

RODZINA PRZEMYSŁOWYCH PRZEŁĄCZNIKÓW

HYPERION

INSTRUKCJA OBSŁUGI SOFTWARE GUI i CLI

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2	2024.01.04	1/147
---	------------	-------



Spis treści

11 Zgodność z normanii zaleceniami. 4 12 Zgoraczenie. 5 2 OPIS FUNKCJONALNY. 5 11 Parkeja Zastosowania. 5 31 Instalacja Iobsługa 6 31 Instalacja Iobsługa 6 32 Instalacja Iobsługa 7 32 Zasady posługiwania się zączami światkowodowymi. 7 42 Zarządzanie. 7 50 pis GUI dostępnego przez przeglądarkę WWW. 7 51 Ochrona urządzenia hastem. 8 53 Konfiguracja otski Ethernet. 11 54 Konfiguracja potów z POreckino Przelacznikach wyposażonych w dodatkowy modul REDBOX). 12 54 Konfiguracja potów zy Poreckino Przelacznikach wyposażonych w dodatkowy modul REDBOX). 12 54 Konfiguracja potów zy Poreckino Przelacznikach wyposażonych w dodatkowy modul REDBOX). 12 54 Konfiguracja Potów Zy POREK OVER ETHERNET (opcja w wybranych przelącznikach). 22 54 Konfiguracja HTTPS 22 51 Konfiguracja Potów Uwierzytelniania oraz autoryzacji. 24 51 Konfiguracja HTTPS 26	1 INFORMACJE PODSTAWOWE	4
12 Corper FUNKCJONALNY. 5 2.1 Funkcje i Zastosowania. 5 3.1 Instalacja i obsługa. 6 3.1 Warunki pracy. 6 3.2 Instalacja i obsługa. 7 3.3 Zasady posłujiwani się zjączami światłowodowymi. 7 3.4 Zaradzania 7 5 Obsługa. 7 6 Konfiguracja brothy Uradite Network Processonych w dodatkowy modul REDBOX). 9 6 Porlu HSR (opcja wybranych przejącznikach wyposażonych w dodatkowy modul REDBOX). 9 7 Rofiguracja Porlow Uradite Network Precedent Proceson. 23 8 Notniguracja Porlow Uradite Network Precedent Proceon. 22	1.1 Zgodność z normami i zaleceniami	4
2 OPIS FUNKCJONALNY. 5 3 Instalacja i obsluga 6 3 Instalacja i obsluga 6 3 Instalacja i obsluga 7 3 Zasady opslugivania się zjączami światlowodowymi 7 3 Zasady opslugivania się zjączami światlowodowymi 7 4 Zarządzanie. 7 5 Opis GUI dostępnego przez przeglądarkę WWW. 7 5 Opis GUI dostępnego przez przeglądarkę WWW. 7 5 Nonfiguracja optów Ethernet. 7 5 Konfiguracja optów Ethernet. 17 5 Konfiguracja potów ZPOWER OVER ETHERNET (opcja w wybranych przełącznikach) 9 6.7 Konfiguracja protów UPWER OVER ETHERNET (opcja w wybranych przełącznikach) 23 50 Konfiguracja metod witerytelniania orza autoryzacji 24 51 SALCoses Scorer 38 51 Stacess Control List 40 51 Natyreitskieniania, and Accounting. 44 51 SALCoses Scorer 38 52 Alektork Access Stever 35 52 Accesacja protów 43 </td <td>1.2 Oznaczenie</td> <td>5</td>	1.2 Oznaczenie	5
2.1 Funkcje i Zastosowania 5 3.1 Instalacja o Iosbluga. 6 3.1 Warunki pracy. 6 3.2 Instalacja o Iosbluga. 7 3.3 Zasady posługiwania się żłączami światkowodowymi. 7 3.7 Zasady posługiwania się żłączami światkowodowymi. 7 4 Zarządzania Jastem 7 5 Ochrona uzrądzenia hastem 8 5.2 Własowości ogólne. 9 5.3 Konfiguracja otstępu urządzenia do sieci IP. 12 5.4 Konfiguracja portów Elhernet. 17 5.6 Konfiguracja portów Urządzenia do sieci IP. 12 5.6 Konfiguracja portów Urządzenia do sieci IP. 12 5.7 Konfiguracja portów Urządzenia do sieci IP. 12 5.8 Konfiguracja portów Urządzenia do sieci IP. 12 5.8 Konfiguracja portów Urządzenia za za utoryzzeji. 24 5.9 Konfiguracja portów Urządzenia do sieci IP. 21 5.10 Konfiguracja metod uwieczytelniania oraz autoryzeji. 24 5.10 Konfiguracja portów Urządzenia do sieci IP. 23 5.11 Network Access Server 24 5.12 Konfiguracja Profitu Urządzenia do sieci IP. 23 5.13 Konfiguracja profitu Urządzenia do sieci IP. 24	2 OPIS FUNKCJONALNY	5
3 Instalacja Lobsluga	2.1 Funkcje i Zastosowania	5
3.1 Warniki pracy	3 Instalacja i obsługa	6
3.2 Testaladja. 7 3.2 Zasady poslugiwania się Złączami światłowodowymi. 7 4.2 Zarządzanie 7 5.0 pis GUI dostępnego przez przeglądarkę WWW. 7 5.1 Ochrona urządzenia hasłem 8 5.2 Właściwości ogólne. 9 5.3 Konfiguracja dostępu urządzenia do sieci IP. 12 5.4 Konfiguracja portów Elhernett. 17 5.5 Konfiguracja portów Elhernett. 17 5.6 Orzniczacja portów Urbarnych przejącznikach wyposażonych w dodatkowy modul REDBOX). 19 5.7 Konfiguracja portów Urbarnych przejącznikach wyposażonych w dodatkowy modul REDBOX). 12 5.7 Konfiguracja portów Urbarnych przejącznikach wyposażonych w dodatkowy modul REDBOX). 12 5.7 Konfiguracja portów Management Protocol. 22 5.10 Konfiguracja metod uwiteryztelniania oraz autoryzacji. 24 5.11 Konfiguracja metod uwiteryztelniania oraz autoryzacji. 24 5.12 SNUP Simple Network Management Protocol. 27 5.13 Natheriters Celard. 43 5.14 Natheriters Celard. 44 <	3.1 Warunki pracy	6
3.3 Zasady posługiwania się żączami światłowodowymi. 7 75 Opis GUI dostępnego przez przeglądarkę WWW. 7 51 Ochrona urządzenia hastem. 8 52 Wiaściwości ogólne. 9 53 Konfiguracja dostępu urządzenia do sieci IP. 12 54 Konfiguracja protów Ethernet. 17 55 Konfiguracja protów Ethernet. 17 56 PPI lub HSR (opcja w wybranych przełącznikach wyposażonych w dodatkowy moduł REDBOX). 19 57 Konfiguracja protów 2 POWER OVER ETHERNET (opcja w wybranych przełącznikach) 21 58 Konfiguracja protów 2 POWER OVER ETHERNET (opcja w wybranych przełącznikach) 23 59 Konfiguracja protów 2 POWER OVER ETHERNET (opcja w wybranych przełącznikach) 23 51 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 51 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 51 Konfiguracja metod uwierzytelniania oraz autoryzacji. 26 51 Konfiguracja metod uwierzytelniania oraz autoryzacji. 26 51 Konfiguracja metod uwierzytelniania oraz autoryzacji. 26 51 Konfiguracja hortów Uroł Configuration. 36 51 Konfiguracja hortów Uroł Configuration. 36 51 Konfiguracja hortów Uroł Configuration. 37 51 Konfiguracja hortó	3.2 Instalacja	7
4 Zarządznie 7 5 Opis GUI dostępnego przez przeglądarkę WWW 7 5 Opis GUI dostępnego przez przeglądarkę WWW 8 5 Właściwości ogólne 9 5 Właściwości ogólne 9 5 Konfiguracja otośw Ethernet 12 5 Konfiguracja portów Ethernet 17 5 Konfiguracja portów Ethernet 19 5 Konfiguracja portów Veybranych przejącznikach wyposażonych w dodatkowy moduł REDBOX). 19 5 Konfiguracja portów Usternet 23 5 Konfiguracja portów Usterzytelniania oraz autoryzacji. 24 5 Konfiguracja netod witerzytelniania oraz autoryzacji. 26 5 Konfiguracja netod witerzytelniania oraz autoryzacji. 26 5 Na Netowick Access Server. 38 5 Na Konfiguracja netod witerzytelniania oraz autoryzacji. 26 5 Konfiguracja netod witerzytelniania oraz autoryzacji. 26 5 Na Nationa and Accounting. 27 5 Na N	3.3 Zasady posługiwania się złączami światłowodowymi	7
5 Opis GUI dostępnego przez przejądarkę WWW	4 Zarządzanie	7
5.1 Ochrona urządzenia hasłem. 8 2.1 Właściwości ogólne 9 5.3 Konfiguracja otoku Ethernet. 12 5.4 Konfiguracja portów Ethernet. 17 5.6 PRP lub KSR (opcja wybranych przejącznikach wyposażonych w dodatkowy moduł REDBOX). 19 5.6 Ornfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przejącznikach). 21 5.8 Ograniczenie dostępu zdalnego. 23 5.9 Konfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przejącznikach). 23 5.0 Konfiguracja prziomu uprawnień. 23 5.10 Konfiguracja HTPS. 26 5.11 Konfiguracja HTPS. 26 5.12 SINJIP Simple Network Management Protocol 27 5.13 Port Secutify Limit Contol Configuration. 36 5.14 Acteess Server. 38 5.15 Access Control List. 40 5.14 Authentication, Authorization and Accounting. 44 5.14 Authentication, Authorization and Accounting. 46 5.21 Server DHCP (dostepny w wybranych wersjach urządzeń). 33 5.22 Stop Protokól IUDP-MCD. 55 5.23 Loop Protokól IUDP-MCD. 56 5.24 Protokól ILDP-MED. 56 5.25 Konfiguracja sici ULAN w wersji oprogramowan	5 Opis GUI dostępnego przez przeglądarkę WWW	7
5.2 Windschwosci ogólne 9 5.3 Konfiguracja dostępu urządzenia do sieci IP. 12 5.4 Konfiguracja dostępu urządzenia do sieci IP. 17 5.5 Konfiguracja hotow Elhernet. 17 5.6 Konfiguracja hotow Elhernet. 17 5.7 Konfiguracja hotow Elovelka OVER OVER ETHERNET (lopcja w wybranych przejącznikach). 23 5.9 Konfiguracja potow u zyborawnień. 23 5.9 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.11 Konfiguracja HTTPS. 26 5.12 Strof Bourde HTPS. 26 5.13 Port Bourde HTPS. 27 5.14 Network Access Server 36 5.15 Access Control Configuration. 36 5.16 IP Source Guard. 37 5.17 ARP Inspection 44 5.28 Konfiguracja portów. 35 5.29 Konfiguracja portók Withorization and Accounting. 46 5.19 ARP Inspection 44 5.21 Sonfiguracja portók. 35 5.22 Aregacja portók. 35 5.23 Konfiguracja portók Withorization and Accounting. 46 5.24 Konfiguracja portók. 55 <t< td=""><td>5.1 Ochrona urządzenia hasłem</td><td>8</td></t<>	5.1 Ochrona urządzenia hasłem	8
5.3 Konfiguracja portów Ehernet. 17 5.4 Konfiguracja portów Ehernet. 17 5.5 Konfiguracja portów Ehernet. 17 5.6 PRP lub INSR (pocja w wybranych przełącznikach wyposażonych w dodatkowy moduł REDBOX). 19 5.7 Konfiguracja portów Urzkalnego. 23 5.8 Ogranizacja notów wierzychelniania oraz autoryzacji. 23 5.10 Konfiguracja moto wierzychelniania oraz autoryzacji. 24 5.11 Konfiguracja moto wierzychelniania oraz autoryzacji. 24 5.12 SNMP Simple Network Management Protocol. 27 5.13 Port Security Limit Control Configuration. 36 5.14 Active Access Server. 36 5.15 Access Control List. 40 5.14 Authentication, Authorization and Accounting. 44 5.18 Active Access 47 5.21 Server DHCP (dostepny w wybranych wersjach urządzeń). 49 5.22 Sorpotection. 54 5.23 Loop Protection. 54 5.24 Konfiguracja protik MVR. 55 5.25 Sorfiguracja serici VLAN. 55	5.2 Właściwości ogólne	9
5.4 Konfiguracja potrów Ethernet. 17 5.5 Konfiguracja Thermal Protection 19 5.6 Konfiguracja potrów 2 POWER OVER ETHERNET (opcja w wybranych przełącznikach) 21 5.7 Konfiguracja potrów 2 POWER OVER ETHERNET (opcja w wybranych przełącznikach) 23 5.9 Konfiguracja potrów 2 POWER OVER 24 5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.11 Konfiguracja HTTPS. 26 5.12 SNMP Simple Network Management Protocol. 27 5.13 Port Security Limit Control Configuration. 38 5.14 Network Access Server 38 5.15 IA PSE Control List. 40 5.16 IP Source Guard. 43 5.17 ACCS+ 47 5.20 Green Ethernet 48 5.21 SouPP Detection 44 5.21 SouP Protection 44 5.22 Green Ethernet 48 5.23 Loop Protection 44 5.24 Konfiguracja protiku MVR. 53 5.25 Konfiguracja protoki MVR. 53 5.26 Konfiguracja protiku MVR. 53 5.27 Protoki ILDP. 53 5.28 Konfiguracja sieci VLAN. 53 5.39 Konfiguracja sieci VLAN.	5.3 Konfiguracja dostępu urządzenia do sieci IP	
5.5 Konfiguracja Thermal Protection. 99 5.6 PRP lub HSR (opcja w wybranych przełącznikach wyposażonych w dodatkowy modul REDBOX). 91 5.7 Konfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przełącznikach). 23 5.8 Organiczenie dostępu zdalnego. 23 5.9 Konfiguracja poziomu uprawnień. 23 5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.11 Konfiguracja metod uwierzytelniania oraz autoryzacji. 26 5.12 SINJP Simple Network Management Protocol. 27 5.13 PortSecontrol List. 40 5.14 Authentication, Authorization and Accounting. 44 5.17 APP Inspection. 44 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 46 5.22 Agregacja portów 53 5.23 Konfiguracja protok MWR. 55 5.24 Konfiguracja protok/MVR. 55 5.25 Konfiguracja protok/MVR. 56 5.28 Protok/d ILDP. 53 5.39 Protok/d ILDP. 53 5.30 Protok/d ILDP. 54 5.31 Rodundancja droji przesytowej. 71 5.32 Konfiguracja sieci VLAN. 53 5.33 Konfiguracja sieci VLAN. 53 5.	5.4 Konfiguracja portów Ethernet	17
5.6 PKP lub HSR (opcja w wybranych przełącznikach wyposażonych w dodatkowy moduł REDBOX). 9.1 5.7 Konfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przełącznikach). 21 5.8 Konfiguracja metod uwierzytelniania oraz autoryzacji. 23 5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji. 23 5.11 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.12 SSMMP Simple Network Management Protocol. 27 5.13 Port Security Limit Control Configuration. 36 5.14 Network Access Server 38 5.15 Access Control List. 40 5.16 IP Source Guard. 43 5.17 Access Control List. 40 5.18 Authentication, Authorization and Accounting. 44 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 52 5.24 Konfiguracja protokół MVR. 56 5.25 Konfiguracja protokół MVR. 56 5.26 Konfiguracja sieci VLAN 53 5.27	5.5 Konfiguracja Thermal Protection	
5.7 Konfiguracja potów z POWER CIVER CITHENNET (opcja w wybranych przełącznikach).	5.6 PRP lub HSR (opcja w wybranych przełącznikach wyposażonych w dodatkowy moduł REDBOX)	19
5.8 Ograniczenie dostępu zdalnego. 23 5.9 Konfiguracja poziomu uprawnień. 23 5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.11 Konfiguracja TIPS. 26 5.12 Stati Konfiguracja MTIPS. 26 5.13 Port Security Limit Control Configuration. 36 5.14 Network Access Server 38 5.15 Access Control List. 40 5.16 IP Source Guard. 43 5.17 ARP Inspection. 44 5.18 Authentication, Authorization and Accounting. 44 5.20 Green Ethernet. 49 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 49 5.21 Sorp Totekotion. 54 5.22 Loop Protection. 54 5.23 Loop Protection. 56 5.24 Konfiguracja Protoki MVR. 56 5.25 Fontiguracja Protoki MVR. 56 5.26 Konfiguracja Protoki MVR. 56 5.27 Protoki IGMP. 53 5.28 Protoki ULDP-MED.	5.7 Konfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przełącznikach)	21
5.9 Konfiguracja pretod uwierzytelniania oraz autoryzacji. 24 5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji. 24 5.11 Konfiguracja metod uwierzytelniania oraz autoryzacji. 27 5.12 SNMP Network Management Protocol. 27 5.13 SnMP Stework Management Protocol. 38 5.14 Network Access Server. 38 5.15 Access Control List. 40 5.16 Access Control List. 40 5.17 API Inspection. 44 5.18 Authentication. Authorization and Accounting. 46 5.19 TACACS+ 47 5.20 Green Ethernet. 48 5.21 Server DHCP (dostepny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 54 5.24 Konfiguracja profilu IPMC. 55 5.25 Konfold ILDP. 63 5.26 Protokoł ILDP. 63 5.37 Protokoł ILDP. 63 5.38 Konfiguracja sieci VLAN. 58 5.39	5.8 Ograniczenie dostępu zdalnego	23
5.11 Konfiguracja HTPS 24 5.11 Konfiguracja HTPS 26 5.12 SMMP Simple Network Management Protocol. 27 5.13 Port Security Limit Control Configuration. 36 5.14 Network Access Server. 38 5.15 Access Control List. 40 5.16 IP Source Guard. 43 5.17 ARP Inspection. 44 5.18 Authentication, Authorization and Accounting. 46 5.12 Server DHCP (dostępny w wybranych wersjach urządzeń). 46 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 49 5.22 Loop Protection. 54 5.23 Loop Protection. 54 5.24 Konfiguracja Protokół MVR. 56 5.25 Konfiguracja Protokół MVR. 56 5.26 Protokół LDP. 56 5.27 Protokół LDP. 56 5.28 Protokół LDP. 56 5.29 Protokół LDP. 56 5.29 Protokół LDP. 56 5.29 Konfiguracja sieci VLAN. 53 <td>5.9 Konfiguracja poziomu uprawnień</td> <td>23</td>	5.9 Konfiguracja poziomu uprawnień	23
6.11 Konfiguracja HTTPS. 26 5.12 SNMP Simple Network Management Protocol. 27 5.13 Port Security Limit Control Configuration. 36 5.14 Network Access Server. 38 5.15 Access Control List. 40 5.16 Access Control List. 40 5.17 ARP Inspection. 44 5.18 Authentication, Authorization and Accounting. 44 5.19 TCACGS+. 47 5.20 Green Ethernet. 47 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 53 5.22 Agregacja portów. 53 5.23 Loop Protection 54 5.24 Konfiguracja profilu IPMC. 55 5.25 Konfiguracja profilu IPMC. 56 5.26 Protokól ILDP. 53 5.27 Protokól ILDP.MED. 58 5.28 Funkcionalność synchronizacji częstotliwości SYNCE (opcja w wybranych przelącznikach). 66 5.29 Funkcionalność synchronizacji częstotliwości SYNCE (opcja w wybranych przelącznikach). 68 5.30 VLAN Translation. <td>5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji</td> <td>24</td>	5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji	24
5.12 SMMP Simple Network Management Protocol. 27 5.13 Ports Security Limit Control Configuration. 36 5.14 Network Access Server. 38 5.15 Access Control List. 40 5.16 IP Source Guard. 43 5.17 ArtP Inspection. 44 5.18 Authentication, Authorization and Accounting. 46 5.19 TACACS+. 47 5.20 Green Ethernet. 48 5.21 Server DHCP (dostepny w wybranych wersjach urządzeń). 49 5.21 Server DHCP (dostepny w wybranych wersjach urządzeń). 49 5.22 Sconfiguracja profilu IPMC. 52 5.23 Konfiguracja profilu IPMC. 56 5.24 Protokół ILDP. 58 5.25 Protokół ILDP.MED. 63 5.26 Protokół ILDP.MED. 64 5.27 Protokół ILDP.MED. 64 5.28 Konfiguracja sieci VLAN 83 5.33 Konfiguracja sieci VLAN 83 5.34 Konfiguracja sieci VLAN 83 5.35 Konfiguracja s	5.11 Konfiguracja HTTPS.	
513 Port Security Limit Control Configuration 36 514 Network Access Server 38 515 Access Control List 40 516 IP Source Guard 43 517 ARP Inspection 44 518 Authentication, Authorization and Accounting 46 519 TACACS+ 47 520 Green Ethernet 48 521 Server DHCP (dostępny w wybranych wersjach urządzeń) 49 522 Agregacja portów 53 523 Loop Protection 54 524 Konfiguracja profilu IPMC 55 525 Konfiguracja profilu IPMC 56 526 Protokół ILDP 63 527 Protokół ILDP 63 528 Protokół ILDP 63 529 Funkoń Jangi drogi przesylowej 74 53 Konfiguracja sieci VLAN 68 53 Konfiguracja sieci VLAN 83 53 Konfiguracja sieci VLAN 83 53 Konfiguracja sieci VLAN 83 53 Konfiguracja sieci V	5.12 SNMP Simple Network Management Protocol	27
5.14 Network Access Server 38 5.15 Access Control List 40 5.16 Access Control List 43 5.17 ARP Inspection 44 5.18 Authentication, Authorization and Accounting 46 5.19 TACACS+ 47 5.20 Green Ethernet. 48 5.21 Server DHCP (dostępny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 54 5.24 Konfiguracja protok MVR. 56 5.25 Konfiguracja Protok MVR. 58 5.26 Protokół ILDP. 63 5.27 Protokół ILDP.MED. 63 5.28 Protokół ILDP.MED. 64 5.29 Forkokół ULDP.MED. 63 5.30 Protokoky do redundancji drogi przesylowej. 74 5.31 Redindancja drogi przesylowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.35 MAC Table. 83 5.35 Moltguracja sieci VLAN 83 5.35 Valky MAC Table. 83	5.13 Port Security Limit Control Configuration	
515 Access Control List. 40 516 IP Source Guard 43 517 ARP Inspection 44 518 IX CACS+ 44 519 TACACS+ 47 520 Green Ethernet. 48 521 Server DHCP (dostępny w wybranych wersjach urządzeń). 49 522 Agregacja portów. 53 523 Loop Protection. 54 524 Konfiguracja profilu IPMC. 55 525 Konfiguracja profilu IPMC. 56 526 Protokół ILDP. 53 527 Protokół ILDP. 63 528 Protokół ILDP.MED. 63 539 Protokół UDP.MED. 63 540 Protokół UDP.MED. 64 530 Protokoły do redundancji drogi przesylowej. 71 531 Redundancja drogi przesylowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 533 Konfiguracja sieci VLAN. 83 534 Konfiguracja sieci VLAN. 83 535 Monitorowanie VIAn. 83 536	5.14 Network Access Server	
516 IP Source Guard	5.15 Access Control List.	40
5.17 ARP Inspection.	5.16 IP Source Guard	43
5.18 Authentication, Authorization and Accounting. 46 5.19 TACACS+. 47 5.20 Green Ethernet. 48 5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 54 5.24 Konfiguracja protokół MVR. 55 5.25 Konfiguracja Protokół ILDP. 53 5.28 Protokół ILDP. 63 5.29 Protokół ILDP. 63 5.20 Protokół ILDP.MED. 63 5.21 Frotokół LDP.MED. 63 5.22 Frotokół LDP.WED. 63 5.30 Protokół Udo redundancji drogi przesylowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Montiforowanie Vlan. 83 5.36 VLAN Translation. 90 5.37 Private VLANs. 91 5.40 VcL 92 5.40 VcL 92	5.17 ARP Inspection	44
5.19 TACACS+	5.18 Authentication, Authorization and Accounting	
5.20 Green Ethernet. 48 5.21 Server DHCP (dostępny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 54 5.24 Konfiguracja Profilu IPMC. 55 5.25 Konfiguracja Protokół MVR. 58 5.26 Protokół ILDP. 53 5.27 Protokół ILDP. 63 5.28 Protokół LLDP. 63 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach). 68 5.29 Funkcjonalność synchronizacji ozęstotliwości SYNCE (opcja w wybranych przełącznikach). 68 5.30 Protokół LDP. 63 5.31 Konfiguracja sieci VLAN. 63 5.32 Konfiguracja sieci VLAN. 83 5.33 Konfiguracja sieci VLAN w wersji oprogramowania V0xx. 85 5.35 Monitrorowanie Vlan. 83 5.36 VLAN Translation. 90 5.37 Voice VLAN. 92 5.38 Voice VLAN. 94 5.39 Voice VLAN. 94 5.40	5.19 TACACS+	
5.21 Serwer DHCP (dostepny w wybranych wersjach urządzeń). 49 5.22 Agregacja portów. 53 5.23 Loop Protection. 54 5.24 Konfiguracja profilu IPMC. 55 5.25 Konfiguracja protiki IPMC. 58 5.26 Protokół IGMP. 59 5.27 Protokół ILDP. 63 5.28 Protokół LLDP.MED. 64 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przelącznikach). 68 5.29 Protokół V o redundancji drogi przesylowej. 71 5.31 Redundancja drogi przesylowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.32 Konfiguracja sieci VLAN. 83 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Monitorowanie Vlan. 87 5.36 Val.N 92 5.38 Voice VLAN. 92 5.39 Voice VLAN. 92 5.30 Voice VLAN. 92 5.31 Voice VLAN. 92 5.33 Voice	5.20 Green Ethernet.	
5.22 Agregacja portów	5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń)	
5.23 Loop Protection 54 5.24 Konfiguracja profilu IPMC 55 5.25 Konfiguracja Protokół MVR 58 5.26 Protokół ILDP 59 5.27 Protokół ILDP 63 5.28 Protokół ILDP 63 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach) 64 5.29 Frotokoł J torogi przesylowej 71 5.30 Protokoł oredundancji drogi przesylowej. 74 5.31 Redundancja drogi przesylowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.32 MAC Table 83 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Monitorowanie Vlan. 83 5.36 VLN Translation. 90 5.37 Private VLANs. 91 5.38 VCL 92 5.39 Voice VLAN. 94 5.40 Funkcja Ping Watchdog PoE. 96 5.41 Static NAT 97 5.42 IRIGB. 97 94 </td <td>5.22 Agregacja portów</td> <td>53</td>	5.22 Agregacja portów	53
5.24 Konfiguracja protiku IPMC 55 5.25 Konfiguracja Protokół MVR. 58 5.26 Protokół IGMP 59 5.27 Protokół ILDP- 63 5.28 Protokół ILDP-MED. 64 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach). 68 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach). 68 5.20 Protokół ULDP-MED. 61 5.21 Redundancja drogi przesyłowej. 71 5.21 Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.23 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Montorowanie Vlan. 83 5.36 Montorowanie Vlan. 83 5.37 Private VLANs. 90 5.38 VCL 92 5.39 Voice VLAN. 94 5.40 Funkcja Ping Watchdog PoE. 96 5.41 Static NAT. 97 5.42 IRIGB. 97 5.43 <td>5.23 Loop Protection.</td> <td>54</td>	5.23 Loop Protection.	54
5.25 Konfiguracja Protokół MVR. 58 5.26 Protokół ILDP. 59 5.27 Protokół ILDP. 63 5.28 Protokół LDP. 64 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach) 68 5.30 Protokoły do redundancji drogi przesyłowej 71 5.31 Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.32 MAC Table. 83 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Molitorowanie Vlan. 83 5.36 VLAN Translation. 90 5.37 Private VLANs. 91 5.38 VCL 92 5.39 Voice VLAN. 94 5.40 Funkcja Ping Watchdog PoE. 96 5.41 Static NAT. 97 5.42 IRIGB. 97 5.43 Upr Configuration. 114 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. 104 5.44 Planista portu wy	5.24 Konfiguracja profilu IPMC	55
5.26 Protokół ILDP. 59 5.27 Protokół LLDP. 63 5.28 Protokół LLDPMED. 64 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach) 68 5.30 Protokół ULDP-MED. 64 5.31 Redundancji drogi przesyłowej. 71 5.31 Redundancji drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.31 Nafuguracja sieci VLAN. 83 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Monitorowanie Vlan. 87 5.35 Monitorowanie Vlan. 87 5.36 VLAN Translation. 90 5.37 Volk VLANs. 91 5.38 VCL. 92 5.39 Voice VLAN 94 5.40 Funkcja Ping Watchdog PoE. 96 5.41 Static NAT 97 5.42 IR[GB. 97 5.43 Quality of Service. 99 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. <td>5.25 Konfiguracja Protokół MVR</td> <td>58</td>	5.25 Konfiguracja Protokół MVR	58
5.27 Protokół LLDP. 63 5.28 Protokół LLDP-MED. 64 5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach). 68 5.30 Protokoły do redundancji drogi przesyłowej. 71 5.31 Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032. 74 5.32 MAC Table. 83 5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN. 83 5.35 Monitorowanie Vlan. 83 5.36 VLAN Translation. 90 5.37 Private VLANs. 91 5.38 VCL 92 5.39 Voice VLAN. 94 5.40 Funkcja Ping Watchdog PoE. 96 5.41 Static NAT. 97 5.42 IRIGB. 97 5.44 Pianista portu wyjściowego Egress Port Schedulers and Shapers. 104 5.44 Pianista portu wyjściowego Egress Port Schedulers and Shapers. 104 5.44 Pianista portu wyjściowego Egress Port Schedulers and Shapers. 104 5.45 VPP Configuratio	5.26 Protokół IGMP	59
5.28Protokół LLDP-MED.645.29Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach).685.30Protokoły do redundancji drogi przesyłowej.715.31Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032.745.32MAC Table.835.33Konfiguracja sieci VLAN.835.34Konfiguracja sieci VLAN.835.35Monitorowanie Vlan.875.36VLAN Translation.905.37Private VLANs.915.38VCL925.39Voice VLAN.945.40Funkcja Ping Watchdog POE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.44GVRP Configuration.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.49SFlow Configuration.1265.50UDLD Port Configuration.1265.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.27 Protokół LLDP	63
5.29 Funkcjonalność synchronizacji częstotilwości SYNCE (opcja w wybranych przełącznikach). .68 5.30 Protokoły do redundancji drogi przesyłowej. .71 5.31 Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032. .74 5.32 MAC Table. .83 5.33 Konfiguracja sieci VLAN. .83 5.34 Konfiguracja sieci VLAN w wersji oprogramowania V0xx. .85 5.35 Monitorowanie Vlan. .87 5.36 VLAN Translation. .90 5.37 Private VLANs. .91 5.38 VCL .92 5.39 Voice VLAN. .94 5.40 Funkcja Ping Watchdog PoE .96 5.41 Static NAT. .97 5.42 IRIGB. .97 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. .104 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. .104 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. .104 5.44 Ustawienia podglądu urchu na portach Mirroring. .112 5.44 Ustawienia podglądu urchu n	5.28 Protokół LLDP-MED	64
5.30Protokoty do redundancji drogi przesyłowej.715.31Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032.745.32MAC Table.835.33Konfiguracja sieci VLAN.835.34Konfiguracja sieci VLAN w wersji oprogramowania V0xx.855.35Monitorowanie Vlan.875.36VLAN Translation.905.37Private VLANs.915.38VCL915.39Voice VLAN.945.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.44PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.49SFlow Configuration.1265.50UDLD Port Configuration.1265.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.29 Funkcjonalność synchronizacji częstotliwości SYNCE (opcja w wybranych przełącznikach)	
5.31Redundancja drogi przesytowej w topologii pierscienia zgodnie z ITU-1 G.8032	5.30 Protokoły do redundancji drogi przesyłowej.	
5.32MAC Table835.33Konfiguracja sieci VLAN835.34Konfiguracja sieci VLAN w wersji oprogramowania V0xx855.35Monitorowanie Vlan875.36VLAN Translation905.37Private VLANs915.38VCL925.39Voice VLAN925.39Voice VLAN945.40Funkcja Ping Watchdog PoE965.41Static NAT975.42IRIGB975.43Quality of Service995.44Planista portu wyjściowego Egress Port Schedulers and Shapers1045.45Ustawienia podglądu ruchu na portach Mirroring1125.46UPn Configuration1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji)1145.48GVRP Configuration1255.49sFlow Configuration1265.50UDLD Port Configuration1275.51DDMI dla wkładek światłowodowych SFP1285.52Moduł Digital InOut (opcja w wybranych modelach)131	5.31 Redundancja drogi przesyłowej w topologii pierscienia zgodnie z 110-1 G.8032	
5.33 Konfiguracja sieci VLAN. 83 5.34 Konfiguracja sieci VLAN w wersji oprogramowania V0xx. 85 5.35 Monitorowanie Vlan. 87 5.36 VLAN Translation. 90 5.37 Private VLANs. 91 5.38 VCL 92 5.39 Voice VLAN 92 5.39 Voice VLAN 94 5.40 Funkcja Ping Watchdog PoE 96 5.41 Static NAT 97 5.42 IRIGB 97 5.43 Quality of Service. 97 5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers. 104 5.45 Ustawienia podglądu ruchu na portach Mirroring. 112 5.46 UPnP Configuration. 114 5.47 PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji). 114 5.49 sFlow Configuration. 125 5.49 sFlow Configuration. 126 5.50 UDLD Port Configuration. 126 5.51 DDMI dla wkładek światłowodowych SFP. 128 5.52 Moduł Digi	5.32 MAC Table	
5.34Konfiguracja sieci VLAN w wersji oprogramowania V0xx.855.35Monitorowanie Vlan.875.36VLAN Translation.905.37Private VLANs.915.38VCL.925.39Voice VLAN.945.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.905.44Ustawienia podglądu ruchu na portach Mirroring.1125.45Ustawienia podglądu ruchu na portach Mirroring.1145.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.49sFlow Configuration.1255.49sFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.33 Kontiguracja sieci VLAN.	
5.35Monitorowanie Vian.875.36VLAN Translation.905.37Private VLANs.915.38VCL.925.39Voice VLAN.945.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49sFlow Configuration.1265.50UDLD Port Configuration.1265.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.34 Konfiguracja sieci VLAN w wersji oprogramowania VUxx	
905.37Private VLANs.5.38VCL5.39Voice VLAN.5.39Voice VLAN.5.40Funkcja Ping Watchdog PoE.5.41Static NAT.5.42IRIGB.5.43Quality of Service.975.435.44Planista portu wyjściowego Egress Port Schedulers and Shapers.104945.45Ustawienia podglądu ruchu na portach Mirroring.5.46UPnP Configuration.5.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).5.48GVRP Configuration.5.49sFlow Configuration.5.50UDLD Port Configuration.5.51DDMI dla wkładek światłowodowych SFP.5.52Moduł Digital InOut (opcja w wybranych modelach).	5.35 Inionitorowanie Vian	
5.37FITVAILE VLAINS.915.38VCL.925.39Voice VLAN.945.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49SFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	0.30 VLAN I FANSIATION	
5.30VOL925.39Voice VLAN.945.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49SFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131		
5.39 Voice VLAN	5.38 VCL	
5.40Funkcja Ping Watchdog PoE.965.41Static NAT.975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49sFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.39 VUICE VLAIN	
5.41Stauc INAT975.42IRIGB.975.43Quality of Service.995.44Planista portu wyjściowego Egress Port Schedulers and Shapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49sFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	D.40 FUTIKOJA FING WAICHOOG FOE	
5.42INGD	5.41 Static INA1	
5.43Guanty of Service	5.42 Quality of Sanciaa	
5.44Fransia porta wyjsciowego Egress Port Schedulers and Snapers.1045.45Ustawienia podglądu ruchu na portach Mirroring.1125.46UPnP Configuration.1145.47PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji).1145.48GVRP Configuration.1255.49sFlow Configuration.1265.50UDLD Port Configuration.1275.51DDMI dla wkładek światłowodowych SFP.1285.52Moduł Digital InOut (opcja w wybranych modelach).131	5.40 Quality UI Set VICE.	
5.40 UPnP Configuration 114 5.47 PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji) 114 5.48 GVRP Configuration 125 5.49 sFlow Configuration 126 5.50 UDLD Port Configuration 127 5.51 DDMI dla wkładek światłowodowych SFP 128 5.52 Moduł Digital InOut (opcja w wybranych modelach) 131	5.44 Fransia politu wyjsolowego Egress Polit Schedulers and Shapers	104
5.40 OF NF Configuration	5.45 Ustawienia pougiąuu ruchu na portach iviironny	2 ۱ ۱۹۸
5.47File Fredstor File dosteprie w Zaležnosti od wybranej wersji)	5.47 DTD Drecision Time Drotocol (Drofile dostopno w zalożności od wybranci warsii)	114
5.40 SVN Configuration 125 5.49 sFlow Configuration 126 5.50 UDLD Port Configuration 127 5.51 DDMI dla wkładek światłowodowych SFP 128 5.52 Moduł Digital InOut (opcja w wybranych modelach) 131	5.48 CVRD Configuration	114 ۱۹۶
5.50 UDLD Port Configuration	5.40 SVN Configuration	120
5.50 DDDI dla wkładek światłowodowych SFP	5.50 LIDED Port Configuration	120 107
5.52 Moduł Digital InOut (opcja w wybranych modelach)	5.51 DDMI dla wkładek światłowodowych SED	۱ <i>21</i> ۱۵۵
	5.52 Moduł Digital InOut (opcja w wybranych modelach)	20 I 121

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 2/147	REV.
--	------



5.53 Konfiguracja oraz monitorowanie funkcji GNSS w przełączniku	132
5.54 Wewnetrzny test ICMP ping w menu Diagnostyka	133
6 Awaryjne przywracanie dostępu do urządzenia	134
7 Zarządzanie konfiguracją, aktualizacja Firmware oraz Restart urządzenia	134
7.1 Aktualizacja oprogramowania	135
7.2 Zarządzanie plikami konfiguracyjnymi w przełącznikach HYPERION	135
8 Konfiguracja przełącznika – interfejs CLI	137
8.1 Opis komend CLI dla nowszej wersji oprogramowania od v1xx	137
8.2 Opis poleceń CLI dla oprogramowania w starszej wersji firmware oznaczonej v0xx	142
9 Dane techniczne	147
10 Instrukcje konfiguracji wybranych funkcji przełączników Hyperion	147
10.1 Zestaw poleceń ze składnią konsoli ICLI w Hyperion dla wybranych poziomów w nowszej wersji firmware	148
10.2 Przykładowa konfiguracja RINGU	148
10.3 Przykładowa konfiguracje Telemetry oraz IN/OUT w H-30x-3	148
10.4 Przykładowa konfiguracja funkcji NTP	148
10.5 Przykładowa konfiguracja funkcji Ping Watchdog	148
10.6 Przykładowa konfiguracja PTP dla Master oraz Boundry Clock	148
10.7 Przykładowa konfiguracja NAT	148
10.8 Konfiguracja protokołu SNMPv3	148
10.9 Konfiguracja RS jako serwera portów szeregowych w HYPERION-30x-3	148

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	3/147
------	------	-----------------------------------	------------	-------



1 INFORMACJE PODSTAWOWE

1.1 Zgodność z normami i zaleceniami

Urządzenia **HYPERION** zostały zaprojektowane w oparciu o obowiązujące normy i zalecenia z zakresu transmisji danych, kompatybilności elektromagnetycznej i bezpieczeństwa użytkowania.

1.1.1 Kompatybilność elektromagnetyczna

Urządzenie zostało zaprojektowane w oparciu o normę PN-EN 55022 klasa A, PN-EN-55024.

Ostrzeżenie: Urządzenie to jest urządzeniem klasy A. W środowisku mieszkalnym może ono powodować zakłócenia radioelektryczne. W takich przypadkach można żądać od jego użytkownika zastosowania odpowiednich środków zaradczych.

1.1.2 Bezpieczeństwo

Rodzina urządzeń HYPERION zostały zaprojektowane w zakresie bezpieczeństwa i użytkowania w oparciu o normę PN-EN-60950.

Konfigurację urządzenia powinny wykonywać osoby z niezbędnymi uprawnieniami po zapoznaniu się z instrukcją obsługi. Producent nie jest odpowiedzialny za wszelkie zdarzenia wynikłe z niezgodnego z niniejszą instrukcją użytkowania.

1.1.3 Transmisja danych

Funkcje transmisji danych oraz parametry interfejsów komunikacyjnych urządzenia definiują następujące normy i zalecenia.

IEEE 802.3-2002 - Interfejsy Ethernet o szybkości 10/100/1000Mbit/s

IEEE 802.1q, p – Definicje mechanizmów sieci **VLAN** i priorytetów transmisji sygnałów dla sieci ETHERNET

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04	4/147
--	-------



1.2 Oznaczenie

UWAGA: Oznaczenia dostępnych wersji urządzeń HYPERION-500; -402; -300; -200; -105 zamieszczone są w IO_SHORT każdego z przełączników.

2 OPIS FUNKCJONALNY

2.1 Funkcje i Zastosowania

Światłowodowy przełącznik **HYPERION** zapewnia niezawodną transmisję danych w standardzie Ethernet w topologii magistrali lub pierścienia światłowodowego z protekcją drogi transmisyjnej w sieciach automatyki przemysłowej. Pozwala na zestawianie połączeń pomiędzy: sterownikami, terminalami, kamerami oraz komputerami przemysłowymi. Zapewnia przy tym redundancję drogi transmisyjnej i zasilania.

Poszczególne wersje urządzenia umożliwiają realizację połączenia z wykorzystaniem dwóch włókien światłowodu jednomodowego lub wielomodowego albo jednego włókna światłowodu jednomodowego w technice WDM. **HYPERION** jest w pełni zgodny ze standardem: 10/100/1000BaseT(X) i 100/1000BaseFX.

Zastosowanie przełącznika **HYPERION** pozwala budować rozległą sieć transmisji danych w oparciu o różne media transmisyjne takie jak skrętka miedziana lub światłowód. Zmiana elektrycznego medium transmisyjnego na tor światłowodowy pozwala na zwiększenie zasięgu transmisji (nawet do 100 km przy zastosowaniu światłowodu jednomodowego) oraz całkowite wyeliminowanie wpływu zakłóceń elektromagnetycznych.

Prosta konfiguracja pozwala dostosować w sposób optymalny tryb pracy urządzenia i portów do aplikacji. Urządzenie przystosowane jest do pracy w trudnych warunkach środowiskowych.



Rys. 1. Przykładowe zastosowanie urządzeń HYPERION.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	5/147
			i l	



2.1.1 Opis złącz urządzenia

Wszystkie złącza (oprócz portów SFP, zasilania i portu USB) znajdujące się w urządzeniu to złącza typu RJ-45. Jego wygląd przedstawiony jest na rysunku poniżej.



Rys. 2.Wygląd i numeracja wyprowadzeń złącza RJ45

Rozmieszczenie poszczególnych sygnałów dla złącz RJ-45 przedstawia tabela.

Port	Przeznaczenie	Opis wyprowadzeń
10/100/1000BaseT(X)	Ethernet 1000Mbit/s	1 – DA+ 2 – DA- 3 – DB+ 4 – DC+ 5 – DC- 6 – DB- 7 – DD+ 8 – DD-
10/100BaseT(X)	Ethernet 10/100Mbit/s	1 – TX+ 2 – TX - 3 – RX+ 6 – RX -

2.1.2 Opis slotów SFP w przełącznikach HYPERION

Porty optyczne są wyposażone w sloty na moduł SFP lub SFP/SFP+ .Zasięg oraz rodzaj złącza uzależniony jest od rodzaju zastosowanej wkładki SFP.

3 Instalacja i obsługa

3.1 Warunki pracy

Przełącznik może pracować w sposób ciągły w pomieszczeniach zamkniętych w warunkach podanych w specyfikacji technicznej. Nie powinien być narażony na bezpośrednie nasłonecznienie. Nie zaleca się ustawiania urządzenia na źródłach ciepła. Montaż powinien zapewniać swobodny przepływ powietrza.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	6/147
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	6/147



3.2 Instalacja

Przełącznik w zależności od modelu przystosowany jest do montażu na szynie DIN EN 50022 lub w szafach RACK 19". Dozwolony jest montaż urządzenia w dowolnej pozycji, ale tak, aby nie zasłaniać otworów wentylacyjnych. Po podłączeniu zasilania, o odpowiednich parametrach zgodnych z wartościami na tabliczce znamionowej, do odpowiedniego złącza, zaświeci się dioda LED POWER (PWR – oznaczenia zależne pod modelu). W urządzeniach wyposażonych w dwie diody LED, sygnalizujące stan każdego zasilania, podłączenie tylko do jednego z wejść zasilających spowoduje zaświecenie tylko jednej diody PWR odpowiadającej temu wejściu.

3.3 Zasady posługiwania się złączami światłowodowymi

Złącza światłowodowe są elementami o bardzo wysokiej precyzji i wymagają bardzo delikatnego obchodzenia się z nimi. Należy je chronić przed kurzem i zabrudzeniem. Rozłączone elementy złącza należy zabezpieczyć nasadkami ochronnymi. W razie zanieczyszczenia, gniazdo można przedmuchać sprężonym, czystym powietrzem, a wtyk przemyć alkoholem izopropylowym lub etylowym. Należy przy tym bezwzględnie posługiwać się chusteczkami bezpyłowymi.

4 Zarządzanie

Zarządzanie urządzenia HYPERION możliwe jest przez dowolny port Ethernet urządzenia wykorzystując protokoły HTTP, HTTPS oraz SNMP. Dodatkowo w niektórych modelach dostęp do konfiguracji parametrów urządzenia możliwy jest przez dedykowany port NMI (RJ45) lub z wykorzystaniem wiersza poleceń przez TELNET/SSH lub z poziomu konsoli RS232.

Domyślny adres IP interfejsu zarządzania to 192.168.0.10, maska 255.255.255.0 (24 bity) domyślny użytkownik to "admin", hasło domyślne - brak. Sterowniki do konsoli CLI dostępnej poprzez port USB znajdują się na stronie do pobrania.

5 Opis GUI dostępnego przez przeglądarkę WWW

Konfiguracja **HYPERION** za pomocą protokołów HTTP i HTPPS wymaga komputera z zainstalowaną przeglądarką internetową – zalecane jest używanie przeglądarki Firefox, Internet Explorer (w wersji 6 lub wyższej), Chrome lub Opera – oraz prawidłowo skonfigurowanego połączenia sieciowego pomiędzy urządzeniem, a komputerem. Interfejsy http i https zapewniają dostęp do wszystkich ustawień możliwych do skonfigurowania w tym urządzeniu.

Aby rozpocząć sesję zarządzania przez http lub https należy uruchomić przeglądarkę internetową i w polu adresu wpisać adres IP urządzenia, domyślny adres to 192.168.0.10, po czym nacisnąć klawisz Enter (lub inny, służący do otwarcia strony w używanej przeglądarce). Na wszystkich stronach, aby zmienić ustawienia należy wpisać nowe wartości do odpowiednich pól, a następnie kliknąć przycisk Save. Na niektórych stronach ustawienia są podzielone na dwie lub więcej grup; każda grupa posiada osobny przycisk Save. Przycisk ten powoduje zapisanie tylko ustawień grupy, do której należy.

<u>UWAGA!!!</u> Aby zapobiec utracie konfiguracji po ponownym uruchomieniu przełącznika zaleca się zapisywanie każdej zmiany konfiguracji do pliku startup-config. Zapisanie odbywa się przez naciśnięcie przycisku Save Configuration w zakładce w menu: Maintenance — Configuration — Save startup-config

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	7/147
------	------	-----------------------------------	------------	-------



Przycisk Reset, obecny na większości stron, powoduje odświeżenie strony z aktualnymi ustawieniami urządzenia i usunięcie ustawień wprowadzonych, ale nie zapisanych. Zarządzanie urządzeniem **HYPERION** przez interfejs www jest podzielone na cztery główne grupy:

- Konfiguracja (Configuration), grupa ta umożliwia zmiany ustawień urządzenia takich jak: zmiana adresu IP urządzenia, ustawienie VLAN, przydział pasma, ograniczenie dostępu do zarządzania,
- Monitorowanie (Monitor), grupa ta udostępnia podgląd na stan pracy urządzenia przede wszystkim pozwala na obserwację: poprawności wykonania połączeń urządzenia z zewnętrznymi segmentami sieci (link), statystyk ruchu na poszczególnych portach, zawartości tablicy MAC adresów,
- Diagnostyka (Diagnostics), grupa ta jest wyposażona w proste narzędzia do sprawdzenia parametrów połączeń z zewnętrznymi segmentami sieci,
- Utrzymanie (Maintenance), grupa ta umożliwia między innymi: wykonanie ponownego uruchomienia urządzenia (tzw. restart), przywrócenie ustawień fabrycznych urządzenia i aktualizację oprogramowania oraz zarządzaniem plikami konfiguracyjnymi (pobieranie, wczytanie, aktywowanie lub usunięcie).

UWAGA: Przed pierwszym uruchomieniem zarządzania przez interfejs http lub https należy włączyć obsługę JavaScript w przeglądarce internetowej.

5.1 Ochrona urządzenia hasłem

W celu ograniczenia dostępu osób nieuprawnionych do zarządzania, urządzenie może być zabezpieczone hasłem. Przy każdej próbie dostępu do urządzenia przez interfejs http lub https, jako pierwszy wyświetli się panel logowania.

Po pierwszym zalogowaniu można ustawić hasło dostępu dla administratora. Sposób konfiguracji użytkowników oraz ustanawiania haseł opisuje punkt **5.7** niniejszej instrukcji.

Wymagane uwierzytelnienie	
http://192.168.0.11 Twoje połączenie z tą stroną nie jest prywatne	
Nazwa użytkownika admin	
Hasło	
Zaloguj się 🛛 A	nuluj

Rys. 3. Panel logowania

Domyślna nazwa użytkownika: admin

Domyślne hasło: brak i to pole należy zostawić puste

Hasło dostępu do urządzenia można nadać podczas pierwszej sesji zarządzania, hasło to jest tym samym hasłem, które jest używane przy logowaniu do konsoli CLI urządzenia przy użyciu protokołu SSH lub telnet. Zmieniając hasło dla interfejsu http zmienia się także hasło dostępu do CLI przez RS i odwrotnie.

Stan zalogowania (sesja) w urządzeniu jest utrzymywany ciągle, aż do momentu wylogowania przez użytkownika, do czego służy ikona w prawym górnym rogu strony z symbolem otwartych drzwi i strzałką .

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	8/147	



Obok tej ikony znajduje się ikona ze znakiem zapytania, która w zależności od kontekstu, uruchamia nowe okno przeglądarki, zawierające opisy pól oraz ich funkcje, jakie w danej chwili udostępnia przeglądana strona urządzenia. Strony, które wyświetlają dane często zmieniające się, jak na przykład statystki ruchu na poszczególnych portach, mogą być odświeżane ręcznie, poprzez kliknięcie przycisku Refresh lub automatycznie co 3 sekundy, przez zaznaczenie pola Auto-refresh.

Uwaga!!!: We wskazanych modelach przełączników aktualizacja firmware z wersji starszej niż:

HYPERION-105 - v120 HYPERION-300 - v120 HYPERION-303 - v120 HYPERION-200 - v308 HYPERION-400 - v308 HYPERION-500 - v308 Spowoduje usupjecje h

Spowoduje usunięcie haseł dla istniejących użytkowników w konfiguracji (w tym także użytkownika "admin").

Po aktualizacji i ponownym uruchomieniu, dla każdego skonfigurowanego użytkownika hasło będzie usunięte to znaczy przy pierwszej próbie zalogowania się do zarządzania przez WWW lub CLI pole hasła należy zostawić puste.

W przypadku downgrade'u oprogramowania do niższej wersji niż wskazana na liście powyżej, nastąpi całkowite usunięcie profili użytkowników, natomiast zostanie utworzony domyślny użytkownik "admin" bez hasła.

5.2 Właściwości ogólne

Po poprawnym zalogowaniu się wyświetli się pierwsza strona z ogólnym rysunkiem przełącznika w postaci graficznej, ukazującym stan pracy poszczególnych portów w urządzeniu. Grafiki poszczególnych urządzeń różnią się w zależności od modelu.



Rys. 4. Przykładowy wycinek portów z urządzeń HYPERION

Grafika może wyświetlać następujące stany:

Port niepodświetlony – niepodłączony.

Port podświetlony na zielono – medium podłączone prawidłowo status portu podniesiony, a po wskazaniu tego portu kursorem pojawia się oznaczenie interfejsu wraz z prędkością oraz trybem.

Port podświetlony na zielono z dodatkowym znakiem błyskawicy - medium podłączone prawidłowo status portu podniesiony, a dodatkowo zasilanie PoE podawane do urządzenia PD. (symbol występuje tylko w wersji z dostępnym PoE)

Bezpośrednie kliknięcie na port na grafice przedstawiającej wizualizację urządzenia spowoduje przeniesienie na stronę przedstawiającą szczegółowe statystyki transmisyjne danego portu. Przedstawiono na rysunku nr 5.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	9/147
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	9/147



Detailed Port Stat	istics Port 5	Port 5 🔻 Auto-refresh 🔲	Refresh Clear
	Receive Total	Tra	ansmit Total
Rx Packets	508669	Tx Packets	358457
Rx Octets	1663396954	Tx Octets	1650433453
Rx Unicast	348717	Tx Unicast	348217
Rx Multicast	65350	Tx Multicast	9884
Rx Broadcast	94602	Tx Broadcast	356
Rx Pause	0	Tx Pause	0
	Receive Size Counters	Transm	nit Size Counters
Rx 64 Bytes	90521	Tx 64 Bytes	1340
Rx 65-127 Bytes	54512	Tx 65-127 Bytes	12256
Rx 128-255 Bytes	17716	Tx 128-255 Bytes	6609
Rx 256-511 Bytes	14320	Tx 256-511 Bytes	9507
Rx 512-1023 Bytes	22077	Tx 512-1023 Bytes	18891
Rx 1024-1526 Bytes	18365	Tx 1024-1526 Bytes	18430
Rx 1527- Bytes	291158	Tx 1527- Bytes	291424
	Dessive Ousue Counters	Tranami	
	Receive Queue Counters	Transmi	t Queue Counters
Rx Q0	508669	Tx Q0	346282
Rx Q0 Rx Q1	508669	Tx Q0 Tx Q1	346282 0
Rx Q0 Rx Q1 Rx Q2	508669 0 0 0	Tx Q0 Tx Q1 Tx Q2	346282 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3	Sosee Counters 508669 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3	346282 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4	508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q2 Tx Q3 Tx Q4	346282 0 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5	508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5	346282 0 0 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6	508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q5 Tx Q6	346282 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q6 Rx Q7	508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q3 Tx Q4 Tx Q5 Tx Q5 Tx Q6 Tx Q7	346282 0 0 0 0 0 9445 2730
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7	Source Counters 508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmi	346282 0 0 0 0 0 9445 2730 it Error Counters
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7	Sose Counters 508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops	346282 0 0 0 0 9445 2730 it Error Counters
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment	Sosee So	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmi Tx Drops Tx Late/Exc. Coll.	346282 0 0 0 0 9445 2730 it Error Counters 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize	Source Guede Counters 508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q7 Tx Drops Tx Late/Exc. Coll.	346282 0 0 0 0 0 9445 2730 it Error Counters 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize	Source Guede Counters 508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmi Tx Drops Tx Late/Exc. Coll.	346282 0 0 0 0 9445 2730 it Error Counters 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize Rx Oversize Rx Fragments	508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Transmi Tx Late/Exc. Coll.	346282 0 0 0 0 0 9445 2730 it Error Counters 0 0
Rx Q0 Rx Q1 Rx Q2 Rx Q3 Rx Q4 Rx Q5 Rx Q6 Rx Q7 Rx Drops Rx CRC/Alignment Rx Undersize Rx Oversize Rx Oversize Rx Fragments Rx Jabber	Source Counters 508669 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tx Q0 Tx Q1 Tx Q2 Tx Q2 Tx Q3 Tx Q4 Tx Q5 Tx Q6 Tx Q7 Tx Drops Tx Late/Exc. Coll.	346282 0 0 0 0 9445 2730 it Error Counters 0 0

Rys. 5. Okno szczegółowych statystyk portu w HYPERION

Wyświetlane liczniki to sumy dla odbioru i nadawania, liczniki rozmiaru dla odbioru i nadawania oraz liczniki błędów dla odbioru i nadawania.

Receive Total and Transmit Total

Rx and Tx Packets - Liczba odebranych i wysłanych (dobrych i złych) pakietów.

Rx and Tx Octets - Liczba odebranych i wysłanych (dobrych i złych) bajtów. Obejmuje FCS, ale nie obejmuje bitów ramek.

Rx and Tx Unicast - Liczba odebranych i wysłanych (dobrych i złych) pakietów unicast.

Rx and Tx Multicast - Liczba odebranych i wysłanych (dobrych i złych) pakietów multicast.

Rx and Tx Broadcast - Liczba odebranych i wysłanych (dobrych i złych) pakietów broadcast.

Rx and Tx Pause - Liczba ramek kontrolnych MAC odebranych lub przesłanych na tym porcie, który ma kod operacji wskazujący na operację PAUSE.

Receive and Transmit Size Counters - Liczba odebranych i wysłanych (dobrych i złych) pakietów podzielonych na kategorie na podstawie ich odpowiednich rozmiarów ramek.

Receive and Transmit Queue Counters - Liczba odebranych i wysłanych pakietów na kolejkę wejściową i wyjściową.

Receive Error Counters

Rx Drops - Liczba ramek porzuconych z powodu braku buforów odbioru lub przeciążenia wyjścia.

Rx CRC/Alignment - Liczba odebranych ramek z błędami Alignment lub "CRC".

Rx Undersize - Liczba odebranych krótkich(1) ramek z prawidłowym CRC.

Rx Oversize - Liczba odebranych długich(2) ramek z prawidłowym CRC.

Rx Fragments - Liczba odebranych krótkich(1) ramek z nieprawidłowym CRC.

Rx Jabber - Liczba odebranych długich(2) ramek z nieprawidłowym CRC.

Rx Filtered - Liczba odebranych ramek przefiltrowanych przez proces przesyłania.

1. Krótkie ramki to ramki mniejsze niż 64 bajty.

2. Długie ramki to ramki dłuższe niż maksymalna długość ramki skonfigurowana dla tego portu.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	10/147
------	------	-----------------------------------	------------	--------



Transmit Error Counters

Tx Drops - Liczba ramek porzuconych z powodu przeciążenia bufora wyjściowego. **Tx Late/Exc. Coll** - Liczba opuszczonych ramek z powodu nadmiernych lub późnych kolizji.

5.2.1 Konfiguracja informacji systemowej w przełączniku

Pola tekstowe można uzupełnić na stronie po kliknięciu na następujące linki Configuration \rightarrow System \rightarrow Information.

А

System Information Configuration

System Contact	
System Name	
System Location	

Save Reset

Okno konfiguracji informacji systemowych w urządzeniach HYPERION.

В

System Information Configuration

System Contact	
System Name	
System Location	
System Timezone Offset (minutes)	0

Save Reset

Rys. 6. Okno konfiguracji informacji systemowych w urządzeniach HYPERION.

System Contact – kontakt do osoby odpowiedzialnej za to urządzenie. System Name – nazwa nadana przez użytkownika dla tego urządzenia. System Location – miejsce w którym urządzenie zostało zainstalowane.

Pole **System Timezone Offset** jak na rysunku B umożliwia ustawienia opóźnienia strefy czasowej do poprawnego wyświetlania aktualnego czasu systemowego podawana w minutach (opcja dostępna w zależności od wersji oprogramowania). W pozostałych wersjach oprogramowania konfiguracja strefy czasowej jest dostępna w zakładce Time opisanej w punkcie 5.3.2

Ogólne właściwości urządzenia wraz z danymi dotyczącymi wersji oprogramowania, adresem MAC urządzenia są dostępne pod linkiem **Monitor > System > Information**. Znaczenie poszczególnych pól jest następujące:

MAC Address – adres MAC urządzenia.

Device Type – wersja urządzenia.

Serial Number – numer seryjny urządzenia.

System Date - aktualna data i czas systemowy.

System Uptime – czas jaki upłynął od włączenia zasilania lub ostatniego restartu.

Software Version – wersja oprogramowania aktualnie zainstalowanego w urządzeniu.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	11/147
------	------	-----------------------------------	------------	--------



Software Date – data i czas wydania wersji oprogramowania, które jest zainstalowane w urządzeniu.

	System
Contact	
Name	
Location	
	Hardware
MAC Address	00-50-c2-0d-c4-38
Device Type	Hyperion-500
Serial Number	95
	Time
System Date	2020-11-16T15:16:34+01:00
System Uptime	0d 07:04:13
	Software
Software Version	BCH500-CUS-1-4SP-NMI-L3-317-7722
Software Date	2020-10-01T14:16:25+02:00

Rys. 7. Ogólne właściwości urządzenia

5.3 Konfiguracja dostępu urządzenia do sieci IP

Komunikacja z urządzeniem może odbywać się standardowo z wykorzystaniem protokołu IP w wersji 4 lub w wersji 6. Użytkownik może dokonać zmian konfiguracji adresu IP przez interfejs www klikając na link **Configuration** → **System** → **IP**. Adres IP urządzenia może być ustawiony na dwa sposoby. Pierwszy sposób to pobieranie przez urządzenie dynamicznego adresu IP z serwera DHCP, drugi to praca urządzenia ze statycznym adresem IP. Ustawienia w tych oknach należy potwierdzić przyciskiem Save lub anulować przyciskiem Reset.

Okna służą do konfiguracji:

IP Configuration – okno umożliwiające konfigurację Hyperiona do pracy w trybie Host lub z funkcjonalnością Routera. Tryby te umożliwiają pracę interfejsów konfigurowanych w oknie **IP Interfaces.** W trybie Host interfejsy nie będą między sobą przesyłać danych, a w trybie Router umożliwiają przesyłanie danych pomiędzy interfejsami. Pola **DNS Server od 0 do 3** służą do przypisywania adresów IP różnych serwerów DNS w zależności od priorytetu – niższy indeks to wyższy priorytet.

Okno do konfiguracji **IP Interfaces** posiada dla wybranych VLAN wiersz do konfiguracji adresów IP v4 lub v6, a także możliwość włączenia DHCP klienta. Pola w każdym wierszu mają następujące znaczenie:

VLAN - służy do konfiguracji numeru wirtualnej sieci LAN, w której będzie możliwość dostępu do interfejsu oraz zarządzania urządzeniem. Domyślny VLAN zarządzania urządzeniem to 1 i również domyślnie wszystkie porty przełącznika pracują z VLAN numer 1, także dostęp do zarządzania urządzeniem jest możliwy z dowolnego portu. Istnieje możliwość skonfigurowania do 8 różnych interfejsów dla 8 różnych VLAN-ów.

DHCPv4 – ustawienia klienta DHCP dla IPv4

Enable – zaznaczenie checkbox-a w tej kolumnie spowoduje, że urządzenie będzie po każdym włączeniu zasilania lub po ponownym uruchomieniu próbować pobierać adres z serwera DHCP. Odznaczenie tego checkbox-a wymusi na urządzeniu pracę ze statycznym adresem.

Fallback – określa czas trwania prób uzyskania dzierżawy DHCP. Gdy próba uzyskania dynamicznego adresu IP nie powiedzie się to po upływie wpisanego w polu czasu urządzenie przełączy się na skonfigurowany statyczny adres IPv4. Wartość zero wyłącza mechanizm czasu trwania prób, dzięki czemu próby uzyskania adresu IP z DHCP będzie kontynuował aż do uzyskania ważnej dzierżawy. Wartości możliwe do wpisania wynoszą od 0 do 4294967295 sekund.

Current Lease. - Jeśli posiadamy dostęp do prawidłowo skonfigurowanego serwera DHCP, to po uzyskaniu dynamicznego adresu IP zostanie on wyświetlony w tym polu.

IPv4 – pola do konfiguracji statycznego adresu IPv4.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	12/147
------	------	-----------------------------------	------------	--------



Address – pole do wpisywania statycznego adresu IP dla interfejsu w urządzeniu. **Mask length** – podajemy maskę podsieci w wersji skróconej.

DHCPv6 – ustawienia klienta DHCP dla IPv6.

Enable – zaznaczenie checkbox-a w tej kolumnie spowoduje, że urządzenie będzie po każdym włączeniu zasilania lub po ponownym uruchomieniu próbować pobierać adres z serwera DHCP. Odznaczenie tego checkbox-a wymusi na urządzeniu pracę ze statycznym adresem.

Rapid Commit - Włącza opcję szybkiego zobowiązania dla dynamicznego adresu lpv6 z serwera DHCPv6. Jeśli ta opcja jest włączona, klient DHCPv6 przerywa proces oczekiwania, gdy tylko otrzyma komunikat odpowiedzi z serwera DHCPv6, ale tylko wtedy, gdy serwer ma włączoną opcję Rapid Commit.

Current Lease. - Jeśli posiadamy dostęp do prawidłowo skonfigurowanego serwera DHCP, to po uzyskaniu dynamicznego adresu IP zostanie on wyświetlony w tym polu.

IPv6 – pola do konfiguracji statycznego adresu IPv6.

Address – pole do wpisywania statycznego adresu IP dla danego interfejsu w urządzeniu. Mask length – podajemy maskę podsieci w wersji skróconej.

IP Routes – okno do konfiguracji protokołu routing-u statycznego.

Network – pole do wpisywania adresu docelowej sieci IP lub adresu hosta. Dla sieci domyślnej należy wpisać wartość "0.0.0.0" lub dla IPv6 "::"

Mask Length – podajemy maskę podsieci w wersji skróconej.

Gateway - bramę domyślną,

Next Hop VLAN (tylko dla adresacji IPv6)

UWAGA! Nowe urządzenie ma domyślnie wyłączone DHCP oraz ustawiony adres IP statycznie na 192.168.0.10 i maskę podsieci 255.255.255.0. Dlatego aby nawiązać sesję z PC należy kartę Ethernet komputera skonfigurować ze statycznym adresem IP jednocześnie pamiętając aby nie nadać tego samego adresu co adres przełącznika

	guratio	n									
Mode	ŀ	Host •									
DNS Serv	ver 0	No DNS serv	/er	•							
DNS Serv	ver 1	No DNS serv	/er	•							
DNS Serv	ver 2	No DNS serv	/er	•							
DNS Serv	ver 3	No DNS serv	/er	•							
DNS Pro:	xy										
IP Interfa	aces										
				DHCPv4		IPv4			DHCPv6		IPv6
Delete	VIAN										
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
Delete	VLAN 1	Enable	Fallback	Current Lease	Address 192.168.0.41	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
Delete Add Interf	VLAN 1 face	Enable	Fallback	Current Lease	Address 192.168.0.41	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
Add Intern	VLAN 1 face	Enable	Fallback	Current Lease	Address 192.168.0.41	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
Delete Add Inter IP Route Delete	VLAN 1 face ss	Enable C	Fallback	Current Lease	Address 192.168.0.41 way Next Hop VL	Mask Length 24 AN	Enable	Rapid Commit	Current Lease	Address	Mask Length
Delete Add Intern IP Route Delete Delete	VLAN 1 face s 0.0.0.0	Enable C	Fallback	Current Lease	Address 192.168.0.41 way Next Hop VL 0	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length

Save Reset

Rys. 8. Konfiguracja i ustawienia dostępu urządzenia do sieci w nowszej wersji firmware oznaczanej v1xx.

Do zarządzania zdalnego należy skonfigurować uniwersalną bramę, której konfiguracja polega na wpisaniu w polu "Network" adresu IP **0.0.0.0** z maską **0** i wymaganym adresem IP bramy. Taka konfiguracja umożliwi kierowanie wszystkich pakietów na wpisaną bramę.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	13/147
------	------	-----------------------------------	------------	--------



IP Configuration

	Current	Configured
eth0:0		
DHCP Client		Renew
IP Address	10.5.5.108	10.5.5.108
IP Mask	255.0.0.0	255.0.0.0
IP Router	10.0.0.2	10.0.0.2
VLAN ID	1	1
DNS Server 1	0.0.0.0	0.0.0
DNS Server 2	0.0.0.0	0.0.0
DNS Server 3	0.0.0	0.0.0
DNS Server 4	0.0.0.0	0.0.0.0
eth0:1	_	
IP Address	0.0.0.0	0.0.0.0
IP Mask	0.0.0.0	0.0.0
IP Router	0.0.0.0	0.0.0
VLAN ID	1	0
eth0:2		
IP Address	0.0.0.0	0.0.0
IP Mask	0.0.0.0	0.0.0.0
IP Router	0.0.0.0	0.0.0
VLAN ID	1	0
eth0:3		
IP Address	0.0.0	0.0.0
IP Mask	0.0.0.0	0.0.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	0

Rys. 9. Konfiguracja i ustawienia dostępu urządzenia do sieci w starszej wersji firmware oznaczanej v0xx .

5.3.1 Konfiguracja NTP

Urządzenia **HYPERION** umożliwiają obsługę protokołu NTP (Network Time Protocol). Dla ustawienia żądanego przez użytkownika sposobu synchronizowania daty i czasu w urządzeniu należy przejść na stronę, która dostępna jest pod linkiem **Configuration > System > NTP**.

NTP Configuration							
Mode	Enabled •						
Server 1	194.146.251.100						
Server 2							
Server 3							
Server 4							
Server 5							
GPS clock							
PTP clock							
Local clock							

Save Reset

Rys. 10. Konfiguracja NTP.

W pierwszej kolumnie tabeli są opisane parametry dla NTP: **Mode** oraz 5 pól do wprowadzenia nazw lub adresów IP serwerów obsługujących synchronizację czasu.

Dodatkowo w różnych wersjach urządzeń HYPERION mogą występować dodatkowe opcje synchronizacji przez PTP lub GPS. Opcja "Local clock" służy tylko do testów i nie należy jej używać do synchronizacji.

Tryb NTP (**Mode)** ma dwie wartości:

Enabled – ten tryb uruchamia działanie klienta NTP, a także urządzenie może funkcjonować jako tzw "pośrednik" protokołu NTP. W urządzeniu które np. ustawia zegar korzystają z zewnętrznych

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	14/147	



serwerów NTP do ustawienia zegara, można wprowadzić adres IP synchronizowanego urządzenia HYPERION, które staje się serwerem dla innych urządzeń, przekazując pakiety NTP do synchronizacji czasu. Ma to znaczenie, jeśli serwer NTP i urządzenie synchronizujące swój zegar znajdują się w innych sieciach.

Disabled – w tym trybie obsługa klienta NTP jest wyłączona.

W polach opisanych jako **Server 1... Server 5** należy wpisać adresy IP serwerów protokołu NTP. Adresy IP mogą być podane w wersji IPv4 jak również w wersji IPv6.

Jeśli posiadamy urządzenie z modułem GPS do synchronizacji NTP zaznaczamy checkbox dla funkcji GPS clock, natomiast jeśli synchronizacja ma odbywać się z PTP zaznaczamy checkbox dla funkcji PTP clock.

Nie jest konieczne wpisywanie wszystkich 5-ciu adresów IP. Dla poprawnego funkcjonowania synchronizacji czasu w **HYPERION** wystarczy wpisać jedynie dwa adresy. Urządzenie próbuje najpierw synchronizować czas z serwerem 1, jeśli próba zakończy się niepowodzeniem to urządzenie dokona próby połączenia z serwerami wpisanymi w kolejnych pozycjach, aż do skutku. W wypadku wybrania trybu NTP **Disabled** nie jest konieczne wpisywanie jakiegokolwiek adresu IP serwera NTP. Po zakończeniu wprowadzania konfiguracji należy kliknąć przycisk **Save.**

WAŻNE: Local clock jest to tryb serwisowy i nie wolno zaznaczać tego okna przy normalnej pracy serwera.

5.3.2 Konfiguracja strefy czasowej oraz ustawienia czasu letniego (dotyczy nowszej wersji oprogramowania)

Aby czas systemowy w przełączniku był prawidłowo wyświetlany należy ustawić odpowiednią strefę czasową oraz jeśli wymaga tego sytuacja wprowadzić dodatkowe przesunięcie dla czasu letniego oraz cykliczną datę rozpoczęcia oraz zakończenia obowiązywania czasu letniego.

	Time	Zone Configuration	
Time Zone	None		
Acronym		(0 - 16 characters)	
Daylight Saving Tim	e Configurat	tion	
Daylight	Saving Time	Mode	
Daylight Saving Time	Disabled	•	
	S-15		
Sta	art Time settin	gs	
Month	Jan	v	
Date	1	v	
Year	2014	Ŧ	
Hours	0	Ŧ	
Minutes	0	τ.	
En	d Time settin	gs	
Month	Jan	Ŧ	
Date	1	Ŧ	
Year	2097	Ŧ	
Hours	0	Ŧ	
Minutes	0	Ŧ	
(Offset settings	5	
	4	(1 1110) Minutes	

Rys. 11. Okno konfiguracji strefy czasowej.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	15/147
------	------	-----------------------------------	------------	--------



5.3.3 Konfiguracja zakładki Alarms

W wybranych modelach dostępna jest funkcja dodatkowych alarmów, które po skonfigurowaniu będą automatycznie wysyłać komunikat jako TRAP-y lub wiadomość email, a także włączania wbudowanych wyjść¹ przekaźnikowych po wskazaniu odpowiednich zdarzeń. Jeśli wersja softu umożliwia taką konfigurację to w zakładce **Configuration** \rightarrow **System** \rightarrow **Alarms** będzie dostępne okno jak poniżej:

Event	SNMP Trap	e-mail	Relay 1	Relay 2
System Events				
Authentication Failure 1				
Link Up				
Port 1				
Port 2				
Port 3				
Port 4				
Port 5				
Port 6				
Port 7		Ē		
Port 8				
Link Down	0	0	0	0
Port 1				
Port 2				
Port 3				0
Port 4				
Port 5				
Port 6				
Poits				U
Port /				
Ethernet Ring Protection Switching	BREAK	0	0	0
Ethernet Chain Protection BREAK				
Digital In Active State				
Digital In Non Active State	0	0		
Digital In 1				
PoF Detected	0	0	0	0
PoE Port 1				
PoE Port 2				
PoE Port 3				0
PoE Port 4				
PoE Classified	0	0	0	0
PoE Port 1			Π	
PoE Port 2				
PoE Port 3				
PoE Port 4				
PoE Powered Up	0		0	
PoE Port 1				
PoE Port 2				
		0		
PoE Port 3				
PoE Port 3				
PoE Port 3 PoE Port 4 PoE Disconnected				
PoE Port 3 PoE Port 4 PoE Disconnected PoE Port 1				
PoE Port 3 PoE Port 4 PoE Disconnected PoE Port 1 PoE Port 2				
PoE Port 3 PoE Port 4 PoE Disconnected PoE Port 1 PoE Port 2 PoE Port 2				

Rys. 12.Okno przykładowej listy zdarzeń i przypisanych alarmów.

W zakładce mamy możliwość konfiguracji, z których zdarzeń będą wysyłane SNMP Trap, wiadomości email lub wyzwolenia wskazanego wyjścia¹. Konfiguracja polega na zaznaczaniu checkbox przy wskazanym zdarzeniu, które opisane są poniżej:

a) grupa Power Up – w przypadku włączenia napięcia na wskazanym złączu Power In.

1 - UWAGA: Wyjścia przekaźnikowe jako opcja dostępne są w wybranych modelach z rodziny Hyperion z oznaczeniami HYPERION-105, HYPERION-300, HYPERION-200

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 16.	/147
--	------



b) grupa Power Down – w przypadku zaniku napięcia na wskazanym złączu Power In.

c) grupa Link Up – w przypadku podniesienia się linku na wskazanym złączu Port.

d) grupa Link Down – w przypadku zaniku linku na wskazanym złączu Port.

e) grupa Ethernet Ring Protection Switching – możliwość konfiguracji alarmów będzie dostępna po skonfigurowaniu funkcji ERPS.

f) grupa Chain Protection – możliwość konfiguracji alarmów będzie dostępna po skonfigurowaniu funkcji CHAIN.

g) grupa Digital In Active State – w przypadku jeśli wejście cyfrowe zmieni stan (np. Zadziała czujka ruchu i styk zostanie zwarty) wtedy urządzenie wyśle Trap lub email lub wyjście¹ przekaźnikowe zadziała czyli zmieni stan na przeciwny.

h) grupa Digital In Non Active State – zasada działania jest taka sama jak w punkcie "g" tylko z negacją to znaczy z odwrotną logiką.

i) grupa PoE Detected – w przypadku detekcji PoE na porcie.

j) grupa PoE Classified – w przypadku prowadzenia klasyfikacji PoE.

k) grupa PoE Powered Up – w przypadku podawania zasilania z portu poprzez skrętkę UTP.

I) grupa PoE Disconnected – w przypadku braku zasilania z PoE.

Znaczenie poszczególnych kolumn:

SNMP Trap – po wykryciu zdarzeniu zostanie wysłany trap z informacją o zaistniałej sytuacji.

e-mail – po wykryciu zdarzeniu zostanie wysłana wiadomość email.

Relay 1 – po wykryciu zdarzeniu wyjście cyfrowe zadziała czyli zmieni stan na przeciwny.

Relay 2 – po wykryciu zdarzeniu wyjście cyfrowe zadziała czyli zmieni stan na przeciwny.

Snmp trap należy włączyć i skonfigurować w zakładce **Security** \rightarrow **Switch** \rightarrow **SNMP** \rightarrow **System**, a następnie skonfigurować w zakładce TRAP. W przypadku wiadomości email funkcję tą należy włączyć i skonfigurować w zakładce **System** \rightarrow **SMTP**. Należy zwrócić uwagę, że w takim wypadku przełącznik wymaga dostępu do internetu oraz serwera pocztowego.

Alarms Priority

System	Power	Link	ERPS	Chain Prot.	Digital In	PoE Plus	
Minor 🗸	Major 🗸	Info 🗸	Critical 🗸	Critical 🗸	Minor 🗸	Major 🗸	
					Minor		
					Major		
					Critical		
					Info		

Rys. 13.Okno do ustawienia priorytetów dla alarmów

Poziom priorytetyzacji alarmów jest następujący:

Minor – odpowiada poziomowi alarm normalny.

Major – odpowiada poziomowi alarm wysoki.

Critical – odpowiada poziomowi alarm krytyczny.

Info – odpowiada poziomowi alarm informacyjny.

5.4 Konfiguracja portów Ethernet

Strona umożliwiająca konfigurację portów Ethernet **HYPERION** jest dostępna pod linkiem **Configuration** → **Ports**. Okno to wyświetla w kolumnie **Link** aktualny stan połączeń na wszystkich portach, natomiast szybkość i tryb połączenia w kolumnie **Speed Current**. W oknie dostępne są następujące funkcje konfiguracyjne:

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	17/147
------	------	-----------------------------------	------------	--------



Speed Configured – ustawianie autonegocjacji lub wskazanej prędkości z half lub full dupleksem oraz umożliwia całkowite wyłączenie portu.

Adv Duplex oraz **Adv speed** – służą do ręcznego włączania/wyłączania poszczególnych trybów oraz prędkości przy porcie ustawionym w trybie Auto negocjacji.

Flow Control Configured – włączenie automatycznej kontroli przepływu poprzez zaznaczenie pola w kolumnie enable.

Maximum Frame Size – ustawienie maksymalnej długości ramki (MTU), jaką przełącznik ma akceptować i retransmitować.

Excessive Collision Mode – ustawienie sposobu zachowania się portu w przypadku wystąpienia szesnastu kolizji przy próbie transmisji jednej ramki, dostępne są dwie opcje: odrzucenie ramki (**Discard**) lub ponowienie próby transmisji (**Restart**). Ustawienie nie ma znaczenia w przypadku pracy portu w trybie full-duplex.

Frame Length Check – Kontrola długości ramki. Włączenie tej opcji spowoduje, że ramki o nieprawidłowej długości w polu EtherType/Length powinny zostać pominięte. Jeśli włączona jest funkcja "Frame Length Check", to ramki o rozmiarze mniejszym niż 1536 bajtów są pomijane, jeśli pole EtherType/Length nie jest zgodne z rzeczywistą długością pola danych. Jeśli opcja "Frame Length Check" jest wyłączona, ramki nie są pomijane. Uwaga: Liczniki nie będą zliczać ramek pominiętych z powodu nieprawidłowej długości ramki.

Ustawienie portu SFP w trybie autonegocjacji (AUTO) spowoduje przesyłanie po torze optycznym informacji o możliwości pracy z prędkością 1000Mbps. Przy skonfigurowaniu portu SFP tylko w trybie 1000Mbps informacja ta nie będzie przesyłana. Aby transmisja na portach SFP+ pracowała z prędkością 10Gb/s to porty muszą być ustawione z wymuszoną prędkością 10Gb, w innym przypadku transmisja nie będzie działać.

Port Configuration																	
Interface	Description	Link		Speed	Adv D	uplex		Adv sp	eed		Flov	v Control		PFC	Maximum	Excessive	Frame
Interrace	Description	LINK	Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority	Frame Size	Collision Mode	Length Check
*				<> ▼	1	√	1	1						0-7	10240	<> ▼	
10GigabitEthernet 1/1			Down	10Gbps FDX 🔹	\$	4	al and a second	s.	4		×	×		0-7	10240		
10GigabitEthernet 1/2			Down	10Gbps FDX 🔹							×	×		0-7	10240		
10GigabitEthernet 1/3			Down	10Gbps FDX 🔹	4	4	4	4	4		×	×		0-7	10240		
10GigabitEthernet 1/4			Down	10Gbps FDX 🔹	4	1	1	1	1		×	x		0-7	10240		
GigabitEthernet 1/1			Down	Disabled	4	4	1	4	4		×	×		0-7	10240		
GigabitEthernet 1/2		•	Down	Auto 100Mbps EDX	4	1	1	1	1		×	x		0-7	10240		
GigabitEthernet 1/3			Down	1Gbps FDX	4	4	1	4	4		×	×		0-7	10240		
GigabitEthernet 1/4			Down	2.5Gbps FDX	1	1	1	1	1		x	x		0-7	10240		
GigabitEthernet 1/5			Down	TUG6ps FDX	4	4	4	4	4		x	x		0-7	10240		
GigabitEthernet 1/6			Down	Auto 🔻	1	1	1	1	1		x	X		0-7	10240		
GigabitEthernet 1/7		۲	Down	Auto 🔻	4	4	1	4	4		×	x		0-7	10240		
GigabitEthernet 1/8		•	Down	Auto 🔻	1	1	1	1	1		×	x		0-7	10240		
GigabitEthernet 1/9		۲	Down	Auto 🔻	1	1	1	1			x	x		0-7	10240	Discard •	
GigabitEthernet 1/10		•	Down	Auto 🔻		1	1	1			X	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/11		۲	Down	Auto 🔻	•	1	1	1			x	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/12			Down	Auto 🔻	e	1	1	1			x	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/13		۲	Down	Auto 🔻	•	1	1	1			x	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/14		٠	Down	Auto 🔻	e	1	1	1			x	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/15		۲	Down	Auto 🔻	•	1	1	1			x	x		0-7	10240	Discard 🔻	
GigabitEthernet 1/16			Down	Auto 🔻		•			1		x	×		0-7	10240	Discard 🔻	

Rys. 14. Konfiguracja trybu pracy poszczególnych portów w przełącznikach Hyperion 500, 402, 200.

Port Configuration

Dout	Link	Speed		Adv [Adv Duplex		lv spee	d	F	low Contr	ol	Maximum	Excessive	Frame
Pon	LINK	Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Frame Size	Collision Mode	Length Check
*			< ▼			√	\$					9600	<> ▼	
1		100fdx	Auto 🔻	-		1	-			×	×	9600	Discard 🔻	
2		100fdx	Auto 🔻	1		√	\$			×	×	9600	Discard 🔻	
3		100fdx	Auto 🔻	1	1	1	\$			×	×	9600	Discard 🔻	
4		Down	Auto 🔻	1	1	√	e			X	×	9600	Discard 🔻	
5	۲	Down	Auto 🔻	1	1	1	1	1		x	×	9600		
6		Down	Auto 🔻	1	1	1	e	1		X	x	9600		
7	۲	Down	Disabled	1	1	1	1	1		x	x	9600		
Save	Rese	ŧt	Auto 100Mbps FDX 1Gbps FDX 2.5Gbps FDX											

Rys. 15.Rys. 15. Konfiguracja trybu pracy poszczególnych portów w przełącznikach Hyperion 105 i 300 w starszej wersji firmware.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	18/147
------	------	-----------------------------------	------------	--------



5.5 Konfiguracja THERMAL PROTECTION

Przełączniki HYPERION umożliwiają ustawienie sprawdzenie i skonfigurowanie bieżących ustawień kontroli ochrony termicznej. Taka ochrona ma na celu zapobiec przegrzaniu chipa procesora. Gdy temperatura przekroczy skonfigurowana temperaturę ochrony termicznej, porty zostaną wyłączone w celu zmniejszenia zużycia energii. Istnieje możliwość zestawienia portów z różnymi grupami. Każdej grupie można nadać temperaturę, przy której odpowiednie porty powinny być wyłączone.

lemperature settings for groups								
Group	Tempera	e						
0	255	°(C					
1	255	°(C					
2	255	°(C					
3	255	C						
Port grou	ıps							
Int	erface		Group					
		*	 v 					
10Gigabi	10GigabitEthernet 1/1							
10Gigabi	Disabled 🗸							
10Gigabi	Disabled 🗸							
10Gigabi	tEthernet 1	/4	Disabled V					

GigabitEthernet 1/1

GigabitEthernet 1/3

Rys.	16. Konfiguracja	Thermal	Protection w	przełą	cznikach.

GigabitEthernet 1/2 Disabled V

Temperature settings for groups - Ustawienie temperatury dla poszczególnej grupy, przy której porty zostaną wyłączone. Zakres możliwy temperatur to od 0 - 255 °C. Port groups - Wybór do jakiej grupy należy dany port.

5.6 PRP lub HSR (opcja w wybranych przełącznikach wyposażonych w DODATKOWY MODUŁ REDBOX)

Disabled 🗸

Disabled V

5.6.1 Konfiguracja PRP lub HSR

Przełączniki HYPERION-500 lub HYPERION-200 wyposażone w moduły REDBOX umożliwiają tworzenie sieci z bezstratną redundancją z wykorzystaniem protokołu PRP. Natomiast protokół HSR umożliwia budowę ringów z bezstratną transmisją.



Rys. 17.PRP/HSR – "zero packet loss ring"

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	19/147
------	------	-----------------------------------	------------	--------



Przełącznik Hyperion-500 może zostać wyposażony w nawet w cztery moduły Redbox, tworząc cztery niezależne sieci redundantne. W **Configuration** \rightarrow **PRP** umożliwia zmianę trybu pracy poszczególnych modułów Redbox.

PRP HSR Configuration

PRP	Description	Mode	Entr	y Forget Time	Forward LAN A <-> LAN B
PRP 1/1		PRP 🗸	[10ms 🗸	
PRP 1/2		Disable 🗸	(10ms 🗸	
PRP 1/3		Disable 🗸		10ms 🖌	
PRP 1/4		Disable 🗸		10ms 🗸	

Save Reset

Rys. 18. Konfiguracja modułów REDBOX.

PRP - To jest logiczny numer instancji HSR/PRP dla tego wiersza.

Description - Opis portu.

Mode - Wybiera dostępne tryby dla danej instancji PRP HSR. Możliwe tryby to:

Disable - wyłącza działanie instancji PRP HSR.

Switch - PRP HSR działa jako przełącznik 3-portowy: LAN A, LAN B oraz port łączący wewnątrz urządzenia z głównym przełącznikiem.

PRP - Włącz tryb PRP.

HSR - Włącz tryb HSR.

Entry Forget Time - maksymalna różnica w czasie transportu odbieranych pakietów do interfejsów A i B w module.

Forward LAN A <-> LAN B – włączona funkcja używana tylko w PRP, umożliwia na przekazywanie pakietów między LAN A, a LAN B. Wyłączona blokuje przekazywanie tych pakietów².

5.6.2 Monitorowanie modułów REDBOX

DDD USD Status

W zakładce **Monitor** \rightarrow **PRP** \rightarrow **Status** możemy odczytać w jakim trybie aktualnie pracuje dana instancja oraz czy porty LAN A i LAN B mają podniesione linki.

FRF Hor otatus						
				LAN A		LAN B
PRP	Description	Mode	Link	Speed	Link	Speed
PRP 1/1		Disable		Down		Down
PRP 1/2		Disable		Down		Down
PRP 1/3		Disable		Down		Down
PRP 1/4		Disable		Down		Down

Rys. 19. Monitorowanie statusu modułów i portów.

Po przejściu do zakładki **Monitor** \rightarrow **PRP** \rightarrow **Detailed** oraz wybraniu jednego z czterech logicznych slotów możemy analizować szczegółowe statystki transmisji na portach A i B.

2 UWAGA!! Nie wolno stosować tej funkcji w trybie HSR!

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	20/147
------	------	-----------------------------------	------------	--------



Detailed PRP HSR Statistics Interface PRP 1/1

PRP 1/1 🗸 Auto-refresh

PRP Description Mode Link	< Speed Link Speed		
PRP 1/1 Disable 🔴	Down 🛑 Down		
•	• • • • • • • • • • • • • • • • • • •		
	LAN A	L	AN B
Receive Total	Transmit Total	Receive Total	Transmit Total
Rx Packets	0 Tx Packets 0	Rx Packets 0	Tx Packets
Rx Octets	0 Tx Octets 0	Rx Octets 0) Tx Octets
Rx Unicast	0 Tx Unicast 0	Rx Unicast 0) Tx Unicast
Rx Multicast	0 Tx Multicast 0	Rx Multicast 0	Tx Multicast
Rx Broadcast	0 Tx Broadcast 0	Rx Broadcast 0) Tx Broadcast
Receive Size Counters		Receive Size Counters	
Rx 64 Bytes	0	Rx 64 Bytes 0)
Rx 65-127 Bytes	0	Rx 65-127 Bytes 0)
Rx 128-255 Bytes	0	Rx 128-255 Bytes 0)
Rx 256-511 Bytes	0	Rx 256-511 Bytes 0)
Rx 512-1023 Bytes	0	Rx 512-1023 Bytes 0)
Rx 1024- Bytes	0	Rx 1024- Bytes 0)
Receive Error Counters		Receive Error Counters	
Rx Errors	0	Rx Errors ()
Rx CRC/Alignment	0	Rx CRC/Alignment 0)
Rx Undersize	0	Rx Undersize 0)
Rx Oversize	0	Rx Oversize 0)
Rx Fragments	0	Rx Fragments 0)
Rx Jabber	0	Rx Jabber 0)
Rx Octets	0	Rx Octets 0)
Receive PRP HSR packets and errors	Transmit PRP HSR packets and drops	Receive PRP HSR packets and errors	Transmit PRP HSR packets and drops
Rx PRP HSR Packets	0 Tx PRP HSR Packets 0	Rx PRP HSR Packets 0	Tx PRP HSR Packets
Rx Wrong Lan	0 Tx Queue Drop Packets 0	Rx Wrong Lan 0	Tx Queue Drop Packets
Rx Duplicte	0 Tx Early Drop Packets 0	Rx Duplicte 0) Tx Early Drop Packets

Rys. 20. Monitorowanie szczegółowych statystyk transmisji.

5.7 Konfiguracja portów z POWER OVER ETHERNET (opcja w wybranych przełącznikach)

Przełącznik **HYPERION** może zostać wyposażony w moduł PoE na portach RJ45 do zasilania zewnętrznych urządzeń np. Kamery poprzez skrętkę UTP. Jeśli urządzenie posiada taki moduł, wtedy w menu zarządzania pojawia się zakładka PoE z pod zakładką "Configuration".

Moduły PoE posiadają zgodność ze standardem IEEE 802.3af/at/bt i PoE++ (90W)- dostępne w wybranych wersjach. W zakładce **Configuration** \rightarrow **PoE** \rightarrow **Configuration**, możemy ustawić żądaną moc na poszczególnych portach poprzez zmianę trybu lub wpisując wartość mocy w polu Maximum Power [W].

W trybie Manual należy zwrócić uwagę na ustawienie pola Maximum Power [W], ponieważ switch dla trybu manual ma wyłączoną detekcję tylko zawsze podaje moc PoE na porcie.

Power over Ethernet Configuration

Global Power over Ethernet Configuration						
Power Supply Budget [W]	240					
Reserved Power determined by	Class T					
Power Management Mode	Reserved v					

Port Configuration

Port	Power Up	PoE Mode	Priority	Maximum Power [W]	Power Up Delay
1		PoE+ IEEE802.3a ▼	High 🔻	30.0	0s 🔻
2		PoE+ IEEE802.3ar ▼	High 🔻	30.0	0s 🔻
3		PoE+ IEEE802.3a ▼	High 🔻	30.0	0s 🔻
4		PoE+ IEEE802.3a ▼	High 🔻	30.0	0s 🔻
Save	Reset	Disable PoE IEEE802.3af PoE+ IEEE802.3at PoE++ Force Manual			

Rys. 21.Konfiguracja trybu pracy portów z PoE.

Power Supply Budget – definiujemy ograniczenie budżetu mocy na całe urządzenia w pełnych jednostkach [W].

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	21/147
------	------	-----------------------------------	------------	--------



Reserved Power determined by – definiujemy ograniczenie mocy na porcie. 'Class' tryb zgłasza urządzenie zdalne, wstępna definicja w polu 'PoE Mode', natomiast 'Allocation' tryb definiowany ręcznie w polu 'Maximum Power'.

Power Management Mode – wybieramy ograniczenie mocy na podstawie rezerwacji 'Reserved' w polu 'Maximum Power'. Natomiast 'Consumption' rozpatruje globalne ograniczenie mocy 'Power Supply Budget' i w przepadku przekroczenia odłącza porty wg priorytetów, a jeśli występuje ten sam priorytet to wg numeracji portów (wyższy nr ma mniejszy priorytet).

PoE Mode – wybieramy tryb, z jakim następuje detekcja i klasyfikacja PoE w urządzenie zasilanym, wiąże się to z ilością mocy na porcie jak i też z możliwością wyłączenia negocjacji mocy w trybie 'Force' lub 'Manual'.

Uwaga: W trybach '**Force'** oraz '**Manual**' moc na porcie podawana jest zawsze z częściową weryfikacją, dla odbiornika obsługującego funkcję zasilania przez skrętkę, co może prowadzić do uszkodzenia w urządzeniu portu podłączanego do portu przełącznika z PoE, a w sporadycznych przypadkach całego urządzenia. Tryb ten jest czasem wymagany przez niektóre odbiorniki.

Priority – podczas przekroczenia budżetu maksymalnego 'Power Supply Budget', porty dostarczające napięcie są wyłączane wg ustawionych priorytetów. Kolejne kryterium, gdy oba mają ten sam 'Priority', to wg nr portu (wyższy nr portu ma niższy priorytet).

Power Up Delay – czas zwłoki uruchamiania portu po starcie urządzenia lub poprzedniego portu.

5.7.1 MONITOROWANIE FUNKCJI POWER OVER ETHERNET (OPCJA W WYBRANYCH PRZEŁĄCZNIKACH)

Monitorowanie portów pozwala określić moc pobieraną przez każdy z odbiorników, jest to szczególnie istotne w przypadku wstąpienia awarii, można wtedy szybko zlokalizować np. uszkodzoną kamerę lub zwarcie na skrętce.

Power	over Et	hernet Status						
Globa	l Status							
Total Port S	Power [W 0.53 tatus	V] Total Energy [Wh] 0.0497						
Port	Power	Detect	Class	Up Time	Voltage [V]	Current [mA]	Power [W]	Energy [Wh]
1		SHORT						
2		Open						
3		OK	4 [25.5W]	0d 0h 0m 28s	48.53	11	0.53	0.0041
4		Open						

Rys. 22. Monitorowanie PoE na portach.

Opis ważniejszych pól

Total Power [W] – sumaryczna moc pobierana przez urządzenia zasilane przez PoE.

Total Energy [W] – Licznik energii [watogodziny] jakie pobrał przełącznik.

Port – numer portu w przełączniku.

Power – sygnalizacja uruchomienia PoE na porcie.

Detect – opisowe pole detekcji PoE.

Class – numer klasy w PoE przy klasyfikacji urządzenia PD przez przełącznik.

Up time – czas pracy PoE.

Voltage [V] – aktualne napięcie na porcie.

Current [mA] – aktualna wartość prądu pobieranego przez PD.

Power [W] - aktualna wartość mocy pobieranej przez PD.

Energy [Wh] - aktualna wartość energii pobieranej przez PD.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	22/147
------	------	-----------------------------------	------------	--------



5.8 Ograniczenie dostępu zdalnego

Przełącznik **HYPERION** wyposażony jest w możliwość ograniczenia zdalnego dostępu do zarządzania. Ograniczenie to jest zrealizowane na cztery sposoby:

- Hasło dostępu,
- Ograniczenie protokołów wymiany danych do zarządzania,
- Ograniczenie zakresu adresów IP stacji roboczych, z których można uzyskać dostęp do zarządzania,
- Listy ACL.

Nowe urządzenie nie jest zabezpieczone hasłem. Hasło dostępu można wprowadzić i/lub zmienić na stronie po kliknięciu na następujące linki:

$\textbf{Configuration} \rightarrow \textbf{Security} \rightarrow \textbf{Switch} \rightarrow \textbf{Users}$

Następnie w oknie klikamy na użytkownika admin.

W celu wprowadzenia hasła należy w polu oznaczonym **Password** wprowadzić żądane hasło, następnie w polu **Password** (**again**) należy ponownie wprowadzić to samo hasło. Następnie kliknąć przycisk **Save**. Zmiana hasła jest możliwa tylko wtedy, gdy zostanie wpisane poprawnie stare hasło i nowe takie samo hasło w obu polach. Po wprowadzeniu haseł w celu potwierdzenia zmian należy kliknąć przycisk **Save**.

Przycisk **Add New User** – służy do dodania kolejnych użytkowników, jednocześnie ustanawiając odpowiedni poziom dostępu.

	Edit User		
Users Configuration	User Settings		
	User Name	admin	
User Name Privilege Level	Password		
admin 15	Password (again)		
Add New User	Privilege Level	15 🔹	
	Save Reset C	ancel	

Rys. 23. Konfiguracja użytkowników oraz okno do ustawiania hasła.

5.9 Konfiguracja poziomu uprawnień

5.9.1 Group Name

Nazwa identyfikująca grupę uprawnień. W większości przypadków grupa poziomów uprawnień składa się z jednego modułu (np. LACP, RSTP lub QoS), ale kilka z nich zawiera więcej niż jeden. Poniższy opis szczegółowo definiuje te grupy z poziomami uprawnień:

System: Kontakt, nazwa, lokalizacja, strefa czasowa, czas letni, dziennik.

Security: Uwierzytelnianie, zarządzanie dostępem do systemu, port (zawiera port Dot1x, oparty na MAC i limit adresów MAC), ACL, HTTPS, SSH, ARP Inspection, ochrona źródła IP.

IP: Wszystko oprócz "pingu".

Port: Wszystko oprócz "VeriPHY".

Diagnostics: 'ping' i 'VeriPHY'.

Maintenance: Ponowne uruchomienie systemu CLI, domyślne przywracanie systemu, hasło systemowe, zapisywanie konfiguracji, ładowanie konfiguracji i ładowanie oprogramowania układowego. Użytkownicy sieci Web, poziomy uprawnień i wszystko w ramach konserwacji. **Debug:** Występuje tylko w CLI.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	23/147
------	------	-----------------------------------	------------	--------



5.9.2 Privilege Levels

Każda grupa posiada poziom uprawnień autoryzacji dla następujących podgrup: konfiguracja tylko do odczytu, konfiguracja/wykonanie do odczytu i zapisu, status/statystyki tylko do odczytu, status/statystyki do odczytu i zapisu (np. do czyszczenia statystyk). Uprawnienia użytkownika powinny być takie same lub wyższe niż poziom uprawnień autoryzacji, aby mieć dostęp do tej grupy.

				Privilege Levels
Group Name	Configuration	Configuration/Execute	Status/Statistics	Status/Statistics
	Read-only	Read/write	Read-only	Read/write
Aggregation	5 🗸	10 🗸	5 🗸	10 🗸
Alarms	5 🗸	10 🗸	5 🗸	10 🗸
BtNet	5 🗸	10 🗸	5 🗸	10 🗸
DDMI	5 🗸	10 🗸	5 🗸	10 🗸
Debug	15 🗸	15 🗸	15 🗸	15 🗸
DHCP	5 🗸	10 🗸	5 🗸	10 🗸
DHCPv6_Client	5 🗸	10 🗸	5 🗸	10 🗸
Diagnostics	5 🗸	10 🗸	5 🗸	10 🗸
E1	5 🗸	10 🗸	5 🗸	10 🗸
EPS	5 🗸	10 🗸	5 🗸	10 🗸
ERPS	5 🗸	10 🗸	5 🗸	10 🗸
GPS	5 🗸	10 🗸	5 🗸	10 🗸
Green Ethernet	5 🗸	10 🗸	5 🗸	10 🗸
IP	5 🗸	10 🗸	5 🗸	10 🗸
IPMC Snooping	5 🗸	10 🗸	5 🗸	10 🗸
JSON RPC	5 🗸	10 🗸	5 🗸	10 🗸
JSON RPC Notification	5 🗸	10 🗸	5 🗸	10 🗸
LACP	5 🗸	10 🗸	5 🗸	10 🗸
LLDP	5 🗸	10 🗸	5 🗸	10 🗸
Loop Protect	5 🗸	10 ~	5 🗸	10 🗸
MAC Table	5 🗸	10 🗸	5 🗸	10 🗸
Maintenance	15 🗸	15 🗸	15 🗸	15 🗸
MEP	5 ¥	10 ¥	5 ¥	10 🗸
Modular	5 ¥	10 ¥	5 🗸	10 🗸
MVR	5 ¥	10 ¥	5 🗸	10 🗸
NTP	5 ¥	10 ¥	5 🗸	10 🗸
Ports	5 ¥		1 -	10 🗸
Private VLANs	5 ×		5 🗸	10 ¥
Pro Chain	5 ¥		5 🗸	10 -
PRP HSR Redundancy	5 ×	10 ~	5 ¥	10 ¥
PTP	5 ¥	10 ¥	5 🗸	10 -
008	5 ¥	10 4	5 🗸	10 -
RMirror	5 4	10 4	5 4	10 -
Security	5 2	10 ¥	5 4	
sElow	5 2	10 -	5 4	10 -
Snanning Tree	5 4	10 4	5 4	10 *
Static NAT	5 4	10 4	5 4	10 +
System	5 4	10 ¥	1 4	10 ¥
	5 4	10 *	5 4	10 +
LIPnP	5 4	10 +	5 4	10 +
VCI	5 4	10 •	5 4	10 ¥
VOL	5 •	10 ¥	5 4	10 ¥
VLAN_TRANSlation	5 •	10 V	5 v	10 V
VICANS	5 •	10 ¥	5 4	10 ¥
VOICE_VEAN	3 V	10 V	○ ▼	10 V
XXRP	> 	10 🗸	5 🗸	10 🗸

Privilege Level Configuration

Save Reset

Rys. 24. Poziomy uprawnień do funkcji i zarządzania.

5.10 Konfiguracja metod uwierzytelniania oraz autoryzacji

Ograniczenie protokołów zarządzania można dokonać na stronie po kliknięciu na następujące linki: **Configuration** — **Security** — **Switch** — **Auth Method**. Domyślnie urządzenie **HYPERION** posiada włączone wszystkie obsługiwane protokoły do zarządzania. W celu wyłączenia z obsługi jednego lub więcej protokołów należy przy nazwie wybranego protokołu przestawić za pomocą pola wyboru

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	24/147
------	------	-----------------------------------	------------	--------



metodę **local** na **none**, a następnie potwierdzić zmianę przez kliknięcie przycisku **Save**. Włączenie obsługi odbywa się podobnie, należy przy nazwie wybranego protokołu przestawić pole wyboru na **local** i również potwierdzić zmianę przez kliknięcie **Save**.

Authentication Method Configuration

Client	Methods					
console	local 🔹	·	no		no	
telnet	local 🔹	'	no	٣	no	٣
ssh	local 🔹	7	no	٣	no	
http	local 🔹	'	no	٣	no	٣

Command Authorization Method Configuration

Client	Met	hod	Cmd Lvl	Cfg Cmd
console	no	•	0	
telnet	no	T	0	
ssh	no	•	0	

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no 🔻		
telnet	no 🔻		
ssh	no 🔻		
Save	Reset		

Rys. 25.Ograniczenie protokołów zarządzania.

Ograniczenie zakresu adresów IP stacji roboczych, z których można uzyskać dostęp do zarządzania można ustawić na stronie po kliknięciu na następujące linki: **Configuration > Security > Switch > Access Management**. W celu ustawienia zakresu należy wpisać w pole **Start IP Address** pierwszy adres z grupy, która może uzyskać dostęp do zarządzania urządzeniem **HYPERION**, a w polu **End IP Address** ostatni adres tej grupy. Następnie należy określić za pomocą jakich protokołów dana grupa może uzyskać dostęp do urządzenia. Na koniec należy w polu **Mode** wybrać z listy parametr **Enabled**.

UWAGA! Błędne wprowadzenie zakresu adresów IP stacji roboczych, doprowadzi do utraty połączenia z urządzeniem.

Mode	Enabled •				
Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	10.10.0.1	10.10.0.12			
Delete	10.10.1.1	10.10.1.9			
Delete	10.10.2.5	10.10.2.5			
Add new	entry				

Save Reset

Access Management Configuration

Rys. 26. Ograniczenie zakresów adresów IP do zarządzania.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	25/147
------	------	-----------------------------------	------------	--------



W przypadku ograniczenia dostępu przez domyślną sieć VLAN 1 w powyższym oknie należy ustawić inny numer VLAN niż 1 wraz z zakresem adresów IP. Spowoduje to całkowite ograniczenie VLAN 1. Podany VLAN musi być skonfigurowany w zakładce IP jako kolejny interfejs z odpowiednim adresem IP ze wskazanej puli.

UWAGA: Wcześniejsze nie skonfigurowanie odpowiedniego VLAN-u w zakładce konfiguracji VLANów oraz jednoczesne ograniczenie VLAN-u 1 doprowadzi do pozbawienia się dostępu do urządzenia.

Włączenie usługi dostępu SSH następuje po przejściu do zakładki **Configuration > Security > Switch > SSH.** Po otwarciu okna usługa jest domyślnie włączona.

SSH Configuration

Rys. 27.Konfiguracja SSH.

Jeśli w polu Mode przełączymy na Disabled usługa zostanie wyłączona.

5.11 Konfiguracja HTTPS

HTTPS Configuration

Mode	Enabled	~	
Automatic Redirect	Enabled		
Certificate Maintain	Upload	~	
Certificate Pass Phrase			
Certificate Upload	Web Browser	~	
File Upload	Wybierz plik Nie wybrano pliku		
Certificate Status	Switch secure HTTP certificate is presented		

Save Reset

Rys. 28.Konfiguracja HTTPS.

5.11.1 Mode

Enabled: Włącz działanie w trybie HTTPS. **Disabled:** Wyłącz działanie w trybie HTTPS.

5.11.2 Automatic Redirect (Automatyczne przekierowanie)

Konfiguracja trybu przekierowania na stronę HTTPS. Ma to znaczenie tylko wtedy, gdy wybrany jest tryb "HTTPS Mode Enabled". Gdy tryb przekierowania jest włączony, połączenie HTTP zostanie automatycznie przekierowane na połączenie HTTPS.

Zwróć uwagę, że przeglądarka może nie zezwalać na operację przekierowania ze względów bezpieczeństwa, a w tym przypadku musisz ręcznie zainicjować połączenie HTTPS.

Enabled: Włącz działanie w trybie przekierowania HTTPS.

Disabled: Wyłącz działanie w trybie przekierowania HTTPS.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	26/147
---	------------	--------



5.11.3 Certificate Maintain

Funkcja do zarządzania certyfikatem.

None: brak operacji.

Delete: Usuń bieżący certyfikat.

Upload: prześlij plik certyfikatu PEM. Możliwe metody to: przeglądarka internetowa lub adres URL. **Generate**: Wygeneruj nowy certyfikat RSA z podpisem własnym.

5.11.4 Certificate Pass Phrase

W tym polu wprowadź hasło, w przypadku gdy ładowany certyfikat jest chroniony hasłem.

5.11.5 Certificate Upload

Umożliwia przesyłanie pliku z certyfikatem PEM do przełącznika. W jednym pliku powinny być zawarte dwa pliki to jest certyfikat i klucz prywatny.

Uwaga: certyfikat RSA jest zalecany, ponieważ większość nowych wersji przeglądarek usunęła obsługę DSA w certyfikacie, m.in. Firefox v37 i Chrome v39.

Możliwe metody to:

Web Browser: Prześlij certyfikat za pomocą przeglądarki internetowej.

URL: Prześlij certyfikat przez adres URL, obsługiwane protokoły to HTTP, HTTPS, TFTP i FTP. Format adresu URL to <protokół>://[<nazwaużytkownika>[:<hasło>]@]<host>[:<port>][/<ścieżka>]/<nazwa_pliku>.

Na przykład

tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10.80/ new_image_path/new_image.dat.

Prawidłowa nazwa pliku to ciąg tekstowy złożony tylko ze znaków takich jak z alfabetu (A-Za-z), cyfr (0-9), kropki (.), łącznika (-), pod myślnika (_). Maksymalna długość to 63, a myślnik nie może być pierwszym znakiem. Nie dozwolona jest nazwy pliku składająca się tylko ze znaku "."

5.11.6 Certificate Status

Wyświetla aktualny stan certyfikatu na przełączniku.

Switch secure HTTP certificate is presented. - oznacza "Wyświetlany jest bezpieczny certyfikat HTTP przełącznika"

Switch secure HTTP certificate is not presented. - oznacza "Bezpieczny certyfikat HTTP przełącznika nie jest prezentowany"

Switch secure HTTP certificate is generating - oznacza "Przełącz bezpieczny certyfikat HTTP jest generowany...."

5.12 SNMP Simple Network Management Protocol

SNMP jest uniwersalnym protokołem wspomagającym zarządzanie urządzeniami pracujących w sieciach IP. Wykorzystuje on głównie protokół UDP na standardowym porcie 161 (wysyłanie żądań) oraz 162 (komunikaty TRAP). **HYPERION** obsługuje następujące wersje SNMP:

- SNMPv1 opisana w RFC 1157 bezpieczeństwo oparte jest o tzw. nazwy społeczności (ang. community name), które są pewnego rodzaju nieszyfrowanymi hasłami dostępu,
- SNMPv2c opisana w RFC 1901 posiada obsługę grupowych zapytań w celu zwiększenia wydajności oraz kilka innych ulepszeń, z bezpieczeństwem jak w SNMPv1,
- SNMPv3 opisana w RFC 3411, obsługująca dostęp oparty na użytkownikach oraz szyfrowanie transmisji.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	27/147
------	------	-----------------------------------	------------	--------



SNMP System Configuration

Mode	Enabled •
Version	SNMP v2c 🔻
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Save Reset

Rys. 29. Konfiguracja ogólna SNMP.

SNMP Trap Configuration

TOCH			
Trap Config Nan	ne		_
Trap Mode		Enabled	•
Trap Version		SNMP v2c	•
Trap Community	/	Public	
Trap Destination	Address		
Trap Destination	Port	162	
Trap Inform Mod	le	Disabled	*
Trap Inform Time	eout (seconds)	3	
Trap Inform Retr	y Times	5	
Trap Probe Secu	urity Engine ID	Enabled	Ŧ
Trap Security Er	ngine ID		
Trap Security Na	ame	None	Ŧ
SNMP Trap Eve	nt		
System	🗆 * 🗆 Warm St	art	Cold Start
	Link up 🔘 r	ione 🔍 specific 🔍 all switches	
Interface	The second secon	● none	
	LLDP 🖲 no	ne 🔍 specific 🔍 all switches	
Authentication	* SNMP A	uthentication Fail	
Switch	🗆 * 🔲 STP		RMON

Save Reset

Rys. 30. Konfiguracja SNMP TRAP.

W nowszej wersji oprogramowania dostępne są dodatkowe alarmy, które po skonfigurowaniu będą automatycznie przesyłane jako TRAP-y. Jeśli dana wersja softu umożliwia taką konfigurację to w zakładce **Configuration** → **System** → **Alarms** będzie dostępne okno konfiguracji. Zakładka Alarms i sposób konfiguracji opisuje punkt 5.3.3 niniejszej instrukcji.

Dostęp do konfiguracji agenta SNMP można uzyskać przez menu link **Configuration** \rightarrow **Security** \rightarrow **Switch** \rightarrow **SNMP**. W sekcji **SNMP System Configuration** można włączyć i wyłączyć obsługę protokołu SNMP oraz wybrać jego główną wersję, wraz z podstawowymi parametrami charakterystycznymi dla tej wersji, które będą używane do komunikacji. Wybranie wersji SNMPv2c umożliwia także dostęp przez wersję SNMPv1, a wybranie SNMPv3 umożliwia dostęp przez wersje 1 oraz 2c, chyba że zostanie on ograniczony przez dodatkowe ustawienia SNMPv3, opisane w dalszej części tego rozdziału. W konfiguracji ogólnej, w zależności od wybranej wersji protokołu dostępne są dodatkowe opcje. Dla SNMPv1 i SNMPv2c należy ustawić nazwy społeczności z prawem odczytu oraz z prawem zapisu; dla SNMPv3 należy ustawić **Engine ID** – jest to unikalny numer urządzenia w sieci SNMP (przypisany do agenta SNMP, obsługującego komunikację). Jest on ciągiem 5 - 32 bajtów zapisanych w postaci par bajtów (od 10 do 64 znaków), który stanowi unikalny identyfikator jednostki SNMP. Sugerowane sposoby konstrukcji tego numeru, zapobiegające powtórzeniom są opisane w normie RFC 3411.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	28/147	
------	------	-----------------------------------	------------	--------	--



W sekcji **SNMP Trap Configuration** możliwe jest skonfigurowanie komunikatów Trap, wysyłanych przez urządzenie. Podstawowe parametry to: wersja protokołu, nazwa społeczności, docelowy adres IPv4 oraz IPv6 (opcjonalnie). Dostępne są także dodatkowe opcje:

- **Trap Authentication Failure** umożliwia włączenie lub wyłączenie wysyłania wiadomości Trap przy próbie nieautoryzowanego dostępu do urządzenia przez SNMP.
- **Trap Inform Mode** jeśli włączone, to **HYPERION** będzie oczekiwać zwrotnego pakietu typu Inform, potwierdzającego odebranie komunikatu Trap. Ten tryb nie jest dostępny w SNMPv1.
- **Trap Inform Timeout i Retry Times –** określa czas w sekundach oczekiwania na potwierdzenie Trap-a (od 0 do 2147) oraz ilość powtórzeń w przypadku nieotrzymania potwierdzenia (od 0 do 255).
- Trap Probe Security Engine ID i Security Engine ID określają sposób uzyskiwania numeru Engine ID, potrzebnego do wysyłania komunikatów Trap i Inform. Jeśli ustawienie Probe Security Engine ID jest włączone, to agent SNMP spróbuje określić tę wartość automatycznie, a jeśli wyłączone – zostanie użyta wartość wprowadzona ręcznie w polu Security Engine ID.
- **Trap Security Name** określa nazwę użytkownika, która będzie używana przy wysyłaniu komunikatów Trap oraz Inform w wersji SNMPv3.

5.12.1 Konfiguracja SNMPv3

HYPERION posiada pełną obsługę SNMPv3 wraz z bezpiecznym uwierzytelnianiem oraz szyfrowaniem transmisji (szyfrowanie DES).

5.12.1.1 Społeczności

W trybie SNMPv3 są także dostępne wersje 1 i 2c, ale ich obsługa i konfiguracja nieco się zmienia. Na stronie konfiguracji społeczności można zdefiniować nazwy społeczności, które będą dostępne dla protokołów SNMPv1 i SNMPv2c.

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
	public	0.0.0.0	0.0.0.0
	private	0.0.0.0	0.0.0.0
Add New	Entry Save	e Reset	

Rys. 31. Konfiguracja społeczności w trybie SNMPv3.

Dodatkowo do każdej społeczności można określić zakres adresów IP, z których będzie możliwy dostęp do niej, co zwiększa bezpieczeństwo. Znaczenie maski jest podobne, jak w sieciach IP: bity ustawione na 1 określają niezmienną część adresu IP, a bity ustawione na 0 – część zmienną. Dla przykładu: jeśli **Source IP** zostanie ustawione na 192.168.0.0, a **Source Mask** na 255.255.255.0, to do danej społeczności będzie można uzyskać dostęp tylko z adresów od 192.168.0.0 do 192.168.0.255. Natomiast przy **Source IP** ustawionym na 192.168.0.45 i **Source Mask**: 255.255.255.254 dostęp będzie możliwy tylko z dwóch adresów: 192.168.0.44 i 192.168.0.45. Ustawienie adresu oraz maski na 0.0.0.0 umożliwia dostęp z dowolnego adresu IP.

W trybie SNMPv3 uprawnienia oraz wersje protokołu dla zdefiniowanych tutaj społeczności określa się w podmenu **Groups**.

Aby uniemożliwić całkowicie dostęp przez SNMPv1 oraz v2 należy usunąć wszystkie społeczności z tej listy. Usuwanie społeczności odbywa się przez zaznaczenie pola **Delete** w wybranym wierszu, a następnie kliknięcie przycisku **Save**.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	29/147	
------	------	-----------------------------------	------------	--------	--



5.12.1.2 Użytkownicy

Konfiguracja użytkowników znajduje się w podmenu Users.

SNMPv3 User Configuration

Delete	Engine ID User Name		Level	Security Authentication Authentication Level Protocol Password		Protocol	Privacy Password
80	00007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete			Auth, Priv 🔹	MD5 🔻		DES V	

Add New Entry Save Reset

Rys. 32. Konfiguracja użytkowników w trybie SNMPv3.

Użytkownicy są podstawowym elementem dostępu do zarządzania przez SNMPv3 (tzw. model USM – User Security Model). Aby ramka SNMPv3 z systemu zarządzania została obsłużona przez urządzenie, musi ona zawierać nazwę użytkownika i w zależności od ustawionego poziomu ochrony, hasło dostępu, które są wcześniej zdefiniowane na liście użytkowników. Poszczególne pola w każdym wierszu mają następujące znaczenia:

Engine ID – określa numer silnika SNMPv3. W podstawowej konfiguracji liczba ta powinna być dla wszystkich użytkowników taka sama, jak odpowiadająca jej liczba w podmenu System, opisana wcześniej.

User Name – nazwa użytkownika – ciąg 1 do 32 znaków; dozwolone są małe i wielkie litery, cyfry oraz większość znaków możliwych do wprowadzenia z klawiatury (zakres ASCII od 33 do 126).

Security Level – poziom bezpieczeństwa konta. Możliwe wartości to: NoAuth, NoPriv – bez autoryzacji i bez szyfrowania – do akceptacji ramki wystarczy nazwa użytkownika, dane są przesyłane otwartym tekstem; Auth, NoPriv – konieczna jest nazwa użytkownika oraz hasło zaszyfrowane jedną z metod MD5 lub SHA; Auth, Priv – jak w Auth, NoPriv, ale dodatkowo dane przesyłane podczas transmisji są szyfrowane algorytmem DES. Ostatnia opcja zapewnia najwyższe bezpieczeństwo transmisji.

Authentication Protocol – protokół używany do szyfrowania hasła, jeśli opcja autoryzacji jest włączona; dostępne wartości to MD5 oraz SHA.

Authentication Password – hasło dostępu, jeśli opcja autoryzacji jest włączona; hasło musi składać się z 8 do 32 znaków.

Privacy Protocol – protokół używany do szyfrowania danych, jeśli opcja szyfrowania jest włączona; aktualnie jedyną dostępną opcją jest DES.

Privacy Password – hasło używane do szyfrowania danych; hasło musi mieć od 8 do 32 znaków.

5.12.1.3 Grupy i widoki

Grupy w SNMPv3 określają i organizują prawa dostępu poszczególnych użytkowników. Konfiguracja grup odbywa się na podstronie **Access.** Można tutaj przypisać prawa poszczególnym grupom.

SNMPv3 Access Configuration

[Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
		default_ro_group	any	NoAuth, NoPriv	default_view ▼	None •
		default_rw_group	any	NoAuth, NoPriv	default_view 🔻	default_view v

Add New Entry Save Reset

Rys. 33. Konfiguracja grup Dostępu w SNMPv3.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	30/147
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	30/1



Każdy wiersz tabeli opisuje jedną grupę dostępu. Dla każdej takiej grupy określone są następujące parametry:

Security Model – opisuje, jakie modele bezpieczeństwa są wspierane przez tę grupę. Można wybrać jeden z modeli: v1, v2c, usm, a także wszystkie (any).

Security Level – określa minimalny poziom bezpieczeństwa wymagany przez tę grupę. Jeśli do danej grupy zostanie przypisany użytkownik lub nazwa społeczności o niższym poziomie bezpieczeństwa, to wymagania grupy będą ważniejsze. Jeśli model bezpieczeństwa takiego użytkownika nie obsługuje poziomu bezpieczeństwa wymaganego przez grupę (np. użytkownik jest nazwą społeczności SNMPv1, a grupa wymaga zabezpieczeń Auth, Priv), to komunikacja przy użyciu tego użytkownika może w ogóle nie być możliwa.

Read/Write View Name – widoki drzewa OID dostępne dla danej grupy odpowiednio przy rozkazach odczytu oraz zapisu.

Widoki możliwe do wybrania przy konfiguracji grup można zdefiniować na podstronie Views,

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
	default_view	included 🔻	.1
Delete		excluded •	
Add New	Entry Save	Reset	

Rys. 34. Konfiguracja widoków SNMPv3

Widoki są to wybrane gałęzie drzewa OID SNMP, które mogą być dostępne do zapisu lub odczytu. Każdy widok może ograniczać dostęp do kilku określonych gałęzi oraz wykluczać niektóre podgałęzie z dostępu. Aby nadać określony status więcej niż jednej gałęzi, należy dodać kilka wierszy posiadających tę samą nazwę widoku. Na przykład, aby ograniczyć widok do standardowej podgałęzi MIB-2 w gałęzi ISO, należy zdefiniować jeden wiersz widoku z polem **View Type** ustawionym na **included**, a w pole **OID Subtree** wpisać **.1.3.6.1.2.1** (jest to numer OID gałęzi mib-2). Następnie aby wykluczyć z tego widoku podgałąź Interfaces należy dodać wiersz z taką samą nazwą widoku, o typie **excluded** i z numerem **.1.3.6.1.2.1**.2 w polu **OID Subtree**. Zawsze kiedy w widoku występuje wiersz typu **excluded**, ten sam widok powinien także zawierać wiersz typu **included** opisujący gałąź obejmującą tę pierwszą.

5.12.1.4 Przypisania użytkowników do grup

Przypisania użytkowników do grup dokonuje się na podstronie Groups.

Delete	Security Model	Security Name	Group Name
	v1	public	default_ro_group
	v1	private	default_rw_group
	v2c	public	default_ro_group
	v2c	private	default_rw_group
	usm	default_user	default_rw_group

SNMPv3 Group Configuration

Add New Entry Save Reset

Rys. 35. Konfiguracja grup w SNMPv3.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	31/147
------	------	-----------------------------------	------------	--------



Każdy wiersz tabeli jest przypisaniem użytkownika do określonej grupy dostępu. Użytkownik może tu być zarówno użytkownikiem w rozumieniu modelu SNMPv3, jak też społecznością w modelu SNMPv1 i v2c. Oba te znaczenia mają tutaj wspólną nazwę: **Security Name**. Kolumna **Group Name** – jest nazwą grupy, do której jest przypisany użytkownik, a **Security Model** określa typ użytkownika: v1 oraz v2c oznaczają, że nazwa w danym wierszu jest nazwą społeczności w modelu odpowiednio SNMPv1 lub v2c (taka też wersja protokołu będzie obsługiwana za pomocą tej nazwy) – musi być to jedna z nazw określonych w **panelu Communities**, opisanego wcześniej; **usm** natomiast oznacza, że nazwa jest nazwą użytkownika (jedną z tych zdefiniowanych w panelu **Users**) i przez tę nazwę można uzyskać dostęp za pomocą protokołu SNMPv3.

5.12.2 RMON Remote Network Monitoring

RMON jest dodatkiem do SNMP, definiującym gałęzie w drzewie MIB-2 służące do bardziej (niż pozwala podstawowa gałąź MIB-2) szczegółowego monitorowania ruchu w najbliższej sieci. Domyślnie funkcje RMON są wyłączone. W celu skorzystania z nich konieczne jest uprzednie skonfigurowanie tego interfejsu. Podstawowa konfiguracja polega na określeniu listy portów w urządzeniu, dla których mają być gromadzone statystyki. Można tego dokonać w menu **Configuration > Security > Switch > RMON > Statistics**.

RMON S	tatistics Co	onfiguration	
Delete	ID	Data Source	
Delete	1	.1.3.6.1.2.1.2.2.1.1.	0
Add New	Entry Sa	ave Reset	

Rys. 36. Konfiguracja statystyk RMON.

W panelu pokazanym na rysunku powyżej definiuje się indeksy portów, które mają być monitorowane (jeden wiersz na port). Indeksy te to numery gałęzi portów w drzewie OID interfaces (podgrupa MIB-2) liczone od 1. W **HYPERION** dostępne numery portów zawierają się w przedziale od 1 do 32. Przy dodawaniu portu należy także podać numer **ID** wiersza – może być to dowolna liczba od 1 do 65535. Po zdefiniowaniu żądanych portów można monitorować ich parametry w panelu monitorowania RMON, do którego dostęp jest przez menu **Monitor > Security > Switch > RMON**.

R	RMON Statistics Status Overview Auto-refresh 🗏 Refresh 🔍 >>																		
St	Start from Control Index 0 with 20 entries per page.																		
I	D	Data Source (ifIndex)	Drop	Octets	Pkts	Broad- cast	Multi- cast	CRC Errors	Under- size	Over- size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
	1	1	0	540599	3430	184	2623	0	0	0	0	0	0	438	2622	109	160	32	69

Rys. 37. Monitorowanie statystyk portów RMON

W tym widoku statystyki wszystkich monitorowanych portów wyświetlone są w formie tabeli – każdy port w osobnym wierszu. W tabeli podane są następujące informacje:

ID – numer wiersza ustawiony ręcznie w konfiguracji statystyk RMON.

Data Source (ifIndex) – indeks portu (gałęzi w drzewie interfaces), dla którego wyświetlone są statystyki w wierszu.

Drop – całkowita ilość pakietów odrzuconych ze względu na niedobór zasobów.

Octets - ilość odebranych bajtów (także w uszkodzonych pakietach).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	32/147



Pkts – ilość odebranych pakietów (razem z pakietami uszkodzonymi, broadcastowymi i multikastowymi).

Broadcast – ilość odebranych dobrych pakietów broadkastowych.

Multicast – ilość odebranych dobrych pakietów multikastowych.

CRC Errors – ilość odebranych pakietów z błędami CRC.

Undersize – ilość odebranych pakietów o długości mniejszej niż 64 bajty.

Oversize – ilość odebranych pakietów o długości większej niż 1518 bajtów.

Frag. – ilość odebranych ramek o długości mniejszej niż 64 bajty, posiadających błędne CRC.

Jabb. – ilość odebranych ramek o długości większej niż 64 bajty, posiadających błędne CRC.

Coll. – szacunkowa całkowita liczba kolizji na porcie.

64 Bytes – całkowita ilość odebranych pakietów (wliczając uszkodzone), o długości 64 bajtów.

65 ~ 127 – całkowita ilość odebranych pakietów (wliczając uszkodzone) o długościach od 65 do 127 bajtów.

128 ~ 255 – całkowita ilość odebranych pakietów (wliczając uszkodzone) o długościach od 128 do 255 bajtów.

256 ~ 511 – całkowita ilość odebranych pakietów (wliczając uszkodzone) o długościach od 256 do 511 bajtów.

512 ~ 1023 – całkowita ilość odebranych pakietów (wliczając uszkodzone) o długościach od 512 do 1023 bajtów.

1024 ~ 1588 – całkowita ilość odebranych pakietów (wliczając uszkodzone) o długościach od 1024 do 1588 bajtów.

Po kliknięciu numeru ID któregoś z wierszy wyświetlają się statystyki tego jednego portu w formie bardziej przejrzystej tabeli.

5.12.2.1 Rejestracja historii

Wybierając menu **Configuration > Security > Switch > RMON > History** uzyskuje się dostęp do konfiguracji historii RMON. Jest to funkcja pozwalająca na zapis regularnie co określony czas danych statystycznych w celu śledzenia ich zmian w czasie. Gromadzona jest większość danych dostępnych w funkcji Statistics (z wyjątkiem danych o ilości pakietów w przedziałach długości 64 bajty, 65-127 bajtów, itd.), oraz dodatkowo chwilowe wykorzystanie pasma na porcie.

RMON History Configuration										
Delete	ID Data Source		Interval	Buckets	Buckets Granted					
	1	.1.3.6.1.2.1.2.2.1.1.	1	10	50	50				
	2	.1.3.6.1.2.1.2.2.1.1.	2	10	50	50				
Add new entry Save Reset										

Rys. 3	8. Kon	figuracja	historii	RMON
--------	--------	-----------	----------	------

Na powyżej przedstawiona jest tabela konfiguracji historii RMON. Każdy wiersz opisuje jeden port, który będzie monitorowany. Poszczególne pola są następujące:

ID – numer identyfikacyjny wiersza, nadany przez użytkownika.

Data Source - numery gałęzi portu w drzewie OID interfaces (podgrupa MIB-2), liczony od 1, dla którego będzie gromadzona historia.

Interval – określa odstęp w sekundach pomiędzy zapisami historii, wartości od 1 do 3600.

Buckets – oznacza ilość wpisów historii, które mają być dostępne dla danego portu. Kiedy dane historii osiągną tę liczbę, najstarsze dane są usuwane aby zrobić miejsce dla nowszych. Maksymalna ilość wpisów to 3600.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	33/147	
------	------	-----------------------------------	------------	--------	--



Buckets Granted – jest to informacja o aktualnie przydzielonym miejscu na wpisy historii. Może być ona mniejsza od żądanej, jeśli w systemie nie ma wystarczającej ilości wolnego miejsca na dane. Wartości: od 1 do 50.

Zarejestrowaną historię można przeglądać wybierając menu **Monitor > Security > Switch > RMON** > **History**. Panel ten jest pokazany poniżej:

RMON Hi	MON History Overview Auto-refresh 🗌 Refresh 🤃 >>													
Start from C	Control Index	0	and Samp	ole Index 0	١	with 20	entries pe	er page.						
History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad- cast	Multi- cast	CRC Errors	Under- size	Over- size	Frag.	Jabb.	Coll.	Utilization
1	1234	20963	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1235	20968	30	246	2	0	2	0	0	0	0	0	0	0
1	1236	20973	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1237	20978	30	492	4	0	4	0	0	0	0	0	0	0
1	1238	20983	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1239	20988	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1240	20993	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1241	20998	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1242	21003	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1243	21008	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1244	21013	5 0	/83	11	0	11	0	0	0	0	0	0	0
1	1245	21018	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1246	21023	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1247	21028	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1248	21033	5 0	246	2	0	2	0	0	0	0	0	0	0
1	1249	21038	3 0	369	3	0	3	0	0	0	0	0	0	0
1	1250	21043	3 O	369	3	0	3	0	0	0	0	0	0	0
1	1251	21048	3 0	246	2	0	2	0	0	0	0	0	0	0
1	1252	21053	3 0	369	3	0	3	0	0	0	0	0	0	0
<u>1</u>	1253	21058	3 0	246	2	0	2	0	0	0	0	0	0	0

Rys. 39. Monitorowanie historii RMON

Pierwsza kolumna tej tabeli zawiera indeks grupy nadany przez użytkownika (**History Index**). W drugiej kolumnie (**Sample Index**) znajduje się kolejny numer próbki. Trzecia zaś kolumna (**Sample Start**) to znacznik czasu – ilość sekund od ostatniego uruchomienia urządzenia, przy której została zapisana dana próbka. Kolejne kolumny zawierają dane o wielkości ruchu, ale nie bezwzględne (jak w statystykach RMON), natomiast względne – przyrost od poprzedniego odczytu. Ostatnia kolumna (**Utilization**) zawiera szacunkową średnią zajętość pasma na porcie w ciągu ostatniego interwału próbkowania w setnych częściach procenta (wartość 100 oznacza 1%). Możliwe jest przeglądanie tej tablicy przy użyciu kontrolek znajdujących się nad nią:

- Start from Control Index indeks historii, od którego powinna rozpoczynać się tabela.
- Sample Index indeks próbki, od którego powinna rozpoczynać się tabela.
- Entries per page maksymalna ilość wyświetlanych jednocześnie wierszy.

Po zdefiniowaniu tych kryteriów należy kliknąć przycisk **Refresh**. Tabelę można też łatwo przeglądać za pomocą przycisków << i >>. Zaznaczenie pola **Auto-refresh** powoduje skasowanie wprowadzonych ustawień wyświetlania.

5.12.2.2 Alarmy i zdarzenia

W ramach **RMON HYPERION** posiada możliwość definiowania kryteriów alarmowych, generowania zdarzeń oraz akcji podejmowanych po ich wystąpieniu. Kryteria alarmowe są definiowane w menu **Configuration** \rightarrow **Security** \rightarrow **Switch** \rightarrow **RMON** \rightarrow **Alarm**.

RMON A	larm	Configurat	ion													
Delete	ID	Interval			Variat	ble		Sample Type	Value	Startup Alarm		Rising Threshold	Rising Index	Falling Thresho	ld	Falling Index
	1		0.1	1.3.6.1.2.	1.2.2.1.	10	0.1	Absolute 👻	178691	Rising	•	410000	78		1	1
Add new	Add new entry Save Reset Rys. 40. Konfiguracja alarmów RMON															
REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI							202	24.01.0	04	34	/147					



Skonfigurowane alarmy są zaprezentowane w postaci tabeli. W celu dodania nowego alarmu należy kliknąć **Add new entry**, co spowoduje dodanie kolejnego wiersza do tabeli, a następnie wypełnić nowy wiersz odpowiednimi wartościami i kliknąć **Save**.

Wartości w tabeli są następujące:

- **ID** numer wpisu definiowany przez użytkownika.
- Interval odstęp czasu w sekundach pomiędzy sprawdzeniami monitorowanego licznika.
- Variable podgałąź drzewa interfaces grupy MIB-2 w SNMP, która ma być monitorowana. Można monitorować tylko liczniki o numerach OID od 10 (InOctets) do 21 (OutQLen). W to pole należy wpisać numer monitorowanego licznika z grupy interfaces, a po kropce numer gałęzi interfejsu, na którym będzie monitorowany ten licznik.
- Sample Type określa typ próbkowania. Możliwe wartości: Absolute do porównywania będzie brana wartość bezwzględna danego licznika, Delta – do porównywania będzie brana różnica wartości licznika od ostatniego próbkowania.
- Value informacja o zarejestrowanej wartości przy ostatniej próbce.
- Startup Alarm określa typ zdarzenia, od którego powinna się rozpocząć rejestracja zdarzeń dla tego licznika: Rising oznacza, że rejestracja rozpocznie się dopiero po przekroczeniu wartości górnego progu alarmowego (wcześniejsze opadnięcie wartości poniżej dolnego progu nie będzie wyzwalało alarmu), Falling rejestracja rozpocznie się dopiero po opadnięciu wartości poniżej dolnego progu alarmowego (wcześniejsze przekroczenie górnego progu alarmowego nie będzie wyzwalało alarmu), RisingOrFalling rejestracja i generowanie alarmów rozpocznie się od przekroczenia przez wartość górnego progu lub opadnięcia wartości poniżej dolnego progu (w zależności co pierwsze wystąpi).
- Rising/Falling Threshold określają odpowiednio górny i dolny próg dla licznika. Jeśli wartość licznika przekroczy górny lub dolny próg, generowany jest alarm RMON. Alarm można ustawić w zdarzeniach RMON – podmenu Events.
- Rising/Falling Index numery zdarzeń (zdefiniowanych w panelu Events), które będą wyzwolone przy odpowiednio przekroczeniu górnego progu oraz opadnięciu poniżej dolnego progu. Alarm od któregoś z progów można wyłączyć przez ustawienie nieistniejącego numeru zdarzenia.

W grupie menu **Monitor** możliwe jest przeglądanie ustawionych tutaj alarmów, ale nie ma tam żadnych dodatkowych informacji.

Jak podano wyżej, w tabeli tej należy określić numery zdarzeń, które będą wywoływanie przy poszczególnych progach. Zdarzenia te definiuje się w panelu **Event**, do którego dostęp jest możliwy po wybraniu podmenu **Event** w grupie **Configuration**.

RMON Event Configuraton								
Delete	ID	Desc		Туре		Community	Event Last Time	
	1	inne	log	•		public	15105	
	78	zdarzenie	log	-		public	15103	
•								

Add new entry Save Reset

Rys. 41. Konfiguracja zdarzeń RMON.

Parametry, opisujące poszczególne zdarzenia są następujące:

ID – unikalny numer zdarzenia określany przez użytkownika (do tego numeru odwołuje się panel alarmów).

Desc – opis zdarzenia ustalany dowolnie przez użytkownika. Znaki polskie i inne narodowe zostaną zamienione na kody HTML.

Type – typ zdarzenia – opisuje działania podejmowane przy wystąpieniu danego zdarzenia. Dostępne opcje to: **none** – brak działań, **log** – zapis informacji w dzienniku zdarzeń RMON (nie jest to dziennik systemowy), **snmptrap** – wysłanie komunikatu **Trap** przez SNMP, **logandtrap** – zapis do dziennika oraz wysłanie Trap.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	35/147



Community – społeczność SNMP, do której ma być wysłany komunikat Trap.

Event Last Time – wyświetla ostatni czas działania systemu (w sekundach) od ostatniego uruchomienia, przy którym wystąpiło ostatnie zdarzenie tego typu.

Poniżej pokazany jest panel monitorowania zdarzeń RMON, który wyświetla się po przejściu do podmenu **Event** w grupie **Configuration**.

RMON	Event Over	view	Auto-refresh 🗌 Refresh << >>
Start from	Control Index	0 and	Sample Index 0 with 20 entries per page.
Event Index	LogIndex	LogTime	LogDescription
1	1	6	Falling:iso.3.6.1.2.1.2.2.1.10.2=246 <= 2000000 :1.1

Rys. 42. Monitorowanie zdarzeń RMON.

W tym panelu widoczne są zdarzenia wywołane przez RMON, które zostały wcześniej skonfigurowane w panelu opisanym wyżej. Każde zdarzenie posiada następujące informacje:

Event Index – jest to indeks typu zdarzenia, ustawiony przez użytkownika w panelu konfiguracyjnym.

LogIndex – jest to kolejny numer wpisu w dzienniku RMON dla danego typu zdarzenia.

LogTime – podaje czas wystąpienia danego zdarzenia – w sekundach od ostatniego uruchomienia urządzenia.

LogDescription – tekstowy opis przyczyny wystąpienia zdarzenia.

Dziennik RMON jest kasowany przy każdym uruchomieniu HYPERION.

Przeglądanie dziennika możliwe jest przy użyciu kontrolek nad tabelą. Można użyć przycisków >> oraz << do przeglądania zawartości, lub określić indeks zdarzenia i indeks wpisu, od których ma się zaczynać tabela, oraz maksymalną ilość elementów na stronie. Aby zatwierdzić ustawienia należy kliknąć przycisk **Refresh**. Zaznaczenie pola **Auto-refresh** powoduje skasowanie ręcznie wprowadzonych parametrów.

5.13 Port Security Limit Control Configuration

Funkcja Limit Control dostępna w menu **Configuration** → **Security** → **Network** → **Limit Control,** pozwala na ograniczenie liczby użytkowników na danym porcie. Użytkownik jest identyfikowany przez adres MAC i identyfikator VLAN. Jeśli kontrola limitu na porcie jest włączona, limit określa maksymalną liczbę użytkowników na tym porcie. Jeśli ta liczba zostanie przekroczona, podejmowane jest działanie. Akcja może być jedną z czterech różnych akcji opisanych poniżej. Moduł Limit Control wykorzystuje moduł Port Security, który zarządza adresami MAC poznanymi na porcie.

5.13.1 System Configuration

Mode – Włączenie/wyłącznie globalnie kontroli limitów na switchu.

Aging Enabled – Jeśli ta opcja jest zaznaczona adresy Mac podlegają przedawnieniu zgodnie z okresem starzenia

Aging Period- jeśli opcja starzenia jest włączona, okres starzenia nastawiamy w tym polu.

Port Security Limit Control Configuration

System Configuration

Mode	Disabled	~
Aging Enabled		
Aging Period	3600	seconds

Rys. 43. Konfiguracja systemowa Limit Control.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	36/147
------	------	-----------------------------------	------------	--------


5.13.2 Port Configuration

Port Configuration

Interface	Mode	Limit	Ac	tion	State	Re-open
*	 • 	4	\diamond	~		
10GigabitEthernet 1/1	Disabled V	4	None	~	Disabled	Reopen
10GigabitEthernet 1/2	Disabled ~	4	None	~	Disabled	Reopen
10GigabitEthernet 1/3	Enabled V	4	None	~	Disabled	Reopen
10GigabitEthernet 1/4	Disabled ~	4	None		Disabled	Reopen
GigabitEthernet 1/1	Disabled ~	4	Shutdown		Disabled	Reopen
GigabitEthernet 1/2	Disabled •	4	Trap & Shutdov	vn	Disabled	Reopen
GigabitEthernet 1/3	Disabled V	4	None	~	Disabled	Reopen
GigabitEthernet 1/4	Disabled V	4	None	~	Disabled	Reopen
GigabitEthernet 1/5	Disabled V	4	None	\sim	Disabled	Reopen

Rys. 44. Konfiguracja portów limit Control.

Interface – Numer portu na którym bedzię konfiguracja

Mode - Określa, czy kontrola limitu jest włączona na tym porcie.

Action - Po osiągnięciu limitu przełącznik może wykonać jedną z opcji:

- **None**: Nie zezwolić na więcej niż jest ustawione to w Limit MAC dla tego portu i nie podejmuj dalszych działań.
- Trap: Jeśli na porcie właczony jest limit adresów MAC wyślij SNMP trap.
- Shutdown: jeśli limit +1 Mac adres jest przekroczony na porcie to zamknij port.
- **Trap & Shutdown**: jeśli limit +1 Mac adres jest przekroczony na porcie, zostanie wysłany SNMP trap i zamkniecie portu.

State - Ta kolumna pokazuje aktualny stan portu widziany z punktu widzenia Kontroli Limitów. Stan przyjmuje jedną z czterech wartości:

- **Disabled**: Kontrola limitów jest globalnie wyłączona lub wyłączona na porcie.
- Ready: Limit nie został jeszcze osiągnięty.
- Limit Reached: Zmiana limitu na danym porcie
- **Shutdown**: wskazuje że port został zamknięty przez kontrolę limitu.

Re-open Button - Jeśli port jest wyłączany przez ten moduł, możesz go ponownie włączyć, klikając ten przycisk, który zostanie podświetlony tylko w takim przypadku. Aby poznać inne metody, zapoznaj się z sekcją Wyłączanie w sekcji "Action".

Pamiętaj, że kliknięcie przycisku ponownego otwarcia powoduje odświeżenie strony, więc niezatwierdzone zmiany zostaną utracone.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	37/147
------	------	-----------------------------------	------------	--------



5.14 Network Access Server

Standard IEEE 802.1X definiuje procedurę kontroli dostępu opartą na portach, która zapobiega nieautoryzowanemu dostępowi do sieci, wymagając od użytkowników podania poświadczeń w celu uwierzytelnienia.

System Configuration		
Mode	Disabled	~
MAC letter size	Small	~
MAC divider	Space	~
Reauthentication Enabled		
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled		
RADIUS-Assigned VLAN Enabled		
Guest VLAN Enabled		
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen		

Rys. 45.Konfiguracja systemu NAS.

5.14.1 System Configuration

Mode – włącznie/wyłączenie globalnie serwera NAS.

Reauthentication Enabled – Jeśli jest zaznaczone,pomyślnie uwierzytelniani subkilenci/klienci są ponownie uwierzytelniani po określonym czasie.

Reauthentication Period - Określa po ilu sekundach ponownie klient ma być uwierzytelniony.

EAPOL Timeout - Określa po jakim czasie ma nastąpić retransmisja ramek EAPOL

Aging Period – Ustawienie następujących trybów wykorzystujących funkcję Port Security adresu MAC:

- Single 802.1X
- Multi 802.1X

• MAC-Based Auth.

Hold Time - Ustawienie następujących trybów wykorzystujących funkcję Port Security adresu MAC:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

RADIUS-Assigned QoS Enabled – The "RADIUS-Assigned QoS Enabled" checkbox zapewnia szybki sposób na globalne włączenie funkcji QoS do serwera Radius

RADIUS-Assigned VLAN Enabled- RADIUS-assigned VLAN zapewnia kontrole sieci VLAN w przełączniku, w której uwierzytelniony jest klient.

Guest VLAN Enabled – Goście VLAN maja specjalny VLAN – najczęściej z ograniczonym dostępem do sieci..

Guest VLAN ID - Wartość Vlanu dla Gościa , gdy ten zostanie przeniesiony

Max. Reauth. Count – To ustawienie reguluje liczbę przypadków, w których przełącznik przesyła ramkę EAPOL Request Identity bez odpowiedzi przed rozważeniem wejścia do gościnnej sieci VLAN.

Allow Guest VLAN if EAPOL Seen - Przełącznik pamięta, czy ramka EAPOL została odebrana na porcie przez cały okres eksploatacji portu.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	38/147
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	38/147



Port Configuration

Interface	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State		Restart
*	<> v						
10GigabitEthernet 1/1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
10GigabitEthernet 1/2	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
10GigabitEthernet 1/3	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
10GigabitEthernet 1/4	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/2	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/3	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/4	Force Authorized V				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/5	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/6	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/7	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/8	Force Authorized V				Globally Disabled	Reauthenticate	Reinitialize
GigabitEthernet 1/9	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize

Rys. 46.Konfiguracja portów w NAS

5.14.2 Port Configuration

Port – Numer portu którego dotyczy konfiguracja **Admin State** :

- **Force Authorized** W tym trybie przełącznik wyśle jedną ramkę EAPOL Success, gdy pojawi się łącze portu, a każdy klient na porcie uzyska dostęp do sieci bez uwierzytelniania.
- Force Unauthorized W tym trybie przełącznik wyśle jedną ramkę błędu EAPOL, gdy zostanie nawiązane łącze do portu, a dostęp do sieci nie będzie możliwy dla każdego klienta na porcie.
- **Port-based 802.1X –** Radius serwerem uwierzytelniającym.
- **Single 802.1X** W przypadku uwierzytelniania 802.1X opartego na portach po pomyślnym uwierzytelnieniu klienta cały port jest otwierany dla ruchu sieciowego
- Multi 802.1X Podobny do Šingle 802.1X- nie jest standardem IEEE ale wariantem posiadającym wiele cech podobnych. W Multi 802.1X jeden lub więcej suplikantów może zostać uwierzytelnionych na tym samym porcie w tym samym czasie. Każdy suplikant jest indywidualnie uwierzytelniany i zabezpieczany w tablicy MAC za pomocą modułu Port Security.

RADIUS-Assigned QoS Enabled – Gdy funkcja RADIUS-Assigned QoS jest globalnie włączona lub włączona za pomocą checkboxa na danym porcie, przełącznik reaguje na informacje o klasie Qos od Serwera RADIUS.

RADIUS-Assigned VLAN Enabled- Gdy sieć VLAN przypisana do usługi RADIUS jest globalnie włączona, lub włączona dla danego portu, przełącznik reaguje na informacje VLAN ID zawarte w pakiecie Access-Accept usługi serwera RADIUS.

Guest VLAN Enabled - Gdy sieć VLAN gościa jest globalnie włączona, jak i włączona dla danego portu, przełącznik rozważa przeniesienie portu do sieci VLAN gościa.

Port State:

- Globally Disabled: NAS jest globalnie wyłączony.
- Link Down: NAS jest globalnie włączony ale nie ma linku na porcie.
- Authorized: Port w trybie Force Authorized lub single-supplicant i klient jest uwierzytelniany.
- Unauthorized: Port w trybie Force Unauthorized lub single-supplicant i klient nie jest uwierzytelniony w serwerze RADIUS
- X Auth/Y Unauth: Port znajduje się w trybie multi-supplicant. Obecnie X klientów jest autoryzowanych, a Y nieautoryzowanych.

Restart – Przyciski aktywne, gdy uwierzytelnianie włączone a port jest w trybie EAPOL lub MAC. Przyciski odpowiadają za:

- Reauthenticate: Planuje ponowne uwierzytelnienie, gdy skończy się okres ciszy w porcie
- Reinitialize: Wymusza ponowną inicjalizację klientów na porcie, a tym samym natychmiastowe ponowne uwierzytelnienie.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	39/147
---	------------	--------



5.15 Access Control List

5.15.1 ACL Ports Configuration

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	< ♥	◇ ▼	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 ▼	< v	◇ ∨	◇ ∨	◇ ∨	*
10GigabitEthernet 1/1	0	Permit ¥	Disabled 🗸	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 -	Disabled ¥	Disabled 🗸	Disabled ¥	Enabled ¥	0
10GigabitEthernet 1/2	0	Permit 🗸	Disabled 🗸	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 -	Disabled V	Disabled ¥	Disabled ¥	Enabled ¥	0
10GigabitEthernet 1/3	0	Permit 🗸	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled 🗸	Enabled ¥	0
10GigabitEthernet 1/4	0	Permit 🗸	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 ▼	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	13670
GigabitEthernet 1/1	0	Permit V	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/2	0	Permit 🗸	Disabled 🗸	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled V	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/3	0	Permit V	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/4	0	Permit 🗸	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/5	0	Permit ¥	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/6	0	Permit 🗸	Disabled V	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/7	0	Permit V	Disabled ¥	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 •	Disabled ¥	Disabled ¥	Disabled ¥	Enabled ¥	0
GigabitEthernet 1/8	0	Permit 🗸	Disabled 🗸	Disabled 10GigabitEthernet 1/1 10GigabitEthernet 1/2 v	Disabled ¥	Disabled V	Disabled ¥	Enabled ¥	0

Rys. 47.Konfiguracja portów ACL

Port — port logiczny dla ustawień zawartych w tym samym wierszu.

Policy ID — wybierz numer polityki, którą chcesz zastosować do tego portu. Dozwolone wartości to od 0 do 255. Wartość domyślna to 0.

Action — wybierz, czy przekazywanie jest dozwolone ("Zezwól"), czy odrzucone ("Odmów"). Wartość domyślna to "Zezwól".

Rate limiter ID — wybierz, który ogranicznik prędkości ma być zastosowany na tym porcie. Dozwolona wartość to wyłącz lub wartości od 1 do 16. Wartość domyślna to "wyłącz".

Port Redirect — Wybierz, na który port ramki mają być przekierowywane. Dozwolone wartości to wyłączone lub określony numer portu i nie można ich ustawić, gdy akcja jest dozwolona.

Mirror — określ działanie kopii lustrzanej tego portu. Dozwolone wartości to:

• Enabled (włącz) : Ramki odebrane przez port są dublowane.

• Disabled (wyłącz).: Ramki odebrane przez port nie są dublowane.

Logging — określ działanie rejestrowania tego portu. Zauważ, że komunikat rejestrowania nie zawiera 4 bajtów CRC. Dozwolone wartości to:

• Enabled (włącz): ramki odebrane przez port są przechowywane w dzienniku systemu.

• Disabled (wyłącz): Ramki odebrane przez port nie są rejestrowane.

Shutdown — określ operację zamknięcia portu tego portu. Dozwolone wartości to:

• Enabled (włącz): Jeśli na porcie zostanie odebrana ramka, port zostanie wyłączony.

• Disabled (wyłącz)Zamknięcie portu jest wyłączone.

State — określ stan portu. Dozwolone wartości to:

• Enabled (włącz): Ponownie otwarte porty po zmianie konfiguracji portu użytkownika ACL

• Disabled:Zamknięte porty po zmianie konfiguracji portu użytkownika ACL.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	40/147



5.15.2 ACL Rate Limiter

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	10	< ▼
1	10	pps 🗸
2	10	pps 🗸
3	10	pps 🗸
4	10	pps 🗸
5	10	pps 🐱
6	10	pps 🗸
7	10	pps 🗸
8	10	pps 🗸
9	10	pps 🗸
10	10	pps 🗸
11	10	pps 🗸
12	10	pps 🗸
13	10	pps 🗸
14	10	pps 🖌
15	10	pps 🖌
16	10	pps 🗸

Rys. 48.Konfiguracja rate Limiter ACL.

Rate Limiter ID - Identyfikator ogranicznika szybkości dla ustawień zawartych w tym samym wierszu i jego zakres wynosi od 1 do 16.

Rate- Prawidłowa szybkość to 0, 10, 20, 30, ..., 5000000 w pps lub 0, 25, 50, 75, ..., 10000000 w kb/s.

Unit - Określ jednostkę. Dozwolone wartości to:

- **pps**: pakiety na sekundy
- **kbps**: kilobity na sekunde.

5.15.3 ACL Configuration

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	All	Any	Any	Permit	Disabled	Disabled	Disabled	19	⊕ ©©⊗ ⊕

Rys. 49.Konfiguracja ACL.

Ingress Port - Wskazuje port wejściowy kontroli dostępu. Możliwe wartości to:

- All: Kontrola dostępu dopasuje wszystkie porty wejściowe.
- Port:Kontrola dostępu dopasuje określony port wejściowy.
- Policy / Bitmask- Wskazuje numer zasady i maskę bitową kontroli dostępu .

Frame Type - Wskazuje typ ramki wpisu kontroli dostępu.

Action - Wskazuje akcję przekazywania przez kontrolę dostępu.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 4 ²	41/147
---	--------



Rate Limiter - Wskazuje numer ogranicznika kontroli dostępu. Dozwolony zakres wynosi od 1 do 16. **Port Redirect** - Wskazuje operację przekierowywania portów kontroli dostępu. Ramki pasujące do kontroli dostępu są przekierowywane na numer portu

Mirror - Określ działanie lustrzane tego portu. Dozwolone wartości to:

- Enabled (włącz): Ramki odbierane na porcie są dublowane.
- **Disabled (wyłącz)**: Ramki odebrane na porcie nie są dublowane.

Counter - licznik wskazuje, ile razy ACE została trafiona przez ramkę

Przyciski modyfikacji:

🕒: Inserts a new ACE before the current row.

(C): Edits the ACE row.

(1): Moves the ACE up the list.

Woves the ACE down the list.

S: Deletes the ACE.

igodold E: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Rys. 50.oznaczenia przycisków w ACL Configuration

5.15.4 ACE Configuration

ACE Configuration

Ingress Port	All 10GigabitEthernet 1/1 10GigabitEthernet 1/2 10GigabitEthernet 1/3 10GigabitEthernet 1/4	•
Policy Filter	Any	~
Frame Type	Any	~

Action	Permit 🗸
Rate Limiter	Disabled 🗸
Mirror	Disabled 🗸
Logging	Disabled ~
Shutdown	Disabled ~
Counter	0

VLAN Parameters

802.1Q Tagged	Any	~
VLAN ID Filter	Any	~
Tag Priority	Any	~

Rys. 51. ACE konfiguracja

Ingress Port- Wybierz port przychodzący, dla którego ma zastosowanie ta pozycja kontroli dostepu. **Policy Filter** - Określ numery zasad dla tej kontroli dostępu

Policy Value - Po wybraniu opcji "Specific" dla filtru polityki można wprowadzić określoną wartość polityki

Policy Bitmask - Po wybraniu opcji "Specific" dla filtru zasad można wprowadzić określoną maskę bitową.

Frame Type - wybierz typ ramki kontroli dostępu. Dozwolone opcje to: Any, Ethernet Type, ARP, IPv4, IPv6.

Action- Określ akcję do wykonania z ramką, która trafia w tą kontrolę dostępu.

Rate Limiter -Określ ogranicznik szybkości w liczbie jednostek podstawowych. Dozwolony zakres to 1 do 16

Port Redirect - Ramki, które trafiają do ACE, są przekierowywane do podanego tutaj numeru portu. Ogranicznik prędkości będzie miał wpływ na te porty..

Mirror -Określ działanie lustrzane tego portu. Dozwolone wartości to:Enabled (włącz) /Disabled (wyłącz).

Logging - Określ operację rejestrowania przez kontrolę dostępu. Dozwolone wartości to:Enabled (włącz) /Disabled (wyłącz).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	42/147
------	------	-----------------------------------	------------	--------



Shutdown - Określ operację zamykania portu przez kontrolę dostepu. Dozwolone wartości to:Enabled (włącz) /Disabled (wyłącz).

802.1Q Tagged- Określ, czy ramki mogą trafić w akcję zgodnie ze znacznikiem 802.1Q. Dozwolone wartości to:

- Any(dowolne):Dozwolona jest dowolna wartość.
- Enabled(włącz) : tylko tagowane ramki
- Disabled(wyłącz): tylko nietagowane ramki

VLAN ID Filter – Specyficzne ustawienia VLAN ID dla tej listy kontroli dostępu. Dozwolone wartości to:

- Any(dowolne): Brak specyficznych ustawień dla VLAN ID.
- **Specific**(specyficzne): Jesli chcesz wybrać specyficzne ustawienia VLAN ID dla tej listy kontroli dostępu wybierz tą opcję. Pokaże się pole do wpisania VLAN ID.

VLAN ID- Kiedy wybrana jest opcja "Specific" w VLAN ID filter, można ustawić inny numer VLAN ID. **Tag Priority** – Specyficzne ustawienia priorytetu tag dla kontroli dostępu. Ramka, która trafiła na tą listę kontroli dostępu opowiada priorytetowi tagu.

5.16 IP Source Guard

IP Source Guard Configuration

Mode Disabled V

Translate dynamic to static



Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	 v 	V
10GigabitEthernet 1/1	Disabled 🗸	Unlimited 🗸
10GigabitEthernet 1/2	Disabled 🗸	Unlimited 🗸
10GigabitEthernet 1/3	Disabled 🗸	Unlimited V
10GigabitEthernet 1/4	Disabled 🗸	Unlimited V
GigabitEthernet 1/1	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/2	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/3	Disabled 🗸	Unlimited V
GigabitEthernet 1/4	Disabled 🗸	Unlimited V
GigabitEthernet 1/5	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/6	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/7	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/8	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/9	Disabled 🗸	Unlimited 🗸
GigabitEthernet 1/10	Disabled 🗸	Unlimited 🗸

Rys. 53.Konfiguracja portów.

Mode – Enable/disable(włącz/wyłącz) Global IP Source Guard.

Port Mode - określ na jakich portach jest włączona ochrona źródła IP.

Max Dynamic Clients – Określ maksymalną liczbę klientów dynamicznych, których można nauczyć się na danym porcie. Ta wartość może wynosić 0, 1, 2 lub nieograniczona.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	43/147
------	------	-----------------------------------	------------	--------



Static IP Source Guard Table

Delete | Port | VLAN ID | IP Address | MAC address

Add New Entry
Save Reset

Rys. 54. Konfiguracja reguł Reguły Ip Source Guard

Port - port logiczny dla ustawień .
VLAN ID – Vlan Id dla ustawień.
IP Address – dozwolony źródłowy adres IP.
MAC address – dozwolony źródłowy adres MAC.

5.17 ARP Inspection

5.17.1 Port Configuration

ARP Inspection Configuration

Mode Disabled V

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	 v 	<> ▼	◇ ∨
10GigabitEthernet 1/1	Disabled 🗸	Disabled V	None 🗸
10GigabitEthernet 1/2	Disabled 🗸	Disabled 🗸	None 🗸
10GigabitEthernet 1/3	Disabled 🗸	Disabled 🗸	None 🗸
10GigabitEthernet 1/4	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/1	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/2	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/3	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/4	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/5	Disabled 🗸	Disabled V	None 🗸
GigabitEthernet 1/6	Disabled 🗸	Disabled 🗸	None 🗸
GigabitEthernet 1/7	Disabled 🗸	Disabled V	None 💙
GigabitEthernet 1/8	Disabled 🗸	Disabled V	None 🗸
GigabitEthernet 1/9	Disabled 🗸	Disabled V	None 🗸
GigabitEthernet 1/10	Disabled 🗸	Disabled 🗸	None 🗸

Rys. 55.Konfiguracja portów ARP Inspection

Mode- Enable/disable(włącz/wyłącz) globalną inspekcje ARP.

Port Mode Configuration- Określ na jakich portach inspekcja ARP ma być włączona. Dozwolone wartości to:

- Enabled: włącz działanie ARP inspekcji .
- **Disabled:** wyłącz działanie ARP inspekcji
- Enabled: włącz sprawdzanie działanie VLAN.
- **Disabled:** wyłącz sprawdzanie działanie VLAN.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	44/147
------	------	-----------------------------------	------------	--------



- None: nie rejestruj nic.
- Deny: Rejestruj odrzucone wpisy.
- Permit: Rejestruj dozwolone wpisy.
- ALL: Rejestruj wszystkie wpisy.

5.17.2 Vlan Configuration

VLAN Mode Configuration



Rys. 56.Konfiguracja Vlanów w ARP Inspection

VLAN Mode Configuration – Określ dla jakich Vlanów ARP Inspection ma być włączona. Możliwe typy wyboru::

- **None:** nie rejestruj nic.
- **Deny:** Rejestruj odrzucone wpisy.
- **Permit:** Rejestruj dozwolone wpisy.
- ALL: Rejestruj wszystkie wpisy.

5.17.3 Static ARP Inspection Table

Static ARP Inspection Table

Delete | Port | VLAN ID | MAC Address | IP Address

Add New Entry

Save Reset

Rys. 57. Konfiguracji Static ARP .

Port - port logiczny dla ustawień.

VLAN ID – Vlan Id dla ustawień.

IP Address –dozwolony źródłowy adres IP.

MAC address – dozwolony źródłowy adres MAC.

5.17.4 Dynamic ARP Inspection Table

Dynamic ARP Inspection	1 Table		
Start from 10GigabitEthernet 1	/1 🗸 , VLAN 1 , MAC address 00	-00-00-00-00-00 and IP address 0.0.0.0	with 20 entries per page.
Port VLAN ID MAC Ad	dress IP Address Translate to stat	ic	
	No more entries		

Rys. 58.Konfiguracja Dynamic ARP Inspection Table

Port - Numer portu, dla którego wyświetlane są wpisy. **VLAN ID**- VLAN-ID, w którym dozwolony jest ruch ARP. **MAC Address** –Adres MAC użytkownika wpisu..

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	45/147
------	------	-----------------------------------	------------	--------



IP Address – Adres IP użytkownika wpisu.. Translate to static – Wybierz ten checkbox by translatować dynamiczny dostęp na statyczny.

5.18 Authentication, Authorization and Accounting

5.18.1 RADIUS SERVER

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key

Rys. 59. Konfiguracja servera Radius

5.18.1.1 Global Configuration

Timeout – Liczba sekund oczekiwania na odpowiedź od RADIUS przed ponownym zapytaniem.

Retransmit – Liczba ilości razy wysyłanych zapytań do servera radius gdy ten nie opowiada.

Deadtime- Okres czasu w którym switch nie będzie wysyłał nowych zapytań do serwera, który nie odpowiedział na poprzednie żądania.

Key – sekretny klucz

NAS-IP-Address – Adres IPV4 który ma być użyty z atrybutem 4 w pakietach RADIUS Access-Request

NAS-IPv6-Address -Adres IPV6 który ma być użyty z atrybutem 95 w pakietach RADIUS Access-Request

NAS-Identifier- Identyfikator który ma być użyty z atrybutem 32 w pakietach RADIUS Access-Request.

5.18.1.2 Server Configuration

Hostname – Adres IP lub nazwa serwera RADIUS.

Auth Port – Port UDP użyty w serwerze RADIUS do uwierzytelniania

Acct Port – Port UDP używany w RADIUS dla konta.

Timeout – Dodatkowa opcja pozwala na zmianę limitu czasu

Retransmit – Dodatkowa opcja pozwalająca na zmianę wartości retransmisji.

Key – opcjonalne pole nadpisujące klucz globalny.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	46/147
------	------	-----------------------------------	------------	--------



5.19 TACACS+

TACACS+ Server Configuration					
Global Cor	nfiguration				
Timeout	5	seconds	7		
Deadtime	0	minutes			
Key					
Server Co	ofiguration				
Server Cor	nfiguration				
Server Cor Delete	nfiguration Hostname	Port Tir	neout	Key	
Server Cor Delete	nfiguration Hostname Ferver	Port Tir	meout	Key	

Rys. 60. Konfiguracja servera TACACS+.

5.19.1 Global Configuration

Timeout – ilość sekund w zakresie o 1-1000 w oczekiwaniu na odpowiedź serwera TACACS+. **Deadtime**- Okres czasu w którym switch nie będzie wysyłał nowych zapytań do serwera, który nie odpowiedział na poprzednie żądania.

Key - Opcjonalne pole nadpisujące klucz globalny.

5.19.2 Server Configuration

Hostname- Adres IP lub nazwa serwera TACACS+. Port- Port TCP użyty do uwierzytelniania w serwerze TACACS+. Timeout- Dodatkowa opcja pozwala na zmianę limitu czasu Key- Opcjonalne pole nadpisujące klucz globalny.

5.20 Green Ethernet

Funkcjonalność umożliwia konfigurację intensywności świecenia diod LED oraz usypiania nie wykorzystywanych portów UTP - dostępna w menu **Configuration** \rightarrow **Green Ethernet**

5.20.1 LED Power Reduction Configuration,

LED Power Reduction Configuration LED Intensity Timers						
Delete Start Time End Time Intensity						
Add Time	9					
Maintenance						
On time at link change On at errors 10 Sec.						
Sava Basat						

Rys. 61. Konfigurowanie intensywności świecenia diod.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04	EV.	47/147
--	-----	--------



5.20.2 Port Power Savings Configuration

Okno umożliwiające optymalizację portów UTP w switch-u

Port P	Port Power Savings Configuration										
Optim	Optimize EEE for Latency										
Port Configuration											
					EE	ΕU	rae	nt G)uei	les	
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
Save	Reset										

Rys. 62. Konfiguracja aktywności portów UTP

5.21 Serwer DHCP (dostępny w wybranych wersjach urządzeń)

Serwer DHCP służy do przydzielania adresów sieciowych i dostarczania parametrów konfiguracyjnych do dynamicznie skonfigurowanych hostów zwanych klientami DHCP. Funkcja dostępna w menu **Configuration** \rightarrow **DHCP**.

5.21.1 Konfiguracja trybu serwera DHCP

5.21.1.1 Główne okno serwera DHCP

Funkcja dostępna w menu Configuration \rightarrow Server \rightarrow Mode umożliwia uruchomienie serwera DHCP oraz konfigurację DHCP dla wybranych VLAN-ów

		DHCP Server Mode Configuration					
Global Mode							
Mode	Disabled 🔻						
VLAN Mode							
	ae						
Delete	VLAN Range	Mode					
Delete	VLAN Range	Mode Enabled V					

Save Reset

Rys. 63. Okno przedstawiające konfigurację serwera DHCP.

Global Mode – globalne włączenie/wyłączenie serwera DHCP. **VLAN Mode** – włączenie/wyłączenie serwera DHCP dla wskazanego zakresu VLAN.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	48/147



5.21.1.2 Konfiguracja zabronionych zakresów adresów IP

Konfiguracja adresów IP zabronionych do przydzielania klientowi przez serwer DHCP. Funkcja dostępna w menu **Configuration** \rightarrow **Server** \rightarrow **Excluded IP.**

DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range
Delete	-
20.000	

Add IP Range

Save Reset

Rys. 64. Okno przedstawiające konfigurację zakresu zabronionych adresów IP.

5.21.1.3 Konfiguracja zarządzania pulami adresów IP oraz czasem dzierżawy

Szczegółowa konfiguracja serwera DHCP, a między innymi adresów IP, maski, oraz czasu dzierżawy. Funkcja dostępna w menu **Configuration** \rightarrow **Server** \rightarrow **Pool.**

DHCP Server Pool Configuration					
Pool Setting					
Delete	Name	Туре	IP	Subnet Mask	Lease Time
	TEST	-	-	-	1 days 0 hours 0 minutes
Add New Pool]				

Save Reset

Rys. 65.Okno przedstawiające konfigurację dodawanie puli w serwerze

Po wpisaniu nazwy i zapisaniu konfiguracji możemy klikając na nazwę "TEST" przejść do szczegółowej konfiguracji serwera DHCP jak w poniższym oknie:

REV. 1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	49/147
-----------	-----------------------------------	------------	--------



DHCP Pool Configuration		
Pool		
Name TEST V		
Setting		
Pool Name	TEST	
Туре	None	•
IP		
Subnet Mask		
	1	days (0-365)
Lease Time	0	hours (0-23)
	0	minutes (0-59)
Domain Name		
Broadcast Address		
	0.0.0.0	
Default Router	0.0.0.0	
Donadit Houter	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
DNE Server	0.0.00	
Divs Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NTD Server	0.0.0.0	
WIP Server	0.0.0.0	
	0.0.0.0	
NetBIOS Node Type	None	•
NetBIOS Scope		
	0.0.0.0	
NetBIOS Name Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NIS Domain Name		
	0.0.0.0	
NIS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0 None	
Client Identifier	None +	
Hardware Address		
Client Name		
Vendor 1 Class Identifier		
Vendor 1 Specific Information		
Vendor 2 Class Identifier		
Vendor 2 Specific Information		
Vendor 3 Class Identifier		
Vendor 3 Specific Information	-	
Vendor 4 Class Identifier		
Vendor 4 Specific Information		
· · · · · · · · · · · · · · · · · · ·		

Rys. 66. Okno przedstawiające szczegółową konfigurację wybranej puli.

Type - Wybór trybu.

Network: pula definiuje pulę adresów IP do obsługi więcej niż jednego klienta DHCP.

Host: pula usług dla konkretnego klienta DHCP identyfikowanego na podstawie identyfikatora klienta lub adresu MAC.

IP – określa adres IP sieci w puli DHCP.

Subnet Mask - Opcja DHCP 1.

określa maskę podsieci w puli adresów DHCP.

Lease Time - Opcja DHCP 51, 58 i 59.

określa czas dzierżawy, który pozwala klientowi żądać czasu dzierżawy dla adresu IP. Jeśli wszystkie mają wartość 0, oznacza to, że czas dzierżawy jest nieskończony.

Domain Name - Opcja 15 DHCP.

Określa nazwę domeny, której klient powinien używać podczas rozpoznawania nazwy hosta przez DNS.

Broadcast Address - Opcja DHCP 28.

określa adres rozgłoszeniowy używany w podsieci klienta.

Default Router - Opcja DHCP 3.

Określa listę adresów IP dla routerów w podsieci klienta.

DNS Server - Opcja DHCP 6.

Określa listę serwerów nazw Domain Name System dostępnych dla klienta.

NTP Server - Opcja DHCP 42.

Określa listę adresów IP wskazujących dostępne dla klienta serwery NTP.

NetBIOS Node Type - Opcja DHCP 46.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	50/147
------	------	-----------------------------------	------------	--------



Opcja określająca typ węzła NetBIOS umożliwiająca skonfigurowanie Netbios za pomocą klienta TCP/IP, które są konfigurowalne zgodnie z opisem w RFC 1001/1002.

NetBIOS Scope - Opcja DHCP 47.

Określa parametr zakresu NetBIOS przez TCP / IP dla klienta, zgodnie z zaleceniem RFC 1001/1002.

NetBIOS Name Server - Opcja DHCP 44.

Określa listę serwerów nazw NBNS wymienionych w kolejności w zależności od preferencji.

NIS Domain Name - Opcja DHCP 40.

Oklreśla nazwę domeny NIS klienta.

NIS Server - Opcja DHCP 41.

Określa listę adresów IP wskazujących dostępne dla klienta serwery NIS.

Client Identifier - Opcja DHCP 61.

Określa unikalny identyfikator klienta, który będzie używany, gdy pula określona jest jako host.

Hardware Address - określa adres sprzętowy klienta (MAC), który ma być używany, gdy pula określona jest jako host.

Client Name - Opcja DHCP 12.

Określa nazwę klienta, który ma być używany, gdy pula określona jest jako host.

Vendor i Class Identifier - Opcja DHCP 60.

Określa, które identyfikatory mają być używane przez klienta DHCP, aby opcjonalnie zidentyfikować typ dostawcy i konfigurację klienta DHCP. Serwer DHCP dostarczy odpowiednie specyficzne informacje w opcji 43 do klienta, który wysyła identyfikator klasy dostawcy zgodnie z opcją 60.

Vendor i Specific Information - Opcja DHCP 43.

Określa informacje dotyczące dostawcy zgodnie z identyfikatorem klasy dostawcy zgodnie z opcją 60.

5.21.2 Konfiguracji DHCP Snooping

Funkcja umożliwiająca zabezpieczenie portów przed dołączeniem nieautoryzowanego serwera DHCP

DHCP Snooping Configuration

Snooping Mode Disabled •

Port Mode Configuration

Port	Mode
*	
10GigabitEthernet 1/1	Trusted •
10GigabitEthernet 1/2	Trusted
10GigabitEthernet 1/3	Untrusted
10GigabitEthernet 1/4	Trusted •
GigabitEthernet 1/1	Trusted •
GigabitEthernet 1/2	Trusted •
GigabitEthernet 1/3	Trusted •
GigabitEthernet 1/4	Trusted •
GigabitEthernet 1/5	Trusted •
GigabitEthernet 1/6	Trusted •
GigabitEthernet 1/7	Trusted •
GigabitEthernet 1/8	Trusted •
GigabitEthernet 1/9	Trusted •
GigabitEthernet 1/10	Trusted •
GigabitEthernet 1/11	Trusted •
GigabitEthernet 1/12	Trusted •
GigabitEthernet 1/13	Trusted •
GigabitEthernet 1/14	Trusted •
GigabitEthernet 1/15	Trusted •
GigabitEthernet 1/16	Trusted •

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	51/147



Rys. 67. Okno włączenia funkcji oraz konfigurację poszczególnych portów.

Snooping Mode - Wskazuje działanie trybu nasłuchiwania DHCP. Możliwe tryby to:

Enabled: Włącza działanie trybu nasłuchiwania DHCP. Po włączeniu trybu nasłuchiwania DHCP komunikaty żądań DHCP będą przekazywane do zaufanych portów i będzie zezwolenie tylko na pakiety odpowiedzi z zaufanych portów.

Disabled: Wyłącza działanie trybu nasłuchiwania DHCP.

Port Mode Configuration - Wskazuje tryb portu nasłuchiwania DHCP. Możliwe tryby portów to: *Trusted:* Konfiguruje port jako zaufane źródło komunikatów DHCP.

Untrusted: Konfiguruje port jako niezaufane źródło komunikatów DHCP.

DHCP Palay Configuration

5.21.3 Opis funkcji DHCP Relay

Agent jest używany do przekazywania i przesyłania komunikatów DHCP między klientami, a serwerem, gdy nie znajdują się w tej samej domenie podsieci. Przechowuje adres IP interfejsu przychodzącego w polu GIADDR pakietu DHCP. Serwer DHCP może użyć wartości pola GIADDR do określenia przypisanej podsieci.

BHOP Relay configuration					
Relay Mode	Disabled •				
Relay Server	0.0.0				
Relay Information Mode	Disabled 🔹				
Relay Information Policy	Keep 🔻				
	Replace				
Save Reset	Кеер				
	Drop				

Rys. 68. Okno włączenia funkcji przekazywania komunikatów DHCP dla urządzeń w innej podsieci.

Relay Mode - Wskazuje działanie w trybie DHCP Relay. Możliwe tryby to:

Enabled: Po włączeniu trybu DHCP Relay, agent transmituje wiadomości DHCP pomiędzy klientami i serwerem, gdy nie znajdują się oni w tej samej domenie podsieci.

Disabled: Wyłączone działanie w trybie DHCP Relay.

Relay Server - Wskazuje adres IP serwera retransmitującego DHCP.

Relay Information Mode - Wskazuje opcję działania trybu informacji DHCP Relay. Format identyfikatora obwodu dla opcji 82 tworzony jest jako "[vlan_id] [identyfikator_modułu] [nr_portu]". Pierwsze cztery znaki to identyfikator sieci VLAN, piąty i szósty znak to identyfikator modułu (w urządzeniu autonomicznym zawsze wynosi 0, w urządzeniu z możliwością łączenia w stos oznacza to identyfikator przełącznika), a ostatnie dwa znaki to numer portu. Na przykład "00030108" oznacza wiadomość DHCP odebraną z VLAN ID 3, ID przełącznika 1, portu nr 8. Wartość zdalnego ID opcji 82 jest równa adresowi MAC przełącznika.

Możliwe tryby to:

Enabled: Włączone działanie w trybie retransmisji informacji DHCP. Gdy tryb retransmisji informacji DHCP jest włączony, agent wstawia określone informacje (opcja 82) do komunikatu DHCP podczas przekazywania do serwera DHCP i usuwa je z komunikatu DHCP podczas przesyłania do klienta DHCP. Działa tylko wtedy, gdy włączony jest tryb pracy DHCP Relay. *Disabled:* Wyłaczone działanie trybu informacji DHCP Relay.

Relay Information Policy - Wskazuje strategię opcji informacji DHCP Relay. Gdy tryb retransmisji informacji DHCP jest włączony, agent otrzyma komunikat DHCP, który już zawiera informacje o agencie, co wymusi stosowanie odpowiednich zasad. Zasada "Zastąp" jest nie ważna, gdy tryb przekazywania informacji jest wyłączony. Możliwe zasady to:

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	52/147
------	------	-----------------------------------	------------	--------



Replace: Zastąp oryginalne informacje o retransmisji, gdy zostanie odebrany komunikat DHCP, który już je zawiera.

Keep: Zachowaj oryginalne informacje o retransmisji, gdy zostanie odebrany komunikat DHCP, który już je zawiera.

Drop: Porzuć pakiet, gdy zostanie odebrany komunikat DHCP, który już zawiera informacje o retransmisji.

5.22 Agregacja portów

Przełącznik **HYPERION** umożliwia agregację portów fizycznych w różnych konfiguracjach (nie ma rozróżnienia pomiędzy typami portów). Agregacja jest to logiczne łączenie kilku portów równolegle w celu uzyskania większej przepustowości łącza oraz redundancji, która zapewnia większą odporność systemu na uszkodzenia.

HYPERION obsługuje agregację statyczną oraz automatyczną przy użyciu protokołu LACP (Link Aggregation Control Protocol).

5.22.1 Agregacja statyczna

Agregacja statyczna umożliwia ręczne wybranie agregowanych portów, które pozostają niezmienne niezależnie od warunków panujących w sieci. Aby rozpocząć konfigurację należy kliknąć **Configuration** \rightarrow **Aggregation** \rightarrow **Static**.

Hash Code Contributors							
Source MAC Address							
Destination M	IAC	Add	ress		1		
IP Address				-	1		
TCP/UDP Por	rt Nu	imbe	er	-	1		
a				~			
Aggregation Group Configuration							
Aggregatio		510	up	00	mış	Jui	auo
հցցլեցում		Po	ort l	Men	nbe	rs	auc
Group ID	1	Pc 2	ort I	Men 4	nbe 5	rs 6	7
Group ID Normal	1	Pc 2 @	ort I 3	Ven 4	nbe 5	rs 6	7 ()
Group ID Normal	1	Pc 2 0	ort f 3 ©	Ven 4 ©	nbe 5 ©	rs 6 0	7 ©
Group ID Normal 1 2	1 © ©	Pc 2 ©	ort 3 ©	Vlen 4 0 0	nbe 5 0	ers 6 ©	7 () () ()
Group ID Normal 1 2 3	1 © ©	Pc 2 © ©	ort 3 © © ©	Vien 4 0 0	nbe 5 0 0	ers 6 0 0	7 © ©
Group ID Normal 1 2 3	1 © ©	Pc 2 © ©	ort 3 © ©	Vlen 4 ◎ ○ ○	nbe 5 © ©	ers 6 © ©	7 © ©

Aggregation Mode Configuration

Rys. 69. Konfiguracja statycznej agregacji portów.

Możliwa jest agregacja maksymalnie w trzech grupach portów. Aby przyporządkować porty do grup, w sekcji **Aggregation Group Configuration** należy zaznaczyć odpowiednie pola dla wybranych portów (kolumny), co spowoduje przypisanie tych portów do wybranej grupy (wiersze **1**, **2** lub **3**). Zaznaczenie wiersza **Normal** wyłącza dany port z agregacji.

W tabeli **Hash Code Contributors** możliwe jest ustawienie jakich danych powinno używać urządzenie w celu określenia portu docelowego dla ramek wychodzących. Dostępne dane od góry to:

Source MAC Address – Źródłowy adres MAC.

Destination MAC Address – Docelowy adres MAC.

IP Address – Adres IP.

TCP/UDP Port Number – Numer portu TCP/UDP.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	53/147
------	------	-----------------------------------	------------	--------



5.22.2 Agregacja automatyczna (dynamiczna)

Agregacja automatyczna w **HYPERION** jest realizowana z wykorzystaniem protokołu LACP, zdefiniowanego w normie IEEE 802.3ad. Protokół ten umożliwia automatyczną negocjację grupowania połączeń pomiędzy urządzeniami go obsługującymi. Aby rozpocząć konfigurację należy kliknąć **Configuration** \rightarrow **Aggregation** \rightarrow **LACP**.

LACP Port Configuration							
Port	LACP Enabled	Ke	ey 🛛	Role	Timeout	Prio	
*		< ▼		<> ▼	<> ▼	32768	
1		Auto 🔻		Active •	Fast •	32768	
2		Auto 🔻		Active •	Fast 🔻	32768	
3		Auto 🔻		Active •	Fast 🔻	32768	
4		Auto 🔻		Active •	Fast 🔻	32768	
5		Auto 🔻		Active •	Fast •	32768	
6		Auto 🔻		Active •	Fast 🔻	32768	
7		Auto 🔻		Active •	Fast •	32768	

Save Reset

Rys. 70. Konfiguracja automatycznej agregacji portów.

Możliwe jest ustawienie następujących parametrów dla każdego portu:

LACP Enabled – jeśli pole jest zaznaczone, to określony port może zostać użyty przy automatycznej agregacji.

Key – klucz agregacji – wartość liczbowa z przedziału od 1 do 65535. Tylko porty o tym samym kluczu mogą być połączone w grupę agregacji (jeśli są podłączone do tego samego urządzenia zdalnego). Ustawienie **Specific** pozwala na ręczne wpisanie wartości, a ustawienie **Auto** powoduje automatyczne dobranie tej wartości na podstawie prędkości łącza na porcie: 10Mb = 1, 100Mb = 2, 1Gb = 3.

Role – określa rolę portu w protokole. Ustawienie **Active** powoduje, że urządzenie będzie wysyłało ramki LACP z tego portu co sekundę, **Passive** oznacza, że port będzie tylko oczekiwał na ramki przychodzące LACP od urządzenia zdalnego.

Timeout – Limit czasu określa czas pomiędzy transmisjami BPDU. Opcja Fast będzie przesyłać pakiety LACP co sekundę, natomiast Slow będzie przesyłał w odstępach 30 sekundowych.

Prio – Prio steruje priorytetem portu, możliwy zakres to 1-65535. Niższa liczba oznacza większy priorytet.

5.23 Loop Protection

Funkcja chroniąca sieci przed nieoczekiwaną pętlą poprzez automatyczne fizyczne wyłączenie portu, na którym switch wykrył pętlę. Wyłączenie portu może być ograniczone czasowo zgodnie z konfiguracją w oknie "General Settings" Funkcja dostępna w menu **Configuration** \rightarrow **Loop Protection.**

General Settings

Enable Loop Protection - Kontroluje, czy zabezpieczenia pętli są włączone (jako całość).

Transmission Time - Odstęp czasu między każdym PDU ochrony pętli wysyłanym na każdym porcie. Prawidłowe wartości to od 1 do 10 sekund. Wartość domyślna to 5 sekund.

Shutdown Time - Okres (w sekundach), przez który port pozostanie wyłączony w przypadku wykrycia pętli (a działanie zabezpieczenia spowoduje zamknięcie portu). Prawidłowe wartości to od 0 do 604800 sekund (7 dni). Wartość zero spowoduje wyłączenie portu (do następnego restartu urządzenia). Wartość domyślna to 180 sekund.



Port Configuration

Port - Numer portu przełącznika.

Enable - Określa, czy ochrona pętli jest włączona na tym porcie przełącznika.

Action - Konfiguruje akcję wykonywaną po wykryciu pętli na porcie. Prawidłowe wartości to Shutdown Port, Shutdown Port i Log lub Log Only.

Tx Mode - Określa, czy port aktywnie generuje PDU ochrony przed pętlami, czy tylko pasywnie szuka zapętlonych PDU.

Loop Protection Configuration

Global Configuration						
Enable Loop Protection Disable V						
Transmission Time	5		seco	onds		
Shutdown Time	180		sec	onds		
Port Configuration						
Port	Enable		Action	Tx Mode		
*		\diamond	•	○ ▼		
10GigabitEthernet 1/1	1	Shutdown Port	•	Enable •		
10GigabitEthernet 1/2	~	Shutdown Port	•	Enable •		
10GigabitEthernet 1/3	\$	Shutdown Port	•	Enable •		
10GigabitEthernet 1/4	~	Shutdown Port	•	Enable •		
GigabitEthernet 1/1	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/2	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/3	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/4	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/5	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/6	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/7	«	Shutdown Port	•	Enable 🔻		
GigabitEthernet 1/8	1	Shutdown Port	•	Enable •		
GigabitEthernet 1/9	1	Shutdown Port	•	Enable 🔻		
GigabitEthernet 1/10		Shutdown Port	•	Enable 🔻		
GigabitEthernet 1/11	«	Shutdown Port	•	Enable •		
		[

Rys. 71. Okno włączenia funkcji Loop protection.

5.24 Konfiguracja profilu IPMC

Funkcja dostępna w menu **Configuration** \rightarrow **IPMC Profile**.

Profil IPMC jest wykorzystywany do wdrażania kontroli dostępu w strumieniach multicast IP. Dopuszcza się tworzenie maksymalnie 64 profili z maksymalnie 128 odpowiednimi regułami dla każdego z nich.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	55/147
------	------	-----------------------------------	------------	--------



5.24.1 Tablice profilu

IPMC Profile Configurations Global Profile Mode Disabled V IPMC Profile Table Setting Delete Profile Name **Profile Description** Rule TEST 👁 🙆 Add New IPMC Profile Save Reset 🔟 IPMC Profile Rule Configuration - Google Chrome × () Niezabezpieczona | 192.168.0.10/ipmc_lib_rule_table.htm?CurSidV=-1&DoPdxOp=0&DynBgnPdx=0x.. IPMC Profile [TEST] Rule Settings (In Precedence Order) Profile Name & Index Entry Name Address Range Action Log

Rys. 72.Okno konfiguracji profilu IPMC oraz lista reguł dla skonfigurowanego profilu

Global Profile Mode - Włącz / wyłącz globalny profil IPMC.

System zaczyna filtrować na podstawie ustawień profilu tylko wtedy, gdy włączony jest tryb profilu globalnego.

Delete - Zaznacz, aby usunąć wpis. Wyznaczony wpis zostanie usunięty podczas następnego zapisu.

Profile Name - Nazwa używana do indeksowania tabeli profili. Każdy wpis ma unikalną nazwę składającą się maksymalnie z 16 znaków alfabetu i cyfr. Musi być obecny co najmniej jeden znak alfabetu.

Profile Description - Po utworzeniu profilu kliknij przycisk edycji, aby wejść na stronę ustawień reguł dla wyznaczonego profilu. Podsumowanie dotyczące wyznaczonego profilu zostanie wyświetlone po kliknięciu przycisku widoku. Możesz zarządzać lub przeglądać reguły wyznaczonego profilu za pomocą następujących przycisków:

Wyświetl listę reguł związanych z wyznaczonym profilem.

(e): Dostosuj reguły związane z wyznaczonym profilem.

Strona do ustawienia reguł filtrowania dla konkretnego profilu IPMC po kliknięciu na symbol wyświetla skonfigurowane wpisy reguł w kolejności pierwszeństwa. Pierwszy wpis reguły ma najwyższy priorytet w wyszukiwaniu, podczas gdy ostatni wpis reguły ma najniższy priorytet.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 50	56/147
---	--------



IPMC Profile Configurations

Global Profile Mode Disabled V

IPMC Profile Table Setting

Delete	Profile Name		Profile	Description	on	Rule
	TEST	A				۵ ک
Add New	/ IPMC Profile					
Save	Reset					
IPMC P	rofile [TEST] R	ule Settings	(In Precedence C	Order)		
Profile	Name & Index	Entry Name	Address Range	Action	Log	
TEST	1	- 🔻	~	Deny T	Disable ▼	⊕© ⊕©
Add Las	t Rule			Permit		
Commit	Reset					

Rys. 73. Okno konfiguracji reguł dla profili IPMC

Profile Name - Nazwa profilu, który ma zostać powiązany. Tego pola nie można edytować.

Entry Name - Nazwa używana przy określaniu zakresu adresów używanego dla tej reguły.

W wybranym polu zostaną wybrane tylko istniejące wpisy adresu profilu. Nie można wybrać tego pola jako brak ("-"), gdy tabela ustawień reguł jest zatwierdzona.

Address Range - Odpowiedni zakres adresów wybranego profilu. To pole nie jest edytowalne i zostanie dostosowane automatycznie zgodnie z wybranym wpisem profilu.

Action - Wskazuje czynność uczenia się po odebraniu ramki Join / Report, której adres grupy jest zgodny z zakresem adresów reguły.

Permit: Adres grupy zgodny z zakresem określonym w regule, zostanie nauczony.

Deny: Adres grupy zgodny z zakresem określonym w regule zostanie usunięty.

Log - Wskazuje preferencje rejestrowania po odebraniu ramki Join / Report, której adres grupy jest zgodny z zakresem adresów reguły.

Enable: Odpowiednie informacje o adresie grupowym, które pasują do zakresu określonego w regule, zostaną zarejestrowane.

Disable: Odpowiednie informacje o adresie grupowym, które pasują do zakresu określonego w regule, nie zostaną zarejestrowane.

Przyciski zarządzania regułami - Możesz zarządzać regułami i odpowiadającą im kolejnością pierwszeństwa za pomocą następujących przycisków:

🕀: Wstaw nową regułę przed obecną regułą.

😢: Usuń bieżący wpis reguły.

🕐: Przenosi bieżący wpis reguły w górę na liście.

😔: Przenosi bieżący wpis reguły w dół na liście.

Przyciski

"Add Last Rule": Kliknij, aby dodać nową regułę na końcu listy reguł określonego profilu. Określ wpis adresu i skonfiguruj nowy wpis. Kliknij "Commit".

"Commit": Kliknij, aby zatwierdzić zmiany reguł dla wyznaczonego profilu.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 57/14	REV.
--	------



5.24.2 Konfiguracja adresów IP dla profilu IPMC

Okno służy do określenia zakresu adresów IP, które będą powiązane z profilem IPMC. Można utworzyć maksymalnie 128 instancji w systemie.

Wpis adresu służy do określenia zakresu adresów, który będzie powiązany z profilem IPMC. W systemie można utworzyć maksymalnie 128 wpisów adresowych.

Delete - Zaznacz, aby usunąć wpis.

Wyznaczony wpis zostanie usunięty podczas następnego zapisu.

Entry Name - Każdy wpis ma unikalną nazwę składającą się maksymalnie z 16 znaków alfabetu i cyfr. Musi być obecny co najmniej jeden znak alfabetu.

Start Address - Początkowy adres grupy Multicast IPv4 / IPv6, który będzie używany jako zakres adresów.

End Address - Końcowy adres grupy Multicast IPv4 / IPv6, który będzie używany jako zakres adresów.

IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page

Delete	Entry Name	Start Address	End Address
Delete			
Add New	Address (Range) Entry		
Save R	leset		

Rys. 74. Okno konfiguracji zakresu adresacji IP

5.25 KONFIGURACJA PROTOKÓŁ MVR

Funkcja dostępna w menu **Configuration** \rightarrow **MVR**.

MVR - Multicast VLAN Registration (MVR) jest protokołem sieciowym warstwy 2 modelu ISO/OSI, który umożliwia współdzielenie ruchu multicastowego ze źródłowej sieci VLAN z abonenckimi sieciami VLAN. Głównym powodem zastosowania MVR jest oszczędność pasma poprzez zapobieganie wysyłaniu duplikatów strumieni multicastowych w sieciach, zamiast tego strumienie te są odbierane w MVR-VLAN i przekazywane do sieci VLAN, w których żądają tego hosty.

Funkcja MVR umożliwia przekierowanie ruchu multicastowego w sieciach VLAN Multicast. W aplikacji telewizyjnej obsługującej tryb Multicast, strumień może być odbierany przez komputer, telewizor lub dekoder. Do jednego portu abonenckiego, który jest portem przełącznika skonfigurowanym jako port odbiornika MVR, można podłączyć wiele dekoderów lub komputerów PC.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	58/147
------	------	-----------------------------------	------------	--------



MVR Configurations

 MVR Mode
 Disabled •

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

D	elete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
D	elete			0.0.0.0	Dynamic 🗸	Tagged 🖌	0	5	- V
1	Port	1 2 3 4	5 6 7 8 9 10 11 12	13 14 15 16 17 18	19 20 21 22 23	24 25 26 27 28	29 30 31 32	33 34 35 36 3	37
F	Role								

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	 v
10GigabitEthernet 1/1	Disabled V
10GigabitEthernet 1/2	Disabled V
10GigabitEthernet 1/3	Disabled V
10GigabitEthernet 1/4	Disabled 🗸
GigabitEthernet 1/1	Disabled V
GigabitEthernet 1/2	Disabled ¥
GigabitEthernet 1/3	Disabled V
GigabitEthernet 1/4	Disabled V
GigabitEthernet 1/5	Disabled V
GigabitEthernet 1/6	Disabled 🗸

Rys. 75. Okno konfiguracji trybu MVR.

MVR VID - Podaj identyfikator sieci VLAN multicastowej.

Uwaga: nie zaleca się nakładania portów źródłowych MVR z portami zarządzania VLAN.

MVR Name - Nazwa MVR to opcjonalny atrybut wskazujący nazwę określonej sieci VLAN MVR. Maksymalna długość ciągu znaków dla nazwy sieci VLAN MVR to 16.

Adres IGMP - Definiuj adres IPv4 jako adres źródłowy używany w nagłówku IP dla kontroli ramek IGMP.

Domyślny adres IGMP nie jest konfigurowany i posiada wartość (0.0.0.0). Gdy adres IGMP nie jest ustawiony, system wykorzystuje adres zarządzania IPv4 interfejsu IP skojarzonego z tą siecią VLAN.

Jeśli adres zarządzania IPv4 nie jest ustawiony, system używa pierwszego dostępnego adresu zarządzania IPv4.

W innym wypadku system użyje wstępnie zdefiniowanej wartości. Domyślnie ta wartość to 192.0.2.1.

Mode - Wybór trybu pracy MVR. W trybie dynamicznym MVR (Dynamic), MVR pozwala na dynamiczne raportowanie członkostwa MVR na portach źródłowych. W trybie Compatible, raporty o przynależności do MVR są zabronione na portach źródłowych. Domyślnie ustawiony jest tryb (Dynamic).

5.26 PROTOKÓŁ IGMP

Funkcja dostępna w menu **Configuration** → **IPMC** → **IGMP Snooping.** Wersja dla adresacji IPv4.

IGMP (Internet Group Management Protocol) - jest to protokół komunikacyjny używany do zarządzania przynależnością w internetowych protokołach multicastowych. IGMP jest używany przez hosty IP i sąsiednie routery multicastowe w celu ustanowienia członkostwa w grupach multicastowych. Jest to integralna część specyfikacji multicast IP, podobnie jak ICMP dla połączeń unicast.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	59/147
------	------	-----------------------------------	------------	--------



5.26.1 Konfiguracja IGMP Snooping dla adresacji IPv4

5.26.1.1 Konfiguracja podstawowa

Configuration \rightarrow IPMC \rightarrow IGMP Snooping \rightarrow Basic Configuration.

IGMP Snooping Configuration

	Global Cont	figuration
Snooping Enabled		
Unregistered IPMCv4 Flooding Enabled	~	
IGMP SSM Range	232.0.0.0	/ 8
Leave Proxy Enabled		
Proxy Enabled		

Port Related Configuration

Dent	Davidan David	East Lasue	The second difference
Ροπ	Router Port	Fast Leave	Inrottling
*			<> ▼
10GigabitEthernet 1/1			unlimited V
10GigabitEthernet 1/2			unlimited
10GigabitEthernet 1/3			1
10GigabitEthernet 1/4			3
GigabitEthernet 1/1			4
GigabitEthernet 1/2			5
GigabitEthernet 1/3			6
GigabitEthernet 1/4			8
GigabitEthernet 1/5			9
GigabitEthernet 1/6			10

Rys. 76. Okno konfiguracji podstawowej IGMP snooping.

Snooping Enabled - Włącz Global IGMP snooping.

Unregistered IPMCv4 Flooding Enabled - Włącz "zalewanie" niezarejestrowanego ruchu IPMCv4. Kontrola "zalewania" działa tylko wtedy, gdy włączona jest funkcja IGMP Snooping. Gdy IGMP Snooping jest wyłączone, niezarejestrowany przepływ ruchu IPMCv4 jest zawsze aktywny pomimo tego ustawienia.

IGMP SSM Range - SSM (Source-Specific Multicast) Zakres umożliwia hostom i routerom obsługującym SSM uruchamianie modelu usług SSM dla grup w zakresie adresów.

Prawidłowy adres multicast IPv4 określany jest jako prefiks o długości prefiksu (od 4 do 32) dla zakresu.

Leave Proxy Enabled - Włącz IGMP Leave Proxy. Aktywowanie funkcji pozwala uniknąć przekazywania niepotrzebnych wiadomości pozostawionych po stronie routera.

Proxy Enabled - Włącz serwer proxy IGMP. Aktywowanie funkcji pozwala uniknąć przekazywania niepotrzebnego łączenia i pozostawiania wiadomości po stronie routera.

Router Port - Określa, które porty działają jako porty routera. Port routera to port w przełączniku Ethernet, który prowadzi do urządzenia multicast warstwy 3 lub kwerendy IGMP.

Jeśli jako port routera wybrano port członka agregacji, cała agregacja będzie działać jako port routera.

Fast Leave - Włączenie szybkiego wyjścia na port.

Throttling - Umożliwia ograniczenie liczby grup multicastowych, do których może należeć port przełącznika.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	60/147
------	------	-----------------------------------	------------	--------



5.26.1.2 Konfiguracja VLAN

$\textbf{Configuration} \rightarrow \textbf{IPMC} \rightarrow \textbf{IGMP Snooping} \rightarrow \textbf{VLAN Configuration}.$

IGMP Snooping VLAN Configuration												
Start from VLAN 1 with 20 entries per page.												
Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QR	l (0.1 sec)	LLQI (0.1 sec	URI (sec)
Delete			✓	0.0.0.0	IGMP-Auto 🗸	0 🗸	2	125	ſ	100	10	1
					IGMP-Auto							
Add New IGMP VLAN				Forced IGMPv1								
			Forced IGMPv2									
Save	leset				Forced IGMPv3							

Rys. 77.Okno konfiguracji VLAN dla IGMP snooping.

Poruszanie się po tablicy IGMP Snooping VLAN

Każda strona zawiera do 99 wpisów z tabeli VLAN, domyślnie 20, wybranych za pomocą pola wprowadzania "entries per page". Przy pierwszej wizycie na stronie zostanie wyświetlonych 20 pierwszych wpisów z początku tabeli sieci VLAN. Jako pierwszy zostanie wyświetlony ten z najniższym identyfikatorem sieci VLAN znalezionym w tabeli sieci VLAN.

Pola wejściowe "VLAN" pozwalają użytkownikowi wybrać punkt początkowy w tabeli VLAN. Kliknięcie przycisku "Refresh" zaktualizuje wyświetlaną tabelę, zaczynając od tej lub następnej najbliższej tabeli sieci VLAN.

Znak >> użyje ostatniego wpisu z aktualnie wyświetlanego wpisu jako podstawy do następnego wyszukiwania. Po osiągnięciu końca w wyświetlonej tabeli pojawi się tekst "No more entries". Użyj |<<, aby zacząć od nowa.

Kolumny tabeli IGMP Snooping VLAN

Delete - Zaznacz, aby usunąć wpis. Wpis zostanie usunięty podczas następnego zapisu.

VLAN ID - Identyfikator sieci VLAN wpisu.

IGMP Snooping Enabled - Włącz śledzenie IGMP dla poszczególnych sieci VLAN. Do protokołu IGMP Snooping można wybrać do 32 sieci VLAN.

Querier Election - Włącz, aby dołączyć do wyborów IGMP Querier w sieci VLAN. Wyłącz, aby działać jako IGMP Non-Querier.

Querier Address - Zdefiniuj adres IPv4 jako adres źródłowy używany w nagłówku IP do wyboru IGMP Querier. Jeśli adres kwerendy nie jest ustawiony, system używa adresu zarządzania IPv4 interfejsu IP powiązanego z tą siecią VLAN. Jeśli adres zarządzania IPv4 nie jest ustawiony, system używa pierwszego dostępnego adresu zarządzania IPv4. W przeciwnym razie system używa wstępnie zdefiniowanej wartości. Domyślnie ta wartość to 192.0.2.1.

Compatibility - Zgodność jest utrzymywana przez hosty i routery podejmujące odpowiednie działania w zależności od wersji protokołu IGMP działających na hostach i routerach w sieci. Dozwolony wybór to **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**, domyślna wartość zgodności to IGMP-Auto.

PRI - Priorytet interfejsu.

Wskazuje poziom priorytetu ramki sterującej IGMP generowany przez system. Te wartości mogą służyć do ustalania priorytetów różnych klas ruchu. Dozwolony zakres wynosi od 0 (best effort) do 7 (najwyższy), domyślna wartość priorytetu interfejsu to 0.

RV - Zmienna odporności (ang. Robustness Variable).

Zmienna odporności umożliwia dostrojenie spodziewanej utraty pakietów w sieci.

Dozwolony zakres to od 1 do 255, domyślna wartość zmiennej odporności to 2.

QI - Interwał zapytań (ang. Query Interval). Interwał zapytań jest interwałem pomiędzy General Queries wysyłanymi przez Querier.

Dozwolony zakres to od 1 do 31744 sekund, domyślny interwał zapytań to 125 sekund.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 6	61/147
--	--------



QRI - Czas odpowiedzi na zapytanie (ang. Query Response Interval). Maksymalne opóźnienie odpowiedzi używane do obliczania maksymalnego kodu odpowiedzi (ang. Maximum Response Code) wstawianego do okresowych zapytań ogólnych (ang. General Queries).

Dozwolony zakres to od **0** do **31744** w dziesiątych częściach sekundy, domyślny interwał odpowiedzi na zapytanie to 100 w dziesiątych częściach sekundy (10 sekund).

LLQI (LMQI for IGMP) - Ostatni interwał zapytań o członków (ang. Last Member Query Interval). Last Member Query Time to wartość czasu reprezentowana przez Last Member Query Interval, pomnożony przez Last Member Query Count.

Dozwolony zakres to od **0** do **31744** w dziesiątych częściach sekundy, domyślny interwał ostatniego zapytania składowego to 10 w dziesiątych częściach sekundy (1 sekunda).

URI - Niezamówiony okres raportowania (ang.Unsolicited Report Interval) to czas między powtórzeniami wstępnego raportu hosta o członkostwie w grupie.

Dozwolony zakres to od **0** do **31744** sekund, domyślny interwał niezamawianych raportów to 1 sekunda.

<u>Przyciski</u>

"Refresh": Odświeża wyświetlaną tabelę, zaczynając od pól wejściowych "VLAN". |<< : Aktualizuje tabelę, zaczynając od pierwszego wpisu w tabeli VLAN, tj. Wpisu o najniższym identyfikatorze VLAN.

>> : Aktualizuje tabelę, rozpoczynając od wpisu następującego po ostatnio wyświetlanej pozycji. "Add new IGMP VLAN": kliknij, aby dodać nowy IGMP VLAN. Określ VID i skonfiguruj nowy wpis. Kliknij "Save". Określona sieć IGMP VLAN zaczyna działać po utworzeniu odpowiedniej statycznej sieci VLAN.

5.26.1.3 Konfiguracja wyboru profilu ICMP dla określonego portu

$\textbf{Configuration} \rightarrow \textbf{IPMC} \rightarrow \textbf{IGMP Snooping} \rightarrow \textbf{Port Filtering Profile}$

Umożliwia wybór profilu IPMC jako warunek filtrowania dla poszczególnych portów.

IGMP Snooping Port Filtering Profile								
Configuration								
Port	Filtering P	rofile						
10GigabitEthernet 1/1	٠	- 7						
10GigabitEthernet 1/2	٠	- 🔻						
10GigabitEthernet 1/3	٠	- 7						
10GigabitEthernet 1/4	٠	- 7						
GigabitEthernet 1/1	٠	- 7						
GigabitEthernet 1/2	٠	- 7						
GigabitEthernet 1/3	٠	- 7						
GigabitEthernet 1/4	۰	- 7						
GigabitEthernet 1/5	٠	- 7						
GigabitEthernet 1/6	۰	- 7						
GigabitEthernet 1/7	٠	- 7						
GigabitEthernet 1/8	۰	- 7						
GigabitEthernet 1/9	٠	- 7						
GigabitEthernet 1/10	٠	- 7						

Rys. 78.Okno konfiguracji VLAN dla IGMP snooping.

Port - Port logiczny dla ustawień.

Filtering Profile - Wybierz profil IPMC jako warunek filtrowania dla określonego portu. Podsumowanie dotyczące wyznaczonego profilu zostanie wyświetlone po kliknięciu przycisku widoku.

Przycisk zarządzania profilami Możesz sprawdzić zasady wyznaczonego profilu za pomocą następującego przycisku:

👁: Wymień reguły związane z wyznaczonym profilem.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	62/147
------	------	-----------------------------------	------------	--------



5.26.2 Konfiguracja MLD Snooping

Strony do konfiguracji IGMP tylko dla adresacji w wersji IPv6. Znaczenie poszczególnych podstron jest identyczne jak w powyższym punkcie 5.15.1.

5.27 PROTOKÓŁ LLDP

LLDP - Link Layer Discovery Protocol - jest protokołem standardu IEEE 802.1ab i umożliwia stacjom, podłączonym do sieci LAN IEEE 802, rozgłaszania do innych stacji sąsiadów podłączonych do tej samej sieci, parametrów przekazywanych przez system przełącznika, a zawierających między innymi nazwę stacji, adres lub adresy zarządzania przełącznika, wersji oprogramowania, numery portów oraz nazwy interfejsów, do których podłączone są inne stacje. Warunkiem możliwości odczytania parametrów jest uruchomiony protokół LLDP na wszystkich przełącznikach.

Tx Interval - Przełącznik okresowo przesyła ramki LLDP do swoich sąsiadów w celu zaktualizowania informacji o wykrywaniu sieci. Odstęp między każdą ramką LLDP jest określany przez wartość Tx Interval. Dopuszczalny zakres wartości to 5 - 32768 sekund.

Tx Hold - Każda ramka LLDP zawiera informacje o okresie ważności informacji w ramce LLDP. Okres ważności informacji LLDP jest ustawiany jako Tx Hold pomnożony przez Tx Interval przedstawiany w sekundach. Dopuszczalny zakres wartości to 2–10 razy.

Tx Delay - Jeśli jakaś konfiguracja zostanie zmieniona (np. Adres IP), zostanie przesłana nowa ramka LLDP, ale okres między ramkami LLDP będzie zawsze równy co najmniej wartości Tx Delay. Tx Delay nie może być większe niż 1/4 wartości Tx Interval. Dopuszczalny zakres wartości to 1 – 8192 w sekundach.

Tx Reinit - Gdy interfejs jest wyłączony lub LLDP jest nieaktywny, ewentualnie przełącznik jest ponownie uruchamiany, ramka dezaktywująca LLDP jest przesyłana do sąsiednich jednostek, aby unieważnić informacje LLDP. Tx Reinit kontroluje ilość sekund pomiędzy ramką dezaktywującą, a nową inicjalizacją LLDP. Dopuszczalny zakres wartości to 1-10 w sekundach.

LLDP Configuration	n						
LLDP Parameters							
Tx Interval 30	seconds						
Tx Hold 4	times						
Tx Delay 2	seconds						
Tx Reinit 2	seconds						
LLDP Interface Confi	uration						
					Ontional TI V		
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
×	 T 			e	1	e	
10GigabitEthernet 1/1	Enabled •		v		\$	1	
10GigabitEthernet 1/2	Enabled •		v		1		S
10GigabitEthernet 1/3	Enabled v				\$	S	
10GigabitEthernet 1/4	Enabled •		 Image: A start of the start of	~	1	1	S
GigabitEthernet 1/1	Enabled v		\$	a	\$	s	\$
GigabitEthernet 1/2	Enabled •		 Image: A start of the start of		1	e	S
GigabitEthernet 1/3	Enabled *		v	v	\$	a	
GigabitEthernet 1/4	Enabled •					s	
GigabitEthernet 1/5	Enabled •		v		\$	\$	\$
GigabitEthernet 1/6	Enabled v				\$		\$
GigabitEthernet 1/7	Enabled •		v		\$	1	
GigabitEthernet 1/8	Enabled *				\$	e	\$
GigabitEthernet 1/9	Enabled •		v		\$	1	s
GigabitEthernet 1/10	Enabled •		1	1	1	1	1

Rys. 79.Okno konfiguracji LLDP.

Funkcja monitorowania parametrów sąsiadów dostępna w menu Monitor \rightarrow LLDP \rightarrow Neighbors.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	63/147



LLDP Neighbor Information

	LLDP Remote Device Summary										
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address					
FastEthernet 1/1	74-DA-38-D8-B9-57	74-DA-38-D8-B9-57									
FastEthernet 1/3	00-50-C2-0E-21-9A	37	FastEthernet 1/1		Bridge(+)	192.168.0.50 (IPv4)					
FastEthernet 1/8	00-50-C2-0E-4C-41	2	GigabitEthernet 1/2		Bridge(+)	192.168.0.47 (IPv4)					

Rys. 80. Okno monitorowania sąsiadów w LLDP dopiętych do switch.

5.28 PROTOKÓŁ LLDP-MED

Rozszerzeniem standardu IEEE 802.1ab - LLDP jest LLDP-MED, który jest zdefiniowany przez stowarzyszenie branży telekomunikacyjnej (TIA-1057) umożliwiający konfigurowanie rozsyłania wybranych lub określonych parametrów dla danej konkretnej grupy urządzeń końcowych.

LL DP-MED Configura	ation								
Fast Start Repeat Cour	nt								
Fast start repeat count	4								
Transmit TLVa	-								
Interface	Capabilitie	s Policies	Location						
10GioabitEthernet 1/1	a	2	v						
10GigabitEthernet 1/2									
10GigabitEthernet 1/3									
10GigabitEthernet 1/4	1	1							
Fast start repeat count Fast start repeat count Transmit TLVs Interface Capabilities Policies Location 10GigabitEhemet 11 0 0 0 Interface Capabilities Policies 10GigabitEhemet 112 0<									
GigabitEthernet 1/2	1	×.	1						
GigabitEthernet 1/3	1	1							
GigabitEthernet 1/4	•	2	•						
GigabitEthernet 1/5	X	×							
GigabitEthernet 1/6	X	N	N						
GigabitEthernet 1/7			 Image: Control of the second se						
GigabitEthernet 1/9	₹	Image: A state of the state	Image: Control of the second secon						
GigabitEthernet 1/10	•	2							
Coordinates Location	° North	 Longitud 	e 0	° East	▼ Altitude	0	Meters V	Map Datum	WGS84 V
GigabitEthernet 1/3 Ø Ø Ø GigabitEthernet 1/3 Ø Ø Ø GigabitEthernet 1/6 Ø Ø Ø GigabitEthernet 1/7 Ø Ø Ø GigabitEthernet 1/10 Ø Ø Ø GigabitEthernet 1/10 Ø Ø Ø Coordinates Location Ø Ø Ø Latitude 0 ° North <v< td=""> Longitude 0 * East<v< td=""> Altitude 0 Meters<v< td=""> Map Datum WGS84 V Civic Address Location Country code State Country Country Country City district Block (Neighborhood) Street Leading street direction Trailing street suffix Mouse no. House no. suffix</v<></v<></v<>									
Country code			State				County		
GigabitEhernet 1/7 Ø Ø Ø GigabitEhernet 1/8 Ø Ø Ø GigabitEhernet 1/0 Ø Ø Ø GigabitEhernet 1/10 Ø Ø Ø Coordinates Location Ø Ø Ø Latitude 0 North ▼ Longitude 0 Map Datum WGS84 ▼ Civic Address Location Civic Address Location Civic Address Location East ▼ Altitude 0 Map Datum WGS84 ▼ Civic Address Location City district Block (Neighborhood) East ▼ East ▼ Block (Neighborhood) City City district Block (Neighborhood) Trailing street suffix East √ Citent utifier Haura en quifier Haura en quifier East √ Haura en quifier									
GigabitEnternet 1/10 Ø Ø Coordinates Location Latitude 0 ° East ▼ Altitude 0 Map Datum WGS84 ▼ Civic Address Location Country code State Country Country City City district Block (Neighborhood) Street Leading street direction Trailing street suffix Street suffix House no. House no. House no.									
Organization Country code Longitude 0 ° East Altitude 0 Map Datum WGS84 V Civic Address Location Civic Address Location Civic Address Location Country code City district Block (Neighborhood) City district Block (Neighborhood) City district Block (Neighborhood) City district Block (Neighborhood) City district City district Block (Neighborhood) City district City district City district Block (Neighborhood) City district City district City district City district Block (Neighborhood) City district City district<									
Landmark	igabitchement 1/2 ₩ ₩ ₩ ₩ ₩ igabitchemet 1/3 Ø Ø Ø Ø igabitchemet 1/3 Ø Ø Ø igabitchemet 1/3 Ø Ø Ø igabitchemet 1/3 Ø Ø Ø igabitchemet 1/8 Ø Ø Ø igabitchemet 1/8 Ø Ø Ø igabitchemet 1/8 Ø Ø Ø igabitchemet 1/9 Ø Ø Ø igabitchemet 1/0 Ø igabitch								
Zip code	GigabitEthernet 1/8 ♥ ♥ ♥ GigabitEthernet 1/9 ♥ ♥ ♥ oordinates Location tritic Address Location Country code State County City district Block (Neighborhood) Street Leading street direction Trailing street suffix Street Leading street direction Trailing street suffix Street Additional location info Name Zip code Building Apartment Zip code P.O. Box Additional code								
Floor	gabitEthernet 1/8								
Postal community name	e		P.O. Box	¢			Additional code		
Emergency Call Servic	e								
Emergency Call Service	e								
Policies									
Policies Delete Policy ID A	Application	Type Tag	VLAN ID	L2 Priority D	SCP				

Rvs.	81.	Okno	konfiguracii	LLDP-MED.
	••••	01010	Renniganalen	

Fast start repeat count - Szybkie uruchamianie i identyfikacja lokalizacji usługi połączeń alarmowych wykrywania punktów końcowych (ang. Emergency Call Service Location Identification Discovery of endpoints) jest aspektem krytycznie ważnym dla systemów VoIP.

Najlepiej jest ogłaszać tylko te informacje, które są szczególnie istotne dla określonych typów punktów końcowych (na przykład ogłaszać zasady sieci głosowej tylko dla dozwolonych urządzeń obsługujących głos), zarówno w celu zachowania ograniczonej przestrzeni LLDPU, jak i zmniejszenia problemów z bezpieczeństwem i integralnością systemu, które mogą wynikać z niewłaściwej znajomości zasad sieciowych.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	64/147
------	------	-----------------------------------	------------	--------



Mając to na uwadze, LLDP-MED definiuje interakcję LLDP-MED Fast Start pomiędzy protokołem a warstwami aplikacji na górze protokołu, w celu osiągnięcia tych powiązanych właściwości. Początkowo, urządzenie łączności sieciowej (ang. Network Connectivity Device) będzie przesyłać LLDP TLV tylko w LLDPDU. Dopiero po wykryciu urządzenia końcowego LLDP-MED, sieciowe urządzenie łączności z obsługą LLDP-MED zacznie rozgłaszać LLDP-MED TLV w wychodzących LLDPDU na powiązanym interfejsie. Aplikacja LLDP-MED tymczasowo przyspieszy transmisję LLDPDU, aby startowała w ciągu sekundy, gdy zostanie wykryty nowy sąsiad LLDP-MED, aby jak najszybciej udostępnić informacje LLDP-MED nowym sąsiadom.

Ponieważ istnieje ryzyko utraty ramki LLDP podczas transmisji między sąsiadami, zaleca się wielokrotne powtarzanie transmisji szybkiego startu, aby zwiększyć możliwość odbioru ramki LLDP przez sąsiadów. Dzięki licznikowi powtórzeń można określić liczbę powtórzeń transmisji szybkiego startu. Zalecana wartość to 4 razy, biorąc pod uwagę, że po odebraniu ramki LLDP z nowymi informacjami zostaną przesłane 4 ramki LLDP z 1-sekundowym odstępem.

Należy zauważyć, że LLDP-MED i mechanizm szybkiego startu LLDP-MED są przeznaczone wyłącznie do działania na łączach między urządzeniami łączności sieciowej LLDP-MED a urządzeniami końcowymi i jako takie nie dotyczą łączy między elementami infrastruktury LAN, w tym urządzeń łączności sieciowej lub innych rodzajów łączy.

Transmit TLVs

Istnieje możliwość wybrania, które informacje LLDP-MED będą przesyłane do sąsiadów. Gdy pole wyboru jest zaznaczone, informacje są zawarte w ramce przesyłanej do sąsiada.

Interface - Nazwa interfejsu, którego dotyczy konfiguracja.

Capabilities - Gdy zaznaczone, możliwości przełącznika są zawarte w przesyłanych informacjach LLDP-MED.

Policies - Po zaznaczeniu tej opcji, skonfigurowane zasady dotyczące interfejsu są zawarte w przesyłanych informacjach LLDP-MED.

Location - Po zaznaczeniu tej opcji, informacje o lokalizacji przełącznika są zawarte w przesyłanych informacjach LLDP-MED.

PoE - Po zaznaczeniu tej opcji, informacje o skonfigurowanym interfejsie PoE (Power Over Ethernet) są zawarte w przesyłanych informacjach LLDP-MED.

Coordinates Location

Latitude – Szerokość geograficzna POWINNA być znormalizowana w zakresie 0-90 stopni z maksymalnie 4 cyframi. Możliwe jest określenie kierunku na północ od równika lub na południe od równika.

Longitude – Długość geograficzna POWINNA być znormalizowana w zakresie 0-180 stopni z maksymalnie 4 cyframi. Możliwe jest określenie kierunku na wschód od południka głównego lub na zachód od południka głównego.

Altitude – Wysokość NALEŻY znormalizować w zakresie od -2097151,9 do 2097151,9.

Można wybrać jeden z dwóch typów wysokości (piętra lub metry).

Meters: reprezentujące metry wysokości nad poziomem morza definiowane przez określony pionowy układ odniesienia.

Floors: Przedstawianie wysokości w bardziej adekwatnej formie w budynkach o różnych wymiarach między kondygnacjami. Wysokość = 0,0 ma znaczenie nawet poza budynkiem i reprezentuje poziom gruntu na danej szerokości i długości geograficznej. Wewnątrz budynku 0,0 oznacza poziom podłogi powiązany z poziomem gruntu przy głównym wejściu.

Map Datum – Układ odniesienia mapy jest używany dla współrzędnych podanych w tych opcjach:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Nazwa głównego południka: Greenwich.

NAD83/NAVD88: North American Datum 1983, kod CRS 4269, nazwa południka zerowego: Greenwich; Powiązany pionowy układ odniesienia to North American Vertical Datum of 1988 (NAVD88). Ta para punktów odniesienia ma być używana podczas odwoływania się do lokalizacji na lądzie, a nie w pobliżu wód pływowych (co wymagałoby użycia Datum = NAD83/MLLW).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	65/147
------	------	-----------------------------------	------------	--------



NAD83/MLLW: North American Datum 1983, kod CRS 4269, nazwa południka zerowego: Greenwich; Powiązanym pionowym układem odniesienia jest Mean Lower Low Water (MLLW). Ta para punktów odniesienia ma być używana podczas odwoływania się do lokalizacji na wodzie/morzu/oceanach.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). Całkowita liczba znaków dla połączonych informacji o adresie obywatelskim nie może przekraczać 250 znaków.

Kilka uwag dotyczących ograniczenia do 250 znaków:

1) Niepuste miejsce w adresie miejskim będzie zawierało 2 dodatkowe znaki oprócz tekstu lokalizacji adresu miejskiego.

2) Dwuliterowy kod kraju nie jest częścią ograniczenia 250 znaków.

Country code - Dwuliterowy kod kraju ISO 3166 zapisany dużymi literami ASCII - przykład: DK, DE lub US.

State - Jednostki krajowe (stan, kanton, region, prowincja, prefektura).

County - Habstwo, gun (Japonia), dystrykt.

City - Miasto, miasteczko, shi (Japonia) - przykład: Kopenhaga.

City district - Podział miasta, dzielnica, okręg, chou (Japonia).

Block (Neighborhood) - Okolica, blok.

Street - Ulica. Przykład:Polna.

Leading street direction - Główny kierunek ulicy. Przykład: N (ang. North-północ).

Trailing street suffix - Przykład: SW.

Street suffix - Przykład: Ave, Platz.

House no. - Numer domu - Przykład: 21.

House no. Suffix – Suffix numeru domu - Przykład: A, 1/2.

Landmark – Punkt orientacyjny - Przykład: Columbia University.

Additional location info - Informacje dodatkowe. Przykład: Wschodnie skrzydło.

Name (mieszkaniec i dzierżawca/lokator biura) - Przykład: Jan Kowalski.

Zip code - Kod pocztowy - Przykład: 2791.

Building - Budynek (struktura) - Przykład: Niska biblioteka.

Apartment - Jednostka (Apartament, lokal) - Przykład: Apt 42.

Floor - Przykład: 4.

Room no. - Numer pokoju - Przykład: 450F.

Place type -Rodzaj miejsca - Przykład: biuro.

Postal community name - Nazwa wspólnoty pocztowej - Przykład: Leonia.

P.O. Box – Skrzynka pocztowa (P.O. BOX) - Przykład: 12345.

Additional code – Dodatkowy kod - Przykład: 1320300003.

Emergency Call Service - Usługa połączeń alarmowych - (np. E911 i inne), takie jak zdefiniowane przez TIA lub NENA.

Emergency Call Service - Format danych identyfikatora ELIN jest zdefiniowany w celu przenoszenia identyfikatora ELIN używanego podczas zestawiania połączenia alarmowego do tradycyjnego PSAP opartego na łączu CAMA lub ISDN. Format ten składa się z ciągu cyfr odpowiadających numerowi ELIN używanemu do połączeń alarmowych.

Policies

Network Policy Discovery umożliwia efektywne wykrywanie i diagnozowanie problemów związanych z niezgodnością konfiguracji sieci VLAN, wraz z powiązanymi atrybutami warstwy 2 i warstwy 3, które dotyczą zestawu określonych aplikacji protokołów na tym porcie. Nieprawidłowe konfiguracje zasad sieciowych są bardzo istotnym problemem w środowiskach VoIP, które często powodują pogorszenie jakości głosu lub utratę usług.

Zasady są przeznaczone wyłącznie do użytku z aplikacjami, które mają określone wymagania dotyczące zasad sieciowych w czasie rzeczywistym, takie jak interaktywne usługi głosowe i / lub wideo.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	66/147
------	------	-----------------------------------	------------	--------



Rozgłaszane atrybuty zasad sieciowych to:

- 1. Identyfikator VLAN warstwy 2 (IEEE 802.1Q-2003),
- 2. Wartość priorytetu warstwy 2 (IEEE 802.1D-2004),
- 3. Warstwa 3 Wartość Differv Code Point (DSCP) (IETF RFC 2474).

Ta polityka sieciowa jest potencjalnie rozgłaszana i powiązana z wieloma zestawami typów aplikacji obsługiwanych na danym porcie. Szczególne typy aplikacji, które są brane pod uwagę to:

- 1. Voice,
- 2. Guest Voice,
- 3. Softphone Voice,
- 4. Video Conferencing,
- 5. Streaming Video,

6. Control / Signalling (warunkowo obsługują oddzielną politykę sieciową dla powyższych typów mediów).

Duże sieci mogą obsługiwać wiele zasad dla VoIP w całej organizacji, i różne zasady dla poszczególnych typów aplikacji. LLDP-MED umożliwia rozgłaszanie wielu zasad na port, z których każda odpowiada innemu typowi aplikacji. Różne porty na tym samych urządzeniach sieciowych mogą anonsować różne zestawy zasad w oparciu o uwierzytelnioną tożsamość użytkownika lub konfigurację portu.

Należy zauważyć, że LLDP-MED nie jest przeznaczony do działania na łączach innych niż między urządzeniami sieciowymi a punktami końcowymi, a zatem nie musi propagować mnóstwa zasad sieciowych, które często działają na z agregowanym łączu wewnętrznym do sieci LAN.

Delete – Zaznaczony checkbox, aby usunąć zasadę. Zostanie ona usunięta podczas następnego zapisu.

Policy ID - Identyfikator zasady. Jest generowany automatycznie i będzie używane podczas wybierania polityk, które mają być mapowane na określone interfejsy.

Application Type - Przeznaczenie typów aplikacji:

1. Voice - do użytku przez dedykowane telefony IP i inne podobne urządzenia obsługujące interaktywne usługi głosowe. Urządzenia te są zazwyczaj instalowane w oddzielnej sieci VLAN, co ułatwia ich wdrożenie i zwiększa bezpieczeństwo poprzez odizolowanie od aplikacji wykorzystujących dane.

2. Voice Signalling (warunkowy) - do stosowania w topologiach sieci, które wymagają innej polityki w zakresie sygnalizacji głosowej niż w przypadku mediów głosowych. Ten typ aplikacji nie powinien być rozgłaszany, jeśli stosuje się wszystkie te same zasady sieciowe, które są stosowane w polityce aplikacji głosowych.

3. Guest Voice - obsługuje oddzielną usługę głosową "o ograniczonej funkcjonalności" dla użytkowników gości i gości posiadających własne telefony IP i inne podobne urządzenia obsługujące interaktywne usługi głosowe.

4. Guest Voice Signalling (warunkowy) - do stosowania w topologiach sieci, które wymagają innych zasad sygnalizacji guest voice niż w przypadku mediów guest voice. Ten typ aplikacji nie powinien być rozgłaszany, jeśli wszystkie te same zasady sieciowe mają zastosowanie do tych samych zasad, które są rozgłaszane w zasadach dotyczących aplikacji guest voice.

5. Softphone Voice - do użytku przez aplikacje typu softphone na typowych urządzeniach skoncentrowanych na danych, takich jak komputery PC lub laptopy. Ta klasa punktów końcowych często nie obsługuje wielu sieci VLAN, jeśli w ogóle, i są zwykle skonfigurowane do korzystania z "nieoznakowanej" (untagged) sieci VLAN lub pojedynczej "oznaczonej"(tagged) sieci VLAN dla określonych danych. Gdy zasada sieci jest zdefiniowana do użytku z nietagowaną (untagged) siecią VLAN (patrz flaga oznaczona poniżej), pole priorytetu L2 jest ignorowane i tylko wartość DSCP ma znaczenie.

6. Video Conferencing - do użytku przez dedykowany sprzęt do wideokonferencji i inne podobne urządzenia obsługujące interaktywne usługi wideo / audio w czasie rzeczywistym.

7. Streaming Video - do użytku w przypadku dystrybucji treści wideo w oparciu o broadcast lub multicast i inne podobne aplikacje obsługujące usługi przesyłania strumieniowego wideo, które wymagają specjalnego traktowania zasad sieciowych. Aplikacje wideo korzystające z protokołu TCP z buforowaniem nie są właściwe do tego typu aplikacji.

REV.	INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.0	REV.	2024.01.04	67/147	
REV.	INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.0	REV.	2024.01.04	67/14	7



8. Video Signalling (conditional) - do użytku w topologiach sieciowych, które wymagają oddzielnych zasad dla sygnalizacji wideo niż dla mediów wideo. Ten typ aplikacji nie powinien być rozgłaszany, jeśli mają zastosowanie wszystkie te same zasady sieciowe, które są ogłaszane w zasadach aplikacji do wideokonferencji.

Tag – Tag wskazujący, czy określony typ aplikacji używa sieci VLAN z opcją "tagged" czy "untagged".

Untagged oznacza, że urządzenie używa nieoznakowanego formatu ramki i nie zawiera nagłówka znacznika, zgodnie z definicją IEEE 802.1Q-2003. W takim przypadku zarówno identyfikator sieci VLAN, jak i pola priorytetu warstwy 2 są ignorowane, a znaczenie ma tylko wartość DSCP.

Tagged oznacza, że urządzenie używa formatu ramki ze znacznikami IEEE 802.1Q i że używane są zarówno identyfikator VLAN ID, jak i wartości priorytetu warstwy 2, a także wartość DSCP. Format ze znacznikami zawiera dodatkowe pole, nazywane nagłówkiem tagu. Format ramki ze znacznikami obejmuje również ramki ze znacznikami priorytetowymi, zgodnie z definicją IEEE 802.1Q-2003.

VLAN ID – identyfikator VLAN (VID) dla interfejsu zdefiniowanego w IEEE 802.1Q-2003.

L2 Priority - Priorytet L2 to priorytet warstwy 2 używany dla określonego typu aplikacji. Priorytet L2 może określać jeden z ośmiu poziomów priorytetu (od 0 do 7), zgodnie z definicją IEEE 802.1D-2004. Wartość 0 oznacza użycie domyślnego priorytetu zdefiniowanego w IEEE 802.1D-2004.

DSCP - wartość DSCP, która ma być używana do zapewnienia zachowania węzła Diffserv dla określonego typu aplikacji, zgodnie z definicją w IETF RFC 2474. DSCP może zawierać jedną z 64 wartości punktów kodowych (od 0 do 63). Wartość 0 oznacza użycie domyślnej wartości DSCP zdefiniowanej w dokumencie RFC 2475.

Adding a new policy – Kliknij, aby dodać nową politykę. Określ typ aplikacji, znacznik, identyfikator sieci VLAN, priorytet L2 i DSCP dla nowej zasady. Kliknij "Zapisz". Liczba obsługiwanych zasad to 32 Policies Interface Configuration - Każdy interfejs może ogłaszać unikalny zestaw zasad sieciowych lub różne atrybuty dla tych samych zasad sieciowych, w oparciu o uwierzytelnioną tożsamość użytkownika lub konfigurację interfejsu.

Interface - Nazwa interfejsu, którego dotyczy konfiguracja.

Policy Id - Zestaw polityk, które będą miały zastosowanie do danego interfejsu. Zestaw polityk wybiera się, zaznaczając pola wyboru odpowiadające politykom.

5.29 FUNKCJONALNOŚĆ SYNCHRONIZACJI CZĘSTOTLIWOŚCI SYNCE (OPCJA W WYBRANYCH PRZEŁĄCZNIKACH)

SyncE to skrót od Synchronous Ethernet. Funkcja służy do synchronizacji częstotliwości zegara w sieci pomiędzy przełącznikami oraz urządzeniami podłączonymi do interfejsów przełącznika posiadających funkcję SYNCE. Nie należy mylić z precyzyjną synchronizacją czasu (IEEE 1588).

Uwaga! Funkcja SyncE w Hyperion-200, Hyperion-402 i Hyperion-500 jest obecnie wspierana tylko na portach optycznych w slotach SFP. Obsługa SYNCE dla portów elektrycznych UTP będzie dostępna w przyszłości.

REV. 1	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	68/147
--------	------	-----------------------------------	------------	--------



SyncE	Configuration
-------	---------------

Clock Source	Nomination	and	State
--------------	------------	-----	-------

Clock Source	Nominate	d		Port	Priority	SSM Over	write	Hold Off	ANE	EG mode		LOC	S S	SM V	VTR	WTR Value	Clear WTR
1	<	GPS	-Slot8	~	0 🗸	Disable	ed 🗸	Disabled 🗸	None	~		•				0	Clear
2		10Gi	gabitEtherne	et 1/1 🗸	0 🗸	Disable	ed 🗸	Disabled 🗸	None	~			(Clear
Clock Selection	Mode and	State															
	Mode So	urce W	/TR Time	SSM H	old Over	SSM Free	Run	SSM Chassis	s Synce	State	Clock	Source	LOL	DHC	DLD		
Auto Revertive	~	1 🗸	1M 🗸	Det	fault 🗸	Default	~	Defa	ult 🗸	Locked		1					
Station Clock Co	onfiguratio	n															
Clock input fre	quency (Clock ou	tput freque	ency													
Dis	abled 🗸		Disable	ed 🗸													
Save Reset																	
SyncE Ports							_										
F	Port SSN	Enable	Tx SSM	Rx SS	M 1000	BaseT Mode											
GigabitEthernet	1/17	~	QL PRC	QL LIN	IK	Master	r										
10GigabitEtherne	t 1/1					Master	r										
10GigabitEtherne	t 1/2					Master	r										
10GigabitEtherne	t 1/3					Master	r										
10GigabitEtherne	t 1/4					Master	r										
GigabitEtherne	t 1/1					Master	r										
GigabitEtherne	t 1/2					Master	r										
GigabitEtherne	t 1/3					Master	r I										
PTP Ports (8265	.1)																
Instance Rx 1 QL N 2 OL N	SSM F	TSF sable															



Częstotliwość zegara możemy odtwarzać z rożnych źródeł takich jak slot wyposażony w moduł GPS lub bezpośrednio z portu optycznego.

Clock Source Nomination and State

Dla każdego możliwego źródła zegara można skonfigurować następujące elementy.

Clock Source - To jest numer instancji źródła zegara. Należy to uwzględnić przy wyborze trybu "Manual".

Nominated - Po wyznaczeniu źródła sygnału zegarowego, wyjście zegara z odpowiedniego PHY (Port) jest odblokowywane względem sterownika zegarowego. Dzięki temu jest ono dostępne jako możliwe źródło w procesie wyboru zegara. Jeśli jest ono obsługiwane przez rzeczywistą konfigurację sprzętową, wejście zegara stacji może być wyznaczone jako źródło zegara.

Port - W tej rozwijanej ramce przedstawione są porty, które można wybrać dla tego źródła zegara. Synce obsługuje wejście zegara stacji 10MHz. Ograniczenia płyty Serval2 NID: Port 5-12 może być skonfigurowany dla prędkości 100M, 1G lub 2.5G. W trybie prędkości 2,5G sprzęt SyncE nie jest w stanie zalokować, ponieważ odzyskana częstotliwość wyjściowa zegara nie pasuje do opcji częstotliwości sprzętowej SyncE.

Uwaga! Funkcja SyncE w Hyperion-200, Hyperion-402 i Hyperion-500 jest obecnie wspierana tylko na portach optycznych w slotach SFP.

Priority - Priorytet źródła zegara. Liczba 0 jest najwyższym priorytetem. Jeśli dwa źródła zegarowe mają ten sam priorytet, wtedy źródło numer 1 ma najwyższy priorytet w procesie wyboru zegara.

SSM Overwrite – Funkcja nadpisywania jakości zegara (QL) dla wszystkich portów z pominięciem otrzymanego QL w SSM. Jeśli dla nominowanego portu QL nie jest odbierany w SSM (funkcja SSM nie jest włączony na tym porcie), SSM Overwrite QL nadpisuje jakość zegara i umożliwia synchronizację przełącznika. Wstawienie wartości QL w tym polu spowoduje wysyłanie tej jakości zegara do sieci na portach nominowanych w funkcji SSM. W przypadku gdy przełącznik jest wyposażony w moduł GNSS i nominowane jest źródło z modułu GNSS nie należy ustawiać w tym polu żadnej wartości, ponieważ GNSS zawsze rozsyła zegar z najwyższa jakością PRC.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	69/147
------	------	-----------------------------------	------------	--------



Hold Off - Wartość zegara Hold Off. Utrata zegara źródła zostanie opóźniona o wybraną ilość czasu. Selektor zegara nie zmieni źródła zegara, jeśli stan utraty źródła zegara zostanie usunięty w określonym czasie.

ANEG Mode - Dotyczy to tylko portów 1000BaseT. Aby odzyskać zegar z portu, należy go wynegocjować w tryb "Slave". W celu dystrybucji zegara port musi być negocjowany w trybie "Master".

Te różne tryby ANEG można aktywować na porcie źródła zegara:

Prefer Slave: Jeśli to możliwe, port będzie negocjowany w tryb "Slave".

Prefer Master: Jeśli to możliwe, port będzie negocjowany w trybie "Master".

Forced Slave: Port zostanie zmuszony do przejścia w tryb "Slave".

Wybrany port w stanie "Locked" będzie zawsze negocjowany jako "Slave", jeśli to możliwe.

LOCS – Sygnalizacja utraty sygnału na tym źródle zegara.

SSM – Sygnalizacja poprawności odbioru SSM (jest włączony) . Rodzaj błędu zostanie wskazany w polu "Rx SSM"

WTR (ang. Wait to Restore) - Licznik czasu oczekiwania na przywrócenie zegara.

Clear WTR - Czyści licznik WTR i udostępnia to źródło zegara dla procesu wyboru zegara.

Clock Selection Mode and State

Selektor Zegarów jest tylko w jednej instancji - tej, która wybiera pomiędzy nominowanymi źródłami zegara.

Mode - Definicja "najlepszego" źródła zegara to po pierwsze to, które ma najwyższy QL, a po drugie (w przypadku równych QL) najwyższy priorytet.

Selektor zegara może być w różnych trybach:

Manual: Selektor zegara wybierze źródło zegara podane w źródle (patrz poniżej). Jeśli to ręcznie wybrane źródło zegara zawiedzie, selektor zegara przejdzie w stan Hold Over.

Manual To Selected: Tak samo jak tryb ręczny, w którym wybrane źródło zegara staje się źródłem.

Auto NonRevertive: Wybór najlepszego źródła zegara jest dokonywany tylko wtedy, gdy wybrany zegar zawiedzie.

Auto Revertive: Wybór najlepszego źródła zegara jest stale dokonywany.

Force Hold Over: Selektor zegara jest zmuszony do utrzymywania stanu Hold Over.

Force Free Run: Selektor zegara jest zmuszony do trybu Free Run.

Source - Istotny tylko wtedy, gdy wybrany jest tryb ręczny (patrz wyżej).

WTR Time - WTR to wartość licznika czasu oczekiwania na przywrócenie w minutach. Czas WTR jest aktywowany po awarii źródła zegara (w trybie Revertive). Oznacza to, że źródło zegara jest dostępne do wyboru po czasie WTR (można go wyczyścić).

SSM Hold Over - Jest to przekazywana wartość QL SSM, gdy selektor zegara znajduje się w stanie Hold Over.

SSM Free Run - Jest to przekazywana wartość QL SSM, gdy selektor zegara znajduje się w stanie Free Run.

State - Wskazuje stan selektora zegara. Możliwe stany to:

Free Run: Brak zewnętrznych źródeł zegara do powiązania. Selektor zegara nigdy nie był powiązany ze źródłem zegara na tyle długo, aby obliczyć przesunięcie częstotliwości względem lokalnego oscylatora.

Hold Over: Nie ma zewnętrznych źródeł zegara do powiązania (stan niepowiązany). Selektor zegara obliczył przesunięcie częstotliwości do lokalnego oscylatora. Częstotliwość tego węzła jest utrzymywana na częstotliwości źródła zegara poprzednio powiązanego.

Locked: Przełącznik zegara jest powiązany ze wskazanym źródłem zegara (patrz dalej).

Top: Selektor zegara jest zablokowany na czas w pakietach, np. PTP

Clock Source - Źródło zegara jest zalokowane, gdy przełącznik zegara jest w stanie "Locked". **LOL** - Sygnalizacja alarmu Los Of Lock.

DHOLD – Sygnalizacja obliczenia przesunięcia częstotliwości podtrzymania dla lokalnego oscylatora. Staje się aktywne przez około 10 sekund, gdy wybierane jest nowe źródło zegara.

 REV.
 1.06
 INSTRUKCJA OBSŁUGI : HYPERION-GUI
 2024.01.04
 70/147



Station Clock Configuration

Moduł Synce może mieć wejście stacyjne zegara i / lub wyjście stacyjne zegara.

Clock input frequency - Jeśli jest obsługiwany przez Synce HW, można skonfigurować częstotliwość wejściową zegara stacji, możliwe częstotliwości to: 1544 MHz, 2048 MHz lub 10 MHz **Clock Output frequency** - Jeśli jest obsługiwana przez Synce HW, częstotliwość wyjściowa zegara stacji może być skonfigurowana, możliwe częstotliwości to: 1544 MHz, 2048 MHz lub 10 MHz

SyncE Ports

Dla każdego możliwego portu przełącznika.

Port - Numer portu do skonfigurowania.

SSM Enable - Włączanie i wyłączanie funkcji SSM na tym porcie.

Tx SSM - Monitorowanie przesyłanych SSM QL na tym porcie. Przesyłana QL powinna być poziomem jakości zegara generowanego przez ten węzeł. Oznacza to, że QL źródła zegara, z którym powiązany jest ten węzeł

Rx SSM - Monitorowanie odebranych SSM QL na tym porcie. Jeśli łącze nie działa na porcie, wskazywany jest QL_LINK. Jeśli nie zostanie odebrany żaden SSM, wskazywany jest QL_FAIL

1000BaseT Mode - Jeśli PHY jest w trybie 1000BaseT, to monitoruje tryb master / slave. Aby odbierać zegar na porcie, musi być w trybie slave. Aby nadawać zegar na porcie, musi być w trybie master

5.30 Protokoły do redundancji drogi przesyłowej

Przełączniki **HYPERION** oferują kilka protokołów zapewniających redundancję drogi przesyłowej, a są to:

- STP Spanning Tree Protocol,
- **RSTP** Rapid Spinning Tree Protocol,
- MSTP Multiple Spanning Tree Protocol,
- LACP (Link Aggregation Control Protocol), protokół powszechnie stosowany do agregacji połączeń, ale może również być używany do zapewnienia redundancji drogi przesyłowej,
- **ERPS** protokół zapewniający redundancję drogi przesyłowej dla przełączników pracujących w topologii pierścienia i multipierścienia zgodny z zaleceniem ITU-T G.8032,
- **CHAIN** praca w trybie łańcucha zapewniająca redundancję drogi przesyłowej dla przełączników połączonych w łańcuch dołączony w dwóch punktach końcowych do sieci Ethernet.

5.30.1 Redundancja drogi przesyłowej z wykorzystaniem Spanning Tree Protocol

Protokół umożliwiający ochronę sieci przed skutkami pętli, a przy połączeniu przełączników w ringi zapewniający redundancję sieci. Podstawowa i zaawansowana konfiguracja protokołu STP przedstawiono poniżej.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	71/147
------	------	-----------------------------------	------------	--------



STP Bridge Configuration

Protocol version	MSTP	MSTP V
Bridge Priority	128	 STP
Hello Time	2	RSTP
Forward Delay	15	MSTP
Max Age	20	
Maximum Hop Count	20	
Transmit Hold Count	6	
Advanced Settings	ing 📃	
Advanced Settings Edge Port BPDU Filter Edge Port BPDU Guar	ing 🗌	
Advanced Settings Edge Port BPDU Filter Edge Port BPDU Guar Port Error Recovery	ing O	

Rys. 83. Podstawowa i zaawansowana konfiguracja protokołu STP.

5.30.2 Konfiguracja mapowania MSTI

Funkcja umożliwiająca użytkownikowi sprawdzenie aktualnej konfiguracji lub zmianę priorytetu bridge dla instancji MSTI oraz dla mapowanych VLAN-ów przez mapowanie MSTI. Niezmapowane sieci VLAN są mapowane na CIST. (Domyślna instancja Bridge)

MSTI Conf	figuration
Add VLANs s	separated by spaces or comma.
Unmapped V	/LANs are mapped to the CIST. (The default bridge instance).
Configurati	ion Identification
Configura Configura	ation Name02-00-c1-93-4a-5fation Revision0
MSTI Map	ping
MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save Reset

Rys. 84. Okno do konfiguracja mapowania MSTI

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	72/147
------	------	-----------------------------------	------------	--------


5.30.3 Konfiguracja priorytetów MSTI

Strona umożliwia konfigurację priorytetów MSTI

MSTI Pri	ority Configu	ratio
MSTI	Priority]
*	< ▼]
CIST	128 🔻	
MSTI1	128 🔻	
MSTI2	128 🔻	1
MSTI3	128 🔻	
MSTI4	128 🔻	
MSTI5	128 🔻	
MSTI6	128 🔻	
MSTI7	128 🔻	

Rys. 85.Okno do konfiguracja priorytetów MSTI.

5.30.4 Konfiguracja STP CIST na portach przełącznika

Stronie umożliwia między innymi włączenie/wyłączenie STP na wybranych portach oraz określenie kosztu trasy, priorytetu CIST, konfiguracja Edge, włączenie na poszczególnych portach ochrony BPDU.

STI	P CIST Port Configur	ation											
- (CIST Aggregated Port Config	uration											
	Interface	STP Enabled			Path Cost	Priority	Admin Edge	Auto Edge	Rest Role	ricted TCN	BPDU Guard	Point- po	-to- bint
	-	4	Auto	۲		128 🔻	Non-Edge ▼	1				Forced True	۲
(CIST Normal Port Configuration												
	Interface	STP Enabled			Path Cost	Priority	Admin Edge	Auto Edge	Rest Role	ricted TCN	BPDU Guard	Point- po	-to- bint
	*	«	\diamond	۲		< ▼	<> ▼					\diamond	۲
	10GigabitEthernet 1/1		Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	10GigabitEthernet 1/2	1	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	10GigabitEthernet 1/3	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	10GigabitEthernet 1/4	se a la constante de la consta	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/1	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/2	4	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/3	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/4	1	Auto	۲		128 🔻	Non-Edge ▼	1				Auto	۲
	GigabitEthernet 1/5	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/6	st.	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/7	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/8	ø	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/9	\$	Auto	۲		128 🔻	Non-Edge ▼					Auto	۲
	GigabitEthernet 1/10	1	Auto	۲		128 🔻	Non-Edge ▼	\$				Auto	۲

Rys. 86. Okno konfiguracji STP CIST na portach fizycznych

5.30.5 Konfiguracja STP MSTI na portach przełącznika

Na stronie dostępne jest konfiguracja wirtualnego portu MSTI, który jest tworzony oddzielnie dla każdego aktywnego portu CIST (fizycznego) dla każdej skonfigurowanej instancji MSTI i mającej

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	73/147
------	------	-----------------------------------	------------	--------



zastosowanie do portu. Instancja MSTI musi zostać wybrana przed wyświetleniem rzeczywistych opcji konfiguracji portu MSTI.

ST1 MSTI Port Cont	figuration									
Port	Path Cost	Priority 128 T								
MSTI Normal Ports Configuration										
Port		Path Cost	Priority							
*	< ▼		< ▼							
10GigabitEthernet 1/1	Auto 🔻		128 🔻							
10GigabitEthernet 1/2	Auto 🔻		128 🔻							
10GigabitEthernet 1/3	Auto 🔻		128 🔻							
10GigabitEthernet 1/4	Auto 🔻		128 🔻							
GigabitEthernet 1/1	Auto 🔻		128 🔻							
GigabitEthernet 1/2	Auto 🔻		128 🔻							
GigabitEthernet 1/3	Auto 🔻		128 🔻							
GigabitEthernet 1/4	Auto 🔻		128 🔻							
GigabitEthernet 1/5	Auto 🔻		128 🔻							
GigabitEthernet 1/6	Auto 🔻		128 🔻							
GigabitEthernet 1/7	Auto 🔻		128 🔻							
GigabitEthernet 1/8	Auto 🔻		128 🔻							
GigabitEthernet 1/9	Auto 🔻		128 🔻							
GigabitEthernet 1/10	Auto 🔻		128 🔻							
GigabitEthernet 1/11	Auto 🔻		128 🔻							
GigabitEthernet 1/12	Auto 🔻		128 🔻							

Rys. 87.Okno konfiguracji STP MSTI na portach fizycznych

5.31 Redundancja drogi przesyłowej w topologii pierścienia zgodnie z ITU-T G.8032

Sieć w topologii pierścienia można budować z urządzeń **HYPERION** bez ograniczeń ilościowych. Do budowy pierścienia można używać dowolnych dwóch portów przełącznika. Szczegółowy opis konfiguracji ringu w urządzeniach **HYPERION** opisuje instrukcja do pobrania klikając na odpowiedni link z punktu **8.1**

Blokowanie portów przełącznika dla danych przychodzących i wychodzących jest realizowana przez dodawanie lub usuwanie z tablicy VLAN odpowiednich wpisów. W trybie którym, przełącznik pracuje z ramkami targowanymi na portach tworzących pierścień, należy bezwzględnie podczas konfiguracji pierścienia dodać informacje o wszystkich używanych numerach sieci VLAN. Pominięcie wpisania do konfiguracji danego VLAN spowoduję, że dla tej sieci VLAN nastąpi zapętlenie i uniemożliwi pracę urządzeń komunikujących się w ramach tego VLAN, jak również spowoduje zakłócenie pracy pozostałych VLAN przez przeciążenie przełącznika pakietami rozgłoszeniowymi, które przemieszczają się w ramach tej nie dodanej sieci VLAN.

5.31.1 Konfiguracja protokołu protekcji drogi transmisyjnej w topologii pierścienia zgodnie z ITU-T G.8032

Przed przystąpieniem do konfiguracji protokołu redundancji, należy skonfigurować punkty MEP (Maintenance Entity Point) dla każdego portu urządzenia tworzącego pierścień. Podczas tej konfiguracji podaje się, w jaki sposób dany port ma dokonywać detekcji awarii na tym połączeniu, czy przez wykrycie zaniku fizycznego sygnału, czy przez wykrycie zaniku odbierania ramek

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 74/147	7
---	---



Continuity Check Message CCM. Poza tą konfiguracją ustawia się również transmisję ramek R-APS i numer VLAN dla tych pakietów.

Dostep do konfiguracji jest pod linkiem Configuration \rightarrow MEP. Dodanie nowego punkty jest możliwe przez naciśnięcie przycisku Add New MEP, po czym pojawi się rząd pól, które należy uzupełnić o właściwe parametry. Znaczenie poszczególnych pól jest następujące:

Delete – podczas wprowadzania parametrów, w tym polu widoczny jest przycisk, naciśnięcie go spowoduje usunięcie danego rzędu wraz z parametrami, podobnie działa przycisk Reset. Po zatwierdzeniu parametrów w tym polu pojawi sie pole typu checkbox. Zaznaczenie tego pola i wciśniecie przycisku Save również spowoduje usuniecie danego punktu MEP.

Instance – numer identyfikacyjny punku MEP,

Domain – domena jaką będzie dany punkt monitorował. Port oznacza monitorowanie fizycznego portu w urządzeniu, EVC monitorowanie Ethernet Virtual Conection.

Mode – Typ punktu: Mep – punkt końcowy, Mip – punkt pośredni.

Direction – kierunek monitorowania: **Down** (**Ingress**) – wejściowy, **Up** (**Egress**) – wyjściowy.

Residence Port – numer portu który ma być monitorowany w przypadku wybrania Domain jako Port, gdy Domain jest EVC należy wpisać 0.

Level – MEG Level.

Flow Instance – W przypadku, gdy Domain jest ustawione jako Port należy wpisać numer fizycznego portu, którego dotyczy ten punkt MEP tak samo jak w przypadku Residence Port, gdy **Domain** jest **EVC** to należy wpisać numer grupy **EVC**.

Tagged VID – numer VLAN z jakim ramki CCM i RAPS będą nadawane. Ten numer VLAN musi być dodany do obsługiwanych VLAN przez dany proces ERPS, dla którego ten punkt MEP jest skonfigurowany.

This MAC – pole informacyjne wyświetla źródłowy adres MAC dla ramek wysyłanych przez ten punkt MEP, adres ten dotyczy ramek CCM, R-APS i L-APS.

Alarm – graficzna informacia o wystapieniu alarmu

Po zakończeniu wprowadzania wszystkich parametrów należy kliknąć przycisk Save, który zapiszę daną konfigurację w pamięci nieulotnej. Jednocześnie można wprowadzić tylko jeden punkt MEP.

Maintenance Entity Point										
Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
	<u>1</u>	Port	Мер	Down	1	0		105	00-50-C2-0E-33-A6	
	2	Port	Мер	Down	2	0		105	00-50-C2-0E-33-A7	•
	<u>3</u>	Port	Мер	Down	1	0		105	00-50-C2-0E-33-A6	•
	<u>4</u>	Port	Мер	Down	2	0		105	00-50-C2-0E-33-A7	•
Delete	5	Port 🔻	Mep 🔻	Down 🔻	1	0	1	0		
				Down						
Add New	MEP	ave Rese	et	Up						

Rys. 88. Konfiguracja ogólna punktów MEP

Wprowadzenie szczegółowej konfiguracji punktów MEP jest możliwe przez menu szczegółowej konfiguracji punktów MEP, dostęp do tego menu jest możliwy przez klikniecie na numer ID danego punktu MEP w kolumnie Instance.

Znaczenie pól nieopisanych wcześniej jest następujące:

Format – sposób formatowania w ramce CCM informacji o danym punkcie MEP, Dostępny wybór to ITU ICC, gdzie użytkownik może wprowadzić swoje dane w polu ICC/Domain Name o długości 6 znaków i w polu MEG id o długości 7 znaków, IEEE String dane w polu ICC/Domain Name mogą mieć długość 8 znaków i taka sama długość w polu MEP Id.

ICC/Domain Name – dane z tego pola będą umieszczane w ramkach CCM,

MEG id – dane z tego pola będą umieszczane w ramkach CCM,

MEP id – identyfikator punktu MEP również umieszczany w ramkach CCM,

W dalszej kolejności umieszczone są sygnalizacje podstawowych parametrów łącza, zielone kółko oznacza brak alarmu, natomiast czerwone oznacza alarm.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	75/147
------	------	-----------------------------------	------------	--------



cLevel – odebrana ramka CCM zawiera pole level o poziomie niższym niż zostało to skonfigurowane w danym punkcie MEP,

cMEG – odebrana ramka CCM zawiera pole MEG ID nie zgodne z konfiguracją danego punktu MEP,

cMEP – odebrana ramka CCM zawiera pole MEP ID nie zgodne z konfiguracją danego punktu MEP, **cAIS** – odebrano ramkę CCM ze znacznikiem AIS (Alarm Indication Signal),

cLCK - odebrano ramkę CCM ze znacznikiem LCK (Locked Signal Function),

cSSF – zanik sygnału warstwy fizycznej,

aBLK - włączono blokowanie ramek CCM danego punktu MEP,

aTSF – informacja o awarii łączą obsługiwanego przez dany punkt MEP została przekazana do procesu zajmującego się uruchomianiem protekcji drogi transmisyjnej.

cLOC – informacja o braku odebrania ramek CCM przez okres dłuższy niż 3,5 okresu nadawania ramek CCM,

cRDI – odebrano ramkę CCM ze znacznikiem RDI (Remote Defect Indication),

cPerdiod – odebrano ramki CCM, ale z okresem innym niż to zostało skonfigurowane w danym punkcie MEP,

cPriority – odebrano ramki CCM, ale z ustawionym priorytetem innym niż to zostało skonfigurowane w danym punkcie MEP,

MEP Configuration
Instance Data
Instance Domain Mode Direction Residence Port Flow Instance Tagged VID EPS Instance This MAC 1 Port Mep Down 1 105 1 00-50-02-0E-33-A6
Instance Configuration
Level Format Domain Name MEG id MEP id Tagged VID Syslog cLevel cMEG cMEP cALS cLCK cLoop cCooffig cDEG cSSF aBLK aTSD aTSF 0 • ITU ICC • ICC000MEG0000 1 105 •
Peer MEP Configuration
Delete Peer MEP ID Unicast Peer MAC cLOC cRDI cPriority 2 00-50-C2-DE-26-2E • • • •
Add New Peer MEP
Functional Configuration
Continuity Check APS Protocol Enable Priority Frame rate TLV Enable Priority Cast Type Last Octet
Fault Management Performance Monitoring
TLV Configuration
Organization Specific TLV (Global) OUI First OUI Second OUI Third Sub-Type Value 0 0 12 1 2
TLV Status
Peer MEP ID CC Organization Specific CC Port Status CC Interface Status OUI First OUI Second OUI Third Sub-Type Value Last RX Value Last RX
Enable
Save Reset

Rys. 89. Konfiguracja szczegółowa punktów MEP.

Peer MEP ID – oczekiwana wartość pola MEP ID odbieranych ramek CCM,

Unicast Peer MAC – MAC adres używany jako źródłowy w CCM, gdy wybrano typ ramek jako unicast. Domyślnie ramki CCM wysyłane są jako multicast i nie ma wprowadzonego żadnego adresu MAC, aby tego dokonać należy kliknąć na przycisk **Add New peer MEP**, następnie wpisać wszystkie dane i kliknąć przycisk **Save**.

Kolejne punku konfiguracji poniżej napisu: **Functional Configuration** dotyczą już sposobu wykrywania przerwy w łączu i typu ramek utrzymaniowych,

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	76/147
------	------	-----------------------------------	------------	--------



Continuity Check

Enable – zaznaczenie tego pola i kliknięcie przycisku **Save** spowoduje rozpoczęcie wysyłania ramek CCM przez przełącznik na porcie, na którym skonfigurowany jest dany punkt MEP, jednocześnie przełącznik rozpoczyna monitorowanie odebranych ramek CCM i w razie stwierdzenia anomalii w ich otrzymywaniu zgłasza alarm. Brak włączenia ramek CCM, sprawi, że dany punkt MEP będzie zgłaszał alarm tylko w sytuacji, gdy nastąpi zanik sygnału w warstwie fizycznej łącza.

Priority – priorytet ramek CCM,

Frame rate – częstotliwość wysyłania ramek CCM,

APS Protocol

Enable – włączenie nadawania ramek utrzymaniowych, R-APS lub L-APS. Jeżeli dany proces realizujący funkcję protekcji drogi transmisyjnej, czy to w topologii RING czy też w topologii liniowej, nie będzie otrzymywał ramek, zgłosi alarm, a wystąpienie przerwy może nie doprowadzić do rekonfiguracji sieci, dlatego też bardzo ważna jest prawidłowa konfiguracja tej opcji.

Priority – priorytet ramek R-APS lub L-APS,

Cast – rodzaj ramek jakie zostają wysłane i tak dla ramek R-APS jest to **Multi** natomiast dla ramek L-APS jest to **Uni**,

Type – typ ramek jakie dany punkt MEP ma wysyłać. Dla protekcji drogi transmisyjnej w topologii pierścienia jest to typ **R-APS**, natomiast dla protekcji drogi w topologii liniowej jest to **L-APS**.

Last Octet – jest to ostatni bajt adresu przeznaczenia MAC ramek R-APS. Zalecenie ITU-T G.8032 podaje adres przeznaczenia multicast dla ramek R-APS 01-19-A7-00-00-XX, gdzie XX oznacza ostatni oktet i może to być wartością dowolna. Wykorzystywany w konfiguracjach dla SUB-RING poprzez zwiększanie wartości o 1 dla MEP'ów w danym sub-ringu.

5.31.2 Konfiguracja procesu protekcji drogi transmisyjnej w topologii pierścienia

Konfiguracja protokołu protekcji drogi transmisyjne w urządzeniach HYPERION po kliknięciu na linki: **Configuration > ERPS**.

Etherne	Ethernet Ring Protection Switching											
Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
	1	1	2	1	2	1	2	Major	No	No	1	
Add New	Add New Protection Group Save Reset											

Rys. 90. Konfiguracja ogólna procesu protekcji.

Dodanie nowej konfiguracji RING polega na kliknięciu przycisku **Add New Protection Group**, wprowadzeniu parametrów pracy układu protekcji i zatwierdzenie przyciskiem **Save**.

Znaczenie poszczególnych pól jest następujące:

Delete – pole typu checkbox, zaznaczenie i kliknięcie przycisku **Save** spowoduje usunięcie danej konfiguracji,

ERPS ID – numer identyfikacyjny dla danej konfiguracji i procesu odpowiedzialnego za protekcję drogi transmisyjnej, każde urządzenie może jednocześnie obsługiwać do 64 procesów i pierścieni.

Port 0 (East Port) – numer pierwszego portu, jaki w danym urządzeniu będzie użyty do budowy pierścienia.

Port 1 (West Port) – numer drugiego portu, jaki w danym urządzeniu będzie użyty do budowy pierścienia.

Port 0 APS MEP – numer identyfikacyjny punktu MEP, którego zadaniem jest wysyłanie ramek utrzymaniowych R-APS dla Port 0.

Port 1 APS MEP – numer identyfikacyjny punktu MEP, którego zadaniem jest wysyłanie ramek utrzymaniowych R-APS dla Port 1.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	77/147



Port 0 SF MEP – numer identyfikacyjny punktu MEP, który ma zgłaszać alarm związany z przerwą ciągłości łącza dla Port 0.

Port 1 SF MEP – numer identyfikacyjny punktu MEP, który ma zgłaszać alarm związany z przerwą ciągłości łącza dla Port 1.

Uwaga: zgłaszanie alarmów i wysyłanie ramek R-APS może dla danej konfiguracji pierścienia prowadzić ten sam punkt MEP jednocześnie.

Ring Type – określa czy dana konfiguracja dotyczy pierścienia głównego (**Major**) czy pobocznego (**Sub**), opcja ta umożliwia tworzenie pierścieni w topologii dual homing,

Interconnected Node – opcja ta informuje proces realizujący protekcję że dane urządzenie jest częścią głównego pierścienia, ale również stanowi miejsce w który następuje odejście pierścienia pobocznego i tworzenie topologii dual doming.

Virtual Channel – opcja ta tworzy wirtualny kanał dla ramek R-APS w pierścieniu Sub.

Major Ring ID – w przypadku konfiguracji pierścienia pobocznego (sub), należy w tym polu podać numer ID pierścienia głównego, do którego ten pierścień jest dołączony.

Alarm – graficzna sygnalizacja czy dany pierścień jest w stanie awarii i zgłasza alarm (czerwony symbol) czy też jest w stanie sprawności (zielony symbol).

Dostęp do szczegółowej konfiguracji pierścienia jest możliwy przez kliknięcie w link znajdujący się w numerze **ID** danego procesu ERPS w kolumnie ERPS ID. Okno konfiguracji szczegółowej jest przedstawione na rysunku 91.

ERPS Configuration 1	Auto-refresh Refresh								
Instance Data									
ERPS ID Port 0 Port 1 Port 0 SF MEP Port 1 SF MEP Port 0 APS MEP Port 1 APS MEP Ring Type									
I I Z I Z I Z Major Ring									
500 1min V 0 VLAN Config									
RPL Configuration									
RPL Role RPL Port Clear RPL_Neighbour Port0 ▼ □									
Instance Command									
Command Port									
Instance State									
Protection Port Port Transmit Port 0 Receive APS Port 1 Receive APS WTR Remaining RPL Un- blocked No APS Port 0 Bloc	k Port 1 Block FOP Status Alarm								
Idle OK OK NR BBPR1 00-50-C2- NR RB BPR1 00-50-C2- 0E-26-2D 0E-26-2D 0 Blocked	Unblocked 🛛 🔵								

Save Reset

Rys. 91. Konfiguracja szczegółowa funkcjonalności protekcji

Znaczenie poszczególnych pól dla okna "Instance Configuration" jest następujące:

Configured – graficzna sygnalizacja poprawności konfiguracji danego pierścienia, zielony symbol oznacza prawidłową konfigurację, a czerwony błędną konfigurację.

Guard Time – czas wstrzymania odbierania ramek R-APS podawany w milisekundach. Urządzenie po zgłoszeniu alarmu w wyniku awarii, a następnie po powrocie połączenia ponownie wyśle informację o powrocie sprawności pierścienia. Po wysłaniu tej informacji odczekuje czas zapisany w tym parametrze za nim zacznie analizować przychodzące ramki R-APS. Domyślna wartość 500 ns jest wartością, która zapewnia poprawną pracę większości pierścieni, zwiększenie tej wartości należy dokonać tylko w przypadku budowy pierścieni o łącznej liczbie przełączników większej niż 100.

WTR Time – (ang. Wait to Restore) czas oczekiwania na przywrócenie podawany z listy wyboru od 1 min. do 12 min. Czas, jaki odmierza urządzenie RPL owner po otrzymaniu informacji o

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	78/147
------	------	-----------------------------------	------------	--------



przywróceniu połączenia, które wcześniej uległo awarii. Po tym czasie RLP owner rozpocznie procedurę rekonfiguracji pierścienia do topologii sprzed awarii, czyli takiej jak jest w stanie idle.

Hold Off Time – czas przetrzymania podawany w krokach co 100ms od 0 do 10 s. Jest to czas jaki urządzenie tworzące pierścień odczekuje po wykryciu awarii, a przed wykonaniem jakiegokolwiek działaniem w reakcji na to zdarzenie. Najlepsze osiągi czasu rekonfiguracji pierścienia uzyskuje, gdy ten parametr jest równy 0.

Version – wybór wersji pracy protokołu zgodnego z zaleceniem ITU-T G.8032, wersja pierwsza **v1** jest zaimplementowana tylko po to, aby zachować kompatybilność wstecz, poza tym ta wersja ma znaczna ograniczenia funkcjonalne i zaleca się w nowych instalacjach stosowanie tylko wersji drugiej **v2** tego protokołu.

Revertive – opcja ta służy do określenia sposobu zachowania się pierścienia po powrocie połączenia po uprzedniej awarii. W przypadku pracy ringu z tą opcją to po przywróceniu połączenia, które uległo wcześniej awarii, RPL owner rozpoczyna po odliczeniu czasu WTR procedurę ponownej rekonfiguracji pierścienia tak, aby połączenie pomiędzy RPL owner, a RPL Neighbour było logiczną przerwą dla danych. W przypadku wyłączenia tej opcji po przywróceniu połączenia, które wcześniej uległo awarii to połączenie staje się logiczną przerwą dla danych na ringu i RPL owner nie dokonuje ponownej rekonfiguracji. Wystąpienie awarii w innym miejscu pierścienia powoduje, że ta przerwa zostaje otworzona dla danych, a nowa przerwa dla przeciwdziałająca powstawaniu pętli w sieci tworzona jest w miejscu, które uległo awarii.

Uwaga! Bardzo ważne jest, aby wszystkie przełączniki pracujące w danym pierścieniu miały tak samo ustawioną opcję Revertive, w przeciwnym wypadku może dojść do błędnego działania protekcji drogi transmisyjnej i utraty danych.

Vlan config – w tym polu znajduje się link, który prowadzi do menu, którego zadaniem jest umożliwienie dodania do konfiguracji pierścienia numerów sieci VLAN, które mają być chronione przez ten pierścień.

ERPS V	LAN Conf	iguration 1
Delete	VLAN ID	
	1	
Add New	Entry Ba	ck
Save	Reset	

W przypadku, gdy porty tworzące pierścień pracują z ramkami targowanymi to należy w tym menu dodać wszystkie numery VLAN na tych portach. Nie dodanie jednego z obsługiwanych VLAN spowoduje powstanie na tym VLAN pętli, a ruch rozgłoszeniowy w ramach tego VLAN, całkowicie uniemożliwi wymianę danych.

Istnieje możliwość stworzenia więcej niż jednego logicznego pierścienia na urządzeniach tworzących takie połączenie, ma to na celu równomierne rozłożenie ruchu w pierścieniu.

W takiej sytuacji tworzymy fizyczny pierścień z urządzeń **HYPERION**, następnie konfigurujemy dwa lub więcej w zależności od potrzeb pierścienie w taki sposób, aby, logiczne przerwy RPL występowały w innych miejscach pierścienia. W tak skonfigurowanym układzie cześć sieci VLAN może chronić jeden logiczny pierścień, a pozostałą cześć drugi. Przykład takiej konfiguracji zostanie przedstawiony w dalszych rozdziałach niniejszej instrukcji obsługi, łącznie z zaletami takiej topologii.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	79/147
------	------	-----------------------------------	------------	--------

Rys. 92. Konfiguracja numerów sieci VLAN dla danego procesu ERPS.



RPL Role – ustala rolę, jaką pełni dany przełącznik w pierścieniu, dostępne opcje to:

None – zwykły przełącznik, którego zadaniem jest tylko sygnalizowanie awarii, takich przełączników w pierścieniu może być nieskończenie wiele.

RPL_Owner – przełącznik zarządca, który steruję pracą pierścienia przez blokowanie lub odblokowywanie połączenie RPL, taki przełącznik w każdym pierścieniu może być tylko jeden.

RPL_Neigbour – przełącznik, który znajduje się przy połączeniu RPL, ale nie jest RPL owner, konfiguracja tego przełącznika pozwala na uniknięcie chwilowego przeciążenia w sieci, jakie się pojawia po rekonfiguracji w momencie wystąpienia awarii w połączeniu RPL.

RPL Port – ustawienie to określa, do którego portu fizycznie w pierścieniu i w danym urządzeniu podłączone jest połączenie RPL.

Clear – zaznaczanie tej opcji i klikniecie przycisku Save spowoduje usunięcie roli, jaką pełni dany przełącznik i wpisanie do konfiguracji roli None.

Command – opcja pozwalająca na wydanie ręcznie komendy dla portu podanego w polu Port dla danego przełącznika. Możliwe opcje komend:

None – brak komendy.

Manual Switch – komenda ta powoduje blokowanie portu podanego w polu Port w danym przełączniku w przypadku gdy nie występuje zanik sygnału, ani nie została wydana komenda **Force Switch**.

Force Switch – komenda ta powoduje blokowanie portu podanego w polu Port w danym przełączniku.

Clear – usuwa działanie poprzednich komend, a także w przypadku pracy pierścienia bez opcji Revertive powoduje powrót logicznej przerwy w pierścieniu do położenia, w którym występuje RPL. Kolejne pola na tej stronie służa tylko do monitorowania stanu pierścienia.

Protection State – stan pierścienia, pierścień może znaleźć się tylko w dwóch stanach stabilnych i w jednym z stanów przejściowych. Możliwe stany to:

Idle – stan pełnej sprawności pierścienia.

Protected – stan awarii jedno lub więcej połączeń w pierścieniu ma przerwę,

Pending – stan przejściowy, który występuje przy przechodzeniu pierścienia ze stanu protected do idle i trwa czas równy WTR. W tym czasie są już sprawne wszystkie połączenia, ale RPL Owner nie dokonał ponownej rekonfiguracji pierścienia zanim nie odliczy czasu WTR.

Port E – stan połączenia portu E tworzącego pierścień, OK – połączenie sprawne, SF – brak połączenia.

Port W – stan połączenia portu W tworzącego pierścień, OK – połączenie sprawne, SF – brak połączenia.

Transmit APS – przedstawia informację z jakim komunikatem wysyła dany przełącznik pakiety R-APS.

Port E Receive APS – wyświetla informację o tym, jaki komunikat niosą pakiety R-APS odbierane na porcie E i adres MAC punktu MEP po drugiej stronie połączenia.

Port W Receive APS – wyświetla informację o tym, jaki komunikat niosą pakiety R-APS odbierane na porcie W i adres MAC punktu MEP po drugiej stronie połączenia.

WTR Remaining – pole aktywne tylko w przełączniku skonfigurowanym, jako RPL owner i przedstawia w stanie pending stan licznika WTR liczącego w dół, wartość wyświetlana jest w ms.

RPL Un-blocked – graficzna wizualizacja stanu blokowania połączenia RPL.

No APS Received – sygnalizacja braku otrzymywania pakietów R-APS, sygnalizacja powiadamia o błędnej konfiguracji przełączników znajdujących się w bezpośrednim otoczeniu tego przełącznika, który ten alarm zgłosił.

Port E Block Status – stan portu E tworzącego pierścień czy jest blokowany **Blocked** lub nie **Unblocked**.

Port W Block Status – stan portu W tworzącego pierścień czy jest blokowany Blocked lub nie Unblocked.

FOP Alarm – sygnalizuje stan, w którym mechanizm protekcji uległ awarii.

REV. 1	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	80/147
--------	------	-----------------------------------	------------	--------



5.31.3 Konfiguracja protekcji drogi transmisyjnej w trybie "CHAIN"

Praca w trybie "CHAIN" umożliwia skonfigurowanie protekcyjnego łańcucha urządzeń dołączanych do sieci LAN. Rozwiązanie to umożliwia szybkie (<20ms) przełączenie na drogę protekcyjną w przypadku przerwania połączenia. Łańcuch dołączany jest do sieci w dwóch punktach (HEAD i TAIL) – połączenie w jednym z tych punktów pozostaje nieaktywne do momentu przerwania transmisji (sygnalizacja z wykorzystaniem komunikatów R-APS). Przełącznik HYPERION umożliwia stworzenie do 16 łańcuchów.



Rys. 93. Schemat pracy w trybie CHAIN przy aktywnym połączeniu od strony portu HEAD.



Rys. 94. Schemat praca w trybie CHAIN w przypadku przerwania połączenia. Aktywowany zostaje port TAIL.

W trybie pracy z zablokowanym portem TAIL komunikacja z urządzeniami stanowiącymi elementy łańcucha odbywa się wyłącznie przez port HEAD. W momencie przerwania jednego z połączeń

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	81/147
------	------	-----------------------------------	------------	--------



wewnątrz łańcucha (Rys 55) połączenie zostaje automatycznie rekonfigurowane, a port TAIL zostaje odblokowany. Do punktu przerwania transmisja realizowana jest nadal z wykorzystaniem portu HEAD, natomiast komunikacja ze wszystkimi urządzeniami za punktem przerwania łańcucha realizowana jest przez port TAIL.

Przed rozpoczęciem konfiguracji należy wyłączyć na portach tworzących łańcuch pozostałe protokoły protekcji np. protokoły z grupy Spanning Tree.

Następnie należy skonfigurować punkty MEP dla każdego portu urządzenia w łańcuchu. Konfiguracja została szczegółowo opisana w punkcie 6.8.5.1

Po zakończeniu konfiguracji punktów MEP można przystąpić do dodania łańcucha, do okna konfiguracji prowadzi ścieżka Configuration>Chain

Znaczenie poszczególnych pól zostało opisane poniżej:

CHAIN ID - numer identyfikacyjny łańcucha

First Port - numer pierwszego portu tworzącego ogniwo łańcucha (jeden z portów ze skonfigurowanym punktem MEP)

First Port Role - rola pierwszego portu:

MEMBER - wszystkie porty pomiędzy portami HEAD i TAIL,

HEAD – port stanowiący podstawowe połączenie z siecią, do której przyłączony jest łańcuch,

TAIL – port stanowiący drugie połączenie z siecią, pozostaje zablokowany do chwili przerwania połączenia od strony portu HEAD.

Second Port - numer drugiego portu tworzącego ogniwo łańcucha (jeden z portów ze skonfigurowanym punktem MEP)

Second Port Role - rola drugiego portu

First Port MEP - numer instancji MEP pierwszego portu

Second Port MEP - numer instancji MEP drugiego portu

Alarm - graficzne przedstawienie alarmu przerwanego połączenia

Ethernet	t Protection	h Chain Sw	itching					
Delete	CHAIN ID	First Port	First Port Role	Second Port	Second Port Role	First Port MEP	Second Port MEP	Alarm
	<u>1</u>	3	Head	4	Member	3	4	
Delete	2	1	Member -	1	Member -	1	1	
	0		Member					
Add new	Protection Gr	oup	ve Head					
			Tail					

Rys. 95. Dodawanie łańcucha

UWAGA! Porty HEAD i TAIL muszą był połączone z siecią Ethernet lub z przełącznikami, które na portach mają skonfigurowany protokół Spanning tree.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	82/147
------	------	-----------------------------------	------------	--------



5.32 MAC TABLE

Strona do konfiguracji tablicy MAC adresów.

Ustawienie limitów czasu dla wpisów w dynamicznej tablicy MAC oraz wyłączenie uczenia się adresów oraz konfiguracja statycznej tablicy MAC.





5.33 Konfiguracja sieci VLAN

Konfiguracja sieci VLAN w **HYPERION** odbywa przez przyporządkowanie portów urządzenia **HYPERION** do wybranego numeru VLAN. Konfiguracja pierwszego etapu jest dostępna na stronie do której prowadzi link **Configuration** → **VLANs**.

Dodanie nowego VLAN polega na wykonaniu następujących czynności: kliknąć na liście w kolumnie Mode i wybrać odpowiedni tryb pomiędzy Access, Trunk lub Hybrid. W polu **Port VLAN** wpisać numer Vlan przy odpowiednich portach fizycznych, które mają należeć do tego VLAN. Zachowanie ustawień następuje po kliknięciu na przycisk **Save**.

Następnie ustawiamy w kolumnie Ingress Acceptance czy port ma akceptować na wejściu ramki tagowane lub nie tagowane lub oba rodzaje. W polu Egress Tagging ustawiamy z jakim znacznikiem ramki mają być transmitowane z portu.

Ostatnie dwie kolumny odpowiadają za dozwalanie i zabranianie wybranych numerów VLAN. Maksymalna ilość VLAN w urządzeniu **HYPERION** zawiera się od 1 do 4095.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	83/147
------	------	-----------------------------------	------------	--------



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	•	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	< ▼	1	\diamond	۲		<> ▼	<> ▼	1-4095	
1	Hybrid 🔻	1	C-Port	۲		Tagged and Untagged v	Untag Port VLAN V	1-4095	
2	Hybrid 🔻	1	C-Port	۲		Tagged and Untagged 🔻	Untag Port VLAN 🔻	1-4095	
3	Access v	1	C-Port	۳	A.	Tagged and Untagged V	Untag All 🔹	1	
4	Access v	1	C-Port	۳	Image: A start of the start	Tagged and Untagged V	Untag All 🔹	1	
5	Access *	1	C-Port	۳	A	Tagged and Untagged 🔻	Untag All 🔹	1	
6	Access *	1	C-Port	۳		Tagged and Untagged 🔻	Untag All 🔹	1	
7	Access *	1	C-Port	۳	1	Tagged and Untagged 🔻	Untag All 🔹	1	
8	Access *	1	C-Port	۳		Tagged and Untagged 🔻	Untag All 🔹	1	
9	Access *	1	C-Port	۳	1	Tagged and Untagged 🔻	Untag All 🔹	1	
10	Access v	1	C-Port	٣	e	Tagged and Untagged 🔻	Untag All 🔹	1	

Save Reset

Rys. 97. Konfiguracja sieci VLAN

Znaczenie pól w tym menu jest następujące:

Allowed Access VLANs – umożliwia obsługę wpisanych numerów VLAN w trybie "Access" oraz dopuszczenie do ruchu tych Vlan-ów.

Ethertype for Custom S-ports – określa własny typu ramki dla ramek tagowanych podwójnym znacznikiem VLAN S-tag.

Port – numery portów urządzenia.

Mode – określa tryby pracy VLAN

Access – w tym trybie następuje akceptacja wszystkich ramek nie tagowanych i nadanie im znacznika, a jeśli dane są wysyłane na port który jest w trybie "Access" to wtedy znacznik zostaje zdjęty. Numery VLAN obsługiwane w tym trybie wprowadzamy w pole "**Allowed Access VLANs**"

Trunk – w tym trybie dzięki temu, że wszystkie ramki są tagowane umożliwia to transmisję wielu VLAN-ów przez jeden port. Jeśli otrzyma ramkę nie tagowaną zostanie ona zatagowana. Dzięki tagowaniu ramki są identyfikowane, do którego VLAN-u należą.

Hybrid – tryb, który łączy tryby Access oraz Trunk, a także wymagany do konfiguracji QandQ

Port VLAN – określa numer VLAN-u natywnego dla danego portu

Port Type – określa typ danego portu:

Unaware – ten typ portu pozwala na obsługę ramek bez znacznika VLAN-u (VLAN tag)

Customer port (C-port) – ten typ portu pozwala na obsługę ramek z pojedynczym znacznikiem VLAN (C-tag).

Service port (S-port) – ten typ pozwala na obsługę ramek z podwójnym znacznikiem VLAN (S-tag).

Custom Service port (S-custom-port) – ten typ portu jest funkcjonalnie podobny do S-port różnica polega na tym, że port obsługuje ramki tylko z podwójnym tagiem i typem ramki wpisanym w polu Ethertype for Custom S-ports.

Ingres Filtering – filtrowania pakietów przychodzących na port. Włączenie tej opcji powoduje sprawdzanie pakietów przychodzących czy tag zawarty w ramce jest zgodny z numerem VLAN ustawionym na porcie, jeśli nie to ramka jest odrzucana.

Ingres Acceptance – służy do określenia jakiego typu ramki będą przekazywane przez port do dalszego przetwarzania:

Tagged and Untagged – wszystkie rodzaje ramek, ze znacznikami VLAN lub bez.

Tagged Only – przekazywane będą tylko ramki tagowane.

Untagged Only – przekazywane będą tylko ramki nie tagowane.

Egress Tagging – pozwala na usuwanie lub wstawianie znaczników VLAN dla ramek, które opuszczają dany port. Możemy wybrać trzy wartości tego pola:

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	84/147



Untag Port VLAN – ta wartość pozwala na wstawianie znacznika Tag dla wszystkich wychodzących ramek z wyjątkiem tych, które mają numer taki jak ustawiony w polu **Port VLAN**.

Tag All - ta wartość powoduje wstawianie znacznika Tag VLAN do każdej opuszczającej port ramki. **Untag All** – ta wartość ustawia port tak, że każda opuszczająca port ramka ma usuwany znacznik Tag VLAN.

5.34 Konfiguracja sieci VLAN w wersji oprogramowania V0xx

Konfiguracja sieci VLAN w **HYPERION-300** odbywa się dwuetapowo, w pierwszym etapie należy przyporządkować porty urządzenia **HYPERION-300** do wybranego numeru VLAN. Konfiguracja pierwszego etapu jest dostępna na stronie do której prowadzi link **Configuration > VLANs > VLAN Memebership**. Dodajemy nowe sieci VLAN i przyporządkowujemy do nich porty przełącznika. Znaczenie poszczególnych pól jest następujące:

Delete – umożliwia usuwanie sieci VLAN z tablicy VLAN urządzenia.

VLAN ID – określa numer VLAN.

VLAN Name – nazwy do określenia VLAN. Pole tekstowe do którego można wpisać dowolną nazwę dla VLAN o długości do 32 znaków, dostępne są tylko litery alfabetu i cyfry arabskie.

W celu przypisania poszczególnych portów do danego VLAN należy klikać na pola w kolumnie **Port Members**. Pola są ponumerowane od 1 do 7 i odpowiadają portom urządzenia np.: klikając na pole numer 2 w kolumnie **Port Members** i wierszu w którym w polu **VLAN ID** jest liczba **100** przypisujemy port 2 do VLAN o numerze 100. Porty można przyporządkować na trzy sposoby:

- 1. port jest przypisany jako port do transmisji danych w obrębie określonego VLAN-u (zielony),
- 2. port jest przypisany do tzw. "listy portów zabronionych". (czerwony),
- 3. port jest usunięty z danego VLAN-u (puste miejsce).

Dodanie nowego VLAN polega na wykonaniu następujących czynności: kliknąć na przycisk **Add New VLAN**. W wierszu który się pojawia się należy wpisać w polu **VLAN ID** numer sieci VLAN. W polu **VLAN Name** wprowadzić opcjonalną nazwę. W polu **Port Members** wybrać porty, które mają należeć do tego VLAN. Zachowanie ustawień następuje po kliknięciu na przycisk **Save**.

Maksymalna ilość VLAN w urządzeniu HYPERION-300 wynosi 4095 od 1 do 4095.

W drugim etapie konfiguracji ustawiamy typ portu i inne opcje związane z filtrowaniem ruchu przychodzącego. Etap ten odbywa się w menu dostępnym przez link Configuration > VLANs > Ports

Start from	VLAN 1	with 20	entries per page.								
	11					Po	rt M	/lei	mb	ers	5
Delete	VLAN ID	١	VLAN Name		1	2	3	4	5	6	7
	1			default	×	1	×	1	\checkmark	\checkmark	\checkmark
	2			Testowy	1	×	1	×	×		
Add New	VLAN	1									

Rys. 98. Konfiguracja sieci VLAN w starszej wersji oprogramowania

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	85/147
------	------	-----------------------------------	------------	--------



Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Dant				Port VL	AN	TY Ter	
Port	Port Type	ingress Filtering	Frame Type	Mode	ID	IXIAG	
1	C-port •		Tagged 🔻	None 🔻	1	Tag_all	
2	Unaware		All	Specific 🔻	1	Untag_pvid	
3	S-port .		Tagged 🔻	None 🔻	1	Untag_pvid	
4	Unaware		All	Specific 🔻	1	Untag_pvid	
5	S-custom-port		Tagged 🔻	None 🔻	1	Tag_all	
6	S-custom-port		Tagged 🔻	None 🔻	1	Tag_all	
7	Unaware		Untagged T	None 🔻	1	Untag all	

Save Reset

Rys. 99.Konfiguracja sieci VLAN i trybu portów w starszej wersji oprogramowania

Znaczenie pól w tym menu jest następujące:

Ethertype for Custom S-ports – określa własny typ ramki dla ramek tagowanych podwójnym znacznikiem VLAN S-tag.

Port – numery portów urządzenia.

Port Type – określa typ danego portu:

Unaware – ten typ portu pozwala na obsługę ramek bez znacznika VLAN-u (VLAN tag)

Customer port (C-port) – ten typ portu pozwala na obsługę ramek z pojedynczym znacznikiem VLAN (C-tag).

Service port (S-port) – ten typ pozwala na obsługę ramek z podwójnym znacznikiem VLAN (S-tag).

Custom Service port (S-custom-port) – ten typ portu jest funkcjonalnie podobny do Sport'u różnica polega na tym, że port obsługuje ramki tylko z podwójnym tagiem i typem ramki wpisany w polu **Ethertype for Custom S-ports**.

Ingres Filtering – filtrowania pakietów przychodzących na port. Włączenie tej opcji powoduje sprawdzanie pakietów przychodzących czy tag zawarty w ramce jest zgodny z numerem VLAN ustawionym na porcie, jeśli nie to ramka jest odrzucana.

Frame type – służy do określenia jakiego typu ramki będą przekazywane przez port do dalszego przetwarzania:

All – wszystkie rodzaje ramek, ze znacznikami VLAN lub bez.

Tagged – przekazywane będą tylko ramki tagowane.

Untagged – przekazywane będą tylko ramki bez Tagu..

Port VLAN – określa numer VLAN i tryb dla ramek nadawanych przez ten port.

Port VLAN Mode – określa tryb wstawiania numeru VLAN:

None – ramki transmitowane w tym trybie nie będą miały przypisywanego numeru VLAN ustawionego w polu *ID*.

Specific – ten tryb powoduje wstawianie ustawionego wcześniej VLAN w polu *ID*. Jeśli ramka dociera do poru bez znacznika VLAN jest on wstawiany i numer VLAN jest wpisywany taki jak jest ustawiony w polu *ID*. Jeśli w polu **Port Type** ustawioną wartość **Unaware** wtedy każda ramka będzie miała ustawiany numer z pola *ID*.

Tx Tag – pozwala na usuwanie lub wstawianie znaczników VLAN dla ramek które opuszczają dany port. Możemy wybrać trzy wartości tego pola:

Untag_pvid – ta wartość pozwala na wstawianie znacznika dla wszystkich wychodzących ramek z wyjątkiem tych, które mają numer taki jak ustawiony w polu **ID**.

Tag_all - ta wartość powoduje wstawianie znacznika VLAN do każdej opuszczającej port ramki.

Untag_all – ta wartość ustawia port tak, że każda opuszczająca port ramka ma usuwany znacznik VLAN.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	86/147
------	------	-----------------------------------	------------	--------



5.35 MONITOROWANIE VLAN

W zakładce Monitor \rightarrow VLANs \rightarrow Membership odczytamy statusy przynależności do Vlanów

5.35.1 VLAN Membership Status for Combined users

Ta strona zawiera przegląd statusu członkostwa użytkowników sieci VLAN..



Rys. 100. Monitorowanie statusu członkostwa w sieci VLAN

VLAN User - Różne wewnętrzne moduły oprogramowania mogą wykorzystywać usługi VLAN do konfigurowania członkostwa w sieci VLAN w locie. Lista rozwijana po prawej stronie umożliwia wybór między wyświetlaniem członkostwa w sieci VLAN skonfigurowanego przez administratora lub skonfigurowanego przez jeden z tych wewnętrznych modułów oprogramowania.

Wpis "Combined" pokaże kombinację konfiguracji administratora i wewnętrznych modułów oprogramowania i zasadniczo odzwierciedla to, co jest faktycznie skonfigurowane w sprzęcie.

Wybierz użytkowników sieci VLAN lub funkcjonalności z listy rozwijanej aby wyświetlić status.

ERPS	~	Select VLAN Users from this drop down list.
Combined		
Admin		
NAS		
GVRP		
MVR		
Voice VLAN		
MSTP		
ERPS		
MEP		
VCL		
RMirror		

Rys. 101. Lista wyboru użytkowników lub funkcjonalności umożliwiająca wyświetlenie statusu portów dla wybranej funkcji lub użytkownika

VLAN ID - Identyfikator sieci VLAN, dla którego są wyświetlani członkowie portu. Port Members – Rząd pól wyboru dla każdego portu, który jest wyświetlany dla każdego VLAN ID. Jeśli port jest zawarty w sieci VLAN, zostanie wyświetlony następujący obrazek: ☑. Jeśli port znajduje się na liście zabronionych portów, zostanie wyświetlony następujący obraz: ☑. Jeśli port znajduje się na liście zabronionych portów i jednocześnie próbował dołączyć do sieci VLAN, zostanie wyświetlony następujący obraz: ☑. W tym przypadku port nie będzie członkiem sieci VLAN.

Poruszanie się po stronie statusu członkostwa w sieci VLAN - Każda strona zawiera do 99 wpisów z tabeli VLAN (domyślnie 20), wybranych za pomocą pola wprowadzania "entries per page".

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	87/147
------	------	-----------------------------------	------------	--------



Przy pierwszej wizycie na stronie zostanie wyświetlonych 20 pierwszych wpisów z początku tabeli sieci VLAN. Jako pierwszy zostanie wyświetlony ten z najniższym identyfikatorem sieci VLAN znalezionym w tabeli sieci VLAN.

Pole wejściowe "VLAN" umożliwia użytkownikowi wybranie punktu początkowego w tabeli sieci VLAN. Kliknięcie przycisku "Refresh" zaktualizuje wyświetlaną tabelę, zaczynając od tej lub najbliższej następnej pasującej tabeli sieci VLAN.

Przycisk >> użyje ostatniego wpisu aktualnie wyświetlanego wpisu VLAN jako podstawy do następnego wyszukiwania. Po osiągnięciu końca w tabeli pojawia się tekst "Brak danych dla wybranego użytkownika". Użyj przycisku |<<, aby zacząć od nowa

5.35.2 Status portu VLAN dla użytkowników połączonych (Combined)

Ta strona zawiera stan portów sieci VLAN.

VLAN User - Różne wewnętrzne moduły oprogramowania mogą wykorzystywać usługi VLAN do konfigurowania portu VLAN w locie. Lista rozwijana po prawej stronie umożliwia wybór między wyświetlaniem członkostwa w sieci VLAN skonfigurowanego przez administratora (Admin) lub skonfigurowanego przez jeden z tych wewnętrznych modułów oprogramowania.

Wpis "Combined" pokaże kombinację konfiguracji administratora i wewnętrznych modułów oprogramowania i zasadniczo odzwierciedla to, co jest faktycznie skonfigurowane w sprzęcie.

Jeśli dany moduł oprogramowania nie nadpisał żadnego z ustawień portu, w tabeli wyświetlany jest tekst "No data exists for the selected user".

Wybierz użytkowników sieci VLAN lub funkcjonalności z listy rozwijanej aby wyświetlić status.



Rys. 102. Lista wyboru użytkowników lub funkcjonalności umożliwiająca wyświetlenie statusu portów dla wybranej funkcji lub użytkownika

Przykładowy status dla funkcji ERPS

VLAN Port Status for ERPS user	ERPS V Auto-refresh Refresh
Interface Port Type Ingress Filtering Frame Type Port VLAN ID Tx Tag Untag	ged VLAN ID Conflicts
10GigabitEthernet 1/1	No NAS
10GigabitEthernet 1/2	No GVRP
	MVR
	Voice VLAN
	MSTP
	ERPS
	MEP
	VCL
	RMirror

Rys. 103. Monitorowanie statusu portów dla funkcjonalności ERPS w sieci VLAN

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	88/147
------	------	-----------------------------------	------------	--------



VLAN Port Status for Combine	d users
------------------------------	---------

Interface	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
10GigabitEthernet 1/1	C-Port	✓	All	1	Untag All		No
10GigabitEthernet 1/2	C-Port	Z	All	1	Untag All		No
10GigabitEthernet 1/3	C-Port	✓	All	1	Untag All		No
10GigabitEthernet 1/4	C-Port	✓	All	1	Untag All		No
GigabitEthernet 1/1	C-Port	~	All	1	Untag All		No
GigabitEthernet 1/2	C-Port	~	All	1	Untag All		No
GigabitEthernet 1/3	C-Port	✓	All	1	Untag All		No
GigabitEthernet 1/4	C-Port	Z	All	1	Untag All		No
GigabitEthernet 1/5	C-Port	✓	All	1	Untag All		No
GigabitEthernet 1/6	C-Port	Z	All	1	Untag All		No
GigabitEthernet 1/7	C-Port	✓	All	1	Untag All		No
GigabitEthernet 1/8	C-Port	~	All	1	Untag All		No
GigabitEthernet 1/9	C-Port	✓	All	1	Untag All		No
GigabitEthernet 1/10	C-Port	~	All	1	Untag All		No

Rys. 104. Monitorowanie statusu portów w sieci VLAN dla wszystkich użytkowników oraz funkcji

Interface (Port) - Port logiczny dla ustawień zawartych w tym samym wierszu.

Port Type - Pokazuje typ portu (Unaware, C-Port, S-Port, S-Custom-Port.), który dany użytkownik chce skonfigurować na porcie. Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Ingress Filtering - Pokazuje, czy dany użytkownik chce włączyć filtrowanie danych wejściowych, czy nie. Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Frame Type - Pokazuje dopuszczalne typy ramek (All, Tagged, Untagged), które dany użytkownik chce skonfigurować na porcie. Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Port VLAN ID - Pokazuje identyfikator portu VLAN ID (PVID), który dany użytkownik chce mieć na porcie. Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Tx Tag - Pokazuje wymagania Tx Tag (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID), które dany użytkownik ma na porcie. Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Untagged VLAN ID - Jeśli Tx Tag jest zastępowany przez wybranego użytkownika i jest ustawiony na Tag lub Untag UVID, to pole pokaże identyfikator VLAN, który użytkownik chce oznaczyć lub odznaczyć przy wyjściu.

Pole jest puste, jeśli nie zostanie nadpisane przez wybranego użytkownika.

Konflikty

Dwóch użytkowników może mieć sprzeczne wymagania dotyczące konfiguracji portu. Na przykład, jeden użytkownik może wymagać, aby wszystkie ramki były oznakowane (tagged) przy wyjściu, podczas gdy inny wymaga, aby wszystkie ramki były nieoznaczane (untagged) przy wyjściu. Ponieważ obaj użytkownicy nie mogą wygrać, powoduje to konflikt, który jest rozwiązywany w sposób uszeregowany według priorytetów. Administrator ma najmniejszy priorytet. Innym modułom oprogramowania nadawane są priorytety zgodnie z ich pozycją na liście rozwijanej: Im wyżej na liście, tym wyższy priorytet. Jeśli istnieją konflikty, zostanie to wyświetlone jako "Yes" dla użytkownika "Combined" i modułu oprogramowania, którego dotyczy problem. Użytkownik "Combined" odzwierciedla faktyczną konfigurację sprzętu.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	89/147
				1



5.36 VLAN TRANSLATION

5.36.1 VLAN Translation Port Configuration

(Configuration \rightarrow VLAN Translation \rightarrow Port to Group Configuration)

Ta strona umożliwia skonfigurowanie portów przełącznika do korzystania z danej grupy mapowania translacji sieci VLAN. Spowoduje to włączenie wszystkich mapowań translacji VLAN tej grupy (jeśli istnieją) na wybranym porcie przełącznika.

Wyświetlane ustawienia to:

Port - Kolumna Port zawiera listę portów, dla których można skonfigurować grupę mapowania translacji VLAN.

Default - Aby ustawić port przełącznika tak, aby używał domyślnej grupy tłumaczeń sieci VLAN, kliknij pole wyboru i naciśnij przycisk Zapisz.

Group ID - Mapowania translacji VLAN są zorganizowane w grupy, identyfikowane przez identyfikator grupy. W ten sposób port jest skonfigurowany do łatwego korzystania z wielu mapowań translacji VLAN, po prostu konfigurując go do korzystania z danej grupy. Wówczas liczba możliwych grup w przełączniku jest równa liczbie portów obecnych w tym przełączniku. Port można skonfigurować do korzystania z dowolnej grupy, ale w danym momencie tylko jednej. Można skonfigurować wiele portów do korzystania z tej samej grupy. Prawidłowy identyfikator grupy to liczba całkowita od 1 do 37.

Uwaga: Domyślnie każdy port jest ustawiony na używanie grupy z identyfikatorem grupy równym numerowi portu. Na przykład port nr 1 jest domyślnie ustawiony na używanie grupy z GID = 1.

Interface	Group Co	nfiguration
interface	Default	Group ID
*		<> ▼
10GigabitEthernet 1/1		1 🗸
10GigabitEthernet 1/2		2 🗸
10GigabitEthernet 1/3		3 🗸
10GigabitEthernet 1/4		4 🗸
GigabitEthernet 1/1		5 🗸
GigabitEthernet 1/2		6 🗸
GigabitEthernet 1/3		7 🗸
GigabitEthernet 1/4		8 🗸
GigabitEthernet 1/5		9 🗸
GigabitEthernet 1/6		10 🗸
GigabitEthernet 1/7		11 🗸
GigabitEthernet 1/8		12 🗸
GigabitEthernet 1/9		13 🗸
GigabitEthernet 1/10		14 🗸

Rys. 105. Konfiguracja portu translacji VLAN-ów

5.36.2 VLAN Translation Mapping Table

Ta strona umożliwia tworzenie mapowań sieci VLAN -> Translated VLAN i organizowanie tych mapowań w globalne grupy.

,	VLAN Tran	slatio	on Map	ping	Table	Mapping (Configuration
	Group ID 1	VID 110	TVID 580	<u>@</u> 8		Mapping	Parameters
l				Ð		Group ID	0
						VID	0
						TVID	0
						Save	set Cancel

Rys. 106.Konfiguracja mapowania sieci VLAN i tworzenia globalnych grup

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	90/147
------	------	-----------------------------------	------------	--------



Group ID - Mapowania translacji VLAN są zorganizowane w grupy, identyfikowane przez identyfikator grupy. W ten sposób port jest skonfigurowany do łatwego korzystania z wielu mapowań translacji VLAN, po prostu konfigurując go do korzystania z danej grupy. Wówczas liczba możliwych grup w przełączniku jest równa liczbie portów obecnych w tym przełączniku. Port można skonfigurować do korzystania z dowolnej grupy, ale w danym momencie tylko jednej. Można skonfigurować wiele portów do korzystania z tej samej grupy. Prawidłowy identyfikator grupy to liczba całkowita od 1 do 37.

Uwaga: Domyślnie każdy port jest ustawiony na używanie grupy z identyfikatorem grupy równym numerowi portu. Na przykład port nr 1 jest domyślnie ustawiony na używanie grupy z GID = 1.

VID - Wskazuje VLAN mapowania (tj. "Źródłową" sieć VLAN). Prawidłowy identyfikator sieci VLAN mieści się w zakresie od 1 do 4095.

TVID - Wskazuje identyfikator VLAN, na który zostanie przetłumaczony identyfikator VLAN ramki wejściowej (pod warunkiem, że mapowanie jest włączone na porcie wejściowym, do którego ramka dotarła). Prawidłowy identyfikator sieci VLAN mieści się w zakresie od 1 do 4095.

Przyciski modyfikacji - Możesz zmodyfikować każde mapowanie translacji sieci VLAN w tabeli za pomocą następujących przycisków:

- 🕑: Edytuje wiersz mapowania.
- 😢: Usuwa mapowanie.
- 🕒: Dodaje nowe mapowanie.

5.37 Private VLANs

W tym miejscu można monitorować i modyfikować konfiguracje członkostwa w prywatnej sieci VLAN dla przełącznika. Tutaj można dodawać lub usuwać prywatne sieci VLAN. W tym miejscu można dodać lub usunąć członków portu każdej prywatnej sieci VLAN.

Prywatne sieci VLAN są oparte na masce portu źródłowego i nie ma połączeń z sieciami VLAN. Oznacza to, że identyfikatory VLAN ID i prywatne identyfikatory VLAN mogą być identyczne.

Port musi należeć zarówno do sieci VLAN, jak i do prywatnej sieci VLAN, aby móc przekazywać pakiety. Domyślnie wszystkie porty nie rozpoznają sieci VLAN i należą do sieci VLAN 1 i Private VLAN 1.

Domyślny port VLAN może być członkiem tylko jednej sieci VLAN, ale może być członkiem wielu prywatnych sieci VLAN.

5.37.1 Private VLAN Membership Configuration

Delete - Aby usunąć prywatny wpis VLAN, zaznacz to pole. Wpis zostanie usunięty podczas następnego zapisu.

Private VLAN ID - Wskazuje identyfikator tej konkretnej prywatnej sieci VLAN.

Port Members - Wiersz pól wyboru dla każdego portu wyświetlanego dla każdego prywatnego identyfikatora sieci VLAN. Aby dołączyć port do prywatnej sieci VLAN, zaznacz to pole. Aby usunąć lub wykluczyć port z prywatnej sieci VLAN, upewnij się, że to pole nie jest zaznaczone. Domyślnie żadne porty nie są członkami, a wszystkie pola są odznaczone.

Add a New Private VLAN - Kliknij "Add New Private VLAN", aby dodać nowy prywatny identyfikator VLAN. Do tabeli zostanie dodany pusty wiersz, po czym można skonfigurować prywatną sieć VLAN. Dozwolony zakres dla prywatnego identyfikatora VLAN jest taki sam, jak zakres numerów portów przełącznika. Wszelkie wartości spoza tego zakresu nie są akceptowane i pojawia się komunikat

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	91/147
I (L V .	1.00		2021.01.01	01/14/



ostrzegawczy. Kliknij "OK", aby odrzucić niepoprawny wpis, lub kliknij "Cancel", aby powrócić do edycji i wprowadzić poprawkę.

Prywatna sieć VLAN jest włączana po kliknięciu przycisku "Save". Za pomocą przycisku "DELETE" można cofnąć dodanie nowych prywatnych sieci VLAN.





5.37.2 Port Isolation Configuration

Ta strona służy do włączania lub wyłączania izolacji portów na portach w prywatnej sieci VLAN. Element portu sieci VLAN może być izolowany od innych izolowanych portów w tej samej sieci VLAN i prywatnej sieci VLAN.



Rys. 108. Menu izolacji portów w prywatnej sieci VLAN

Port Members - Ta strona służy do włączania lub wyłączania izolacji portów na portach w prywatnej sieci VLAN.

Element portu sieci VLAN może być izolowany od innych izolowanych portów w tej samej sieci VLAN i prywatnej sieci VLAN.

5.38 VCL

5.38.1 VCL MAC-Based VLAN Configuration

Ta strona umożliwia konfigurację mapowania adresu MAC na identyfikator VLAN ID. Daje możliwość dodawania i usuwania wpisów listy klasyfikacyjnej VLAN opartej na adresach MAC i przypisywania wpisów do różnych portów.

Delete - Aby usunąć wpis mapowania MAC do VLAN ID, zaznacz to pole i naciśnij Zapisz. **MAC Address -** Wskazuje adres MAC mapowania.

VLAN ID - Wskazuje identyfikator sieci VLAN, na który zostanie zmapowany powyższy adres MAC.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	92/147
------	------	-----------------------------------	------------	--------



Port Members - Wiersz pól wyboru dla każdego portu, który jest wyświetlany dla każdego wpisu mapowania MAC do VLAN ID. Aby uwzględnić port w mapowaniu, zaznacz pole. Aby usunąć lub wykluczyć port z mapowania, upewnij się, że to pole nie jest zaznaczone. Domyślnie żadne porty nie są uwzględnione, a wszystkie pola są odznaczone.

Adding a New MAC to VLAN ID mapping entry - Kliknij "Add New Entry", aby dodać nowy wpis mapowania MAC do VLAN ID. Do tabeli dodawany jest pusty wiersz, a mapowanie można skonfigurować w razie potrzeby. Do skonfigurowania mapowania można użyć dowolnego adresu MAC unicast. Nie sa dozwolone żadne adresy MAC broadcast ani multicast. Prawidłowe wartości identyfikatora sieci VLAN to od 1 do 4095.

Wpis MAC do VLAN ID jest włączony po kliknięciu na "Save". Bez żadnych członków portu, po kliknięciu na "Save" (Zapisz), nie zostanie dodane mapowanie.

Za pomocą przycisku "Delete" można cofnąć dodawanie nowych mapowań. Maksymalnie możliwe wpisy mapowania MAC do VLAN ID sa ograniczone do 256.



MAC-based VLAN Membership Configuration

Save Reset

Rys. 109. Okno konfiguracji przynależności do wskazanej sieci VLAN na podstawie adresów MAC

5.38.2 IP Subnet-based VLAN Membership Configuration

Podsieć IP do mapowania VLAN ID można skonfigurować tutaj. Na tej stronie można dodawać, aktualizować i usuwać wpisy mapowania IP podsieci do VLAN ID oraz przypisywać je do różnych portów.

IP Subne	Subnet-based VLAN Membership Configuration																												
														F	ort l	Nem	bers												
Delete	IP Address	Mask Length	VLAN ID	10GigabitEthernet 1/1	10GigabitEthernet 1/2 10GigabitEthernet 1/3	10GigabitEthernet 1/4 GigabitEthernet 1/1	GigabitEthemet 1/2	GigabitEthem et 1/3 GigabitEthem et 1/4	GigabitEthemet 1/5	GigabitEthem et 1/7 GigabitEthem et 1/7	GigabitEthemet 1/8	GigabitEthem et 1/9 GigabitEthem et 1/10	GigabitEthemet 1/11	GigabitEthemet 1/12 GigabitEthemet 1/13	GigabitEthemet 1/14	GigabitEthemet 1/15	GigabitEthemet 1/16 GigabitEthemet 1/17	GigabitEthemet 1/18	GigabitEthemet 1/19	GigabitEthemet 1/20 GigabitEthemet 1/21	GigabitEthemet 1/22	GigabitEthemet 1/23	GigabitEthemet 1/24	GigabitEthemet 1/25	GigabitEthemet 1/27	GigabitEthemet 1/28	GigabitEthemet 1/29	GigabitEthemet 1/31	GigabitEthemet 1/32 FastEthernet 1/1
Delete	0000	24	1					חר		חר		חר			חו			П			חו				חו			חו	
Delete	0.0.0.0	24																	0										00
Delete	0.0.0.0	24	Z		Uυ	υU	UL		UL						JU	U								υL			υL		UU
Add New	Add New Entry																												

Rys. 110.Okno konfiguracji przynależności do wskazanej sieci VLAN na podstawie adresów IP

Delete - Aby usunać mapowanie, zaznacz to pole i naciśnij Zapisz. Wpis zostanie usuniety ze stosu. IP Address - Wskazuje adres IP podsieci (można tu również podać dowolny adres hosta podsieci, aplikacja skonwertuje go automatycznie).

Mask Length - Wskazuje długość maski podsieci.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	93/147
------	------	-----------------------------------	------------	--------



VLAN ID - Wskazuje identyfikator sieci VLAN, do której zostanie zmapowana podsieć. Podsieć IP dopasowana jest do identyfikatora VLAN unikalnie.

Port Members - Wiersz pól wyboru dla każdego portu, który jest wyświetlany dla każdej podsieci IP do wpisu mapowania identyfikatora VLAN. Aby uwzględnić port w mapowaniu, zaznacz pole. Aby usunąć lub wykluczyć port z mapowania, upewnij się, że to pole nie jest zaznaczone. Domyślnie żadne porty nie są uwzględnione, a wszystkie pola są odznaczone.

Dodawanie nowej sieci VLAN opartej na podsieci IP - Kliknij "Add New Entry", aby dodać nową podsieć IP do wpisu mapowania VLAN ID. Do tabeli dodawany jest pusty wiersz, a mapowanie można skonfigurować w razie potrzeby. Do mapowania można skonfigurować dowolny adres IP / maskę. Prawidłowe wartości identyfikatora sieci VLAN to od 1 do 4095. Wpis mapowania podsieci IP na identyfikator VLAN jest włączany po kliknięciu przycisku "Zapisz". Za pomocą przycisku Usuń można cofnąć dodanie nowych mapowań. Maksymalne możliwe mapowania podsieci IP na identyfikatory VLAN są ograniczone do 128.

5.39 Voice VLAN

Funkcja Voice VLAN umożliwia przekazywanie ruchu głosowego w Voice VLAN, a następnie switch może klasyfikować i planować ruch w sieci. Zaleca się, aby na porcie znajdowały się dwie sieci VLAN - jedna do przesyłania głosu, druga do przesyłania danych.

5.39.1 Voice VLAN Configuration

Voice VLAN Configuration

Przed podłączeniem urządzenia IP do przełącznika, telefon IP powinien posiadać poprawnie skonfigurowany głosowy identyfikator VLAN ID. Parametr ten powinien być skonfigurowany za pomocą własnego GUI telefonu IP.

Mode	Disabl	ed	~	
VLAN ID	1000			
Aging Time	86400	sec	onds	
Traffic Class	7 (Hig	h)	~	
Dant Canfin				
Port Configu	ration			
	Port	Mode	Security	Discovery Protocol
	*	◇ ∨	<u> </u>	○
10GigabitEther	net 1/1	Disabled 🗸	Disabled ~	0UI 🗸
10GigabitEther	net 1/2	Disabled 🗸	Disabled 🗸	0UI 🗸
10GigabitEther	net 1/3	Disabled 🗸	Disabled 🗸	0UI 🗸
10GigabitEther	met 1/4	Disabled 🗸	Disabled 🗸	OUI 🗸
GigabitEther	net 1/1	Disabled 🗸	Disabled 🗸	OUI 🗸
GigabitEther	met 1/2	Disabled 🗸	Disabled 🗸	OUI 🗸
GigabitEther	net 1/3	Disabled 🗸	Disabled ¥	OUI 🗸
GigabitEther	net 1/4	Disabled 🗸	Disabled 🗸	OUI 🗸
GigabitEther	net 1/5	Disabled 🗸	Disabled V	OUI 🗸
GigabitEther	net 1/6	Disabled 🗸	Disabled V	OUI 🗸
GigabitEther	net 1/7	Disabled 🗸	Disabled V	OUI 🗸
GigabitEther	net 1/8	Disabled 🗸	Disabled ~	OUI 🗸
GigabitEther	net 1/9	Disabled 🗸	Disabled ~	OUI 🗸
GigabitEthern	et 1/10	Disabled 🗸	Disabled ~	OUI 🗸
GigabitEthern	et 1/11	Disabled V	Disabled V	OUI
GigabitEthern	et 1/12	Disabled V	Disabled V	LLDP
01 1151		D'antitation	D'and the days	Both

Rys. 111. Okno konfiguracji Voice VLAN

Mode - Aktywuje działanie w trybie Voice VLAN. Zanim włączymy Voice VLAN, należy wyłączyć funkcję MSTP. Pozwala to uniknąć konfliktu filtrowania danych wejściowych. Możliwe tryby to:

Enabled: Włącz działanie w trybie Voice VLAN.

Disabled: Wyłącz działanie w trybie Voice VLAN.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	94/147
------	------	-----------------------------------	------------	--------



VLAN ID - Wskazuje identyfikator Voice VLAN. Powinien to być unikalny identyfikator sieci VLAN w systemie i nie może równać się poszczególnym PVID portów. Konflikt w konfiguracji występuje, jeśli wartość jest równa VID zarządzania, MVR VID, PVID itp. Dopuszczalny zakres to 1 do 4095.

Aging Time - Wskazuje czas starzenia bezpiecznego uczenia się Voice VLAN. Dopuszczalny zakres to 10 do 10000000 sekund. Jest używany, gdy włączony jest tryb bezpieczeństwa lub tryb automatycznego wykrywania. W innych przypadkach będzie to oparte na sprzętowym czasie starzenia. Rzeczywisty czas starzenia będzie się mieścić między [age_time; 2 * age_time].

Traffic Class - Wskazuje klasę ruchu Voice VLAN. Cały ruch w Voice VLAN będzie dotyczył tej klasy.

Port Mode - Wskazuje tryb portu Voice VLAN. Możliwe tryby portów to:

Disabled: Odłącz się od Voice VLAN.

Auto: Włącz tryb automatycznego wykrywania. Wykrywa, czy do określonego portu jest podłączony telefon VoIP i automatycznie konfiguruje członków Voice VLAN.

Forced: Wymuś przyłączenie do Voice VLAN.

Port Security - Wskazuje tryb zabezpieczeń portu Voice VLAN. Gdy funkcja jest włączona, wszystkie nietelefoniczne adresy MAC w głosowej sieci VLAN zostaną zablokowane na 10 sekund. Możliwe tryby portów to:

Enabled: Włącz działanie w trybie bezpieczeństwa Voice VLAN..

Disabled: Wyłącz działanie w trybie bezpieczeństwa Voice VLAN.

Port Discovery Protocol - Wskazuje protokół wykrywania portów Voice VLAN. Będzie działać tylko wtedy, gdy włączony jest tryb automatycznego wykrywania. Powinniśmy włączyć funkcję LLDP przed skonfigurowaniem protokołu wykrywania na "LLDP" lub "Both". Zmiana protokołu wykrywania na "OUI" lub "LLDP" spowoduje ponowne uruchomienie procesu automatycznego wykrywania. Możliwe protokoły wykrywania to:

OUI: Wykryj urządzenie telefoniczne według adresu OUI.

LLDP: Wykryj urządzenie telefoniczne przez LLDP.

Both: Obydwa protokoły: OUI i LLDP.

5.39.2 Voice VLAN OUI

5.39.3 Konfiguracja Voice VLAN OUI

Strona służy do konfiguracji VOICE VLAN OUI. Maksymalna liczba wpisów to 16. Modyfikacja tabeli OUI spowoduje ponowne uruchomienie automatycznego wykrywania procesu OUI.

Delete - Zaznacz, aby usunąć wpis. Zostanie usunięty podczas następnego zapisu.

Telephony OUI - Adres OUI telefonii to globalnie unikalny identyfikator przypisany dostawcy przez IEEE. Musi mieć 6 znaków, a format wejściowy to "xx-xx-xx" (x to cyfra szesnastkowa).

Description - Opis adresu OUI. Zwykle opisuje urządzenie telefoniczne producenta, do którego należy. Dozwolona długość łańcucha wynosi od 0 do 32.

Delete	Telephony OUI	Description				
	00-01-e3	Siemens AG phones				
	00-03-6b	Cisco phones				
	00-0f-e2	H3C phones				
	00-60-b9	Philips and NEC AG phones				
	00-d0-1e	Pingtel phones				
	00-e0-75	Polycom phones				
	00-e0-bb	3Com phones				
Delete						
Add New Entry						



REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	95/147
------	------	-----------------------------------	------------	--------



5.40 FUNKCJA PING WATCHDOG POE

5.40.1 Konfiguracja Ping Watchdog

Na tej stronie skonfigurujesz funkcję monitor połączenia (Ping Watchdog). Klikamy Configuration \rightarrow Ping Watchdog \rightarrow Configuration. Za pomocą tej funkcji monitorujemy odpowiedź na wysłane pingi urządzenia PD np. Kamera IP.

Zasada działania Ping Watchdoga PoE polega na tym, że w przełącznikach zasilających przez PoE urządzenia PD, w przypadku gdy wystąpi brak odpowiedzi z urządzenia PD na wysłany ping ip przełącznik przeprowadzi automatyczne chwilowe wyłączenie zasilania PoE na porcie, na którym stwierdzi brak odpowiedzi co spowoduje zdalny reset urządzenia PD np. kamery. Brak odpowiedzi na trzykrotnie występujące po sobie zapytania ping powoduje uruchomienie funkcji.

Ping Watchdog Configuration

Interface	Enable	IP Address	Startup Time	e [s] Interval Tin	ne [s] Trap SNMP
FastEthernet 1/1		0.0.0.0	60	20	
FastEthernet 1/2		0.0.0.0	60	20	
FastEthernet 1/3		0.0.0.0	60	20	
FastEthernet 1/4		0.0.0.0	60	20	

Save Reset

Rys. 113. Okno konfiguracji Watchdog PoE

Dla portu z którego będziemy zasilać urządzenie włączamy funkcję przez zaznaczenie chekbox w kolumnie **Enable**. W polu "**IP Address**" wpisujemy adres IP urządzenia które będzie zasilane z portu PoE z funkcją watchdoga.

Pole "**Startup Time [s]**" służy do ustawiania czasu, po którym urządzenie PD po starcie jest gotowe do normalnej pracy, a tym samym będzie odpowiadać na pingi ze switch-a.

Zakres czasu wynosi min 0 sekund do max 240 sekund.

Pole "**Interval Time [s]**" służy do ustawiania odstępu czasowego pomiędzy wysyłanymi pingami do urządzenia PD. Zakres czasu wynosi min 1 sekund do max 180 sekund. W przypadku braku odpowiedzi na trzy kolejne próby wysłanych pingów switch automatycznie wyłącza zasilanie na porcie co powoduje restart urządzenia zasilanego.

Pole "**Trap SNMP**" służy do wysyłania trapów z komunikatami o nieodpowiadaniu urządzenia na ping, restartu lub powrotu do normalnej pracy urządzenia zasilanego. Usługa Trap SNMP wymaga konfiguracji.

Przykładową konfigurację funkcji Ping Watchdog znajduje się w punkcie 10 niniejszej instrukcji

5.40.2 Monitorowanie Ping Watchdog

Dla weryfikacji poprawności konfiguracji po wejściu do zakładek Monitor \rightarrow Watchdog PoE \rightarrow Status - możemy sprawdzić czy urządzenie prawidłowo odpowiada na pingi co obrazuje kolor zielony diody w kolumnie "**state**".

Ping Watchdog

Status

Port	Enable	IP Address	StartUp Time	e [s] Interval Tim	e [s] Email	Trap SNMP	State
1		0.0.0.0	60	20			
2		0.0.0.0	60	20			
3	\$	10.0.0.118	60	10			
4		10.0.0.117	60	10			

Rys. 114. Okno monitorowania Watchdog PoE

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	96/147
------	------	-----------------------------------	------------	--------



5.41 Static NAT

Funkcja dostępna w przełącznikach HYPERION-200, HYPERION-402, HYPERION-500

Przykładowa konfiguracje funkcji NAT znajduje sie w punkcie 10 niniejszej instrukcji

Static NAT									
Configuration									
Enal	ble	Alias address		Mask					
	0.0.0	0.0	0						
Redir	rect setti	ngs							
ID	Enable	IPI	ocal		IP public				
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

Rys. 115.Konfiguracja Statycznego NAT

Lista w oknie "Redirect settings" w Static NAT umożliwia utworzenie 128 wpisów translacji adresów.

W oknie "Configuration" aby włączyć całą funkcji należny zaznaczyć chekbox w kolumnie Enable. Alias address – adres główny w sieci lokalnej – interfejs w switchu z NAT

Mask – maska do podsieci lokalnej

W liście do włączenia poszczególnych wierszy w funkcji należny zaznaczyć chekbox w kolumnie Enable dla każdego wiersza.

IP local – adres sieci lokalnej, który ma być translatowany

IP public – adres sieci zewnętrznej np. WAN, który ma wykorzystywany do translacji

5.42 IRIGB

IRIG-B to ustandaryzowany protokół przesyłania informacji o czasie i dacie, który używany jest do synchronizacji urządzeń wyposażonych w ten typ interfejsu.

Przełącznik HYPERION-500 umożliwia wyposażenie go w moduł IRIG-B, który zgodny jest ze standardami: IRIG Standard 200-04 oraz IEEE C37.118.1-2011.

Synchronizacja modułu IRIGB może odbywać się poprzez moduł GNSS, zainstalowany w urządzeniu HYPERION-500 albo z wykorzystaniem protokołu PTP uruchomionego w HYPERION-500 w trybie boundry clock.

Moduł posiada następujące interfejsy wyjściowe:

2x IRIG-B DCLS – sygnał niemodulowany, złącza BNC.

2x IRIG-B AM – sygnał modulowany 1kHz, impedancja wyjściowa 600 Ohm, złącza BNC. 2x PPS lub IRIG-B - Transceivery nadawcze HFBR, złacze ST 850 nm światłowód MM - 50/125 lub 62.5/125 um.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	97/147
------	------	-----------------------------------	------------	--------



Konfiguracja interfejsów modułu IRIG-B odbywa się w oknie dostępnym pod linkiem Configuration \rightarrow IRIGB.

PPS LOCK

IRIGB Configuration

Interface	Туре	Enable	IRIG Signal Identification Number	User defined CF	Phase shift enable	Phase shift [ns]
IRIG 1	AM	✓	IRIG B120 (BCD_TOY, CF, SBS)	IRIG STANDARD 200-04 🗸		0
IRIG 2	AM	~	IRIG B127 (BCD_TOY, BCD_Year, SBS)	IRIG STANDARD 200-04 🗸		0
IRIG 3	DCLS	<	IRIG B000 (BCD_TOY, CF, SBS)	IRIG STANDARD 200-04 🗸		0
IRIG 4	DCLS	Z	IRIG B007 (BCD_TOY, BCD_Year, SBS)	IRIG STANDARD 200-04 🗸		0
			IRIG B000 (BCD_TOY, CF, SBS)			
			IRIG B001 (BCD_TOY, CF)			
			IRIG B002 (BCD_TOY)			
			IRIG B003 (BCD_TOY, SBS)			
			IRIG B004 (BCD_TOY, BCD_Year, CF, SBS)			
			IRIG B005 (BCD_TOY, BCD_Year, CF)			
			IRIG B006 (BCD_TOY, BCD_Year)			
			IRIG B007 (BCD_TOY, BCD_Year, SBS)			

FO Configuration

Interface	Туре	Enable	Output negation	Phase shift enable	Phase shift [ns]
FO 1	PPS 🗸				0
FO 2	PPS 🗸				0

Time Mode UTC 🗸

Save Reset

Rys. 116. Menu konfiguracji trybów sygnałów w module IRIG-B

Znaczenie poszczególnych pól jest następujące:

PPS LOCK – LED sygnalizujący synchronizację modułu z backplane.

Interfejsy:

- IRIG 1, IRIG 2 – interfejsy modulowane generujące sygnał AM;

- IRIG 3, IRIG 4 – interfejsy niemodulowane generujące sygnał DCLS

- FO 1, FO 2 – interfejsy światłowodowe dla których można konfigurować różne typu sygnałów

takich jak: PPS, PPM oraz różne typy sygnałów IRIG

Enable – włączenie/wyłączenie interfejsu

IRIG Signals Identification Number – konfiguracja ramki IRIG umożliwiająca wybór wysyłanych informacji. Skróty w formatach oznaczają:

- BCD (Binary Coded Decimal) – odczyt informacji zawierający czas w godzinach, minutach sekundach oraz dniach (HH,MM,SS,DDD),

- SBS (Straight Binary Second) – liczba określająca sekundę obecnego dnia, przybiera wartości od 0 do 86400,

- CF (Control Functions) - funkcje kontrolne zdefiniowane przez użytkownika,

- BCD_TOY (Binary Coded Decimal Time of Year) – rozpoczyna odliczanie czasu od zera (0) dla godzin, minut, sekund oraz frakcji sekundy każdego dnia o godzinie 24:00, także rozpoczyna odliczanie od 001 o godzinie 24:00 ostatniego dnia w roku,

- BCD_Year (Binary Coded Decimal Year) – pole zawierające dwie ostatnie cyfry bieżącego roku, przybiera wartości od 1 do 99.

User defined CF – wybór trybu ze zdefiniowanymi funkcjami kontrolnymi:

- IRIG Standard 200-04 – zawiera standardowe dane w polu funkcji kontrolnych,

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	98/147
------	------	-----------------------------------	------------	--------



- IEEE C37.118.1-2011 – zawiera rozszerzone dane w polu funkcji kontrolnych.

Phase shift enable – włączenie przesunięcia fazowego używanego do korekty opóźnień wprowadzanych przez kable

Phase shift [ns] – wartość przesunięcia fazowego sygnału względem PPS używana do korekty opóźnień wprowadzanych przez kable

5.43 Quality of Service

5.43.1 Klasyfikacja ramek wejściowych Ingress Port Classification

Funkcja ta klasyfikuje ramki przychodzące na port przełącznika do jednej z QoS class i DP Level (Drop Precedence Level). Mapuje ramki posiadające tag zgodnie z IEEE802.1q oraz ramki warstwy trzeciej posiadające znacznik DSCP do jednej z QoS class również z nadaniem znacznika DP Level. Konfiguracja tych parametrów odbywa się w oknie dostępnym po kliknięciu na linki **Configuration** \rightarrow **QoS** \rightarrow **Port Classification**.

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>▼	 T 	< ▼	< ▼			<> ▼
1	0 🔻	0 🔻	0 🔻	0 •	Disabled		Source •
2	0 🔻	0 🔻	0 🔻	0 🔻	Disabled		Source •
3	0 🔻	0 🔻	0 🔻	0 🔻	Disabled		Source •
4	0 🔻	0 🔻	0 🔻	0 🔻	Disabled		Source 🔻
5	0 •	0 🔻	0 •	0 •	Disabled		Source •
6	0 🔻	0 🔻	0 🔻	0 🔻	Disabled		Source T
7	0 🔻	0 🔻	0 🔻	0 •	Disabled		Source 🔻
8	0 🔻	0 🔻	0 🔻	0 🔻	Disabled		Source •
9	0 🔻	0 🔻	0 🔻	0 •	Disabled		Source •
10	0 🔻	0 🔻	0 •	0 •	Disabled		Source •

QoS Ingress Port Classification

Save Reset

Rys. 117. Menu QoS Ingress Port Classification

Znaczenie poszczególnych pól jest następujące:

Pierwszy wiersz oznaczony przez gwiazdkę '*' pozwala na konfigurację danego parametru globalnie dla wszystkich portów.

Port – numer fizycznego portu dla którego odnosi się dane ustawienie,

CoS - Steruje domyślną klasą usług (ang. Class of Service)

Wszystkie ramki są klasyfikowane do CoS. Istnieje mapowanie jeden do jednego między CoS, kolejką i priorytetem. Wartość CoS równa 0 (zero) ma najniższy priorytet.

Jeśli port obsługuje sieć VLAN, ramka jest oznaczona i ma włączone Tag Class. Następnie ramka jest klasyfikowana do CoS, który jest odwzorowywany na podstawie wartości PCP i DEI w znaczniku. W przeciwnym razie ramka jest klasyfikowana do domyślnego CoS.

Sklasyfikowany CoS może zostać zastąpiony wpisem QCL.

Uwaga: Jeśli domyślny CoS został zmieniony dynamicznie, to aktualny domyślny CoS jest wyświetlany w nawiasach po skonfigurowanym domyślnym CoS.

DPL - Steruje domyślnym poziomem pierwszeństwa usuwania (ang. Drop Precedence Level) Wszystkie ramki są sklasyfikowane w kryterium poziomu pierwszeństwa usuwania.

Jeśli port obsługuje sieci VLAN, ramka jest oznaczana i ma włączone Tag Class. Następnie ramka jest klasyfikowana do DPL, która jest odwzorowywana na podstawie wartości PCP i DEI w znaczniku. W przeciwnym razie ramka jest klasyfikowana do domyślnego DPL.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	99/147
------	------	-----------------------------------	------------	--------



Sklasyfikowany DPL można zastąpić wpisem QCL.

PCP - Steruje domyślną wartością PCP.

Wszystkie ramki są klasyfikowane według wartości PCP.

Jeśli port obsługuje sieć VLAN, a ramka jest oznaczona, wówczas ramka jest klasyfikowana według wartości PCP w znaczniku. W przeciwnym razie ramka jest klasyfikowana według domyślnej wartości PCP.

DEI - Steruje domyślną wartością DEI.

Wszystkie ramki są klasyfikowane według wartości DEI.

Jeśli port obsługuje sieć VLAN, a ramka jest oznaczona, wówczas ramka jest klasyfikowana według wartości DEI w znaczniku. W przeciwnym razie ramka jest klasyfikowana do domyślnej wartości DEI. **Tag Class.** – opcja ta dotyczy ramek tagowanych zgodnie z IEEE802.1q i pozwala przypisać ramkę do QoS class i DP level na podstawie znaczników PCP i DEI umieszczonych w tagach ramek VLAN. Uruchomienie tej funkcji jest możliwe w oknie dostępnym po kliknięciu na linki w tej kolumnie. W menu tym w polu: **Tag Cassification** – wybrać czy funkcjonalność ta ma być włączona **Enable** lub wyłączona **Disable**. W tabeli poniżej jest możliwość wyboru dla wszystkich możliwych kombinacji znaczników **PCP** i **DEI** przydziału **QoS class** i **DP level**. Po zakończeniu konfiguracji, aby zmiany odniosły skutek należy nacisnąć przycisk **Save**. W prawym górnym rogu tego menu jest pole wyboru pozwalające na bezpośrednie przejście do konfiguracji tej funkcjonalności dla innych portów.

DSCP Based – opcja ta dotyczy wszystkich ramek, mapuje pole DSCP ramek warstwy trzeciej do jednej z QoS class i nadaje DP level. Konfiguracja tej opcji odbywa się w menu dostępnym pod linkiem **Configuration > QoS > Port DSCP**. Przełącznik przed przystąpieniem do klasyfikacji ramek do QoS class może wcześniej znacznik DSCP zmodyfikować do wymaganej wartości. Do tego służy opcja dostępna po zaznaczeniu pola checkbox w kolumnie **Translate**. Zmiany DSCP w ramkach są dokonywane na podstawie wpisów w menu dostępnym po kliknięciu na linki **Configuration** → **QoS** → **DSCP Translation**. Kolumna **DSCP** tego menu przedstawia wszystkie możliwe wartości DSCP, natomiast w kolumnie **Ingress Translate** można wybrać na jaką dana wartość ma być zmieniana. **DSCP Based** - Kliknij, aby włączyć klasyfikację portu wejściowego QoS opartą na DSCP.

1

WRED Group - Kontroluje członkostwo w grupie WRED.

QoS	Ingres	ss Por	t Tag (Class	ificat	tion Por
Tagg	ed Frai	mes Se	ttings			
Tag	Classifi	cation	Disabl	ed 🔻		
(PCP	, DEI) t	o (QoS	class,	DP le	evel)	Mapping
PCF	P DEI	QoS	class	DP I	evel	
*	*	\diamond	T	\diamond	T	
0	0	1	•	0	Ŧ	
0	1	1	T	1	T	
1	0	0	T	0	T	
1	1	0	۲	1	۲	
2	0	2	T	0	T	
2	1	2	۲	1	۲	
3	0	3	•	0	T	
3	1	3	T	1	T	
4	0	4	T	0	۲	
4	1	4	T	1	T	
5	0	5	T	0	۲	
5	1	5	T	1	T	
6	0	6	T	0	۲	
6	1	6	T	1	T	
7	0	7	T	0	۲	
7	1	7	T	1	T	
Save	e Res	et Ca	ncel			

Rys. 118. Ingress Port Classification klasyfikacja ramek tagowanych

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	100/147
------	------	-----------------------------------	------------	---------



QoS Port DSCP Configuration

Port		Ingress	Egress
1011	Translate	Classify	Rewrite
*		<> ▼	<> ▼
10GigabitEthernet 1/1	✓	DSCP=0 V	Enable 🗸
10GigabitEthernet 1/2		Disable 🗸	Disable 🗸
10GigabitEthernet 1/3		Disable 🗸	Disable ◄
10GigabitEthernet 1/4		Disable 🗸	Disable 🗸
GigabitEthernet 1/1		Disable 🗸	Disable 🗸
GigabitEthernet 1/2		Disable 🗸	Disable 🗸
GigabitEthernet 1/3		Disable 🗸	Disable 🗸
GigabitEthernet 1/4		Disable 🗸	Disable 🗸
GigabitEthernet 1/5		Disable 🗸	Disable ◄
GigabitEthernet 1/6		Disable 🗸	Disable 🗸
GigabitEthernet 1/7		Disable 🗸	Disable 🗸
GigabitEthernet 1/8		Disable 🗸	Disable 🗸
GigabitEthernet 1/9		Disable 🗸	Disable 🗸
GigabitEthernet 1/10		Disable 🗸	Disable 🗸
GigabitEthernet 1/11		Disable 🗸	Disable 🗸

Rys. 119. Konfiguracja klasyfikacji ramek wejściowych warstwy trzeciej i wartości znacznika DSCP w ramkach wyjściowych

DSCP Tra	nslation					
DSCD	Ingre	SS	Egress			
Dace	Translate	Classify	Remap DP0	Remap DP1		
*	< ▼		< ▼	<> ▼		
0 (BE)	0 (BE) 🔻		0 (BE) 🔻	0 (BE) 🔻		
1	1 •		1 •	1 •		
2	2 🔻		2 🔻	2 🔻		
3	3 🔻		3 🔻	3 🔹		
4	4 🔻		4 ▼	4 🔻		
5	5 🔻		5 🔻	5 •		
6	6 v		6 🔹	6 •		
7	7 🔻		7 🔻	7 •		
8 (CS1)	8 (CS1) 🔻		8 (CS1) 🔻	8 (CS1) 🔻		
9	9 🔻		9 🔻	9 🔻		
10 (AF11)	10 (AF11) 🔻		10 (AF11) 🔻	10 (AF11) 🔻		
11	11 🔻		11 🔻	11 🔻		
12 (AF12)	12 (AF12) 🔻		12 (AF12) 🔻	12 (AF12) 🔻		
13	13 🔻		13 🔻	13 🔻		
14 (AF13)	14 (AF13) 🔻		14 (AF13) 🔻	14 (AF13) 🔻		

Rys. 120. Konfiguracja translacji znaczników DSCP

Konfiguracja sposobu klasyfikacji na podstawie DSCP odbywa się w menu **QoS Port DSCP Configuration** w kolumnie **Classify**. Dostępne są cztery opcje:

Disable – klasyfikacja ramek nie odbywa się i wszystkie ramki klasyfikowane są do QoS class 0.

DSCP=0 – klasyfikowane są tylko ramki, które posiadają pole DSCP równe 0, wartość tą można osiągnąć również przez wcześniejsze użycie opcji **DSCP Translation**.

Selected – do klasyfikacji brane są tylko ramki z wartością DSCP dla której zaznaczona i zatwierdzona jest opcja **Classify** w menu **DSCP Translation**.

All – wszystkie ramki warstwy trzeciej są klasyfikowane według pola DSCP. Konfiguracja klasyfikacji ramek odbywa się w menu dostępnym pod linkiem Configuration → QoS → DSCP-Based Qos. Kolumna DSCP zawiera wszystkie możliwe wartości jakie to pole może przyjąć, opcja Trust pozwala wybrać tylko "zaufane" usługi dla których ma odbywać się mapowanie do QoS class i DP level. Kolumny QoS Class i DPL pozwalają na przypisanie do każdej usługi kolejki QoS i znacznika DP Level. Zatwierdzenie zmian obywa się przez naciśnięcie przycisku Save.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	101/147
------	------	-----------------------------------	------------	---------



DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*		<> ♥	◇♥
0 (BE)		0 🗸	0 🗸
1		0 🗸	0 🗸
2		0 🗸	0 🗸
3		0 🗸	0 🗸
4		0 🗸	0 🗸
5		0 🗸	0 🗸
6		0 🗸	0 ~
7		0 🗸	0 🗸
8 (CS1)		0 🗸	0 ~
9		0 🗸	0 🗸
10 (AF11)		0 🗸	0 ~
11		0 🗸	0 🗸
12 (AF12)		0 🗸	0 ~
13		0 🗸	0 🗸
14 (AF13)		0 🗸	0 🗸
15		0 ~	0 ~
16 (CS2)		0 🗸	0 🗸
17		0 🗸	0 ~

Rys. 121. Konfiguracja klasyfikacji na podstawie znacznika DSCP ramek warstwy trzeciej

Menu **QoS Port DSCP Configuration** pozwala również na modyfikację pola DSCP w ramkach wychodzących z przełącznika. Służy do tego konfiguracja w kolumnie **Egress Rewrite**. W menu tym dostępne są cztery opcje:

Disable – znaczniki DSCP nie są zmieniane.

Enable – znacznik DSCP jest nadawany w zależności od zatwierdzonych ustawień w menu DSCP Classification.

Remap DP Unaware – znacznik DSCP jest zmieniany w zależności od ustawień kolumny **Egress Remap DP0** w menu **DSCP Translation**.

Remap DP Aware - znacznik DSCP jest zmieniany w zależności od wartości pola DP Level dla ramki i ustawień kolumny **Egress Remap DP0** i **Egress Remap DP1** w menu **DSCP Translation**.

QoS Class	DSCP DP0		DSCP	DP1	DSCP	DP2	DSCP DP3		
*	\diamond	~	\diamond	~	\diamond	*	\diamond	<	
0	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
1	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
2	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
3	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
4	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
5	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
6	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	
7	0 (BE)	~	0 (BE)	~	0 (BE)	~	0 (BE)	~	

DSCP Classification

Save Reset

Rys. 122. Konfiguracja znacznika DSCP w ramkach wychodzących

5.43.2 Policer portu wejściowego Ingress Port Policers

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	102/147
------	------	-----------------------------------	------------	---------



Menu to pozwala na ograniczenie pasma dla ramek wejściowych dla każdego portu fizycznego, oddzielnie i do poziomu zdefiniowanego przez użytkownika. Policer dokonuje pomiaru wielkości pasma przychodzącego w drugiej warstwie modelu ISO/OSI.

Qos ingress Port Policers	QoS	Ingress	Port	Po	licers
---------------------------	-----	---------	------	----	--------

Rate	Unit	Flow Control
500	< ▼	
500	kbps 🔻	
	500 500 500 500 500 500 500 500 500	500 <> ▼ 500 kbps ▼

Save Reset

Rys. 123. Konfiguracja Policerów portu wejściowego

Znaczenie poszczególnych kolumn jest następujące:

Port – określa fizyczny port którego to ustawienia będzie dotyczyło.

Enabled – pole checkbox, zaznaczenie tego pola i zatwierdzenie zmian spowoduje, że zostanie włączone ograniczenie pasma na danym porcie w kierunku wejściowym do poziomu z kolumn **Rate** i **Unit**.

Rate – określa ilościową wielkość ograniczenia. Wartość tego pola ograniczona jest do 100-1000000 kiedy jednostką jest kbps lub fps i do 1-3300 kiedy jednostką jest Mbps lub kfps.

Unit – jednostkę w jakich to ograniczenie jest kontrolowane, znaczenie skrótów użytych w tym polu wyboru jest następujące: **fps** – organicznie w ramkach na sekundę, **kfps** – organicznie w tysiącach ramek na sekundę, **kbps** – ograniczenie w kilobitach na sekundę, **Mbps** – ograniczenie w megabitach na sekundę.

5.43.3 Policer kolejek wejściowych Ingress Queue Policers

Menu to pozwala na ograniczenie pasma dla ramek wejściowych dla każdego portu fizycznego i dla każdej sprzętowej kolejki wejściowej, oddzielnie i do poziomu zdefiniowanego przez użytkownika. Policer dokonuje pomiaru wielkości pasma przychodzącego w drugiej warstwie modelu ISO/OSI.

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
FUIL	Enable							
*								
10GigabitEthernet 1/1								
10GigabitEthernet 1/2								
10GigabitEthernet 1/3								
10GigabitEthernet 1/4								
GigabitEthernet 1/1								
GigabitEthernet 1/2								
GigabitEthernet 1/3								
GigabitEthernet 1/4								
GigabitEthernet 1/5								
GigabitEthernet 1/6								
GigabitEthernet 1/7								
GigabitEthernet 1/8								
GigabitEthernet 1/9								
GigabitEthernet 1/10								

QoS Ingress Queue Policers

Rys. 124. Konfiguracja Policerów kolejek sprzętowych portów wejściowych

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	103/147
------	------	-----------------------------------	------------	---------



Znaczenie poszczególnych kolumn jest następujące:

Port – określa fizyczny port którego to ustawienia będzie dotyczyło.

Queue 0 do **Queue 7 Enable** – pole checkbox, którego zaznaczenie powoduje włączenie ograniczenia pasma dla danej kolejki. Zaznaczenie chociaż jednego z pól spowoduje wyświetlenie dodatkowego menu dla danej kolejki z kolumnami **Rate** i **Unit**.

Rate – określa ilościową wielkość ograniczenia. Wartość tego pola ograniczona jest do 100-1000000 kiedy jednostką jest kbps i do 1-3300 kiedy jednostką jest Mbps.

Unit – określa jednostkę w jakiej to ograniczenie jest kontrolowane, znaczenie skrótów użytych w tym polu wyboru jest następujące: **kbps** – ograniczenie w kilobitach na sekundę, **Mbps** – ograniczenie w megabitach na sekundę.

	_			- 0	0				0	0	1		E	0			
Port			Jueu	eu	Queue 1			Jueue 2	Queue 3	Queue 4			aueue o	Queue 6	<u> </u>		ueue /
	E	Rate		Unit	Enable	E	Rate	Uni	Enable	Enable	E	Rate	Uni	t Enable	E	Rate	Unit
*		500		~			500] 🗆			500	◇ ∨			500	◇ ♥
10GigabitEthernet 1/1	$\mathbf{\overline{\mathbf{v}}}$	500	kbps	s 🗸			500	kbps 🗸) 🗆			500	kbps 🗸] 🗆		500	kbps 🛩
10GigabitEthernet 1/2		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸			500	kbps 🛩
10GigabitEthernet 1/3		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸] 🗆		500	kbps 🗸
10GigabitEthernet 1/4		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/1		500	kbps	s 🗸		~	500	kbps 🗸] 🗆			500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/2		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/3		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸]0		500	kbps 🗸
GigabitEthernet 1/4		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/5		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸	10		500	kbps 🗸
GigabitEthernet 1/6		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/7		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸		~	500	kbps 🗸
GigabitEthernet 1/8		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸			500	kbps 🗸
GigabitEthernet 1/9		500	kbps	s 🗸			500	kbps 🗸] 🗆			500	kbps 🗸] 🗆		500	kbps 🗸
GigabitEthernet 1/10		500	kbps	s 🗸			500	kbps 🗸				500	kbps 🗸			500	kbps 🗸

QoS Ingress Queue Policers

Rys. 125. Konfiguracja ograniczenia pasma dla kolejek wejściowych

5.44 Planista portu wyjściowego Egress Port Schedulers and Shapers

Każdy fizyczny port urządzenia jest wyposażony w własny układ scheduler i shaper, dodatkowo każda z ośmiu kolejek sprzętowych ma wbudowany własny układ shaper. Układy te przekazują ramki do wyjścia w jednym z dwóch trybów:

Strict priority – ramki z wyższym priorytetem wysyłane są zawsze jako pierwsze,

Deficit Weighted Round Robin (DWRR) – kolejki 6 i 7 pracują zawsze jako strict, a pozostałe kolejki od 0 do 5 pracują z podziałem wagowym określanym procentowo dla każdej z nich.

Dostęp do konfiguracji układów Schedulers jest możliwy w oknie dostępnym pod linkiem **Configuration** → **QoS** → **Port Scheduler**. Okno to przedstawia tylko bieżącą konfigurację układów Schedulers dla wszystkich fizycznych portów i dla pięciu pierwszych kolejek. W przypadku, gdy dany port pracuje jako strict priority to wyświetlane są tylko znaki '-'.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	104/147
------	------	-----------------------------------	------------	---------



QoS Egress Port Schedulers

Devt	Mada							We	ight
Port	wode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
10GigabitEthernet 1/1	2 Queues Weighted	50%	50%	-	-	-	-	-	-
10GigabitEthernet 1/2	Strict Priority	-	-	-	-	-	-	-	-
10GigabitEthernet 1/3	Strict Priority	-	-	-	-	-	-	-	-
10GigabitEthernet 1/4	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/1	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/2	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/3	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/4	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/5	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/6	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/7	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/8	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/9	Strict Priority	-	-	-	-	-	-	-	-
GigabitEthernet 1/10	Strict Priority	-	-	-	-	-	-	-	-

Rys. 126. Konfiguracja układu Scheduler

Konfiguracja układu Scheduler odbywa się niezależnie dla każdego portu, a dostęp do niej jest możliwy po kliknięciu na linki na numerze fizycznego portu w kolumnie **Port** Dostęp do tej konfiguracji wymaga jeszcze zmiany sposobu przekazywania ramek na **DWRR**. W polu **Scheduler Mode** należy wybrać opcję **Weighted**. Uaktywnią się pola w kolumnie **Queue Scheduler Weight** i **Percent**. W polach **Weight** można wpisać wagowy udział danej kolejki i priorytetu w kolejce wyjściowej, natomiast w polu **Percent** zostanie obliczony automatycznie udział procentowy na podstawie wpisów we wszystkich polach. Pole wyboru w prawym górnym rogu pozwala na bezpośrednie przejście do konfiguracji tych parametrów dla innych portów.



Rys. 127. Konfiguracja układów scheduler dla portu

Dostęp do konfiguracji układów Shapers jest możliwy pod linkiem **Configuration** \rightarrow **QoS** \rightarrow **Port Shaping**. Okno to przedstawia tylko bieżącą konfigurację układów Shapers dla wszystkich fizycznych portów i dla wszystkich obsługiwanych kolejek.

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 10	05/147
---	--------



Konfiguracja układu Scheduler odbywa się niezależnie dla każdego portu, a dostęp do niej jest możliwy po kliknięciu na linki na numerze fizycznego portu w kolumnie **Port**.

QoS Egress Port Shapers

Port									Shapers
FUIL	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
10GigabitEthernet 1/1	-	-	500 kbps	-	-	100 Mbps	-	-	500 kbps
10GigabitEthernet 1/2	-	-	-	-	-	-	-	-	-
10GigabitEthernet 1/3	-	-	-	-	-	-	-	-	-
10GigabitEthernet 1/4	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/1	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/2	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/3	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/4	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/5	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/6	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/7	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/8	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/9	-	-	-	-	-	-	-	-	-
GigabitEthernet 1/10	-	-	-	-	-	-	-	-	-

Układ ten pozwala na ograniczenie pasma dla wszystkich kolejek w kierunku wyjściowym i ustawienie zbiorczego ograniczenia pasma wyjściowego na port.

W polu **Queue Shaper** kolumna **Enable** pozwala na włączenie lub wyłączenie ograniczenia na daną kolejkę. Pola w kolumnach **Rate** i **Unit** pozwalają na określenie wielkości tego ograniczenia w sposób taki jak dla kolejek wejściowych. Kolumna **Excess** określa czy dana kolejka może korzystać z wolnego pasma wyjściowego w momencie jak wykorzysta swój przydział.

W polu **Port Shaper** można określić zbiorcze ograniczenie pasma wyjściowego dla portu fizycznego, w taki sam sposób jak dla kolejek.



Rys. 129. Konfiguracja układów Shaper dla portu

5.44.1 Priorytet ramek wyjściowych Egress Port Tag Remarking

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	106/14
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	106/14



Funkcja ta pozwala ustawiać znaczniki PCP i DEI w wychodzących ramkach tagowanych zgodnie z IEEE802.1q. Dostępna jest po kliknięciu na linki **Configuration** → **Qos** → **Port Tag Remarking**. Konfiguracja jest niezależna dla każdego fizycznego portu i dostępna po kliknięciu na linki w kolumnie **Port**.

Port	Mode
10GigabitEthernet 1/1	Classified
10GigabitEthernet 1/2	Classified
10GigabitEthernet 1/3	Classified
10GigabitEthernet 1/4	Classified
GigabitEthernet 1/1	Classified
GigabitEthernet 1/2	Classified
GigabitEthernet 1/3	Classified
GigabitEthernet 1/4	Classified
GigabitEthernet 1/5	Classified
GigabitEthernet 1/6	Classified
GigabitEthernet 1/7	Classified
GigabitEthernet 1/8	Classified
GigabitEthernet 1/9	Classified
GigabitEthernet 1/10	Classified

Rys. 130. Bieżąca konfiguracja priorytetów ramek wychodzących

Funkcja ta ma trzy tryby pracy, które ustawia się w polu **Tag Remarking Mode**. W momencie wyboru stosownego trybu zostanie wyświetlone menu, które pozwala dokończyć konfigurację.

QoS Egress Port Tag Remarking 10GigabitEthernet 1/1					
Tag Remarking Mode Default 🗸					
PCP/DEI Conf	figuratio	n			
Default PCP	0 🗸				
Default DEI	0 🗸				
Save Reset	Cance	Ι			

Rys. 131. Konfiguracja priorytetu ramek wyjściowych w trybie default dla portu

Pierwszy tryb **Classified** pozostawia wartości w polach PCP i DEI nie naruszone względem tych jakie zostały odebrane przez przełącznik. W przypadku, gdy ramka została odebrana jako nie tagowana i w trakcie przetwarzania przez przełącznik zostaje jej nadany tag to te pola otrzymują wartość 0.

Tryb **Default** pozwala ustawić dla wszystkich tagowanych ramek wychodzących pola PCP i DEI do tej samej wartości. W polu **Default PCP** wybiera się wartość którą będzie przełącznik **HYPERION** umieszczał w ramkach wychodzących w polu PCP ramek tagowanych, a w polu **Default DEI** wybiera się wartość wskaźnika DEI dla tych ramek. Ustawienia zatwierdza się przyciskiem **Save**.

Tryb **Mapped** pozwala na nadanie wartości pól PCP i DEI w zależności od QoS class i DP level. Kolumny **QoS class** i **DP level** wyświetlają wszystkie możliwe kombinacje tych parametrów, natomiast w kolumnach **PCP** i **DEI** można wybrać stosowną wartość dla każdej z tych kombinacji.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	107/147
------	------	-----------------------------------	------------	---------



QoS Egress Port Tag Remarking 10GigabitEthernet 1/1

Tag Remarking Mode Mapped V

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP		DEI	
*	*	\diamond	~	\diamond	<
0	0	1	~	0	~
0	1	1	~	1	~
1	0	0	~	0	~
1	1	0	~	1	~
2	0	2	~	0	~
2	1	2	~	1	~
3	0	3	~	0	~
3	1	3	~	1	~
4	0	4	~	0	~
4	1	4	~	1	~
5	0	5	~	0	~
5	1	5	~	1	~
6	0	6	~	0	~
6	1	6	~	1	~
7	0	7	~	0	~
7	1	7	~	1	~

Save Reset Cancel

Rys. 132. Konfiguracja priorytetu ramek wyjściowych w trybie mapped dla portu

5.44.2 Lista kontrolna QoS Control List Configuration

Funkcja ta dostępna jest pod linkiem **Configuration > QoS > QoS Control List**, pozwala na stworzenie do 256 list kontrolnych dla różnego typu ramek i protokołów łącznie z protokołami warstwy transportowej w zależności od aplikacji i przydzielenia ich do jednej z ośmiu QoS class. Znaczenie poszczególnych kolumn jest następujące:

QCE# – index QCE (QoS Control Entry).

Port – przedstawia listę portów fizycznych dla tej listy.

Frame Type – przedstawia typ ramek jaką dana lista będzie kontrolować możliwe wartości to: *Any* – do danej listy będą zaliczane wszystkie ramki.

Ethernet – tylko ramki Ethernet z polem Ether Type w zakresie wartości 0x600-0xFFFF.

LLC – tylko ramki protokołu LLC (Logical Link Control).

SNAP – tylko ramki protokołu SNAP (Subnetwork Access Protocol).

IPv4 – tylko ramki protokołu IPv4.

IPv6 – tylko ramki protokołu IPv6.

SMAC – wyświetla źródłowy adres MAC kontrolowany przez tą listę.

DMAC – wyświetla adres przeznaczenia MAC kontrolowany przez tą listę, możliwe wartości to:

Any – wszystkie ramki adres przeznaczenia nie jest analizowany.

Unicast – tylko ramki Unicast.

Multicast – tylko ramki Multicast.

Broadcast - tylko ramki Broadcast.

VID – przedstawia numer lub zakres numerów sieci VLAN jaką ta lista kontroluje.

PCP – przedstawia numer PCP jaki ta lista kontroluje, możliwe wartości są w zakresie od 0 do 7.

DEI – przedstawia numer DEI jaki ta lista kontroluje możliwe wartości to 0 lub 1.

Action – Kolumna ta informuje do jakiej QoS class będą zaliczane ramki, które dana grupa wybierze po przeanalizowaniu wcześniejszych parametrów. Znaczenie pól jest następujące

Class: Numer QoS class do której zostaną ramki przydzielone.

DPL: Wartość Drop Precedence Level jaka zostanie dopisana ramki w celu dalszej jej analizy przez układy QoS przełącznika.

DSCP: Numer DSCP (DiffServ) do którego zostaną ramki przydzielone.

Ostatnia kolumna wyświetla przyciski do modyfikacji listy, znaczenie symboli jest następujące: **Plus** (pierwszy na górze) – pozwala dodać nową listę przed bieżącą.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	108/147
------	------	-----------------------------------	------------	---------


e – pozwala na edycję bieżącej listy.

Strzałka w górę – pozwala przesuwać listę w górę w celu przypisania kolejności jej analizowania przez układ Policera, jeżeli ramka zostanie przypisana do danej grupy to dalej jest już niesprawdzana pod kątem zgodności z listami poniżej.

Strzałka w dół – pozwala przesuwać listę w dół w celu przypisania kolejności jej analizowania. **x** – usuwa bieżącą listę.

Plus (ostatni na dole) – pozwala dodać nową listę jako następną po bieżącej.

QoS Control List Configuration

OCE	Port	DMAC	SMAC	Tag		DCD	DEI	Frame						Action	
QUE	For	DIVIAC	SIVIAC	Туре		FGF		Type	CoS	DPL	DSCP	PCP	DEI	Policy]
1	1-36	Unicast	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	
															Ð

Rys. 133. Bieżąca konfiguracja list kontrolnych QoS QCL

Dodanie nowej listy kontrolnej odbywa się przez naciśnięcie przycisku (+) w kolumnie pierwszej od prawej.

QCE Configuration

	Port Members	
10GigabitEthernet 1/1 10GigabitEthernet 1/2 10GigabitEthernet 1/3 10GigabitEthernet 1/4 GigabitEthernet 1/2 GigabitEthernet 1/3 GigabitEthernet 1/3 GigabitEthernet 1/5 GigabitEthernet 1/5	GigabitEthemet 18 GigabitEthemet 19 GigabitEthemet 111 GigabitEthemet 111 GigabitEthemet 113 GigabitEthemet 114 GigabitEthemet 115 GigabitEthemet 117 GigabitEthemet 117 GigabitEthemet 119 GigabitEthemet 120 GigabitEthemet 120	GigabitEthemet 1/22 GigabitEthemet 1/23 GigabitEthemet 1/25 GigabitEthemet 1/25 GigabitEthemet 1/27 GigabitEthemet 1/20 GigabitEthemet 1/30 GigabitEthemet 1/31 GigabitEthemet 1/31

Key Parameters

DMAC	Multicast 🗙
CHAC	A
SMAC	Any 🗸
Tag	Tagged 🗸
VID	Specific Value: 100
РСР	2 🗸
DEI	0 🗸
Inner Tag	Untagged 🗸
Inner VID	Any 🗸
Inner PCP	Any 🗸
Inner DEI	Any 🗸
Frame Type	IPv4 🗸

IPv4 Parameters

Protocol	TCP 🖌
SIP	Any 🗸
DIP	Any 🗸
IP Fragment	Any 🗸
DSCP	Any 🗸

Save Reset Cancel

Action Parameters

CoS	0 🗸
DPL	Default 🗸
DSCP	Default 🗸
РСР	Default 🗸
DEI	Default 🗸
Policy	

TCP Parameters						
Sport	Any	~				
Dport	Any	~				

Rys. 134. Konfiguracja listy kontrolnej QCL

Znaczenie poszczególnych parametrów pól jest następujące: **Port members** – określa porty fizyczne urządzenia jakie będą brane przy analizie przez tą listę.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	109/147
------	------	-----------------------------------	------------	---------



Key Parameters – określa kluczowe parametry ramki jakie musi spełnić, aby dana lista mogła dokonać modyfikacji, a znaczenie pól jest następujące:

Tag – określa czy ramka ma poosiadać znacznik zgodnie z IEEE802.1Q.

Any – dowolne ramki,

Untag – ramki tylko nie tagowane,

Tag - ramki tylko tagowane,

W przypadku wyboru w polu **Tag** ramek tagowanych lub dowolnych, można okręcić jaki VLAN ID, pola PCP i DEI ma posiadać ramka klasyfikowana do danej listy kontrolnej.

VID – VLAN ID

Specific – pozwala na określenie tylko jednego VLAN ID, które należy wpisać w pole Value,

Range – pozwala na określenie zakresu VLAN ID, który należy wpisać w pola From i To.

PCP – pozwala określić wartość pola PCP lub zakres tej wartości.

DEI – pozwala określić wartość w polu DEI

SMAC – adres źródłowy ramek, może być dowolny opcja **Any**, lub sprecyzowany opcja **Specific** i w polu obok należy wpisać trzy najbardziej znaczące bajty adresu źródłowego MAC.

DAMC – określa typ adresu przeznaczenia dla ramek: **UC** – adres unicast, **MC** – adres multicast, **BC**– adres broadcast.

Frame Type – określa typ protokołu ramki:

Any – ramki dowolnego protokołu.

Ethertype – ramki, które w polu type posiadają wartość heksadecymalną od 0x600 do 0xFFFF. Po wybraniu tej opcji pojawi się dodatkowe menu **EtherType Parameters** w którym w polu **Ether Type** można określić typ ramek jaki dana lista będzie klasyfikować. Z listy wyboru można wybrać **Any**, wtedy wszystkie ramki z polem Ether Type w zakresie od 0x600 do 0xFFFF będą klasyfikowane lub **Specific** i w polu **Value** należy wpisać wartość heksadecymalna pola typu ramki jaką ta lista będzie klasyfikować.

LLC – ramki typu Logical Link Control specyfikowane w IEEE 802.2. Wybranie tej opcji spowoduje że pojawi się dodatkowe menu **LLC Parameters** w którym można dokładniej sprecyzować pola tej ramki jakie mają być sprawdzane przez daną listę kontrolną. **SSAP Address** – adres SSAP (Source Service Access Point), gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Specific** to można określić ten adres przez wpisanie odpowiedniej wartości w polu **Value**, dopuszczalne wartości są od 0x00 to 0xFF. **DSAP Address** – adres DSAP(Destination Service Access Point), gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Specific** to można określić ten adres przez wpisanie odpowiedniej wartości w polu **Value**, dopuszczalne wartości są od 0x00 to 0xFF. **Control** – pole (Valid Control field), gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Specific** to można określić ten adres przez wpisanie odpowiedniej wartości w polu **Value**, dopuszczalne wartości są od 0x00 to 0xFF.

SNAP – ramki typu Subnetwork Access Protocol specyfikowane w IEEE 802. Wybranie tej opcji spowoduje, że pojawi się dodatkowe menu **SNAP Parameters** w którym można dokładniej sprecyzować pola tej ramki jakie mają być sprawdzane przez daną listę kontrolną. **PID** – Protocol IDentifier, gdy wybrana jest opcja **Any** to pole to nie jest sprawdzane przez listę, a gdy wybrana jest opcja **Specific** to można określić ten adres przez wpisanie odpowiedniej wartości w polu **Value**, dopuszczalne wartości są od 0x0000 to 0xFFFF.

IPv4 – ramki protokołu IP (internet protocol) w wersji 4. Wybranie tej opcji spowoduje że pojawi się dodatkowe menu **IPv4 Parameters**, w którym można dokładniej sprecyzować pola nagłówka ramki IPv4 jakie mają być sprawdzane przez daną listę kontrolną. **Protocol** – pozwala określić protokół warstwy transportowej modelu ISO/OSI. Dostępne opcje to **Any** – lista nie sprawdza typu protokołu, **UDP** – protokół UDP (User Datagram Protocol), **TCP** – protokół TCP (Transmission Control Protocol), **Other** – pozwala na określenie typu protokołu przez podanie w polu **Value** znacznika tego protokołu umieszczanego w ramkach IPv4 w polu **Protocol. Source IP** – pozwala kontrolować przez tą listę adres źródłowy IP. **Any** oznacza, że dana lista nie kontroluje tego parametru, natomiast **Specific** pozwala kontrolować zakres adresów przez wprowadzenie parametrów **IP** i **Mask** w formacie: x.y.z.w, gdzie x, y, z, i w są liczbami decymalnymi w zakresie od 0 do 255. Parametr **Mask** musi przyjąć taką wartość żeby po przekonwertowaniu do 32 bitowej liczby

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	110/147



binarnej i czytaniu od lewej do prawej, wystąpienie pierwszego bitu równego 0 powodowało że kolejne bity też będą zerami. **IP Fragment** – pozwala określić jakie ramki ma kontrolować ta lista pod względem opcji fragmentowania. **Any** – nie sprawdza tego znacznika, **Yes** – tylko ramki fragmentowane, **No** – tylko ramki niefragmentowane. **DSCP Diffserv Code Point value** (DSCP): również pozwala na kontrolowanie tego parametru w ramkach IPv4, przez sprecyzowanie jednej wartości **Specific** lub zakresu wartości **Range**, lub brak kontroli **Any**. DSCP wartości mogą przyjąć zakres od 0 do 63 włączając BE, CS1-CS7, EF lub AF11-AF43.

IPv6 – ramki protokołu IP (internet protocol) w wersji 6. Wybranie tej opcji spowoduje że pojawi sie dodatkowe menu IPv6 Parameters, w którym można dokładniej sprecyzować pola nagłówka tej ramki jakie mają być sprawdzane przez daną listę kontrolną. Protocol – pozwala określić protokół warstwy transportowej modelu ISO/OSI. Dostępne opcje to Any – lista nie sprawdza typu protokołu, UDP – protokół UDP, TCP – protokół TCP, Other – pozwala na określenie typu protokołu przez podanie w polu Value znacznika tego protokołu umieszczanego w ramkach IPv6 w polu Protocol. Source IP(32 LSB) – pozwala kontrolować przez ta liste 32 najmłodsze bity adresu źródłowy IP. Any oznacza że dana lista nie kontroluje tego parametru, natomiast Specific pozwala kontrolować ten zakres adresów przez wprowadzenie parametrów IP i Mask w formacie: x.y.z.w, gdzie x, y, z, i w są liczbami decymalnymi w zakresie od 0 do 255. Parametr Mask musi przyjąć taką wartość żeby po przekonwertowaniu do 32 bitowej liczby binarnej i czytaniu od lewej do prawej, wystąpienie pierwszego bitu równego 0 powodowało że kolejne bity też bedą zerami. DSCP Diffserv Code Point value (DSCP) również pozwala na kontrolowanie tego parametru w ramkach IPv6, przez sprecyzowanie jednej wartości Specific lub zakresu wartości Range, lub brak kontroli Any. DSCP wartości mogą przyjąć zakres od 0 do 63 włączając BE, CS1-CS7, EF lub AF11-AF43. Wartość DSCP dla ramek IPv6 jest pobierana z pola Traffic Class.

W przypadku klasyfikacji ramek IPv4 i IPv6 i protokołu warstwy transportowej UDP lub TCP, można wprowadzić dodatkową klasyfikację po numerach portów źródłowych i przeznaczenia. Odpowiednie wpisy należy wprowadzić w pola oznaczone jako **Sport** i **Dport**. Menu z tymi pola pojawi się tylko wtedy, gdy zostanie w polu **Protocol** wybrana opcja **TCP** lub **UDP**.

Pola **Action Parameters** określają w jaki sposób ramki będą klasyfikowane, gdy spełnią wszystkie powyższe kryteria. Znaczenie pól jest następujące:

CoS – określa QoS class do której dana lista będzie kierować ramki.

DPL – określa znacznik DPL jaki zostanie przypisany do ramki przez daną lista.

DSCP - określa znacznik DSCP w ramkach IP jaki zostanie przypisany do ramki przez daną lista.

Po zakończeniu wprowadzania parametrów należy zatwierdzić zmiany przyciskiem Save.

5.44.3 Ochrona przed sztormem – Storm Control Configuration

Funkcjonalność ta pozwala zabezpieczyć sieć i urządzenia przed sztormem ramkami i atakami typu DoS (Denial of Service). Menu konfiguracji dostępne jest pod linkiem **Configuration** \rightarrow **QoS** \rightarrow **Storm Policing**

Dla określonego typu ramki, aby włączyć tą funkcję należy zaznaczyć pole typu chechbox w kolumnie **Enable** i wybrać wielkość akceptowalnego ruchu w ramkach na sekundę w polu **Rate** (**pps**). Dostępne typy ramek to:

Unicast – ramki typu unicast z nieznanym adresem przeznaczenia, który nie został zarejestrowany w tablicy MAC.

Multicast – ramki typu multicast z najmłodszym bitem pierwszego bajtu adresu przeznaczenia MAC równym 1, ale nie typu broadcast.

Broadcast – ramki z adresem przeznaczenia MAC: FF-FF-FF-FF-FF.

REV.	1		06	
------	---	--	----	--



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast		10	fps 🗸
Multicast		10	kbps
Broadcast		10	Mbps
			kfps

Rys. 135. Konfiguracja ochrony przed sztormem

Układ analizuje wszystkie ramki typów podanych wyżej i je zlicza, w momencie w którym zostanie zliczona ilość ramek równa tej wprowadzonej w polu Rate (pps), przełacznik odrzuca ten typ ramek do następnego okresu pomiarowego.

Port Storm Policer Configuration										
Dort		Unicas	t Frames		Broadcas	t Frames		Unknow	n Frames	
Pon	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit	
*		500	<> ♥		500	< ▼		500	< ♥	
10GigabitEthernet 1/1		500	kbps 🗸		500	kbps 🛩		500	kbps 🐱	
10GigabitEthernet 1/2		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸	
10GigabitEthernet 1/3		500	kbps 🐱		500	kbps 🛩		500	kbps 🐱	
10GigabitEthernet 1/4		500	kbps 🖌		500	kbps 🗸		500	kbps 🗸	
GigabitEthernet 1/1		500	kbps 🖌		500	kbps 🖌		500	kbps 🗸	
GigabitEthernet 1/2		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸	
GigabitEthernet 1/3		500	kbps 🗸		500	kbps 🛩		500	kbps 🗸	
GigabitEthernet 1/4		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸	
GigabitEthernet 1/5		500	kbps 🖌		500	kbps 🖌		500	kbps 🗸	
GigabitEthernet 1/6		500	kbps 🗸		500	kbps 🖌		500	kbps 🗸	
GigabitEthernet 1/7		500	kbps 🗸		500	kbps 🗸		500	kbps 🗸	
GigabitEthernet 1/8		500	kbps 🗸		500	kbps 🖌		500	kbps 🗸	
GigabitEthernet 1/9		500	kbps 🖌		500	kbps 🛩		500	kbps 🐱	
GigabitEthernet 1/10		500	kbps 🖌		500	kbps 🖌		500	kbps 🖌	

Rys. 136.Konfiguracja ochrony przed sztormem na wybranych portach

5.45 Ustawienia podglądu ruchu na portach Mirroring

Urządzenie HYPERION posiada możliwość śledzenia ruchu na danym porcie poprzez kopiowanie każdej ramki na port służący do podglądu ruchu. W zależności od wybranych parametrów mamy możliwość wyboru portu monitorującego ruch jaki i portu monitorowanego. Oprócz tego istnieje możliwość ustawienia kierunku ruchu, który ma być monitorowany.

Żeby przejść do ustawień Mirroring-u klikamy na link **Configuration** \rightarrow **Mirroring**. Wyświetla nam się strona z parametrami do ustawienia podglądu ruchu sieciowego.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	112/147
------	------	-----------------------------------	------------	---------



Mirroring & Remote Mirroring Configuration

	-		
Mode	Dis	abled	
Туре	Min	ror	
VLAN	ID 200		
Reflec	tor Port Por	t 1	
Source	e VLAN(s) Co	onfiguration	
Source	e VLANs		
Port C	onfiguration		
Port Co	onfiguration Source	Intermediate	Destination
Port Co Port	onfiguration Source Disabled V	Intermediate	Destination
Port Control Port	onfiguration Source Disabled ▼ Disabled ▼	Intermediate	Destination
Port Control C	onfiguration Source Disabled ▼ Disabled ▼ Disabled ▼	Intermediate	Destination
Port C Port 1 2 3 4	Disabled ▼ Disabled ▼ Disabled ▼ Disabled ▼ Disabled ▼	Intermediate	Destination
Port C Port 1 2 3 4 5	Source Disabled V Disabled V Disabled V Disabled V Disabled V Disabled V	Intermediate	Destination
Port C Port 1 2 3 4 5 6	Source Disabled V Disabled V Disabled V Disabled V Disabled V Disabled V Disabled V	Intermediate	Destination
Port Co Port 1 1 2 3 4 5 6 7	Source Disabled ▼ Disabled ▼	Intermediate	Destination

Rys. 137. Konfiguracja monitorowania ruchu na portach

Apply Reset

Okno Mirroring & Remote Mirroring Configuration umożliwia konfigurację portu, który będzie służył do monitorowania ruchu na innych wybranych portach.

Znaczenie poszczególnych parametrów pól jest następujące:

Enabled/Disabled – umożliwia włączenie lub wyłączenie monitorowania ruchu na portach

Type – ustawienie trybów dla przełącznika w jakim ma pracować

Mirror - Przełącznik pracuje w trybie Mirror, który będzie służył do monitorowania ruchu na wybranych portach. Port(y) źródłowy(e) i port docelowy znajduja sie na tym przełaczniku.

Source (RMirror) – Przełącznik jest węzłem źródłowym dla monitorowania przepływu. Na tym przełączniku znajduje się port(-y) źródłowy(-y), port(-y) reflektora i port(-y) pośredni(-e).

Intermediate (RMirror) - Przełącznik jest węzłem przekazującym dla monitorowania przepływu i przełącznik jest węzłem wolnego wyboru. Celem jest przekazywanie ruchu z przełącznika źródłowego do przełącznika docelowego poprzez porty pośrednie znajdujące się w tym przełączniku.

Destination (RMirror) – Przełacznik jest wezłem końcowym dla monitorowania przepływu. Na tym przełączniku znajdują się porty docelowe i pośrednie.

VLAN ID - Identyfikator VLAN wskazuje miejsce skopiowania pakietu monitora. Domyślny identyfikator sieci VLAN to 200

Reflector Port - Port reflektora jest metoda przekierowania ruchu do sieci VLAN Remote Mirroring.

SourceVLANs – Pole służy do wpisywania numerów VLAN które mogą obsługiwać Mirroring oparty na VLAN. Dzieki czemu można monitorować niektóre VLAN-v na przełaczniku.

Port Configuration – Okno do konfiguracji roli portów, które przeznaczone będą do zdalnego monitorowania przepływu w przełacznikach.

Port – numery portów do ustawienia portów jako Remote Mirroring.

W kolumnie drugiej mamy **Source** gdzie wybieramy tryby dla portu:

Disabled – wyłącza port z monitorowania, czyli ramki z tego poru nie będą kopiowane do portu monitorujacego

Both – włącza port jako port monitorowany. Ramki, zarówno przychodzące jak i wychodzące z portu są kopiowane na porcie pośrednim / docelowym.

Rx only – włącza port jako port monitorowany, ale tylko ramki przychodzące do portu będą kopiowane do portu monitorującego

Tx only – włącza port jako port monitorowany jednak tylko ramki wychodzące z portu będą kopiowane na port monitorujący.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	113/147



Przycisk **Save** zapisuje ustawienia i zatwierdza zmiany.

5.46 UPnP Configuration

UPnP to skrót od Universal Plug and Play. Celem UPnP jest umożliwienie bezproblemowego łączenia urządzeń i uproszczenie wdrażania sieci w domu (udostępnianie danych, komunikacja i rozrywka) oraz w środowiskach korporacyjnych w celu uproszczenia instalacji komponentów komputerowych.

UPnP Configuration

Mode	Disabled	~
TTL	4	
Advertising Duration	100	

Save Reset

Rys. 138. Okno konfiguracji UPnP

Znaczenie poszczególnych parametrów pól jest następujące:

Mode - Wskazuje tryb pracy UPnP. Możliwe tryby to::

Enabled: Włącz tryb UPnP.

Disabled: Wyłącz działanie w trybie UPnP.

Gdy tryb jest włączony, dwa wpisy ACE są dodawane automatycznie, aby przechwytywać pakiety związane z UPNP do procesora. ACE są automatycznie usuwane, gdy tryb jest wyłączony. **TTL -** Wartość TTL jest używana przez UPnP do wysyłania komunikatów rozgłoszeniowych SSDP. Prawidłowe wartości mieszczą się w zakresie od 1 do 255.

Advertising Duration - Czas trwania, przenoszony w pakietach SSDP, służy do informowania punktu kontrolnego lub punktów kontrolnych, jak często powinny otrzymywać komunikat rozgłoszeniowy SSDP z tego przełącznika. Jeśli punkt kontrolny nie otrzyma żadnej wiadomości w tym czasie, pomyśli, że przełącznik już nie istnieje. Ze względu na zawodny charakter UDP, w standardzie zaleca się, aby takie odświeżanie rozgłaszania odbywało się w czasie krótszym niż połowa czasu trwania rozgłaszania. W implementacji przełącznik wysyła komunikaty SSDP okresowo w odstępach równych połowie czasu trwania rozgłoszenia minus 30 sekund. Prawidłowe wartości mieszczą się w zakresie od 100 do 86400.

5.47 PTP Precision Time Protocol (Profile dostępne w zależności od wybranej wersji)

Precyzyjny protokół czasu jest protokołem używanym do synchronizacji czasu w sieciach komputerowych. W sieci lokalnej umożliwia on osiągnięcie dokładności poniżej 1 mikrosekundy, dzięki czemu można go stosować w systemach pomiarowych i sterujących. Protokół PTP jest opisany przez standard IEEE 1588-2002 (wersja 1), oraz IEEE 1588-2008 (wersja 2). **HYPERION** obsługuje tylko drugą wersję protokołu (wersje 1 i 2 nie są ze sobą kompatybilne). Panel konfiguracji PTP znajduje się w menu **Configuration** \rightarrow **PTP**.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	114/147
------	------	-----------------------------------	------------	---------



PTP External Clock Mode

One_PPS_Mode	Input	*
PPS module	Slot8	~
PPS module input	Synchronizer	~
GPS Module PPS output	Synchronizer	~
PPS offset	0	
External Enable	False	~
Adjust Method	LTC frequency	~
Clock Frequency	1	

PTP Clock Configuration

Delete	C Insta	lock Ince	Device Type		Profile
	<u>0</u>		Mastronly	C37.238-2011	
Delete	1		Ord-Bound 🗸	No Profile 🗸 🗸	
			Inactive	No Profile	
Add New PTP	Clock Save	Re	s Ord-Bound	1588	
			P2pTransp	 G8265.1	
Set client ports			E2eTransp	 G8275.1	
			Mastronly	 C37.238-2011	
			Slaveonly	 C37.238-2017	
			BC-frontend	 	

Rys. 139. Podstawowa konfiguracja PTP

Tabela **PTP External Clock Mode** służy do konfiguracji żródła synchronizacji urządzenia MASTER i nie ma żadnego znaczenia dla pozostałych profili.

One_PPS_Mode - To pole wyboru umożliwia wybranie konfiguracji One_PPS_mode.

Możliwe są następujące wartości:

Output : Włącz wyjście zegara 1 pps

Input : Włącz wejście zegara 1 pps

Disable : Wyłącz wejście / wyjście zegara 1 pps

PPS module - To pole wyboru umożliwia wybranie numeru gniazda, w którym zainstalowany jest moduł GNSS

PPS module input

External - Sygnał 1PPS z zewnętrznego źródła

GPS - Sygnał bezpośrednio z modułu GNSS

Synchronizer - Moduły wykorzystujące systemy DPLL do tłumienia nieprzewidywalnych odchyleń losowych

GPS Module PPS output

External - Sygnał 1PPS z zewnętrznego źródła

GPS - Sygnał bezpośrednio z modułu GNSS

Synchronizer - Moduły wykorzystujące systemy DPLL do tłumienia nieprzewidywalnych odchyleń losowych

External Enable - To pole wyboru umożliwia skonfigurowanie wyjścia zegara zewnętrznego.

Możliwe są następujące wartości:

True : Włącz wyjście zegara zewnętrznego

False : Wyłącz wyjście zegara zewnętrznego

Adjust Method - To pole wyboru umożliwia skonfigurowanie ustawień regulacji częstotliwości.

LTC frequency : Wybierz sterowanie częstotliwością licznika czasu lokalnego (ang. Local Time Counter - LTC)

SyncE-DPLL : Wybierz sterowanie częstotliwością SyncE DPLL, jeśli pozwala na to SyncE Oscillator: Wybierz oscylator niezależny od SyncE do regulacji częstotliwości, jeśli jest obsługiwany przez HW

LTC phase : Wybierz sterowanie fazowe licznika czasu lokalnego (LTC) (zakłada, że częstotliwość jest zablokowana za pomocą SyncE)

Clock Frequency - Umożliwi to ustawienie częstotliwości zegara.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	115/147
------	------	-----------------------------------	------------	---------



Możliwy zakres wartości to 1 - 25000000 (1 - 25 MHz)

W tabeli **PTP Clock Configuration** konfiguruje się funkcje PTP, która będą działać w urządzeniu. Można zdefiniować do czterech instancji PTP (o numerach **Clock Instance** od 0 do 3). Domyślnie nie są skonfigurowane żadne instancje PTP. Aby dodać instancje należy kliknąć przycisk **Add New PTP Clock**, wpisać ustawienia nowej instancji, a następnie zatwierdzić przyciskiem **Save**. Ustawień wprowadzonych w tym panelu nie można później zmienić (w celu zmiany konieczne jest usunięcie instancji i utworzenie nowej). Ustawienia konfigurowane są następujące:

Clock Instance – numer instancji – może być dowolną cyfrą of 0 do 3, która oznacza jeden z zegarów PTP dostępnych w **HYPERION**. Instancja o numerze 0 jest wspomagana sprzętowo (jest więc najdokładniejsza), pozostałe tylko programowo.

Device Type – określa tryb PTP w urządzeniu. Dostępne tryby to:

Inactive – zegar wyłączony,

Ord-Bound – tryb zwykły (Ordinary) lub brzegowy (Boundary) – jest to zegar, który potrafi sam określić swoją rolę w sieci (tzn. czy jest zegarem Master, czy Slave). Jeśli w domenie nie ma wyraźnie określonego urządzenia z trybem Master, to urządzenia tego typu automatycznie wybierają spośród siebie zegar o najlepszych parametrach i używają go jako Master (jeśli jest określony więcej niż jeden Master, to pozostałe urządzenia wybierają najlepszy spośród nich).

P2p transp – przezroczysty tryb peer to peer – zegar tego typu mierzy zarówno czas przebywania ramki synchronizacyjnej w urządzeniu, jak i czas przejścia ramki od poprzedniego urządzenia – oba te czasy są uwzględniane w ramkach synchronizacyjnych.

E2e transp – przezroczysty zegar end to end – podobnie jak p2p mierzy czas przebywania ramki w urządzeniu, ale nie mierzy czasu przejścia ramek pomiędzy urządzeniami, jest więc mniej dokładny od p2p.

Oba typy zegarów przezroczystych nie synchronizują samych siebie do przechodzących ramek synchronizacyjnych (tylko pośredniczą w ich przepływie), a zatem, jeśli zachodzi potrzeba synchronizacji także ich zegarów, należy utworzyć na nich dodatkowe zegary typu Ord-Bound lub Slaveonly.

Masteronly – to urządzenie będzie zawsze typu Master, niezależnie od warunków panujących w sieci. Takie urządzenie periodycznie rozsyła ramki zawierające aktualny czas, które są używane przez urządzenia Slave do synchronizacji swoich zegarów.

Slaveonly – to urządzenie będzie zawsze typu Slave, niezależnie od warunków panujących w sieci. BC-frontend – obecnie tryb nie używany

Profile – wybór odpowiedniego profilu w jakim zegar będzie działać. Do wyboru jest (w zależności od wybranej wersji):

No Profile – bez profilu

1588 – Profil IEEE-1588[™]

G.8265.1 – ITU-T G.8265.1 – Profil częstotliwości (Frequency profile)

G.8275.1 – Profil ITU-T G.8275.1 – Profil czasu i fazy (Time and Phase profile)

C37.238-2011 - profil Power Profile 2011, zgodny ze standardem IEC61850-9-3,

C37.238-2017 - profil Power Profile 2017, zgodny ze standardem IEC61850-9-3,

Jeśli w sieci występują urządzenia z określonym profilem to przy konfiguracji kolejnych musimy wybrać ten sam profil. Synchronizacja na różnych profilach nie będzie działać.

5.47.1 Ustawienia zaawansowane Protokołu PTP

Klikając na instancję zegara w panelu ogólnym PTP można wyświetlić jego konfigurację zaawansowaną.

REV.	1.06 INSTRUKCJA OBSŁUGI : HYPERION-G	GUI 2024.01.04	116/147
------	--------------------------------------	----------------	---------



PTP Clo	ock's Con	figui	ratio	n ar	nd S	stat	us																								
Clock Type and Profile																															
	Clo	ck In:	stanc	e				Dev	/ice	Тур)e	Profile					Apply Profile Defaults														
0 Ord-Bound												No F	Profi	le							n/	а									
Port Ena	Port Enable and Configuration											C C C																			
												Configuration																			
10 GigabitEthemet 1/1 10 GigabitEthemet 1/2 10 GigabitEthemet 1/2	10-39200000000000000000000000000000000000	GigabitEthemet 1/3	GigabitEthemet 1/4 GigabitEthemet 1/6	GigabitEthemet 1/6	GigabitEthernet 1/7	GigabitEthemet 1/8	GigabitEthemet 1/9	GigabitEthemet 1/10	GigabitEthemet 1/11	GigabitEthemet 1/12	GigabitEthemet 1/13		GigabitEthemet 1/15 GigabitEthemet 1/16	GigabitEthemet 1/17	GigabitEthemet 1/18	GigabitEthemet 1/19	GigabitEthemet 1/20	GigabitEthemet 1/21	GigabitEthemet 1/22	GigabitEthernet 1/23	GigabitEthemet 1/24	GigabitEthemet 1/25	GigabitEthemet 1/26	GigabitEthemet 1/27	GigabitEthemet 1/28	GigabitEthemet 1/29	GigabitEthernet 1/30	GigabitEthemet 1/31	GigabitEthernet 1/32	FastEthemet 1/1	Ports Configuration
) (
Local Cl	ock Curre	nt Tir	me																												
1070					PT	P Ti	me			Clo	ck /	١dj	ustn	nen	t me	eth	od		_	Sy	nch	ron	ize	to	Sys	ter	n C		:k		
1970-	-01-01103:2	24:20+	+02:00	814	,597	,520)				Inte	erna	al lin	ner						Syn	chror	nize	to S	Syst	em	Clo	ck				
Clock Cu	urrent Dat	aSet										_				_										_			_		
stpRm Offset From Master Mean Path Delay																															
	0						0.0	00,0	00,0	00											0.000	0,00	0,00	00							
Clock Pa	arent Data	Set																													
Pai	rent Port I	DF	Port	PS	stat	V	ar	Ra	te	(Gra	nd	Mas	ter	ID	- (Gra	ndl	las	ter	Cloc	k C	Jual	lity		Pri	Ц	Pr	i2		
00:50:c2	TT.10:00:36.	38	0	⊦a	ise	()	0		00:5	50:C	Z:Π.	te:ue	:36	38		CI:2	487	AC:U	nkn	wn va	a:6:	0030	•		128	_	12	8		
Clock De	efault Data	iSet On	o Wa	v	2	Sto	n El	20	D	ort			- (-k la	lon	titu		Do	-						ck	0	uali	tv.		
Ord-E	Bound	Fal	se 🗸	<u>y</u>	1	rue	~	ay		37	•	00	:50:c	2:ff:f	fe:0e	:36	:38	0)	-	CI	248	Ac:	Unk	nwr		1:65	5535	5		
Pri1	Pri2		ocal	Prio	T		P	roto	col		VL		Tag	En	ahle			V		P	CP	Г	SC	PI	0	rN	lae	tor	ID		
128	128	4			E	ther	net	010	~	-		Tr	ue	~	abre	-	1	-		4	~	0			_	0	au				
Clock Ti	me Brone	rtion	Data	Fot					_			_		_							_						_	_			
UtcO	Offset	Valio	1	lear	59		ear	61		Tin	ne T	ra	c	F	rea	Tra	с		ptr	o Tii	ne S	ica	le		Ti	me	Sc	ourc	ce		
0	Fa	lse 🗸	F	alse	~	F	alse	~		Fals	se 🗸	•		Fa	ilse	~			T	rue	~				1	60	_	1			
Filter Pa	rameters				_			_				_				_											_				
T Inter Fu	Tumotors	F	ilter `	Туре								Del	lay F	ilte	r						Per	ioc						Di	st		
	Basic	~		-					6	_								1	_	_					2	_	٦				
1PPS Fil	Iter Param	eters																									_				
	Frequency	(P)			Alp	ha				Bet	a		Н	yst	eres	sis			P	has	e Alı	oha	1		F	ha	se	Be	ta		
1.	.000		0.	500	_			0.10	0		_		3	-				(0.50	0				ſ	0.10	00	_				
Servo Pa	arameters		_																								_				
Displa	ay P-er	able	-	ena	ble)-er	ıabl	e	'P	" cc	ns	tant		Т	con	sta	nt		'D' (cons	tar	It	(Gai	n c	on	star	nt		
False V	 True 	~	Tr	ue	~	[Frue	~		3	3				80				[40					1		_				
																											_				
Unicast	Slave Con	figur	ation																												
Index	Duration	T	i	o ac	ldre	SS	gr	ant	C	omi	m St	ate	e																		
0	100	0.0.	0.0					0		ID	DLE																				
1	100	0.0.	0.0					0		ID	DLE																				
2	100	0.0.	0.0					0		ID	DLE																				
3	100	0.0.	0.0					0		ID	DLE																				
4	100	0.0.	0.0			_		0		ID	LE																				

Save Reset

Rys. 140. Konfiguracja zaawansowana instancji PTP

W tabeli **PTP Clock's Configuration** wyświetlony jest aktualny czas zegara PTP oraz sposób realizacji synchronizacji zegara. Można tu także wymusić jego synchronizację z zegarem systemowym oraz przejść do panelu konfiguracji portów (opisanego poniżej).

Tabela **Clock Default DataSet** – pokazuje parametry ustawione przy tworzeniu zegara oraz jakość lokalnego zegara (**Clock Quality**) a także umożliwia skonfigurowanie dodatkowych opcji:

Step Flag – określa czy ten zegar używa dodatkowych ramek followup razem z ramkami synchronizacji i pomiaru opóźnień przesyłu. Użycie tych ramek poprawia niezawodność synchronizacji.

Clock Identity – unikalny (w sieci) identyfikator zegara, domyślnie oparty na adresie MAC urządzenia.

One Way – dotyczy tylko urządzenia pracującego jako Slave – w tym trybie nie jest możliwy pomiar opóźnień przesyłu do tego urządzenia (urządzenie tylko odbiera ramki, a nic nie wysyła).

Protocol – protokół transportowy używany przez zegar PTP: **Ethernet** – warstwa 2, ramki multikastowe; **IPv4Multi** – protokół IP, ramki multikastowe; **IPv4Uni** – protokół IP, ramki unikastowe – ta opcja jest możliwa tylko dla trybów Master only i Slave only (konieczna jest dodatkowa konfiguracja w ustawieniach zaawansowanych PTP).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	117/147
------	------	-----------------------------------	------------	---------



VLAN Tag Enable – włączenie dodawania znaczników VLAN do wysyłanych ramek PTP (znaczniki będą dodawane tylko jeśli port będzie skonfigurowany na możliwość wysyłania ramek ze znacznikami VLAN).

VID – numer VLAN, który będzie wpisany do znacznika.

PCP – numer priorytetu (wg normy 802.1p), który będzie wstawiony do znacznika VLAN.

Po skonfigurowaniu tych ustawień nowy zegar PTP pojawi się na liście i będzie możliwe wybranie portów, których ma używać zegar do komunikacji z innymi urządzeni. Szczegółowa konfiguracja poszczególnych portów jest dostępna w ustawieniach zaawansowanych PTP.

Dom – numer domeny PTP – domeny umożliwiają działanie niezależnych systemów PTP w jednej sieci bez zakłócania się nawzajem. Standard definiuje trzy domeny alternatywne (różnią się adresem rozgłoszeniowym).

Pri1, Pri2 – priorytety zegara określane przez użytkownika (mniejsza liczba oznacza wyższy priorytet). Wartości te brane są pod uwagę na różnych etapach przy automatycznym wybieraniu zegara typu Master. Pri1 – sprawdzany jest na początku procesu, Pri2 – na końcu, jako przedostatni krok, jeśli poprzednie kroki wskażą więcej niż jeden najlepszy zegar (ostatni krok to wybranie zegara o mniejszym numerze identyfikacyjnym).

Jakość zegara opisuje fizyczne parametry lokalnego zegara. Składa się ona z trzech liczb:

CI – klasa zegara. Standard definiuje następujące klasy zegarów:

0: Zarezerwowane, aby umożliwić zgodność z przyszłymi wersjami.

6: bardzo dokładny zegar zsynchronizowany z pewnym źródłem czasu TAI, np. zegar GPS lub skalibrowany zegar atomowy (zegar tej klasy nigdy nie powinien być synchronizowany od innego zegara w sieci PTP),

7: Wyznacza zegar, który wcześniej był oznaczony jako clockClass 6, ale który utracił możliwość synchronizacji z głównym referencyjnym źródłem czasu i znajduje się w trybie holdover oraz w ramach specyfikacji holdover. Rozkład czasowy odpowiada PTP. clockClass 7 nie może być w roli slave względem innego zegara w domenie.

52: Alternatywa degradacji A dla zegara klasy 7, który nie mieści się w specyfikacji holdover. Zegar clockClass 52 nie może być w roli slave względem innego zegara w domenie.,

248 – Domyślna. Ta klasa clockClass zostanie użyta, jeśli żadna z innych definicji clockClass nie ma zastosowania,

254: domyślna,

255: clockClass tylko dla zegarów w roli slave.

Ac – dokładność zegara – wartość 100 ns. Dokładność czasu do 100 ns

Va – wariancja (stabilność) zegara.

Tabela **Clock Current DataSet** wyświetla stan synchronizacji aktualnego zegara względem zegara Master. Wyświetlone wartości są następujące:

stpRm – ilość urządzeń pośredniczących (obsługujących PTP), pomiędzy zegarem Master, a lokalnym urządzeniem.

Offset From Master – różnica czasów pomiędzy zegarem Master, a lokalnym zegarem (Slave), w nanosekundach.

Mean Path Delay – średni czas przejścia ramki od zegara Master do zegara lokalnego.

W tabeli Filter Parameters można zdefiniować sposób obliczania wartości w tabeli Clock Current DataSet.

DelayFilter – określa sposób działania filtra dolnoprzepustowego ograniczającego wartości średniego opóźnienia przejścia (Mean Path Delay). Jest to dolnoprzepustowy filtr, który sprawia, że szybko zmieniające się odczyty nie są brane pod uwagę przy obliczaniu tej wartości. Wartość DelayFilter określa siłę tego filtra w skali od 1 (najsłabszy) do 6 (najsilniejszy).

Period i **dist** – konfigurują filtr stosowany przy obliczaniu różnicy czasów względem zegara Master (Offset From Master). Jeśli **dist** jest równe 1, to różnica jest obliczana jako średnia kolejnych próbek, których ilość opisuje **period** (okres). Jeśli **dist** jest większe od 1, to różnica jest obliczana jako najmniejsza wartość z okresów, których ilość opisuje **dist**.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	118/147
------	------	-----------------------------------	------------	---------



W tabeli **Clock Parent DataSet** znajdują się dane zegara Master, do którego aktualnie zsynchronizowany jest lokalny zegar. Dane te są następujące:

Parent Port Identity – identyfikator portu urządzenia Master – może być on taki sam, jak identyfikator urządzenia Master.

Port – numer portu urządzenia Master, z którego lokalny zegar otrzymuje ramki synchronizacji (lub zero, jeśli urządzenie samo jest Masterem).

PStat – nieużywane.

Var – podaje zmierzoną wariancję zegara Master.

Change Rate – opisuje szybkość zmiany różnicy czasów pomiędzy lokalnym zegarem, a Masterem w nanosekundach na sekundę.

Grand Master Identity – identyfikator urządzenia Master (lub własny identyfikator, jeśli zegar lokalny nie jest zegarem Slave).

Grand Master Clock Quality – jakość zegara Master – opisuje fizyczne parametry zegara. Znaczenie poszczególnych wartości jest identyczne, jak w części o lokalnym zegarze (Clock Default DataSet).

Pri1 i Pri2 – priorytety zegara Master.

Tabela Clock Time Properties DataSet

Zestaw danych dotyczących właściwości zegara jest zdefiniowany w standardzie IEEE 1588. Zestaw danych jest konfigurowalny i dynamiczny, tj. Parametry można skonfigurować dla grandmastera. W zegarze slave parametry są nadpisywane przez właściwości czasowe grandmasterów. Parametry nie są używane w bieżącej implementacji protokołu PTP.

W tabeli **Servo Parameters** znajdują się ustawienia regulatora zegara lokalnego – jest to regulator typu PID, dążący do wyzerowania różnicy czasów względem Mastera. Wartością zadaną jest aktualna różnica czasów obliczona po otrzymaniu ramki synchronizacyjnej. Ustawienia te są następujące:

Display – włącza wyświetlanie danych regulacji w konsoli szeregowej (która nie jest dostępna dla użytkownika).

P/I/D-enable – umożliwiają włączenie poszczególnych członów regulatora PID.

'P'/'I'/'D' constant - określają parametry członów PID.

Tabela **Unicast Slave Configuration** dotyczy sytuacji, kiedy zegar PTP korzysta z ramek unikastowych w protokole IP (opcja IPv4Uni w ustawieniach przy tworzeniu zegara). W tabeli tej można zdefiniować do pięciu adresów urządzeń typu Master (zegar lokalny automatycznie wybierze najlepszy z nich do synchronizacji), do których zegar lokalny będzie wysyłał zapytania o dane i synchronizację. Dla każdego adresu IP można także ustawić czas (**Duration**) wysyłany w zapytaniu, informujący zegar Master, przez ile kolejnych sekund powinien on wysyłać ramki synchronizacyjne oraz z danymi do urządzenia lokalnego. Zapytania o dane i synchronizację (do Mastera) ponawiane są co jedną czwartą tego czasu.

5.47.1.1 Ustawienia portów

Ustawienia portów zegara PTP są dostępne w górnej tabeli ustawień zaawansowanych (Local Clock Current Time) za pośrednictwem odnośnika **Ports Configuration**.

PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dim	MPR	₹ Delay Asymmetry		Ingress Latend	y Egress Later	cy Version	Version Mcast Addr		Local Prio
1	dsbl	3	0.000,000,000	0	3	0	p2p 🗸	0	0		0	0	2	Default 🗸	False 🗸	128
2	dsbl	3	0.000,000,000	0	3	0	p2p 🗸	0	0		0	0	2	Default 🗸	False 🗸	128
3	dsbl	3	0.000,000,000	0	3	0	p2p 🗸	0	0		0	0	2	Default 🗸	False 🗸	128
4	dsbl	3	0.000,000,000	0	3	0	p2p 🗸	0	0		0	0	2	Default 🗸	False ►	128

Save Reset

Rys. 141. Konfiguracja portów zegara PTP

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	119/147
------	------	-----------------------------------	------------	---------



W tabeli tej wyświetlone są porty przypisane do aktualnego zegara PTP w konfiguracji globalnej PTP. Dla każdego portu wyświetlone są następujące informacje:

Port – numer portu, którego dotyczy wiersz,

Stat – aktualny stan portu,

MDR – minimalny interwał zapytań o opóźnienie linii sugerowany przez urządzenie Master (sugerowana minimalna wartość pola MPR),

PeerMinPathDel – zmierzone opóźnienie drogi do sąsiedniego urządzenia na tym porcie (tylko dla trybu P2P),

Version – wersja protokołu PTP; aktualnie HYPERION obsługuje tylko PTPv2.

Parametry portów możliwe do skonfigurowania w tej tabeli są następujące:

Anv – interwał wysyłania komunikatów informacyjnych, kiedy port jest w trybie Master,

ATo – czas oczekiwania na komunikaty informacyjne na tym porcie,

Syv - interwał wysyłania komunikatów synchronizacyjnych, kiedy port jest w stanie Master,

Dim – mechanizm pomiaru opóźnienia (ma znaczenie tylko jeśli zegar jest typu Ord-Bound; w zegarach przezroczystych jest to określone przez typ zegara). **E2e** – end to end – prostszy mechanizm, uwzględnia tylko czas przejścia ramki przez urządzenie; **p2p** – peer to peer – bardziej zaawansowany i dokładniejszy mechanizm, uwzględnia także czas przechodzenia ramek pomiędzy sąsiednimi urządzeniami PTP,

MPR – interwał wysyłania zapytań pomiaru opóźnienia do urządzenia Master (w trybie e2e) lub do urządzeń sąsiednich (w trybie p2p),

Delay Asymmetry – jeśli opóźnienie łącza nie jest symetryczne, w tym parametrze można podać wielkość asymetrii, która zostanie uwzględniona w pomiarach opóźnień; jednostka: nanosekundy, dodatnie wartości oznaczają większe opóźnienie ścieżki wychodzącej, ujemne – przychodzącej,

Ingress/Egress Latency – opóźnienie wejścia/wyjścia w nanosekundach – jest to dodatkowe opóźnienie, którego urządzenie może nie być w stanie wykryć i skompensować automatycznie.

5.47.2 Monitorowanie PTP

Panel monitorowania PTP dostępny jest w menu **Monitor** \rightarrow **PTP**. Wygląd wszystkich paneli monitorowania PTP oraz ich obsługa są takie same, jak paneli konfiguracyjnych, z tą różnicą, że możliwy jest wyłącznie odczyt danych konfiguracyjnych oraz informacyjnych. Panele monitorowania posiadają także przycisk **Refresh**, odświeżający dane na stronie, oraz pole **Auto-refresh**, którego zaznaczenie powoduje cykliczne automatyczne odświeżanie.

			PTP External Cl	ock Mode
PTP E	xternal Cloc	k Mode	One PPS Mode	Disable
One	PPS Mode	inut	External Enable	False
Exter	nal Enable F	alse	Adjust Method	LTC frequency
Δdius	t Method	TC frequency	Clock Frequency	1
Clock	Frequency 1		clock ricquelley	
РТР С	Clock Configu	iration	PTP Clock Cont	iguration
Inst	Device Type	106(gabitEthernet 1/1106(gabitEthernet 1/2106(gabitEthernet 1/3106(gabitEthernet 1/16(gabitEthernet 1/26(gabitEthernet 1/36(gabitEthernet 1/3	Inst Device Ty	G 10Gig abitEthernet 1/ 10Gig abitEthernet 1/ 10Gig abitEthernet 1/ 10Gig abitEthernet 1/ 0GgabitEthernet 1/ 0GgabitEthernet 1/ 0GgabitEthernet 1/2 0GgabitEthernet 1/2 0GgabitEthernet 1/2 0GgabitEthernet 1/2 0GgabitEthernet 1/2 0GgabitEthernet 1/3 0GgabitEthernet 1/3 0GgabitEthernet 1/3 0GgabitEthernet 1/3 0GgabitEthernet 1/3 0GgabitEthernet 1/3
0	Mastronly		<u>0</u> Ord-Boun	d 🗸

Rys. 142. Monitoring funkcji PTP

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	120/147
------	------	-----------------------------------	------------	---------



5.47.2.1 Szczegółowe monitorowanie PTP

PTP Clo	ock's Co	onfiguratio	n														
Clock Ty	pe and	Profile															
Clock I	nstance	HW Dom	ain Devic	е Туре	Profile												
	0	0	Mas	tronly	C37.238-11]											
Local Cl	ock Cur	rent Time				-											
			PTP	Time C	lock Adju	istment me	thod	Ports M	onitor Page	Foreig	n Maste	r Monitor Pa	ige Packe	t Stats	Monite	or Page	
2023-03-	30T10:31	:31+02:00 00	1,440,040 (U	TC=0)	Inte	rnal Timer		Port	s Monitor	<u>Fc</u>	oreign Ma	<u>ster Monitor</u>	<u>P</u> :	acket St	ats Mon	<u>itor</u>	
Clock D	efault Da	ataSet															
Device	Type	One-Way 🗄	2 Step Flag	Ports	Cloc	k Identity	Dom		Clock Quali	ty Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP	\square
Mastr	only	False	True	5	00:50:c2:f	ff:fe:0b:ac:e7	0	CI:006 A	:100 ns Va:658	535 124	124	128	Ethernet	0	4	0	150
Clock C	urrent D	ataSet															
stpRm	Offset	From Mast	ter Mean	Path Del	av Slave	e Port Sla	ave Sta	te Holo	(dqq)revol								
0	0.0	00,000,000	0.000	0,000,000		FF	REERU	N	N.A.								
Clock P:	arent Da	taSet															
Parent	Port Ide	ntity Port	PStat V	/ar Cha	ngeRate	Grand M	aster l	dentity	Grand Maste	r Clock	Quality	Pri1 Pri2	,				
00:50:c2	2:ff:fe:0b:	ac:e7 0	False	0	0	00:50:c2	:ff:fe:0b	ac:e7	CI:006 Ac:10	00 ns Va:	65535	124 124	-				
Clock Ti	me Brer	ortion Data	Set														
	set Val	id leap59	lean61	Time Tra	C Fred	Trac ntn	Time S	cale Ti	me Source								
37	Tn	e False	False	True	Fal	se	True	oure in	160								
Serve B	aramete		1 4100														
Dieplay	/ P.en:	able Lena	hle D-ena	hla 'P'	constant	'l' const	ant 'E)' consta	nt Gain con	stant							
Falso	Tri				3	80		10	1	Stant							
1 4130			6 114	-	J	00		40	•								
Filter Pa	rameter	S	Devie d D	- 4													
Fliter I	ype Di	elayFilter		St													
DdSl	6	0	1 2														
1pps Se	rvo Stat	us															
State	Error fr	eq. Error	phase														
Lock	0	(J														
Unicast	Slave C	onfiguration	n														
Index	Duratio	n IP_Add	ress Gran	nt Com	mState												
0	100	0.0.0	.0 0	1	DLE												
1	100	0.0.0	.0 0		DLE												
2	100	0.0.0	.0 0		DLE												
3	100	0.0.0	.0 0														

Rys. 143. Okno szczegółowych parametrów w monitoringu funkcji PTP

Poniżej przedstawiono opis pól w monitorowaniu funkcji PTP:

5.47.2.1.1 Local Clock Current time

PTP Time - Pokazuje rzeczywisty czas PTP z dokładnością do nanosekund.

Clock Adjustment Method - Pokazuje aktualną metodę regulacji zegara. Metoda zależy od dostępnego sprzętu.

Ports Monitor Page - Kliknij, aby monitorować zestawy danych dla portów przypisanych do tej instancji zegara.

5.47.2.1.2 Clock Default Dataset

Domyślny zestaw danych zegara jest zdefiniowany w standardzie IEEE 1588. Zawiera trzy grupy danych: statyczne elementy członkowskie zdefiniowane w czasie tworzenia zegara, dynamiczne elementy zdefiniowane przez system i konfigurowalne elementy, które można ustawić tutaj. **Clockld -** Wewnętrzny identyfikator instancji (0..3)

Device Type - Wskazuje typ instancji zegara. Istnieje pięć typów urządzeń.

- 1. Ord-Bound Typ zegara to Ordinary-Boundary Clock (zegar zwykły graniczny).
- 2. P2p Transp Typ zegara to Peer to Peer Transparent Clock (przezroczysty zegar peer to peer).
- 3. E2e Transp Typ zegara to End to End Transparent Clock (przezroczysty zegar end to end).
- 4. Master Only Typ zegara to Master Only (tylko master).
- 5. Slave Only Typ zegara to Slave Only (tylko slave).

Two-Step Flag – Prawda, jeśli używane są zdarzenia two-step Sync oraz Pdelay_Resp.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	121/147
------	------	-----------------------------------	------------	---------



Ports - Całkowita liczba portów fizycznych w węźle

Clock Identity - Pokazuje unikalny identyfikator zegara

Dom - Domena zegara [0..127].

Clock Quality - Jakość zegara jest określana przez system i składa się z 3 części: klasy zegara (wartości opisane w punkcie 5.46.1 niniejszej instrukcji), dokładności zegara i odchylenia wartości OffsetScaledLog zgodnie z definicją w IEEE1588.

Wartości dokładności zegara są zdefiniowane w tabeli 6 IEEE1588 (obecnie dokładność zegara jest domyślnie ustawiona na "Unknown" (nieznane)).

Pri1 - Priorytet zegara 1 [0..255] używany przez algorytm wyboru urządzenia głównego BMC.

Pri2 - Priorytet zegara 2 [0..255] używany przez algorytm wyboru urządzenia głównego BMC.

Protocol - Protokół transportowy używany przez silnik protokołu PTP

Ethernet PTP over Ethernet multicast

ip4multi PTP over IPv4 multicast

ip4uni PTP over IPv4 unicast

Uwaga : Protokół unicast IPv4 działa tylko w zegarach Master i Slave

Patrz parametr Device Type

W pojedynczym zegarze Slave only musisz także skonfigurować, które zegary główne

mają żądać rozgłaszania i synchronizowania wiadomości. Zobacz: Unicast Slave Configuration

One-Way - Jeśli prawda (true), stosowane są pomiary jednokierunkowe. Ten parametr dotyczy tylko slave'a. W trybie jednokierunkowym nie są wykonywane pomiary opóźnienia, tj. Ma to zastosowanie tylko wtedy, gdy wymagana jest synchronizacja częstotliwości. Master zawsze odpowiada na żądania opóźnienia.

VID - Identyfikator sieci VLAN używany do oznaczania ramek PTP.

Uwaga: Pakiety są znakowane, jeśli port jest skonfigurowany do znakowania sieci VLAN dla skonfigurowanego identyfikatora VID.

PCP - Wartość Priority Code Point używana dla ramek PTP.

5.47.2.1.3 Clock current Data Set

Aktualny zestaw danych zegara jest zdefiniowany w standardzie IEEE 1588. Aktualny zestaw danych jest dynamiczny.

stpRm - Usunięte kroki: Jest to liczba zegarów PTP, które przeszły od grandmastera do lokalnego zegara podrzędnego.

Offset from master - Różnica czasu między zegarem głównym a lokalnym zegarem slave, mierzona w ns.

mean Path Delay - Średni czas propagacji połączenia między urządzeniem master a lokalnym urządzeniem slave

Slave Port - Pokazuje, który port jest w trybie slave. Wartość wynosi 0, jeśli żaden port nie jest w trybie slave.

Slave State - Pokazuje stan synchronizacji slave'a.

Holdover(ppb) – Po tym, jak slave był w trybie Locked podczas okresu stabilizacji, ta wartość pokazuje rzeczywistę przesunięcie zegara między freerunem a rzeczywistą częstotliwością holdover, wartość jest pokazana w częściach na miliard (parts per billion - ppb). Podczas okresu stabilizacji wartość jest wyświetlana jako "N.A". Okres stabilizacji domyślnie wynosi 60 sekund, można go zmienić z poziomu interfejsu CLI.

5.47.2.1.4 Clock Parent Data Set

Nadrzędny zestaw danych zegara jest zdefiniowany w standardzie IEEE 1588. Nadrzędny zbiór danych jest dynamiczny.

Parent Port Identity – Clock ID zegara nadrzędnego. Jeśli lokalny zegar nie jest podrzędny, wartością jest własny identyfikator zegara.

Port - Identyfikator nadrzędnego portu głównego

Pstat - Statystyki urządzenia nadrzędnego (zawsze false).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	122/147



Var - Obserwuje się skalowane odchylenie logarytmiczne offsetu urządzenia nadrzędnego

Change Rate - Zaobserwowana szybkość zmian fazy zegara nadrzędnego. tj. przesunięcie częstotliwości taktów slave w porównaniu do mastera. (jednostka = ns na s)..

Grand Master Identity - Identyfikator zegara nadrzędnego, jeśli lokalny zegar nie jest podrzędny, wartością jest własny identyfikator zegara.

Grand Master Clock Quality - Jakość zegara ogłaszana przez grandmastera (wartości opisane w punkcie 5.46.1 niniejszej instrukcji)

Pri1 - Priorytet 1 ogłoszony przez Grandmastera.

Pri2 - Priorytet 2 ogłoszony przez Grandmastera.

5.47.2.1.5 Clock Time Properties Data Set

Zestaw danych dotyczących właściwości zegara jest zdefiniowany w standardzie IEEE 1588. Zestaw danych jest konfigurowalny i dynamiczny, tj. Parametry można skonfigurować dla grandmastera. W zegarze slave parametry są nadpisywane przez właściwości czasowe grandmasterów. Parametry nie są używane w bieżącej implementacji protokołu PTP.

5.47.2.1.6 Servo Parameters

Domyślne serwo zegara wykorzystuje regulator PID do obliczenia aktualnej częstotliwości zegara:

Regulacja zegara (clockAdjustment) =

OffsetFromMaster/ P constant +

Integral(OffsetFromMaster)/ I constant +

Differential OffsetFromMaster)/ D constant) * Gain

Display - Jeśli true, to Offset From Master, MeanPathDelay i clockAdjustment są rejestrowane na terminalu debugowania

P-enable - Jeśli true, część P algorytmu jest uwzględniona

I-Enable - Jeśli true, część I algorytmu jest uwzględniona

D-enable - Jeśli true, część D algorytmu jest uwzględniona

'P' constant - [1..1000] stała P (patrz powyżej)

'l' constant - [1..10000] stała I (patrz powyżej)

'D' constant - [1..10000] stała D (patrz powyżej)

Gain constant - [1..10000] stała Gain (patrz powyżej)

5.47.2.1.7 Filter Parameters

Domyślnym filtrem opóźniającym (ang. default delay filter) jest filtr dolnoprzepustowy o stałej czasowej 2 * DelayFilter * DelayRequestRate.

Jeśli parametr **DelayFilter** ma wartość 0 lub parametr Dist ma wartość 0, filtr opóźnienia używa tego samego algorytmu, co filtr przesunięcia (ang. offset filter).

Domyślny filtr przesunięcia używa minimalnego przesunięcia lub średniej filtru tj. do obliczeń używane jest minimalne zmierzone przesunięcie podczas próbek okresu (ang. Period).

Period - okres

Dist - Odległość między dwoma obliczeniami.

Jeśli **Dist** wynosi 0, przesunięcie jest filtrowane dolnoprzepustowo, filtr BW ma wartość 0,1 Hz, filtr automatycznie dostosowuje się do szybkości pakietów,

Jeśli Dist wynosi 1, przesunięcie jest uśredniane w Period,

Jeśli **Dist** > 1, offset jest obliczany przy użyciu minimalnego offsetu.

Filter Type - Pokazuje typ użytego filtru, który może być filtrem podstawowym lub filtrem zaawansowanym, który można skonfigurować tak, aby używał tylko części odebranych pakietów (tj. Pakietów, które doświadczyły najmniejszego opóźnienia).

Height - Wysokość okna próbki mierzona w mikrosekundach (dotyczy tylko zaawansowanego filtra offsetowego).

 REV.
 1.06
 INSTRUKCJA OBSŁUGI : HYPERION-GUI
 2024.01.04
 123/147



Percentage - Procent pakietów synchronizacyjnych (z najmniejszym opóźnieniem) używany przez filtr przesunięcia (dotyczy tylko zaawansowanego filtru przesunięcia).

Reset Threshold - Próg w mikrosekundach, przy którym filtr przesunięcia zostanie zresetowany i zegar podrzędny zsynchronizowany z nadrzędnym.

5.47.2.1.8 Unicast Slave Configuration

Podczas pracy w trybie unicast IPv4 urządzenie podrzędne jest skonfigurowane z maksymalnie pięcioma głównymi adresami IP. Następnie slave żąda ogłoszenia komunikatów od wszystkich skonfigurowanych modułów głównych. Urządzenie podrzędne używa algorytmu BMC, aby wybrać zegar jako zegar główny, a następnie urządzenie podrzędne żąda komunikatów synchronizacji od wybranego urządzenia głównego.

Duration - Liczba sekund, przez które master jest proszony o wysłanie wiadomości Announce / Sync. Żądanie jest powtarzane od slave'a co czas Duration / 4 sekundy.

IP_address - Adres IPv4 zegara master.

Grant - Przyznany okres powtarzania dla wiadomości sync

CommState - Stan komunikacji z masterem, możliwe wartości to:

IDLE: Wpis nie jest używany.

INIT: Wiadomość Announce jest wysyłane do mastera (oczekiwanie na odpowiedź).

CONN: Master odpowiedział.

SELL: Przypisany master jest wybierany jako aktualny master.

SYNC: Master wysyła wiadomości sync.

5.48 GVRP Configuration

GVRP to akronim od GARP VLAN Registration Protocol. Jest to protokół do dynamicznej rejestracji sieci VLAN na portach i jest określony w IEEE 802.1Q-2005, klauzula 11. GVRP jest przykładem wykorzystania GARP, stąd G w GVRP.

GVRP Configuration							
Enable GVRP							
Parameter		Value					
Join-time:	20						
Leave-time:	60						
LeaveAll-time:	1000						
Max VLANs:	20						
Save							



Enable GVRP globally - Funkcję GVRP można włączyć globalnie, ustawiając znacznik wyboru w polu wyboru o nazwie Enable GVRP i naciskając przycisk Save.

GVRP protocol timers - Join-time to wartość z zakresu 1-20 cs, czyli w jednostkach jednej setnej sekundy. Wartość domyślna to 20cs. Leave-time to wartość z przedziału 60-300 cs, czyli w jednost-kach jednej setnej sekundy. Wartość domyślna to 60cs. LeaveAll-time to wartość z zakresu 1000-5000cs, czyli z dokładnością do jednej setnej sekundy. Wartość domyślna to 1000cs.

Max number of VLANs - Gdy GVRP jest włączony, określana jest maksymalna liczba sieci VLAN obsługiwanych przez GVRP. Domyślnie jest to 20. Liczbę tę można zmienić tylko wtedy, gdy GVRP jest wyłączone.

5.48.1 GVRP Port Configuration

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	124/147
------	------	-----------------------------------	------------	---------



GVRP Port Configuration

Devet	Mar da
Ροπ	Iviode
*	 v
10GigabitEthernet 1/1	Disabled 🗸
10GigabitEthernet 1/2	Disabled 🗸
10GigabitEthernet 1/3	Disabled 🗸
10GigabitEthernet 1/4	Disabled 🗸
GigabitEthernet 1/1	Disabled 🗸
GigabitEthernet 1/2	Disabled 🗸
GigabitEthernet 1/3	Disabled 🗸
GigabitEthernet 1/4	Disabled 🗸
GigabitEthernet 1/5	Disabled 🗸
GigabitEthernet 1/6	Disabled
GigabitEthernet 1/7	GVRP enabled

Rys. 145. Okno konfiguracji funkcji poszczególnych portów do włączenia funkcji GVRP

5.49 sFlow Configuration

Ta strona umożliwia konfigurację sFlow. Konfiguracja jest podzielona na dwie części: Konfiguracja odbiornika sFlow (czyli kolektora sFlow) oraz konfiguracja przepływomierza na port i licznika próbników.

Konfiguracja sFlow nie jest utrwalana w pamięci nieulotnej, co oznacza, że ponowne uruchomienie wyłączy próbkowanie sFlow.

sFlow Configuratio	n				
Agent Configuration					
IP Address 127.0.0	1				
Receiver Configuration	on				
Owner	<none></none>			elease	
IP Address/Hostname	0.0.0.0				
UDP Port	6343				
Timeout	0		se	conds	
Max. Datagram Size	1400		by	tes	
Port Configuration			Flow Sampler	Cour	nter Poller
Ροπ	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*		0	128		0
10GigabitEthernet 1/1		0	128		0
10GigabitEthernet 1/2		0	128		0
10GigabitEthernet 1/3		0	128		0
10GigabitEthernet 1/4		0	128		0
GigabitEthernet 1/1		0	128		0
GigabitEthernet 1/2		0	128		0
GigabitEthernet 1/3		0	128		0
GigabitEthernet 1/4		0	128		0
GigabitEthernet 1/5		0	128		0
GigabitEthernet 1/6		0	128		0
GigabitEthernet 1/7		0	128		0
GigabitEthernet 1/8		0	128		0
GigabitEthernet 1/9		0	128		0
GigabitEthernet 1/10		0	128		0

Rys. 146. Okno konfiguracji funkcji sFLOW

5.49.1 Agent Configuration

IP Address - Adres IP używany jako adres IP agenta w datagramach sFlow. Służy jako unikalny klucz, który będzie identyfikował tego agenta przez dłuższy czas. Obsługiwane są adresy IPv4 i IPv6.

5.49.2 Receiver Configuration

Owner - Zasadniczo sFlow można skonfigurować na dwa sposoby: poprzez lokalne zarządzanie za pomocą interfejsu WWW lub CLI lub przez SNMP. To pole tylko do odczytu pokazuje właściciela bieżącej konfiguracji sFlow i przyjmuje następujące wartości:

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	125/147
------	------	-----------------------------------	------------	---------



• Jeśli sFlow jest obecnie unconfigured / unclaimed, Owner zawiera <none>.

• Jeśli sFlow jest obecnie skonfigurowany przez sieć Web lub CLI, Owner zawiera <Configured by local management>.

• Jeśli sFlow jest obecnie skonfigurowany przez SNMP, właściciel zawiera ciąg identyfikujący odbiornik sFlow.

Jeśli sFlow jest skonfigurowany przez SNMP, wszystkie kontrolki - z wyjątkiem przycisku Release - są wyłączone, aby uniknąć niezamierzonej ponownej konfiguracji.

Przycisk "Release" pozwala na zwolnienie aktualnego właściciela i wyłączenie samplowania sFlow. Przycisk jest wyłączony, jeśli sFlow nie jest aktualnie odebrany. W przypadku skonfigurowania przez SNMP zwolnienie musi zostać potwierdzone (pojawi się prośba o potwierdzenie).

IP Address/Hostname - Adres IP lub nazwa hosta odbiornika sFlow. Obsługiwane są adresy IPv4 i IPv6.

UDP Port - Port UDP, na którym odbiornik sFlow nasłuchuje datagramów sFlow. Jeśli ustawione na 0 (zero), używany jest port domyślny (6343).

Timeout - Liczba sekund pozostałych do zatrzymania próbkowania i zwolnienia aktualnego właściciela sFlow. Gdy jest aktywny, aktualny pozostały czas można zaktualizować, klikając przycisk Odśwież. Jeśli jest zarządzany lokalnie, limit czasu można zmienić na bieżąco, bez wpływu na inne ustawienia. Prawidłowy zakres to od 0 do 2147483647 sekund.

Max. Datagram Size - Maksymalna liczba bajtów danych, które mogą być wysłane w jednym przykładowym datagramie. Powinna być ona ustawiona na wartość, która pozwoli uniknąć fragmentaryzacji datagramów sFlow. Ważny zakres to 200 do 1468 bajtów, domyślnie 1400 bajtów.

5.49.3 Port Configuration

Port - Numer portu, którego dotyczy poniższa konfiguracja.

Flow Sampler Enabled - Włącza / wyłącza próbkowanie przepływu na tym porcie.

Flow Sampler Sampling Rate - Statystyczna częstotliwość próbkowania dla próbkowania pakietów. Ustaw na N, aby próbkować średnio 1 / n pakietów wysłanych / odebranych przez port. Nie wszystkie częstotliwości próbkowania są osiągalne. Jeśli zażądano nieobsługiwanej częstotliwości próbkowania, przełącznik automatycznie dostosuje ją do najbliższej osiągalnej. Zostanie to zgłoszone z powrotem w tym polu. Prawidłowy zakres to od 1 do 4294967295.

Flow Sampler Max. Header - Maksymalna liczba bajtów, które powinny zostać skopiowane z próbkowanego pakietu do datagramu sFlow. Prawidłowy zakres to od 14 do 200 bajtów, przy czym domyślnie to 128 bajtów. Jeśli maksymalny rozmiar datagramu nie uwzględnia maksymalnego rozmiaru nagłówka, próbki mogą zostać odrzucone.

Counter Poller Enabled - Włącza / wyłącza odpytywanie liczników na tym porcie.

Counter Poller Interval - Przy włączonym odpytywaniu liczników określa interwał - w sekundach - między próbkami licznika. Prawidłowy zakres to od 1 do 3600 sekund.

5.50 UDLD Port Configuration

UDLD to akronim dla Uni Directional Link Detection. Protokół UDLD monitoruje fizyczną konfigurację łączy między urządzeniami i portami obsługującymi UDLD. Wykrywa istnienie łączy jednokierunkowych, a jego funkcjonalnością jest zapewnienie mechanizmów przydatnych do wykrywania połączeń jednokierunkowych, zanim utworzą pętlę lub inne usterki protokołu. RFC 5171 określa sposób wykrywania łącza jednokierunkowego w warstwie łącza danych.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	126/147
------	------	-----------------------------------	------------	---------



UDLD Port Configuration

Port	UDLD mod	de	Message Interval
*	\diamond	~	7
10GigabitEthernet 1/1	Disable	~	7
10GigabitEthernet 1/2	Disable		7
10GigabitEthernet 1/3	Normal		7
10GigabitEthernet 1/4	Disable	•	7
GigabitEthernet 1/1	Disable	~	7
GigabitEthernet 1/2	Disable	~	7
GigabitEthernet 1/3	Disable	~	7
GigabitEthernet 1/4	Disable	~	7
GigabitEthernet 1/5	Disable	~	7

Rys. 147.Okno konfiguracji funkcji UDLD

Port - Numer portu przełącznika.

UDLD Mode - Konfiguruje tryb UDLD na porcie. Prawidłowe wartości to Disable, Normal i Aggressive. Domyślnym trybem jest Disable.

Disable - W trybie wyłączonym funkcja UDLD nie istnieje na porcie.

Normal - W trybie Normal, jeśli stan połączenia portu został określony jako jednokierunkowy, nie będzie to miało wpływu na stan portu.

Aggressive - W trybie Aggresive, jednokierunkowe porty zostaną wyłączone. Aby przywrócić te porty, należy wyłączyć UDLD na tym porcie.

Message Interval - Konfiguruje okres czasu pomiędzy komunikatami sondy UDLD na portach, które znajdują się w fazie rozgłaszania i są określone jako dwukierunkowe. Zakres wynosi od 7 do 90 sekund (Domyślna wartość to 7 sekund) (Obecnie obsługiwany jest domyślny przedział czasowy, ze względu na brak szczegółowych informacji w RFC 5171).

5.51 DDMI dla wkładek światłowodowych SFP

Funkcje monitorowania parametrów wkładek SFP są wykorzystywane do analizy aktualnych parametrów odczytanych z wkładek, a także możliwość konfigurowania poziomu poszczególnych progów alarmowych wyświetlanych w logach przełącznika. Zakładka DDMI → Thresholds umożliwia konfigurację progów dla następujących parametrów: temperatura, napięcie, prądu nadajnika "TX Bias", mocy nadajnika "TX Power" oraz mocy odbiornika "RX Power". Konfiguracja polega na przypisaniu minimalnych i maksymalnych wartości dla ostrzeżeń "Warn" oraz minimalnych i maksymalnych wartości dla "Alarm". W kolumnie Log dla każdego parametrów jeśli zaznaczymy checkbox, wszystkie ostrzeżenia i alarmy będą wyświetlane w logach przełącznika. W kolumnie overwrite zaznaczenie checkbox spowoduje nadpisanie wartości z pamięci wkładki SFP progami ustawionymi przez użytkownika w przełączniku.

UWAGA! Do prawidłowego działania progów alarmowych wkładka SFP musi wspierać funkcję DDMI

Znaczenie poszczególnych pól jest następujące i dotyczy wszystkich poniższych parametrów **Interface -** Port logiczny dla ustawień zawartych w tym samym wierszu.

Overwrite - Użyj wartości threshold z tego wiersza, nie z pamięci DDMI rom.

High Alarm Threshold - Wartość progu wysokiego alarmu.

High Warn Threshold - Wartość progu wysokiego ostrzeżenia. Wartość progowa dla Warn musi być ustawiona poniżej wartości dla Alarmu

Low Warn Threshold - Wartość progu niskiego ostrzeżenia. Wartość progowa dla Warn musi być ustawiona poniżej wartości dla Alarmu

Low Alarm Threshold - Wartość progu niskiego alarmu.

Log - Próg wstawiania do logów.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	127/147
------	------	-----------------------------------	------------	---------



5.51.1 Konfiguracja progów temperatury

DDMI Temperature Thresholds Configuration

Interface	Overwrite	High Alarm Thres	hold High	Warn Three	shold	Low	Warn Thres	shold	Low	Alarm Three	shold	Log
*		115.000		105.000		[-35.000			-40.000		~
10GigabitEthernet 1/1		115.000		105.000		(-35.000			-40.000		<
10GigabitEthernet 1/2		115.000		105.000		[-35.000			-40.000		
10GigabitEthernet 1/3		115.000		105.000		[-35.000			-40.000		~
10GigabitEthernet 1/4		115.000		105.000		[-35.000			-40.000		
GigabitEthernet 1/1		115.000		105.000		[-35.000			-40.000		~
GigabitEthernet 1/2		115.000		105.000		[-35.000			-40.000		
GigabitEthernet 1/3		115.000		105.000		[-35.000			-40.000		~
GigabitEthernet 1/4		115.000		105.000			-35.000			-40.000		

Rys. 148. Okno konfiguracji parametru Temperatura w wybranym modelu

5.51.2 Konfiguracja progów napięcia

DDMI Voltage Thresholds Configuration

Interface	Overwrite	High Alarm Thresho	ld High W	arn Thres/	hold Lo	w Warn Thresh	old Low	Alarm Three	shold	Log
*		3.9000	3.	7500		2.9500		2.8000		Z
10GigabitEthernet 1/1		3.9000	3.	7500		2.9500		2.8000		<
10GigabitEthernet 1/2		3.9000	3.	7500		2.9500		2.8000		
10GigabitEthernet 1/3		3.9000	3.	7500		2.9500		2.8000		~
10GigabitEthernet 1/4		3.9000	3.	7500		2.9500		2.8000		
GigabitEthernet 1/1		3.9000	3.	7500		2.9500		2.8000		✓
GigabitEthernet 1/2		3.9000	3.	7500		2.9500		2.8000		
GigabitEthernet 1/3		3.9000	3.	7500		2.9500		2.8000		✓
GigabitEthernet 1/4		3.9000	3.	7500		2.9500		2.8000		

Rys. 149.Okno konfiguracji parametru napięcie w wybranym modelu

5.51.3 Konfiguracja progów prądu nadajnika "TX Bias"

		•				
Interface	Overwrite	High Alarm Thresh	hold High Warn Three	shold Low Warn Thre	eshold Low Alarm Th	reshold Log
*		35.000	30.000	0.500	0.100	
10GigabitEthernet 1/1		35.000	30.000	0.500	0.100	Z
10GigabitEthernet 1/2		35.000	30.000	0.500	0.100	
10GigabitEthernet 1/3		35.000	30.000	0.500	0.100	Z
10GigabitEthernet 1/4		35.000	30.000	0.500	0.100	
GigabitEthernet 1/1		35.000	30.000	0.500	0.100	Z
GigabitEthernet 1/2		35.000	30.000	0.500	0.100	
GigabitEthernet 1/3		35.000	30.000	0.500	0.100	Z
GigabitEthernet 1/4		35.000	30.000	0.500	0.100	

DDMI Tx Bias Thresholds Configuration

Rys. 150. Okno konfiguracji parametru prądu nadajnika Bias w wybranym modelu

5.51.4 Konfiguracja progów mocy nadajnika "TX Power"

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 128/



DDMI TX Power Thresholds Configuration

Interface	Overwrite	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold Log
*		15.000	10.000	-25.000	-30.000
10GigabitEthernet 1/1		15.000	10.000	-25.000	-30.000
10GigabitEthernet 1/2		15.000	10.000	-25.000	-30.000
10GigabitEthernet 1/3		15.000	10.000	-25.000	-30.000
10GigabitEthernet 1/4		15.000	10.000	-25.000	-30.000
GigabitEthernet 1/1		15.000	10.000	-25.000	-30.000
GigabitEthernet 1/2		15.000	10.000	-25.000	-30.000
GigabitEthernet 1/3		15.000	10.000	-25.000	-30.000
GigabitEthernet 1/4		15.000	10.000	-25.000	-30.000

Rys. 151.Okno konfiguracji parametru mocy nadajnika w wybranym modelu

5.51.5 Konfiguracja progów mocy odbiornika "RX Power"

Interface	Overwrite	High Alarm Threshold	d High Warn Thres	hold Low Warn Three	shold Low Alarm Thre	shold Log
*		10.000	5.000	-40.000	-50.000	
10GigabitEthernet 1/1		10.000	5.000	-40.000	-50.000	
10GigabitEthernet 1/2		10.000	5.000	-40.000	-50.000	
10GigabitEthernet 1/3		10.000	5.000	-40.000	-50.000] 🔽
10GigabitEthernet 1/4		10.000	5.000	-40.000	-50.000	
GigabitEthernet 1/1		10.000	5.000	-40.000	-50.000] 🔽
GigabitEthernet 1/2		10.000	5.000	-40.000	-50.000	
GigabitEthernet 1/3		10.000	5.000	-40.000	-50.000] 🔽
GigabitEthernet 1/4		10.000	5.000	-40.000	-50.000	

DDMI RX Power Thresholds Configuration

Rys. 152.Okno konfiguracji parametru mocy odbiornika w wybranym modelu

5.51.6 Monitorowanie parametrów wkładek SFP

Zakładka Monitor \rightarrow DDMI \rightarrow Overview umożliwia odczyt podstawowych parametrów oraz po kliknięciu na wybrany port, wyświetli szczegółowe parametry z wkładek SFP.

DDMI Overview								
Interface	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver	Code CC_BASE	Code CC_EXT
10GigabitEthernet 1/1						NONE		
10GigabitEthernet 1/2	3C-LINK	3C-SFP+-LR	OW1701060044	В	2017-01-06	10G	\checkmark	\checkmark
10GigabitEthernet 1/3						NONE		
10GigabitEthernet 1/4						NONE		
GigabitEthernet 1/1	Ruby Tech	SFP.LC	9429070666	0000	2009-05-11	1000BASE_SX	\checkmark	\checkmark
GigabitEthernet 1/2						NONE		
GigabitEthernet 1/3						NONE		
GigabitEthernet 1/4						NONE		

Rys. 153.Okno monitorowania w funkcji DDMI - dane ogólne

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	129/147
------	------	-----------------------------------	------------	---------



Transceiver Information

Vendor	AOA
Part Number	SFP-10G-LR
Serial Number	G1712074427
Revision	A
Data Code	2017-12-16
Transeiver	10G
Check Code CC_BASE	\checkmark
Check Code CC_EXT	\checkmark
Check Code CC DMI	\checkmark

DDMI Thresholds Information

Tx: transmit, Rx: receive, mA: milliamperes, dBm: decibel ref to 1mW.

Туре	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	80.000	75.000	-5.000	-10.000
Voltage(V)	3.7999	3.7000	2.9000	2.7999
Tx Bias(mA)	80.000	75.000	6.000	5.000
Tx Power(dBm)	1.000	0.500	-6.002	-7.001
Rx Power(dBm)	1.000	0.000	-16.003	-17.011

Alarm Information

++ : high alarm, + : high warning, - : low warning, -- : low alarm. Tx: transmit, Rx: receive, mA: milliamperes, dBm: decibel ref to 1mW

Туре	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	40.217	80.000	75.000	-5.000	-10.000
Voltage(V)	3.2677	3.7999	3.7000	2.9000	2.7999
Tx Bias(mA)	40.434	80.000	75.000	6.000	5.000
Tx Power(dBm)	-3.001	1.000	0.500	-6.002	-7.001
Rx Power(dBm)	-40.000	1.000	0.000	-16.003	-17.011

Rys. 154.Okno monitorowania w funkcji DDMI – dane szczegółowe wybranego slotu

5.52 Moduł Digital InOut (opcja w wybranych modelach)

Wybrane przełączniki mogą być opcjonalnie wyposażone w moduł wejść służących do zbierania danych z czujników t.j. kontrakton lub czujnik ruchu, oraz wyposażony w wyjścia przekaźnikowe do sterowania np. włączania urządzeń poprzez przekaźniki

5.52.1 Konfiguracja w module wejść / wyjść

W zakładce Configuration → Digital InOut możemy aktywować lub dezaktywować wejście "Input" lub wyjścia "Relay", a także włączyć negację tych interfejsów. Domyślnie interfejsy są aktywne.

Input O	utput M	odule Co	nfiguration
Digital	Input Co	onfigurati	on
Input	Active	Negate	
1	Z		
Output	Relay C	onfigura	tion
Output Relay	Relay C Active	onfigura Negate	tion
Output Relay	Relay C Active	onfigura Negate	tion
Output Relay 1 2	Relay C Active ✓	onfigura Negate	tion

Rys. 155. Okno konfiguracji modułu I/O

Input – numer wejścia

Active – aktywowanie lub dezaktywowanie wejścia odbywa się przez zaznaczenie lub odznaczenie pola checkbox

Negate – aktywowanie negacji logicznej działania wejścia

Relay – numer wyjścia

Active – aktywowanie lub dezaktywowanie wyjścia odbywa się przez zaznaczenie lub odznaczenie pola checkbox

Negate – aktywowanie negacji logicznej działania wyjścia

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	130/147



Pozostała konfigurację w zakresie alarmowania należy należy wykonać w zakładce Alarms zgodnie z opisami w punkcie 5.3.3 niniejszej instrukcji.

5.52.2 Monitorowanie stanu wejść / wyjść

Input Output Module State
Digital Input State
1 Non Active
Output Relay State
Relay State
1 OFF
2 OFF

Rys. 156. Okno monitorowania stanów modułu I/O

Input – numer wejścia State – Non Active/Active – wejście nie aktywne/aktywne Relay – numer wyjścia State – OFF/ON – wyjście nie aktywne/aktywne

5.53 Konfiguracja oraz monitorowanie funkcji GNSS w przełączniku

(w wybranych modelach)

GPS Module Co	onfiguration
---------------	--------------

Antenna Cable Delay [ns]	PTP time update	Coordinate ECEF	Coordinate LLH
50	Z	Z	✓

Rys. 157. Konfiguracja funkcji GPS w przełączniku

Antenna Cable Delay - Ustaw opóźnienie sygnału w ns w zależności od długości kabla antenowego. Zwykle 1 m kabla antenowego powoduje opóźnienie sygnału około 4 ns. W Hyperion domyślnie ustawiono 50ns.

PTP Time update – Zaznacz checkbox, który jest wymagany do aktualizacji czasu w protokole PTP z modułu GNSS

Coordinate ECEF - włacz/wyłacz wyświetlanie koordynatów ECEF

Coordinate LLH – włacz/wyłacz wyświetlanie koordynatów LLH

Poprawnie zsynchronizowany moduł GPS przedstawia poniższe okno

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	131/147
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	13



GPS Module State

Communication	•
Date time	2023-03-30T13:34:52+02:00 116,617,630
GPS epoch	week:2255 seconds:387310 leap seconds:18
Future leap second change	0
GPSfix Type	3D Fix
Num. of satelites	10
ECEF X	369334339
ECEF Y	153802828
ECEF Z	495094933
Latitude	51.060714
Longitude	22.608433
Ellipsoidal Height	630173994.727282

DPLL State		
State	LOCK	
LOS		
LOT		
LOL		
DHOLD		

Rys. 158.Okno statusu GNSS oraz petli DPLL

Znaczenie pól jest następujące:

GPS Module State:

Communication – sygnalizacja wewnętrznej komunikacji modułu GNSS z przełącznikiem Data time – aktualny czas pobrany z GPS

GPSfix Type – stan zalokowania się modułu GNSS do systemu GPS

Num. Of satelites – wskazuje ilość satelitów z których odbierany jest prawidłowy sygnał GPS ECEF (X,Y,Z) – Pozycja odbiornika GNSS prezentowana w systemie koordynatów ECEF Latitude, Longitude, Ellipsoidal Height – Pozycja odbiornika GNSS prezentowana w systemie koordynatów LLH

DPLL State:

State – aktualny stan pętli DPLL; LOCK - zalokowana

LOS – Informacja o zagubieniu sygnału 1PPS – kolor zielony oznacza odbieranie sygnału 1PPS

LOT – sprawdzanie prawidłowości sygnału 1PPS – kolor zielony oznacza prawidłowy sygnał

LOL – Informacja o zalokowaniu pętli DPLL – kolor zielony oznacza zalokowanie

HOLDOVER – sygnalizacja statusu Holdover – kolor zielony oznacza, że urządzenie pracuje z rzeczywistymi parametrami, w momencie utraty sygnału GNSS pętla DPLL jest w stanie holdover co sygnalizuje się kolorem czerwonym.

DHOLD – Informacja o zbieraniu odpowiedniej ilości próbek dla stanu holdover – kolor zielony oznacza, że urządzenie posiada już odpowiednią ilość próbek

5.54 Wewnetrzny test ICMP ping w menu Diagnostyka

Strona umożliwia wysyłanie pakietów ICMP PING pomagająca w diagnozie problemów z komunikacją po IP .

ICMP Ping

IP Address	0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start



REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	132/147



6 Awaryjne przywracanie dostępu do urządzenia

W przypadku utraty hasła istnieje mechanizm generowania tymczasowego hasła w celu uzyskania dostępu do urządzenia przez www lub telnet lub CLI. Jeśli wprowadzisz hasło niepoprawnie pięć razy przez telnet lub CLI lub wpisując polecenie %bitstream% w polu password, zostanie wygenerowany tymczasowy kod. Kod należy przekazać do Działu wsparcia BitStream dostępnego od 8:00 do 16:00 pod numerem tel 817438643 wew. 28 lub wysłać e-mailem: <u>support@bitstream.pl</u>, aby otrzymać tymczasowe 6-godzinne hasło dostępu do urządzenia. Jeśli nie możesz się zalogować do urządzenia (z powodu niepoprawnie wprowadzonej konfiguracji np.: vlan itp.), możesz przywrócić domyślną konfigurację za pomocą przycisku "DEF". Przytrzymanie przycisku "DEF" przez 5 sekund spowoduje usunięcie konfiguracji bez utraty adresu IP, a przytrzymanie przycisku przez ponad 10 sekund spowoduje przywrócenie konfiguracji do ustawień fabrycznych.

7 Zarządzanie konfiguracją, aktualizacja Firmware oraz Restart urządzenia

Interfejs www umożliwia ponowne uruchomienie urządzenia tzw. restart. W tym celu należy uruchomić stronę dostępną pod linkiem **Maintenance** → **Restart Device** i nacisnąć przycisk **Yes**. Ponowne uruchomienie trwa około dziesięciu sekund, po tym czasie zostanie ponownie uruchomiony system operacyjny wraz ze wszystkimi aplikacjami jak również odświeżony zostanie interfejs www i wyświetlona zostanie strona jak poniżej.



Przywrócenie ustawień domyślnych urządzenia **HYPERION** jest możliwe na stronie w menu: **Maintenance > Factory Defaults**. W celu przywrócenia ustawień domyślnych należy kliknąć przycisk **Yes**. Ustawienia domyślne zostaną przywrócone natychmiast i potwierdzone komunikatem: "Configuration Factory Reset Done The configuration has been reset. The new configuration is available immediately._"

UWAGA! Przez interfejs WEB przywracanie ustawień domyślnych nie zawiera adresu IP urządzenia, w związku z tym po tej operacji będzie możliwość dalszego zarządzania urządzeniem o ile dostęp do urządzenia nie wymaga zamian innych ustawień sieciowych np. VLAN. W przypadku konieczności resetów wszystkich ustawień należy posłużyć się komendą "reload defaults" przez linię poleceń

UWAGA! Ustawienia domyślne usuwają również użytkowników oraz hasła dostępu do urządzenia.

Factory Defaults

	Are you sure you want to reset the configuration to Factory Defaults?	
Yes No		

Rys. 161. Strona umożliwiająca przywrócenie ustawień domyślnych urządzenia

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	133/147
------	------	-----------------------------------	------------	---------



7.1 Aktualizacja oprogramowania

Interfejs www udostępnia możliwość aktualizacji oprogramowania w **HYPERION**. Początkowa strona aktualizacji dostępna jest pod linkiem **Maintenance** → **Software Upload**.

W celu zaktualizowania oprogramowania należy klikną przycisk **Przeglądaj...**, wybrać plik o rozszerzeniu *.dat zawierający nowe oprogramowanie, a następnie kliknąć przycisk **Upload**. Po wykonaniu tej czynności strona zostanie odświeżona i rozpocznie się proces aktualizacji. Na stronie będą wyświetlane komunikaty instalatora, po czym pojawi się informacja o pomyślnym wykonaniu lub o błędzie. W czasie aktualizacji oprogramowania nie należy restartować urządzenia ani wyłączać zasilania. Wymiana oprogramowania trwa około 3 - 4 minut, po tym czasie urządzenie uruchomi się ponownie już z nowym oprogramowaniem i odświeży interfejs www wyświetlając stronę Ports \rightarrow State.

Software Upload

Wybierz plik BCH500-C...-317-7722.dat Upload

Rys. 162. Strona początkowa aktualizacji oprogramowania z załadowanym plikiem .dat

Uwaga!!!: We wskazanych modelach przełączników aktualizacja firmware z wersji starszej niż: HYPERION-105 - v120

HYPERION-300 - v120 HYPERION-303 - v120 HYPERION-200 - v308 HYPERION-400 - v308

HYPERION-500 - v308

Spowoduje usunięcie haseł dla istniejących użytkowników w konfiguracji (w tym także użytkownika "admin").

Po aktualizacji i ponownym uruchomieniu, dla każdego skonfigurowanego użytkownika hasło będzie usunięte to znaczy przy pierwszej próbie zalogowania się do zarządzania przez WWW lub CLI pole hasła należy zostawić puste.

W przypadku downgrade'u oprogramowania do niższej wersji niż wskazana na liście powyżej, nastąpi całkowite usunięcie profili użytkowników, natomiast zostanie utworzony domyślny użytkownik "admin" bez hasła.

7.2 Zarządzanie plikami konfiguracyjnymi w przełącznikach HYPERION

Przełącznik przechowuje swoją konfigurację w wielu plikach tekstowych w formacie CLI. Pliki są albo wirtualne (oparte na pamięci RAM), albo przechowywane w pamięci flash na przełączniku. Zakładka **Maintenance** → **Configuration** umożliwia zapisywanie konfiguracji, a także zarządzanie plikami konfiguracyjnymi użytkownika czyli ich pobieranie na komputer oraz ładowanie do Hyperiona.

Dostępne pliki to:

- running-config: wirtualny plik reprezentujący aktualnie aktywną konfigurację na przełączniku, ale do czasu restartu. Ten plik jest nietrwały.
- *startup-config*: Konfiguracja startowa przełącznika, odczytywana podczas jego startu. Jeśli ten plik nie istnieje w czasie startu, przełącznik zostanie uruchomiony w domyślnej konfiguracji.
- default-config: Konfiguracja domyślna: Plik tylko do odczytu z konfiguracją specyficzną dla danego producenta. Plik ten jest wczytywany po przywróceniu ustawień domyślnych systemu.
- Maksymalnie do 31 innych plików, zwykle używanych do tworzenia kopii zapasowych konfiguracji lub konfiguracji alternatywnych.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	134/147
------	------	-----------------------------------	------------	---------



Save startup-config – Spowoduje to skopiowanie *running-config* do *startup-config*, zapewniając w ten sposób, że aktualnie aktywna konfiguracja zostanie użyta przy następnym uruchomieniu.

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

Rys. 163. Strona do zapisywania konfiguracji startup-config

Download – Możliwe jest pobranie dowolnego pliku po przez przeglądarkę internetową. Wybierz plik i kliknij przycisk "Download Configuration".

Pobieranie *running-config* może zająć trochę czasu, ponieważ plik musi być przygotowany do pobrania.

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
running-config
○ default-config
○ startup-config
Download Configuration

Rvs.	164.	Strona do	pobierania	plików	konfigura	cvinvcł	h
						- ,	

Upload – Możliwe jest ładowanie różnych plików z przeglądarki internetowej do przełącznika, z wyjątkiem konfiguracji domyślnej, która jest tylko do odczytu. Wybierz plik do przesłania, wybierz plik docelowy w miejscu docelowym, a następnie kliknij "Upload Configuration".

Jeśli wskażemy miejsce pliku jako running-config, plik zostanie załadowany oraz konfiguracja zastosowana w przełączniku. Można to zrobić na dwa sposoby:

Replace – bieżąca konfiguracja jest w całości zastąpiona konfiguracją z przesłanego pliku.

Merge – przesłany plik jest łączony w running-config czyli nadpisywane są różnice pomiędzy plikami. Jeśli system plików flash jest pełny (tj. Zawiera plik default-config i 32 inne pliki, włącznie ze startup-config), nie jest możliwe utworzenie nowych plików. Zamiast tego istniejący plik musi zostać nadpisany lub należy usunąć inny plik.

Upload Configuration

File To Upload

Wybierz plik running-config

Destination File

File Name		Parameters
running-config	Replace	○ Merge
○ startup-config		
○ Create new file		

Upload Configuration

Rys. 165. Strona do ładowania plików konfiguracyjnych

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	135/147



Activate – Możliwe jest aktywowanie dowolnego z plików konfiguracyjnych obecnych na przełączniku, z wyjątkiem konfiguracji aktualnie uruchomionej, Wybierz plik do aktywacji i kliknij "Activate Configuration". Spowoduje to rozpoczęcie procesu całkowitego zastąpienia istniejącej konfiguracji przez konfigurację z wybranego pliku.

Uwaga: Aktywowany plik konfiguracyjny nie zostanie zapisany do konfiguracji startup-config automatycznie.

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
O default-config
O startup-config
new_configuration
Activate Configuration

Rys. 166. Strona do aktywowania plików konfiguracyjnych

Delete – Możliwe jest usunięcie dowolnych plików przechowywanych w pamięci flash, w tym pliku *startup-config*. Jeśli po usunięciu pliku startowego przełącznik zostanie ponownie uruchomiony bez wcześniejszej operacji zapisywania "save startup-config", spowoduje to skuteczne zresetowanie przełącznika do konfiguracji domyślnej.



Rys. 167. Strona do usuwania plików konfiguracyjnych

8 Konfiguracja przełącznika – interfejs CLI

8.1 Opis komend CLI dla nowszej wersji oprogramowania op v1xx

CLI (ang. Command Line Interface) interfejs linii poleceń dostępny jest tylko przy połączeniu przez sieć Ethernet i protokół IP oraz przez protokoły: telnet lub SSH, a także w niektórych modelach za pomocą KONSOLI RS-232. Konfiguracja **HYPERION** za pomocą interfejsu CLI wymaga komputera z zainstalowanym programem konsoli.

Połączenie przez konsolę zdalną wymaga odpowiedniego programu (dla systemu Windows rekomendowany jest program PuTTY oraz poprawnie skonfigurowanego połączenia LAN pomiędzy urządzeniem a komputerem lub poprawnie skonfigurowanego połączenia przez port szeregowy).

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	136/147
------	------	-----------------------------------	------------	---------



W tym rozdziale opisany jest jedynie sposób użycia interfejsu CLI wraz z krótkimi opisami odpowiednich funkcji dla **HYPERION**. Aby rozpocząć zarządzanie przez CLI należy uruchomić jeden z programów konsoli SSH lub telnet lub serial (np. putty) i skonfigurować go tak, aby mógł uzyskać połączenie z **HYPERION**. Po tej czynności powinien on wyświetlić komunikat logowania.



Rys. 168. Ekran logowania przez Telnet/SSH

Wprowadź tutaj nazwę użytkownika, domyślnie jest to admin, naciśnij Enter, a następnie wprowadź hasło dostępu do urządzenia, jeśli zostało ono założone. Po pomyślnym zalogowaniu przechodzimy na wysoki poziom w drzewie menu z włączonymi komendami uprzywilejowanymi. Wyświetlany jest następujący znak:

#

W podpowiedzi # można wprowadzić polecenia do konfiguracji i monitorowania urządzenia.

Dla dolnego poziomu drzewa menu z wyłączonymi komendami uprzywilejowanymi wyświetlany jest następujący znak: >

Po wpisaniu słowa help wyświetlany jest następujący komunikat:



Rys. 169. Prezentacja odpowiedzi po wpisaniu polecenia "help"

W dowolnym momencie możliwe jest wyświetlenie listy dostępnych komend w danym miejscu poprzez wpisanie znaku '?' i kliknięcie Enter.

Listę komend w grupie menu głównego z wyłączonymi komendami uprzywilejowanymi przedstawia poniższy rysunek:

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	137/147
------	------	-----------------------------------	------------	---------



ا- 192.168.0.95	PuTTY — 🗆	×
Hyperion1# di	sahle	^
Hyperionl> ?	54510	
clear	Reset functions	
disable	Turn off privileged commands	
do	To run exec commands in the configuration mode	
enable	Turn on privileged commands	
exit	Exit from EXEC mode	
help	Description of the interactive help system	
logout	Exit from EXEC mode	
no	Negate a command or set its defaults	
ping	Send ICMP echo messages	
show	Show running system information	
Hyperionl>		\sim



Lista komend w grupie menu głównego z włączonymi komendami uprzywilejowanymi przedstawiona jest na rysunku poniżej:

UWAGA: Poziom ten jest domyślny podczas każdego logowania.

PuTTY		×
Hyperion1# 2		1
clear	Reset functions	
configure	Enter configuration mode	
conv	Copy from source to destination	
debug	Debugging functions	
delete	Delete one file in flash: file system	
dir	Directory of all files in flash: file system	
disable	Turn off privileged commands	
do	To run exec commands in the configuration mode	
dotlx	IEEE Standard for port-based Network Access Control	
enable	Turn on privileged commands	
erns	Ethernet Ring Protection Switching	
exit	Exit from EXEC mode	
firmware	Firmware upgrade/swap	
help	Description of the interactive help system	
ip	IPv4 commands	
ipv6	IPv6 configuration commands	
logout	Exit from EXEC mode	
more	Display file	
no	Negate a command or set its defaults	
ping	Send ICMP echo messages	
platform	Platform configuration	
ptp	Misc non persistent 1588 settings	
reload	Reload system.	
send	Send a message to other tty lines	
show	Show running system information	
terminal	Set terminal line parameters	
veriphy	VeriPHY keyword	
Hyperionl#		
		~

Rys. 171. Lista poleceń w głównym menu

Polecenia wywoływane są po wpisaniu ich nazwy i naciśnięciu Enter, co powoduje dodanie nazwy danej grupy do tekstu zachęty. W takiej sytuacji dostępne są wyłącznie polecenia znajdujące się w danej grupie. Wyjście do grupy nadrzędnej możliwe jest po zastosowaniu polecenia "**exit"**. Wejście do konfiguracji przełącznika następuje po wpisaniu polecenia "**configure terminal**". Po

kliknięciu Enter przed znakiem zachęty pojawi się słowo "(config)#"

Dla ułatwienia pracy z wierszem poleceń CLI można używać tabulatora TAB na klawiaturze dzięki czemu system sam podpowie dostępne polecenia w danej grupie lub parametry jakie należy podać przy poleceniu.

Wyjście z programu następuje po wpisaniu polecenia logout.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	138/147
------	------	-----------------------------------	------------	---------



Za pomocą klawiszy strzałek w górę i w dół można przeglądać historię ostatnio wykonywanych poleceń. Historia ta nie jest zapamiętywana po wyjściu z programu. Klawisze strzałek w lewo i w prawo służą do poruszania kursorem po wpisanym poleceniu. Umożliwia to edycję polecenia przed jego wykonaniem.

Parametry dla poleceń wpisuje się za poleceniem oddzielając je spacjami. Np. Wielkość liter przy wprowadzaniu poleceń nie ma znaczenia.

Uwaga!: Dostępność poszczególnych poleceń jest uzależniona od wersji urządzenia HYPERION

Struktura poleceń

Polecenia są zorganizowane w formie drzewa. Struktura tego drzewa jest następująca:

clear	Funkcje resetowania
configure	Przejdź do trybu konfiguracji
сору	Kopiuj ze źródła do miejsca docelowego
delete	Usuń jeden plik w pamięci flash: system plików
dir	Katalog wszystkich plików w pamięci flash: system plików
disable	Wyłącz polecenia uprzywilejowane
do	Aby uruchomić polecenia w trybie konfiguracji
enable	Włącz polecenia uprzywilejowane
erps	Ethernet Ring Protection Switching
exit	Wyjdź z trybu EXEC
firmware	Aktualizacja / wymiana oprogramowania
help	Opis systemu pomocy interaktywnej
ip	Polecenia IPv4
ipv6	Polecenia konfiguracyjne IPv6
logout	Wyjdź z trybu EXEC
more	Wyświetl plik
no	Neguj polecenie lub ustaw jego wartości domyślne
ping	Wysyłaj komunikaty ICMP echo
platform	Konfiguracja platformy
ptp	Różne nietrwałe ustawienia 1588
reload	Przeładuj system.
send	Wyślij wiadomość do innych linii tty
show	Pokaż działające informacje o systemie
terminal	Ustaw parametry linii terminala
veriphy	Diagnostyka warstwy fizycznej dla kabli miedzianych

Po wejściu w tryb konfiguracji mamy do dyspozycji następujące:

(config)#	?			
àaa		Authentication, Authorization and Accounting		
access access-list		(Owierzyteinianie, autoryzacja i księgowanie) Access management (Zarządzanie dostępem) Lista dostępu		
aggregation		I ryb agregacji		
banner		Zdefiniuj baner		
chain		Skonfiguruj protokół redundancji CHAIN		
clock		Skonfiguruj zegar time-of-day		
ddmi		Informacje DDMI		
default		Ustaw polecenie na jego wartości domyślne		
REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	139/147



do	Aby uruchomić polecenia exec w trybie konfiguracij
dot1x	Standard IEEE dla kontroli dostepu do sieci w oparciu o portv
e1	Skonfigurui svgnał svnchronizacji F1
enable	Zmodyfikui parametry hasła dostepu
end	Wróć do trybu FXFC
ens	Ethernet Protection Switching
erns	Ethernet Ring Protection Switching
exit	Wvidź z bieżącego trybu
ans	Skonfigurui moduł GPS i aktualizacie czasu PTP
areen-ethernet	Green Ethernet (redukcia mocy)
avro	Włacz funkcie GVRP
heln	Opis systemu pomocy interaktywnei
hostname	Listaw nazwe sieci systemu
interface	Wybierz interfeis do skonfigurowania
in	Internet Protocol
inmc	Konfiguracia multicast IPv/L / IPv6
ip///c ip//6	Polecenia konfiguracyjne IPv6
ison	lavaScrint Object Notation RPC
Jach	
lino	Skonfigurui linie terminala
lldn	
logging	Komunikat logowania systemu
loop protect	Konfiguracia ochrony przed potla
100p-p101ect maa	Moley / konfiguracia tablicy MAC
mon	Maintananaa Entity Point
monitor	Maniterance Entity Form Meniterowenie réžoveb zderzeń systemowych
mornior	Konfiguracia rejectracii Multicast VI AN
IIIVI notwork clock	
network-clock	Zegal Sleciowy Nagui palacania lub ustawiago wartaści domyślno
110 nto	
nip	Skoniiguruj NTP
port-security	włącz / wyłącz globalne zabezpieczenia portow
privilege	Parametry uprawnien polecen
prp	Skonfiguruj protokoł redundancji PRP / HSR
ρτρ	Precision time Protocol (1588)
qos	Quality of Service
radius-server	Skonfiguruj RADIUS
rmon	Zdainy monitoring
StiOW	Przepływ statystyk
snmp-server	Ustaw konfiguracje serwera SNMP
spanning-tree	Spanning Tree protocol
switchport	Ustaw charakterystykę trybu przełączania
tacacs-server	Skonfiguruj TACACS+
thermal-protect	Konfiguracje ochrony termicznej
udid	Włącz UDLD w trybie agresywnym lub normalnym i ustaw konfigurowalny licznik
	komunikatów na wszystkich portach światłowodowych
upnp	Ustaw konfigurację UPnP
username	Ustanow uwierzytelnianie nazwy użytkownika
vlan	VLAN commands
voice	Atrybuty urządzenia głosowego
web	Web

Poniżej znajduje się kilka wybranych poleceń i ich zastosowanie

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	140/147
------	------	-----------------------------------	------------	---------



8.1.1 Ustaw nazwę hosta urządzenia i hasło administratora

Aby ustawić nazwę hosta urządzenia, najpierw przejdź do trybu konfiguracji, wpisując configure terminal i naciśnij klawisz Enter, a następnie wpisz nazwę hosta Hyperion i naciśnij klawisz Enter. Sekwencja powinna wyglądać tak, jak pokazano tutaj.

Ustaw nazwę hosta urządzenia # configure terminal (config)# hostname Hyperion1 Hyperion1(config)# exit Hyperion1#

Należy ustawić hasło dla administratora. # configure terminal Hyperion1(config)# username admin privilege 15 password unencrypted bitstream Hyperion1(config)# exit Hyperion1#

8.1.2 Ustaw adres IP sieci VLAN 1

Celem jest przypisanie adresu IP do urządzenia w sieci VLAN 1.

Hyperion1# configure terminal Hyperion1(config)# interface vlan 1 Hyperion1(config-if-vlan)# ip address 192.168.0.95 255.255.255.0 Hyperion1(config)# exit Hyperion1#

8.1.3 Weryfikacja ustawionego statycznego adresu IP

Hyperion1# show ip interface brief					
Interface	Address	Method	Status		
VLAN 1	192.168.0.126/24	Manual	UP		
VLAN 2	192.168.1.126/24	Manual	DOWN		
VLAN 3	192.168.2.126/24	Manual	DOWN		
Hyperion1#					

8.1.4 Zapisz konfigurację we Flashu

Konfiguracje można również zapisać w CLI do konfiguracji początkowej.

Hyperion1# copy running-config startup-config Building configuration... % Saving 3483 bytes to flash:startup-config Hyperion1#

8.2 Opis poleceń CLI dla oprogramowania w starszej wersji firmware oznaczonej v0xx

Do grup poleceń można wchodzić wpisując ich nazwy i naciskając Enter, co powoduje dodanie nazwy danej grupy do tekstu zachęty. W takiej sytuacji dostępne są wyłącznie polecenia znajdujące się w danej grupie. Wyjście do grupy nadrzędnej możliwe jest przez wpisanie "**exit"**.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	141/147
------	------	-----------------------------------	------------	---------



Polecenia w grupach można też wykonywać bez wchodzenia do grup – przez wpisanie nazwy grupy, a następnie nazwy polecenia w tej grupie po spacji. Np. wpisanie **ip setup** spowoduje wykonanie polecenia **setup** z grupy **ip**. Będąc w grupie poleceń nie jest możliwe wykonanie polecenia z grupy nadrzędnej.

Wyjście z programu następuje po wpisaniu polecenia logout.

Za pomocą polecenia **help** można uzyskać pomoc w programie na temat jego obsługi. Pomoc na temat konkretnych poleceń można wyświetlić wpisując **help** po słowie komendy np. **setup help**. Działa to także dla poleceń w grupach, np. **ip setup help**.

Za pomocą klawiszy strzałek w górę i w dół można przeglądać historię ostatnio wykonywanych poleceń. Historia ta nie jest zapamiętywana po wyjściu z programu. Klawisze strzałek w lewo i w prawo służą do poruszania kursorem po wpisanym poleceniu. Umożliwia to edycję polecenia przed jego wykonaniem.

Parametry dla poleceń wpisuje się za poleceniem oddzielając je spacjami. Np. **ip dhcp enable**, gdzie słowo **enable** jest parametrem.

Wielkość liter przy wprowadzaniu poleceń nie ma znaczenia.

Struktura poleceń

Polecenia są zorganizowane w formie drzewa. Struktura tego drzewa jest następująca:

- 1) System: Podstawowe ustawienia systemu i dziennik zdarzeń
- 2) IP: Konfiguracja adresu IP urządzenia i serwera NTP,
- 3) Port: Konfiguracja ustawień portów,
- 4) MAC: Konfiguracja i podgląd tablicy adresów MAC,
- 5) VLAN: Konfiguracja i monitorowanie wirtualnych sieci LAN,
- 6) PVLAN: Konfiguracja i monitorowanie prywatnych wirtualnych sieci LAN,
- 7) Security: Konfiguracja ograniczenia dostępu do zarządzania urządzeniem,
- 8) STP: Konfiguracja protokołów drzewa rozpinającego STP, RSTP, MSTP,
- 9) IGMP: Konfiguracja protokołu: Internet Group Management Protocol snooping,
- 10) Aggr: Konfiguracja agregacji portów,
- 11) LACP: Konfiguracja agregacji portów i protokołu: LACP IEEE 802.3ad,
- 12) LLDP: Konfiguracja i monitorowanie protokołu: LLDP IEEE 802.3ab,
- 13) EEE: Konfiguracja ustawień oszczędzania energii,
- 14) Led_power: Konfiguracja intensywności świecenia sygnalizacyjnych diod LED,
- 15) EPS: Konfiguracja liniowego protokołu protekcji drogi transmisyjnej,
- 16) MEP: Konfiguracja punktów końcowych ITU-T Y.1731,
- 17) QoS: Zarządzanie jakością usług i ochrony przed sztormem pakietów,
- 18) Mirror: Konfiguracja portów do podglądu transmisji (tzw. sniffer),
- 19) Firmware: Polecenie do pobrania pliku oprogramowani urządzenia z serwera TFTP,
- 20) PTP: Konfiguracja protokołu: IEEE1588 Precision Time Protocol,
- 21) ERPS: Konfiguracja protokołu protekcji drogi transmisyjnej dla urządzeń pracujących w topologii pierścienia,
- 22) CHAIN: Konfiguracja protekcji drogi transmisyjnej dla urządzeń pracujących w trybie łańcucha
- 23) LOAM: Konfiguracja protokołu opisanego w ITU-T Y.1731 używanego do implementacji funkcjonalności carrier Ethernet.

8.2.1 Grupa System

System Configuration [all | (port <port_list>)] – polecenie to wprowadzone bez parametrów wyświetla ogólne właściwości urządzenia, wśród których są informacje utrzymaniowe takie jak:

System Contact	 pole to pozwala na zapisanie np. kontaktu do administratora sieci,
System Name	– nazwa urządzenia,

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	142/147
------	------	-----------------------------------	------------	---------



System Location– lokalizacja urządzenia,Timezone Offset– offset strefy czasowej od strefy GMT w godzinach,MAC Address– adres MAC urządzenia,System Time– czas systemowy,System Uptime– czas, jaki upłyną od ostatniego restartu lub od włączenia urządzenia,Software Version– wersja oprogramowania,Software Date– data kompilacji oprogramowania,Previous Restart– sposób poprzednjego uruchomjenia urządzenia Cold – przez

Previous Restart – sposób poprzedniego uruchomienia urządzenia **Cold** – przez włączenie zasilania, **Cool** – przez powtórne uruchomienie.

Dodanie do polecenia parametru **all** spowoduje wyświetlenie pełnej konfiguracji portów dostępnych w urządzeniu. Parametr **port_list** określa, dla których portów ma zostać wyświetlona konfiguracja, można wpisać pojedynczą liczbę wtedy zostanie wyświetlona konfiguracja portu odpowiadającego temu numerowi. Można wprowadzić listę portów, których konfigurację chcemy wyświetlić, należy wprowadzać numery portów po przecinku bez spacji np. 2,5,7. Można również określić zakres portów przez wprowadzenie parametru, np. 1-3, spowoduje to wyświetlenie konfiguracji dla portów od 1 do 3. Wprowadzanie parametrów w sposób opisany wyżej jest możliwe również dla innych poleceń, w których występuje parametr **port_list**.

Log Configuration – polecenie bez parametrów wyświetla konfigurację syslog.

Version – polecenie bez parametrów wyświetla wersję oprogramowania zainstalowanego i uruchomionego.

Log Server Mode [enable|disable] – włącza parametr enable lub wyłącza parametr disable sysloga. Podanie tego polecenia bez parametrów wyświetli aktualną konfigurację sysloga. Kiedy syslog jest włączony i poprawnie skonfigurowany to wiadomości są wysyłane do serwera natychmiast po wystąpienia zdarzenia. Protokół syslog wykorzystuje do komunikacji UDP i port 514. Serwer syslog nie wysyła potwierdzeń do nadawcy. Protokół UDP jest bezpołączeniowym protokołem, dlatego też urządzenie po skonfigurowaniu sysloga będzie wysyłać komunikaty nawet, jeśli serwer syslog nie istnieje lub jest wyłączony.

Name [<name>] – polecenie bez parametru pozwala wyświetlić nazwę systemu, natomiast dodanie parametru w postaci ciągu znaków spowoduje przypisanie tego ciągu jako nazwa systemu.

Contact [<contact>] – podobnie jak wyżej, ale polecenie dotyczy pola System Contact.

Log Server Address [<ip_addr_string>] – polecenie ustawia adres IP serwera syslog. Adres ten należy podać, jako parametr w postaci WW.XX.YY.ZZ. Syslog w tym urządzeniu obsługuje tylko protokół IP w wersji 4. Podanie tego polecenia bez parametrów wyświetli aktualnie skonfigurowany adres serwera syslog.

Location [<location>] – również jak wyżej, polecenie dotyczy pola System Location.

Timezone [<offset>] – polecenie bez parametru wyświetla offset strefy czasowej od strefy GMT w godzinach, podanie liczby, jako parametru powoduje przypisanie jej jako offset strefy czasowej.

Log Lookup [<log_id>] [all|info|warning|error][clear] – polecenie to wpisane bez parametrów wyświetla całą zawartość systemowego dziennika zdarzeń. System rejestrując zdarzenie automatycznie przypisuje je do jednej z trzech grup stanowiących informacje o ważności wystąpienia zdarzenia. Występują trzy grupy zdarzeń:

- 1. Info zdarzenia informujące o zmianach stanu pracy urządzenia,
- 2. Warning zdarzenia pracy urządzenia wymagające ostrzeżenia użytkownika,

3. Error – zdarzenia sygnalizujące błąd w pracy urządzeń.

Dodanie parametru **log_id** powoduje zawężenie zakresu wyświetlania zdarzeń. System rejestrując zdarzenia nadaje numery ID w kolejności chronologicznej zaczynając od 1. Kolejny parametr pozwala zawęzić do jednej grupy zdarzeń wynik wyświetlania: **info**, **warning**, **error**, lub do wszystkich grup **all**. Ostatni parametr **clear** służy do wyczyszczenia listy dziennika zdarzeń.

Reboot – polecenie bez parametrów, powodujące natychmiastowe zamknięcie systemu operacyjnego w urządzeniu i ponowne go uruchomienie (tzw. restart). Po wykonaniu tego polecenia urządzenie nie będzie odpowiadać przez 10 sekund.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	143/147
------	------	-----------------------------------	------------	---------



Restore Default [keep_ip] – polecenie służy do przywrócenia ustawień domyślnych urządzenia, dodanie parametru keep_ip spowoduje przywrócenie domyślne wszystkich ustawień poza adresem IP.

Uwaga: Przywrócenie ustawień domyślnych może spowodować utratę łączności z urządzeniem, zależy to od ustawień sieci.

Load – polecenie bez parametru, którego zadaniem jest wyświetlenie informacji o aktualnym obciążeniu procesora przez system operacyjny i uruchomione aplikacje.

8.2.2 Grupa IP

Configuration – wyświetla aktualną informację o konfiguracji adresów IP urządzenia i informacje o włączeniu protokołu DHCP.

DHCP [enable|disable] – polecenie włącza lub wyłącza obsługę protokołu DHCP, urządzenie wyposażone jest tylko w klienta DHCP. Parametr **enable** włącza obsługę protokołu, zaś **disable** wyłącza. Wydanie polecenia **DHCP** bez parametru wyświetli informację o tym czy włączona jest obsługa protokołu DHCP i jeśli jest włączona nastąpi próba pobrania adresu IP z serwera DHCP.

Setup [<interface>][<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>] – polecenie ustawia statyczny adres ip wersji 4 urządzenia, znaczenie parametrów tego polecenia jest następujące: interface – wybór konfigurowanego interfejsu (eth0:0 – adres IP urządzenia, interfejsy eth0:1, eth0:2 oraz eth0:3 odpowiadają za adresy IP portów szeregowych) ip_addr – adres IP urządzenia, ip_mask – maska podsieci, ip_router – brama domyślna, vid – numer vlan zarządzania. Wydanie tego polecenia bez parametrów spowoduje wyświetlenie aktualnych ustawień protokołu IPv4 urządzenia.

Ping <ip_addr_string> [<ping_length>] – urządzenie wysyła zapytanie ICMP do hosta o adresie podanym w miejscu parametru **ip_addr_string**, parametr **ping_lenght** określa długość ramki i jest opcjonalny

IPv6 AUTOCONFIG [enable|disable] [<autoconfig_timeout>] – polecenie pozwala na włączenie parametr **enable** lub wyłączenie parametr **disable** autokonfiguracji adresów IP dla protokołu IP w wersji 6. Parametr **[<autoconfig_timeout>]** pozwala określić czas, po jakim urządzenie ma zaniechać prób automatycznej konfiguracji IP. Wartości dopuszczalne są w zakresie od 36 do 3600 sekund, domyślnie ten parametr ma wartość 300.

IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>] – polecenie ustawia statyczny adres IP w wersji 6 urządzenia, znaczenie parametrów tego polecenia jest następujące: **ipv6_addr** – adres IP urządzenia, **ipv6_prefix** – maska podsieci, **ipv6_router** – brama domyślna. Wydanie tego polecenia bez parametrów spowoduje wyświetlenie aktualnych ustawień protokołu IPv6 urządzenia. Adres IPv6 składa się z ośmiu 16-bitowych bloków złożonych z cyfr szesnastkowych i oddzielonych dwukropkiem. Możliwe jest pomijanie początkowych zer w bloku. Adres IPv6 należy wprowadzać w następującej postaci: aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh.

NTP Configuration – polecenie to wyświetla listę adresów IP serwerów czasu skonfigurowanych w celu aktualizacji czasu systemowego. Urządzenie aktualizując czas systemowy korzysta z protokołu Network Time Protocol przedstawionego w RFC5905.

NTP Mode [enable|disable] – wydanie tego polecenia z parametrem **enable** spowoduje włączenie funkcjonalności aktualizacji czasu systemowego przez protokół NTP, natomiast użycie parametru **disable** spowoduje, że ta funkcjonalność będzie nie aktywna.

NTP Server Add <server_index> <ip_addr_string> - polecenie to dodaje do listy serwerów adres IP serwera czasu NTP. Parametr **server_index** określa, na której pozycji ma zostać wpisany dany serwer dozwolone są pozycje od 1 do 5. Pozycje określają kolejność, w jakiej urządzenie będzie próbowało się łączyć z serwerem czas, jeśli uda się synchronizacja czasu z serwerem, którego adres znajduje się na pierwszej pozycji to zaniecha kolejnych prób z serwerami umieszczonymi na dalszych pozycjach. Parametr **ip_addr_string** określa adres IP w wersji 4 serwera czasu, ten parametr należy podać w postaci WW.XX.YY.ZZ. Urządzenie nie obsługuje protokołu DNS i nie można wprowadzić samej nazwy serwera. Przykładowy serwer czasu to serwer Głównego Urzędu Miar tempus1.gum.gov.pl, którego adres to 212.244.36.227.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	144/147
------	------	-----------------------------------	------------	---------


https://www.bitstream.pl

NTP Server lpv6 Add <server_index> <server_ipv6> - polecenie to działa w taki sam sposób jak poprzednie tylko pozwala wprowadzić adres IP w wersji 6. Adres IPv6 należy wprowadzać w następującej postaci: aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh.

NTP Server Delete <server_index> – polecenie to usuwa z listy serwerów NTP server o numerze podanym, jako parametr **<server_index>**.

8.2.3 Grupa Port

Configuration [<port_list>] [up|down] – wprowadzenie tego polecenia bez parametrów spowoduje wyświetlenie listy portów dostępnych w urządzeniu wraz z ich konfiguracją. Parametr **port_list** zawęża listę wybranych portów. Stosując drugi parametr **up|down** możemy zawęzić listę portów wyświetlanych do portów, które odbierają poprawny sygnał Ethernet (link). Do tego służy parametr **up,** lub wyświetlić porty, które takiego sygnału nie odbierają **down**.

Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx] – wprowadzenie tego polecenia bez parametrów spowoduje wyświetlenie listy portów dostępnych w urządzeniu wraz z aktualną konfiguracja, parametr **port_list** zawęża listę wyświetlonych portów, natomiast dodając jeden z parametrów na drugiej pozycji ustawiamy prędkość transmisji i duplex. Znaczenie parametrów jest następujące:

auto : Autonegocjacja szybkości transmisji i trybu połączenia

- 10hdx : 10 Mbps, half duplex
- **10fdx** : 10 Mbps, full duplex
- 100hdx : 100 Mbps, half duplex
- 100fdx : 100 Mbps, full duplex
- 1000fdx : 1 Gbps, full duplex

Uwaga! Prędkość 10 Mbps Dostępna jest tylko dla połączeń wykonanych kablem miedzianym.

Flow Control [<port_list>] [enable|disable] – wprowadzenie tego polecenia bez parametrów wyświetla listę portów wraz z konfiguracją, parametr **port_list** zawęża listę wyświetlonych portów, drugi parametr określa czy kontrola przepływu ma być włączona **enable** lub wyłączona **disable**.

State [<port_list>] [enable|disable] – polecenie to pozwala na wyłączenie portów Ethernet w celu oszczędzania energii, parametr **port_list** zawęża listę wybranych portów, drugi parametr określa czy port ma być włączony **enable** lub wyłączony **disable**. Polecenie to wprowadzone bez parametrów powoduje wyświetlenie listy portów dostępnych w urządzeniu i informacji o stanie tego portu.

MaxFrame [<port_list>] [<max_frame>] – polecenie to pozwala na określenie maksymalnej długości ramek obsługiwanych na poszczególnych portach Ethernet. Parametr port_list zawęża listę wybranych portów, drugi parametr max_frame określa maksymalna długość ramki w bajtach, dozwolony zakres dla tego parametru to 1528 - 9600. Polecenie to, wprowadzone bez parametrów powoduje wyświetlenie listy portów dostępnych w urządzeniu i informacji o maksymalnej długości ramki obsługiwanej na tym porcie.

Power [<port_list>] [enable|disable|actiphy|dynamic] - polecenie to pozwala na włączenie oszczędzania energii przez układy nadawczo/odbiorcze pracujące na portach Ethernet. Parametr **port_list** zawęża listę wybranych portów. Dostępne są trzy tryby oszczędzania energii: podczas gdy port nie odbiera poprawnego sygnału Ethernet (ActiPhy) parametr **actiphy**, w czasie normalnej pracy portu z poprawnym sygnałem Ethernet (PerfectReach) parametr **dynamic** i w obu przypadkach (Enable). Oszczędzanie energii można również wyłączyć przez podanie parametru **diable.**

Excessive [<port_list>] [discard|restart] – polecenie to określa sposób zachowania się portu w przypadku wystąpienia szesnastu kolizji przy próbie transmisji jednej ramki. Parametr **port_list** zawęża listę wybranych portów. Drugi parametr określa czy urządzenie ma zaprzestać transmisji ramki i w konsekwencji tego ją odrzucić - parametr **discard** lub czy ma próbować ponownie transmitować parametr **restart**.

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	145/147
------	------	-----------------------------------	------------	---------



https://www.bitstream.pl

Statistics [<port_list>] [<command>] [up|down] – polecenie to wyświetla statystyki ruchu na dostępnych w urządzeniu portach. Parametr **port_list** zawęża listę wybranych portów. Parametr **command** może przyjąć jedną z poniższych wartości:

clear: czyści statystyki ustawia wszystkie liczniki na 0,packets: wyświetla ilość pakietów odebranych i nadanych,bytes: wyświetla ilość bajtów odebranych i nadanych,errors: wyświetla ilość pakietów odebranych i nadanych z błędem,discards: wyświetla ilość pakietów odrzuconych,filtered: wyświetla ilość pakietów odebranych krótszych niż 64B i dłuższych niż maksymalnadługość skonfigurowana przez polecenie MaxFrame.

0..7 : wyświetla ilość pakietów odebranych i nadanych z nadanymi priorytetami w miejsce parametru **command** należy wprowadzić numer priorytetu od 0 do 7.

VeriPHY [<port_list>] – polecenie to sprawdza poprawność wykonania okablowania na portach RJ-45 dostępnych w urządzeniu, sprawdza poprawność wszystkich czterech par skręcanych w kablu, a także dokonuje pomiaru długości kabla dołączonego do portu. W trakcie pomiaru transmisja odbywa się w sposób niezakłócony. Parametr **port_list** zawęża listę wybranych portów.

8.2.4 Grupa Chain

Chain add <group-id> <first_port> [head|member|tail] <second_port> [head|member|tail] <first_port_mep_id> <second_port_mep_id> - polecenie to umożliwia dodanie nowego łańcucha. Poniżej zostały opisane poszczególne parametry:

group-id – parametr opcjonalny, numer identyfikacyjny łańcucha; brak podania tego parametru spowoduje wyświetlenie wszystkich skonfigurowanych grup

first_port - numer pierwszego portu

head|member|tail - rola pierwszego portu

second_port - numer drugiego portu

first_port_mep_id - numer identyfikacyjny punktu MEP pierwszego portu

second_port_mep_id - numer identyfikacyjny punktu MEP pierwszego portu

Chain remove <group-id> - polecenie to umożliwia usunięcie łańcucha o podanym numerze ID

Chain conf [<group-id>] - polecenie to wyświetla konfigurację łańcucha o podanym numerze id

Chain status [<group-id>] - polecenie to wyświetla pełny status łańcucha o podanym numerze id

9 Dane techniczne

Parametry indywidualne poszczególnych modeli przełączników zawarte są w instrukcjach skróconych dostarczanych w zestawie z przełącznikami

10 Instrukcje konfiguracji wybranych funkcji przełączników Hyperion

Instrukcje konfiguracji wybranych funkcji w przełącznikach Hyperion są do pobrania za pomocą poniższych linków z naszego serwera FTP

REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	146/147
------	------	-----------------------------------	------------	---------



https://www.bitstream.pl

10.1 Zestaw poleceń ze składnią konsoli ICLI w Hyperion dla wybranych poziomów w nowszej wersji firmware

http://anymux.pl/files/Produkty/HYPERION_MANUAL_GUI_CLI/Command_syntax_in_CLI.pdf

10.2 Przykładowa konfiguracja RINGU

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_Ring_Hyp-105_30x_40x_50x_short.pdf

10.3 Przykładowa konfiguracje Telemetry oraz IN/OUT w H-30x-3

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_Telemetry_Hyp-301_3_short.pdf http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_IN_OUT_Hyp-30x-3.pdf

10.4 Przykładowa konfiguracja funkcji NTP

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_NTP_Hyp-105_30x_40x_500_short.pdf

10.5 Przykładowa konfiguracja funkcji Ping Watchdog

(UWAGA: Funkcja dostępna w wybranych wersjach przełączników z PoE)

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_Watchdog_PoE_Hyp-105_301_402_short.pdf

10.6 Przykładowa konfiguracja PTP dla Master oraz Boundry Clock

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_PTP_Hyp-105_30x_40x_50x_short.pdf

10.7 Przykładowa konfiguracja NAT

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/Static_NAT_Hyp-200_402_500_short.pdf

10.8 Konfiguracja protokołu SNMPv3

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_SNMPv3_konfiguracja_Hyperion_all.pdf ,

10.9 Konfiguracja RS jako serwera portów szeregowych w HYPERION-30x-3

http://www.anymux.pl/files/Soft/IO_short-konfiguracje/pl/IO_RS_Hyp-30x_short.pdf

REV. 1.06 INSTRUKCJA OBSŁUGI : HYPERION-GUI 2024.01.04 147/14	REV.	1.06	INSTRUKCJA OBSŁUGI : HYPERION-GUI	2024.01.04	147/147
---	------	------	-----------------------------------	------------	---------