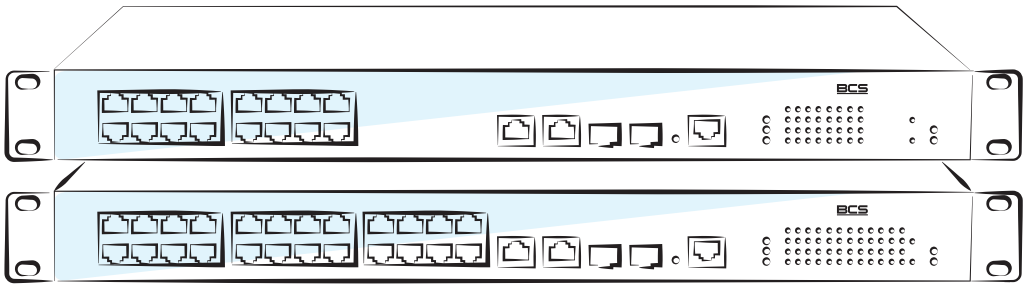
PL

Instrukcja konfiguracji sieciowej

przełącznika 16/24-portowego PoE

BCS-L-SP1602G-2SFP-M
BCS-L-SP1602G-2SFP-M(II)
BCS-L-SP2402G-2SFP-M
BCS-L-SP2402G-2SFP-M(II)



www.bcscctv.pl
NSS Sp. z o.o. ul. Modularna 11 (Hala IV), 02-238 Warszawa
tel. +48 22 846 25 31, fax. +48 22 846 23 31 wew.140
e-mail: info@bcscctv.pl, NIP: 521-312-46-74

Wersja podręcznika: 2.05

WAŻNE ZABEZPIECZENIA I OSTRZEŻENIA

Prosimy o uważne przeczytanie poniższych środków ostrożności i ostrzeżeń przed użyciem tego produktu, aby uniknąć szkód i strat.

WAŻNE

- Nie wystawiaj urządzenia na działanie czerni, pary ani kurzu. W przeciwnym razie może to spowodować pożar lub porażenie prądem.
- Nie instaluj urządzenia w miejscu wystawionym na działanie promieni słonecznych lub w wysokiej temperatury. Wzrost temperatury w urządzeniu może spowodować pożar.
- Nie wystawiaj urządzenia na działanie wilgoci. W przeciwnym razie może to spowodować pożar.
- Urządzenie musi być zainstalowane na twardym i płaskim podłożu w celu zagwarantowania bezpieczeństwa pod obciążeniem i w przypadku trzęsienia ziemi. W przeciwnym razie może to spowodować upadek lub przewrócenie się urządzenia.
- Nie umieszczaj urządzenia na dywanie lub kołdrze.
- Nie blokuj otworów wentylacyjnych urządzenia ani wentylacji wokół urządzenia. W przeciwnym razie temperatura w urządzeniu wzrośnie i może spowodować pożar.
- Nie umieszczaj żadnych przedmiotów na urządzeniu
- Nie demontuj urządzenia bez fachowej instrukcji.
- Aby uniknąć obrażeń ciała lub uszkodzenia urządzenia, wyłącz urządzenie przed odłączeniem kabla.
- Stabilizator napięcia i odgromnik są opcjonalne w zależności od źródła zasilania i otaczającego środowiska.

OSTRZEŻENIE

- Aby uniknąć pożaru, eksplozji i innych niebezpieczeństw, należy prawidłowo używać baterii.
- Proszę wymienić zużytą baterię na baterię tego samego typu.
- Nie używaj innego przewodu zasilającego niż określony. Proszę, używaj go prawidłowo. W przeciwnym razie może to spowodować pożar lub porażenie prądem.
- Upewnij się, że urządzenie jest uziemione (przekrój przewodu miedzianego:> 2,5 mm2, rezystancja uziemienia: ≤ 4 Ω).

OGŁOSZENIE SPECJALNE

- Niniejsza instrukcja służy wyłącznie jako odniesienie.
- Wszystkie projekty i oprogramowanie tutaj mogą ulec zmianie bez wcześniejszego pisemnego powiadomienia.
- Zawsze postępuj zgodnie z wytycznymi zawartymi w instrukcji. Nie odpowiadamy za jakiekolwiek problemy spowodowane przez nieautoryzowane modyfikacje lub próby naprawy.
- Wszystkie znaki towarowe i zarejestrowane znaki towarowe są własnością ich odpowiednich właścicieli.
- W przypadku jakichkolwiek wątpliwości lub kontrowersji prosimy o zapoznanie się z naszym ostatecznym wyjaśnieniem.
- Aby uzyskać więcej informacji, proszę odwiedzić naszą stronę internetową**.**

SPIS TREŚCI

1. PRZEGLĄD

1.1 WPROWADZENIE DO PRODUKTU

Produkt jest rodzajem zarządzanego przełącznika, zapewnia port Ethernet 16/24 * 10 / 100M PoE i 2 łącza uplink Porty Combo 1000M, obsługują zarządzanie siecią warstwy 2 i funkcje zarządzania PoE w oparciu o Sieć, która pomaga realizować szybkie przekazywanie danych.

1.2 CECHY PRODUKTU

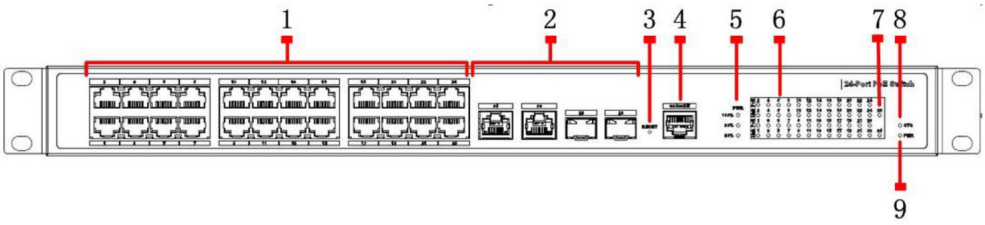
- Zapewnia zarządzanie siecią w warstwie 2 przez Internet.
- Obsługa transmisji na odległość 250 metrów.
- Obsługa portów Combo 2 * 1000 M.
- Obsługa samodostosowujących się portów RJ45 16/24 * 10 / 100M
- Obsługuje jeden port konsoli.
- Zgodność ze standardami IEEE802.3, IEEE802.3u, IEEE802.3ab / z i IEEE802.3X.
- Standardowa sieć VLAN 802.1Q (dostęp / trunk / hybrydowa)
- Wszystkie porty automatycznie dostosowują się do trybu MDI / MDIX.
- Automatyczne uczenie i starzenie się adresów MAC, pojemność listy adresów MAC to 4K.
- Kontrola przepływu IEEE802.3X w trybie pełnego dupleksu i kontrola przepływu w trybie półdupleksu wstecznego.
- Obsługa zasilania AC 100 ~ 240 V.
- Zgodne ze standardami IEEE802.3af i IEEE802.3at, oba porty 1 i 2 obsługują Hi-PoE 60 W.
- Obsługa zarządzania zużyciem energii PoE.
- Obsługa zarządzania siecią SNMP V1 / V2 / V3.
- Obsługa platformy zarządzania siecią iLinksView.
- Obsługa pierścieniowego protokołu sieciowego STP / RSTP.
- Obsługa ręcznej agregacji i statycznego LACP.
- Obsługa dublowania wielu do jednego.
- Obsługa wiązania adresu MAC portu.
- Doskonała ochrona obwodu izolowanego.
- Ochrona odgromowa do poziomu 4.

2. STRUKTURA URZĄDZENIA

2.1 STRUKTURA 24-PORTOWEGO PRZEŁĄCZNIKA POE

2.1.1 PRZEDNI PANEL

Panel przedni urządzenia pokazano na rysunku 2-1.



Rysunek 2-1 Panel przedni urządzenia

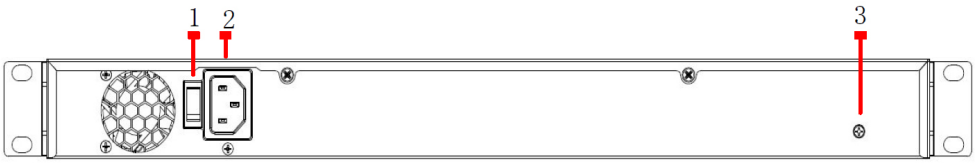
W tabeli 2-1 przedstawiono opis panelu przedniego 24-portowego przełącznika PoE.

Nr	Parametr	Funkcja
1	RJ45 port	Port Ethernet, obsługa samodostosowania 10/100 M
2	Combo port	Port Ethernet, obsługa samodostosowania 10/100/1000 M Port światłowodowy obsługuje 1000 M.
3	Przycisk resetu	Długo naciśnij przycisk, aby zresetować urządzenie i odzyskać konfigurację domyślną.
4	Port szeregowy konsoli	Port debugowania urządzenia
5	Zużycie energii PoE wskaźnik	Wyświetlanie aktualnego zużycia energii
6	Kontrolka łącza Downlink	Bieżący stan łącza portu i stan PoE.
7	Kontrolka portu combo	Port combo wskazuje łącze/działanie
8	Kontrolka systemu	Status systemu: • Podczas uruchamiania urządzenia lampka miga szybko • Gdy urządzenie działa prawidłowo, lampka miga powoli
9	Kontrolka zasilania	Aktualny stan zasilania urządzenia.

Tabela 2-1 Panel przedni urządzenia

2.1.2 PANEL TYLNI

Panel tylni urządzenia pokazano na rysunku 2-2.



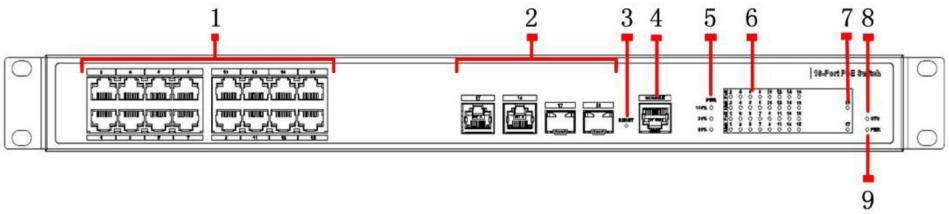
Rysunek 2-2 Panel tylni urządzenia

Opis panelu tylnego zawiera tabela 2-2.

Nr	Parametr	Funkcja
1	Włącznik zasilania	Włączanie i wyłączanie urządzenia sterującego
2	Gniazdo zasilania	Obsługa AC 100~240 V
3	Zacisk uziemienia	Uziemienie

Tabela 2-2 Panel tylni urządzenia

2.2 PANEL PRZEDNI 16-PORTOWEGO PRZEŁĄCZNIKA POE



Rysunek 2-3 Panel urządzenia

Więcej informacji zawiera tabela 2-3.

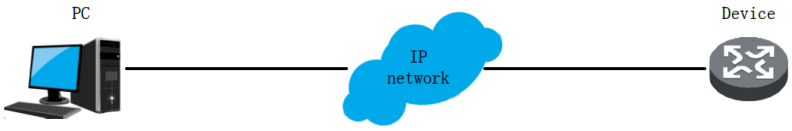
Nr	Parametr	Funkcja
1	RJ45 port	Port Ethernet, obsługa samodostosowania 10/100 M
2	Combo port	Port Ethernet, obsługa samodostosowania 10/100/1000 M Port światłowodowy obsługuje 1000 M
3	Przycisk resetu	Długo naciśnij przycisk, aby zresetować urządzenie
4	Port szeregowy konsoli	Port debugowania urządzenia
5	Zużycie energii PoE wskaźnik	Wyświetlanie aktualnego zużycia energii
6	Kontrolka łącza Downlink	Bieżący stan łącza portu i stan PoE
7	Kontrolka portu combo	Port combo wskazuje łącze/działanie
8	Kontrolka systemu	Status systemu: • Podczas uruchamiania urządzenia lampka miga szybko • Gdy urządzenie działa prawidłowo, lampka miga powoli
9	Kontrolka zasilania	Aktualny stan zasilania urządzenia.

Tabela 2-3 Panel urządzenia

3. LOGOWANIE DO SWITCHA

3.1 LOGOWANIE

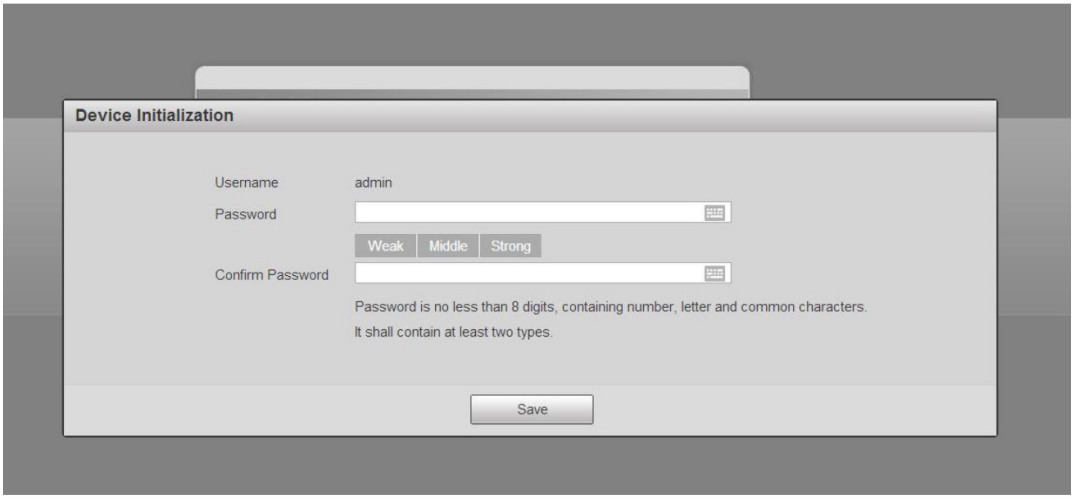
Należy zalogować się do przełącznika zanim będzie można go skonfigurować, użytkownicy mogą intuicyjnie zarządzać przełącznikiem Ethernet z serii PFS42 za pośrednictwem sieci.



Rysunek 3-1

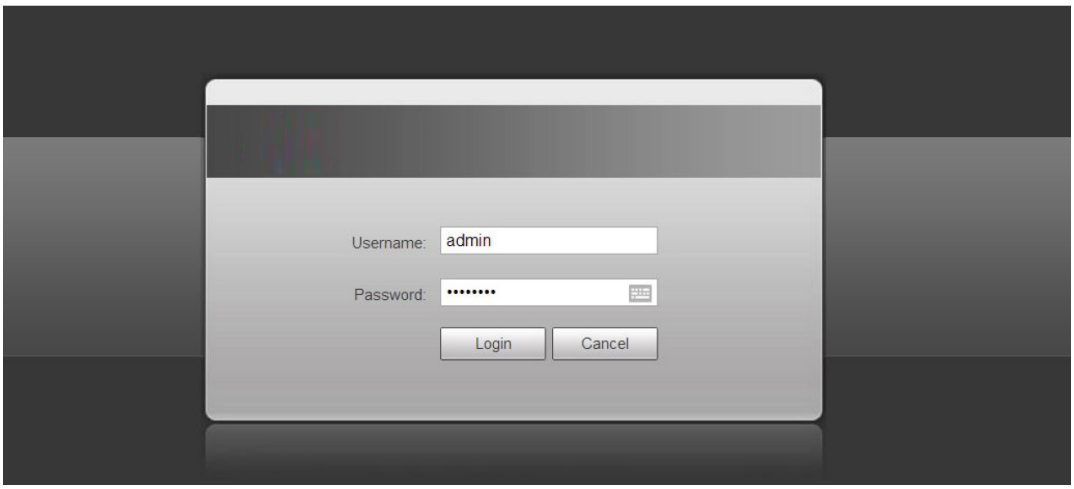
Dostęp do przełącznika można uzyskać za pośrednictwem przeglądarki internetowej, upewnij się, że komputer jest połączony do sieci, w której znajduje się przełącznik. Nie wymaga dodatkowej konfiguracji, jeśli używasz przełącznika po raz pierwszy, teraz możesz się logować za pośrednictwem sieci.

1. Zmień adres IP i maskę podsieci karty sieciowej komputera na 192.168.1.50 i 255.255.255.0 odpowiednio.
2. Otwórz przeglądarkę internetową, wprowadź 192.168.1.110 w pasku adresu i pamiętaj, że 192.168.1.110 to domyślny adres zarządzania przełącznikiem.
3. Ustaw hasło administratora, które nie powinno być mniejsze niż 8 znaków, a następnie kliknij Zapisz.



Rysunek 3-2

4. Wprowadź konto użytkownika i hasło, a następnie kliknij Zaloguj się, aby zalogować się do urządzenia.

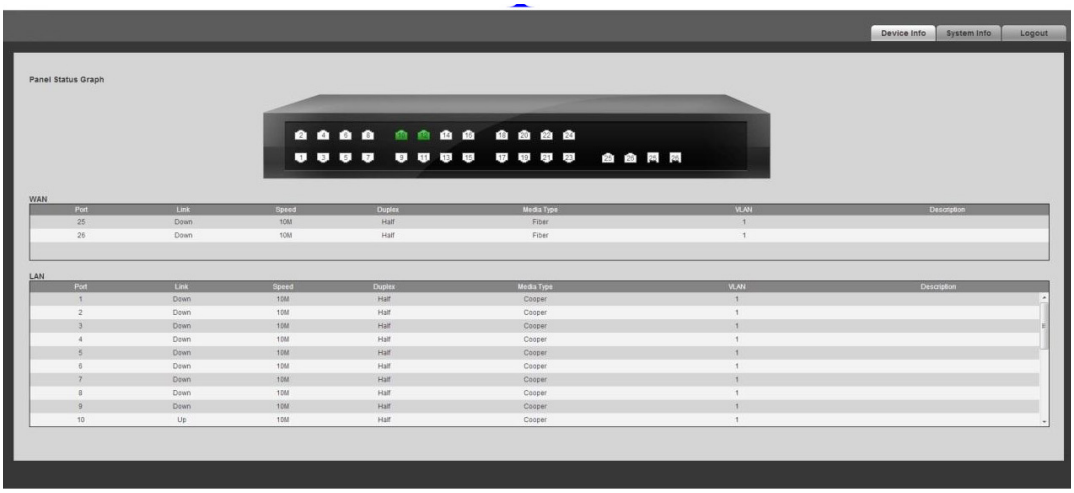


Rysunek 3-3

5. Interfejs informacji o systemie przełącznika zostanie wyświetlony, jeśli nazwa użytkownika i hasło są poprawne.

- iLinksView jest domyślnie włączony, a domyślna nazwa użytkownika to admin, a domyślne hasło to lt_91_il_02_nmp.
- Korzystając z iLinksView do zarządzania urządzeniem, należy pamiętać, że nazwa użytkownika i hasło muszą być takie same, jak ustawione w iLinksView, w przeciwnym razie iLinksView nie może wykryć urządzenia.

3.2 WPROWADZENIE DO INTERFEJSU INTERNETOWEGO

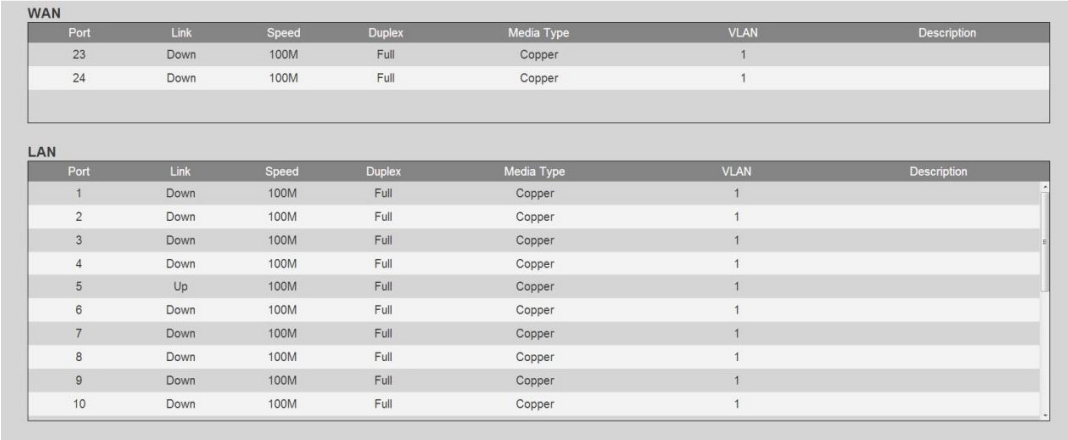


Rysunek 3-4

Jak pokazano na rysunku 3-4, cały interfejs zarządzania WEB jest podzielony na kilka części, które zawierają sekcję wyświetlania informacji o urządzeniu, pasek nawigacji, sekcję konfiguracji itp.

3.2.1 SEKCJA WYŚWIETLANIA INFORMACJI O PORCIE

Na rysunku 3-5 pokazano, że wyświetlanie informacji o porcie jest podzielone na stan portu WAN i stan portu LAN. Jest w stanie wyświetlić aktualny stan łącza portu, prędkość portu, tryb dupleksu i tak dalej.



WAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
23	Down	100M	Full	Copper	1	
24	Down	100M	Full	Copper	1	

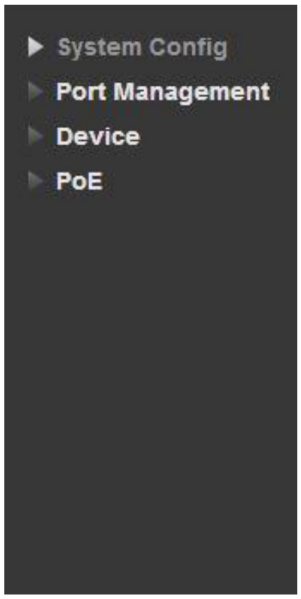
LAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
1	Down	100M	Full	Copper	1	
2	Down	100M	Full	Copper	1	
3	Down	100M	Full	Copper	1	
4	Down	100M	Full	Copper	1	
5	Up	100M	Full	Copper	1	
6	Down	100M	Full	Copper	1	
7	Down	100M	Full	Copper	1	
8	Down	100M	Full	Copper	1	
9	Down	100M	Full	Copper	1	
10	Down	100M	Full	Copper	1	

Rysunek 3-5

3.2.2 PASEK NAWIGACJI

Pasek nawigacji kontroluje, co jest wyświetlane w sekcji konfiguracji. Zawartość paska nawigacji jest wyświetlana w formie listy i podzielona według kategorii. W razie potrzeby najpierw kliknij nazwę grupy, jeżeli potrzebujesz skonfigurować jakąś pozycję, kliknij pozycje podrzędne po rozwinięciu listy. Na przykład, najpierw kliknij Zarządzanie portami, jeśli chcesz sprawdzić przepływ bieżącego portu, a następnie kliknij Statystyki portu, patrz rys 3-6 po więcej szczegółów.



Rysunek 3-6

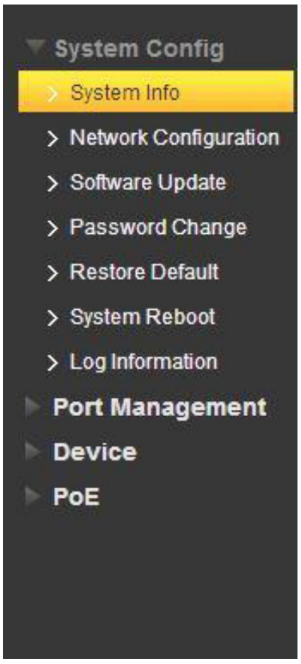
3.2.3 KONFIGURACJA SEKCJI WYŚWIETLANIA

Sekcja konfiguracji wyświetli zawartość wybraną z paska nawigacji i można ją sprawdzić, a konfigurację zmodyfikować w sekcji konfiguracji. Cztery moduły konfiguracyjne zostaną wprowadzone w kolejnych czterech rozdziałach, które obejmują konfigurację systemu, zarządzanie portami, zarządzanie urządzeniami i PoE.

4. KONFIGURACJA SYSTEMU

4.1 PRZEGLĄD KONFIGURACJI SYSTEMU

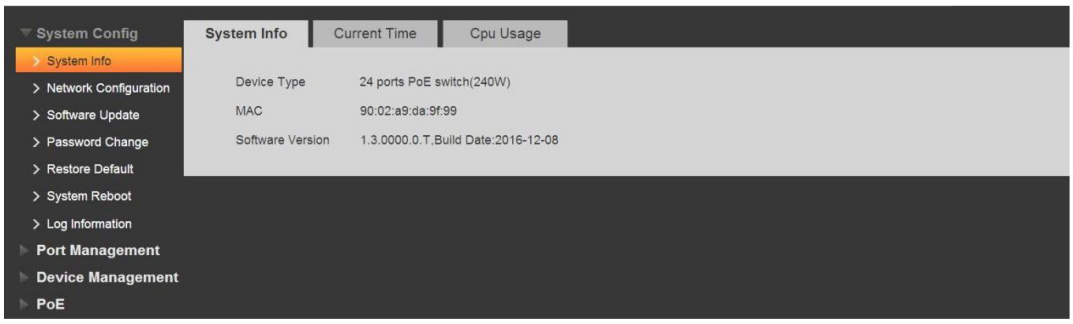
Kliknij informacje o systemie, aby zobaczyć, co pokazano na rysunku 4-1.



Rysunek 4-1

4.1.1 INFORMACJA O SYSTEMIE

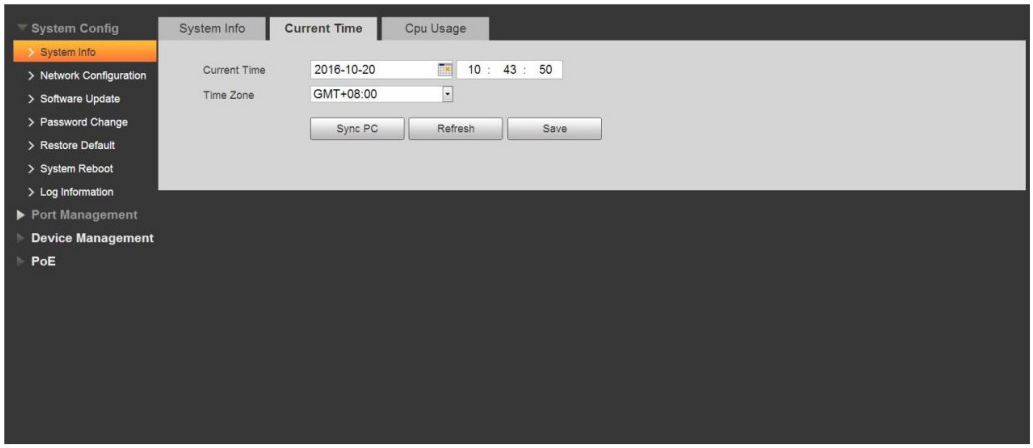
Na rysunku 4-2 przedstawiono interfejs wyświetlania informacji o systemie przełącznika, na którym można wyszukać model urządzenia, adres MAC i wersję oprogramowania.



Rysunek 4-2

4.1.2 OBECNY CZAS

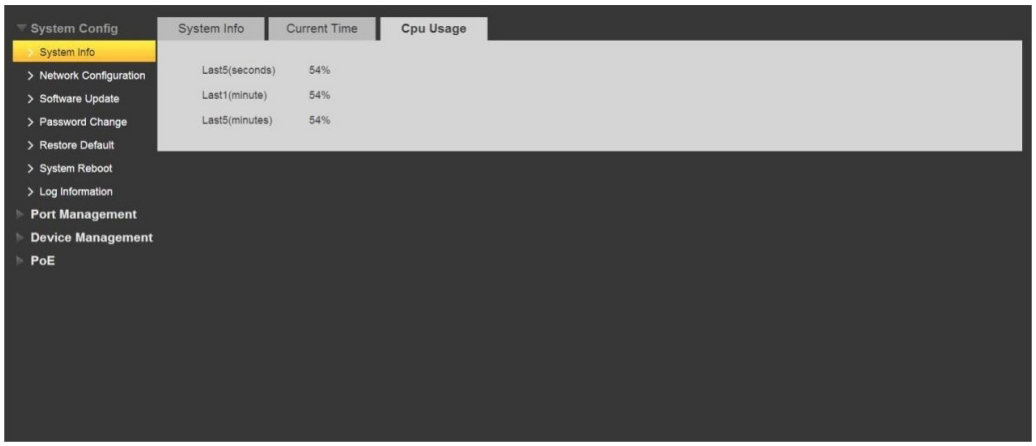
Zobacz Rysunek 4-3, aby zapoznać się z interfejsem wyświetlania czasu systemowego przełącznika, gdzie można ustawić aktualny czas i strefę czasową urządzenia.



Rysunek 4-3

4.1.3 UŻYCIE PROCESORA

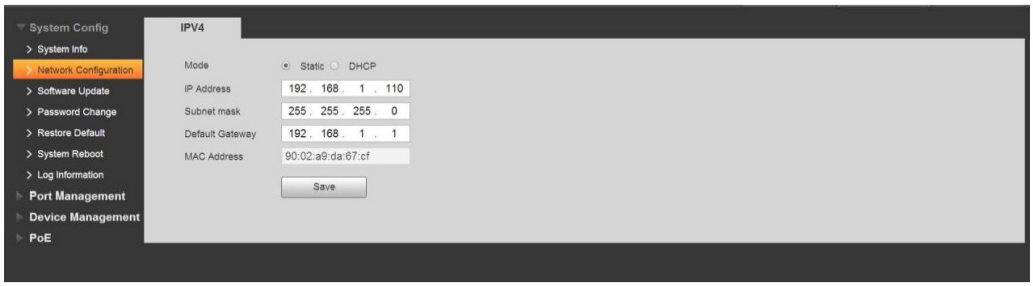
Zobacz Rysunek 4-4, aby zapoznać się z interfejsem wyświetlania użycia procesora przełącznika, gdzie można zobaczyć zużycie procesora, gdy urządzenie jest uruchomione.



Rysunek 4-4

4.2 KONFIGURACJA SIECI

Każdy host potrzebuje adresu IP do komunikacji sieciowej. Adres IP (Internet Protocol) to 32-bitowy adres używany w Internecie, jest to rodzaj jednolitego formatu adresu zapewnianego przez protokół IP, który jest zwykle wyświetlany za pomocą 4 liczb dziesiętnych. Adres IP to logiczny adres dystrybuowany dla każdej sieci i hosta w Internecie, który jest używany do identyfikacji każdego hosta i realizowania komunikacji międzysieciowej.



Rysunek 4-5

Interfejs konfiguracji IP, na którym można sprawdzić adres IP urządzenia, maskę podsieci, bramę domyślną i adres MAC, przedstawia Rysunek 4-5. Domyślny adres IP przełącznika to 192.168.1.110, który można zmodyfikować w tym interfejsie.

Konfiguracja adresu znajduje się w tabeli 4-1.

Parametr	Funkcja
Adres IP	Adres IP zarządzania przełącznikiem, który może modyfikować IP zarządzania przełącznikiem
Maska podsieci	Adres maski podsieci Przełącznika, może modyfikować konfigurację.
Brama domyślna	Zmień trasę domyślną
Adres MAC	Fizyczny adres Przełącznika, którego nie można zmienić.

Tabela 4-1

UWAGA

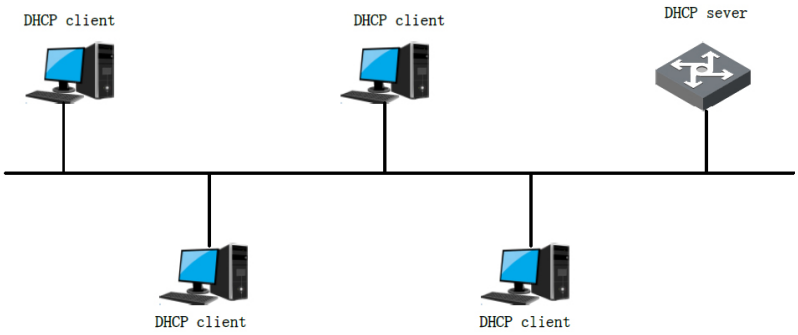
Nie należy losowo modyfikować maski podsieci przełącznika. Logowanie do przełącznika może być niemożliwe, jeśli zostanie zmodyfikowana niewłaściwie.

4.3 DHCP

Protokół DHCP (Dynamic Host Configuration Protocol) służy do dynamicznego przydzielania adresu IP i innych parametrów konfiguracji sieci dla urządzeń sieciowych.

DHCP przyjmuje tryb komunikacji klient / serwer, klient tworzy aplikację konfiguracyjną na serwerze, a serwer powraca do adresu IP i innych odpowiednich informacji konfiguracyjnych przydzielonych przez klienta, co ma na celu realizację dynamicznej konfiguracji adresu IP i tak dalej.

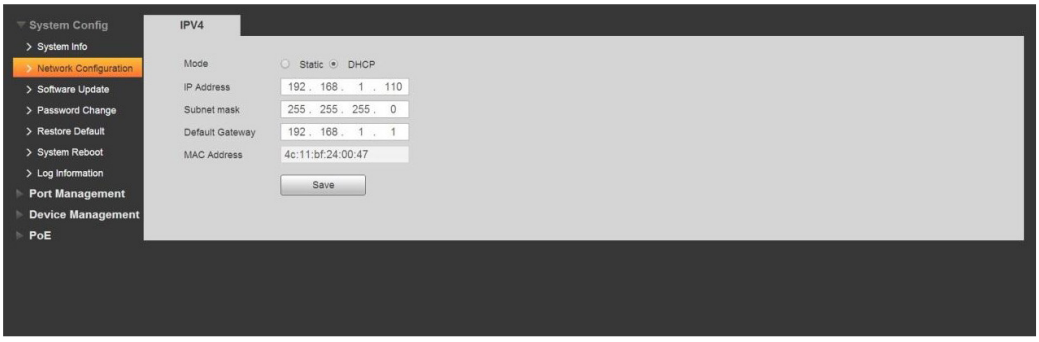
W typowym zastosowaniu DHCP zazwyczaj obejmuje jeden serwer DHCP i kilka klientów (takich jak komputer stacjonarny i laptop), co pokazano na rysunku 4-6.



Rysunek 4-6

PRZYKŁADY KONFIGURACJI

1. Wymagania dotyczące sieci:
   a) Skonfiguruj przełącznik jako klienta DHCP, automatycznie uzyskaj adres IP zarządzania przełącznikiem.
2. Kroki konfiguracji:
   a) Zaznacz „DHCP”, tak jak pokazano na Rysunku 4-7.

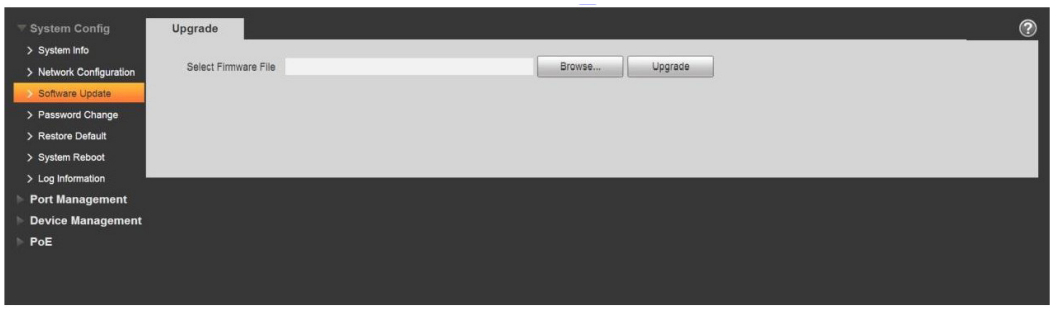


Rysunek 4-7

   b) Kliknij „Zapisz”.

4.4 AKTUALIZACJA OPROGRAMOWANIA

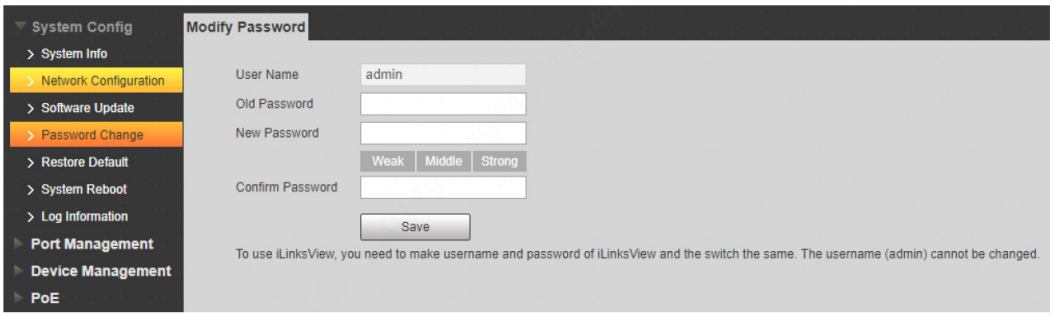
W poniższym interfejsie zapewnia funkcję aktualizacji plików systemowych przez SIEĆ dla Przełącznika. Najnowszą wersję pliku systemowego można pobrać ze strony internetowej.



Rysunek 4-8

4.5 ZMIANA HASŁA

Możesz zmienić hasło logowania użytkownika w następującym interfejsie; nazwa użytkownika to admin, której nie można modyfikować, a domyślne hasło fabryczne to admin.



Rysunek 4-9

4.6 PRZYWRÓĆ WARTOŚCI DOMYŚLNE

Możesz wybrać funkcję domyślną, gdy konieczne jest przywrócenie konfiguracji przełącznika z powrotem do początkowych ustawień domyślnych systemu. Z wyjątkiem adresu IP zarządzania i hasła logowania, wszystkie inne informacje zostaną przywrócone do domyślnych ustawień fabrycznych.

UWAGA

Gdy przełącznik zostanie zresetowany przez naciśnięcie przycisku resetowania, wszystkie konfiguracje zostaną przywrócone do domyślnych ustawień fabrycznych, adres zarządzania zostanie przywrócony do 192.168.1.110, a użytkownik będzie musiał zmienić hasło przy pierwszym logowaniu.

Rysunek 4-10

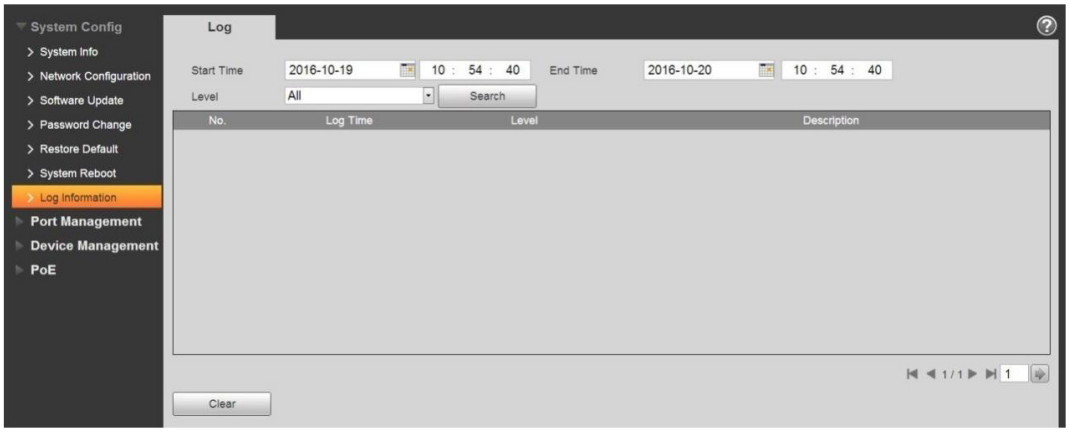
4.7 RESTART SYSTEMU

Należy zapisać konfigurację przed ponownym uruchomieniem urządzenia. W przeciwnym razie wszystkie konfiguracje zostaną utracone po ponownym uruchomieniu. Musisz ponownie zalogować się do interfejsu sieciowego urządzenia po ponownym uruchomieniu urządzenia.

Rysunek 4-11

4.8 INFORMACJE DZIENNIKA

Zobacz Rysunek 4-12, aby zapoznać się z interfejsem wyświetlania dziennika systemowego, w którym można sprawdzić niektóre informacje dziennika systemowego podczas pracy urządzenia, co ma ułatwić personelowi konserwacyjnemu analizę problemów.



Rysunek 4-12

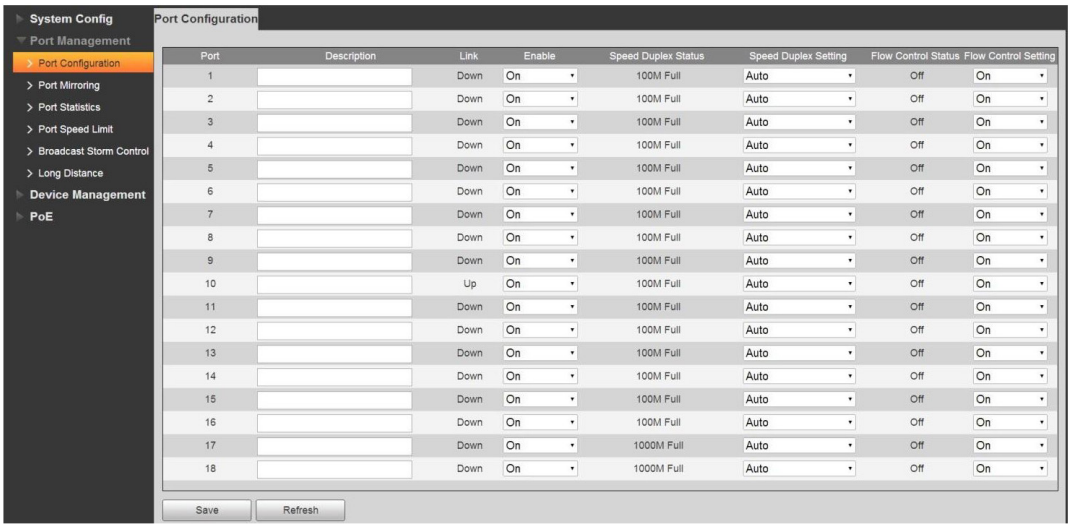
PRZYKŁAD KONFIGURACJI

1. Skonfiguruj „Czas Rozpoczęcia” i „Czas Zakończenia”, ustaw okres, który ma zostać przeszukany.
2. Wybierz poziom zdarzenia, w tym błąd, ostrzeżenie i informacje.
3. Kliknij „Wyszukaj”.

5. ZARZĄDZANIE PORTAMI

5.1 KONFIGURACJA PORTU

Konfiguracji portu można użyć do skonfigurowania każdego podstawowego parametru związanego z portem przełącznika. Podstawowy parametr portu będzie miał bezpośredni wpływ na tryb pracy portu, skonfiguruj zgodnie z praktycznymi wymaganiami.



Rysunek 5-1

Interfejs konfiguracji portu przełącznika przedstawia rysunek 5-1, w tym interfejsie można sprawdzić opis, stan łącza, stan szybkości dupleksu, stan kontroli przepływu każdego portu, można również dodać informacje o opisie portu, skonfigurować stan włączenia i wyłączenia , prędkość, tryb dupleksu i funkcję kontroli przepływu każdego portu.

- Port: Wyświetla numer portu przełącznika;
- Opis portu: dodaje informacje o opisie portu;
- Włącz: Służy do konfiguracji włączania / wyłączania portu.

W tabeli 5-1 przedstawiono konfigurację statusu portu.

Status	Funkcja
On	Łącze do konfiguracji jest włączone
Off	Łącze do konfiguracji jest wyłączone.

Tabela 5-1

- Łącze do konfiguracji jest włączone

Aby uzyskać informacje o wyświetlaniu stanu portu, zobacz tabelę 5-2.

Status	Funkcja
Góra	Oznacza to, że łącze ma status „włączony”.
Dół	Oznacza to, że łącze ma status „wyłączony”

Tabela 5-2

• Prędkość - aktualna: Wyświetla aktualny stan prędkości portu.

W tabeli 5-3 przedstawiono wyświetlanie dupleksowe szybkości portu.

Port	Obecna prędkość	Tryb szybkiego dupleksu
Port Ethernet	Auto (domyślnie)	Tryb automatycznej negocjacji
	10M Pełny	10M Pełny dupleks
	10M pół	10M Półdupleks
	100M Pełny	100M Pełny dupleks
	100M pół	100M Półdupleks
	1000M Pełny	1000M Pełny dupleks
Port światłowodowy	10000M-X	1000M Pełny dupleks

Tabela 5-3

• Prędkość –konfig: służy do konfigurowania trybu portu dupleksu szybkości.

UWAGA

Wpłynie to bezpośrednio na komunikację portu, jeśli zmienisz tryb dupleksu szybkości portu; więc modyfikuj ten parametr ostrożnie.

W tabeli 5-4 przedstawiono konfigurację portu dupleksu szybkości.

Port	Tryb prędkości	Definicja
Port Ethernet	Auto (domyślnie)	Samodostosowanie się szybkości portu w trybie dupleksu
	10M Pełny	Tryb dupleksu prędkości portu 10 M pełny dupleks
	10M pół	Tryb dupleksu szybkości portu 10 M pół dupleks
	100M Pełny	Tryb dupleksu szybkości portu 100 M pół dupleksu
	100M pół	Tryb dupleksu prędkości portu 100 M pełny dupleks
	1000M Pełny	Tryb dupleksu prędkości portu 1000 M pełny dupleks
Port światłowodowy	10000M-X	Port światłowodowy jest ustawiony na tryb pełnego dupleksu 1000M

Tabela 5-4

• Kontrola przepływu: Służy do ustawienia funkcji kontroli przepływu. Domyślna konfiguracja jest włączona).

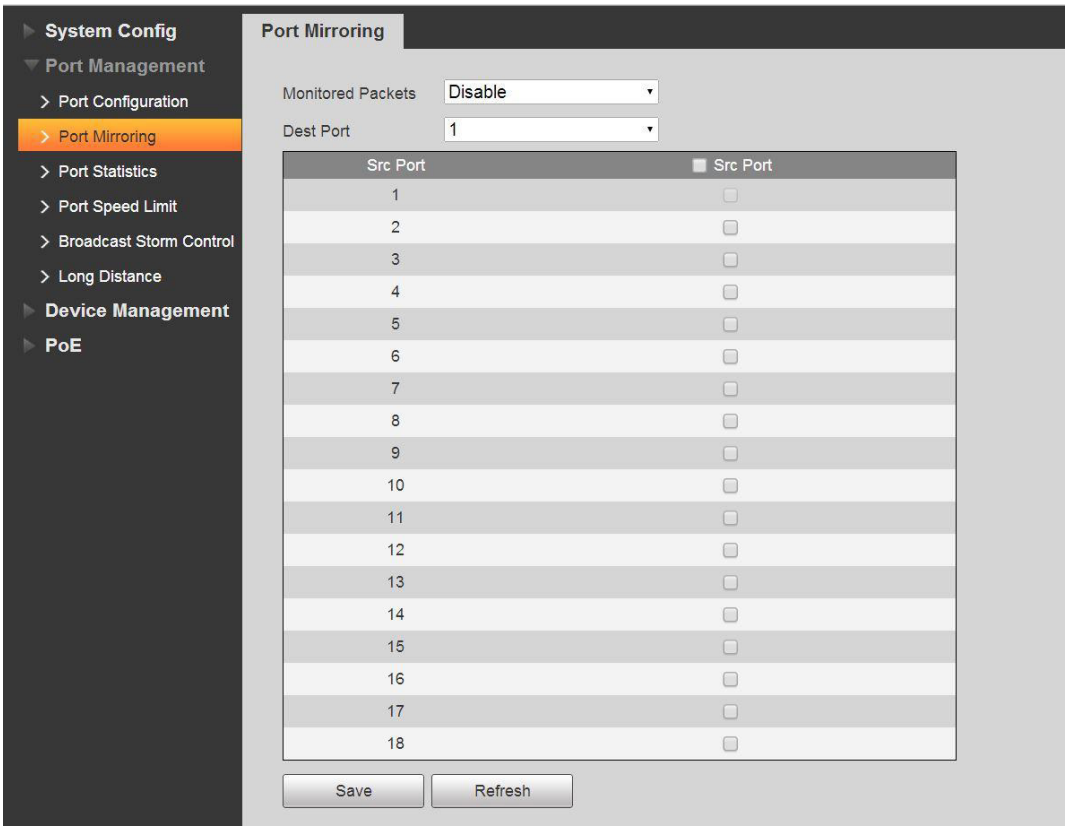
W interfejsie sterowania przepływem w porcie, "on" służy do włączania funkcji sterowania przepływem w porcie, a ramki pauzy mogą być wysyłane lub odbierane normalnie, natomiast "off" służy do wyłączania funkcji sterowania przepływem w porcie.

UWAGA

W przypadku portu Ethernet należy włączyć funkcję kontroli przepływu portów, aby zsynchronizować prędkość przychodzącą i wychodzącą w przypadku utraty pakietów wynikającej z różnych prędkości.

5.2 DUBLOWANIE PORTÓW

Dublowanie portów (zwane monitorem portu) to proces kopiowania pakietu przechodzącego przez port lub kilka portów (nazywanych portem źródłowym) do innego portu (nazywanego portem docelowym) połączonego z urządzeniem monitorującym w celu analizy pakietów. Służy on do monitorowania sieci i rozwiązywania problemów z siecią. Patrz rysunek 5-2.



Rysunek 5-2

- Port docelowy: port monitora. Wybierz tylko jedną pozycję. Domyślna konfiguracja jest wyłączona.
- Port źródłowy: monitorowany port. Wybierz co najmniej jeden element (y).
- Włącz kopię lustrzaną: dostępne są cztery tryby: Wyłącz, Tylko Tx, Tylko Rx, Włącz.

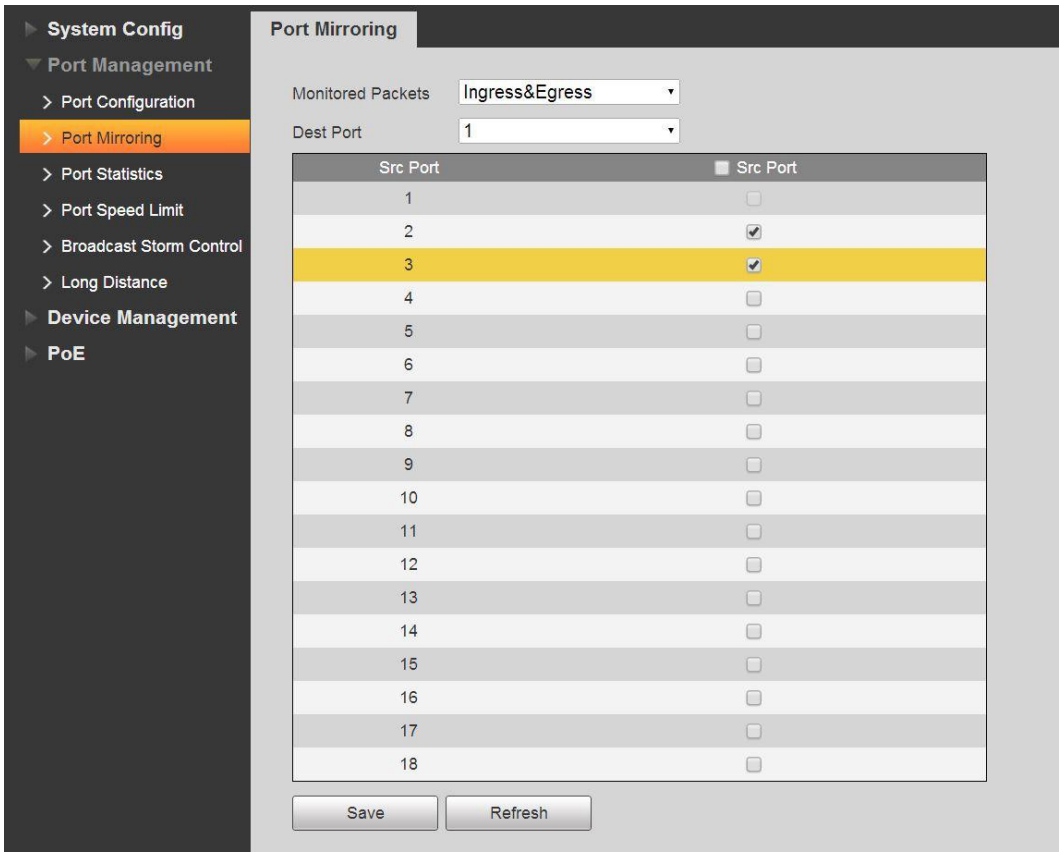
Informacje na temat konfiguracji funkcji dublowania portów znajdują się w tabeli 5-5.

Nazwa	Funkcje	
Pakiety lustrzane	Wyłącz (domyślne)	Wyłącz funkcję monitorowania
	Tylko nadawanie	Monitoruj pakiety wyjściowe
	Tylko odbieranie	Monitoruj pakiety wejściowe
	Włącz	Monitoruj pakiety wejścia / wyjścia
Port Docelowy	Port monitora. Wybierz tylko jedną pozycję. Domyślna konfiguracja jest wyłączona.	
Port źródłowy	Monitorowany port. Wybierz co najmniej jeden element (y).	

Tabela 5-4

PRZYKŁADY KONFIGURACJI

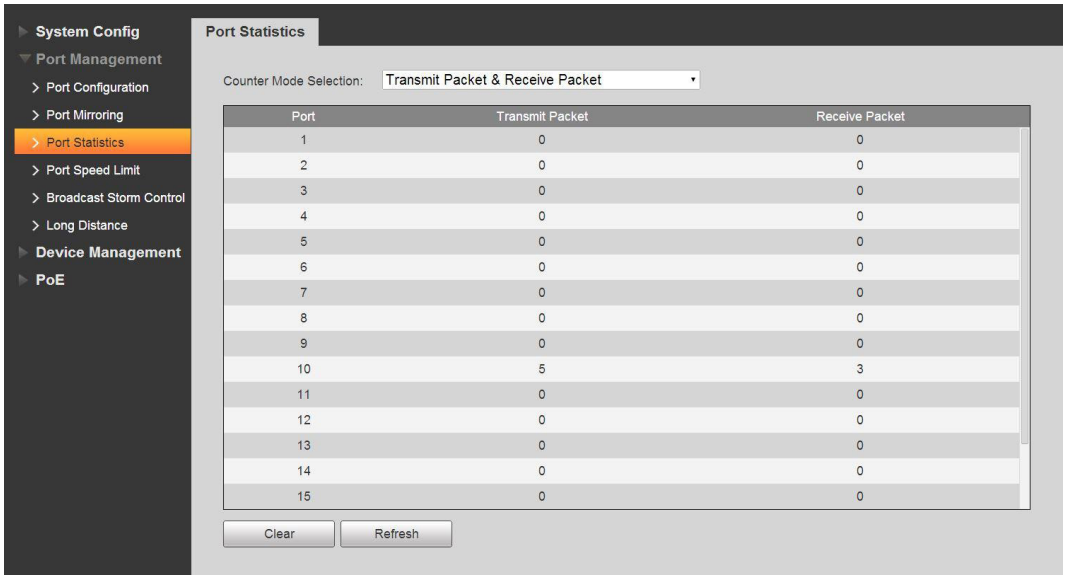
1. Połączenie internetowe
   a) Włącz funkcję dublowania portów, aby port 1 mógł monitorować pakiety portów 2 i 3.
2. Ustawienia
   a) Włącz funkcję dublowania portów i wybierz strumienie danych do monitorowania.
   b) Wybierz port źródłowy.
   c) Wybierz port docelowy. Teraz interfejs jest pokazany na rysunku 5-3.



Rysunek 5-3

5.3 STATYSTYKI PORTÓW

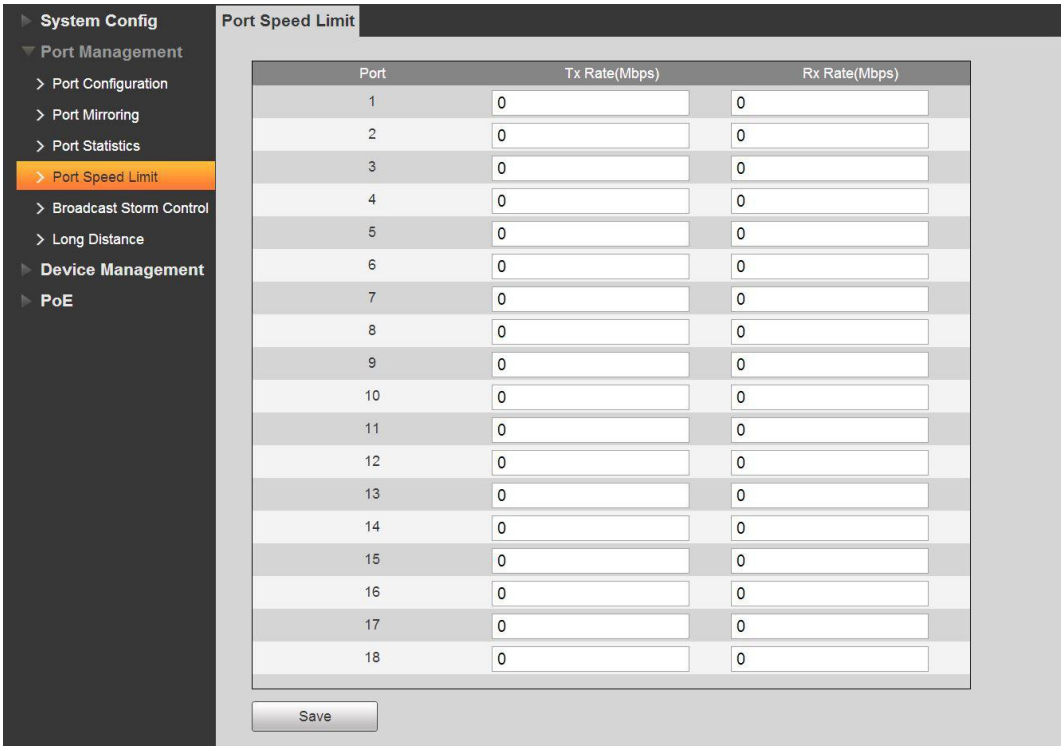
Rysunek 5-4 przedstawia interfejs statystyk portu przełącznika. Tutaj wyświetla się ilość pakietów przychodzących / wychodzących każdego portu, statystyki konfliktów, ilość utraconych pakietów, pakiet błędów CRC itp. Wydajność pracy portu jest niska, jeśli liczba błędnych pakietów jest zbyt duża, sprawdź połączenie kabla portu lub potwierdź, czy odpowiedni port przeciwny ma problem, czy nie.



Rysunek 5-4

5.4 OGRANICZENIE PRĘDKOŚCI PORTU

Tutaj można ustawić parametry ograniczenia prędkości portu, ograniczyć szybkość wymiany przychodzących / wychodzących pakietów danych. Patrz rysunek 5-5.



Rysunek 5-5

Zobacz Rysunek 5-5, aby ustawić politykę ograniczenia prędkości dla każdego portu.

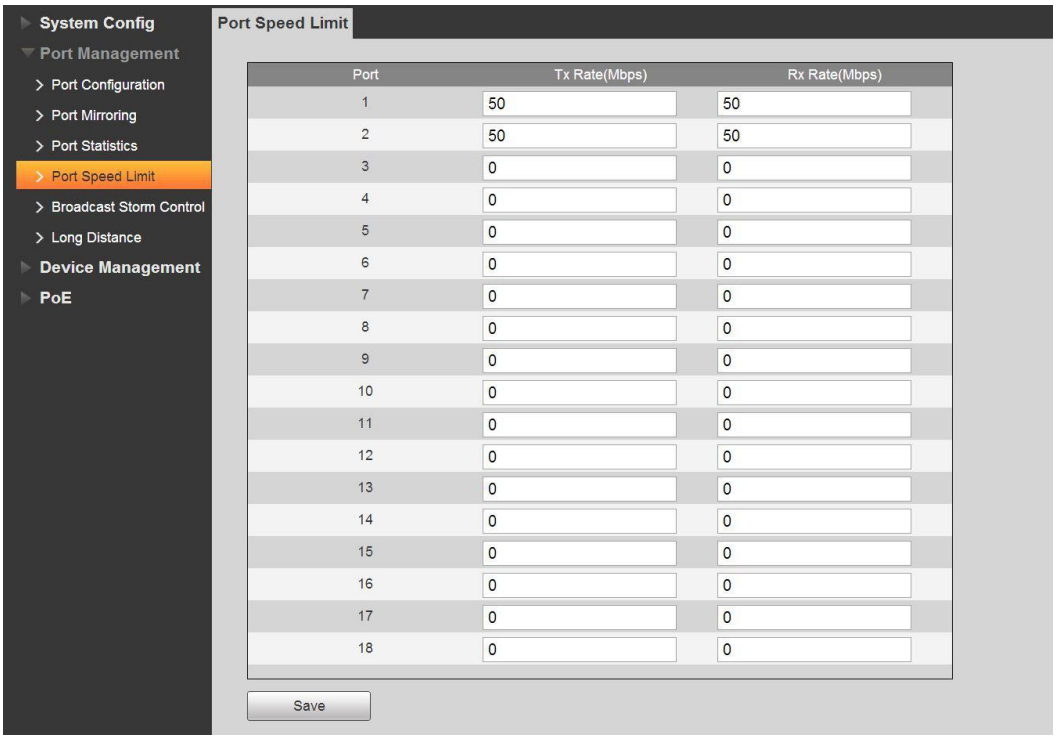
Aby zapoznać się z parametrami ograniczenia szybkości portu, patrz Tabela 5-6.

Nazwa	Funkcja
Port	Służy do ustawiania szybkości ruchu wychodzącego portu. Zakres wartości wynosi od 0 do 63 Mb / s. Domyślna konfiguracja to 0, nie ma ograniczenia prędkości.
Szybkość transmisji	Oznacza to, że łącze ma status „wyłączony”
Szybkość odbioru	Służy do ustawiania szybkości ruchu przychodzącego do portu. Zakres wartości wynosi od 0 do 63 Mb / s. Domyślna konfiguracja to 0, nie ma ograniczenia prędkości.

Tabela 5-6

PRZYKŁADY KONFIGURACJI

1. Połączenie internetowe
   a) Ustaw limit szybkości portu 1 i portu 2. Prędkość każdego portu jest mniejsza niż 50 Mb / s.
2. Ustawienia
   a) Ustaw prędkość Tx / Rx portu. Patrz rysunek 5-6.

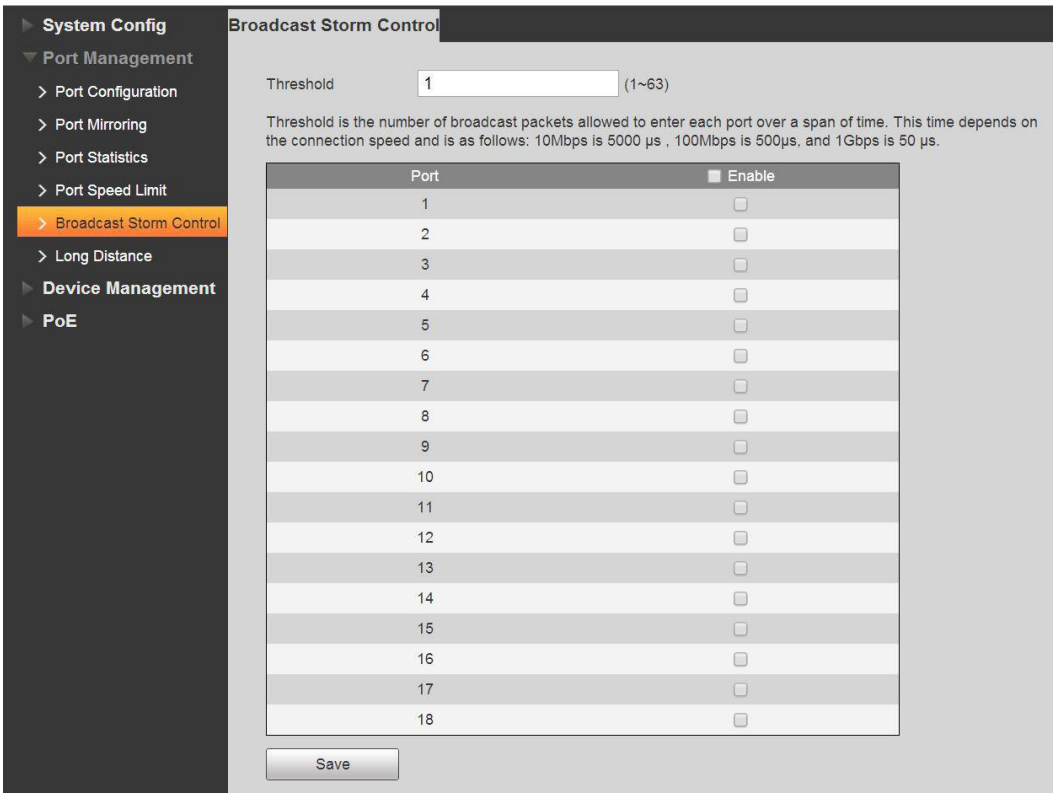


Rysunek 5-6

b) Kliknij przycisk Zapisz.

5.5 KONTROLA BURZY ROZGŁOSZENIOWEJ

Burza rozgłoszeniowa odnosi się do zjawiska: ramki rozgłoszeniowe w sieci są wielokrotnie przekazywane, co ma wpływ na prawidłową komunikację. Znacznie zmniejsza wydajność sieci. Kontrola burzy może ograniczyć przepływy rozgłoszeniowe portu i może odrzucić ramki rozgłoszeniowe, gdy przepływ przekroczy określony próg. Ma to na celu zmniejszenie ryzyka burzy rozgłoszeniowej i gwarancję prawidłowego działania sieci. Patrz rysunek 5-7.



Rysunek 5-7

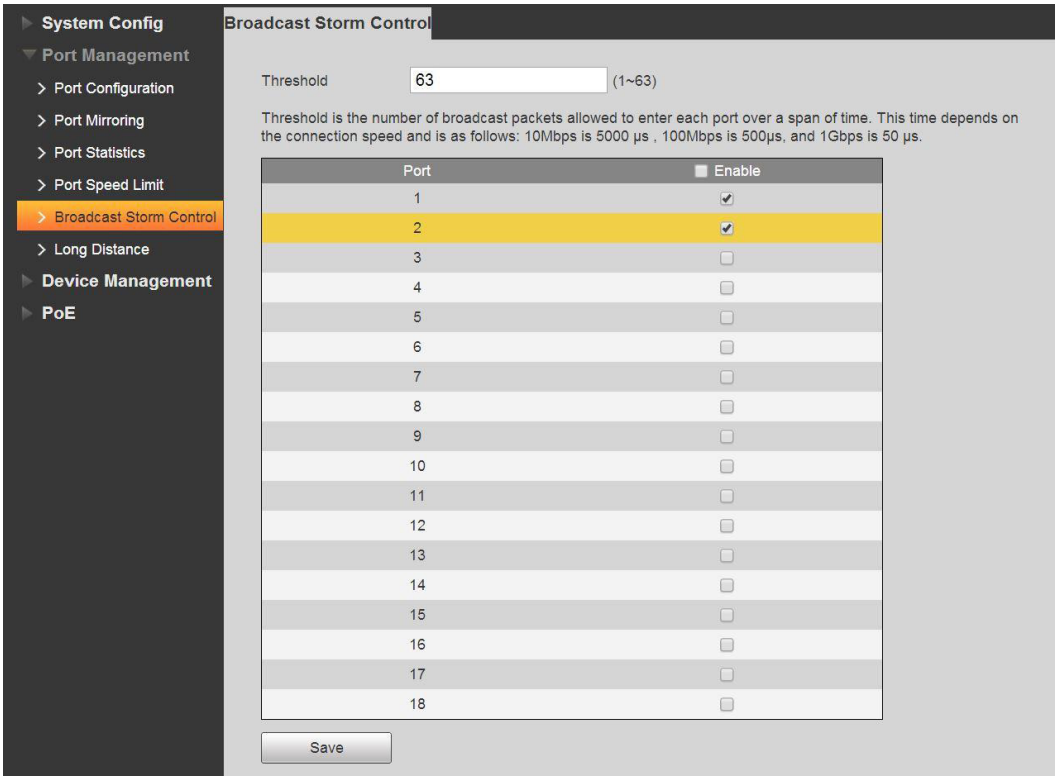
Patrz Tabela 5-7 w celu uzyskania parametrów sterowania rozgłaszaniem.

Nazwa	Funkcja
Próg	Limit pakietów rozgłoszeniowych na jednym porcie w podanym okresie.
Port	Nazwa Portu

Tabela 5-7

PRZYKŁADY KONFIGURACJI

1. Połączenie internetowe
   a) Ustaw funkcję kontroli burzy rozgłoszeniowej na wszystkich portach. W przypadku awarii, port i urządzenie nie może prawidłowo przesyłać danych, gdy jest tak dużo pakietów rozgłoszeniowych.
2. Ustawienia
   a) Ustaw wartość progową. Jest to liczba pakietów rozgłoszeniowych na jednym porcie.
   b) Wybierz port do skonfigurowania.

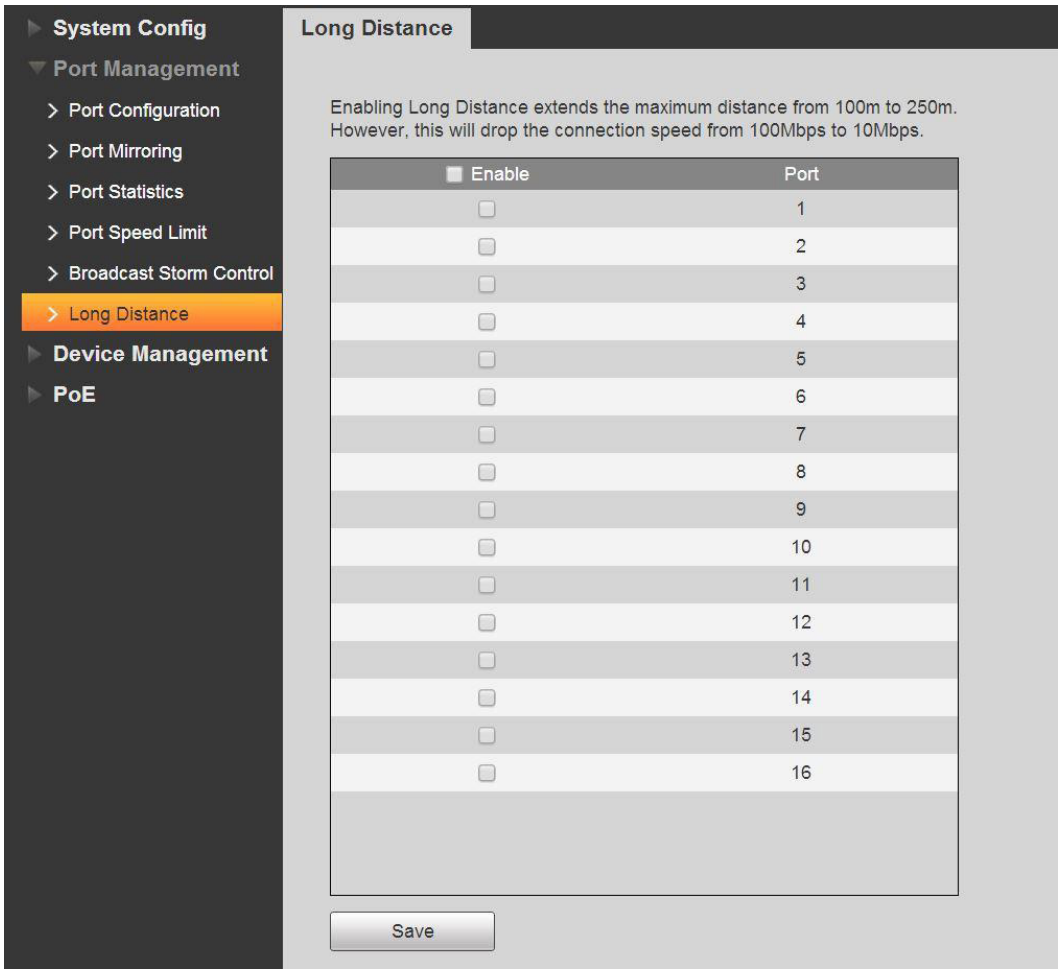


Rysunek 5-8

c) Kliknij przycisk Zapisz.

5.6 TRANSMISJA NA DUŻE ODLEGŁOŚCI

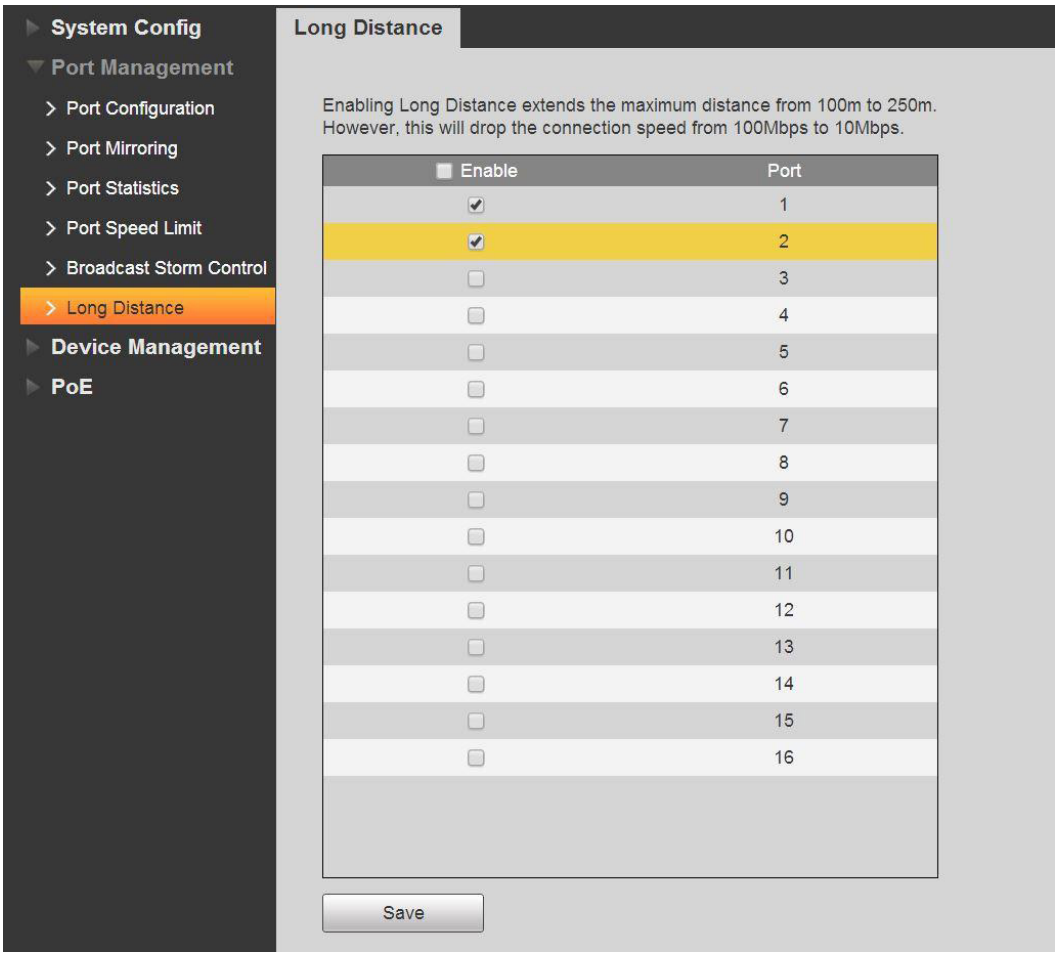
W tym interfejsie służy do ustawienia portu na tryb transmisji na duże odległości. W przypadku standardowego trybu Ethernet prędkość transmisji może wynosić 10 Mb / s / 250 metrów zamiast 100 Mb / s / 100 metrów. Patrz rysunek 5-9.



Rysunek 5-9

PRZYKŁADY KONFIGURACJI

1. Połączenie internetowe
   a) Ustaw funkcję transmisji na duże odległości na wszystkich portach, aby mogła obsługiwać prawidłową transmisję danych do 250 metrów.
2. Ustawienia
   a) Zaznacz port, aby włączyć funkcję transmisji na duże odległości.
   b) Kliknij przycisk Zapisz. Patrz rysunek 5-10.



Rysunek 5-10

6. ZARZĄDZANIE URZĄDZENIEM

6.1 SIEĆ PIERŚCIENIA

6.1.1 DEFINICJA STP

Podstawowa idea protokołu STP jest bardzo prosta. Wszyscy wiemy, że drzewa rosnące w naturze nie generują obwodu pętli, więc nie generuje obwodu pętli sieć, która rośnie jak drzewa w naturze. Dlatego definiuje most główny, port główny, wyznaczony port, koszt ścieżki i inne koncepcje w protokole STP, które mają na celu realizację celu obcinania nadmiarowego obwodu pętli poprzez strukturę drzewa, a tymczasem może realizować tworzenie kopii zapasowych łącza i optymalizację ścieżki. Algorytm strukturyzacji drzewa nazywa się algorytmem Spanning Tree.

Pakiet protokołu przyjęty przez STP to BPDU (Bridge Protocol Data Unit), który jest również nazywany informacjami o konfiguracji. Jednostka BPDU zawiera wystarczającą ilość informacji, aby zapewnić proces obliczania całego drzewa opinającego. STP może potwierdzić strukturę topologiczną sieci, przesyłając BPDU między urządzeniami. Format BPDU i opis pola mogą realizować funkcje drzewa opinającego, polega to na realizacji interakcji informacji poprzez przesyłanie pakietu BPDU między przełącznikami. Wszystkie przełączniki obsługujące protokół STP będą odbierać i obsługiwać odebrany pakiet. Pakiet zawiera wszystkie przydatne informacje w obszarze danych, które można wykorzystać do obliczenia drzewa opinającego. Format ramki BPDU i opis pól standardowego drzewa rozpinającego przedstawiono na rysunku 6-1.

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Rysunek 6-1

- Identyfikator protokołu: identyfikacja protokołu.
- Wersja: wersja protokołu.
- Typ wiadomości: typ jednostki BPDU.
- Flaga: bit flagi.
- ID ROOT: ID mostu głównego, które składa się z 2-bajtowego priorytetu i 6-bajtowego adresu MAC.
- Koszt ścieżki głównej: koszt ścieżki głównej.
- Identyfikator mostu: oznacza identyfikator mostu, który wysyła BPDU, składający się z 2-bajtowego priorytetu i 6-bajtowego adresu MAC.
- Identyfikator portu: służy do identyfikacji portu, który wysyła BPDU.
- Wiek wiadomości: czas życia BPDU
- Maksymalny wiek: czas starzenia się bieżącej jednostki BPDU, który jest najdłuższym czasem, w jakim port może zapisać jednostkę BPDU.
- Hello time: Cykl okresu, w którym Bridge Root wysyła jednostkę BPDU.
- Opóźnienie przekazywania: oznacza czas utrzymywania statusu wyszukiwania i badania przed wysłaniem pakietu danych po zmianie topologii.

6.1.2 PODSTAWOWE POJĘCIA STP

Identyfikator mostu: jest to kompleksowa wartość liczbowa priorytetu mostu i jego adresu MAC, a priorytet mostu to parametr, który można ustawić. Im niższy identyfikator mostu, tym wyższy staje się priorytet mostu, co zwiększa możliwość uzyskania przez niego statusu mostu głównego.

Root Bridge: Jest to przełącznik z minimalnym identyfikatorem mostu. Wybierz najlepszy przełącznik spośród obwodu pętli i ustaw go jako przełącznik Root Bridge, który zapewni najlepszą wydajność i niezawodność sieci.

Wyznaczony most: w każdym segmencie sieci most o najniższym koszcie ścieżki do Root Bridge stanie się wyznaczonym mostem, przez który pakiet danych zostanie przekazany do segmentu sieci. Przełącznik z najniższym identyfikatorem mostu zostanie wybrany jako wyznaczony most, gdy wszystkie przełączniki mają ten sam koszt ścieżki głównej.

Koszt ścieżki głównej: jest to suma wszystkich kosztów ścieżki na ścieżce między dwoma mostami sieciowymi Koszt ścieżki głównej mostu głównego wynosi zero.

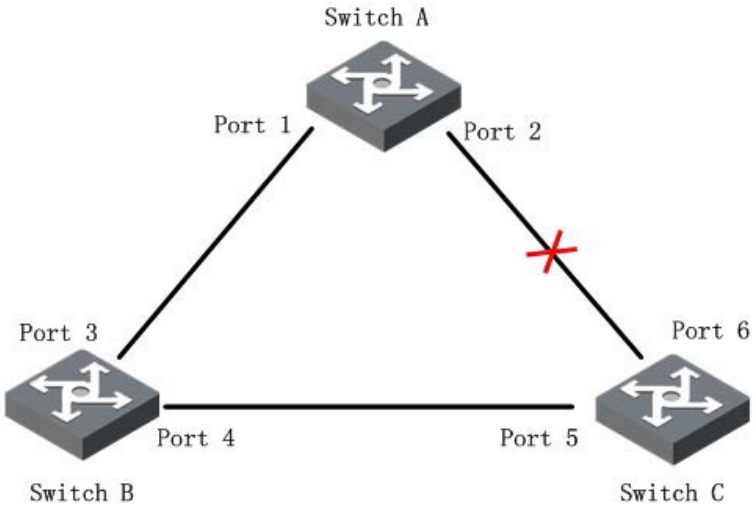
Priorytet mostu: jest to parametr, który może być ustawiany przez użytkownika, zakres liczbowy wynosi od 0 do 61440. Im mniejsza wartość zostanie ustawiona, tym wyższy ma priorytet. Im wyższy priorytet mostu, tym większe prawdopodobieństwo, że stanie się on mostem głównym.

Root Port: the nearest port to root bridge on the non-root bridge switch, responsible for communication with Root Bridge, the path cost from this port to root bridge is the lowest. Port o najwyższym priorytecie stanie się portem głównym, jeśli kilka portów ma ten sam koszt ścieżki do mostu głównego.

Wyznaczony port: jest to port na wyznaczonym moście, który realizuje przekazywanie danych do przełącznika.

Priorytet portu: zakres wartości liczbowych wynosi od 0 do 240 i musi być całkowitą wielokrotnością 16. Im niższy priorytet portu, tym wyższy priorytet i istnieje większe prawdopodobieństwo, że stanie się portem głównym.

Koszt ścieżki: protokół STP służy do wyboru wartości odniesienia łącza. Protokół STP może przypiąć sieć do struktury sieci w kształcie drzewa bez obwodu pętli, obliczając koszt ścieżki i blokując nadmiarowe łącza..



Rysunek 6-2

Schemat sieciowy podstawowej koncepcji drzewa opinającego pokazano na rysunku 6-2. Przełączniki A, B i C są połączone sekwencyjnie, przełącznik A jest wybrany jako mostek główny po obliczeniach przez STP, obwód między portem 2 i port 6 jest zablokowany.

Mostek: przełącznik A jest mostem głównym całej sieci; Przełącznik B to wyznaczony mostek przełącznika C Port: port 3 i port 5 to odpowiednio porty główne przełącznika B i przełącznika C; port 1 i port 4 to wyznaczone porty odpowiednio przełącznika A i przełącznika B; port 6 to zablokowany port przełącznika C.

Zegar STP
Czas wysyłania wiadomości Hello.
Wynosi od 1 s do 10 s. Jest to interwał, w którym Root Bridge wysyła pakiet danych BPDU do wszystkich przełączników, który jest używany do sprawdzenia, czy nie ma awarii łącza wykrywania przełącznika.

Maksymalny wiek
Waha się od 6 do 40 sekund. Przełącznik wyśle pakiet danych BPDU do wszystkich przełączników i ponownie obliczy drzewo opinające, jeśli przekroczy on czas starzenia i nie otrzyma pakietu danych BPDU wysłanego przez most główny.

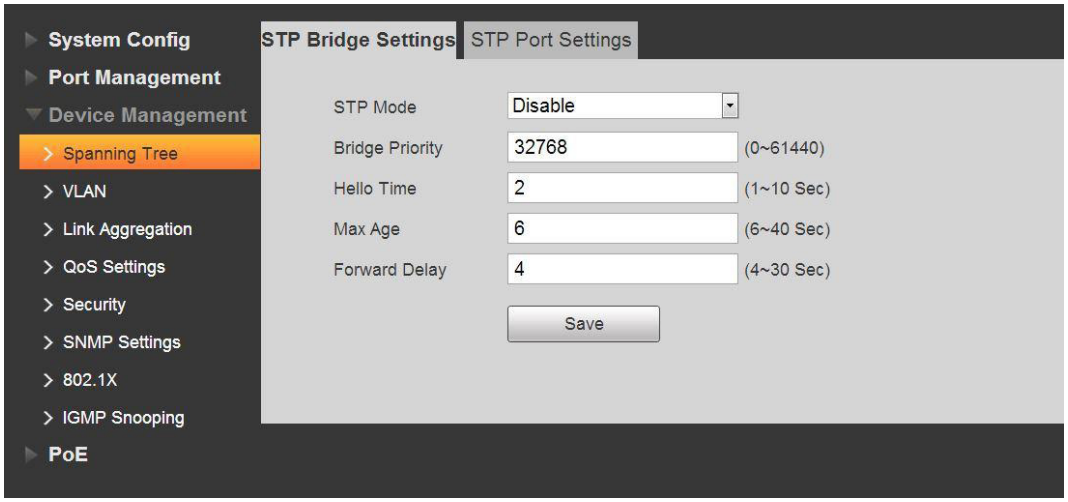
Opóźnienie do przodu
Waha się od 4 do 30 sekund. Jest to czas spędzony na zmianie stanu portu przełącznika.

Struktura drzewa opinającego wygeneruje odpowiednią zmianę po ponownym obliczeniu drzewa opinającego, co jest spowodowane awarią sieci. Jednak nowa wiadomość konfiguracyjna, która została ponownie obliczona, nie może zostać natychmiast rozpowszechniona w całej sieci, spowoduje to tymczasową pętlę, jeśli stan portu zostanie natychmiast przeniesiony. Dlatego protokół drzewa opinającego przyjmuje mechanizm zmiany stanów. Przed przekazaniem danych zarówno dla nowego portu głównego, jak i dla wyznaczonego portu, nastąpi dwukrotne opóźnienie transmisji.

UWAGA
W stanie stabilizacji topologicznej tylko port główny i port wyznaczony realizują przekazywanie danych, pozostałe porty są w stanie zablokowania, odbierają tylko pakiet BPDU, ale nie przekazują danych.

6.1.3 USTAWIENIA MOSTKA STP

Interfejs konfiguracji mostka STP pokazano na rysunku 6-3.

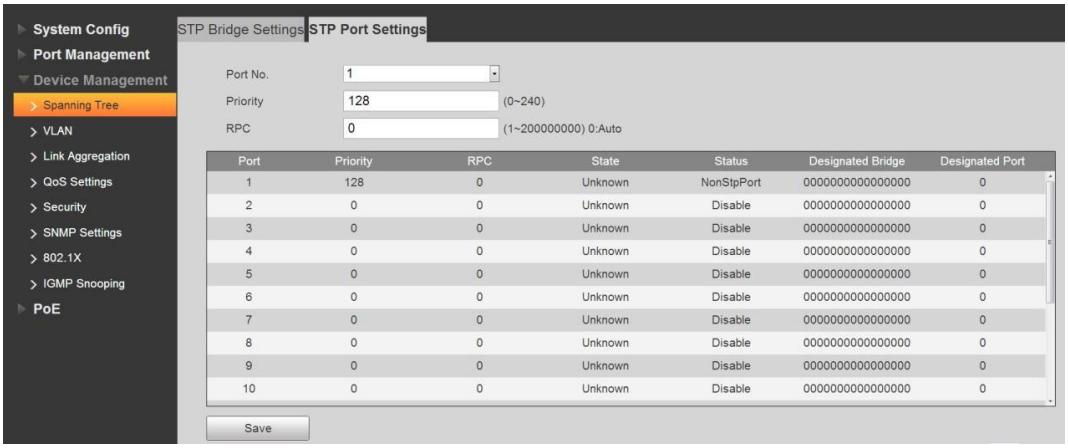


Rysunek 6-3

- Tryb STP: Włącz lub wyłącz funkcję sieci pierścieniowej.
- Priorytet mostu: ustaw priorytet mostu, w zakresie od 0 do 61440.
- Hello Time: Ustaw okres, w którym Root Bridge wysyła BPDU, w zakresie od 1 s do 10 s.
- Maksymalny Wiek: Ustaw czas starzenia bieżącego BPDU, w zakresie od 6 s do 40 s.
- Forward Delay: Po ustawieniu zmiany topologicznej most utrzymuje czas przeszukiwania i stanu badania, waha się od 4 do 30 sekund.

6.1.4 USTAWIENIA PORTU STP

Interfejs konfiguracji portu STP pokazano na rysunku 6-4.



Rysunek 6-4

- Numer Portu: Wybierz port, który chcesz skonfigurować.
- Priorytet: Skonfiguruj priorytet portu, mieści się w zakresie od 0 do 240, musi być całkowitą wielokrotnością 16.
- RPC: Skonfiguruj koszt ścieżki od bieżącego portu do mostu głównego, mieści się w zakresie 1-200000000, jest to domyślny koszt ścieżki, gdy jest ustawiony na 0.

6.2 USTAWIENIA SIECI VLAN

6.2.1 DEFINICJA SIECI VLAN

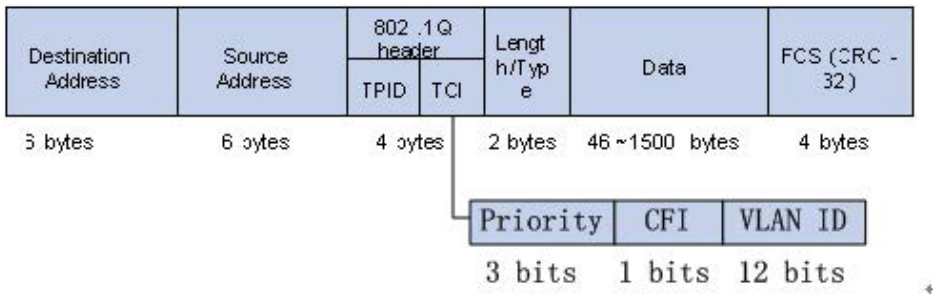
Logicznie rzecz biorąc, polega to na podzieleniu jednej sieci LAN na wiele podzbiorów. Każdy podzbiór ma swój własny obszar rozgłoszeniowy, tzw. Wirtualną sieć LAN (VLAN). Sieć VLAN jest logicznie podzielona na podstawie organizacyjnej, a nie na podstawie fizycznej, dzięki czemu realizuje izolowany obszar rozgłoszeniowy w sieci VLAN.

6.2.2 FUNKCJA VLAN

1. Zwiększenie wydajności sieci. Pakiety rozgłoszeniowe znajdują się w sieci VLAN, mogą skutecznie kontrolować burzę rozgłoszeń w sieci, zmniejszać przepustowość sieci i zwiększać możliwości procesów sieciowych
2. Zwiększenie wydajności sieci. Urządzenia w różnych sieciach VLAN nie mogą się ze sobą łączyć, a hosty w różnych sieciach VLAN nie mogą się ze sobą komunikować. Potrzebują routera lub przełącznika trójwarstwowego, aby dalej przekazać ramkę.
3. Uproszczenie zarządzania siecią. Host tej samej wirtualnej grupy roboczej nie jest ograniczony do jednego fizycznego obszaru; upraszcza zarządzanie siecią i ułatwia utworzenie grupy roboczej dla użytkowników z różnych obszarów.

6.2.3 VLAN NA PODSTAWIE PORTU

Ramki przełącznika mają ramkę znacznika i ramkę odznaczania. Patrz poniższy rysunek, aby sprawdzić położenie znacznika.



Rysunek 6-5

Untag to ogólna ramka Ethernet. Karta sieciowa komputera PC może rozpoznać ramkę, a następnie rozpocząć komunikację. W przypadku ramki znacznika dodaje 4-bajtowe informacje o sieci VLAN po źródłowym adresie mac i adresie docelowym. Jest to niebieska szyba (główka tagu VLAN) na powyższym rysunku. Zwykle karta sieciowa komputera PC nie może rozpoznać tego rodzaju ramki, przełącznik musi używać znacznika vlan, aby rozróżnić różne sieci VLAN, aby różne sieci VLAN nie mogły się ze sobą komunikować. Czasami musi komunikować się między różnymi sieciami VLAN. Tak więc istnieją różne typy portów umożliwiające komunikację sieciom VLAN. Port ma trzy typy:

- Port typu dostępu należy do jednej sieci VLAN. Zwykle łączy się z portem komputera.
- Port typu trunk umożliwia przejście kilku sieci VLAN i może odbierać lub wysyłać ramki kilku sieci VLAN. Zwykle dotyczy portów przełącznika.
- Typ hybrydowy umożliwia przejście wielu sieci VLAN i może odbierać lub wysyłać ramki kilku sieci VLAN. Służy do podłączenia przełączników i komputerów użytkowników.

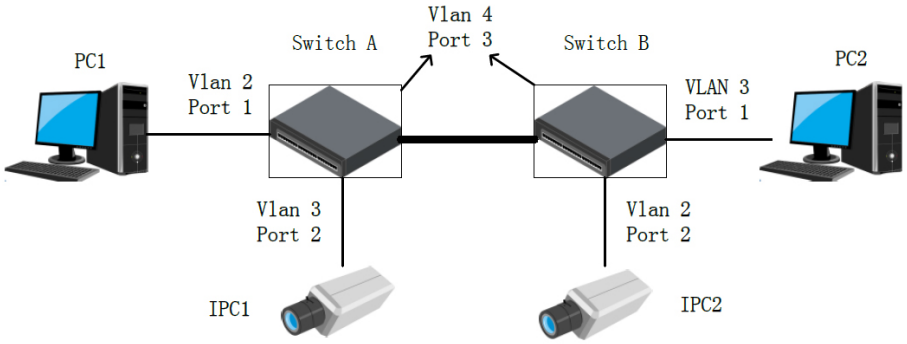
Podczas przetwarzania danych port hybrydowy i port trunk są takie same. Jedyna różnica ma miejsce przy wysyłaniu danych: port hybrydowy może wysyłać ramki z kilku sieci VLAN i bez tagu, podczas gdy port trunk może wysyłać tylko domyślną ramkę VLAN bez tagu. W tabeli 6-1 przedstawiono typ połączenia i metody przetwarzania ramek dla domyślnej sieci VLAN.

Typ Portu	Dla ramek bez tagu	Dla ramek z tagiem	Dla wysyłanych ramek
Dostęp	Odbierz ramkę i umieść tag domyślnej sieci VLAN.	Gdy identyfikator sieci VLAN jest taki sam jak domyślny identyfikator sieci VLAN, odbierz bieżącą ramkę. Jeśli identyfikator sieci VLAN różni się od domyślnego identyfikatora sieci VLAN, odrzuć ramkę.	Usuń znacznik i wyślij ramkę.
Trunk	Umieść domyślny identyfikator sieci VLAN, gdy domyślny identyfikator sieci VLAN znajduje się na akceptowanej liście, odbierz ramkę i umieść domyślny tag sieci VLAN.	Gdy identyfikator sieci VLAN znajduje się na akceptowanej liście, odbierz ramkę. Gdy identyfikator sieci VLAN znajduje się na liście zablokowanych, odrzuć ramkę.	Jeśli identyfikator sieci VLAN jest taki sam, jak domyślny identyfikator sieci VLAN i znajduje się na liście akceptowanych, usuń znacznik i wyślij ramkę.
Hybryda	Umieść domyślny identyfikator sieci VLAN, gdy domyślny identyfikator sieci VLAN znajduje się na liście zablokowanych, odrzuć ramkę.		Jeśli identyfikator sieci VLAN znajduje się na akceptowanej liście, wyślij ramkę. Użyj opcji „hybrydowy port nieotagowany / oznaczony vlan”, aby ustawić tag lub nie podczas wysyłania.

Tabela 6-1

PRZYKŁADY KONFIGURACJI

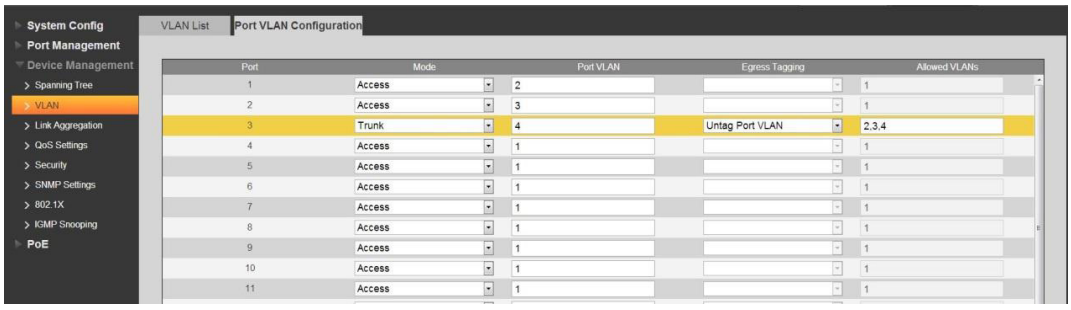
1. Połączenie internetowe
   a) PC1 i IPC2 należą do jednego działu, jeżeli PC2 i IPC1 należą do jednego działu, mogą realizować komunikację wewnętrzną w ramach działu, ale nie realizują komunikacji między działami.



Rysunek 6-6

2. Połączenie sprzętowe
   a) PC1 łączy się z portem 1 przełącznika A i należy do sieci vlan2, IPC1 łączy się z portem 2 przełącznika A i należy do sieci vlan3;
   b) PC2 łączy się z portem 1 przełącznika B i należy do sieci VLAN3, IPC2 łączy się z portem 2 przełącznika B i należy do sieci VLAN2;
   c) Port 3 przełącznika A łączy się z portem 3 przełącznika B i należy do sieci VLAN4.
3. Ustawienia
   a) Przełącznik A: Port 1 należy do sieci vlan2, skonfigurowany jako port dostępu, port 2 należy do sieci vlan3, skonfigurowany jako port dostępu, port 3 jest skonfigurowany jako port trunk i należy do sieci vlan4 i umożliwia przejście sieci vlan2, 3 i 4.
   b) Przełącznik B: Port 1 należy do sieci vlan2, skonfigurowany jako port dostępu, port 2 należy do sieci vlan3, skonfigurowany jako port dostępu, port 3 jest skonfigurowany jako port trunk i należy do sieci vlan4 i umożliwia przejście sieci VLAN2, 3 i 4.
   c) Port 3 przełącznika A łączy się z portem 3 przełącznika B i należy do sieci VLAN4.

Zobacz Rysunek 6-7.



Rysunek 6-7

6.3 AGREGACJA ŁĄCZA

Agregacja łączy polega na utworzeniu kilku fizycznych portów przełącznika w jeden port logiczny, przy czym kilka łączy należących do tej samej grupy agregacji można uznać za łącze logiczne o większej przepustowości. Agregacja łączy może realizować współdzielenie odpowiedzialności za przepływ komunikacji między każdym portem członkowskim w grupie agregacji, co ma na celu zwiększenie przepustowości. W międzyczasie można zrealizować wzajemne dynamiczne tworzenie kopii zapasowych dla każdego portu członkowskiego w tej samej grupie agregacji, co ma poprawić niezawodność łącza.

Musi istnieć określona konfiguracja dla portów członkowskich należących do tej samej grupy agregacji. Te konfiguracje obejmują STP, QoS, VLAN, właściwości portu, badanie adresu MAC, dublowanie, filtrowanie 802.1xi Mac itp.

UWAGA

Nie zaleca się implementowania konfiguracji portu i funkcji zaawansowanych dla portów używanych do agregacji łączy.
Agregację łączy można podzielić na agregację statyczną i LACP, generalnie przeciwnymi urządzeniami końcowymi agregacji łączy przełączników są przełączniki i karty sieciowe.

6.3.1 TRYB AGREGACJI STATYCZNEJ

Statyczny tryb agregacji umożliwia ręczne dodawanie kilku portów członkowskich w grupie agregacji, wszystkie porty są w stanie przekazywania i współużytkują przeciążony przepływ. Musi utworzyć grupę agregacji i dodać porty członkowskie poprzez ręczną konfigurację bez udziału pakietu protokołu LACP (Link Aggregation Control Protocol).

- Tryb równoważenia obciążenia

Istnieją trzy typy algorytmów równoważenia obciążenia dla portu, które przedstawiono w poniższej tabeli.

Tryb równoważenia obciążenia	Funkcja
Źródłowy adres MAC	Obliczanie bilansu obciążenia na podstawie źródłowego pakietu adresu MAC
Docelowy adres MAC	Obliczanie bilansu obciążenia na podstawie docelowego pakietu Adresu MAC
MAC Źródłowy i Docelowy	Obliczanie równoważenia obciążenia na podstawie źródłowego i docelowego pakietu adresu MAC

Tabela 6-2

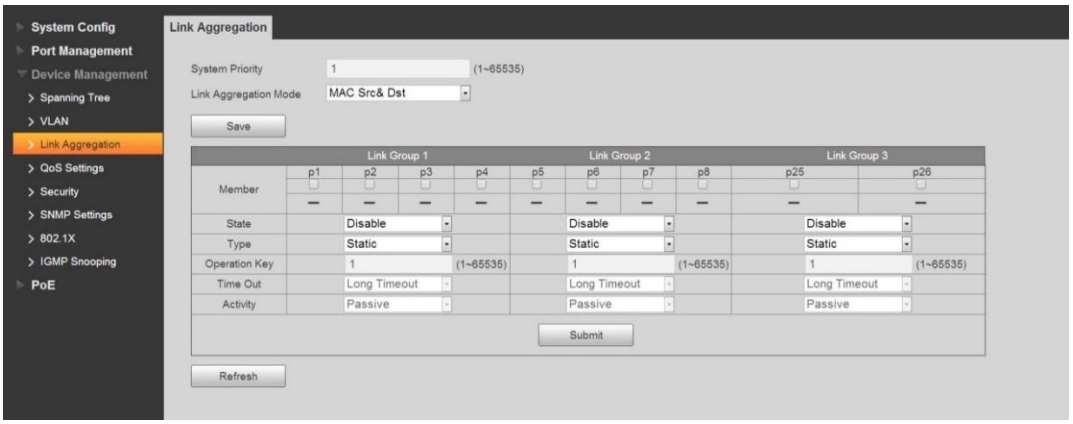
- Grupa agregacji

Jest to zespół portów Ethernet. Obsługiwana liczba grup agregacji to domyślnie trzy, których nie można modyfikować. Domyślny stan wszystkich grup agregacji to wyłączone, port członka ma domyślnie wartość zero.

- Port członkowski

Przełącznik domyślnie utworzył wszystkie grupy agregacji, a członkowie portu mają wartość zero. Najpierw należy włączyć grupę agregacji, jeśli chcesz skonfigurować porty członków dla grupy agregacji, a następnie kliknąć grupę agregacji, w której znajduje się port, aby włączyć funkcję agregacji.

Na rysunku 6-8 przedstawiono interfejs konfiguracji agregacji statycznej, który obejmuje tryb równoważenia obciążenia, grupę agregacji i członków portu.



Rysunek 6-8

6.3.2 TRYB LACP

Protokół LACP (Link Aggregation Control Protocol) służy do realizacji dynamicznej konwergencji łącza i separacji zbieżności opartej na standardzie IEEE 802.3ad. Obie strony urządzeń konwergencji łączą dopasowane łącza razem i odbierają i wysyłają dane za pośrednictwem pakietów LACPDU dokonuje interakcji informacji o konwergencji. Protokół może automatycznie dodawać i usuwać porty w grupie konwergencji, jest wyposażony w dużą elastyczność i zapewnia możliwość równoważenia obciążenia.

Po włączeniu funkcji LACP portu, port poinformuje przeciwległy koniec o priorytecie systemu, adresie MAC systemu, numerze portu o priorytecie portu i kluczu operacji (decydują o tym właściwości fizyczne, informacje o protokole wyższej warstwy i kluczu zarządzania portu).

Koniec o wysokim priorytecie urządzenia zdominuje zbieżność i separację zbieżności, o priorytecie urządzenia decyduje priorytet systemu i systemowy MAC, urządzenie o mniejszej wartości priorytetu systemu ma wyższy priorytet, urządzenie z mniejszym systemowym MAC ma wyższy priorytet, gdy wartość priorytetu systemu jest taka sama. Koniec z wyższym priorytetem urządzenia wybierze port konwergencji zgodnie z priorytetem portu, numerem portu i kluczem operacji, porty z tym samym Kluczem operacji można wybrać do tej samej grupy konwergencji, port o mniejszej wartości priorytetu portu zostanie wybrany według priorytetu w tej samej grupie konwergencji, port o mniejszym numerze zostanie wybrany, gdy priorytet portu jest taki sam. Wybrane porty połączą się w celu odbierania i wysyłania danych po interakcji obu stron z informacjami o konwergencji.

Parametr config protokołu LACP obejmuje głównie włączenie funkcji LACP portu, wartość klucza, aktywność (tryb aktywny / pasywny) i konfigurację limitu czasu.

Porty, które obsługują tylko protokół LACP, mogą realizować negocjacje LACP, a następnie mogą tworzyć łącze konwergencji. Klucz tajny jest podstawą negocjacji, a porty z tym samym kluczem tajnym mogą negocjować w celu utworzenia łącza konwergencji. Tryb negocjacji obejmuje tryb „aktywny / pasywny". Urządzenie będzie aktywnie uruchamiać łącze konwergencji, gdy wybierze opcję „aktywny"; urządzenie będzie pasywnie akceptować negocjacje zbieżności uruchomione przez inne urządzenia, gdy wybierze opcję „pasywne".

Istnieje co najmniej jeden lub dwa końce, które muszą być ustawione jako „aktywne", aby przeprowadzić udaną negocjację, gdy dwa urządzenia są połączone.

- Wartość klucza: członkowie tej samej grupy konwergencji, muszą skonfigurować ten sam klucz operacyjny, zakres od 1 do 65535
- Aktywność: domyślnie można wybrać Aktywny i pasywny, jeden koniec urządzenia, który jest zaangażowany w konwergencję dynamiczną, musi wybrać tryb Aktywny, a drugi koniec musi być skonfigurowany w trybie pasywnym;
- Limit czasu: Domyślnie jest to długi limit czasu, można wybrać długi limit czasu i krótki limit czasu;

PRZYKŁADY KONFIGURACJI

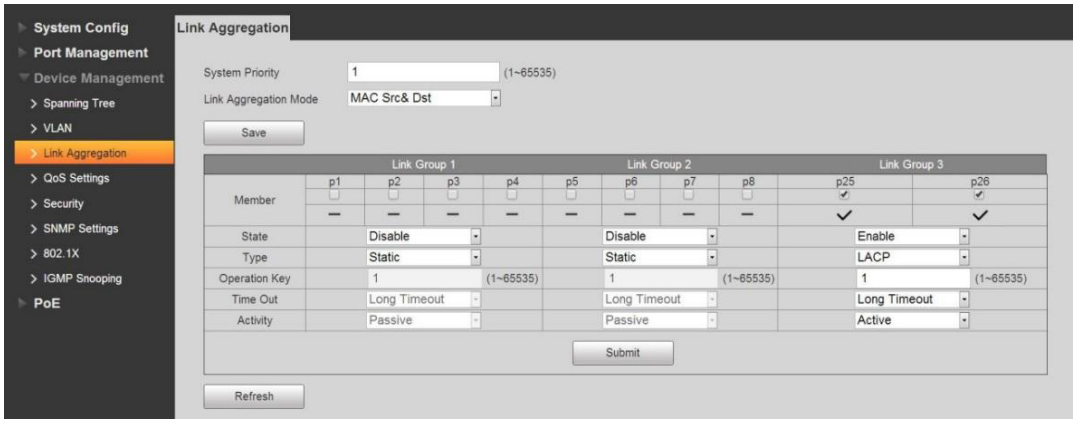
1. Wymagania Sieciowe
   a) Musi zrealizować kopię zapasową łącza i łącze w górę z podwójnym GB za pośrednictwem funkcji agregacji łączy, ponieważ istnieje ukryty problem z pojedynczym łączem GN.
2. Kroki konfiguracji

a) Wybierz grupę agregacji 3, kliknij porty 25 i 26.

b) Wybierz tryb agregacji łączy jako LACP, skonfiguruj działanie jako „Aktywność".

c) Kliknij „Prześlij", aby zastosować konfigurację

d) Wybierz tryb agregacji łącza jako „MAC Src & Dst", a wynik konfiguracji jest pokazany na Rysunku 6-10, a odpowiadające im porty, które zostały pomyślnie agregowane, wyświetlą „√".



Rysunek 6-9

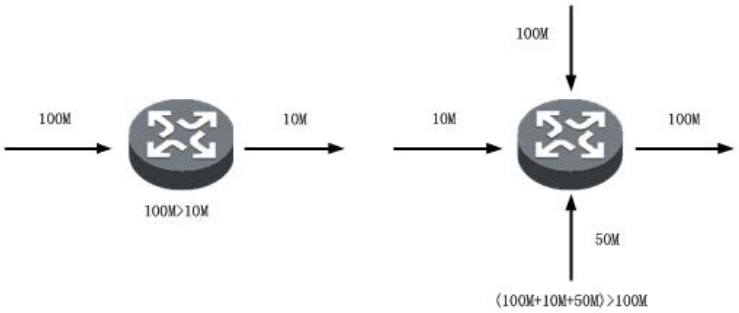
6.4 USTAWIENIA QOS

Quality of Service (QoS) odzwierciedla zdolność sieci do spełniania potrzeb klientów. W Internecie QoS ocenia zdolność sieci do przekazywania pakietów różnych usług. Ocena może opierać się na różnych kryteriach, ponieważ sieć może świadczyć różne usługi. Ogólnie rzecz biorąc, wydajność QoS jest mierzona w odniesieniu do szerokości pasma, opóźnienia, drgań i współczynnika utraty pakietów podczas procesu przekazywania pakietów. W tradycyjnej sieci IP bez QoS urządzenie traktuje wszystkie pakiety jako takie same, a zasada procesu polega na: pierwszy wchodzi, pierwszy wychodzi (FIFO). Przydziela wymagane zasoby w zależności od czasu nadejścia pakietu. Wszystkie pakiety współużytkują zasoby sieciowe i urządzenia, a zasoby, które pakiet może otrzymać, zależą od czasu jego nadejścia. Ten rodzaj usługi nazywa się Best-Effort. Wykonuje maksymalny wysiłek, aby wysłać pakiet do miejsca przeznaczenia, ale nie ma gwarancji ani pewności co do opóźnienia, jittera i współczynnika utraty pakietów podczas procesu przekazywania pakietów.

Tradycyjne zasady dotyczące najlepszych usług dotyczą WWW, usługi poczty e-mail, która nie jest wrażliwa na przepustowość ani opóźnienia. Ale teraz nowo powstający biznes wymaga wysokiego poziomu usług w sieci IP. Użytkownik chce nie tylko wysłać pakiet do miejsca docelowego, ale także cieszyć się lepszą obsługą podczas procesu przekazywania, np. Istnieje specjalna przepustowość sieci, zmniejszenie wskaźnika utraty pakietów, zarządzanie przeciążeniem sieci lub unikanie go, dostosowywanie przepływów w sieci. Wszystko to wymaga, aby sieć miała doskonałe możliwości usługowe.

6.4.1 ZATOR W SIECI

W skomplikowanych środowiskach grupujących i wymieniających się Internetem zatory są wszędzie. Patrz rysunek 6-10



Rysunek 6-10

1. Strumienie grupowe są przesyłane z połączenia o dużej szybkości do urządzenia i przesyłane dalej przez łącze o niskiej szybkości.
2. Strumienie grupowe są podłączane do urządzenia sieciowego za pośrednictwem kilku portów, a następnie przesyłane dalej przez jeden port (prędkości wielu portów wejściowych są większe niż prędkość portu wyjściowego).

Jeśli prędkość przepływu jest zbyt duża, może napotkać próg zasobów i spowodować zatory przepływu. Nie tylko przepustowość łącza ma przeciążenie, wszelkie niewystarczające zasoby miejsca przekazywania (takie jak dostępny czas procesu, bufor, zasoby pamięci są niewystarczające) mogą powodować przeciążenie. Poza tym, jeśli kontrola przepływu jest w pewnym momencie poza zakresem i nie ma wystarczających zasobów sieciowych, może to również spowodować przeciążenie sieci.
Zatory mają szereg negatywnych skutków:

- Przeciążenie zwiększa opóźnienie i fluktuację transmisji pakietu, duże opóźnienie może skutkować ponownym wysłaniem pakietu.
- Przeciążenie spowalnia przychodzące i wychodzące przepływy sieciowe i zmniejsza stopień wykorzystania zasobów sieciowych.
- Przeciążenie pochłania ogromną ilość zasobów sieciowych (zwłaszcza zasobów pamięci masowej), niewłaściwa alokacja zasobów może spowodować awarię systemu.

Widzimy więc, że przeciążenie uniemożliwia przepływom pobieranie zasobów na czas i jest to oryginalne źródło obniżające wydajność usługi. W skomplikowanych środowiskach, w których istnieje wymiana grupowa i biznes z wieloma użytkownikami, przeciążenie jest nieuniknione. Musi więc istnieć właściwy sposób radzenia sobie z zatorami.

6.4.2 ROZLICZENIE ZATORÓW

Bezpośrednią metodą rozwiązania problemu z niewystarczającymi zasobami jest dodanie przepustowości sieci. Ale przepustowość ma swoje ograniczenia, nie jest w stanie rozwiązać wszystkich problemów wynikających z przeciążenia sieci. Bardziej efektywnym sposobem rozwiązania problemu zatorów w sieci jest dodanie funkcji kontroli przepływu i alokacji zasobów w sieci. Może świadczyć różne usługi zgodnie z różnymi wymaganiami biznesowymi oraz bardziej rozsądnie przydzielać i wykorzystywać zasoby. Podczas procesu alokacji zasobów i kontroli przepływu staraj się kontrolować kierunek lub czynniki pośrednie, które mogą powodować przeciążenie sieci, co ma na celu zmniejszenie częstotliwości występowania zatorów. Kiedy występuje przeciążenie sieci, może przydzielić zasoby zgodnie z rodzajem działalności i wymaganiami, aby zredukować efekt przeciążenia do minimalnego poziomu.

6.4.3 PLANOWANIE KOLEJEK

Zwykle stosujemy planowanie kolejek, aby załatwić zarządzanie przeciążeniami. Wykorzystanie algorytmu liniowego do kategoryzacji przepływów i wykorzystanie algorytmu priorytetu do wysyłania najpierw tego rodzaju przepływów. Każdy algorytm kolejki ma na celu naprawienie oczekujących problemów z przepływem w sieci; ma duży wpływ na alokację zasobów przepustowości, opóźnienia, jitter itp.

Ta seria produktów obsługuje dwie kolejki priorytetowe: kolejkę o wysokim priorytecie i kolejkę o niskim priorytecie. Priorytet każdego pakietu jest ustalany zgodnie z następującymi czterema planami.

1. Port fizyczny.
2. Znacznik VLAN 802.1Q.
3. Ciąg TOS / DS pakietu IP.
4. Port TCP / UDP.

Gdy istnieje kilka ustawień QoS, gdy jeden priorytetowy element konfiguracji stanie się priorytetem o wysokim priorytecie, zostanie on umieszczony w wierszu o wysokim priorytecie, a następnie przekazany dalej. Gdy istnieje kilka priorytetów, np. na tym samym poziomie, adoptuje metodę First In First Out (FIFO).

6.4.4 TRYB PRIORYTETOWY

Każdy odebrany pakiet jest odwzorowywany na wysoki lub niski priorytet. Konfiguracja priorytetu pakietów ma trzy tryby. Patrz rysunek 6-11.

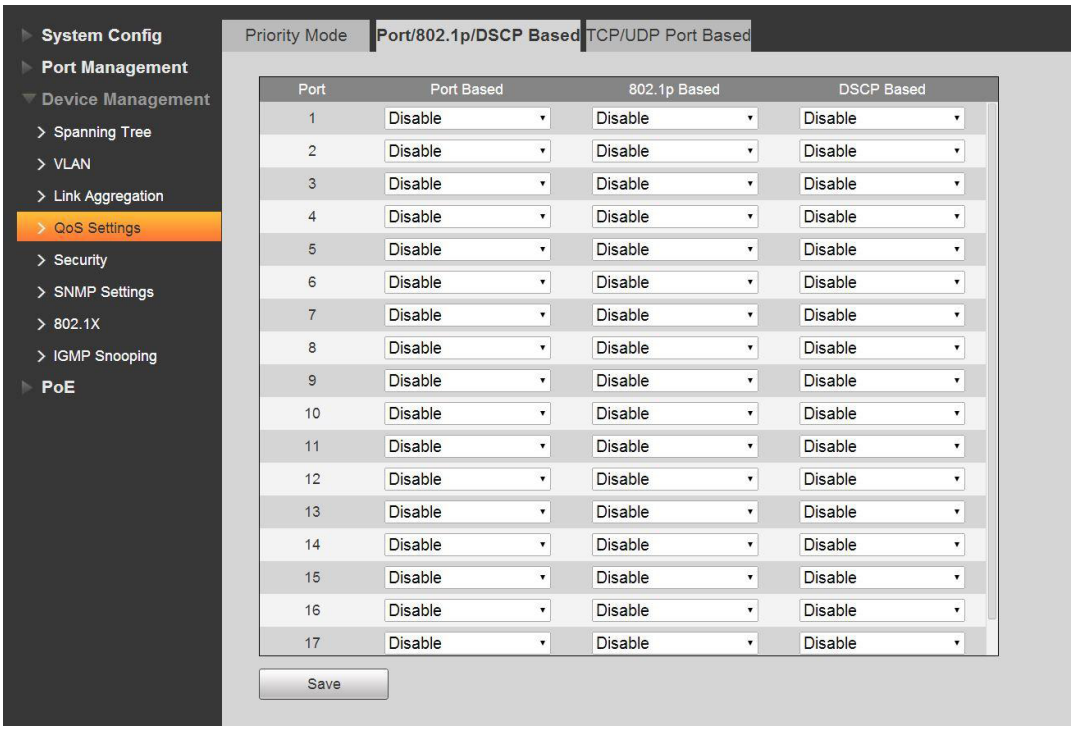
Rysunek 6-11

Informacje o trybie priorytetu zawiera Tabela 6-3

Nazwa	Funkcja
Pierwsze weszło, pierwsze wyszło (FIFO)	Pierwszy odebrany pakiet zostanie przesłany jako pierwszy. Gdy funkcja QoS jest wyłączona, urządzenie przyjmuje tryb FIFO do przetwarzania pakietów.
Wszystkie wysokie przed niskimi	Urządzenie przekazuje pakiety zgodnie z określonym priorytetem.
Działanie okrężne - Waga	Ustaw poziom wagi, aby zmienić procent przekazywania pakietów na wysoki i niski priorytet.

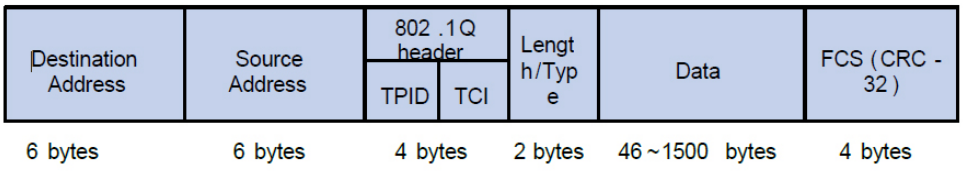
Tabela 6-3

6.4.5 QOS W OPARCIU O PORT / 802. 1P / DSCP



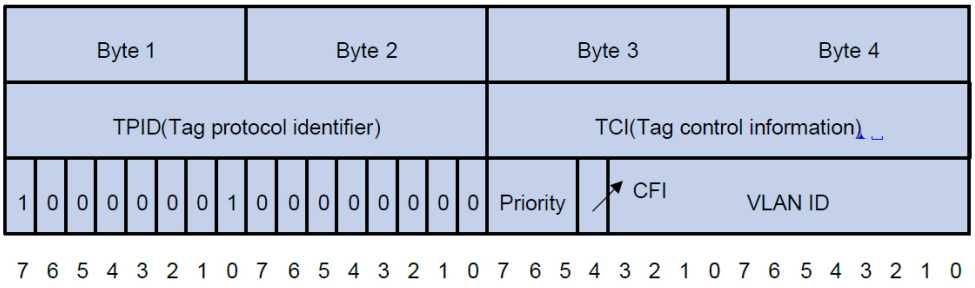
Rysunek 6-12

Bazowane na porcie.
Gdy port ma ustawiony wysoki priorytet, odebrane pakiety są umieszczane w kolejce o wysokim priorytecie. Każdy port można ustawić jako wysoki priorytet.
Oparty na standardzie 802.1p
Priorytet 802.1p znajduje się na 2-warstwowej głowicy pakietu. Przeznaczony jest do środowiska, w którym nie ma potrzeby analizowania trzeciej głowy i gwarantuje QoS w 2-warstwie.



Rysunek 6-13

Na rysunku 6-14, czterobajtowa głowica tagu 802.1Q zawiera 2-bajtowy TPI (Identyfikator protokołu tagu) i 2-bajtowy TCI (Informacje o sterowaniu znacznikiem). Wartość TPID to 0x8100. Na rysunku 6-9 przedstawia szczegółową zawartość nagłówka znacznika w standardzie 802.1Q, ciąg Priority to priorytet 802.1p. Priorytet nazywa się 802.1p, ponieważ jest zdefiniowany w specyfikacjach 802.1p.



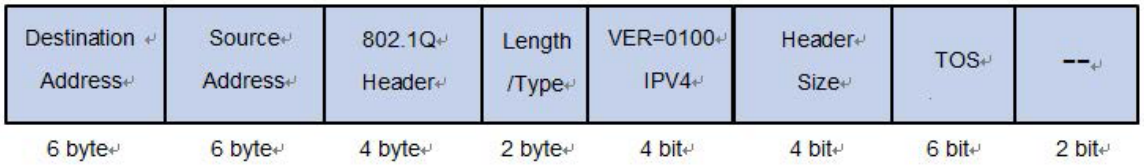
Rysunek 6-14

Aby uzyskać informacje na temat priorytetów 802.1p, patrz Tabela 6-4.

Kolejka priorytetowa	Priorytet 802.1p (System dziesiętny)	Priorytet 802.1p (System binarny)	Słowa kluczowe
Kolejka o niskim priorytecie	0	000	Najlepszy wysiłek
	1	001	Tło
	2	010	Zapasowy
	3	011	Doskonały wysiłek
Kolejka o wysokim priorytecie	4	100	Kontrolowane obciążenie
	5	101	Wideo
	6	110	Głos
	7	111	Zarządzanie siecią

Tabela 6-4

Na podstawie ciągu TOS / DS pakietu IP



Rysunek 6-15

Na rysunku 6-10 ciąg ToS nagłówka pakietu IP ma 8 bitów, RFC2474 redefiniuje domenę ToS głowy pakietu IP i nazywa się (Differentiated Services). Priorytet DSCP wykorzystuje pierwsze 6-bitowe (0-5). Zakres wartości wynosi od 0 do 63, a ostatnie 2 bity (6, 7) to zarezerwowany bit.

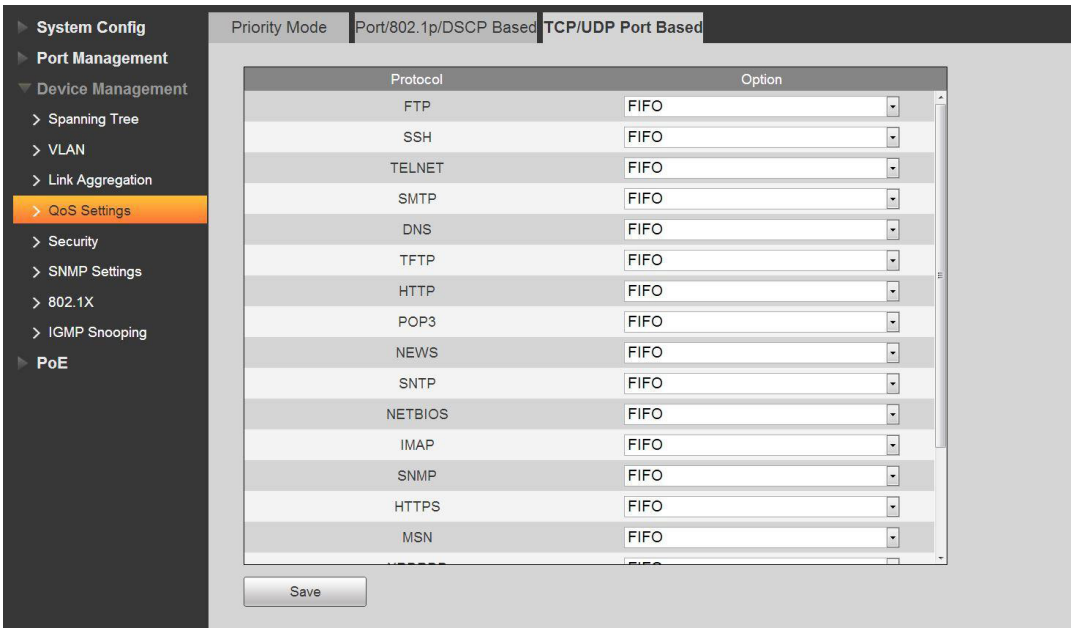
Informacje o priorytecie IP zawiera Tabela 6-5

Kolejka priorytetowa	Priorytet IP (Dziesiętny system)	Priorytet IP (System binarny)	Słowa kluczowe
Kolejka I o wysokim priorytecie	46	101110	ef
	10	001010	af11
	18	010010	af21
	26	011010	af31
	34	100010	af41
	48	110000	cs6
	56	111000	cs7
Kolejka o niskim priorytecie	Inne	xxxxxx	

Tabela 6-5

6.4.6 PORT TCP / UDP

TCP i UDP przyjmują 16-bitowy port do rozpoznawania aplikacji. Serwer zwykle używa portu do rozpoznawania. Na przykład port TCP serwera FTP to 21, port TCP każdego serwera Telnet to 23, a port UDP każdego serwera TFTP to 69. Wszystkie usługi TCP / IP korzystają z dobrze znanego portu 1-1023.

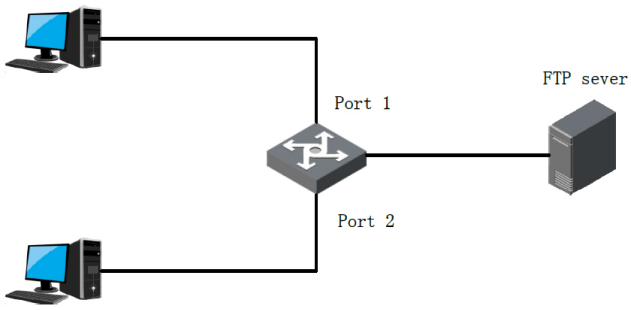


Rysunek 6-16

Na rysunku 6-11 ta seria produktów może przetwarzać odebrane pakiety w oparciu o port TCP / UDP, taki jak FTP, SSH, TELNET, SMTP i DNS. Tutaj można ustawić pakiet o wysokim priorytecie, niskim priorytecie lub odrzucenie. Domyślna konfiguracja to FIFO.

PRZYKŁADY KONFIGURACJI

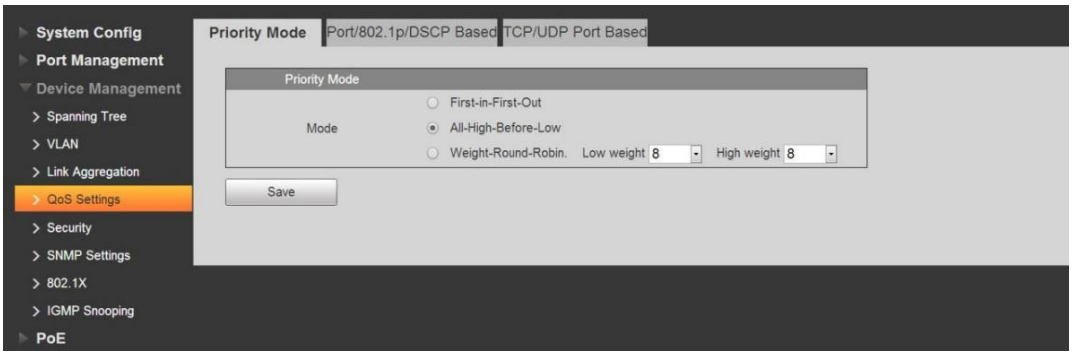
1. Połączenie sieciowe
   a) Na rysunku 6-12 podłącz urządzenie do serwera FTP i użyj portów 1 i 2 do podłączenia urządzenia.
   b) Prawidłowo ustawiona funkcja QoS, port 2 ma wyższy priorytet niż port 1 i ma zablokowany dostęp do serwera FTP.



Rysunek 6-17

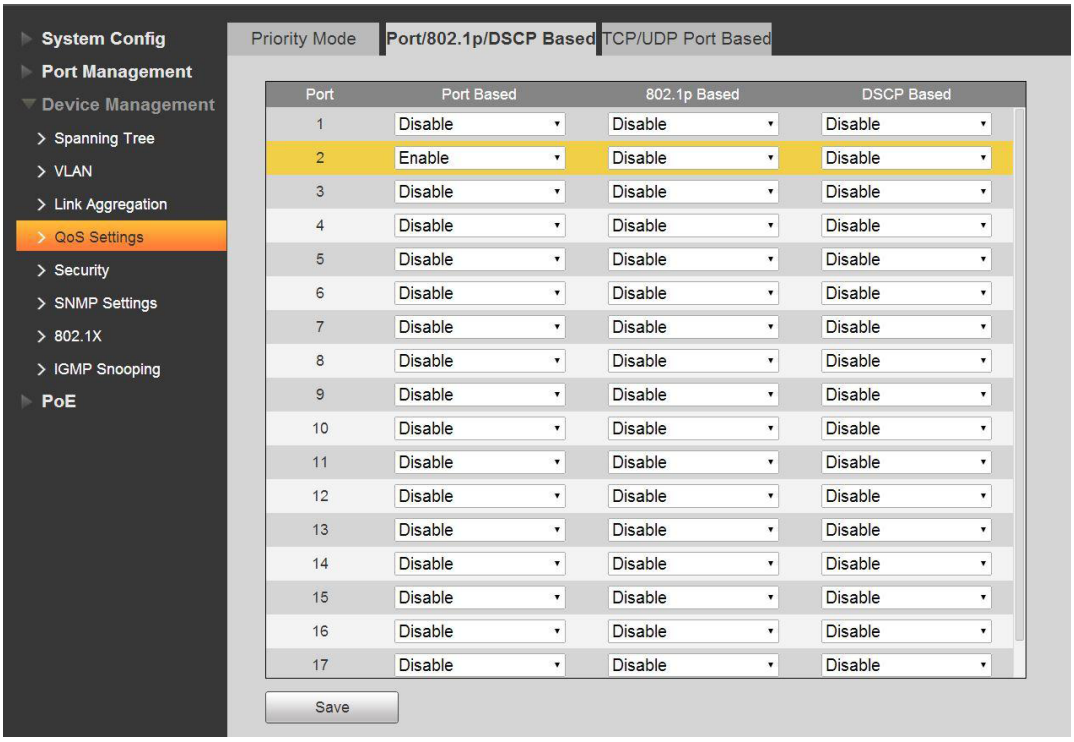
2. Ustawienia

a) Ustaw tryb urządzenia na „wszystkie wysokie przed niskimi”



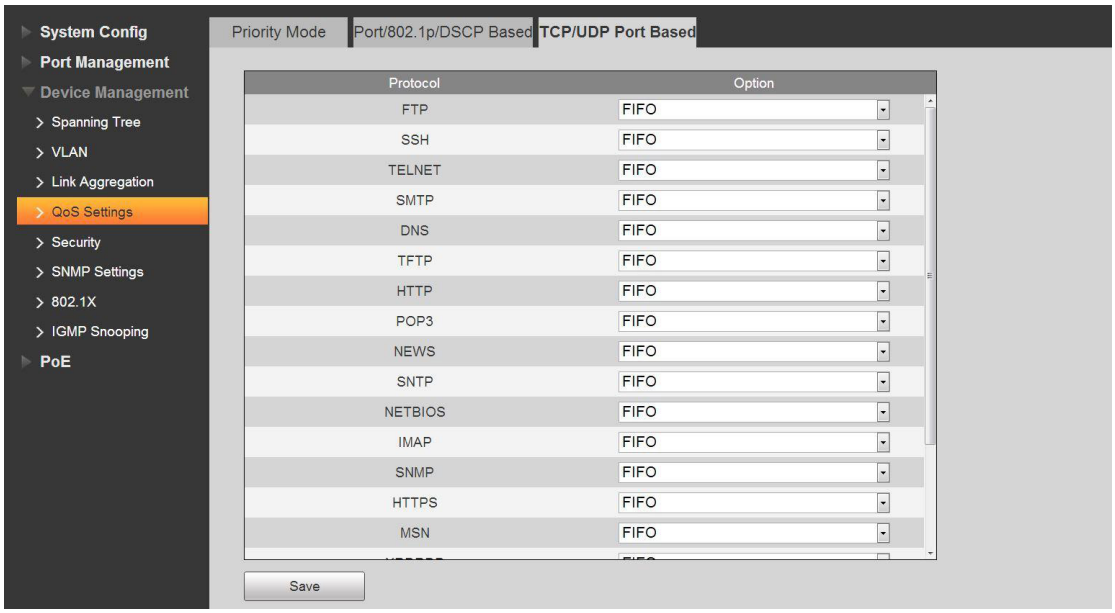
Rysunek 6-18

b) Ustaw Port 2 jako priorytetowy.



Rysunek 6-19

c) Ustaw urządzenie tak, aby odrzucało pakiet danych FTP, blokowało użytkownikowi dostęp do serwera FTP.



Rysunek 6-20

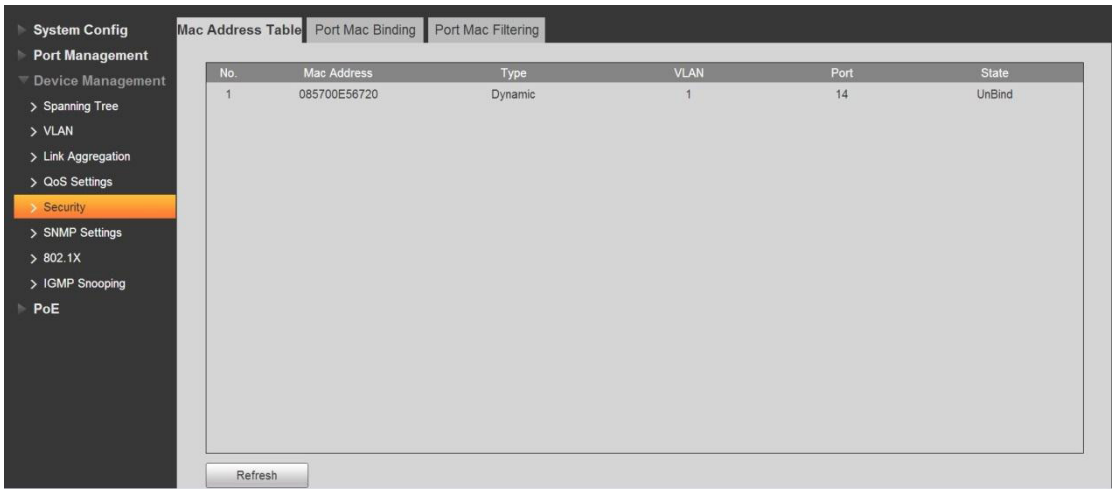
6.5 BEZPIECZEŃSTWO

MAC (Media Access Control) rejestruje związek między adresem MAC a portem oraz informacjami o przynależności do portu VLAN itp.

6.5.1 LISTA ADRESÓW MAC

Gdy urządzenie przekazuje pakiet, przeszukuje arkusz adresów MAC zgodnie z docelowym adresem MAC pakietu. Jeśli lista adresów MAC zawiera pozycję pasującą do adresu MAC docelowego pakietu, używa portu wyjściowego do przekazania pakietu. Jeśli adres MAC nie ma pozycji pasującej do adresu MAC docelowego pakietu, urządzenie przyjmuje tryb rozgłoszeniowy, aby przesłać pakiet przez odpowiednią sieć VLAN (z wyjątkiem portu wejściowego).

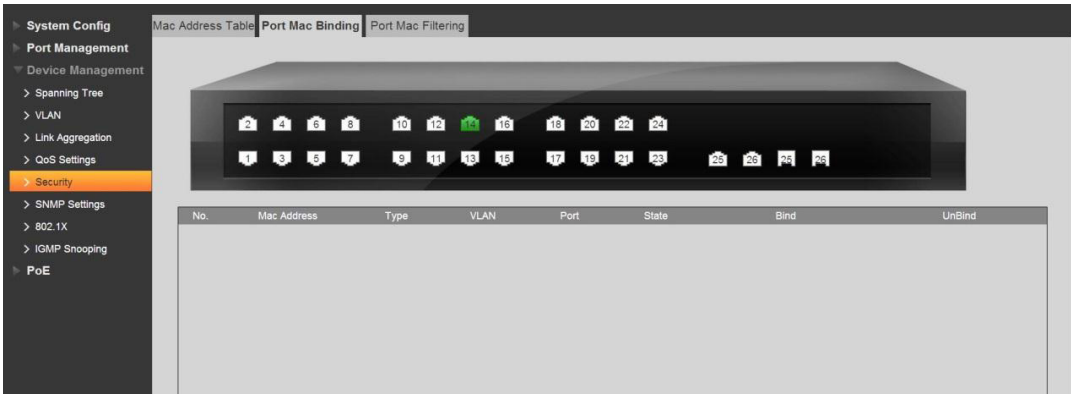
Informacje o adresie MAC znajdują się na poniższym rysunku.



Rysunek 6-21

6.5.2 WIĄZANIE PORTU MAC

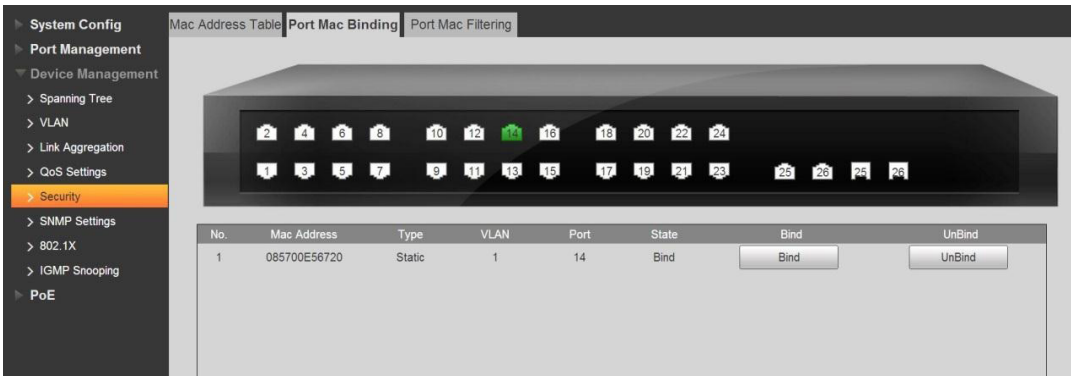
Na rysunku 6-22 kliknij bieżący podłączony port, ustaw funkcję wiązania adresu MAC portu tak, aby bieżący port przekazywał tylko wiążący adres MAC.



Rysunek 6-22

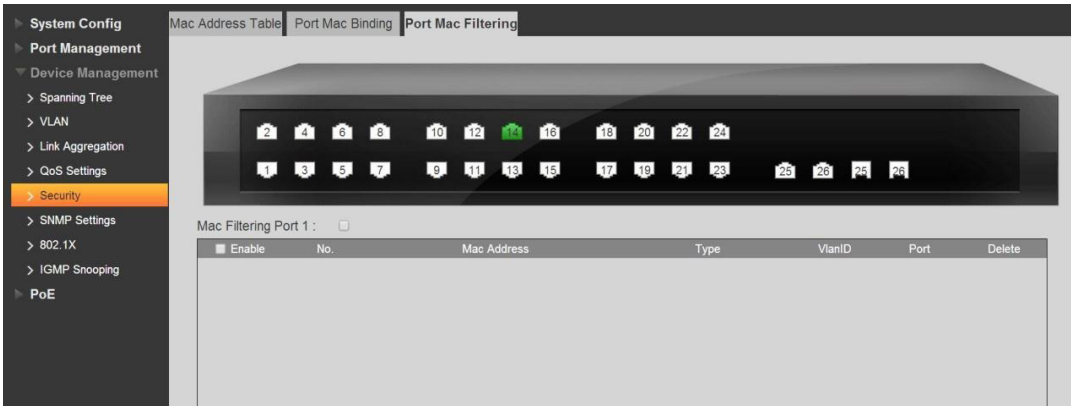
PRZYKŁADY KONFIGURACJI

1. Połączenie sieciowe
   a) Użytkownik używa sieci WEB do ustawienia przypisania adresu MAC portu, aby port mógł być używany tylko przez bieżące urządzenie.
2. Ustawienia
   a) W sekcji Zarządzanie urządzeniami> Bezpieczeństwo przejdź do interfejsu tabeli adresów MAC.
   b) Wybierz interfejs powiązania adresu MAC portu.
   c) Wybierz port, którego stan połączenia jest zielony, a następnie kliknij przycisk Powiąż. Patrz rysunek 6-23.



Rysunek 6-23

6.5.3 FILTROWANIE PORTÓW MAC



Rysunek 6-24

Jak pokazano na rysunku 6-24, funkcja służy do ograniczenia dozwolonych pakietów MAC pod portem, co może zapobiec fałszywemu atakowi. Po skonfigurowaniu portu z funkcją, gdy port odbierze pakiet, sprawdzi, czy źródłowy adres MAC pakietu jest taki sam, jak dozwolony adres MAC:

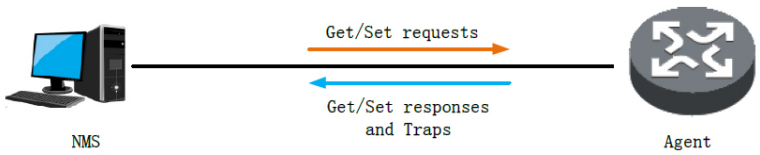
- Jeśli jest taki sam, pakiet jest uznawany za legalny i będzie nadal wdrażał dalsze przetwarzanie;
- Jeśli natomiast jest inny, pakiet jest uznawany za nielegalny i zostanie odrzucony.

6.6 USTAWIENIA SNMP

Sieć SNMP obejmuje dwa elementy: NMS i Agenta.

- NMS (Network Management System) jest administratorem sieci SNMP. Zapewnia przyjazny dla użytkownika interaktywny interfejs. Jest odpowiedni dla administratora sieci do wykonywania większości prac związanych z zarządzaniem.
- Agent to obiekt zarządzany w sieci SNMP. Służy do odbierania, przetwarzania wiadomości zapytania NMS. W niektórych pilnych sytuacjach, takich jak zmiana stanu portu, Agent może automatycznie wysłać informacje o alarmie do NMS.

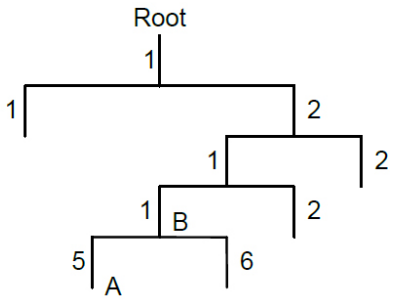
Kiedy NMS zarządza urządzeniem, zwraca dużą uwagę na niektóre parametry, takie jak stan portu, stopień wykorzystania procesora itp. Wszystkie te parametry razem nazywane są bazą informacji zarządzania (MIB). Te parametry są nazywane węzłami w MIB. MIB definiuje warstwy tych węzłów i właściwości tych obiektów, takie jak nazwa obiektu, prawa dostępu, typ danych itp. Każdy agent ma własną bazę MIB. Wszystkie zarządzane urządzenia mają własny plik MIB, a kompilacja tych plików MIB w NMS może wygenerować MIB każdego urządzenia. NMS odczytuje i zapisuje węzły MIB zgodnie z ustawieniami praw dostępu, tak aby mógł zarządzać agentem. Na poniższym rysunku przedstawiono relacje między NMS, agentem i MIB.



Rysunek 6-25

MIB przyjmuje organizację drzewa, składa się z wielu węzłów. Każdy węzeł reprezentuje jeden obiekt zarządzany. Zarządzany obiekt może używać unikatowego numeru reprezentującego ścieżkę zaczynającą się w katalogu głównym. Ten numer jest nazywany identyfikatorem obiektu (OID).

Szczegółowe informacje można znaleźć na poniższym rysunku. Zarządzany obiekt B może używać numeru seryjnego {1.2.1.1} do identyfikacji. To jest OID zarządzanego obiektu.



Rysunek 6-26

SNMP zapewnia trzy podstawowe operacje umożliwiające interakcję między NMS a agentem.

- Get: NMS używa go do wyszukiwania wartości jednego lub więcej węzłów w bazie MIB agenta.
- Zestaw: NMS używa go do ustawienia wartości jednego lub kilku węzłów bazy MIB agenta.
- Pułapka: NMS używa go do wysyłania informacji o pułapce do NMS. Agent nie wymaga od NMS wysłania odpowiedzi, a NMS nie odpowiada na informacje o pułapce. SNMPv1, SNMPv2 i SNMPv3 obsługują działanie pułapki.

Wersja protokołu SNMP

Obecnie agent obsługuje protokoły SNMPv1, SNMPv2 i SNMPv3.

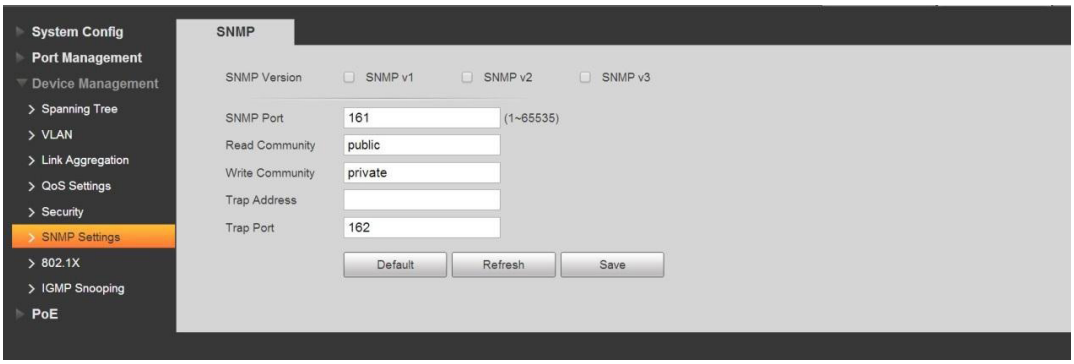
- SNMPv1 przyjmuje nazwę społeczności do certyfikacji. Nazwa wspólnoty jest jak hasło, ma na celu ograniczenie komunikacji pomiędzy NMS a Agentem. Jeśli nazwa zbiorowości NMS i nazwa zbiorowości urządzeń zarządzanych nie są takie same, NMS i agent nie mogą ustanowić połączenia SNMP, co oznacza, że NMS nie może uzyskać dostępu do agenta, a NMS odrzuca informacje ostrzegawcze od agenta.
- SNMPv2 przyjmuje nazwę społeczności do certyfikacji. SNMPv2c rozszerzył funkcje protokołu SNMPv1. Zapewnia więcej typów operacji i obsługuje więcej typów danych, zapewnia liczne kody błędów i może dokładnie rozróżniać błędy.
- SNMPv3 przyjmuje do certyfikacji model zabezpieczeń oparty na użytkownikach (USM). Administrator sieci może ustawić funkcję uwierzytelniania i szyfrowania. Uwierzytelnienie ma na celu sprawdzenie ważności nadawcy wiadomości w celu uniknięcia nielegalnego dostępu. Szyfrowanie ma na celu zaszyfrowanie wiadomości komunikacyjnych między NMS a Agentem w przypadku podsłuchu. Uwierzytelnianie i funkcja szyfrowania mogą zwiększyć poziom bezpieczeństwa między NMS a agentem.

UWAGA

Upewnij się, że NMS i agent używają tej samej wersji SNMP, w przeciwnym razie połączenie NMS i agenta może się nie udać.

6.6.1 SNMP

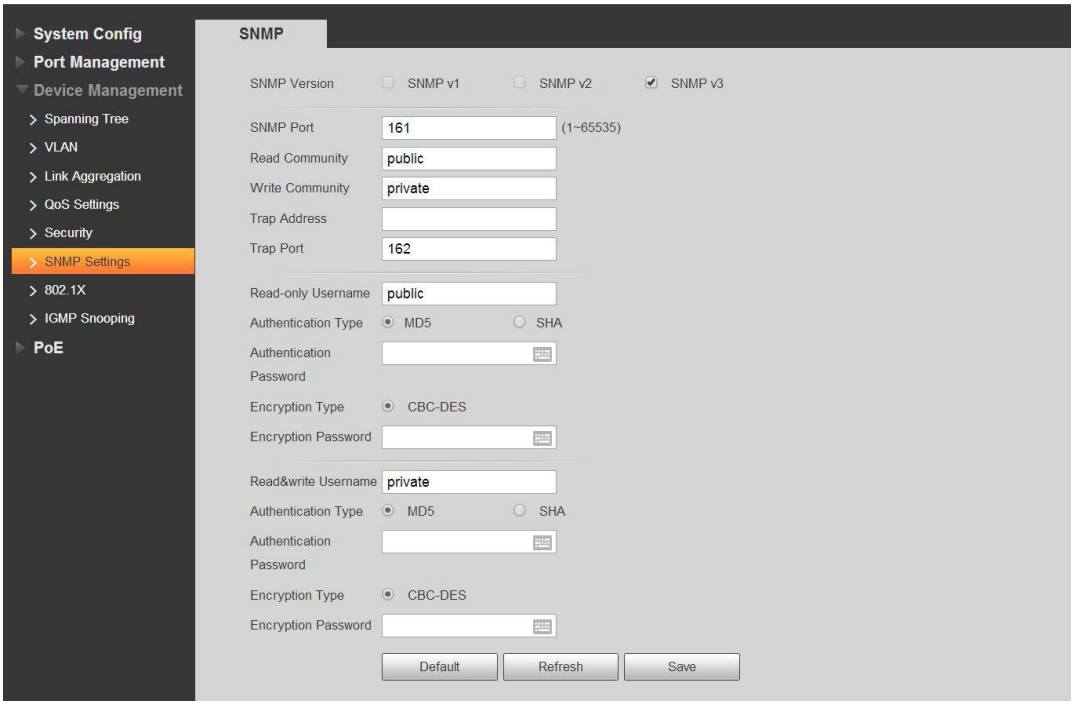
Ten interfejs służy do ustawiania SNMP. V1 i V2 obejmują następujące konfiguracje.



Rysunek 6-27

Na rysunku 6-21 interfejs konfiguracji SNMP V1 i V2 zawiera port SNMP, wersję, społeczność odczytu, społeczność zapisu, adres pułapki i port pułapki.

Rysunek 6-28 przedstawia interfejs konfiguracji SNMP V3.



Rysunek 6-28

Szczegółowe informacje zawiera Tabela 6-6

Nazwa	Funkcja
Społeczność - Odczyt	Nazwa wspólnoty umożliwiająca dostęp do administratora sieci. Prawo jest czytane. Domyślna konfiguracja jest publiczna.
Społeczność - Zapis	Nazwa wspólnoty umożliwiająca dostęp do administratora sieci. Posiada uprawnienia do zapisu. Domyślna konfiguracja jest prywatna.
Adres pułapki	Służy do określenia adresu IP serwera.
Port pułapki	Służy do ustawienia portu docelowego pułapki.
Nazwa użytkownika tylko do odczytu	Ustaw nazwę użytkownika tylko do odczytu. To jest tylko dla V3.
Tryb uwierzytelniania	Służy do ustawiania trybu uwierzytelniania, gdy poziom bezpieczeństwa to „Uwierzytelnianie bez szyfrowania” lub „Uwierzytelnianie i szyfrowanie”. Tryb uwierzytelniania obejmuje MDS i SHA.
Hasło uwierzytelniające	Służy do ustawienia hasła uwierzytelniającego.
Tryb szyfrowania	Gdy tryb uwierzytelniania to „uwierzytelnianie i szyfrowanie”, należy ustawić tryb szyfrowania. Ta seria produktów obsługuje tylko 3DES.
Hasło szyfrowania	Gdy tryb uwierzytelniania to „uwierzytelnianie i szyfrowanie”, należy ustawić hasło szyfrowania.
Hasło do odczytu / zapisu	Służy do ustawienia użytkownika do odczytu / zapisu.

Tabela 6-6

PRZYKŁADY KONFIGURACJI

SNMPv1/v2

1. Połączenie sieciowe

a) Patrz Rysunek 6-29, NMS łączy się z Switch i powinien spełniać następujące wymagania. NMS monitoruje Switch i zarządza nim poprzez SNMPv1 i SNMPv2c. Switch może automatycznie wysłać wiadomość Trap do NMS, gdy wystąpi awaria.

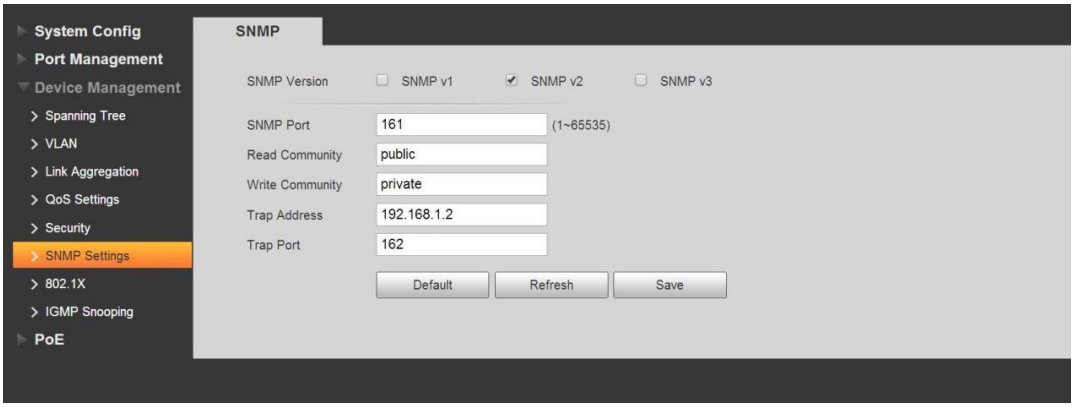
Rysunek 6-29

2. Ustawienia

a) Na pasku nawigacji, w menu Urządzenie> Ustawienia SNMP, system domyślnie przechodzi do interfejsu SNMPv1

b) Wybierz wersję SNMP jako v1 lub v2.

c) Numer portu SNMP to 161, ustaw „Read Community", „Write Community", „Trap address" i „Trap Port". Patrz rysunek 6-30.



Rysunek 6-30

SNMPv3

1. Połączenie sieciowe

a) Patrz Rysunek 6-31, NMS łączy się z przełącznikiem i powinien spełniać następujące wymagania.

- NMS monitoruje Switch i zarządza nim przez SNMPv3
- Switch może automatycznie wysłać wiadomość Trap do NMS, gdy wystąpi awaria.
- Kiedy NMS łączy się z Agentem przez SNMP, wymaga uwierzytelnienia. Tryb uwierzytelniania to MD5, hasło uwierzytelniania to admin123.
- Wiadomość SNMP między NMS i Agentem powinna być zaszyfrowana, tryb szyfrowania to DES56, a hasło szyfrowania to admin123.

Rysunek 6-31

2. Ustawienia

a) Na pasku nawigacyjnym, w menu Urządzenie> Ustawienia SNMP, system domyślnie przechodzi do interfejsu SNMPv1.

b) Wybierz wersję SNMP jako v3.

c) Numer portu SNMP to 161, ustaw „Read Community", „Write Community", „Trap address" i „Trap Port". Port pułapki to 162.

d) Wprowadź nazwę użytkownika tylko do odczytu jako „użytkownik".

e) Tryb uwierzytelniania to MD5.

f) Hasło uwierzytelniające to „admin123".

g) Tryb szyfrowania to „CBC-DES"

h) Hasło szyfrowania i hasło potwierdzające to „admin123".

i) Wprowadź nazwę użytkownika do odczytu / zapisu jako „użytkownik1".

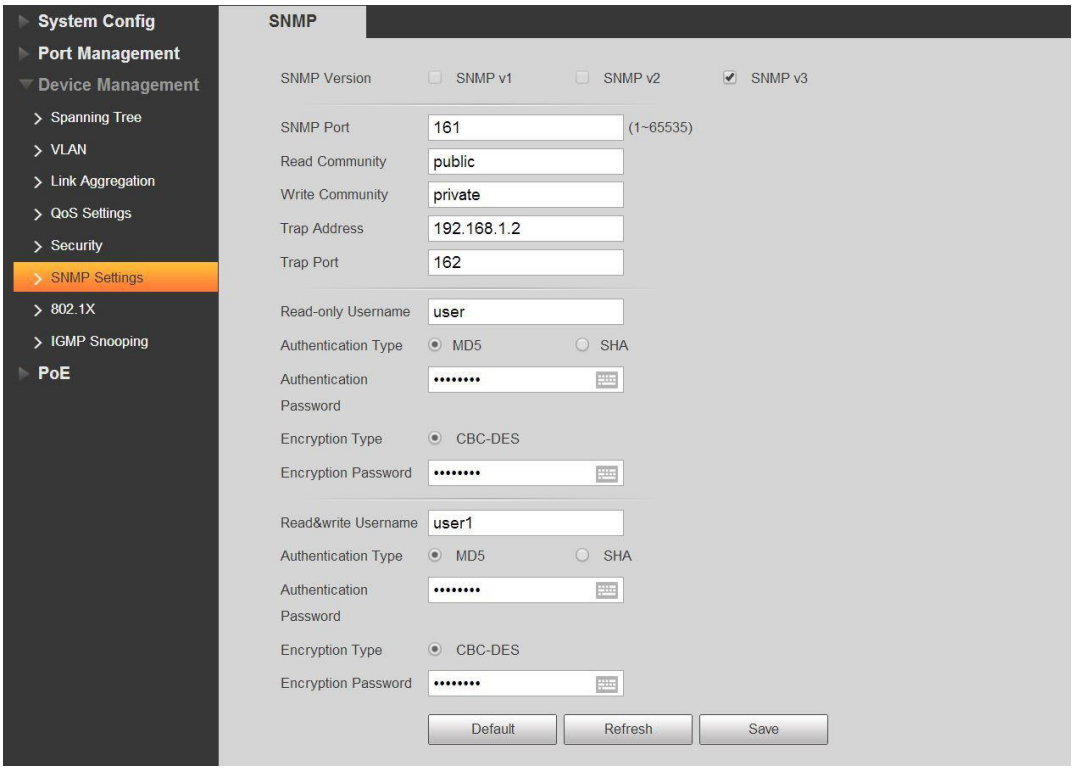
j) Tryb uwierzytelniania to „MD5".

k) Hasło szyfrowania to „admin123".

l) Tryb szyfrowania to „CBC-DES"

m) Hasło szyfrowania to „admin123".

n) Kliknij przycisk Zapisz. Patrz rysunek 6-32.



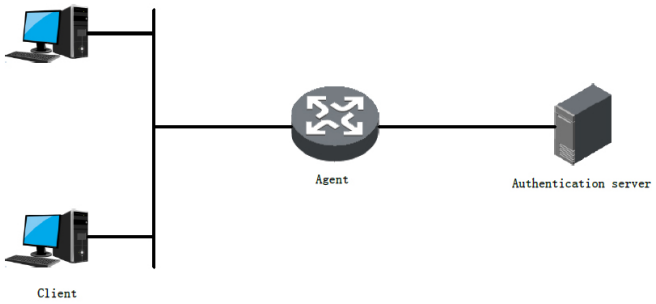
Rysunek 6-31

6.7 802.1X

IEEE 802.1x to standard uwierzytelniania dotyczący dostępu użytkownika do sieci, który jest wyznaczony przez IEEE, jest to rodzaj protokołu kontroli dostępu do sieci oparty na porcie, dlatego na porcie urządzenia należy skonfigurować dokładną funkcję uwierzytelniania 802.1x. Jeśli chodzi o urządzenie użytkownika, które uzyskuje dostęp do portu, musi kontrolować dostęp do źródła sieciowego poprzez uwierzytelnianie.

6.7.1 STRUKTURA SIECI 802.1X

System 802.1x składa się z trzech części, które są klientem, urządzeniem i serwerem uwierzytelniającym, co pokazano na rysunku 6-33.



Rysunek 6-33

- Klient jest urządzeniem końcowym użytkownika, które wymaga dostępu do sieci LAN, uwierzytelnianego przez urządzenie znajdujące się w sieci LAN. Klient musi zainstalować oprogramowanie klienckie, które obsługuje uwierzytelnianie 802.1x.
- Urządzenie końcowe to urządzenie sieciowe, które kontroluje dostęp klienta w sieci LAN, znajduje się między klientem a serwerem uwierzytelniającym, który zapewnia klientom port dostępu LAN (port fizyczny lub logiczny) i realizuje uwierzytelnianie na podłączonym kliencie poprzez interakcję z serwerem
- Serwer uwierzytelniania służy do implementacji uwierzytelniania, autoryzacji i rozliczeń, zwykle jest to serwer RADIUS (Remote Authentication Dial-In User Service) Serwer uwierzytelniający może weryfikować legalność klienta na podstawie informacji uwierzytelniających klienta wysyłanych przez urządzenie końcowe i informować urządzenie o wynikach weryfikacji; urządzenie decyduje o tym, czy zezwala na dostęp klienta, czy nie. W niektórych środowiskach sieciowych o małej skali rolę serwera uwierzytelniającego można zastąpić urządzeniem, co oznacza, że urządzenie realizuje lokalne uwierzytelnianie, autoryzację i naliczanie opłat.

6.7.2 PORT KONTROLOWANY / NIEKONTROLOWANY PRZEZ UWIERZYTELNIANIE 802.1X

Porty dostępowe LAN dostarczane przez urządzenie dla klienta można podzielić na dwa porty logiczne, które są portem kontrolowanym i portem niekontrolowanym. Każda ramka, która dotarła do portu, może być wyświetlana zarówno na porcie kontrolowanym, jak i niekontrolowanym.

- Niekontrolowany port jest zawsze w stanie połączenia dwukierunkowego, które jest używane głównie do przesyłania pakietu uwierzytelniającego i upewnienia się, że klient zawsze może wysłać lub odebrać pakiet uwierzytelniający.
- Kontrolowany port jest zawsze w stanie połączenia dwukierunkowego w ramach statusu autoryzacji, który jest używany do przesyłania pakietu biznesowego; zabronione jest odbieranie jakichkolwiek pakietów od klienta, gdy jest on w stanie nieautoryzowanym.

6.7.3 TRYB WYZWALANIA UWIERZYTELNIANIA 802.1X

Proces uwierzytelniania w standardzie 802.1x jest aktywnie uruchamiany przez klienta, może być również uruchamiany przez urządzenie.

1. Tryb wyzwalania aktywnego klienta.
   - Wyzwalacz multiemisji: klient aktywnie wysyła pakiet żądania uwierzytelnienia do urządzenia w celu uruchomienia procesu uwierzytelnienia, adres docelowy pakietu to adres MAC multiemisji 01-80-C2-00-00 03.
   - Wyzwalacz emisji: klient aktywnie wysyła pakiet żądania uwierzytelnienia do urządzenia w celu wyzwolenia uwierzytelnienia, adres docelowy pakietu to adres rozgłoszeniowy MAC. Ten tryb jest w stanie rozwiązać problem polegający na tym, że urządzenie nie otrzymuje żądania uwierzytelnienia od klienta, ponieważ niektóre urządzenia nie obsługują powyższego pakietu multiemisji w sieci.

2. Tryb wyzwalania aktywnego urządzenia

Tryb aktywnego wyzwalacza urządzenia jest używany do obsługi klienta, który nie może aktywnie wysłać pakietu żądania uwierzytelnienia, istnieją dwa typy uwierzytelniania aktywnego wyzwalacza urządzenia:

- Wyzwalacz multiemisji: urządzenie aktywnie wysyła pakiet żądania weryfikacji tożsamości, aby wywołać proces uwierzytelniania klienta w regularnych odstępach czasu (domyślnie jest to co 30 sekund).
- Wyzwalacz emisji pojedynczej: gdy urządzenie otrzyma nieznany pakiet ze źródłowego adresu MAC, aktywnie wyśle pakiet żądania weryfikacji tożsamości do emisji pojedynczej adresu MAC w celu wywołania procesu uwierzytelnienia. Pakiet zostanie wysłany ponownie, jeśli urządzenie nie otrzyma odpowiedzi klienta w określonym czasie.

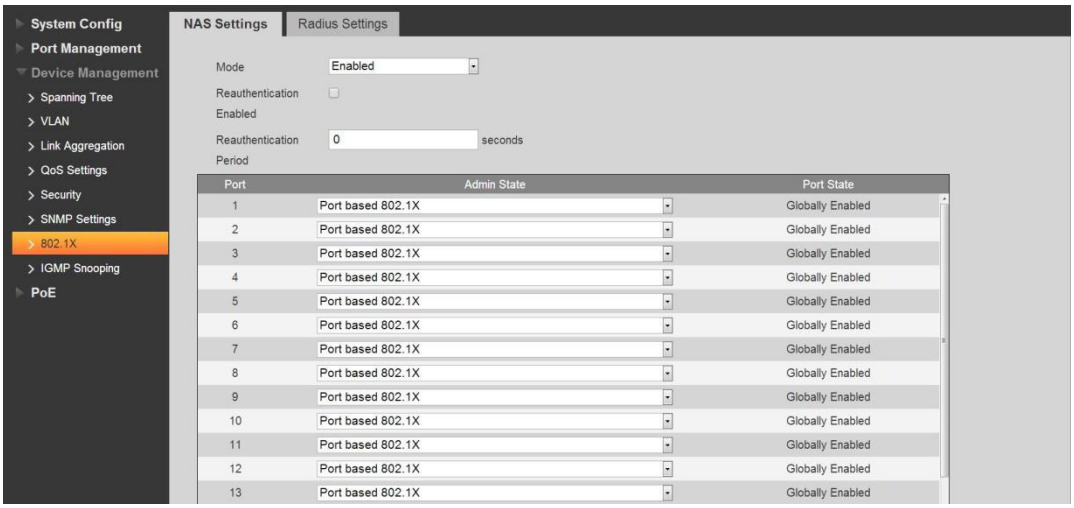
6.7.4 STATUS AUTORYZACJI PORTU

Może kontrolować, czy użytkownicy uzyskujący dostęp do portu muszą odwiedzić źródło sieciowe poprzez uwierzytelnienie, konfigurując status autoryzacji dla portu. Port obsługuje trzy następujące autoryzowane stany:

- Authorized-force: Oznacza to, że port ma zawsze status autoryzacji, co umożliwia użytkownikom odwiedzanie źródła sieciowego bez uwierzytelniania.
- Unauthorized-force: oznacza, że port jest zawsze w stanie nieautoryzowanym, co nie pozwala na uwierzytelnianie użytkowników. Urządzenie nie zapewnia usługi uwierzytelniania dla klienta, do którego uzyskuje się dostęp do portu.
- W oparciu o port 802.1x: oznacza, że początkowy stan portu to stan nieautoryzowany, który nie pozwala użytkownikom na odwiedzanie źródła sieciowego; Port zostanie przełączony do statusu autoryzowanego, jeśli użytkownicy przejdą uwierzytelnianie i będą odwiedzać źródło sieciowe.

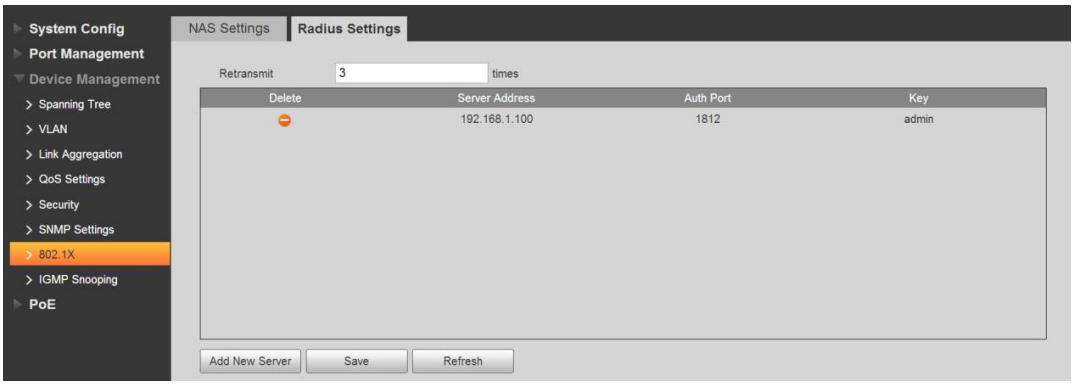
PRZYKŁADY KONFIGURACJI

1. Wymagania Sieciowe
   a) Adres IP klienta to segment 192.168.1.1/24, adres IP serwera uwierzytelniania to 192.168.1.100 i wymagane jest uwierzytelnienie przez serwer uwierzytelniania, gdy uzyskuje się dostęp do wszystkich portów urządzenia.
2. Kroki w celu konfiguracji
   a) Włącz funkcję uwierzytelniania, wszystkie porty są włączone w oparciu o uwierzytelnianie 802.1x, co pokazano na rysunku 6-34.



Rysunek 6-34

b) Skonfiguruj adres serwera uwierzytelniającego pokazany na rysunku 6-35.



Rysunek 6-35

6.8 IGMP SNOOPING

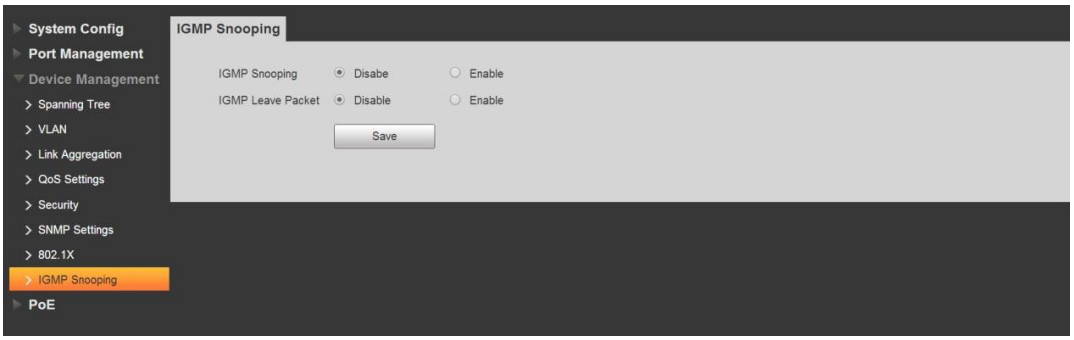
IGMP Snooping (Internet Group Management Protocol Snooping) jest obsługiwany na urządzeniu warstwy drugiej, ma na celu generowanie tablicy przesyłania multiemisji w warstwie drugiej poprzez szpiegowanie pakietu IGMP między urządzeniem warstwy trzeciej a hostem, który ma zarządzać i kontrolować przekazywanie pakietów danych multiemisji i zrealizować wymaganą dystrybucję pakietu danych multiemisji w warstwie drugiej.

6.8.1 IGMP SNOOPING TEORIA

Urządzenie warstwy drugiej protokołu IGMP Snooping może ustanowić relację mapowania dla portu i adresu multiemisji MAC poprzez analizę odebranego pakietu IGMP i ma przesyłać dane multiemisji zgodnie z relacją mapowania.

Dane multiemisji będą rozgłaszane w sieci warstwy drugiej, gdy urządzenie warstwy drugiej nie obsługuje funkcji IGMP Snooping; po uruchomieniu urządzenia warstwy drugiej IGMP Snooping, znane dane multiemisji z grupy multiemisji nie będą rozgłaszane w sieci warstwy drugiej, ale przesyłane grupowo do wyznaczonych odbiorników. IGMP Snooping może przekazywać informacje tylko do potrzebnych odbiorników za pośrednictwem multiemisji w warstwie drugiej, co może przynieść następujące korzyści:

- Zmniejsza ilości pakietów rozgłoszeniowych w sieci warstwy drugiej, oszczędza przepustowość sieci
- Zwiększa bezpieczeństwo informacji multiemisji
- Zapewnia wygodę realizacji indywidualnych rozliczeń dla każdego gospodarza.



Rysunek 6-36

Interfejs konfiguracji IGMP Snooping pokazano na rysunku 6-36.

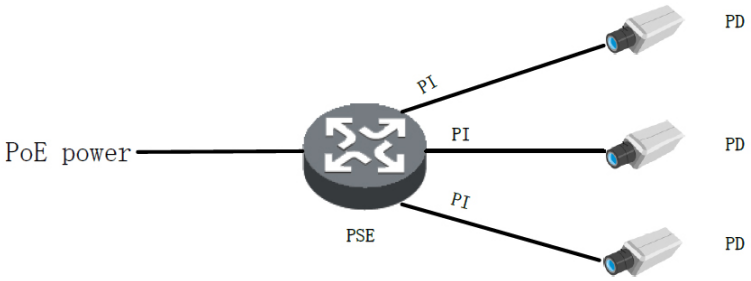
- IGMP Snooping: włącz lub wyłącz funkcję IGMP Snooping.
- IGMP Leave Packet: włącza lub wyłącza funkcję szybkiego wyjścia.

7. PoE

7.1 USTAWIENIA PoE

Power over Ethernet (PoE) oznacza, że urządzenie wykorzystuje port Ethernet do zdalnego zasilania urządzenia za pomocą skrętki komputerowej. Funkcja PoE realizuje funkcję scentralizowanego zasilania i ułatwia tworzenie kopii zapasowych. Terminal sieciowy używa tylko jednego prostego kabla sieciowego bez zewnętrznego źródła zasilania. Jest zgodny ze standardami IEEE 802.3af i IEEE 802.3at i przyjmuje uniwersalny rozpoznawany port zasilania. Przeznaczony jest do kamery IP, telefonu IP, bezprzewodowego punktu dostępowego (bezprzewodowego punktu dostępowego), ładowarki do urządzeń przenośnych, punktu sprzedaży, akwizycji danych itp.

Patrz Rysunek 7-1 dla systemu PoE. Obejmuje zasilanie PoE, sprzęt do pozyskiwania energii (PSE), interfejs zasilania (PI) i urządzenie zasilane (PD).



Rysunek 7-1

1. Zasilanie PoE
PoE ma zapewnić zasilanie całego systemu.
2. PSE
PSE ma bezpośrednio zasilać PD. PSE obsługuje takie funkcje, jak wyszukiwanie, wykrywanie wyładowań niezupełnych, kategoryzowanie wyładowań niezupełnych i ich zasilanie, zarządzanie zużyciem energii, sprawdzanie połączenia wyładowań niezupełnych itp.
3. PI
PI oznacza interfejs Ethernet z funkcją PoE. Nazywa się to portem PoE. Obejmuje Wf i Wn.

Zdalne zasilanie PoE ma dwa tryby:

- Przewody sygnałowe - PSE wykorzystuje pary (1, 2, 3, 6) do przesyłania danych w skrętce kategorii 3/5 do zasilania prądem stałym podczas przesyłania danych do PD.
- Nad zapasowymi przewodami - PSE wykorzystuje pary (4, 5, 7, 8) nie przesyłając danych w skrętce dwużyłowej kategorii 3/5 do zasilania PD DC.

UWAGA

Tryb zasilania zależy od specyfikacji PD. Wybrany tryb będzie obsługiwał jednocześnie PSE i PD. Jeśli tryb zasilania PSE i PD nie są takie same (np. PSE nie obsługuje zasilania zapasowego przewodu lub PD obsługuje tylko zasilanie zapasowego przewodu), użyj konwertera, aby zapewnić zasilanie PD.

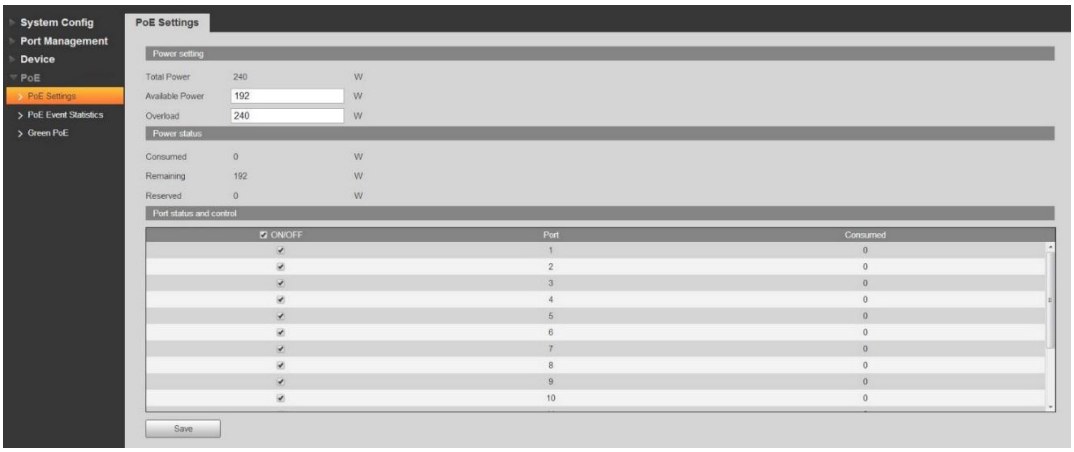
4. PD
PD oznacza urządzenie pobierające energię z PSE. Obejmuje telefon IP, bezprzewodowy punkt dostępowy, przenośną ładowarkę, punkt sprzedaży, kamerę sieciową itp. Gdy PD korzysta z zasilania z urządzenia PoE, może łączyć się z innym urządzeniem w celu tworzenia kopii zapasowych.

Szczegółowe informacje na temat konfiguracji portu zawiera Tabela 7-1.

Nazwa	Funkcja
Port	Na rysunku panelu wybierz port PoE. Wybrane porty będą wyświetlane na liście wybranych portów w dolnej części interfejsu.
Power Status	Włącz lub wyłącz PoE na wybranych portach. • System nie dostarcza zasilania ani nie rezerwuje mocy dla PD podłączonego do portu PoE, jeśli port PoE nie ma włączonej funkcji PoE. • Możesz włączyć PoE dla portu PoE, jeśli port PoE nie spowoduje przeciążenia zasilania PoE; w przeciwnym razie nie możesz włączyć PoE dla portu PoE. Domyślnie funkcja PoE jest wyłączona na porcie PoE. **Ważne** Przeciążenie PSE - gdy łączna wielkość poboru mocy wszystkich portów przekracza maksymalną moc PSE, system uznaje, że PSE jest przeciążony.
Wartość rezerwowa całkowitego zużycia energii	Służy do ustawienia zarezerwowanej wartości całkowitego poboru mocy portu PoE. Wartość całkowitego zużycia energii PoE odnosi się do całkowitego zużycia energii przez PD ze wszystkich portów PoE. Gdy pobór mocy podłączonego PD jest wyższy niż całkowity pobór mocy PoE, urządzenie przestaje dostarczać moc do PD.

Tabela 7-1

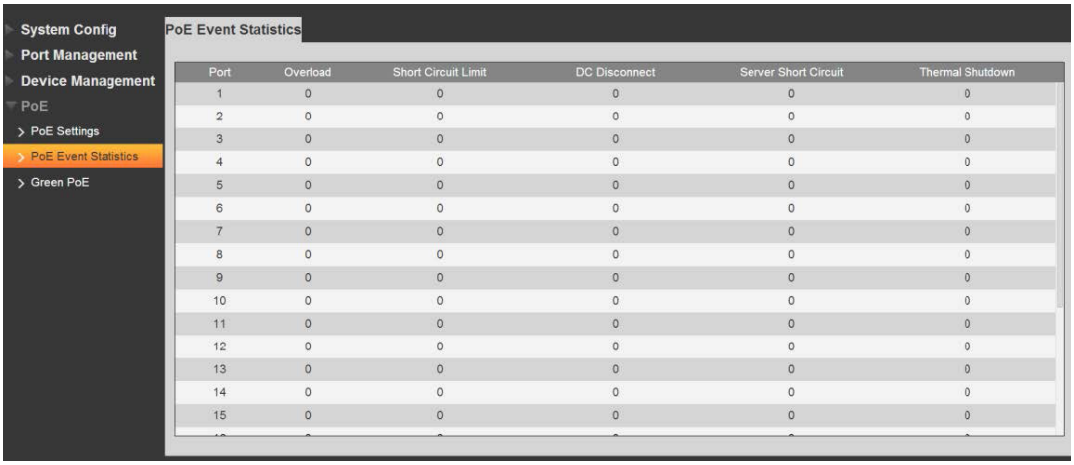
Interfejs konfiguracji przedstawia Rysunek 7-2.



Rysunek 7-2

7.2 ZDARZENIA POE

Na rysunku 7-3 przedstawiono statystyki zdarzeń PoE dla każdego portu. Obejmuje przeciążenie, ograniczenie zwarcia, odłączenie DC, zwarcie serwera i wyłączenie termiczne.



Rysunek 7-3

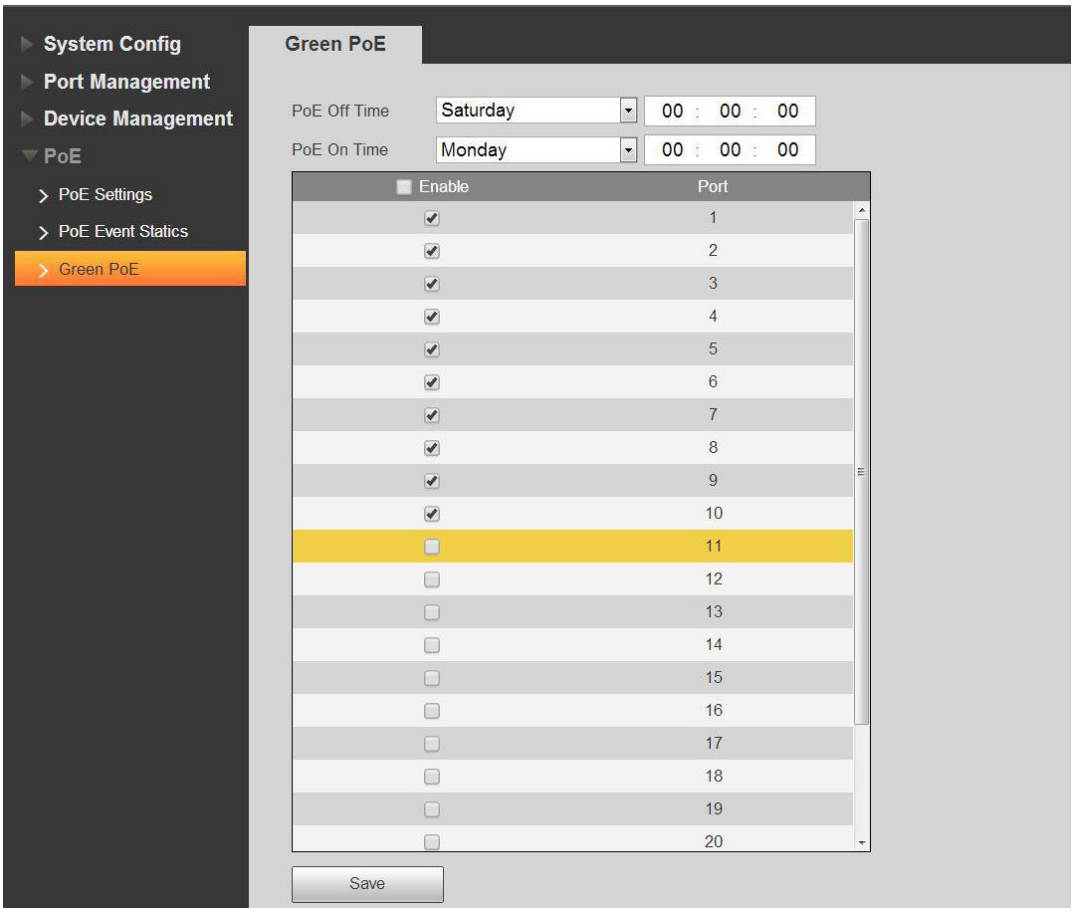
Patrz Tabela 7-2 w celu uzyskania parametrów zdarzenia PoE.

Nazwa	Funkcja
Przeciążenie	Prąd zasilania przy uruchamianiu pojedynczego portu przekroczył dopuszczalny próg.
Limit zwarcia	Gdy zasilanie chipa przesyła moc do portu, powoduje zwarcie.
Odłączenie DC	Zasilanie pojedyńczego portu jest wyłączone
Zwarcie serwera	Dochodzi do zwarcia zasilania, gdy układ zasilający wysyła moc zasilającą.
Wyłączenie termiczne	Temperatura chipa zasilającego jest zbyt wysoka z powodu zwarcia lub z innego powodu.

Tabela 7-2

7.3 ZIELONE POE

Na rysunku 7-4 służy do ustawienia parametrów oszczędzania energii PoE. Funkcja PoE jest wyłączona w określonym czasie, aby oszczędzać energię. Po upływie tego okresu port automatycznie wznawia zasilanie.



Rysunek 7-4

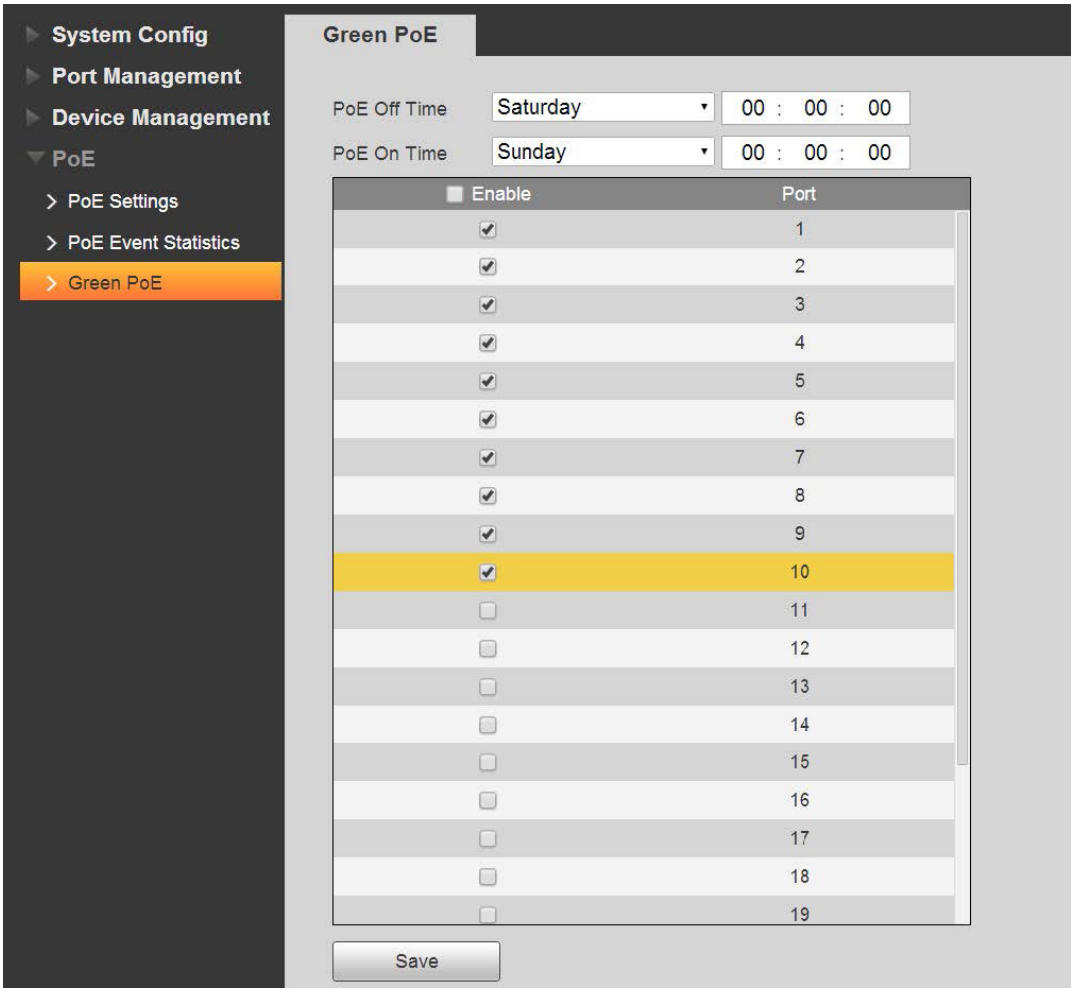
Szczegółowe informacje na temat konfiguracji zielonego PoE zawiera Tabela 7-3.

Nazwa	Funkcja
Czas wyłączenia PoE	Prąd wejściowy pojedynczego portu przekroczył próg prądu portu wyjściowego.
Czas działania PoE	Port wysyłający jest zwarty, gdy chip dostarcza zasilanie do portu.
Port	Porty do wyboru

Tabela 7-2

PRZYKŁADY KONFIGURACJI

1. Połączenie Sieciowe
   a) Port 1 do 10 ma być zamykany w każdą sobotę i każdą niedzielę, a automatycznie wznawiany w każdy poniedziałek.
2. Ustawienia
   a) Ustaw okres wyłączenia portu na sobotę do niedzieli i automatyczne wznowienie zasilania w poniedziałek.
   b) Ustaw Porty.
   c) Kliknij Zapisz. Szczegółowe informacje zawiera Rysunek 7-5.



Rysunek 7-5

NSS Sp. z o.o.
ul. Modularna 11 (hala IV)
02-238 Warszawa