PRZEŁĄCZNIK PRZEMYSŁOWY

HYPERION-105

INSTRUKCJA OBSŁUGI

SPIS TREŚCI

1 INFORMACJE PODSTAWOWE

1.1 Zgodność z normami i zaleceniami

Urządzenie **HYPERION-105** zostało zaprojektowane w oparciu o obowiązujące normy i zalecenia z zakresu transmisji danych, kompatybilności elektromagnetycznej i bezpieczeństwa użytkowania.

1.1.1 Kompatybilność elektromagnetyczna

Urządzenia zostały zaprojektowane w oparciu o normę PN-EN 55011:2016-05 klasa B, PN-EN 61000-6-2:2008 + Ap1:2008P + Ap2:2009P. Urządzenia **BITSTREAM** są przeznaczone do pracy w pomieszczeniach zamkniętych.

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

HYPERION-105 jest zaprojektowany 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 10/100Mbit/s

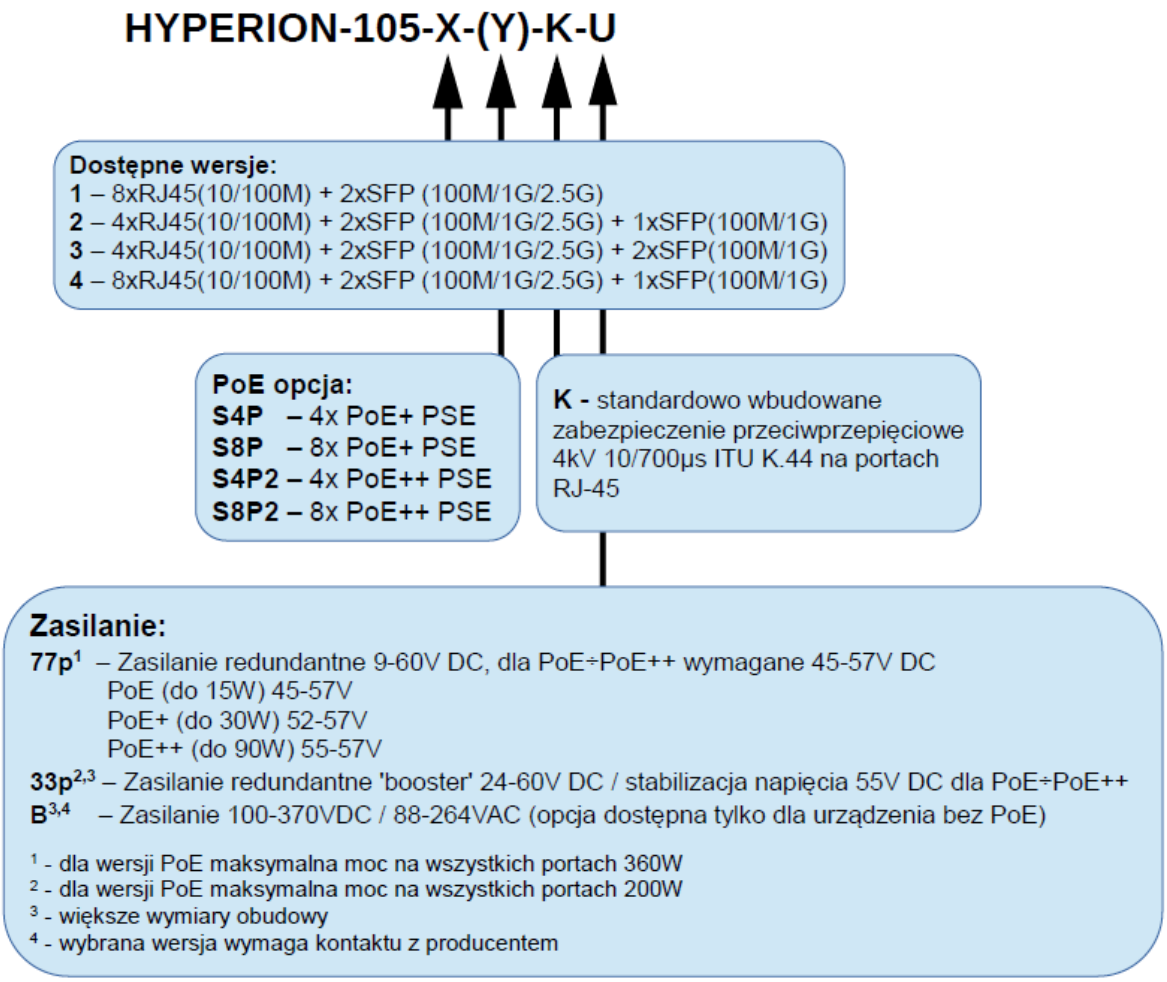
IEEE 802.1q, p – Definicje mechanizmów sieci **VLAN** i priorytetów transmisji sygnałów dla sieci ETHERNET

IEEE 802.3af - zgodność interfejsów Ethernet ze standardem PoE

IEEE 802.3at - zgodność interfejsów Ethernet ze standardem PoE+

PoE++ do 90W/port

1.2 Oznaczenie



Przykładowe oznaczenia:

HYPERION-105-1-K-B

Hyperion 105 w wersji z interfejsem 8xRJ45(10/100M) + 2xSFP (100M/1G/2.5G) i standardowo wbudowanym zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45, zasilanie 100-370VDC / 88-264VAC

HYPERION-105-1-S8P2-K-77p

Hyperion 105 w wersji z interfejsem 8xRJ45(10/100M) PoE++ do 90W + 2xSFP (100M/1G/2.5G), ale sumaryczna moc na wszystkich portach PoE nie może przekroczyć 360W, standardowo wbudowane zabezpieczenie przeciwprzepięciowe 4kV 10/700µs ITU K.44 na portach RJ45, zasilanie redundantne 6-60VDC (dla PoE++ 55-57V)

2 OPIS FUNKCJONALNY

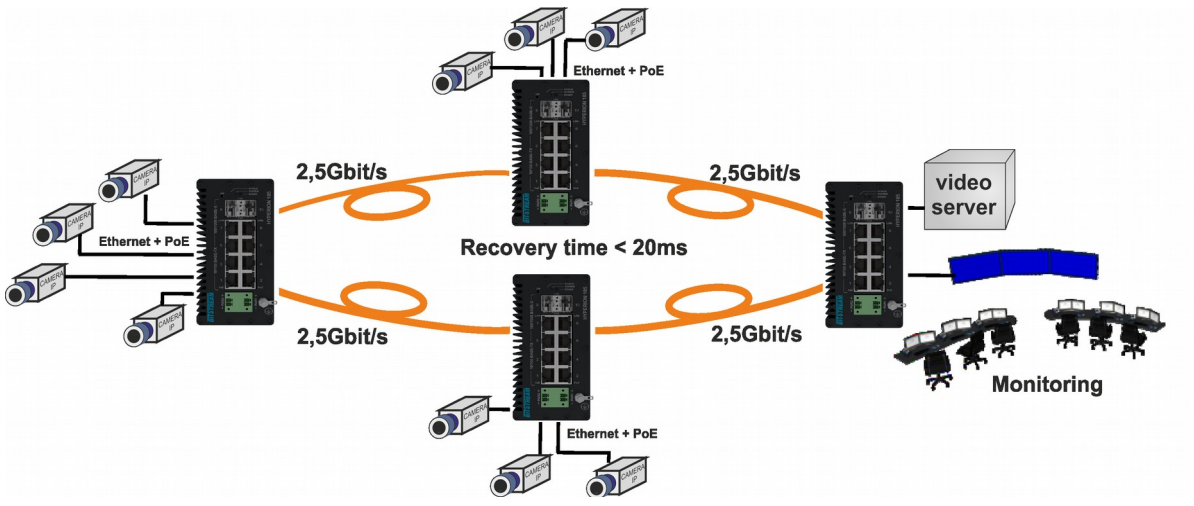
2.1 Funkcje i Zastosowania

Światłowodowy przełącznik **HYPERION-105** 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-105** jest w pełni zgodny ze standardem: 10/100BaseT(X) i 100/1000BaseFX.

Zastosowanie przełącznika **HYPERION-105** pozwala budować rozległą sieć transmisji danych w oparciu o różne media transmisyjne to jest skrętkę miedzianą 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-105

3 Złącza i sygnalizacja

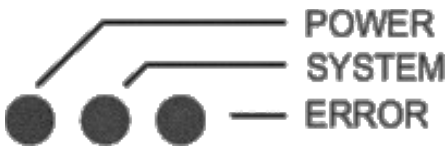
3.1 Panel przedni

Rys. 2. Panel przedni urządzenia Hyperion-105

1 – Zacisk uziemienia
2 – Złącza zasilania
3 – Porty Ethernet - 8x RJ45 + 2x SFP

4 – DEF – przycisk do przywracania konfiguracji domyślnej
5 – Diody sygnalizacyjne

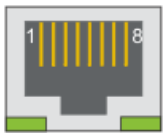
3.2 Oznaczenie diod sygnalizacyjnych



Rys. 3. Panel przedni urządzeń, cd.

POWER – wskaźnik zasilania
SYSTEM – sygnalizuje poprawność działania urządzenia
ERROR – sygnalizuje wystąpienie błędu

3.2.1 Opis złącz urządzenia



Rys. 4. *Wygląd i numeracja wyprowadzeń złącza RJ45*

Rozmieszczenie poszczególnych sygnałów dla złącz RJ-45 przedstawia tabela.

Port	Przeznaczenie	Opis wyprowadzeń
10/100 BaseT(X)	Ethernet 10/100Mbps	1 – TX+ 2 – TX - 3 – RX+ 6 – RX -

Dioda prawa dolna:
- LED PoE – sygnalizuje podawaną moc: zielona PoE/ PoE+; żółta PoE++, tryb Force – żółta miga

Dioda lewa dolna:
- LED Link-act
- LED 10M – żółta link 10Mbps (aktywność miga)
- LED 100M – zielona link 100Mbps (aktywność miga)

4 Instalacja i obsługa

4.1 Warunki pracy

Przełącznik może pracować w sposób ciągły w pomieszczeniach zamkniętych w warunkach podanych w danych technicznych. Nie powinien być narażony na bezpośrednie nasłonecznienie. Nie zaleca się ustawiania urządzenia na źródłach ciepła, choć dopuszczalne jest powieszenie go, obok innych urządzeń na szynie DIN EN 50022, ale tak by ścianka urządzenie zawierająca otwory wentylacyjne była odsunięta od sąsiedniego urządzenia, o co najmniej 15mm. W tym wypadku powinien być zapewniony swobodny przepływ powietrza.

4.2 Zasilanie

Przełącznik **HYPERION-105** powinien być zasilany ze źródła napięcia stałego o wartości 6 - 60 V DC, nie jest istotna polaryzacja na złączu zasilającym. Parametry zasilania są identyczne dla obydwu wejść zasilających

Wykorzystując redundancję zasilania dla przełącznika **HYPERION-105** należy do obydwu wejść PWR1 i PWR2 podłączyć zasilanie o parametrach zgodnych z danymi technicznymi. Urządzenie zapewnia separację galwaniczną pomiędzy dwoma wejściami zasilania. Przełącznik może pracować również bez redundancji zasilania, wtedy należy podłączyć zasilanie tylko do jednego z wejść.

4.3 Instalacja

Przełącznik wykonany jest jako urządzenie do montażu na szynie DIN EN 50022. Jednakże dozwolony jest montaż urządzenia w dowolnej pozycji poza szyną DIN, ale tak, aby nie zasłaniać otworów wentylacyjnych. Po podłączeniu zasilania o odpowiednich parametrach do obu wejść powinna zaświecić się dioda LED PWR. W przypadku .

4.4 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 szmatką niepozostawiającą włókien.

5 Zarządzanie

Zarządzanie urządzenia wykorzystuje protokoły HTTP, HTTPS oraz SNMP i możliwe jest przez dowolny port Ethernet urządzenia. Dodatkowo dostęp do niektórych parametrów urządzenia dostępny jest przez SSH lub z poziomu konsoli.

Domyślny adres IP interfejsu zarządzania to 192.168.0.10, domyślny użytkownik to „admin", domyślnie brak hasła.

6 Opis GUI dostępnego przez przeglądarkę WWW

Konfiguracja **HYPERION-105** za pomocą protokołów http i https wymaga komputera z zainstalowaną przeglądarką internetową – zalecane jest używanie przeglądarki Firefox, Internet Explorer (w wersji 6 lub wyższej) 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.

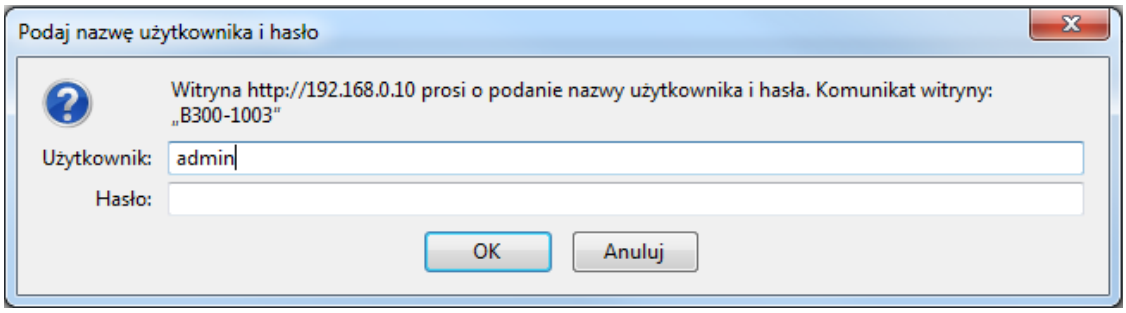
Przycisk *Reset* obecny na większości stron powoduje odświeżenie strony z aktualnymi ustawieniami urządzenia i usunięcie ustawień wprowadzonych, a nie zapisanych. Zarządzanie urządzeniem **HYPERION-105** przez interfejs www jest podzielone na cztery grupy główne:

- Konfiguracja (*Configuration*), grupa ta umożliwia zmiany ustawień urządzenia między innymi: 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: wykonanie ponownego uruchomienia urządzenia (tzw. restart), przywrócenie ustawień fabrycznych urządzenia i aktualizację oprogramowania.

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

6.1 Ochrona urządzenia hasłem

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



Rys. 5. Panel logowania

Domyślna nazwa użytkownika: *admin*
Domyślne hasło: nie ma i należy to pole 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 pod interfejsem http zmienia się także hasło dostępu do CLI i odwrotnie.

Stan zalogowania (sesja) w urządzeniu jest utrzymywany ciągle do momentu wylogowania, a można tego dokonać przez kliknięcie ikony w prawym górnym rogu strony z symbolem otwartych drzwi i strzałką. Obok tej ikony znajduje się ikona ze znakiem zapytania, która uruchamia w zależności od kontekstu nowe okno przeglądarki, w którym są opisane wszystkie dostępne funkcje, jakie w danej chwili udostępnia strona główna urządzenia. Strony, które wyświetlają dane często zmieniające się jak na przykład statystki ruchu na poszczególnych portach mogą być odświeżane ręcznie prze kliknięcie przycisku *Refresh* lub automatycznie przez zaznaczenie pola *Auto-refresh*.

6.2 Właściwości ogólne

Po poprawnym zalogowaniu się wyświetli się pierwsza strona z ogólnymi informacjami dotyczącymi stanu pracy poszczególnych portów. Bezpośrednie kliknięcie na port na rysunku przedstawiającym wizualizację urządzenia spowoduje przeniesienie na stronę przedstawiającą szczegółowe statystyki danego portu. Ogólne właściwości urządzenia wraz z danymi dotyczącymi wersji oprogramowania, numerem MAC urządzenia są dostępne pod linkiem **Monitor > System > Information**. Znaczenie poszczególnych pól jest następujące:

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.

Powyższe pola można uzupełnić na stronie dostępnej przez link **Configuration > System > Information**. Na stronie tej można również ustawić offset strefy czasowej do poprawnego wyświetlania aktualnego czasu systemowego.

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

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-50-c2-0e-3f-94
Device Type	Hyperion-301-3
Serial Number	94
Time	
System Date	1970-01-01T23:37:03+00:00
System Uptime	0d 23:37:03
Software	
Software Version	B301-3010
Software Date	2015-02-16T09:27:04+01:00

Rys. 6. Ogólne właściwości urządzenia

6.3 KONFIGURACJA DOSTĘPU URZĄDZENIA DO SIECI IP

Komunikacja z urządzeniem odbywa się standardowo z wykorzystaniem protokołu IP w wersji 4. 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 adresu dynamicznego z serwera DHCP, drugi to praca urządzenia ze statycznym adresem IP. Tabelka do konfiguracji IP posiada dwie kolumny pierwsza kolumna od lewej *Configured* posiada możliwość edycji i wprowadzania adresów IP. Ustawienia w tej kolumnie należy potwierdzić przyciskiem *Save* lub anulować przyciskiem *Reset*. Druga kolumna wyświetla bieżący adres IP urządzenia. Znaczenie poszczególnych wierszy tej tabelki jest następujące:
DHCP Client – ustawienia klienta DHCP – zaznaczenie pola w kolumnie ***Configured*** spowoduje, że urządzenie będzie po każdym włączeniu zasilania lub po ponownym uruchomieniu próbować pobierać adres z serwera DHCP. Odznaczenie tego pola wymusi na urządzeniu pracę ze statycznym adresem i zablokuje możliwości naciśnięcia na przycisk ***Renew***. Brak obecności serwera DHCP w sieci spowoduje, że urządzenie rozpocznie dalszą pracę z adresem statycznym wpisanym w wierszu poniżej. Jeśli prawidłowo skonfigurowany serwer DHCP jest obecny w sieci, to po uzyskaniu dynamicznego adresu IP zostanie on wyświetlony w kolumnie ***Current***. Przycisk ***Renew*** służy do ręcznego wymuszenia na kliencie DHCP pracującym w przełączniku ponowienia próby pobrania adresu dynamicznego. Kolejne kolumny:

- ***IP Address*** - oznacza adres IP urządzenia.
- ***IP Mask*** – maskę podsieci.
- ***IP Router*** – bramę domyślną.

- ***VLAN ID*** - służy do konfiguracji numeru wirtualnej sieci LAN w której będzie możliwość dostępu do 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.

UWAGA! Nowe urządzenie ma domyślnie wyłączone DHCP oraz ustawiony adres IP statycznie na 192.168.0.10 i maskę podsieci 255.255.255.0.

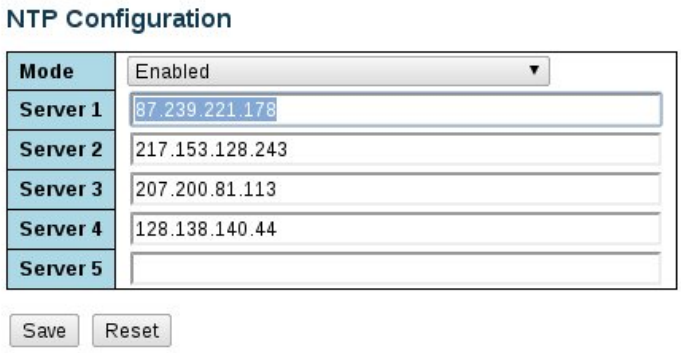
IP Configuration

	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	0.0.0.0
DNS Server 2	0.0.0.0	0.0.0.0
DNS Server 3	0.0.0.0	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	0.0.0.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	0
eth0:2		
IP Address	0.0.0.0	0.0.0.0
IP Mask	0.0.0.0	0.0.0.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	0
eth0:3		
IP Address	0.0.0.0	0.0.0.0
IP Mask	0.0.0.0	0.0.0.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	0

Rys. 7. Konfiguracja i ustawienia dostępu urządzenia do sieci.

6.3.1 Konfiguracja NTP

W urządzeniu **HYPERION-105** jest dostępna obsługa 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**.



Rys. 8. Konfiguracja NTP

W pierwszej kolumnie tabeli są opisane parametry dla NTP: ***Mode*** oraz 5 adresów IP. Są to adresy serwerów obsługujących synchronizację czasu.

Tryb NTP (***Mode)*** ma dwie wartości:
Enabled – w tym trybie urządzenie funkcjonuje jako tzw „pośrednik" protokołu NTP. W urządzeniu które np. ustawia zegar korzystając z NTP można podać numer IP urządzenia HYPERION-105 i może ono przekazywać pakiety NTP do serwera i odpowiedź od tegoż do urządzenia, które wysłało zapytanie o synchronizację. Ma to znaczenie, jeśli serwer NTP i urządzenie ustawiające swój zegar znajdują się w innych sieciach. **HYPERION-105** jest w takim wypadku „widziane" przez urządzenie ustawiające zegar jako serwer NTP. Natomiast Serwer NTP „widzi" **HYPERION-105** jako klienta żądającego synchronizacji.

Disabled – w tym trybie obsługa protokołu NTP jest wyłączona.

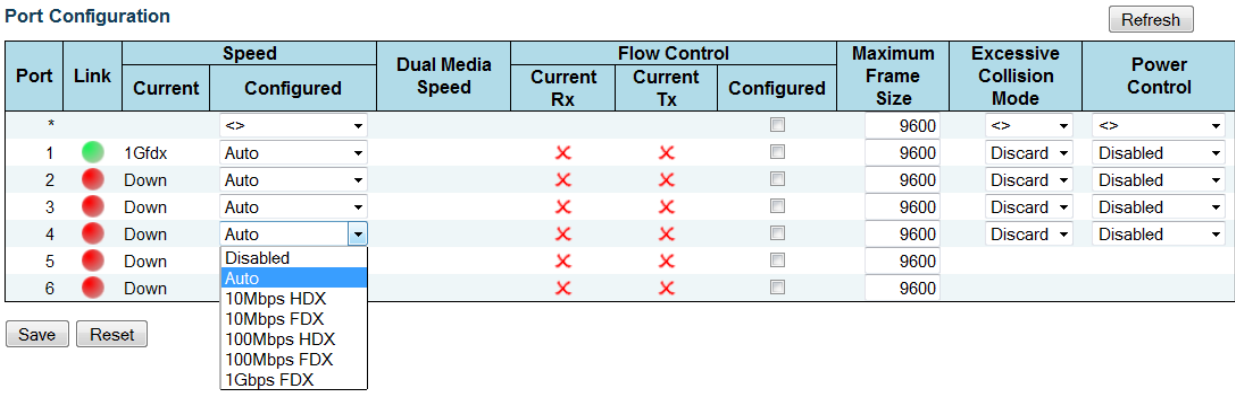
W polach opisanych jako ***Server 1, Server 2, ... , Server 5*** należy wpisać adresy IP serwerów protokołu NTP. Adresy IP mogą być podane w wersji IPv4 jak również w wersji IPv6.
Serwery wpisane w tabelę są serwerami obsługującymi protokół NTP. Są one potrzebne do poprawnej konfiguracji **HYPERION-105** jako „pośrednika" dla protokołu NTP.
Nie jest konieczne wpisywanie wszystkich 5-ciu adresów IP. Dla poprawnego funkcjonowania synchronizacji czasu w **HYPERION-105** wystarczy wpisać tylko jeden adres IP serwera NTP. Urządzenie próbuje najpierw synchronizować czas z serwerem 1, jeśli próba zakończy się niepowodzeniem to urządzenie próbuje łączyć się 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.***

6.4 Konfiguracja portów Ethernet

Strona umożliwiająca konfigurację portów Ethernet **HYPERION-105** jest dostępna pod linkiem **Configuration > Ports**. Strona ta wyświetla w kolumnie ***Link*** aktualny stan połączeń na wszystkich portach, szybkość i tryb połączenia w kolumnie ***Speed Current***, a poza tym udostępnia następujące funkcje konfiguracyjne:

Speed Configured – ustawianie dupleksu oraz prędkości transmisji kanałów Ethernet, lub wyłączenie portu.
Flow Control Configured – włączenie automatycznej kontroli przepływu.
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 ponowne próby transmisji (***Restart***). Ustawienie nie ma znaczenia w przypadku pracy portu w trybie full-duplex,
Power Control – konfiguracja sposobu oszczędzania energii, domyślnie oszczędzanie energii przez port jest wyłączone (***Disabled***). Dostępne są trzy tryby oszczędzania energii: podczas gdy port nie odbiera poprawnego sygnału Ethernet (***ActiPhy***), w czasie normalnej pracy portu z poprawnym sygnałem Ethernet (***PerfectReach***) i w obu przypadkach (***Enable***).

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.



Rys. 9. Konfiguracja trybu pracy poszczególnych portów przełącznika

6.5 Ograniczenie dostępu zdalnego

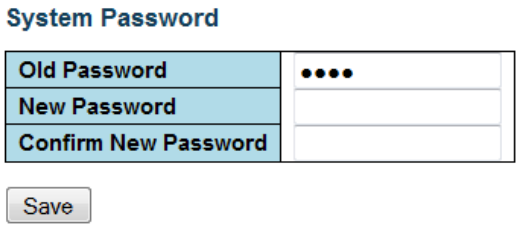
Przełącznik **HYPERION-105** wyposażony jest w możliwość ograniczenia zdalnego dostępu do zarządzania. Ograniczenie to jest zrealizowane na cztery sposoby:

- 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 dostępnej przez link: **Configuration > Security > Switch > Password.** W celu wprowadzenia hasła należy w polu oznaczonym ***New Password*** wprowadzić żądane hasło, następnie w polu ***Confirm New Password*** należy ponownie wprowadzić to samo hasło, natomiast pole ***Old Password*** należy pozostawić puste. Następnie należy 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***.

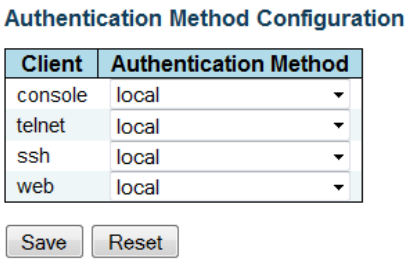
Ograniczenie protokołów zarządzania można dokonać na stronie dostępnej przez link: **Configuration > Security > Switch > Auth Method**. Domyślnie urządzenie **HYPERION-105** posiada włączone wszystkie obsługiwane protokoły do zarządzania. W celu wyłączenia z obsługi jednego lub więcej protokołów należy przy nazwie wybranego protokołu przestawić za pomocą pola wyboru 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***.



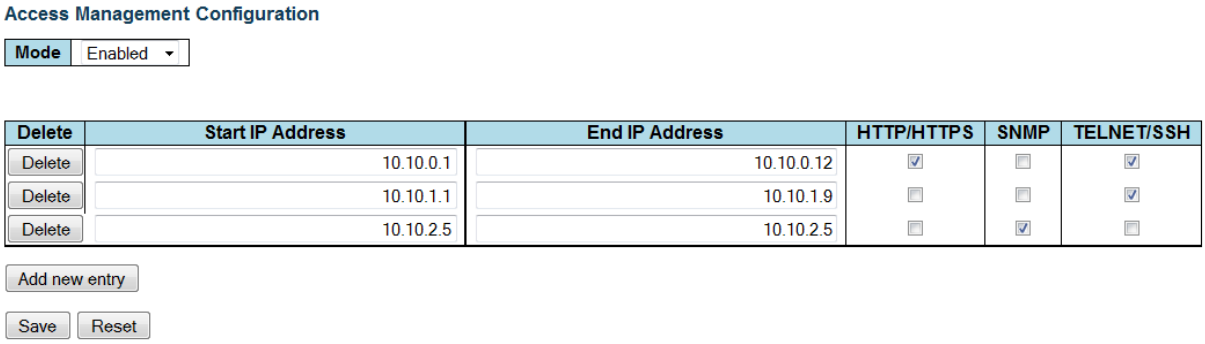
Rys. 10. Ustawianie hasła

Ograniczenie zakresu adresów IP stacji roboczych, z których można uzyskać dostęp do zarządzania można ustawić na stronie dostępnej przez link: **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-105**, 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.



Rys. 11. Ograniczenie protokołów zarządzania

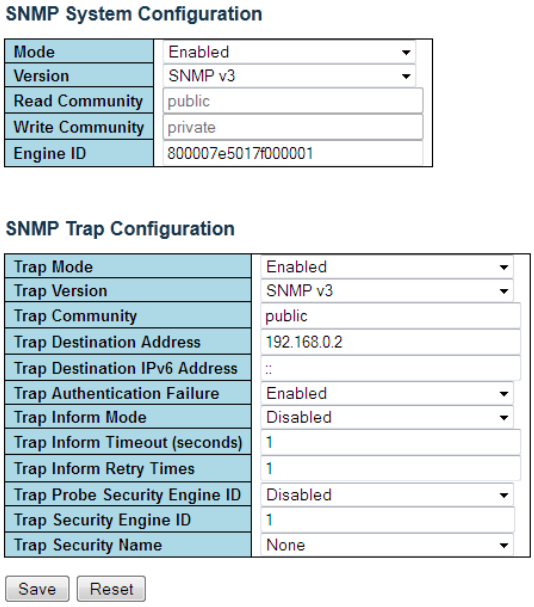


Rys. 12. Ograniczenie zakresów adresów IP do zarządzania

6.6 SNMP Simple Network Management Protocol

SNMP jest uniwersalnym protokołem wspomagającym zarządzanie urządzeń pracujących w sieciach IP. Wykorzystuje on głównie protokół UDP na standardowym porcie 161 (wysyłanie żądań) oraz 162 (komunikaty *TRAP*). **HYPERION-105** 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.



Rys. 13. Konfiguracja ogólna SNMP

Dostęp do konfiguracji agenta SNMP można uzyskać przez menu link **Configuration > Security> Switch > 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.

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:

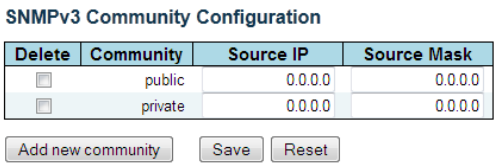
- ***Trap Authentication Failure*** – umożliwia włączenie lub wyłączenie wysyłania wiadomości *Trap* przy próbie nieautoryzowanego dostępu do urządzenia przez SNMP.
- ***Trap Inform Mode*** **–** jeśli włączone, to **HYPERION-105** będzie oczekiwać zwrotnego pakietu typu *Inform*, potwierdzającego odebranie 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.

6.6.1 Konfiguracja SNMPv3

HYPERION-105 posiada pełną obsługę SNMPv3 wraz z bezpiecznym uwierzytelnianiem oraz szyfrowaniem transmisji (szyfrowanie *DES*).

6.6.1.1 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.



Rys. 14. Konfiguracja społeczności w trybie SNMPv3

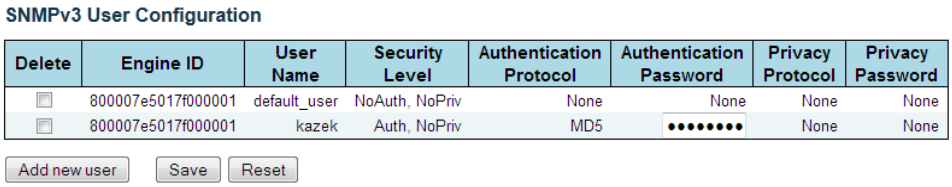
Dodatkowo do każdej społeczności można określić zakres adresów IP, z których będzie możliwy dostęp do niej, co zwiększa bezpieczeństwo. Znaczenie maski jest podobne, jak w sieciach IP: bity ustawione na 1 określają niezmienną część adresu IP, a bity ustawione na 0 – część zmienną. Dla przykładu: jeśli ***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***.

6.6.1.2 Użytkownicy

Konfiguracja użytkowników znajduje się w podmenu ***Users***.



Rys. 15. 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*.

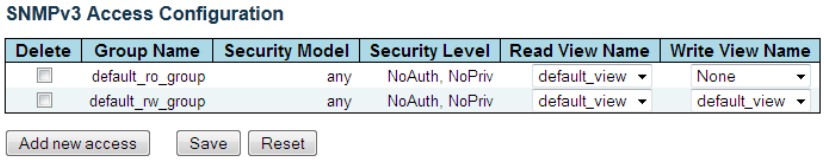
Authentication Password – hasło dostępu, jeśli opcja autoryzacji jest włączona; hasło musi składać się z 8 do 32 znaków.

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.

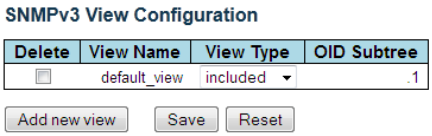
6.6.1.3 Grupy i widoki

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



Rys. 16. Konfiguracja grup Dostępu w SNMPv3

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**,

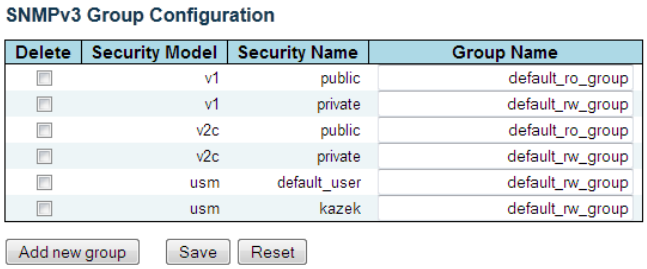


Rys. 17. Konfiguracja widoków SNMPv3

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.

6.6.1.4 Przypisania użytkowników do grup

Przypisania użytkowników do grup dokonuje się na podstronie **Groups**.

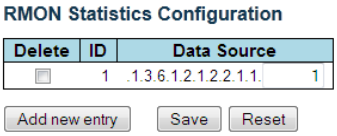


Rys. 18. Konfiguracja grup w SNMPv3

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.

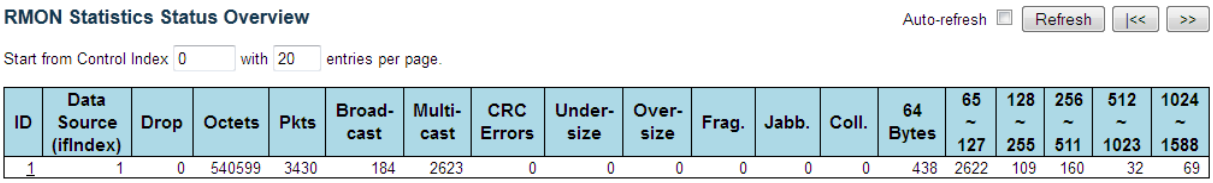
6.6.2 RMON Remote Network Monitoring

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 podmenu **RMON > Statistics**.



Rys. 19. 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-105** dostępne numery portów zawierają się w przedziale od 1 do 6 dla **HYPERION-105.1-2** i od 1 do 7 dla **HYPERION-105.1-3**. 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 > SNMP > RMON**.



ID	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. 20. 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).
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.

6.6.2.1 Rejestracja historii

Wybierając menu **Configuration > Security > Switch > SNMP > 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. 21. Konfiguracja 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.
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 > SNMP > RMON > History**. Panel ten jest pokazany poniżej:

RMON History Overview

Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per 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	0	369	3	0	3	0	0	0	0	0	0	0
1	1235	20968	0	246	2	0	2	0	0	0	0	0	0	0
1	1236	20973	0	246	2	0	2	0	0	0	0	0	0	0
1	1237	20978	0	492	4	0	4	0	0	0	0	0	0	0
1	1238	20983	0	246	2	0	2	0	0	0	0	0	0	0
1	1239	20988	0	246	2	0	2	0	0	0	0	0	0	0
1	1240	20993	0	369	3	0	3	0	0	0	0	0	0	0
1	1241	20998	0	246	2	0	2	0	0	0	0	0	0	0
1	1242	21003	0	369	3	0	3	0	0	0	0	0	0	0
1	1243	21008	0	369	3	0	3	0	0	0	0	0	0	0
1	1244	21013	0	783	11	0	11	0	0	0	0	0	0	0
1	1245	21018	0	369	3	0	3	0	0	0	0	0	0	0
1	1246	21023	0	369	3	0	3	0	0	0	0	0	0	0
1	1247	21028	0	246	2	0	2	0	0	0	0	0	0	0
1	1248	21033	0	246	2	0	2	0	0	0	0	0	0	0
1	1249	21038	0	369	3	0	3	0	0	0	0	0	0	0
1	1250	21043	0	369	3	0	3	0	0	0	0	0	0	0
1	1251	21048	0	246	2	0	2	0	0	0	0	0	0	0
1	1252	21053	0	369	3	0	3	0	0	0	0	0	0	0
1	1253	21058	0	246	2	0	2	0	0	0	0	0	0	0

Rys. 22. 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*), ale względne – przyrost od poprzedniego odczytu. Ostatnia kolumna (***Utilization***) zawiera

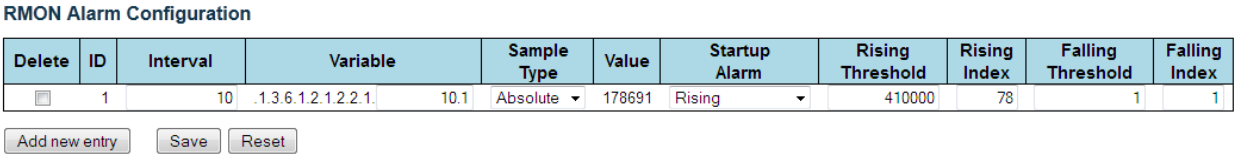
szacunkową średnią zajętość pasma na porcie w ciągu ostatniego interwału próbkowania w setnych częściach procenta (wartość 100 oznacza 1%).
Możliwe jest przeglądanie tej tablicy przy użyciu kontrolek znajdujących się nad nią:

- ***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.

6.6.2.2 Alarmy i zdarzenia

W ramach RMON **HYPERION-105** posiada możliwość definiowania kryteriów alarmowych, generowania zdarzeń oraz akcji podejmowanych po ich wystąpieniu. Kryteria alarmowe są definiowane w menu **Configuration > Security > Switch > SNMP > RMON > Alarm**.



Rys. 23. Konfiguracja alarmów RMON

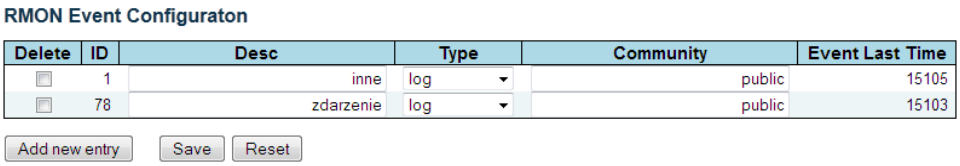
Skonfigurowane alarmy są zaprezentowane w postaci tabeli. W celu dodania nowego alarmu należy kliknąć ***Add new entry***, co spowoduje dodanie kolejnego wiersza do tabeli, a następnie wypełnić nowy wiersz odpowiednimi wartościami i kliknąć ***Save***. Wartości w tabeli są następujące:

- ***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 (wcześniej opadnięcie wartości poniżej dolnego progu nie będzie wyzwalało alarmu), ***Falling*** – rejestracja rozpocznie się dopiero po opadnięciu wartości poniżej dolnego progu alarmowego (wcześniej 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 wystąpi pierwsze).

- ***Rising/Falling Threshold*** – określają odpowiednio górny i dolny próg dla badanego licznika. Jeśli wartość licznika przekroczy górny próg lub spadnie poniżej dolnego progu, generowany jest alarm RMON. Akcję dla alarmu 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**.

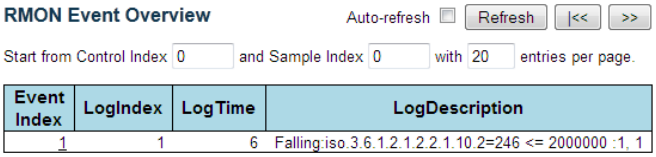


Rys. 24. Konfiguracja zdarzeń RMON

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*.
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***.



Rys. 25. 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-105**.
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.

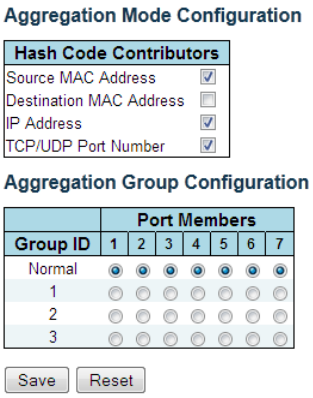
6.7 Agregacja portów

Przełącznik **HYPERION-105** umożliwia agregację portów Ethernet oraz światłowodowych w różnych konfiguracjach (nie ma rozróżnienia pomiędzy typami portów). Agregacja jest to łączenie kliku portów równolegle w celu uzyskania większej przepustowości łącza oraz redundancji, która zapewnia większą odporność systemu na uszkodzenia.

HYPERION-105 obsługuje agregację statyczną oraz automatyczną przy użyciu protokołu LACP (*Link Aggregation Control Protocol*).

6.7.1 Agregacja statyczna

Agregacja statyczna umożliwia ręczne wybranie agregowanych portów, które pozostają niezmienne niezależnie od warunków panujących w sieci.



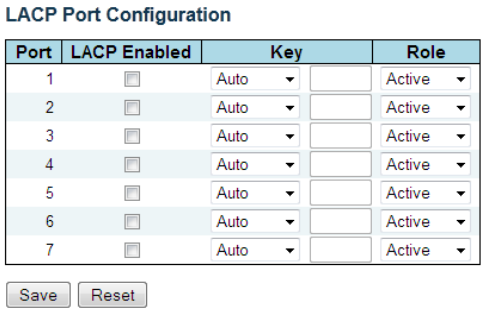
Rys. 26. Konfiguracja statycznej agregacji portów

Możliwa jest agregacja w maksymalnie 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.**

6.7.2 Agregacja automatyczna

Agregacja automatyczna w **HYPERION-105** jest realizowana z wykorzystaniem protokołu LACP, zdefiniowanego w normie IEEE 802.3ad. Protokół ten umożliwia automatyczną negocjację grupowania połączeń pomiędzy urządzeniami go obsługującymi.



Rys. 27. 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.

6.8 Redundancja drogi przesyłowej

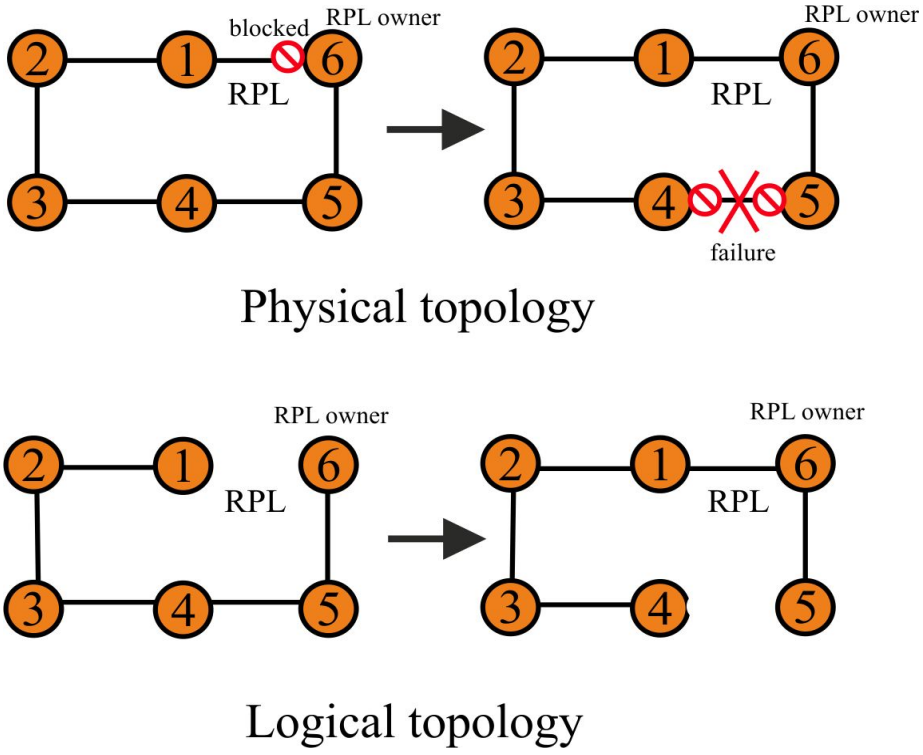
Przełączniki **HYPERION-105** oferują kilka protokołów zapewniających redundancję drogi przesyłowej, a są to:

- 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,
- 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.

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

Sieć w topologii pierścienia można budować z urządzeń **HYPERION-105** bez ograniczeń ilościowych. Do budowy pierścienia można używać dowolnych dwóch portów przełącznika. Budowę pierścienia i możliwe stany pracy pierścienia przedstawia rysunek poniżej.



Rys. 28. Budowa i sposób działania protekcji drogi transmisyjnej w topologii pierścienia

Mechanizm protekcji, aby przeciwdziałać powstawaniu pętli w sieci Ethernet działa w następujący sposób: W stanie *idle* czyli w stanie pełnej sprawności pierścienia, gdy wszystkie połączenia tworzące pierścień są sprawne. Jedno z fizycznych połączeń pomiędzy przełącznikami zostaje wyróżnione i staje się połączeniem redundantnym, które stanowi logiczną przerwę w sieci. . Połączenie to nosi nazwę *RPL* (ring protection link), na jednym z końców tego polaczenia występuje przełącznik, który steruje pracą całego pierścienia i nosi nazwę *RPL Owner*. Zadaniem tego przełącznika jest logiczne blokowanie odbierania i nadawania danych na port podłączony do *RPL*. Drugi koniec połączenia *RPL* jest podłączony do przełącznika, który nazywa się *RPL Neighbour*. Wyróżnienie dwóch przełączników na obu końcach połączenia *RPL* ma tylko jedno zadanie, które polega na tym, że w sytuacji wystąpienia przerwy na połączeniu *RPL* przełączniki te nie doprowadzą do rekonfiguracji pierścienia, a jedynie poinformują pozostałe urządzenia o awarii. Taka rekonfiguracja nie jest potrzebna, gdyż fizyczne połączenie, które uległo awarii nie ma wpływu na logiczną budowę sieci. Ta cecha przełącznika **HYPERION-105** powoduje, że urządzenia tworzące pierścień nie czyszczą

tablic adresów MAC. Jest to jedno z działań podczas rekonfiguracji i tym samym nie doprowadzają do chwilowego zwiększeniu ruchu w sieci, jaki w sposób naturalny powstaje, gdy przełączniki posiadają puste tablice MAC i nie znając położenia stacji w sieci rozsyłają pakiety na wszystkie porty.

6.8.2 Sposób działania protekcji drogi transmisyjnej zgodnie z zaleceniem ITU-T G.8032

W stanie *idle* wszystkie przełączniki monitorują porty i stany połączeń, jakie tworzą pierścień, oprócz tego, aby stan pierścienia był znany przez wszystkie przełączniki każdy z nich na porty tworzące pierścień wysyła pakiety utrzymaniowe *R-APS*, co 5 sekund.

W momencie wystąpienia przerwy w jednym z połączeń, przełącznik rozpoczyna blokowanie portu, który utracił połączenia dla danych przychodzących i wychodzących oraz jednocześnie na drugi port tworzący pierścień wysyła natychmiast trzy pakiety *R-APS* z informacją o awarii i dalej kontynuuje wysyłanie tej informacji w odstępach pięciosekundowych. Pakiety te docierają do wszystkich przełączników, które dokonują wymazania wpisów tablicy MAC portów tworzących pierścień. Przełącznik *RPL owner* również dokonuje czyszczenia tablicy MAC i podejmuje akcję związaną z odblokowaniem portu tworzącego połączenie *RPL* i tym samym zapewnienie łączności pomiędzy segmentami sieci. Stan, w jakim znajduje się teraz pierścień jest stanem *protected.* Pierścień pozostanie w nim do momentu przywrócenia połączenia, które jest w stanie awaryjnym.

W momencie przywrócenia połączenia, które uległo awarii przełączniki, które to wykryją dalej blokują ten port, aby przeciwdziałać powstawaniu pętli. Na drugi port tworzący pierścień taki przełącznik wysyła pakiety *R-APS* z informacją o braku awarii, informacja ta dociera do wszystkich przełączników, ale żaden z nich nie podejmuje akcji jedynie *RPL owner* włącza licznik liczący w dół od czasu, jaki jest ustawiony dla *HOLD OFF time* domyślnie jest to jedna minuta. Po upływie tego czasu *RPL owner* wysyła na oba swoje porty tworzące pierścień informację o powrocie do stanu *idle* i informację o tym, aby dokonać czyszczenia tablicy adresów MAC. Wszystkie przełączniki dokonują czyszczenia tablicy MAC adresów portów pierścienia, przełącznik *RPL owner* rozpoczyna blokowanie portu podłączonego do RPL, a przełączniki, które zgłosiły awarię przestają blokować porty tym samym zakańcza się rekonfiguracja do stanu *idle*.

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 rozgłoszeniowym, które przemieszczają się w ramach tej niedodanej sieci VLAN.

Ramki utrzymaniowe *R-APS* są wysyłane, jako *multicast*, dlatego konieczne jest ograniczenie domeny rozgłoszeniowej dla tych ramek przez ustawienia odpowiedniej konfiguracji VLAN. Szczegóły zostaną podane podczas omawiania przykładów konfiguracji.

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

Przed przystąpieniem do konfiguracji protokołu redundancji, należy skonfigurować punkty *MEP (Maintenance Entity Point)* dla każdego portu urządzenia tworzące pierścień. Podczas tej konfiguracji podaje się, w jaki sposób dany port ma dokonywać detekcji awarii na tym polaczeniu, czy przez wykrycie zaniku fizycznego sygnału, czy przez wykrycie zaniku odbierania ramek *Continuity Check Message CCM*. Poza tą konfiguracją ustawia się również transmisję ramek *R-APS* i numer VLAN dla tych pakietów.
Dostęp do konfiguracji jest pod linkiem **Configuration > 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 się pole typu checkbox. Zaznaczenie tego pola i wciśnięcie przycisku ***Save*** również spowoduje usunięcie 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: ***Ingress*** – wejściowy, ***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 informacja o wystąpieniu alarmu

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

Maintenance Entity Point Refresh

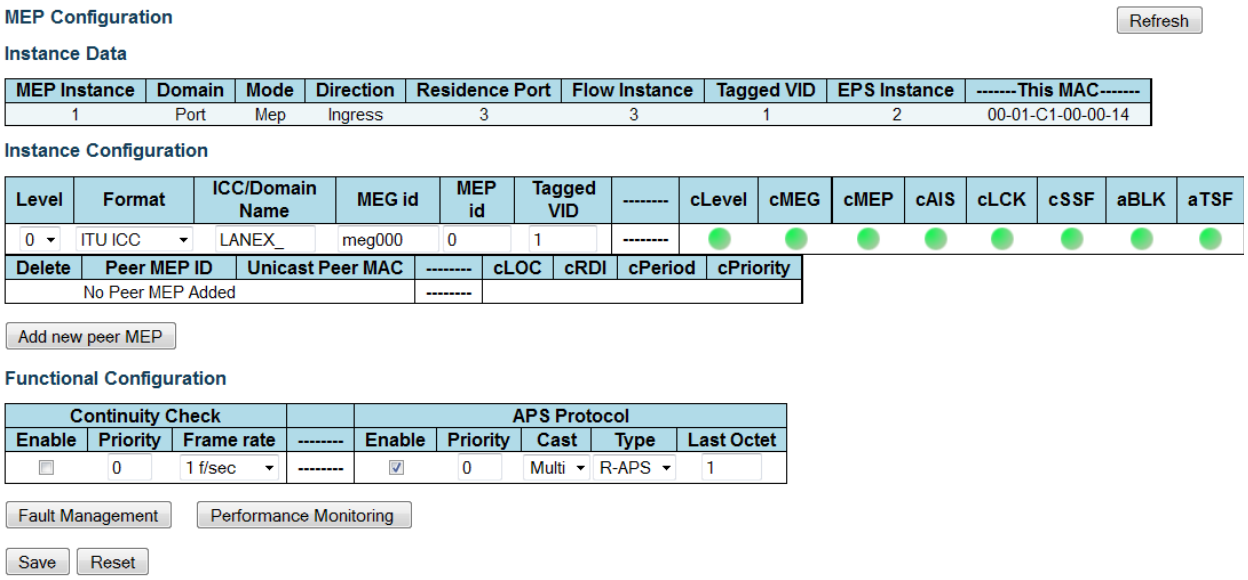
Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	-------This MAC-------	Alarm
☐	1	Port	Mep	Ingress	3	0	3	1	00-01-C1-00-00-14	
☐	2	Port	Mep	Ingress	4	0	4	1	00-01-C1-00-00-15	
☐	3	Port	Mep	Ingress	5	0	5	1	00-01-C1-00-00-16	
Delete	4	Port	Mep	Ingress	1	0	1	0		

Add new MEP Save Reset

Rys. 29. Konfiguracja ogólna punktów MEP

Wprowadzenie szczegółowej konfiguracji punktów *MEP* jest możliwe przez menu pokazane konfiguracji ogólnej punktów MEP , dostęp do tego menu jest możliwy przez kliknięci 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 taką samą 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.
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*,

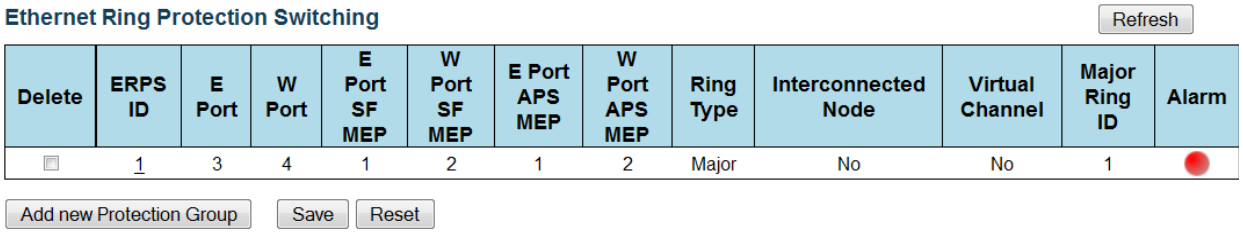


Rys. 30. Konfiguracja szczegółowa punktów MEP

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,
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 będzie zgłaszał 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.

6.8.4 Konfiguracja procesu protekcji drogi transmisyjnej w topologii pierścienia

Konfiguracja protokołu protekcji drogi transmisyjne w urządzeniach HYPERION-105 dostępna jest przez link **Configuration > ERPS**.



Rys. 31. Konfiguracja ogólna procesu protekcji

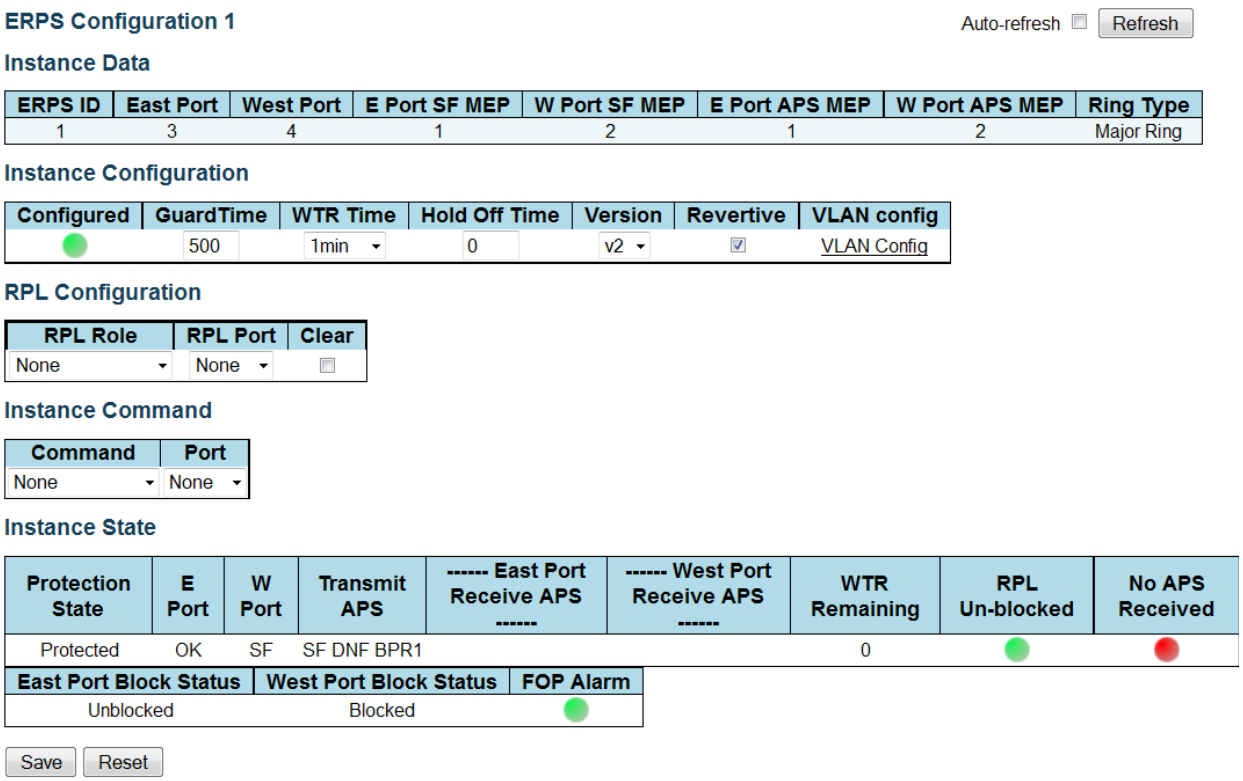
Dodanie nowej konfiguracji RING polega na kliknięciu przycisku ***Add New Protection Group***, wprowadzeniu parametrów pracy układu protekcji i zatwierdzenie przyciskiem ***Save***.

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.
East Port – numer pierwszego portu, jaki w danym urządzeniu będzie użyty do budowy pierścienia.
West Port – numer drugiego portu, jaki w danym urządzeniu będzie użyty do budowy pierścienia.
East Port SF MEP – numer identyfikacyjny punktu *MEP*, który ma zgłaszać alarm związany z przerwą ciągłości łącza dla Port E.
West Port SF MEP – numer identyfikacyjny punktu *MEP*, który ma zgłaszać alarm związany z przerwą ciągłości łącza dla Port W.
Port East APS MEP – numer identyfikacyjny punktu *MEP*, którego zadaniem jest wysyłanie ramek utrzymaniowych *R-APS* dla Port E.
Port West APS MEP – numer identyfikacyjny punktu *MEP*, którego zadaniem jest wysyłanie ramek utrzymaniowych *R-APS* dla Port W.

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 sytuacji awaryjnej i zgłasza alarm czerwony symbol czy jest w sytuacji pełnej 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 .



Rys. 32. Konfiguracja szczegółowa procesu protekcji

Znaczenie poszczególnych pól jest następujące:

Configured – graficzna sygnalizacja poprawności konfiguracji danego pierścienia, zielony symbol oznacza prawidłową konfigurację, a czerwony bledną konfigurację.

Guard Time – czas wstrzymania odbierania ramek *R-APS* podawany w milisekundach. Urządzenie, które zgłasza alarm w momencie wystąpienia awarii, a następnie w wyniku prac operatora to polaczenie zostaje przywrócone to urządzenie ponownie wyśle informację, ale o powrocie sprawności pierścienia i po wysłaniu tej informacji odczekuje czas zapisany w tym parametrze za nim zacznie analizować przychodzące ramki R-APS. Domyślna wartość 500 ms 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 – *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 przywróceniu polaczenia, 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 działania 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 tylko implementowana 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 przywróceniu awaryjnego połączenia. 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.

Rys. 33. Konfiguracja numerów sieci VLAN dla danego procesu ERPS

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-105**, 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.

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 kliknięcie 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 służą 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.

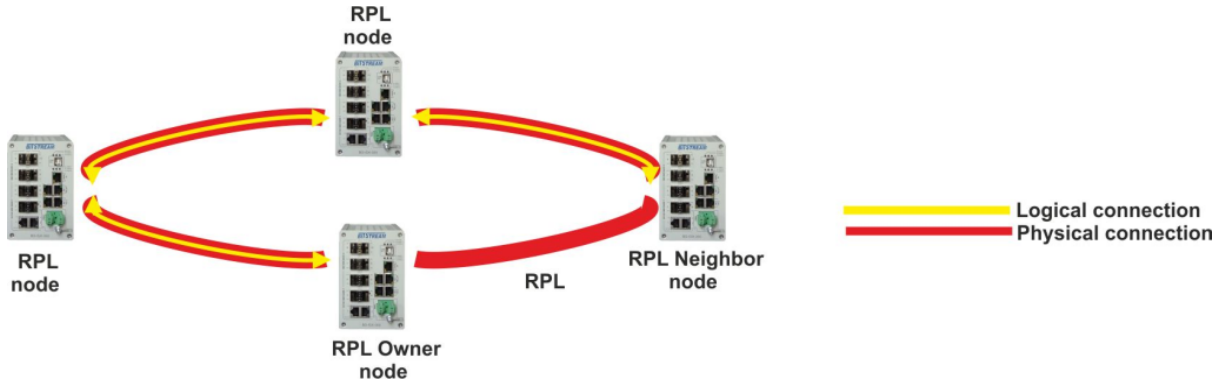
6.8.5 Przykłady konfiguracji protokołu protekcji drogi transmisyjnej w topologii pierścienia

Przed przystąpieniem do konfiguracji protokołu protekcji należy zawsze w każdym pierścieniu jedno dowolne połączenie utrzymywać w stanie rozłączonym, aby nie dopuścić do zapętlenia sieci. Przed rozpoczęciem konfiguracji należy wyłączyć na

portach tworzących pierścień pozostałe protokoły protekcji np. protokoły z grupy spanning tree.

6.8.5.1 Przykład I

Urządzenia pracują tylko z jedną domyślnie ustawioną siecią VLAN nr 1, schemat funkcjonalny takiego układu przedstawia rysunek poniżej. Urządzenie **HYPERION-105** zawsze pracuje w trybie VLAN i do prawidłowej pracy przełącznika i systemu zarządzania wymaga, co najmniej jednego poprawnie skonfigurowanego VLAN. Ustawienia domyślne urządzenia **HYPERION-105** przypisują wszystkie porty przełącznika łącznie z portem systemu zarządzania do sieci VLAN o numerze 1, a ramki wychodzące z przełącznika nie mają umieszczonych tagów zgodnie z IEEE802.1Q.



Rys. 34. Schemat funkcjonalny przykładu I

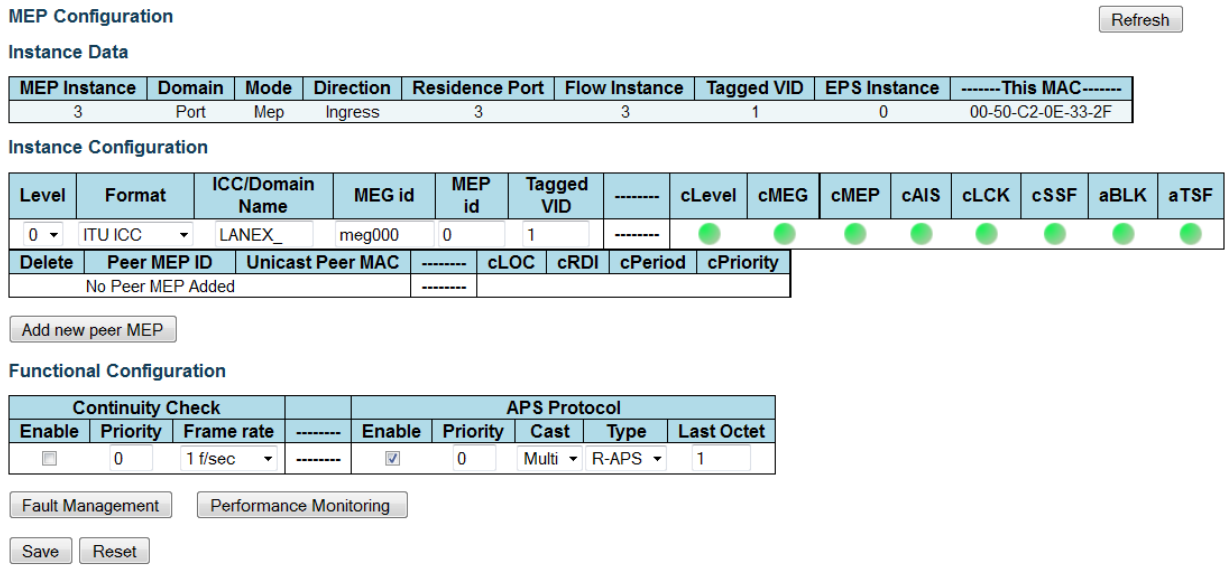
W tym przykładzie ruch Ethernetowy nie będzie ograniczony wirtualnymi sieciami LAN, ale podczas konfiguracji protokołu protekcji należy w każdym z przełączników wprowadzić informację o tym, że protekcja dotyczy tej sieci VLAN o numerze 1.
W tej konfiguracji należy wyróżnić dwa przełączniki, jeden *RPL Owner*, a drugi *RPL Neighbour*. Wszystkie urządzenia tworzące pierścień będą reagowały na zanik sygnału Fast Link Fail. We wszystkich przełącznikach logiczny port E dla protokołu protekcji będzie fizycznym portem numer 3, a port W natomiast będzie portem fizycznym numer 4.

Podczas konfiguracji pierwszym elementem, jaki należy skonfigurować to punkty MEP odnoszące się do portów tworzących pierścień we wszystkich przełącznikach.

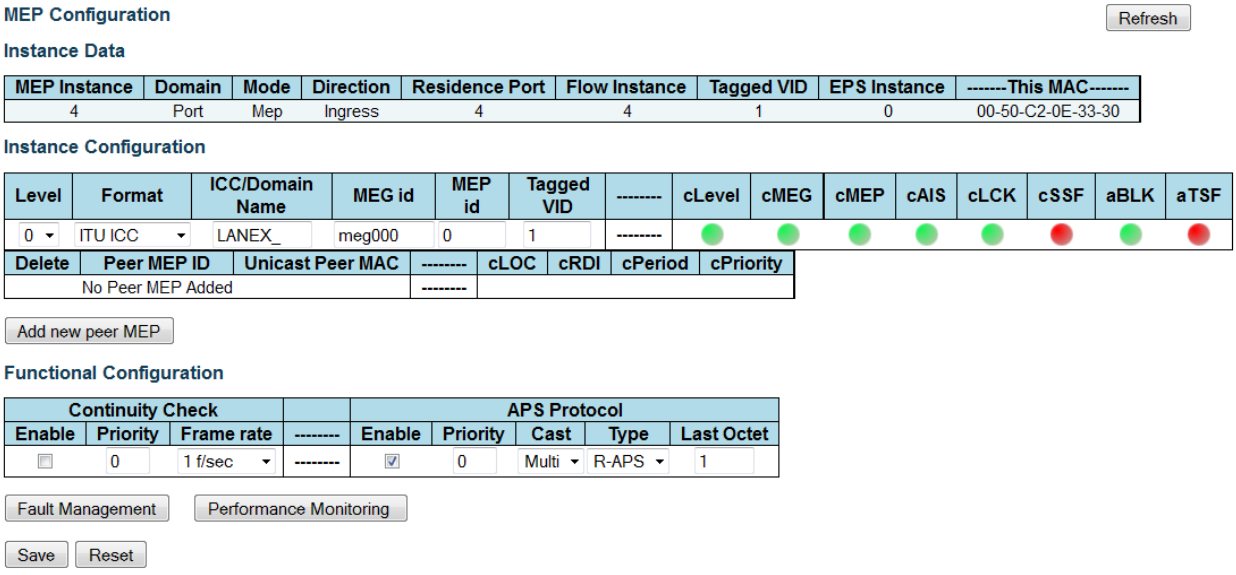
- **Konfiguracja punktu MEP dla logicznego portu E**
  Instance – dowolny numer *id* danego punktu *MEP*, dla ułatwienia konfiguracji może być taki sam jak numer portu fizycznego na którym tworzymy ten punkt czyli 3.
  Parametry: Domain, Mode, Direction, Level – pozostają domyślne.
  Residence Port, Flow Instance – należy wpisać numer portu fizycznego czyli 3.
  Tagged Vid – numer Vlan modułu zarządzania, czyli w tym wypadku 1.
  Następnie wchodzimy do szczegółowej konfiguracji tego punktu przez link w kolumnie ***Instance***.
  Dokonujemy konfiguracji wysyłania ramek utrzymaniowych *R-APS*, w tabeli ***APS Protocol*** zaznaczamy ***Enable. Priority*** i ***Last Octet*** pozostają domyślne, ***Cast*** wybieramy: ***Multi*** i ***Type: R-APS***.

- **Konfiguracja punktu MEP dla logicznego portu W**

Instance – dowolny numer *id* danego punktu *MEP*, dla ułatwienia konfiguracji może być taki sam jak numer portu fizycznego na którym tworzymy ten punkt czyli 4.
Parametry – Domain, Mode, Direction, Level pozostają domyślne.
Residence Port, Flow Instance – należy wpisać numer portu fizycznego czyli 4.
Tagged Vid – numer Vlan dla ramek *R-APS*, czyli w tym wypadku 1.
Następnie wchodzimy do szczegółowej konfiguracji tego punktu przez link w kolumnie ***Instance***.
Dokonujemy konfiguracji wysyłania ramek utrzymaniowych *R-APS*, w tabeli ***APS Protocol*** zaznaczamy ***Enable. Priority*** i ***Last Octet*** pozostają domyślne, ***Cast*** wybieramy: ***Multi*** i ***Type***: ***R-APS***.



Rys. 35. Konfiguracja szczegółowa punktu MEP dla portu E



Rys. 36. Konfiguracja szczegółowa punktu MEP dla portu W

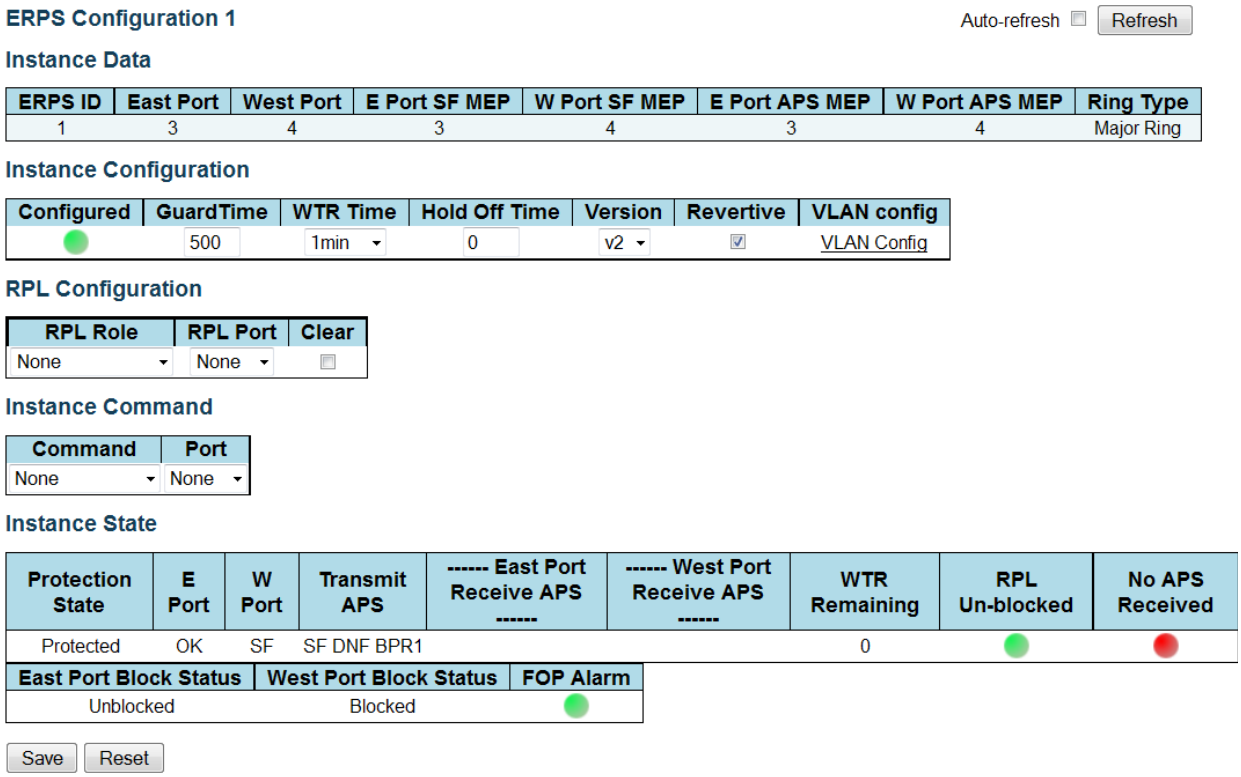
- **Konfiguracja protokołu protekcji**
  W jednym pierścieniu może pracować nieskończenie dużo przełączników, które nie są wyróżnione. Wszystkie przełączniki tworzące pierścień należy najpierw skonfigurować jako niewyróżnione, a następnie wybrane urządzenia wyróżnić. Konfiguracji dokonuje się w oknie **Configuration > ERPS**. Należy wprowadzić następujące parametry:
  ERPS ID – numer identyfikacyjny danej konfiguracji, dowolna liczba z zakresu 1 – 64, np. pierwszy niezajęty, czyli 1.
  Port East – konfiguracja pierwszego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 3.
  Port West – konfiguracja drugiego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 4.
  Port East SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego E, czyli portu fizycznego 3.
  Port West SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego, W czyli portu fizycznego 4.
  Port East APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego E, czyli portu fizycznego 3.
  Port West APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego, W czyli portu fizycznego 4.
  Zapisujemy konfigurację przez kliknięcie przycisku ***Save***.
  Następnie należy przejść do okna szczegółowej konfiguracji danego pierścienia, przez kliknięcie linku na numerze ID w ***kolumnie ERPS ID***. W kolejnym kroku należy wejść przez link ***VLAN Config*** do menu i wprowadzić numery VLAN, jakie mają być chronione przez ten proces protekcji. W tym przypadku będzie to tylko domyślny VLAN nr 1.
  Pozostałe parametry należy pozostawić domyślne. Na tym rysunku sygnalizowany jest alarm ***No APS Received***, informujący o braku odbierania ramek utrzymaniowych, R-APS, ponieważ pozostałe przełączniki nie zostały jeszcze skonfigurowane.

  Punkty: 1, 2 i 3 należy powtórzyć dla wszystkich przełączników tworzących pierścień łącznie z przełącznikami, które będą wyróżnione.

- **Konfiguracja przełącznika *RPL Neighbour***
  Należy określić, które połączenie ma być połączeniem RPL, czyli redundantnym, następnie przełącznik na jednym z jego końców skonfigurować, jako *RPL Neighbour*. Dokonując tego w oknie szczegółowej konfiguracji, w polu ***RPL Role*** wybierać funkcję ***RPL_Neighbour*** i w polu, ***RPL Port*** wybierać port logiczny, który jest dołączony do RPL.

- **Konfiguracja przełącznika *RPL Owner***
  Przełącznik na drugim końcu polaczenia RPL konfigurujemy, jako *RPL Owner*. W oknie szczegółowej konfiguracji w polu ***RPL Role*** wybieramy funkcję ***RPL_Owner*** i w polu ***RPL Port*** wybieramy port logiczny, który jest dołączony do RPL.

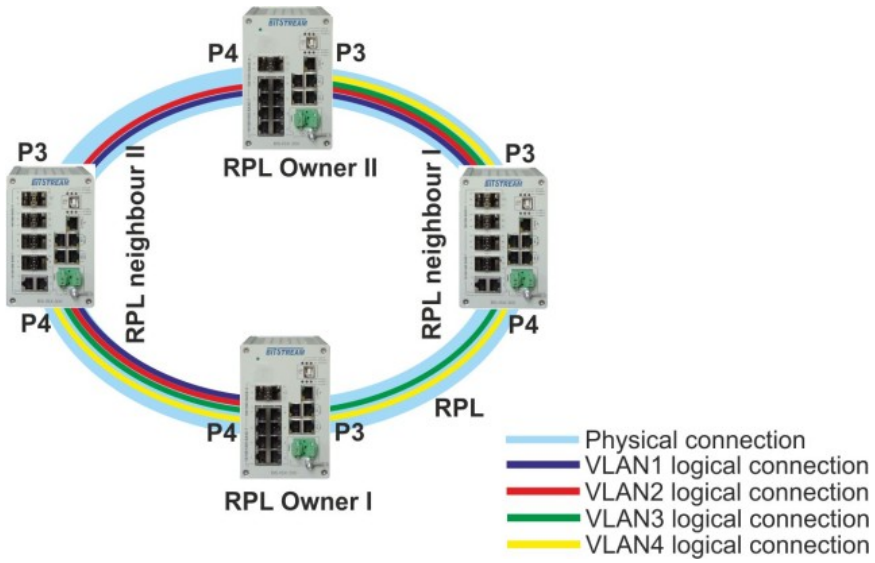
  Na tym etapie wszystkie przełączniki są skonfigurowane do pracy w pierścieniu i można włączyć połączenie, które na czas konfiguracji urządzeń musiało być przerwane, dalej przełączniki będą pracować już z redundancją drogi przesyłowej z czasem rekonfiguracji mniejszym niż 20ms.



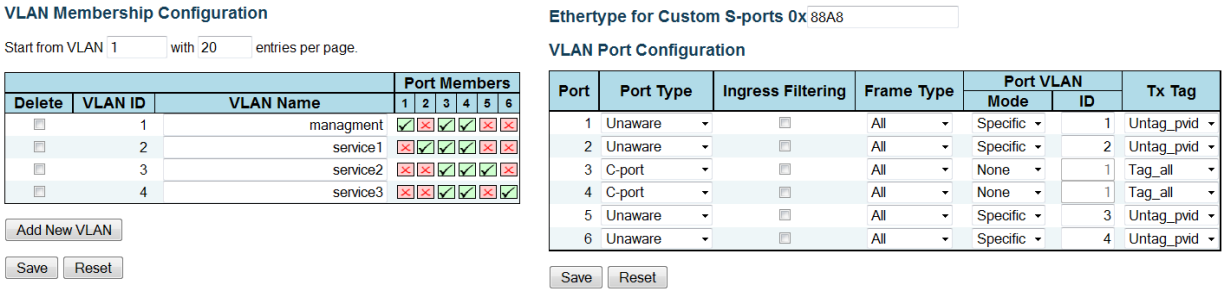
Rys. 37. Szczegółowa konfiguracja procesu protekcji dla sieci pracującej w topologii pierścienia

6.8.5.2 Przykład II

Wszystkie urządzenia posiadają następującą konfigurację VLAN: fizyczne porty 3 i 4 tworzące pierścień pracują w trybie trunk z ramkami tagowanymi i z takimi samymi numerami sieci VLAN: 1, 2, 3 i 4. Pozostałe porty przełączników pracują w trybie normalnym bez tagownia ramek. Do każdego portu przypisany jest jeden z czterech VLAN w następujący sposób: port 1: VLAN 1, port 2: VLAN 2, port 5: VLAN 3, port 6: VLAN 4. Szczegół konfiguracji VLAN przedstawia schemat poniżej:



Rys. 38. Schemat funkcjonalny przykład II



Rys. 39. Konfiguracja VLAN dla przykładu II konfiguracji protekcji w topologii pierścienia

Takie podzielenie ruchu przez sieci VLAN i na oddzielne pierścienie logiczne pozwala na równomierne rozłożenie obciążenia wszystkich połączeń w stanie pełnej sprawności pierścienia.
Istnieje możliwość ustanowienia więcej niż dwa procesy protekcji tak jak w tym przykładzie, maksymalnie można skonfigurować do 64 pierścieni w jednym urządzeniu.

Do prawidłowej pracy pierścienia w tym przykładzie należy skonfigurować po dwa punkty *MEP* dla każdego z portów tworzących pierścień i dwa procesy protekcji.

W tej konfiguracji będą po dwa przełączniki wyróżnione po jednym dla każdego procesu ERPS, dwa *RPL Owner* i dwa *RPL Neighbour*. Wszystkie urządzenia tworzące pierścień będą reagowały na zanik sygnału Fast Link Fail. We wszystkich przełącznikach logiczny port East dla protokołu protekcji będzie fizycznym portem numer 3, port West natomiast będzie portem fizycznym numer 4.
Proces ERPS o ID 1 będzie obsługiwał tylko VLAN numer: 1 i 3, a proces ERPS o ID 2 będzie obsługiwał VLAN numer: 2 i 4.

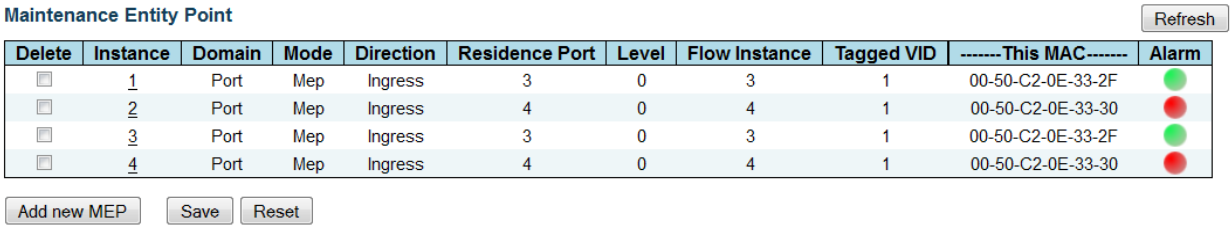
Podczas konfiguracji pierwszym elementem, jaki należy skonfigurować to punkty MEP odnoszące się do portów tworzących pierścień we wszystkich przełącznikach.

- **Konfiguracja punktów MEP dla logicznego portu East dla dwóch procesów ERPS**

Instance – dowolny numer *id* danego punktu *MEP*,
Parametry: ***Domain, Mode, Direction, Level*** – należy pozostawić domyślne.
Residence Port, ***Flow Instance*** – należy wpisać numer portu fizycznego czyli 3.
Tagged Vid – numer Vlan dla ramek *R-APS*, dla pierwszego procesu protekcji będzie to 1, a dla drugiego procesu będzie to 2.
Następnie należy wejść do szczegółowej konfiguracji tego punktu przez link w kolumnie ***Instance***.
Dokonujemy konfiguracji wysyłania ramek utrzymaniowych *R-APS*, w tabeli ***APS Protocol*** zaznaczyć ***Enable. Priority*** i ***Last Octet*** pozostają domyślne, *Cast* wybieramy: *Multi* i *Type*: ***R-APS***. Czynność tą powtórzyć dla dwóch punków *MEP* dla obu procesów ERPS.

- **Konfiguracja punktów MEP dla logicznego portu West dla dwóch procesów ERPS**

Instance – dowolny numer *id* danego punktu *MEP*,
Parametry: ***Domain***, ***Mode***, ***Direction***, ***Level*** – należy pozostawić domyślne.
Residence Port, ***Flow Instance*** – należy wpisać numer portu fizycznego czyli 4.
Tagged Vid – numer Vlan dla ramek *R-APS*, dla pierwszego procesu protekcji będzie to 1, a dla drugiego procesu będzie to 2.
Następnie wchodzimy do szczegółowej konfiguracji tego punktu przez link w kolumnie ***Instance***.
Dokonujemy konfiguracji wysyłania ramek utrzymaniowych *R-APS*, w tabeli ***APS Protocol*** należy zaznaczyć ***Enable. Priority*** i ***Last Octet*** pozostawić domyślne, ***Cast*** wybierać: ***Multi*** i ***Type***: ***R-APS***. Czynność tą powtórzyć dla dwóch punków *MEP* dla obu procesów ERPS.
Całą konfigurację punków MEP dla przykładu II przedstawia zrzut poniżej:



Rys. 40. Konfiguracja punktów MEP dla przykładu II

- **Konfiguracja protokołu protekcji proces ERPS 1**

ERPS ID – numer identyfikacyjny danej konfiguracji, dowolna liczba z zakresu 1 – 64, w tym przykładzie będzie to 1.
Port East – konfiguracja pierwszego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 3.
Port West – konfiguracja drugiego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 4.
Port East SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego E, czyli portu fizycznego 3, zgodnie z wcześniejszą konfiguracją będzie to 1.
Port West SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego, W czyli portu fizycznego 4, zgodnie z wcześniejszą konfiguracją będzie to 2.
Port East APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego E, czyli portu fizycznego 3, zgodnie z wcześniejszą konfiguracją będzie to 1.
Port West APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego, W czyli portu fizycznego 4, zgodnie z wcześniejszą konfiguracją będzie to 2.
Zapisujemy konfigurację przez kliknięcie przycisku ***Save***.
Następnie należy przejść do okna szczegółowej konfiguracji danego pierścienia, przez kliknięcie linku na numerze *ID* w kolumnie ***ERPS ID***. W kolejnym kroku należy wejść przez link ***VLAN Config*** do menu i wprowadzić numery VLAN, jakie mają być obsługiwane przez ten proces protekcji. W tym przypadku będzie to VLAN nr 1 i 3.
Punkty: 1, 2 i 3 należy powtórzyć dla wszystkich przełączników tworzących pierścień łącznie z przełącznikami, które będą wyróżnione.

- **Konfiguracja przełącznika RPL Neighbour dla procesu ERPS 1**

Określamy, które połączenie ma być połączeniem RPL, czyli redundantnym, następnie przełącznik na jednym z jego końców konfigurujemy, jako *RPL Neighbour*. Dokonuje tego w oknie szczegółowej konfiguracji w polu ***RPL Role*** wybieramy funkcję ***RPL_Neighbour*** i w polu, ***RPL Port*** wybieramy port logiczny, który jest dołączony do RPL.

- **Konfiguracja przełącznika RPL Owner dla procesu ERPS 1**

Przełącznik na drugim końcu połączenia RPL konfigurujemy, jako *RPL Owner*. W oknie szczegółowej konfiguracji w polu ***RPL Role*** wybieramy funkcję ***RPL_Owner*** i w polu ***RPL Port*** wybieramy numer portu logicznego, który jest dołączony do RPL.

W tym momencie nie można jeszcze przywrócić połączenia, które jest rozłączone na czas konfiguracji, ponieważ spowoduje to wystąpienie zapętlenia sieci, dla VLAN nr 2 i 4. Zapętlenie to może całkowicie zakłócić komunikację w ramach, VLAN nr 1 i 3, a tym samym doprowadzić do utraty komunikacji z systemem zarządzania w każdym z urządzeń.

- **Konfiguracja protokołu protekcji proces ERPS 2**

ERPS ID – numer identyfikacyjny danej konfiguracji, dowolna liczba z zakresu 1 – 64, w tym przykładzie będzie to 2.

Port East – konfiguracja pierwszego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 3.
Port West – konfiguracja drugiego portu logicznego, jaki tworzy pierścień w danym przełączniku, zgodnie z założeniami jest to port 4.
Port East SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego East, czyli portu fizycznego 3, zgodnie z wcześniejszą konfiguracją będzie to 3.
Port West SF MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za zgłaszanie wystąpienia zaniku sygnału dla portu logicznego, West czyli portu fizycznego 4, zgodnie z wcześniejszą konfiguracją będzie to 4.
Port East APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego East, czyli portu fizycznego 3, zgodnie z wcześniejszą konfiguracją będzie to 3.
Port West APS MEP – numer *id* punktu *MEP*, który jest odpowiedzialny za wysyłanie ramek utrzymaniowych *R-APS* dla portu logicznego, West czyli portu fizycznego 4, zgodnie z wcześniejszą konfiguracją będzie to 4.
Zapisujemy konfigurację przez kliknięcie przycisku ***Save***.

Następnie należy przejść do okna szczegółowej konfiguracji danego pierścienia, przez kliknięcie linku na numerze *ID* w kolumnie ***ERPS ID***. W kolejnym kroku należy wejść przez link ***VLAN Config*** do Menu i wprowadzić numery VLAN, jakie mają być obsługiwane przez ten proces protekcji. W tym przypadku będzie to VLAN nr 2 i 4.

- **Konfiguracja przełącznika RPL Neighbour dla procesu ERPS 2**

Należy określić, które połączenie ma być połączeniem RPL, czyli redundantnym, następnie przełącznik na jednym z jego końców skonfigurować, jako *RPL Neighbour*. Dokonując tego w oknie szczegółowej konfiguracji w polu ***RPL Role*** wybieramy funkcję ***RPL_Neighbour*** i w polu, ***RPL Port*** wybieramy numer port logiczny, który jest dołączony do RPL.

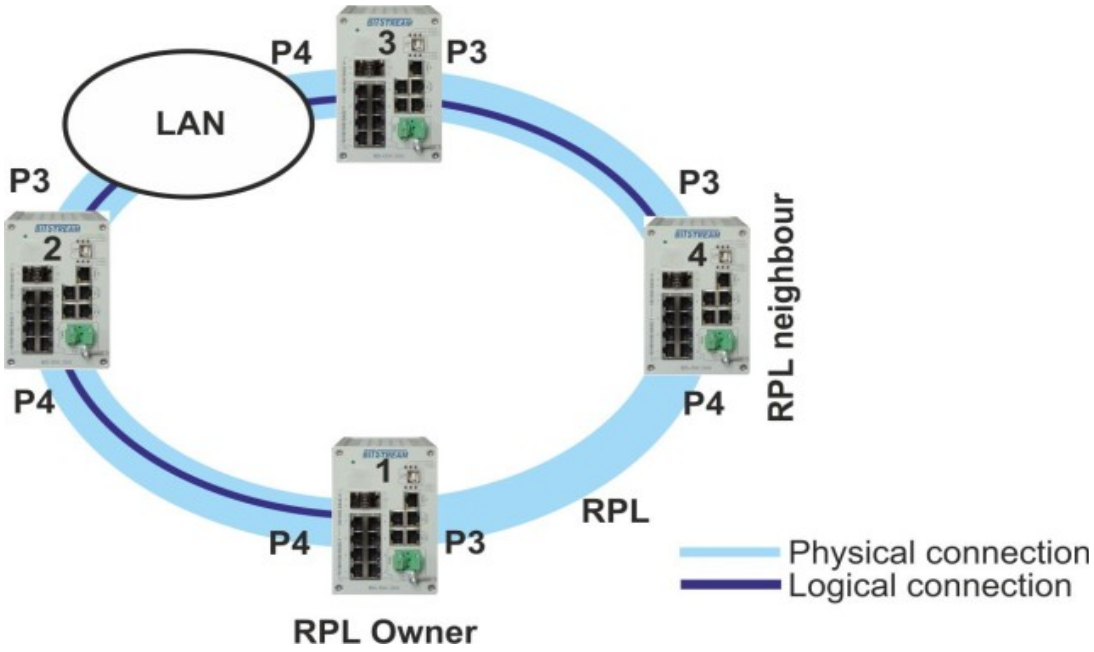
- **Konfiguracja przełącznika RPL Owner dla procesu ERPS 2**

Przełącznik na drugim końcu połączenia RPL skonfigurować, jako *RPL Owner*. W oknie szczegółowej konfiguracji w polu ***RPL Role*** wybieramy funkcję ***RPL_Owner*** i w polu ***RPL Port*** wybieramy numer portu logicznego, który jest dołączony do RPL.

Na tym etapie wszystkie przełączniki są skonfigurowane do pracy w pierścieniu i można włączyć połączenie, które na czas konfiguracji urządzeń musiało być przerwane, dalej przełączniki będą pracować już z redundancją drogi przesyłowej z czasem rekonfiguracji mniejszym niż 20ms.

6.8.5.3 Przykład III

Topologię sieci przedstawia rysunek poniżej. Sposób działania takiego układu jest następujący wszystkie przełączniki pracują tak samo jak w typowym układzie opisanym w p. 6.8.5.1. Przełączniki, których porty tworzące pierścień dołączone są do chmury posiadają możliwość wysyłania i analizowania ramek *CCM*. Ramki te są wysyłane z konfigurowalną częstotliwością od 105 ramek na sekundę do 6 ramek na godzinę. Po drugiej stronie chmury przełącznik analizuje te ramki pod kątem ich spójności i częstotliwości przychodzenia. Utrata trzech kolejnych ramek powoduje wysłanie informacji alarmowej przez punkt MEP do procesu protekcji, który reaguję na ten przekaz w sposób identyczny jak przy zaniku sygnału na porcie. Dalsze działanie protekcji jest identyczne jak w p. 6.8.2.

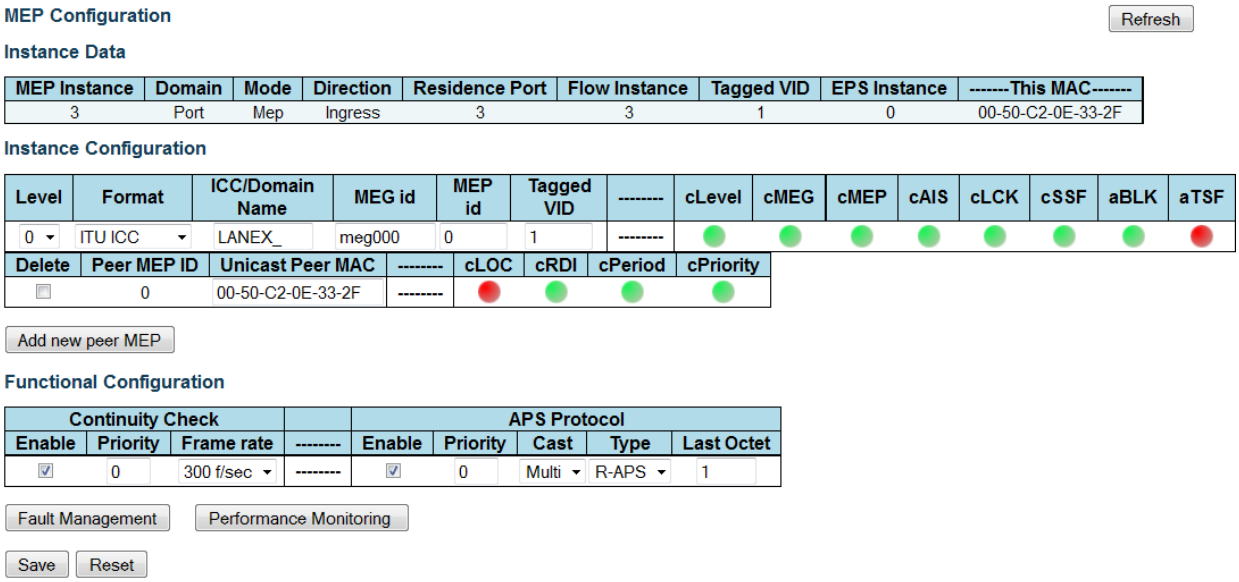


Rys. 41. Schemat funkcjonalny przykład III

Sposób konfiguracji wszystkich parametrów jest taki sam jak w przykładzie I. Różnica w konfiguracji polega na włączeniu nadawania i analizowania ramek *CCM* przez punkty, MEP portów, które są w tym przykładzie dołączone do chmury.

Uruchomienie ramek *CCM* jest możliwe w konfiguracji szczegółowej punktu *MEP*, aby przełącznik rozpoczął wysyłanie i analizowanie ramek *CCM*, należy kliknąć na przycisk ***Add New peer MEP*** i w polu ***Unicast Peer MAC*** podać unicastowy adres *MAC* dla ramek *CCM*, może to być adres MAC urządzenia **HYPERION-105**, który dostępny jest w polu: ***MAC Address*** pod linkiem **Monitor > System > Information**.
Następnie w polu ***Continuity Check Enable*** należy zaznaczyć pole checkbox, wybierać priorytet dla ramek *CCM* i w polu ***Frame rate*** określić częstotliwość wysyłania ramek *CCM*.
Tak skonfigurowany pierścień charakteryzuje się czasem rekonfiguracji poniżej 20ms dla połączeń wykonanych bezpośrednio pomiędzy urządzeniami **HYPERION-105**, natomiast czas rekonfiguracji w momencie wystąpienia przerwy lub przeciążenia w chmurze jest zależny od częstotliwości wysyłania ramek *CCM*. Dla częstotliwości 105 ramek na sekundę ten czas wynosi 50ms.

Dalsza konfiguracja procesu protekcji odbywa się w sposób identyczny jak to zostało opisane w przykładzie I.



Rys. 42. Szczegółowa konfiguracja punktu MEP z włączoną obsługa ramek CCM

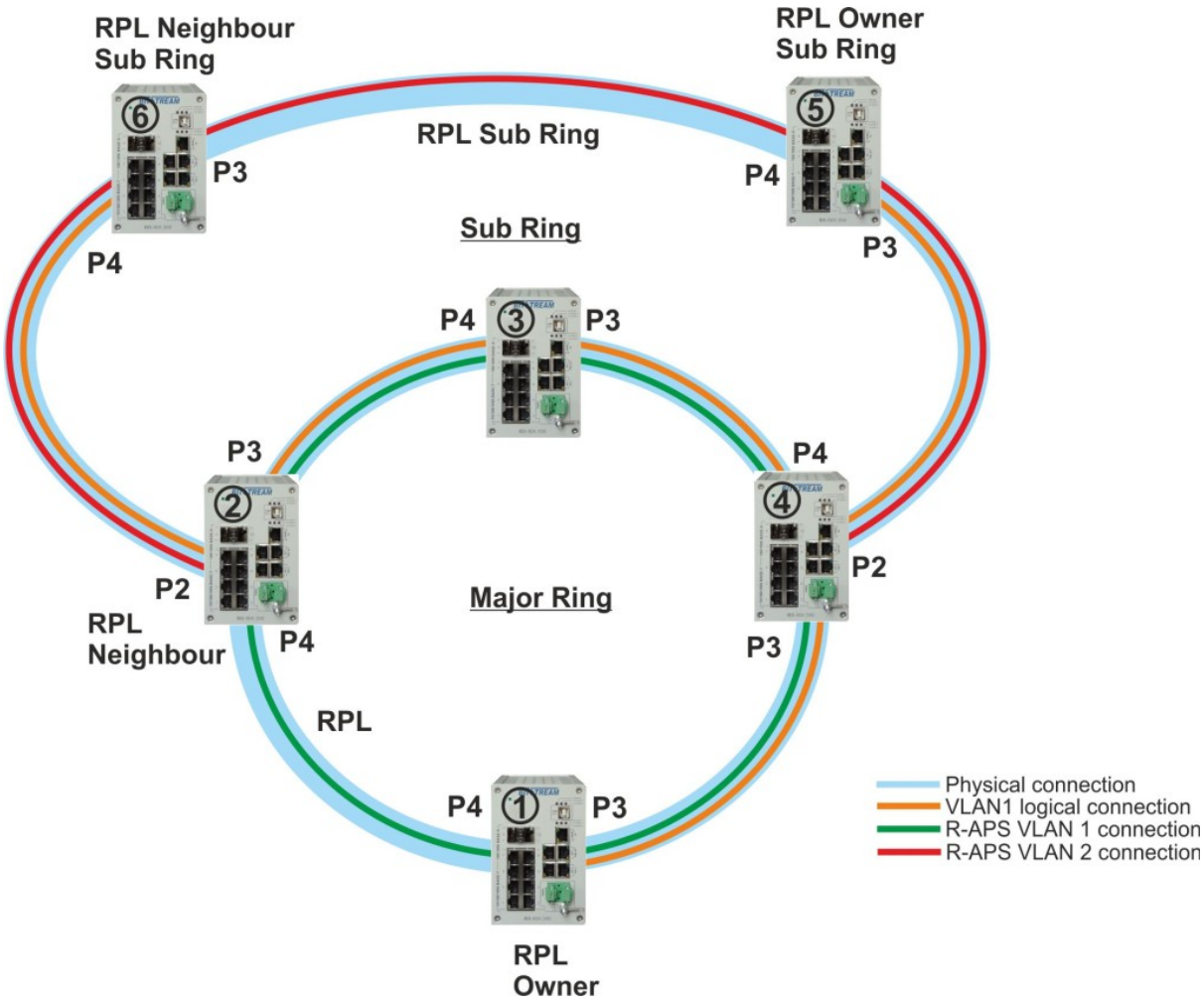
6.8.6 Sposób działania protekcji drogi transmisyjnej w topologii multiring

Sposób działania takiego układu jest następujący, pierścień główny złożony z przełączników I, II, III i IV pracuje w sposób identyczny jak w p. 6.8.2. Pierścień *Sub* złożony z przełączników II, III, IV, V i VI tworzy drugi pierścień z własnym polaczeniem RPL, sposób jego działania jest analogiczny jak w pierścieniu głównym *Major*. Połączenie pomiędzy przełącznikami II, III i IV jest połączeniem wspólnym dla obu pierścieni. Stan tego połączenia jest monitorowany tylko przez pierścień główny. Przekazywania ramek utrzymaniowych *R-APS* w pierścieniu główny odbywa się identycznie jak przykładzie I. Natomiast sposób przekazywania ramek *R-APS* w pierścieniu *Sub* jest zrealizowany podobnie, ale wymaga oddzielnego kanału do ich przenoszenia, ponieważ ramki *R-APS* z pierścienia *Sub* mogłyby zakłócić pracę pierścienia *Major*. Sam protokół protekcji zapewnia możliwość wydzielenia takiego kanału przez wybranie opcji *Virtual Channel*. Taki kanał może być również zrealizowane przez odpowiednie skonfigurowanie sieci VLAN.

6.8.6.1 Przykład IV konfiguracja multiring bez wirtualnego kanału

W konfiguracji tej ruch użytkownika, oraz zarządzanie urządzeniami **HYPERION-105** odbywa się w ramach VLAN nr 1. Zasięg tego VLAN w stanie pełnej sprawności pierścienia przedstawia rysunek poniżej na którym jest to zaznaczony linią żółtą „Połączenie logiczne VLAN 1”. Linie przerywane przedstawiają sposób przekazywania ramek *R-APS.* Linia zielona dla pierścienia głównego *Major*, ruch ten odbywa się w ramach VLAN 1, a linia czerwona dla pierścienia *Sub*, ruch ramek *R-APS* w tym wypadku odbywa się w ramach VLAN 2. Zachowanie transmisji rozdzielonej na dwie sieci VLAN w pierścieniu *Sub*, jest możliwe tylko, gdy porty tworzące pierścień *Sub* pracują z ruchem tagowanym.

Bardzo ważne jest, aby VLAN w ramach, którego przekazywane są ramki *R-APS* pierścienia, Sub, miał zasięg tylko do urządzeń tworzących pierścień *Sub*. Dodawania kolejnych VLAN w tej topologii jest możliwe łącznie ze stworzeniem układu sieci, VLAN podobnie jak w przykładzie II.

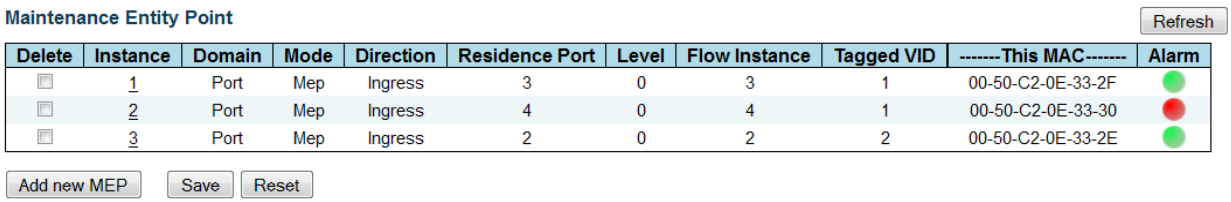


Rys. 43. Schemat funkcjonalny dla przykładu IV (trzeba zrobić o mniejszej średnicy połączenia)

Konfiguracja pierścienia *Major* odbywa się w sposób identyczny jak w przykładzie I. Konfigurację pierścienia *Sub* należy rozpocząć od ustawiania VLAN w przełącznikach: II, III, IV, V i VI. Każdy port tworzący pierścień *Sub* musi pracować z ruchem targowanym i przekazywać ramki VLAN 1 (ruch i zarządzanie) i VLAN 2 (*R-APS* dla *sub* ring).

- **Konfiguracja punktów MEP**

Wszystkie porty tworzące pierścień *Sub* muszą mieć skonfigurowane punkty *MEP* łącznie z włączoną opcja wysyłania ramek *R-APS*. Konfiguracja tych punków jest taka sama jak dla pierścienia *Major* poza polem ***Tagged VID***, gdzie należy podać numer VLAN dla *R-APS* w pierścieniu *Sub* w tym przypadku to będzie 2.



Rys. 44. Konfiguracja punktów MEP dla przykładu IV

- **Konfiguracja protokołu protekcji przełączniki tworzące odczep od pierścienia Major**

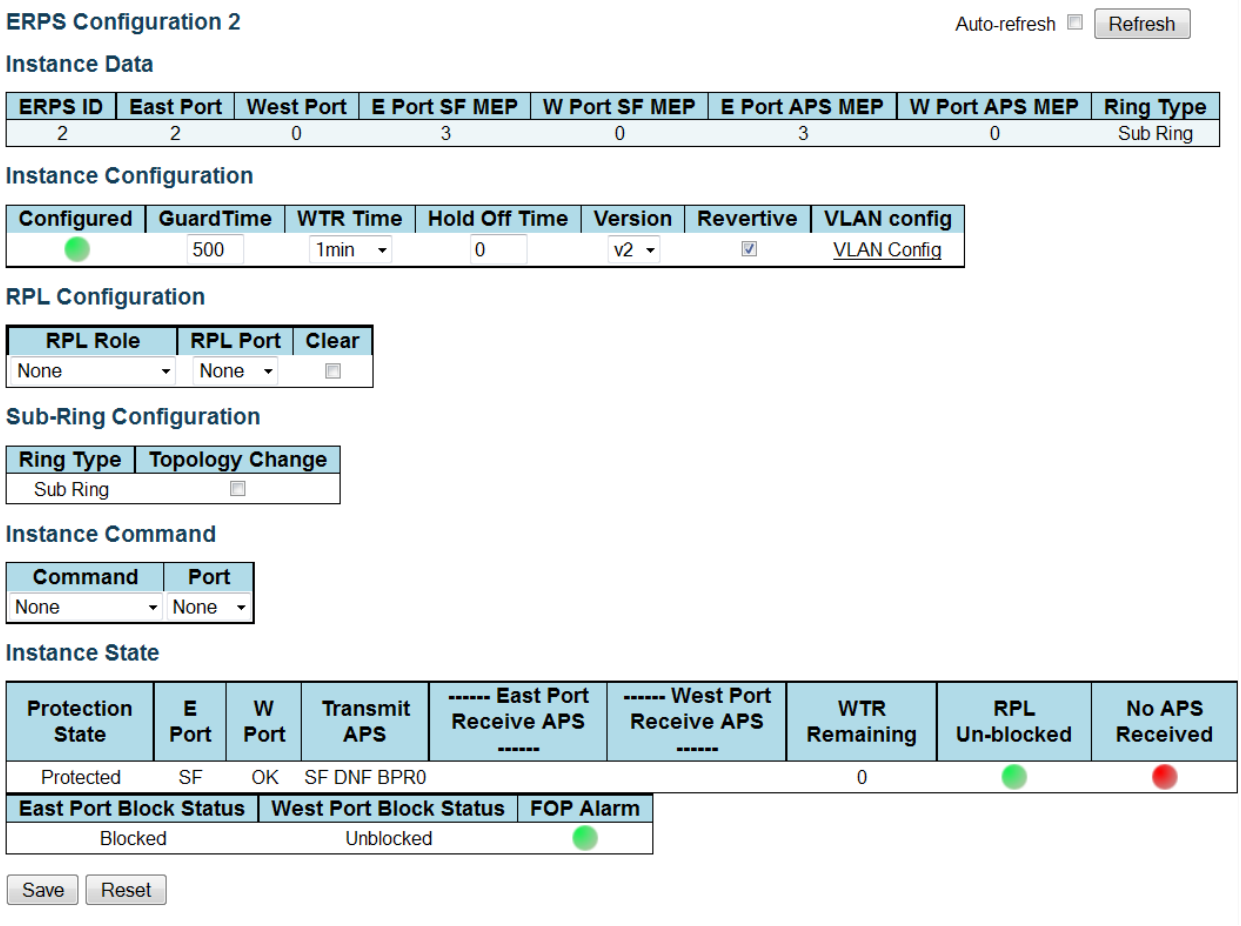
  W urządzeniach tych należy dodać nowy proces obsługujący protekcję, numer ***Id*** dowolny np. 2.
  Port East – numer portu będący odgałęzieniem od pierścienia *Major*.
  Port West – 0.
  Port E SF MEP – numer id punktu *MEP* dla portu podanego w kolumnie port *E* odpowiedzialnego za zgłoszenie informacji o awarii połączenia,
  Port W SF MEP – 0.
  Port E APS MEP – numer id punktu *MEP* dla portu podanego w kolumnie port *E* odpowiedzialnego za wysyłanie ramek *R-APS*,
  Port W APS MEP – 0.
  Ring Type – Sub.
  Interconnected Node – Yes zaznaczony Checkbox.
  Virtual Channel – No nie zaznaczony Checkbox.
  Major Ring ID – numer *ID* procesu zapewniającego protekcję w pierścieniu *Major*.

  Następnie w konfiguracji szczegółowej dla tego procesu należy w menu ***VLAN Config*** dodać numery sieci VLAN obsługiwanych przez *sub* ring, czyli w tym przypadku będzie to 1 i 2.

- **Konfiguracja protokołu protekcji pozostałe przełączniki tworzące Sub ring**

  W urządzeniach tych należy dodać nowy proces obsługujący protekcję,
  numer ***Id*** dowolny np. 2,
  Port East – numer pierwszego portu tworzącego pierścień Sub,
  Port West – numer drugiego portu tworzącego pierścień Sub,
  Port East SF MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za zgłoszenie informacji o awarii połączenia,
  Port West SF MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port W*est* odpowiedzialnego za zgłoszenie informacji o awarii połączenia,
  Port East APS MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za wysyłanie ramek *R-APS*,
  Port West APS MEP – numer id punktu *MEP* dla portu podanego w kolumnie port W*est* odpowiedzialnego za wysyłanie ramek *R-APS*,
  Ring Type – Sub.
  Interconnected Node: – ***No*** nie zaznaczony Checkbox.
  Virtual Channel: – ***No*** nie zaznaczony Checkbox.
  Major Ring ID: – domyślnie.

Następnie w konfiguracji szczegółowej dla tego procesu należy w menu ***VLAN Config*** dodać numery sieci VLAN obsługiwanych przez *sub* ring, czyli w tym przypadku będzie to 1 i 2.



Rys. 45. Szczegółowa konfiguracja dla pierścienia Sub w przełączniku, który jest częścią pierścienia Major

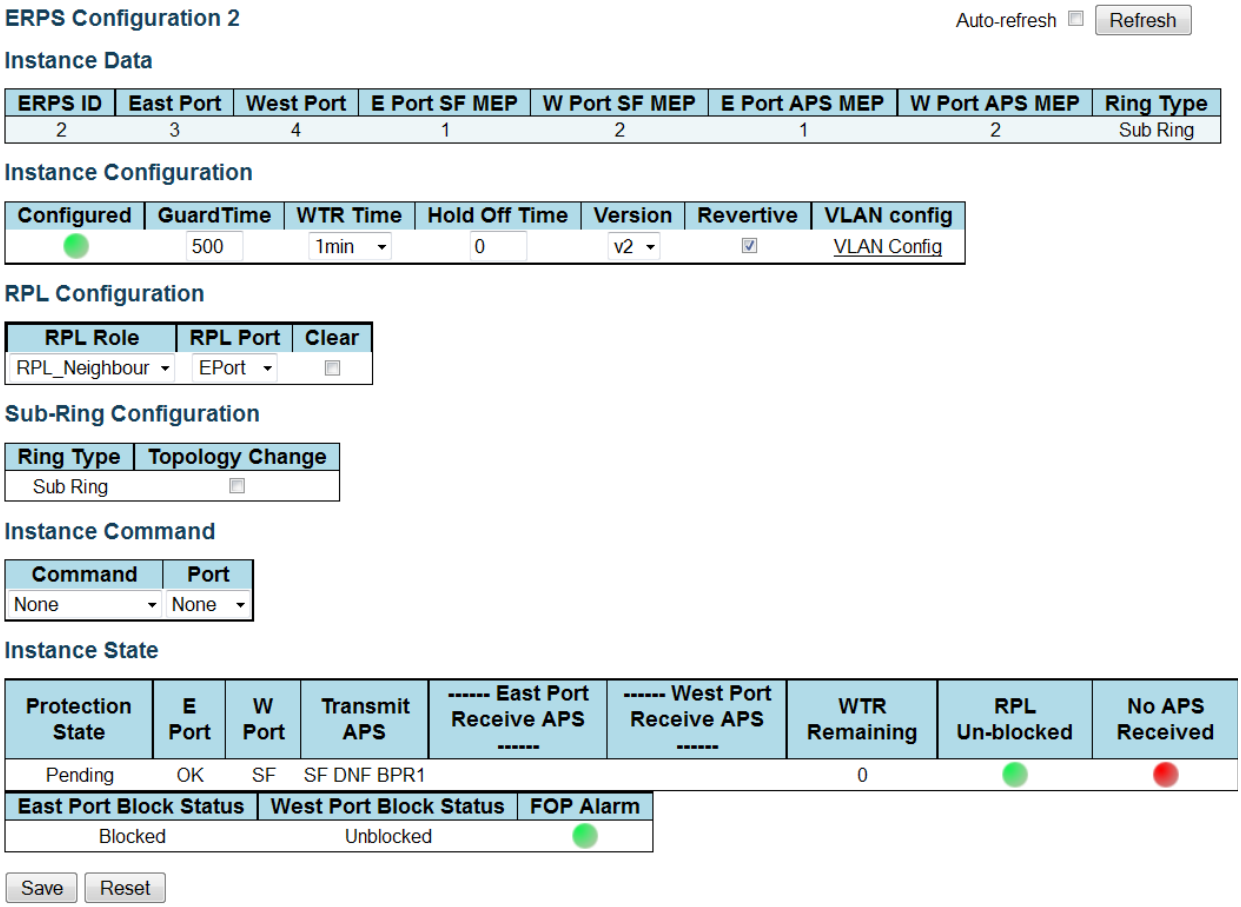
- **Konfiguracja przełącznika RPL Neighbour dla pierścienia Sub**

  Określić, które połączenie ma być połączeniem RPL, czyli redundantnym, następnie przełącznik na jednym z jego końców skonfigurować, jako *RPL Neighbour*. Dokonując tego w oknie szczegółowej konfiguracji w polu ***RPL Role*** wybrać funkcję ***RPL_Neighbour*** i w polu, ***RPL Port*** wybierać port logiczny, który jest dołączony do RPL.

- **Konfiguracja przełącznika RPL Owner dla pierścienia Sub**

  Przełącznik na drugim końcu polaczenia RPL skonfigurować, jako *RPL Owner*. W oknie szczegółowej konfiguracji w polu ***RPL Role*** wybierać funkcję ***RPL_Owner*** i w polu ***RPL Port*** wybierać numer port logiczny, który jest dołączony do RPL.

  Na tym etapie wszystkie przełączniki są skonfigurowane do pracy w pierścieniu i można włączyć połączenia, które na czas konfiguracji urządzeń musiało być przerwane, dalej przełączniki będą pracować już z redundancją drogi przesyłowej z czasem rekonfiguracji mniejszym niż 20 ms dla obu pierścieni.



Rys. 46. Szczegółowa konfiguracja dla pierścienia Sub

6.8.6.2 Przykład V multiring z wirtualnym kanałem R-APS

W konfiguracji tej ruch użytkownika, oraz zarządzanie urządzeniami **HYPERION-105** odbywa się w ramach VLAN nr 1. Zasięg tego VLAN w stanie pełnej sprawności pierścienia przedstawia schemat poniżej, na którym jest to zaznaczone linią fioletową „Połączenie logiczne VLAN 1”. Linie przerywane przedstawiają sposób przekazywania ramek R-APS pierścienia Sub w wirtualnym kanale,
Konfiguracja pierścienia Major odbywa się w sposób identyczny jak w przykładzie I.

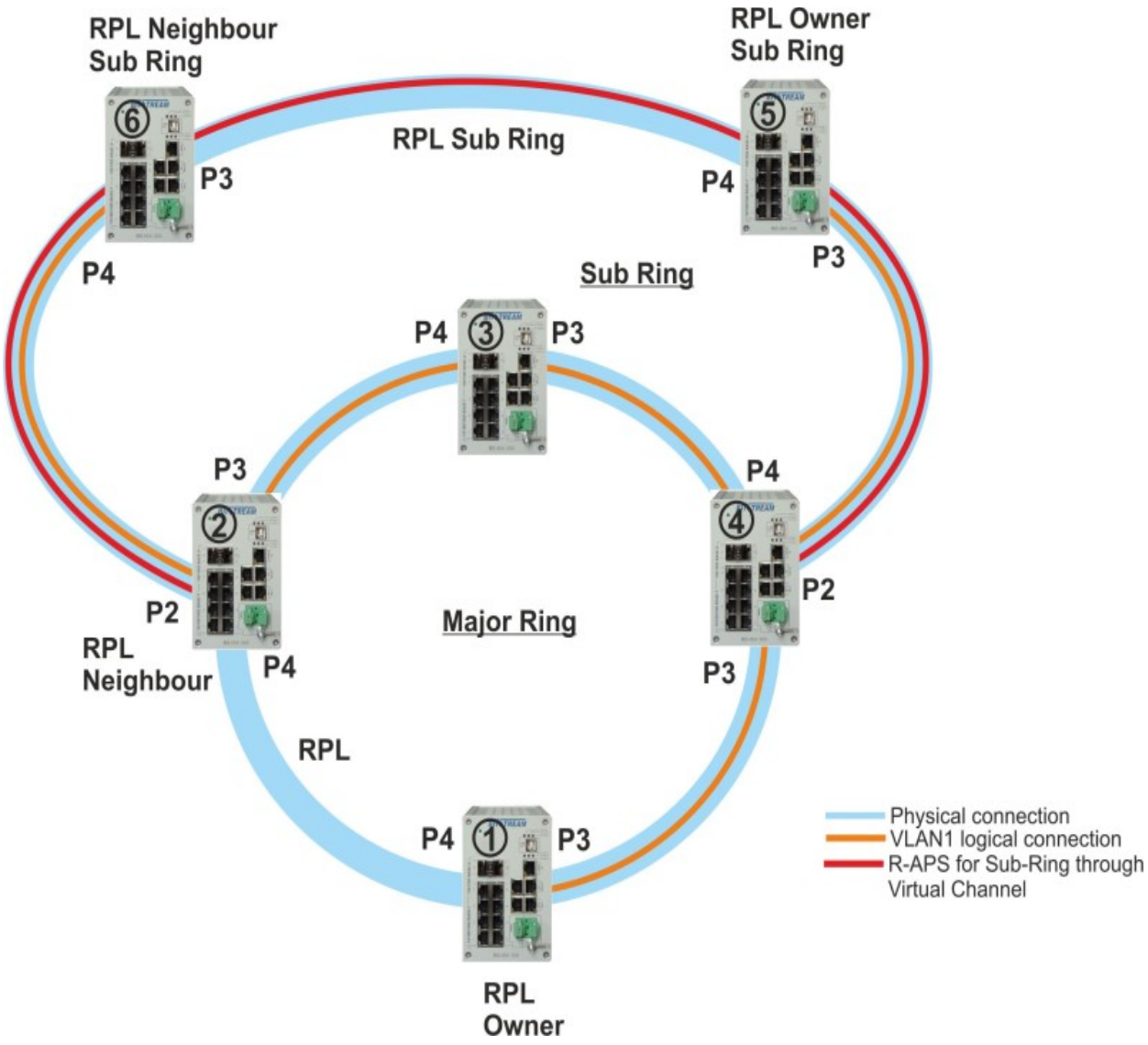
1) Konfiguracja punktów MEP

Wszystkie porty tworzące pierścień *Sub* muszą mieć skonfigurowane punkty *MEP* łącznie z włączoną opcja wysyłania ramek *R-APS*. Konfiguracja tych punków jest taka sama jak dla pierścienia Major pole ***Tagged VID***, gdzie należy podać numer VLAN dla *R-APS* w pierścieniu *Sub* w tym przypadku jest również taki sam jak w pierścieniu *Major*.

2) Konfiguracja protokołu protekcji przełączników tworzących odczep od pierścienia Major

W urządzeniach tych należy dodać nowy proces obsługujący protekcję,
numer ***Id*** dowolny np. 2,
Port East – numer portu będący odgałęzieniem od pierścienia *Major*,
Port West – 0,

Port East SF MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za zgłoszenie informacji o awarii połączenia,
Port West SF MEP – 0
Port East APS MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za wysyłanie ramek *R-APS*,
Port West APS MEP – 0
Ring Type – Sub.
Interconnected Node – Yes zaznaczony Checkbox.
Virtual Channel – Yes zaznaczony Checkbox.
Major Ring ID – numer ***ID*** procesu zapewniającego protekcję w pierścieniu *Major*.

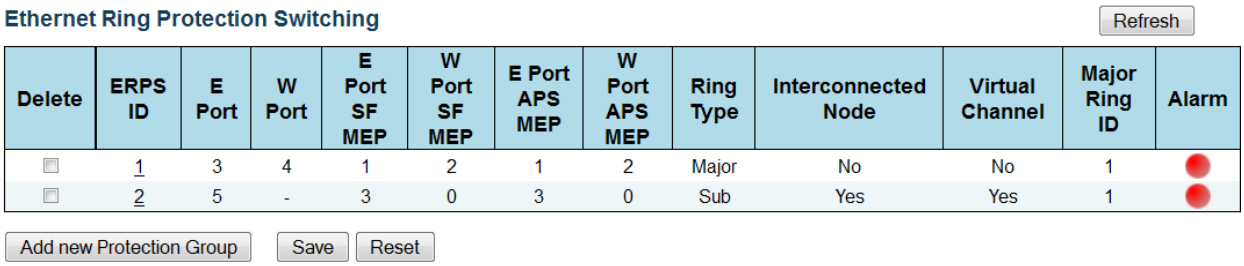


Rys. 47. Schemat funkcjonalny dla przykładu V

Następnie w konfiguracji szczegółowej dla tego procesu należy w menu ***VLAN Config*** dodać numery sieci VLAN obsługiwanych przez *Sub* ring, czyli w tym przypadku będzie to tylko VLAN nr 1.

3) Konfiguracja protokołu protekcji pozostałe przełączniki tworzące Sub ring

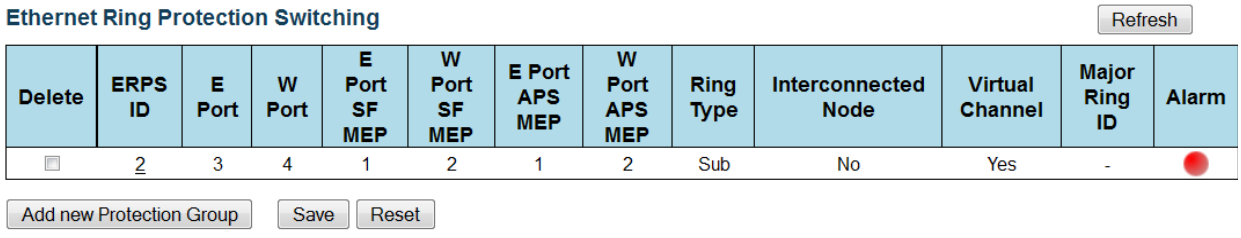
W urządzeniach tych należy dodać nowy proces obsługujący protekcję,
numer ***Id*** dowolny np. 2,
Port East – numer pierwszego portu tworzącego pierścień *Sub*,
Port West – numer drugiego portu tworzącego pierścień *Sub*,
Port East SF MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za zgłoszenie informacji o awarii połączenia,
Port West SF MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port West odpowiedzialnego za zgłoszenie informacji o awarii połączenia,



Rys. 48. Konfiguracja procesów protekcji dla przykładu V przełączniki tworzące odczep od pierścienia głównego

Port East APS MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port East odpowiedzialnego za wysyłanie ramek *R-APS*,
Port West APS MEP – numer *id* punktu *MEP* dla portu podanego w kolumnie port West odpowiedzialnego za wysyłanie ramek *R-APS*,
Ring Type – Sub.
Interconnected Node – No nie zaznaczony Checkbox.
Virtual Channel – Yes zaznaczony Checkbox.
Major Ring ID – domyślnie.

Następnie w konfiguracji szczegółowej dla tego procesu należy w menu ***VLAN Config*** dodać numery sieci VLAN obsługiwanych przez *sub* ring, czyli w tym przypadku będzie to tylko VLAN nr 1.



Rys. 49. Konfiguracja procesów protekcji dla przykładu V przełączniki tworzące Sub nietworzące odczepu

4) Konfiguracja przełącznika RPL Neighbour dla pierścienia Sub

Określić, które połączenie ma być połączeniem RPL, czyli redundantnym, następnie przełącznik na jednym z jego końców skonfigurować jako *RPL Neighbour*. Dokonując

tego w oknie szczegółowej konfiguracji w polu ***RPL Role*** wybrać funkcję ***RPL_Neighbour*** i w polu, ***RPL Port*** wybrać port logiczny, który jest dołączony do RPL.

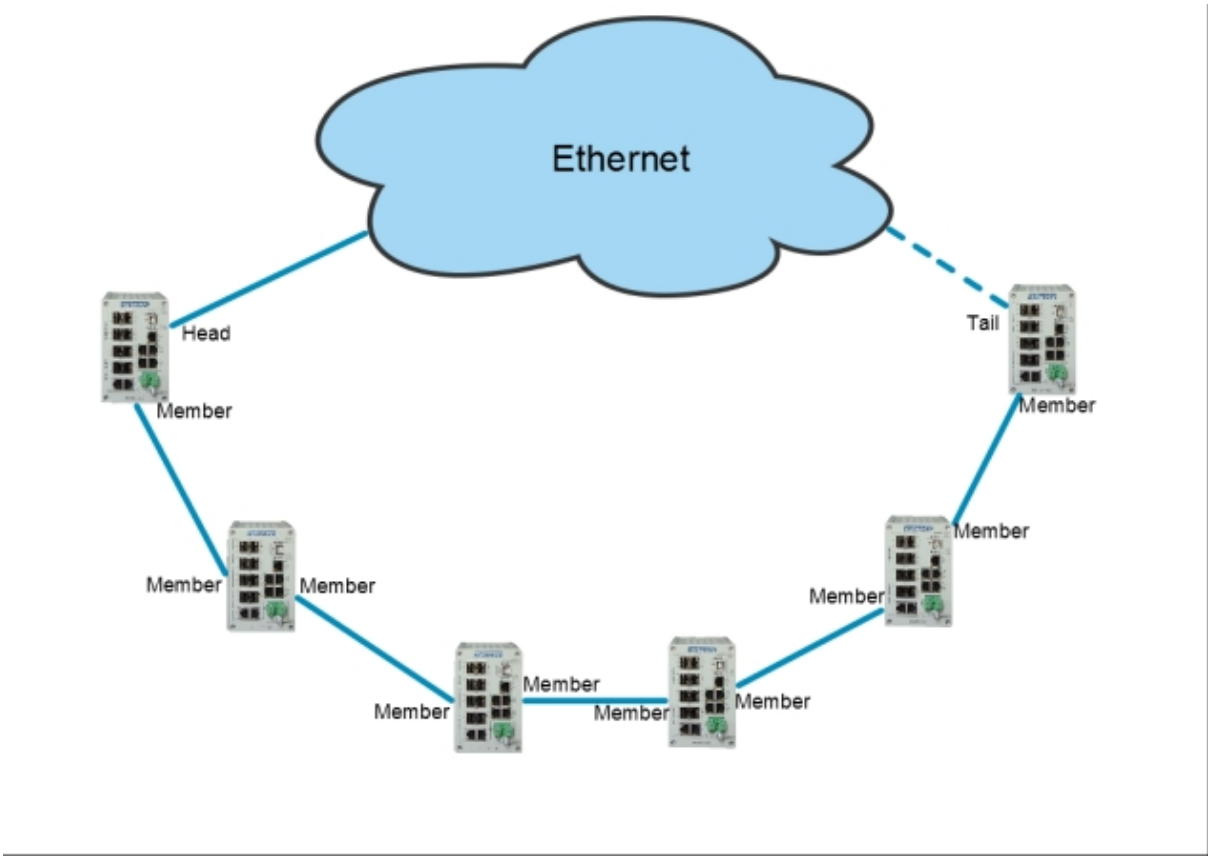
5) Konfiguracja przełącznika RPL Owner dla pierścienia Sub

Przełącznik na drugim końcu polaczenia RPL skonfigurować, jako *RPL Owner*. W oknie szczegółowej konfiguracji w polu ***RPL Role*** wybrać funkcję ***RPL_Owner*** i w polu ***RPL Port*** wybrać port logiczny, który jest dołączony do RPL.

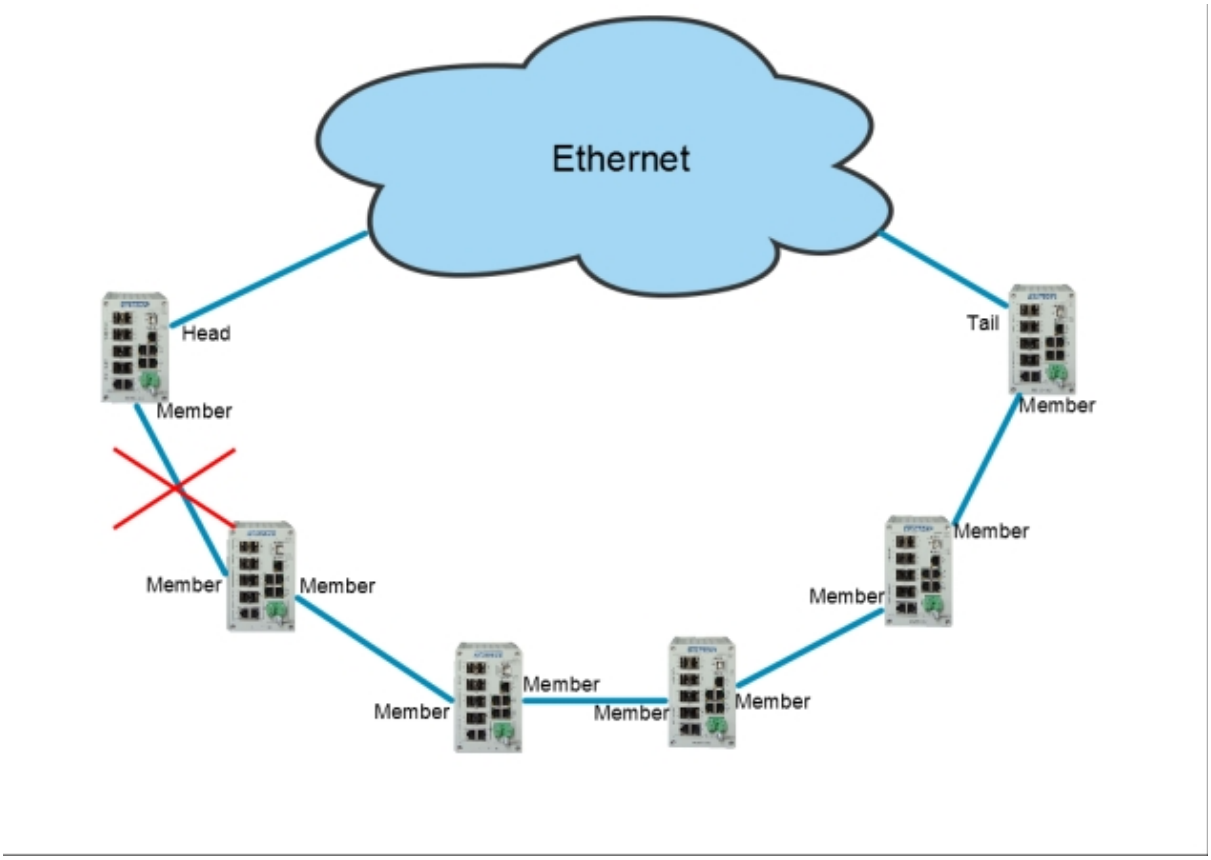
Na tym etapie wszystkie przełączniki są skonfigurowane do pracy w pierścieniu i można włączyć połączenie, które na czas konfiguracji urządzeń musiało być przerwane, dalej przełączniki będą pracować już z redundancją drogi przesyłowej z czasem rekonfiguracji mniejszym niż 20ms dla obu pierścieni.

6.8.7 Konfiguracja protekcji drogi transmisyjnej w trybie "CHAIN"

Praca w trybie "CHAIN" umożliwia skonfigurowanie protekcyjnego łańcucha urządzeń dołączanego 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. 50. Praca w trybie CHAIN przy aktywnym połączeniu od strony portu HEAD.



Rys. 51. 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 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.

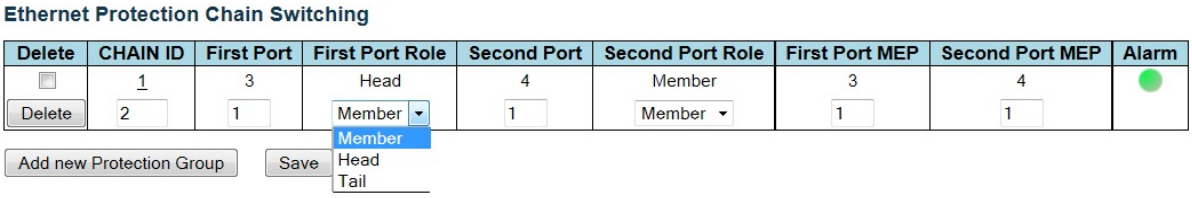
Przed rozpoczęciem konfiguracji należy wyłączyć na portach tworzących łańcuch pozostałe protokoły protekcji np. protokoły z grupy Spanning Tree.

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 mozna 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



Rys. 52. Dodawanie łańcucha

UWAGA! Porty HEAD i TAIL muszą był połączone z siecią Ethernet.

6.9 Konfiguracja sieci VLAN

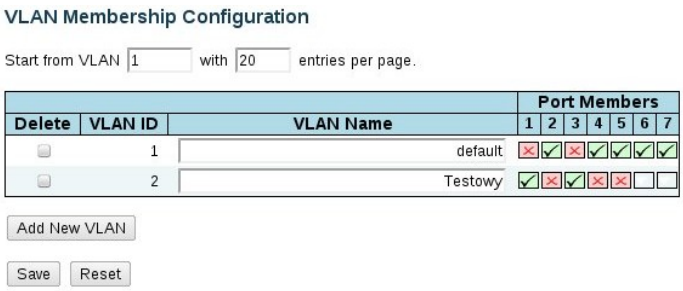
Konfiguracja sieci VLAN w **HYPERION-105** odbywa się dwuetapowo, w pierwszym etapie należy przyporządkować porty urządzenia **HYPERION-105** do wybranego numeru VLAN. Konfiguracja pierwszego etapu jest dostępna na stronie do której prowadzi link **Configuration > VLANs > VLAN Memebership**. Dodajemy 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-105** 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**

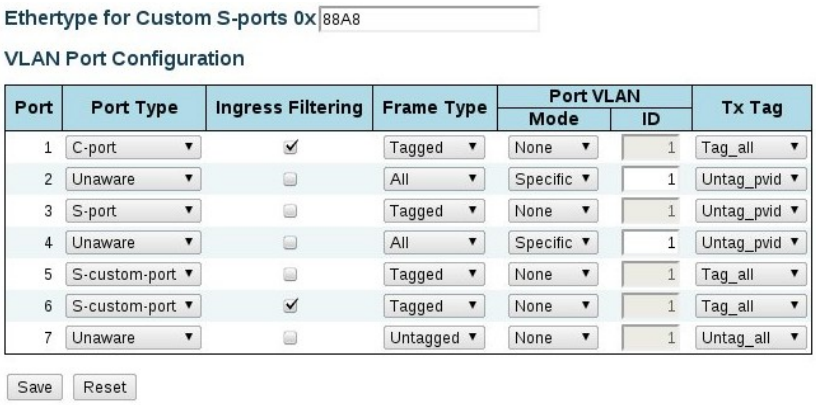


Rys. 53. Konfiguracja sieci VLAN

Znaczenie pól w tym menu jest następujące:

Ethertype for Custom S-ports – określa własny typu 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 S-port 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.
Untagget – 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.

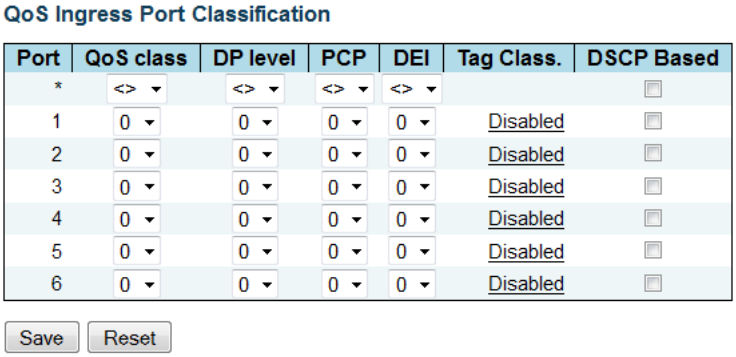


Rys. 54. Konfiguracja sieci VLAN i trybu pracy portów

6.10 QUALITY OF SERVICE

6.10.1 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 przez link **Configuration > QoS > Port Classification**.



Rys. 55. Menu Ingress Port Classification

Znaczenie poszczególnych pól jest następujące:

Port – numer fizycznego portu dla którego odnosi się dane ustawienie, pierwszy wiersz oznaczony przez gwiazdkę '*' pozwala na konfigurację danego parametru globalnie dla wszystkich portów.

QoS class – ustawienie dotyczy tylko ramek przychodzących nie posiadających tagów zgodnie z IEEE802.1q i przypisuje ramki do jednej z ośmiu *QoS class*. Występuje zależność jeden do jednego pomiędzy *QoS class*, a kolejkowaniem i uwzględnianiem priorytetów przy dalszym przetwarzaniu ramek. To znaczy że ramka po przydzieleniu do klasy zostaje

przeniesiona do jednej z ośmiu wejściowych kolejek sprzętowych. *QoS class* równy 0 ma najniższy priorytet, 7 ma najwyższy priorytet.

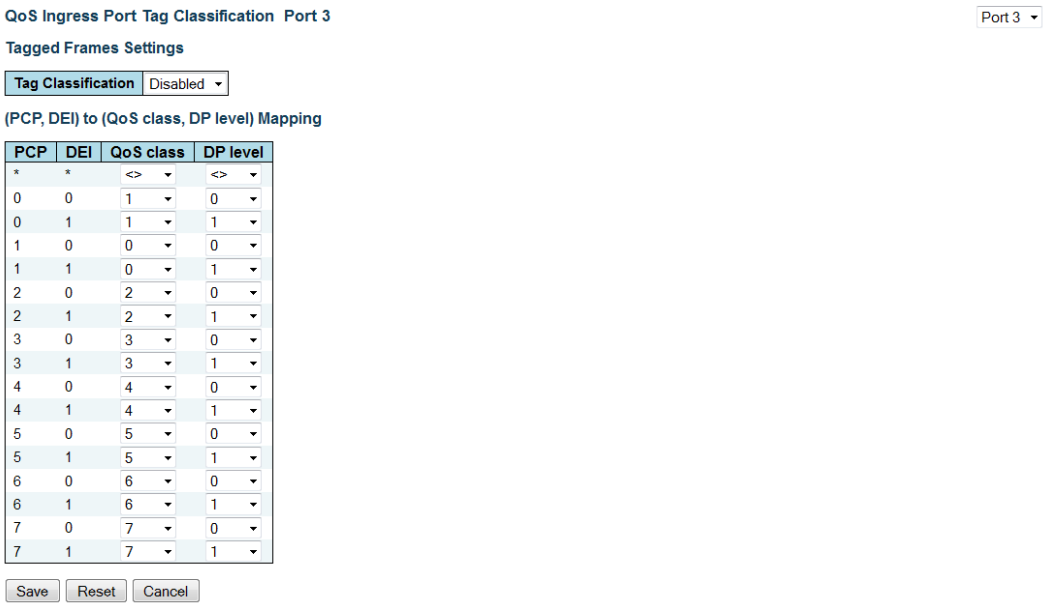
DP level – ustawienie dotyczy tylko ramek przychodzących nie posiadających tagów zgodnie z IEEE802.1q i przypisuje do ramek znacznik *Drop Precedence Level*. Poziom ten używany jest w całym przełączniku w celu kontroli zatorów.

PCP – ustawienie dotyczy tylko ramek przychodzących nie posiadających tagów zgodnie z IEEE802.1q i przypisuje do ramki znacznik *PCP* (*Priority Code Point*) jest to trzy bitowe pole przechowujące priorytet ramki zgodnie z IEEE802.1q.

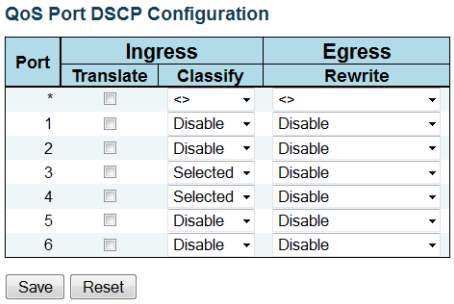
DEI - ustawienie dotyczy tylko ramek przychodzących nie posiadających tagów zgodnie z IEEE802.1q i przypisuje do ramki znacznik *DEI* (*Drop Eligible Indicator*) jest to jedno bitowe pole w tagach VLAN ramek.

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 przez link 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.

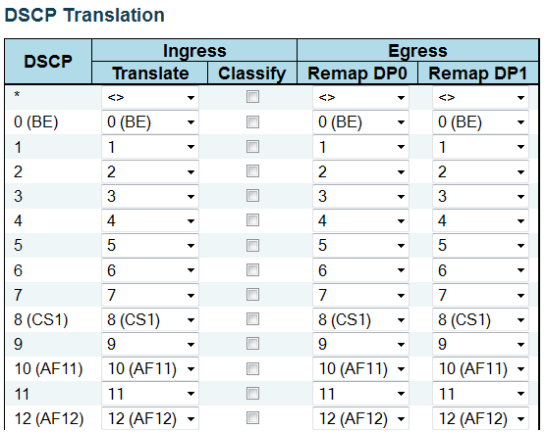
DSCP Based – opcja ta dotyczy wszystkich ramek, mapuje pole DSCP ramek warstwy trzeciej do jednej z *QoS class* i nadaje *DP level*. Konfiguracja tej opcji odbywa się w menu dostępnym pod linkiem **Configuration > QoS > Port DSCP**. Przełącznik przed przystąpieniem do klasyfikacji ramek do *QoS class* 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 przez link **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.



Rys. 56. Ingress Port Classification klasyfikacja ramek tagowanych



Rys. 57. Konfiguracja klasyfikacji ramek wejściowych warstwy trzeciej i wartości znacznika DSCP w ramkach wyjściowych



Rys. 58. Konfiguracja translacji znaczników DSCP

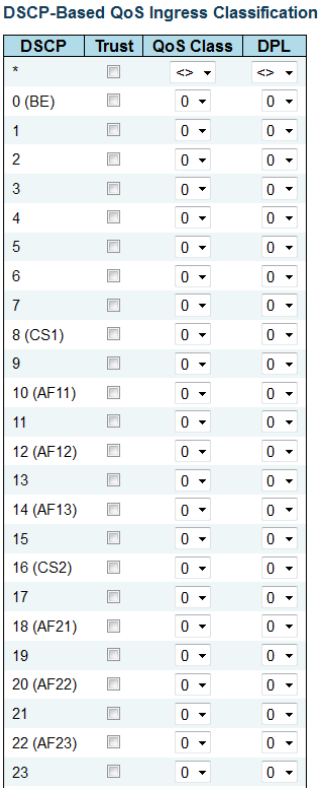
Konfiguracja sposobu klasyfikacji na podstawie *DSCP* odbywa się w menu ***QoS Port DSCP Configuration*** w kolumnie ***Classify***. Dostępne są cztery opcje:

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***.

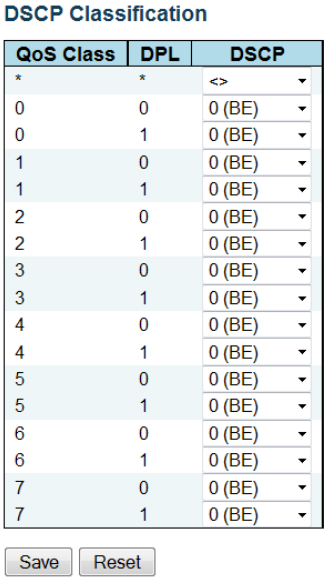
Selected – do klasyfikacji brane są tylko ramki z wartością DSCP dla której zaznaczona i zatwierdzona jest opcja ***Classify*** w menu ***DSCP Translation***.

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***.



Rys. 59. Konfiguracja klasyfikacji na podstawie znacznika DSCP ramek warstwy trzeciej

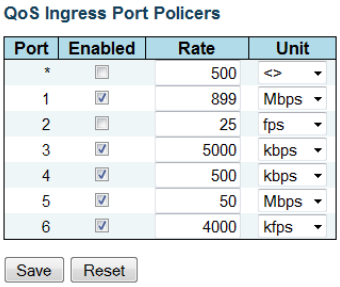
Menu ***QoS Port DSCP Configuration*** pozwala również na modyfikację pola *DSCP* w ramkach wychodzących z przełącznika. Służy do tego konfiguracja w kolumnie ***Egress Rewrite***. W menu tym dostępne są cztery opcje:
Disable – znaczniki *DSCP* nie są zmieniane.
Enable – znacznik *DSCP* jest nadawany 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 DP01*** w menu ***DSCP Translation***.



Rys. 60. Konfiguracja znacznika DSCP w ramkach wychodzących

6.10.2 Policer portu wejściowego Ingress Port Policers

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.

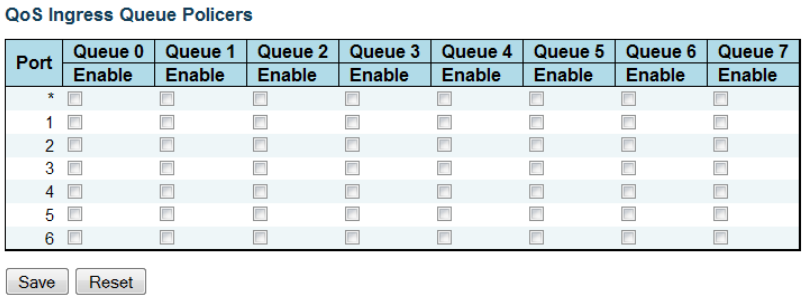


Rys. 61. Konfiguracja Policerów portu wejściowego

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 1-3105 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.

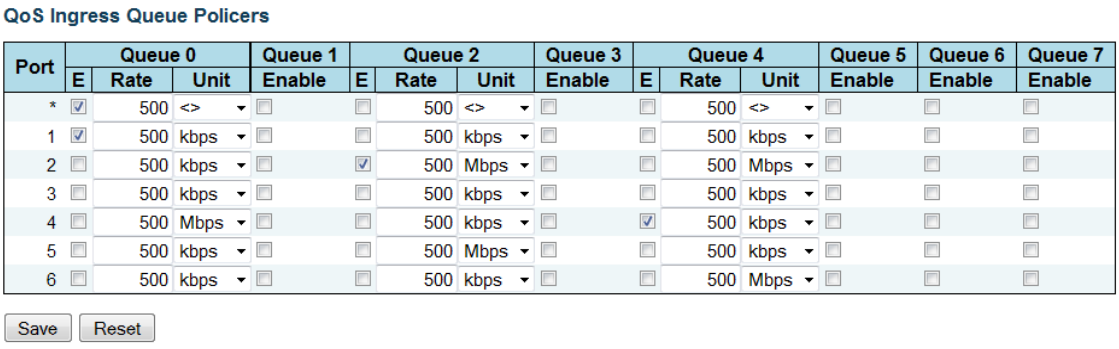
6.10.3 Policer kolejek wejściowych Ingress Queue Policers

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.



Rys. 62. Konfiguracja Policerów kolejek sprzętowych portów wejściowych

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 1-3105 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.



Rys. 63. Konfiguracja ograniczenia pasma dla kolejek wejściowych

6.11 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.

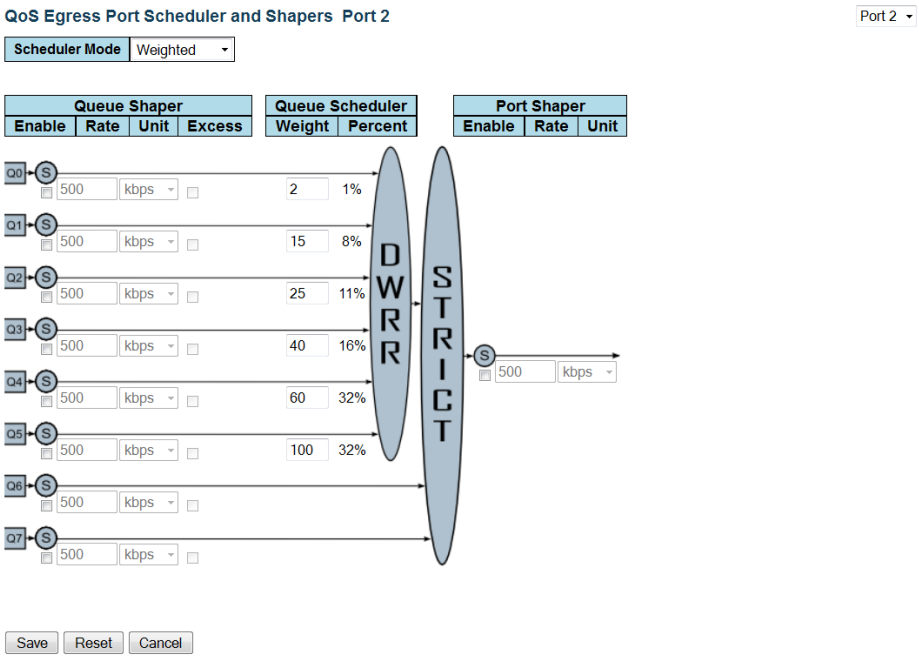
Dostęp do konfiguracji układów *Schedulers* jest możliwy w oknie dostępnym pod linkiem **Configuration > QoS >Port Scheduler**. Okno to przedstawia tylko bieżącą konfigurację układów *Schedulers* dla wszystkich fizycznych portów i dla pięciu pierwszych kolejek. W przypadku, gdy dany port pracuje jako s*trict priority* to wyświetlane są tylko znaki '-'.

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Weighted	17%	17%	17%	17%	17%	17%
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Rys. 64. Konfiguracja układu Scheduler

Konfiguracja układu Scheduler odbywa się niezależnie dla każdego portu, a dostęp do niej jest możliwy przez link 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. 65. Konfiguracja układów scheduler dla portu

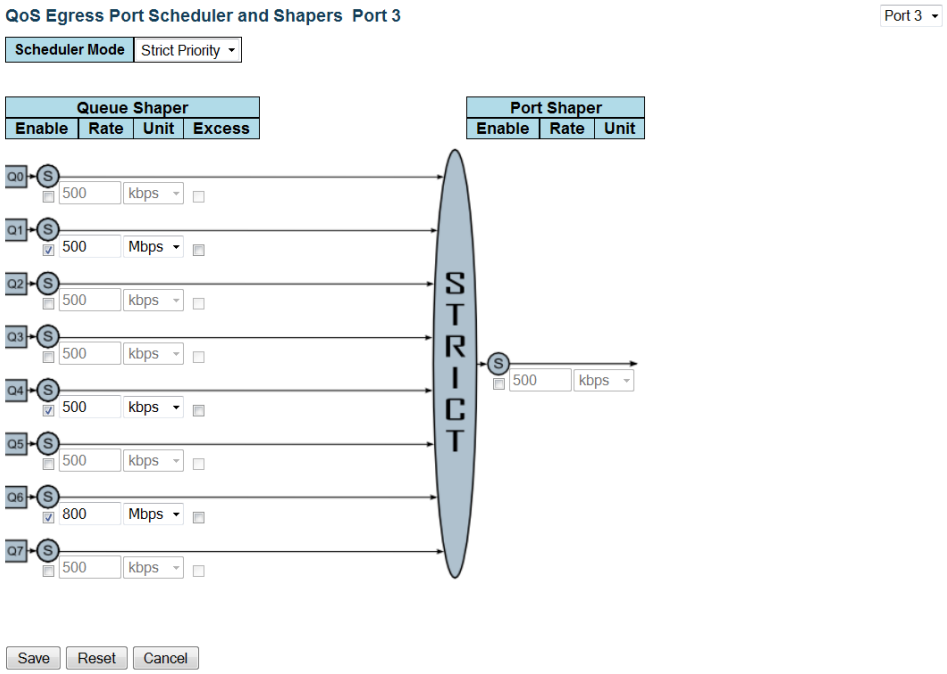
Dostęp do konfiguracji układów *Shapers* jest możliwy pod linkiem **Configuration > QoS > Port Shaping**. Okno to przedstawia tylko bieżącą konfigurację układów *Shapers* dla wszystkich fizycznych portów i dla wszystkich obsługiwanych kolejek.
Konfiguracja układu Scheduler odbywa się niezależnie dla każdego portu, a dostęp do niej jest możliwy przez link na numerze fizycznego portu w kolumnie ***Port***.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	500 Mbps	disabled	disabled	500 kbps	disabled	800 Mbps	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Rys. 66. Konfiguracja układu Shaper

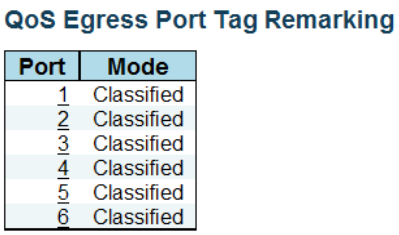
Układ ten pozwala na ograniczenie pasma dla wszystkich kolejek w kierunku wyjściowym i ustawienie zbiorczego ograniczenia pasma wyjściowego na port.
W polu ***Queue Shaper*** kolumna ***Enable*** pozwala na włączenie lub wyłączenie ograniczenia na daną kolejkę. Pola w kolumnach ***Rate*** i ***Unit*** 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. 67. Konfiguracja układów shaper dla portu

6.11.1 Priorytet ramek wyjściowych Egress Port Tag Remarking

Funkcja ta pozwala ustawiać znaczniki PCP i DEI w wychodzących ramkach tagowanych zgodnie z IEEE802.1q. Dostępna jest przez link **Configuration > Qos > Port Tag Remarking**. Konfiguracja jest niezależna dla każdego fizycznego portu i dostępna przez link w kolumnie ***Port***.



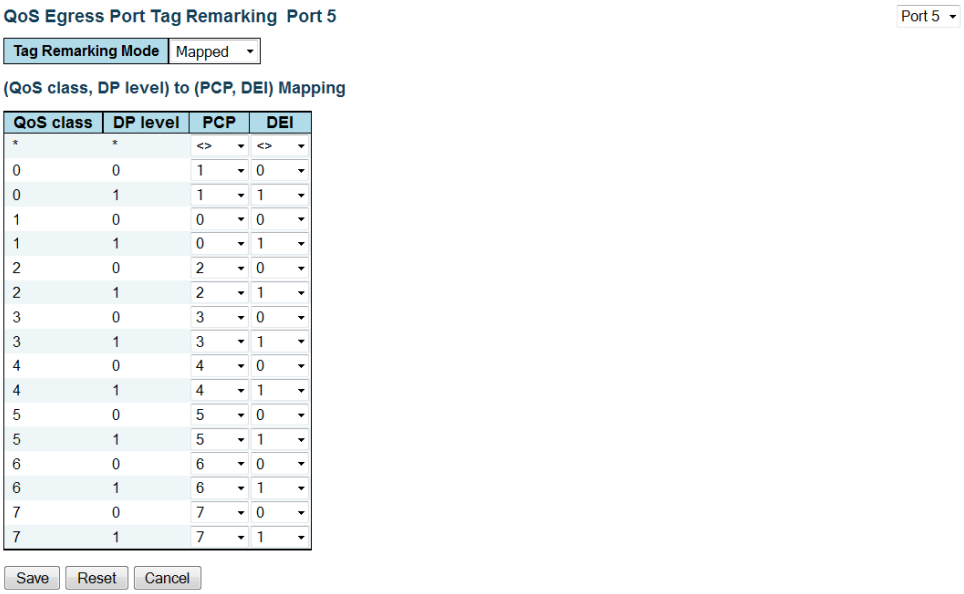
Rys. 68. Bieżąca konfiguracja priorytetów ramek wychodzących

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.

Rys. 69. 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-105** 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.



Rys. 70. Konfiguracja priorytetu ramek wyjściowych w trybie mapped dla portu

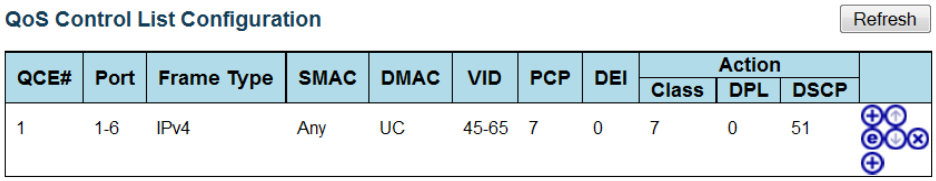
6.11.2 Lista kontrolna QoS Control List Configuration

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*.

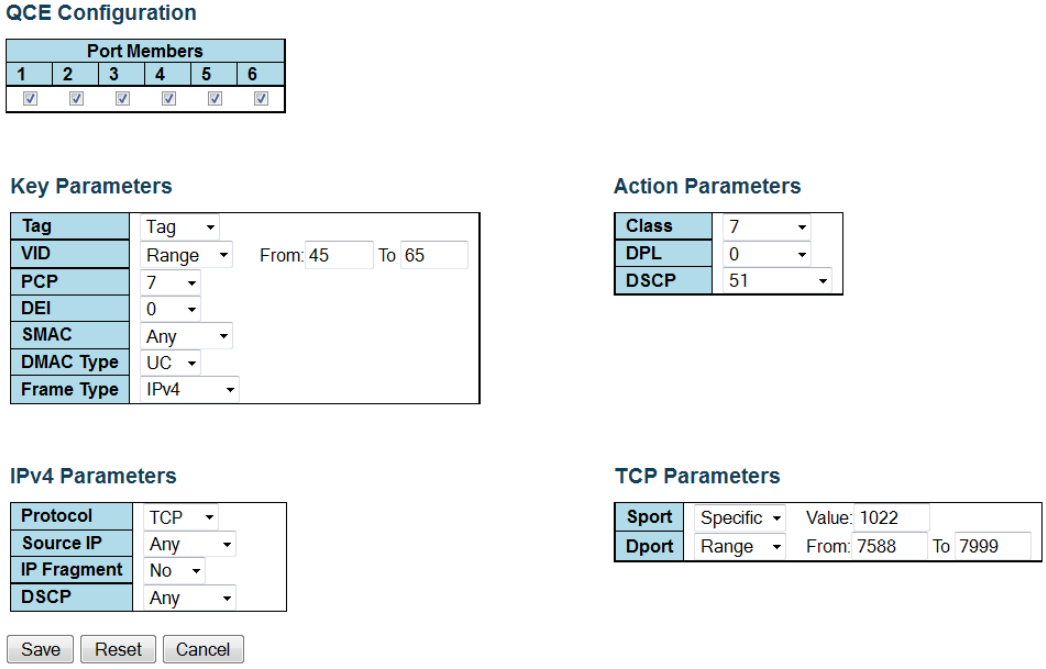
SMAC – wyświetla źródłowy adres MAC kontrolowany przez tą listę.
DMAC – wyświetla adres przeznaczenia MAC kontrolowany przez tą listę, możliwe wartości to:
Any – wszystkie ramki adres przeznaczenia nie jest analizowany.
Unicast – tylko ramki Unicast.
Multicast – tylko ramki Multicast.
Broadcast – tylko 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 pod pól jest następujące
Class: Numer *QoS class* do której zostaną ramki przydzielone.
DPL: Wartość Drop Precedence Leveljaka 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.
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.



Rys. 71. Bieżąca konfiguracja list kontrolnych QoS QCL

Dodanie nowej listy kontrolnej odbywa się przez naciśnięcie przycisku + w kolumnie pierwszej od prawej.



Rys. 72. Konfiguracja listy kontrolnej QCL

Znaczenie poszczególnych parametrów jest następujące:

Port members – określa porty fizyczne urządzenia jakie będą brane przy analizie przez tą listę.

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.

Ethernet – ramki, które w polu *type* posiadają wartość heksadecymalną od 0x600 do 0xFFFF. Po wybraniu tej opcji pojawi się dodatkowe menu ***MAC 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 ***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 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 nie fragmentowane. ***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 się 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 tą listę 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 będą 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:

Class – określa *QoS class* do której dana lista będzie kierować ramki.

DPL – określa znacznik *DPL* jaki zostanie przypisany do ramki przez daną lista.

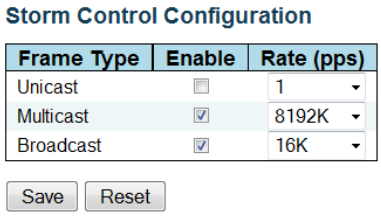
DSCP - określa znacznik *DSCP* w ramkach IP jaki zostanie przypisany do ramki przez daną lista.

Po zakończeniu wprowadzania parametrów należy zatwierdzić zmiany przyciskiem ***Save***.

6.11.3 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 > QoS > Storm Control**

Dla rządnego 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-FF.

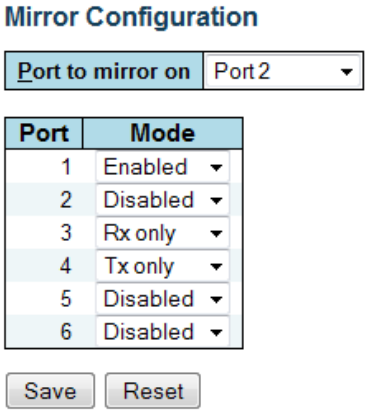


Rys. 73. Konfiguracja ochrony przed sztormem ramkami

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), przełącznik odrzuca ten typ ramek do następnego okresu pomiarowego.

6.12 USTAWIENIA PODGLĄDU RUCHU NA PORTACH MIRRORING

Urządzenie **HYPERION-105** 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 wejść do ustawień Mirroring-u klikamy na link **Configuration > Mirroring**. Wyświetla nam się strona z parametrami do ustawienia podglądu ruchu sieciowego.



Rys. 74. Konfiguracja podglądu ruchu na portach

Tabela ***Port to mirror on*** zawiera wybór portu, który będzie służył do podglądu ruchu na wybranych portach.
W tabeli możemy ustawić 8 wartości, przy czym jedną z nich jest wyłączenie podglądu natomiast inne wartości odpowiadają numerowi portu urządzenia, który miałby służyć za port monitorujący ruch.
Disabled – ta wartość powoduje wyłączenie podglądu ruchu w urządzeniu,
Port 1, ..., Port 7 – te wartości ustanawiają, który port będzie portem do podglądu ruchu. ***Port 1*** ustawia port numer 1 jako port monitorujący ruch, ***Port 2*** ustawia port numer 2 jako port monitorujący itd.

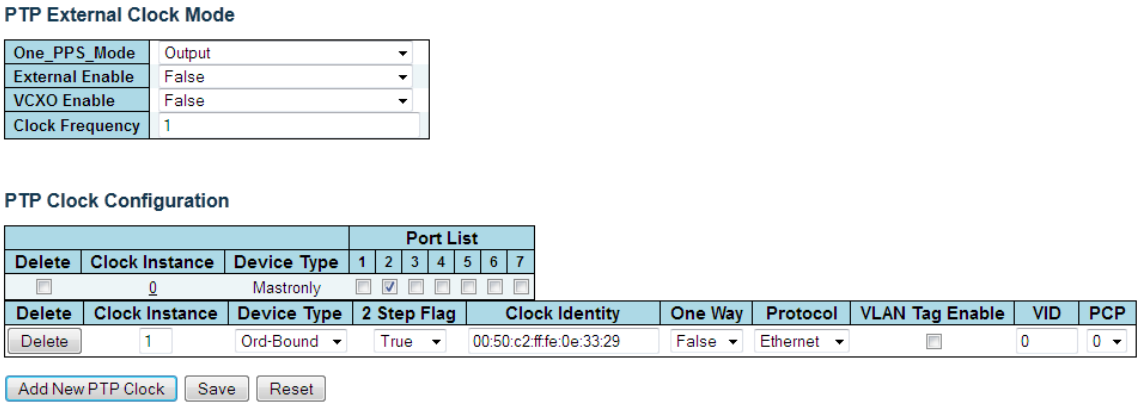
Druga tabela zawiera wiersze do konfiguracji dla każdego portu osobno. W kolumnie pierwszej mamy kolejne numery portów, a w drugiej kolumnie ***Mode*** możemy przypisać do danego portu wartości:

Disabled – wyłącza port z monitorowania, czyli ramki z tego poru nie będą kopiowane do portu monitorującego
Enabled – włącza port jako port monitorowany. Ramki, zarówno przychodzące jak i wychodzące z portu są kopiowane do portu monitorującego.
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.

Przycisk ***Save*** zapamiętuje ustawienia w pamięci nieulotnej urządzenia i zatwierdza zmiany.

6.13 PTP Precision Time Protocol

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-105** obsługuje tylko drugą wersję protokołu (wersje 1 i 2 nie są ze sobą kompatybilne). Panel konfiguracji PTP znajduje się w menu **Configuration > PTP**.



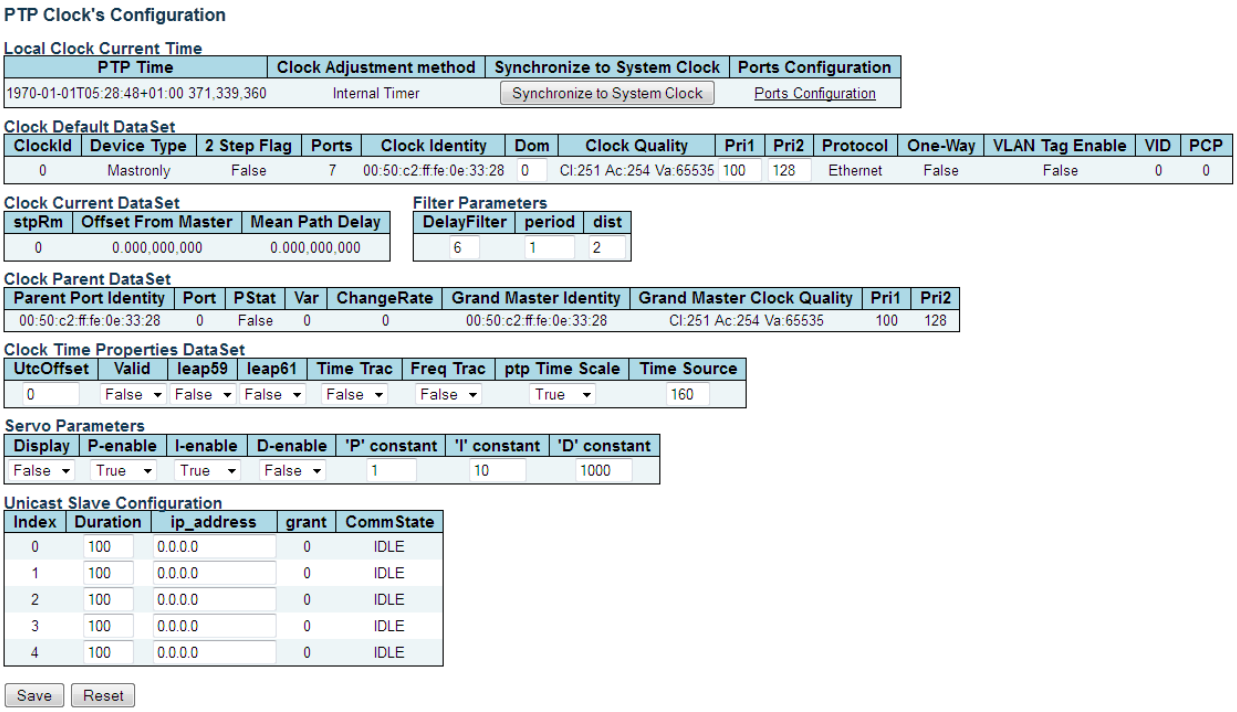
Rys. 75. Podstawowa konfiguracja PTP

Tabela ***PTP External Clock Mode*** służy wyłącznie do testów i nie ma żadnego znaczenia dla użytkownika.
W tabeli ***PTP Clock Configuration*** konfiguruje się zegary PTP, które będą działać w urządzeniu. Można zdefiniować do czterech zegarów PTP (o numerach ***Clock***

Instance od 0 do 3). Domyślnie nie są skonfigurowane żadne zegary PTP. Aby dodać zegar należy kliknąć przycisk ***Add New PTP Clock***, wpisać ustawienia nowego zegara, a następnie zatwierdzić przyciskiem ***Save***. Ustawień zegara wprowadzonych w tym panelu nie można później zmienić (w celu zmiany konieczne jest usunięcie zegara i utworzenie nowego). Ustawienia konfigurowane przy tworzeniu zegara są następujące:
Clock Instance – numer zegara – może być dowolną cyfrą of 0 do 3, która oznacza jeden z zegarów PTP dostępnych w **HYPERION-105**. Zegar o numerze 0 liczy czas sprzętowo (jest więc najdokładniejszy), pozostałe liczą czas programowo.
Device Type – określa typ zegara PTP. Dostępne typy to: ***Inactive*** – zegar wyłączony, ***Ord-Bound*** – zegar 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 zegara *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 zegar *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*. ***Mastronly*** **–** 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.
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 unikatowe – ta opcja jest możliwa tylko dla trybów *Master only* i *Slave only* (konieczna jest dodatkowa konfiguracja w ustawieniach zaawansowanych PTP).
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.

6.13.1 Ustawienia zaawansowane zegarów

Klikając na numer zegara w panelu ogólnym PTP można wyświetlić jego konfigurację zaawansowaną.



Rys. 76. Konfiguracja zaawansowana zegara PTP

W tabeli ***PTP Clock's Configuration*** wyświetlony jest aktualny czas zegara PTP oraz sposób realizacji 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:

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:

Cl – klasa zegara. Standard definiuje następujące klasy zegarów:

0: może być używana tymczasowo, do testów,

1: 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),

2: drugorzędny zegar o możliwych nieco gorszych parametrach (np. wyeksploatowany zegar pierwszej klasy lub zegar synchronizujący się do innego zegara pierwszej klasy za pomocą PTP),

3: zarezerwowana dla komisji P1588,

4 – 253: zarezerwowana dla profili,

254: domyślna,
255: zegary zawsze występujące w roli *Slave* powinny posiadać tę klasę.

Ac – dokładność zegara.
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***.

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 informacjach o lokalnym zegarze (*Clock Default DataSet*).
Pri1 i ***Pri2*** – priorytety zegara *Master*.

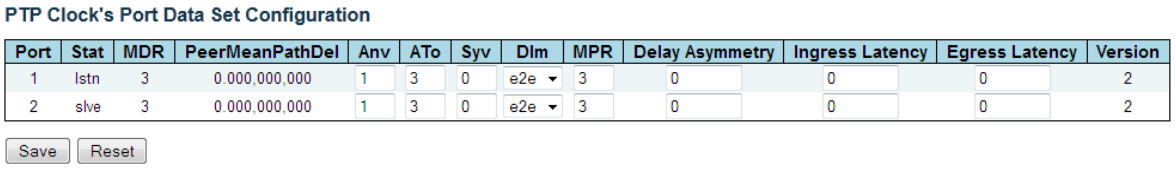
Tabela ***Clock TIme Properties DataSet*** zawiera ustawienia określone w normie IEEE 1588, ale nieobsługiwane w aktualnej wersji oprogramowania.

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.

6.13.1.1 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	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
1	lstn	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2
2	slve	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2

Save Reset

Rys. 77. Konfiguracja portów zegara PTP

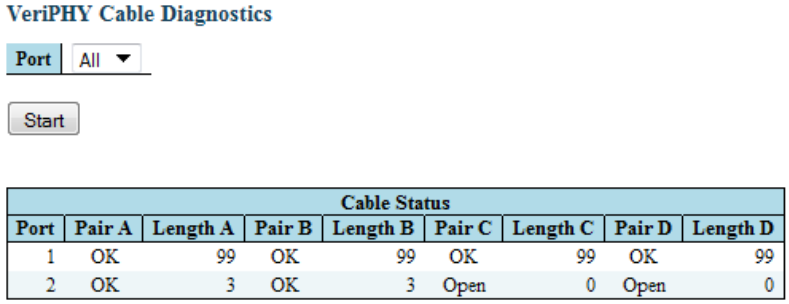
W tabeli tej wyświetlone są porty przypisane do aktualnego zegara PTP w konfiguracji globalnej PTP. Dla każdego portu wyświetlone są następujące informacje:
Port – numer portu, którego dotyczy wiersz,
Stat – aktualny stan portu,
MDR – minimalny interwał zapytań o opóźnienie linii sugerowany przez urządzenie *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-105** 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*,
Dlm* –** 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.

6.13.2 Monitorowanie PTP

Panel monitorowania PTP dostępny jest w menu **Monitor > 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.

6.14 Diagnostyka kabla

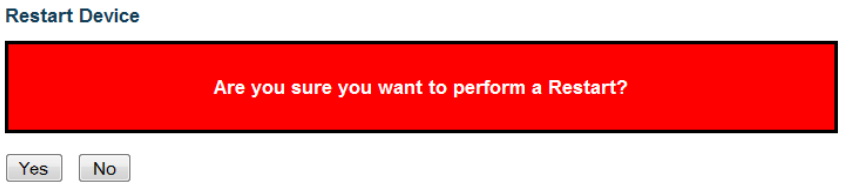
Interfejsy ethernetowe posiadają funkcje diagnostyczne, umożliwiające kontrolę parametrów kabli połączeniowych. Każda para kabla jest diagnozowana niezależnie – ***Pair A***, ***Pair B***, ***Pair C***, ***Pair D***. Można określić jej długość w metrach – ***Length A***, ***Length B***, ***Length C***, ***Length D*** oraz niewłaściwe dopasowanie, przerwę lub zwarcie. Dokładny pomiar długości kabla zawiera się w zakresie od 7 do 140 metrów. Podczas pomiaru, następuje wyłączenie portów skonfigurowanych na 10 i 100 Mbit/s. Po pomiarze, porty włączane są ponownie w stan aktywności.



Rys. 78. Diagnostyka kabli połączeniowych.

6.15 Ustawienia domyślne i ponowne uruchomienie

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.



Rys. 79. Strona umożliwiająca ponowne uruchomienie urządzenia

Przywrócenie ustawień domyślnych urządzenia **HYPERION-105** jest możliwe na stronie dostępnej pod linkiem: **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! Przywracanie ustawień domyślnych nie obejmuje 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.

UWAGA! Ustawienia domyślne usuwają również hasło dostępu do urządzenia.

Rys. 80. Strona umożliwiająca przywrócenie ustawień domyślnych urządzenia

6.16 AKTUALIZACJA OPROGRAMOWANIA

Interfejs www udostępnia możliwość aktualizacji oprogramowania w **HYPERION-105**. Początkowa strona aktualizacji dostępna jest pod linkiem **Maintenance> Software Upload.**
W celu zaktualizowania oprogramowania należy klikną przycisk ***Przeglądaj...***, wybrać plik 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 minut, po tym czasie urządzenie uruchomi się ponownie już z nowym oprogramowaniem i odświeży interfejs www wyświetlając stronę.

Rys. 81. Strona początkowa aktualizacji oprogramowania

Rys. 82. Strona postępu instalacji oprogramowania

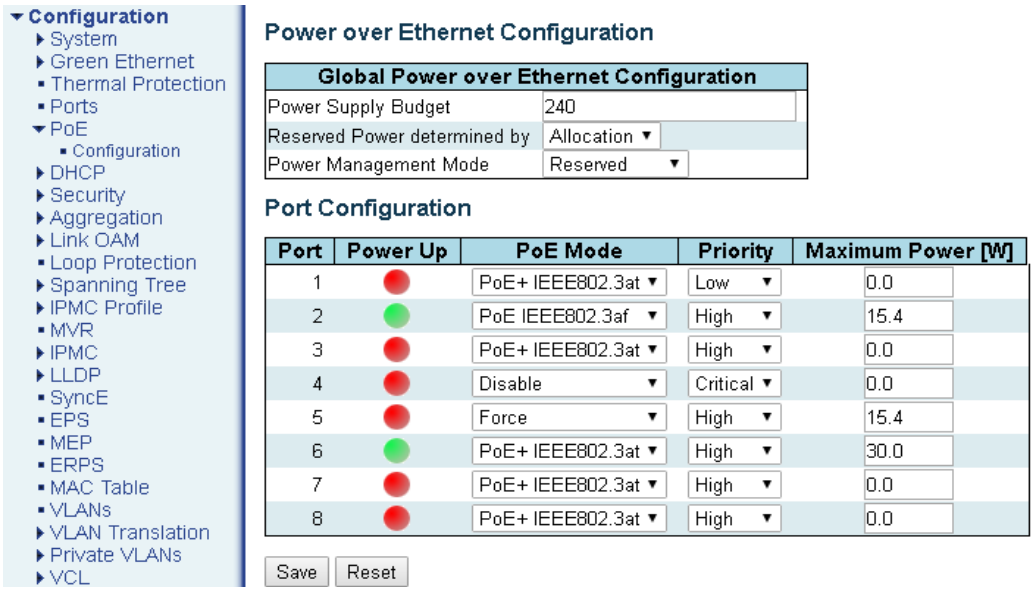
6.17 POWER OVER ETHERNET

PoE w Hyperion-105 jest zgodne ze standardem IEEE 802.3af/at typ 1/2 i PoE++ (90W). Przy standardowej wersji wymagane jest napięcie zasilania zgodnie z poziomem dostarczanym przez PoE:

77p – Zasilanie redundantne 9-60V DC, dla PoE wymagane 45-57V DC
PoE (do 15W) 45-57V
PoE+ (do 30W) 52-57V
PoE++ (do 90W) 55-57V
Maksymalnie na wszystkich portach 360W.

Dla wersji zasilania '33p' jest możliwość zasilania napięciem niższym lub wyższym (24-60V DC) od wymaganego przez standard PoE. Wbudowana przetwornica **'booster'** zapewnia stabilizację napięcia dla PoE÷PoE++ na poziomie 55V DC.

33p – Zasilanie redundantne 'booster' 24-60V DC / stabilizacja napięcia 55V DC dla PoE÷PoE++
Maksymalnie na wszystkich portach 200W, dodatkowo wiąże się z większymi kosztami produktu, wymiarami obudowy oraz temperaturą.



Rys. 83. Ustawienia PoE

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

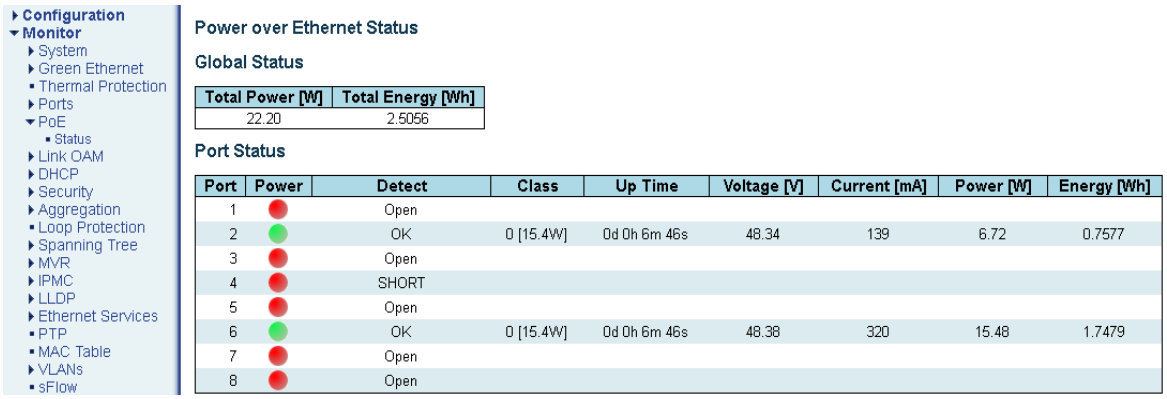
Reserved Power determined by – definiujemy ograniczenie mocy na porcie.
'Class' tryb zgłasza urządzenie zdalne, wstępna definicja w polu 'PoE Mode', 'Allocation' tryb definiowany ręcznie w polu 'Maximum Power'.

Power Management Mode – wybieramy ograniczenie mocy na podstawie rezerwacji 'Reserved' w polu 'Maximum Power'. Natomiast 'Consuption' 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 jest odpytywane urządzenie zdalne, wiąże się to z ilością mocy na porcie jak i też z możliwością włączenia negocjacji mocy w trybie 'Force'. Uwaga: tryb 'Force' podaje moc na sztywno niezależnie, czy odbiornik jej

potrzebuje czy też nie, może to uszkodzić port w urządzeniu zdalnym. Tryb ten czasem wymagany przez niektóre odbiorniki.

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



Rys. 84. Monitorowanie PoE

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, które jest sygnalizowane 'Short'.

7 Konfiguracja przełącznika – interfejs CLI

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. Konfiguracja **HYPERION-105** za pomocą interfejsu CLI wymaga komputera z zainstalowanym programem konsoli zdalnej SSH lub telnet.

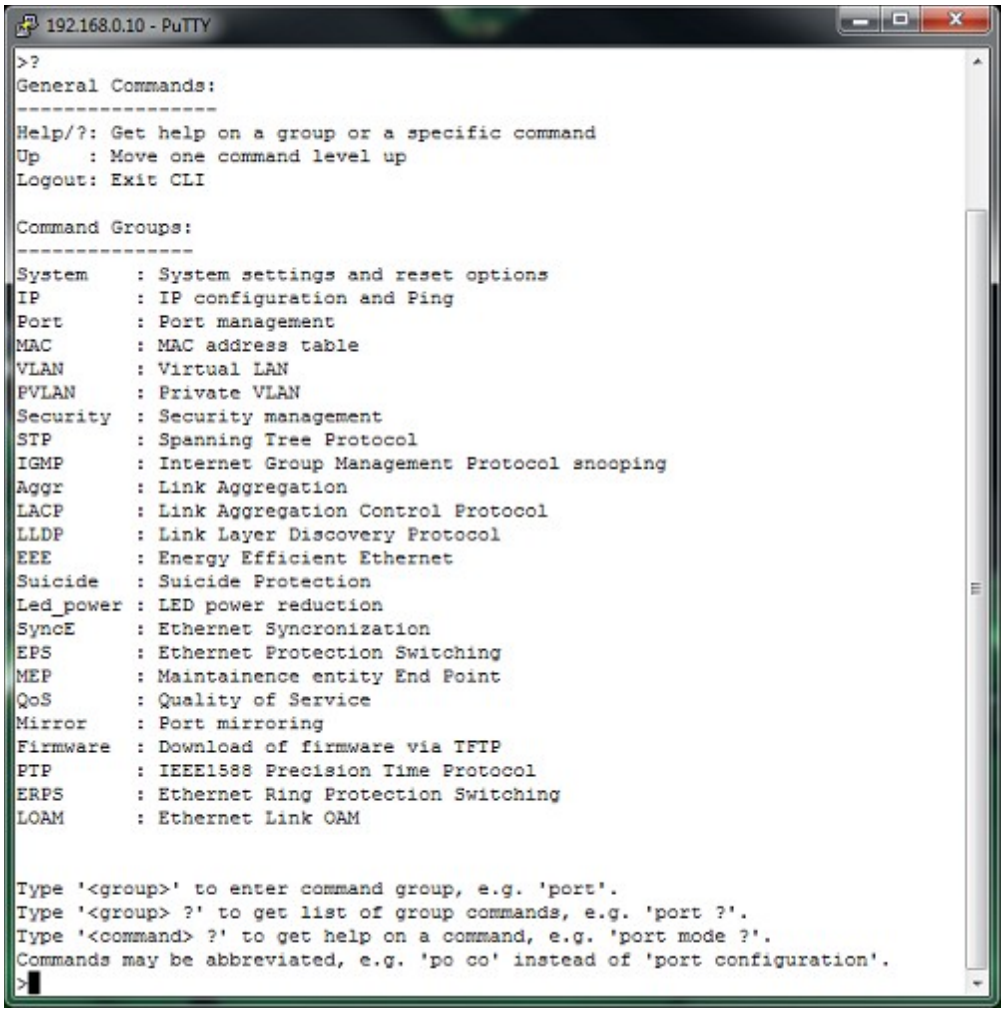
Połączenie przez konsolę zdalną wymaga odpowiedniego programu (dla systemu Windows zalecany jest program *putty*, dostępny pod adresem http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) oraz poprawnie skonfigurowanego połączenia LAN pomiędzy urządzeniem a komputerem.

W tym rozdziale opisany jest jedynie sposób użycia interfejsu CLI wraz z krótkimi opisami odpowiednich funkcji dla **HYPERION-105**. Aby rozpocząć zarządzanie przez CLI należy uruchomić jeden z programów konsoli SSH lub telnet (np. *putty*) i skonfigurować go tak, aby mógł uzyskać połączenie z **HYPERION-105**. Po tej czynności powinien on wyświetlić komunikat logowania.

Rys. 85. Ekran logowania do CLI

W tym miejscu należy wpisać nazwę użytkownika, domyślnie jest to **admin**, nacisnąć klawisz *Enter*, a następnie wpisać hasło dostępu do urządzenia, jeśli zostało wcześniej wprowadzone. Po poprawnym zalogowaniu zostanie wyświetlony tekst:
Welcome to HYPERION-105 Command Line Interface.
Type 'help' or '?' to get help.

>
Po znaku zachęty **>** można wpisywać polecenia obsługi urządzenia.
W każdym momencie możliwe jest wyświetlenie listy dostępnych poleceń w danym miejscu przez wpisanie znaku ? lub słowa help i kliknięciu klawisza *Enter*. Lista poleceń w grupie głównej, jest przedstawiona na poniższym rysunku.



Rys. 86. Lista poleceń głównych

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 **up**.

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:

6) **System** : Podstawowe ustawienia systemu i dziennik zdarzeń
7) **IP** : Konfiguracja adresu IP urządzenia i serwera NTP,
8) **Port** : Konfiguracja ustawień portów,
9) **MAC** : Konfiguracja i podgląd tablicy adresów MAC,
10) **VLAN** : Konfiguracja i monitorowanie wirtualnych sieci LAN,
11) **PVLAN** : Konfiguracja i monitorowanie prywatnych wirtualnych sieci LAN,
12) **Security** : Konfiguracja ograniczenia dostępu do zarządzania urządzeniem,
13) **STP** : Konfiguracja protokołów drzewa opinającego STP, RSTP, MSTP,
14) **IGMP** : Konfiguracja protokołu: Internet Group Management Protocol snooping,
15) **Aggr** : Konfiguracja agregacji portów,
16) **LACP** : Konfiguracja agregacji portów i protokołu: LACP IEEE 802.3ad,
17) **LLDP** : Konfiguracja i monitorowanie protokołu: LLDP IEEE 802.3ab,
18) **EEE** : Konfiguracja ustawień oszczędzania energii,
19) **Led_power** : Konfiguracja intensywności świecenia sygnalizacyjnych diod LED ,
20) **EPS** : Konfiguracja liniowego protokołu protekcji drogi transmisyjnej,
21) **MEP** : Konfiguracja punktów końcowych ITU-T Y.1731,
22) **QoS** : Zarządzanie jakością usług i ochrony przed sztormem pakietów,
23) **Mirror** : Konfiguracja portów do podglądu transmisji (tzw. sniffer),
24) **Firmware** : Polecenie do pobrania pliku oprogramowani urządzenia z serwera TFTP,
25) **PTP** : Konfiguracja protokołu: IEEE1588 Precision Time Protocol,
26) **ERPS** : Konfiguracja protokołu protekcji drogi transmisyjnej dla urządzeń pracujących w topologii pierścienia,
27) **CHAIN** : Konfiguracja protekcji drogi transmisyjnej dla urządzeń pracujących w trybie łańcucha
28) **LOAM** : Konfiguracja protokołu opisanego w ITU-T Y.1731 używanego do implementacji funkcjonalności carrier Ethernet.Opis poleceń

7.1.1 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,
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 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.
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.

7.1.2 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 105.
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.
NTP Server Ipv6 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 serwer o numerze podanym, jako parametr **<server_index>**.

7.1.3 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**.

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 maksymalna długość 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.

7.1.4 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

8 Dane techniczne

8.1 Parametry elektryczne

8.1.1 Porty optyczne Ethernet

Parametr	Wartość parametru
Znamionowa przepływność binarna	100/1000 Mbit/s
Stopa błędów	$\leq 10^{-11}$
Typ złączy,	W zależności od modułu SFP

8.1.2 Porty elektryczne Ethernet

Parametr lub cecha	Wartość parametru lub opis cechy
Szybkość transmisji	10/100 Mbit/s
Typ złącza	RJ-45
Typ portu	MDI/MDIX – wykrywane automatycznie

8.1.3 Parametry mechaniczne

Parametr	Wartość parametru
Szerokość	65mm
Wysokość	135 mm
Głębokość	125 mm
Masa	0,9 kg
Obudowa	IP 30

8.1.4 Parametry mechaniczne dla wersji '33p' i wersji ‘B’

Parametr	Wartość parametru
Szerokość	99mm
Wysokość	135 mm
Głębokość	125 mm
Masa	1.1 kg
Obudowa	IP 30

8.2 Wymagania środowiskowe

8.2.1 Eksploatacja

Urządzenie **HYPERION-105** może pracować w pomieszczeniach zamkniętych nierównomiernie ogrzewanych w następujących warunkach klimatycznych:

Parametr Środowiskowy	Wartość dopuszczalna
Temperatura otoczenia	-40 ÷ +70°C (+50°C przy pełnym obciążeniu PoE-PoE++)
Wilgotność względna powietrza	max. 95 % w temperaturze +20°C (bez kondensacji)

8.2.2 Transport

Urządzenie **HYPERION-105** w opakowaniu fabrycznym może być przewożone lądowymi i powietrznymi środkami transportu w zakresie temperatur -40....+70 °C

8.2.3 Przechowywanie

Urządzenie **HYPERION-105** należy przechowywać w pomieszczeniach zamkniętych, w następujących warunkach środowiskowych:

Parametr Środowiskowy	Wartość Dopuszczalna
Temperatura otoczenia	-40 ÷ +70°C
Wilgotność	0 % do 95 % / +40°C

8.3 Zasilanie

8.3.1 Stałe napięcie zasilające

Parametr lub cecha	Wartość parametru lub opis cechy
Znamionowe napięcie zasilające dla wersji 77p	9-60V DC / 8W (bez PoE)
Pobór prądu	800mA przy 9 V (bez PoE) 140mA przy 60V (bez PoE)
Znamionowe napięcie zasilające dla wersji 33p	'booster' 24-60V DC
Znamionowe napięcie zasilające dla wersji B	100-370V DC / 88-264V AC