy Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlany jest „Port ID“.
Priority		1 … 65535	W tej kolumnie wyświetlany jest priorytet LACP portu.

9.3.10.3 LACP info.



Ilustracja 84: Strona WBM „Link Aggregation“ – zakładka „LACP info.“

Tabela 86: Strona WBM „Link Aggregation“ – zakładka „LACP Info.“

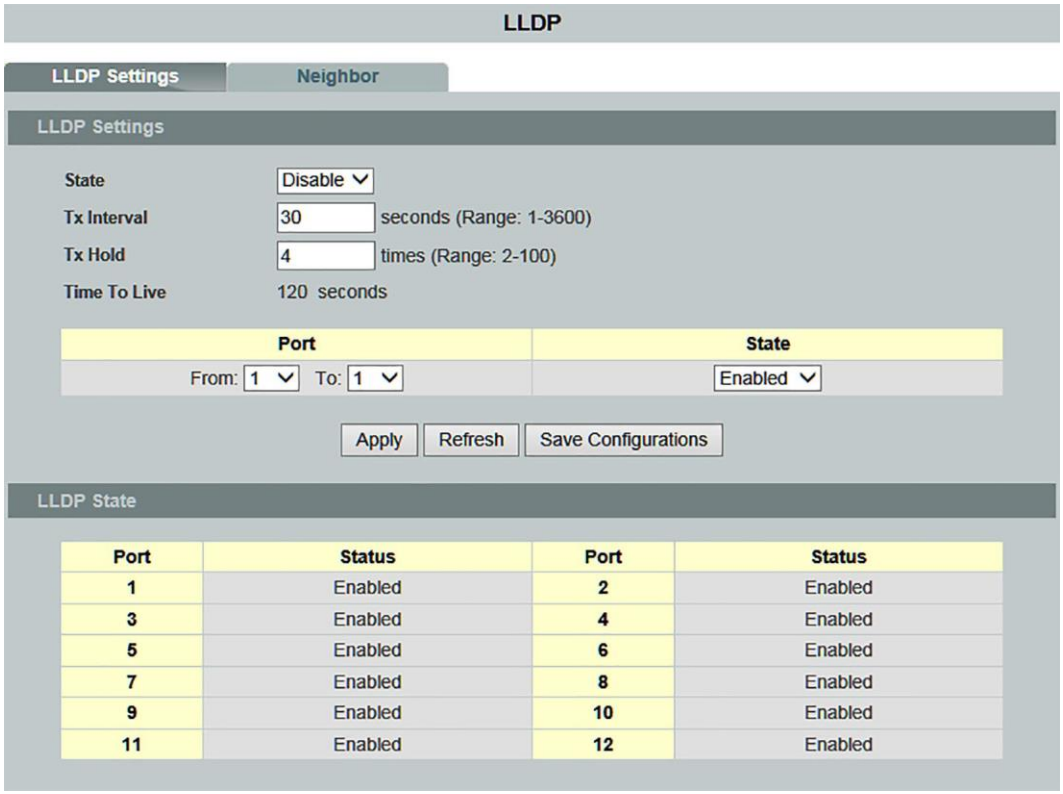
LACP Information		
Parametr	**Domyślnie**	**Opis**
Group ID	-	W polu wyboru należy wybrać „LACP Group“, która ma być wyświetlona.
Neighbor Information		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10 (12)	W tej kolumnie wyświetlany jest LACP ID portu uczestnika.
System Priority	0 … 65535	W tej kolumnie wyświetlany jest priorytet systemu LACP.
System ID		W tej kolumnie wyświetlany jest System ID sąsiedniego switcha.
Port	1 … 10 (12)	W tej kolumnie wyświetlany jest ID podłączonego bezpośrednio portu sąsiedniego switcha.
Age		W tej kolumnie wyświetlany jest dostępny czas dla informacji LACP sąsiedniego switcha.
Port State		W tej kolumnie wyświetlany jest stan podłączonego bezpośrednio portu sąsiedniego switcha.
Port Priority		W tej kolumnie wyświetlany jest priorytet podłączonego bezpośrednio portu sąsiedniego switcha.
Oper Key		W tej kolumnie wyświetlany jest „Oper-Key“ sąsiedniego switcha.
Internal Information		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlany jest LACP ID portu uczestnika.
Port Priority		W tej kolumnie wyświetlany jest priorytet portu uczestnika LACP.
Admin Key		W tej kolumnie wyświetlany jest „Admin Key“ portu uczestnika LACP.
Oper Key		W tej kolumnie wyświetlany jest „Oper Key“ portu uczestnika LACP.
Port State		W tej kolumnie wyświetlany jest stan portu uczestnika LACP.

9.3.11 LLDP

Wskazówka

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

9.3.11.1 LLDP Settings

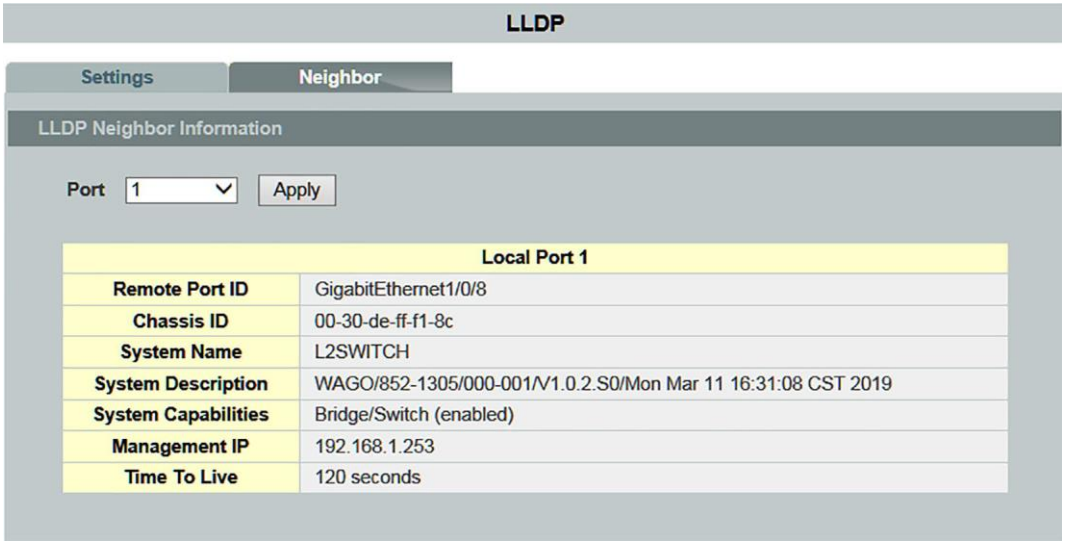


Ilustracja 85: Strona WBM „LLDP“ – zakładka „LLDP Settings“

Tabela 87: 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** seconds (Range: 1~3600)	W polu edycji należy wpisać wartość „Tx Interval“ dla pakietów „LLDP“.
Tx Hold		**4** times (Range: 2~100)	W polu edycji należy wpisać wartość „Tx Hold- Time“, która określa TTL wiadomości switcha. (TTL = tx-hold * tx-interval)
Time To Live		**120** second	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.

9.3.11.2 Neighboring Detection



Ilustracja 86: Strona WBM „LLDP“ – zakładka „Neighboring Detection“

Tabela 88: Strona WBM „LLDP“ – zakładka „Neighboring Detection“

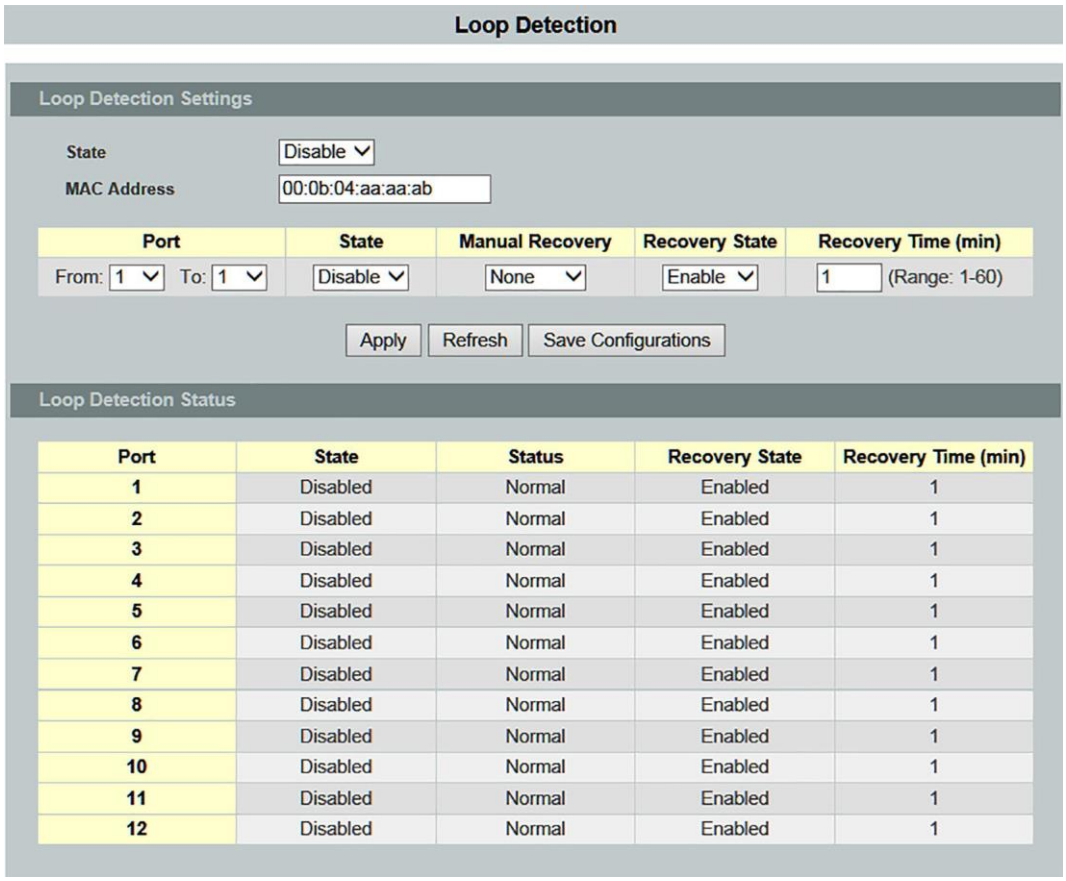
LLDP Neighbor Information		
Parametr	**Domyślnie**	**Opis**
Port	**All**	W polu wyboru należy wybrać „All“, gdy mają być wyświetlane informacje od wszystkich sąsiednich portów.
	1 … 10 (12)	W polu wyboru należy wybrać port, którego sąsiadującego portu mają być wyświetlane informacje.
Local Port	1 … 10 (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.

9.3.12 Loop Detection

Wskazówka

Dodatkowa informacja

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



Port	State	Status	Recovery State	Recovery Time (min)
1	Disabled	Normal	Enabled	1
2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1
4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1
6	Disabled	Normal	Enabled	1
7	Disabled	Normal	Enabled	1
8	Disabled	Normal	Enabled	1
9	Disabled	Normal	Enabled	1
10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1
12	Disabled	Normal	Enabled	1

Ilustracja 87: Strona WBM „Loop Detection“

Tabela 89: Strona WBM „Loop Detection“

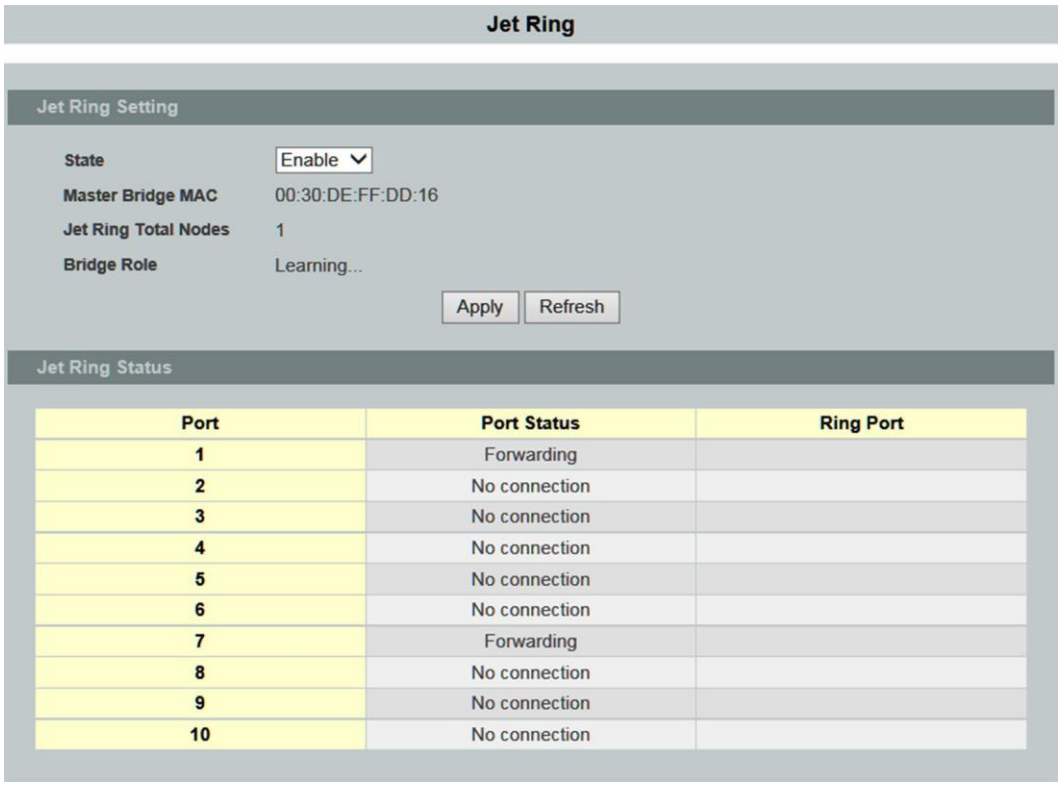
Loop Detection Settings			
Parametr		**Domyślnie**	**Opis**
Status		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
MAC Address			W polu edycji należy wybrać docelowy adres MAC, na który mają być wysyłane pakiety sondujące. Gdy port otrzyma te same pakiety danych, 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“.
State		**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“.
Manual Recovery		**None**	W polu wyboru należy wybrać „None“, aby wyłączyć dla portu funkcję „Loop Detection“.
		Unblock	W polu wyboru należy wybrać „Activate“, jeśli nie mają być zmienione funkcje „Status“ i „Loop Correction“.
Recovery State		**Enable**	W polu wyboru należy wybrać „Enable“, aby port aktywował się automatycznie po upływie wyznaczonego czasu „Recovery Time“.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.
Recovery Time (min) (Range: 1~60)		**1**	W polu edycji należy wpisać wartość „Recovery Time“ (w minutach), jaki switch musi odczekać, zanim reaktywuje port. Zakres czasowy: 1 … 60 min
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.
Recovery State		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 „Recovery Time“ dla funkcji „Recovery Status“.

9.3.13 Jet Ring

Wskazówka

Dodatkowa informacja

Więcej informacji o „Jet Ring” można znaleźć w rozdziale „Opis funkcji”.

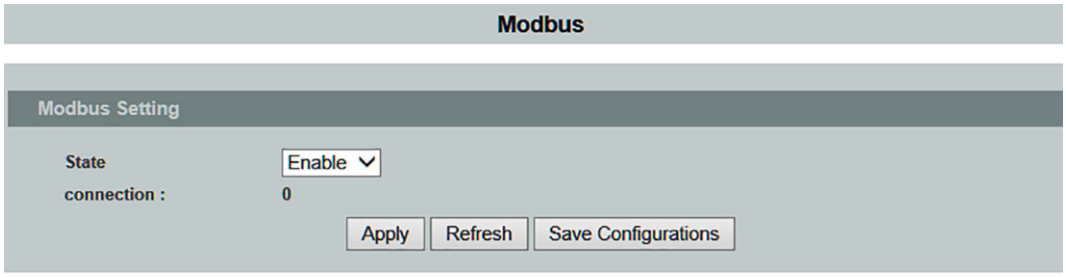


Ilustracja 88: Strona WBM „Jet Ring“

Tabela 90: Strona WBM „Jet Ring“

Jet Ring Setting		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Jet Ring” na poszczególnych portach.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Jet Ring” na poszczególnych portach.
Alarm Relay	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Alarm Relay“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Alarm Relay“.
Jet Ring Status		
Parametr	**Domyślnie**	**Opis**
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Port Status	No Connection Forwarding Blocking	W tej kolumnie wyświetlany jest status portu.
Ring Port	Yes	W tej kolumnie wyświetlana jest informacja, czy port pracuje w pierścieniu.

9.3.14 Modbus



Ilustracja 89: Strona WBM „Modbus“

Tabela 91: Strona WBM „Modbus“

Modbus Setting		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Modbus” na poszczególnych portach.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Modbus” na poszczególnych portach.
Connection		W tym polu wyświetlane jest połączenie.

Wskazówka

Modbus Tables

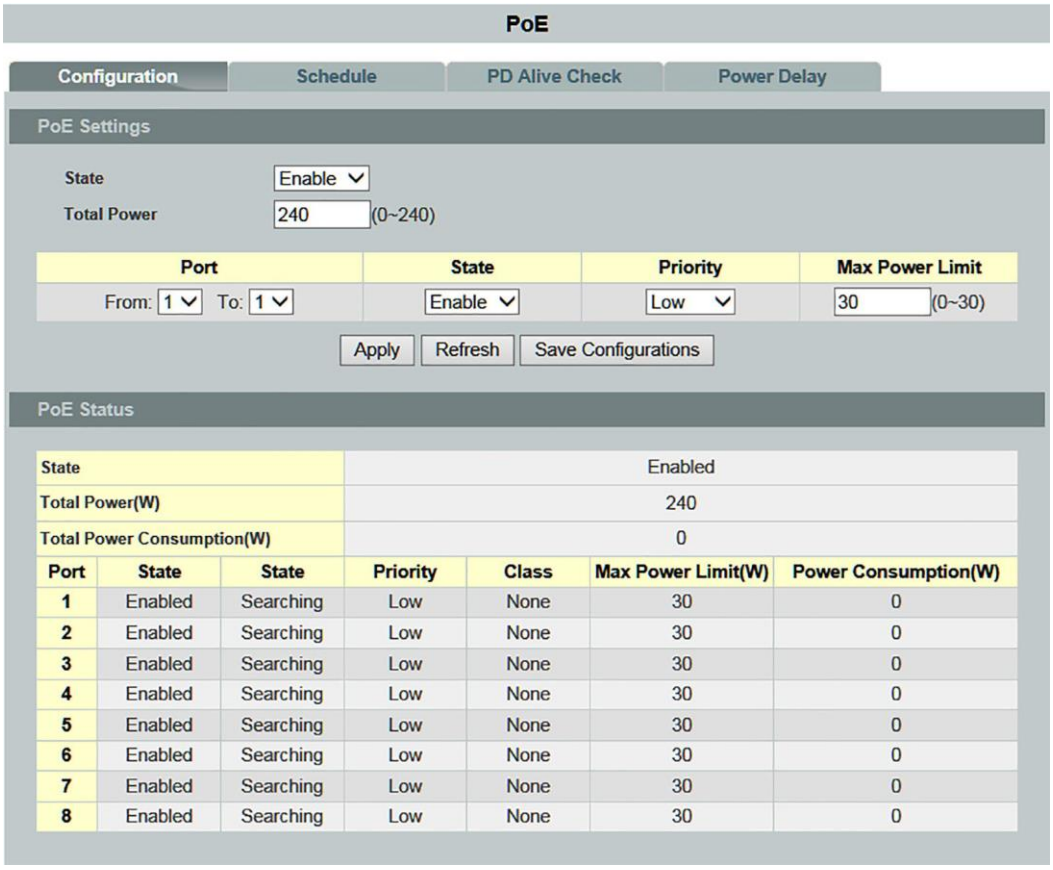
Tabelę „Rejestry Modbus” można znaleźć w rozdziale „Załącznik” > … > „Rejestry Modbus”.

9.3.15 PoE

Wskazówka

Dodatkowa informacja
Więcej informacji o „**P**ower **o**ver **E**thernet” (PoE) można znaleźć w rozdziale „Opis funkcji”.

9.3.15.1 Configuration

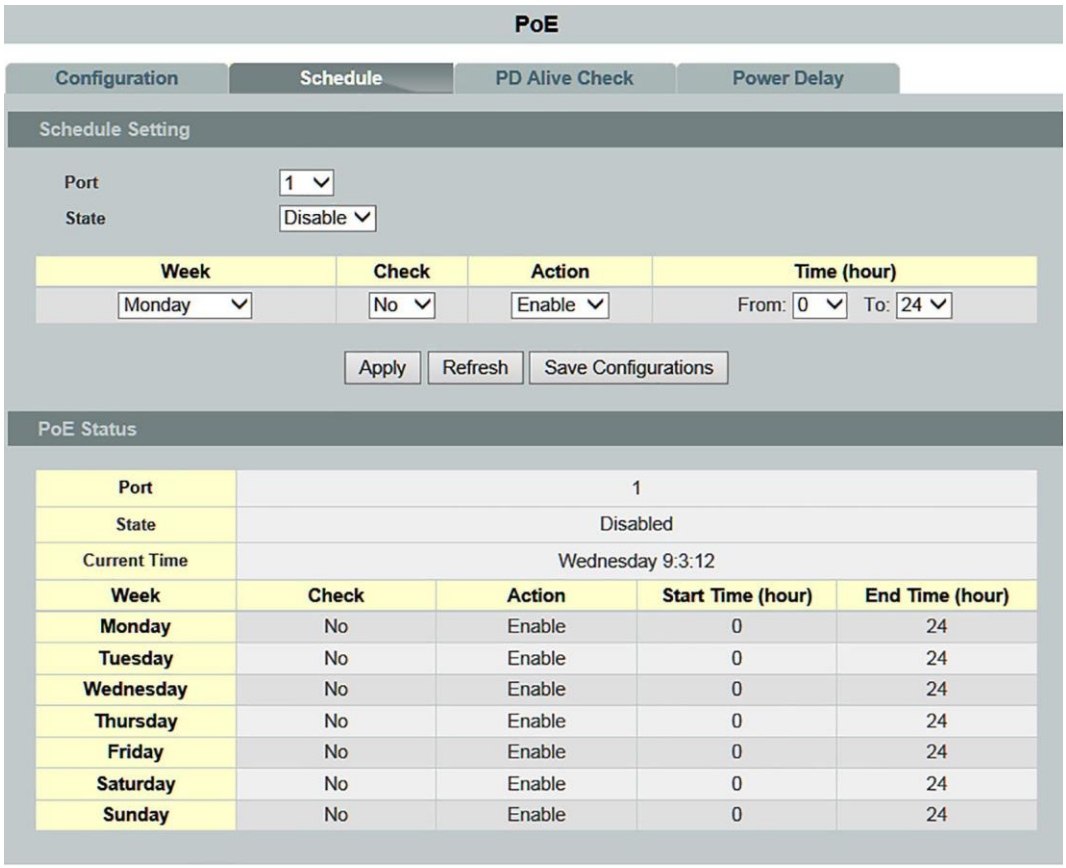


Ilustracja 90: Strona WBM „PoE“ – zakładka „Configuration“

Tabela 92: Strona WBM „PoE“ – zakładka „Configuration“

PoE Settings			
Parametr		**Domyślnie**	**Opis**
State		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję.
Total Power (0-240)		**240**	W polu edycji należy wpisać całkowitą moc switcha.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „PoE.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie „PoE.
State		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować „PoE” na poszczególnych portach.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować „PoE” na poszczególnych portach.
Priority		Low High Critical	W polu wyboru należy wybrać priorytet PoE dla wybranego portu lub zakresu portów.
Max. Power Limit (0-30)		**30**	W polu edycji należy wpisać maksymalne ograniczenie mocy dla wybranego portu.
PoE Status			
Parametr		**Domyślnie**	**Opis**
State		Enable Disable	W tym polu wyświetlany jest stan funkcji „PoE”.
Total Power (W)		0 … 240	W tym polu wyświetlana jest całkowita moc obsługiwana przez switcha.
Total Power Consumption (W)		0 … 240	W tym polu wyświetlany jest całkowity pobór mocy wszystkich urządzeń PD („Powered Device”).
Port		1 … 8	W tym polu wyświetlany jest numer portu.
Status		Enable Disable	W tym polu wyświetlany jest stan „PoE” dla konkretnego portu.
Status			W tym polu wyświetlany jest stan funkcji „PoE”.
Priority		Low High Critical	W tym polu wyświetlany jest priorytet „PoE” dla konkretnego portu.
Class			W tym polu wyświetlany jest tryb klasy dla konkretnego portu, który urządzenie zasilające „PSE” („Power Sourcing Equipment”) uzgodniło z urządzeniem końcowym „PD” („Powered Device”).
Max. Power Limit (W)		0 … 30	W tym polu wyświetlany jest limit mocy dla konkretnego portu.
Power Consumption (W)		0 … 240	W tym polu wyświetlany jest pobór mocy dla konkretnego portu.

9.3.15.2 Schedule



Ilustracja 91: Strona WBM „PoE“ – zakładka „Schedule“

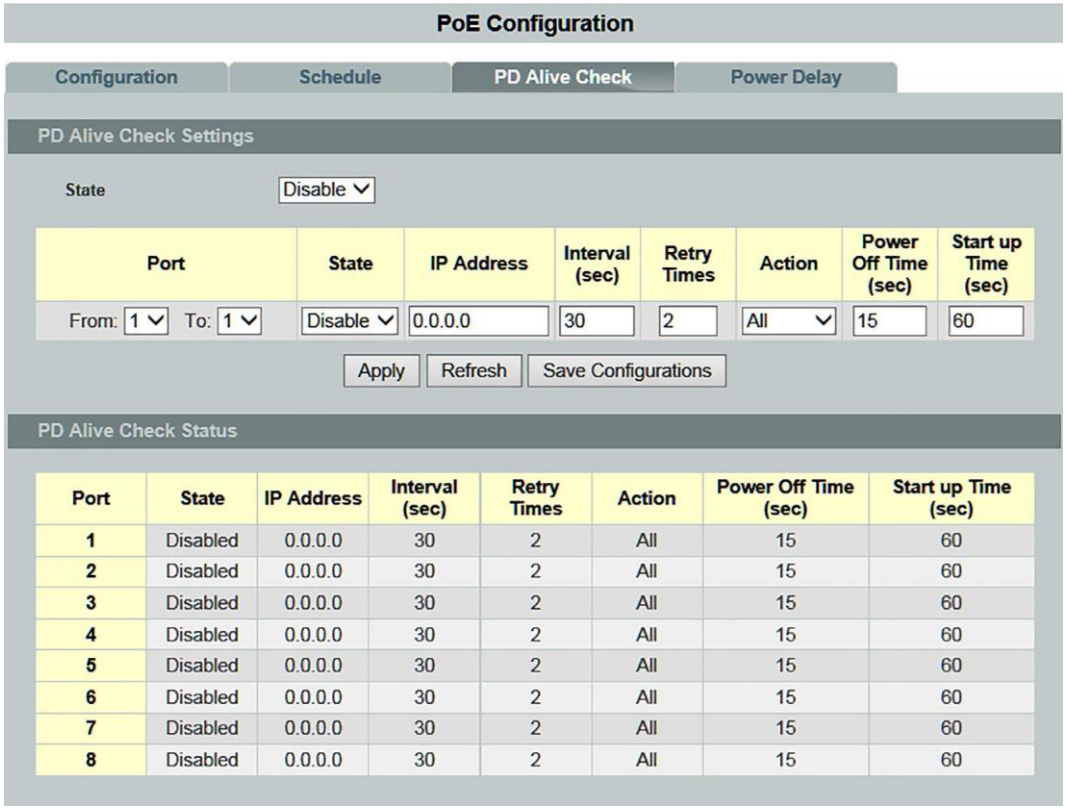
Tabela 93: Strona WBM „PoE“ – zakładka „Schedule“

Schedule Setting			
Parametr		**Domyślnie**	**Opis**
Port		**1** … 8	W polu wyboru należy wybrać port, dla którego ma zostać skonfigurowana funkcja harmonogramu „PoE“.
		All	W polu wyboru należy wybrać „All”, aby skonfigurować funkcję harmonogramu „PoE“ dla wszystkich portów.
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję harmonogramu „PoE“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję harmonogramu „PoE“.
Week		**Monday** Tuesday Wednesday Thursday Friday Saturday Sunday	W polu wyboru należy wybrać dzień tygodnia, dla którego ma zostać skonfigurowany harmonogram.
		All	W polu wyboru należy wybrać „All”, aby skonfigurować harmonogram dla wszystkich dni tygodnia.
Check		**Yes**	W polu wyboru należy wybrać „Yes“, aby sprawdzić harmonogram przez określony czas dla konkretnego portu.
		No	W polu wyboru należy wybrać „No“, aby nie sprawdzać harmonogramu przez określony czas dla konkretnego portu.
Action		**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować harmonogram „PoE“ przez określony czas dla konkretnego portu.
		Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować harmonogram „PoE“ przez określony czas dla konkretnego portu.
Time (hour)	From:	**0** … 24	W polu wyboru należy wybrać godzinę rozpoczęcia harmonogramu „PoE” dla danego dnia tygodnia i konkretnego portu.
	To:	0 … **24**	W polu wyboru należy wybrać godzinę zakończenia harmonogramu „PoE” dla danego dnia tygodnia i konkretnego portu.

Tabela 93: Strona WBM „PoE“ – zakładka „Schedule“

Status PoE		
Parametr	**Domyślnie**	**Opis**
Port	1 … 8 All	W tym polu wyświetlany jest numer portu.
State	Enable Disable	W tym polu wyświetlany jest stan funkcji harmonogramu „PoE“.
Current Time		W tym polu wyświetlany jest aktualny czas.
Week	Monday Tuesday Wednesday Thursday Friday Saturday Sunday	W tej kolumnie wyświetlany jest określony dzień tygodnia.
Check	Yes No	W tej kolumnie wyświetlany jest status sprawdzania harmonogramu „PoE“.
Action	Enable Disable	W tej kolumnie wyświetlany jest status harmonogramu „PoE” przez określony czas dla konkretnego portu.
Start Time (hour)	0 … 24	W tej kolumnie wyświetlany jest czas rozpoczęcia harmonogramu „PoE” w danym dniu tygodnia dla konkretnego portu.
End Time (hour)		W tej kolumnie wyświetlany jest czas zakończenia harmonogramu „PoE” w danym dniu tygodnia dla konkretnego portu.

9.3.15.3 PD Alive Check



Ilustracja 92: Strona WBM „PoE“ – zakładka „PD Alive Check“

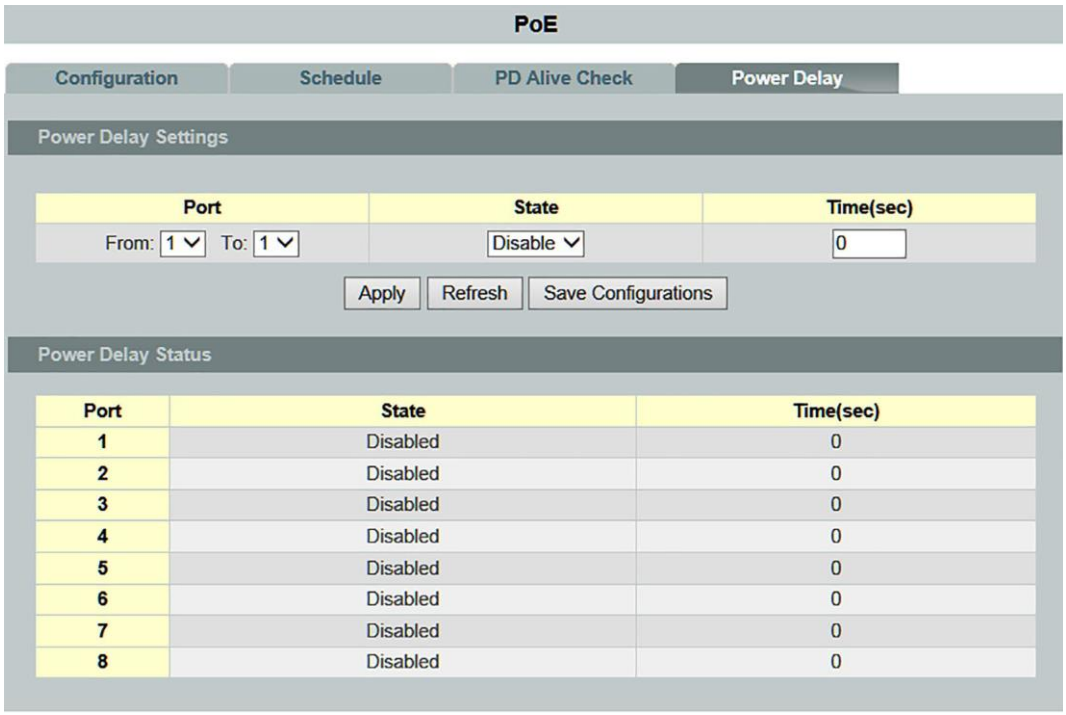
Tabela 94: Strona WBM „PoE“ – zakładka „PD Alive Check“

PD Alive Check Settings			
Parametr		**Domyślnie**	**Opis**
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „PD Alive Check“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „PD Alive Check“.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „PD Alive Check”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „PD Alive Check”.
State		**Disable**	W polu wyboru należy wybrać „Disble“, aby dezaktywować funkcję „PD Alive Check” na poszczególnych portach.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „PD Alive Check” na poszczególnych portach.
IP Address			W polu edycji należy wpisać „Host-IP Address“, który łączy się z portem.
Interval (sec)		**30**	W polu edycji należy wpisać interwał wysyłania pakietów sprawdzających stan urządzenia do hosta.
Retry Times		**2**	W polu edycji należy wpisać liczbę powtórzeń wysyłania pakietów sprawdzających aktywność. Zakłada się przy tym, że host nie odpowiada.
Action		**All**	W polu wyboru należy wybrać „All”, aby wysłać komunikat alarmu do administratora i następnie zrestartować urządzenie końcowe PD („Powered Device”).
		None	W polu wyboru należy wybrać „None“, jeśli urządzenie końcowe PD („Powered Device”) ciągle „pinguje”, nie wykonując żadnych dodatkowych działań.
		Reboot	W polu wyboru należy wybrać „Reboot”, aby odłączyć port PoE od zasilacza i zrestartować urządzenie końcowe PD („Powered Device”).
		Alarm	W polu wyboru należy wybrać „Alarm”, aby wysłać komunikat alarmu do administratora.
Power Off Time (sec)		**15**	W polu wyboru należy wprowadzić czas, po którym port PoE zostanie ponownie podłączony do zasilania po restarcie urządzenia końcowego PD („Powered Device”).
Startup Time (sec)		**15**	W polu edycji należy wprowadzić czas, przez jaki switch czeka po restarcie urządzenia końcowego PD („Powered Device”), zanim przeprowadzi automatyczną kontrolę PoE.

Tabela 94: Strona WBM „PoE“ – zakładka „PD Alive Check“

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

9.3.15.4 Power Delay



Ilustracja 93: Strona WBM „PoE“ – zakładka „Power Delay“

Tabela 95: Strona WBM „PoE“ – zakładka „Power Delay“

Power Delay Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Power Delay”.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być skonfigurowane ustawienie dla „Power Delay”.
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Power Delay” na poszczególnych portach.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Power Delay” na poszczególnych portach.
Time (sec)			W polu edycji należy wpisać czas opóźnienia dla poszczególnych portów.
Power Delay Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 8	W tej kolumnie wyświetlany jest numer portu.
State		Enable Disable	W tej kolumnie wyświetlany jest stan zwłoki przy załączaniu „PoE”.
Time (sec)			W tej kolumnie wyświetlany jest czas zwłoki przy załączaniu „PoE”.

Wskazówka



Wartość zwłoki przy załączaniu

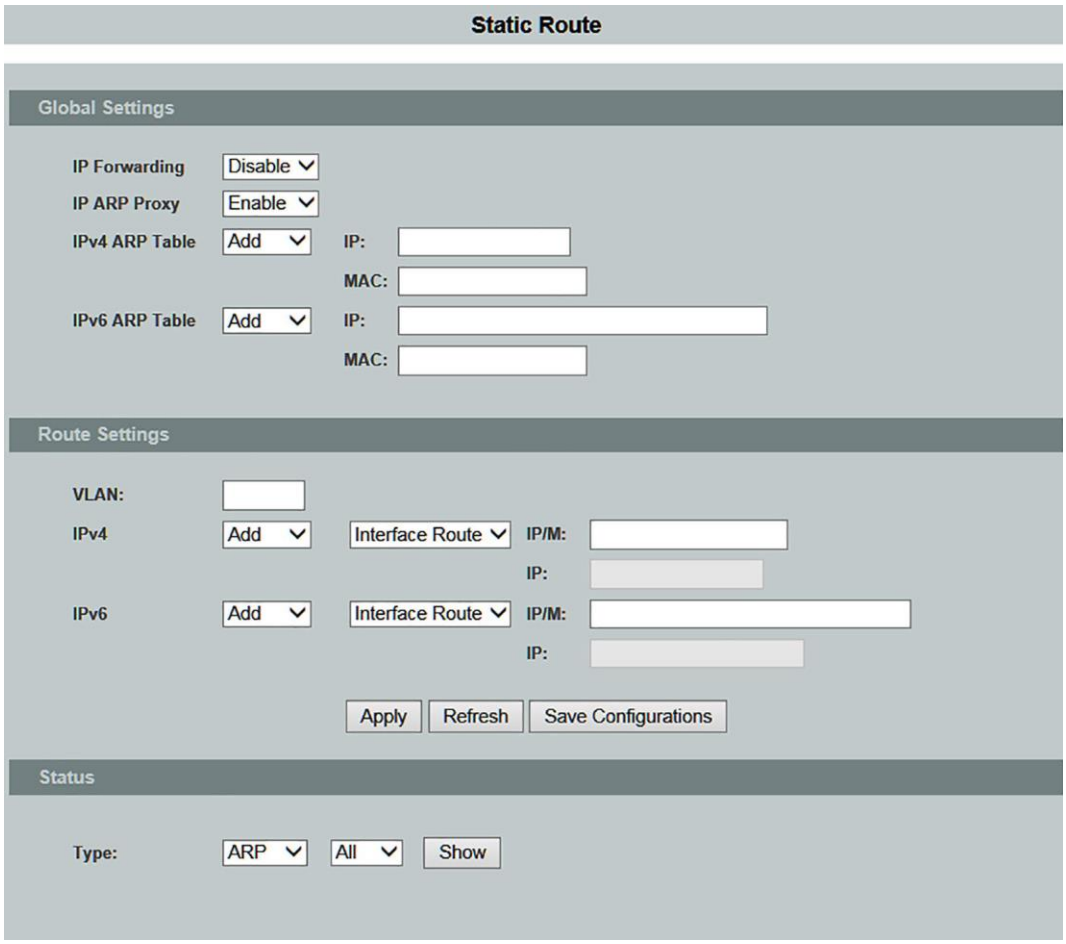
Port o wysokim priorytecie powinien mieć niską wartość zwłoki przy załączaniu.

9.3.16 Static Route

Wskazówka

Dodatkowa informacja

Więcej informacji o „Static Route” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 94: Strona WBM „Static Route“

Tabela 96: Strona WBM „Static Route“

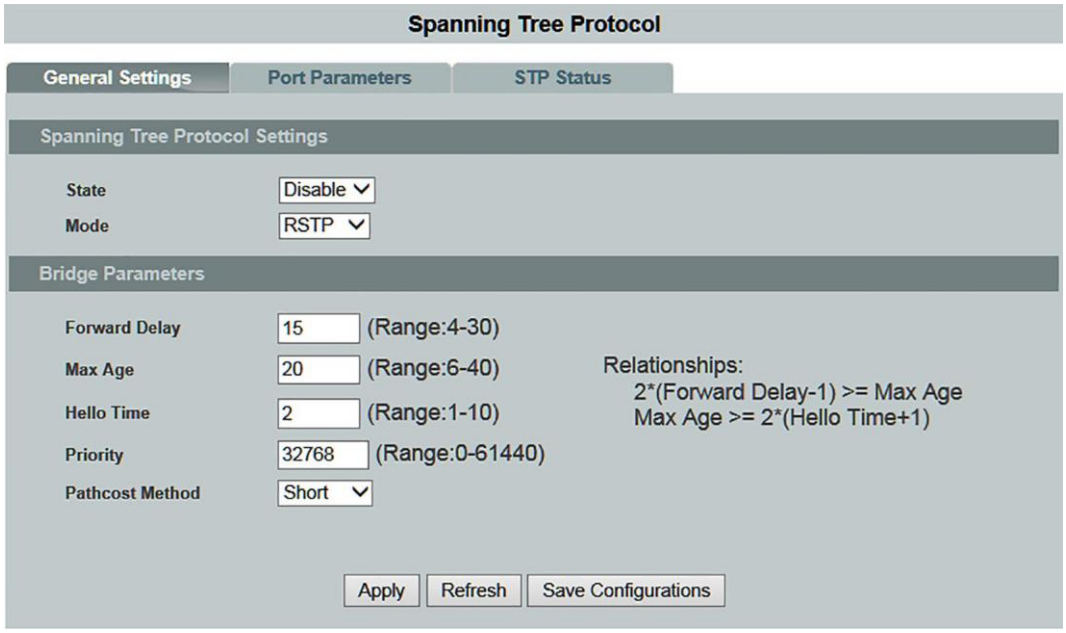
Global Settings			
Parametr	**Domyślnie**	**Opis**	
IP Forwarding	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować tę funkcję.	
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.	
IP ARP Proxy	**Enable**	W polu wyboru należy wybrać „Enable“, aby dezaktywować globalnie „Route“ jako „ARP Proxy“.	
	Disable	W polu wyboru należy wybrać „Disable“, aby aktywować globalnie „Route“ jako „ARP Proxy“.	
IPv4 ARP Table	**Add**	W polu wyboru należy wybrać „Add“, aby dodać do tabeli ARP statyczny wpis ARP IPv4.	
	Delete	W polu wyboru należy wybrać „Delete“, aby usunąć z tabeli ARP statyczny wpis ARP IPv4.	
IPv6 ARP Table	**Add**	W polu wyboru należy wybrać „Add“, aby dodać do tabeli ARP statyczny wpis ARP IPv6.	
	Delete	W polu wyboru należy wybrać „Delete“, aby usunąć z tabeli ARP statyczny wpis ARP IPv6.	
Route Settings			
Parametr	**Domyślnie**	**Opis**	
VLAN		W polu edycji należy wpisać specyficzny „Interface VLAN“.	
IPv4 IPv6	**Add**	W polu wyboru należy wybrać „Add“, aby dodać „Route“ do „Interface VLAN“. W sąsiednim polu wyboru należy wybrać typ (Interface Route / Static Route).	
	Delete	W polu wyboru należy wybrać „Delete“, aby usunąć „Route“. W sąsiednim polu wyboru należy wybrać typ (Interface Route / Static Route).	
IP/M		W polu edycji należy wpisać adres IP i maskę sieci.	
IP		W polu edycji należy wpisać statyczny adres „Route“ dla statycznego typu.	
Status			
Parametr	**Domyślnie**	**Opis**	
Type	**ARP**	**All**	Wyświetlane są konfiguracje tabeli ARP / tabeli hosta i „Route“.
		IPv4	
		IPv6	
	Host	**All**	
		IPv4	
		IPv6	
	Routing	**All**	
		IPv4	
		IPv6	

9.3.17 Spanning Tree Protocol (STP)

Wskazówka

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

9.3.17.1 General Settings

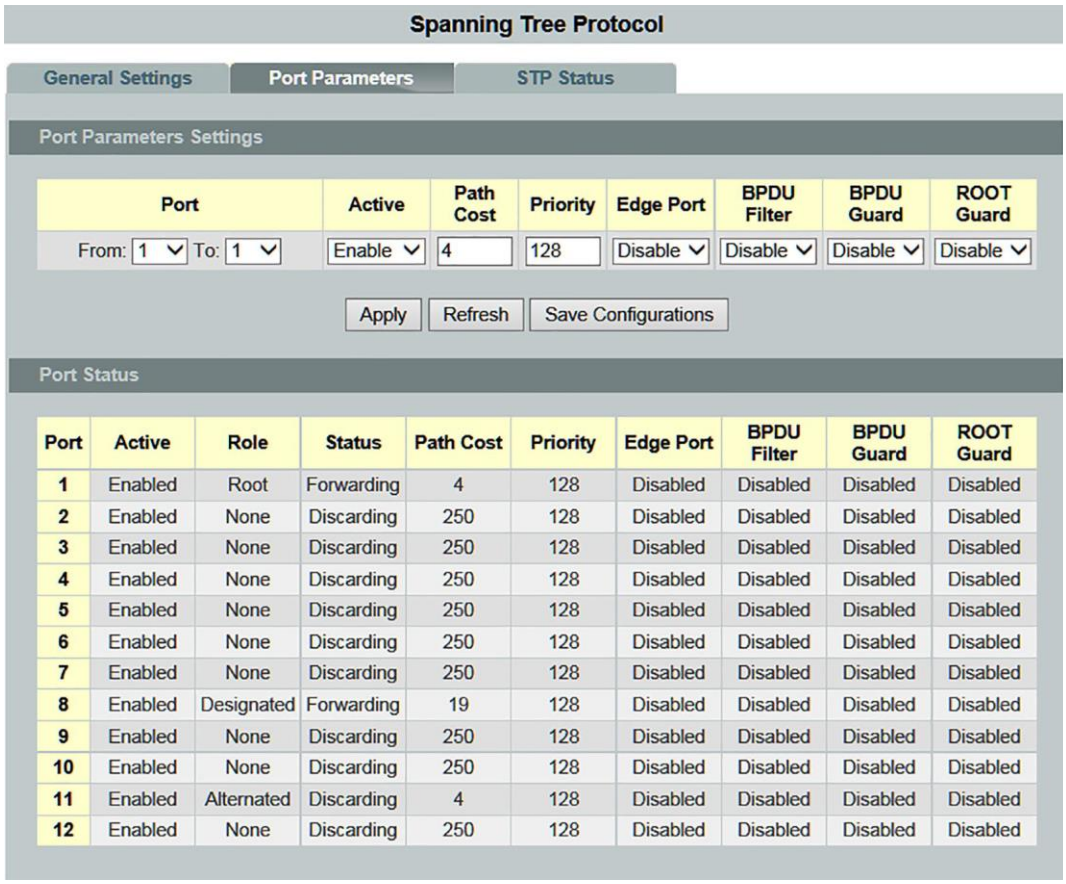


Ilustracja 95: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“

Tabela 97: 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 (Range: 4~30)	**15**	W polu edycji należy wpisać czas „Forward Delay“. Właściwy zakres: 4 … 30 s
Max Age (Range: 6~40)	**20**	W polu edycji należy wpisać czas „Max Age“. Właściwy zakres: 6 … 40 s
Hello Time (Range: 1~10)	**2**	W polu edycji należy wpisać czas „Hello Time“. Właściwy zakres: 1 … 10 s
Priority (Range: 0~61440)	**32768**	W polu edycji należy wpisać wartość priorytetu. Im niższa przypisana wartość numeryczna, tym wyższy priorytet bridge'a. Właściwy zakres: 0 … 61440
Pathcost 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

9.3.17.2 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 96: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“

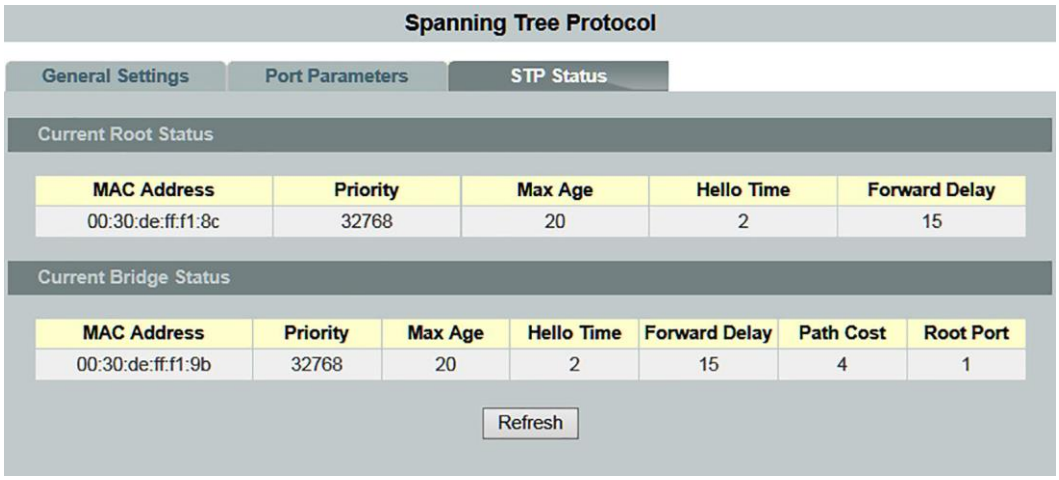
Tabela 98: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“

Port Parameters 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 Cost			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 „Edge Port“ dla specyficznego portu.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować typ „Edge Port“ dla specyficznego portu.
BPDU Filter		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję filtra BPDU dla specyficznego portu.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „BPDY 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 98: 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 Cost	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“.

9.3.17.3 STP Status



Ilustracja 97: Strona WBM „Spanning Tree Protocol“ – zakładka „STP Status“

Tabela 99: Strona WBM „STP“ – zakładka „STP-Status“

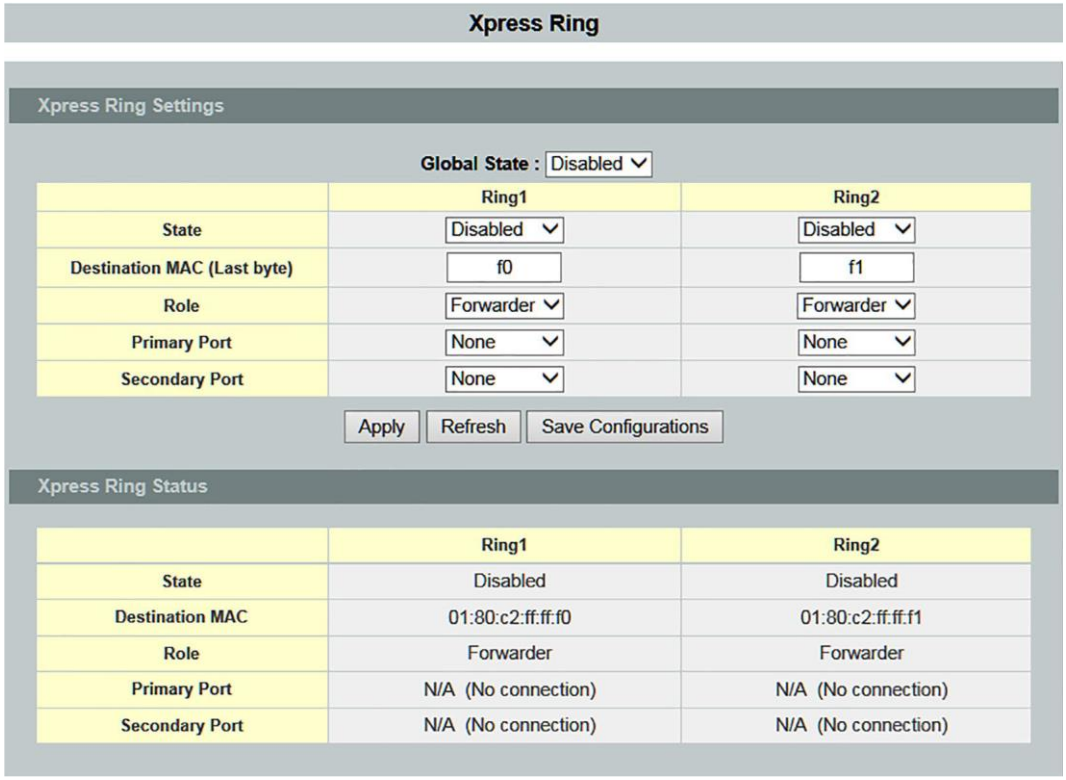
Current Root Status		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tym polu wyświetlany jest adres MAC dla „Root Bridge“.
Priority		W tym polu wyświetlany jest priorytet dla „Root Bridge“. Również ten switch może być „Root Bridge“.
Max Age		W tym polu wyświetlany jest „Max Age“ dla „Root Bridge“.
Hello Time		W tym polu wyświetlany jest „Hello Time“ dla „Root Bridge“. „Root Bridge“ określa „Hello Time“, „Max Age“ i „Forward 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 Delay“.
Path Cost		W tym polu wyświetlana jest wartość „Path Cost“.
ROOT Port		W tym polu wyświetlany jest numer portu switcha, przez który switch musi komunikować się z „Root“ „Spanning Tree“.

9.3.18 Xpress Ring

Wskazówka

Dodatkowa informacja

Więcej informacji o „Xpress Ring” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 98: Strona WBM „Xpress Ring“

Tabela 100: Strona WBM „Xpress Ring“

Xpress Ring Settings		
Parametr	**Domyślnie**	**Opis**
Global State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Xpress Ring“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Xpress Ring“.
Ring 1		W tej kolumnie można wprowadzić konfigurację dla „Ring 1“.
Ring 2		W tej kolumnie można wprowadzić konfigurację dla „Ring 2“.
State	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Xpress Ring“ dla danego pierścienia.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Xpress Ring“ dla danego pierścienia.
Destination MAC (Last byte)		W polu edycji należy wpisać adres MAC dla danego pierścienia.
Role	**Forwarder**	W polu wyboru należy wybrać rolę „Forwarder“ dla switcha.
	Arbiter	W polu wyboru należy wybrać rolę „Arbiter“ dla switcha.
Primary Port	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być aktywowany podstawowy port w pierścieniu.
	1 … 10 (12)	W polu wyboru należy wybrać odpowiedni podstawowy port.
Secondary Port	**None**	W polu wyboru należy wybrać „None“, jeśli nie ma być aktywowany rezerwowy port w pierścieniu.
	1 … 10 (12)	W polu wyboru należy wybrać odpowiedni rezerwowy port.
Xpress Ring Status		
Parametr	**Domyślnie**	**Opis**
Status	Disable Enable	W tym polu wyświetlany jest aktualny stan „Xpress Ring“.
Ring 1		W tej kolumnie wyświetlane są konfiguracje dla „Ring 1“.
Ring 2		W tej kolumnie wyświetlane są konfiguracje dla „Ring 2“.
Destination MAC		W tym polu wyświetlany jest ostatni bajt danego adresu MAC „Xpress Ring“.
Role	Forwarder Arbiter	W tym polu wyświetlana jest rola switcha.
Primary Port	N/D (No Connection) 0 … 10 (12) (Forwarding, Blocking)	W tym polu wyświetlany jest status podstawowego portu.
Secondary Port	N/D (No Connection) 0 … 10 (12) (Forwarding, Blocking)	W tym polu wyświetlany jest status rezerwowego portu.

9.4 Security

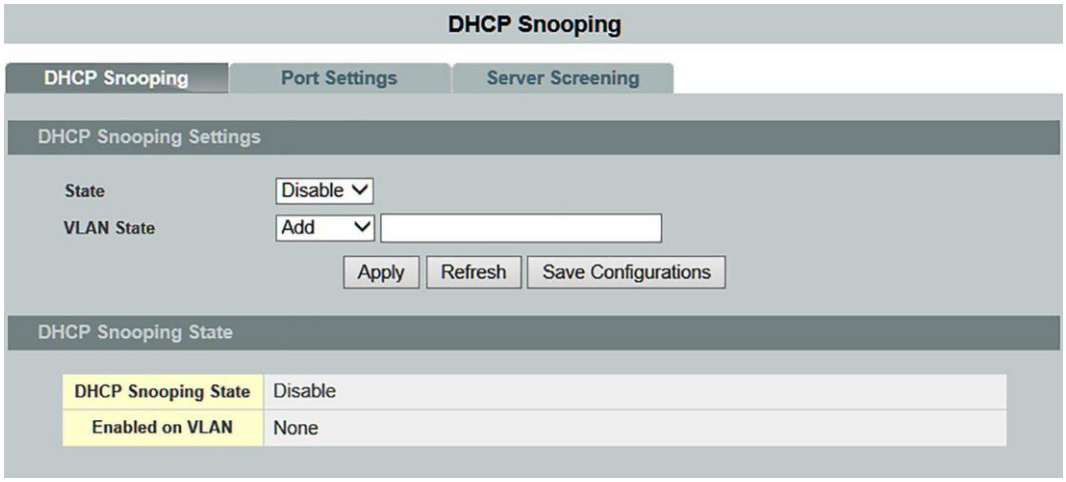
9.4.1 IP Source Guard

Wskazówka **Dodatkowa informacja**
Więcej informacji o „IP Source Guard“ można znaleźć w rozdziale „Opis funkcji“.

9.4.1.1 DHCP Snooping

Wskazówka **Dodatkowa informacja**
Więcej informacji o „DHCP Snooping“ (**D**ynamic **H**ost **C**onfiguration **P**rotocol) można znaleźć w rozdziale „Opis funkcji“.

9.4.1.1.1 DHCP Snooping

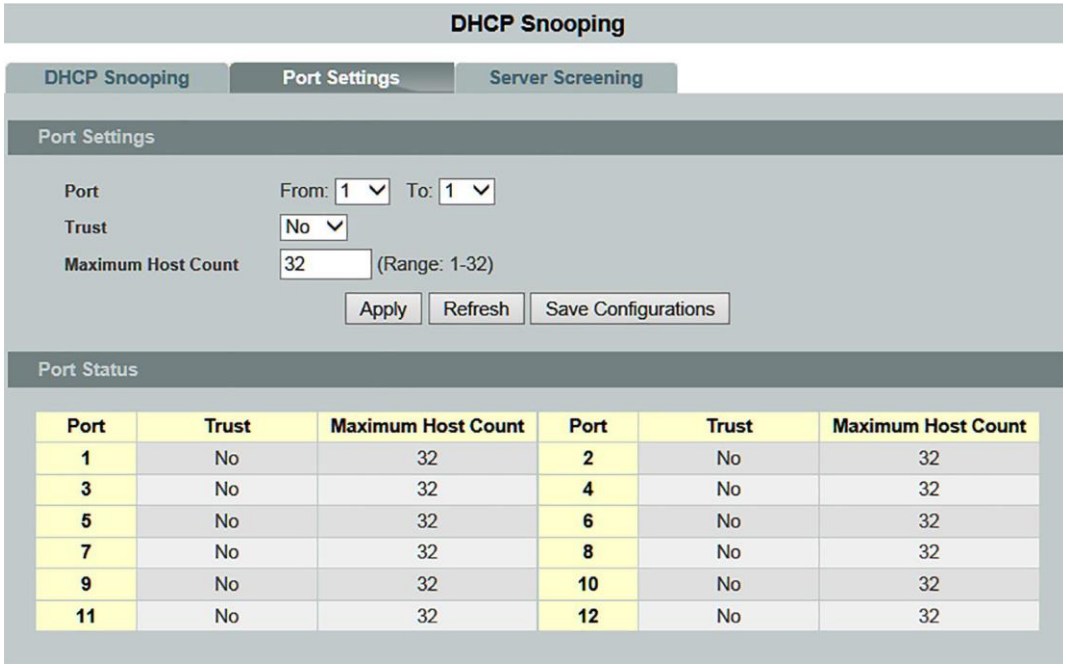


Ilustracja 99: Strona WBM „DHCP Snooping“ – zakładka „DHCP Snooping“

Tabela 101: Strona WBM „DHCP Snooping“ – zakładka „DHCP Snooping“

IGMP Snooping Settings		
Parametr	**Domyślnie**	**Opis**
State	**Disable**	W polu wyboru należy wybrać „Disable“, gdy ta funkcja nie ma być wykorzystana.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „DHCP Snooping“. Następnie należy jeszcze tę funkcję aktywować dla specyficznych sieci VLAN oraz skonfigurować „Trusted Ports“.
		Wskazówka  Konfiguracja żąda DHCP Switch odrzuca wszystkie żądania DHCP, gdy aktywowany jest „DHCP Snooping“, ale nie ma „Trusted Ports“. W polu wyboru należy wybrać „Disable“, gdy ta funkcja nie ma być wykorzystana.
VLAN State	**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, dla których switch ma aktywowany „DHCP 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, dla których switch ma dezaktywowany „DHCP Snooping“.
DHCP Snooping State		
Parametr	**Domyślnie**	**Opis**
DHCP Snooping State	Disable Enable	W tym polu wyświetlana jest informacja, czy funkcja „DHCP Snooping“ jest aktywowana, czy dezaktywowana.
Enabled on VLAN	None 1 … 4094	W tym polu wyświetlane są sieci VLAN, dla których aktywowana jest funkcja „DHCP Snoopng“. Wartość „None“ wyświetlana jest, gdy nie zostały wyspecyfikowane sieci VLAN.

9.4.1.1.2 Port Settings



Ilustracja 100: Strona WBM „DHCP Snooping“ – zakładka „Port Settings“

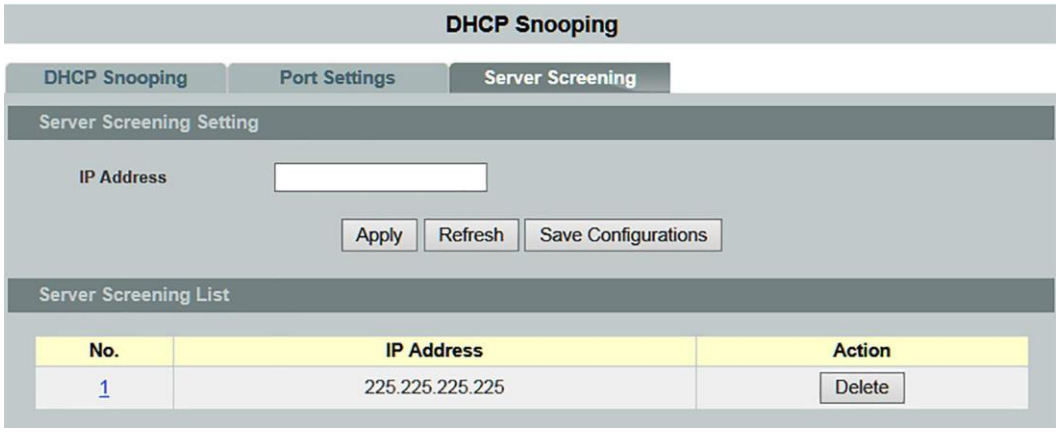
Tabela 102: Strona WBM „DHCP Snooping“ – zakładka „Port Settings“

Port Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być podana maksymalna liczba hostów.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, dla którego ma być podana maksymalna liczba hostów.
Trust		**No**	W polu wyboru należy wybrać „No“, gdy wyspecyfikowany port nie ma pełnić roli „Trusted Port“.
		Yes	W polu wyboru należy wybrać „Yes“, gdy wyspecyfikowany port ma pełnić rolę „Trusted Port“.
Maximum Host Count (Range: 1~32)		**32**	W polu edycji należy podać maksymalną liczbę hostów, które mogą równocześnie łączyć się z portem. Właściwy zakres: 1 … 32
Port Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Trust		None Yes	W tej kolumnie wyświetlany jest status „Trusted Port“.
Maximum Host Count			W tej kolumnie wyświetlana jest maksymalna liczba hostów, które mogą równocześnie łączyć się z portem.

9.4.1.1.3 Server Screening

Wskazówka

Dodatkowa informacja
Więcej informacji o „Server-Screening” można znaleźć w rozdziale „Opis funkcji”.



Ilustracja 101: Strona WBM „DHCP Snooping“ – zakładka „Server Screening“

Tabela 103: Strona WBM „DHCP Snooping“ – zakładka „Server Screening“

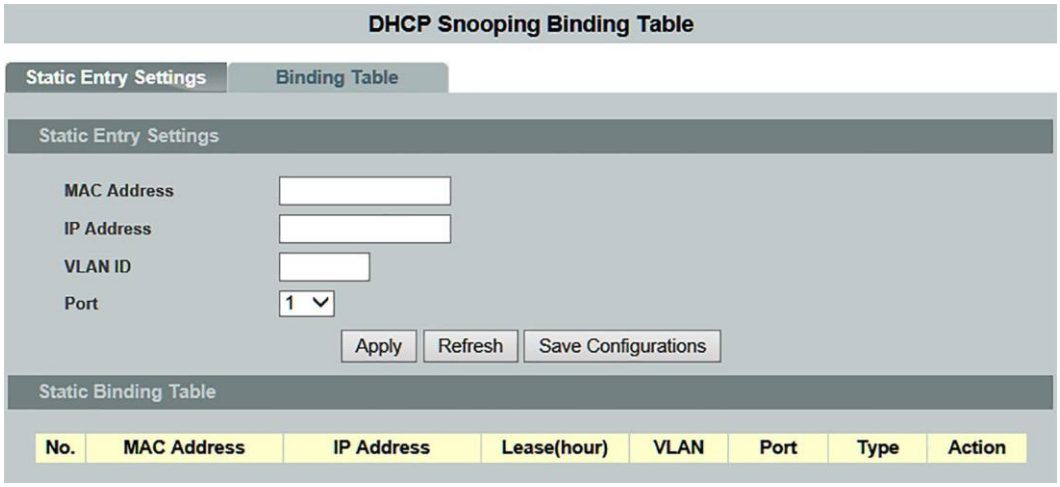
Server Screening Setting		
Parametr	**Domyślnie**	**Opis**
IP Address		W polu edycji należy wpisać adres IP ważnego serwera DHCP.
Server Screening List		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlany jest numer indeksu wpisu serwera DHCP. Należy kliknąć ten numer, aby zmodyfikować ten wpis.
IP Address		W tej kolumnie wyświetlany jest adres IP serwera DHCP.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

9.4.1.2 DHCP Snooping Binding Table

Wskazówka

Dodatkowa informacja
Więcej informacji o „Sooping Binding Table“ można znaleźć w rozdziale „Opis funkcji“.

9.4.1.2.1 Static Entry Settings

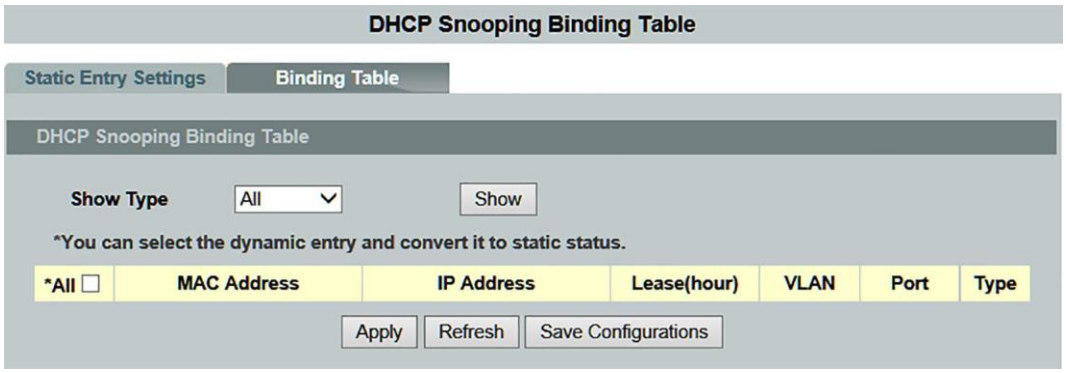


Ilustracja 102: Strona WBM „DHCP Snooping Binding Table“ – zakładka „Static Entry Settings“

Tabela 104: Strona WBM „DHCP Snooping Binding Table“ – zakładka „Static Entry Settings“

Static Entry Settings		
Parametr	**Domyślnie**	**Opis**
MAC Address		W polu edycji należy wpisać „MAC Source Address“ dla powiązania.
IP Address		W polu edycji należy wpisać adres IP przydzielony dla „MAC Source Address“ dla powiązania.
VLAN ID		W polu edycji należy wpisać „Source VLAN ID“ dla powiązania.
Port	**1** … 10 (12)	W polu wyboru należy wybrać fizyczny port powiązania.
Static Binding Table		
Parametr	**Domyślnie**	**Opis**
No.	1 … 10 (12)	W tej kolumnie wyświetlane są kolejne numery dla każdego powiązania. Należy tu kliknąć, aby zaktualizować istniejące wpisy.
MAC Address		W tej kolumnie wyświetlany jest adres MAC dla powiązania.
IP Address		W tej kolumnie wyświetlany jest adres „MAC Source Address“ dla powiązania.
Lease (hour)		W tej kolumnie wyświetlana jest informacja, jak długo powiązanie jest ważne.
VLAN		W tej kolumnie wyświetlany jest adres „Source VLAN ID“ dla powiązania.
Port	1 … 10 (12)	W tej kolumnie wyświetlany jest numer portu dla powiązania.
Type	Static Dynamic	W tej kolumnie wyświetlana jest informacja, jak switch został powiadomiony o powiązaniu. „Static“: Do powiązanie zostało wprowadzone ręcznie przez administratora. „Dynamic“: To powiązanie zostało wpisane przez informacje z „DHCP- Snooping“.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

9.4.1.2.2 Binding Table



Ilustracja 103: Strona WBM „DHCP-Snooping-Binding Table“ – zakładka „Binding Table“

Tabela 105: Strona WBM „DHCP-Snooping-Binding Table“ – zakładka „Binding Table“

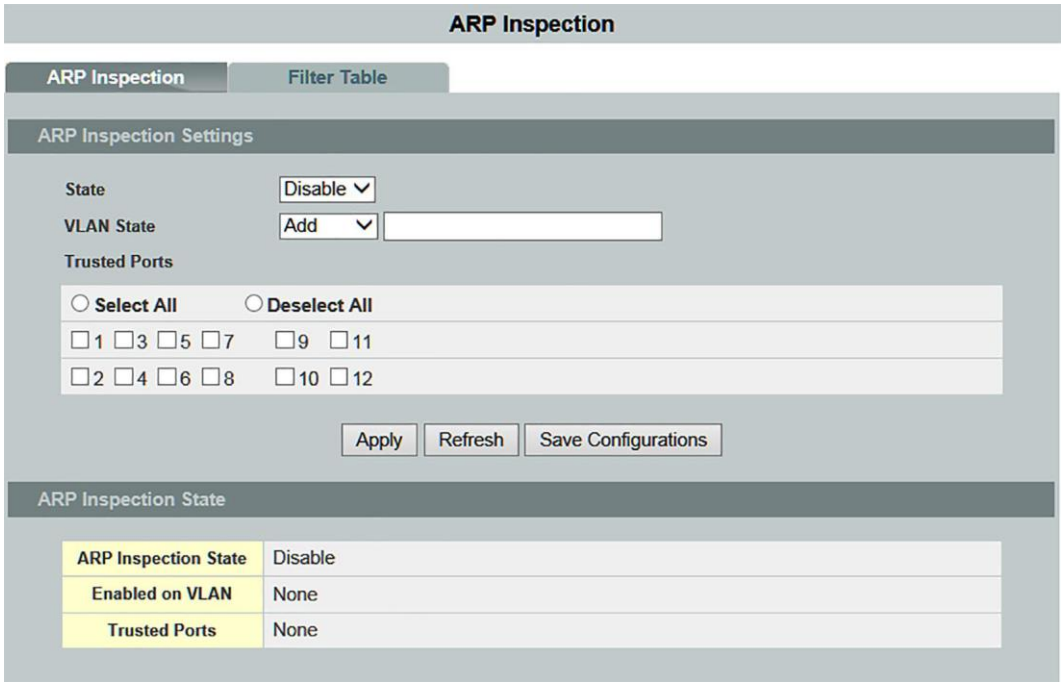
DHCP Snooping Binding Table		
Parametr	**Domyślnie**	**Opis**
Show Type	**All**	W polu wyboru należy wybrać „All“, gdy mają być wyświetlone wszystkie wpisy „Binding Table“.
	Dynamic	W polu wyboru należy wybrać „Dynamic“, gdy mają być wyświetlone dynamiczne wpisy „Binding Table“.
	Static	W polu wyboru należy wybrać „Static“, gdy mają być wyświetlone statyczne wpisy „Binding Table“.
Parametr	**Domyślnie**	**Opis**
All	1 … 10 (12)	W tej kolumnie wyświetlane są kolejne numery dla każdego powiązania. Należy tu kliknąć, aby zaktualizować istniejące wpisy.
MAC Address		W tej kolumnie wyświetlany jest adres MAC dla powiązania.
IP Address		W tej kolumnie wyświetlany jest adres „MAC Source Address“ dla powiązania.
Lease (hour)		W tej kolumnie wyświetlana jest informacja, jak długo powiązanie jest ważne.
VLAN		W tej kolumnie wyświetlany jest adres „Source VLAN ID“ dla powiązania.
Port		W tej kolumnie wyświetlany jest numer portu dla powiązania. Gdy to pole pozostaje puste, powiązanie jest transmitowane do wszystkich portów.
Type	Static Dynamic	W tej kolumnie wyświetlana jest informacja, jak switch został powiadomiony o powiązaniu. „Static“: Do powiązanie zostało wprowadzone ręcznie przez administratora. „Dynamic“: To powiązanie zostało wpisane przez informacje z „DHCP- Snooping“.

9.4.1.3 ARP Inspection

Wskazówka

Dodatkowa informacja
Więcej informacji o „ARP Inspection“ („**A**ddres **R**esolution **P**rotocol“) można znaleźć w rozdziale „Opis funkcji“.

9.4.1.3.1 ARP Inspection



Ilustracja 104: Strona WBM „ARP Inspection“ – zakładka „ARP Inspection“

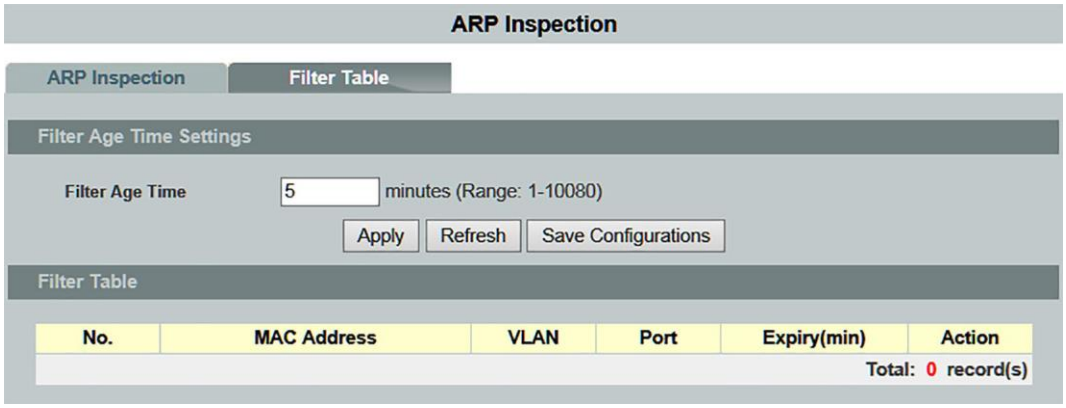
Tabela 106: Strona WBM „ARP Inspection“ – zakładka „ARP Inspection“

ARP Inspection Settings				
Parametr		**Domyślnie**	**Opis**	
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować w switchu „ARP Inspection“.	
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować w switchu „ARP Inspection“.	
VLAN State		**Add**	W polu wyboru należy wybrać „Add“ i wpisać sieci VLAN, dla których switch ma aktywowany „ARP Inspection“. 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 nie ma wykonywać „IGMP Snooping“.	
Trusted Ports			Należy wybrać porty, które mają być lub nie mają być „Trusted Ports“. Switch w żadnym razie nie odrzuci pakietów ARP z „Trusted Ports“. Switch odrzuca pakiety DHCP z „Untrusted Ports“ w następujących sytuacjach: • Informacje nadawcy w pakiecie ARP nie zgadzają się z żadnym z aktualnych powiązań. • Prędkość transmisji odebranych pakietów DHCP jest za wysoka. Można określić maksymalną szybkość odbioru na „Untrusted Ports”.	
	Sellect All	○	○	Żaden port nie jest wybrany jako „Trusted“.
			◉	Wszystkie porty są wybrane jako „Trusted“.
	Cancel Selection	○	○	Żaden port nie jest dezaktywowany jako „Trusted“.
			◉	Wszystkie porty są dezaktywowane jako „Trusted“.
	☐ 1 … ☐ 10 (12)	☐	☐	Port nie jest aktywowany.
			☑	Port jest aktywowany.
ARP Inspection State				
Parametr		**Domyślnie**	**Opis**	
ARP Inspection State		Disable Enable	W tym polu wyświetlany jest aktualny status „ARP Inspection“.	
Enabled on VLAN		None 1 … 10 (12)	W tym polu wyświetlane są VLAN ID, dla których aktywowana jest funkcja „ARP Inspection“.	
Trusted Ports		None 1 … 10 (12)	W tym polu wyświetlane są porty, wyspecyfikowane jako „Trusted Ports“.	

9.4.1.3.2 Filter Table

Wskazówka

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



Ilustracja 105: Strona WBM „ARP Inspection“ – zakładka „Filter Table“

Tabela 107: Strona WBM „ARP Inspection“ – zakładka „Filter Table“

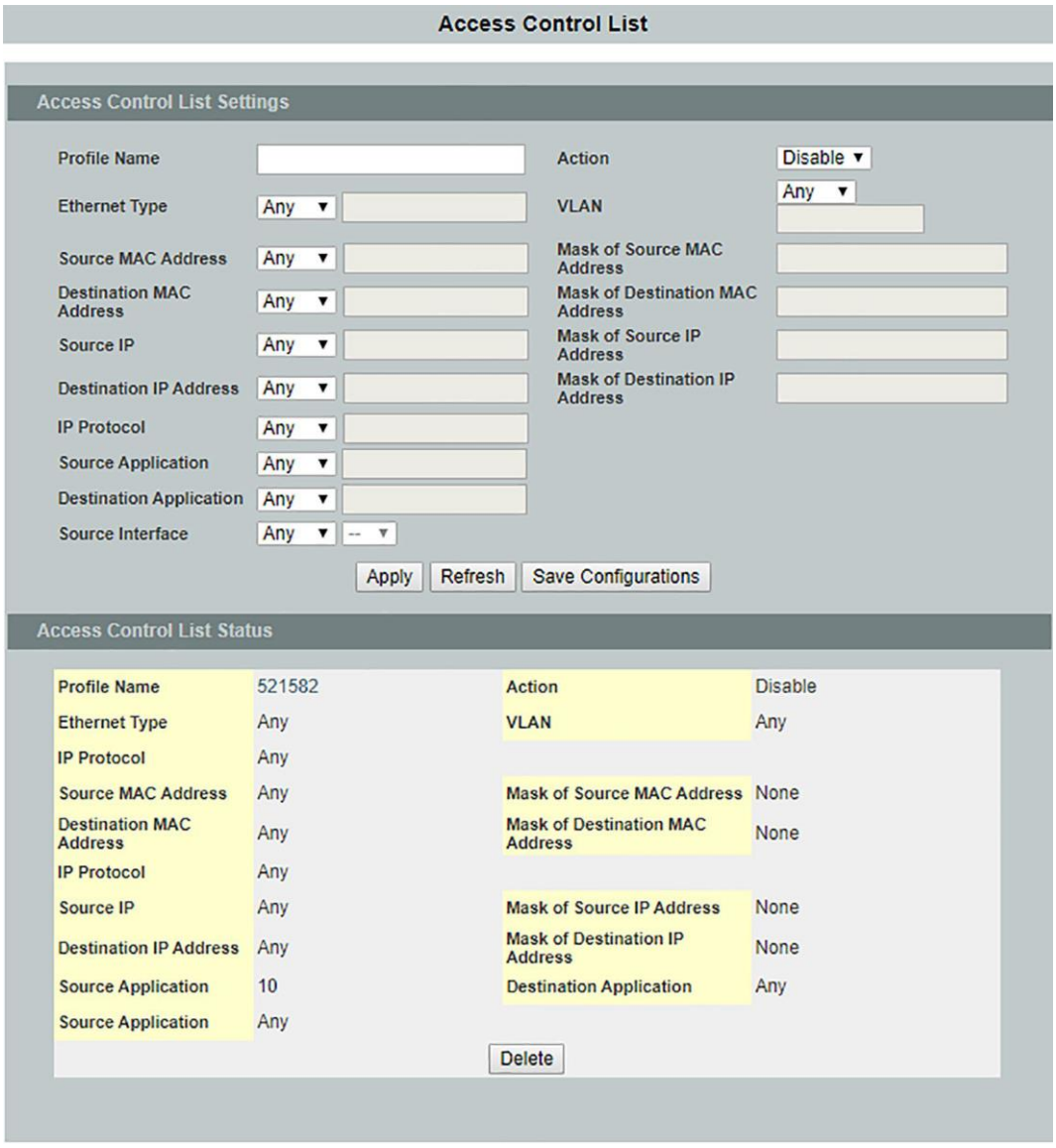
Filter Age Time Settings		
Parametr	**Domyślnie**	**Opis**
Filter Age Time minutes (Range: 1~10080)	**5**	W polu edycji należy wpisać czas, jak długo wpis filtra adresu MAC ma pozostać w switchu po odebraniu nieautoryzowanego pakietu ARP. Okres: 1 … 10 080 min Po upływie tego czasu switch automatycznie usuwa wpis. To ustawienie nie działa na już istniejące filtry adresów MAC.
Filter Table		
Parametr	**Domyślnie**	**Opis**
No.		W tej kolumnie wyświetlane są kolejne numery każdego wpisu filtra adresu MAC.
MAC Address		W tej kolumnie wyświetlane są źródłowe adresy MAC w filtrze adresów MAC.
VLAN		W tej kolumnie wyświetlane są źródłowe VLAN ID w filtrze adresów MAC.
Port		W tej kolumnie wyświetlane są źródłowe porty odrzuconych pakietów ARP.
Expiry Time (min)		W tej kolumnie wyświetlany jest czas (w minutach), przez który wpis filtra adresów MAC pozostaje w switchu.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.
Quantity		W tym polu wyświetlana jest zbiorcza liczba aktualnych wpisów filtrów adresów MAC, które wygenerował switch na podstawie rozpoznanych, nieautoryzowanych pakietów ARP.

9.4.2 Access Control List (ACL)

Wskazówka

Dodatkowa informacja

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



Ilustracja 106: Strona WBM „Access Control List“

Tabela 108: Strona WBM „Access Control List“

Access Control List Settings		
Parametr	**Domyślnie**	**Opis**
IP Type	**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.
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.
	DSCP	W polu wyboru należy wybrać „DSCP“, aby nadać nowy priorytet pakietom danych, odpowiadających informacjom. (tylko przy IPv4)
ETHERNET Type (tylko przy IPv4)	**Any**	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**	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 (tylko przy IPv4)	**Any**	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 the Source MAC Address (tylko przy IPv4)		W polu edycji należy wpisać źródłowy adres MAC maski bitowej dla źródłowych adresów MAC pakietów danych, 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 (tylko przy IPv4)	**Any**	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 the Destination MAC Address (tylko przy IPv4)		W polu edycji należy wpisać docelowy adres MAC maski bitowej dla docelowych adresów MAC pakietów danych, 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“.

Tabela 108: Strona WBM „Access Control List“

DSCP (tylko przy IPv4)	**Any**	Należy wybrać „Any“, aby każdy priorytet DSCP dla „Access Control List“ był ważny.	
	Other	**0** … 63	W polu wyboru należy wybrać priorytet DSCP.
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 danych, 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.	
Mask of Destination IP Address		W polu edycji należy wpisać docelowy adres IP maski bitowej dla docelowych adresów IP pakietów danych, 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 Protocol	**Any**	Należy wybrać „Any“, aby każdy protokół IP dla „Access Control List“ był ważny.	
	Other	W polu wyboru należy wybrać „Add“, aby wpisać protokół.	
Source Application	**Any**	Należy wybrać „Any“, aby każda aplikacja była ważna.	
	Other	W polu wyboru należy wybrać „Other“, aby wpisać port źródłowy (np. 2234).	
Destination Applikation	**Any**	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 108: Strona WBM „Access Control List“

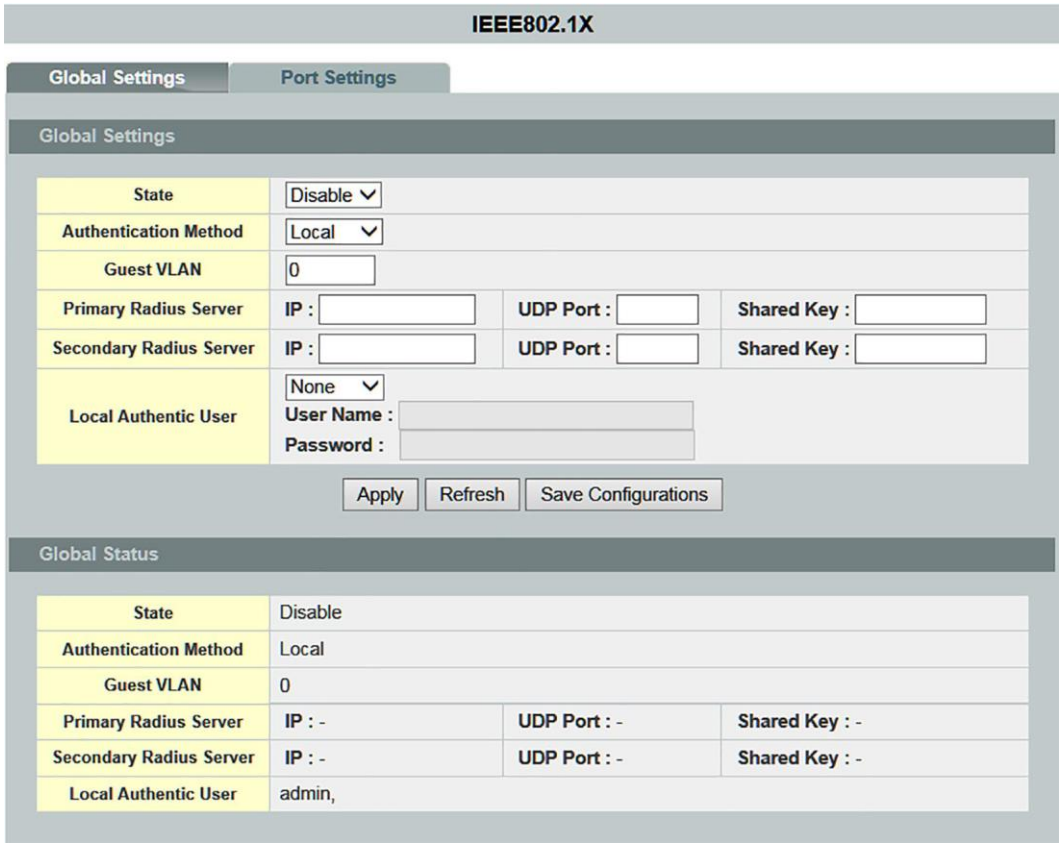
Access Control List Status		
Parametr	**DomyślnIe**	**Opis**
IP Type	IPv4 IPv6	W tym polu wyświetlany jest wybrany typ IP.
Profile Name		W tym polu wyświetlana jest wybrana nazwa profilu.
Action	Disable Permission Discard DSCP	W tym polu wyświetlany jest status sterowania dostępem. (DSCP tylko przy IPv4)
ETHERNET Type (tylko przy IPv4)	Any Other	W tym polu wyświetlany jest typ ETHERNET.
VLAN	Any Other	W tym polu wyświetlany jest VLAN ID.
Source MAC Address (tylko przy IPv4)	Any Other	W tym polu wyświetlany jest „Source MAC Address“.
Mask of the Source MAC Address (tylko przy IPv4)		W tym polu wyświetlany jest źródłowy adres MAC maski bitowej.
Destination MAC Address (tylko przy IPv4)	Any Other	W tym polu wyświetlany jest docelowy adres MAC.
Mask of the Destination MAC Address (tylko przy IPv4)		W tym polu wyświetlany jest docelowy adres MAC maski bitowej.
DSCP (tylko przy IPv4)	Any Other	W tym polu wyświetlany jest priorytet DSCP.
IP Protocol	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.

9.4.3 IEEE 802.1X

Wskazówka

Dodatkowa informacja
Więcej informacji o standardzie „IEEE 802.1X” można znaleźć w rozdziale „Opis funkcji”.

9.4.3.1 Global Settings



Ilustracja 107: Strona WBM „IEEE 802.1X“ – zakładka „Global Settings“

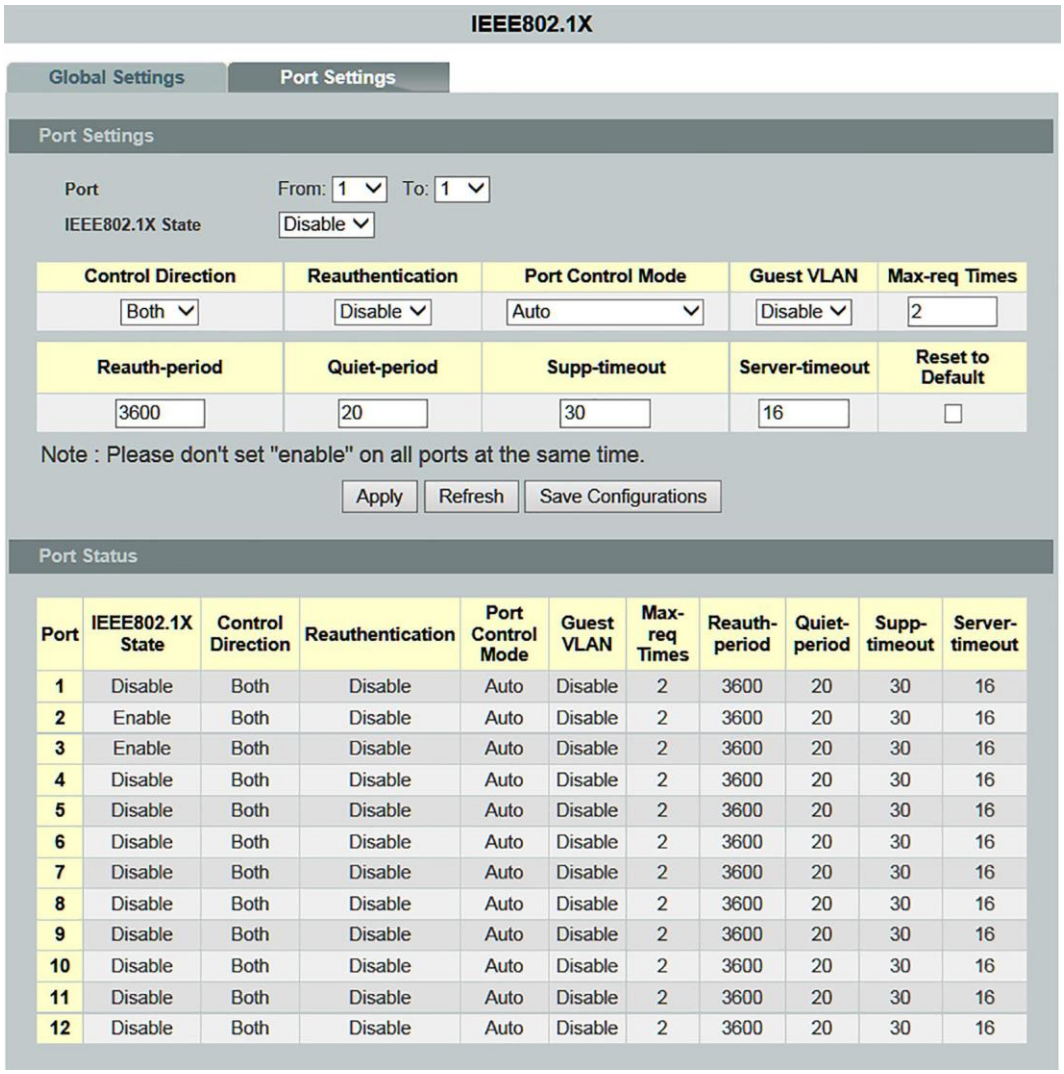
Tabela 109: Strona WBM „IEEE 802.1X“ – zakładka „Global Settings“

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

Tabela 109: Strona WBM „IEEE 802.1X“ – zakładka „Global Settings“

Global Settings				
Parametr		**Domyślnie**	**Opis**	
Secondary Radius Server			Jest to serwer rezerwowy, wykorzystywany tylko wtedy, gdy podstawowy serwer „Radius“ ma awarię.	
	IP:		W polu edycji należy wpisać adres IP zewnętrznego serwera „Radius“, używając zapisu z kropkami.	
	UDP Port:	**0 … 65535**	W polu edycji należy wpisać numer portu serwera „Radius“.	
	Shared Key:		W polu edycji należy wpisać hasło (32 znaki alfanumeryczne), które jest stosowane jako wspólny klucz dla połączenia między zewnętrznym serwerem „Radius“ i switchem. Klucz ten nie może być przesłany przez sieć. Klucze na zewnętrznym serwerze „Radius” i switchu muszą być identyczne.	
Local Authentic User			W polu edycji wyświetlane/uzupełniane/usuwane są nazwa użytkownika i hasło.	
		None	Gdy w polu wyboru wybrana jest opcja „None“, nie ma możliwości zmiany nazwy użytkownika i hasła.	
		Delete	User Name:	Gdy w polu wyboru wybrana jest opcja „Delete“, istnieje możliwość zmiany nazwy użytkownika.
		Add	Password:	Gdy w polu wyboru wybrana jest opcja „Add“, można zmienić nazwę użytkownika i hasła.
Global Status				
Parametr		**Domyślnie**	**Opis**	
State		Disable Enable	W tym polu wyświetlana jest informacja, czy uwierzytelnienie IEEE-802.1X jest aktywowane, czy dezaktywowane.	
Authentication Method		Lokal Radius	W tym polu wyświetlana jest metoda uwierzytelniania.	
Guest VLAN			W tym polu wyświetlana jest sieć „Guest VLAN“.	
Primaty Radius Server	IP:		W tym polu wyświetlane są adres IP, port dla UDP i wspólne klucze dla podstawowego serwera „Radius“. Pola są puste, jeśli nie wykonano konfiguracji.	
	UDP Port:			
	Shared Key:			
Secondary Radius Server	IP:		W tym polu wyświetlane są adres IP, port dla UDP i wspólne klucze dla rezerwowego serwera „Radius“. Pola są puste, jeśli nie wykonano konfiguracji.	
	UDP Port:			
	Shared Key:			
Local Authentic User		admin,	W tym polu wyświetlana jest lista zgłoszonych użytkowników.	

9.4.3.2 Port Settings



Port	IEEE802.1X State	Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
2	Enable	Both	Disable	Auto	Disable	2	3600	20	30	16
3	Enable	Both	Disable	Auto	Disable	2	3600	20	30	16
4	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
5	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
6	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
7	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
8	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
9	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
10	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
11	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
12	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16

Ilustracja 108: Strona WBM „IEEE 802.1X“ – zakładka „Port Settings“

Tabela 110: Strona WBM „IEEE 802.1X“ – 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“.
IEEE-802.1X State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować dla portu uwierzytelnienie IEEE 802.1X.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować dla portu uwierzytelnienie IEEE 802.1X.
			Wskazówka  **Uwierzytelnienie IEEE 802.1X** Najpierw należy aktywować w switchu uwierzytelnienie IEEE 802.1X, a dopiero potem można konfigurować tę funkcję dla poszczególnych portów.
Control Direction		**Both**	W polu wyboru należy wybrać „Both“, gdy po niepomyślnym uwierzytelnieniu IEEE 802.1X użytkownika zarówno pakiety danych, wchodzące na port, jak i wychodzące, zostają odrzucone.
		Incoming	W polu wyboru należy wybrać „Incoming“, gdy po niepomyślnym uwierzytelnieniu IEEE 802.1X użytkownika tylko pakiety danych, wchodzące na port, zostają odrzucone.
Reauthentication		**Disable**	W polu wyboru należy wybrać „Disable“, gdy w celu utrzymania połączenia z portem uczestnik nie musi regularnie podawać na nowo nazwę użytkownika i hasło.
		Enable	W polu wyboru należy wybrać „Enable“, gdy w celu utrzymania połączenia z portem uczestnik musi regularnie podawać na nowo nazwę użytkownika i hasło.
Port Control Mode		**Auto**	W polu wyboru należy wybrać „Auto“, aby aktywować dla portu uwierzytelnienie.
		Force Authorized	W polu wyboru należy wybrać „Force Authorized“, aby aktywować dla portu stałe uwierzytelnianie.
		Force Unauthorized	W polu wyboru należy wybrać „Force Unauthorized“, aby aktywować dla portu stałą odmowę uwierzytelniania. W efekcie na tym porcie nie mogą być przekazywane pakiety danych.
Guest VLAN		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować na port „Guest VLAN“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować na porcie „Guest VLAN“.
Max-req Times		**2**	W polu edycji należy wpisać wartość wymaganych maksymalnych okresów czasu, przez które switch ma próbować łączyć się z serwerem uwierzytelniającym, zanim uzna go za niepołączony.
Reauth Period		**3600**	W polu edycji należy wybrać wartość interwału czasowego, w którym uczestnik musi podać ponownie nazwę użytkownika i hasło, w celu utrzymania połączenia z portem.

Tabela 110: Strona WBM „IEEE 802.1X“ – zakładka „Port Settings“

Quiet Period	**60**		W polu edycji należy podać wartość czasu, jaki Client musi odczekać, zanim będzie mógł ponowić żądanie uwierzytelnienia. Zapobiega to przeciążeniu switcha przez powtarzające się żądania klienta.
Supp Timeout	**30**		W polu edycji należy wpisać wartość czasu, przez które switch musi czekać, zanim skomunikuje się z serwerem.
Server Timeout	**30**		W polu edycji należy wpisać wartość czasu, przez które switch ma czekać na odpowiedź serwera uwierzytelnienia.
Reset to Default!	☐	☐	Zmienione ustawienia dla uwierzytelnienia portu IEEE 802.1X nie są resetowane do ustawień domyślnych.
		☑	Zmienione ustawienia dla uwierzytelnienia portu IEEE 802.1X są resetowane do ustawień domyślnych.

Tabela 110: Strona WBM „IEEE 802.1X“ – zakładka „Port Settings“

Port Status		
Parametr	**Domyślnie**	**Opis**
Port	1 **…** 10 (12)	W tej kolumnie wyświetlane są numery portów.
IEEE-802.1X State	Disable Enable	W tej kolumnie wyświetlana jest informacja, czy uwierzytelnienie IEEE-802.1X jest dla portu aktywowane, czy dezaktywowane.
Control Direction	Both Incoming	W tej kolumnie wyświetlana jest „Control Direction“.
Reauthentication	Disable Enable	W tej kolumnie wyświetlana jest informacja, czy w celu utrzymania połączenia z portem uczestnik musi regularnie podawać na nowo nazwę użytkownika i hasło w celu utrzymania połączenia z portem.
Port Control Mode	Automatic Force Authorized Force Unauthorized	W tej kolumnie wyświetlany jest „Port Control Mode“.
Guest VLAN	Disable Enable	W tej kolumnie wyświetlane jest ustawienie „Guest VLAN“ dla hostów, dla których autoryzacja się nie powiodła.
Max-req Times	1 … 10	W tej kolumnie wyświetlana jest informacja, jak często switch będzie próbował łączyć się z serwerem uwierzytelniającym, zanim uzna go za niepołączony.
Reauth Period	0 … 65535	W tej kolumnie wyświetlana jest informacja, w jakich interwałach czasowych uczestnik musi podawać na nowo nazwę użytkownika i hasło w celu utrzymania połączenia z portem.
Quiet Period	0 … 65535	W tej kolumnie wyświetlany jest czas, jaki Client musi odczekać, zanim będzie mógł ponowić żądanie uwierzytelnienia.
Supp Timeout	0 … 65535	W tej kolumnie wyświetlana jest informacja, jak długo musi czekać switch, zanim skomunikuje się z serwerem.
Server Timeout	0 … 65535	W tej kolumnie wyświetlana jest informacja, jak długo musi czekać switch, zanim skomunikuje się z klientem.

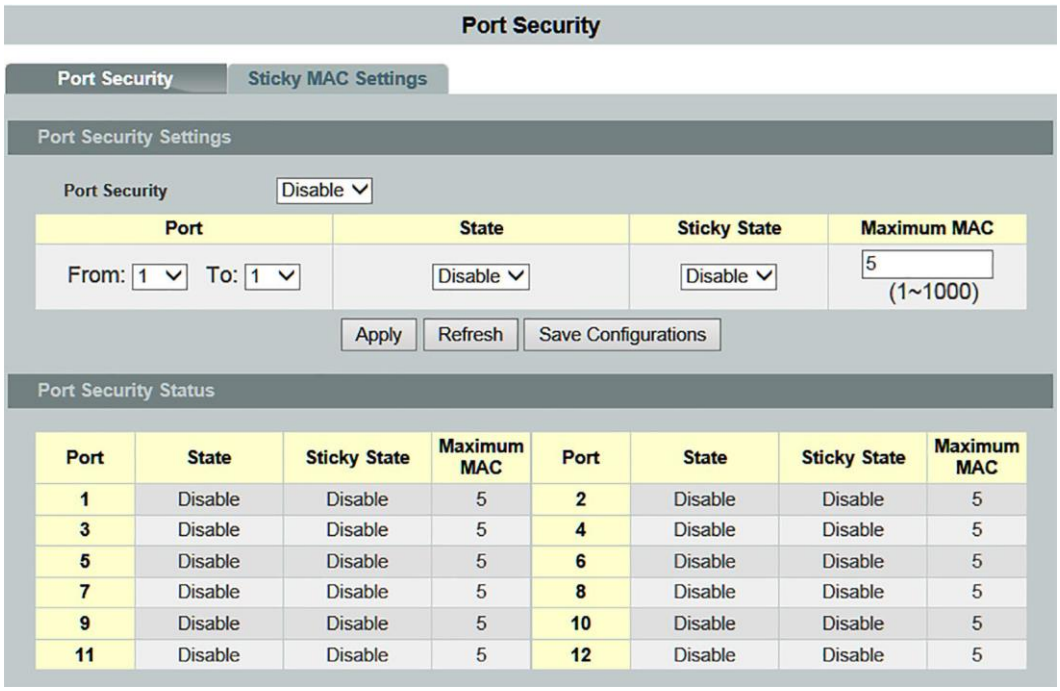
9.4.4 Port Security

9.4.4.1 Port Security

Wskazówka

Dodatkowa informacja

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



Port	State	Sticky State	Maximum MAC	Port	State	Sticky State	Maximum MAC
1	Disable	Disable	5	2	Disable	Disable	5
3	Disable	Disable	5	4	Disable	Disable	5
5	Disable	Disable	5	6	Disable	Disable	5
7	Disable	Disable	5	8	Disable	Disable	5
9	Disable	Disable	5	10	Disable	Disable	5
11	Disable	Disable	5	12	Disable	Disable	5

Ilustracja 109: Strona WBM „Port Security“ – zakładka „Port Security“

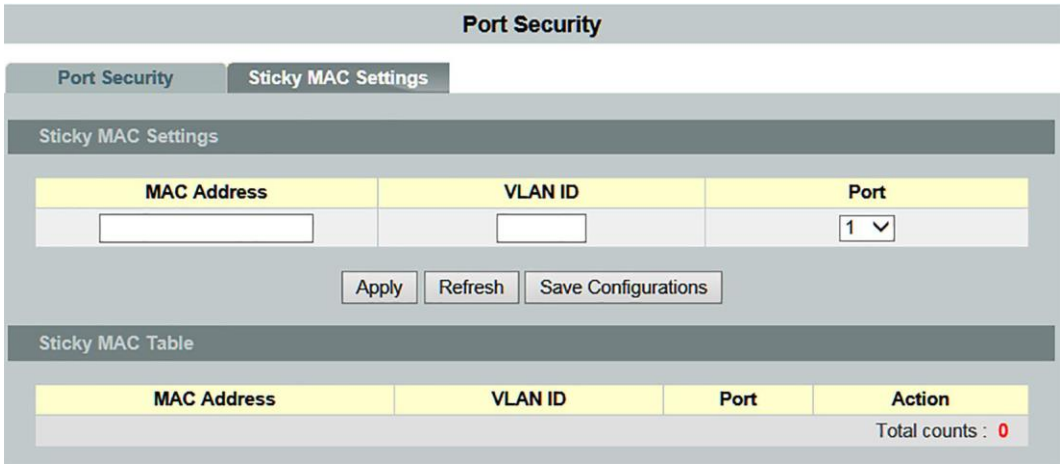
Tabela 111: Strona WBM „Port Security“ – zakładka „Port Security“

Port Security Settings			
Parametr		**Domyślnie**	**Opis**
Port Security		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Port Security“.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Port Security“.
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Security“.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, aby skonfigurować „Port Security“.
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować „Port Security“ dla portu lub zakresu portów.
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować „Port Security“ dla portu lub zakresu portów.
Maximum MAC (1~1000)		**5**	W polu edycji należy wpisać maksymalną liczbę adresów MAC na interfejs.
Port Security Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
State		Enable Disable	W tej kolumnie wyświetlana jest informacja, czy „Port Security“ jest aktywowany, czy dezaktywowany.
Maximum MAC		0 … 1000	W tej kolumnie wyświetlana jest maksymalna liczba adresów MAC.

9.4.4.2 Sticky MAC Settings

Wskazówka

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



Ilustracja 110: Strona WBM „Port Security“ – zakładka „Sticky MAC Settings“

Tabela 112: Strona WBM „Port Security“ – zakładka „Sticky MAC Settings“

Sticky MAC Settings		
Parametr	**Domyślnie**	**Opis**
MAC Address		W polu edycji należy wpisać adres MAC dla powiązania.
VLAN ID		W polu edycji należy wpisać „Source VLAN ID“ dla powiązania.
Port	**1** … 10 (12)	W polu wyboru należy wybrać fizyczny port powiązania.
Port Security Status		
Parametr	**Domyślnie**	**Opis**
MAC Address		W tej kolumnie wyświetlany jest adres MAC dla powiązania.
VLAN ID		W tej kolumnie wyświetlany jest VLAN ID dla powiązania.
Port	1 … 10 (12)	W tej kolumnie wyświetlane są numery portów.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

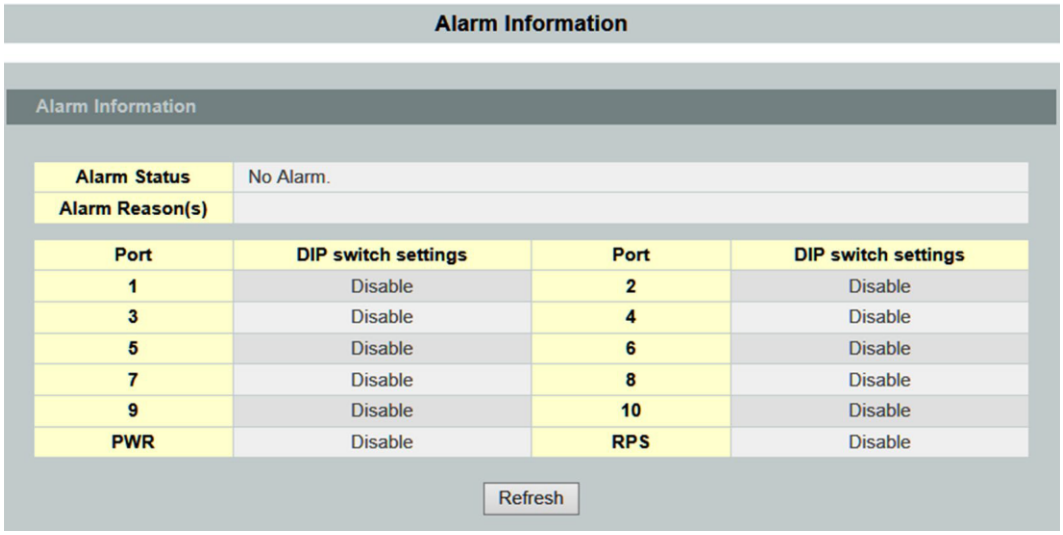
9.5 Monitor

9.5.1 Alarm Information

Wskazówka

Dodatkowa informacja

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



Ilustracja 111: Strona WBM „Alarm Information“

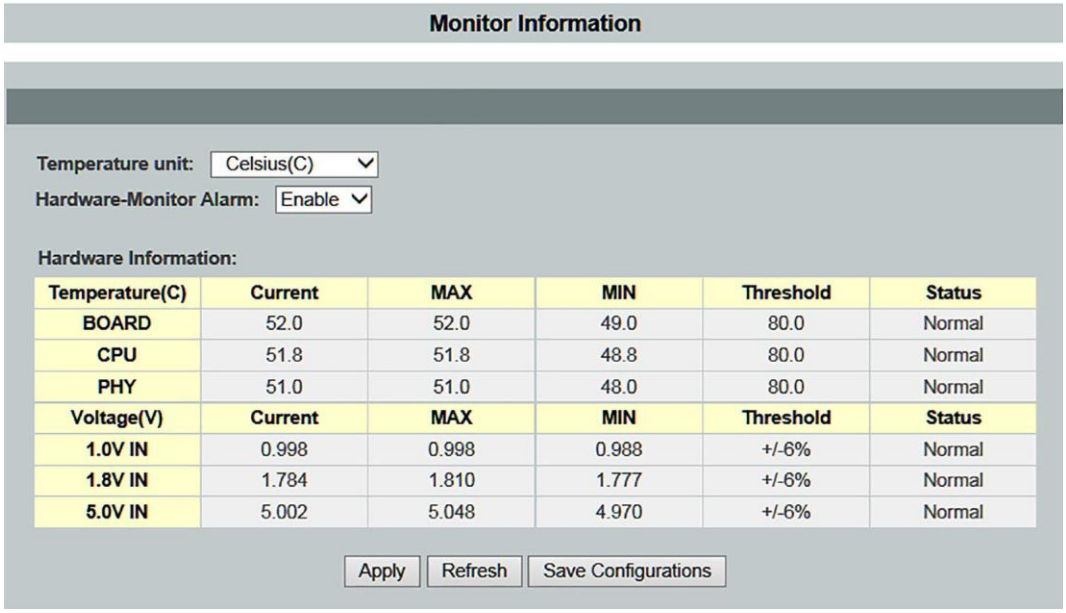
Tabela 113: Strona WBM „Alarm Information“

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 (12) PWR RPS	W tej kolumnie wyświetlana jest nazwa mikroprzełącznika DIP.
DIP switch settings	Enable Disable	W tej kolumnie wyświetlany jest aktualny status mikroprzełącznika DIP.

9.5.2 System Information

Wskazówka

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



Ilustracja 112: Strona WBM „System Information”

Tabela 114: Strona WBM „System 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 Monitor Alarm	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Hardware Monitor Alarm“.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Hardware Monitor Alarm“.
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“, „1,8 V IN“ i „5,0 V IN“.
MAX		W tej kolumnie wyświetlane jest maksymalne napięcie dla wejść „1,0 V IN“, „1,8 V IN“ i „5,0 V IN“.
MIN		W tej kolumnie wyświetlane jest minimalne napięcie dla wejść „1,0 V IN“, „1,8 V IN“ i „5,0 V IN“.
Threshold		W tej kolumnie wyświetlany jest ustawiony próg.
Status		W tej kolumnie wyświetlany jest status.

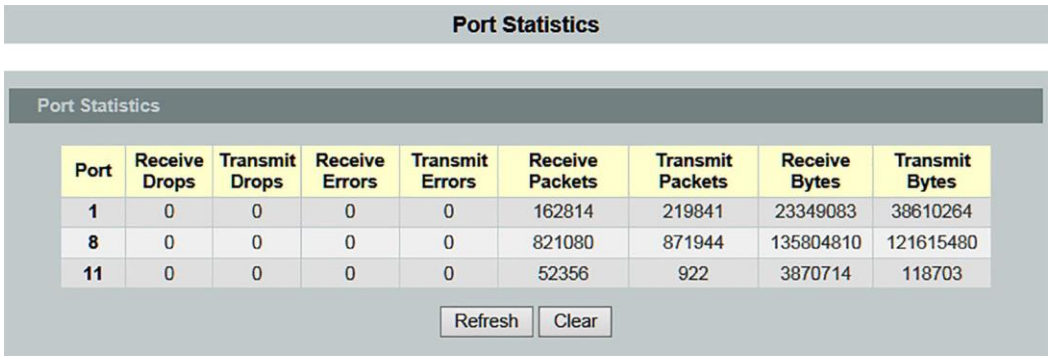
9.5.3 Port Statistics

Wskazówka



Dodatkowa informacja

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



Ilustracja 113: Strona WBM „Port Statistics“

Tabela 115: Strona WBM „Port Statistics“

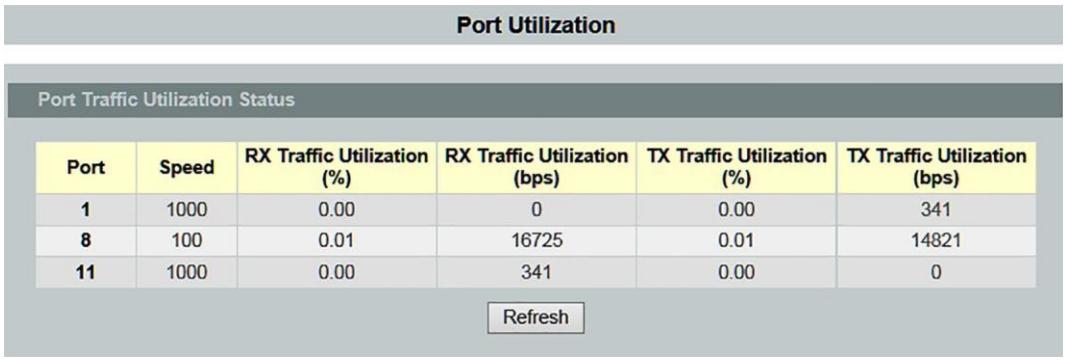
Port Statistics		
Parametr	**Domyślnie**	**Opis**
Port		W tej kolumnie wyświetlane są numery portów.
Receive Drops		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych na linii odbiorczej.
Transmit Drops		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych na linii nadawczej.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

9.5.4 Port Utilization

Wskazówka

Dodatkowa informacja

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



Ilustracja 114: Strona WBM „Port Utilization“

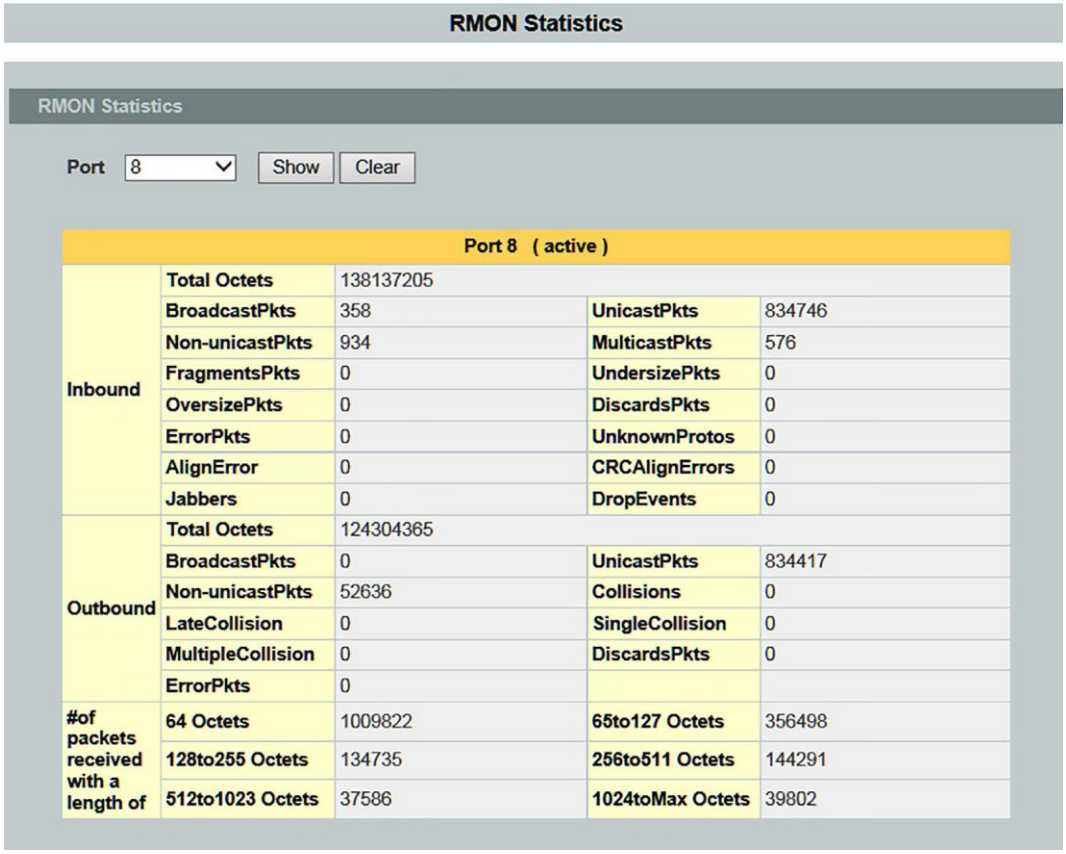
Tabela 116: Strona WBM „Port Utilization“

Port Traffic 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.

9.5.5 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 115: Strona WBM „RMON Statistics“

Tabela 117: Strona WBM „RMON Statistics“

RMON Statistics			
Parametr		**Domyślnie**	**Opis**
Port		**-**	W polu wyboru należy wybrać „-“, jeśli statystyka nie ma być wyświetlona.
		1 … 10 (12) All	W polu wyboru należy wybrać port lub wszystkie porty, dla których mają być wyświetlone statystyki RMON.
Port x (active)			
Parametr		**Domyślnie**	**Opis**
Inbound	Total Octets		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych.
	BroadcastPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów broadcast.
	UnicastPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów unicast.
	Non-unicastPkts		W tej kolumnie wyświetlana jest liczba odebranej przez port sumy pakietów broadcast i multicast.
	MulticastPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów multicast.
	FragmentiertsPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port fragmentarycznych pakietów danych.
	UndersizePkts		W tej kolumnie wyświetlana jest liczba odebranych przez port zbyt małych pakietów danych.
	OversizePkts		W tej kolumnie wyświetlana jest liczba odebranych przez port zbyt dużych pakietów danych.
	DiscardsPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych, które zostały odrzucone.
	ErrorPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port błędnych pakietów danych.
	UnknownPkts		W tej kolumnie wyświetlana jest liczba odebranych przez port pakietów danych, które zawierały jako cel nieznany lub nieobsługiwany protokół.
	AlignError		W tej kolumnie wyświetlana jest liczba odebranych pakietów danych, dla których łączna liczba bitów ramki nie jest podzielna przez 8.
	CRCAlignErrors		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“.
	DropEvents		W tej kolumnie wyświetlana jest liczba odrzuconych pakietów danych.

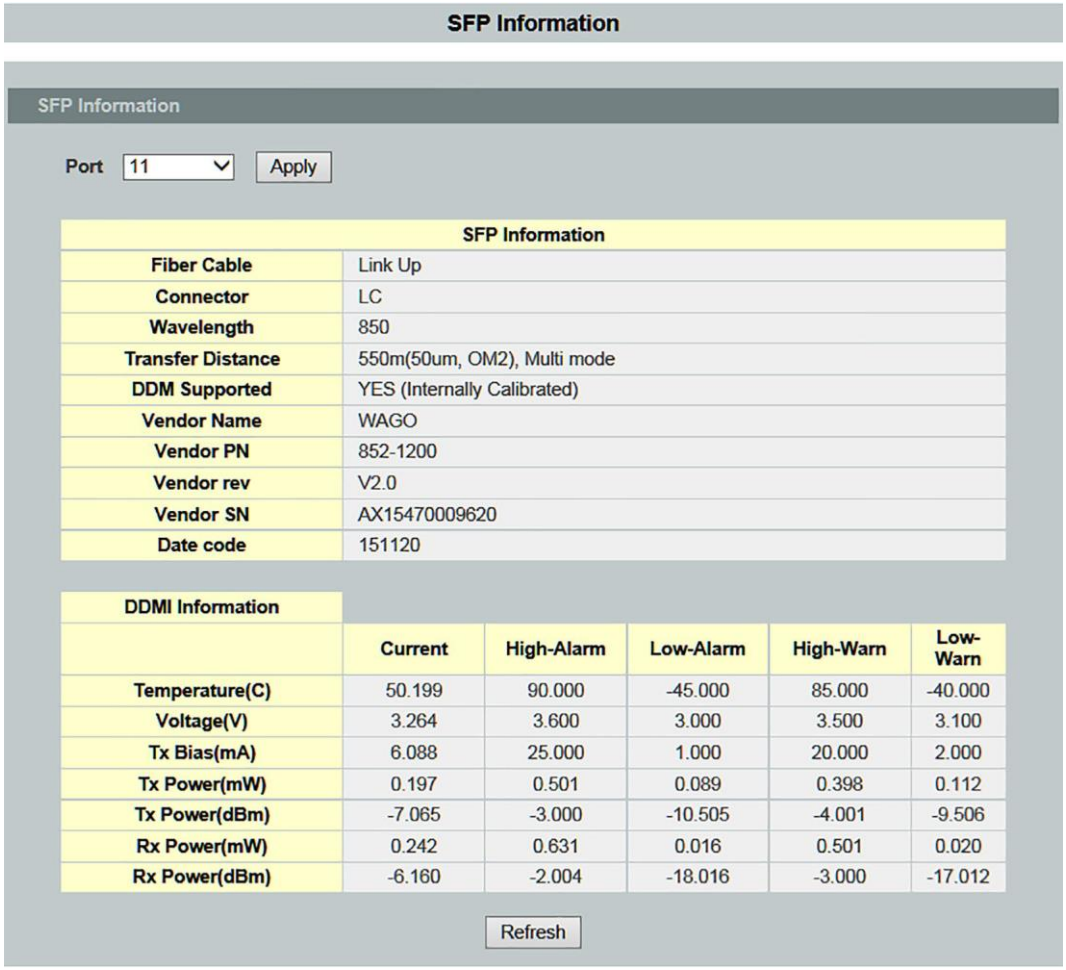
Tabela 117: Strona WBM „RMON Statistics“

Outbound	Total Octets		W tej kolumnie wyświetlana jest liczba wysłanych przez port pakietów danych.
	BroadcastPkts		W tej kolumnie wyświetlana jest liczba wysyłanych przez port pakietów broadcast.
	UnicastPkts		W tej kolumnie wyświetlana jest liczba wysyłanych przez port pakietów unicast.
	Non-unicastPkts		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.
	LateCollision		W tej kolumnie wyświetlana jest liczba pakietów danych, które mają być wysłane, miały kolizję lub zostały odrzucone.
	SingleCollision		W tej kolumnie wyświetlana jest liczba pojedynczych kolizji wysłanych pakietów danych.
	MultipleCollision		W tym polu wyświetlana jest liczba wielokrotnych kolizji wysłanych pakietów danych.
	DiscardsPkts		W tej kolumnie wyświetlana jest liczba pakietów danych wysłanych przez port, które zostały odrzucone.
	ErrorPkts		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 tej kolumnie wyświetlana jest liczba odebranych pakietów danych, które miały długość większą niż 1024 oktety.

9.5.6 SFP Information

Wskazówka

Dodatkowa informacja
Więcej informacji o „SFP“ (Small Form-factor Pluggable) można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 116: Strona WBM „SFP Information“

Tabela 118: Strona WBM „SFP Information“

SFP Information		
Parametr	**Domyślnie**	**Opis**
Port	**-**	W polu wyboru należy wybrać „-“, gdy nie jest wetknięty moduł SFP.
	9, 10, (11, 12)	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.
Wavelenght		W tym polu wyświetlana jest długość fali.
Transfer Distance		W tym polu wyświetlana jest odległość, na jaką wykonany ma być transfer.
DDM Supported		W tej kolumnie wyświetlana jest informacja, czy moduł SFP obsługuje DDM („**D**ynamic **D**evice **M**apping“).
Vendor Name		W tej kolumnie wyświetlana jest nazwa dostawcy SFP.
Vendor PN		W tym polu wyświetlany jest numer części.
Vendor rev		W tym polu wyświetlana jest wersja numeru części.
Serial Number		W tym polu wyświetlany jest numer serii (ASCII).
Date Code		W tym polu wyświetlana jest data wersji.

Tabela 118: Strona WBM „SFP Information“

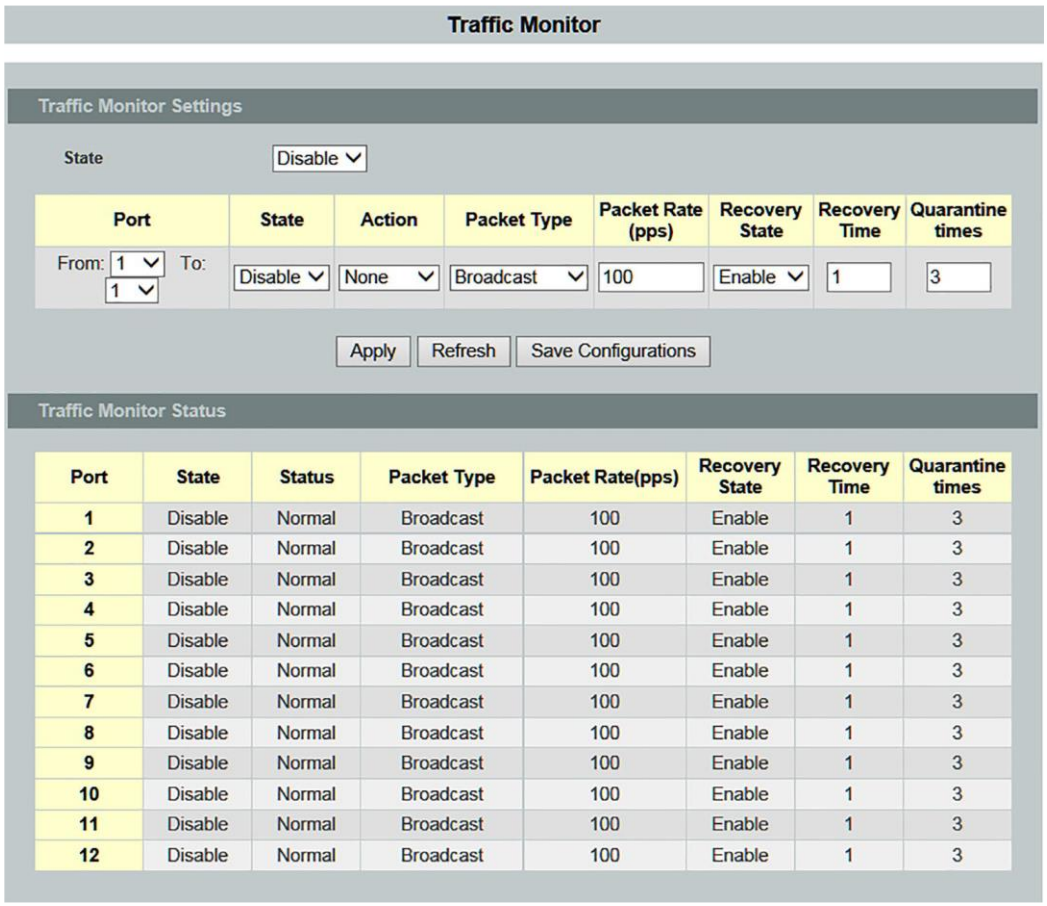
DDMI Information		
Parametr	**Domyślnie**	**Opis**
Current		W tej kolumnie wyświetlane są następujące aktualne wartości: - temperatura (C) - napięcie (V) - Tx-bias (mA) - Tx-power (mW) - Tx-power (dBm) - Rx-power (mW) - Rx-power (dBm)
High-Alarm		W tej kolumnie wyświetlane są wartości „Alarm High“ dla poniższych wartości: - temperatura (C) - napięcie (V) - Tx-bias (mA) - Tx-power (mW) - Tx-power (dBm) - Rx-power (mW) - Rx-power (dBm)
Low-Alarm		W tej kolumnie wyświetlane są wartości „Alarm Low“ dla poniższych wartości: - temperatura (C) - napięcie (V) - Tx-bias (mA) - Tx-power (mW) - Tx-power (dBm) - Rx-power (mW) - Rx-power (dBm)
High-Warn		W tej kolumnie wyświetlane są wartości „Warning High“ dla poniższych wartości: - temperatura (C) - napięcie (V) - Tx-bias (mA) - Tx-power (mW) - Tx-power (dBm) - Rx-power (mW) - Rx-power (dBm)
Low-Warn		W tej kolumnie wyświetlane są wartości „Warning Low“ dla poniższych wartości: - temperatura (C) - napięcie (V) - Tx-bias (mA) - Tx-power (mW) - Tx-power (dBm) - Rx-power (mW) - Rx-power (dBm)

9.5.7 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 117: Strona WBM „Traffic Monitor“

Tabela 119: 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 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 polu edycji należy wpisać czas „Recovery“ dla „Traffic Monitor“ na tych portach. Właściwy zakres: 1 … 60 minut
Quarantine Time		**3**	W polu edycji należy wpisać wartość „Quarantine Time“ dla „Traffic Monitor“.
Traffic Monitor Status			
Parametr		**Domyślnie**	**Opis**
Port		1 … 10 (12)	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		1 … 60	W tej kolumnie wyświetlany jest wybrany „Recovery Time“.

Tabela 119: Strona WBM „Traffic Monitor”

Quarantine Time	3	W tej kolumnie wyświetlany jest wybrany „Quarantine Time“.

9.6 Management

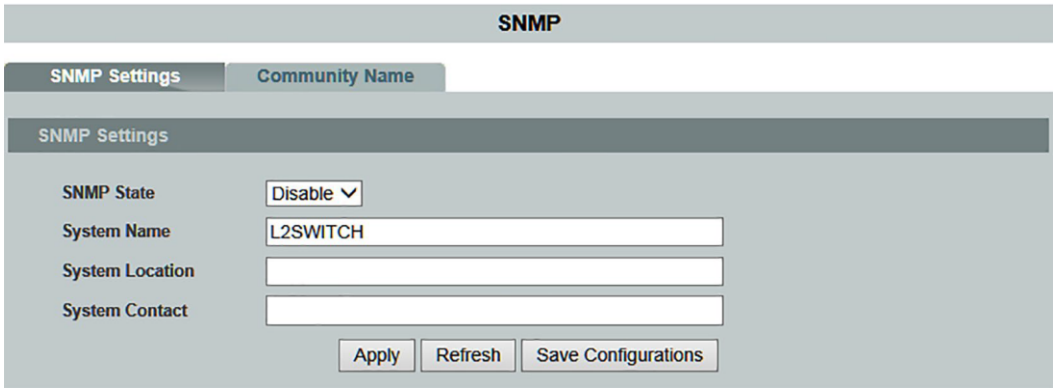
9.6.1 SNMP

9.6.1.1 SNMP

Wskazówka

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

9.6.1.1.1 SNMP Settings

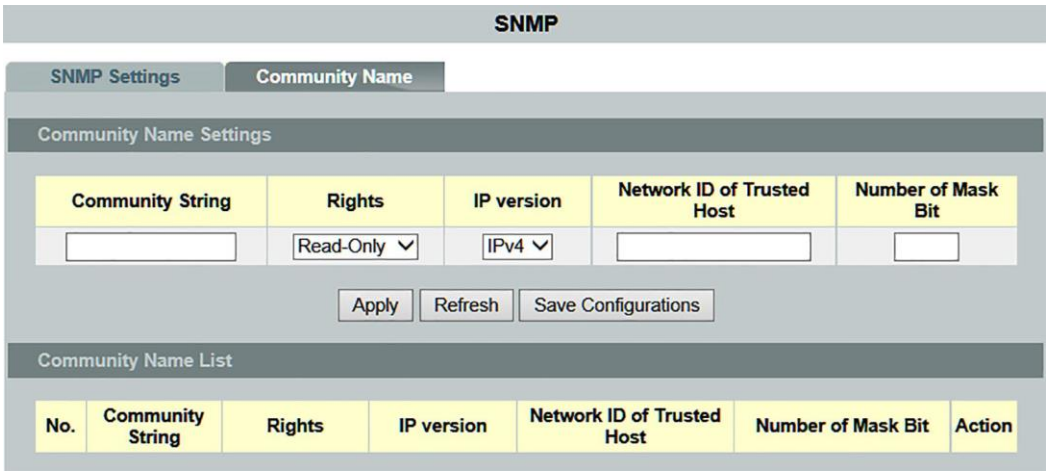


Ilustracja 118: Strona WBM „SNMP“ – zakładka „SNMP Settings“

Tabela 120: 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.

9.6.1.1.2 Community Name



Ilustracja 119: Strona WBM „SNMP“ – zakładka „Community Name“

Tabela 121: Strona WBM „SNMP“ – zakładka „Community Name“

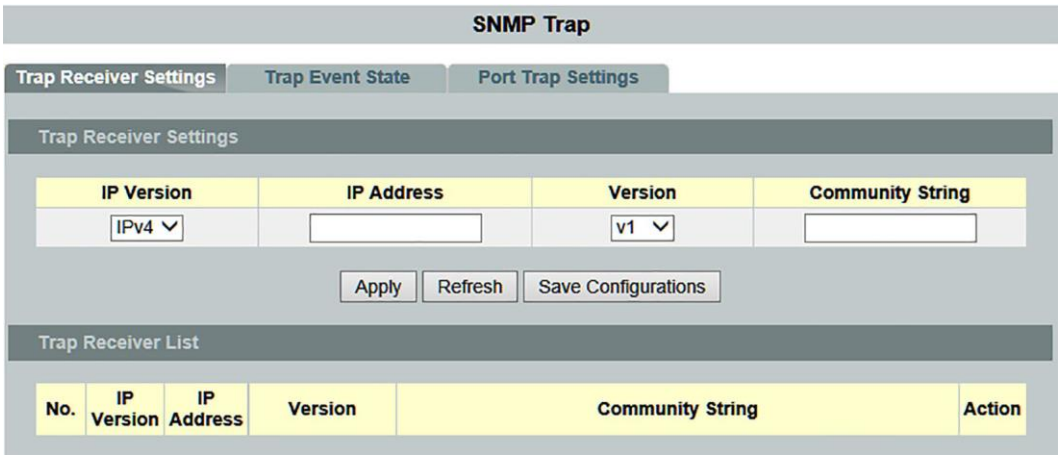
Community Name Settings		
Parametr	**Domyślnie**	**Opis**
Community String		GW polu edycji należy wpisać „Community String“, funkcjonujący jako hasło dla żądań stacji zarządzającej.
Rights	**Read Only**	W polu wyboru należy wybrać „Read Only“, aby manager SNMP mógł wykorzystać te stringi w celu otrzymywania informacji od switcha.
	Read/ Write	W polu wyboru należy wybrać „Read/Write“, aby manager SNMP mógł wykorzystać te stringi w celu skonfigurowania ustawień switcha.
IP Version	**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.
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 „Community String“ SNMP. Jest on elementem tekstowym, funkcjonującym jako hasło.
Rights	Read Only, Read/ Write	W tej kolumnie wyświetlane są uprawnienia dla „SNMP-Community-String”.
IP Version	IPv4 IPv6	W tym polu wyświetlany jest wybrany typ IP.
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”.

9.6.1.2 SNMP Trap

Wskazówka

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

9.6.1.2.1 Trap Receiver Settings

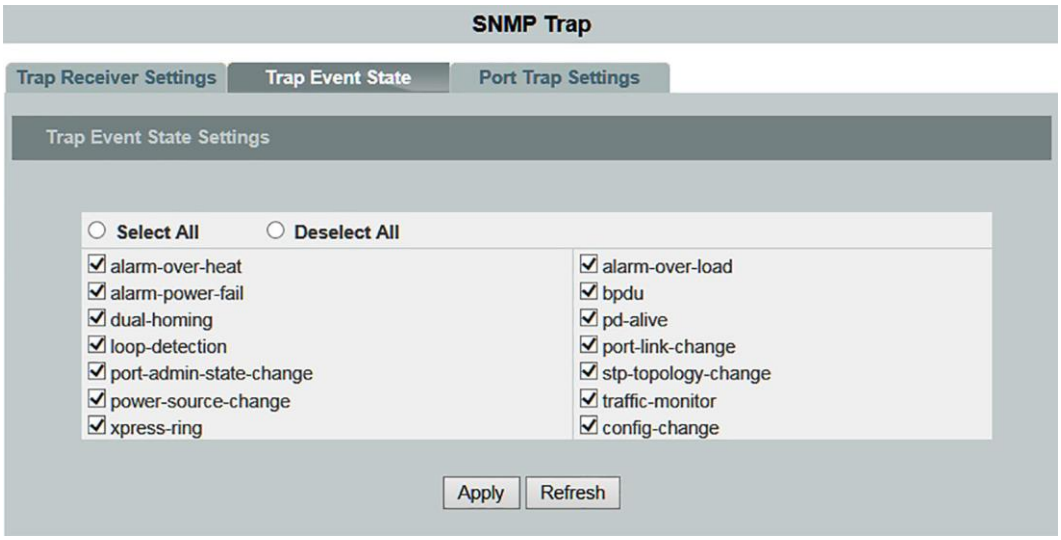


Ilustracja 120: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“

Tabela 122: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“

Trap Receiver Settings		
Parametr	**Domyślnie**	**Opis**
IP Version	**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.
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 Version	IPv4 IPv6	W tej kolumnie wyświetlany jest typ IP.
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]**.

9.6.1.2.2 Trap Event State

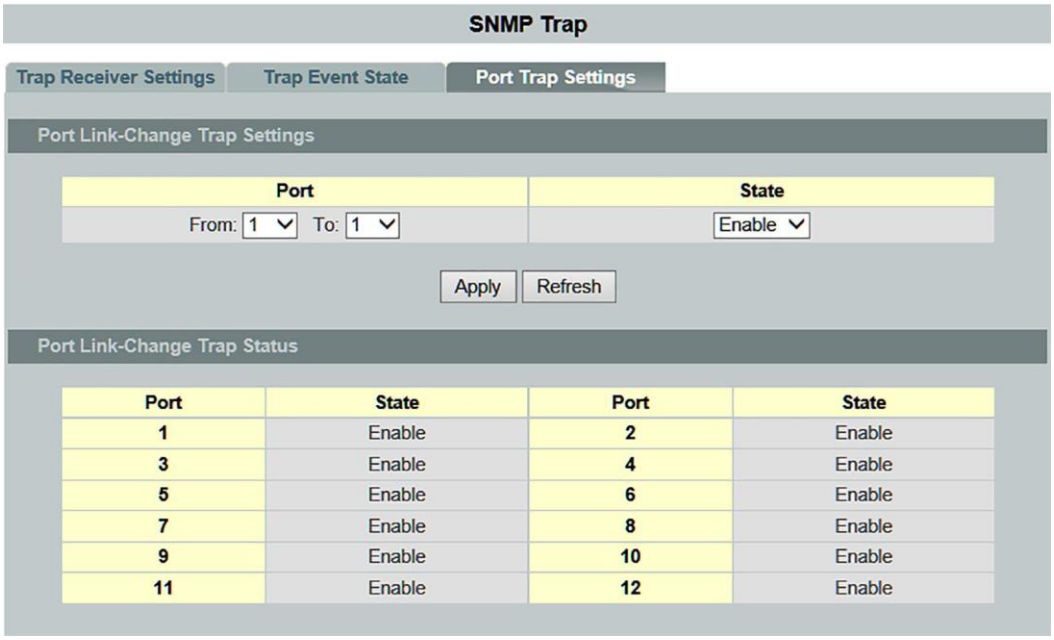


Ilustracja 121: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“

Tabela 123: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“

Trap Event State Settings		
Parametr	**Wartość standardowa**	**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)
xpress-ring	☑	Aktywuje / dezaktywuje trap SNMP, gdy port zablokowany jest przez „Xpress Ring“.
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.
pd-alive	☑	Aktywuje / dezaktywuje trap SNMP, gdy urządzenie PD nie ma odpowiedzi.
port-link-change	☑	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 jest zablokowany przez „Traffic Monitor”.
config-change	☑	Aktywuje / dezaktywuje trap SNMP, gdy konfiguracja zostaje zmieniona.

9.6.1.2.3 Port Trap Settings



Ilustracja 122: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“

Tabela 124: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“

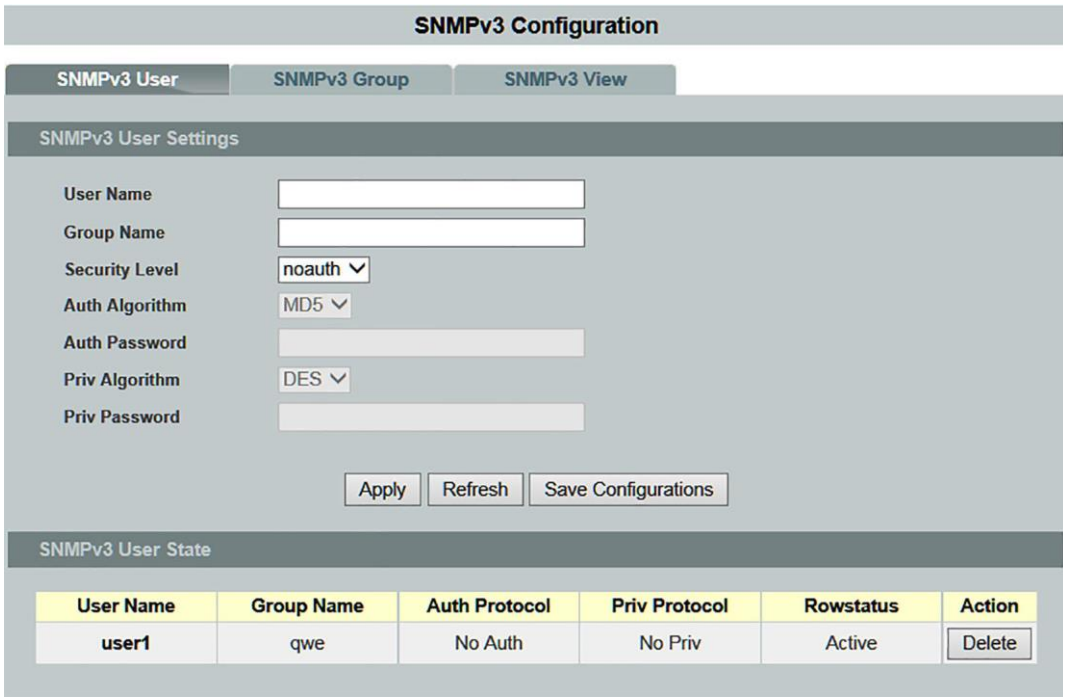
Port Link-Change Trap Settings			
Parametr		**Domyślnie**	**Opis**
Port	From:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
	To:	**1**	W polu wyboru należy wybrać port lub zakres portów, który ma być skonfigurowany.
State		**Enable**	W polu wyboru należy wybrać „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.

9.6.1.3 SNMPv3 Configuration

9.6.1.3.1 SNMPv3 User

Wskazówka

Dodatkowa informacja
Więcej informacji o „SNMPv3” można znaleźć w rozdziale „Opis funkcji”.

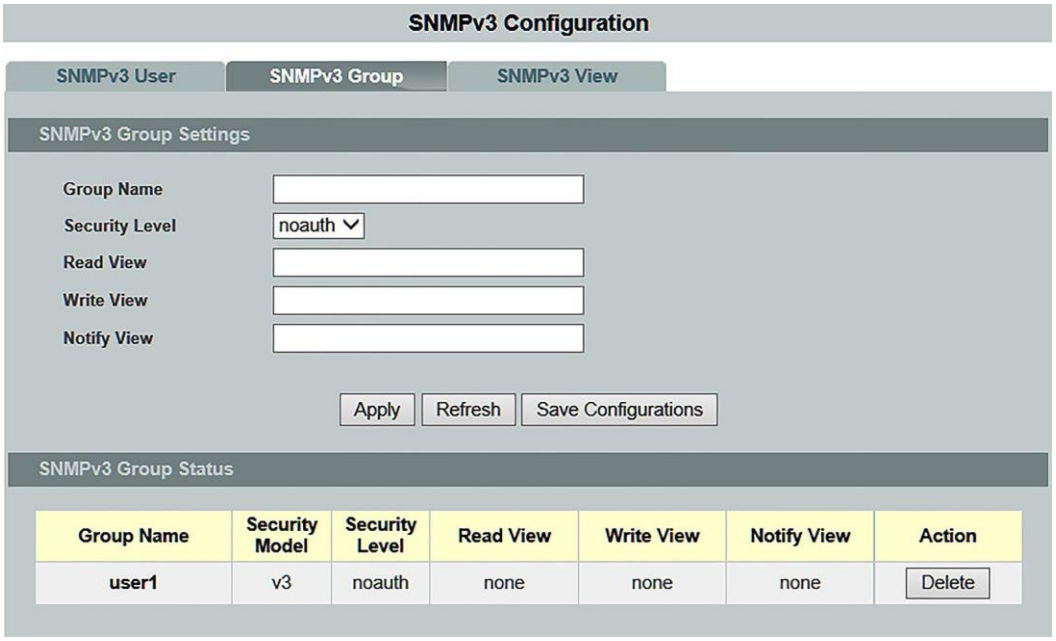


Ilustracja 123: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“

Tabela 125: 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 Algorithmus“ i „Priv Algorithmus“.
	auth	Gdy w polu wyboru wybrana jest opcja „auth“, istnieje możliwość zmiany „Auth Algorithmus“ i „Auth Password“.
	priv	Gdy w polu wyboru wybrana jest opcja „priv“, istnieje możliwość zmiany „Auth Algorithmus“, „Auth Password“, „Priv Algorithmus“ i „Priv Password“.
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 Algorithmus“.
Priv Protocol		W tej kolumnie wyświetlany jest wybrany „Priv Algorithmus“.
Rowstatus		W tej kolumnie wyświetlany jest „Rowstatus“.
Action		Aby usunąć daną pozycję, należy kliknąć **[Delete]**.

9.6.1.3.2 SNMPv3 Group

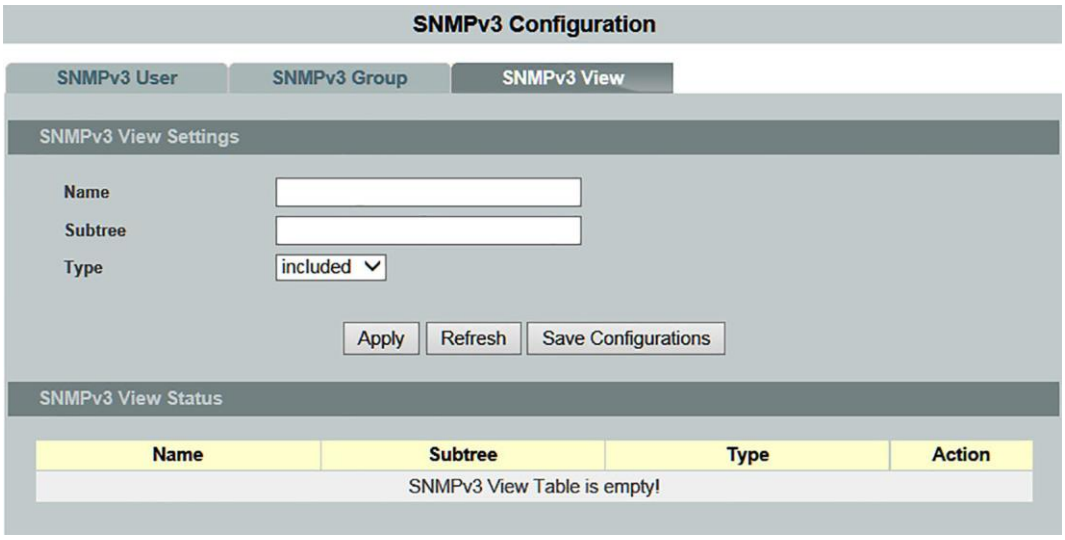


Ilustracja 124: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“

Tabela 126: 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 poziom 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]**.

9.6.1.3.3 SNMPv3 View



Ilustracja 125: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“

Tabela 127: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“

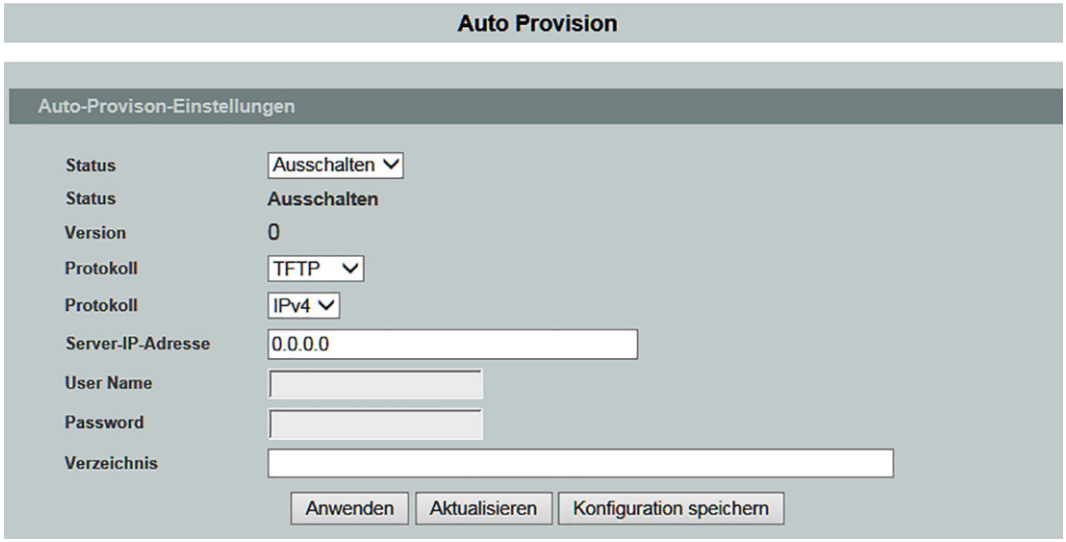
SNMPv3 View Settings		
Parametr	**Domyślnie**	**Opis**
Name		W polu edycji należy wpisać nazwę dla „SNMPv3 View“.
Subtree		W polu edycji należy wpisać nazwę dla „Subtree“.
Type	**Inserted**	Gdy w polu wyboru wybrana jest opcja „Inserted“, dodane zostaje „Subtree“.
	Removed	Gdy w polu wyboru wybrana jest 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]**.

9.6.2 Auto Provision

Wskazówka

Dodatkowa informacja

Więcej informacji o „Auto Provision“ można znaleźć w rozdziale „Opis funkcji“.



Ilustracja 126: Strona WBM „Auto Provision“

Tabela 128: Strona WBM „Auto Provision“

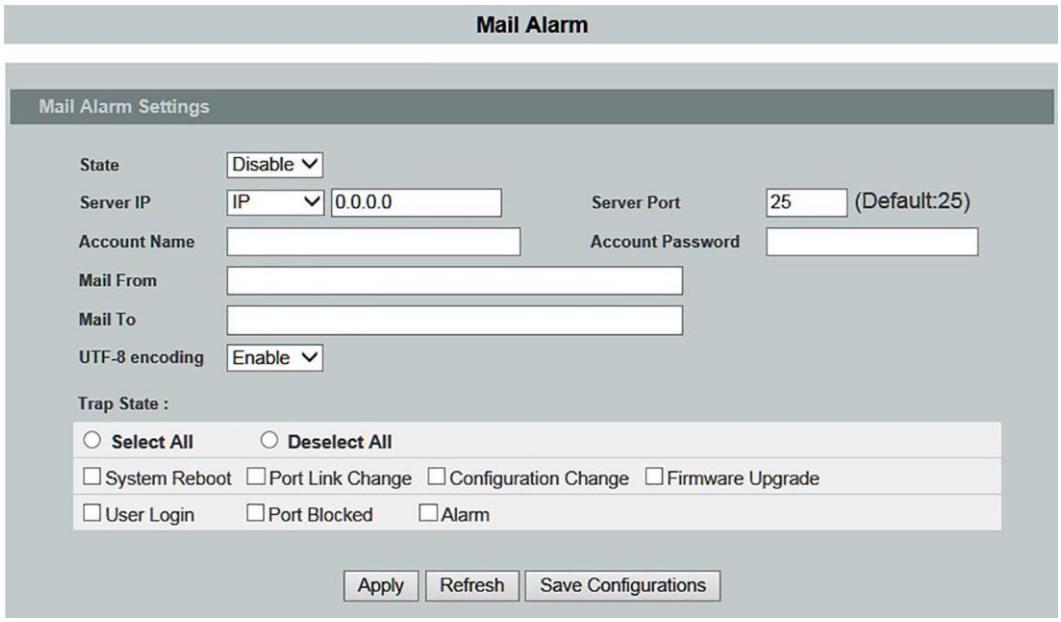
Auto Provision Settings		
Parametr	**Domyślnie**	**Opis**
Status	**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować w switchu funkcję „Auto Provision“.
	Enable	W polu wyboru należy wybrać „Enable“, aby aktywować w switchu funkcję „Auto Provision“.
Status	**Disable**	W tym polu wyświetlany jest status „Auto Provision“.
Version	**0**	W tym polu wyświetlana jest wersja.
Protocol	**FTP**	W polu wyboru należy wybrać „FTP“ („**F**ile **T**ransfer **P**rotocol“), jeśli ten typ ma być wybrany jako serwer „Auto Provision“.
	TFTP	W polu wyboru należy wybrać „TFTP“ („**T**rivial **F**ile **T**ransfer **P**rotocol“), jeśli ten typ ma być wybrany jako serwer „Auto Provision“.
	HTTP	W polu wyboru wybierz „HTTP” („**H**yper**t**ext **T**ransfer **P**rotocol”), jeśli ten typ ma być wybrany jako serwer „Auto Provision”.
Server IP		W polu edycji należy wpisać adres IP maski podsieci switcha, używając zapisu z kropkami.
User Name		W polu edycji należy wpisać nazwę serwera FTP.
Password		W polu edycji należy wpisać hasło do serwera FTP.
Folder Path		W polu edycji należy wpisać strukturę katalogów serwera FPT.

9.6.3 Mail Alarm

Wskazówka

Dodatkowa informacja

Więcej informacji o „Mail-Alarm” można znaleźć w rozdziale „Opis funkcji”.



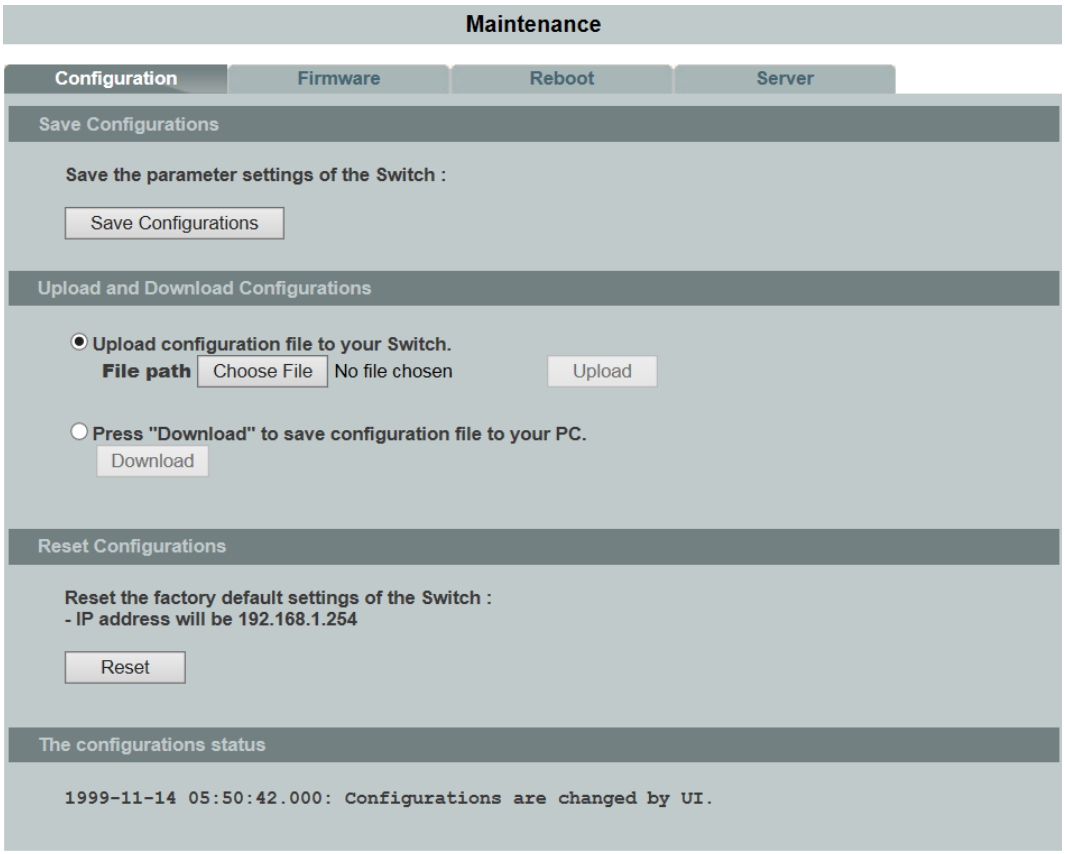
Ilustracja 127: Strona WBM „Mail Alarm“

Tabela 129: Strona WBM „Mail Alarm“

Mail Alarm Settings				
Parametr		**Domyślnie**	**Opis**	
State		**Disable**	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję „Mail Alarm“.	
		Enable	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję „Mail Alarm“.	
Server IP		**IP**	W polu wyboru należy wybrać „IP“, gdy ma być wykorzystany IP serwera pocztowego.	
		IPv6	W polu wyboru należy wybrać „IPv6“, gdy ma być wykorzystany IP serwera IPv6.	
		Domain	W polu wyboru należy wybrać „Domain“, gdy ma być wykorzystany adres domeny serwera pocztowego.	
		0.0.0.0	W polu edycji należy wpisać adres IP.	
Server Port (Default:25)		**25**	W polu edycji należy wpisać port TCP dla SMTP.	
Account Name			W polu edycji należy wpisać nazwę konta e-mail.	
Account Password			W polu edycji należy wpisać hasło konta e-mail.	
Mail From			W polu edycji należy wpisać nazwę nadawcy e-mail.	
Mail To			W polu edycji należy wpisać nazwę odbiorcy e-mail.	
Trap State	Select All	○	○	Żaden port nie jest wybrany do wysłania trapów o zdarzeniach.
			◉	Wszystkie porty są wybrane do wysłania trapów o zdarzeniach.
	Disable All	○	○	Żaden port nie jest dezaktywowany do wysłania trapów o zdarzeniach.
			◉	Wszystkie porty są dezaktywowane do wysłania trapów o zdarzeniach.
	System Restart	☐	☐	Port nie jest aktywowany.
			☑	Port jest aktywowany.
	Port Link Change	☐	☐	Stan „Port Link Change“ jest dezaktywowany.
			☑	Stan „Port Link Change“ jest aktywowany.
	Configuration Change	☐	☐	Stan „Configuration Change“ jest dezaktywowany.
			☑	Stan „Configuration Change“ jest aktywowany.
	Firmware Upgrade	☐	☐	Stan „Firmware Upgrade“ jest dezaktywowany.
			☑	Stan „Firmware Upgrade“ jest aktywowany.
	User Login	☐	☐	Stan „User Login“ jest dezaktywowany.
			☑	Stan „User Login“ jest aktywowany.
	Port Blocked	☐	☐	Stan „Port Blocked“ jest dezaktywowany.
			☑	Stan „Port Blocked“ jest aktywowany.
	Alarm	☐	☐	Stan „Alarm“ jest dezaktywowany.
			☑	Stan „Alarm“ jest aktywowany.

9.6.4 Maintenance

9.6.4.1 Configuration



Ilustracja 128: 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 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.

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.

Reset Configurations

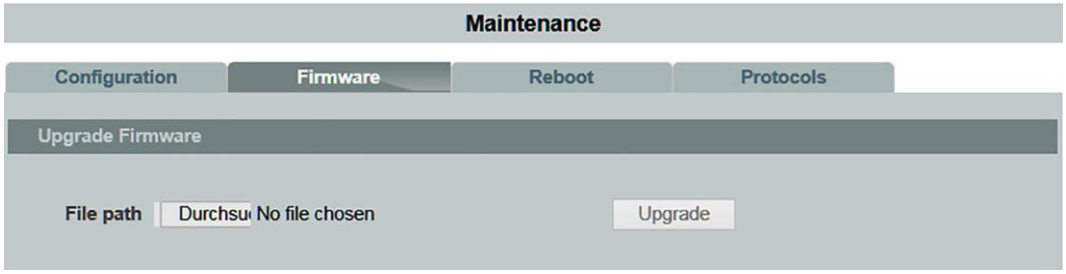
- Kliknij przycisk **[Reset]**, aby cofnąć konfigurację switcha do ustawień fabrycznych.

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 te default“. The configurations are default values.“.

9.6.4.2 Firmware



Ilustracja 129: Strona WBM „Maintenance“ – zakładka „Firmware“

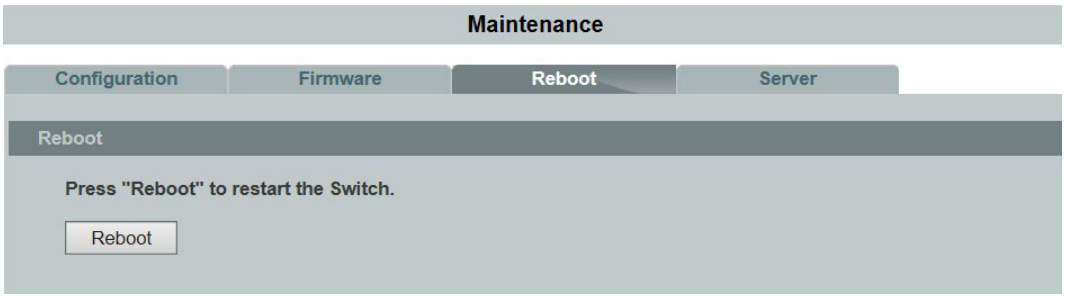
Firmware Upgrade

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

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

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

9.6.4.3 Reboot



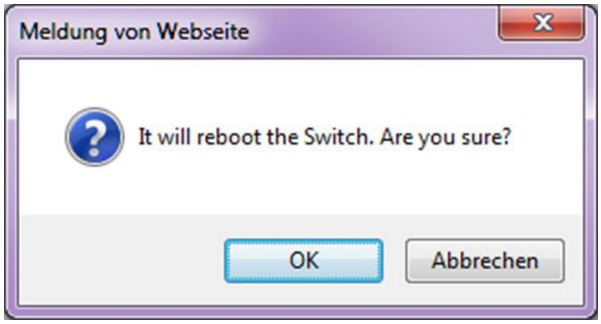
Ilustracja 130: Strona WBM „Maintenance“ – zakładka „Reboot“

Reboot

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

W celu przeprowadzenia restartu switcha należy wykonać następujące kroki:

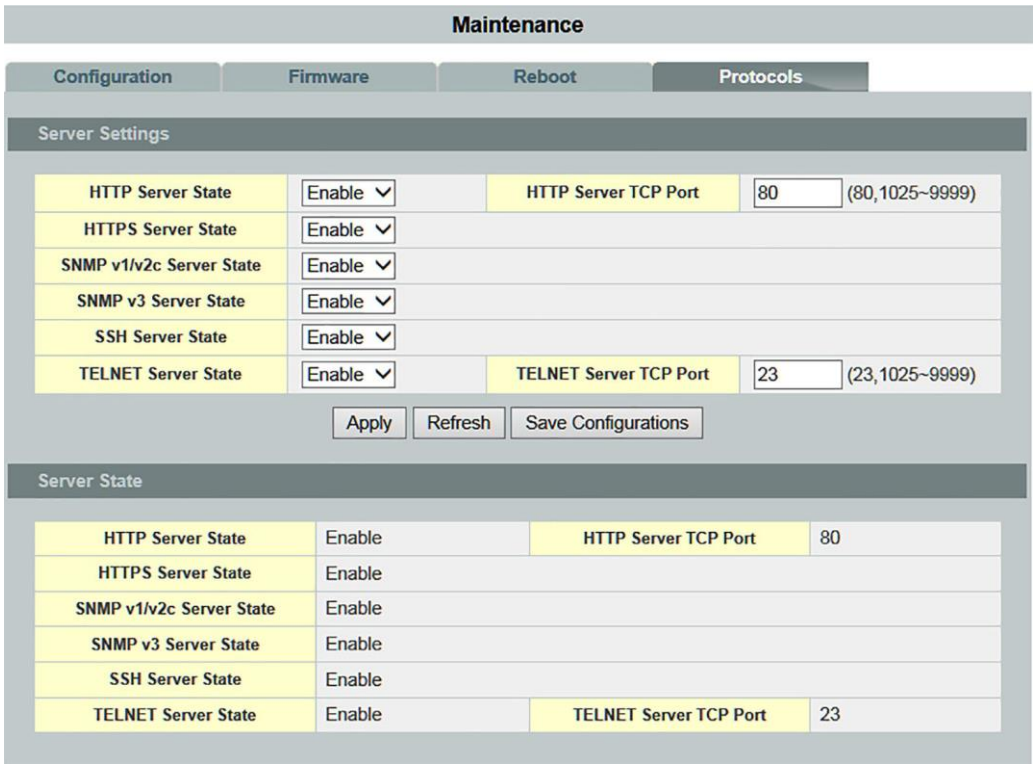
1. W menu „Reboot“ kliknij przycisk **[Reboot]**. Pojawi się widoczne niżej okno.



Ilustracja 131: 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.

9.6.4.4 Protocols



Ilustracja 132: Strona WBM „Maintenance“ – zakładka „Protocols“

Tabela 130: Strona WBM „Maintenance“ – zakładka „Protocols“

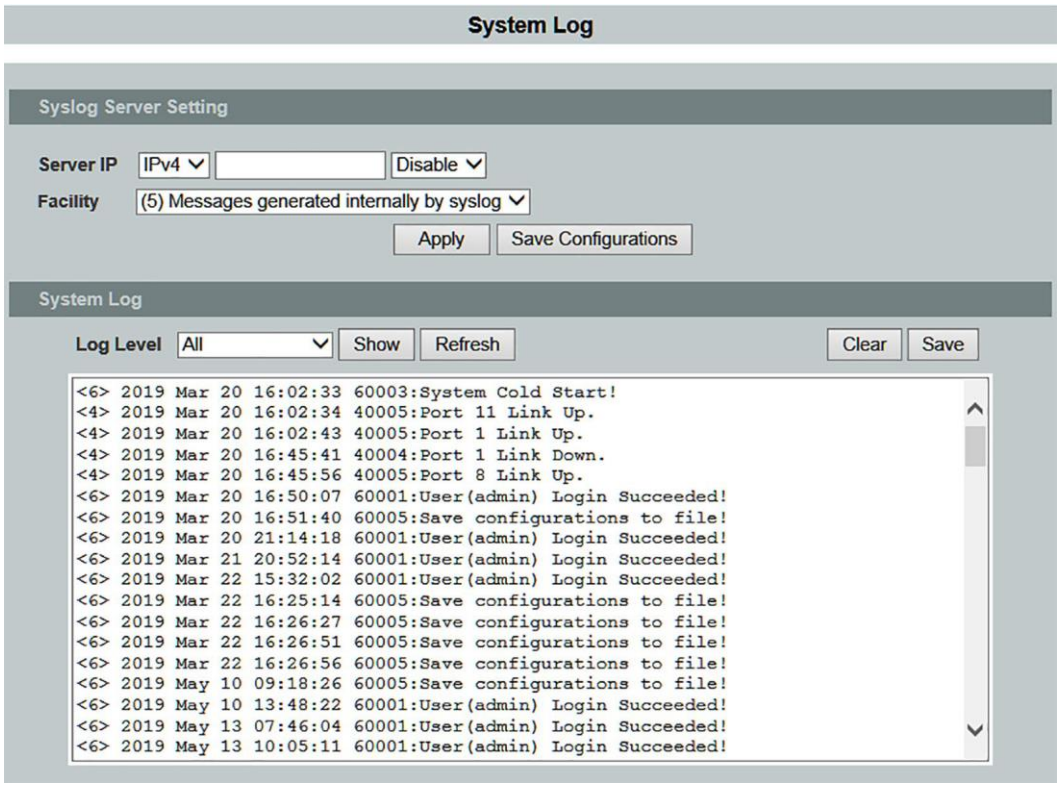
Server Settings		
Parametr	**Domyślnie**	**Opis**
HTTP Server State	**Enable**	Należy wybrać „Enable“, aby aktywować „HTTP Server“.
	Disable	Należy wybrać „Disable“, aby dezaktywować „HTTP Server“.
HTTP Server TCP Port (80, 1025~9999)	**80** 1025 … 9999	W polu edycji należy wpisać „HTTP Server TCP Port“.
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“.

9.6.5 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.

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



Ilustracja 133: Strona WBM „System Log“

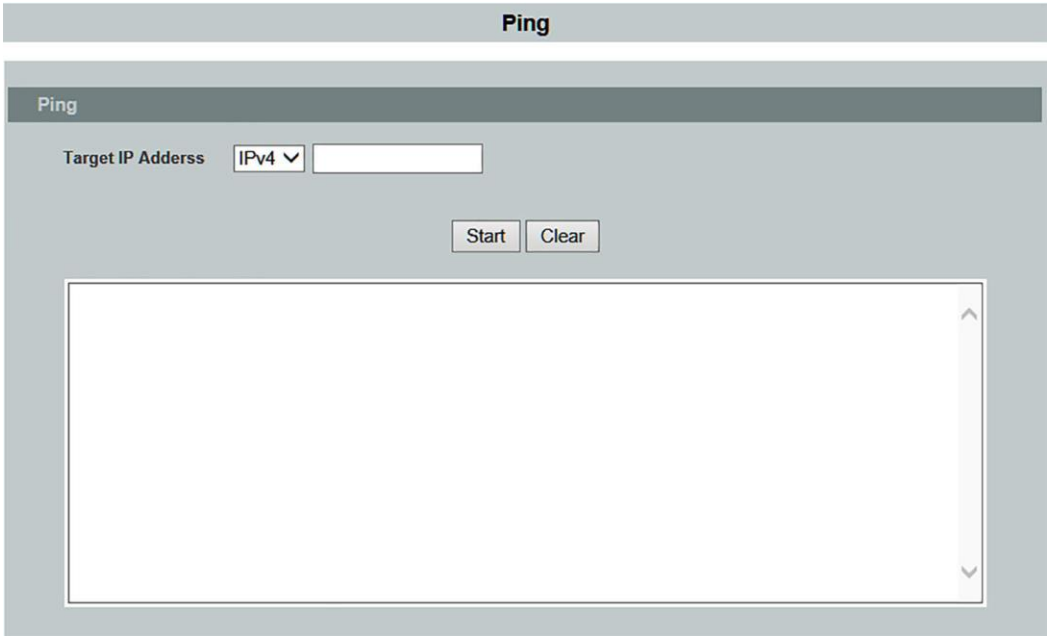
Tabela 131: Strona WBM „System Log“

Syslog Server Settings		
Parametr	**Domyślnie**	**Opis**
Server IP	**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“.
Facility	(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.

9.6.6 Ping

Wskazówka

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



Ilustracja 134: Strona WBM „Ping“

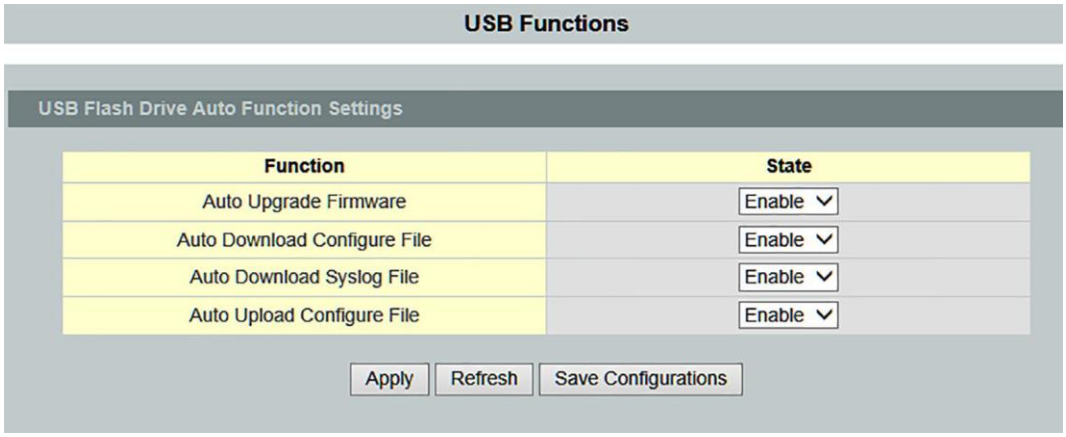
Tabela 132: Strona WBM „Ping“

Ping		
Parametr	**Domyślnie**	**Opis**
Target 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.

9.6.7 USB Funktions

Złącze USB switcha może służyć do realizacji następujących funkcji:

- ładowanie oprogramowania firmware
- zapisywanie pliku konfiguracyjnego
- zapisywanie pliku syslog
- ładowanie pliku konfiguracyjnego



Ilustracja 135: Strona WBM „USB Functions“

Tabela 133: Strona WBM „USB Functions“

USB Flash Drive Auto Funktion Settings		
Parametr	**Domyślnie**	**Opis**
Function		W tej kolumnie można wybrać funkcję USB.
Auto Upgrade Firmware Auto Download Configure File Auto Download Syslog File Auto Upload Configure File	**Enable**	W polu wyboru należy wybrać „Enable“, aby aktywować funkcję.
	Disable	W polu wyboru należy wybrać „Disable“, aby dezaktywować funkcję.

9.6.8 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.

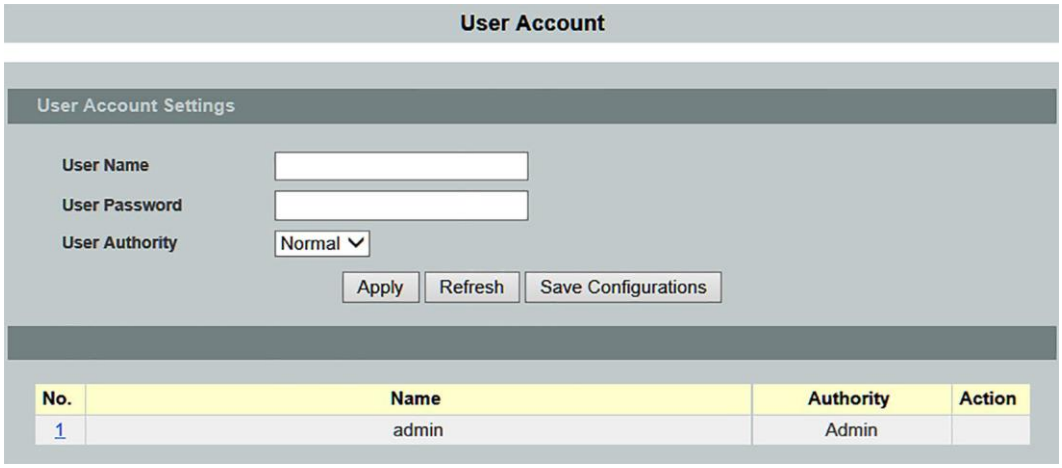
Uprawnienia użytkowników

Switch wspiera dwa rodzaje kont użytkownika:

Domyślne konta użytkownika zawierają następujące informacje:
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 136: Strona WBM „User Account”

Tabela 134: Strona WBM „User Account”

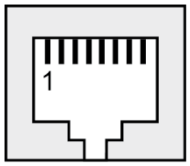
User Account Settings		
Parametr	**Domyślnie**	**Opis**
User Name		W polu edycji należy wpisać nową nazwę użytkownika lub zmodyfikować już istniejącą.
User Passwort		W polu edycji należy wpisać nowe hasło lub zmodyfikować już istniejące. Można wpisać 32 znaki alfanumeryczne lub cyfry.
User Authority		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.

Parametr	**Domyślnie**	**Opis**	
No.		W tej kolumnie wyświetlany jest numer indeksu wpisu.	
Name		W tej kolumnie wyświetlana jest nazwa konta użytkownika.	
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.

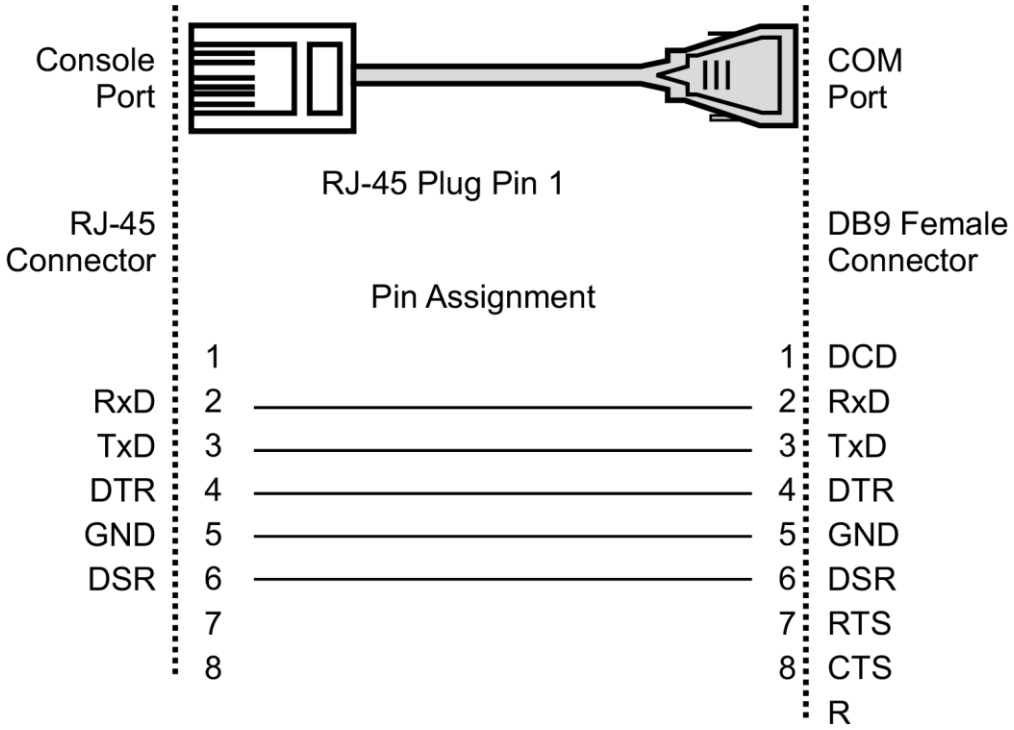
10 Załącznik

10.1 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 137: Obłożenie zacisków RJ-45



Ilustracja 138: Obłożenie zacisków RJ-45 do DB9

10.2 Przewód RJ-45

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

Tabela 135: Przewód RJ-45

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

Wskazówka

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

10.3 Configuring in the Command Line Interface (CLI)

10.3.1 System Status

10.3.1.1 System Information

Table 136: CLI “System Information” Configuration

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

10.3.2 Basic Settings

10.3.2.1 System

Table 137: 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”: Use the DHCP client to get an IP address from the DHCP server.
eth0	management vlan VLAN_ID	This command configures the management VLAN.
eth0	ip ipv6-addressAAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/M	This command configures a global scope of IPv6 address and subnet mask for the system.
eth0	ip ipv6-addressdefault-gatewayAAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH	This command configures a default gateway for the system.
eth0	ip ipv6-dhcp client (disable|enable|renew)	This command configures a DHCPv6 client function for the system.

10.3.2.1.1 Jumbo Frame

Table 138: 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.
configure	interface IFNAME	This command enters the interface configure node.
interface	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes of frame size.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes of frame size.

10.3.2.1.2 SNTP

Table 139: 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 ntp-server domain-name STRING	This command sets the domain names of the time server.
configure	time timezone STRING	This command sets the time difference between UTC (formerly GMT) and the time zone. Valid range: −1200 … +1200

Example

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

L2SWITCH(config)*#time timezone +0800*

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

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

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

10.3.2.1.3 Management Host

Table 140: CLI “Management Host” Configuration

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

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#interface eth0*

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

10.3.2.2 MAC Management

Table 141: 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*

10.3.2.2.1 Blackhole MAC

Table 142: CLI “Blackhole MAC” Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current rejected MAC address only.
configure	mac-address-table refusal MACADDR vlan VLANID	This command configures the rejection of a MAC address in a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures the rejection of a MAC address.

Example

L2SWITCH(config)*#mac-address-table refusal 00:11:22:33:44:55*

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

10.3.2.3 Port Mirroring

Table 143: 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 3-10 mode both*

10.3.2.4 Port Settings:

Table 144: 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	This command diagnostics the Ethernet cable and shows the broken distance.
interface	clean cable-test result	This command cleans the test result of the Ethernet cable test.
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 gil/0/1*

L2SWITCH(config-if)*#speed auto*

10.3.3 Advanced Settings

10.3.3.1 Bandwidth Control

10.3.3.1.1 QoS

Table 145: 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.

10.3.3.1.2 Rate Limitation

Table 146: 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*

10.3.3.1.2.1 Storm Control

Table 147: 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*

10.3.3.2 IGMP Snooping

Table 148: 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.
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.

if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the ports are (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. Default: 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*

10.3.3.2.1 IGMP Snooping Querier♠

Table 149: 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.

10.3.3.2.2 IGMP Snooping Filtering

Table 150: 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.

10.3.3.2.3 MVR

Table 151: CLI “MVR” Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLANID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current “IGMP Snooping” configurations.
configure	mvr VLANID	This command creates the MVR configurations for the specific VLAN.
configure	no mvr VLANID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command creates a group configuration for the MVR.
MVR	no group NAME	This command deletes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic|compatible)	This command configures the mode for the MVR. - Dynamic: Sends “IGMP reports” to all MVR source ports in the multicast VLAN. - Compatibility: The switch does not send any “IGMP Reports”.
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port or receiver port range. Normally, the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the list of receiver ports.
MVR	source-port PORTLIST	This command sets the source port or source port range. Normally, the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the list of source ports.
MVR	tagged PORTLIST	This command assigns a tagged port or port range. The same applies to VLAN tagged ports.
MVR	no tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).
MVR	priority-override (disable|enable)	This command enables/disables the multicast priority override.

10.3.3.2.4 Multicast Address

Table 152: 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.

10.3.3.3 VLAN

10.3.3.3.1 Port Isolation

Table 153: 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*

10.3.3.3.2 VLAN Settings

Table 154: 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 154: 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*

10.3.3.3.3 GARP/GVRP

Table 155: CLI “GARP/GVRP” Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations for one port or all ports.
enable	show garp timer	This command displays the timers for GARP.
configure	gvrp (disable|enable)	This command disables/enables GVRP on the switch.
configure	no gvrp configuration	This command resets the GVRP configuration to the default setting.
interface	gvrp (disable|enable)	This command disables/enables GVRP on a specific port.
interface	gvrp registration (normal|forbidden)	This command configures the registration mode for GVRP on a specific port.
interface	no gvrp configuration	This command resets the GVRP configuration for a specific port to the default setting.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the “Join Time,” “Leave Time” and “Leaveall Time” for GVRP on a specific port.
interface	no garp time	This command resets the Join, Leave and Leave all times for GVRP on a specific port to the default settings.

10.3.3.3.4 IP Subnet VLAN

Table 156: CLI “IP Subnet VLAN” Configuration

Node	Command	Description
enable	show ip-subnet-vlan	This command displays the all of the IP subnet vlan configurations.
configure	ip-subnet-vlan ip IPADDR mask IPADDR vlan <1-4094> priority <0-7>	This command creates an IP subnet vlan entry with the IP address, subnet mask, vlan and priority.
configure	no ip-subnet-vlan ip IPADDR	This command deletes an IP subnet vlan entry.
configure	no ip-subnet-vlan all	This command deletes all of the IP subnet vlan entries.

Example

L2SWITCH(config)*#ip-subnet-vlan 192.168.203.1 mask 255.255.255.0 vlan2 priority 3l*

L2SWITCH#*show ip-subnet-vlan*

10.3.3.3.5 MAC VLAN

Table 157: 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-vlanall	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*

10.3.3.3.6 Protocol VLAN

Table 158: CLI “Protocol VLAN” Configuration

Node	Command	Description
enable	show protocol-vlan	This command displays the all of the protocol-vlan configurations.
configure	protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLAN ID ports PORTLISTS	This command creates a protocol-vlan entry with ethernetII frame type.
configure	protocol-vlan frame-type nonLLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with nonLLC-SNAP frame type.
configure	protocol-vlan frame-type LLC-SNAP vlan VLAN ID ports PORTLISTS	This command creates a protocol-vlan entry with LLC-SNAP frame type.
configure	no protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLAN ID	This command deletes a protocol-vlan entry with ethernetII frame type.
configure	no protocol-vlan frame-type nonLLC-SNAP vlan VLAN ID	This command deletes a protocol-vlan entry with nonLLC-SNAP frame type and vlan.
configure	no protocol-vlan frame-type LLC-SNAP vlan VLAN ID	This command deletes a protocol-vlan entry with LLC-SNAP frame type and vlan.
configure	no protocol-vlan all	This command deletes all of the protocol-vlan entries.

Example

L2SWITCH(config)# *protocol-vlan frame-type LLC-SNAP vlan 12 ports 1-2*

L2SWITCH(config)# *protocol-vlan frame-type ethernetII ether-type 0800 vlan 14 ports 1-2*

10.3.3.3.7 Q-in-Q

10.3.3.3.7.1 VLAN Stacking

Table 159: CLI “VLAN Stacking” Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current vlan-stacking type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
configure	vlan-stacking (disable|port-based|selective)	This command disables the vlan stacking or enable the vlan-stacking with port-based or selective on the switch.
configure	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with the name.
configure	no vlan-stacking selective-qinq STRINGS	This command removes the selective Q-in-Q profile with the name.
configure	vlan-stacking tpid-table index<2-6> value STRINGS	This command configures TPID table.
interface	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider’s VID of the specified port.
interface	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider’s VID of the specified port.
if-range	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the customer’s VLAN range on the incoming packets.
qinq	spvid VLANID	This command sets the service provider’s VLAN ID for outgoing packets in selective Q-in-Q.
qinq	priority <0-7>	This command sets priority in selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the access ports to apply the rule.
qinq	tunnel-ports PORTLISTS	This command specifies the tunnel ports to apply the rule.
qinq	end	The command exits the CLI Q-in-Q node and enters the CLI enable node.
qinq	exit	The command exits the CLI Q-in-Q node and enter the CLI configure node.

Table 159: CLI “VLAN Stacking” Configuration

Node	Command	Description
qinq	show	The command shows the current selective Q-in-Q profile configurations.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider’s VID of the specified port.
if-range	vlan-stacking tunnel-tpid index<1-6>	This command sets TPID for a Q-in-Q tunnel port.

10.3.3.4 DHCP Relay

Table 160: CLI “DHCP Relay” Configuration

Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the DHCP relay.
configure	dhcp relay (disable|enable)	This command disables/enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	This command configures the DHCP server’s IP address.
configure	no dhcp helper-address	This command removes the DHCP server’s IP address.

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)#*dhcp relay enable*

L2SWITCH(config)# *dhcp relay vlan 1*

L2SWITCH(config)# *dhcp helper-address 172.20.1.1*

10.3.3.5 DHCP Options

Table 161: CLI “DHCP Options” Configuration

Node	Command	Description
enable	show dhcp-options	This command displays the configurations and status for the DHCP option 66 and 67.
configure	dhcp-options option_66_67 (disable|enable)	This command disables/enables the DHCP option 66 and 67 on the Switch.
configure	dhcp-options option_66_67 auto-backup	This command uploads the current configurations to TFTP server. The file name is vcmsh_config_MODEL-NAME_MAC if you didn’t specifiy a filename for it.
configure	dhcp-options option_66_67 auto-backupfile FILENAME	This command configures a filename for the auto-backup function.

10.3.3.6 Dual Homing

Table 162: CLI “Dual Homing” Configuration

Node	Command	Description
enable	show dual-homing	This command displays the “Dual Homing” information.
configure	dual-homing (disable|enable)	This command disables/enables the “Dual Homing” function in the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for “Dual Homing” from the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for “Dual Homing” from the system.
configure	dual-homing secondary-channel (port|trunk) VALUE	This command configures the secondary channel for “Dual Homing” in the system. The channel can be a single port or a “Trunk Group”.
configure	no dual-homing secondary-channel	This command deletes the secondary channel for “Dual Homing” from the system.

Example

L2SWITCH(config)# *link-aggregation 1 ports 5-6*

L2SWITCH(config)# *link-aggregation 1 enable*

L2SWITCH(config)# *dual-homing primary-channel port 2*

L2SWITCH(config)# *dual-homing secondary -channel trunk 1*

L2SWITCH(config)# *dual-homing enable*

10.3.3.7 ERPS

Table 163: CLI “ERPS” Configuration

Node	Command	Description
enable	show erps	This command displays the ERPS configurations.
enable	show erps instance	This command displays the ERPS instance configurations.
enable	show erps instance INSTANCE_ID	This command displays the specific ERPS instance configurations.
configure	erps enable	This command enables the global ERPS on the Switch.
configure	no erps enable	This command disables the global ERPS on the Switch.
configure	erps ring-id VALUE	This command creates an ERPS ring and its ID and enter ERPS node.
configure	erps instance	This command enters the instance configure node.
configure	no erps ring-id VALUE	This command creates an ERPS ring and enter ERPS node to configure detail ring configurations.
erps-ring	show	This command displays the configurations of the ring.
erps-ring	control-vlan	This command configures a control-vlan for the ERPS ring.
erps-ring	guard-timer	This command configures the Guard Timer for the ERPS ring. (default:500ms)
erps-ring	holdoff-timer	This command configures the Hold-off Timer for the ERPS ring. (default:0 ms)
erps-ring	left-port PORTID type [owner|neighbor|normal]	This command configures the left port and type for the ERPS ring.
erps-ring	mel VALUE	This command configures a Control MEL for the ERPS ring.
erps-ring	name STRING	This command configures a name for the ERPS ring.
erps-ring	revertive	This command configures the revertive mode for the ERPS ring.
erps-ring	no revertive	This command configures then on-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner|neighbor|normal]	This command configures the right port and type for the ERPS ring.
erps-ring	ring enable	This command enables the ring.
erps-ring	no ring enable	This command disables the ring.
erps-ring	version	This command configures a version for the ERPS ring.
erps-ring	wtr-timer	This command configures the WTR Timer for the ERPS ring. (default: 5 minutes)
config-erps-inst	instance INSTANCE_ID control-vlan VLAN_ID data-vlan VLAN_ID	This command configures a new instance and specifies its control vlan and data vlan.
config-erps-inst	no instance INSTANCE_ID	This command removes an instance.
config-erps-inst	show	This command displays all of the instance configurations.

10.3.3.8 Link Aggregation

Table 164: CLI “Link Aggregation” Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current configuration for “Trunking.”
configure	link-aggregation [GROUP_ID] (disable|enable)	The command disables/enables “Trunking” for the specific “Trunk Group.”
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific “Trunk Group.”
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The command deletes ports from a specific “Trunk Group.”

Example

L2SWITCH(config)# *configure terminal*

L2SWITCH(config)# *link-aggregation 1 enable*

L2SWITCH(config)# *link-aggregation 1 ports 1-4*

10.3.3.8.1 LACP

Table 165: CLI “LACP” Configuration

Node	Command	Description
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor’s information for the specific group or all groups.
enable	show lacp port_priority	This command c displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor’s and partner’s system ID.
configure	lacp (disable|enable)	This command disables/enables the LACP on the switch.
configure	lacp GROUP_ID (disable|enable)	This command disables/enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority<1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	lacp port_priority <1-65535>	This command configures the priority for the specific ports. Note: The default value is 32768.
if-range	no lacp port_priority	This command configures the default for the priority for the specific ports.

10.3.3.9 LLDP

Table 166: 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 tansmitted 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.

10.3.3.10 Loop Detection

Table 167: 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*

10.3.3.11 Modbus

Table 168: CLI “Modbus” Configuration

Node	Command	Description
enable	show modbus	This command displays the current Modbus configurations.
configure	modbus(disable|enable)	This command disables/enables the Modbus on the switch.

10.3.3.12 PoE

Table 169: CLI “PoE” Configuration

Node	Command	Description
enable	show poe	This command displays the PoE configurations and status.
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
configure	poe (disable|enable)	This command disables or enables the global PoE for the Switch.
configure	poe total-power	This command configures the total power which the Switch can support.
interface	poe (disable|enable)	This command enables or disables the PoE function on the specific port.
interface	poe priority(critical|high|low)	This command configures the priority of the PoE function for the specific port. – critical: The highest priority. – high: The middle priority. – low: The lowest priority.

10.3.3.12.1 PoE Schedule

Table 170: CLI “PoE Schedule” Configuration

Node	Command	Description
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
interface	poe schedule (disable|enable)	This command disables or enables the PoE schedule on the specific port.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) check (yes|no)	This command enables or disables the PoE schedule on the specific day.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) start-time VALUE end-time VALUE action (enable|disable)	This command configures the PoE schedule start-time and end-time on a specific day on the specific port. Users can enable or disable the PoE on the time period.

10.3.3.12.2 PD Alive Check

Table 171: CLI “PD Alive Check” Configuration

Node	Command	Description
enable	show pd-alive	This command displays the configuration of the PD Alive Check.
configure	pd-alive (disable|enable)	This command disables or enables the global PD Alive Check for the Switch.
Interfejs	pd-alive action (reboot|alarm|all|none)	This command configures the action when the system detects that the host cannot respond the keep-a-live probe packet.
Interfejs	pd-alive interval VALUE	This command configures the interval to send the keep-a-live probe packets to check if the host is still alive for the specific port.
Interfejs	pd-alive ip IP_ADDR	This command configures the Host IP address which connects to the specific port.
Interfejs	pd-alive retry-time VALUE	This command configures the retry times when no response from the host for the keep-a-live probe packet for the specific port.
Interfejs	pd-alive power-off-time VALUE startup-time VALUE	This command configures the power-off time and startup time.

10.3.3.12.3 Power Delay

Table 172: CLI “Power Delay” Configuration

Node	Command	Description
enable	show poe power-delay	This command displays the PoE power delay configurations.
interface	poe power-delay(enable|disable)	This command enables/disables of the Power Delay function for the specific port.
interface	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	poe power-delay(enable|disable)	This command enables/disables of the Power Delay function for the range of ports.
if-range	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the range of ports.

10.3.3.13 Static Route

Table 173: CLI “Static Route” Configuration

Node	Command	Description
enable	show ip forwarding status	This command displays the current configuration of the ip forwarding status.
enable	show ip routes(all|ipv4|ipv6)	This command displays the configurations of IPv4 or IPv6 or both routes from routing table.
enable	show ip arp(all|ipv4|ipv6)	This command displays dynamic and static IPv4 orIPv6or both ARP entries in ARP table.
enable	show ip hosts(all|ipv4|ipv6)	This command displays assigned IPv4 or IPv6 or both addresses for interfaces in router.
configure	ip forwarding enable	This command enables layer 3 IPv4 and IPv6 forwarding/routing globally.
configure	no ip forwarding enable	This command disables layer 3 IPv4 and IPv6 forwarding/routing globally. Spowoduje to usunięcie wszystkich przypisanych adresów IP i statycznych tras z interfejsów.
configure	ip arp proxy enable	This command enables route to act as an ARP proxy globally; It will be useful in Inter VLAN routing.
configure	no ip arp proxy enable	This command disables route to act as an ARP proxy.
configure	ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command allows adding static IPv4 ARP entry in ARP table.
configure	ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command allows adding static IPv4 ARP entry in ARP table.
configure	ip6 arp <IPv6_ADDR><MAC_ADDR>	This command allows adding static IPv6 ARP entry in ARP table.
configure	no ipv4 arp <IPv4_ADDR><MAC_ADDR>	This command deletes a static IPv4 ARP entry from ARP table.
configure	interface vlan VLAN-ID	This command enters the L3 interface node.
L3 interface	ipv4 address A.B.C.D/M	This command assigns a specified IPv4 interface route to the interface. We can assign multiple IPv4 interface route to a single interface with different IP segment. If this configuration is a first IP assigning to the interface then automatically interface is enabled for routing.
L3 interface	ipv6 address <IPv6_ADDR>/M	This command assigns a specified IPv6 interface route to the interface. We can assign only one IPv6 interface route for an interface vlan. If this configuration is a first IP assigning to the interface then it automatically enables the interface with routing.
L3 interface	no ipv4 address A.B.C.D/M	This command deletes a specified IPv4 interface route from the interface vlan. This command deletes all dependent static routes on the specified IPv4 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface.

Table 173: CLI “Static Route” Configuration

Node	Command	Description
L3 interface	no ipv4 address <IPv6_ADDR>/M	This command deletes a specified IPv6 interface route from the interface. This command deletes all dependent static routes on the specified IPv6 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface vlan.
L3 interface	ipv4 route A.B.C.D/M A.B.C.D	This command configures anIPv4 static route onto the specified interface vlan.
L3 interface	ipv6 route <IPv6_ADDR>/M <IPv6_ADDR>	This command configures anIPv6 static route onto the specified interface vlan.
L3 interface	no ipv4 route A.B.C.D/M A.B.C.D	This command deletes a specified IPv4 static route from an interface vlan.
L3 interface	no ipv6 route<IPv6_ADDR>/M <IPv6_ADDR>	This command deletes a specified IPv6 static route from an interface vlan.

10.3.3.14 STP

Table 174: 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 174: 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.

10.3.3.14.1 MSTP

Table 175: CLI “MSTP” Configuration

Node	Command	Description
enable	show spanning-tree mst configuration	This command displays the MSTP configurations.
enable	show spanning-tree mst instance	This command displays all of the instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63>	This command displays specific instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63>interface IFNAME	This command displays specific instance configurations on an interface of the MSTP.
enable	show spanning-tree mst interface IFNAME	This command displays the configurations on an interface of the MSTP.
enable	show spanning-tree mst root	This command displays the root bridge configurations.
configure	spanning-tree(disable|enable)	This command enables / disables the spanning tree.
configure	spanning-tree mode mst	This command configures the mode of the spanning tree. (one of the three modes STP/RSTP/MSTP.)
configure	spanning-tree mst forward-time	This command configures the forward time for the MSTP.
configure	no spanning-tree mst forward-time	This command resets the forward time for the MSTP. The default forward delay time is 15 seconds.
configure	spanning-tree mst hello-time	This command configures the hello time for the MSTP.
configure	no spanning-tree mst hello-time	This command resets the hello time for the MSTP. The default hello time is 2 seconds.
configure	spanning-tree mst max-age	This command configures the maximum age time for the MSTP.
configure	no spanning-tree mst max-age	This command resets the maximum age time for the MSTP. The default maximum age time is 20 seconds.
configure	spanning-tree mst max-hops	This command configures the maximum hop count.
configure	no spanning-tree mst max-hops	This command resets the maximum hop count. The default maximum hop count is 20.
configure	spanning-tree mst instance STRING priority <0-61440>	This command resets the maximum hop count. The default maximum hop count is 20.
configure	no spanning-tree mst instance STRING priority	This command resets the priority for the specific instance.
interface	spanning-tree mst instance STRING cost <1-200000000>	This command configures a cost on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING cost	This command resets the cost on the specific port for the MSTP.
interface	spanning-tree mst instance STRING port-priority <0-240>	This command configures a priority on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING port-priority	This command resets the priority on the specific port for the MSTP.
configure	spanning-tree mst configuration	This command enters the MSTP configure node.
configure	no spanning-tree mst configuration	This command resets all of configurations for the MSTP.

Table 175: CLI “MSTP” Configuration

Node	Command	Description
mst	apply	This command applies configurations to current instant.
mst	instance	This command configures the instance and vlan map.
mst	name	This command configures a region name for the MSTP.
mst	no name	This command reset the region name for the MSTP.
mst	revision	This command configures the revision for the MSTP.
mst	no revision	This command resets the revision for the MSTP.
mst	show (current|pending)	This command shows the MSTP configures. Current – the working configurations. Pending – the not applied configurations.

Example

L2SWITCH(config)# *spanning-tree mst configuration*

L2SWITCH(config)# *name MSTP*

L2SWITCH(config)# *revision 1*

L2SWITCH(config)# *instance 1 vlan 1-10*

10.3.3.15 Xpress Ring

Table 176: CLI “Xpress Ring” Configuration

Node	Command	Description
enable	show xpress-ring	This command displays the current Xpress-Ring configurations.
configure	xpress-ring(disable|enable)	This command enables/disables the Xpress-Ring on the Switch.
configure	xpress-ring ring (RING1|RING2) state (disable|enable)	This command enables/disables the ring on the Switch.
configure	xpress-ring ring (RING1|RING2) last-byte-destination-mac VALUE	This command configures the last byte of the destination MAC for the ring on the Switch.
configure	xpress-ring ring (RING1|RING2) role (forwarder|arbiter)	This command configures the role (forwarder/arbiter) for the ring on the Switch.
configure	xpress-ring ring (RING1|RING2) primary-port PORTID	This command configures the primary port for the ring on the Switch. Note: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.
configure	xpress-ring ring (RING1|RING2) secondary-port PORTID	This command configures the secondary port for the ring on the Switch. Note: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.

10.3.4 Security

10.3.4.1 IP Source Guard

10.3.4.1.1 DHCP Snooping

Table 177: CLI “DHCP Snooping” Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current “DHCP Snooping” configurations.
configure	dhcp-snooping (disable|enable)	This command disables/enables “DHCP Snooping” on the switch.
configure	dhcp-snooping vlan VLANID	This command enables the “DHCP Snooping” function on a VLAN or VLAN range.
configure	no dhcp-snooping vlan VLANID	This command disables the “DHCP Snooping” function on a VLAN or VLAN range.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	dhcp-snooping host	This command configures the maximum host count for the specific ports.
if-range	no dhcp-snooping host	This command configures the maximum host count to default for the specific ports.
if-range	dhcp-snooping trust	This command configures the trust port for the specific ports.
if-range	no dhcp-snooping trust	This command configures the un-trust port for the specific ports.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*dhcp-snooping enable*

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

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

L2SWITCH(config-if)#*dhcp-snooping trust*

10.3.4.1.1.1 Server Screening

Table 178: CLI “Server Screening” Configuration

Node	Command	Description
enable	show dhcp-snooping server	This command displays the IP address of the valid DHCP server.
configure	dhcp-snooping server IPADDR	This command configures the IP address of a valid DHCP server.
configure	no dhcp-snooping server IPADDR	This command deletes the IP address of a valid DHCP server.

10.3.4.1.2 Binding Table

Table 179: CLI “Binding Table” Configuration

Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current “DHCP Snooping” binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLANID port PORT_NO	This command configures a static host in the “DHCP Snooping” binding table.
configure	no dhcp-snooping binding mac MACADDR	This command deletes a static host from the “DHCP Snooping” binding table.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1 port 2*

L2SWITCH(config)#*no dhcp-snooping binding mac 00:11:22:33:44:55*

L2SWITCH#*show dhcp-snooping binding*

10.3.4.1.3 ARP Inspection

Table 180: CLI “ARP Inspection” Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current configurations for the ARP Inspection.
configure	arp-inspection (disable|enable)	This command disables/enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLANID	This command enables the ARP Inspection function on a VLAN or VLAN range.
configure	no arp-inspection vlan VLANID	This command disables the ARP Inspection function on a VLAN or VLAN range.
interface	arp-inspection trust	This command configures the “Trusted Port” for the specific port.
interface	no arp-inspection trust	This command configures the “Untrusted Port” for the specific port.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*arp-inspection enable*

L2SWITCH(config)#*arp-inspection vlan 1*

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

L2SWITCH(config-if)#*arp-inspection trust*

10.3.4.1.3.1 Filter Table

Table 181: CLI “Filter Table” Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current MAC address filter for the ARP Inspection.
configure	arp-inspection mac-filter age VALUE	This command configures the “Age Time” for the MAP address filter entries of the ARP Inspection.
configure	clear arp-inspection mac-filter	This command clears all of entries in the filter table.
configure	no arp-inspection mac-filter mac MACADDR vlan VLAN ID	This command deletes a MAC address filter entry from the MAC filter table of the ARP Inspection.

10.3.4.2 Access Control List

Table 182: CLI “Access Control List” Configuration

Node	Command	Description
enable	show access-list	This command displays all access control profiles.
configure	access-list STRING ip-type (ipv4|ipv6)	This command creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6.
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	action dscp remarking <0-63>	This command actives this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.
acl	action 802.1p remarking <0-7>	This command actives this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	This command configures the 802.1p value for the profile.
acl	dscp VALUE	This command configures the DSCP value for the profile.
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.

Table 182: CLI “Access Control List” Configuration

Node	Command	Description
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.
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*

10.3.4.3 802.1X

Table 183: CLI “802.1X” Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1X configurations.
enable	show dot1x username	This command displays the current user accounts for local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable|enable)	This command enables/disables 802.1X authentication on the switch.
configure	dot1x authentic-method (local|radius)	This command configures the 802.1X authentication method.
configure	no dot1x authentic-method	This command sets the 802.1X authentication method to the default setting.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary RADIUS server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary RADIUS server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary RADIUS server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary RADIUS server.
configure	no dot1x radius secondary-server-ip	This command deletes the secondary RADIUS server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable|enable)	This command enables/disables the local .1x accounting records.
configure	dot1x guest-vlan VLANID	This command configures the guest VLAN.
configure	no dot1x guest-vlan	This command deletes the guest VLAN.
interface	dot1x admin-control-direction (both|in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command resets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the “Max Req Times” of a port (1 to 10).
interface	dot1x port-control (auto|force-authorized|force-unauthorized)	This command configures the port control mode for the port.
interface	dot1x authentication (disable|enable)	This command enables/disables 802.1X authentication on the port.
interface	dot1x reauthentication (disable|enable)	This command enables/disables the authentication interval on the port.
interface	dot1x timeout quiet-period	This command configures the “Quiet Period” value on the port.
interface	dot1x timeout server-timeout	This command configures the server timeout value on the port.

Table 183: CLI “802.1X” Configuration

Node	Command	Description
interface	dot1x timeout reauth-period	This command configures the authentication interval value on the port.
interface	dot1x timeout supp-timeout	This command configures the supplicant timeout value on the port.
interface	dot1x guest-vlan (disable|enable)	This command configures the 802.1X state on the port.

10.3.4.4 Port Security

Table 184: CLI “Port Security” Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
config	port-security (disable|enable)	This command enables/disables the global port security function.
interface	port-security (disable|enable)	This command enables/disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum number of MAC address entries for the specific port.

10.3.5 Monitor

10.3.5.1 Alarm

Table 185: CLI “Alarm” Configuration

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

10.3.5.2 Monitor Information

Table 186: CLI “Monitor Information” Configuration

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

10.3.5.3 Port Statistics

Table 187: CLI “Port Statistics” Configuration

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

10.3.5.4 Port Utilization

Table 188: CLI “Port Statistics” Configuration

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

10.3.5.5 RMON Statistics

Table 189: 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.

10.3.5.6 SFP Information

Table 190: CLI “SFP Information” Configuration

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

10.3.5.7 Traffic Monitor

Table 191: 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.

10.3.6 Management

10.3.6.1 SNMP

10.3.6.1.1 SNMP

Table 192: 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*

10.3.6.1.2 SNMP Trap

Table 193: 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.

10.3.6.1.2.1 Port Trap Settings

Table 194: 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.

10.3.6.1.3 SNMPv3

Table 195: 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.

10.3.6.2 Auto Provision

Table 196: CLI “Auto Provision” Configuration

Node	Command	Description
enable	show auto-provision	This command displays the current auto provision configurations.
configure	auto-provision	This command enters the auto-provision node.
auto-provision	show	This command displays the current auto provision configurations.
auto-provision	active (enable|disable)	This command enables/disables the auto provision function.
auto-provision	server-addressIPADDR	This command configures the auto provision server’s IP.
auto-provision	protocol (tftp|http|ftp)	The command configurations the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	The command configurations the username and password for the FTP server.
auto-provision	folder STRING	The command configurations the folder for the auto provision server.
auto-provision	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

10.3.6.3 Mail Alarm

Table 197: CLI “Mail Alarm” Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the Mail Alarm configurations.
configure	mail-alarm (disable|enable)	This command disables/enables the Mail Alarm function.
configure	mail-alarm auth-account	This command configures the Mail server authentication account.
configure	mail-alarm mail-from	This command configures the mail sender.
configure	mail-alarm mail-to	This command configures the mail receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures the mail server IP address and the TCP port.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the mail server IP address and configures 25 as the server’s TCP port.
configure	mail-alarm trap-event (reboot|link-change|config.|firmware| login|port-blocked|alarm) (disable|enable)	This command disables/enables mail trap events.

10.3.6.4 Maintenance

Table 198: 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*

10.3.6.4.1 Reboot

Table 199: CLI “Reboot” Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	http server	This command enables the http on the Switch.
configure	no http server	This command disables the http on the Switch.
configure	http server port VALUE	This command configures the TCP port for the HTTP server.
configure	no http server port	This command resets the HTTP TCP port to 80.
configure	https server	This command enables the https on the Switch.
configure	no https server	This command disables the https on the Switch.
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	telnet server port VALUE	This command configures the TCP port for the TELNET server.
configure	no telnet server port	This command resets the TELNET TCP port to 23.

10.3.6.5 System Log

Table 200: 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 ipv6-ip IPADDR	The command configures the syslog server’s IP address in IPv6 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*syslog-server ipv4-ip 192.168.200.106*

L2SWITCH(config)#*syslog-server enable*

10.3.6.6 USB Flash

Table 201: CLI “USB Flash” Configuration

Node	Command	Description
enable	show usb status	This command displays the current USB function configurations.
configure	usb auto-upgrade-fw (disable|enable)	This command disables/enables the USB upgrade firmware automatically.
configure	usb auto-download-config (disable|enable)	This command disables/enables the USB download configuration file automatically.
configure	usb auto-download-syslog (disable|enable)	This command disables/enables the USB download syslog file automatically.

Example

L2SWITCH#*show usb status*

L2SWITCH#*configure terminal*

L2SWITCH(config)#*usb auto-upgrade-fw enable*

L2SWITCH(config)#*usb auto-download-config enable*

L2SWITCH(config)#*usb auto-download-syslog enable*

10.3.6.7 User Account

Table 202: CLI “System Log” Configuration

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

Example

L2SWITCH#*configure terminal*

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

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

10.4 Tabele MODBUS/TCP

10.4.1 Format danych i kod funkcji

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

Tabela 203: Format danych i kod funkcji

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

10.4.2 Rejestry MODBUS

Przestrzeń adresowa MODBUS przemysłowego switcha zarządzalnego rozpoczyna się od 1000 (dziesiętne) dla kodu funkcji 4.

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
1000	3E8	1	HEX	Vendor ID = 0x30DE
1001	3E9	16	ASCII	Vendor Name = “WAGO” Word 0 Hi byte = ‘W’ Word 0 Lo byte = ‘A’ Word 1 Hi byte = ‘G’ Word 1 Lo byte = ‘O’ Word 2 Hi byte = ‘\0’
1032	408	16	ASCII	**Product Name = “852-1505/000-001”** Word 0 Hi byte = ‘8’ Word 0 Lo byte = ‘5’ Word 1 Hi byte = ‘2’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘5’ Word 3 Hi byte = ‘0’ Word 3 Lo byte = ‘5’ Word 4 Hi byte = ‘/’ Word 4 Lo byte = ‘0’ Word 5 Hi byte = ‘0’ Word 5 Lo byte = ‘0’ Word 6 Hi byte = ‘-’ Word 6 Lo byte = ‘0’ Word 7 Hi byte = ‘0’ Word 7 Lo byte = ‘1’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0
1064	428	7	ASCII	**Product Serial Number** Ex: Serial No=A000000000001

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
1080	438	12	ASCII	**Firmware Version=" V1.0.2.S0"**
				Word 0 Hi byte = 'V'
				Word 0 Lo byte = '1'
				Word 1 Hi byte = '.'
				Word 1 Lo byte = '0'
				Word 2 Hi byte = '.'
				Word 2 Lo byte = '2'
				Word 3 Hi byte = '.'
				Word 3 Lo byte = 'S'
				Word 4 Hi byte = '0'
				Word 4 Lo byte = '\0'
				Word 5 Hi byte = '\0'
				Word 5 Lo byte = '\0'
				Word 6 Hi byte = '\0'
				Word 6 Lo byte = '\0'
				Word 7 Hi byte = '\0'
				Word 7 Lo byte = '\0'
				Word 8 Hi byte = '\0'
				Word 8 Lo byte = '\0'
1096	448	16	ASCII	Firmware Release Date="Mon Jun 17 13:36:33 CST 2019"
1112	458	3	HEX	**ETHERNET MAC Address**
				Np: MAC = 00 30 DE FF F1 99
				Word 0 Hi byte = 0 x 00
				Word 0 Lo byte = 0 x 30
				Word 1 Hi byte = 0 x DE
				Word 1 Lo byte = 0 x FF
				Word 2 Hi byte = 0 x F1
				Word 2 Lo byte = 0 x 99
1128	468	1	HEX	**Power 1 (PWR) Alarm, DIP switch 1 need ON**
				0x0000: no alarm
				0x0001: input voltage < 11.7V
				0x0002: input voltage > 57V
				0x0003: No PWR input
1129	469	1	HEX	**Power 2(RPS) Alarm, DIP switch 1 need ON**
				0x0000: no alarm
				0x0001: input voltage < 11.7V
				0x0002: input voltage > 57V
				0x0003: No RPS input
1144	478	1	HEX	**Fault LED Status**
				0x0000: No
				0x0001: Yes

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
Port Information				
		1	HEX	**1256 (Port 1) ... 1267 (Port 12)** **Port 1 to 12 Link Status**
				0x0000: Link down
1256	4E8			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1257	4E9			0x0002: 10M-Full-FC_OFF
1258	4EA			0x0003: 10M-Half-FC_ON
1259	4EB			0x0004: 10M-Half-FC_OFF
1260	4EC			0x0005: 100M-Full-FC_ON
1261	4ED			0x0006: 100M-Full-FC_OFF
1262	4EE			0x0007: 100M-Half-FC_ON
1263	4EF			0x0008: 100M-Half-FC_OFF
1264	4F0			0x0009: 1000M-Full-FC_ON
1265	4F1			0x000A: 1000M-Full-FC_OFF
1266	4F2			0x000B: 1000M-Half-FC_ON
1267	4F3			0x000C: 1000M-Half-FC_OFF
				0xFFFF: No port
		32	ASCII	**Port 1 to 12 Medium**
1512	5E8			Port Description = “100TX, RJ45.” Or “1000TX, SFP.”
1544	608			Word 0 Hi byte = ‘1’
1576	628			Word 0 Lo byte = ‘0’
1608	648			Word 1 Hi byte = ‘0’
1640	668			Word 1 Lo byte = ‘T’
1672	688			…
1704	6A8			Word 4 Hi byte = ‘4’
1736	6C8			Word 4 Lo byte = ‘5’
1768	6E8			Word 5 Hi byte = ‘.’
1800	708			Word 5 Lo byte = ‘\0’
1832	728			
1864	748			
		2	HEX	**2024 (Port 1) ... 2046 (Port 12)** **Port 1 to 12 Tx Packets**
2024	7E8			Ex: port 1 Tx Packet Amount = 0x87654321
2026	7EA			Word 0 = 8765
2028	7EB			Word 1 = 4321
2030	7EE			
2032	7F0			
2034	7F2			
2036	7F4			
2038	7F6			
2040	7F8			
2042	7FA			
2044	7FC			
2046	7FE			

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
		2	HEX	**2088 (Port 1) ... 2110 (Port 12)** **Port 1 to 12 Rx Packets**
2088	828			Ex: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2090	82A			
2092	82C			
2094	82E			
2096	830			
2098	832			
2100	834			
2102	836			
2104	838			
2106	83A			
2108	83C			
2110	83E			
		2	HEX	**2152 (Port 1) ... 2174 (Port 12)** **Port 1 to 12 Tx Error Packets**
2152	868			Ex: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
2154	86A			
2156	86C			
2158	86E			
2160	870			
2162	872			
2164	874			
2166	876			
2168	878			
2170	87A			
2172	87C			
2174	87E			
		2	HEX	**2216 (Port 1) ... 2238 (Port 12)** **Port 1 to 12 Rx Error Packets**
2216	8A8			Ex: port 1 Rx Error Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
2218	8AA			
2220	8AC			
2222	8AE			
2224	8B0			
2226	8B2			
2228	8B4			
2230	8B6			
2232	8B8			
2234	8BA			
2236	8BC			
2238	8BE			

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
Redundancy & Ring Information				
2280	8E8	1	HEX	**Spanning Tree Status** 0x0000 : none 0x0001 : STP 0x0002 : RSTP 0x0003 : MSTP
2281	8E9	1	HEX	**Xpress-ring Status** 0x0000 : Disabled 0x0001 : Enabled
2282	8EA	1	HEX	**Jet-ring Status** 0x0000 : Disabled 0x0001 : Enabled
2283	8EB	1	HEX	**Dual-ring Status** 0x0000 : Disabled 0x0001 : Enabled
2284	8EC	1	HEX	**ERPS Status** 0x0000 : Disabled 0x0001 : Enabled
2296	8F8	1	HEX	**Xpress-ring Status Ring 1** 0x0000 : Disabled 0x0001 : Enabled
2297	8F9	1	HEX	**Xpress-ring Status Ring 2** 0x0000 : Disabled 0x0001 : Enabled
2298	8FA	3	HEX	**Xpress-ring MAC Ring 1** Ex: Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
2301	8FD	3	HEX	**Xpress-ring MAC Ring 2** Ex: Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
2304	900	1	HEX	**Primary Port of Xpress_Ring 1** Ex: Port 5 = 0x0005
2305	901	1	HEX	**Secondary Port of Xpress_Ring 1** Ex: Port 6 = 0x0006

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
2306	902	1	HEX	**Primary Port of Xpress_Ring 2**
				Ex: Port 5 = 0x0005
2307	903	1	HEX	**Secondary Port of Xpress_Ring 2**
				Ex: Port 6 = 0x0006
2308	904	1	HEX	**Xpress-ring Role Ring 1**
				0x0000 : **Forwarder** 0x0001 : **Arbiter**
2309	905	1	HEX	**Xpress-ring Role Ring 2**
				0x0000 : **Forwarder** 0x0001 : **Arbiter**
2310	906	1	HEX	**Xpress-ring Current status for Ring 1**
				Primary Port
				0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2311	907	1	HEX	**Xpress-ring Current status for Ring 1**
				Secondary Port
				0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2312	908	1	HEX	**Xpress-ring Current status for Ring 2**
				Primary Port
				0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking
2313	909	1	HEX	**Xpress-ring Current status for Ring 2**
				Secondary Port
				0x0000 : No connection 0x0001 : Forwarding 0x0002 : Blocking

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
Jet-Ring Information				
2536	9E8	1	HEX	**Jet Ring State**
				0x0000: Disabled.
				0x0001: Enabled.
2537	9E9	3	HEX	**Master Bridge MAC:**
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
				Word 2, low byte=0x05.
2540	9EC	1	HEX	**Jet Ring Total Nodes:**
				Ex: When total nodes is 255(0xff).
				Word 0, high byte=0x00.
				Word 0, low byte=0xff.
2541	9ED	1	HEX	**Bridge Role:**
				0x0000: Learning.
				0x0001: Master.
				0x0002: Arbiter.
				0x0003: Forwarder.
				0x0004: Pre-Forwarder.
		1	HEX	**2552 (Port 1) ... 2563 (Port 12)** **Port Role (Port 1 to Port 12)**
2552	9F8			0x0000: Disabled.
2553	9F9			0x0001: Listening.
2554	9FA			0x0002: Learning.
2555	9FB			0x0003: Forwarding.
2556	9FC			0x0004: Blocking.
2557	9FD			0x0005: No connection.
2558	9FE			
2559	9FF			
2560	A00			
2561	A01			
2562	A02			
2563	A03			

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
		1	HEX	**2584 (Port 1) ... 2595 (Port 12)** **Ring Role (Port 1 to Port 12)**
2584	A18			0x0000: No 0x0001: Yes
2585	A19			
2586	A1A			
2587	A1B			
2588	A1C			
2589	A1D			
2590	A1E			
2591	A1F			
2592	A20			
2593	A21			
2594	A22			
2595	A23			
Dual-Ring Information				
2792	AE8	1	HEX	**Dual-Ring State:**
				0x0000: Disabled. 0x0001: Enabled.
2793	AE9	3	HEX	**Xpress-ring MAC for Dual-Ring:**
				Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.
2796	AEC	1	HEX	**Xpress-ring Role for Dual-Ring:**
				0x0000 : Forwarder 0x0001 : Arbiter

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
2797	AED	1	HEX	**Xpress-ring Current status for Dual-Ring**
				Port-1 – (Primary Port)
				High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
2798	AEE	1	HEX	**Xpress-ring Current status for Dual-Ring**
				Port-2 – (Secondary Port)
				High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
2799	AEF	3	HEX	**Sub-Ring Master Bridge MAC :**
				Ex: MAC=00:01:02:03:04:05 Word 0, high byte=0x00. Word 0, low byte=0x01. Word 1, high byte=0x02. Word 1, low byte=0x03. Word 2, high byte=0x04. Word 2, low byte=0x05.
2802	AF2	1	HEX	**Jet Ring Total Nodes for Sub-Ring.**
				Ex: When total nodes is 255(0xff). Word 0, high byte=0x00. Word 0, low byte=0xff.
2803	AF3	1	HEX	**Bridge Role for Sub-Ring:**
				0x0000: Learning. 0x0001: Master. 0x0002: Arbiter. 0x0003: Forwarder. 0x0004: Pre-Forwarder.
2804	AF4	1	HEX	**Sub-ring Current status for Dual-Ring**
				Subport-1 – (Primary Port)
				High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
2805	AF5	1	HEX	***Subport-2 – (Secondary Port)***
				High byte – Port No. 0x01~ 0x0a: Port 1~Port 12 Low byte – Port Status 0x00 : No connection 0x01 : Forwarding 0x02 : Blocking Ex: 0x0501– Port 5 Forwarding 0x0b02 – Port 12 Blocking
ERPS Information(Active Ring Only)				
3048	BE8	1	HEX	**Ring ID for ERPSn (n=1)**
				Ex: 0x001 Ring ID=1
3049	BE9	1	HEX	**State for ring of ERPS**
				0x0000: Disabled. 0x0001: Enabled.
3050	BEA	33	ASCII	**Name of Ring**
				Ring Name = “Ring1” Word 1 Lo byte = ‘R’ Word 2 Lo byte = ‘i’ Word 3 Lo byte = ‘n’ Word 4 Lo byte = ‘g’ Word 5 Lo byte = ‘1’ Word 6 Lo byte = ‘\0’
3083	C0B	1	HEX	**Version & Ring Type**
				High byte – Version. Low byte – Ring Type. 0x01:Major-ring 0x02:Sub-ring Ex: 0x0201– Version2, Type:Major-ring
3084	C0C	1	HEX	**Instance of Ring**
				Ex: 0x0001 Instance ID=1
3085	C0D	1	HEX	**Control VLAN of Ring**
				E:0x000b Control VLAN=11

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
3086	C0E	1	HEX	**Right Port of Ring**
				High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0502– Port 5, RPL Owner
3087	C0F	1	HEX	**Left Port of Ring**
				High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0303– Port 3, RPL Neighbour
3088	C10	1	HEX	**Ring port state**
				High byte –Left port state. Low byte – Right port state. 0x00: No connection 0x01: Forwarding 0x02: Blocking Ex: 0x0001– Left Port No connection Right Port Forwarding
3089	C11	1	HEX	**Ring ID for ERPSn (n=2)**
3090	C12	1		State of ERPS Ring
3091	C13	33	ASCII	Name of Ring
3124	C34	1	HEX	Version & Ring Type
3125	C35	1		Instance of Ring
3126	C36	1		Control VLAN of Ring
3127	C37	1		Right Port of Ring
3128	C38	1		Left Port of Ring
3129	C39	1		Ring port state
3130	C3A	1	HEX	**Ring ID for ERPSn (n=3)**
3131	C3B	1		State of ERPS Ring
3132	C3C	33	ASCII	Name of Ring
3165	C5D	1	HEX	Version & Ring Type
3166	C5E	1		Instance of Ring
3167	C5F	1		Control VLAN of Ring
3168	C60	1		Right Port of Ring
3169	C61	1		Left Port of Ring
3170	C62	1		Ring port state

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
3171	C63	1	HEX	**Ring ID for ERPSn (n=4)**
3172	C64	1		State of ERPS Ring
3173	C65	33	ASCII	Name of Ring
3206	C86	1	HEX	Version & Ring Type
3207	C87	1		Instance of Ring
3208	C88	1		Control VLAN of Ring
3209	C89	1		Right Port of Ring
3210	C8A	1		Left Port of Ring
3211	C8B	1		Ring port state
3212	C8C	1	HEX	**Ring ID for ERPSn (n=5)**
3213	C8D	1		State of ERPS Ring
3214	C8E	33		Name of Ring
3247	CAF	1		Version & Ring Type
3248	CB0	1		Instance of Ring
3249	CB1	1		Control VLAN of Ring
3250	CB2	1		Right Port of Ring
3251	CB3	1		Left Port of Ring
3252	CB4	1		Ring port state
3253	CB5	1	HEX	**Ring ID for ERPSn (n=6)**
3254	CB6	1		State of ERPS Ring
3255	CB7	33	ASCII	Name of Ring
3288	CD8	1	HEX	Version & Ring Type
3289	CD9	1		Instance of Ring
3290	CDA	1		Control VLAN of Ring
3291	CDB	1		Right Port of Ring
3292	CDC	1		Left Port of Ring
3293	CDD	1		Ring port state
MSTP Information				
3304	CE8	1	HEX	**Instance ID (Fixed 0x00, 0)**
				High byte –Instance ID.
				Low byte –Used State.
				0x01: used
				0x00: non used
3305	CE9	3	HEX	**Root bridge MAC**
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
				Word 2, low byte=0x05.
3308	CEC	1	HEX	**Port 1 status**
				High byte –Port No.
				Low byte –Port Status.
				b'0:1 Type

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
				00: Bound(STP) 01: Bound(RSTP) 10: Bound(MSTP) 11: Internal(MSTP) **b'2 P2P** 0: non P2P 1: P2P **b'3:4 State** 00: Blocking 01: Learning 10: Forwarding **b'5:7 Role** 000: Master 001:Alternate 010: Root 011: Designated 100: Backup 101: Disabled 110: Boundary 111: Unknow
3309	CED			Port 2 status
3310	CEE			Port 3 status
3311	CEF			Port 4 status
3312	CF0			Port 5 status
3313	CF1			Port 6 status
3314	CF2			Port 7 status
3315	CF3			Port 8 status
3316	CF4			Port 9 status
3317	CF5			Port 10 status
3318	CF6			Port 11 status
3319	CF7			Port 12 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
3336	D08	1	HEX	Instance ID (Fixed 0x00, 1)
3337	D09	3		Root bridge MAC
3340	D0C	1		Port 1 status
3341	D0D	1		Port 2 status
3342	D0E	1		Port 3 status
3343	D0F	1		Port 4 status
3344	D10	1		Port 5 status
3345	D11	1		Port 6 status
3346	D12	1		Port 7 status
3347	D13	1		Port 8 status
3348	D14	1		Port 9 status
3349	D15	1		Port 10 status
3350	D16	1		Port 11 status
3351	D17	1		Port 12 status
3368	D28	1	HEX	Instance ID (Fixed 0x00, 2)
3369	D29	3		Root bridge MAC
3372	D2C	1		Port 1 status
3373	D2D	1		Port 2 status
3374	D2E	1		Port 3 status
3375	D2F	1		Port 4 status
3376	D30	1		Port 5 status
3377	D31	1		Port 6 status
3378	D32	1		Port 7 status
3379	D33	1		Port 8 status
3380	D34	1		Port 9 status
3381	D35	1		Port 10 status
3382	D36	1		Port 11 status
3383	D37	1		Port 12 status
3400	D48	1	HEX	Instance ID (Fixed 0x00, 3)
3401	D49	3		Root bridge MAC
3404	D4C	1		Port 1 status
3405	D4D	1		Port 2 status
3406	D4E	1		Port 3 status
3407	D4F	1		Port 4 status
3408	D50	1		Port 5 status
3409	D51	1		Port 6 status
3410	D52	1		Port 7 status
3411	D53	1		Port 8 status
3412	D54	1		Port 9 status
3413	D55	1		Port 10 status
3414	D56	1		Port 11 status
3415	D57	1		Port 12 status
3432	D68	1	HEX	Instance ID (Fixed 0x00, 4)
3433	D69	3		Root bridge MAC
3436	D6C	1		Port 1 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
3437	D6D	1		Port 2 status
3438	D6E	1		Port 3 status
3439	D6F	1		Port 4 status
3440	D70	1		Port 5 status
3441	D71	1		Port 6 status
3442	D72	1		Port 7 status
3443	D73	1		Port 8 status
3444	D74	1		Port 9 status
3445	D75	1		Port 10 status
3446	D76	1		Port 11 status
3447	D77	1		Port 12 status
3464	D88	1	HEX	Instance ID (Fixed 0x00, 5)
3465	D89	3		Root bridge MAC
3468	D8C	1		Port 1 status
3469	D8D	1		Port 2 status
3470	D8E	1		Port 3 status
3471	D8F	1		Port 4 status
3472	D90	1		Port 5 status
3473	D91	1		Port 6 status
3474	D92	1		Port 7 status
3475	D93	1		Port 8 status
3476	D94	1		Port 9 status
3477	D95	1		Port 10 status
3478	D96	1		Port 11 status
3479	D97	1		Port 12 status
3496	DA8	1	HEX	Instance ID (Fixed 0x00, 6)
3497	DA9	3		Root bridge MAC
3500	DAC	1		Port 1 status
3501	DAD	1		Port 2 status
3502	DAE	1		Port 3 status
3503	DAF	1		Port 4 status
3504	DB0	1		Port 5 status
3505	DB1	1		Port 6 status
3506	DB2	1		Port 7 status
3507	DB3	1		Port 8 status
3508	DB4	1		Port 9 status
3509	DB5	1		Port 10 status
3510	DB6	1		Port 11 status
3511	DB7	1		Port 12 status
3528	DC8	1	HEX	Instance ID (Fixed 0x00, 7)
3529	DC9	3		Root bridge MAC
3532	DCC	1		Port 1 status
3533	DCD	1		Port 2 status
3534	DCE	1		Port 3 status
3535	DCF	1		Port 4 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
3536	DD0	1		Port 5 status
3537	DD1	1		Port 6 status
3538	DD2	1		Port 7 status
3539	DD3	1		Port 8 status
3540	DD4	1		Port 9 status
3541	DD5	1		Port 10 status
3542	DD6	1		Port 11 status
3543	DD7	1		Port 12 status
3560	DE8	1	HEX	Instance ID (Fixed 0x00, 8)
3561	DE9	3		Root bridge MAC
3564	DEC	1		Port 1 status
3565	DED	1		Port 2 status
3566	DEE	1		Port 3 status
3567	DEF	1		Port 4 status
3568	DF0	1		Port 5 status
3569	DF1	1		Port 6 status
3570	DF2	1		Port 7 status
3571	DF3	1		Port 8 status
3572	DF4	1		Port 9 status
3573	DF5	1		Port 10 status
3574	DF6	1		Port 11 status
3575	DF7	1		Port 12 status
3592	E08	1	HEX	Instance ID (Fixed 0x00, 9)
3593	E09	3		Root bridge MAC
3596	E0C	1		Port 1 status
3597	E0D	1		Port 2 status
3598	E0E	1		Port 3 status
3599	E0F	1		Port 4 status
3600	E10	1		Port 5 status
3601	E11	1		Port 6 status
3602	E12	1		Port 7 status
3603	E13	1		Port 8 status
3604	E14	1		Port 9 status
3605	E15	1		Port 10 status
3606	E16	1		Port 11 status
3607	E17	1		Port 12 status
3624	E28	1	HEX	Instance ID (Fixed 0x00, 10)
3625	E29	3		Root bridge MAC
3628	E2C	1		Port 1 status
3629	E2D	1		Port 2 status
3630	E2E	1		Port 3 status
3631	E2F	1		Port 4 status
3632	E30	1		Port 5 status
3633	E31	1		Port 6 status
3634	E32	1		Port 7 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
3635	E33	1		Port 8 status
3636	E34	1		Port 9 status
3637	E35	1		Port 10 status
3638	E36	1		Port 11 status
3639	E37	1		Port 12 status
3656	E48	1	HEX	Instance ID (Fixed 0x00, 11)
3657	E49	3		Root bridge MAC
3660	E4C	1		Port 1 status
3661	E4D	1		Port 2 status
3662	E4E	1		Port 3 status
3663	E4F	1		Port 4 status
3664	E50	1		Port 5 status
3665	E51	1		Port 6 status
3666	E52	1		Port 7 status
3667	E53	1		Port 8 status
3668	E54	1		Port 9 status
3669	E55	1		Port 10 status
3670	E56	1		Port 11 status
3671	E57	1		Port 12 status
3688	E68	1	HEX	Instance ID (Fixed 0x00, 12)
3689	E69	3		Root bridge MAC
3692	E6C	1		Port 1 status
3693	E6D	1		Port 2 status
3694	E6E	1		Port 3 status
3695	E6F	1		Port 4 status
3696	E70	1		Port 5 status
3697	E71	1		Port 6 status
3698	E72	1		Port 7 status
3699	E73	1		Port 8 status
3700	E74	1		Port 9 status
3701	E75	1		Port 10 status
3702	E76	1		Port 11 status
3703	E77	1		Port 12 status
3720	E88	1	HEX	Instance ID (Fixed 0x00, 13)
3721	E89	3		Root bridge MAC
3724	E8C	1		Port 1 status
3725	E8D	1		Port 2 status
3726	E8E	1		Port 3 status
3727	E8F	1		Port 4 status
3728	E90	1		Port 5 status
3729	E91	1		Port 6 status
3730	E92	1		Port 7 status
3731	E93	1		Port 8 status
3732	E94	1		Port 9 status
3733	E95	1		Port 10 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
3734	E96	1		Port 11 status
3735	E97	1		Port 12 status
3752	EA8	1	HEX	Instance ID (Fixed 0x00, 14)
3753	EA9	3		Root bridge MAC
3756	EAC	1		Port 1 status
3757	EAD	1		Port 2 status
3758	EAE	1		Port 3 status
3759	EAF	1		Port 4 status
3760	EB0	1		Port 5 status
3761	EB1	1		Port 6 status
3762	EB2	1		Port 7 status
3763	EB3	1		Port 8 status
3764	EB4	1		Port 9 status
3765	EB5	1		Port 10 status
3766	EB6	1		Port 11 status
3767	EB7	1		Port 12 status
3784	EC8	1	HEX	Instance ID (Fixed 0x00, 15)
3785	EC9	3		Root bridge MAC
3788	ECC	1		Port 1 status
3789	ECD	1		Port 2 status
3790	ECE	1		Port 3 status
3791	ECF	1		Port 4 status
3792	ED0	1		Port 5 status
3793	ED1	1		Port 6 status
3794	ED2	1		Port 7 status
3795	ED3	1		Port 8 status
3796	ED4	1		Port 9 status
3797	ED5	1		Port 10 status
3798	ED6	1		Port 11 status
3799	ED7	1		Port 12 status
3816	EE8	1	HEX	Instance ID (Fixed 0x00, 16)
3817	EE9	3		Root bridge MAC
3820	EEC	1		Port 1 status
3821	EED	1		Port 2 status
3822	EEE	1		Port 3 status
3823	EEF	1		Port 4 status
3824	EF0	1		Port 5 status
3825	EF1	1		Port 6 status
3826	EF2	1		Port 7 status
3827	EF3	1		Port 8 status
3828	EF4	1		Port 9 status
3829	EF5	1		Port 10 status
3830	EF6	1		Port 11 status
3831	EF7	1		Port 12 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
3848	F08	1	HEX	Instance ID (Fixed 0x00, 17)
3849	F09	3		Root bridge MAC
3852	F0C	1		Port 1 status
3853	F0D	1		Port 2 status
3854	F0E	1		Port 3 status
3855	F0F	1		Port 4 status
3856	F10	1		Port 5 status
3857	F11	1		Port 6 status
3858	F12	1		Port 7 status
3859	F13	1		Port 8 status
3860	F14	1		Port 9 status
3861	F15	1		Port 10 status
3862	F16	1		Port 11 status
3863	F17	1		Port 12 status
3880	F28	1	HEX	Instance ID (Fixed 0x00, 18)
3881	F29	3		Root bridge MAC
3884	F2C	1		Port 1 status
3885	F2D	1		Port 2 status
3886	F2E	1		Port 3 status
3887	F2F	1		Port 4 status
3888	F30	1		Port 5 status
3889	F31	1		Port 6 status
3890	F32	1		Port 7 status
3891	F33	1		Port 8 status
3892	F34	1		Port 9 status
3893	F35	1		Port 10 status
3894	F36	1		Port 11 status
3895	F37	1		Port 12 status
3912	F48	1	HEX	Instance ID (Fixed 0x00, 19)
3913	F49	3		Root bridge MAC
3916	F4C	1		Port 1 status
3917	F4D	1		Port 2 status
3918	F4E	1		Port 3 status
3919	F4F	1		Port 4 status
3920	F50	1		Port 5 status
3921	F51	1		Port 6 status
3922	F52	1		Port 7 status
3923	F53	1		Port 8 status
3924	F54	1		Port 9 status
3925	F55	1		Port 10 status
3926	F56	1		Port 11 status
3927	F57	1		Port 12 status
3944	F68	1	HEX	Instance ID (Fixed 0x00, 20)
3945	F69	3		Root bridge MAC
3948	F6C	1		Port 1 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
3949	F6D	1		Port 2 status
3950	F6E	1		Port 3 status
3951	F6F	1		Port 4 status
3952	F70	1		Port 5 status
3953	F71	1		Port 6 status
3954	F72	1		Port 7 status
3955	F73	1		Port 8 status
3956	F74	1		Port 9 status
3957	F75	1		Port 10 status
3958	F76	1		Port 11 status
3959	F77	1		Port 12 status
3976	F88	1	HEX	Instance ID (Fixed 0x00, 21)
3977	F89	3		Root bridge MAC
3980	F8C	1		Port 1 status
3981	F8D	1		Port 2 status
3982	F8E	1		Port 3 status
3983	F8F	1		Port 4 status
3984	F90	1		Port 5 status
3985	F91	1		Port 6 status
3986	F92	1		Port 7 status
3987	F93	1		Port 8 status
3988	F94	1		Port 9 status
3989	F95	1		Port 10 status
3990	F96	1		Port 11 status
3991	F97	1		Port 12 status
4008	FA8	1	HEX	Instance ID (Fixed 0x00, 22)
4009	FA9	3		Root bridge MAC
4012	FAC	1		Port 1 status
4013	FAD	1		Port 2 status
4014	FAE	1		Port 3 status
4015	FAF	1		Port 4 status
4016	FB0	1		Port 5 status
4017	FB1	1		Port 6 status
4018	FB2	1		Port 7 status
4019	FB3	1		Port 8 status
4020	FB4	1		Port 9 status
4021	FB5	1		Port 10 status
4022	FB6	1		Port 11 status
4023	FB7	1		Port 12 status
4040	FC8	1	HEX	Instance ID (Fixed 0x00, 23)
4041	FC9	3		Root bridge MAC
4044	FCC	1		Port 1 status
4045	FCD	1		Port 2 status
4046	FCE	1		Port 3 status
4047	FCF	1		Port 4 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
4048	FD0	1		Port 5 status
4049	FD1	1		Port 6 status
4050	FD2	1		Port 7 status
4051	FD3	1		Port 8 status
4052	FD4	1		Port 9 status
4053	FD5	1		Port 10 status
4054	FD6	1		Port 11 status
4055	FD7	1		Port 12 status
4072	FE8	1	HEX	Instance ID (Fixed 0x00, 24)
4073	FE9	3		Root bridge MAC
4076	FEC	1		Port 1 status
4077	FED	1		Port 2 status
4078	FEE	1		Port 3 status
4079	FEF	1		Port 4 status
4080	FF0	1		Port 5 status
4081	FF1	1		Port 6 status
4082	FF2	1		Port 7 status
4083	FF3	1		Port 8 status
4084	FF4	1		Port 9 status
4085	FF5	1		Port 10 status
4086	FF6	1		Port 11 status
4087	FF7	1		Port 12 status
4104	1008	1	HEX	Instance ID (Fixed 0x00, 25)
4105	1009	3		Root bridge MAC
4108	100C	1		Port 1 status
4109	100D	1		Port 2 status
4110	100E	1		Port 3 status
4111	100F	1		Port 4 status
4112	1010	1		Port 5 status
4113	1011	1		Port 6 status
4114	1012	1		Port 7 status
4115	1013	1		Port 8 status
4116	1014	1		Port 9 status
4117	1015	1		Port 10 status
4118	1016	1		Port 11 status
4119	1017	1		Port 12 status
4136	1028	1	HEX	Instance ID (Fixed 0x00, 26)
4137	1029	3		Root bridge MAC
4140	102C	1		Port 1 status
4141	102D	1		Port 2 status
4142	102E	1		Port 3 status
4143	102F	1		Port 4 status
4144	1030	1		Port 5 status
4145	1031	1		Port 6 status
4146	1032	1		Port 7 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4147	1033	1		Port 8 status
4148	1034	1		Port 9 status
4149	1035	1		Port 10 status
4150	1036	1		Port 11 status
4151	1037	1		Port 12 status
4168	1048	1	HEX	Instance ID (Fixed 0x00, 27)
4169	1049	3		Root bridge MAC
4172	104C	1		Port 1 status
4173	104D	1		Port 2 status
4174	104E	1		Port 3 status
4175	104F	1		Port 4 status
4176	1050	1		Port 5 status
4177	1051	1		Port 6 status
4178	1052	1		Port 7 status
4179	1053	1		Port 8 status
4180	1054	1		Port 9 status
4181	1055	1		Port 10 status
4182	1056	1		Port 11 status
4183	1057	1		Port 12 status
4200	1068	1	HEX	Instance ID (Fixed 0x00, 28)
4201	1069	3		Root bridge MAC
4204	106C	1		Port 1 status
4205	106D	1		Port 2 status
4206	106E	1		Port 3 status
4207	106F	1		Port 4 status
4208	1070	1		Port 5 status
4209	1071	1		Port 6 status
4210	1072	1		Port 7 status
4211	1073	1		Port 8 status
4212	1074	1		Port 9 status
4213	1075	1		Port 10 status
4214	1076	1		Port 11 status
4215	1077	1		Port 12 status
4232	1088	1	HEX	Instance ID (Fixed 0x00, 29)
4233	1089	3		Root bridge MAC
4236	108C	1		Port 1 status
4237	108D	1		Port 2 status
4238	108E	1		Port 3 status
4239	108F	1		Port 4 status
4240	1090	1		Port 5 status
4241	1091	1		Port 6 status
4242	1092	1		Port 7 status
4243	1093	1		Port 8 status
4244	1094	1		Port 9 status
4245	1095	1		Port 10 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4246	1096	1		Port 11 status
4247	1097	1		Port 12 status
4264	10A8	1	HEX	Instance ID (Fixed 0x00, 30)
4265	10A9	3		Root bridge MAC
4268	10AC	1		Port 1 status
4269	10AD	1		Port 2 status
4270	10AE	1		Port 3 status
4271	10AF	1		Port 4 status
4272	10B0	1		Port 5 status
4273	10B1	1		Port 6 status
4274	10B2	1		Port 7 status
4275	10B3	1		Port 8 status
4276	10B4	1		Port 9 status
4277	10B5	1		Port 10 status
4278	10B6	1		Port 11 status
4279	10B7	1		Port 12 status
4296	10C8	1	HEX	Instance ID (Fixed 0x00, 31)
4297	10C9	3		Root bridge MAC
4300	10CC	1		Port 1 status
4301	10CD	1		Port 2 status
4302	10CE	1		Port 3 status
4303	10CF	1		Port 4 status
4304	10D0	1		Port 5 status
4305	10D1	1		Port 6 status
4306	10D2	1		Port 7 status
4307	10D3	1		Port 8 status
4308	10D4	1		Port 9 status
4309	10D5	1		Port 10 status
4310	10D6	1		Port 11 status
4311	10D7	1		Port 12 status
4328	10E8	1	HEX	Instance ID (Fixed 0x00, 32)
4329	10E9	3		Root bridge MAC
4332	10EC	1		Port 1 status
4333	10ED	1		Port 2 status
4334	10EE	1		Port 3 status
4335	10EF	1		Port 4 status
4336	10F0	1		Port 5 status
4337	10F1	1		Port 6 status
4338	10F2	1		Port 7 status
4339	10F3	1		Port 8 status
4340	10F4	1		Port 9 status
4341	10F5	1		Port 10 status
4342	10F6	1		Port 11 status
4343	10F7	1		Port 12 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
4360	1108	1	HEX	Instance ID (Fixed 0x00, 33)
4361	1109	3		Root bridge MAC
4364	110C	1		Port 1 status
4365	110D	1		Port 2 status
4366	110E	1		Port 3 status
4367	110F	1		Port 4 status
4368	1110	1		Port 5 status
4369	1111	1		Port 6 status
4370	1112	1		Port 7 status
4371	1113	1		Port 8 status
4372	1114	1		Port 9 status
4373	1115	1		Port 10 status
4374	1116	1		Port 11 status
4375	1117	1		Port 12 status
4392	1128	1	HEX	Instance ID (Fixed 0x00, 34)
4393	1129	3		Root bridge MAC
4396	112C	1		Port 1 status
4397	112D	1		Port 2 status
4398	112E	1		Port 3 status
4399	112F	1		Port 4 status
4400	1130	1		Port 5 status
4401	1131	1		Port 6 status
4402	1132	1		Port 7 status
4403	1133	1		Port 8 status
4404	1134	1		Port 9 status
4405	1135	1		Port 10 status
4406	1136	1		Port 11 status
4407	1137	1		Port 12 status
4424	1148	1	HEX	Instance ID (Fixed 0x00, 35)
4425	1149	3		Root bridge MAC
4428	114C	1		Port 1 status
4429	114D	1		Port 2 status
4430	114E	1		Port 3 status
4431	114F	1		Port 4 status
4432	1150	1		Port 5 status
4433	1151	1		Port 6 status
4434	1152	1		Port 7 status
4435	1153	1		Port 8 status
4436	1154	1		Port 9 status
4437	1155	1		Port 10 status
4438	1156	1		Port 11 status
4439	1157	1		Port 12 status
4456	1168	1	HEX	Instance ID (Fixed 0x00, 36)
4457	1169	3		Root bridge MAC
4460	116C	1		Port 1 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4461	116D	1		Port 2 status
4462	116E	1		Port 3 status
4463	116F	1		Port 4 status
4464	1170	1		Port 5 status
4465	1171	1		Port 6 status
4466	1172	1		Port 7 status
4467	1173	1		Port 8 status
4468	1174	1		Port 9 status
4469	1175	1		Port 10 status
4470	1176	1		Port 11 status
4471	1177	1		Port 12 status
4488	1188	1	HEX	Instance ID (Fixed 0x00, 37)
4489	1189	3		Root bridge MAC
4492	118C	1		Port 1 status
4493	118D	1		Port 2 status
4494	118E	1		Port 3 status
4495	118F	1		Port 4 status
4496	1190	1		Port 5 status
4497	1191	1		Port 6 status
4498	1192	1		Port 7 status
4499	1193	1		Port 8 status
4500	1194	1		Port 9 status
4501	1195	1		Port 10 status
4502	1196	1		Port 11 status
4503	1197	1		Port 12 status
4520	11A8	1	HEX	Instance ID (Fixed 0x00, 38)
4521	11A9	3		Root bridge MAC
4524	11AC	1		Port 1 status
4525	11AD	1		Port 2 status
4526	11AE	1		Port 3 status
4527	11AF	1		Port 4 status
4528	11B0	1		Port 5 status
4529	11B1	1		Port 6 status
4530	11B2	1		Port 7 status
4531	11B3	1		Port 8 status
4532	11B4	1		Port 9 status
4533	11B5	1		Port 10 status
4534	11B6	1		Port 11 status
4535	11B7	1		Port 12 status
4552	11C8	1	HEX	Instance ID (Fixed 0x00, 39)
4553	11C9	3		Root bridge MAC
4556	11CC	1		Port 1 status
4557	11CD	1		Port 2 status
4558	11CE	1		Port 3 status
4559	11CF	1		Port 4 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4560	11D0	1		Port 5 status
4561	11D1	1		Port 6 status
4562	11D2	1		Port 7 status
4563	11D3	1		Port 8 status
4564	11D4	1		Port 9 status
4565	11D5	1		Port 10 status
4566	11D6	1		Port 11 status
4567	11D7	1		Port 12 status
4584	11E8	1	HEX	Instance ID (Fixed 0x00, 40)
4585	11E9	3		Root bridge MAC
4588	11EC	1		Port 1 status
4589	11ED	1		Port 2 status
4590	11EE	1		Port 3 status
4591	11EF	1		Port 4 status
4592	11F0	1		Port 5 status
4593	11F1	1		Port 6 status
4594	11F2	1		Port 7 status
4595	11F3	1		Port 8 status
4596	11F4	1		Port 9 status
4597	11F5	1		Port 10 status
4598	11F6	1		Port 11 status
4599	11F7	1		Port 12 status
4616	1208	1	HEX	Instance ID (Fixed 0x00, 41)
4617	1209	3		Root bridge MAC
4620	120C	1		Port 1 status
4621	120D	1		Port 2 status
4622	120E	1		Port 3 status
4623	120F	1		Port 4 status
4624	1210	1		Port 5 status
4625	1211	1		Port 6 status
4626	1212	1		Port 7 status
4627	1213	1		Port 8 status
4628	1214	1		Port 9 status
4629	1215	1		Port 10 status
4630	1216	1		Port 11 status
4631	1217	1		Port 12 status
4648	1228	1	HEX	Instance ID (Fixed 0x00, 42)
4649	1229	3		Root bridge MAC
4652	122C	1		Port 1 status
4653	122D	1		Port 2 status
4654	122E	1		Port 3 status
4655	122F	1		Port 4 status
4656	1230	1		Port 5 status
4657	1231	1		Port 6 status
4658	1232	1		Port 7 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
4659	1233	1		Port 8 status
4660	1234	1		Port 9 status
4661	1235	1		Port 10 status
4662	1236	1		Port 11 status
4663	1237	1		Port 12 status
4680	1248	1	HEX	Instance ID (Fixed 0x00, 43)
4681	1249	3		Root bridge MAC
4684	124C	1		Port 1 status
4685	124D	1		Port 2 status
4686	124E	1		Port 3 status
4687	124F	1		Port 4 status
4688	1250	1		Port 5 status
4689	1251	1		Port 6 status
4690	1252	1		Port 7 status
4691	1253	1		Port 8 status
4692	1254	1		Port 9 status
4693	1255	1		Port 10 status
4694	1256	1		Port 11 status
4695	1257	1		Port 12 status
4712	1268	1	HEX	Instance ID (Fixed 0x00, 44)
4713	1269	3		Root bridge MAC
4716	126C	1		Port 1 status
4717	126D	1		Port 2 status
4718	126E	1		Port 3 status
4719	126F	1		Port 4 status
4720	1270	1		Port 5 status
4721	1271	1		Port 6 status
4722	1272	1		Port 7 status
4723	1273	1		Port 8 status
4724	1274	1		Port 9 status
4725	1275	1		Port 10 status
4726	1276	1		Port 11 status
4727	1277	1		Port 12 status
4744	1288	1	HEX	Instance ID (Fixed 0x00, 45)
4745	1289	3		Root bridge MAC
4748	128C	1		Port 1 status
4749	128D	1		Port 2 status
4750	128E	1		Port 3 status
4751	128F	1		Port 4 status
4752	1290	1		Port 5 status
4753	1291	1		Port 6 status
4754	1292	1		Port 7 status
4755	1293	1		Port 8 status
4756	1294	1		Port 9 status
4757	1295	1		Port 10 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4758	1296	1		Port 11 status
4759	1297	1		Port 12 status
4776	12A8	1	HEX	Instance ID (Fixed 0x00, 46)
4777	12A9	3		Root bridge MAC
4780	12AC	1		Port 1 status
4781	12AD	1		Port 2 status
4782	12AE	1		Port 3 status
4783	12AF	1		Port 4 status
4784	12B0	1		Port 5 status
4785	12B1	1		Port 6 status
4786	12B2	1		Port 7 status
4787	12B3	1		Port 8 status
4788	12B4	1		Port 9 status
4789	12B5	1		Port 10 status
4790	12B6	1		Port 11 status
4791	12B7	1		Port 12 status
4808	12C8	1	HEX	Instance ID (Fixed 0x00, 47)
4809	12C9	3		Root bridge MAC
4812	12CC	1		Port 1 status
4813	12CD	1		Port 2 status
4814	12CE	1		Port 3 status
4815	12CF	1		Port 4 status
4816	12D0	1		Port 5 status
4817	12D1	1		Port 6 status
4818	12D2	1		Port 7 status
4819	12D3	1		Port 8 status
4820	12D4	1		Port 9 status
4821	12D5	1		Port 10 status
4822	12D6	1		Port 11 status
4823	12D7	1		Port 12 status
4840	12E8	1	HEX	Instance ID (Fixed 0x00, 48)
4841	12E9	3		Root bridge MAC
4844	12EC	1		Port 1 status
4845	12ED	1		Port 2 status
4846	12EE	1		Port 3 status
4847	12EF	1		Port 4 status
4848	12F0	1		Port 5 status
4849	12F1	1		Port 6 status
4850	12F2	1		Port 7 status
4851	12F3	1		Port 8 status
4852	12F4	1		Port 9 status
4853	12F5	1		Port 10 status
4854	12F6	1		Port 11 status
4855	12F7	1		Port 12 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4872	1308	1	HEX	Instance ID (Fixed 0x00, 49)
4873	1309	3		Root bridge MAC
4876	130C	1		Port 1 status
4877	130D	1		Port 2 status
4878	130E	1		Port 3 status
4879	130F	1		Port 4 status
4880	1310	1		Port 5 status
4881	1311	1		Port 6 status
4882	1312	1		Port 7 status
4883	1313	1		Port 8 status
4884	1314	1		Port 9 status
4885	1315	1		Port 10 status
4886	1316	1		Port 11 status
4887	1317	1		Port 12 status
4904	1328	1	HEX	Instance ID (Fixed 0x00, 50)
4905	1329	3		Root bridge MAC
4908	132C	1		Port 1 status
4909	132D	1		Port 2 status
4910	132E	1		Port 3 status
4911	132F	1		Port 4 status
4912	1330	1		Port 5 status
4913	1331	1		Port 6 status
4914	1332	1		Port 7 status
4915	1333	1		Port 8 status
4916	1334	1		Port 9 status
4917	1335	1		Port 10 status
4918	1336	1		Port 11 status
4919	1337	1		Port 12 status
4936	1348	1	HEX	Instance ID (Fixed 0x00, 51)
4937	1349	3		Root bridge MAC
4940	134C	1		Port 1 status
4941	134D	1		Port 2 status
4942	134E	1		Port 3 status
4943	134F	1		Port 4 status
4944	1350	1		Port 5 status
4945	1351	1		Port 6 status
4946	1352	1		Port 7 status
4947	1353	1		Port 8 status
4948	1354	1		Port 9 status
4949	1355	1		Port 10 status
4950	1356	1		Port 11 status
4951	1357	1		Port 12 status
4970	136A	1	HEX	Instance ID (Fixed 0x00, 52)
4971	136B	3		Root bridge MAC
4972	136C	1		Port 1 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
4973	136D	1		Port 2 status
4974	136E	1		Port 3 status
4975	136F	1		Port 4 status
4976	1370	1		Port 5 status
4977	1371	1		Port 6 status
4978	1372	1		Port 7 status
4979	1373	1		Port 8 status
4980	1374	1		Port 9 status
4981	1375	1		Port 10 status
4982	1376	1		Port 11 status
4983	1377	1		Port 12 status
5000	1388	1	HEX	Instance ID (Fixed 0x00, 53)
5001	1389	3		Root bridge MAC
5004	138C	1		Port 1 status
5005	138D	1		Port 2 status
5006	138E	1		Port 3 status
5007	138F	1		Port 4 status
5008	1390	1		Port 5 status
5009	1391	1		Port 6 status
5010	1392	1		Port 7 status
5011	1393	1		Port 8 status
5012	1394	1		Port 9 status
5013	1395	1		Port 10 status
5014	1396	1		Port 11 status
5015	1397	1		Port 12 status
5032	13A8	1	HEX	Instance ID (Fixed 0x00, 54)
5033	13A9	3		Root bridge MAC
5036	13AC	1		Port 1 status
5037	13AD	1		Port 2 status
5038	13AE	1		Port 3 status
5039	13AF	1		Port 4 status
5040	13B0	1		Port 5 status
5041	13B1	1		Port 6 status
5042	13B2	1		Port 7 status
5043	13B3	1		Port 8 status
5044	13B4	1		Port 9 status
5045	13B5	1		Port 10 status
5046	13B6	1		Port 11 status
5047	13B7	1		Port 12 status
5064	13C8	1	HEX	Instance ID (Fixed 0x00, 55)
5065	13C9	3		Root bridge MAC
5068	13CC	1		Port 1 status
5069	13CD	1		Port 2 status
5070	13CE	1		Port 3 status
5071	13CF	1		Port 4 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
5072	13D0	1		Port 5 status
5073	13D1	1		Port 6 status
5074	13D2	1		Port 7 status
5075	13D3	1		Port 8 status
5076	13D4	1		Port 9 status
5077	13D5	1		Port 10 status
5078	13D6	1		Port 11 status
5079	13D7	1		Port 12 status
5096	13E8	1	HEX	Instance ID (Fixed 0x00, 56)
5097	13E9	3		Root bridge MAC
5100	13EC	1		Port 1 status
5101	13ED	1		Port 2 status
5102	13EE	1		Port 3 status
5103	13EF	1		Port 4 status
5104	13F0	1		Port 5 status
5105	13F1	1		Port 6 status
5106	13F2	1		Port 7 status
5107	13F3	1		Port 8 status
5108	13F4	1		Port 9 status
5109	13F5	1		Port 10 status
5110	13F6	1		Port 11 status
5111	13F7	1		Port 12 status
5130	140A	1	HEX	Instance ID (Fixed 0x00, 57)
5131	140B	3		Root bridge MAC
5132	140C	1		Port 1 status
5133	140D	1		Port 2 status
5134	140E	1		Port 3 status
5135	140F	1		Port 4 status
5136	1410	1		Port 5 status
5137	1411	1		Port 6 status
5138	1412	1		Port 7 status
5139	1413	1		Port 8 status
5140	1414	1		Port 9 status
5141	1415	1		Port 10 status
5142	1416	1		Port 11 status
5143	1417	1		Port 12 status
5160	1428	1	HEX	Instance ID (Fixed 0x00, 58)
5161	1429	3		Root bridge MAC
5164	142C	1		Port 1 status
5165	142D	1		Port 2 status
5166	142E	1		Port 3 status
5167	142F	1		Port 4 status
5168	1430	1		Port 5 status
5169	1431	1		Port 6 status
5170	1432	1		Port 7 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	Hex			
System Information				
5171	1433	1		Port 8 status
5172	1434	1		Port 9 status
5173	1435	1		Port 10 status
5174	1436	1		Port 11 status
5175	1437	1		Port 12 status
5192	1448	1	HEX	Instance ID (Fixed 0x00, 59)
5193	1449	3		Root bridge MAC
5196	144C	1		Port 1 status
5197	144D	1		Port 2 status
5198	144E	1		Port 3 status
5199	144F	1		Port 4 status
5200	1450	1		Port 5 status
5201	1451	1		Port 6 status
5202	1452	1		Port 7 status
5203	1453	1		Port 8 status
5204	1454	1		Port 9 status
5205	1455	1		Port 10 status
5206	1456	1		Port 11 status
5207	1457	1		Port 12 status
5224	1468	1	HEX	Instance ID (Fixed 0x00, 60)
5225	1469	3		Root bridge MAC
5228	146C	1		Port 1 status
5229	146D	1		Port 2 status
5230	146E	1		Port 3 status
5231	146F	1		Port 4 status
5232	1470	1		Port 5 status
5233	1471	1		Port 6 status
5234	1472	1		Port 7 status
5235	1473	1		Port 8 status
5236	1474	1		Port 9 status
5237	1475	1		Port 10 status
5238	1476	1		Port 11 status
5239	1477	1		Port 12 status
5256	1488	1	HEX	Instance ID (Fixed 0x00, 61)
5257	1489	3		Root bridge MAC
5260	148C	1		Port 1 status
5261	148D	1		Port 2 status
5262	148E	1		Port 3 status
5263	148F	1		Port 4 status
5264	1490	1		Port 5 status
5265	1491	1		Port 6 status
5266	1492	1		Port 7 status
5267	1493	1		Port 8 status
5268	1494	1		Port 9 status
5269	1495	1		Port 10 status

Tabela 204: Rejestry MODBUS

Adres rejestru		Długość danych/ słowo	Pozycja	Opis
Dec	**Hex**			
System Information				
5270	1496	1		Port 11 status
5271	1497	1		Port 12 status
5288	14A8	1	HEX	Instance ID (Fixed 0x00, 62)
5289	14A9	3		Root bridge MAC
5292	14AC	1		Port 1 status
5293	14AD	1		Port 2 status
5294	14AE	1		Port 3 status
5295	14AF	1		Port 4 status
5296	14B0	1		Port 5 status
5297	14B1	1		Port 6 status
5298	14B2	1		Port 7 status
5299	14B3	1		Port 8 status
5300	14B4	1		Port 9 status
5301	14B5	1		Port 10 status
5302	14B6	1		Port 11 status
5303	14B7	1		Port 12 status
5320	14C8	1	HEX	Instance ID (Fixed 0x00, 63)
5321	14C9	3		Root bridge MAC
5324	14CC	1		Port 1 status
5325	14CD	1		Port 2 status
5326	14CE	1		Port 3 status
5327	14CF	1		Port 4 status
5328	14D0	1		Port 5 status
5329	14D1	1		Port 6 status
5330	14D2	1		Port 7 status
5331	14D3	1		Port 8 status
5332	14D4	1		Port 9 status
5333	14D5	1		Port 10 status
5334	14D6	1		Port 11 status
5335	14D7	1		Port 12 status

Spis ilustracji

Ilustracja 1: Widok przemysłowego switcha zarządzalnego z przodu 23
Ilustracja 2: Widok przemysłowego switcha zarządzalnego z góry 25
Ilustracja 3: Śruba uziemienia 26
Ilustracja 4: Złącze zasilające (PWR/RPS) 27
Ilustracja 5: Złącza sieciowe 28
Ilustracja 6: LED urządzeń 31
Ilustracja 7: LED złącz 32
Ilustracja 8: Mikroprzełączniki DIP 33
Ilustracja 9: Przycisk resetu 34
Ilustracja 10: Naklejka 35
Ilustracja 11: Diagram przebiegu tabeli adresów MAC 50
Ilustracja 12: Tryb half duplex 52
Ilustracja 13: Tryb full duplex 52
Ilustracja 14: MOD bez MVR 67
Ilustracja 15: MOD wspiera MVR 67
Ilustracja 16: Adres multicast 70
Ilustracja 17: Q-in-Q na bazie portów 80
Ilustracja 18: Przykład konfiguracji 81
Ilustracja 19: Zastosowanie 1 (przez ruter) 83
Ilustracja 20: Zastosowanie 2 (lokalnie w różnych sieciach VLAN) 83
Ilustracja 21: Dual Homing 87
Ilustracja 22: Dual Ring Switch ABC 88
Ilustracja 23: Dual Ring switch AB 88
Ilustracja 24: Jet Ring 96
Ilustracja 25: DHCP Snooping 109
Ilustracja 26: IEEE 802.1X 114
Ilustracja 27: Serwer RADIUS 114
Ilustracja 28: Funkcje USB, zakładanie katalogu 124
Ilustracja 29: Funkcje USB, plik firmware'u w katalogu 124
Ilustracja 30: Funkcje USB, zakładanie katalogu 125
Ilustracja 31: Funkcje USB, plik konfiguracyjny w katalogu 126
Ilustracja 32: Strona WBM „System Information“ 134
Ilustracja 33: Strona WBM „General Settings“ – zakładka „System“ 136
Ilustracja 34: Strona WBM „General Settings“ – zakładka „Jumbo Frame” 138
Ilustracja 35: Strona WBM „General Settings“ – zakładka „SNTP” 139
Ilustracja 36: Strona WBM „General Settings“ – zakładka „Management Host“ 142
Ilustracja 37: Strona WBM „MAC Management“ – zakładka „Static MAC Settings” 143
Ilustracja 38: Strona WBM „MAC Management“ – zakładka „MAC Table” 145
Ilustracja 39: Strona WBM „MAC Management“ – zakładka „Age Time Setting” 146
Ilustracja 40: Strona WBM „MAC Management“ – zakładka „Blacklisting” 147
Ilustracja 41: Strona WBM „Port Mirroring” 148
Ilustracja 42: Strona WBM „Port Settings“ – zakładka „General Settings“ 150
Ilustracja 43: Strona WBM „Port Settings” – zakładka „Information” 152
Ilustracja 44: Strona WBM „QoS” – zakładka „Port Priority” 153
Ilustracja 45: Strona WBM „QoS” – zakładka „IP DiffServ (DSCP)” 154

Ilustracja 46: Strona WBM „QoS” – zakładka „Priority/Queue Mapping“ 155
Ilustracja 47:: Strona WBM „QoS“ – zakładka „Schedule Mode“.....156
Ilustracja 48: Strona WBM „Rate Limitation“ – zakładka „Strom Control“.....158
Ilustracja 49: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“ 160
Ilustracja 50: Strona WBM „IGMP Snooping“ – zakładka „General Settings“ 162
Ilustracja 51: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“ 164
Ilustracja 52: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings“.....166
Ilustracja 53: Strona WBM „IGMP Filtering“ – zakładka „General Settings“ 167
Ilustracja 54: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“ 168
Ilustracja 55: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“ 169
Ilustracja 56: Strona WBM „Multicast VLAN Registration“ – zakładka „MVR Settings“.....170
Ilustracja 57: Strona WBM „Multicast VLAN Registration“ – zakładka „Group Settings“.....172
Ilustracja 58: Strona WBM „Static Multicast“.....173
Ilustracja 59: Strona WBM „Multicast Statistics“ 174
Ilustracja 60: Strona WBM „Port Isolation“.....175
Ilustracja 61: Strona WBM „VLAN“ – zakładka „VLAN Settings“ 177
Ilustracja 62: Strona WBM „VLAN“ – zakładka „Tag Settings“ 179
Ilustracja 63: Strona WBM „VLAN“ – zakładka „Port Settings“.....180
Ilustracja 64: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP“ 182
Ilustracja 65: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP Timer“ 184
Ilustracja 66: Strona WBM „IP Subnet VLAN“.....186
Ilustracja 67: Strona WBM „MAC VLAN“ 187
Ilustracja 68: Strona WBM „Protocol VLAN“ 188
Ilustracja 69: Strona WBM „Q-in-Q“ – zakładka „VLAN Stacking“.....189
Ilustracja 70: Strona WBM „Q-in-Q“ – zakładka „Port-based Q-in-Q“.....191
Ilustracja 71: Strona WBM „Q-in-Q“ – zakładka „Selective Q-in-Q“.....192
Ilustracja 72: Strona WBM „DHCP Relay“ 194
Ilustracja 73: Strona WBM „DHCP Options“ 195
Ilustracja 74: Strona WBM „DHCP Server“ – zakładka „General Settings“.....197
Ilustracja 75: Strona WBM „DHCP Server“ – zakładka „Pool Settings“ 199
Ilustracja 76: Strona WBM „DHCP Server“ – zakładka „Binding Information“ ...203
Ilustracja 77: Strona WBM „DHCP Server“ – zakładka „Statistics“.....204
Ilustracja 78: Strona WBM „Dual Homing“ 205
Ilustracja 79: Strona WBM „Dual Ring“ 207
Ilustracja 80: Strona WBM „ERPS“ – zakładka „Ring Settings“.....209
Ilustracja 81: Strona WBM „ERPS“ – zakładka „Instance Settings“.....213
Ilustracja 82: Strona WBM „Link Aggregation“ – zakładka „Static Trunk“.....214
Ilustracja 83: Strona WBM „Link Aggregation“ – zakładka „LACP“.....216
Ilustracja 84: Strona WBM „Link Aggregation“ – zakładka „LACP info.“.....218
Ilustracja 85: Strona WBM „LLDP“ – zakładka „LLDP Settings“.....220
Ilustracja 86: Strona WBM „LLDP“ – zakładka „Neighboring Detection“.....222
Ilustracja 87: Strona WBM „Loop Detection“.....223
Ilustracja 88: Strona WBM „Jet Ring“ 225
Ilustracja 89: Strona WBM „Modbus“.....227
Ilustracja 90: Strona WBM „PoE“ – zakładka „Configuration“.....228

Ilustracja 91: Strona WBM „PoE“ – zakładka „Schedule“ 230
Ilustracja 92: Strona WBM „PoE“ – zakładka „PD Alive Check“ 233
Ilustracja 93: Strona WBM „PoE“ – zakładka „Power Delay“....236
Ilustracja 94: Strona WBM „Static Route“ 238
Ilustracja 95: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“....240
Ilustracja 96: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“ 242
Ilustracja 97: Strona WBM „Spanning Tree Protocol“ – zakładka „STP Status“ 245
Ilustracja 98: Strona WBM „Xpress Ring“ 246
Ilustracja 99: Strona WBM „DHCP Snooping“ – zakładka „DHCP Snooping“ ...248
Ilustracja 100: Strona WBM „DHCP Snooping“ – zakładka „Port Settings“ 250
Ilustracja 101: Strona WBM „DHCP Snooping“ – zakładka „Server Screening“ 251
Ilustracja 102: Strona WBM „DHCP Snooping Binding Table“ – zakładka „Static Entry Settings“ 252
Ilustracja 103: Strona WBM „DHCP-Snooping-Binding Table“ – zakładka „Binding Table“....254
Ilustracja 104: Strona WBM „ARP Inspection“ – zakładka „ARP Inspection“....255
Ilustracja 105: Strona WBM „ARP Inspection“ – zakładka „Filter Table“ 257
Ilustracja 106: Strona WBM „Access Control List“ 258
Ilustracja 107: Strona WBM „IEEE 802.1X“ – zakładka „Global Settings“ 262
Ilustracja 108: Strona WBM „IEEE 802.1X“ – zakładka „Port Settings“....265
Ilustracja 109: Strona WBM „Port Security“ – zakładka „Port Security“....269
Ilustracja 110: Strona WBM „Port Security“ – zakładka „Sticky MAC Settings“ .271
Ilustracja 111: Strona WBM „Alarm Information“....272
Ilustracja 112: Strona WBM „System Information” 273
Ilustracja 113: Strona WBM „Port Statistics“ 275
Ilustracja 114: Strona WBM „Port Utilization“....276
Ilustracja 115: Strona WBM „RMON Statistics“....277
Ilustracja 116: Strona WBM „SFP Information“ 280
Ilustracja 117: Strona WBM „Traffic Monitor“....283
Ilustracja 118: Strona WBM „SNMP“ – zakładka „SNMP Settings“ 286
Ilustracja 119: Strona WBM „SNMP“ – zakładka „Community Name“....287
Ilustracja 120: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“ 289
Ilustracja 121: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“ 291
Ilustracja 122: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“ 292
Ilustracja 123: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“ 293
Ilustracja 124: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“....295
Ilustracja 125: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“ 296
Ilustracja 126: Strona WBM „Auto Provision“....297
Ilustracja 127: Strona WBM „Mail Alarm“....298
Ilustracja 128: Strona WBM „Maintenance“ – zakładka „Configuration“....300
Ilustracja 129: Strona WBM „Maintenance“ – zakładka „Firmware“ 302
Ilustracja 130: Strona WBM „Maintenance“ – zakładka „Reboot“....303
Ilustracja 131: Strona WBM „Maintenance“ – zakładka „Reboot“ – Message ...303
Ilustracja 132: Strona WBM „Maintenance“ – zakładka „Protocols“ 304

Ilustracja 133: Strona WBM „System Log“ 306
Ilustracja 134: Strona WBM „Ping“ 308
Ilustracja 135: Strona WBM „USB Functions“ 309
Ilustracja 136: Strona WBM „User Account” 310
Ilustracja 137: Obłożenie zacisków RJ-45 312
Ilustracja 138: Obłożenie zacisków RJ-45 do DB9 312

Spis tabel

Tabela 1: Zastosowane systemy liczbowe....13
Tabela 2: Sposoby zapisu....13
Tabela 3: Opis do ilustracji „Widok przemysłowego switcha zarządzalnego z przodu”....23
Tabela 4: Opis do ilustracji „Widok przemysłowego switcha zarządzalnego z góry”....25
Tabela 5: Opis ilustracji „Złącze zasilające (PWR/RPS)”....27
Tabela 6: Opis ilustracji „Złącza sieciowe”....28
Tabela 7: Opis ilustracjii „LED urządzeń“....31
Tabela 8: Opis ilustracji „LED złącz“....32
Tabela 9: Opis ilustracji „Mikroprzełączniki DIP“....33
Tabela 10: Opis ilustracji „Przycisk resetu“....34
Tabela 11: Opis ilustracji „Naklejka“....35
Tabela 12: Dane techniczne – dane urządzenia....36
Tabela 13: Dane techniczne – dane systemowe....36
Tabela 14: Dane techniczne – zasilanie....36
Tabela 15: Dane techniczne – Power over Ethernet (PoE)....36
Tabela 16: Dane techniczne – komunikacja....37
Tabela 17: Dane techniczne – warunki środowiskowe....38
Tabela 18: Poziomy priorytetu....58
Tabela 19: Klasy multicast i zakresy adresów....69
Tabela 20: Adres IP multicast....70
Tabela 21: Option Frame Format....85
Tabela 22: Option Frame Format....85
Tabela 23: Frame Format podopcji „Circuit ID“....85
Tabela 24: Frame Format podopcji „Remote ID“....85
Tabela 25: Format podopcji „Circuit ID“....85
Tabela 26: Porównanie PoE i PoE+....97
Tabela 27: Przykład obliczeń dla PoE+....97
Tabela 28: Koszty trasy STP....101
Tabela 29: Domyślne ustawienia dla portu Telnet....128
Tabela 30: Domyślne ustawienia dla portu konsolowego....129
Tabela 31: Ekran logowania....129
Tabela 32: Przegląd – linki nawigacyjne i strony systemu zarządzania przez WWW (WBM)....131
Tabela 33: Strona WBM „System Information“....135
Tabela 34: Strona WBM „General Settings“ – zakładka „System“....137
Tabela 35: Strona WBM „General Settings“ – zakładka „Jumbo Frame”....138
Tabela 36: Strona WBM „General Settings“ – zakładka „SNTP”....140
Tabela 37: Strona WBM „General Settings“ – zakładka „Management Host“....142
Tabela 38: Strona WBM „MAC Management“ – zakładka „Static MAC Settings”....144
Tabela 39: Strona WBM „MAC Management“ – zakładka „MAC Table”....145
Tabela 40: Strona WBM „MAC Management” – zakładka „Age Time Setting”....146
Tabela 41: Strona WBM „MAC Management“ – zakładka „Blacklisting”....147
Tabela 42: Strona WBM „Port Mirroring”....149
Tabela 43: Strona WBM „Port Settings” – zakładka „General Settings”....151

Tabela 44: Strona WBM „Port Settings” – zakładka „Information”.....152
Tabela 45: Strona WBM „QoS” – zakładka „Port Priority”.....153
Tabela 46: Strona WBM „QoS” – zakładka „IP DiffServ (DSCP)”.....154
Tabela 47: Strona WBM „QoS“ – zakładka „Priority/Queue Mapping“.....155
Tabela 48: Default Settings.....155
Tabela 49: Strona WBM „QoS“ – zakładka „Schedule Mode“.....157
Tabela 50: Strona WBM „Rate Limitation“ – zakładka „Storm Control“.....159
Tabela 51: Strona WBM „Rate Limitation“ – zakładka „Bandwidth Limitation“..161
Tabela 52: Strona WBM „IGMP Snooping“ – zakładka „General Settings“.....163
Tabela 53: Strona WBM „IGMP Snooping“ – zakładka „Port Settings“.....165
Tabela 54: Strona WBM „IGMP Snooping“ – zakładka „Querier Settings.....166
Tabela 55: Strona WBM „IGMP Filtering“ – zakładka „General Settings“.....167
Tabela 56: Strona WBM „IGMP Filtering“ – zakładka „Multicast Groups“.....168
Tabela 57: Strona WBM „IGMP Filtering“ – zakładka „Port Settings“.....169
Tabela 58: Strona WBM „Multicast VLAN Registration“ – zakładka „MVR Settings“.....171
Tabela 59: Strona WBM „Multicast VLAN Registration“ – zakładka „Group Settings“.....172
Tabela 60: Strona WBM „Static Multicast“.....173
Tabela 61: Strona WBM „Multicast Statistics“.....174
Tabela 62: Strona WBM „Port Isolation“.....176
Tabela 63: Strona WBM „VLAN“ – zakładka „VLAN Settings“.....178
Tabela 64: Strona WBM „VLAN“ – zakładka „Tag Settings“.....179
Tabela 65: Strona WBM „VLAN“ – zakładka „Port Settings“.....181
Tabela 66: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP“.....183
Tabela 67: Strona WBM „GARP VLAN Registration Protocol“ – zakładka „GVRP Timer“.....185
Tabela 68: Strona WBM „IP Subnet VLAN“.....186
Tabela 69: Strona WBM „MAC VLAN“.....187
Tabela 70: Strona WBM „Protocol VLAN“.....188
Tabela 71: Strona WBM „Q-in-Q“ – zakładka „VLAN Stacking“.....190
Tabela 72: Strona WBM „Q-in-Q“ – zakładka „Port-based Q-in-Q“.....191
Tabela 73: Strona WBM „Q-in-Q“ – zakładka „Selective Q-in-Q“.....193
Tabela 74: Strona WBM „DHCP Relay“.....194
Tabela 75: Strona WBM „DHCP Options“.....196
Tabela 76: Strona WBM „DHCP Server“ – zakładka „General Settings“.....198
Tabela 77: Strona WBM „DHCP Server“ – zakładka „Pool Settings“.....200
Tabela 78: Strona WBM „DHCP Server“ – zakładka „Binding Information“.....203
Tabela 79: Strona WBM „DHCP Server“ – zakładka „Statistics“.....204
Tabela 80: Strona WBM „Dual Homing“.....206
Tabela 81: Strona WBM „Dual Ring“.....208
Tabela 82: Strona WBM „ERPS“ – zakładka „Ring Settings“.....210
Tabela 83: Strona WBM „ERPS“ – zakładka „Instance Settings“.....213
Tabela 84: Strona WBM „Link Aggregation“ – zakładka „Static Trunk“.....215
Tabela 85: Strona WBM „Link Aggregation“ – zakładka „LACP“.....217
Tabela 86: Strona WBM „Link Aggregation“ – zakładka „LACP Info.“.....219
Tabela 87: Strona WBM „LLDP“ – zakładka „LLDP Settings“.....221
Tabela 88: Strona WBM „LLDP“ – zakładka „Neighboring Detection“.....222
Tabela 89: Strona WBM „Loop Detection“.....224

Tabela 90: Strona WBM „Jet Ring“ 226
Tabela 91: Strona WBM „Modbus“ 227
Tabela 92: Strona WBM „PoE“ – zakładka „Configuration“ 229
Tabela 93: Strona WBM „PoE“ – zakładka „Schedule“ 231
Tabela 94: Strona WBM „PoE“ – zakładka „PD Alive Check“ 234
Tabela 95: Strona WBM „PoE“ – zakładka „Power Delay“ 237
Tabela 96: Strona WBM „Static Route“ 239
Tabela 97: Strona WBM „Spanning Tree Protocol“ – zakładka „General Settings“ 241
Tabela 98: Strona WBM „Spanning Tree Protocol“ – zakładka „Port Parameters“ 243
Tabela 99: Strona WBM „STP“ – zakładka „STP-Status“ 245
Tabela 100: Strona WBM „Xpress Ring“ 247
Tabela 101: Strona WBM „DHCP Snooping“ – zakładka „DHCP Snooping“ 249
Tabela 102: Strona WBM „DHCP Snooping“ – zakładka „Port Settings“ 250
Tabela 103: Strona WBM „DHCP Snooping“ – zakładka „Server Screening“ 251
Tabela 104: Strona WBM „DHCP Snooping Binding Table“ – zakładka „Static Entry Settings“ 253
Tabela 105: Strona WBM „DHCP-Snooping-Binding Table“ – zakładka „Binding Table“ 254
Tabela 106: Strona WBM „ARP Inspection“ – zakładka „ARP Inspection“ 256
Tabela 107: Strona WBM „ARP Inspection“ – zakładka „Filter Table“ 257
Tabela 108: Strona WBM „Access Control List“ 259
Tabela 109: Strona WBM „IEEE 802.1X“ – zakładka „Global Settings“ 263
Tabela 110: Strona WBM „IEEE 802.1X“ – zakładka „Port Settings“ 266
Tabela 111: Strona WBM „Port Security“ – zakładka „Port Security“ 270
Tabela 112: Strona WBM „Port Security“ – zakładka „Sticky MAC Settings“ 271
Tabela 113: Strona WBM „Alarm Information“ 272
Tabela 114: Strona WBM „System Information“ 274
Tabela 115: Strona WBM „Port Statistics“ 275
Tabela 116: Strona WBM „Port Utilization“ 276
Tabela 117: Strona WBM „RMON Statistics“ 278
Tabela 118: Strona WBM „SFP Information“ 281
Tabela 119: Strona WBM „Traffic Monitor” 284
Tabela 120: Strona WBM „SNMP“ – zakładka „SNMP Settings“ 286
Tabela 121: Strona WBM „SNMP“ – zakładka „Community Name“ 288
Tabela 122: Strona WBM „SNMP Trap“ – zakładka „Trap Receiver Settings“ ..290
Tabela 123: Strona WBM „SNMP Trap“ – zakładka „Trap Event State“ 291
Tabela 124: Strona WBM „SNMP Trap“ – zakładka „Port Trap Settings“ 292
Tabela 125: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 User“ 294
Tabela 126: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 Group“ 295
Tabela 127: Strona WBM „SNMPv3 Configuration“ – zakładka „SNMPv3 View“ 296
Tabela 128: Strona WBM „Auto Provision“ 297
Tabela 129: Strona WBM „Mail Alarm“ 299
Tabela 130: Strona WBM „Maintenance“ – zakładka „Protocols“ 305
Tabela 131: Strona WBM „System Log“ 307
Tabela 132: Strona WBM „Ping“ 308

Tabela 133: Strona WBM „USB Functions“ 309
Tabela 134: Strona WBM „User Account” 311
Tabela 135: Przewód RJ-45 313
Table 136: CLI “System Information” Configuration 314
Table 137: CLI “System” Configuration 315
Table 138: CLI “Jumbo Frame” Configuration 316
Table 139: CLI “SNTP” Configuration 317
Table 140: CLI “Management Host” Configuration 318
Table 141: CLI “MAC Management” Configuration 319
Table 142: CLI “Blackhole MAC” Configuration 319
Table 143: CLI “Port Mirroring” Configuration 320
Table 144: CLI “Port Settings” Configuration 321
Table 145: CLI “QoS” Configuration 322
Table 146: CLI “Rate Limitation” Configuration 323
Table 147: CLI “Storm Control” Configuration 323
Table 148: CLI “IGMP Snooping” Configuration 324
Table 149: CLI “IGMP Snooping Querier” Configuration 326
Table 150: CLI “IGMP Snooping Filtering” Configuration 326
Table 151: CLI “MVR” Configuration 327
Table 152: CLI “Multicast Address” Configuration 328
Table 153: CLI “Port Isolation” Configuration 328
Table 154: CLI “VLAN Settings” Configuration 330
Table 155: CLI “GARP/GVRP” Configuration 331
Table 156: CLI “IP Subnet VLAN” Configuration 332
Table 157: CLI “MAC VLAN” Configuration 332
Table 158: CLI “Protocol VLAN” Configuration 333
Table 159: CLI “VLAN Stacking” Configuration 335
Table 160: CLI “DHCP Relay” Configuration 336
Table 161: CLI “DHCP Options” Configuration 337
Table 162: CLI “Dual Homing” Configuration 337
Table 163: CLI “ERPS” Configuration 338
Table 164: CLI “Link Aggregation” Configuration 339
Table 165: CLI “LACP” Configuration 340
Table 166: CLI “LLDP” Configuration 341
Table 167: CLI “Loop Detection” Configuration 342
Table 168: CLI “Modbus” Configuration 343
Table 169: CLI “PoE” Configuration 343
Table 170: CLI “PoE Schedule” Configuration 343
Table 171: CLI “PD Alive Check” Configuration 344
Table 172: CLI “Power Delay” Configuration 344
Table 173: CLI “Static Route” Configuration 346
Table 174: CLI “STP” Configuration 349
Table 175: CLI “MSTP” Configuration 352
Table 176: CLI “Xpress Ring” Configuration 353
Table 177: CLI “DHCP Snooping” Configuration 354
Table 178: CLI “Server Screening” Configuration 355
Table 179: CLI “Binding Table” Configuration 355
Table 180: CLI “ARP Inspection” Configuration 356
Table 181: CLI “Filter Table” Configuration 356
Table 182: CLI “Access Control List” Configuration 358

Table 183: CLI “802.1X” Configuration 361
Table 184: CLI “Port Security” Configuration 362
Table 185: CLI “Alarm” Configuration 363
Table 186: CLI “Monitor Information” Configuration 363
Table 187: CLI “Port Statistics” Configuration 363
Table 188: CLI “Port Statistics” Configuration 363
Table 189: CLI “RMON Statistics” Configuration 363
Table 190: CLI “SFP Information” Configuration 363
Table 191: CLI “Traffic Monitor” Configuration 364
Table 192: CLI “SNMP” Configuration 365
Table 193: CLI “SNMP Trap” Configuration 366
Table 194: CLI “Port Trap Settings” Configuration 366
Table 195: CLI “SNMPv3” Configuration 367
Table 196: CLI “Auto Provision” Configuration 368
Table 197: CLI “Mail Alarm” Configuration 368
Table 198: CLI “Maintenance” Configuration 369
Table 199: CLI “Reboot” Configuration 370
Table 200: CLI “System Log” Configuration 370
Table 201: CLI “USB Flash” Configuration 371
Table 202: CLI “System Log” Configuration 372
Tabela 203: Format danych i kod funkcji 373
Tabela 204: Rejestry MODBUS 374

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