Podręcznik użytkownika

Seria przełączników T1500

T1500G-8T(TL-SG2008) / T1500G-10PS (TL-SG2210P)
T1500G-10MPS 2.0 / T1500-28PCT (TL-SL2428P)

1910012393 REV3.0.0

SPIS TREŚCI

Informacje wstępne

Jak zacząć

Zarządzanie systemem

Zarządzanie interfejsami

Konfiguracja LAG

Zarządzanie tablicą adresów MAC

Konfiguracja 802.1Q VLAN

Konfiguracja MAC VLAN

Konfiguracja protokołu VLAN

Konfiguracja GVRP

Konfiguracja multicastu L2

Konfiguracja Spanning Tree

Konfiguracja LLDP

Konfiguracja usługi DHCP

Konfiguracja QoS

Konfiguracja Access Security

Konfiguracja AAA

Konfiguracja 802.1x

Konfiguracja Port Security

Konfiguracja ACL

Konfiguracja IMPB IPv4

Konfiguracja IMPB IPv6

Konfiguracja filtrowania DHCP

Konfiguracja DoS Defend

Monitorowanie systemu

Monitorowanie ruchu

Mirroring ruchu

Konfiguracja DLDP

Konfiguracja SNMP i RMON

Diagnostyka urządzenia i sieci

Konfiguracja dzienników systemowych

Informacje wstępne

Ten podręcznik konfiguracji zawiera informacje dotyczące zarządzania przełącznikami serii T1500. Zapoznaj się uważnie z podręcznikiem przed rozpoczęciem pracy.

Do kogo skierowany jest przewodnik

Ten przewodnik jest przeznaczony dla administratorów sieci, zaznajomionych z pojęciami z dziedziny IT i terminologią sieciową.

Założenia przewodnika

Niektóre urządzenia opisane w tym przewodniku mogą nie być dostępne w twoim kraju lub regionie. Informacje o dostępnych modelach znajdują się na stronie *https://www.tp-link.com/pl/*.

Korzystając z tego przewodnika pamiętaj, że funkcje przełącznika mogą się nieznacznie różnić w zależności od posiadanego modelu i wersji oprogramowania. Wszystkie zrzuty ekranu, rysunki, parametry i opisy znajdujące się w tym przewodniku mają charakter poglądowy.

Informacje zawarte w tym dokumencie mogą ulegać zmianom bez uprzedniego powiadomienia. W przygotowaniu tego dokumentu dołożono wszelkich starań, aby zapewnić dokładność i rzetelność treści, ale wszelkie oświadczenia, informacje i zalecenia zawarte w tym dokumencie nie stanowią gwarancji ani pośredniej, ani wyrażonej wprost. Użytkownicy ponoszą pełną odpowiedzialność za użytkowanie zakupionych produktów.

W tym przewodniku występują następujące oznaczenia:

Symbol  odnosi się do hasła *Uwaga*. Uwagi zawierają sugestie lub odniesienia, które są pomocne przy użytkowaniu urządzenia.

- Przez GUI:

Menu Name > Submenu Name > Tab page odnosi się do struktury menu. **SYSTEM > System Info > System Summary** oznacza, że strona System Summary wyświetli się po naciśnięciu opcji System Info, która z kolei znajduje się w sekcji System.

Pogrubiona czcionka oznacza przycisk, ikonę paska narzędzi, menu lub element menu.

- Przez CLI:

Pogrubiona czcionka	Niepodlegające zmianom słowo kluczowe. Przykład: **show logging**

Zwykła czcionka	Stała (jedna opcja do wyboru spośród kilku dostępnych). Przykład: **no bandwidth** {all | ingress | egress}
{}	Elementy w nawiasach klamrowych { } są wymagane.
[]	Elementy w nawiasach kwadratowych [ ] są opcjonalne.
|	Alternatywne elementy są pogrupowane w nawiasach i oddzielone pionowymi kreskami |. Przykład: **speed** {10 | 100 | 1000}
Kursywa czcionki	Zmienna (należy podać rzeczywistą wartość). Przykład: **bridge aging-time** *aging-time*

Często występujące połączenie:

{[ ][ ][ ]}	Należy wybrać co najmniej jeden element z nawiasu kwadratowego. Przykład: **bandwidth** {[**ingress** *ingress-rate*] [**egress** *egress-rate*]} To polecenie można zastosować w trzech przypadkach: **bandwidth ingress** *ingress-rate* służy do ograniczania przepustowości na wejściu. **bandwidth egress** *egress-rate* służy do ograniczania przepustowości na wyjściu. **bandwidth ingress** *ingress-rate* **egress** *egress-rate* służy do ograniczania przepustowości na wejściu i wyjściu.

Dodatkowe informacje

- Najnowsze wersje oprogramowania i dokumenty znajdują się w na stronie Do pobrania pod adresem *https://www.tp-link.com/pl/support*.
- Instrukcja instalacji (IG) znajduje się na tej samej stronie co ten przewodnik lub w opakowaniu produktu.
- Szczegółowe specyfikacje urządzeń znajdują się na stronach produktowych pod adresem *https://www.tp-link.com/pl/*.
- Forum wsparcia technicznego TP-Link znajduje się pod adresem *https://community.tp-link.com.*
- Kontakt do wsparcia technicznego znajduje się na stronie Wsparcie pod adresem *https://www.tp-link.com/pl/support*.

Część 1

Jak zacząć

ROZDZIAŁY

1 Dostęp do interfejsu webowego

Dostęp do interfejsu webowego przełącznika uzyskać można przez uwierzytelnianie przez stronę internetową. Do uwierzytelniania użytkowników przełącznik wykorzystuje dwa wbudowane serwery sieciowe, serwer HTTP i HTTPS.

Poniższy przykład prezentuje, jak zalogować się przez serwer HTTP.

1.1 Logowanie

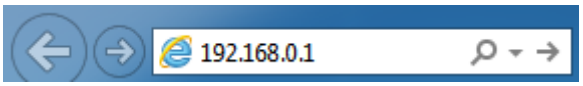
Aby zarządzać przełącznikiem przez przeglądarkę hosta:

1) Upewnij się, że ścieżka pomiędzy hostem a przełącznikiem jest dostępna.

2) Uruchom przeglądarkę. Przykładowe obsługiwane przeglądarki:
   - IE 8.0, 9.0, 10.0, 11.0
   - Firefox 26.0, 27.0
   - Chrome 32.0, 33.0

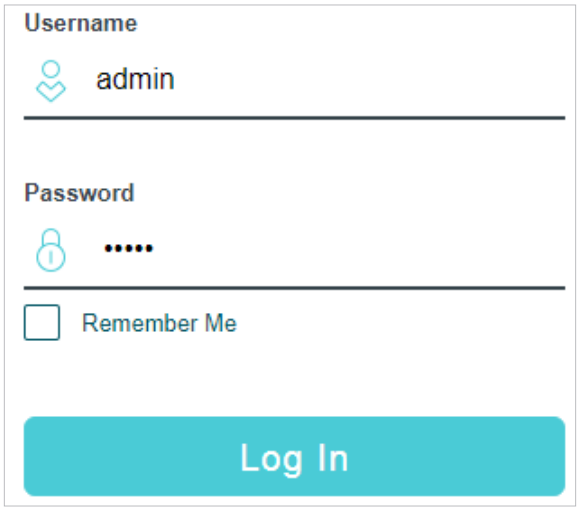
3) W pasku adresu przeglądarki wpisz adres IP przełącznika. Domyślny adres to T192.168.0.1.

Rys. 1-1 Wpisz adres IP przełącznika w przeglądarce



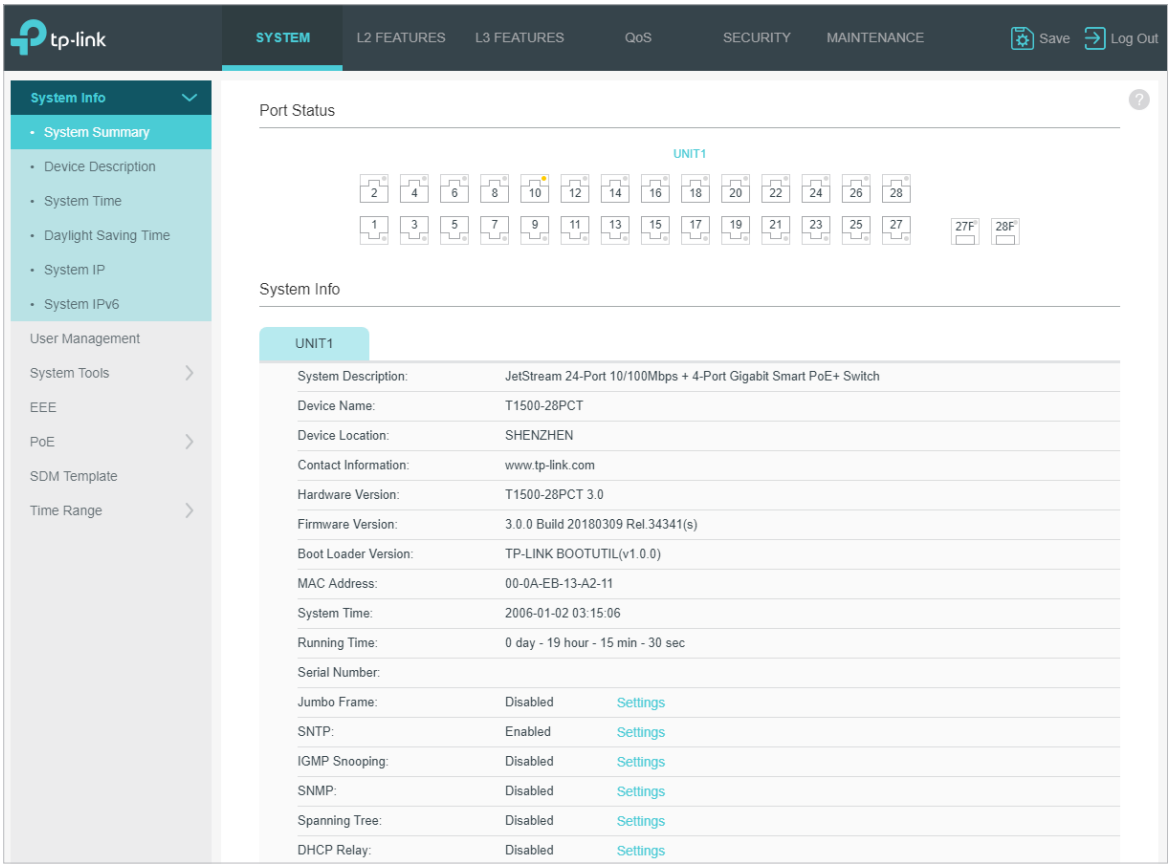
4) W wyskakującym oknie logowania wpisz nazwę użytkownika i hasło (domyślna wartość obu pól to: admin).

Rys. 1-2 Uwierzytelnianie logowania



5) Poniżej zamieszczono zdjęcie typowego interfejsu webowego. W interfejsie możesz sprawdzić aktualny status przełącznika oraz skonfigurować przełącznik.

Rys. 1-3 Interfejs webowy



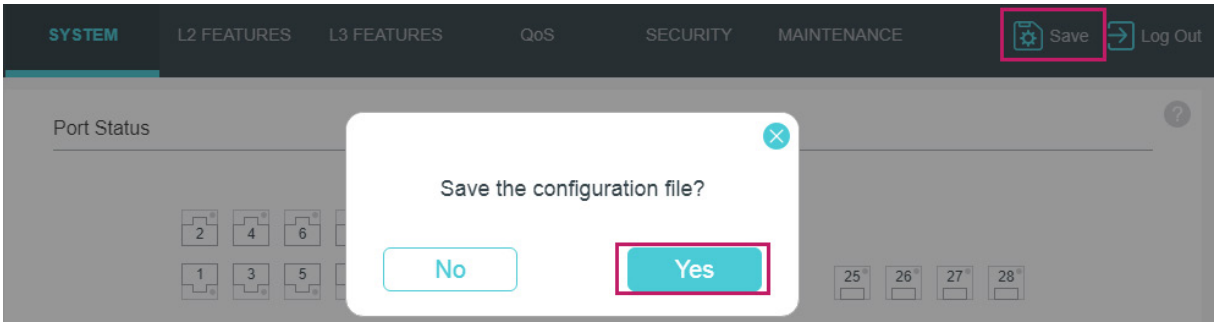
1.2 Zapisywanie konfiguracji

Pliki konfiguracyjne przełącznika dzielą się na dwa typy - plik bieżącej konfiguracji i plik konfiguracji startowej.

Po przeprowadzeniu konfiguracji na subinterfejsach i kliknięciu Apply zmiany zostaną zapisane w pliku bieżącej konfiguracji. Po restarcie przełącznika ustawienia zostaną utracone.

Chcąc zachować konfigurację po restarcie przełącznika należy użyć funkcji **Save** w interfejsie głównym - konfiguracja zostanie zapisana w pliku konfiguracji startowej.

Rys. 1-4 Zapisz konfigurację

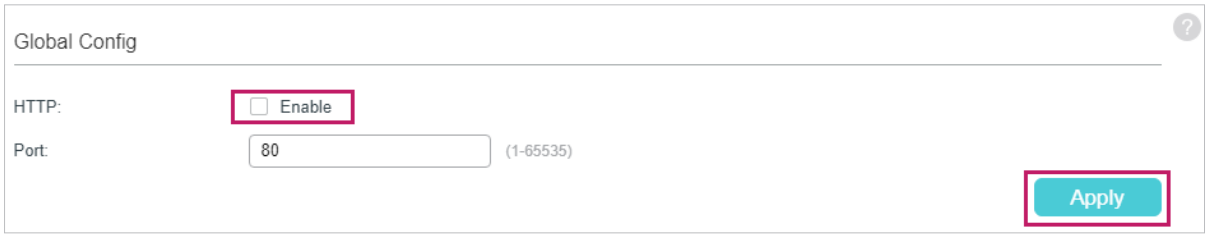


1.3 Wyłączanie serwera

Aby zablokować dostęp do interfejsu webowego, możesz wyłączyć serwer HTTP lub HTTPS.

Wybierz **SECURITY > Access Security > HTTP Config**, wyłącz serwer HTTP i kliknij Apply

Rys. 1-5 Wyłączanie serwera HTTP



Wybierz **SECURITY > Access Security > HTTPS Config**, wyłącz serwer HTTPS i kliknij **Apply**.

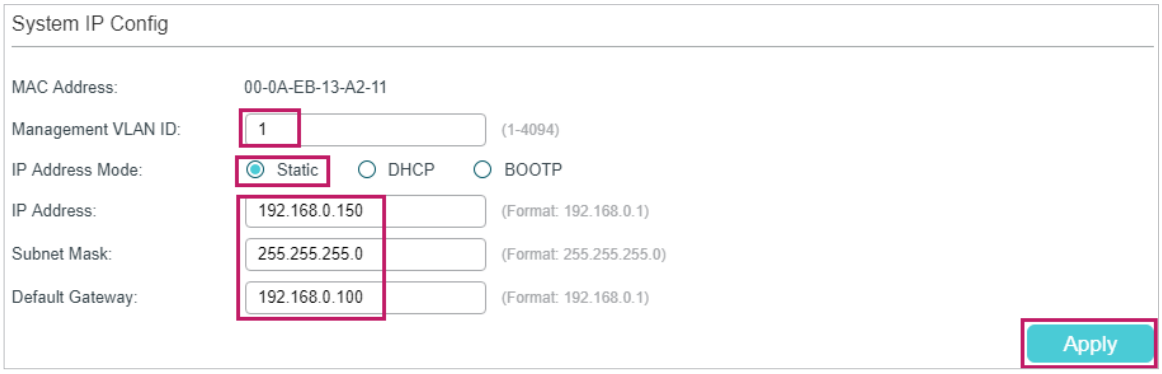
Rys. 1-6 Wyłączanie serwera HTTPS

1.4 Zmiana adresu IP i bramy domyślnej przełącznika

Jeżeli chcesz uzyskać dostęp do przełącznika, możesz ustawić adres IP przełącznika. Jeżeli chcesz, żeby przełącznik miał dostęp do sieci, możesz skonfigurować bramę domyślną urządzenia. Tylko komputery w sieci zarządzającej VLAN mają dostęp do interfejsu zarządzania przełącznikiem. Domyślnie wszystkie porty w sieci zarządzającej VLAN należą do VLAN 1, możesz więc połączyć się z przełącznikiem przez każdy port. Domyślny adres IP to **192.168.0.1**. Przełącznik nie ma bramy domyślnej. Poniższy przykład prezentuje zmianę adresu IP i bramy domyślnej przełącznika.

1) Wybierz **SYSTEM > System Info > System IP.** Podaj ID sieci zarządzającej VLAN. Ustaw tryb adresu IP jako **Static**. Wpisz nowy adres IP, maskę podsieci i bramę domyślną. Upewnij się, że ścieżka między hostem a nowym adresem IP przełącznika jest dostępna. Kliknij **Apply**.

Rys. 1-7 Zmiana IP przełącznika i bramy domyślnej



2) Aby uzyskać dostęp do przełącznika, w polu adresowym przeglądarki wpisz nowy adres IP.

3) Kliknij Save, aby zapisać ustawienia.

Uwaga:

Ustawieniem domyślnym jest pobieranie adresu IP z serwera DHCP.

2 Dostęp do interfejsu linii poleceń (CLI)

Użytkownicy mogą przez konsolę (tylko w przypadku przełączników z portem konsoli), połączenie Telnet lub SSH uzyskać dostęp do CLI przełącznika i zarządzać urządzeniem przez linie poleceń.

Połączenie przez konsolę wymaga bezpośredniego podłączenia hosta do portu konsoli przełącznika. Połączenie przez Telnet i SSH umożliwia zarówno dostęp lokalny, jak i dostęp zdalny.

Poniższa tabela prezentuje typowe wykorzystanie dostępu do interfejsu linii poleceń.

Table 2-1 Tabela sposobów połączenia

Sposób połączenia	Wykorzystywany port	Typowe zastosowanie
Konsola	Port konsoli (bezpośrednio połączony)	Hyper Terminal
Telnet	Port RJ-45	CMD
SSH	Port RJ-45	Putty

2.1 Logowanie przez Telnet

Domyślnie przełącznik wykorzystuje do uwierzytelniania tryb logowania lokalnego (Login Local Mode).

Tryb logowania lokalnego: wymagane jest podanie nazwy użytkownika i hasła (domyślna wartość obu pól to: admin).

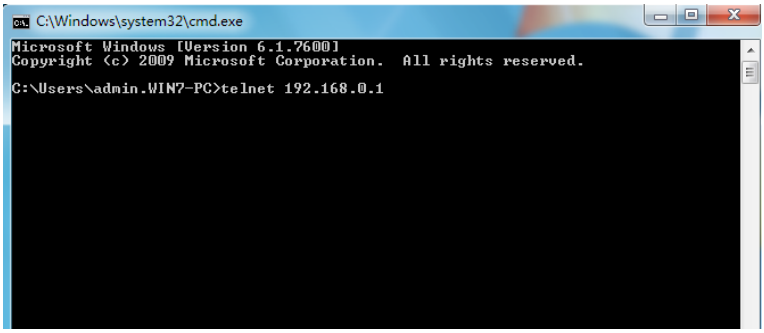
Poniższe kroki prezentują, jak zarządzać przełącznikiem poprzez tryb logowania lokalnego:

1) Upewnij się, że przełącznik i komputer należą do tej samej sieci LAN (Local Area Network). Kliknij **Start**, wpisz **cmd** w pasku wyszukiwania i kliknij Enter.

Rys. 2-2 Otwieranie okna cmd

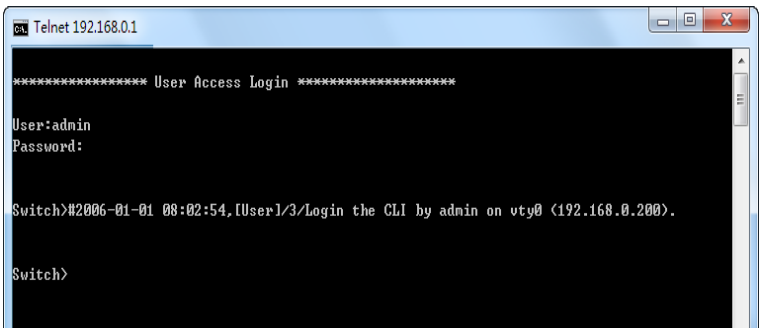
2) W oknie cmd wpisz **telnet 192.168.0.1** i kliknij **Enter**.

Rys. 2-3 Logowanie do przełącznika



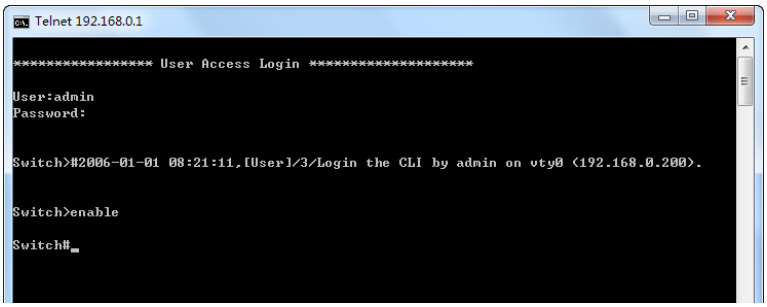
3) Wpisz nazwę użytkownika i hasło (domyślna wartość obu pól to: admin). Po kliknięciu **Enter** przejdziesz do trybu użytkownika (User EXEC Mode).

Rys. 2-4 User EXEC Mode



4) Po wpisaniu polecenia **enable** (włącz) wejdziesz w tryb użytkownika uprzywilejowanego (Privileged EXEC Mode). Domyślnie hasło nie jest wymagane. Możesz później ustawić hasło dla użytkowników, którzy chcą mieć dostęp do trybu użytkownika uprzywilejowanego.

Rys. 2-5 Privileged EXEC Mode



Możesz teraz zarządzać przełącznikiem za pomocą poleceń CLI poprzez połączenie Telnet.

2.2 Logowanie przez SSH

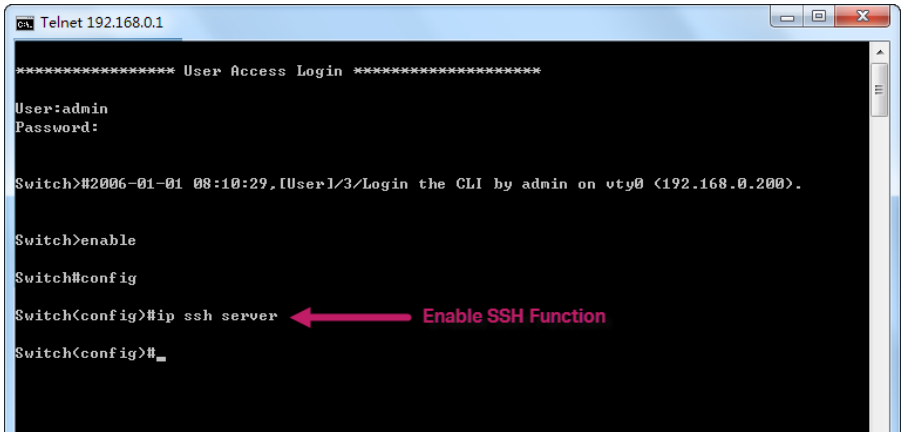
Logowanie przez SSH obsługuje dwa tryby: Password Authentication Mode (uwierzytelnianie hasła) i Key Authentication Mode (uwierzytelnianie klucza). Możesz wybrać jeden tryb, według potrzeb.

- Password Authentication Mode: wymagane jest podanie nazwy użytkownika i hasła (domyślna wartość obu pól to: admin).

- Key Authentication Mode (zalecany): wymagane jest podanie klucza publicznego do przełącznika i klucza prywatnego do oprogramowania klienta (PuTTY). Klucz publiczny i klucz prywatny możesz wygenerować przez narzędzie PuTTY Key Generator.

Przed zalogowaniem się przez SSH postępuj zgodnie z krokami przedstawionymi poniżej w celu włączenia SSH w programie emulującym terminal.

Rys. 2-6 Włączanie SSH



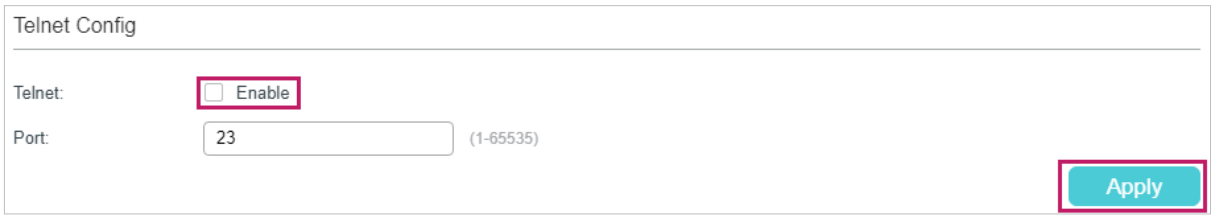
2.3 Wyłączanie logowania przez Telnet

Aby zablokować dostęp przez Telnet do interfejsu CLI, możesz wyłączyć funkcję Telnet.

- Przez GUI:

Wybierz **SECURITY > Access Security > Telnet Config**, wyłącz funkcję Telnet i kliknij **Apply**.

Figure 2-7 Wyłączanie logowania przez Telnet



- Przez CLI:

Switch#configure

Switch(config)#telnet disable

2.4 Wyłączanie logowania przez SSH

Aby zablokować dostęp przez SSH do interfejsu CLI, możesz wyłączyć serwer SSH.

- Przez GUI:

Wybierz **SECURITY > Access Security > SSH Config**, wyłącz serwer SSH i kliknij **Apply**.

Rys. 2-8 Wyłączanie serwera SSH

- Przez CLI:

Switch#configure

Switch(config)#no ip ssh server

2.5 Polecenie Copy running-config startup-config

Pliki konfiguracyjne przełącznika dzielą się na dwa typy - plik bieżącej konfiguracji i plik konfiguracji startowej.

Po wpisaniu każdej linii poleceń zmiany zostaną zapisane w pliku bieżącej konfiguracji. Po restarcie przełącznika konfiguracje zostaną utracone.

Chcąc zachować konfigurację po restarcie przełącznika należy użyć polecenia **copy running-config startup-config**, a konfiguracja zostanie zapisana w pliku konfiguracji startowej.

Switch(config)#end

Switch#copy running-config startup-config

2.6 Zmiana adresu IP i bramy domyślnej przełącznika

Jeżeli chcesz uzyskać dostęp do przełącznika, możesz ustawić adres IP przełącznika. Jeżeli chcesz, żeby przełącznik miał dostęp do sieci, możesz skonfigurować bramę domyślną urządzenia. Tylko komputery w sieci zarządzającej VLAN mają dostęp do interfejsu zarządzania przełącznikiem. Domyślnie wszystkie porty w sieci zarządzającej VLAN należą do VLAN 1, możesz więc połączyć się z przełącznikiem przez każdy port. Domyślny adres IP to **192.168.0.1**. Przełącznik nie ma bramy domyślnej. Poniższy przykład prezentuje ustawianie adresu IP przełącznika jako **192.168.0.10/24** i konfigurację bramy domyślnej jako **192.168.0.100**.

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.0.10 255.255.255.0 gateway 192.168.0.100

Połączenie zostanie zerwane. Należy wtedy połączyć się przez Telnet z nowym adresem IP przełącznika **192.168.0.10**.

C:\Users\Administrator>telnet 192.168.0.10

User:admin

Password:admin

Switch>enable

Switch#copy running-config startup-config

Część 2

Zarządzanie systemem

Rozdziały

1 System

1.1 Obsługiwane funkcje

Informacje systemowe

Na bieżąco sprawdzaj stan portów przełącznika, przeglądaj informacje systemowe, konfiguruj opisy urządzeń, czas systemowy, czas letni oraz systemowy adres IP/IPv6 (tylko dla przełączników z serii T1500/T1500G).

Zarządzanie kontami użytkowników

Zarządzaj kontami użytkowników, logujących się na stronę przełącznika. Do wyboru są różne typy użytkowników oraz różne poziomy dostępu dla kont. Dostosuj te ustawienia do swoich potrzeb.

Narzędzia systemowe

Skorzystaj z możliwości konfiguracji pliku startowego przełącznika, tworzenia kopii zapasowej ustawień i przywracania ich z pliku, aktualizacji firmware'u urządzenia, a także resetu lub restartu przełącznika.

EEE

EEE (Energy Efficient Ethernet) to technologia ograniczania zużycia energii przez przełączniki w okresach niskiego przepływu danych. Aby uruchomić oszczędzanie energii, włącz tę funkcję dla wybranych portów.

PoE

Uwaga:

Funkcję PoE obsługują tylko przełączniki T1500-28PCT, T1500G-10MPS i T1500G-10PS.

Power over Ethernet (PoE) to funkcja przesyłu energii elektrycznej do urządzeń. Przełącznik wyposażony w tę funkcję może zasilać podłączone urządzenia poprzez skrętki.

Niektóre urządzenia, takie jak telefony IP, punkty dostępowe (AP) i kamery mogą znajdować się daleko od źródła zasilania prądem przemiennym. Funkcja PoE sprawia, że urządzenia mogą być zasilane bez konieczności instalowania przewodów zasilających. W ten sposób za pomocą jednego przewodu do urządzenia przesyłane są zarówno dane, jak i energia elektryczna.

IEEE 802.3af i 802.3at to standardy PoE. Standardowy proces zasilania PoE obejmuje wykrywanie urządzeń z obsługą PoE, zarządzanie zasilaniem, wykrywanie utraty połączenia i opcjonalną klasyfikację mocy zasilanego urządzenia.

- PSE

Power Sourcing Equipment (PSE) to urządzenie, które zapewnia możliwość zasilania urządzeń PD w sieci Ethernet, takie jak przełącznik PoE. PSE jest w stanie wykryć urządzenie PD i określić wymagania dotyczące mocy urządzenia.

- Urządzenie PD

Urządzenie PD to urządzenie, które odbiera energię elektryczną od urządzenia PSE, takie jak telefon IP lub punkt dostępowy. W zależności od tego, czy urządzenie PD jest zgodne ze standardem IEEE, może być zaklasyfikowane jako standardowe lub niestandardowe. Tylko standardowe urządzenia PD mogą być zasilane przez przełączniki TP-Link PoE.

Szablon SDM

Szablon SDM (Switch Database Management) służy priorytetyzacji zasobów sprzętowych dla określonych funkcji. Przełącznik zapewnia trzy szablony, które przydzielają różnym zastosowaniom określone zasoby sprzętowe.

Przedział czasowy

Funkcja umożliwia konfigurację przedziałów czasowych oraz powiązanie ich z portami PoE i regułami ACL.

2 Konfiguracja informacji systemowych

Dostęp do ustawień systemowych umożliwia:

- podgląd wszystkich informacji systemowych;
- zmianę opisu urządzenia;
- zmianę czasu systemowego;
- konfigurację czasu letniego;
- konfigurację systemowych parametrów adresu IP (tylko przełączniki z serii T1500 i T1500G);
- konfigurację systemowych parametrów adresu IPv6 (tylko przełączniki z serii T1500 i T1500G).

2.1 Przez GUI

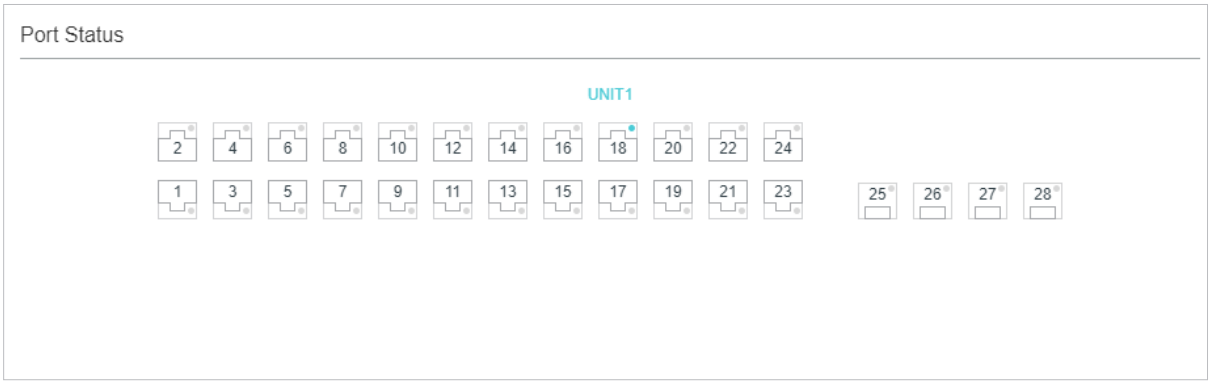
2.1.1 Podgląd najważniejszych ustawień systemowych

Aby uzyskać podgląd informacji systemowych, wybierz **SYSTEM** > **System Info** > **System Summary**. Tutaj znajdziesz informacje o stanie portów oraz ustawieniach systemowych przełącznika.

Podgląd stanu portów

W sekcji **Port Status** możesz śledzić stan oraz poziom wykorzystania przepustowości łącza dla każdego portu przełącznika.

Rys. 2-1 Podgląd informacji systemowych



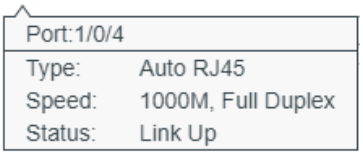
Poniższa tabela wyjaśnia znaczenie możliwych stanów portów.

Stan portu	Wyjaśnienie
	Dany port 1000 Mb/s nie jest połączony z urządzeniem.

	Dany port 1000 Mb/s działa z prędkością 1000 Mb/s.
	Dany port 1000Mb/s działa z prędkością 10 Mb/s lub 100Mb/s.
	Dany port SFP nie jest połączony z urządzeniem.
	Dany port SFP działa z prędkością 1000 Mb/s.
	Dany port SFP działa z prędkością 100 Mb/s.

Aby uzyskać szczegółowe informacje o danym porcie, najedź na niego kursorem.

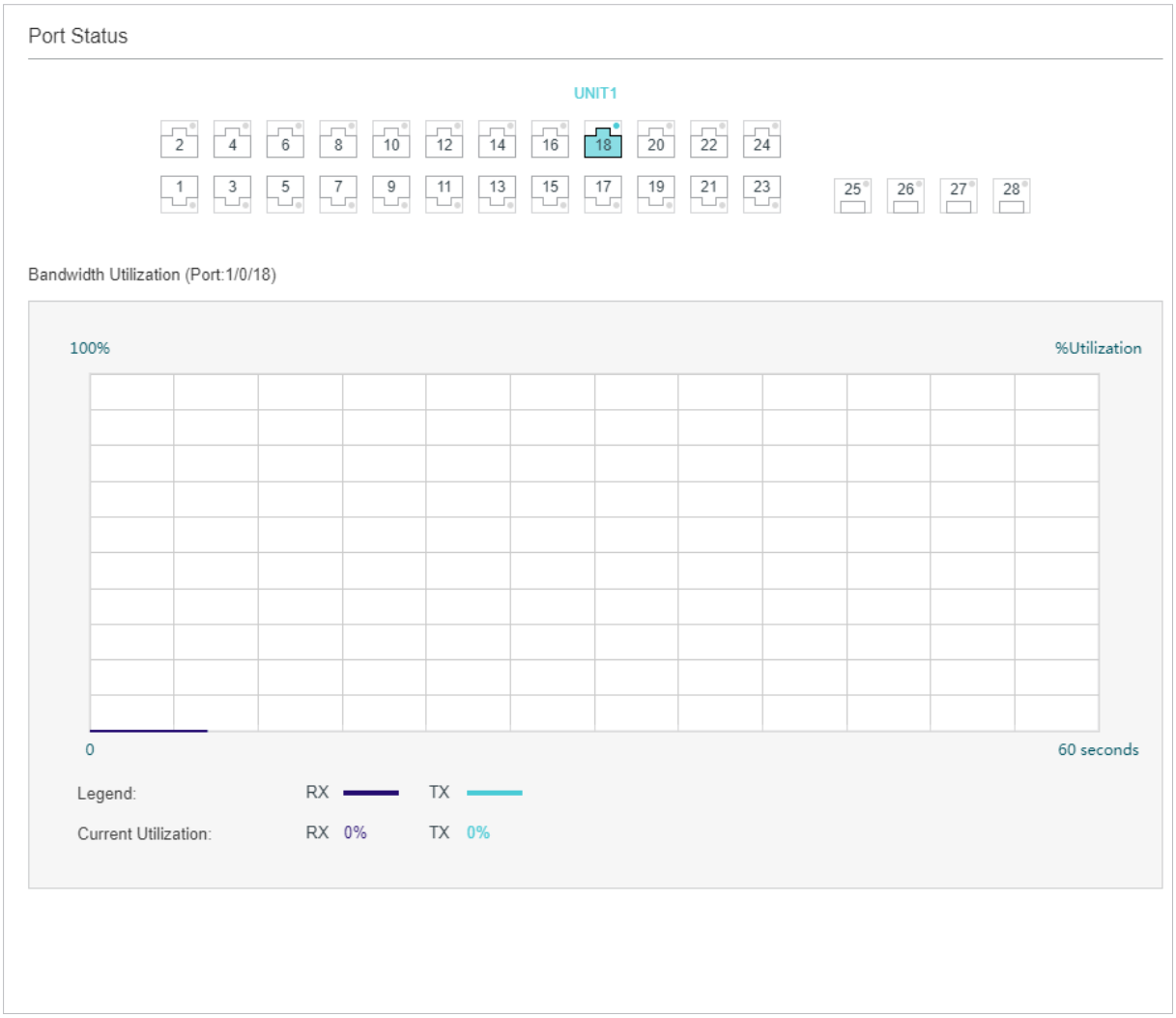
Rys. 2-2 Informacje o porcie



Informacje o porcie	Wyjaśnienie
Port	Numer portu.
Type	Typ portu
Speed	Maksymalna prędkość transmisji i tryb dupleksu portu
Status	Stan połączenia portu

Gdy klikniesz port, pojawi się informacja o jego wykorzystaniu przepustowości łącza.

Rys. 2-3 Wykorzystanie przepustowości łącza

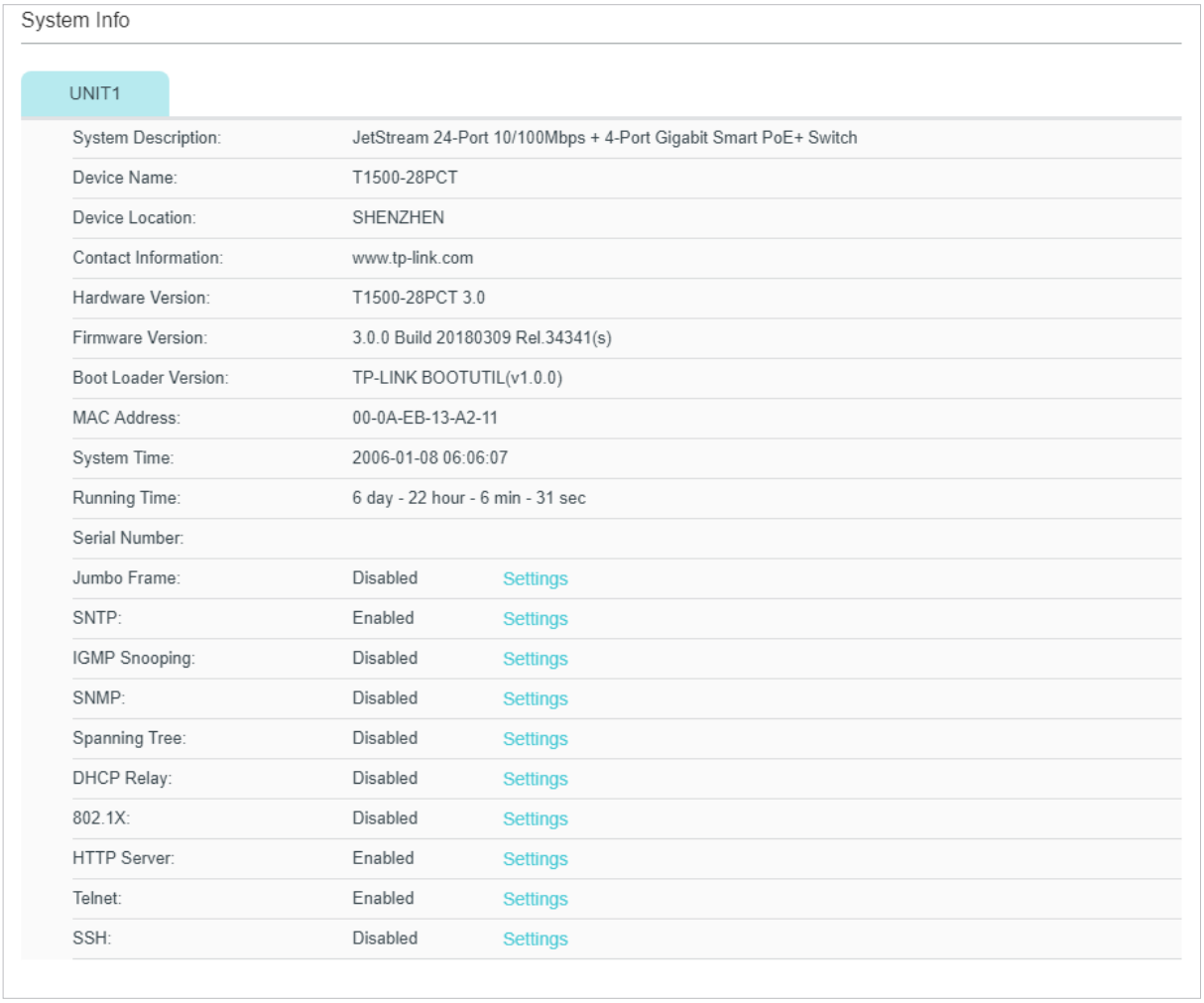


RX	Wykorzystana przepustowość łącza przez pakiety odbierane na danym porcie.
TX	Wykorzystania przepustowość łącza przez pakiety wysyłane na danym porcie.

Podgląd informacji systemowych

W sekcji **System Info** możesz uzyskać informacje systemowe na temat przełącznika.

Rys. 2-4 Informacje systemowe



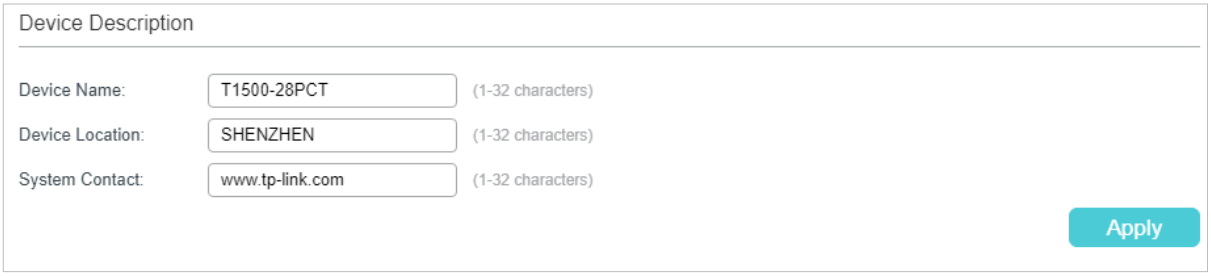
System Description	Opis systemowy przełącznika.
Device Name	Nazwa przełącznika. Możesz ją edytować na stronie Device Description.
Device Location	Lokalizacja przełącznika. Możesz ją edytować na stronie Device Description.
Contact Information	Informacje kontaktowe dla przełącznika. Możesz je edytować na stronie Device Description.
Hardware Version	Wersja sprzętowa przełącznika.
Firmware Version	Wersja firmware'u przełącznika.
Boot Loader Version	Wersja programu rozruchowego przełącznika.
MAC Address	Adres MAC przełącznika.
System Time	Czas systemowy przełącznika.

Running Time	Czas pracy przełącznika.
Serial Number	Numer seryjny przełącznika.
Jumbo Frame	Informacja o stanie ramki Jumbo (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej ramki Jumbo.
SNTP	Informacja o miejscu pobierania czasu systemowego (Serwer NTP). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej czasu systemowego.
IGMP Snooping	Informacje o stanie usługi IGMP Snooping (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej IGMP Snooping.
SNMP	Informacja o stanie usługi SNMP (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej SNMP.
Spanning Tree	Informacja o stanie usługi Spanning Tree (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej Spanning Tree.
DHCP Relay	Informacja o stanie usługi DHCP Relay (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej DHCP Relay.
802.1x	Informacja o dostępności standardu 802.1x. Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej standardu..
HTTP Server	Informacja o stanie serwera HTTP (włączony/wyłączony). o kliknięciu **Settings** przejdziesz do strony konfiguracyjnej serwera HTTP.
Telnet	Informacja o stanie sługi Telnet (włączona/wyłączona). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej Telnet.
SSH	Informacja o stanie szyfrowania SSH (włączone/wyłączone). Po kliknięciu **Settings** przejdziesz do strony konfiguracyjnej SSH.

2.1.2 Zmiana opisu urządzenia

Wybierz z menu **SYSTEM** > **System Info** > **Device Description**, aby otworzyć poniższą stronę.

Rys. 2-5 Zmiana opisu urządzenia



1) W sekcji **Device Description** skonfiguruj poniższe parametry.

Device Name	Wpisz nazwę przełącznika.

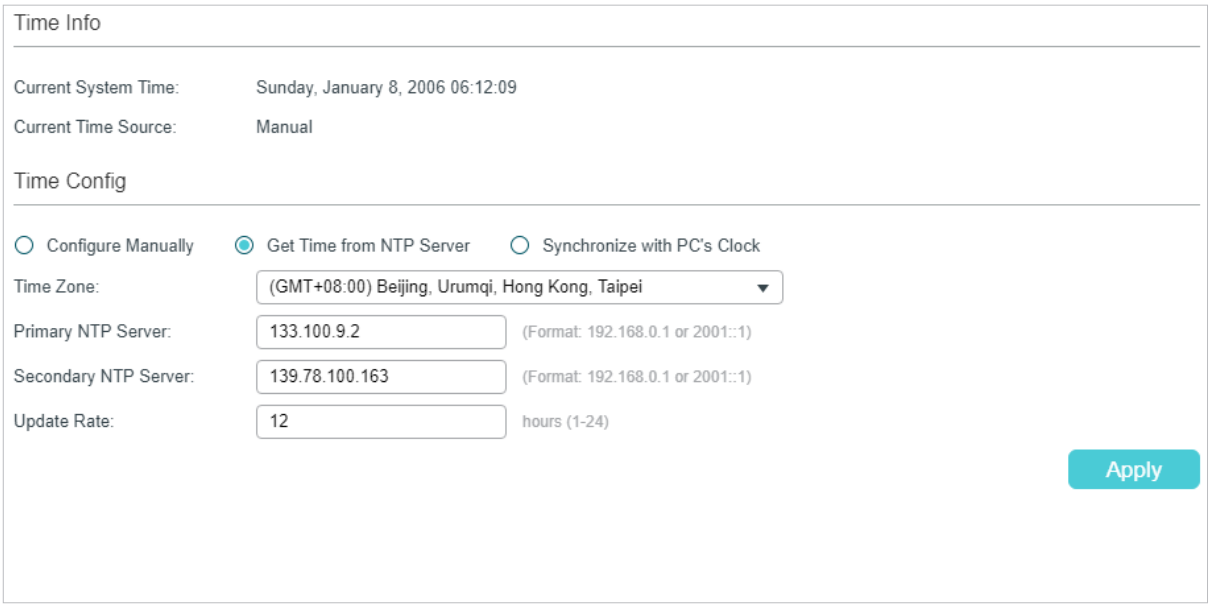
Device Location	Określ lokalizację przełącznika.
System Contact	Wprowadź informacje kontaktowe.

2) Kliknij **Apply**.

2.1.3 Zmiana czasu systemowego

Wybierz z menu **SYSTEM** > **System Info** > **System Time**, aby otworzyć poniższą stronę.

Rys. 2-6 Zmiana czasu systemowego



W sekcji **Time Info** uzyskasz informacje o aktualnym czasie przełącznika.

Current System Time	Aktualna data i czas przełącznika.
Current Time Source	Informacja o sposobie pobierania czasu przez przełącznik.

Aby skonfigurować czas systemowy, wykonaj poniższe kroki w sekcji **Time Config**:

1) Wybierz jedną metodę pobierania czasu systemowego i uzupełnij odpowiednie parametry.

Manual	Ustaw czas systemowy ręcznie. **Date**: Wprowadź datę systemową. **Time**: Wprowadź czas systemowy.

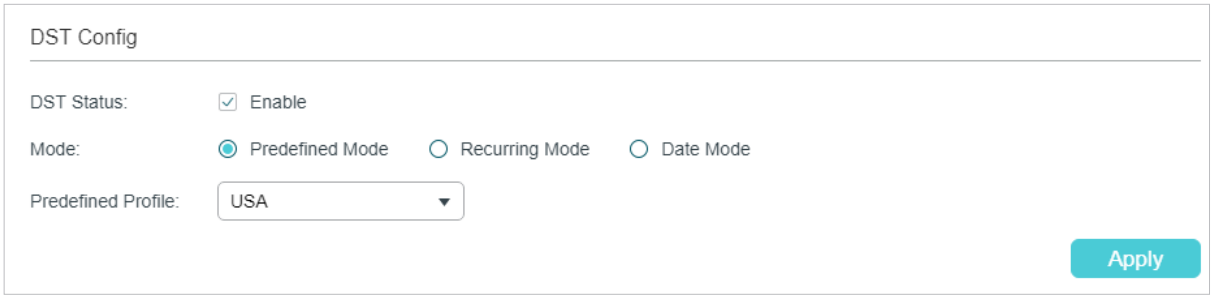
Get Time from NTP Server	Pobierz czas systemowy z serwera czasu. Upewnij się, że serwer NTP jest dostępny w twojej sieci. Jeżeli chcesz skorzystać z serwera NTP poprzez łącze internetowe, upewnij się najpierw, że przełącznik jest połączony z Internetem. **Time Zone**: Wybierz swoją strefę czasową. **Primary Server**: Wprowadź adres IP preferowanego serwera czasu. **Secondary Server**: Wprowadź adres IP alternatywnego serwera czasu. Gdy preferowany serwer czasu nie będzie dostępny, urządzenie może pobrać czas z alternatywnego serwera. **Update Rate**: Określ częstotliwość pobierania czasu z serwera NTP (od 1 do 24 godzin).
Synchronize with PC's Clock	Zsynchronizuj czas systemowy z zegarem aktualnie zalogowanego hosta..

2) Kliknij **Apply**.

2.1.4 Konfiguracja czasu letniego

Wybierz z menu **SYSTEM** > **System Info** > **Daylight Saving Time**, aby otworzyć poniższą stronę.

Rys. 2-7 Konfiguracja czasu letniego



Aby skonfigurować czas letni, wykonaj poniższe kroki:

1) W sekcji **DST Config** włącz funkcję czasu letniego.

2) Wybierz metodę ustawiania czasu letniego i uzupełnij odpowiednie parametry.

Predefined Mode	Jeżeli wybierzesz **Predefined Mode**, określ predefiniowany harmonogram czasu letniego dla przełącznika. **USA**: Czas letni w USA. Trwa od godziny 2:00 drugiej niedzieli marca do godziny 2:00 pierwszej niedzieli listopada. **Australia**: Czas letni w Australii. Trwa od godziny 2:00 pierwszej niedzieli października do 3:00 pierwszej niedzieli kwietnia. **Europe**: Czas letni w Europie. Trwa od godziny 1: 00 ostatniej niedzieli marca do godziny 1:00 ostatniej niedzieli października. **New Zealand**: Czas letni w Nowej Zelandii. Trwa od godziny 2: 00 ostatniej niedzieli września do godziny 3:00 pierwszej niedzieli kwietnia.

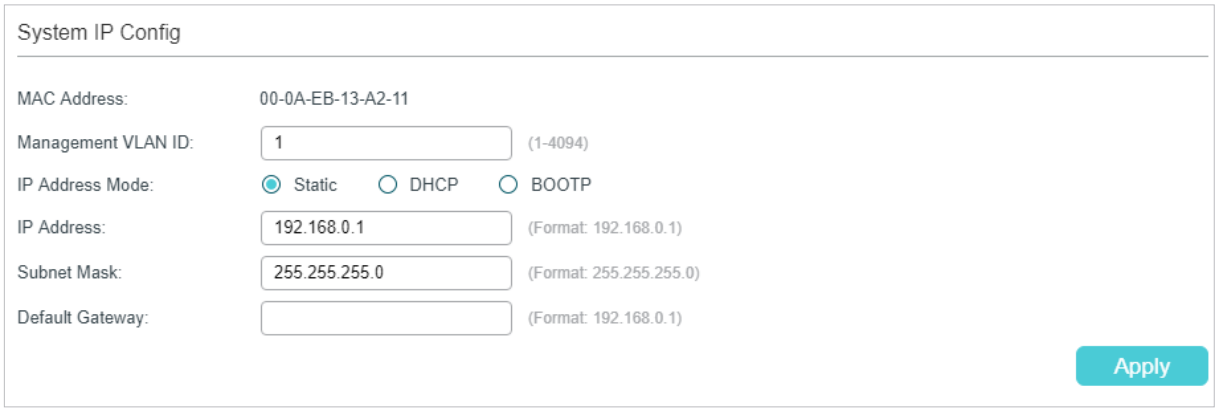
Recurring Mode	Jeżeli wybierzesz **Recurring Mode**, określ cykl czasu letniego dla przełącznika. Te ustawienia będą obowiązywać także w kolejnych latach. **Offset**: Określ wartość przesunięcia zegara do przodu. **Start Time**: Określ termin początkowy dla czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni). **End Time**: Określ termin końcowy czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).
Date Mode	Jeżeli wybierzesz **Date Mode**, określ całkowity okres czasu letniego dla przełącznika. Te ustawienia będą obowiązywać tylko jednorazowo. **Offset**: Określ wartość przesunięcia zegara do przodu. **Start Time**: Określ termin początkowy dla czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni). **End Time**: Określ termin końcowy czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).

3) Kliknij **Apply**.

2.1.5 Konfiguracja parametrów systemowych adresu IP

Wybierz z menu **SYSTEM** > **System Info** > **System IP**, aby wyświetlić poniższą stronę.

Rys. 2-8 Konfiguracja parametrów systemowych adresu IP



Aby skonfigurować parametry systemowe adresu IP, wykonaj poniższe kroki:

1) Skonfiguruj odpowiednie parametry systemowe adresu IP

Management VLAN ID	Określ sieć VLAN dla swojego przełącznika. Dostęp do interfejsu zarządzania przełącznikiem będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN. Domyślnie wybraną siecią jest VLAN 1, która obejmuje wszystkie porty, dlatego dostęp do przełącznika można uzyskać korzystając z dowolnego portu.

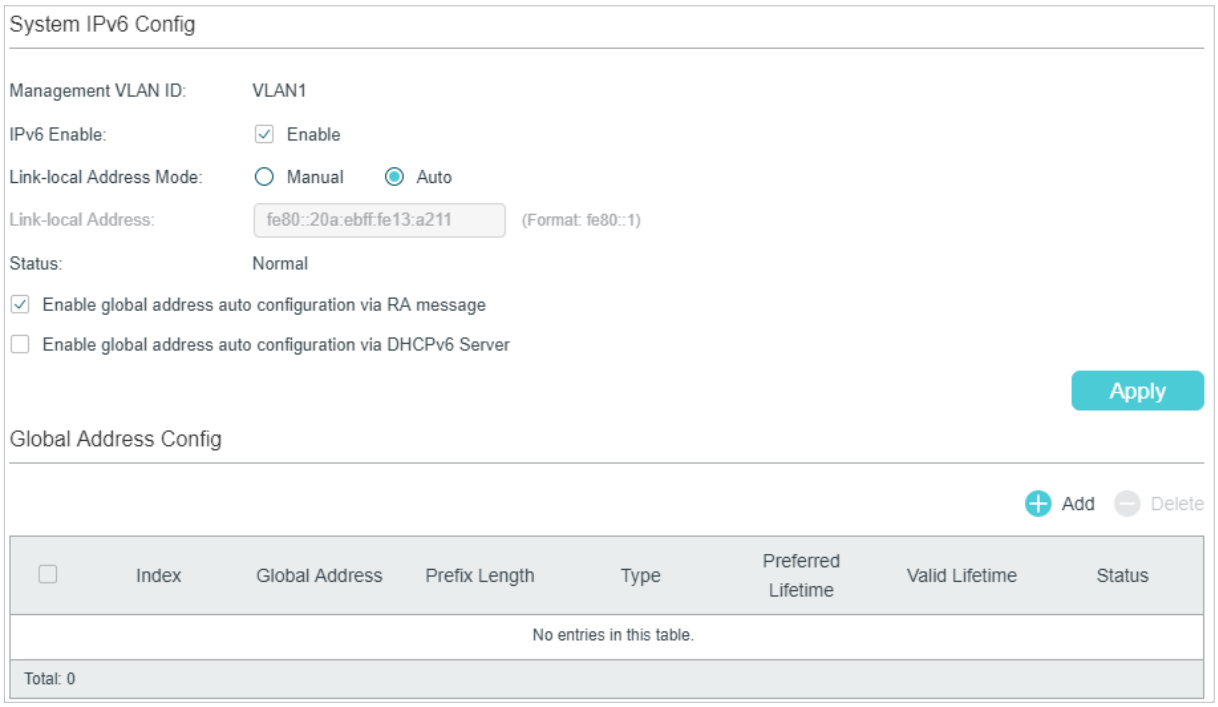
IP Address Mode	Wybierz tryb przydzielania adresów IP dla interfejsu. **Static:** Przydzielanie statycznego adresu IP dla interfejsu zarządzania. **DHCP:** Przydzielanie adresu IP dla interfejsu zarządzania poprzez serwer DHCP. **BOOTP:** Przydzielanie adresu IP dla interfejsu zarządzania poprzez serwer BOOTP.
DHCP Option 12	Jeżeli wybrałeś przydzielanie adresu IP w trybie DHCP, skonfiguruj tę opcję. DHCP Option 12 służy do określania nazwy klienta.
IP Address	Wprowadź adres IP interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static.
Subnet Mask	Wprowadź maskę podsieci interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static.
Default Gateway	Wprowadź bramę domyślną interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static. Brama domyślna to adres IP, na który pakiet zostanie następnie przesłany.

2) Kliknij **Apply**.

2.1.6 Konfiguracja parametrów systemowych adresu IPv6

Wybierz z menu **SYSTEM** > **System Info** > **System IPv6**, aby wyświetlić poniższą stronę.

Rys. 2-9 Konfiguracja systemowych parametrów adresu IPv6



1) W sekcji **System IPv6 Config** włącz funkcję IPv6 dla interfejsu i skonfiguruj odpowiednie parametry. Następnie kliknij **Apply**.

Management VLAN ID	Sieć VLAN przełącznika. Dostęp do interfejsu zarządzania przełącznikiem będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN. Domyślnie wybraną siecią jest VLAN 1, która obejmuje wszystkie porty, dlatego dostęp do przełącznika można uzyskać korzystając z dowolnego portu.
IPv6 Enable	Włącz funkcję IPv6 w interfejsie zarządzania.
Link-local Address Mode	Wybierz tryb konfiguracji adresu lokalnego dla łącza. **Manual:** Ten tryb umożliwia ręczny przydział adresu lokalnego dla łącza. **Auto:** W tym trybie przełącznik automatycznie generuje adres lokalny dla łącza.
Link-local Address	Jeżeli wybierzesz tryb "Manual", wprowadź adres lokalny dla łącza.
Status	Status adresu lokalnego dla łącza. Nie można korzystać z adresu IPv6, który nie przeszedł kontroli DAD. Duplicate Address Detection służy wykrywaniu konfliktów adresów. Podczas kontroli DAD adres IPv6 może otrzymać trzy różne statusy: **Normal:** Adres lokalny dla łącza przeszedł kontrolę DAD i można z niego korzystać. **Try:** Adres lokalny dla łącza jest w trakcie kontroli DAD i nie można z niego aktualnie korzystać. **Repeat:** Adres lokalny dla łącza został uznany za duplikat, co oznacza, że jest już używany przez inny węzeł i nie można z niego korzystać.

2) Skonfiguruj globalny adres IPv6 interfejsu, wybierając jeden z poniższych sposobów:

Poprzez wiadomość RA:

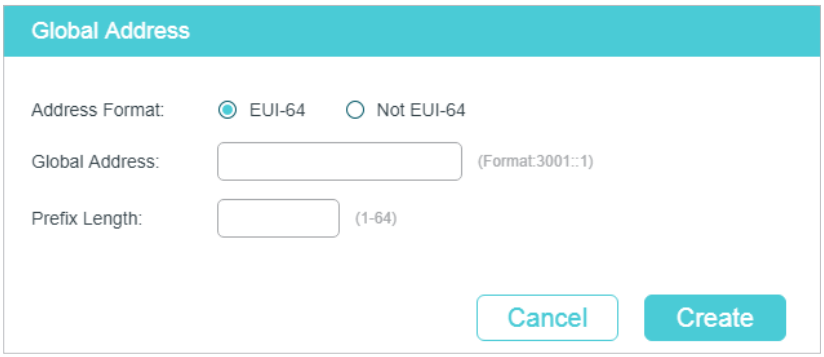
Enable global address auto configuration via RA message	Wybranie tej opcji umożliwi automatyczne wygenerowanie adresu globalnego i innych informacji przez interfejs, zgodnie z prefiksem adresu i innymi parametrami konfiguracji otrzymanymi w komunikacie RA (Router Advertisement).

Poprzez serwer DHCPv6:

Enable global address auto configuration via DHCPv6 Server	Wybranie tej opcji umożliwi przełącznikowi pobranie adresu globalnego z serwera DHCPv6.

Ręcznie:

W sekcji **Global Address Config** kliknij Add, aby ręcznie przydzielić globalny adres IPv6 do interfejsu.



Address Format	Wybierz format adresu globalnego zgodnie ze swoimi potrzebami. **EUI-64:** Oznacza, że musisz podać tylko prefiks adresu, a system automatycznie utworzy adres globalny. **Not EUI-64:** Oznacza, że musisz podać stały adres globalny.
Global Address	Jeżeli wybierzesz format EUI-64, wprowadź tutaj prefiks adresu. W innym wypadku wprowadź tutaj stały adres IPv6.
Prefix Length	Skonfiguruj długość prefiksu adresu globalnego.

3) Przeglądaj parametry globalnego adresu w sekcji **Global Address Config**.

Global Address	Sprawdź lub edytuj adres globalny.
Prefix Length	Sprawdź lub edytuj długość prefiksu adresu globalnego.
Type	Tryb konfiguracji adresu globalnego. **Manual:** Oznacza, że dany adres został skonfigurowany ręcznie. **Auto:** Oznacza, że dany adres został utworzony automatycznie, na podstawie wiadomości RA, lub został pobrany z serwera DHCPv6.
Preferred Lifetime	Okres ważności preferowania adresu globalnego. Preferred lifetime to okres preferowania ważnego adresu IPv6. Po upłynięciu tego okresu adres staje is przestarzały, ale nadal można z niego korzystać. Aby jednak urządzenie mogło nawiązać nowe połączenie, konieczna jest zmiana adresu.
Valid Lifetime	Okres ważności adresu globalnego. Valid lifetime to okres ważności adresu IPv6. Po upłynięciu tego okresu adres wygasa i nie można już z niego korzystać.

Status	Status adresu lokalnego dla łącza. Nie można korzystać z adresu IPv6, który nie przeszedł kontroli DAD. Duplicate Address Detection służy wykrywaniu konfliktów adresów. Podczas kontroli DAD adres IPv6 może otrzymać trzy różne statusy: **Normal:** Adres lokalny dla łącza przeszedł kontrolę DAD i można z niego korzystać. **Try:** Adres lokalny dla łącza jest w trakcie kontroli DAD i nie można z niego aktualnie korzystać. **Repeat:** Adres lokalny dla łącza został uznany za duplikat, co oznacza, że jest już używany przez inny węzeł i nie można z niego korzystać.

2.2 Przez CLI

2.2.1 Podgląd najważniejszych informacji systemowych

Aby uzyskać podgląd informacji systemowych przełącznika w trybie uprzywilejowanym (privileged EXEC mode) lub w innym trybie konfiguracji, można skorzystać z poniższych poleceń:

show interface status [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port*]

Wyświetla stan interfejsu.

port: Wprowadź numer portu Ethernet.

show system-info

Wyświetla informacje systemowe, w tym opis systemowy, nazwę urządzenia, lokalizację urządzenia, informacje kontaktowe, wersję sprzętową, wersję firmware'u, czas systemowy, czas działania itd..

Poniższy przykład przedstawia sposób, w jaki można sprawdzić stan interfejsu i uzyskać dostęp do informacji systemowych przełącznika.

Switch#show interface status

Port	Status	Speed	Duplex	FlowCtrl	Jumbo	Active-Medium
Gi1/0/1	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/2	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/3	LinkUp	1000M	Full	Disable	Disable	Copper

...

Switch#show system-info

System Description - JetStream 48-Port Gigabit Smart Switch with 4 SFP Slots

System Name - T1500-28PCT

System Location - SHENZHEN

Contact Information - www.tp-link.com

Hardware Version - T1500-28PCT 3.0

Software Version - 3.0.0 Build 20171129 Rel.38400(s)

Bootloader Version - TP-LINK BOOTUTIL(v1.0.0)

Mac Address - 00-0A-EB-13-23-A0

Serial Number -

System Time - 2017-12-12 11:23:32

Running Time - 1 day - 2 hour - 33 min - 42 sec

2.2.2 Konfiguracja opisu urządzenia

Wykonaj poniższe kroki, aby skonfigurować opis urządzenia:

Krok 1	**configure** Włącz tryb konfiguracji globalnej.
Krok 2	**hostname [** *hostname* **]** Określ nazwę systemową przełącznika. *hostname*: Podaj nazwę urządzenia, wprowadzając od 1 do 32 znaków. Domyślną nazwą jest model przełącznika.
Krok 3	**location [** *location* **]** Określ lokalizację systemową przełącznika. *location*: Wprowadź lokalizację urządzenia. Pole może zawierać maksymalnie 32 znaki. Domyślną lokalizacją jest “SHENZHEN”.
Krok 4	**contact-info [** *contact-info* **]** Podaj systemowe informacje kontaktowe. *contact-info*: Wprowadź informacje kontaktowe. Pole może zawierać maksymalnie 32 znaki. Domyślnie podany jest adres “www.tp-link.com”.
Krok 5	**show system-info** Sprawdź informacje systemowe, w tym opis systemowy, nazwę urządzenia, lokalizację urządzenia, informacje kontaktowe, wersję sprzętową, wersję firmware’u, czas systemowy, czas działania itd.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację parametrów, w tym ustawianie Switch_A jako nazwy urządzenia, BEIJING jako lokalizacji oraz http://www.tp-link.com jako informacji kontaktowych.

Switch#configure

Switch(config)#hostname Switch_A

Switch(config)#location BEIJING

Switch(config)#contact-info http://www.tp-link.com

Switch(config)#show system-info

System Description - JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots

System Name - Switch_A

System Location - BEIJING

Contact Information - http://www.tp-link.com

...

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Konfiguracja czasu systemowego

Wykonaj poniższe kroki, aby skonfigurować czas systemowy:

Uwaga:

Tryb Synchronize with PC's Clock nie może być obsługiwany za pomocą poleceń CLI.

Krok 1	**configure** Włącz tryb konfiguracji globalnej.

Krok 2 Skorzystaj z poniższego polecenia, aby ustawić czas systemowy ręcznie:

system-time manual *time*

Skonfiguruj czas systemowy ręcznie.

time: Ręcznie wprowadź datę i czas w formacie MM/DD/RRRR-GG:MM:SS. Poprawna wartość roku mieści się w przedziale 2000 - 2037.

Skorzystaj z poniższej komendy, aby ustawić czas systemowy poprzez pobranie go z serwera NTP. Upewnij się, że serwer NTP jest dostępny. Jeżeli serwer NTP wymaga połączenia internetowego, połącz najpierw przełącznik z Internetem.

system-time ntp { *timezone* **} {** *ntp-server* **} {** *backup-ntp-server* **} {** *fetching-rate* **}**

timezone: Określ swoją lokalną strefę czasową, wybierając z przedziału UTC-12:00 - UTC+13:00.

Poniższej znajdziesz informacje o poszczególnych strefach czasowych:

UTC-12:00 —— Strefa czasowa zachodniej strony linii zmiany daty.

UTC-11:00 —— Uniwersalny czas koordynowany-11.

UTC-10:00 —— Strefa czasowa Hawajów.

UTC-09:00 —— Strefa czasowa Alaski.

UTC-08:00 —— Czas pacyficzny (US, Kanada).

UTC-07:00 —— Czas górski (US, Kanada).

UTC-06:00 —— Czas centralny (US, Kanada).

UTC-05:00 —— Czas wschodni (US, Kanada).

UTC-04:30 —— Strefa czasowa Caracas.

UTC-04:00 —— Czas atlantycki (Kanada).

UTC-03:30 —— Strefa czasowa Nowej Fundlandii.

UTC-03:00 —— Strefa czasowa Buenos Aires, Salvadoru, Brasilii.

UTC-02:00 —— Strefa czasowa Stanów Środkowoatlantyckich.

UTC-01:00 —— Strefa czasowa Azorów i Republiki zielonego przylądka.

UTC —— Strefa czasowa Dublinu, Edynburgu, Lizbony, Londynu.

UTC+01:00 —— Strefa czasowa Amsterdamu, Berlina, Berna, Rzymu, Sztokholmu, Wiednia.

UTC+02:00 —— Strefa czasowa Kairu, Aten, Bukaresztu, Ammanu, Bejrutu, Jerozolimy.

UTC+03:00 —— Strefa czasowa Kuwejtu, Rijadu, Bagdadu.

UTC+03:30 —— Strefa czasowa Teheranu.

UTC+04:00 —— Strefa czasowa Moskwy, Petersburgu, Wołgogradu, Tbilisi, Portu Louis.

UTC+04:30 —— Strefa czasowa Kabulu.

UTC+05:00 —— Strefa czasowa Islamabadu, Karaczi, Taszkentu.

	UTC+05:30 —— Strefa czasowa Madrasu, Kalkuty, Bombaju, Nowego Delhi. UTC+05:45 —— Strefa czasowa Katmandu. UTC+06:00 —— Strefa czasowa Dhaki, Astany, Jekaterynburgu. UTC+06:30 —— Strefa czasowa Rangunu. UTC+07:00 —— Strefa czasowa Nowosybirska, Bangkoku, Hanoi, Dżakarty. UTC+08:00 —— Strefa czasowa Pekinu, Chongqingu, Hongkongu, Urumczi, Singapuru. UTC+09:00 —— Strefa czasowa Seulu, Irkucka, Osaki, Sapporo, Tokio. UTC+09:30 —— Strefa czasowa Darwina, Adelaide. UTC+10:00 —— Strefa czasowa Canberry, Melbourne, Sydney, Brisbane. UTC+11:00 —— Strefa czasowa Wysp Salomona, Nowej Kaledonii, Władywostoku. UTC+12:00 —— Strefa czasowa Fidżi, Magadanu, Auckland, Welington. UTC+13:00 —— Strefa czasowa Nuku'alofa, Samoa. *ntp-server*: Podaj adres IP preferowanego serwera NTP. *backup-ntp-server*: Podaj adres IP alternatywnego serwera NTP. *fetching-rate*: Określ interwał pobierania z serwera NTP.
Krok 3	Skorzystaj z poniższego polecenia, aby zweryfikować informacje o czasie systemowy. **show system-time** Sprawdź czas systemowy. Skorzystaj z poniższego polecenia, aby zweryfikować informacje dotyczące ustawień trybu serwera NTP. **show system-time ntp** Sprawdź czas systemowy trybu NTP.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację czasu systemowego za pomocą trybu pobierania czasu z serwera NTP, strefy czasowej jako UTC+08:00, serwera NTP jako 133.100.9.2, alternatywnego serwera NTP jako 139.78.100.163 oraz częstotliwości aktualizacji jako 11.

Switch#configure

Switch(config)#system-time ntp UTC+08:00 133.100.9.2 139.78.100.163 11

Switch(config)#show system-time ntp

Time zone : UTC+08:00

Prefered NTP server: 133.100.9.2

Backup NTP server: 139.78.100.163

Last successful NTP server: 133.100.9.2

Update Rate: 11 hour(s)

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Konfiguracja czasu letniego

Wykonaj poniższe kroki, aby skonfigurować czas letni:

Krok 1	**configure** Włącz tryb konfiguracji globalnej.
Krok 2	Skorzystaj z poniższego polecenia, aby wybrać gotową konfigurację czasu letniego: **system-time dst predefined [** USA | Australia | Europe | New-Zealand **]** Określ czas letni za pomocą predefiniowanego harmonogramu. USA | Australia | Europe | New-Zealand: Wybierz tryb czasu letniego. **USA**: Od 02:00 drugiej niedzieli marca do 02:00 pierwszej niedzieli listopada. **Australia**: Od 02:00 pierwszej niedzieli października do 03:00 pierwszej niedzieli kwietnia. **Europe**: Od 01:00 ostatniej niedzieli marca do 01:00 ostatniej niedzieli października. **New Zealand**: Od 02:00 ostatniej niedzieli września do 03:00 pierwszej niedzieli kwietnia. Skorzystaj z poniższego polecenia, aby ustawić tryb cykliczny czasu letniego: **system-time dst recurring {** *sweek* **} {** *sday* **} {** *smonth* **} {** *stime* **} {** *eweek* **} {** *eday* **} {** *emonth* **} {** *etime* **} [** *offset* **]** Określ okres czasu letniego w trybie cyklicznym. *sweek*: Podaj tydzień początku czasu letniego. Do wyboru jest 5 wartości: first, second, third, fourth, last (pierwszy, drugi, trzeci, czwarty, ostatni). *sday*: Podaj dzień tygodnia początku czasu letniego. Do wyboru jest 7 dni tygodnia: Sun, Mon, Tue, Wed, Thu, Fri, Sat. *smonth*: Podaj miesiąc początku czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *stime*: Podaj godzinę początku czasu letniego w formacie GG:MM. *eweek*: Podaj tydzień końca czasu letniego. Do wyboru jest 5 wartości: first, second, third, fourth, last (pierwszy, drugi, trzeci, czwarty, ostatni). *eday*: Podaj dzień tygodnia końca czasu letniego. Do wyboru jest 7 dni tygodnia: Sun, Mon, Tue, Wed, Thu, Fri, Sat. *emonth*: Podaj miesiąc końca czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *etime*: Podaj godzinę końca czasu letniego w formacie GG:MM. *offset*: Podaj wartość przesunięcia zegara do przodu. Wartością domyślną jest 60.

	Skorzystaj z poniższego polecenia, aby ustawić całkowity okres czasu letniego: **system-time dst date { *smonth* } { *sday* } { *stime* } { *syear* } { *emonth* } { *eday* } { *etime* } { *eyear* } [*offset*]** Określ czas letni, ustawiając jego całkowity okres. *smonth*: Podaj miesiąc początku czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *sday*: Podaj datę początku czasu letniego, wybierając wartość z przedziału 1 - 31. *stime*: Podaj godzinę początku czasu letniego w formacie GG:MM. *syear*: Podaj rok początkowy dla czasu letniego. *emonth*: Podaj miesiąc końca czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *eday*: Podaj datę końca czasu letniego, wybierając wartość z przedziału 1 - 31. *etime*: Podaj godzinę końca czasu letniego w formacie GG:MM. *eyear*: Podaj rok końcowy dla czasu letniego. *offset*: Podaj wartość przesunięcia zegara do przodu. Wartością domyślną jest 60.
Krok 3	**show system-time dst** Zweryfikuj informacje dotyczące czasu letniego przełącznika.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację czasu letniego do Date Mode. Terminem początkowym będzie godzina 01:00 1 sierpnia 2017, a terminem końcowym godzina 01:00 1 września 2017, natomiast wartością przesunięcia 50.

Switch#configure

Switch(config)#system-time dst date Aug 1 01:00 2017 Sep 1 01:00 2017 50

Switch(config)#show system-time dst

DST starts at 01:00:00 on Aug 1 2017

DST ends at 01:00:00 on Sep 1 2017

DST offset is 50 minutes

DST configuration is one-off

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Konfiguracja parametrów systemowych adresu IP

Wykonaj poniższe kroki, aby skonfigurować parametry systemowe adresu IP.

Krok 1	**configure** Włącz tryb konfiguracji globalnej.
Krok 2	**ip management-vlan** { *vlan-id*} Skonfiguruj sieć VLAN przełącznika. Dostęp do interfejsu zarządzania przełącznikiem będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN.
Krok 3	**interface vlan** { *vlan-id*} Wybierz tryb Interface VLAN. *vlan-id:* ID sieci VLAN przełącznika.
Krok 4	Automatycznie przydziel adres IP i bramę domyślną interfejsowi zarządzania poprzez serwer DHCP lub BOOTP: **ip address-alloc {** dhcp **|** bootp **}** Określ tryb przydziału adresu IP dla interfejsu zarządzania. dhcp: Określ interfejs zarządzania, aby pobrać adres IPv4 z serwera DHCP. bootp: Określ interfejs zarządzania, aby pobrać adres IPv4 z serwera BOOTP. Ręcznie przydziel adres IP i bramę domyślną interfejsowi zarządzania: **ip address {** *ip-addr* **} {** *mask* **} gateway {** *default-gateway* **}** Skonfiguruj ręcznie adres IP i bramę domyślną dla interfejsu zarządzania. *ip-addr*: Określ adres IP interfejsu zarządzania. *mask*: Określ maskę podsieci interfejsu zarządzania. *default gateway*: Wprowadź bramę domyślną interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static. Brama domyślna to adres IP, na który pakiet zostanie następnie przesłany.
Krok 5	**show interface vlan {** *vlan-id* **}** *vlan-id:* ID sieci VLAN przełącznika. Zweryfikuj najważniejsze informacje dotyczące interfejsu zarządzania.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację adresu IP przełącznika jako **192.168.0.10/24** i bramy domyślnej jako **192.168.0.100**.

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.0.10 255.255.255.0 gateway 192.168.0.100

The connection will be interrupted and you should telnet to the switch's new IP address **192.168.0.10**.

C:\Users\Administrator>telnet 192.168.0.10

User:admin

Password:admin

Switch>enable

Switch#show interface vlan 1

Switch#copy running-config startup-config

2.2.6 Konfiguracja parametrów systemowych adresu IPv6

Wykonaj poniższe kroki, aby skonfigurować systemowe parametry adresu IPv6.

Krok 1	**configure** Włącz tryb konfiguracji globalnej.
Krok 2	**ip management-vlan** { *vlan-id*} Skonfiguruj sieć VLAN przełącznika. Dostęp do interfejsu zarządzania przełącznikiem będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN.
Krok 3	**interface vlan** { *vlan-id*} Wybierz tryb Interface VLAN. *vlan-id:* ID sieci VLAN przełącznika.
Krok 4	**ipv6 enable** Włącz funkcję IPv6 w interfejsie zarządzania.
Krok 5	Skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: Ręcznie skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: **ipv6 address** *ipv6-addr* **link-local** *ipv6-addr*: Wprowadź adres lokalny dla łącza. Powinien to być standardowy adres IPv6 z prefiksem fe80::/10, w przeciwnym razie polecenie to będzie nieprawidłowe. Automatycznie skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: **ipv6 address autoconfig**

Krok 6	Skonfiguruj globalny adres IPv6 dla interfejsu zarządzania: Automatycznie skonfiguruj globalny adres IPv6 interfejsu za pomocą komunikatu RA: **ipv6 address ra** Skonfiguruj globalny adres IPv6 zgodnie z prefiksem adresu i innymi parametrami konfiguracji otrzymanymi w komunikacie RA (Router Advertisement). Automatycznie skonfiguruj globalny adres IPv6 interfejsu poprzez serwer DHCPv6: **ipv6 address dhcp** Włącz funkcję klienta DHCPv6. Gdy funkcja jest włączona, interfejs warstwy 3 podejmie próbę uzyskania adresu IPv6 z serwera DHCPv6. Ręcznie skonfiguruj globalny adres IPv6 interfejsu: **ipv6 address** *ipv6-addr* *ipv6-addr:* Globalny adres IPv6 z prefiksem sieci, np. 3ffe::1/64. **ipv6 address** *ipv6-addr* **eui-64** Określ globalny adres IPv6 za pomocą extended unique identifier (EUI) w 64 bitach niższego rzędu adresu IPv6. Podaj tylko prefiks sieci; końcowe 64 bity są automatycznie obliczane z adresu MAC przełącznika. To umożliwia przetwarzanie IPv6 na poziomie interfejsu.
Krok 7	**show ipv6 interface** Zweryfikuj skonfigurowane ustawienia IPv6.
Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji IPv6 i konfiguracji parametrów IPv6 interfejsu zarządzania:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ipv6 enable

Switch(config-if)#ipv6 address autoconfig

Switch(config-if)#ipv6 address dhcp

Switch(config-if)#show ipv6 interface

Vlan2 is up, line protocol is up

IPv6 is enable, Link-Local Address: fe80::20a:ebff:fe13:237b[NOR]

Global Address RA: Disable

Global Address DHCPv6: Enable

Global unicast address(es): ff02::1:ff13:237b

Joined group address(es): ff02::1

ICMP error messages limited to one every 1000 milliseconds

ICMP redirects are enable

MTU is 1500 bytes

ND DAD is enable, number of DAD attempts: 1

ND retrans timer is 1000 milliseconds

ND reachable time is 30000 milliseconds

Switch(config-if)#end

Switch#copy running-config startup-config

3 Zarządzanie kontami użytkowników

Dzięki funkcji zarządzania kontami możesz tworzyć i zarządzać kontami użytkowników logujących się do przełącznika.

3.1 Przez GUI

Do wyboru są cztery typy kont użytkowników, o różnych poziomach dostępu: Admin, Operator, Power User oraz User.

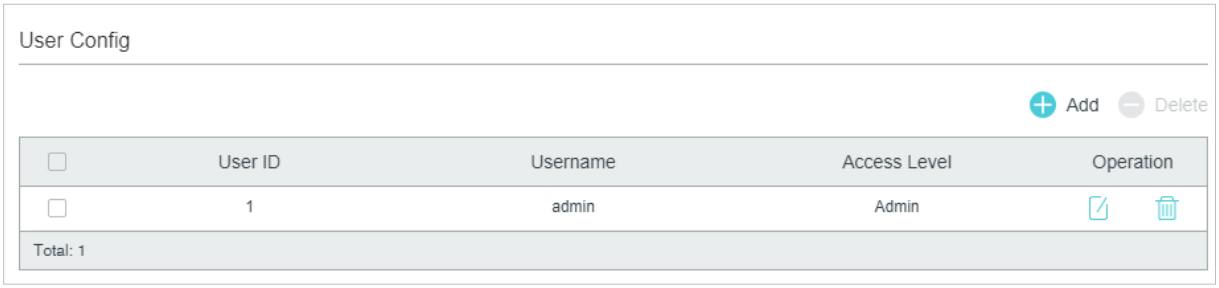
- Admin jest kontem domyślnym i nie można go usunąć. Domyślną nazwą użytkownika i hasłem dla tego konta jest admin. Możesz także tworzyć dodatkowe konta Admin.

- Jeżeli utworzysz konto Operator, Power User lub User, przejdź do sekcji AAA, aby utworzyć hasło dostępu. Te typy użytkowników mogą także korzystać z hasła dostępu, aby zmienić swój poziom dostępu i otrzymać uprawnienia administratora.

3.1.1 Tworzenie kont

Wybierz z menu **SYSTEM** > **User Management** > **User Config**, aby wyświetlić poniższą stronę.

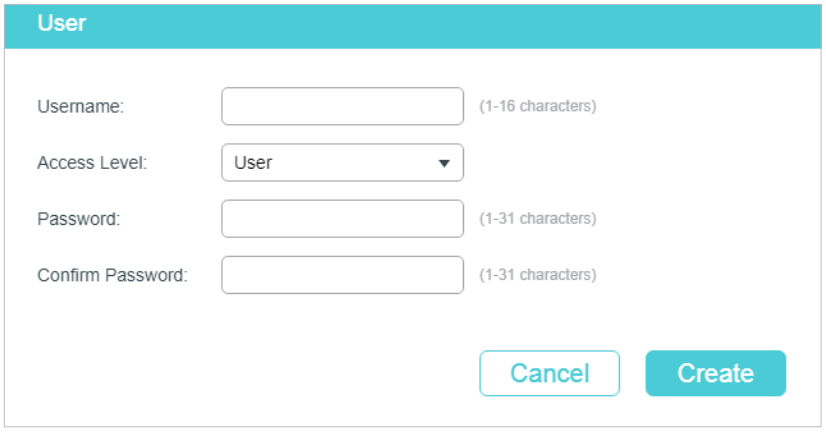
Rys. 3-1 Strona konfiguracji kont użytkowników



Domyślnie w tabeli znajduje się konto Admin. Możesz kliknąć , aby edytować to konto, ale nie możesz go usunąć.

Utwórz nowe konto użytkownika. Kliknij Add, a pojawi się poniższe okno.

Rys. 3-2 Dodawanie konta



Wykonaj poniższe kroki, aby utworzyć nowe konto użytkownika.

1) Skonfiguruj poniższe parametry:

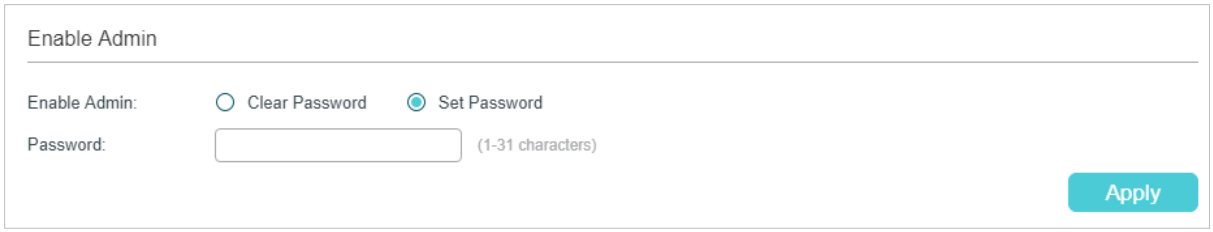
Username	Podaj nazwę użytkownika dla konta. Może ona zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego lub znaki podkreślenia.
Access Level	Wybierz poziom dostępu. Do wyboru są cztery opcje: **Admin**: Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. **Operator**: Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. **Power User**: Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. **User**: Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.
Password	Podaj hasło dla konta, wprowadzając od 1 do 31 znaków alfanumerycznych. Możesz korzystać z cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnastu znaków specjalnych. .
Confirm Password	Wprowadź ponownie hasło.

2) Kliknij **Create**.

3.1.2 Konfiguracja hasła dostępu

Wybierz z menu **SECURITY** > **AAA** > **Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja hasła dostępu



Wykonaj poniższe kroki, aby skonfigurować hasło dostępu:

1) Wybierz **Set Password** i wpisz hasło dostępu w polu **Password**.
2) Kliknij **Apply**.

Wskazówka:

Zalogowani użytkownicy mogą podać na tej stronie hasło dostępu, aby otrzymać uprawnienia administratorskie.

3.2 Przez CLI

Do wyboru są cztery typy kont użytkowników, o różnych poziomach dostępu: Admin, Operator, Power User oraz User.

- Admin jest kontem domyślnym i nie można go usunąć. Domyślną nazwą użytkownika i hasłem dla tego konta jest admin. Możesz także tworzyć dodatkowe konta Admin.
- Jeżeli utworzysz konto Operator, Power User lub User, przejdź do sekcji AAA, aby utworzyć hasło dostępu. Te typy użytkowników mogą także korzystać z hasła dostępu, aby zmienić swój poziom dostępu i otrzymać uprawnienia administratora.

3.2.1 Tworzenie kont

Wykonaj poniższe kroki, aby utworzyć konto:

Krok 1	**configure** Włącz tryb konfiguracji globalnej.

Krok 2 Skorzystaj z poniższego polecenia, aby utworzyć konto nieszyfrowane lub szyfrowane symetrycznie.

user name *name* **{ privilege** admin | operator | power_user | user **} password {** [0] *password* **|** 7 *encrypted-password* **}**

name: Podaj nazwę użytkownika, która posłuży za login do konta. Nazwa może zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego i znaki podkreślenia.

admin | operator | power_user | user: Określ poziom dostępu dla użytkownika. Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.

0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane i w takiej formie zapisywane jest w pliku konfiguracyjnym. Domyślnie ustawioną wartością jest 0.

password: Podaj hasło, potrzebne do logowania na konto. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.

7: Wybierz typ szyfrowania. 7 oznacza, że hasło jest szyfrowane symetrycznie i w takiej formie zapisywane jest w pliku konfiguracyjnym.

encrypted-password: Wprowadź hasło szyfrowane symetrycznie o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb.

Skorzystaj z poniższego polecenia, aby utworzyć konto szyfrowane algorytmem MD5.

user name *name* **{ privilege** admin | operator | power_user | user **} secret {** [0] *password* **|** 5 *encrypted-password* **}**

Utwórz konto o poziomie dostępu Admin.

name: Podaj nazwę użytkownika, która posłuży za login do konta. Nazwa może zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego i znaków podkreślenia.

admin | operator | power_user | user: Określ poziom dostępu dla użytkownika. Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.

0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane, ale hasło zapisane w pliku konfiguracyjnym ma szyfrowanie MD5. Domyślnie ustawioną wartością jest 0.

password: EPodaj hasło, potrzebne do logowania na konto. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.

5: Wybierz typ szyfrowania. 5 oznacza, że hasło ma szyfrowanie MD5 encrypted i w takiej formie zapisywane jest w pliku konfiguracyjnym.

encrypted-password: Wprowadź hasło z szyfrowaniem MD5 o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika.

Krok 3 **show user account-list**
Zweryfikuj szczegóły utworzonych kont.

Krok 4 **end**
Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

3.2.2 Konfiguracja hasła dostępu

Wykonaj poniższe kroki, aby utworzyć konto innego typu:

Krok 1	**configure** Włącz tryb konfiguracji globalnej..
Krok 2	**aaa enable** Włącz globalnie funkcję AAA.
Krok 3	Skorzystaj z poniższego polecenia, aby utworzyć hasło dostępu nieszyfrowane lub szyfrowane symetrycznie. **enable admin password { [** 0 **]** *password* | 7 *encrypted-password* **}** Utwórz hasło dostępu. Poziom dostępu użytkownika może zmienić się na Admin. Domyślnie to pole jest puste. 0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane i w takiej formie zapisywane jest w pliku konfiguracyjnym. Domyślnie ustawioną wartością jest 0.. *password*: Podaj hasło dostępu. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych. 7: Wybierz typ szyfrowania. 7 oznacza, że hasło jest szyfrowane symetrycznie i w takiej formie zapisywane jest w pliku konfiguracyjnym. *encrypted-password*: Wprowadź hasło szyfrowane symetrycznie o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb. Skorzystaj z poniższego polecenia, aby utworzyć hasło dostępu nieszyfrowane lub szyfrowane algorytmem MD5. **enable admin secret { [** 0 **]** *password* | 5 *encrypted-password* **}** Utwórz hasło dostępu. Poziom dostępu użytkownika może zmienić się na Admin. Domyślnie to pole jest puste. 0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane, ale hasło zapisane w pliku konfiguracyjnym ma szyfrowanie MD5. Domyślnie ustawioną wartością jest 0. *password*: Podaj hasło dostępu. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych. 5: Wybierz typ szyfrowania. 5 oznacza, że hasło ma szyfrowanie MD5 encrypted i w takiej formie zapisywane jest w pliku konfiguracyjnym. *encrypted-password*: Wprowadź hasło z szyfrowaniem MD5 o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb.

Krok 4	**show user account-list** Zweryfikuj skonfigurowane informacje.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Wskazówka:

Zalogowani użytkownicy mogą podać na tej stronie hasło dostępu, aby otrzymać uprawnienia administratorskie.

Poniższy schemat przedstawia przykładowy sposób tworzenia nowych użytkowników o poziomie dostępu konta Operator, ustawiania nazwy użytkownika jako user1, a hasła jako 123, włączania funkcji AAA oraz ustawiania hasła dostępu jako abc123.

Switch#configure

Switch(config)#user name user1 **privilege** operator **password** 123

Switch(config)#aaa enable

Switch(config)#enable admin password abc123

Switch(config)#show user account-list

Index	User-Name	User-Type
-----	---------	---------
1	user1	Operator
2	admin	Admin

Switch(config)#end

Switch#copy running-config startup-config

4 Konfiguracja narzędzi systemowych

Narzędzia systemowe umożliwiają:

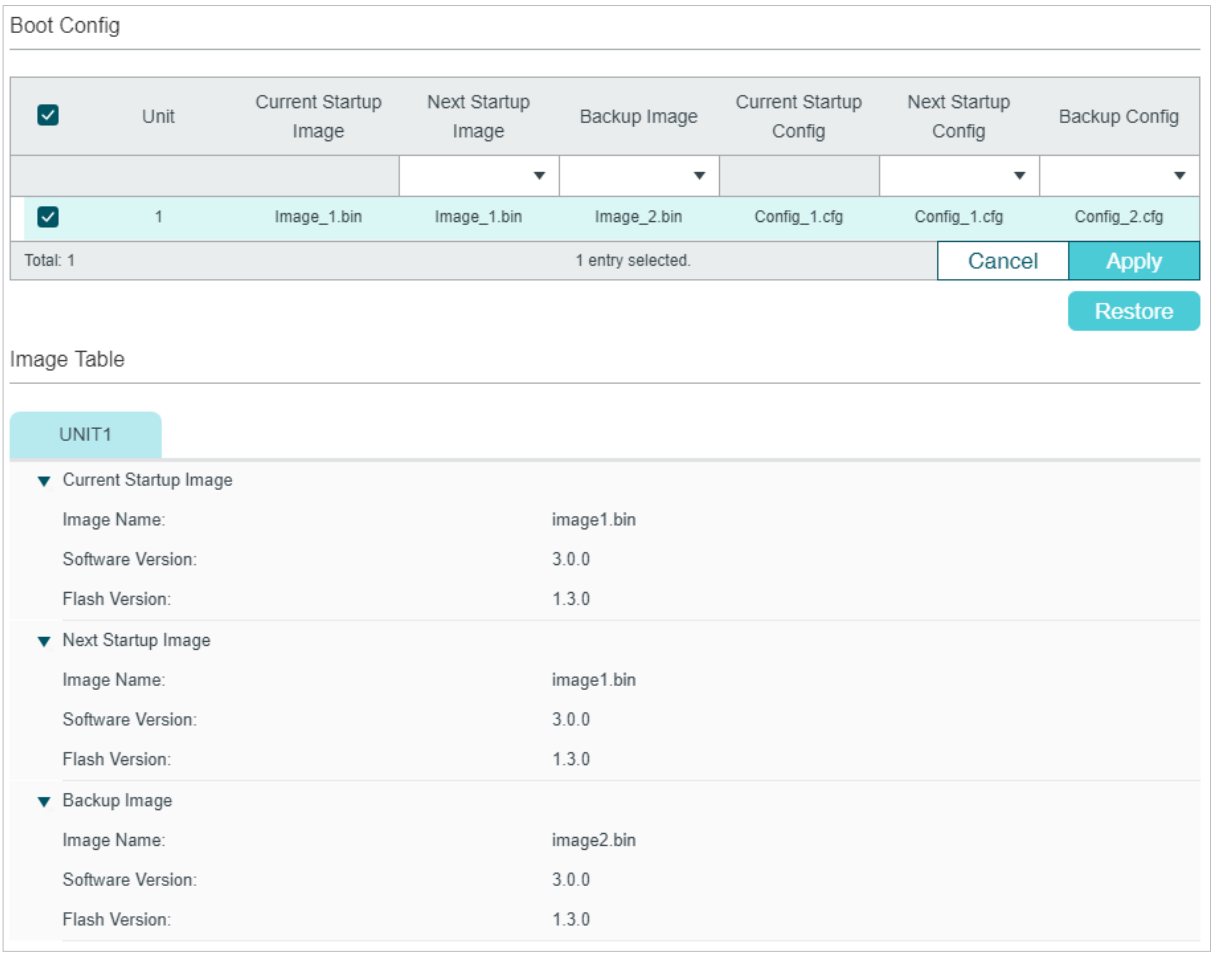
- konfigurację pliku rozruchowego;
- przywracanie ustawień przełącznika;
- tworzenie kopii zapasowej pliku konfiguracyjnego;
- aktualizację firmware'u;
- restartowanie przełącznika;
- reset przełącznika.

4.1 Przez GUI

4.1.1 Konfiguracja pliku rozruchowego

Wybierz z menu **SYSTEM** > **System Tools** > **Boot Config**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja pliku rozruchowego



Wykonaj poniższe kroki, aby skonfigurować plik rozruchowy:

1) W sekcji **Boot Table** wybierz jeden lub więcej modułów i skonfiguruj odpowiednie parametry.

Unit	Numer modułu.
Current Startup Image	Aktualny obraz rozruchowy.
Next Startup Image	Wybierz kolejny obraz rozruchowy. Po podłączeniu przełącznika, będzie on starał się uruchomić przy pomocy kolejnego obrazu rozruchowego. Kolejny obraz rozruchowy i obraz kopii zapasowej nie mogą być takie same.
Backup Image	Wybierz obraz kopii zapasowej. Gdy przełącznik nie będzie mógł się uruchomić za pomocą kolejnego obrazu rozruchowego, skorzysta z obrazu kopii zapasowej. Kolejny obraz rozruchowy i obraz kopii zapasowej nie mogą być takie same.
Current Startup Config	Aktualna konfiguracja rozruchowa.
Next Startup Config	Wybierz kolejną konfigurację rozruchową. Po podłączeniu przełącznika, będzie on starał się uruchomić przy pomocy kolejnej konfiguracji rozruchowej. Kolejna konfiguracja rozruchowa i konfiguracja kopii zapasowej nie mogą być takie same. .
Backup Config	Wybierz konfigurację kopii zapasowej. Gdy przełącznik nie będzie mógł się uruchomić za pomocą kolejnej konfiguracji rozruchowej, skorzysta z konfiguracji kopii zapasowej. Kolejna konfiguracja rozruchowa i konfiguracja kopii zapasowej nie mogą być takie same.

2) Kliknij **Apply**.

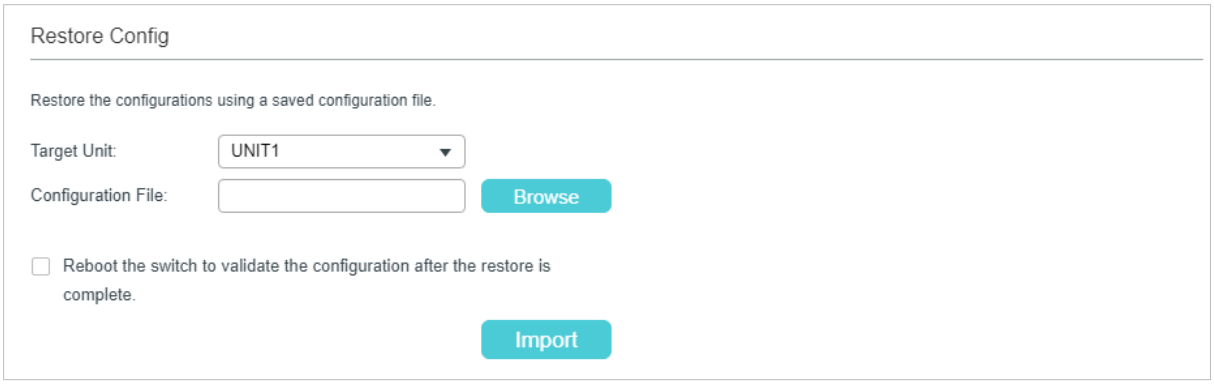
W **Image Table** znajdują się informacje o aktualnym obrazie rozruchowym. Wyświetlane informacje wyglądają następująco:

Image Name	Nazwa obrazu.
Software Version	Wersja oprogramowania obrazu.
Flash Version	Wersja wtyczki Flash obrazu.

4.1.2 Przywracanie ustawień przełącznika

Wybierz z menu **SYSTEM** > **System Tools** > **Restore Config**, aby wyświetlić poniższą stronę.

Rys. 4-2 Przywracanie konfiguracji przełącznika



Wykonaj poniższe kroki, aby przywrócić aktualną konfigurację przełącznika:

1) W sekcji **Restore Config** wybierz moduł, który ma być przywrócony.
2) Kliknij **Browse** i wybierz plik konfiguracyjny, który ma być zaimportowany.
3) Zdecyduj czy przełącznik ma się uruchomić ponownie, gdy przywracanie ustawień zostanie ukończone. Zaimportowany obraz będzie obowiązywać dopiero po restarcie przełącznika.
4) Kliknij **Import**, aby zaimportować plik konfiguracyjny.

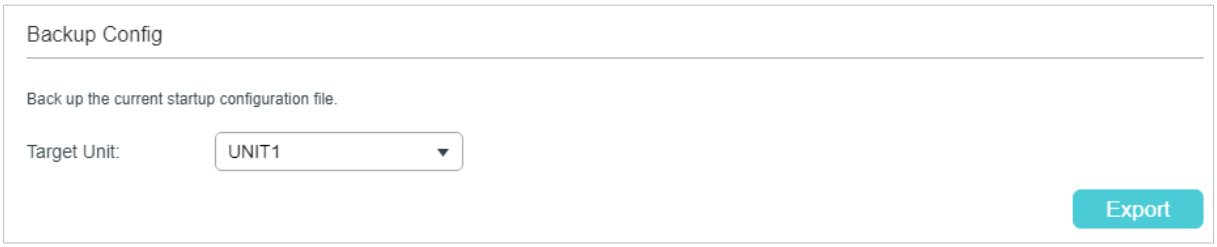
Uwaga:

Przywrócenie konfiguracji zajmie trochę czasu. Czekaj, nie wykonując żadnych działań.

4.1.3 Tworzenie kopii zapasowej pliku konfiguracyjnego

Wybierz z menu **SYSTEM** > **System Tools** > **Backup Config**, aby wyświetlić poniższą stronę.

Rys. 4-3 Tworzenie kopii zapasowej pliku konfiguracyjnego



W sekcji **Config Backup** wybierz jeden moduł i kliknij **Export**, aby wyeksportować plik konfiguracyjny.

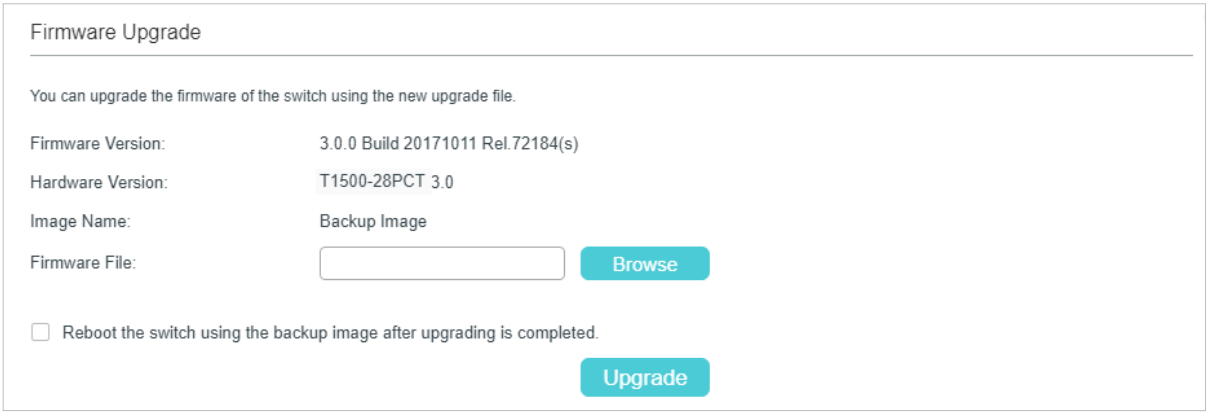
Uwaga:

Wyeksportowanie konfiguracji może chwilę potrwać. Czekaj, nie wykonując żadnych działań

4.1.4 Aktualizacja firmware'u

Wybierz z menu **SYSTEM** > **System Tools** > **Firmware Upgrade**, aby wyświetlić poniższą stronę.

Rys. 4-4 Aktualizacja firmware'u



Na tej stronie znajdują się aktualne informacje dotyczące firmware'u:

Firmware Version	Aktualna wersja firmware'u systemu.
Hardware Version	Aktualna wersja sprzętowa systemu.
Image Name	Obraz, który ma być zaktualizowany. To działanie będzie miało wpływ wyłącznie na ten obraz.

Wykonaj poniższe kroki, aby zaktualizować firmware przełącznika:

1) Kliknij **Browse** i wybierz odpowiedni plik z aktualizacją firmware'u.
2) Zdecyduj czy przełącznik ma się uruchomić ponownie po zakończeniu aktualizacji. Zaktualizowany firmware będzie obowiązywać dopiero po restarcie przełącznika.
3) Kliknij **Upgrade**, aby zaktualizować system.

Uwaga:

- Aktualizacja przełącznika może chwilę potrwać. Czekaj, nie wykonując żadnych działań.
- Zaleca się zrobić kopię zapasową ustawień przed aktualizacją.

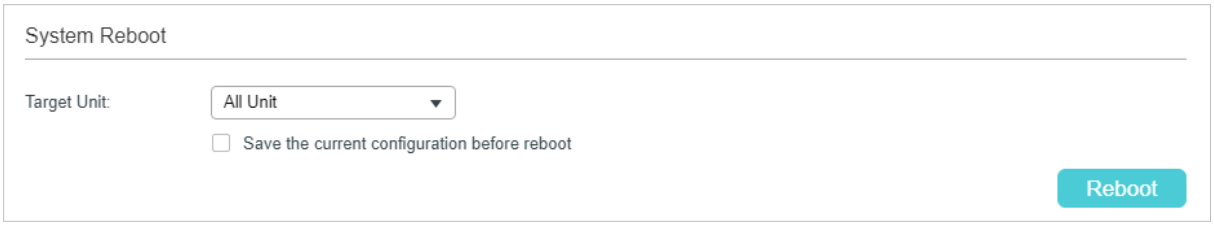
4.1.5 Restartowanie przełącznika

Istnieją dwie metody restartu przełącznika: restart ręczny i automatyczny po ustawieniu harmonogramu restartu.

Ręczny restart przełącznika

Wybierz z menu **SYSTEM** > **System Tools** > **System Reboot > System Reboot**, aby wyświetlić poniższą stronę.

Rys. 4-5 Ręczny restart przełącznika



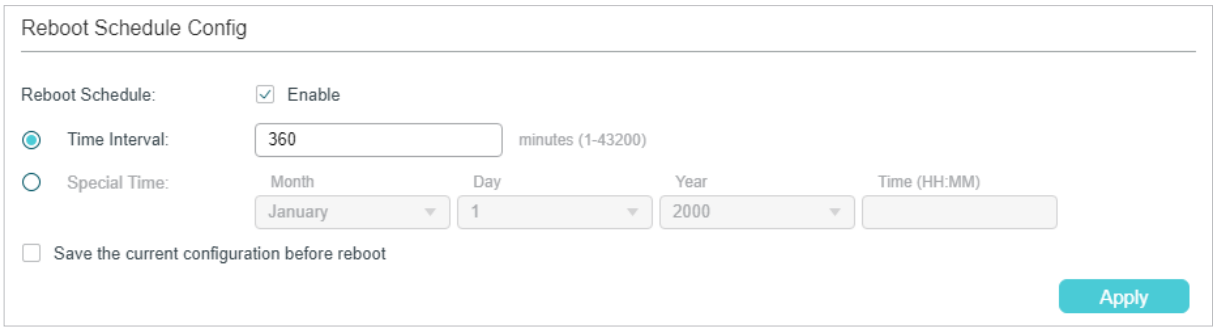
Wykonaj poniższe kroki, aby zrestartować przełącznik:

1) W sekcji **System Reboot** wybierz moduł.
2) Zdecyduj czy zapisać aktualną konfigurację przed restartem.
3) Kliknij **Reboot**.

Konfiguracja harmonogramu restartu

Wybierz z menu **SYSTEM > System Tools > System Reboot > Reboot Schedule**, aby wyświetlić poniższą stronę.

Rys. 4-6 Konfiguracja harmonogramu restartu



Wykonaj poniższe kroki, aby skonfigurować harmonogram restartu:

1) W sekcji **Reboot Schedule Config** wybierz jedną metodę i uzupełnij odpowiednie parametry.

Time Interval	Podaj określony czas. Przełącznik zrestartuje się po upływie tego czasu. Prawidłowe wartości mieszczą się w przedziale 1 - 43200 minut. Aby harmonogram miał charakter cykliczny, kliknij Save, aby zapisać aktualną konfigurację lub włącz opcję **Save the current configuration before reboot**.

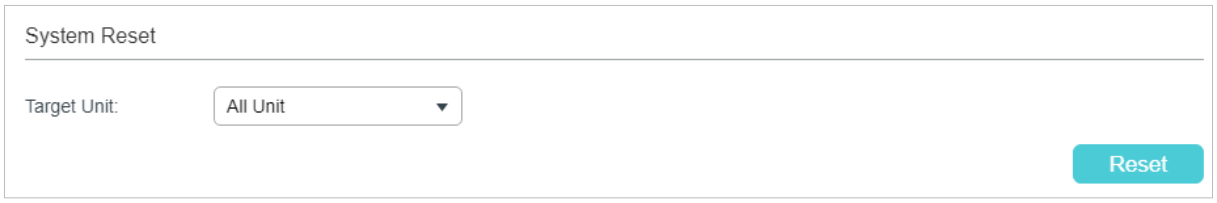
Special Time	Podaj czas i datę restartu przełącznika. **Month/Day/Year:** Podaj datę restartu przełącznika. **Time (HH:MM)**: Podaj czas restartu przełącznika w formacie GG:MM.

2) Zdecyduj czy zapisać aktualną konfigurację przed restartem.
3) Kliknij **Apply**.

4.1.6 Resetowanie przełącznika

Wybierz z menu **SYSTEM** > **System Tools** > **System Reset**, aby wyświetlić poniższą stronę.

Rys. 4-7 Resetowanie przełącznika



W sekcji **System Reset** wybierz moduł i kliknij **Reset**. Wszystkie ustawienia przełącznika zostaną przywrócone do wartości domyślnych.

4.2 Przez CLI

4.2.1 Konfiguracja pliku rozruchowego

Wykonaj poniższe kroki, aby skonfigurować plik rozruchowy:

Krok 1	**configure** Włącz tryb konfiguracji globalnej.
Krok 2	**boot application filename {** image1 | image2 **} {** startup | backup **}** Określ konfigurację pliku rozruchowego. Domyślnie obrazem rozruchowym jest image1.bin, a image2.bin obrazem kopii zapasowej. image1 | image2: Wybierz plik obrazu do skonfigurowania. startup | backup: Wybierz właściwości pliku obrazu.
Krok 3	**boot config filename {** config1 | config2 **} {** startup | backup **}** Określ konfigurację pliku rozruchowego. Domyślnie plikiem konfiguracji rozruchowej jest config1.cfg, a config2.cfg plikiem konfiguracji kopii zapasowej. config1 | config2: Wybierz plik konfiguracyjny do skonfigurowania. startup | backup: Określ właściwości pliku konfiguracyjnego.
Krok 4	**show boot** Zweryfikuj systemową konfigurację pliku rozruchowego.

Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania kolejnego obrazu rozruchowego jako image1, obrazu kopii zapasowej jako image2, kolejnego pliku konfiguracji rozruchowej jako config1 oraz pliku konfiguracji kopii zapasowej jako config2.

Switch#configure

Switch(config)#boot application filename image1 startup

Switch(config)#boot application filename image2 backup

Switch(config)#boot config filename config1 startup

Switch(config)#boot config filename config2 backup

Switch(config)#show boot

Boot config:

Current Startup Image - image2.bin

Next Startup Image - image1.bin

Backup Image - image2.bin

Current Startup Config - config2.cfg

Next Startup Config - config1.cfg

Backup Config - config2.cfg

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 Przywracanie konfiguracji przełącznika

Wykonaj poniższe kroki, aby przywrócić konfigurację przełącznika:

Krok 1	**enable** Uruchom tryb uprzywilejowany.
Krok 2	**copy tftp startup-config ip-address** *ip-addr* **filename** *name* Pobierz na przełącznik plik konfiguracyjny z serwera TFTP. *ip-addr*: Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i IPv6 są obsługiwane. *name*: Podaj nazwę pliku konfiguracyjnego, który ma być pobrany.

Uwaga:

Aktualizacja przełącznika zajmie trochę czasu. Czekaj, nie wykonując żadnych działań.

Poniższy schemat przedstawia przykładowy sposób przywracania pliku konfiguracyjnego o nazwie file1 z serwera TFTP za pomocą adresu IP 192.168.0.100.

Switch>enable

Switch#copy tftp startup-config ip-address 192.168.0.100 **filename** file1

Start to load user config file.....

Operation OK! Now rebooting system.....

4.2.3 Tworzenie kopii zapasowej pliku konfiguracyjnego

Wykonaj poniższe korki, aby utworzyć w pliku kopię zapasową aktualnej konfiguracji przełącznika:

Krok 1	**enable** Uruchom tryb uprzywilejowany.
Krok 2	**copy startup-config tftp ip-address** *ip-addr* **filename** *name* Utwórz kopię zapasową pliku konfiguracyjnego na serwerze TFTP. *ip-addr*: Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i IPv6 są obsługiwane. *name*: Podaj nazwę pliku konfiguracyjnego, aby go zapisać.

Poniższy schemat przedstawia przykładowy sposób tworzenia kopii zapasowej pliku konfiguracyjnego o nazwie file2 na serwerze TFTP za pomocą adresu IP 192.168.0.100.

Switch>enable

Switch#copy startup-config tftp ip-address 192.168.0.100 **filename** file2

Start to backup user config file.....

Backup user config file OK.

4.2.4 Aktualizacja firmware'u

Wykonaj poniższe kroki, aby zaktualizować firmware:

Krok 1	**enable** Uruchom tryb uprzywilejowany.

Krok 2	**firmware upgrade ip-address** *ip-addr* **filename** *name* Zaktualizuj obraz kopii zapasowej przełącznika poprzez serwer TFTP. Aby uruchomić system przy użyciu nowego firmware'u, musisz zrestartować przełącznik za pomocą obrazu kopii zapasowej. *ip-addr*: Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i IPv6 są obsługiwane. *name*: Podaj nazwę wybranego pliku firmware'u.
Krok 3	Wpisz Y, aby kontynuować, a następnie wpisz Y, aby zrestartować przełącznik za pomocą obrazu kopii zapasowej.

Poniższy schemat przedstawia przykładowy sposób aktulizacji firmware'u za pomocą pliku konfiguracyjnego o nazwie file3.bin. Adresem serwera TFTP jest 190.168.0.100.

Switch>enable

Switch#firmware upgrade ip-address 192.168.0.100 **filename** file3.bin

It will only upgrade the backup image. Continue? (Y/N):Y

Operation OK!

Reboot with the backup image? (Y/N): Y

4.2.5 Restartowanie przełącznika

Ręczne restartowanie przełącznika

Wykonaj poniższe kroki, aby zrestartować przełącznik:

Krok 1	**enable** Uruchom tryb uprzywilejowany.
Krok 2	**reboot** Uruchom ponownie przełącznik.

Konfiguracja harmonogramu restartu

Wykonaj poniższe kroki, aby skonfigurować harmonogram restartu:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	Skorzystaj z poniższego polecenia, aby ustawić interwał restartu: **reboot-schedule in** *interval* **[save_before_reboot]** (Opcjonalnie) Ustaw harmonogram restartu. *interval*: Podaj określony czas. Przełącznik uruchomi się ponownie po upływie tego czasu. Prawidłowe wartości mieszczą się w przedziale 1 - 43200 minut. **save_before_reboot**: Zapisz plik konfiguracyjny przed restartem przełącznika. Aby harmonogram miał charakter cykliczny, dodaj tę część do polecenia. Skorzystaj z poniższego polecenia, aby ustawić specjalny czas restartu: **reboot-schedule at** *time* **[** *date* **] [save_before_reboot]** (Opcjonalnie) Ustaw harmonogram restartu. *time*: Podaj czas restartu przełącznika w formacie GG:MM. *date*: Podaj datę restartu przełącznika w formacie DD/MM/YYYY. Data nie powinna przekraczać okresu najbliższych 30 dni. **save_before_reboot**: Zapisz plik konfiguracyjny przed restartem przełącznika. Jeżeli nie podasz żadnej daty, przełącznik zrestartuje się zgodnie z czasem, który ustawiłeś. Jeżeli czas, który ustawiłeś jest późniejszy niż czas wykonania polecenia, przełącznik zrestartuje się później w tym samym dniu. W innym wypadku przełącznik zrestartuje się kolejnego dnia.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawienia restartu przełącznika na godzinę 12:00 dnia 15/08/2017.

Switch#configure

Switch(config)#reboot-schedule at 12:00 15/08/2017 save_before_reboot

Reboot system at 15/08/2017 12:00. Continue? (Y/N): Y

Reboot Schedule Settings

Reboot schedule at 2017-08-15 12:00 (in 25582 minutes)

Save before reboot: Yes

Switch(config)#end

Switch#copy running-config startup-config

4.2.6 Resetowanie przełącznika

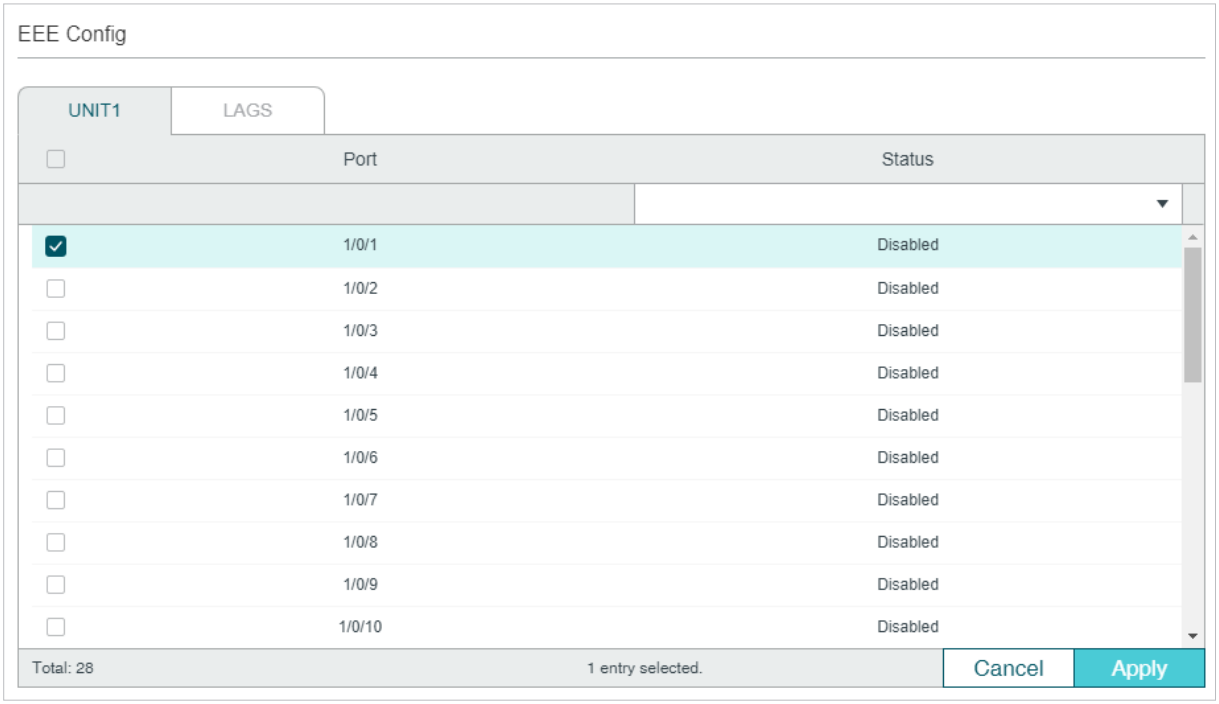
Wykonaj poniższe kroki, aby zresetować przełącznik:

Krok 1	**enable** Uruchom tryb uprzywilejowany.
Krok 2	**reset** Zresetuj przełącznik. Wszystkie ustawienia przełącznika zostaną przywrócone do wartości fabrycznych..

5 Konfiguracja EEE

Wybierz z menu **SYSTEM** > **EEE**, aby wyświetlić poniższą stronę.

Rys. 5-1 Konfiguracja EEE



Wykonaj poniższe kroki, aby skonfigurować EEE:

1) W sekcji **EEE Config** wybierz jeden lub więcej portów, które chcesz skonfigurować.
2) Włącz lub wyłącz EEE dla poszczególnych portów.
3) Kliknij **Apply**.

5.1 Przez CLI

Wykonaj poniższe kroki, aby zaktualizować EEE:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**eee** Włącz EEE na porcie.

Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji EEE na porcie 1/0/1.

Switch#config

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#eee

Switch(config-if)#show interface eee

Port EEE status

Gi1/0/1 Enable

Gi1/0/2 Disable

...

Switch(config-if)#end

Switch#copy running-config startup-config

6 Konfiguracja PoE

Uwaga:

Tylko przełączniki T1500-28PCT, T1500G-10MPS i T1500G-10PS obsługują funkcję PoE.

Funkcja PoE umożliwia:

- Ręczną konfigurację parametrów PoE
- Konfigurację parametrów PoE za pomocą profilu

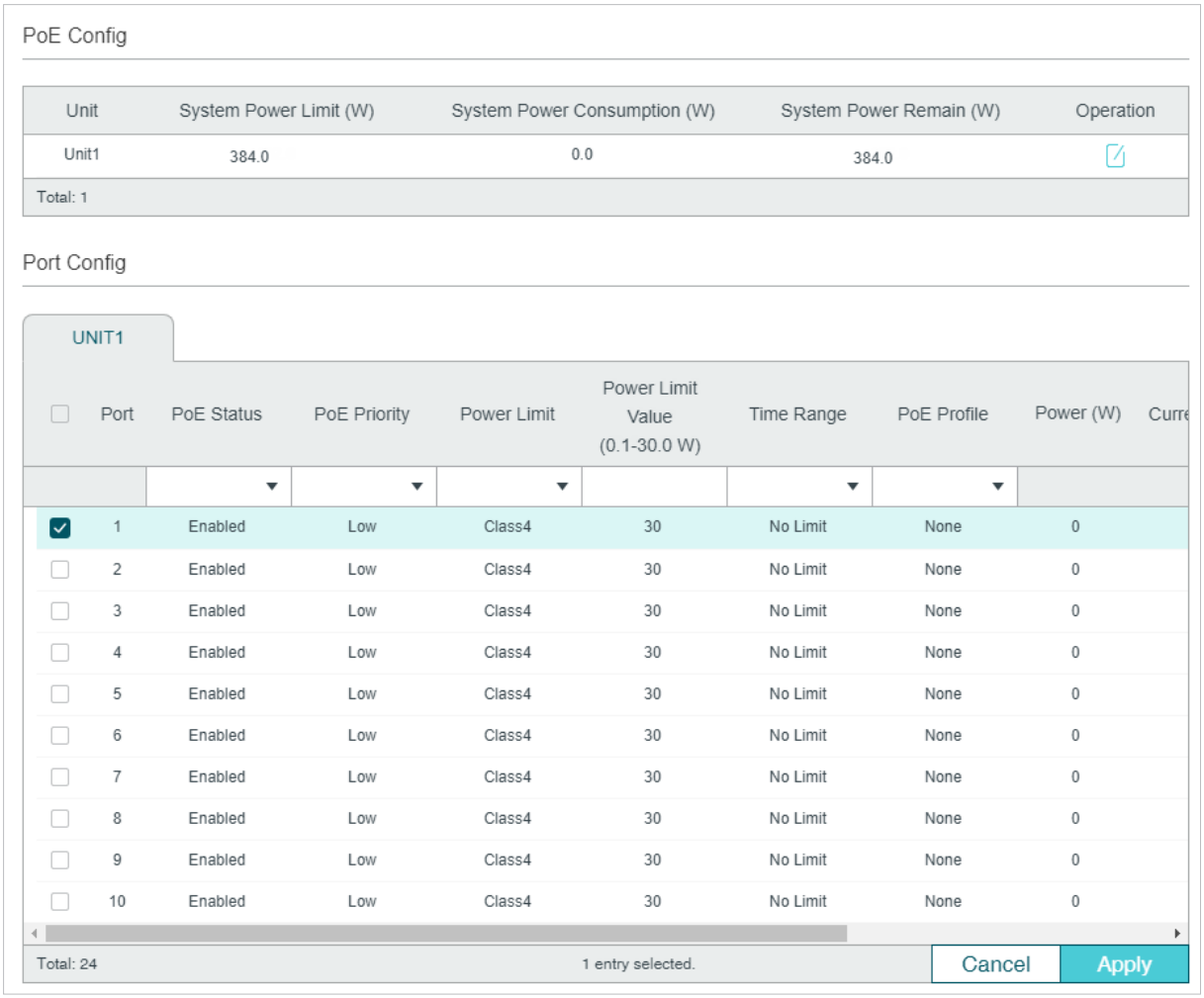
Parametry możesz skonfigurować ręcznie lub poprzez utworzenie profilu z pożądanymi parametrami. Profil można powiązać z wybranymi portami, aby szybko skonfigurować parametry PoE.

6.1 Przez GUI

6.1.1 Ręczna konfiguracja parametrów PoE

Wybierz z menu **SYSTEM > PoE** > **PoE Config**, aby wyświetlić poniższą stronę.

Rys. 6-1 Ręczna konfiguracja parametrów PoE



Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry PoE:

1) W sekcji **PoE Config** możesz uzyskać podgląd aktualnych parametrów PoE.

System Power Limit (w)	Maksymalna moc, jaką może dostarczyć przełącznik PoE.
System Power Consumption (w)	Zużycie energii przez przełącznik PoE w czasie rzeczywistym.
System Power Remain (w)	Pozostała moc przełącznika PoE w czasie rzeczywistym.

Ponadto, klikając , możesz skonfigurować limit mocy systemowej. Kliknij **Apply**.

Rys. 6-2 Konfiguracja limitu mocy systemowej

Unit	Numer modułu.
System Power Limit	Podaj maksymalną moc dostarczaną przez przełącznik PoE.

2) W sekcji **Port Config** wybierz port, który chcesz skonfigurować i określ jego parametry. Kliknij **Apply**.

PoE Status	Włącz lub wyłącz funkcję PoE dla danego portu. Włączenie funkcji na porcie umożliwia dostarczanie energii urządzeniu PD.
PoE Priority	Wybierz priorytet dla danego portu. Gdy moc zasilania przekroczy limit mocy systemu, przełącznik wyłączy zasilanie urządzeń PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń.
Power Limit	Określ maksymalną moc, jaką dany port może dostarczać. Dostępne są następujące opcje: **Auto**: Przełącznik automatycznie przydzieli wartość maksymalnej mocy, którą port może dostarczyć. **Class1**: Maksymalna moc na porcie to 4W. **Class2**: Maksymalna moc na porcie to 7W. **Class3**: Maksymalna moc na porcie to 15,4W. **Class4**: Maksymalna moc na porcie to 30W. **Manual**: Wprowadź wartość ręcznie.
Power Limit Value (0.1w-30w)	Jeżeli wybranym trybem limitu mocy jest **Manual** wpisz w tym polu wartość maksymalnej mocy zasilania. Jeżeli wybranym trybem limitu mocy jest **Class1** - **Class4**, w typu polu pojawi się wartość maksymalnej mocy zasilania.
Time Range	Wybierz przedział czasowy. Urządzenia będą mogły być zasilane na danym porcie tylko w tym czasie. Wskazówki dotyczące konfiguracji przedziałów czasowych znajdziesz w rozdziale *Konfiguracja przedziału czasowego*.

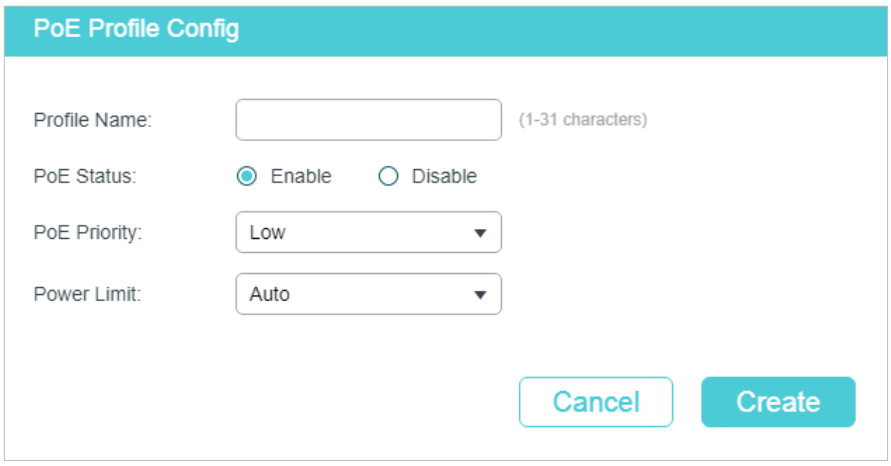
PoE Profile	Metoda szybkiej konfiguracji wybranych portów. Jeżeli skorzystasz z profilu, ręczna konfiguracja stanu PoE, priorytetu PoE lub limitu mocy nie będzie możliwa. Wskazówki dotyczące tworzenia profilu znajdziesz w rozdziale *Konfiguracja parametrów PoE za pomocą profilu*.
Power (w)	Moc zasilania portu w czasie rzeczywistym.
Current (mA)	Prąd dostarczany na porcie w czasie rzeczywistym.
Voltage (v)	Napięcie na porcie w czasie rzeczywistym.
PD Class	Klasa podłączonego urządzenia PD.
Power Status	Stan zasilania na porcie w czasie rzeczywistym.

6.1.2 Konfiguracja parametrów PoE za pomocą profilu

- Tworzenie profilu PoE

Wybierz z menu **SYSTEM > PoE > PoE Profile** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 6-3 Tworzenie profilu PoE



Wykonaj poniższe kroki, aby utworzyć profil PoE:

1) W sekcji **Create PoE Profile** skonfiguruj pożądane ustawienia profilu.

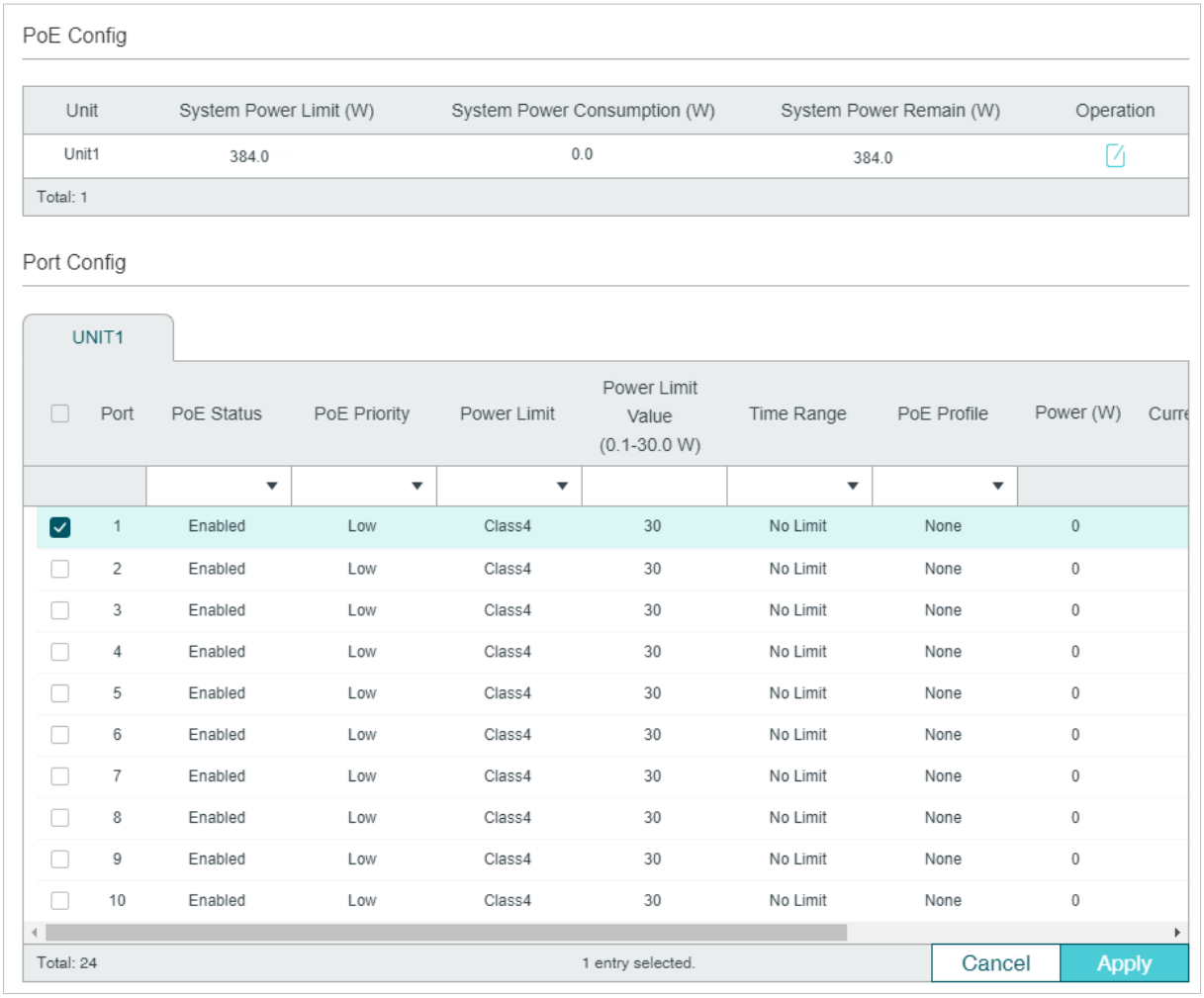
Profile Name	Podaj nazwę profilu PoE.
PoE Status	Określ stan PoE dla profilu PoE.
PoE Priority	Wybierz priorytet dla profilu PoE. Dostępne są następujące opcje: **High**, **Middle** i **Low**. Gdy moc zasilania przekroczy limit mocy systemowej, przełącznik wyłączy zasilanie urządzeń PD na portach o niskim priorytecie, aby zapewnić stabilne działanie pozostałych urządzeń.
Power Limit	Określ maksymalną moc, jaką dany port może dostarczać. Dostępne są następujące opcje: **Auto**: Przełącznik automatycznie przydzieli wartość maksymalnej mocy, którą port może dostarczyć. **Class1 (4w)**: Maksymalna moc na porcie to 4W. **Class2 (7w)**: Maksymalna moc na porcie to 7W. **Class3 (15.4w)**: Maksymalna moc na porcie to 15,4W. **Class4 (30w)**: Maksymalna moc na porcie to 30W. **Manual**: Wprowadź wartość ręcznie.

2) Kliknij **Create**.

■ Wiązanie profilu z wybranymi portami

Wybierz z menu **SYSTEM > PoE** > **PoE Config**, aby wyświetlić poniższą stronę.

Rys. 6-1 Wiązanie profilu z wybranymi portami



Wykonaj poniższe kroki, aby powiązać profil z wybranymi portami:

1) W sekcji **PoE Config** możesz uzyskać podgląd aktualnych parametrów PoE.

System Power Limit (w)	Maksymalna moc, jaką może dostarczyć przełącznik PoE.
System Power Consumption (w)	Zużycie energii przez przełącznik PoE w czasie rzeczywistym..
System Power Remain (w)	Pozostała moc przełącznika PoE w czasie rzeczywistym.

Ponadto, klikając możesz skonfigurować limit mocy systemowej. Kliknij **Apply**.

Rys. 6-4 Konfiguracja limitu mocy systemowej

Unit	Numer modułu.
System Power Limit	Podaj maksymalną moc dostarczaną przez przełącznik PoE..

2) W sekcji **Port Config** wybierz port lub porty, które chcesz skonfigurować i określ ich parametry: przedział czasowy i profil PoE. Kliknij **Apply**, a parametry PoE wybranego profilu PoE, takie jak stan PoE i priorytet PoE wyświetlą się w poniższej tabeli.

PoE Status	Stan PoE na danym porcie. Port może zasilać urządzenie PD, gdy funkcja PoE jest włączona.
PoE Priority	Priorytet danego portu. Gdy moc zasilania przekroczy limit mocy systemu, przełącznik wyłączy zasilanie urządzeń PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń.
Power Limit	Maksymalna moc zasilania danego portu.
Power Limit Value (0.1W-30.0W)	Wartość limitu mocy.
Time Range	Wybierz przedział czasowy. Urządzenia będą mogły być zasilane na danym porcie tylko w tym czasie. Wskazówki dotyczące konfiguracji przedziałów czasowych znajdziesz w rozdziale *Konfiguracja przedziału czasowego*.
PoE Profile	Wybierz profil PoE dla wybranego portu. Po ustawieniu profilu, ręczna konfiguracja stanu PoE, priorytetu PoE lub limitu mocy nie będzie możliwa.
Power (W)	Moc zasilania portu w czasie rzeczywistym.
Current (mA)	Prąd dostarczany na porcie w czasie rzeczywistym.
Voltage (V)	Napięcie na porcie w czasie rzeczywistym.
PD Class	Klasa podłączonego urządzenia PD.
Power Status	Stan zasilania na porcie w czasie rzeczywistym.

6.2 Przez CLI

6.2.1 Ręczna konfiguracja parametrów PoE

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry PoE:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**power inline consumption** *power-limit* Podaj maksymalną moc dostarczaną przez przełącznik PoE. *power-limit*: Podaj maksymalną moc dostarczaną przez przełącznik PoE. Wpisz wartość z przedziału 1.0 - 384.0W. Wartością domyślną jest 384.0W.
Krok 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu. *port*: Podaj numer portu Ethernet, np. 1/0/1. *port-list:* Podaj listę portów Ethernet, np. 1/0/1-3, 1/0/5.
Krok 4	**power inline supply {** enable **|** disable **}** Określ stan PoE dla poszczególnych portów. enable **|** disable: Włącz lub wyłącz funkcję PoE. Domyślnie funkcja jest włączona.
Krok 5	**power inline priority {** low **|** middle **|** high **}** Określ priorytet PoE dla poszczególnych portów. low **|** middle **|** high: Wybierz priorytet dla danego portu. Gdy moc zasilania przekroczy limit mocy systemu, przełącznik wyłączy zasilanie urządzeń PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń. Domyślnie ustawiony jest priorytet niski.
Krok 6	**power inline consumption {** *power-limit* **|** auto **|** class1 **|** class2 **|** class3 **|** class4 **}** Określ maksymalną moc zasilania danego portu. *power-limit* | auto | class1 | class2 | class3 | class4: Wybierz lub wpisz maksymalną moc zasilania danego portu. Dostępne są następujące opcje: Auto oznacza, że przełącznik automatycznie przydzieli wartość maksymalnej mocy, którą port może dostarczyć. Class1 oznacza 4W, Class2 oznacza 7W, Class3 oznacza 15,4W, a Class4 oznacza 30W. Możesz też wpisać tą wartość ręcznie. Wartość musi mieścić się w przedziale 1 - 300. Jedna jednostka to 0,1W. Stąd jeżeli chcesz ustawić np. 5W, wpisaną wartością musi być 50. Domyślne ustawienie to Class4.
Krok 7	**time-range** *name* Wybierz przedział czasowy. Urządzenia będą mogły być zasilane na danym porcie tylko w tym czasie. Wskazówki dotyczące konfiguracji przedziałów czasowych znajdziesz w rozdziale *Konfiguracja przedziału czasowego*. *name:* Podaj nazwę utworzonego przedziału czasowego.
Krok 8	**show power inline** Zweryfikuj systemowe informacje globalne PoE.

Krok 9	**show power inline configuration interface [fastEthernet { *port* | *port-list* } | gigabitEthernet { *port* | *port-list* } | ten-gigabitEthernet { *port* | *port-list* }]** Zweryfikuj ustawienia PoE na danym porcie. *port*: Podaj numer portu Ethernet, np. 1/0/1. *port-list*: Podaj listę portów Ethernet, np. 1/0/1-3, 1/0/5.
Krok 10	**show power inline information interface [fastEthernet { *port* | *port-list* } | gigabitEthernet { *port* | *port-list* } | ten-gigabitEthernet { *port* | *port-list* }]** Zweryfikuj stan PoE w czasie rzeczywistym na danym porcie. *port*: Podaj numer portu Ethernet, np. 1/0/1. *port-list*: Podaj listę portów Ethernet, np. 1/0/1-3, 1/0/5.
Krok 11	**end** Powróć do trzybu uprzywilejowanego (privileged EXEC mode).
Krok 12	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania limitu mocy systemowej jako 160W, średniego priorytetu i limitu mocy jako class3 dla portu 1/0/5.

Switch#configure

Switch(config)#power inline consumption 160

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#power inline supply enable

Switch(config-if)#power inline priority middle

Switch(config-if)#power inline consumption class3

Switch(config-if)#show power inline

System Power Limit: 160.0w

System Power Consumption: 0.0w

System Power Remain: 160.0w

Switch(config-if)#show power inline configuration interface gigabitEthernet 1/0/5

Interface	PoE-Status	PoE-Prio	Power-Limit(w)	Time-Range	PoE-Profile
Gi1/0/5	Enable	Middle	Class3	No Limit	None

Switch(config-if)#show power inline information interface gigabitEthernet 1/0/5

Interface	Power(w)	Current(mA)	Voltage(v)	PD-Class	Power-Status
Gi1/0/5	1.3	26	53.5	Class 2	ON

Switch(config-if)#end

Switch#copy running-config startup-config

6.2.2 Konfiguracja parametrów PoE za pomocą profilu

Wykonaj poniższe kroki, aby skonfigurować profil PoE:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**power inline consumption** *power-limit* Podaj maksymalną moc dostarczaną przez przełącznik PoE. *power-limit*: Podaj maksymalną moc dostarczaną przez przełącznik PoE. Wpisz wartość z przedziału 1.0 - 384.0W. Wartością domyślną jest 384.0W.
Krok 3	**power profile** *name* **[supply {** enable **|** disable **} [priority {** low **|** middle **|** high **} [consumption {** *power-limit* **|** auto **|** class1 **|** class2 **|** class3 **|** class4 **}]]]** Utwórz profil PoE dla przełącznika. W profilu stan PoE, priorytet PoE i limit mocy są skonfigurowane. Możesz powiązać profil z wybranym portem, aby szybko skonfigurować funkcję PoE. *name*: Podaj nazwę profilu PoE. Nazwa może zawierać od 1 do 16 znaków. Jeżeli pojawiają się w niej spacje, zamknij nazwę w cudzysłowie. enable **|** disable: Określ stan PoE dla profilu. Domyślnie funkcja jest włączona. low	middle	high: Wybierz priorytet dla profilu. Gdy moc zasilania przekroczy limit mocy systemu, przełącznik wyłączy zasilanie urządzeń PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń. *power-limit*	auto	class1	class2	class3	class4: Wybierz lub wpisz maksymalną moc zasilania danego portu. Dostępne są następujące opcje: Auto oznacza, że przełącznik automatycznie przydzieli wartość maksymalnej mocy, którą port może dostarczyć. Class1 oznacza 4W, Class2 oznacza 7W, Class3 oznacza 15,4W, a Class4 oznacza 30W. Możesz też wpisać tą wartość ręcznie. Wartość musi mieścić się w przedziale 1 - 300. Jedna jednostka to 0,1W. Stąd jeżeli chcesz ustawić np. 5W, wpisaną wartością musi być 50.
Krok 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu. *port*: Podaj numer portu Ethernet np. 1/0/1. *port-list:* Podaj listę portów Ethernet, np. 1/0/1-3, 1/0/5.

Krok 5	**power inline profile** *name* Powiąż profil PoE z wybranym portem. Po ustawieniu profilu, ręczna konfiguracja stanu PoE, priorytetu PoE lub limitu mocy nie będzie możliwa. *name*: Podaj nazwę profilu PoE. Jeżeli pojawiają się w niej spacje, zamknij nazwę w cudzysłowie.
Krok 6	**time-range** *name* Wybierz przedział czasowy dla portu. Urządzenia będą mogły być zasilane na danym porcie tylko w tym czasie. Wskazówki dotyczące konfiguracji przedziałów czasowych znajdziesz w rozdziale *Konfiguracja przedziału czasowego*. *name:* Podaj nazwę utworzonego przedziału czasowego.
Krok 7	**show power profile** Zweryfikuj utworzony profil PoE.
Krok 8	**show power inline configuration interface [fastEthernet {** *port* **|** *port-list* **} | gigabitEthernet {** *port* **|** *port-list* **} | ten-gigabitEthernet {** *port* **|** *port-list* **}]** Zweryfikuj ustawienia PoE na poszczególnych portach. *port*: Podaj numer portu Ethernet, np. 1/0/1. *port-list*: Podaj listę portów Ethernet w formacie 1/0/1-3, 1/0/5.
Krok 9	**show power inline information interface [fastEthernet {** *port* **|** *port-list* **} | gigabitEthernet {** *port* **|** *port-list* **} | ten-gigabitEthernet {** *port* **|** *port-list* **}]** Zweryfikuj stan PoE w czasie rzeczywistym dla poszczególnych portów. *port*: Podaj numer portu Ethernet, np. 1/0/1. *port-list*: Podaj listę portów Ethernet w formacie 1/0/1-3, 1/0/5.
Krok 10	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia profilu o nazwie profile1 i wiązania profilu z portem 1/0/6.

Switch#configure

Switch(config)#power profile profile1 **supply** enable **priority** middle **consumption** class2

Switch(config)#show power profile

Index	Name	Status	Priority	Power-Limit(w)
1	profile1	Enable	Middle	Class2

Switch(config)#interface gigabitEthernet 1/0/6

Switch(config-if)#power inline profile profile1

Switch(config-if)#show power inline configuration interface gigabitEthernet 1/0/6

Interface	PoE-Status	PoE-Prio	Power-Limit(w)	Time-Range	PoE-Profile
Gi1/0/6	Enable	Middle	Class2	No Limit	profile1

Switch(config-if)#end

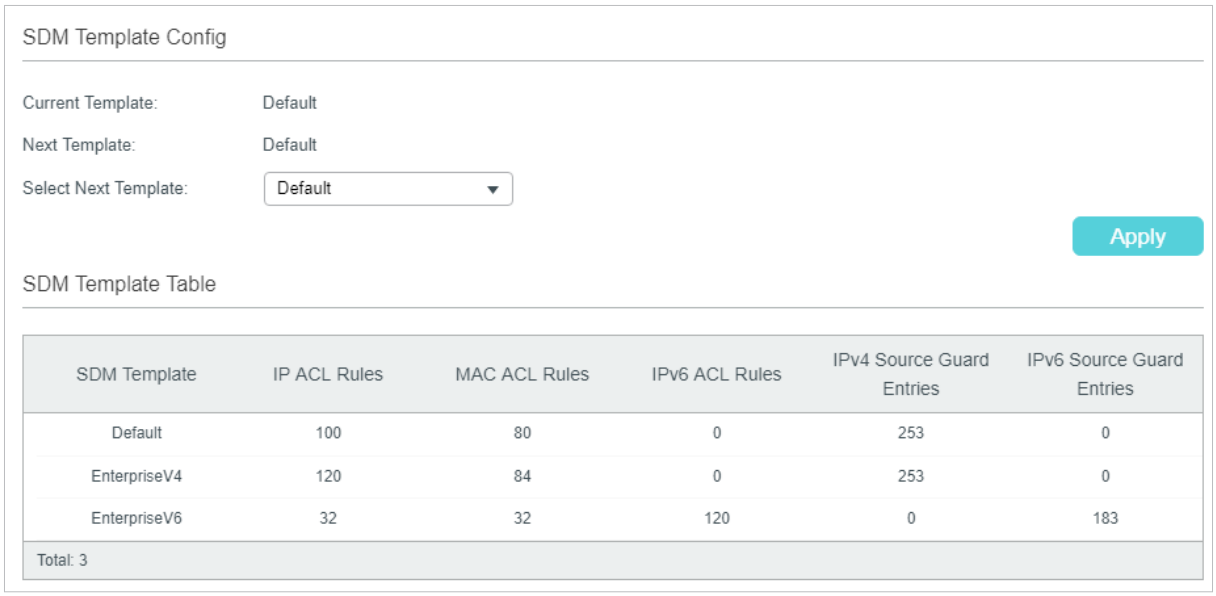
Switch#copy running-config startup-config

7 Konfiguracja szablonów SDM

7.1 Przez GUI

Wybierz z menu **SYSTEM** > **SDM Template**, aby wyświetlić poniższą stronę.

Rys. 7-1 Konfiguracja szablonu SDM



W sekcji **SDM Template Config** wybierz jeden szablon i kliknij **Apply**. Ustawienie zostanie wprowadzone po restarcie przełącznika.

Current Template	Aktualnie obowiązujący szablon.
Next Template	Szablon, który będzie obowiązujący po restarcie przełącznika.
Select Next Template	Wybierz szablon, który będzie obowiązujący po najbliższym restarcie przełącznika. **Default**: Wybierz szablon domyślny. Ten szablon równoważy działanie reguł ACL IP i ACL MAC oraz wpisów ochrony ARP. **EnterpriseV4**: Wybierz szablon enterpriseV4. Ten szablon maksymalizuje zasoby systemowe dla reguł ACL IP i ACL MAC. **EnterpriseV6**: Wybierz szablon enterpriseV6. Ten szablon przydziela zasoby regułom ACL IPv6.

Tabela szablonów prezentuje przydział zasobów dla każdego z szablonów.

SDM Template	Nazwa szablonów.
IP ACL Rules	Liczba reguł ACL IP, w tym reguł ACL warstwy 3 i warstwy 4.

MAC ACL Rules	Liczba reguł ACL warstwy 2.
Combined ACL Rules	Liczba wszystkich reguł ACL.
IPv6 ACL Rules	Liczba reguł ACL IPv6.
IPv4 Source Guard Entries	Liczba wpisów IPv4 Source Guard.
IPv6 Source Guard Entries	Liczba wpisów IPv6 Source Guard.

7.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować szablon SDM:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**show sdm prefer {** used | default | enterpriseV4 | enterpriseV6 **}** Przejrzyj tabelę szablonów. To pomoże ci zdecydować, który szablon jest najodpowiedniejszy dla twojej sieci. used: Przydział zasobów dla aktualnego szablonu. default: Przydział zasobów dla szablonu domyślnego. enterpriseV4: Przydział zasobów dla szablonu enterpriseV4. enterpriseV6: Przydział zasobów dla szablonu enterpriseV6.
Krok 3	**sdm prefer {** default | enterpriseV4 | enterpriseV6 **}** Wybierz szablon, który będzie obowiązujący po restarcie przełącznika. default: Wybierz szablon domyślny. Ten szablon równoważy działanie reguł ACL IP i ACL MAC oraz wpisów ochrony ARP. enterpriseV4: Wybierz szablon enterpriseV4. Ten szablon maksymalizuje zasoby systemowe dla reguł ACL IP i ACL MAC. enterpriseV6: Wybierz szablon enterpriseV6. Ten szablon przydziela zasoby regułom ACL IPv6.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania szablonu SDM jako enterpriseV4.

Switch#config

Switch(config)#show sdm prefer enterpriseV4

“enterpriseV4” template:

number of IP ACL Rules : 120

number of MAC ACL Rules : 84

number of IPV6 ACL Rules : 0

number of IPV4 Source Guard Entries : 253

number of IPV6 Source Guard Entries : 0

Switch(config)#sdm prefer enterpriseV4

Switch to “enterpriseV4” tempale.

Changes to the running SDM preferences have been stored, but cannot take effect until reboot the switch.

Switch(config)#end

Switch#copy running-config startup-config

8 Konfiguracja przedziałów czasowych

Aby skonfigurować przedziały czasowe, wykonaj poniższe kroki:

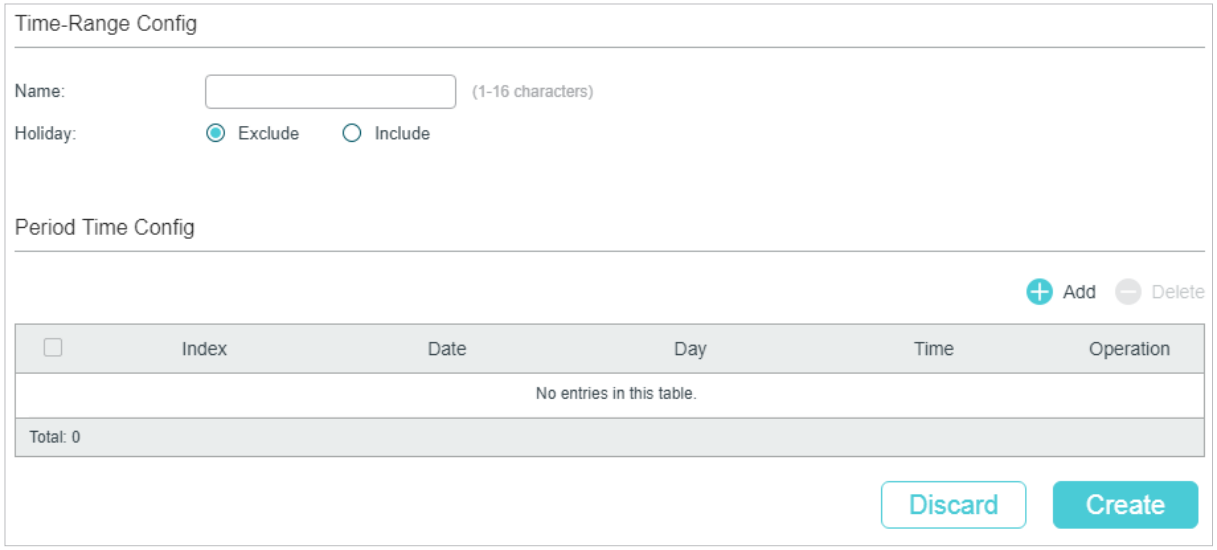
1) Dodaj pozycje z przedziałami czasowymi.
2) Skonfiguruj okres wakacyjny.

8.1 Przez GUI

8.1.1 Dodawanie pozycji z przedziałami czasowymi

Wybierz z menu **SYSTEM** > **Time Range** > **Time Range Config** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 8-1 Konfiguracja przedziału czasowego



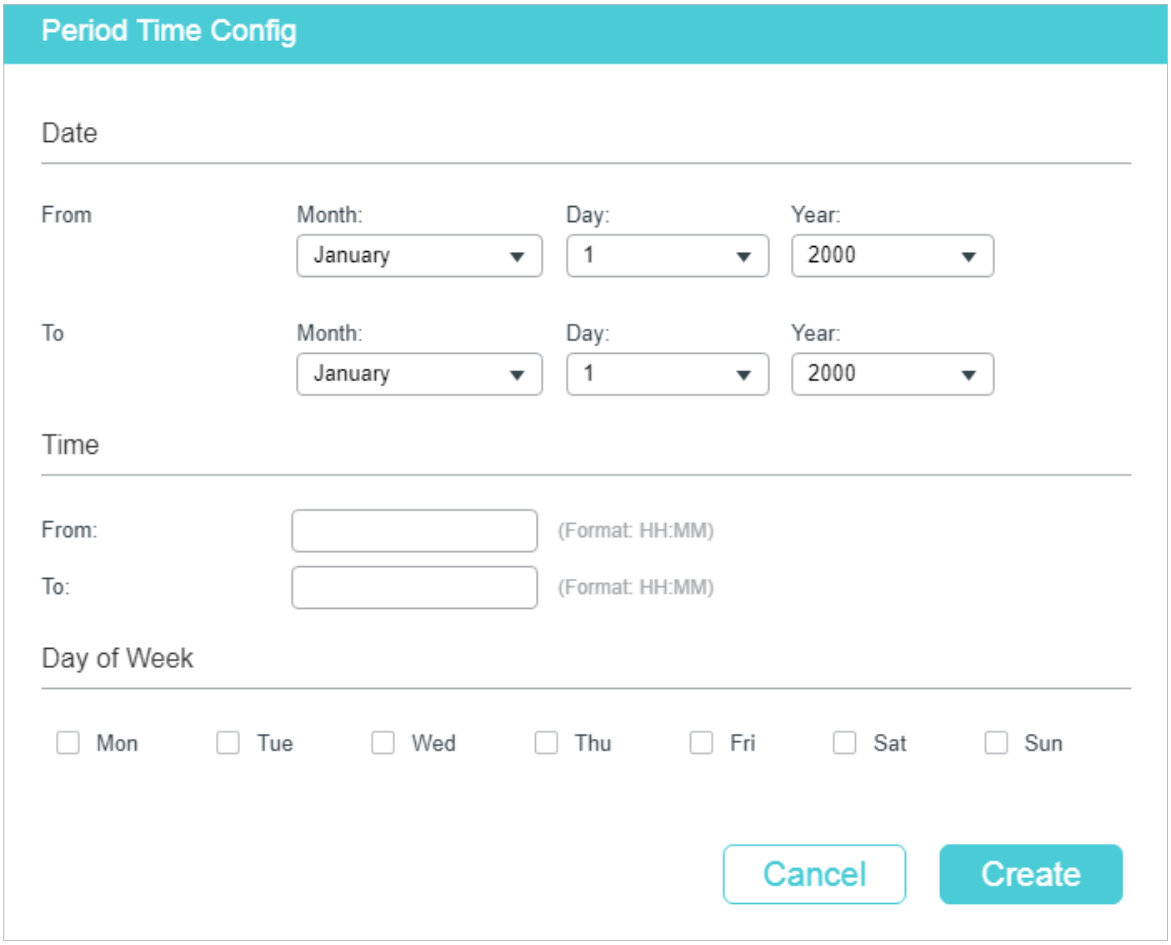
Wykonaj poniższe kroki, aby dodać wpisy z przedziałami czasowymi:

1) W sekcji **Time-Range Config** podaj nazwę pozycji i zaznacz tryb Holiday.

Name	Podaj nazwę pozycji.
Holiday	Zaznacz, aby przedział czasowy obowiązywał/nie obowiązywał w okresie wakacyjnym. **Exclude:** Przedział czasowy nie będzie obowiązywał w okresie wakacyjnym. **Include:** Okres wakacyjny nie będzie miał wpływu na przedział czasowy. Aby skonfigurować okres wakacji, zapoznaj się z rozdziałem *Konfiguracja okresu wakacyjnego.*.

2) W sekcji **Period Time Config** kliknij Add. Pojawi się poniższe okno.

Rys. 8-2 Dodawanie przedziału czasowego

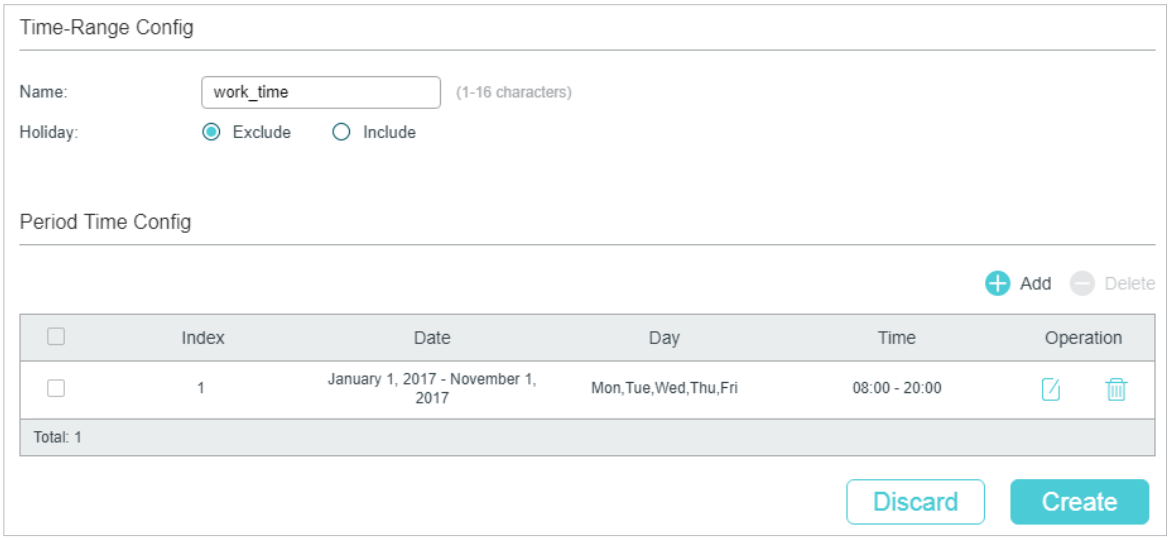


Skonfiguruj poniższe parametry i kliknij **Create**:

Date	Podaj datę początkową i datę końcową tego przedziału czasowego.
Time	Podaj godzinę początku i godzinę końca dnia.
Day of Week	Wybierz dni tygodnia, dla których dany przedział czasowy będzie obowiązujący.

3) W taki sam sposób może dodać kolejne pozycje. Końcowy przedział czasowy jest sumą wszystkich przedziałów w tabeli. Kliknij **Create**.

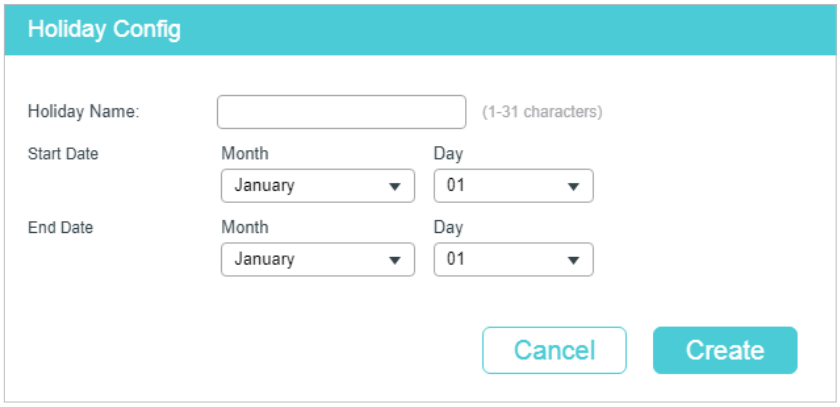
Rys. 8-3 Wyniki konfiguracji



8.1.2 Konfiguracja okresu wakacyjnego

Wybierz z menu **SYSTEM** > **Time Range** > **Holiday Config** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 8-4 Konfiguracja okresu wakacyjnego



Skonfiguruj poniższe parametry i kliknij **Create**, aby dodać nową pozycję.

Holiday Name	Podaj nazwę pozycji.
Start Date	Podaj datę początkową okresu wakacyjnego.
End Date	Podaj datę końcową okresu wakacyjnego.

W podobny sposób możesz dodać kolejne pozycje. Końcowy okres wakacyjny to suma wszystkich pozycji.

8.2 Przez CLI

8.2.1 Dodawanie pozycji z przedziałami czasowymi

Wykonaj poniższe kroki, aby dodać pozycje z przedziałami czasowymi:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**time-range** *name* Utwórz pozycję z przedziałem czasowym. *name*: Podaj nazwę pozycji.
Krok 3	**holiday {** exclude | include **}** Zdecyduj, czy przedział czasowy ma obowiązywać w okresie wakacyjnym. exclude: Przedział czasowy nie będzie obowiązywał w okresie wakacyjnym. include: Okres wakacyjny nie będzie miał wpływu na przedział czasowy. Aby skonfigurować okres wakacji, zapoznaj się z rozdziałem *Konfiguracja okresu wakacyjnego.*.
Krok 4	**absolute from** *start-date* **to** *end-date* Podaj datę początkową i datę końcową tego przedziału czasowego. *start-date*: Podaj datę początkową w formacie MM/DD/RRRR. *end-date*: Podaj datę końcową w formacie MM/DD/RRRR.
Krok 5	**periodic { [start** *start-time* **] [end** *end-time* **] [day-of-the-week** *week-day* **] }** Wybierz dni tygodnia, dla których dany przedział czasowy będzie obowiązujący. *start-time*: Podaj godzinę początku dnia w formacie GG:MM. *end-time*: Podaj godzinę końca dnia w formacie GG:MM. *week-day*: Podaj dni tygodnia w formacie 1-3, 7. Cyfry 1-7 oznaczają odpowiednio Poniedziałek, Wtorek, Środę, Czwartek, Piątek, Sobotę i Niedzielę.
Krok 6	**show time-range** Sprawdź konfigurację przedziału czasowego.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia pozycji z przedziałem czasowym i ustawiania nazwy jako time1, okresu wakacji do trybu exclude, czasu

całkowitego jako 10/01/2017 - 10/31/2017, a godzinowego jako 8:00 - 20:00 w każdy poniedziałek i wtorek:

Switch#config

Switch(config)#time-range time1

Switch(config-time-range)#holiday exclude

Switch(config-time-range)#absolute from 10/01/2017 **to** 10/31/2017

Switch(config-time-range)#periodic start 08:00 **end** 20:00 **day-of-the-week** 1,2

Switch(config-time-range)#show time-range

Time-range entry: 12 (Inactive)

Time-range entry: time1 (Inactive)

holiday: exclude

number of time slice: 1

01 - 10/01/2017 to 10/31/2017

- 08:00 to 20:00 on 1,2

Switch(config-time-range)#end

Switch#copy running-config startup-config

8.2.2 Konfiguracja okresu wakacyjnego

Wykonaj poniższe kroki, aby skonfigurować okres wakacyjny:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**holiday** *name* **start-date** *start-date* **end-date** *end-date* Utwórz pozycję. *name*: Podaj nazwę pozycji. *start-date* : Podaj datę początkową w formacie MM/DD. *end-date*: Podaj datę końcową w formacie MM/DD.
Krok 3	**show holiday** Sprawdź konfigurację okresu wakacyjnego.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia pozycji czasu wakacyjnego, ustawiania nazwy pozycji jako holiday1 oraz dat początkowych i końcowych jako 07/01 i 09/01:

Switch#config

Switch(config)#holiday holiday1 **start-date** 07/01 **end-date** 09/01

Switch(config)#show holiday

Index Holiday Name Start-End

----- ------------ ---------

1 holiday1 07.01-09.01

Switch(config)#end

Switch#copy running-config startup-config

Część 3

Zarzadzanie interfejsami

ROZDZIAŁY

1 Interfejs fizyczny

1.1 Obsługiwane funkcje

Przełącznik obsługuje następujące funkcje dla interfejsów fizycznych:

Parametry podstawowe

Możesz skonfigurować status, tryb prędkości, tryb dupleksu, kontrolę przepływu i inne parametry podstawowe portów.

Izolacja portów

Funkcja umożliwia ograniczenie działania wybranego portu do wysyłania pakietów jedynie do portów ze skonfigurowanej przez ciebie listy portów przesyłających.

Loopback Detection

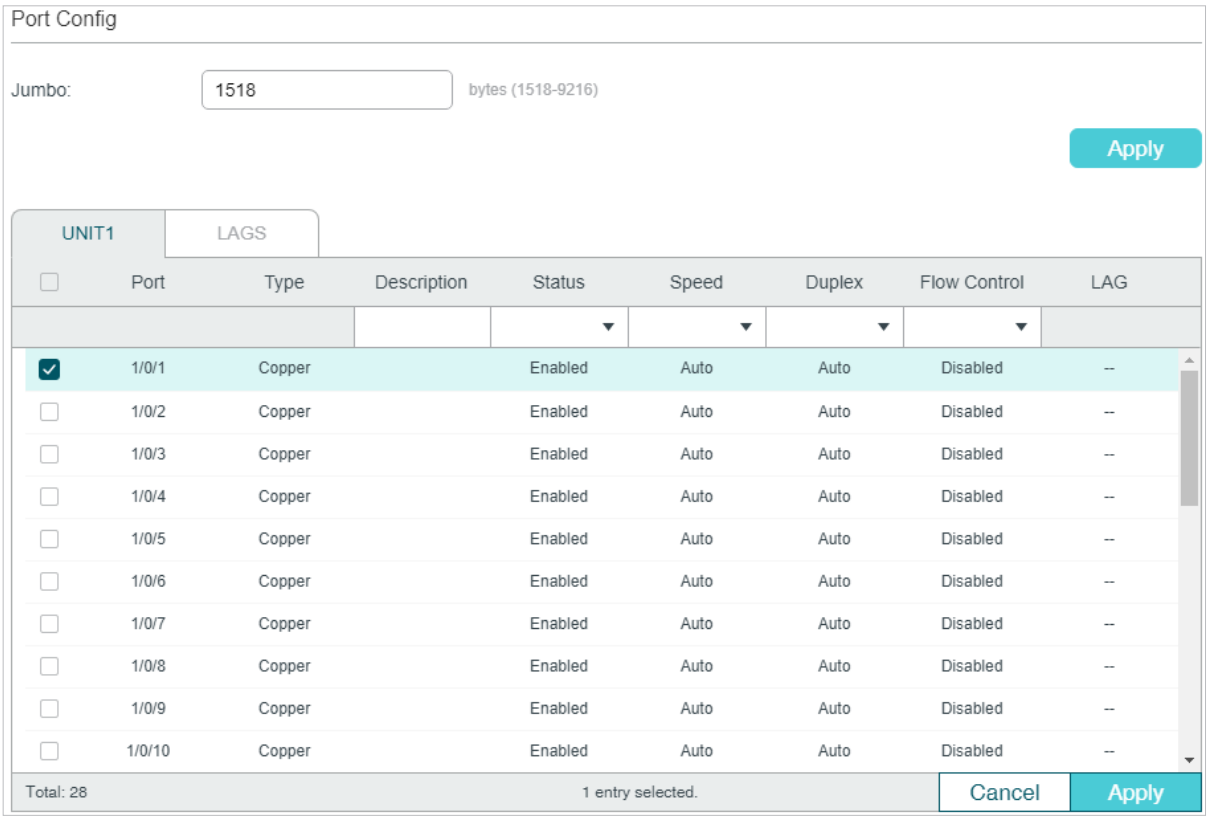
Dzięki tej funkcji przełącznik może wykrywać pętle w sieci. Po wykryciu pętli na porcie lub w sieci VLAN przełącznik wyświetli ostrzeżenie na interfejsie zarządzania i zgodnie z ustawieniami zablokuje odpowiedni port lub sieć VLAN.

2 Konfiguracja podstawowych parametrów

2.1 Przez GUI

Wybrać menu **L2 FEATURES > Switching > Port > Port Config** i załadować następującą stronę.

Rys. 2-1 Konfiguracja parametrów podstawowych



Aby skonfigurować parametry podstawowe portów, wykonaj następujące kroki:

1) Skonfiguruj rozmiar MTU ramek Jumbo dla wszystkich portów i kliknij **Apply**.

Jumbo	Skonfiguruj rozmiar ramek jumbo. Wielkość domyślna to 1518 bajtów. Z reguły rozmiar MTU (Maximum Transmission Unit) standardowej ramki to 1518 bajtów. Jeżeli chcesz, żeby przełącznik wysyłał ramki o MTU większym niż 1518 bajtów, w tym miejscu możesz ręcznie skonfigurować rozmiar MTU.

2) Wybierz co najmniej jeden port do konfiguracji parametrów podstawowych i kliknij **Apply**.

UNIT/LAGS	Kliknij **UNIT**, aby skonfigurować porty fizyczne. Kliknij **LAGS**, aby przeprowadzić konfigurację LAG.

Type	Informacja dotyczy typu portu. **Copper** oznacza port Ethernet, a **Fiber** oznacza port SFP.
Description	(Opcjonalnie) Wprowadź opis portu.
Status	Przy włączonej funkcji port normalnie przekierowuje pakiety. Port nie działa przy wyłączonej opcji. Funkcja jest domyślnie włączona.
Speed	Wybierz odpowiedni tryb prędkości dla portu. Przy wybraniu opcji **Auto** port automatycznie negocjuje prędkość z sąsiednim urządzeniem. Opcja **Auto** jest ustawiona domyślnie. Jeżeli obie strony łącza obsługują autonegocjację, zaleca się wybranie ustawienia **Auto**.
Duplex	Wybierz odpowiedni tryb dupleksu dla portu. Dostępne są trzy opcje: **Half (półdupleks)**, **Full (pełny dupleks)** i **Auto**. Domyślnie ustawiona opcja to **Auto**. **Half**: Port może wysyłać i otrzymywać pakiety, ale nie jednocześnie. **Full**: Port może jednocześnie wysyłać i otrzymywać pakiety. **Auto**: Port automatycznie negocjuje dupleks z urządzeniem równorzędnym.
Flow Control	Po włączeniu tej opcji, gdy przełącznik będzie przeciążony, wyśle ramkę PAUSE, aby powiadomić urządzenie równorzędne o zaprzestaniu wysyłania danych przez określony czas, co wyeliminuje problem utraty pakietów. Domyślnie opcja jest wyłączona.

Uwaga:

Zaleca się ustawić ten sam tryb prędkości i dupleksu dla portów na obu stronach łącza.

2.2 Przez CLI

Postępuj zgodnie z poniższymi krokami, aby skonfigurować podstawowe parametry portów.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**jumbo-size** *size* Zmień rozmiar MTU (Maximum Transmission Unit) do obsługi ramek jumbo. Domyślny rozmiar MTU ramek otrzymywanych i wysyłanych dla wszystkich portów wynosi 1518 bajtów. Aby przekazywać ramki jumbo, możesz ręcznie ustawić rozmiar MTU ramek, maksymalna wartość to 9216 bajtów. *size*: Skonfiguruj rozmiar MTU ramek jumbo. Może być to wartość między 1518 a 9216 bajtów.
Krok 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Wejdź w tryb konfiguracji interfejsu.

Krok 4	Skonfiguruj podstawowe parametry portu. **description** *string* Dodaj opis portu. *string*: Treść opisu portu, zawierająca od 1 do 16 znaków. **shutdown** **no shutdown** Wybierz **shutdown**, aby wyłączyć port i **no shutdown**, aby włączyć port. Włączony port normalnie przekierowuje pakiety. Port wyłączony odrzuca otrzymywane pakiety. Domyślnie wszystkie porty są włączone. **speed {** 10 | 100 | 1000 | 10000 | auto **}** Ustaw odpowiedni tryb prędkości dla portu. 10 | 100 | 1000 | 10000 | auto: tryb prędkości portu. Dostępne opcje różnią się w zależności od posiadanego urządzenia. Zaleca się ustawić ten sam tryb prędkości i dupleksu dla portu i połączonego z nim urządzenia. W przypadku wybrania opcji auto tryb prędkości wybierany jest na podstawie autonegocjacji. **duplex {** auto | full | half **}** Ustaw odpowiedni tryb dupleksu dla portu. auto | full | half: tryb dupleksu dla portu. Zaleca się ustawić ten sam tryb prędkości i dupleksu dla portu i połączonego z nim urządzenia. W przypadku wybrania opcji auto tryb dupleksu wybierany jest na podstawie autonegocjacji. **flow-control** Funkcja kontroli przepływu umożliwia przełącznikowi synchronizację prędkości transmisji danych z urządzeniem równorzędnym, co wyeliminuje problem utraty pakietów. Domyślnie opcja jest wyłączona.
Krok 5	**show interface configuration [fastEthernet** *port* **| gigabitEthernet** *port* **| | ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Sprawdź konfigurację portu lub konfigurację LAG.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje jak wprowadzić podstawowe konfiguracje portu1/0/1, takie jak ustawianie opisu portu, konfiguracja ramki jumbo, ustawianie autonegocjacji prędkości i dupleksu z sąsiadującym portem i włączanie funkcji kontroli przepływu:

Switch#configure

Switch#jumbo-size 9216

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#no shutdown

Switch(config-if)#description router connection

Switch(config-if)#speed auto

Switch(config-if)#duplex auto

Switch(config-if)#flow-control

Switch(config-if)#show interface configuration gigabitEthernet 1/0/1

Port	State	Speed	Duplex	FlowCtrl	Jumbo	Description
---	---	---	---	---	---	---
Gi1/0/1	Enable	Auto	Auto	Enable	Disable	router connection

Switch(config-if)#show jumbo-size

Global jumbo size : 9216

Switch(config-if)#end

Switch#copy running-config startup-config

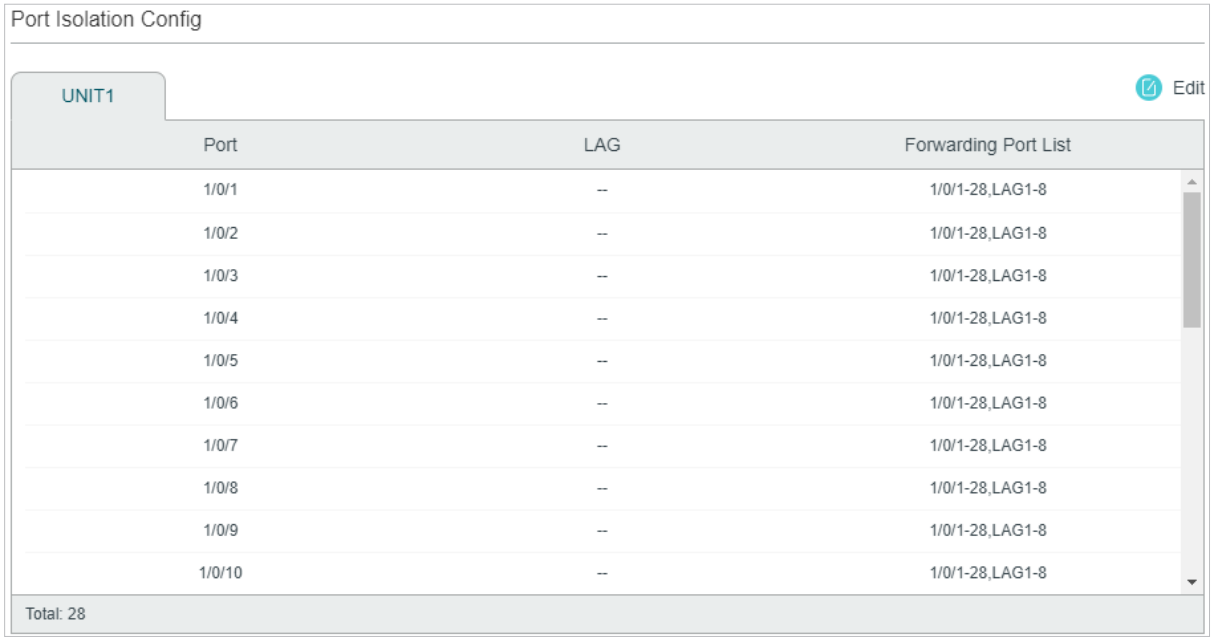
3 Konfiguracja funkcji izolacji portów

3.1 Przez GUI

Funkcja izolacji portów (Port Isolation) służy do ograniczania ilości danych przekazywanych przez port. Izolowany port może wysyłać pakiety jedynie do portów znajdujących się na jego liście (Forwarding Port List).

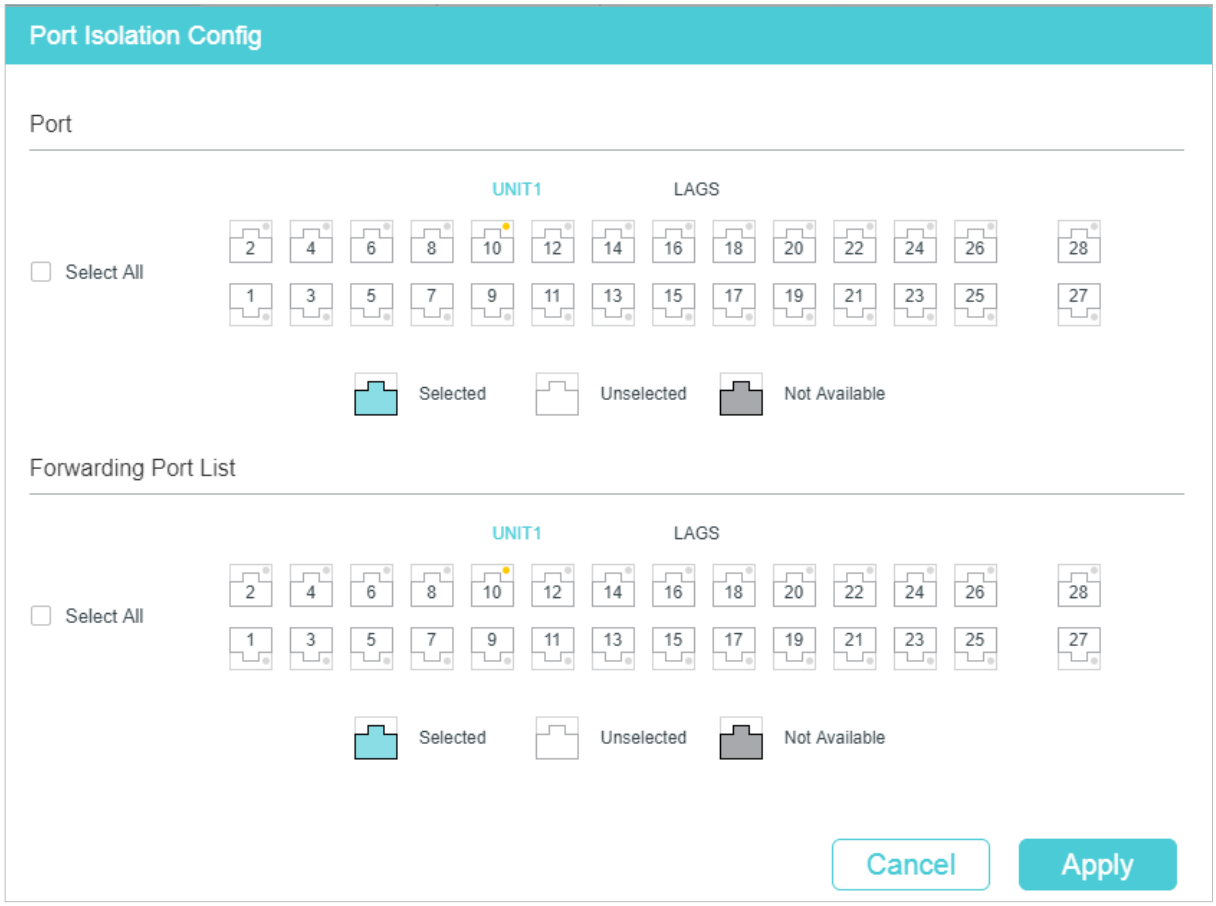
Wybierz menu **L2 FEATURES > Switching > Port > Port Isolation**, aby załadować poniższą stronę.

Rys. 3-1 Lista izolacji portów



Na powyższej stronie wyświetlana jest lista izolacji portów. Kliknij Edit, aby skonfigurować izolację portów na następnej stronie.

Rys. 3-2 Izolacja portów



Aby skonfigurować izolację portów, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Port** wybierz jeden lub wiele portów, które będą izolowane.
2) W sekcji **Forwarding Port List** wybierz porty przekazujące lub porty LAG, z którymi izolowane porty będą mogły się komunikować. Można wybrać więcej niż jeden port.
3) Kliknij **Apply**.

3.2 Przez CLI

Aby skonfigurować izolację portów, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Wybierz izolowany port i wejdź w tryb konfiguracji interfejsu.

Krok 3	**port isolation { [fa-forward-list** *fa-forward-list*] **[gi-forward-list** *gi-forward-list*] **[te-forward-list** *te-forward-list*] **[po-forward-list** *po-forward-list* **] }** Dodaj porty lub LAG do listy Forwarding Port List izolowanego portu. Można dodać wiele portów. *fa-forward-list / gi-forward-list / te-forward-list*: Określ przesyłające porty Ethernet. *po-forward-list:* Określ przesyłające porty LAG.
Krok 4	**show port isolation interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel* **}** Sprawdź konfigurację izolacji wyznaczonych portów.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym..

Poniższy przykład prezentuje jak dodać porty 1/0/1-3 i LAG 4 do listy przekierowywania portu 1/0/5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#port isolation gi-forward-list 1/0/1-3 **po-forward-list** 4

Switch(config-if)#show port isolation interface gigabitEthernet 1/0/5

Port LAG Forward-List

---- --- ----------

Gi1/0/5 N/A Gi1/0/1-3,Po4

Switch(config-if)#end

Switch#copy running-config startup-config

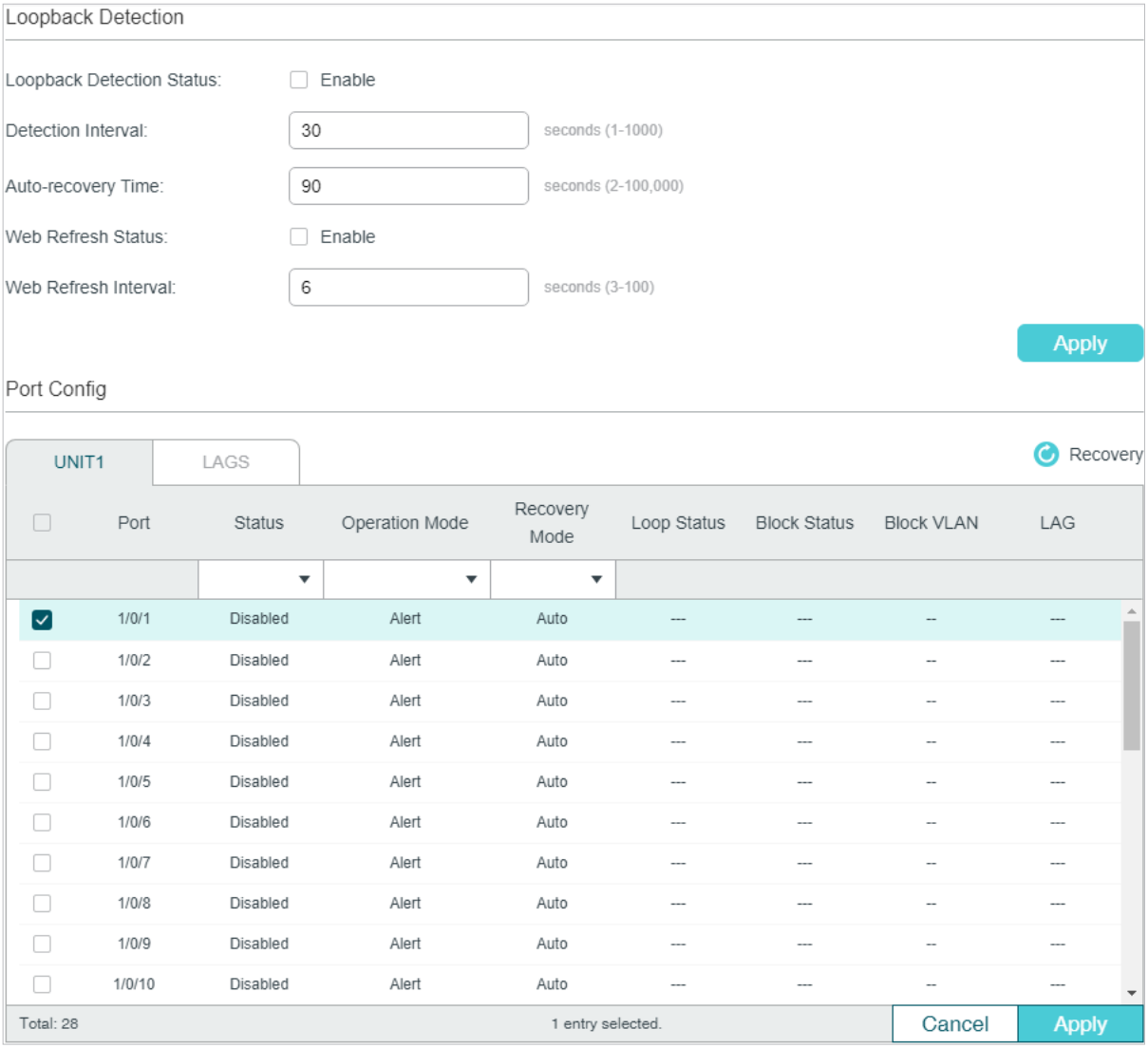
4 Konfiguracja funkcji Loopback Detection

4.1 Przez GUI

W celu uniknięcia burzy broadcastowej przed włączeniem funkcji loopback detection zalecamy włączenie funkcji storm control. Szczegółowe informacje dotyczące funkcji storm control znajdziesz w części *Konfiguracja QoS.*

Wybierz menu **L2 FEATURES > Switching > Port > Loopback Detection**, aby załadować poniższą stronę.

Rys. 4-1 Konfiguracja funkcji Loopback Detection



Aby skonfigurować funkcję Loopback Detection, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Loopback Detection** włącz funkcję loopback detection i skonfiguruj parametry globalne, następnie kliknij **Apply**.

Loopback Detection Status	Włącz funkcję Loopback Detection globalnie.
Detection Interval	Ustaw odstęp między wysyłaniem pakietów wykrywania pętli zwrotnych (loopback detection), w sekundach. Wartość musi zawierać się w zakresie od 1 do 1000, wartość domyślna to 30.
Auto-recovery Time	Ustaw czas przywrócenia globalnie. Zablokowany port w trybie Auto Recovery zostanie automatycznie przywrócony do normalnego stanu po wygaśnięciu czasu automatycznego przywrócenia. Wartość może wynosić od 2 do 100,000 s, wartość domyślna to 90.
Web Refresh Status	Przy włączonej funkcji przełącznik będzie w odpowiednim momencie odświeżał sieć. Funkcja jest domyślnie wyłączona.
Web Refresh Interval	Jeżeli opcja Web Refresh Status jest włączona, ustaw odstęp odświeżania, między 3 a 100 s. Wartość domyślna to 6 s.

2) W sekcji **Port Config** wybierz co najmniej jeden port do konfiguracji parametrów wykrywania pętli zwrotnych. Kliknij **Apply**.

Status	Włącz funkcję Loopback Detection dla portu.
Operation Mode	Po wykryciu pętli zwrotnej na porcie wybierz tryb działania: **Ostrzeżenie:** Status Loop wyświetli, czy na odpowiadającym porcie wykryto pętlę. Jest to ustawienie domyślne. **Port Based**: Poza wyświetlaniem ostrzeżeń przełącznik również zablokuje port, na którym wykryto pętlę. **VLAN-Based**: Jeżeli wykryto pętlę w sieci VLAN portu, przełącznik wyświetli ostrzeżenia, jak również zablokuje daną sieć VLAN. Ruch z innych sieci VLAN może być w dalszym ciągu normalnie przekierowywany przez port.
Recovery Mode	Jeżeli wybierzesz tryb działania **Port Based** lub **VLAN-Based,** musisz również skonfigurować tryb odzyskiwania dla zablokowanego portu: **Auto**: Po wygaśnięciu czasu automatycznego odzyskiwania zablokowany port będzie automatycznie przywracany do normalnego statusu. Jest to ustawienie domyślne. **Manual**: Wymagane jest ręczne zwolnienie zablokowanego portu. Kliknij **Recovery**, aby zwolnić wybrany port.

3) (Opcjonalnie) Sprawdź dane funkcji Loopback Detection.

Loop Status	Pokazuje, czy na porcie wykryto pętlę.
Block Status	Pokazuje, czy port jest zablokowany.
Block VLAN	Pokazuje zablokowane sieci VLAN.

4.2 Przez CLI

Aby skonfigurować funkcję Loopback Detection, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej..
Krok 2	**loopback-detection** Włącz funkcję Loopback Detection globalnie. Domyślnie funkcja jest wyłączona.
Krok 3	**loopback-detection interval** *interval-time* Ustaw odstęp wysyłania pakietów wykrywania pętli zwrotnych, aby umożliwić wykrycie pętli w sieci. *interval-time:* Odstęp czasu, w jakim wysyłane są pakiety wykrywania pętli. Wartość może wynosić od 1 do 1000 s. Wartość domyślna to 30 s.
Krok 4	**loopback-detection recovery-time** *recovery-time* Ustaw czas automatycznego przywracania, po którym zablokowany port w trybie Auto Recovery może automatycznie powrócić do normalnego statusu. *recovery-time*: Ustaw interwał wykrywania na czas miedzy 2 a 100,000 s. Wartość domyślna to 90.
Krok 5	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Wejdź w tryb konfiguracji interfejsu.
Krok 6	**loopback-detection** Włącz funkcję Loopback Detection dla portu. Domyślnie funkcja jest wyłączona.
Krok 7	**loopback-detection config process-mode {** alert | port-based | vlan-based **} recovery-mode {** auto | manual **}** Ustaw tryb przetwarzania na wypadek wykrycia na porcie pętli zwrotnej. Dostępne są trzy tryby. alert: Po wykryciu pętli zwrotnej przełącznik jedynie wyświetli ostrzeżenia. Jest to ustawienie domyślne. port-based: Przełącznik wyświetli ostrzeżenia i zablokuje port, na którym wykryto pętlę. vlan-based: Przełącznik wyświetli ostrzeżenia i zablokuje VLAN portom, na którym wykryto pętlę. Ustaw tryb odzyskiwania dla zablokowanego portu. Dostępne są dwa tryby. auto: Po wygaśnięciu czasu automatycznego odzyskiwania zablokowany port będzie automatycznie przywracany do normalnego statusu i na nowo zacznie wykrywać pętle w sieci. manual: Wymagane jest ręczne zwolnienie zablokowanego portu. Aby przywrócić wybrany port, możesz użyć polecenia 'loopback-detection recover'.
Krok 8	**show loopback-detection global** Sprawdź konfigurację globalną funkcji Loopback Detection.

Krok 9	**show loopback-detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel* **}** Sprawdź konfigurację funkcji Loopback Detection wybranego portu.
Krok 10	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład przedstawia jak włączyć funkcję Loopback Detection globalnie (zachowaj parametry domyślne):

Switch#configure

Switch(config)#loopback-detection

Switch(config)#show loopback-detection global

Loopback detection global status : enable

Loopback detection interval : 30s

Loopback detection recovery time : 3 intervals

Switch(config-if)#end

Switch#copy running-config startup-config

Poniższy przykład prezentuje jak włączyć funkcję Loopback Detection dla portów 1/0/3, ustawić tryb przetwarzania na ostrzeżenie (alert) i tryb odzyskiwania na auto.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode alert **recovery-mode** auto

Switch(config-if)#show loopback-detection interface gigabitEthernet 1/0/3

Port	Enable	Process Mode	Recovery Mode	Loopback	Block	LAG
----	------	----------	----------	--------	-----	----
Gi1/0/3	enable	alert	auto	N/A	N/A	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

Część 4

Konfiguracja LAG

ROZDZIAŁY

1 Grupy agregacji łączy (LAG)

1.1 Wprowadzenie

Funkcja LAG (Link Aggregation Group) umożliwia połączenie ze sobą wielu portów fizycznych przełącznika w jedną logiczną całość, co pozwala uzyskać większą przepustowość oraz niezawodność połączeń.

1.2 Obsługiwane funkcje

Funkcję LAG można skonfigurować na dwa sposoby: jako statyczne LAG i dynamiczne LACP (Link Aggregation Control Protocol).

Statyczne LAG

Porty muszą być dodawane ręcznie do LAG.

LACP

Przełącznik korzysta z protokołu LACP, aby wdrożyć dynamiczną agregację i dezagregację łączy poprzez wymianę pakietów LACP z urządzeniem równorzędnym. Protokół LACP zwiększa elastyczność konfiguracji LAG.

2 Konfiguracja LAG

Aby przeprowadzić proces konfiguracji LAG, wykonaj poniższe kroki:

1) Skonfiguruj globalny algorytm równoważenia obciążenia pasma.
2) Skonfiguruj do statycznego LAG lub LACP.

Wskazówki dotyczące konfiguracji

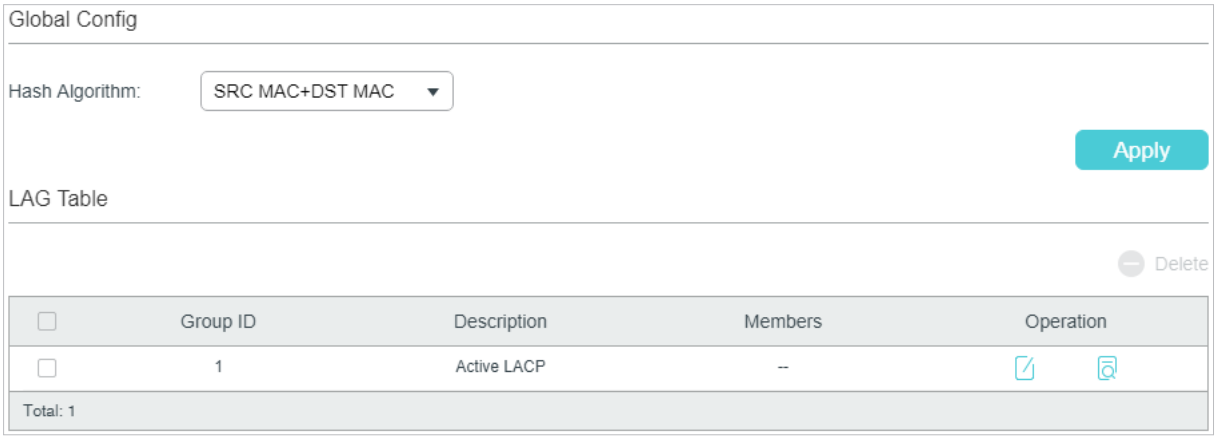
- Upewnij się, że obydwie strony łącza agregacji pracują w tym samym trybie LAG. Np., jeżeli lokalna strona pracuje w trybie LACP, urządzenie równorzędne też musi mieć ustawiony tryb LACP.
- Upewnij się, że urządzenia po obydwu stronach łącza agregacji korzystając z tych samych numerów portów fizycznych, o tych samych prędkościach, trybie dupleksu, ramce jumbo i kontroli przepływu.
- Jeden port może być jednocześnie dodany do więcej niż jednego łącza agregacji.
- LACP nie obsługuje połączeń w trybie półdupleksu.
- Jedno statyczne LAG obsługuje do 8 portów. Wszystkie te porty korzystają po równo z dostępnej przepustowości. Jeżeli aktywne łącze napotka błąd, pozostałe aktywne łącza dzielą przepustowość równomiernie.
- Jedno LACP LAG obsługuje wiele portów, ale tylko osiem z nich może działać w tym samym czasie. Pozostałe porty są portami alternatywnymi. Korzystając z protokołu LACP, przełączniki negocjują parametry i wybierają porty pracujące. Gdy na pracującym porcie wystąpi błąd, port alternatywny o najwyższym priorytecie zastępuje go i rozpoczyna przesyłanie danych.
- Dla funkcji takich jak IGMP Snooping, 802.1Q VLAN, MAC VLAN, protokół VLAN, VLAN-VPN, GVRP, Voice VLAN, STP, QoS, DHCP Snooping i kontrola przepustowości, port LAG korzysta z konfiguracji LAG, a nie z ustawień własnych. Konfiguracja portu obowiązuje dopiero po opuszczeniu LAG.
- Port uruchomiony poprzez Port Security, Port Mirror, filtrowanie adresów MAC lub 802.1X nie może być dodany do LAG, a port LAG nie może być uruchomiony za pomocą tych funkcji.

2.1 Przez GUI

2.1.1 Konfiguracja algorytmu równoważenia obciążenia pasma

Wybierz z menu **L2 FEATURES > Switching > LAG > LAG Table**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna



W sekcji **Global Config** wybierz algorytm równoważenia obciążenia pasma (Hash Algorithm) i kliknij **Apply**.

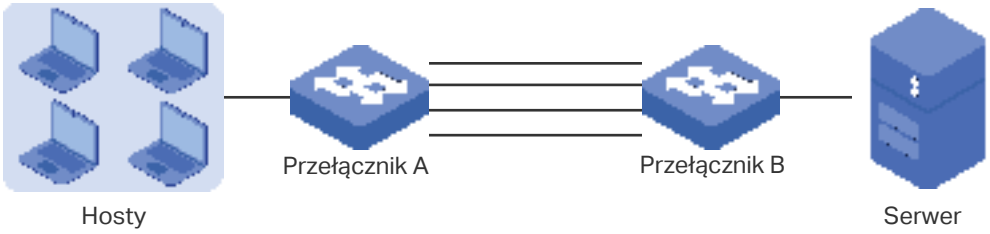
Hash Algorithm	Wybierz algorytm Hash, aby przełącznik mógł wybierać porty do przesyłania odebranych pakietów. W ten sposób przepływ danych jest równomierny, a obciążenie pasma zrównoważone. Do wyboru są trzy możliwości: **SRC MAC**: Obliczenia są oparte na źródłowych adresach MAC pakietów. **DST MAC**: Obliczenia są oparte na docelowych adresach MAC pakietów. **SRC MAC+DST MAC**: Obliczenia są oparte na źródłowych i docelowych adresach MAC pakietów. **SRC IP**: Obliczenia są oparte na źródłowych adresach IP pakietów. **DST IP**: Obliczenia są oparte na docelowych adresach IP pakietów. **SRC IP+DST IP**: Obliczenia są oparte na źródłowych i docelowych adresach IP pakietów.

Wskazówki:

- Algorytm równoważenia obciążenia pasma obowiązuje tylko dla ruchu wychodzącego. Jeżeli strumień danych nie jest dobrze współdzielony przez łącza, zmień algorytm interfejsu wychodzącego.
- Wybierz prawidłowy algorytm równoważenia obciążenia, aby uniknąć przesyłania strumienia danych tylko na jednym fizycznym łączu. Np., gdy przełącznik A odbiera pakiety od kilku hostów i przesyła je do serwera ze stałym adresem MAC,

ustaw algorytm jako “SRC MAC”, aby umożliwić przełącznikowi A wybranie portu przesyłającego w oparciu o źródłowy adres MAC odebranych pakietów.

Rys. 2-2 Konfiguracja algorytmu Hash



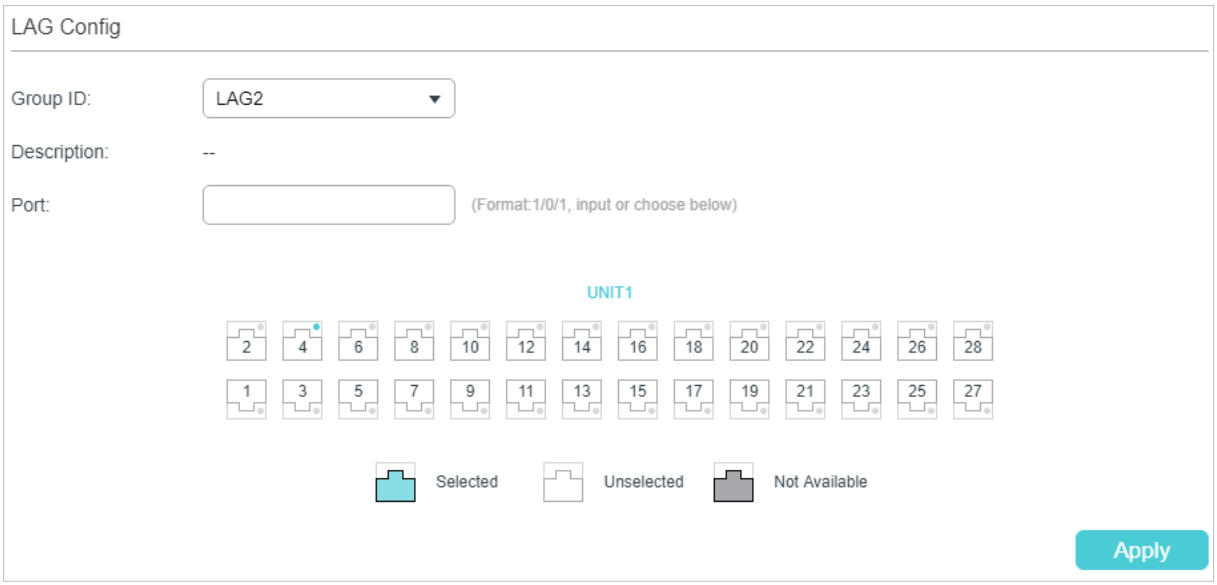
2.1.2 Konfiguracja do statycznego LAG lub LACP

Dla jednego portu można wybrać tylko jeden tryb LAG: statyczny LAG lub LACP. Upewnij się, że obie strony łącza korzystają z tego samego trybu LAG.

- Konfiguracja do statycznego LAG

Wybierz z menu **L2 FEATURES > Switching > LAG > Static LAG**, aby wyświetlić poniższą stronę.

Rys. 2-3 Statyczne LAG



Wykonaj poniższe kroki, aby skonfigurować statyczne LAG:

1) Wybierz LAG do konfiguracji.

Group ID	Wybierz LAG do konfiguracji jako statyczne LAG.
Description	Tryb LAG.

2) Wybierz porty LAG. Jest tutaj wiele opcji.
3) Kliknij **Apply**.

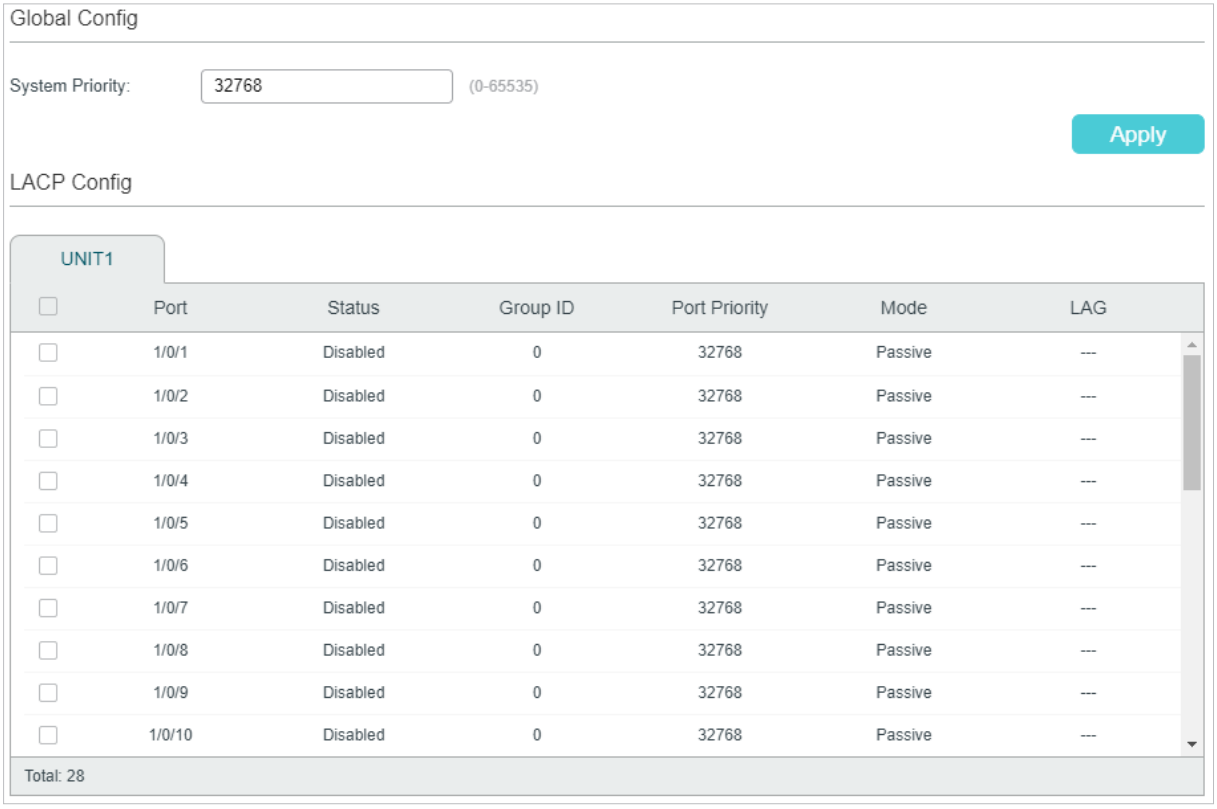
Uwaga:

Usunięcie wszystkich portów spowoduje usunięcie LAG.

Konfiguracja do LACP

Wybierz z menu **L2 FEATURES > Switching > LAG > LACP**, aby wyświetlić poniższą stronę.

Rys. 2-4 Konfiguracja do LACP



Wykonaj poniższe kroki, aby skonfigurować do LACP:

1) Określ priorytety dla przełącznika i kliknij **Apply**.

System Priority	Określ priorytety dla przełącznika, pamiętając, że im mniejsza wartość, tym wyższy priorytet. Aby zachować zgodność portów po obydwu stronach, priorytet jednego urządzenia może być wyższy niż priorytet drugiego urządzenia. Urządzenie o wyższym priorytecie określi porty aktywne, a drugie urządzenie wybierze porty aktywne, spośród portów zidentyfikowanych przez urządzenie pierwsze. Jeżeli obie strony mają tą samą wartość priorytetu, urządzenie o niższym adresie MAC uznawane jest za urządzenie o wyższym priorytecie.

2) Wybierz porty LAG i skonfiguruj odpowiednie parametry. Kliknij **Apply**.

Group ID	Podaj grupowe ID LAG. Pamiętaj, że nie możesz tutaj wpisać grupowego ID innego statycznego LAG. Prawidłowa wartość grupowego ID zależy od maksymalnej liczby LAG obsługiwanych przez przełącznik. Np., jeżeli przełącznik obsługuje do 14 LAG, prawidłowa wartość waha się od 1 do 14.
Port Priority (0-65535)	Określ priorytety portów, pamiętając, że im niższa wartość, tym wyższy priorytet. Port o wyższym priorytecie w LAG zostanie wybrany jako port aktywny do przesyłu danych. Maksymalnie 8 portów może pracować w tym samym czasie. Jeżeli dwa porty mają tą samą wartość priorytetu, port o niższym numerze poru uznawany jest za port o wyższym priorytecie.
Mode	Wybierz tryp LACP dla portu. W trybie LACP przełącznik korzysta z LACPDU (Link Aggregation Control Protocol Data Unit) do negocjacji parametrów z urządzeniem równorzędnym. W ten sposób obie strony wybierają porty aktywne i tworzą łączę agregacji. W trybie LACP można ustalić czy dany port ma służyć do przesyłu LACPDU. Do wyboru są dwa tryby: **Passive**: Port nie prześle LACPDU przed odebraniem LACPDU od urządzenia równorzędnego. **Active**: Port podejmie inicjatywę przesłania LACPDU.
Status	Włącz funkcję LACP portu. Domyślnie ta funkcja jest wyłączona.

2.2 Przez CLI

2.2.1 Konfiguracja algorytmu równoważenia obciążenia pasma

Wykonaj poniższe kroki, aby skonfigurować algorytm równoważenia obciążenia pasma:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**port-channel load-balance {** src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip **}** Wybierz algorytm Hash, aby przełącznik mógł wybierać porty do przesyłania odebranych pakietów. W teb sposób przepływ danych jest równomierny, a obciążenie pasma zrównoważone. Do wyboru są trzy możliwości. src-mac: Obliczenia są oparte na źródłowych adresach MAC pakietów. dst-mac: Obliczenia są oparte na docelowych adresach MAC pakietów. src-dst-mac: Obliczenia są oparte na źródłowych i docelowych adresach MAC pakietów. src-ip: Obliczenia są oparte na źródłowych adresach IP pakietów. dst-ip: Obliczenia są oparte na docelowych adresach IP pakietów. src-dst-ip: Obliczenia są oparte na źródłowych i docelowych adresach IP pakietów.
Krok 3	**show etherchannel load-balance** Zweryfikuj konfigurację algorytmu równoważenia obciążenia pasma.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania trybu globalnego równoważenia obciążenia pasma jako src-dst-mac:

Switch#configure

Switch(config)#port-channel load-balance src-dst-mac

Switch(config)#show etherchannel load-balance

EtherChannel Load-Balancing Configuration: src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:

Non-IP: Source XOR Destination MAC address

IPv4: Source XOR Destination MAC address

IPv6: Source XOR Destination MAC address

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja do statycznego LAG lub LACP

Dla jednego portu można wybrać tylko jeden tryb LAG: statyczny LAG lub LACP. Upewnij się, że obie strony łącza korzystają z tego samego trybu LAG.

Konfiguracja do statycznego LAG

Wykonaj poniższe kroki, aby skonfigurować statyczne LAG:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**channel-group** *num* **mode on** Dodaj port do statycznego LAG. *num*: Grupowy ID LAG.
Krok 4	**show etherchannel** *num* **summary** Zweryfikuj konfigurację statycznego LAG. *num*: Grupowy ID LAG.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób dodawania potrów 1/0/5-8 do LAG 2 i ustawiania trybu jako statyczne LAG:

Switch#configure

Switch(config)#interface range gigabitEthernet 1/0/5-8

Switch(config-if-range)#channel-group 2 **mode** on

Switch(config-if-range)#show etherchannel 2 **summary**

Flags: D - down P - bundled in port-channel U - in use

I - stand-alone H - hot-standby(LACP only) s - suspended

R - layer3 S - layer2 f - failed to allocate aggregator

u - unsuitable for bundling w - waiting to be aggregated d - default port

Group Port-channel Protocol Ports

----- --------- ------- -------------------------------

2 Po2(S) - Gi1/0/5(D) Gi1/0/6(D) Gi1/0/7(D) Gi1/0/8(D)

Switch(config-if-range)#end

Switch#copy running-config startup-config

Konfiguracja do LACP

Wykonaj poniższe kroki, aby skonfigurować do LACP:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**lacp system-priority** *pri* Określ priorytety dla przełącznika. Aby zachować zgodność portów po obydwu stronach, priorytet jednego urządzenia może być wyższy niż priorytet drugiego urządzenia. Urządzenie o wyższym priorytecie określi porty aktywne, a drugie urządzenie wybierze porty aktywne, spośród portów zidentyfikowanych przez urządzenie pierwsze. Jeżeli obie strony mają tą samą wartość priorytetu, urządzenie o niższym adresie MAC uznawane jest za urządzenie o wyższym priorytecie. pri: Priorytet systemowy. Prawidłowa wartość wahs się od 0 do 65535, a wartością domyślną jest 32768. Im mniejsza wartość, tym wyższy priorytet urządzenia.
Krok 3	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 4	**channel-group** *num* **mode {** active | passive **}** Dodaj port do LAG i ustaw tryb LACP. *num*: Grupowy ID LAG. **mode**: Tryb LAG. Wybierz jeden z trybów LACP: active lub passive. W trybie LACP przełącznik korzysta z LACPDU (Link Aggregation Control Protocol Data Unit) do negocjacji parametrów z urządzeniem równorzędnym. W ten sposób obie strony wybierają porty aktywne i tworzą łączę agregacji. W trybie LACP można ustalić czy dany port ma służyć do przesyłu LACPDU. passive: Port nie prześle LACPDU przed odebraniem LACPDU od urządzenia równorzędnego. active: Port podejmie inicjatywę przesłania LACPDU.
Krok 5	**lacp port-priority** *pri* Określ priorytet portów. Port o wyższym priorytecie w LAG zostanie wybrany jako port aktywny do przesyłu danych. Jeżeli dwa porty mają tą samą wartość priorytetu, port o niższym numerze poru uznawany jest za port o wyższym priorytecie. pri: Priorytet portu. Prawidłowa wartość waha się od 0 do 65535, a wartością domyślną jest 32768. Im mniejsza wartość, tym wyższy priorytet portu.
Krok 6	**show lacp sys-id** Zweryfikuj priorytety systemu globalnego.
Krok 7	**show lacp internal** Zweryfikuj konfigurację do LACP lokalnego przełącznika.

Krok 8	**end** Powróć do trzybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia do pliku konfiguracyjnego.

Poniższy schemat przedstawia przykładowy sposób ustawiania priorytetu przełącznika jako 2:

Switch#configure

Switch(config)#lacp system-priority 2

Switch(config)#show lacp sys-id

2, 000a.eb13.2397

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to add ports 1/0/1-4 to LAG 6, set the mode as LACP, and select the LACPDU sending mode as active:

Switch#configure

Switch(config)#interface range gigabitEthernet 1/0/1-4

Switch(config-if-range)#channel-group 6 **mode** active

Switch(config-if-range)#show lacp internal

Flags: S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in active mode

P - Device is in passive mode

Channel group 6

Port	Flags	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Gi1/0/1	SA	Up	32768	0x6	0x4b1	0x1	0x7d
Gi1/0/2	SA	Down	32768	0x6	0	0x2	0x45
Gi1/0/3	SA	Down	32768	0x6	0	0x3	0x45
Gi1/0/4	SA	Down	32768	0x6	0	0x4	0x45

Switch(config-if-range)#end

Switch#copy running-config startup-config

Część 5

Zarządzanie tablicą adresów MAC

ROZDZIAŁY

1 Tablica adresów MAC

1.1 Obsługiwane funkcje

Tablica adresów przełącznika zawiera adresy dynamiczne, adresy statyczne i umożliwia filtrowanie adresów. Wpisy możesz odpowiednio dodawać i usuwać.

Konfiguracja adresu

- Dynamic address (adres dynamiczny)

Adresy dynamiczne to adresy, których przełącznik uczy się automatycznie. Przełącznik regularnie pozbywa się adresów, które nie są już używane. Przełącznik usuwa wpisy adresów MAC powiązanych z urządzeniami sieciowymi, jeżeli dane urządzenia w trakcie czasu starzenia adresów nie wysłały żadnego pakietu. W razie potrzeby, możesz samodzielnie określić czas starzenia się adresów.

- Static address (adres statyczny)

Adresy statyczne dodawane są do tablicy adresów ręcznie i nie starzeją się. Dla stosunkowo stałych połączeń, np. często odwiedzanego serwera, możesz ręcznie ustawić adres MAC serwera jako statyczny - zwiększy to wydajność przesyłania przełącznika.

- Filtering address (filtrowanie adresów)

Filtrowanie adresów umożliwia wyznaczenie pakietów z określonymi źródłowymi lub docelowymi adresami MAC, które będą odrzucane przez przełącznik.

2 Konfiguracja adresów MAC

Tablica adresów MAC umożliwia:

- dodawanie wpisów statycznych adresów MAC;
- zmianę czasu starzenia się adresów MAC;
- dodawanie wpisów filtrowania adresów;
- wyświetlanie wpisów tablicy adresów.

2.1 Przez GUI

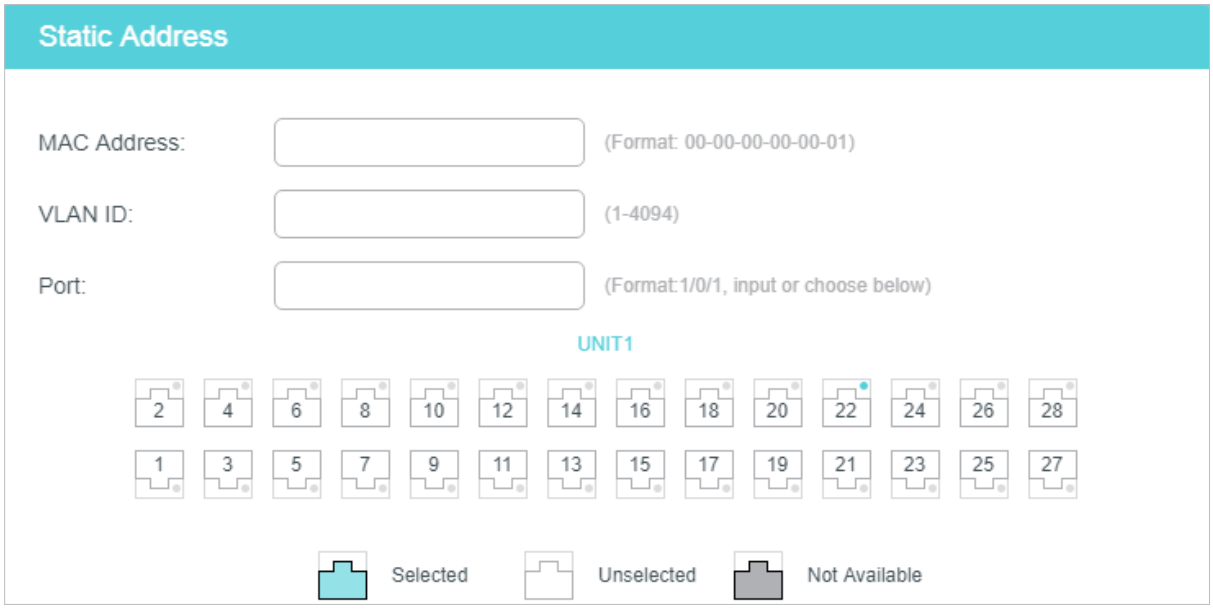
2.1.1 Dodawanie wpisów statycznych adresów MAC

Możesz dodać do tabeli wpisy statycznych adresów MAC ręcznie, wyznaczając wybrane adresy MAC lub wiążąc wpisy dynamicznych adresów MAC.

- Ręczne dodawanie adresów MAC

Wybierz menu **L2 FEATURES > Switching > MAC Address > Static Address** i kliknij Add, aby załadować następującą stronę.

Rys. 2-1 Ręczne dodawanie adresów MAC



Aby dodać wpis statycznego adresu MAC, postępuj zgodnie z poniższymi krokami:

1) Wprowadź adres MAC, VLAN ID i wybierz port, aby powiązać je w jeden wpis adresu.

MAC Address	Wprowadź statyczny adres MAC, który będzie dodany do wpisu statycznego adresu MAC.
VLAN ID	Wyznacz istniejącą sieć VLAN, w której odbierane są pakiety z określonymi adresami MAC.
Port	Wyznacz port, do którego pakiety z określonymi adresami MAC są przekierowywane. Port musi należeć do wyznaczonej sieci VLAN. Po dodaniu statycznego adresu MAC, przełącznik nie może prawidłowo przekierowywać pakietów, jeżeli numer odpowiadającego portu adresu MAC jest nieprawidłowy lub zmieniono połączony port (lub urządzenie). Należy odpowiednio zresetować wpis adresu statycznego.

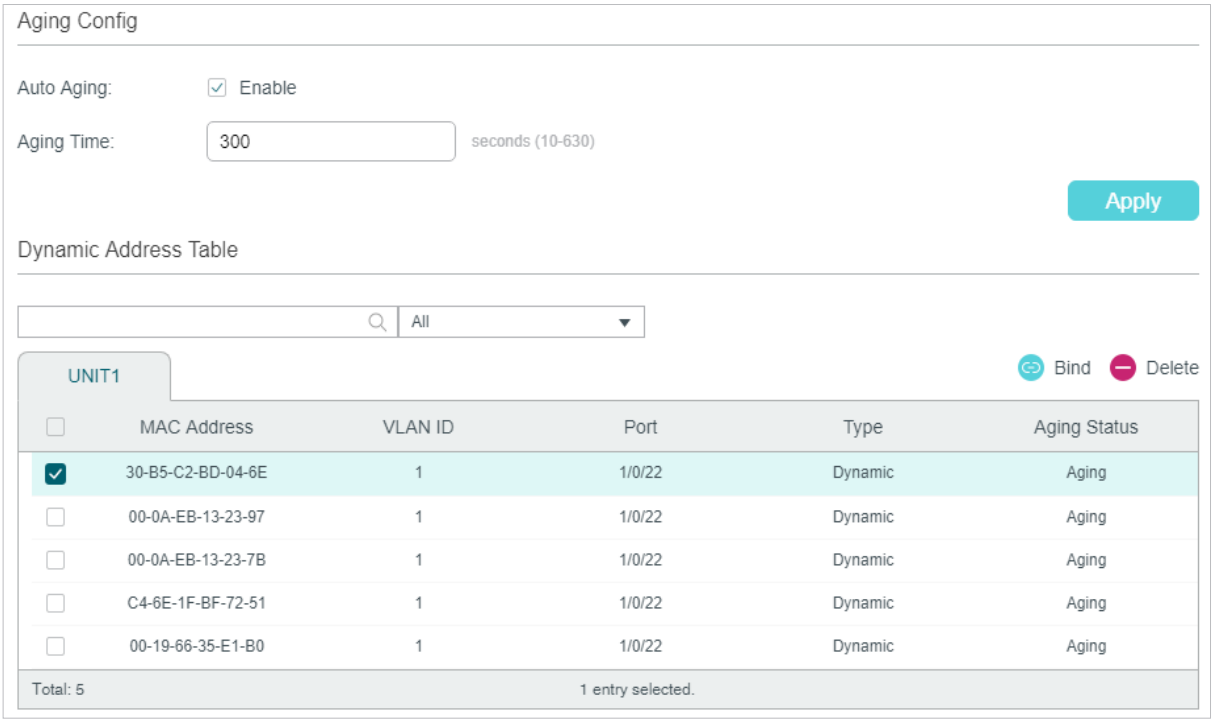
2) Kliknij **Create**.

■ Wiązanie wpisów adresu dynamicznego

Jeżeli wpisy adresu dynamicznego są często używane, możesz powiązać wpisy jako wpisy statyczne.

Wybierz menu **L2 FEATURES > Switching > MAC Address > Dynamic Address**, aby załadować następującą stronę.

Rys. 2-2 Wiązanie wpisów dynamicznego adresu MAC



Aby powiązać wpisy dynamicznego adresu MAC, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Dynamic Address Table wybierz wpisy adresów MAC**.

2) Kliknij **Bind. Wybrane wpisy zmienią typ na wpisy statycznego adresu MAC**.

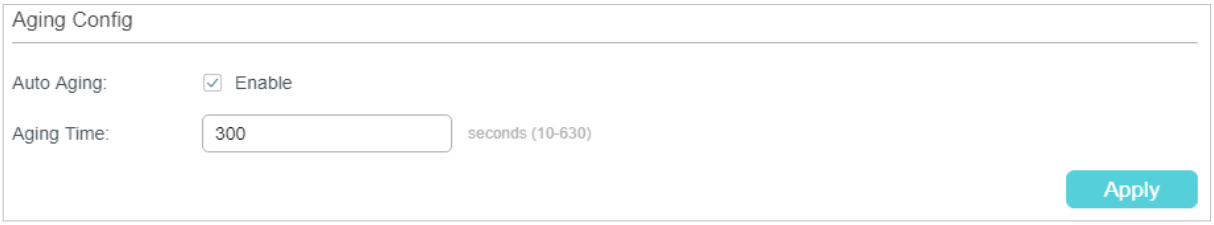
Uwaga:

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy statyczne.
- Porty w grupach LAG (Link Aggregation Group) nie są obsługiwane w konfiguracji adresów statycznych.

2.1.2 Zmiana czasu utraty ważności wpisów adresów dynamicznych

Wybierz menu **L2 FEATURES > Switching > MAC Address > Dynamic Address**, aby załadować następującą stronę.

Rys. 2-3 Zmiana czasu utraty ważności wpisów adresów dynamicznych



Aby zmienić czas utraty ważności wpisów adresów dynamicznych, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Aging Config** włącz Auto Aging i wprowadź wybraną długość okresu.

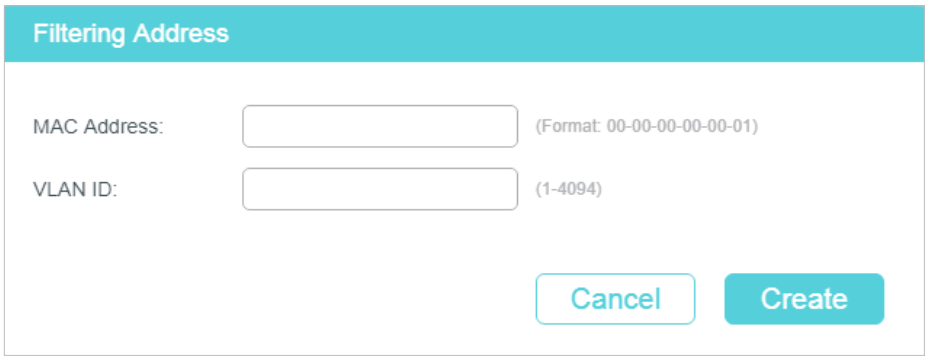
Auto Aging	Włącz Auto Aging. Przełącznik będzie automatycznie aktualizował tablicę dynamicznych adresów, zgodnie z mechanizmem starzenia. Funkcja jest domyślnie włączona.
Aging Time	Ustaw długość okresu, przez który po ostatnim użyciu lub aktualizacji wpis dynamiczny pozostaje na tablicy adresów MAC. Wartość musi zawierać się między 10 a 630 s. Wartość domyślna to 300. Krótki czas utraty ważności sprawdzi się w sieciach, których topologia często się zmienia. Długi czas utraty ważności jest odpowiedni w stabilnych sieciach. W przypadku braku pewności w kwestii wybrania najlepszego ustawienia, zaleca się zachowanie wartości domyślnej.

2) Kliknij **Apply.**

2.1.3 Dodawanie wpisów filtrowania adresów MAC

Wybierz menu **L2 FEATURES > Switching > MAC Address > Filtering Address** i kliknij Add, aby załadować następującą stronę.

Rys. 2-4 Dodawanie wpisów filtrowania adresów MAC



Aby dodać wpisy filtrowania adresów MAC, postępuj zgodnie z poniższymi krokami.

1) Wprowadź adres MAC i VLAN ID.

MAC Address	Wyznacz adres MAC, który będzie wykorzystywany przez przełącznik do filtrowania otrzymywanych pakietów.
VLAN ID	Wyznacz sieć VLAN, w której pakiety o wyznaczonym adresie MAC są odrzucane.

2) Kliknij **Create**.

Uwaga:

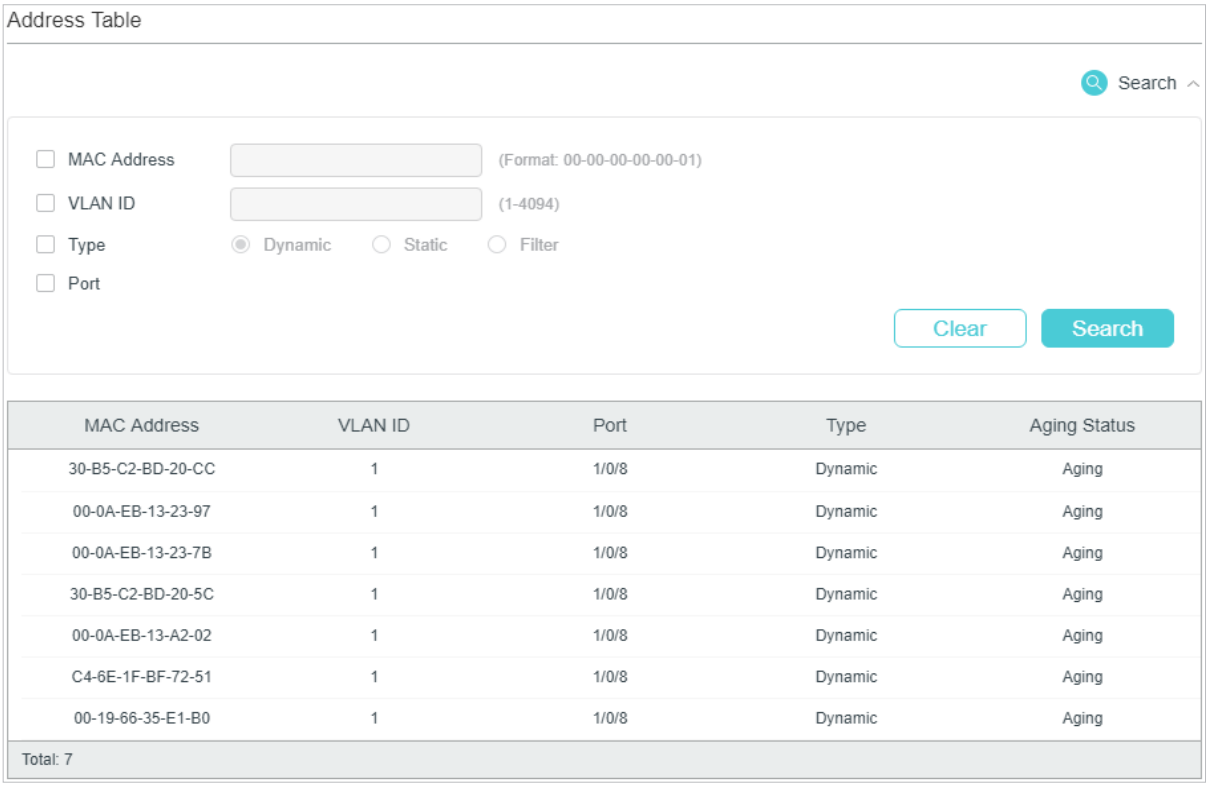
- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy filtrowania.

2.1.4 Wyświetlanie wpisów tablicy adresów

Możesz wyświetlać wpisy na tablicy adresów MAC, aby sprawdzać poprzednie działania i dane adresu.

Wybierz menu **L2 FEATURES > Switching > MAC Address > Address Table** i kliknij Search, aby załadować następującą stronę.

Rys. 2-5 Wyświetlanie wpisów tablicy adresów



2.2 Przez CLI

2.2.1 Dodawanie wpisów statycznych adresów MAC

Aby dodać wpisy statycznych adresów MAC, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**mac address-table static** *mac-addr* **vid** *vid* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Powiąż adres MAC, VLAN i port, aby dodać adres statyczny do VLAN. *mac-addr*: Wprowadź adres MAC. Pakiety z tym adresem docelowym otrzymane w wyznaczonej sieci VLAN są przekierowywane do wyznaczonego portu. Format to xx:xx:xx:xx:xx:xx, np. 00:00:00:00:00:01. *vid*: Wyznacz istniejącą sieć VLAN, w której odbierane są pakiety z określonym adresem MAC. *port:* Wyznacz port, do którego przesyłane są pakiety z określonym adresem MAC. Port musi należeć do wyznaczonej sieci VLAN.

Krok 3	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy statyczne.
- Porty w grupach LAG (Link Aggregation Group) nie są obsługiwane w konfiguracji adresów statycznych.

Poniższy przykład prezentuje jak dodać wpis statycznego adresu MAC dla adresu 00:02:58:4f:6c:23, VLAN 10 i portu 1. Jeżeli pakiet jest odebrany we VLAN 10 z tym adresem jako docelowym, pakiet zostanie przekierowany jedynie do portu 1/0/1.

Switch#configure

Switch(config)# mac address-table static 00:02:58:4f:6c:23 **vid** 10 **interface gigabitEthernet** 1/0/1

Switch(config)#show mac address-table static

MAC Address Table

MAC	VLAN	Port	Type	Aging
00:02:58:4f:6c:23	10	Gi1/0/1	config static	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Zmiana czasu utraty ważności wpisów adresów dynamicznych

Aby zmienić czas utraty ważności wpisów adresów dynamicznych, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2	**mac address-table aging-time** *aging-time* Ustaw czas utraty ważności adresów dla wpisów adresów dynamicznych. *aging-time:* Ustaw długość okresu, przez który po ostatnim użyciu lub aktualizacji wpis dynamiczny pozostaje w tablicy adresów MAC. Wartość musi zawierać się między 10 a 630 s. Wartość 0 oznacza wyłączoną funkcję Auto Aging. Wartość domyślna to 300. W przypadku braku pewności w kwestii wybrania najlepszego ustawienia, zaleca się zachowanie wartości domyślnej.
Krok 3	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje zmianę czasu utraty ważności na 500 s. Wpis dynamiczny pozostaje na tablicy adresów MAC przez 500 s od użycia lub aktualizacji wpisu.

Switch#configure

Switch(config)# mac address-table aging-time 500

Switch(config)#show mac address-table aging-time

Aging time is 500 sec.

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Dodawanie wpisów filtrowania adresów MAC

Aby dodać wpisy filtrowania adresów MAC, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**mac address-table filtering** *mac-addr* **vid** *vid* Dodaj adres filtrowania do sieci VLAN. *mac-addr:* Określ adres MAC, który będzie wykorzystywany przez przełącznik do filtrowania otrzymywanych pakietów. Pakiety z tym adresem źródłowym lub docelowym będą odrzucane przez przełącznik. Format to xx:xx:xx:xx:xx:xx, np. 00:00:00:00:00:01. *vid:* Określ istniejącą sieć VLAN, w której pakiety z określonym adresem MAC będą odrzucane.
Krok 3	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy filtrowania.

Poniższy przykład przedstawia dodawanie adresu filtrowania MAC 00:1e:4b:04:01:5d do VLAN 10. Przy tym ustawieniu przełącznik będzie odrzucał pakiet odbierany w sieci VLAN 10 z tym adresem jako źródłowym lub docelowym.

Switch#configure

Switch(config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 10

Switch(config)#show mac address-table filtering

MAC Address Table

MAC	VLAN	Port	Type	Aging
---	------	----	----	-----
00:1e:4b:04:01:5d	10		filter	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

Część 6

Konfiguracja 802.1Q VLAN

ROZDZIAŁY

1 Konfiguracja 802.1Q VLAN

Aby przeprowadzić konfigurację 802.1Q VLAN, wykonaj poniższe kroki:

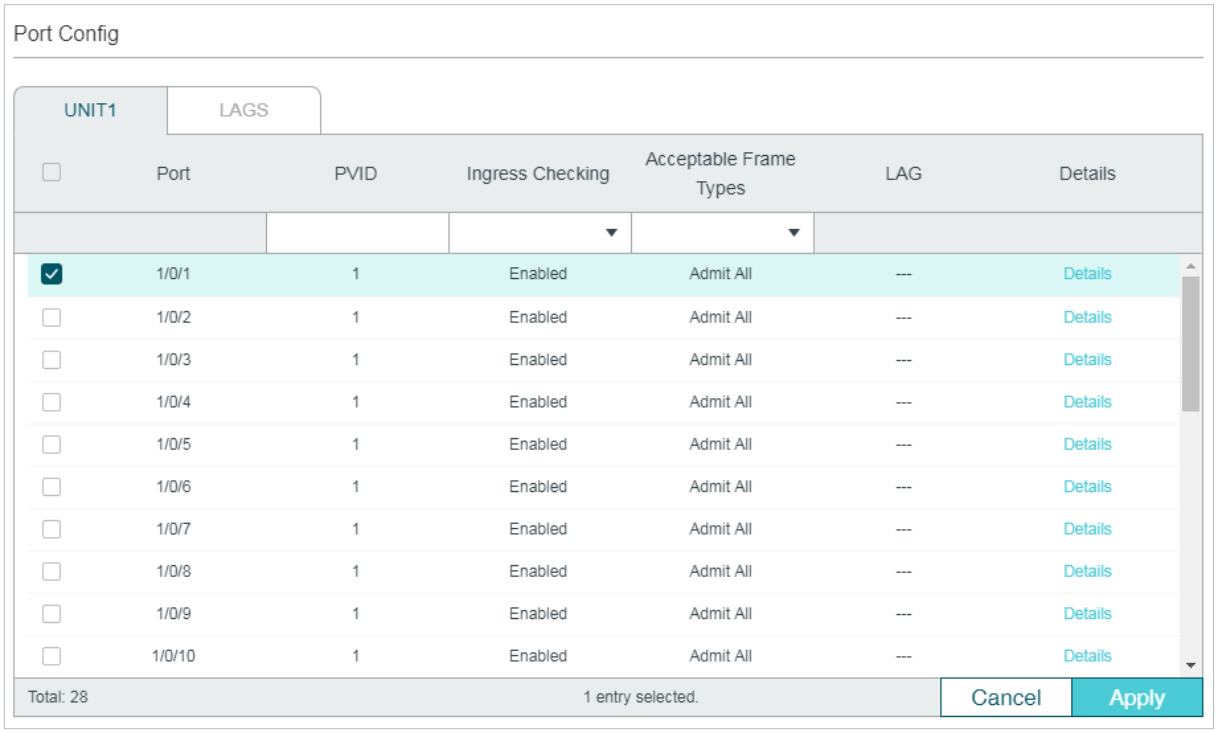
1) Skonfiguruj parametry portu;
2) Skonfiguruj sieć VLAN - utwórz sieć VLAN i dodaj do sieci skonfigurowane porty.

1.1 Przez GUI

1.1.1 Konfiguracja PVID portów

Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę.

Rys. 1-1 Konfiguracja portów



Wybierz port i skonfiguruj jego parametry. Kliknij **Apply**.

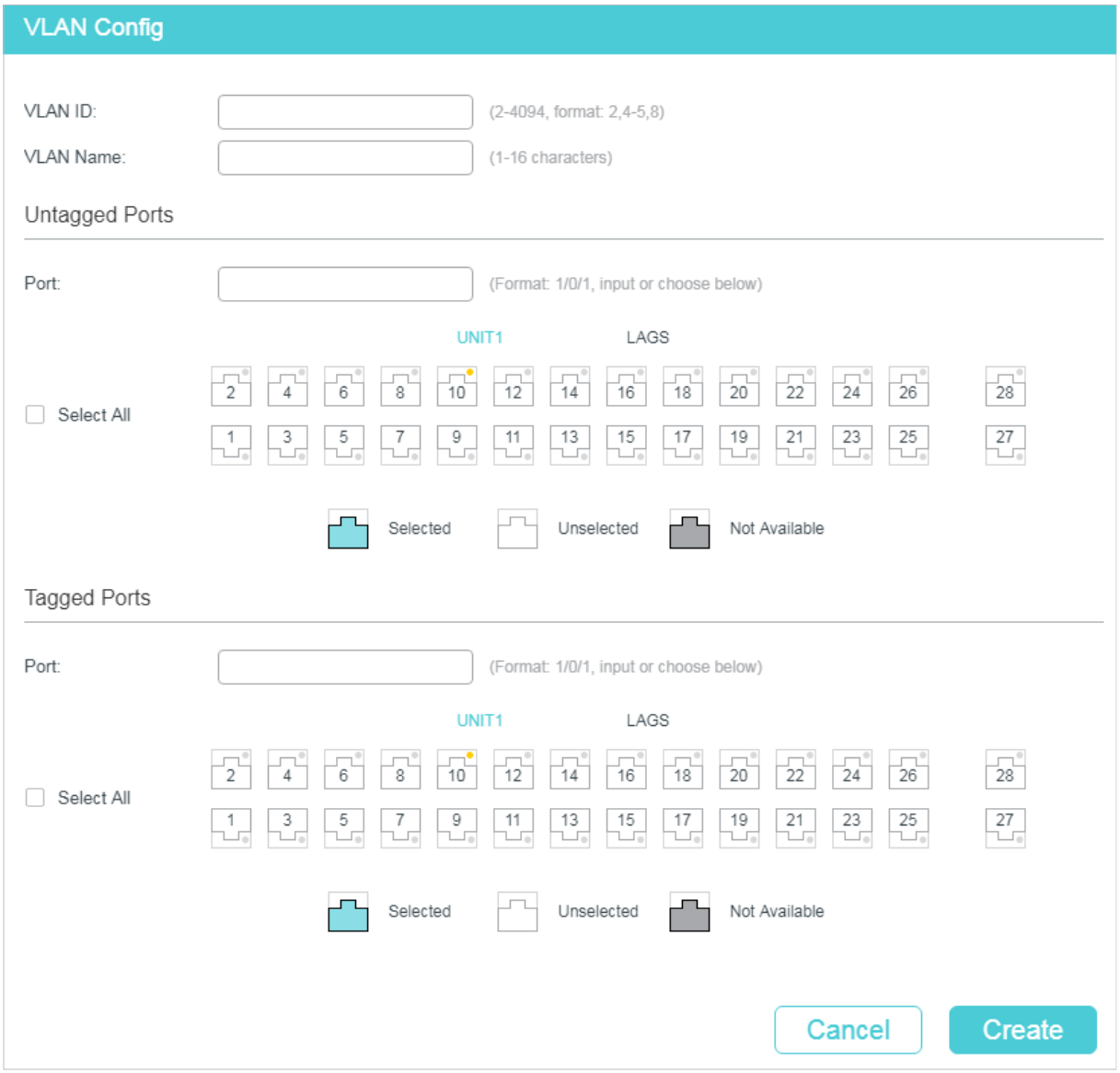
PVID	Ustaw domyślny VLAN ID portu. Prawidłowe wartości wahają się od 1 do 4094. Gdy port odbiera pakiet nietagowany, przełącznik oznacza pakiet tagiem VLAN w oparciu o PVID.
Ingress Checking	Kontrola na wejściu. Jeżeli włączysz tę funkcję, port będzie przyjmować tylko te pakiety, których VLAN ID znajdują się na liście VLAN portu, a inne będzie odrzucać. Jeżeli wyłączysz tę funkcję, port będzie przesyłać wszystkie pakiety.

Acceptable Frame Types	Wybierz dopuszczalny typ ramki dla portu, a port będzie przeprowadzać to działanie przed uruchomieniem kontroli na wejściu. **Admit All:** Port będzie przyjmować zarówno pakiety tagowane, jak i nietagowane. **Tagged Only:** Port będzie przyjmować tylko pakiety tagowane.
LAG	LAG (Link Aggregation Group), do której należy port.
Details	Kliknij przycisk Details, aby zobaczyć sieci VLAN, do których należy port.

1.1.2 Konfiguracja VLAN

Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 1-2 Konfiguracja VLAN



Wykonaj poniższe kroki, aby skonfigurować sieć VLAN:

1) Uzupełnij VLAN ID i opis identyfikacyjny, aby stworzyć sieć VLAN.

VLAN ID	Uzupełnij identyfikacyjny VLAN ID wartością z przedziału 2 - 4094.
VLAN Name	Uzupełnij opis identyfikacyjny sieci VLAN, wprowadzając do 16 znaków.

2) Wybierz odpowiednio port(y) tagowany(e) i port(y) nietagowany(e), aby dodać je do utworzonej sieci VLAN, w oparciu o topologię sieci.

Untagged port	Wybrane porty będą przesyłać pakiety nietagowane w docelowej sieci VLAN.
Tagged port	Wybrane porty będą przesyłać pakiety tagowane w docelowej sieci VLAN.

3) Kliknij **Apply**.

1.2 Przez CLI

1.2.1 Tworzenie sieci VLAN

Wykonaj poniższe kroki, aby utworzyć sieć VLAN:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**vlan** *vlan-list* Gdy wpisujesz nowy VLAN ID, przełącznik tworzy nową sieć VLAN i uruchamia tryb konfiguracji VLAN. Gdy wpisujesz istniejący VLAN ID, przełącznik bezpośrednio uruchamia tryb konfiguracji VLAN. *vlan-list*: Podaj ID lub ułóż listę ID sieci VLAN do konfiguracji. Prawidłowe wartości wahają się od 2 do 4094, np. 2-3,5.
Krok 3	**name** *descript* (Opcjonalnie) Uzupełnij identyfikacyjny opis VLAN. *descript*: Długość opisu musi mieścić się w zakresie 1 - 16 znaków.
Krok 4	**show vlan** [id *vlan-list*] Wyświetl globalne informacje określonych sieci VLAN. Jeżeli nie określisz żadnych sieci VLAN, polecenie wyświetli globalne informacje o wszystkich sieciach 802.1Q VLAN. *vlan-list*: Podaj ID lub ułóż listę ID sieci VLAN do konfiguracji. Prawidłowe wartości wahają się od 1 do 4094.
Krok 5	**end** Powórć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób utworzenia sieci VLAN 2 o nazwie RD :

Switch#configure

Switch(config)#vlan 2

Switch(config-vlan)#name RD

Switch(config-vlan)#show vlan id 2

VLAN	Name	Status	Ports
2	RD	active	

Switch(config-vlan)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja portu

Wykonaj poniższe kroki, aby skonfigurować port:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**switchport pvid** *vlan-id* Skonfiguruj PVID portu(ów). Domyślną wartością jest 1. *vlan-id*: Domyślny VLAN ID portu o wartości z zakresu 1 - 4094.
Krok 4	**switchport check ingress** Kontrola na wejściu. Jeżeli włączysz tę funkcję, port będzie przyjmować tylko te pakiety, których VLAN ID znajdują się na liście VLAN portu, a inne będzie odrzucać. Jeżeli wyłączysz tę funkcję, port będzie przesyłać wszystkie pakiety.
Krok 5	**switchport acceptable frame {**all **|** tagged**}** Wybierz dopuszczalny typ ramki dla portu, a port będzie przeprowadzać to działanie przed uruchomieniem kontroli na wejściu. all: Port będzie przyjmować zarówno pakiety tagowane, jak i nietagowane. tagged: Port będzie przyjmować tylko pakiety tagowane.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji PVID portu 1/0/5 jako 2, włączania kontroli na wejściu i ustawiania odpowiedniego typu ramki jako all:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#switchport pvid 2

Switch(config-if)#switchport check ingress

Switch(config-if)#switchport acceptable frame all

Switch(config-if)#show interface switchport gigabitEthernet 1/0/5

Port Gi1/0/5:

PVID: 2

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

Vlan	Name	Egress-rule
----	----------	----------
1	System-VLAN	Untagged

Switch(config-if)#end

Switch#copy running-config startup-config

1.2.3 Dodawanie portu do określonej sieci VLAN

Wykonaj poniższe kroki, aby dodać port do określonej sieci VLAN:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.

Krok 3	**switchport general allowed vlan** *vlan-list* **{** tagged **|** untagged **}** Dodaj porty do określonej sieci VLAN. *vlan-list:* Podaj ID lub ułóż listę ID sieci VLAN, do których porty będą dodawane. Wartość ID waha się od 1 do 4094. tagged **|** untagged: Wybierz regułę wyjścia dla portu.
Krok 4	**show interface switchport [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *lag-id***]** Zweryfikuj informacje o porcie.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób dodawania portu 1/0/5 do sieci VLAN 2, i określania jego reguły wyjścia jako tagowanej:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#switchport general allowed vlan 2 tagged

Switch(config-if)#show interface switchport gigabitEthernet 1/0/5

Port Gi1/0/5:

PVID: 2

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

Vlan	Name	Egress-rule
----	----------	----------
1	System-VLAN	Untagged
2	RD	Tagged

Switch(config-if)#end

Switch#copy running-config startup-config

Część 7

Konfiguracja MAC VLAN

ROZDZIAŁY

1 Konfiguracja MAC VLAN

Aby przeprowadzić konfigurację MAC VLAN, postępuj zgodnie z poniższymi krokami:

1) Skonfiguruj VLAN 802.1Q.
2) Powiąż adres MAC z VLAN.
3) Włącz MAC VLAN dla portu.

Wskazówki dotyczące konfiguracji

Kiedy port w MAC VLAN odbiera nieotagowany pakiet danych przełącznik sprawdza najpierw, czy źródłowy adres MAC pakietu danych został powiązany z MAC VLAN. Jeżeli tak, przełącznik wprowadzi odpowiadający tag do pakietu danych i przekieruje go w obrębie VLAN. Jeżeli nie, przełącznik będzie kontynuował dopasowywanie pakietu danych do reguł innych sieci VLAN (jak np. protokół VLAN). Jeżeli odnajdzie dopasowanie, przełącznik przekieruje pakiet danych. W odwrotnym przypadku, przełącznik przetworzy pakiet danych zgodnie z regułą procesowania VLAN 802.1 Q. Jeżeli port odbiera otagowany pakiet danych, przełącznik bezpośrednio procesuje pakiet danych zgodnie z regułą procesowania VLAN 802.1 Q VLAN.

1.1 Przez GUI

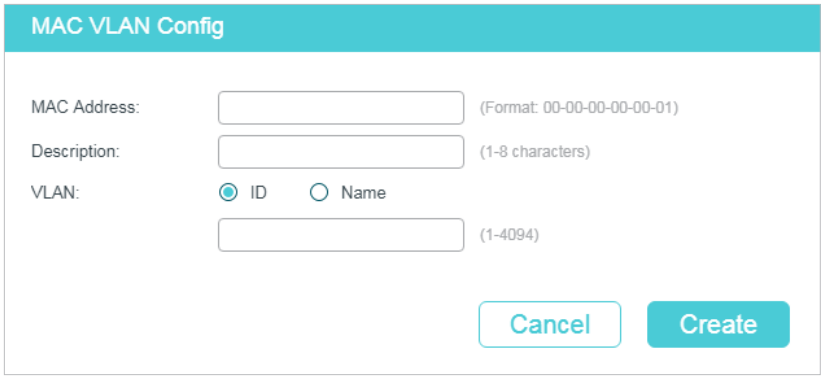
1.1.1 Konfiguracja VLAN 802.1Q

Przed konfiguracją MAC VLAN utwórz VLAN 802.1Q i ustaw typ portu zgodnie z wymaganiami sieciowymi. Więcej informacji znajdziesz w części *Konfiguracja 802.1Q VLAN*.

1.1.2 Wiązanie adresu MAC z VLAN

Wybierz menu **L2 FEATURES > VLAN > MAC VLAN** i kliknij Add, aby załadować następującą stronę.

Rys. 1-1 Tworzenie MAC VLAN



Aby powiązać adres MAC z VLAN 802.1Q, postępuj zgodnie z poniższymi krokami:

1) Wprowadź adres MAC urządzenia, dodaj opis i wprowadź VLAN ID, aby powiązać go z siecią VLAN.

MAC Address	Wprowadź adres MAC urządzenia w formacie 00-00-00-00-00-01.
Description	Dodaj opis adresu MAC, maks. 8 znaków.
VLAN ID/Name	Wprowadź numer ID lub nazwę VLAN 802.1Q VLAN, która zostanie powiązana z MAC VLAN.

2) Kliknij **Create**.

Uwaga:

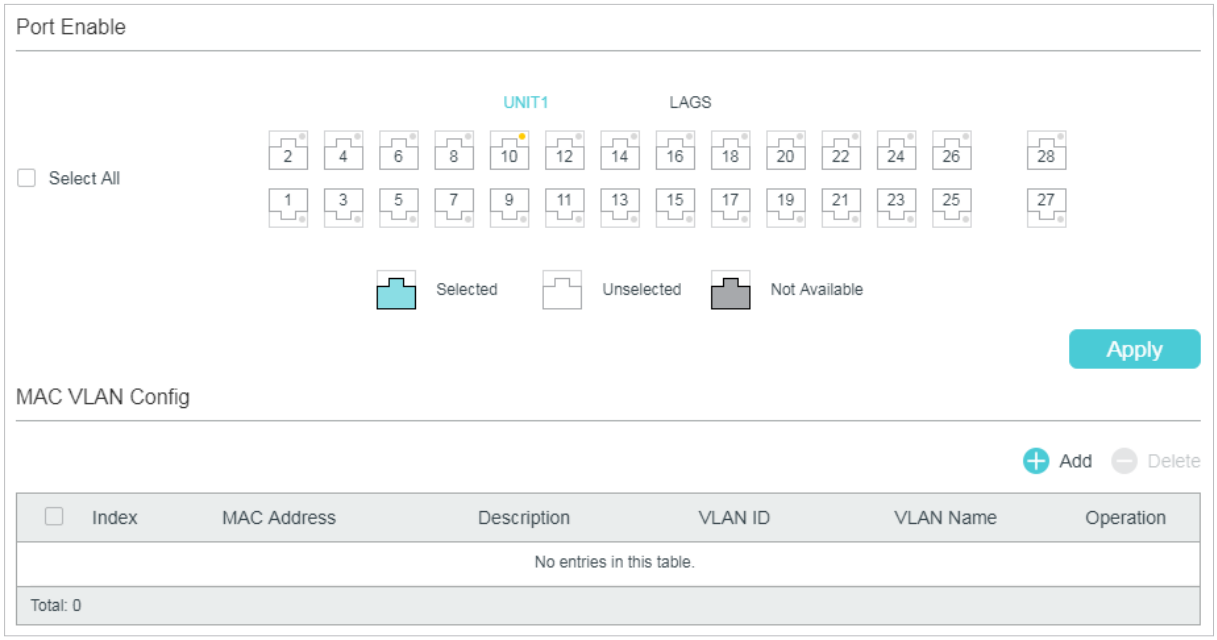
Jeden adres MAC może zostać powiązany tylko z jedną siecią VLAN.

1.1.3 Włączanie MAC VLAN dla portu

Domyślnie MAC VLAN jest wyłączony na wszystkich portach. Dla wybranych portów należy włączyć MAC VLAN ręcznie.

Wybierz menu **L2 FEATURES > VLAN > MAC VLAN, aby załadować następującą stronę**.

Rys. 1-2 Włączanie MAC VLAN dla portu



W sekcji **Port Enable** wybierz porty, dla których włączony będzie MAC VLAN i kliknij **Apply**.

Uwaga:

Port należący do grupy LAG (Link Aggregation Group) poddany jest konfiguracji LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

1.2 Przez CLI

1.2.1 Konfiguracja VLAN 802.1Q

Przed konfiguracją MAC VLAN utwórz VLAN 802.1Q i ustaw typ portu zgodnie z wymaganiami sieciowymi. Więcej informacji znajdziesz w części *Konfiguracja 802.1Q VLAN*.

1.2.2 Wiązanie adresu MAC z VLAN

Aby powiązać adres MAC z VLAN, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej..
Krok 2	**mac-vlan mac-address** *mac-addr* **vlan** *vlan-id* **[description** *descript***]** Powiąż adres MAC i VLAN. *mac-addr*: Określ adres MAC urządzenia w formacie xx:xx:xx:xx:xx:xx. *vlan-id*: Wprowadź numer ID VLAN 802.1Q, który zostanie powiązany z MAC VLAN. *descript*: Dodaj opis adresu MAC, maks. 8 znaków.
Krok 3	**show mac-vlan { all | mac-address** *mac-addr* **| vlan** *vlan-id* **}** Sprawdź konfigurację MAC VLAN. *vid*: Określ, który MAC VLAN ma być wyświetlony.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje wiązanie adresu MAC 00:19:56:8A:4C:71 i VLAN 10. Opis adresu to Dept.A.

Switch#configure

Switch(config)#mac-vlan mac-address 00:19:56:8a:4c:71 **vlan** 10 **description** Dept.A

Switch(config)#show mac-vlan vlan 10

MAC-Addr	Name	VLAN-ID
00:19:56:8A:4C:71	Dept.A	10

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Włączanie MAC VLAN dla portu

Aby włączyć MAC VLAN dla portu, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**mac-vlan** Włącz MAC VLAN dla portu.
Krok 4	**show mac-vlan interface** Sprawdź konfigurację MAC VLAN na interfejsie.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie MAC VLAN dla portu 1/0/1.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#mac-vlan

Switch(config-if)#show mac-vlan interface

Port STATUS

------- -----------

Gi1/0/1 Enable

Gi1/0/2 Disable

...

Switch(config-if)#end

Switch#copy running-config startup-config

Część 8

Konfiguracja protokołu VLAN

ROZDZIAŁY

1 Konfiguracja protokołu VLAN

Aby przeprowadzić konfigurację protokołu VLAN, wykonaj poniższe kroki:

1) Skonfiguruj 802.1Q VLAN.
2) Utwórz szablon protokołu.
3) Skonfiguruj protokół VLAN.

Wskazówki dotyczące konfiguracji

- Możesz skorzystać z szablonów protokołu IP, ARP, RARP lub innych oferowanych przez przełączniki TP-Link lub utworzyć nowe szablony protokołu.

- W przypadku protokołu VLAN, gdy port otrzymuje nietagowany pakiet danych, przełącznik wyszukuje najpierw protokołu VLAN zgodnego z typem protokołu pakietu. Jeżeli pojawi się dopasowanie, przełącznik opatrzy pakiet danych odpowiednim tagiem VLAN i prześle go w ramach sieci VLAN. W innym wypadku, przełącznik prześle pakiet danych do domyślnej sieci VLAN, w oparciu o PVID (VLAN ID) portu odbierającego. (Jeżeli adres MAC sieci VLAN także został skonfigurowany, przełącznik najpierw przetworzy protokół VLAN, a następnie MAC VLAN.) Gdy port otrzymuje otagowany pakiet danych, przełącznik bezpośrednio przetwarza pakiet danych, zgodnie z regułą przetwarzania 802.1 Q VLAN.

1.1 Przez GUI

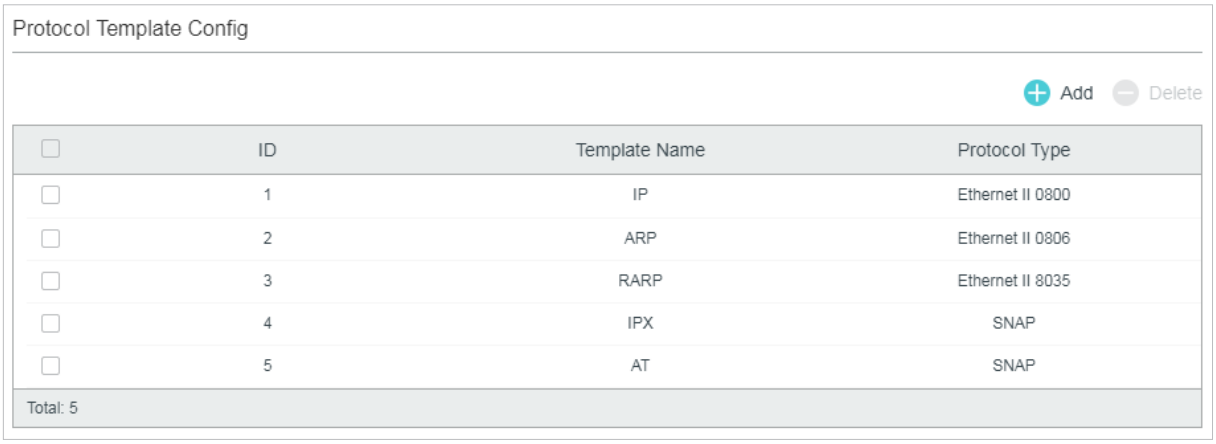
1.1.1 Konfiguracja 802.1Q VLAN

Przed konfiguracją protokołu VLAN, utwórz sieć 802.1Q VLAN ustaw typ portu zgodnie z wymaganiami środowiska sieciowego. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

1.1.2 Tworzenie szablonów protokołu

Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol Template**, aby wyświetlić poniższą stronę.

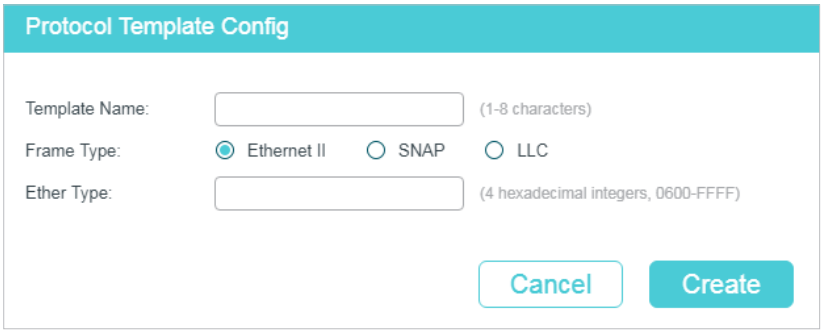
Rys. 1-1 Przeglądanie szablonów protokołu



Wykonaj poniższe kroki, aby utworzyć szablon protokołu:

1) Sprawdź czy pożądany szablony nie istnieje już w sekcji **Protocol Template Config**. Jeżeli nie istnieje, kliknij Add, aby stworzyć nowy szablon.

Rys. 1-2 Tworzenie szablonu protokołu



Template Name	Nadaj nazwę szablonowi, aby łatwo go zidentyfikować.
Frame Type	Wybierz typ ramki nowego szablonu protokołu. **Ethernet II:** Typowy format ramki sieci Ethernet. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType. **SNAP:** Format ramki sieci Ethernet 802.3 oparty o standard IEEE 802.3 i IEEE 802.2 SNAP. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType. **LLC:** Format ramki sieci Ethernet 802.3 oparty o standard IEEE 802.3 i IEEE 802.2 LLC. Po wybraniu opcji określ typ ramki poprzez wpisanie DSAP i SSAP.
Ether Type	Uzupełnij typ protokołu Ethernet dla szablonu protokołu. Opcja jest dostępna przy wyborze **Ethernet II** i **SNAP**. Wpisanie EtherType służy identyfikacji typu danych ramki.

DSAP	Uzupełnij wartość DSAP dla szablonu protokołu. Opcja jest dostępna przy wyborze **LLC**. Wpisanie DSAP służy identyfikacji typu danych ramki.
SSAP	Uzupełnij wartość SSAP dla szablonu protokołu. Opcja jest dostępna przy wyborze **LLC**. Wpisanie SSAP służy identyfikacji typu danych ramki.

2) Kliknij **Create**.

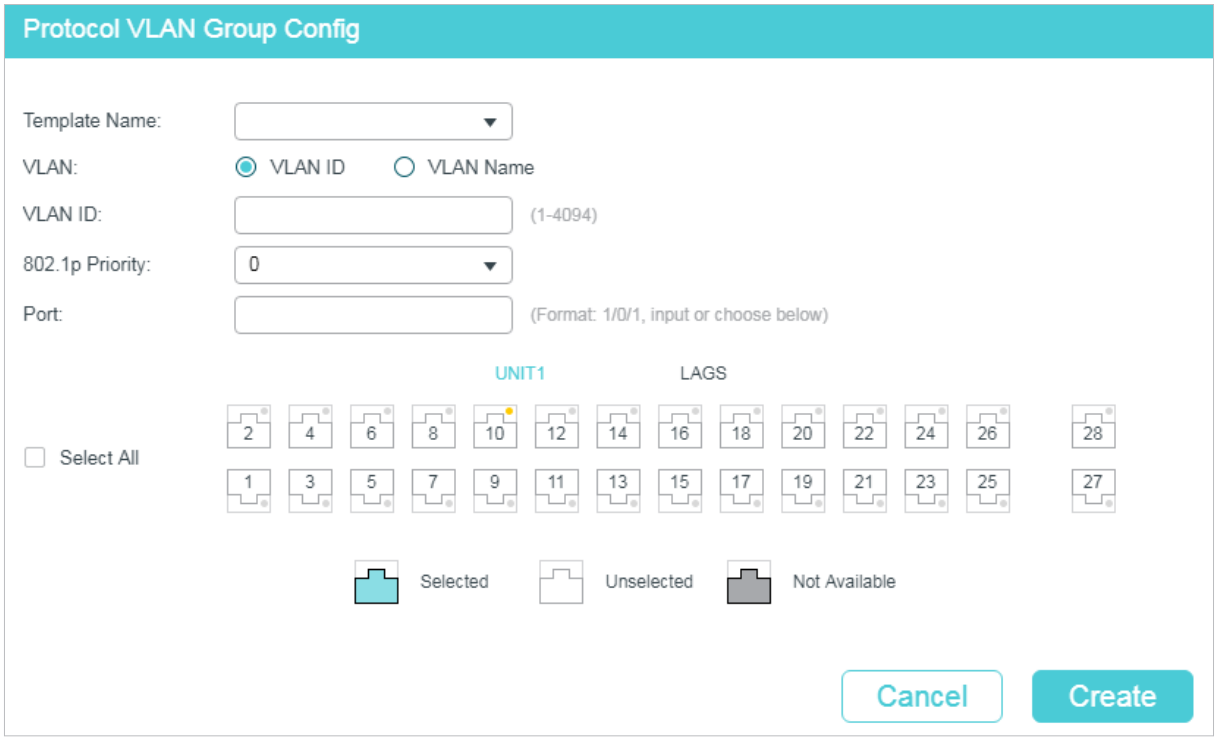
Uwaga:

Szablon protokołu powiązany z siecią VLAN nie może być usunięty.

1.1.3 Konfiguracja protokołu VLAN

Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol VLAN Group** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 1-3 Konfiguracja grupy protokołu VLAN



Wykonaj poniższe kroki, aby skonfigurować grupę protokołu:

1) W sekcji **Protocol Group Config** określ następujące parametry.

Template Name	Wybierz wcześniej zdefiniowany szablon protokołu.
VLAN ID/Name	Podaj numer ID lub nazwę sieci 802.1Q VLAN, która będzie powiązana z protokołem VLAN.
802.1p Priority	Określ priorytet 802.1p dla pakietów należących do protokołu VLAN. Przełącznik określi sekwencję przesyłania zgodnie z tą wartością. Pakiety o wyższej wartości priorytetu 802.1p są uznawane za pakiety o wyższym priorytecie.

2) Wybierz porty. Kliknij **Create**.

Uwaga:

Port LAG (Link Aggregation Group) działa według konfiguracji LAG, a nie konfiguracji własnej. Konfiguracji portu obowiązuje jedynie po opuszczeniu LAG.

1.2 Przez CLI

1.2.1 Konfiguracja 802.1Q VLAN

Przed skonfigurowaniem protokołu VLAN, utwórz sieć 802.1Q VLAN i ustaw typ portu, zgodnie z wymaganiami środowiska sieciowego. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

1.2.2 Tworzenie szablonu protokołu

Wykonaj poniższe kroki, aby utworzyć szablon protokołu:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**protocol-vlan template name** *protocol-name* **frame { ether_2 ether-type** *type* **| snap ether-type** *type* **| llc dsap** *dsap_type* **ssap** *ssap_type* **}** Utwórz szablon protokołu. *protocol-name:* Uzupełnij nazwę protokołu, wprowadzając od 1 do 8 znaków. *type*: Wpisz 4 liczby systemu szesnastkowego jako typ protokołu Ethernet dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType. *dsap_type*: Wpisz 2 liczby systemu szesnastkowego jako wartość DSAP dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie DSAP. *ssap_type*: Wpisz 2 liczby systemu szesnastkowego jako wartość SSAP dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie SSAP.
Krok 3	**show protocol-vlan template** Zweryfikuj szablony protokołu.
Krok 4	**end** Powróć do trybu uprzywilejowanego (Privileged EXEC Mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia szablonu protokołu IPv6:

Switch#configure

Switch(config)#protocol-vlan template name IPv6 **frame ether_2 ether-type** 86dd

Switch(config)#show protocol-vlan template

Index	Protocol Name	Protocol Type
1	IP	EthernetII ether-type 0800
2	ARP	EthernetII ether-type 0806
3	RARP	EthernetII ether-type 8035
4	IPX	SNAP ether-type 8137
5	AT	SNAP ether-type 809B
6	IPv6	EthernetII ether-type 86DD

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Konfiguracja protokołu VLAN

Wykonaj poniższe kroki, aby skonfigurować protokół VLAN:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**show protocol-vlan template** Sprawdź indeks każdego szablonu protokołu.
Krok 3	**protocol-vlan vlan** *vid* **priority** *priority* **template** *index* Powiąż szablon protokołu z siecią VLAN. *vid* : Podaj numer ID sieci 802.1Q VLAN, który ma być powiązany z protokołem VLAN. *priority* : Określ priorytet 802.1p dla pakietów należących do protokołu VLAN. Przełącznik określi sekwencję przesyłania zgodnie z tą wartością. Pakiety o wyższej wartości priorytetu 802.1p są uznawane za pakiety o wyższym priorytecie. *index* : Uzupełnij indeks szablonu protokołu.
Krok 4	**show protocol-vlan vlan** Sprawdź indeksy protokołu VLAN (entry-id) wszystkich grup protokołu.
Krok 5	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.

Krok 6	**protocol-vlan group** *entry-id* Dodaj określony port do grupy protokołu. *entry-id:* Indeks protokołu VLAN.
Krok 7	**end** Powróć do trybu uprzywilejowanego (Privileged EXEC Mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania szablonu protokołu IPv6 jako VLAN 10 i dodawania portu 1/0/2 do protokołu VLAN:

Switch#configure

Switch(config)#show protocol-vlan template

Index	Protocol Name	Protocol Type
1	IP	EthernetII ether-type 0800
2	ARP	EthernetII ether-type 0806
3	RARP	EthernetII ether-type 8035
4	IPX	SNAP ether-type 8137
5	AT	SNAP ether-type 809B
6	IPv6	EthernetII ether-type 86DD

Switch(config)#protocol-vlan vlan 10 **priority** 5 **template** 6

Switch(config)#show protocol-vlan vlan

Index	Protocol-Name	VID	Priority	Member
1	IPv6	10	0	

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#protocol-vlan group 1

Switch(config-if)#show protocol-vlan vlan

Index	Protocol-Name	VID	Priority	Member
1	IPv6	10	5	Gi1/0/2

Switch(config-if)#end

Switch#copy running-config startup-config

Część 9

Konfiguracja GVRP

ROZDZIAŁY

1 Konfiguracja GVRP

Aby przeprowadzić konfigurację GVRP, postępuj zgodnie z poniższymi krokami.

1) Utwórz VLAN.
2) Włącz GVRP globalnie.
3) Włącz GVRP na każdym porcie i skonfiguruj odpowiednie parametry.

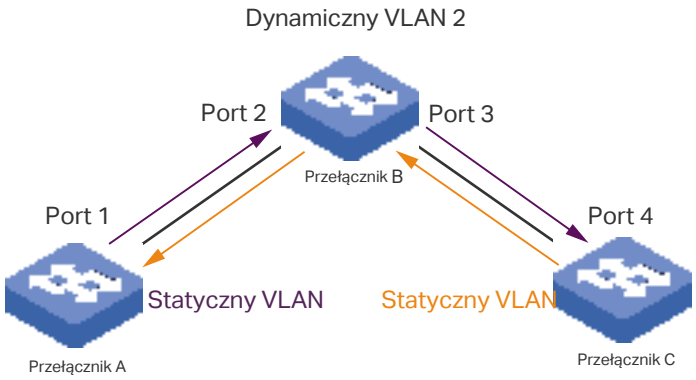
Wskazówki dotyczące konfiguracji

Aby dynamicznie utworzyć VLAN na wszystkich portach na łączu sieci, należy ustawić ten sam statyczny VLAN po obu stronach łącza.

Ręcznie skonfigurowany VLAN 802.1Q nazywany jest statycznym, a VLAN utworzony przez GVRP to dynamiczny VLAN. Porty w statycznej sieci VLAN mogą inicjować wysyłanie komunikatu rejestracyjnego GVRP do innych portów. Port rejestruje sieci VLAN tylko po otrzymaniu komunikatu GVRP. Jako że komunikaty mogą być wysyłane tylko między dwoma podmiotami GVRP, do konfiguracji sieci VLAN na wszystkich portach łącza wymagana jest rejestracja dwustronna. Aby przeprowadzić rejestrację dwustronną należy ręcznie skonfigurować ten sam statyczny VLAN po obu stronach łącza.

Jak pokazano na poniższym rysunku, rejestracja VLAN z Przełącznika A do Przełącznika C skutkuje dodaniem Portu 2 do VLAN 2. Rejestracja VLAN z Przełącznika C do Przełącznika A skutkuje dodaniem Portu 3 do VLAN 2.

Rys. 1-1

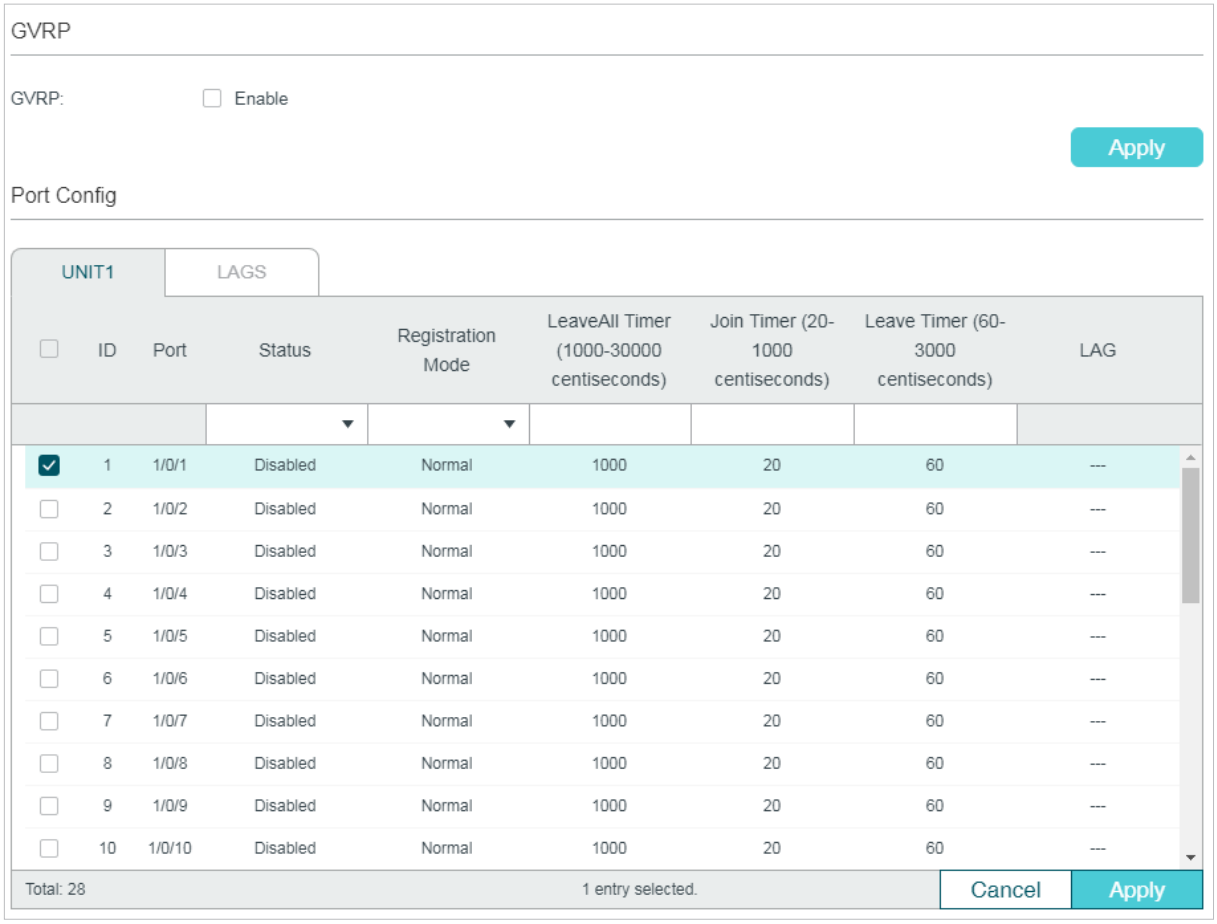


Analogicznie, aby usunąć z łącza VLAN, wymagane jest dwustronne wyrejestrowanie. Należy ręcznie usunąć statyczny VLAN po obu stronach łącza.

1.1 Przez GUI

Wybierz menu **L2 FEATURES > VLAN > GVRP > GVRP Config**, aby załadować następującą stronę.

Rys. 1-2 Konfiguracja GVRP



Aby skonfigurować GVRP, postępuj zgodnie z poniższymi krokami:

1) W sekcji **GVRP**, włącz GVRP globalnie i kliknij **Apply**.
2) W sekcji **Port Config** wybierz co najmniej jeden port, ustaw stan jako Enable i odpowiednio skonfiguruj powiązane parametry.

Port	Wybierz port do konfiguracji GVRP. Możesz zaznaczyć więcej niż jeden port.
Status	Włącz lub wyłącz GVRP na porcie. Opcja jest domyślnie wyłączona.

Registration Mode	Wybierz tryb rejestracji GVRP dla portu. **Normal**: W tym trybie port może dynamicznie rejestrować i wyrejestrowywać sieci VLAN oraz przekazywać dane rejestracyjne dynamicznych i statycznych sieci VLAN. **Fixed**: W tym trybie port nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane rejestracyjne tylko statycznych sieci VLAN. **Forbidden**: W tym trybie nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane tylko VLAN 1.
LeaveAll Timer (centisecond)	Po włączeniu podmiotu GARP, włączony zostanie licznik LeaveAll. Po wygaśnięciu czasu LeaveAll podmiot GARP wyśle komunikaty LeaveAll do pozostałych podmiotów GARP, żeby te ponownie zarejestrowały wszystkie informacje o jego atrybutach. Po wszystkim podmiot restartuje licznik LeaveAll. Parametr czasowy licznika wynosi od 1000 do 30000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 1000 setnych sekundy.
Join Timer (centisecond)	Licznik Join kontroluje wysyłanie komunikatów Join. Podmiot GVRP włącza licznik Join po wysłaniu pierwszego komunikatu Join. Jeżeli podmiot nie otrzyma żadnej odpowiedzi, po wygaśnięciu czasu Join wyśle drugi komunikat, aby upewnić się, że komunikat Join może być wysłany do pozostałych podmiotów. Parametr czasowy licznika wynosi od 20 do 1000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 20 setnych sekundy.
Leave Timer (centisecond)	Licznik Leave kontroluje wyrejestrowywanie atrybutów. Podmiot wyśle komunikat Leave, jeżeli będzie wymagał od innych podmiotów wyrejestrowania części jego atrybutów. Po otrzymaniu komunikatu przez podmiot włączony zostaje licznik Leave. Jeżeli podmiot nie dostanie żadnego komunikatu Join dla odpowiadającego atrybutu przed wygaśnięciem czasu Leave, podmiot wyrejestrowuje atrybut. Parametr czasowy licznika wynosi od 60 do 3000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 60 setnych sekundy.
LAG	Wyświetl grupę LAG do której należy port.

3) Kliknij **Apply**.

Uwaga:

- Port należący do grupy LAG konfigurowany jest z grupą, nie oddzielnie. Konfiguracja portu może być przeprowadzona dopiero, gdy port opuści grupę LAG.
- Reguła wyjścia portów dodanych dynamicznie do sieci VLAN jest tagowana.
- Reguła wyjścia portów stałych powinna być tagowana.
- Ustawiając parametry czasowe licznika upewnij się, że wartości mieszczą się w wymaganym zakresie. Wartość LeaveAll powinna być większa niż dziesięciokrotność wartości Leave lub równa z nią. Wartość Leave powinna być większa niż dwukrotność wartości Join lub równa z nią.

1.2 Przez CLI

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**gvrp** Włącz GVRP globalnie.
Krok 3	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.
Krok 4	**gvrp** Włącz GVRP na porcie.
Krok 5	**gvrp registration** { normal | fixed | forbidden } Skonfiguruj tryb rejestracji GVRP dla portu. Domyślnie ustawiony jest tryb Normal. normal: W tym trybie port może dynamicznie rejestrować i wyrejestrowywać sieci VLAN oraz przekazywać dane rejestracyjne dynamicznych i statycznych sieci VLAN. fixed (stały): W tym trybie port nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane rejestracyjne tylko statycznych sieci VLAN. forbidden (zabroniony): W tym trybie nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane tylko VLAN 1.
Krok 6	**gvrp timer** { leaveall | join | leave } *value* Ustaw odpowiednio liczniki GARP. leaveall: Po włączeniu podmiotu GARP, włączony zostanie licznik LeaveAll. Po wygaśnięciu czasu LeaveAll podmiot GARP wyśle komunikaty LeaveAll do pozostałych podmiotów GARP, żeby te ponownie zarejestrowały wszystkie informacje o jego atrybutach. Po wszystkim podmiot restartuje licznik LeaveAll. join: Licznik Join kontroluje wysyłanie komunikatów Join. Podmiot GVRP włącza licznik Join po wysłaniu pierwszego komunikatu Join. Jeżeli podmiot nie otrzyma żadnej odpowiedzi, wyśle drugi komunikat po wygaśnięciu czasu Join, aby upewnić się, że komunikat Join może być wysłany do pozostałych podmiotów. leave: Licznik Leave kontroluje wyrejestrowywanie atrybutów. Podmiot wyśle komunikat Leave, jeżeli będzie wymagał od innych podmiotów wyrejestrowania części jego atrybutów. Po otrzymaniu komunikatu przez podmiot włączony zostaje licznik Leave. Jeżeli podmiot nie dostanie żadnego komunikatu Join dla odpowiadającego atrybutu przed wygaśnięciem czasu Leave, podmiot wyrejestrowuje atrybut. *value*: Ustaw parametr czasowy licznika. Powinien być całkowitą wielokrotnością liczby 5. Dla licznika LeaveAll wartość powinna wynosić od 1000 do 30000 setnych sekundy, wartość domyślna to 1000. Dla licznika Join wartość powinna wynosić od 20 do 1000 setnych sekundy, wartość domyślna to 20. Dla licznika Leave wartość powinna wynosić od 60 do 3000 setnych sekundy, wartość domyślna to 60.

Krok 7	**show gvrp global** Sprawdź globalne ustawienia GVRP.
Krok 8	**show gvrp interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Sprawdź konfigurację GVRP wybranego portu lub LAG.
Krok 9	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Note:

- Port należący do grupy LAG konfigurowany jest z grupą, nie oddzielnie. Konfiguracja portu może być przeprowadzona dopiero, gdy port opuści grupę LAG.
- Reguła wyjścia portów dodanych dynamicznie do sieci VLAN jest tagowana.
- Reguła wyjścia portów stałych powinna być tagowana.
- Ustawiając parametry czasowe licznika upewnij się, że wartości mieszczą się w wymaganym zakresie. Wartość LeaveAll powinna być większa niż dziesięciokrotność wartości Leave lub równa z nią. Wartość Leave powinna być większa niż dwukrotność wartości Join lub równa z nią.

Poniższy przykład prezentuje włączanie GVRP globalnie i na porcie 1/0/1, konfigurację trybu rejestracji GVRP na stały i zachowanie wartości domyślnych liczników.

Switch#configure

Switch(config)#gvrp

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#gvrp

Switch(config-if)#gvrp registration fixed

Switch(config-if)#show gvrp global

GVRP Global Status

Enabled

Switch(config-if)# show gvrp interface gigabitEthernet 1/0/1

Port	Status	Reg-Mode	LeaveAll	JoinIn	Leave	LAG
----	------	--------	--------	------	-----	---
Gi1/0/1	Enabled	Fixed	1000	20	60	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

Część 10

Konfiguracja multicastu L2

ROZDZIAŁY

1 Multicast warstwy 2

1.1 Obsługiwane funkcje

Protokół multicastu warstwy 2 dla IPv4: IGMP Snooping

Na urządzeniach warstwy 2 IGMP Snooping sprawdza pakiety IGMP przesyłane przez sieć, przechwytując informacje. Potrafi pasywnie nasłuchiwać komunikatów IGMP i w ten sposób uczyć się grup multicastowych. Potem następuje automatyczna konfiguracja portów przełącznika lub VLAN-ów i w efekcie ruch multicastowy jest wysyłany wyłącznie na odpowiednie porty przełącznika

Protokół multicastu warstwy 2 dla IPv6: MLD Snooping

Na urządzeniach warstwy 2 MLD Snooping sprawdza pakiety MLD przesyłane przez sieć, przechwytując informacje. Potrafi pasywnie nasłuchiwać komunikatów MLD i w ten sposób uczyć się grup multicastowych. Potem następuje automatyczna konfiguracja portów przełącznika lub VLAN-ów i w efekcie ruch multicastowy jest wysyłany wyłącznie na odpowiednie porty przełącznika.

MVR (Multicast VLAN Registration)

Funkcja MVR umożliwia kierowanie ruchu multicastowego VLAN-u do portów multicastu należących do innych VLAN-ów protokołu IPv4. W przypadku IGMP Snooping, jeżeli porty należą do innych VLAN-ów, kopia strumienia multicastowego przesyłana jest do każdego VLAN-u, który ma przypisane porty. Natomiast MVR zapewnia VLAN dedykowany transmisji multicastowej w sieci warstwy 2, aby zapobiec powielaniu strumieni multicastowych skierowanych do klientów przynależących do różnych VLAN-ów. Klienci mogą dynamicznie dołączać do VLAN-u multicastowego, a także go opuszczać, bez ingerencji w swoje powiązania z innymi VLAN-ami.

Dostępne są dwa tryby MVR:

- Tryb kompatybilności

W trybie kompatybilności przełącznik MVR nie przesyła urządzeniu odpytującemu (IGMP querier) otrzymanych od przełącznika raportów oraz komunikatów leave, Zatem IGMP querier nie ma możliwości nauczenia się przynależności grup multicastowych od przełącznika MVR. Aby możliwe było przesłanie wszystkich wymaganych strumieni multicastowych do przełącznika MVR poprzez VLAN multicastowy, IGMP querier musi być skonfigurowany statycznie.

- Tryb dynamiczny

W trybie dynamicznym, po otrzymaniu od hostów raportu lub komunikatu leave, przełącznik MVR prześle te informacje do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). Zatem IGMP querier może nauczyć się przynależności grup

multicastowych poprzez raporty i komunikaty leave, a także może przesyłać strumienie multicastowe do przełącznika MVR poprzez VLAN multicastowy, zgodnie z tabelą przekierowań ruchu multicastowego.

Filtrowanie pakietów multicastu

Funkcja filtrowania pakietów multicastu umożliwia kontrolę grup multicastowych, do których host może przynależeć. Filtrowanie przyłączeń do grup multicastowych może odbywać się dla poszczególnych portów, poprzez konfigurację profili IP multicast (profili IGMP lub MLD), a następnie wiązanie ich z poszczególnymi portami przełącznika.

2 Konfiguracja IGMP Snooping

Aby przeprowadzić proces konfiguracji IGMP Snooping wykonaj poniższe kroki:

1) Uruchom IGMP Snooping globalnie i skonfiguruj parametry globalne.
2) Skonfiguruj IGMP Snooping dla VLAN-ów.
3) Skonfiguruj IGMP Snooping dla portów.
4) Skonfiguruj statyczne dołączanie hostów do grup (opcjonalnie).

Uwaga:

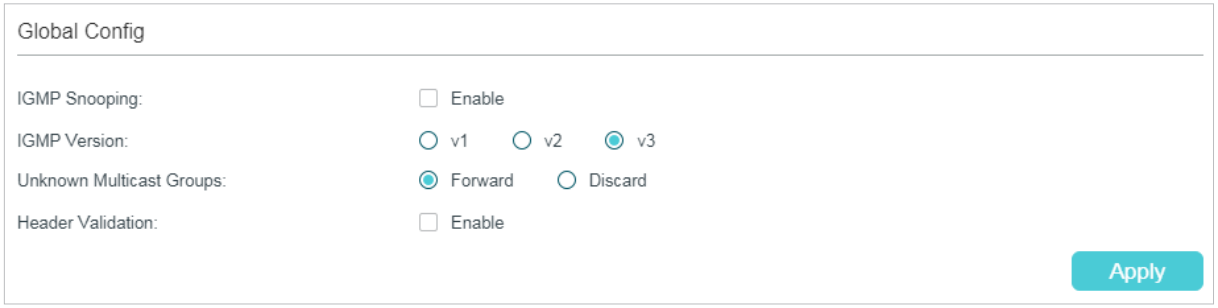
Funkcja IGMP Snooping działa wyłącznie przy uruchomieniu globalnym - dla VLAN-u oraz odpowiednich portów.

2.1 Przez GUI

2.1.1 Konfiguracja globalna IGMP Snooping

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config,** aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna IGMP Snooping



Wykonaj poniższe kroki, aby skonfigurować globalnie IGMP Snooping:

1) W sekcji **Global Config** uruchom globalnie IGMP Snooping i skonfiguruj parametry globalne.

IGMP Snooping	Uruchom lub wyłącz globalnie IGMP Snooping.

IGMP Version	Podaj wersję IGMP. **v1**: Przełącznik działa w trybie IGMPv1 Snooping. Może przetwarzać wyłącznie otrzymane od hosta komunikaty IGMPv1. Komunikaty innych wersji są ignorowane. **v2**: Przełącznik działa w trybie IGMPv2 Snooping. Może przetwarzać zarówno komunikaty IGMPv1, jak i IGMPv2, otrzymane od hosta. Komunikaty IGMPv3 są ignorowane. **v3**: Przełącznik działa w trybie IGMPv3 Snooping. Może przetwarzać otrzymane od hosta komunikaty wszystkich wersji: IGMPv1, IGMPv2 oraz IGMPv3.
Unknown Multicast Groups	Zdecyduj w jaki sposób przełącznik ma przetwarzać dane, które są przesyłane do nieznanych grup multicastowych , wybierając spośród “Forward” (przesyłaj) lub “Discard” (odrzuć). Domyślnym ustawieniem jest Forward. Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich w tabeli przekierowań ruchu multicastowego przełącznika. *Uwaga:* IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest przejście w tym samym czasie do strony **L2 FEATURES > Multicast > MLD Snooping > Global Config** i globalne uruchomienie funkcji MLD Snooping.
Header Validation	Włącz lub wyłącz Header Validation. Domyślnie opcja jest wyłączona. Dla pakietów IGMP wartością TTL powinno być 1, pola ToS 0xC0, a opcji Router Alert 0x94040000. Pola, które muszą być uzupełnione, zależą od wersji IGMP. IGMPv1 wymaga jedynie pola TTL. IGMPv2 wymaga pól TTL oraz Router Alert. IGMPv3 wymaga natomiast pól TTL, ToS oraz Router Alert. Pakiety, które nie przejdą pomyślnie procesu weryfikacji zostaną odrzucone.

2) Kliknij **Apply**.

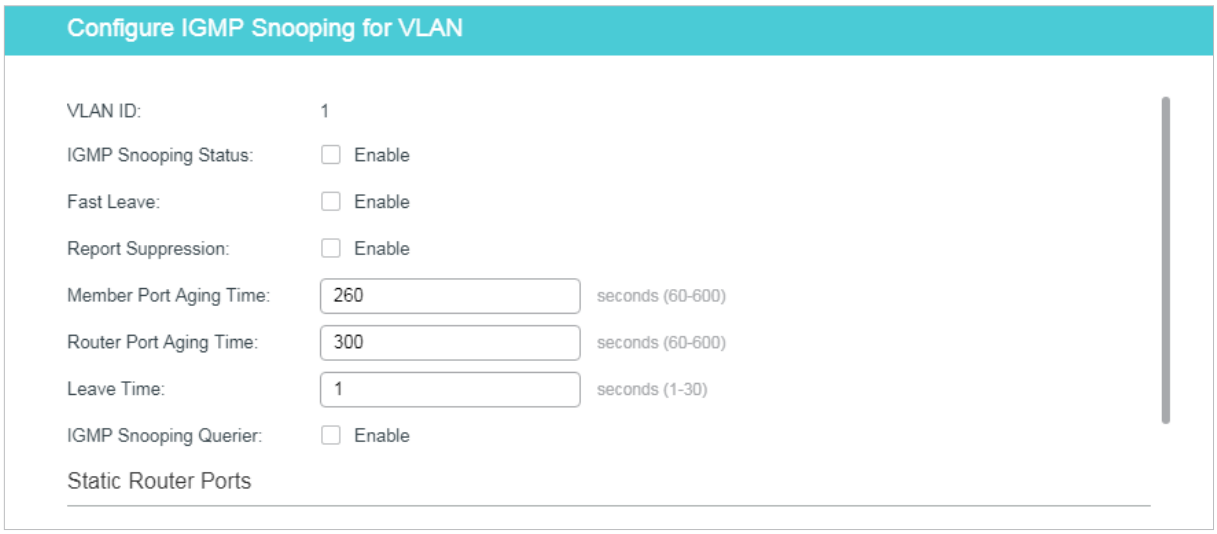
2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów

Przed konfiguracją IGMP Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację IGMP Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** i kliknij przy wybranej pozycji VLAN-u w sekcji **IGMP VLAN Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja IGMP Snooping dla VLAN-u



Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla określonych VLAN-ów:

1) Włącz IGMP Snooping dla VLAN-u i skonfiguruj odpowiednie parametry.

VLAN ID	Identyfikator VLAN-u.
IGMP Snooping Status	Włącz lub wyłącz IGMP Snooping dla VLAN-u.
Fast Leave	Włącz lub wyłącz funkcję szybkiego przełączania dla VLAN-u. IGMPv1 nie obsługuje Fast Leave. Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysyła komunikat leave IGMP, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier). Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu leave, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Member Query Count) dla określonych grup na tym porcie w ustalonym interwale czasowym (Last Member Query Interval), a następnie czeka na raporty dotyczące przynależności do grup IGMP. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na te zapytania prześlą przed wygaśnięciem Last Member Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej. Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysyła komunikat leave musi poczekać aż port z listy przekierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time). Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tabeli przekierowań ruchu multicastowego przed przekazaniem komunikatu leave do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat leave.

Report Suppression	Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-u. Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport IGMP dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do IGMP querier zdublowanych komunikatów.
Member Port Aging Time	Podaj czas utraty ważności portów przynależących do VLAN-u. Gdy przełącznik otrzymuje z portu raport IGMP, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi. Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów IGMP dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.
Router Port Aging Time	Podaj czas utraty ważności portów routera przynależących do VLAN-u. Gdy przełącznik otrzymuje z portu komunikat z zapytaniem IGMP, dodaje on ten porty do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera. Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem IGMP przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.
Leave Time	Podaj czas opuszczenia grupy dla VLAN-u. Gdy przelącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje: • Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time. • Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave. Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.
IGMP Snooping Querier	Włącz lub wyłącz funkcję IGMP Snooping Querier dla VLAN-u. Włączona funkcja oznacza, że przełącznik pełni rolę IGMP Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytujące cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów leave, rozsyła zapytania do grup. *Uwaga:* Aby możliwe było włączenie IGMP Snooping Querier dla VLAN-u, funkcja IGMP Snooping powinna być uruchomiona zarówno globalnie, jak i dla VLAN-u.

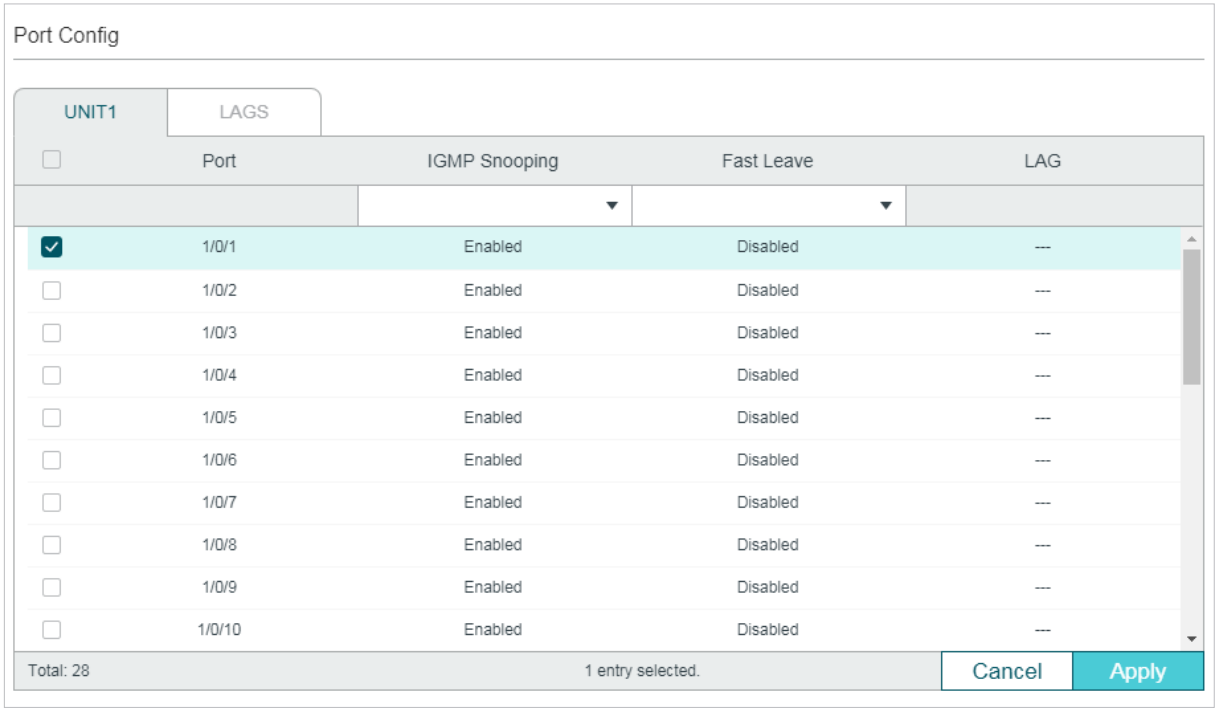
Query Interval	Gdy włączysz funkcję IGMP Snooping Querier, podaj interwał wysyłania przez przełącznik zapytań ogólnych.
Maximum Response Time	Gdy włączysz funkcję IGMP Snooping Querier, podaj maksymalny czas odpowiedzi hostów na zapytania ogólne.
Last Member Query Interval	Włączona funkcja IGMP Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat leave IGMP, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła określone zapytania bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty leave. Ten parametr jest wartością interwału pomiędzy zapytaniami przesyłanymi bezpośrednio do grup.
Last Member Query Count	Gdy włączysz funkcję IGMP Snooping Querier, podaj liczbę zapytań, które mają być przesłane bezpośednio do grup. Jeżeli ustalona liczba zapytań zostanie wysłana, ale w odpowiedzi żaden raport nie zostanie przesłany, przełącznik usunie adres tego ruchu multicastowego z listy przekierowań ruchu multicastowego.
General Query Source IP	Gdy włączysz funkcję IGMP Snooping Querier, podaj źródłowy adres IP zapytań ogólnych, wysyłanych przez przełącznik. Wartość powinna być adresem unicast.
Static Router Ports	Wybierz jeden lub więcej portów, które mają być statycznymi portami routera w sieci VLAN. Statyczne porty routera nie tracą ważności. Strumienie multicastowe i pakiety IGMP będą przesyłane na statycznych portach routera do wszystkich grup tego VLAN-u. Strumienie multicastowe i pakiety IGMP grup, do których przynależą porty dynamiczne routera, będą przesyłane na odpowiednich dynamicznych portach routera.
Forbidden Router Ports	Wybierz porty, które nie będą mogły być portami routera w sieci VLAN.

2) Kliknij **Save**.

2.1.3 Konfiguracja IGMP Snooping dla portów

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-3 Konfiguracja IGMP Snooping dla portów



Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla portów:

1) Włącz IGMP Snooping dla portu i włącz Fast Leave, jeżeli z portem połączony jest tylko jeden odbiorca.

IGMP Snooping	Włącz lub wyłącz IGMP Snooping dla portu.
Fast Leave	Wlącz lub wyłącz Fast Leave na porcie. IGMPv1 nie obsługuje tej funkcji. Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu leave do urządzenia odpytującego. Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale *2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów*.
LAG	Grupa agregacji łączy, do której należy port.

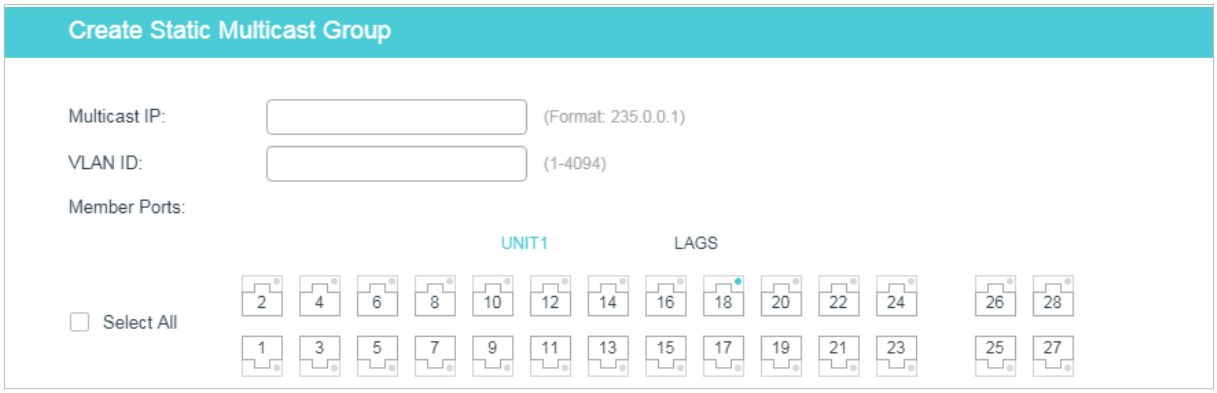
2) Kliknij **Apply**.

2.1.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączanie się hostów do grup.

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Static Group Config** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 2-4 Konfiguracja statycznego dołączania hostów do grup



Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

1) Podaj adres IP i VLAN ID ruchu multicastowego. Zaznacz porty, które mają statycznie przynależeć do grupy multicastowej.

Multicast IP	Podaj adres grupy multicastowej, do której mają dołączyć hosty.
VLAN ID	Określ VLAN hostów.
Member Ports	Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależeć do grupy multicastowej i nie będą tracić ważności.

2) Kliknij **Create**.

2.2 Przez CLI

2.2.1 Globalna konfiguracja IGMP Snooping

Wykonaj poniższe kroki, aby globalnie skonfigurować IGMP Snooping:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip igmp snooping** Włącz globalnie IGMP Snooping.

Krok 3	**ip igmp snooping version {**v1 | v2 | v3**}** Podaj wersję IGMP. v1: Przełącznik działa w trybie IGMPv1 Snooping. Może przetwarzać wyłącznie otrzymane od hosta komunikaty IGMPv1. Komunikaty innych wersji są ignorowane. v2: Przełącznik działa w trybie IGMPv2 Snooping. Może przetwarzać zarówno komunikaty IGMPv1, jak i IGMPv2, otrzymane od hosta. Komunikaty IGMPv3 są ignorowane. v3: Przełącznik działa w trybie IGMPv3 Snooping. Może przetwarzać otrzymane od hosta komunikaty wszystkich wersji: IGMPv1, IGMPv2 oraz IGMPv3.
Krok 4	**ip igmp snooping drop-unknown** (Opcjonalnie) Ustaw sposób, w jaki przełącznik ma przetwarzać strumienie multicastowe, które są przesyłane do nieznanych grup multicastowych, wybierając “Discard” (odrzuć). Domyślnym ustawieniem jest Forward. Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich w tabeli przekierowań ruchu multicastowego przełącznika. *Uwaga:* IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest upewnienie się, że funkcja MLD Snooping jest uruchomiona globalnie. Aby to zrobić, skorzystaj z polecenia **ipv6 mld snooping** w trybie konfiguracji globalnej.
Krok 5	**ip igmp snooping header-validation** (Opcjonalnie) Włacz funkcję Header Validation. Dla pakietów IGMP wartością TTL powinno być 1, pola ToS 0xC0, a opcji Router Alert 0x94040000. Pola, które muszą być uzupełnione, zależą od wersji IGMP. IGMPv1 wymaga jedynie pola TTL. IGMPv2 wymaga pól TTL oraz Router Alert. IGMPv3 wymaga natomiast pól TTL, ToS oraz Router Alert. Pakiety, które nie przejdą pomyślnie procesu weryfikacji zostaną odrzucone.
Krok 6	**show ip igmp snooping** Przejrzyj podstawową konfigurację IGMP Snooping.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia sposób globalnego uruchamiania IGMP Snooping i Header Validation, ustawiania wersji IGMP Snooping jako IGMPv3 oraz przetwarzania przez przełącznik strumieni multicastowych wysyłanych do nieznanych grup multicastowych jako “Discard”.

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping version v3

Switch(config)#ipv6 mld snooping

Switch(config)#ip igmp snooping drop-unknown

Switch(config)#ip igmp snooping header-validation

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

IGMP Version :V3

Unknown Multicast :Discard

Header Validation :Enable

..

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja IGMP Snooping dla VLAN-ów

Przed konfiguracją IGMP Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację IGMP Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla VLAN-ów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip igmp snooping vlan-config** *vlan-id-list* **mtime** *member-time* Włącz IGMP Snooping dla określonych VLAN-ów i ustal czas utraty ważności portów dla VLAN-ów. *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *member-time:* Podaj czas utraty ważności portów w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 260 sekund. Gdy przełącznik otrzymuje z portu raport IGMP, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi. Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów IGMP dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.

Krok 3 **ip igmp snooping vlan-config** *vlan-id-list* **rtime** *router-time*

Podaj czas utraty ważności portów routera przynależących do VLAN-u.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

router-time: Podaj czas utraty ważności portów routera w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 300 sekund.

Gdy przełącznik otrzymuje z portu komunikat z zapytaniem IGMP, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera.

Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem IGMP przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.

Krok 4 **ip igmp snooping vlan-config** *vlan-id-list* **ltime** *leave-time*

Podaj czas opuszczenia grupy dla VLAN-ów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

leave-time: Podaj czas opuszczania grupy dla VLAN-u(-ów). Prawidłowe wartości wahają się od 1 do 30 sekund. Domyślną wartością jest 1 sekunda.

Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje:

- Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.
- Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.

Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.

Krok 5 **ip igmp snooping vlan-config** *vlan-id-list* **report-suppression**

(Opcjonalnie) Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-ów. Domyślnie opcja jest wyłączona.

Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport IGMP dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do IGMP querier zdublowanych komunikatów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

Krok 6 **ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave**

(Opcjonalnie) Włącz funkcję szybkiego przełączania dla VLAN-ów. IGMPv1 nie obsługuje Fast Leave.

Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysyła komunikat IGMP o opuszczeniu grupy multicastowej, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).

Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu leave, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Member Query Count) dla określonych grup na tym porcie w ustalonym interwale czasowym (Last Member Query Interval), a następnie czeka na raporty dotyczące przynależności do grup IGMP Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na te zapytania prześlą przed wygaśnięciem Last Member Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przesyłu odpowiedniej grupy multicastowej.

Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysyła komunikat leave musi poczekać aż port z listy przesyłu przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).

Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tabeli przekierowań ruchu multicastowego przed przekazaniem komunikatu leave do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat leave.

Przez funkcji Fast Leave dla VLAN-u jest zalecane tylko, gdy do tego VLAN-u przynależy tylko jeden odbiorca na każdym porcie VLAN-u.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

Krok 7 **ip igmp snooping vlan-config** *vlan-id-list* **rport interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Opcjonalnie) Wybierz jeden lub więcej portów, które mają być statycznymi portami routera dla VLAN-ów. Statyczne porty routera nie tracą ważności.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

port-list: Numery lub lista portów Ethernet, które mają być statycznymi portami routera.

lag-list: ID lub lista grup agregacji łączy (LAG), które mają być statycznymi portami routera.

Krok 8 **ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Opcjonalnie) Wybierz porty, które nie będą mogły być portami routera dla VLAN-ów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

port-list: Numery lub lista portów Ethernet, które nie będą mogłby być portami routera.

lag-list: ID lub lista LAG, które nie będą mogłby być portami routera.

Krok 9	**ip igmp snooping vlan-config** *vlan-id-list* **querier** (Opcjonalnie) Włącz IGMP Snooping Querier dla VLAN-u. Domyślnie funkcja jest wyłączona. Włączona funkcja oznacza, że przełącznik pełni rolę IGMP Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytujące cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów leave, rozsyła zapytania do grup. *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *Uwaga:* Aby możliwe było włączenie IGMP Snooping Querier dla VLAN-u, funkcja IGMP Snooping powinna być uruchomiona zatówno globalnie, jak i dla VLAN-u. Po włączeniu funkcji IGMP Snooping Querier, konieczne jest uzupełnienie odpowiednich parametrów, w tym Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval i General Query Source IP. Skorzystaj z poniższego polecenia w trybie konfiguracji globalnej, aby skonfigurować te parametry: **ip igmp snooping vlan-config** *vlan-id-list* **querier { max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-member-query-count** *num* **| last-member-query-interval** *interval* **}** *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *response-time:* Podaj maksymalny czas odpowiedzi hostów na zapytania ogólne. Prawidłowe wartości wahają się od 1 do 25 sekund, a wartością domyślną jest 10 sekund. **query-interval** *interval:* Podaj interwał pomiędzy zapytaniami ogólnymi przesyłanymi przez przełącznik. Prawidłowe wartości wahają się od 10 do 300 sekund, a wartością domyślną jest 60 sekund. *ip-addr:* Podaj źródłowy adres IP zapytań ogólnych wysyłanych przez przełącznik. Wartość powinna być adresem unicast. Domyślną wartością jest 0.0.0.0. *num:* Podaj liczbę zapytań, które mają być przesłane bezpośrednio do grup. Włączona funkcja IGMP Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat leave IGMP, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła określone zapytania bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty leave. Jeżeli ustalona liczba zapytań zostanie wysłana bez odpowiedzi zwrotnej pod postacią komunikatu, przełącznik usunie adresy ruchu multicastowego z tabeli przekierowań ruchu multicastowego. Prawidłowe wartości wahają się od 1 do 5, a wartością domyślną jest 2. **last-member-query-interval** *interval:* Podaj interwał wysyłania zapytań do określonych grup. Prawidłowe wartości wahają się od 1 do 5 sekund, a wartością domyślną jest 1 sekunda.
Krok 10	**show ip igmp snooping vlan** *vlan-id* Przejrzyj podstawową konfigurację IGMP Snooping dla wybranegu VLAN-u.
Krok 11	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 12	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania IGMP Snooping dla VLAN 1, ustawiania czasu utraty ważności portu jako 300 sekund, czasu utraty ważności portu routera jako 320 sekund, a następnie włączania funkcji Fast Leave i Report Suppression dla VLAN-u:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 1 mtime 300

Switch(config)#ip igmp snooping vlan-config 1 rtime 320

Switch(config)#ip igmp snooping vlan-config 1 immediate-leave

Switch(config)#ip igmp snooping vlan-config 1 report-suppression

Switch(config)#show ip igmp snooping vlan 1

Vlan Id: 1

Vlan IGMP Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time:320

Member Time: 300

Querier: Disable

..

Switch(config)#end

Switch#copy running-config startup-config

Poniższy schemat przedstawia przykładowy sposób włączania IGMP Snooping querier dla VLAN 1, ustawiania interwału wysyłania zapytań jako 100 sekund, maksymalnego czasu odpowiedzi jako 15 sekund, interwału last member query jako 2 seconds, wartości last member query count jako 3 i ogólnego źrodłowego IP dla zapytań jako192.168.0.5:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 1 querier

Switch(config)#ip igmp snooping vlan-config 1 querier query-interval 100

Switch(config)#ip igmp snooping vlan-config 1 querier max-response-time 15

Switch(config)#ip igmp snooping vlan-config 1 querier last-member-query-interval 2

Switch(config)#ip igmp snooping vlan-config 1 querier last-member-query-count 3

Switch(config)#ip igmp snooping vlan-config 1 querier general-query source-ip192.168.0.5

Switch(config)#show ip igmp snooping vlan 1

Vlan Id: 1

..

Querier:

Maximum Response Time: 15

Query Interval: 100

Last Member Query Interval: 2

Last Member Query Count: 3

General Query Source IP: 192.168.0.5

..

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Konfiguracja IGMP Snooping dla portów

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla portów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list*| **port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu**.**
Krok 3	**ip igmp snooping** Włącz IGMP Snooping dla portu. Domyślnie funkcja jest włączona.
Krok 4	**ip igmp snooping immediate-leave** (Opcjonalnie) Włącz Fast Leave na określonym porcie. Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu leave do urządzenia odpytującego. Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale *2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów*.
Krok 5	**show ip igmp snooping interface [fastEthernet [** *port-list* **] | gigabitEthernet [** *port-list* **] | ten-gigabitEthernet [** *port-list* **] | port-channel [***port-channel-list***]] basic-config** Przejrzyj podstawową konfigurację IGMP Snooping poszczególnych lub wszystkich portów.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji IGMP Snooping i Fast Leave dla portu 1/0/1-3:

Switch#configure

Switch(config)#interface range fastEhternet 1/0/1-3

Switch(config-if-range)#ip igmp snooping

Switch(config-if-range)#ip igmp snooping immediate-leave

Switch(config-if-range)#show ip igmp snooping interface gigabitEthernet 1/0/1-3

Port	IGMP-Snooping	Fast-Leave
Gi1/0/1	enable	enable
Gi1/0/2	enable	enable
Gi1/0/3	enable	enable

Switch(config-if-range)#end

Switch#copy running-config startup-config

2.2.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączanie się hostów do grup.

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip igmp snooping vlan-config** *vlan-id-list* **static** *ip* **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}** *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *ip:* Podaj adres IP grupy multicastowej, do której mają dołączyć hosty. *port-list* / *lag-list:* Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależeć do grupy.
Krok 3	**show ip igmp snooping groups static** Przejrzyj statyczną konfigurację MLD Snooping.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji statycznego dołączania portu 1/0/1-3 w sieci VLAN 2 do grupy multicastowej 239.1.2.3:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 2 **static** 239.1.2.3 **interface gigabitEthernet** 1/0/1-3

Switch(config)#show ip igmp snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
239.1.2.3	2	static	Gi1/0/1-3

Switch(config)#end

Switch#copy running-config startup-config

3 Konfiguracja MLD Snooping

Wykonaj poniższe kroki, aby przeprowadzić konfigurację MLD Snooping:

1) Uruchom globalnie funkcję MLD Snooping i skonfiguruj parametry globalne.
2) Skonfiguruj MLD Snooping dla VLAN-ów.
3) Skonfiguruj MLD Snooping dla portów.
4) Skonfiguruj statyczne dołączanie hostów do grup (opcjonalnie).

Uwaga:

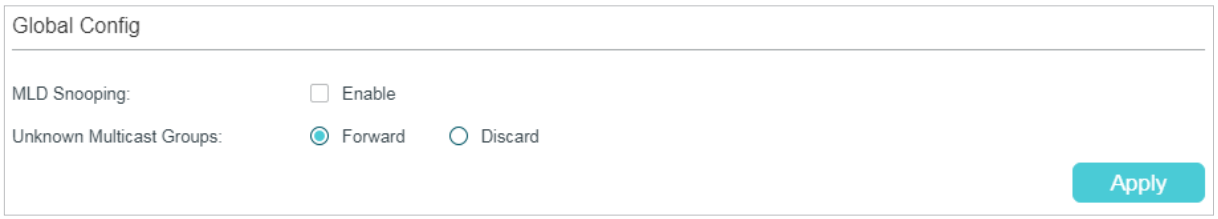
Funkcja MLD Snooping działa wyłącznie przy uruchomieniu globalnym - dla VLAN-u oraz odpowiednich portów.

3.1 Przez GUI

3.1.1 Konfiguracja globalna MLD Snooping

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Global Config,** aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja globalna MLD Snooping



Wykonaj poniższe kroki, aby skonfigurować globalnie MLD Snooping:

1) W sekcji **Global Config** włącz MLD Snooping i skonfiguruj globalnie opcję Unknown Multicast Groups.

MLD Snooping	Uruchom lub wyłącz globalnie MLD Snooping.

Unknown Multicast Groups	Zdecyduj w jaki sposób przełącznik ma przetwarzać dane, które są przesyłane do nieznanych grup multicastowych, wybierając spośród “Forward” (przesyłaj) lub “Discard” (odrzuć). Domyślnym ustawieniem jest Forward. Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich w tabeli przekierowań ruchu multicastowego przełącznika. *Uwaga:* IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest przejście w tym samym czasie do strony **L2 FEATURES > Multicast > IGMP Snooping > Global Config** i globalne uruchomienie funkcji IGMP Snooping.

2) Kliknij **Apply**.

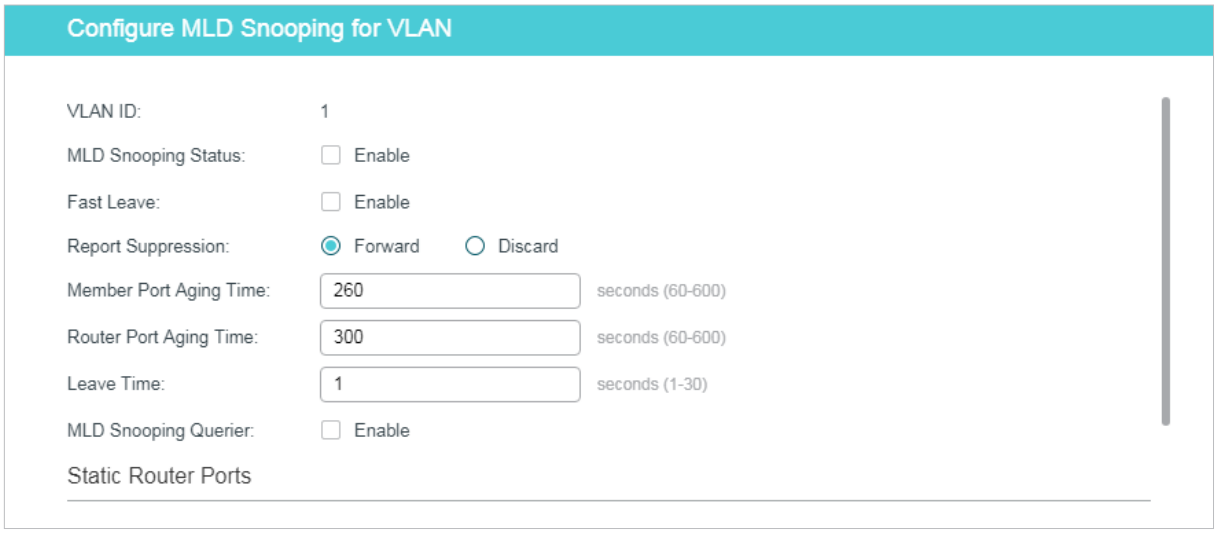
3.1.2 Konfiguracja MLD Snooping dla VLAN-ów

Przed konfiguracją MLD Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację MLD Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Global Config** i kliknij przy wybranej pozycji VLAN-u w sekcji **MLD VLAN Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 Konfiguracja MLD Snooping dla VLAN-u



Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla określonych VLAN-ów:

1) Włącz MLD Snooping dla VLAN-u i skonfiguruj odpowiednie parametry.

VLAN ID	Identyfikator VLAN-u.

MLD Snooping Status	Włącz lub wyłącz MLD Snooping dla VLAN-u.
Fast Leave	Włącz lub wyłącz funkcję szybkiego przełączania dla VLAN-u. IGMPv1 nie obsługuje Fast Leave. Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysyła komunikat leave IGMP, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier). Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu done, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Listener Query Count) dla określonych adresów ruchu multicastowego (MASQs) na tym porcie w ustalonym interwale czasowym (Last Listener Query Interval), a następnie czeka na raporty MLD. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na zapytania MASQs prześlą przed upływem Last Listener Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej. Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysyła komunikat done musi poczekać aż port z listy przkierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time). Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tabeli przekierowań ruchu multicastowego przed przekazaniem komunikatu done do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat done.
Report Suppression	Włącz ograniczanie wysyłania raportów dla VLAN-u. Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport MLD dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do MLD querier zdublowanych komunikatów.
Member Port Aging Time	Podaj czas utraty ważności portów przynależących do VLAN-u. Gdy przełącznik otrzymuje z portu raport MLD, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi. Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów MLD dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.

Router Port Aging Time	Podaj czas utraty ważności portów routera przynależących do VLAN-u. Gdy przełącznik otrzymuje z portu komunikat z zapytaniem MLD, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera. Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem MLD przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.
Leave Time	Podaj czas opuszczenia grupy dla VLAN-u. Gdy przelącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje: • Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time. • Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave. Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.
MLD Snooping Querier	Włącz lub wyłącz funkcję MLD Snooping Querier dla VLAN-u. Włączona funkcja oznacza, że przełącznik pełni rolę MLD Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytujące cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów done, rozsyła zapytania MASQs. *Uwaga:* Aby możliwe było włączenie MLD Snooping Querier dla VLAN-u, funkcja MLD Snooping powinna być uruchomiona zatrwno globalnie, jak i dla VLAN-u.
Query Interval	Gdy włączysz funkcję MLD Snooping Querier, podaj interwał wysyłania przez przełącznik zapytań ogólnych.
Maximum Response Time	Gdy włączysz funkcję MLD Snooping Querier, podaj maksymalny czas odpowiedzi hostów na zapytania ogólne.
Last Listener Query Interval	Włączona funkcja MLD Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat done, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła zapytania MASQs bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty done. Ten parametr jest wartością interwału pomiędzy przesyłanymi zapytaniami MASQs.
Last Listener Query Count	Gdy włączysz funkcję MLD Snooping Querier, podaj liczbę zapytań MASQs, które mają być przesłane. Jeżeli ustalona liczba zapytań zostanie wysłana, ale w odpowiedzi żaden raport nie zostanie przesłany, przełącznik usunie adres tego ruchu multicastowego z listy przekierowań ruchu multicastowego.

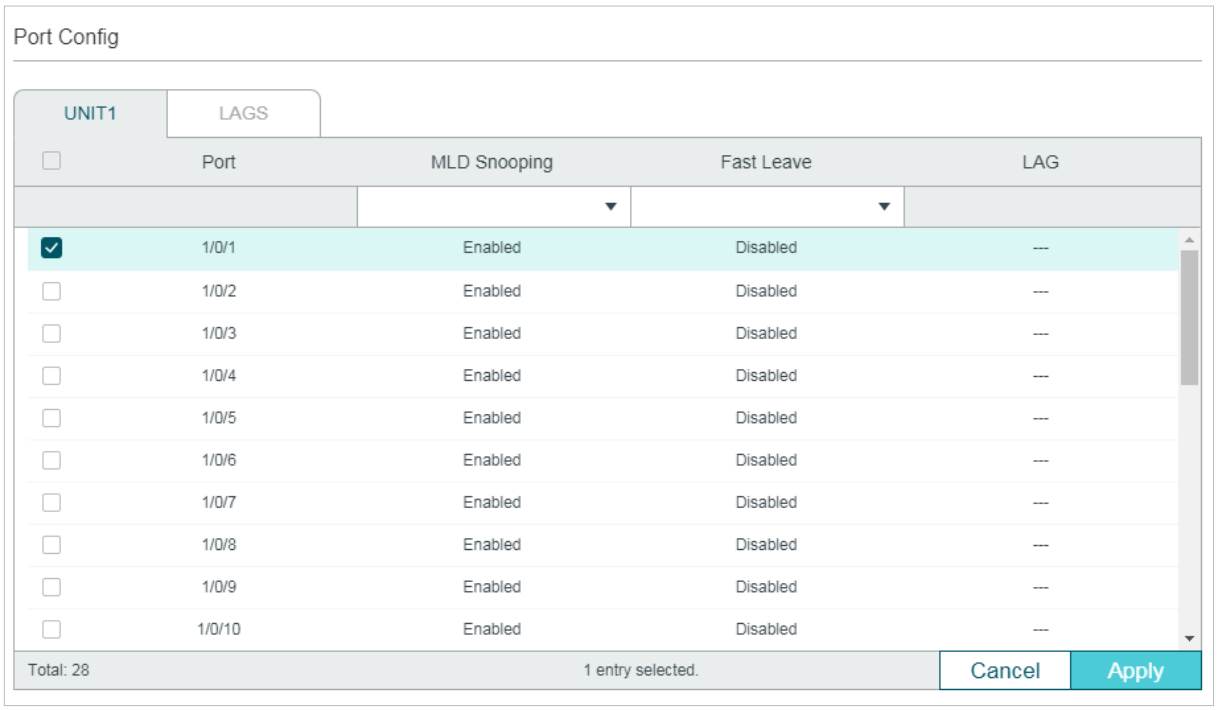
General Query Source IP	Gdy włączysz funkcję MLD Snooping Querier, podaj źródłowy adres IPv6 zapytań ogólnych, wysyłanych przez przełącznik. Wartość powinna być adresem unicast.
Static Router Ports	Wybierz jeden lub więcej portów, które mają być statycznymi portami routera w sieci VLAN. Statyczne porty routera nie tracą ważności. Strumienie multicastowe i pakiety MLD będą przesyłane na statycznych portach routera do wszystkich grup tego VLAN-u. Strumienie multicastowe i pakiety MLD grup, do których przynależą porty dynamiczne routera, będą przesyłane na odpowiednich dynamicznych portach routera.
Forbidden Router Ports	Wybierz porty, które nie będą mogły być portami routera w sieci VLAN.

2) Kliknij **Save**.

3.1.3 Konfiguracja MLD Snooping dla portów

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja MLD Snooping dla portów



Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla portów:

1) Włącz MLD Snooping dla portu i włącz Fast Leave, jeżeli z portem połączony jest tylko jeden odbiorca.

MLD Snooping	Włącz lub wyłącz MLD Snooping dla portu.

Fast Leave	Włącz lub wyłącz Fast Leave na porcie. Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu done do urządzenia odpytującego. Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale *3.1.2 Konfiguracja MLD Snooping dla VLAN-ów*.
LAG	Grupa agregacji łączy, do której należy port.

2) Kliknij **Apply**.

3.1.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączanie się hostów do grup.

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Static Group Config** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 3-4 Konfiguracja statycznego dołączania hostów do grup

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

1) Podaj adres IPv6 i VLAN ID ruchu multicastowego. Zaznacz porty, które mają statycznie przynależeć do grupy multicastowej.

Multicast IP	Podaj adres IPv6 grupy multicastowej, do której mają dołączyć hosty.
VLAN ID	Określ VLAN hostów.
Member Ports	Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależeć do grupy multicastowej i nie będą tracić ważności.

2) Kliknij **Create**.

3.2 Przez CLI

3.2.1 Globalna konfiguracja MLD Snooping

Wykonaj poniższe kroki, aby globalnie skonfigurować MLD Snooping:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ipv6 mld snooping** Włącz globalnie MLD Snooping.
Krok 3	**ipv6 mld snooping drop-unknown** (Opcjonalnie) Ustaw sposób, w jaki przełącznik ma przetwarzać strumienie multicastowe, które są przesyłane do nieznanych grup multicastowych, wybierając “Discard” (odrzuć). Domyślnym ustawieniem jest Forward. Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności MLD, a zatem nie ma ich w tabeli przekierowań ruchu multicastowego przełącznika. *Uwaga:* IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest upewnienie się, że funkcja IMPG Snooping jest uruchomiona globalnie. Aby to zrobić, skorzystaj z polecenia **ip igmp snooping** w trybie konfiguracji globalnej.
Krok 4	**show ipv6 mld snooping** Show the basic IGMP Snooping configuration.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania MLD Snooping oraz przetwarzania przez przełącznik strumieni multicastowych wysyłanych do nieznanych grup multicastowych jako “Discard”.

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping drop-unknown

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Discard

..

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Konfiguracja MLD Snooping dla VLAN-ów

Przed konfiguracją MLD Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację MLD Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu MLD Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla VLAN-ów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **mtime** *member-time* Włącz MLD Snooping dla określonych VLAN-ów i ustal czas utraty ważności portów dla VLAN-ów. *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *member-time:* Podaj czas utraty ważności portów w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 260 sekund. Gdy przełącznik otrzymuje z portu raport MLD, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi. Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów MLD dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.
Krok 3	**ipv6 mld snooping vlan-config** *vlan-id-list* **rtime** *router-time* Podaj czas utraty ważności portów routera przynależących do VLAN-u. *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *router-time:* Podaj czas utraty ważności portów routera w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 300 sekund. Gdy przełącznik otrzymuje z portu komunikat z zapytaniem MLD, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera. Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem MLD przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.

Krok 4 **ipv6 mld snooping vlan-config** *vlan-id-list* **ltime** *leave-time*

Podaj czas opuszczenia grupy dla VLAN-ów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

leave-time: Podaj czas opuszczania grupy dla VLAN-u(-ów). Prawidłowe wartości wahają się od 1 do 30 sekund. Domyślną wartością jest 1 sekunda.

Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje:

- Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.
- Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.

Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.

Krok 5 **ipv6 mld snooping vlan-config** *vlan-id-list* **report-suppression**

(Opcjonalnie) Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-ów. Domyślnie opcja jest wyłączona.

Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport MLD dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do MLD querier zdublowanych komunikatów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

Krok 6 **ipv6 mld snooping vlan-config** *vlan-id-list* **immediate-leave**

(Opcjonalnie) Włącz funkcję szybkiego przełączania dla VLAN-ów. Domyślnie funkcja jest wyłączona.

Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysyła komunikat done MLD (równoważny komunikatowi leave IGMP), przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).

Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu done, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Listener Query Count) dla określonych adresów ruchu multicastowego (MASQs) na tym porcie w ustalonym interwale czasowym (Last Listener Query Interval), a następnie czeka na raporty MLD. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na zapytania MASQs prześlą przed upływem Last Listener Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej.

Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysyła komunikat done musi poczekać aż port z listy przkierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).

Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tabeli przekierowań ruchu multicastowego przed przekazaniem komunikatu done do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat done.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

Krok 7 **ipv6 mld snooping vlan-config** *vlan-id-list* **rport interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Opcjonalnie) Wybierz jeden lub więcej portów, które mają być statycznymi portami routera dla VLAN-ów. Statyczne porty routera nie tracą ważności.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

port-list: Numery lub lista portów Ethernet, które mają być statycznymi portami routera.

lag-list: ID lub lista grup agregacji łączy (LAG), które mają być statycznymi portami routera.

Krok 8 **ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *lag-list* **}**

(Opcjonalnie) Wybierz porty, które nie będą mogły być portami routera dla VLAN-ów.

vlan-id-list: Podaj ID lub listę ID VLAN-u(-ów).

port-list: Numery lub lista portów Ethernet, które nie będą mogłby być portami routera.

lag-list: ID lub lista LAG, które nie będą mogłby być portami routera.

Krok 9	**ipv6 mld snooping vlan-config** *vlan-id-list* **querier** (Opcjonalnie) Włącz funkcję MLD Snooping Querier dla VLAN-u. Domyślnie funkcja jest wyłączona. Włączona funkcja oznacza, że przełącznik pełni rolę MLD Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytujące cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów done, rozsyła zapytania MASQs. *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *Uwaga:* Aby możliwe było włączenie MLD Snooping Querier dla VLAN-u, funkcja MLD Snooping powinna być uruchomiona zarówno globalnie, jak i dla VLAN-u. Po włączeniu funkcji MLD Snooping Querier, konieczne jest uzupełnienie odpowiednich parametrów, w tym Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval i General Query Source IP. Skorzystaj z poniższego polecenia w trybie konfiguracji globalnej, aby skonfigurować te parametry: **ipv6 mld snooping vlan-config** *vlan-id-list* **querier { max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-listener-query-count** *num* **| last-listener-query-interval** *interval* **}** *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *response-time:* Podaj maksymalny czas odpowiedzi hostów na zapytania ogólne. **query-interval** *interval:* Podaj interwał pomiędzy zapytaniami ogólnymi przesyłanymi przez przełącznik. *ip-addr:* Podaj źródłowy adres IP zapytań ogólnych wysyłanych przez przełącznik. Wartość powinna być adresem unicast. *num:* Podaj liczbę zapytań, które mają być przesłane bezpośrednio do grup. Włączona funkcja MLD Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat done, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła zapytania MASQs bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty done. Jeżeli ustalona liczba zapytań MASQs zostanie wysłana bez odpowiedzi zwrotnej pod postacią komunikatu, przełącznik usunie adresy ruchu multicastowego z tabeli przekierowań ruchu multicastowego. **last-listener-query-interval** *interval:* Podaj interwał wysyłania zapytań MASQs.
Krok 10	**show ipv6 mld snooping vlan** *vlan-id* Przejrzyj podstawową konfigurację MLD Snooping dla wybranegu VLAN-u.
Krok 11	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 12	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania MLD Snooping dla VLAN 1, ustawiania czasu utraty ważności portu jako 300 sekund, czasu utraty ważności portu routera jako 320 sekund, a następnie włączania funkcji Fast Leave i Report Suppression dla VLAN-u:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 1 mtime 300

Switch(config)#ipv6 mld snooping vlan-config 1 rtime 320

Switch(config)#ipv6 mld snooping vlan-config 1 immediate-leave

Switch(config)#ipv6 mld snooping vlan-config 1 report-suppression

Switch(config)#show ipv6 mld snooping vlan 1

Vlan Id: 1

Vlan MLD Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time: Enable

Member Time: Enable

Querier: Disable

..

Switch(config)#end

Switch#copy running-config startup-config

Poniższy schemat przedstawia przykładowy sposób włączania MLD Snooping querier dla VLAN 1, ustawiania interwału wysyłania zapytań jako 100 sekund, maksymalnego czasu odpowiedzi jako 15 sekund, interwału last listener query jako 2 seconds, wartości last member query count jako 3 i ogólnego źrodłowego IP dla zapytań jako FE80::1:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 1 querier

Switch(config)#ipv6 mld snooping vlan-config 1 querier query-interval 100

Switch(config)#ipv6 mld snooping vlan-config 1 querier max-response-time 15

Switch(config)#ipv6 mld snooping vlan-config 1 querier last-listener-query-interval 2

Switch(config)#ipv6 mld snooping vlan-config 1 querier last-listener-query-count 3

Switch(config)#ipv6 mld snooping vlan-config 1 querier general-query source-ip FE80::1

Switch(config)#show ipv6 mld snooping vlan 1

Vlan Id: 1

..

Querier: Enable

Maximum Response Time: 15

Query Interval: 100

Last Member Query Interval: 2

Last Member Query Count: 3

General Query Source IP: fe80::1

..

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Konfiguracja MLD Snooping dla portów

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla portów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list*| **port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu**.**
Krok 3	**ipv6 mld snooping** Włącz MLD Snooping dla portu. Domyślnie funkcja jest włączona.
Krok 4	**ipv6 mld snooping immediate-leave** (Opcjonalnie) Włącz Fast Leave na określonym porcie. Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu done do urządzenia odpytującego. Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale *3.1.2 Konfiguracja MLD Snooping dla VLAN-ów*.
Krok 5	**show ipv6 mld snooping interface [fastEthernet [** *port-list* **] | gigabitEthernet [** *port-list* **] | ten-gigabitEthernet [** *port-list* **] | port-channel [***port-channel-list***]] basic-config** Przejrzyj podstawową konfigurację MLD Snooping poszczególnych lub wszystkich portów.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji MLD Snooping i Fast Leave dla portu 1/0/1-3:

Switch#configure

Switch(config)#interface range fastEhternet 1/0/1-3

Switch(config-if-range)#ipv6 mld snooping

Switch(config-if-range)#ipv6 mld snooping immediate-leave

Switch(config-if-range)#show ipv6 mld snooping interface gigabitEthernet 1/0/1-3

Port	MLD-Snooping	Fast-Leave
Gi1/0/1	enable	enable
Gi1/0/2	enable	enable
Gi1/0/3	enable	enable

Switch(config-if-range)#end

Switch#copy running-config startup-config

3.2.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączanie się hostów do grup.

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **static** *ip* **interface {fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *lag-list***}** *vlan-id-list:* Podaj ID lub listę ID VLAN-u(-ów). *ip:* Podaj adres IP grupy multicastowej, do której mają dołączyć hosty. *port-list* / *lag-list:* Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależeć do grupy.
Krok 3	**show ipv6 mld snooping groups static** Przejrzyj statyczną konfigurację MLD Snooping.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji statycznego dołączania portu 1/0/1-3 w sieci VLAN 2 do grupy multicastowej FF80::1234:01:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 2 **static** FF80::1234:01 **interface gigabitEthernet** 1/0/1-3

Switch(config)#show ipv6 mld snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
ff80::1234:01	2	static	Gi1/0/1-3

Switch(config)#end

Switch#copy running-config startup-config

4 Konfiguracja MVR

Wykonaj poniższe kroki, aby przeprowadzić konfigurację MVR:

1) Skonfiguruj sieci 802.1Q VLAN.
2) Skonfiguruj MVR globalnie.
3) Dodaj grupy multicastowe do MVR.
4) Skonfiguruj MVR dla portów.
5) Skonfiguruj statyczne dodawanie portów do grup MVR (opcjonalnie).

Wskazówki dotyczące konfiguracji

- MVR nie obsługuje komunikatów IGMPv3.
- Nie konfiguruj MVR na prywatnych portach VLAN-u, w innym przypadku MVR nie będzie działać.
- MVR działa na podstawowym mechanizmie IGMP Snooping, ale funkcje te działają niezależnie od siebie. Możliwe jest włączenie na porcie obydwu protokołów jednocześnie. Uruchomienie obdywu funkcji spowoduje, że MVR będzie nasłuchiwać raportów i zostawiać komunikaty przeznaczone tylko dla grup multicastowych skonfigurowanych za pomocą tego protokołu. Wszystkie inne grupy multicastowe będę zarządzane przez IGMP Snooping.

4.1 Przez GUI

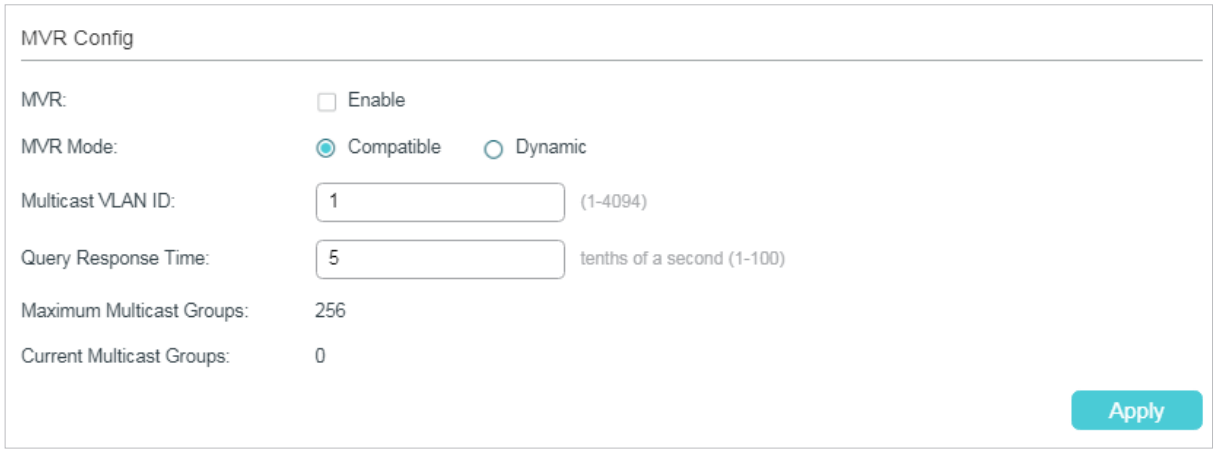
4.1.1 Konfiguracja VLAN-ów standardu 802.1Q

Przed rozpoczęciem konfiguracji MVR, utwórz 802.1Q VLAN jako VLAN multicastowy. Dodaj wszystkie porty źrodłowe (porty uplink, które odbierają dane ruchu multicastowego z routera) do VLAN-u multicastowego jako porty tagowane. Skonfiguruj sieci 802.1Q VLAN dla portów odbierających (porty, które łączą się z hostami), zgodnie z wymaganiami sieci. Pamiętaj, że porty odbierające mogą należeć tylko do jednej sieci VLAN i nie mogą być dodane do VLAN-u multicastowego. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

4.1.2 Globalna konfiguracja MVR

Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Config,** aby wyświetlić poniższą stronę.

Rys. 4-1 Globalna konfiguracja MVR



Wykonaj poniższe kroki, aby skonfigurować MVR globalnie:

1) Uruchom MVR globalnie i i skonfiguruj parametry globalne.

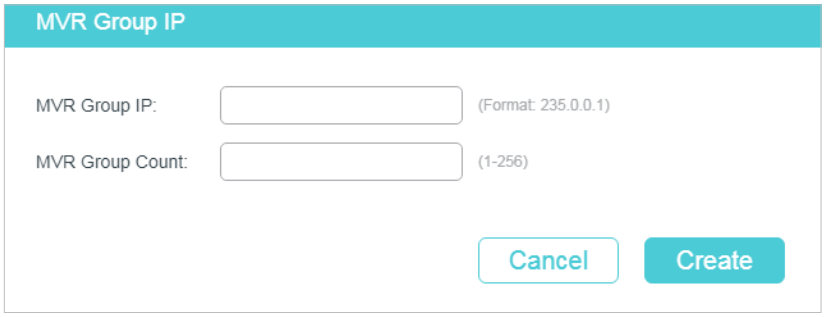
MVR	Włącz lub wyłącz MVR globalnie.
MVR Mode	Wybierz tryb MVR spośród “compatible” i “dynamic”. **Compatible:** W trym trybie przełącznik nie przesyła do IGMP querier raportów, ani komunikatów leave od hostów. To oznacza, że IGMP querier nie może nauczyć się przynależności do grup multicastowych z przełącznika. IGMP querier musi mieć statyczną konfigurację, aby móc transmitować wszystkie strumienie multicastowe do przełącznika poprzez VLAN multicastowy. **Dynamic:** W tym trybie, po otrzymianiu raportów lub komunikatów leave od hostów, przełącznik przesyła je do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). IGMP querier może uczyć się przynależności do grup multicastowych poprzez otrzymane raporty lub komunikaty leave i transmitować strumienie multicastowe do przełącznika poprzez VLAN multicastowy, zgodnie z tabelą przekierowań ruchu multicastowego.
Multicast VLAN ID	Ustaw istniejącą sieć 802.1Q VLAN jako VLAN multicastowy.
Query Response Time	Podaj maksymalny czas oczekiwania na porcie odbierającym na raport IGMP przed usunięciem portu z grupy multicastowej.
Maximum Multicast Groups	Maksymalna liczba grup multicastowych dla przełącznika.
Current Multicast Groups	Aktualna liczba skonfigurowanych na przełączniku grup multicastowych.

2) Kliknij **Apply**.

4.1.3 Dodawanie grup multicastowych do MVR

Dodawanie grup multicastowych do MVR odbywa się ręcznie. Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Group Config** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 4-2 Dodawanie grup multicastowych do MVR



Wykonaj poniższe kroki, aby dodać grupy multicastowe do MVR:

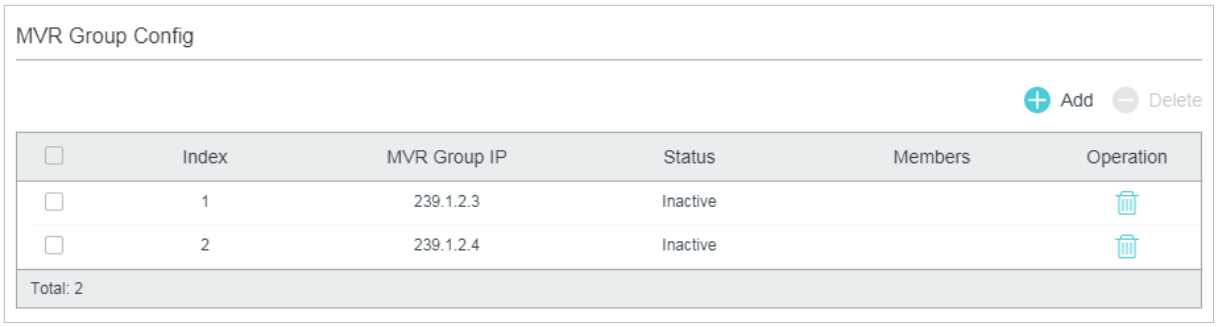
1) Podaj adres IP grup multicastowych.

MVR Group IP / MVR Group Count	Podaj początkowy adres IP i liczbę następujących po sobie grup multicastowych. Dane ruchu mutlicastowego przesłane na podany tutaj adres zostaną także przesłane do wszystkich portów źródłowych przełącznka i do wszystkich portów odbierających, które wysłały żądanie otrzymywania danych z tego adresu multicastowego.

2) Kliknij **Create**.

Dodane grupy multicastowe pojawią się w tabeli grup MVR, tak jak pokazano poniżej:

Rys. 4-3 Tabela grup MVR



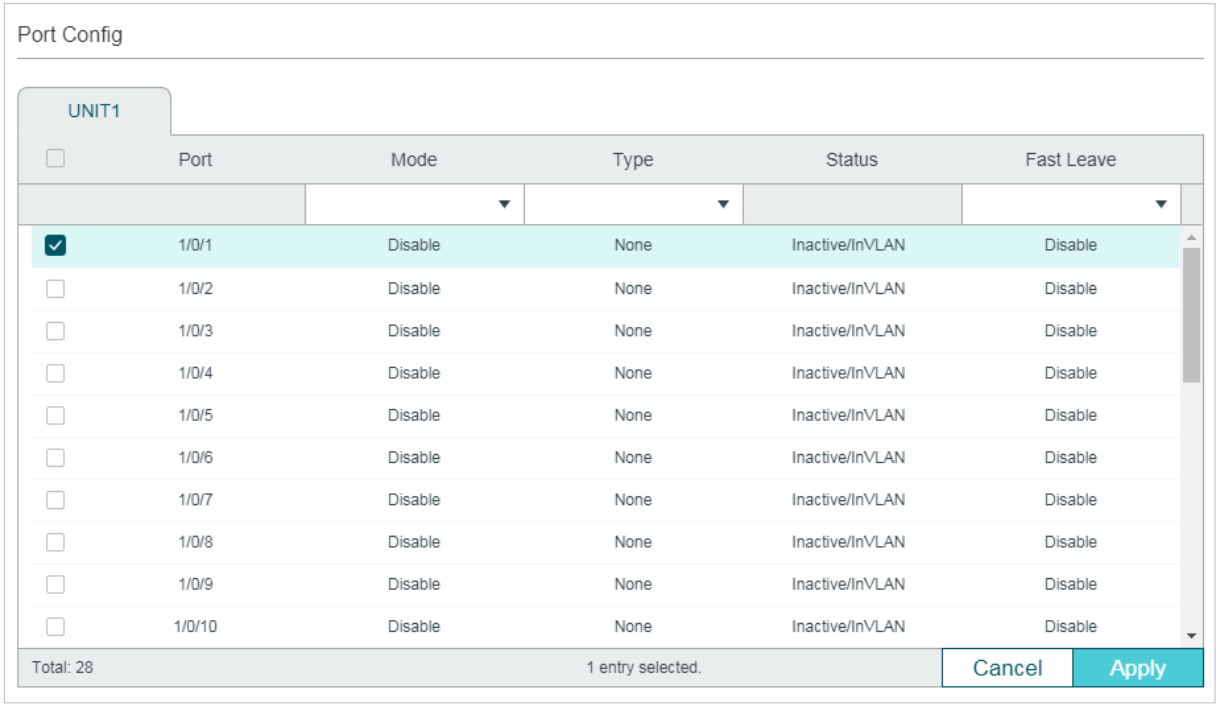
MVR Group IP	Adres IP grupy multicastowej.

Status	Stan grupy MVR. W trybie “compatible”, wszystkie grupy MVR są dodawane ręcznie, dlatego ich stanem jest zawsze “active”. W trybie “dynami” możliwe są dwa stany: **Inactive**: Grupa MVR group została dodana poprawnie, ale na port źródłowy nie zostały przesłane żadne zapytania z tej grup multicastowej. **Active**: Grupa MVR została dodana poprawnie, a na port źródłowy zostały przesłane zapytania z tej grup multicastowej.
Member	Porty danej grupy MVR.

4.1.4 Konfiguracja MVR dla portu

Wybierz z menu **L2 FEATURES > Multicast > MVR > Port Config,** aby wyświetlić poniższą stronę.

Rys. 4-4 Konfiguracja MVR dla portu



Wykonaj poniższe kroki, aby dodać grupy multicastowe do MVR:

1) Wybierz jeden lub więcej portów do konfiguracji.
2) Włącz MVR i skonfiguruj typ portu oraz funkcję Fast Leave dla portu.

Mode	Włącz lub wyłącz MVR dla wybranych portów.

Type	Skonfiguruj typ portu. **None**: Port nie jest portem MVR. Jeżeli podejmiesz próbę konfiguracji takiego portu korzystając z właściwości MVR, ta operacja zakończy się niepowodzeniem. **Source**: Ustaw porty uplink, które otrzymują i przesyłają dane ruchu mutlicastowego poprzez VLAN multicastowy jako porty źródłowe (“source ports”). Takie porty powinny należeć do VLAN-u multicastowego. W trybie “compatible” porty źródłowe są automatycznie dodawane do wszystkich grup multicastowych, natomiast w trybie “dynamic” konieczne jest ręczne dodawanie ich do odpowiednich grup multicastowych. **Receiver**: Skonfiguruj porty, które łączą się z hostami jako porty odbierające. Port odbierający może należeć tylko do jednego VLAN-u, z wykluczeniem VLAN-u multicastowego. W obydwu trybach przełącznik dodaje porty odbierające do odpowiednich grup multicastowych lub je usuwa na podstawie raportów i wiadomości leave, otrzymanych od hostów.
Status	Stan portu. **Active/InVLAN**: Port jest fizycznie włączony i przynależy do jednego lub kilku VLAN-ów. **Active/NotInVLAN**: Port jest fizycznie włączony, ale nie przynależy do żadnego VLAN-u. **Inactive/InVLAN**: Port jest fizycznie wyłączony, ale przynależy do jednego lub kilku VLAN-ów. **Inactive/NotInVLAN**: Port jest fizycznie wyłączony i nie prznależy do żadnego VLAN-u.
Fast Leave	Włącz lub wyłącz Fast Leave dla wybranych portów. Tylko porty odbierające obsługują Fast Leave. Przed włączeniem Fast Leave dla portu, upewnij się, że z portem połączone jest tylko jedno urządzenie odbierające.

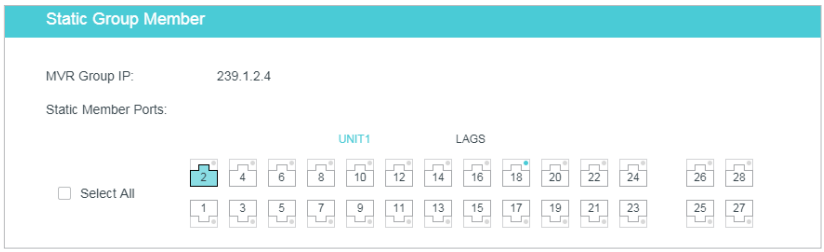
3) Kliknij **Apply**.

4.1.5 (Opcjonalnie) Statyczne dodawanie portów do grup MVR

Tylko porty odbierające mogą być dodawane do grup MVR statycznie. Przełącznik dodaje porty do odpowiednich grup multicastowych lub usuwa je na podstawie raportów i komunikatów leave, otrzymanych od hostów.

Wybierz z menu **L2 FEATURES > Multicast > MVR > Static Group Members** i kliknij przy wybranej pozycji z grupą MVR, aby wyświetlić poniższą stronę.

Rys. 4-5 Konfiguracja statycznego dołączania hostów do grupy MVR



Wykonaj poniższe kroki, aby statycznie dodać porty do grupy MVR:

1) Wybierz porty, aby dodać je do grupy MVR.
2) Kliknij **Save**.

4.2 Przez CLI

4.2.1 Konfiguracja VLAN-ów standardu 802.1Q

Przed rozpoczęciem konfiguracji MVR, utwórz 802.1Q VLAN jako VLAN multicastowy. Dodaj wszystkie porty źrodłowe do VLAN-u multicastowego jako porty tagowane. Skonfiguruj sieci 802.1Q VLAN dla portów odbierających, zgodnie z wymaganiami sieci. Pamiętaj, że porty odbierające mogą należeć tylko do jednej sieci VLAN i nie mogą być dodane do VLAN-u multicastowego. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

4.2.2 Globalna konfiguracja MVR

Wykonaj poniższe kroki, aby skonfigurować MVR globalnie:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**mvr** Włącz MVR globalnie.

Krok 3	**mvr mode {** compatible | dynamic **}** Wybierz tryb MVR spośród “compatible” i “dynamic”. compatible: W trym trybie przełącznik nie przesyła do IGMP querier raportów, ani komunikatów leave od hostów. To oznacza, że IGMP querier nie może nauczyć się przynależności do grup multicastowych z przełącznika. IGMP querier musi mieć statyczną konfigurację, aby móc transmitować wszystkie strumienie multicastowe do przełącznika poprzez VLAN multicastowy. dynamic: W tym trybie, po otrzymianiu raportów lub komunikatów leave od hostów, przełącznik przesyła je do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). IGMP querier może uczyć się przynależności do grup multicastowych poprzez otrzymane raporty lub komunikaty leave i transmitować strumienie multicastowe do przełącznika poprzez VLAN multicastowy, zgodnie z tabelą przekierowań ruchu multicastowego.
Krok 4	**mvr vlan** *vlan-id* Określ VLAN multicastowy. *vlan-id:* Podaj ID VLAN-u multicastowego. Prawidłowe wartości wahają się od 1 do 4094.
Krok 5	**mvr querytime** *time* Podaj maksymalny czas oczekiwania na porcie odbierającym na raport IGMP przed usunięciem portu z grupy multicastowej. *time:* Podaj maksymalny czas odpowiedzi. Poprawne wartości wahają się od 1 do 100 dziesiątych części sekundy, a wartością domyślną jest 5 dziesiątych sekundy.
Krok 6	**mvr group** *ip-addr count* Dodaj grupę multicastową do MVR. *ip-addr:* Podaj początkowy adres IP następujących po sobie grup multicastowych. *count:* Podaj liczbę grup multicastowych, które mają być dodane do MVR. Prawidłowe wartości wahają się od 1 do 256.
Krok 7	**show mvr** Przejrzyj globalną konfigurację MVR. **show mvr members** Przejrzyj istniejące grupy MVR.
Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania MVR, ustawiania trybu MVR jako compatible, VLAN-u multicastowego jako VLAN 2, czasu odpowiedzi na zapytanie jako 5 dziesiątych sekundy oraz dodawania 239.1.2.3-239.1.2.5 do grupy MVR.

Switch#configure

Switch(config)#mvr mode compatible

Switch(config)#mvr vlan 2

Switch(config)#mvr querytime 5

Switch(config)#mvr group 239.1.2.3 3

Switch(config)#show mvr

MVR :Enable

MVR Multicast Vlan :2

MVR Max Multicast Groups :256

MVR Current Multicast Groups :3

MVR Global Query Response Time :5 (tenths of sec)

MVR Mode Type :Compatible

Switch(config)#show mvr members

MVR Group IP	status	Members
239.1.2.3	active	
239.1.2.4	active	
239.1.2.5	active	

Switch(config)#end

Switch#copy running-config startup-config

4.2.3 Konfiguracja MVR dla portów

Wykonaj poniższe kroki, aby skonfigurować MVR dla portów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu**.**
Krok 3	**mvr** Włącz MVR dla portu.

Krok 4	**mvr type {** source | receiver **}** Skonfiguruj typ portu MVR. Domyślnie wybranym portem jest port non-MVR. Jeżeli podejmiesz próbę konfiguracji takiego portu korzystając z właściwości MVR, ta operacja zakończy się niepowodzeniem. source: Ustaw porty uplink, które otrzymują i przesyłają dane ruchu mutlicastowego poprzez VLAN multicastowy jako porty źródłowe. Takie porty powinny należeć do VLAN-u multicastowego. receiver: Skonfiguruj porty, które łączą się z hostami jako porty odbierające. Port odbierający może należeć tylko do jednego VLAN-u, z wykluczeniem VLAN-u multicastowego.
Krok 5	**mvr immediate** (Opcjonalnie) Włącz Fast Leave dla portu. Tylko porty odbierające obsługują Fast Leave. Przed włączeniem Fast Leave dla portu, upewnij się, że z portem połączone jest tylko jedno urządzenie odbierające.
Krok 6	**mvr vlan** *vlan-id* **group** *ip-addr* (Opcjonalnie) Dodaj port do grupy MVR statycznie. Taki port może odbierać transmisję ruchu mutlicastowego przesłanego na adres IP multicastowy poprzez VLAN multicastowy. Tylko porty odbierające mogą być dodawane do grup MVR statycznie. Przełącznik dodaje porty do odpowiednich grup multicastowych lub usuwa je na podstawie raportów i komunikatów leave, otrzymanych od hostów. *vlan-id*: Podaj ID VLAN-u multicastowego. *ip-addr*: Podaj adres IP grupy multicastowej.
Krok 7	**show mvr interface {fastEthernet [***port-list* **] | gigabitEthernet [***port-list* **] | ten-gigabitEthernet [***port-list* **] }** Przejrzyj konfigurację MVR określonych interfejsów. **show mvr members** Przejrzyj informacje o przynależności do wszystkich grup MVR.
Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania portu 1/0/7 jako source port, portów 1/0/1-3 jako receiver ports, statycznego dodawania portu 1/0/1-3 do grupy 239.1.2.3 i włączania Fast Leave dla tych portów. VLAN-em multicastowym jest VLAN 2.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#mvr

Switch(config-if)#mvr type source

Switch(config-if)#exit

Switch(config)#interface range gigabitEthernet 1/0/1-3

Switch(config-if-range)#mvr

Switch(config-if-range)#mvr type receiver

Switch(config-if-range)#mvr immediate

Switch(config-if-range)#mvr vlan 2 **group** 239.1.2.3

Switch(config-if-range)#show mvr interface fastEtnernet 1/0/1-3,1/0/7

Port	Mode	Type	Status	Immediate Leave
Gi1/0/1	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/2	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/3	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/7	Enable	Source	INACTIVE/InVLAN	Disable

Switch(config-if-range)#show mvr members

MVR Group IP	status	Members
239.1.2.3	active	Gi1/0/1-3, 1/0/7

Switch(config)#end

Switch#copy running-config startup-config

5 Konfiguracja filtrowania pakietów multicastu

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji filtrowania pakietów multicastu:

1) Utwórz profil IGMP lub profil MLD.
2) Wybierz, do których grup multicastowych można dołączać porty i skonfiguruj działania w przypadku zbyt wielu grup.

5.1 Przez GUI

5.1.1 Tworzenie profili multicast

Możesz tworzyć profile multicast zarówno dla sieci IPv4, jak i IPv6. Korzystając z profilu multicast przełącznik może tworzyć czarne i białe listy grup multicastowych, co pozwala filtrować źródła pakietów multicastu.

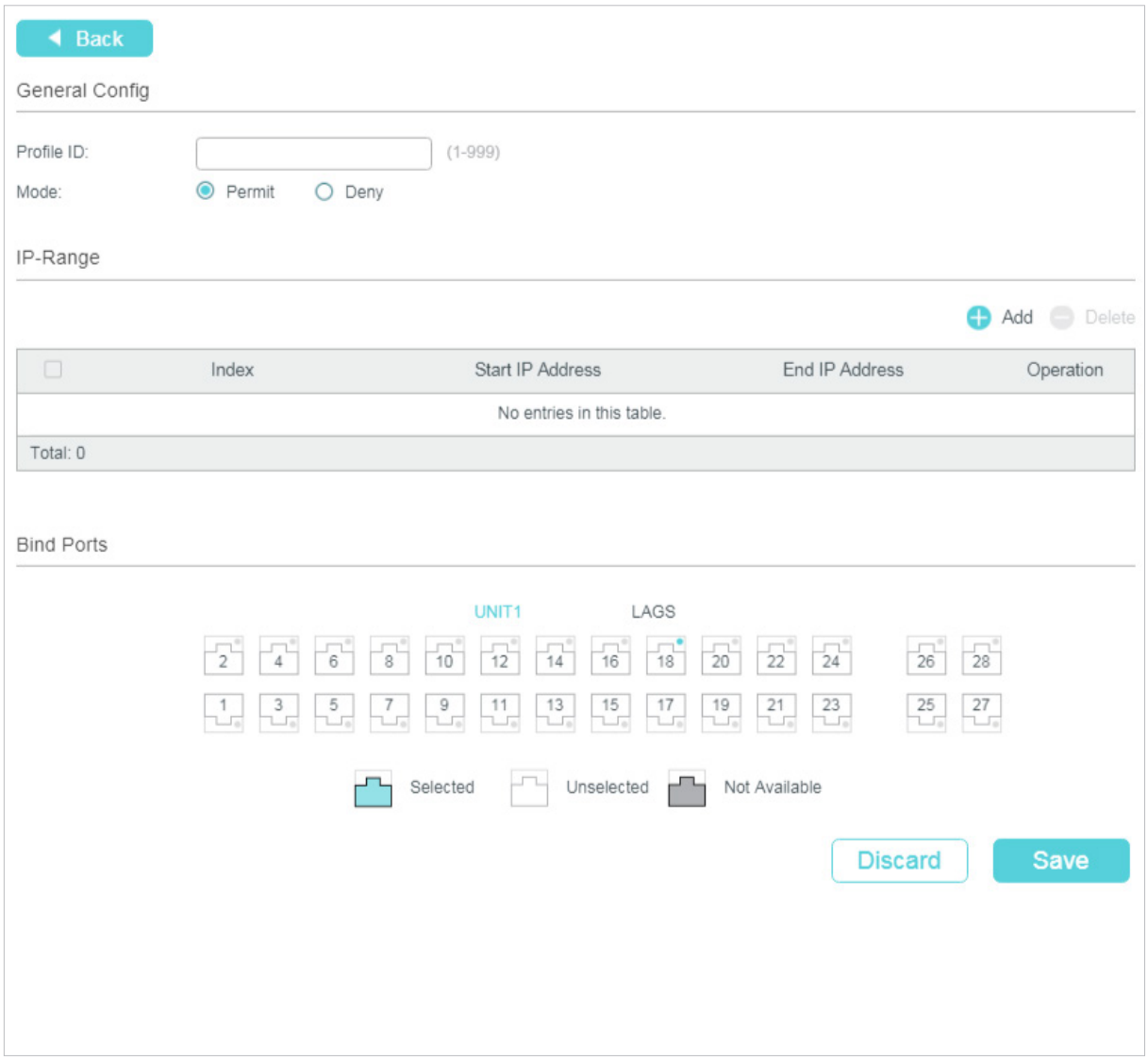
Tworzenie profili multicastu wygląda w ten sam sposób dla IPv4 i IPv6. Dla przykładu utworzymy profil IPv4.

Wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Profile** i kliknij Add , aby wyświetlić poniższą stronę.

Uwaga:

Aby utworzyć profil multicast dla IPv6, wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Profile**.

Rys. 5-1 Konfiguracja profilu IPv4



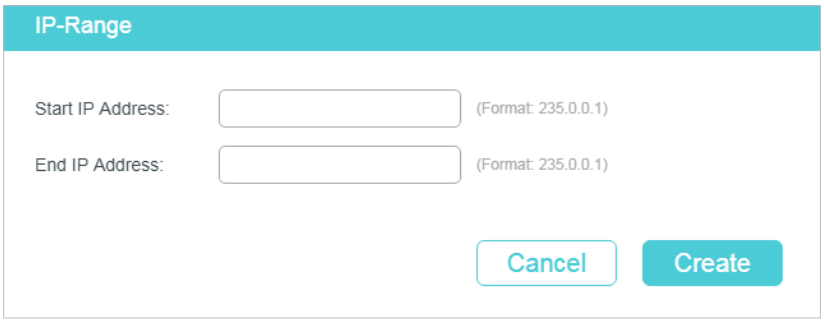
Wykonaj poniższe kroki, aby utworzyć profil.

1) W sekcji **General Config** wybierz ID profilu i tryb filtrowania.

Profile ID	Podaj ID, wybierając wartość z przedziału 1 - 999.
Mode	Ustal tryb filtrowania, wybierając **Permit** lub **Deny**. **Permit**: Pełni funkcję białej listy, zezwalając tylko określonym portom na dołącznie do wybranych grup multicastowych. **Deny**: Pełni funkcję czarnej listy, uniemożliwiając określonym portom na dołączanie do wybranych grup multicastowych.

2) W sekcji **IP-Range** kliknij Add , aby wyświetlić poniższą stronę. Skonfiguruj początkowy adres IP i końcowy adres IP grup multicastowych, które mają podlegać filtrowaniu i kliknij **Create**.

Rys. 5-2 Konfiguracja filtrowania grup multicastowych



3) W sekcji **Bind Ports** wybierz porty, które chcesz powiązać z profilem.

4) Kliknij **Save**.

5.1.2 Konfiguracja filtrowania pakietów multicastu dla portów

Mapowanie relacji między portami i profilami możesz modyfikować partami. Masz także możliwość konfiguracji liczby grup, do których port może dołączyć oraz działań w przypadku zbyt wielu grup.

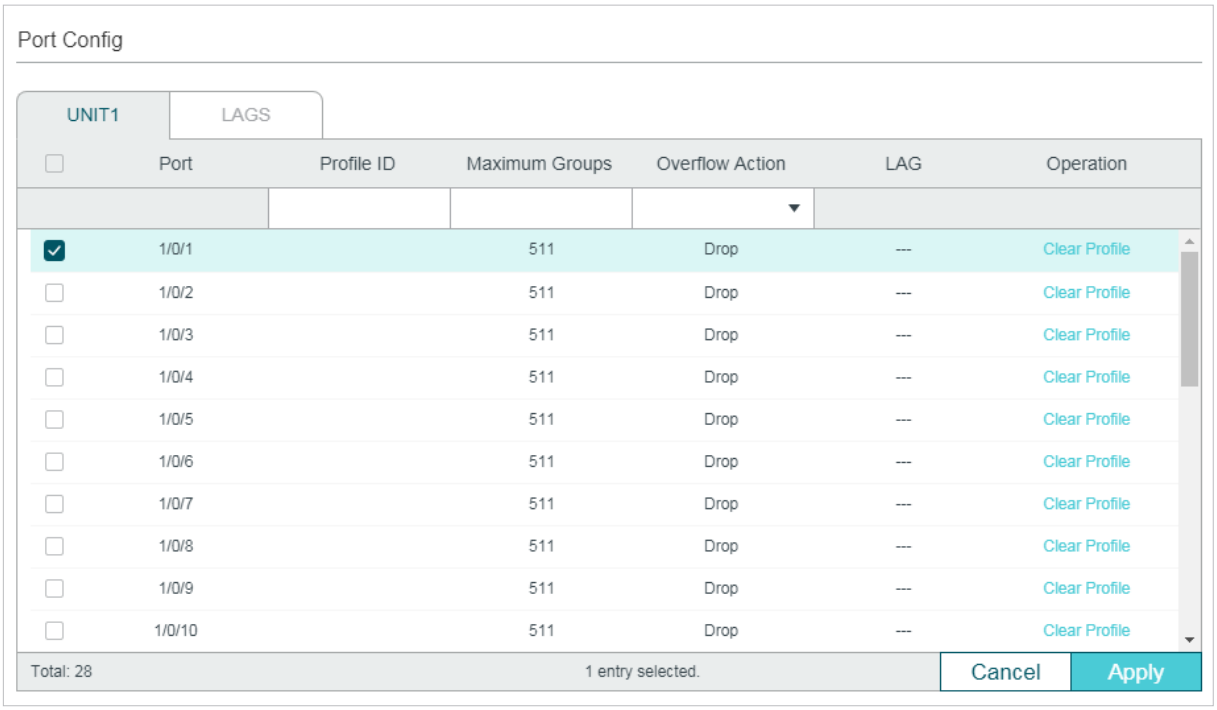
Konfiguracja filtrowania pakietów multicastu dla portów jest taka sama dla IPv4 i IPv6. Dla przykładu skonfigurujemy filtrowanie w sieci IPv4.

Wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Port Config**, aby wyświetlić poniższą stronę.

Uwaga:

Dla IPv6 wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Port Config**.

Rys. 5-3 Konfiguracja filtrowania pakietów multicastu dla portów



Wykonaj poniższe kroki, aby powiązać profil z portami i skonfigurować odpowiednie parametery dla portów:

1) Wybierz jeden lub kilka portów do konfiguracji.
2) Wybierz profil, z którym chcesz powiązać porty i skonfiguruj maksymalną liczbę grup, do których port może dołączyć oraz działania w przypadku zbyt wielu grup.

Profile ID	Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami. Jeden port może być powiązany tylko z jednym profilem.
Maximum Groups	Podaj liczbę grup multicastowych, do których port może dołączyć. Prawidłowe wartości wahają się od 1 do 511.
Overflow Action	Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych. **Drop**: Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych. **Replace**: Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową.
LAG	Grupa agregacji łączy, do której należy port.
Operation	Kliknij **Clear Profile**, aby usunąć powiązanie między profilem a portem.

3) Kliknij **Apply**.

5.2 Przez CLI

5.2.1 Tworzenie profili multicast

Możesz tworzyć profile multicast zarówno dla sieci IPv4, jak i IPv6. Korzystając z profilu multicast przełącznik może tworzyć czarne i białe listy grup multicastowych, co pozwala filtrować źródła pakietów multicastu.

Tworzenie profilu IGMP (Profil multicast dla IPv4)

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip igmp profile** *id* Utwórz nowy profil i uruchom tryb konfiguracji profilu.

Krok 3	**Permit** Ustaw dla profilu tryb filtrowania jako permit. Profil będzie pełnić funkcję białej listy, zezwalając tylko określonym portom na dołącznie do wybranych grup multicastowych. **deny** Ustaw dla profilu tryb filtrowania jako deny. Profil będzie pełnić funkcję czarnej listy, uniemożliwając określonym portom na dołączanie do wybranych grup multicastowych.
Krok 4	**range** *start-ip end-ip* Skonfiguruj zakres adresów IP grup multicastowych, które mają podlegać filtrowaniu. *start-ip* / *end-ip:* Podaj początkowy adres IP i końcowy adres IP.
Krok 5	**show ip igmp profile [***id***]** Przejrzyj szczegóły konfiguracji profilu IGMP.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji Profile 1, tak aby przełącznik filtrował strumienie mutlicastowe przesyłane na adres 226.0.0.5-226.0.0.10:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp profile 1

Switch(config-igmp-profile)#deny

Switch(config-igmp-profile)#range 226.0.0.5 226.0.0.10

Switch(config-igmp-profile)#show ip igmp profile

IGMP Profile 1

deny

range 226.0.0.5 226.0.0.10

Switch(config)#end

Switch#copy running-config startup-config

Tworzenie profilu MLD (profil multicast dla IPv6)

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**ipv6 mld profile** *id* Utwórz nowy profil i uruchom tryb konfiguracji profilu.
Krok 3	**Permit** Ustaw dla profilu tryb filtrowania jako permit. Profil będzie pełnić funkcję białej listy, zezwalając tylko określonym portom na dołącznie do wybranych grup multicastowych. **deny** Ustaw dla profilu tryb filtrowania jako deny. Profil będzie pełnić funkcję czarnej listy, uniemożliwiając określonym portom na dołączanie do wybranych grup multicastowych.
Krok 4	**range** *start-ip end-ip* Skonfiguruj zakres adresów IP grup multicastowych, które mają podlegać filtrowaniu. *start-ip* / *end-ip:* Podaj początkowy adres IP i końcowy adres IP.
Krok 5	**show ipv6 mld profile [***id***]** Przejrzyj szczegóły konfiguracji profilu MLD.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji Profile 1, tak aby przełącznik filtrował strumienie mutlicastowe przesyłane na adres ff01::1234:5-ff01::1234:8:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld profile 1

Switch(config-mld-profile)#deny

Switch(config-mld-profile)#range ff01::1234:5 ff01::1234:8

Switch(config-mld-profile)#show ipv6 mld profile

MLD Profile 1

deny

range ff01::1234:5 ff01::1234:8

Switch(config)#end

Switch#copy running-config startup-config

5.2.2 Tworzenie powiązań portów z profilami

Możesz już tworzyć powiązania pomiędzy portami a utworzonymi profilami IGMP lub MLD. Masz także możliwość konfiguracji liczby grup, do których port może dołączyć oraz działań w przypadku zbyt wielu grup.

Wiązanie portów z profilem IGMP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**ip igmp filter** *profile-id* Powiąż profil IGMP z wybranymi portami. *profile-id*: Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami.
Krok 4	**ip igmp snooping max-groups** *maxgroup* Podaj liczbę grup multicastowych, do których port może dołączyć. *maxgroup*: Podaj maksymalną liczbę grup multicastowych. Prawidłowe wartości wahają się od 1 do 511.
Krok 5	**ip igmp snooping max-groups action {**drop | replace**}** Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych. drop: Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych. replace: Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową.
Krok 6	**show ip igmp profile [***id***]** Przejrzyj szczegóły konfiguracji profilu IGMP. **show ip igmp snooping interface [fastEthernet** [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*] **] max-groups** Przejrzyj limity grup multicastowych dla wybranych portów lub dla wszystkich portów.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącego Profile 1 z portem 1/0/2, ustawiania maksymalnej liczby grup multicastowych, do których port 1/0/2 może dołączyć jako 50 i Overflow Action jako Drop:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp filter 1

Switch(config-if)#ip igmp snooping max-groups 50

Switch(config-if)#ip igmp snooping max-groups action drop

Switch(config-if)#show ip igmp profile

IGMP Profile 1

..

Binding Port(s)

Gi1/0/2

Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/2 **max-groups**

Port	Max-Groups	Overflow-Action
Gi1/0/2	50	Drops

Switch(config)#end

Switch#copy running-config startup-config

Wiązanie portów z profilem MLD

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**ipv6 mld filter** *profile-id* Powiąż profil MLD z wybranymi portami. *profile-id*: Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami.

Krok 4	**ipv6 mld snooping max-groups** *maxgroup* Podaj liczbę grup multicastowych, do których port może dołączyć. *maxgroup*: odaj maksymalną liczbę grup multicastowych. Prawidłowe wartości wahają się od 1 do 511.
Krok 5	**ipv6 mld snooping max-groups action {**drop | replace**}** Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych. drop: Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych. replace: Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową.
Krok 6	**show ipv6 mld profile [***id***]** Przejrzyj szczegóły konfiguracji profilu MLD. **show ipv6 mld snooping interface [fastEthernet** [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*] **] max-groups** Przejrzyj limity grup multicastowych dla wybranych portów lub dla wszystkich portów.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącego Profile 1 z portem 1/0/2, ustawiania maksymalnej liczby grup multicastowych, do których port 1/0/2 może dołączyć jako 50 i Overflow Action jako Drop:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#ipv6 mld filter 1

Switch(config-if)#ipv6 mld snooping max-groups 50

Switch(config-if)#ipv6 mld snooping max-groups action drop

Switch(config-if)#show ipv6 mld profile

MLD Profile 1

..

Binding Port(s)

Gi1/0/2

Switch(config-if)#show ipv6 mld snooping interface gigabitEthernet 1/0/2 **max-groups**

Port	Max-Groups	Overflow-Action
Gi1/0/2	50	Drops

Switch(config)#end

Switch#copy running-config startup-config

6 Przeglądanie informacji o Multicast Snooping

Możesz przeglądać następujące informacje dotyczące Multicast Snooping:

- Tabela adresów IPv4 multicast.
- Statystyki pakietów IPv4 multicast na każdym porcie.
- Tabela adresów IPv6 multicast.
- Statystyki pakietów IPv6 multicast na każdym porcie.

6.1 Przez GUI

6.1.1 Przeglądanie tabeli adresów IPv4 multicast

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Table**, aby wyświetlić poniższą stronę:

Rys. 6-1 Tabela adresów IPv4 multicast

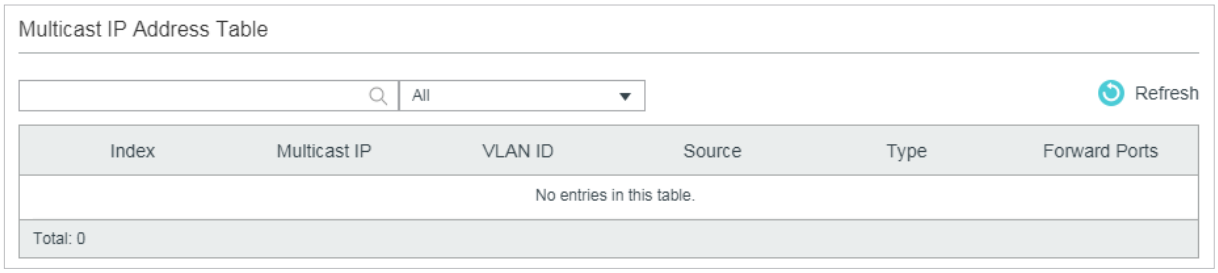


Tabela adresów IP multicast zawiera wszystkie aktualne pozycje IP-VLAN-Port multicast:

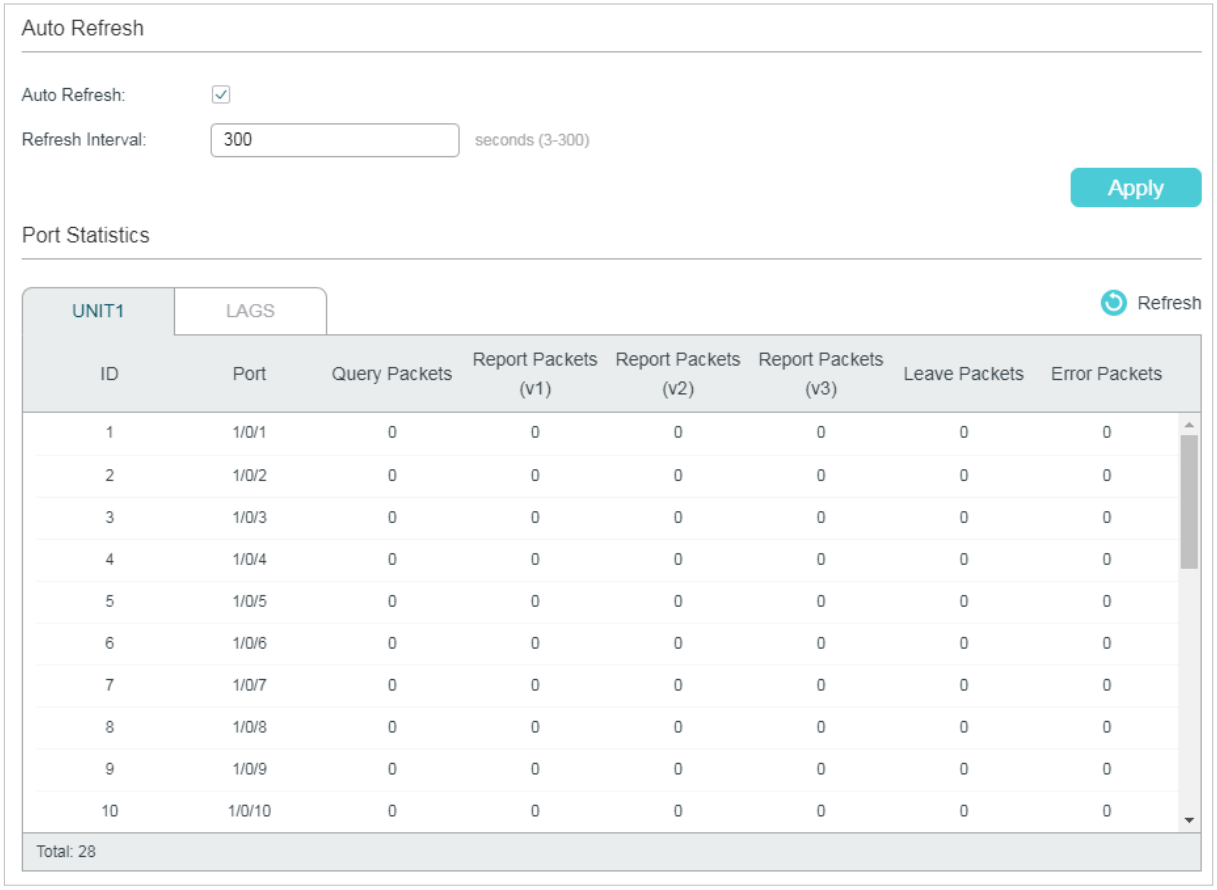
Multicast IP	Źródłowy adres IP multicast.
VLAN ID	ID sieci VLAN, do której przynależy grupa multicastowa.
Source	Źródło wpisu ruchu multicastowego. **IGMP Snooping**: IGMP Snooping uczy się wpisu ruchu multicastowego. **MVR**: MVR uczy się wpisu ruchu multicastowego.

Type	Metody generowania wpisów ruchu multicastowego. **Dynamic**: Wpis jest przyswajany dynamicznie. Wszystkie porty członkowskie dodawane są dynamicznie do grupy multicastowej. **Static**: Wpis jest dodawany ręcznie. Wszystkie porty członkowskie dodawane są ręcznie do grupy multicastowej. **Mix**: Wpis jest przyswajany dynamicznie (lub ręcznie) i niektóre porty członkowskie dodawane są ręcznie (lub dynamicznie) do grupy multicastowej.
Forward Ports	Wszystkie porty grupy multicastowej, w tym porty routera i porty przełącznika.

6.1.2 Przeglądanie statystyk pakietów IPv4 na wszystkich portach

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Statistics**, aby wyświetlić poniższą stronę:

Rys. 6-2 Statystyki pakietów IPv4



Wykonaj poniższe kroki, aby wyświetlić statystyki pakietów IPv4 na każdym porcie:

1) Aby zobaczyć statystyki w czasie rzeczywistym, włącz **Auto Refresh** lub kliknij **Refresh**.

Auto Refresh	Włącz lub wyłącz Auto Refresh. Włączenie opcji spowoduje automatyczne odświeżanie statystyk przez przełącznik.

Refresh Interval	Gdy włączysz **Auto Refresh**, podaj interwał odświeżania statystyk.

2) W sekcji **Port Statistics** możesz przeglądać statystyki pakietów IPv4 na każdym porcie.

Query Packets	Liczba pakietów zapytań odebranych na porcie.
Report Packets (v1)	Liczba pakietów raportów IGMPv1 odebranych na porcie.
Report Packets (v2)	Liczba pakietów raportów IGMPv2 odebranych na porcie.
Report Packets (v3)	Liczba pakietów raportów IGMPv3 odebranych na porcie.
Leave Packets	Liczba pakietów leave odebranych na porcie.
Error Packets	Liczba pakietów error odebranych na porcie.

6.1.3 Przeglądanie tabeli adresów IPv6 multicast

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Table**, aby wyświetlić poniższą stronę:

Rys. 6-3 Tabela adresów IPv6 multicast

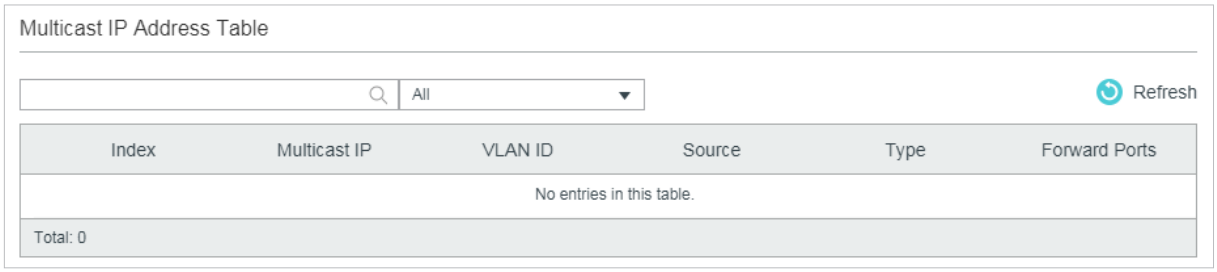


Tabela adresów IP multicast zawiera wszystkie aktualne wpisy IP-VLAN-Port multicast:

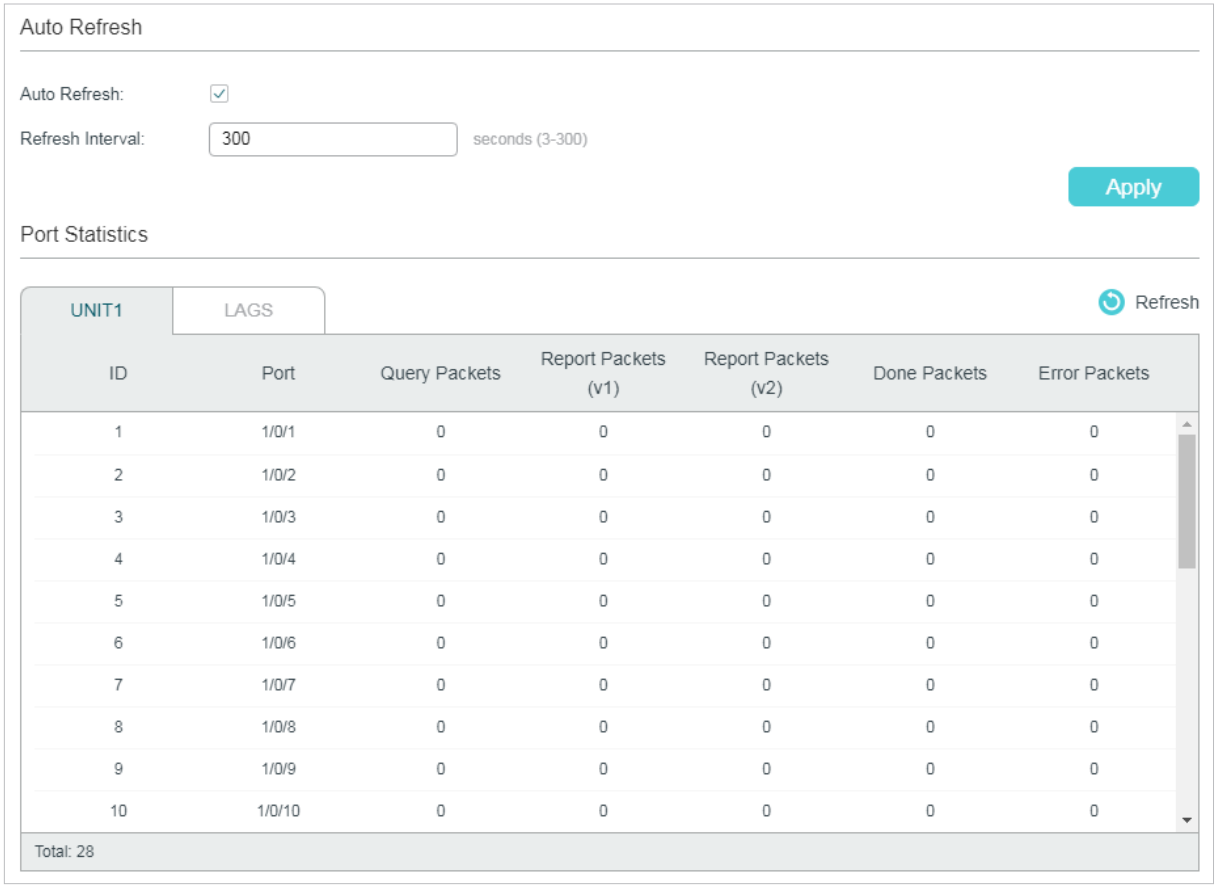
Multicast IP	Źródłowy adres IP multicast.
VLAN ID	ID sieci VLAN, do której przynależy grupa multicastowa.
Source	Źródło wpisu ruchu multicastowego. **MLD Snooping**: MLD Snooping uczy się wpisu ruchu multicastowego.

Type	Metody generowania wpisów ruchu multicastowego. **Dynamic**: Wpis jest przyswajany dynamicznie. Wszystkie porty członkowskie dodawane są dynamicznie do grupy multicastowej. **Static**: Wpis jest dodawany ręcznie. Wszystkie porty członkowskie dodawane są ręcznie do grupy multicastowej. **Mix**: Wpis jest przyswajany dynamicznie (lub ręcznie) i niektóre porty członkowskie dodawane są ręcznie (lub dynamicznie) do grupy multicastowe.
Forward Port	Wszystkie porty grupy multicastowej, w tym porty routera i porty przełącznika.

6.1.4 Przeglądanie statystyk pakietów IPv6 na wszystkich portach

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Statistics,** aby wyświetlić poniższą stronę:

Rys. 6-4 Statystyki pakietów IPv6



Wykonaj poniższe kroki, aby wyświetlić statystyki pakietów IPv6 na każdym porcie:

1) Aby zobaczyć statystyki w czasie rzeczywistym, włącz **Auto Refresh** lub kliknij **Refresh**.

Auto Refresh	Włącz lub wyłącz Auto Refresh. Włączenie opcji spowoduje automatyczne odświeżanie statystyk przez przełącznik.

Refresh Interval	Gdy włączysz **Auto Refresh**, podaj interwał odświeżania statystyk.

2) W sekcji **Port Statistics** możesz przeglądać statystyki pakietów IPv6 na każdym porcie.

Query Packets	Liczba pakietów zapytań odebranych przez port.
Report Packets (v1)	Liczba pakietów raportów MLDv1 odebranych na porcie.
Report Packets (v2)	Liczba pakietów raportów MLDv2 odebranych na porcie.
Done Packets	Liczba pakietów done odebranych na porcie.
Error Packets	Liczba pakietów error odebranych na porcie.

6.2 Przez CLI

6.2.1 Przeglądanie informacji o Multicast Snooping IPv4

show ip igmp snooping groups [vlan *vlan-id* **] [**count | dynamic | dynamic count | static | static count **]**

Polecenie pokazuje informacje o określonych grupach mutlicastowych we wszystkich VLAN-ach lub tylko w wybranych VLAN-ach.

count: Liczba grup multicastowych.

dynamic: Informacje o wszystkich dynamicznych grupach multicastowych.

dynamic count: Liczba dynamicznych grup multicastowych.

static: Informacje o wszystkich statycznych grupach multicastowych.

static count: Liczba statycznych grup multicastowych.

show ip igmp snooping interface [fastEthernet [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **] packet-stat**

Statystyki pakietów na wybranych portach lub na wszystkich portach.

clear ip igmp snooping statistics

Wyczyść statystyki wszystkich pakietów IGMP.

6.2.2 Przeglądanie informacji o Multicast Snooping IPv6

show ipv6 mld snooping groups [vlan *vlan-id* **] [**count | dynamic | dynamic count | static | static count **]**

Polecenie pokazuje informacje o określonych grupach mutlicastowych we wszystkich VLAN-ach lub tylko w wybranych VLAN-ach.

count: Liczba grup multicastowych.

dynamic: Informacje o wszystkich dynamicznych grupach multicastowych.

dynamic count: Liczba dynamicznych grup multicastowych.

static: Informacje o wszystkich statycznych grupach multicastowych.

static count: Liczba statycznych grup multicastowych.

show ipv6 mld snooping interface [fastEthernet [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **] packet-stat**

Statystyki pakietów na wybranych portach lub na wszystkich portach.

clear ipv6 mld snooping statistics

Wyczyść statystyki wszystkich pakietów MLD.

Część 11

Konfiguracja Spanning Tree

ROZDZIAŁY

1 Konfiguracja STP/RSTP

Aby przeprowadzić konfigurację STP/RSTP, postępuj zgodnie z poniższymi krokami:

1) Skonfiguruj parametry STP/RSTP na portach.
2) Skonfiguruj STP/RSTP globalnie.
3) Sprawdź ustawienia STP/RSTP.

Wytyczne konfiguracyjne

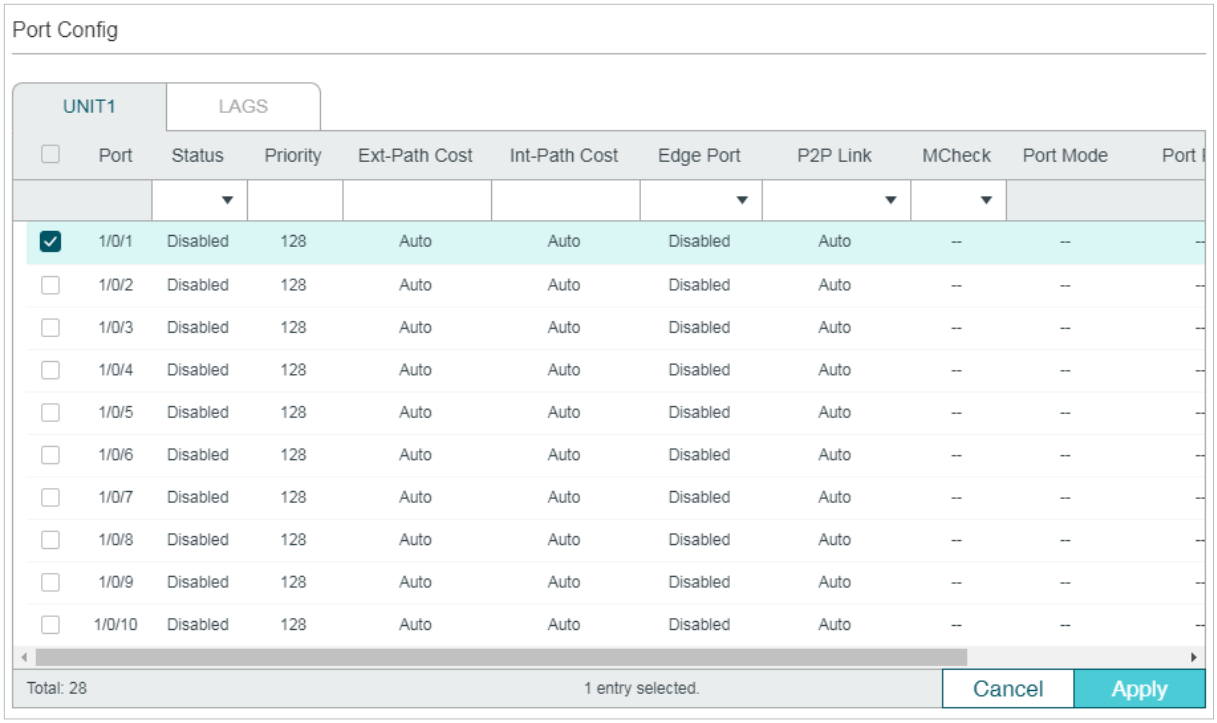
- Przed konfiguracją drzewa rozpinającego (spanning tree) trzeba koniecznie jasno zaznaczyć, jaka rola przypisana jest każdemu przełącznikowi w drzewie rozpinającym.
- Aby zapobiec migotaniu sieci (ang. flapping) spowodowanemu zmianą parametrów STP/RSTP, po skonfigurowaniu odpowiednich parametrów zaleca się globalne włączenie funkcji STP/RSTP.

1.1 Przez GUI

1.1.1 Konfiguracja parametrów STP/RSTP na portach

Wybierz menu **L2 FEATURES > Spanning Tree > Port Config**, aby załadować następującą stronę.

Rys. 1-1 Konfiguracja parametrów STP/RSTP na portach



Aby skonfigurować na portach parametry STP/RSTP, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Port Config** skonfiguruj parametry STP/RSTP na portach.

UNIT	Wybierz właściwą jednostkę lub grupy LAG.
Status	Włącz lub wyłącz funkcję drzewa rozpinającego na wybranym porcie.
Priority	Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240. Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.
Ext-Path Cost	Wpisz wartość kosztu ścieżki zewnętrznej. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika. W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.
Int-Path Cost	Wpisz wartość kosztu ścieżki wewnętrznej. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki wewnętrznej, w zależności od prędkości łącza portu. Ten parametr używany jest jedynie w MSTP, nie trzeba go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP. W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do obliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.
Edge Port	Wybierz Enable, aby ustawić port jako końcowy. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.

P2P Link	Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Dostępne są trzy opcje: Auto, Open(Force) i Closed(Force). Domyślnie ustawiona jest opcja Auto. **Auto**: Przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open(Force)**: Port ustawiony jest jako podłączony do łącza P2P. Najpierw należy sprawdzić łącze. **Close(Force)**: Port ustawiony jest jako niepodłączony do łącza P2P. Najpierw należy sprawdzić łącze..
MCheck	Wybierz, czy na porcie wykonywane będą operacje MCheck. Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enable. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).
Port Mode	Wyświetla tryb drzewa rozpinającego portu. **STP**: Tryb drzewa rozpinającego to STP. **RSTP**: Tryb drzewa rozpinającego to RSTP. **MSTP**: Tryb drzewa rozpinającego to MSTP.
Port Role	Wyświetla rolę portu w drzewie rozpinającym. **Root Port**: Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym. **Designated Port**: Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci. **Alternate Port**: Port jest portem zastępczym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu. **Backup Port**: Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego. **Disabled**: Port nie jest częścią drzewa rozpinającego.

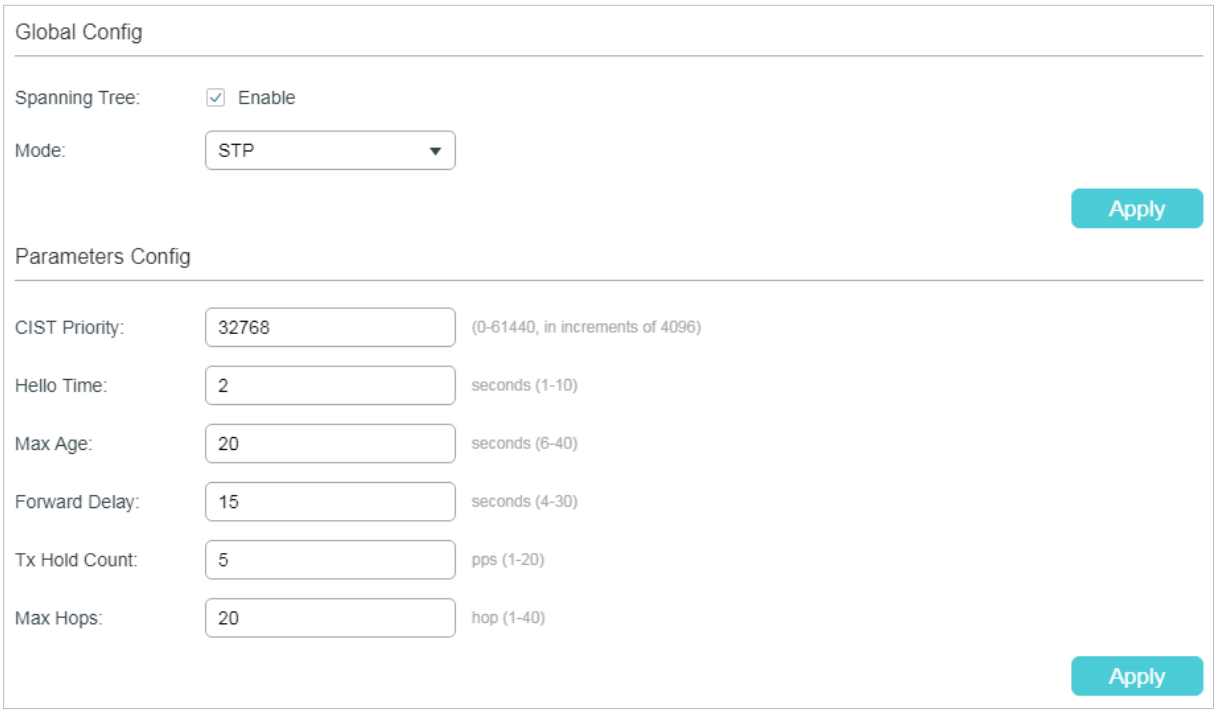
Port Status	Wyświetla stan portu. **Forwarding**: Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika. **Learning**: Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go. **Blocking**: Port jedynie odbiera i wysyła ramki BPDU. **Disconnected**: Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem.
LAG	Wyświetla grupę LAG, do której należy port.

2) Kliknij **Apply**.

1.1.2 Konfiguracja globalna STP/RSTP

Wybierz menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby załadować następującą stronę.

Rys. 1-2 Konfiguracja globalna STP/RSTP



Aby skonfigurować STP/RSTP globalnie, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Parameters Config** skonfiguruj parametry globalne STP/RSTP i kliknij **Apply**.

CIST Priority	Wyznacz priorytet CIST dla przełącznika. Priorytet CIST jest parametrem wykorzystywanym do ustawienia mostu głównego w drzewie rozpinającym. Przełącznik o niższej wartości ma wyższy priorytet. W przypadku STP/RSTP, priorytet CIST jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik o najwyższym priorytecie wybrany zostanie mostem głównym. W przypadku MSTP, priorytet CISP jest priorytetem przełącznika w CIST. Przełącznik z najwyższym priorytetem wybrany zostanie mostem głównym w CIST.
Hello Time	Wyznacz odstęp czasu wysyłania ramek BPDU. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.
Max Age	Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość domyślna to 2.
Forward Delay	Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.
Tx Hold Count	Wyznacz maksymalną liczbę ramek BPDU wysyłanych w jedną sekundę. Wartość domyślna to 5
Max Hops	Wyznacz maksymalną liczbę BPDU wysyłanych w obszar MST. Wartość domyślna to 20. Przełącznik odbiera BPDU, zmniejsza liczbę przeskoków generuje ramki BPDU o nowej wartości. Kiedy wartość przeskoku wyniesie zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w obszarze MST. *Note:* Maks. liczba przeskoków to parametr konfigurowany w MSTP. Nie musisz go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP.

Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

2) W sekcji **Global Config** włącz funkcję drzewa rozpinającego, wybierz tryb STP jako STP/RSTP i kliknij **Apply**.

Spanning Tree	Zaznacz pole, aby włączyć funkcję drzewa rozpinającego globalnie.

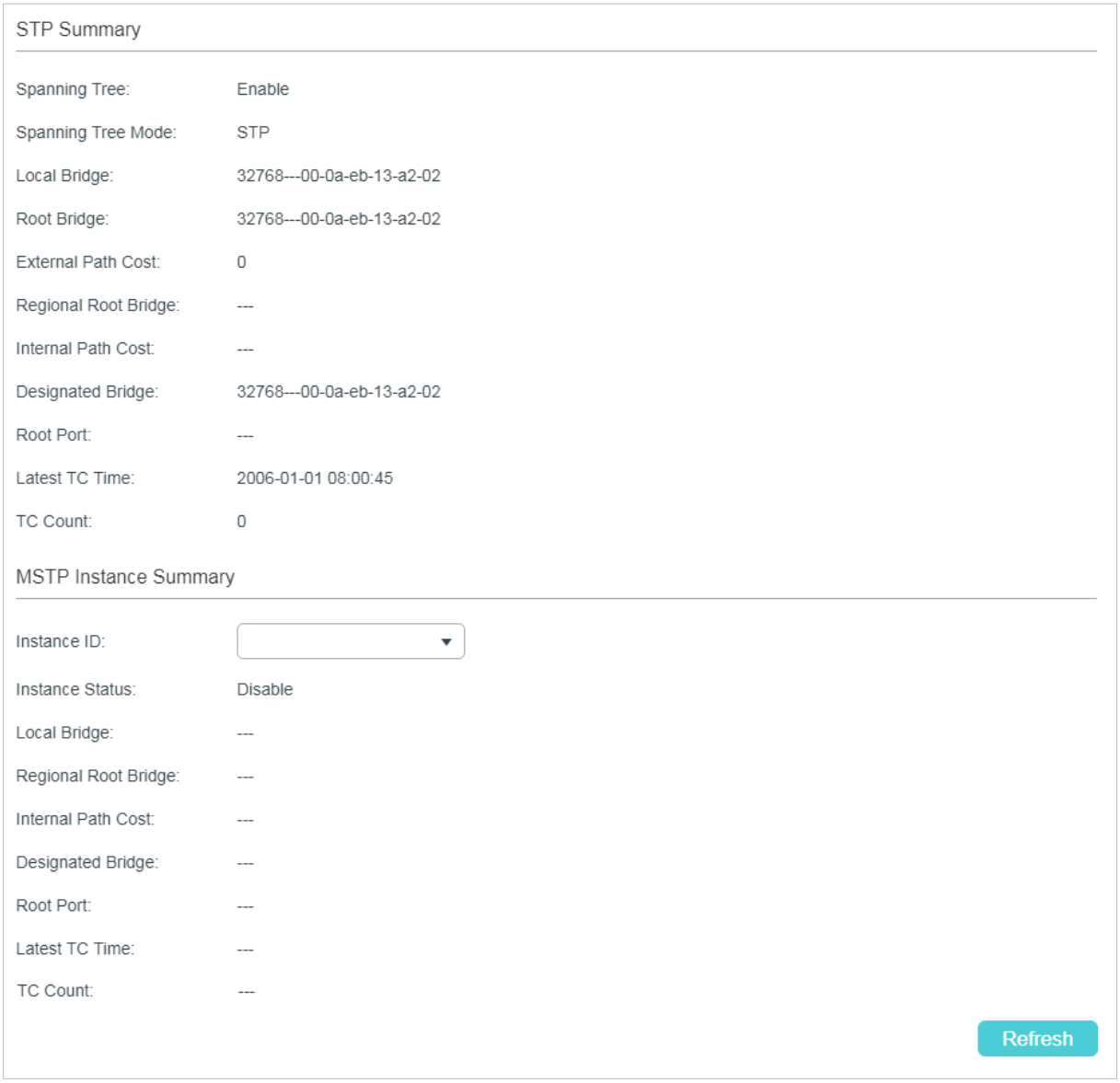
Mode	Ustaw tryb drzewa rozpinającego na STP/RSTP na przełączniku. Domyślnie ustawiony jest tryb STP. **STP**: Ustaw tryb drzewa rozpinającego na STP. **RSTP**: Ustaw tryb drzewa rozpinającego na RSTP. **MSTP**: Ustaw tryb drzewa rozpinającego na MSTP.

1.1.3 Sprawdzanie konfiguracji STP/RSTP

Po zakończeniu całego procesu konfiguracji, sprawdź dane STP/RSTP przełącznika.

Wybierz menu **L2 FEATURES > Spanning Tree > STP Config > STP Summary**, aby załadować następującą stronę.

Rys. 1-3 Sprawdzanie konfiguracji STP/RSTP



Sekcja **STP Summary** przedstawia podsumowanie informacji dotyczących drzewa rozpinającego :

Spanning Tree	Informuje o stanie funkcji drzewa rozpinającego.
Spanning Tree Mode	Informuje o trybie drzewa rozpinającego.
Local Bridge	Informuje o bridge ID mostu lokalnego. Mostem lokalnym jest wykorzystywany przełącznik.
Root Bridge	Informuje o bridge ID mostu głównego.
External Path Cost	Informuje o koszcie ścieżki głównej z przełącznika do mostu głównego.
Regional Root Bridge	To most główny IST. Nie wyświetla się, jeżeli wybrany tryb drzewa rozpinającego to STP/RSTP.
Internal Path Cost	Koszt ścieżki wewnętrznej to koszt ścieki głównej od przełącznika do mostu głównego IST. Nie wyświetla się, jeżeli wybrany tryb drzewa rozpinającego to STP/RSTP.
Designated Bridge	Informuje o bridge ID mostu desygnowanego. Most desygnowany to przełącznik z portami desygnowanymi.
Root Port	Informuje o porcie głównym wykorzystywanego przełącznika.
Latest TC Time	Informuje o ostatnim czasie zmiany topologii.
TC Count	Informuje o tym, ile razy zmieniła się topologia.

1.2 Przez CLI

1.2.1 Konfiguracja parametrów STP/RSTP na portach

Aby skonfigurować parametry STP/RSTP na portach, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**spanning-tree** Włącz funkcję drzewa rozpinającego dla wybranych portów.

Krok 4 **spanning-tree common-config** [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**portfast** { enable | disable }] [**point-to-point** { auto | open | close }]

Skonfiguruj parametry STP/RSTP na wybranym porcie.

pri: Wyznacz Priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16 i mieścić się w zakresie od 0 do 240. Wartość domyślna to 128. Porty z mniejszymi wartościami ma ją wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.

ext-cost: Wyznacz wartość kosztu ścieżki zewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.

W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.

W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.

portfast { enable | disable }: Wybierz Enable (Włącz), aby ustawić port jako końcowy. Funkcja jest domyślnie wyłączona. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.

point-to-point { auto | open | close }: Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Opcja **Auto** oznacza, że przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open wskazuje na to, że** port ustawiony jest jako podłączony do łącza P2P; **Close -** Port ustawiony jest jako niepodłączony do łącza P2P.

Krok 5 **spanning-tree mcheck**

(Opcjonalnie) Przeprowadź MCheck na porcie.

Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enable. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).

Krok 6 **show spanning-tree interface** [**fastEthernet** *port* **| gigabitEthernet** *port* | **ten- gigabitEthernet** *port* **| port-channel** *lagid*] [**edge** | ext-cost | int-cost | mode | p2p | priority | role | state | status]

(Opcjonalnie) Sprawdź dane wszystkich portów lub wybranego portu.

port: Określ numer portu.

lagid: Określ ID grupy LAG.

ext-cost | int-cost | mode | p2p | priority | role | state | status: Pokaż określone informacje.

Krok 7 **end**
Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).

Krok 8 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji drzewa rozpinającego na porcie 1/0/3 i konfigurację priorytetu portu na 32 :

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#spanning-tree

Switch(config-if)#spanning-tree common-config port-priority 32

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A

Role	Status	LAG
N/A	LnkDwn	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja globalna parametrów STP/RSTP

Aby skonfigurować parametry STP/RSTP globalnie na przełączniku, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**spanning-tree priority** *pri* Skonfiguruj priorytet przełącznika. *pri:* Określ priorytet przełącznika. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego drzewa rozpinającego. Przełącznik z niższą wartością ma wyższy priorytet. W przypadku STP/RSTP wartość jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny. W przypadku MSTP wartość jest priorytetem przełącznika w CIST. Przełącznik z wyższym priorytetem zostanie wybrany na most główny w CIST.

Krok 3	**spanning-tree timer** {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]} (Opcjonalnie) Skonfiguruj Forward Delay, Hello Time i Max Age. *forward-time:* Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość powinna wynosić od 4 do 30 s. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay. *hello-time:* Wyznacz wartość Hello Time, czyli odstęp czasu pomiędzy wysyłaniem ramek BPDU. Wartość powinna mieścić się w zakresie miedzy 1 a 10 s. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające. *max-age:* Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość powinna wynosić od 6 do 40 s. Wartość domyślna to 20.
Krok 4	**spanning-tree hold-count** *value* Określ maksymalną liczbę ramek BPDU wysyłanych na sekundę. *value:* Określ maksymalną liczbę pakietów BPDU wysyłanych na sekundę. Wartość powinna wynosić od 1 do 20 p/s. Wartość domyślna to 5.
Krok 5	**show spanning-tree bridge** (Opcjonalnie) Sprawdź parametry globalne STP/RSTP przełącznika.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

Poniższy przykład prezentuje konfigurację priorytetu przełącznika na 36864 i Forward Delay na 12 sekund:

Switch#configure

Switch(config)#spanning-tree priority 36864

Switch(config)#spanning-tree timer forward-time 12

Switch(config)#show spanning-tree bridge

State	Mode	Priority	Hello-Time	Fwd-Time	Max-Age	Hold-Count	Max-Hops
Enable	Rstp	36864	2	12	20	5	20

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Włączanie STP/RSTP globalnie

Aby ustawić tryb drzewa rozpinającego jako STP/RSTP i włączyć funkcję Spanning Tree globalnie, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**spanning-tree mode** { stp | rstp } Ustaw tryb drzewa rozpinającego na STP/RSTP. stp: Ustaw tryb drzewa rozpinającego na STP. rstp: Ustaw tryb drzewa rozpinającego na RSTP .
Krok 3	**spanning-tree** Włącz funkcję drzewa rozpinającego globalnie.
Krok 4	**show spanning-tree active** (Opcjonalnie) Sprawdź dane aktywne STP/RSTP.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji drzewa rozpinającego, konfigurację trybu na RSTP i sprawdzanie ustawień:

Switch#configure

Switch(config)#spanning-tree mode rstp

Switch(config)#spanning-tree

Switch(config)#show spanning-tree active

Spanning tree is enabled

Spanning-tree's mode: RSTP (802.1w Rapid Spanning Tree Protocol)

Latest topology change time: 2006-01-02 10:04:02

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode
Gi1/0/16	Enable	128	200000	200000	No	Yes(auto)	Rstp
Gi1/0/18	Enable	128	200000	200000	No	Yes(auto)	Rstp
Gi1/0/20	Enable	128	200000	200000	No	Yes(auto)	Rstp

Role	Status	LAG
Desg	Fwd	N/A
Desg	Fwd	N/A
Desg	Fwd	N/A

Switch(config)#end

Switch#copy running-config startup-config

2 Konfiguracja MSTP

Aby przeprowadzić konfigurację MSTP, postępuj zgodnie z poniższymi krokami:

1) Skonfiguruj parametry na portach w CIST.
2) Skonfiguruj region MSTP.
3) Skonfiguruj MSTP globalnie.
4) Sprawdź ustawienia MSTP.

Wytyczne konfiguracyjne

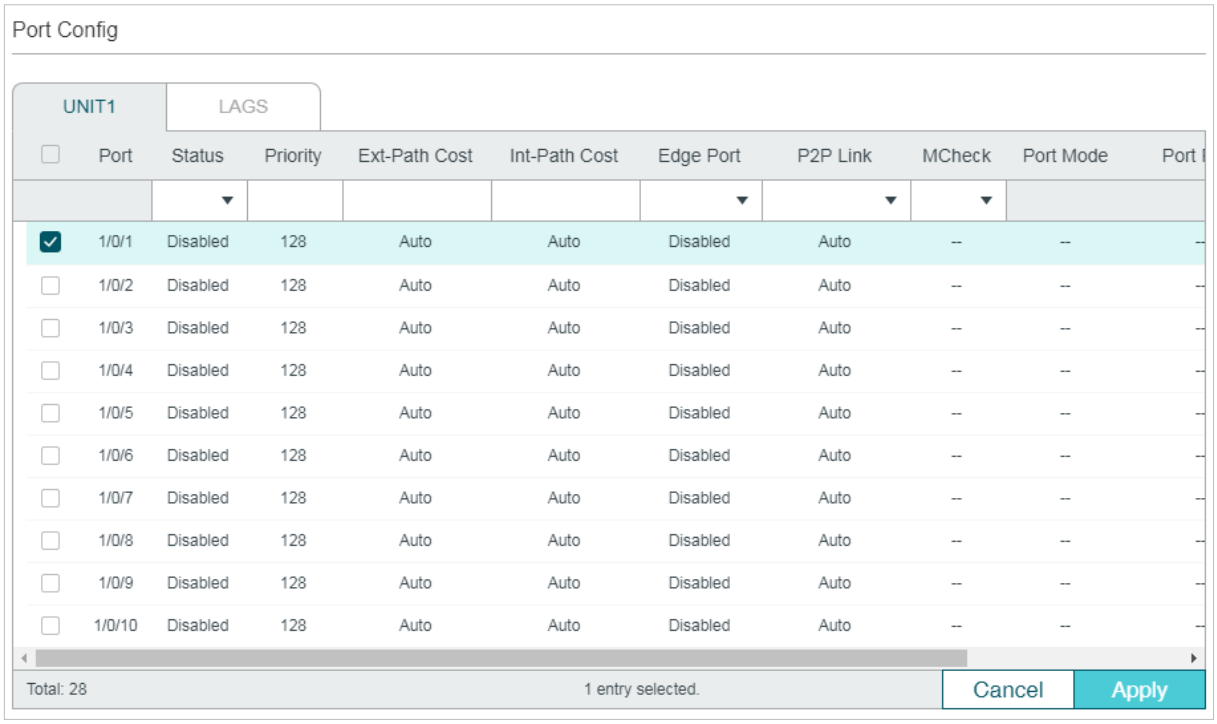
- Przed konfiguracją drzewa rozpinającego (spanning tree) trzeba koniecznie jasno zaznaczyć, jaka rola przypisana jest każdemu przełącznikowi w drzewie rozpinającym.
- Aby zapobiec migotaniu sieci (ang. flapping) spowodowanemu zmianą parametrów MSTP, po skonfigurowaniu odpowiednich parametrów zaleca się globalne włączenie funkcji MSTP.

2.1 Przez GUI

2.1.1 Konfiguracja parametrów na portach w CIST

Wybierz menu **L2 FEATURES > Spanning Tree > Port Config**, aby załadować następującą stronę.

Rys. 2-1 Konfiguracja parametrów na portach



Aby skonfigurować parametry na portach w CIST, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Port Config** skonfiguruj parametry na portach.

UNIT	Wybierz właściwą jednostkę lub grupy LAG.
Status	Włącz lub wyłącz funkcję drzewa rozpinającego na wybranym porcie.
Priority	Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240. Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.
Ext-Path Cost	Wpisz wartość kosztu ścieżki zewnętrznej. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika. W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.
Int-Path Cost	Wpisz wartość kosztu ścieżki wewnętrznej. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki wewnętrznej, w zależności od prędkości łącza portu. Ten parametr używany jest jedynie w MSTP, nie trzeba go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP. W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do obliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.
Edge Port	Wybierz Enable, aby ustawić port jako końcowy. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.

P2P Link	Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Dostępne są trzy opcje: Auto, Open(Force) i Closed(Force). Domyślnie ustawiona jest opcja Auto. **Auto**: Przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open(Force)**: Port ustawiony jest jako podłączony do łącza P2P. Najpierw należy sprawdzić łącze. **Close(Force)**: Port ustawiony jest jako niepodłączony do łącza P2P. Najpierw należy sprawdzić łącze.
MCheck	Wybierz, czy na porcie wykonywane będą operacje MCheck. Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enable. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).
Port Mode	Wyświetla tryb drzewa rozpinającego portu. **STP**: Tryb drzewa rozpinającego to STP. **RSTP**: Tryb drzewa rozpinającego to RSTP. **MSTP**: Tryb drzewa rozpinającego to MSTP.
Port Role	Wyświetla rolę portu w drzewie rozpinającym. **Root Port**: Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym. **Designated Port**: Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci. **Alternate Port**: Port jest portem zastępczym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu. **Backup Port**: Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego. **Disabled**: Port nie jest częścią drzewa rozpinającego.

Port Status	Wyświetla stan portu. **Forwarding**: Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika. **Learning**: Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go. **Blocking**: Port jedynie odbiera i wysyła ramki BPDU. **Disconnected**: Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem.
LAG	Wyświetla grupę LAG, do której należy port.

2) Kliknij **Apply**.

2.1.2 Konfiguracja regionu MSTP

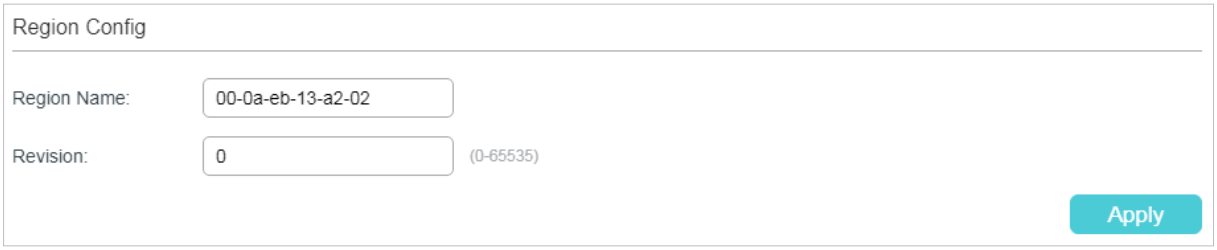
Skonfiguruj nazwę regionu, poziom weryfikacji i mapowanie VLAN do instancji przełącznika. Przełączniki z tą samą nazwą regionu, jednakowym poziomem weryfikacji i mapowaniem VLAN do instancji należą do tego jednego regionu.

Dodatkowo należy skonfigurować priorytet przełącznika oraz priorytet i koszt ścieżki portów w wybranej instancji.

- Konfiguracja nazwy regionu i poziomu weryfikacji

Wybierz menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config**, aby załadować następującą stronę.

Rys. 2-2 Konfiguracja regionu



Aby utworzyć region MST, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Region Config** ustaw nazwę i poziom weryfikacji, aby określić region MSTP.

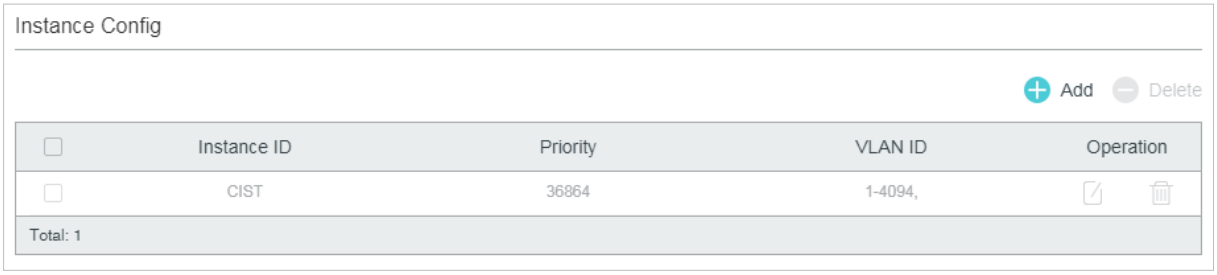
Region Name	Skonfiguruj nazwę regionu MST, używając maks. 32 znaków. Domyślnie nazwą jest adres MAC przełącznika.
Revision	Wprowadź poziom weryfikacji. Wartość domyślna to 0.

2) Kliknij **Apply**.

Konfiguracja mapowania VLAN do instancji i priorytetu przełącznika

Wybierz menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**, aby załadować następującą stronę.

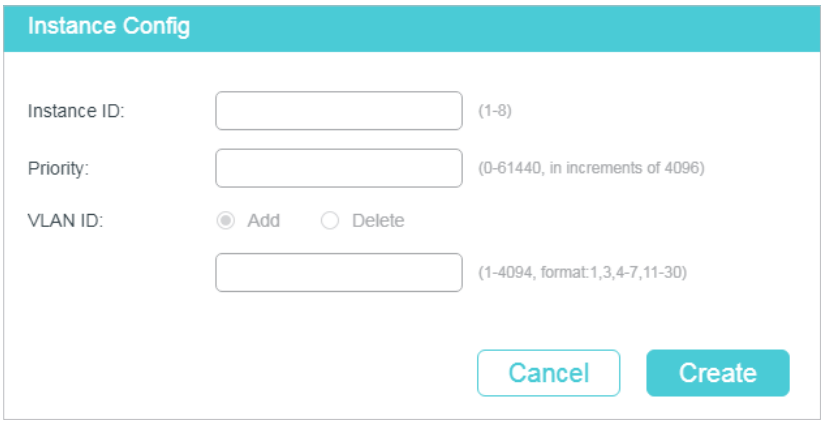
Rys. 2-3 Konfiguracja mapowania VLAN do instancji



Aby mapować VLAN do odpowiedniej instancji i skonfigurować priorytet przełącznika w wybranej instancji, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Instance Config** kliknij **Add** i wpisz ID instancji, Priorytet i odpowiedni VLAN ID.

Rys. 2-4 Konfiguracja instancji



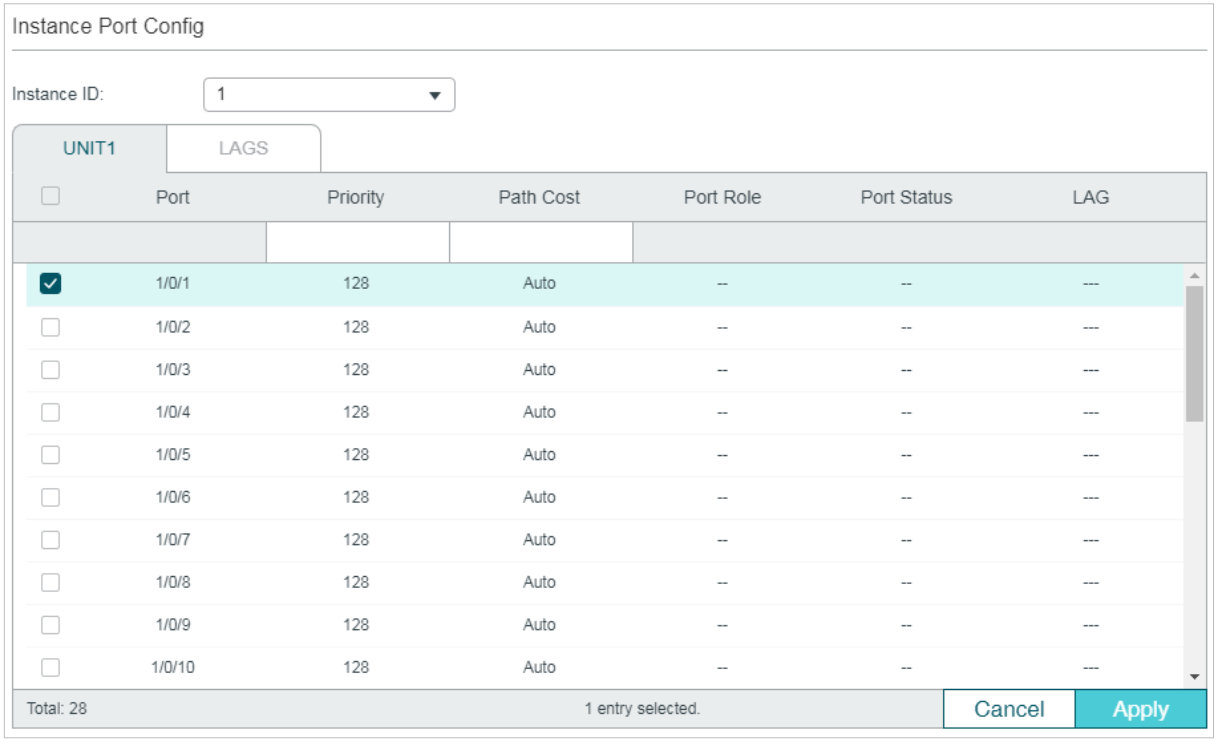
Instance ID	Wprowadź odpowiedni ID instancji.
Priority	Określ priorytet przełącznika w odpowiedniej instancji. Wartość powinna być całkowitą wielokrotnością liczby 4096 i powinna mieścić się w zakresie od 0 do 61440. Priorytet wykorzystywany jest do określania mostu głównego instancji. Przełączniki z niższą wartością mają wyższy priorytet. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny w odpowiadającej instancji.
VLAN ID	Wpisz VLAN ID, aby mapować VLAN do wybranej instancji lub rozwiązać mapowanie VLAN do instancji.

2) Kliknij **Create**.

■ Konfiguracja parametrów na portach w instancji

Wybierz menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config**, aby załadować następującą stronę.

Rys. 2-5 Konfiguracja parametrów portów w instancji



Aby skonfigurować parametry portów w instancji, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Instance Port Config** wybierz odpowiedni ID instancji.

Instance ID	Wybierz numer ID instancji, którą chcesz skonfigurować.

2) Skonfiguruj parametry portu w wybranej instancji.

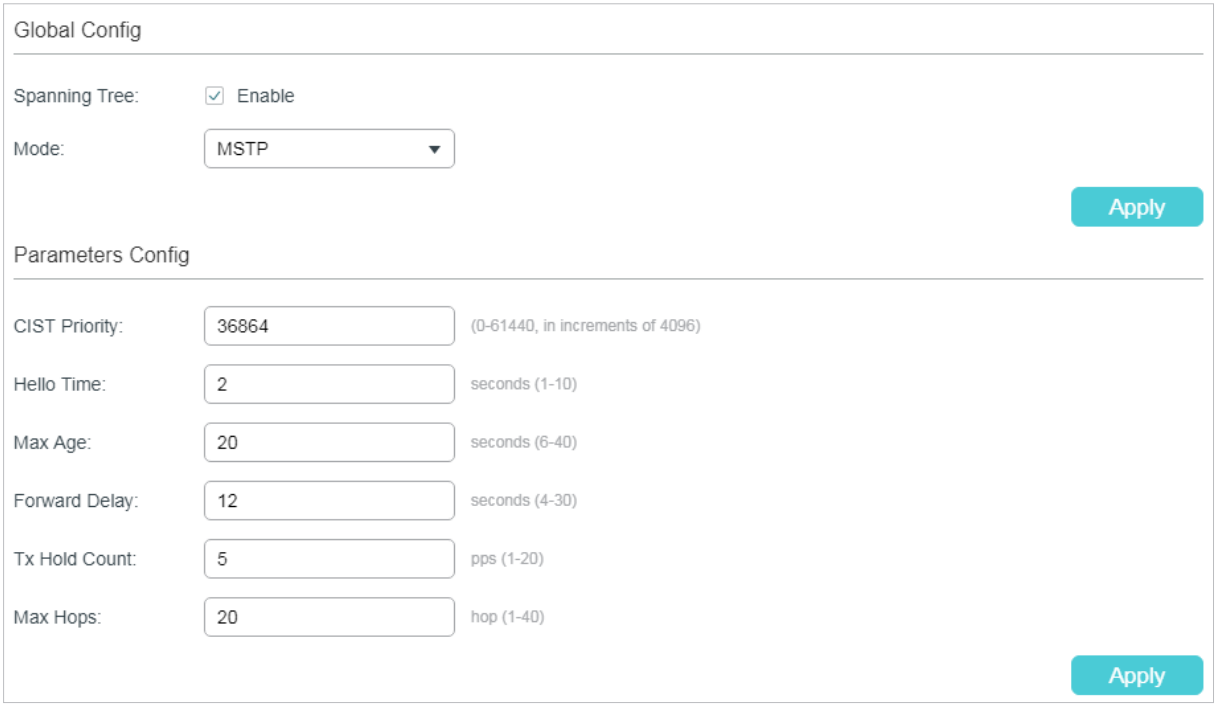
UNIT	Wybierz jednostkę lub grupę LAG do skonfigurowania.
Priority	Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240. Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.
Path Cost	Wpisz wartość kosztu ścieżki w odpowiadającej instancji. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.

Port Role	Wyświetla rolę portu w drzewie rozpinającym. **Root Port**: Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym. **Designated Port**: Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci. **Alternate Port**: Port jest portem zastępczym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu. **Backup Port**: Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego. **Disabled**: Port nie jest częścią drzewa rozpinającego.
Port Status	Wyświetla stan portu. **Forwarding**: Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika. **Learning**: Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go. **Blocking**: Port jedynie odbiera i wysyła ramki BPDU. **Disconnected**: Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem.
LAG	Wyświetla grupę LAG, do której należy port.

2.1.3 Konfiguracja globalna MSTP

Wybierz menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby załadować następującą stronę.

Rys. 2-6 Konfiguracja globalna funkcji MSTP



Aby skonfigurować MSTP globalnie, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Parameters Config** skonfiguruj parametry globalne MSTP i kliknij **Apply**.

CIST Priority	Wyznacz priorytet CIST dla przełącznika. Priorytet CIST jest parametrem wykorzystywanym do ustawienia mostu głównego w drzewie rozpinającym. Przełącznik o niższej wartości ma wyższy priorytet. W przypadku STP/RSTP, priorytet CIST jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik o najwyższym priorytecie wybrany zostanie mostem głównym. W przypadku MSTP, priorytet CISP jest priorytetem przełącznika w CIST. Przełącznik z najwyższym priorytetem wybrany zostanie mostem głównym w CIST.
Hello Time	Wyznacz odstęp czasu wysyłania ramek BPDU. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.
Max Age	Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość domyślna to 20.

Forward Delay	Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.
Tx Hold Count	Wyznacz maksymalną liczbę ramek BPDU wysyłanych w jedną sekundę. Wartość domyślna to 5
Max Hops	Wyznacz maksymalną liczbę BPDU wysyłanych w obszar MST. Wartość domyślna to 20. Przełącznik odbiera BPDU, zmniejsza liczbę przeskoków generuje ramki BPDU o nowej wartości. Kiedy wartość przeskoku wyniesie zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w obszarze MST. Uwaga: Maks. liczba przeskoków to parametr konfigurowany w MSTP. Nie musisz go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP.

Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

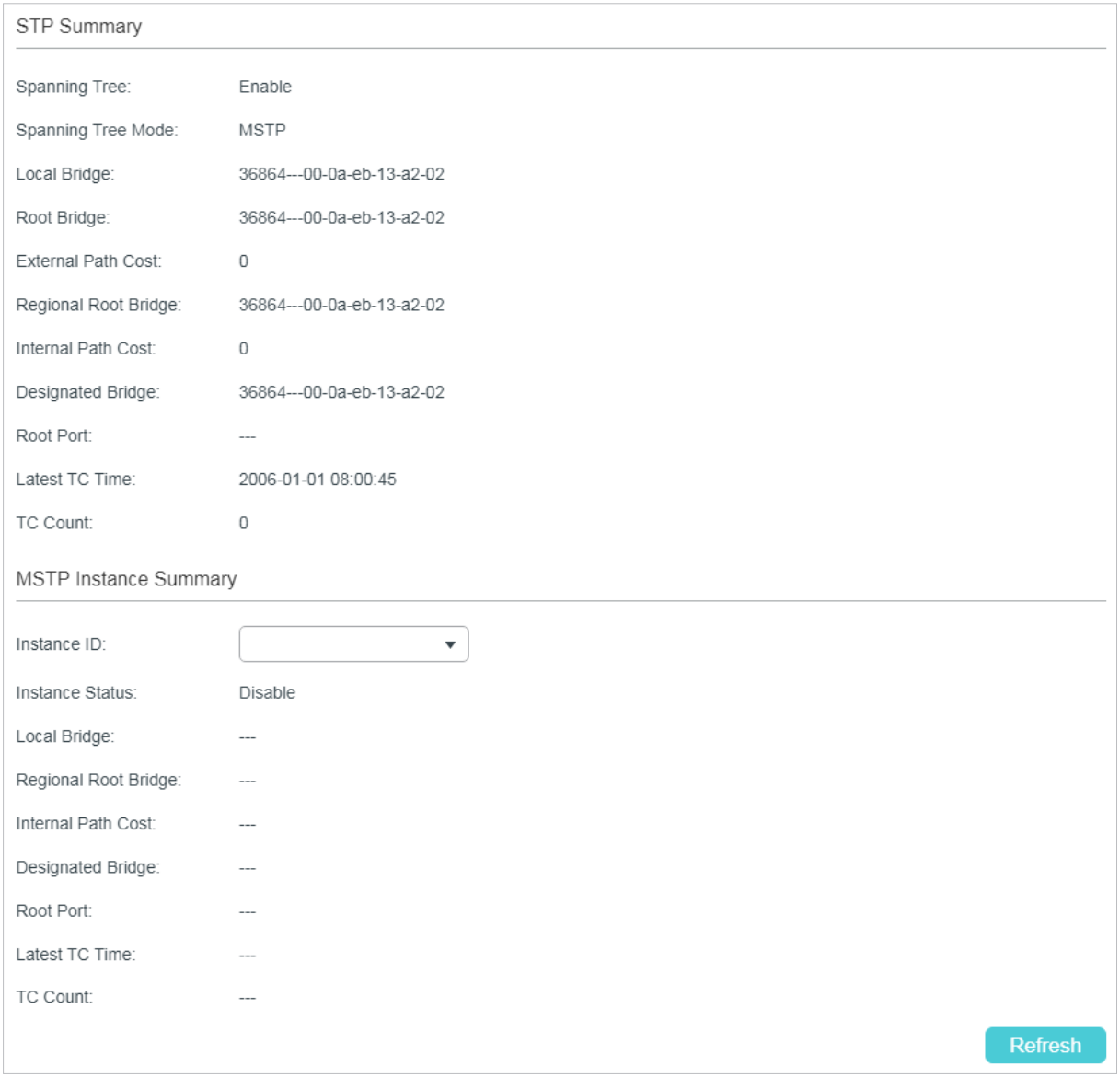
2) W sekcji **Global Config** włącz funkcję Spanning-Tree, wybierz tryb STP jaki MSTP i kliknij **Apply**.

Spanning-Tree	Zaznacz pole, aby włączyć funkcję drzewa rozpinającego globalnie.
Mode	Ustaw tryb drzewa rozpinającego na STP/RSTP na przełączniku. Domyślnie ustawiony jest tryb STP. **STP**: Ustaw tryb drzewa rozpinającego na STP. **RSTP**: Ustaw tryb drzewa rozpinającego na RSTP. **MSTP**: Ustaw tryb drzewa rozpinającego na MSTP.

2.1.4 Sprawdzanie konfiguracji MSTP

Wybierz menu **Spanning Tree > STP Config > STP Summary**, aby załadować następującą stronę.

Rys. 2-7 Sprawdzanie konfiguracji MSTP



Sekcja **STP Summary** przedstawia podsumowanie informacji dotyczących CIST:

Spanning Tree	Informuje o stanie funkcji drzewa rozpinającego.
Spanning-Tree Mode	Informuje o trybie drzewa rozpinającego.
Local Bridge	Informuje o bridge ID mostu lokalnego. Mostem lokalnym jest wykorzystywany przełącznik.
Root Bridge	Informuje o bridge ID mostu głównego w CIST.
External Path Cost	Informuje o koszcie ścieżki głównej z przełącznika do mostu głównego w CIST.

Regional Root Bridge	Informuje o bridge ID mostu głównego w IST.
Internal Path Cost	Informuje o koszcie ścieżki wewnętrznej. Jest to koszt ścieżki głównej z wykorzystywanego przełącznika do mostu głównego w IST.
Designated Bridge	Informuje o bridge ID mostu desygnowanego w CIST.
Root Port	Informuje o porcie głównym w CIST.
Latest TC Time	Informuje o ostatnim czasie zmiany topologii.
TC Count	Informuje o tym, ile razy zmieniła się topologia.

Sekcja **MSTP Instance Summary** przedstawia dane w instancjach MST:

Instance ID	Wybierz odpowiednią instancję.
Instance Status	Informuje o statusie wybranej instancji.
Local Bridge	Informuje o bridge ID przełącznika lokalnego. Most lokalny to wykorzystywany przełącznik.
Regional Root Bridge	Informuje o bridge ID mostu głównego w wybranej instancji.
Internal Path Cost	Informuje o koszcie ścieżki wewnętrznej. Jest to koszt ścieżki głównej z wykorzystywanego przełącznika to głównego mostu regionalnego.
Designated Bridge	Informuje o bridge ID mostu desygnowanego w wybranej instancji.
Root Port	Informuje o porcie głównym wybranej instancji.
Latest TC Time	Informuje o ostatnim czasie zmiany topologii.
TC Count	Informuje o tym, ile razy zmieniła się topologia.

2.2 Przez CLI

2.2.1 Konfiguracja parametrów na portach w CIST

Aby skonfigurować parametry portu w CIST, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.

Krok 3 **spanning-tree**

Włącz funkcję drzewa rozpinającego dla wybranych portów.

Krok 4 **spanning-tree common-config** [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**int-cost** *int-cost*][**portfast** { enable | disable }] [**point-to-point** { auto | open | close }]

Skonfiguruj parametry na portach w CIST.

pri: Wyznacz Priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16 i mieścić się w zakresie od 0 do 240. Wartość domyślna to 128. Porty z mniejszymi wartościami ma ją wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.

ext-cost: Wyznacz wartość kosztu ścieżki zewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.

W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.

W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.

int-cost: Wyznacz wartość kosztu ścieżki wewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Parametr ten stosuje się jedynie w MSTP.

W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do wyliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.

portfast { enable | disable }*:* Wybierz Enable (Włącz), aby ustawić port jako końcowy. Funkcja jest domyślnie wyłączona. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.

point-to-point { auto | open | close }*:* Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Opcja **Auto** oznacza, że przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open wskazuje na to, że** port ustawiony jest jako podłączony do łącza P2P; **Close -** Port ustawiony jest jako niepodłączony do łącza P2P.

Krok 5 **spanning-tree mcheck**

(Opcjonalnie) Przeprowadź MCheck na porcie.

Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enable. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).

Krok 6	**show spanning-tree interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *lagid*] [**edge |** ext-cost | int-cost | mode | p2p | priority | role | state | status] (Opcjonalnie) Sprawdź dane wszystkich portów lub wybranego portu. *port:* Określ numer portu. *lagid:* Określ ID grupy LAG. ext-cost | int-cost | mode | p2p | priority | role | state | status: Pokaż określone informacje.
Krok 7	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji Spanning Tree dla portu 1/0/3 i konfigurację priorytetu portu na 32 :

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#spanning-tree

Switch(config-if)#spanning-tree common-config port-priority 32

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

MST-Instance 0 (CIST)

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn

MST-Instance 5

Interface	Prio	Cost	Role	Status
Gi1/0/3	144	200	N/A	LnkDwn

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja regionu MSTP

Konfiguracja regionu MST

Aby skonfigurować region MST i priorytet przełącznika w instancji, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**spanning-tree mst instance** *instance-id* **priority** *pri* Skonfiguruj priorytet przełącznika w instancji. *instance-id*: **Określ** ID instancji. Wartość powinna wynosić od 1 do 8. *pri*: Określ priorytet przełącznika w odpowiadającej instancji. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego instancji. Przełącznik z niższą wartością ma wyższy priorytet, a przełącznik z najwyższym priorytetem zostanie wybrany na most główny w odpowiadającej instancji.
Krok 3	**spanning-tree mst configuration** Wejdź w tryb konfiguracji MST, żeby skonfigurować mapowanie VLAN do instancji, nazwę regionu i poziom weryfikacji.
Krok 4	**name** *name* Skonfiguruj nazwę regionu. *name*: Określ nazwę regionu, wykorzystywaną do identyfikacji regionu MST. Wartość musi zawierać od 1 do 32 znaków.
Krok 5	**revision** *revision* Skonfiguruj poziom weryfikacji regionu. *revision:* Określ poziom weryfikacji regionu. Wartość powinna mieścić się w zakresie od 0 do 65535.
Krok 6	**instance** *instance-id* **vlan** *vlan-id* Skonfiguruj mapowanie VLAN do instancji. *instance-id*: Określ ID instancji. Wartość powinna wynosić od 1 do 8. *vlan-id*: **Określ** VLAN mapowaną do odpowiedniej instancji.
Krok 7	**show spanning-tree mst** { **configuration** [digest] | **instance** *instance-id* [**interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *lagid* | **ten-gigabitEthernet** *port*]] } (Opcjonalnie) Podejrzyj powiązane dane instancji MSTP. *digest*: **Zaznacz wyświetlanie skrótu wyliczonego przez mapę VLAN do instancji**. *instance-id*: **Określ instancję** ID, którą chcesz wyświetlić, w zakresie od 1 do 8. *port:* Określ numer portu. *lagid:* Określ numer ID grupy LAG.

Krok 8	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie regionu MST o nazwie R1, poziomie weryfikacji 100, w którym VLAN 2-VLAN 6 są mapowane do instancji 5:

Switch#configure

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#name R1

Switch(config-mst)#revision 100

Switch(config-mst)#instance 5 **vlan** 2-6

Switch(config-mst)#show spanning-tree mst configuration

Region-Name : R1

Revision : 100

MST-Instance Vlans-Mapped

---------- ----------

0 1,7-4094

5 2-6,

Switch(config-mst)#end

Switch#copy running-config startup-config

■ Konfiguracja parametrów na portach w instancji

Aby skonfigurować priorytet i koszt ścieżki portów w określonej instancji, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.

Krok 3	**spanning-tree mst instance** *instance-id* **{[port-priority** *pri* **]	[cost** *cost* **]}** Skonfiguruj priorytet i koszt ścieżki portów w wyznaczonej instancji. *instance-id:* Określ ID instancji, wartość powinna wynosić od 1 do 8. *pri:* Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240. Wartość domyślna to128. Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem. *cost:* Wpisz wartość kosztu ścieżki w odpowiadającej instancji. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.
Krok 4	**show spanning-tree mst** { **configuration** [digest]	**instance** *instance-id* [**interface** [**fastEthernet** *port*	**gigabitEthernet** *port*	**port-channel** *lagid*	**ten-gigabitEthernet** *port*]] } (Opcjonalnie) Podejrzyj powiązane dane instancji MSTP. *digest:* **Zaznacz wyświetlanie skrótu wyliczonego przez mapę VLAN do instancji**. *instance-id:* Określ ID instancji, którą chcesz wyświetlić, w zakresie od 1 do 8. *port:* Określ numer portu. *lagid:* Określ ID grupy LAG.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację priorytetu na 144, kosztu ścieżki portu1/0/3 na 200 w instancji 5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#spanning-tree mst instance 5 **port-priority** 144 **cost** 200

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

MST-Instance 0 (CIST)

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status	LAG
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn	N/A

MST-Instance 5

Interface	Prio	Cost	Role	Status	LAG
Gi1/0/3	144	200	N/A	LnkDwn	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Konfiguracja globalna parametrów MSTP

Aby skonfigurować globalnie parametry MSTP przełącznika, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**spanning-tree priority** *pri* Skonfiguruj priorytet przełącznika dla porównania w CIST. *pri:* Określ priorytet przełącznika. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego drzewa rozpinającego. Przełącznik z niższą wartością ma wyższy priorytet. W przypadku STP/RSTP wartość jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny. W przypadku MSTP wartość jest priorytetem przełącznika w CIST. Przełącznik z wyższym priorytetem zostanie wybrany na most główny w CIST.
Krok 3	**spanning-tree timer** {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]} (Opcjonalnie) Skonfiguruj Forward Delay, Hello Time i Max Age. *forward-time:* Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość powinna wynosić od 4 do 30 s. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay. *hello-time:* Wyznacz wartość Hello Time, czyli odstęp czasu pomiędzy wysyłaniem ramek BPDU. Wartość powinna mieścić się w zakresie miedzy 1 a 10 s. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające. *max-age:* Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość powinna wynosić od 6 do 40 s. Wartość domyślna to 20.
Krok 4	**spanning-tree hold-count** *value* Określ maksymalną liczbę ramek BPDU wysyłanych na sekundę. *value:* Określ maksymalną liczbę pakietów BPDU wysyłanych na sekundę. Wartość powinna wynosić od 1 do 20 p/s. Wartość domyślna to 5.

Krok 5	**spanning-tree max-hops** *value* (Opcjonalnie) Wyznacz maksymalną liczbę przeskoków BPDU przesyłanych w region MST. Przełącznik odbiera BPDU, obniża liczbę przeskoków i generuje BPDU z nową wartością. Jeżeli przeskok osiągnie wartość zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w regionie MST. *value:* Określ maks. liczbę przeskoków pojawiających się w określonym regionie przed odrzuceniem BPDU. Wartość powinna wynosić od 1 do 40 w przeskoku, wartość domyślna to 20.
Krok 6	**show spanning-tree bridge** (Opcjonalnie) Sprawdź parametry globalne przełącznika.
Krok 7	**end** Wejdź w tryb użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami.

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

Poniższy przykład prezentuje konfigurację priorytetu CIST na 36864, Forward Delay na 12 sekund, Hold Count na 8 i Max Hop na 25:

Switch#configure

Switch(config)#spanning-tree priority 36864

Switch(config-if)#spanning-tree timer forward-time 12

Switch(config-if)#spanning-tree hold-count 8

Switch(config-if)#spanning-tree max-hops 25

Switch(config-if)#show spanning-tree bridge

State	Mode	Priority	Hello-Time	Fwd-Time	Max-Age	Hold-Count	Max-Hops
Enable	Mstp	36864	2	12	20	8	25

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Włączanie globalne funkcji Spanning Tree

Aby skonfigurować tryb drzewa rozpinającego (spanning tree mode) na MSTP i włączyć funkcję drzewa rozpinającego globalnie, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**spanning-tree mode** mstp Skonfiguruj tryb drzewa rozpinającego na MSTP. *mstp:* Określ tryb drzewa rozpinającego jako MSTP.
Krok 3	**spanning-tree** Włącz funkcję drzewa rozpinającego globalnie.
Krok 4	**show spanning-tree active** (Opcjonalnie) Podejrzyj dane aktywne MSTP.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację trybu drzewa rozpinającego na MSTP i globalne włączanie funkcji Spanning Tree:

Switch#configure

Switch(config)#spanning-tree mode mstp

Switch(config)#spanning-tree

Switch(config)#show spanning-tree active

Spanning tree is enabled

Spanning-tree's mode: MSTP (802.1s Multiple Spanning Tree Protocol)

Latest topology change time: 2006-01-04 10:47:42

MST-Instance 0 (CIST)

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

External Cost : 200000

Root Port : Gi/0/20

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

Regional Root Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

Local bridge is the regional root bridge

Local Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi/0/16	Enable	128	200000	200000	No	Yes(auto)	Mstp	Altn	Blk
Gi/0/20	Enable	128	200000	200000	No	Yes(auto)	Mstp	Root	Fwd

MST-Instance 1

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Interface	Prio	Cost	Role	Status
Gi/0/16	128	200000	Altn	Blk
Gi/0/20	128	200000	Mstr	Fwd

Switch(config)#end

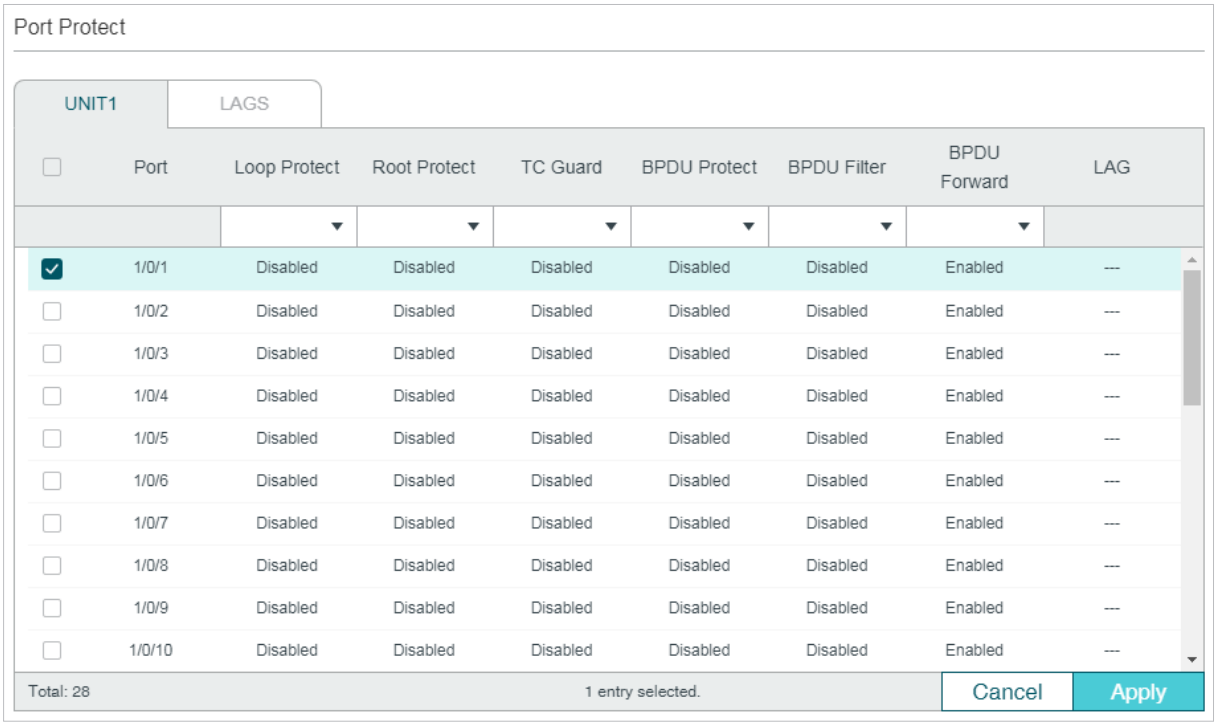
Switch#copy running-config startup-config

3 Konfiguracja ochrony STP

3.1 Przez GUI

Wybierz menu **L2 FEATURES > Spanning Tree > STP Security**, aby załadować następującą stronę.

Rys. 3-1 Konfiguracja ochrony portu



Skonfiguruj funkcje ochrony portów na wybranych portach i kliknij **Apply**.

UNIT	Wybierz jednostkę lub grupy LAG, które chcesz skonfigurować.
Loop Protect	Włącz lub wyłącz Loop Protect. Zaleca się włączenie funkcji na portach głównych i portach zastępczych. W przypadku przeciążenia lub usterek łącza w sieci przełącznik nie odbierze ramek BPDU z urządzeń upstream na czas. Funkcja Loop Protect służy do unikania pętli spowodowanych przeliczeniem w danej sytuacji. Przy włączonej funkcji Loop Protect port będzie czasowo przechodził w stan blokowania, po tym jak nie otrzyma ramek BPDU na czas.

Root Protect	Włącz lub wyłącz Root Protect. Zaleca się włączenie funkcji na portach desygnowanych mostu głównego. Przełączniki z błędnymi ustawieniami mogą produkować BPDU z wyższym priorytetem, niż BPDU mostu głównego, co będzie skutkowało ponownym przeliczeniem drzewa rozpinającego. Funkcja Root Protect pozwala zapewnić, że wybrany most główny nie straci swojej pozycji w powyższym scenariuszu. Przy włączonej funkcji port będzie czasowo przechodził w stan blokowania po otrzymaniu BDPU z wyższym priorytetem. Po dwóch opóźnieniach przekazywania, jeżeli port nie otrzyma innych BDPU z wysokim priorytetem, przejdzie w normalny stan.
TC Guard	Włącz lub wyłącz funkcję TC Guard. Zaleca się włączenie funkcji na portach i przełącznikach, które nie są przełącznikami głównymi. Funkcja TC Guard służy do zapobiegania częstym zmianom tablicy adresów MAC przez przełącznik. Przy włączonej funkcji jeżeli przełącznik otrzyma TC-BPDU, nie będzie ich od razu przetwarzał. Przełącznik odczeka przez ustalony czas i przetworzy wszystkie TC-BPDU razem, po odebraniu pierwszego pakietu TC-BPDU, a następnie zresetuje czas.
BPDU Protect	Włącz lub wyłącz BPDU Protect. Zaleca się włączenie funkcji na portach końcowych. Porty końcowe w drzewie rozpinającym służą do łączenia się z urządzeniami końcowymi i, w standardowej sytuacji, nie otrzymują pakietów BPDU. Otrzymywanie BPDU przez porty końcowe może wskazywać na atak. Funkcja BPDU Protect służy do ochrony przełącznika przed takim zagrożeniem. Przy włączonej funkcji porty końcowe po otrzymaniu pakietu BPDU będą odrzucane, a sytuacja zostanie zaraportowana administratorowi. Jedynie administrator może przywrócić poprzedni stan portów.
BPDU Filter	Włącz lub wyłącz BPDU Filter. Zaleca się włączenie funkcji na portach końcowych. Przy włączonej funkcji BPDU filter port nie odbiera i nie przekazuje pakietów BPDU, ale rozsyła własne BPDU. BPDU Filter pozwala zapobiegać atakom na przełącznik (tak samo, jak funkcja BPDU Protect).
BPDU Forward	Opcjonalnie) Włącz funkcję BPDU Forward. Funkcja działa jedynie przy globalnym wyłączeniu funkcji drzewa rozpinającego. Przy włączonej funkcji BPDU forward, mimo wyłączonej funkcji Spanning Tree, port może nadal przesyłać BPDU drzewa rozpinającego.

3.2 Przez CLI

3.2.1 Konfiguracja ochrony STP

Aby skonfigurować dla portów funkcje Root protect, BPDU protect i BPDU filter, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**spanning-tree guard loop** (Opcjonalnie) Włącz Loop Protect. Zaleca się włączenie funkcji na potrach głównych i zastępczych. W przypadku przeciążenia lub usterek łącza w sieci przełącznik nie odbierze ramek BPDU z urządzeń upstream na czas. Funkcja Loop Protect służy do unikania pętli spowodowanych przeliczeniem w danej sytuacji. Przy włączonej funkcji Loop Protect port będzie czasowo przechodził w stan blokowania, po tym jak nie otrzyma ramek BPDU na czas.
Krok 4	**spanning-tree guard root** (Opcjonalnie) Włącz Root Protect. Zaleca się włączenie funkcji na portach desygnowanych mostu głównego. Przełączniki z błędnymi ustawieniami mogą produkować BPDU z wyższym priorytetem, niż BPDU mostu głównego, co będzie skutkowało ponownym przeliczeniem drzewa rozpinającego. Funkcja Root Protect pozwala zapewnić, że wybrany most główny nie straci swojej pozycji w powyższym scenariuszu. Przy włączonej funkcji port będzie czasowo przechodził w stan blokowania po otrzymaniu BDPU z wyższym priorytetem. Po dwóch opóźnieniach przekazywania, jeżeli port nie otrzyma innych BDPU z wysokim priorytetem, przejdzie w normalny stan.
Krok 5	**spanning-tree guard tc** (Opcjonalnie) Włącz TC Guard. Zaleca się włączenie funkcji na portach i przełącznikach, które nie są przełącznikami głównymi. Funkcja TC Guard służy do zapobiegania częstym zmianom tablicy adresów MAC przez przełącznik. Przy włączonej funkcji jeżeli przełącznik otrzyma TC-BPDU, nie będzie ich od razu przetwarzał. Przełącznik odczeka przez ustalony czas i przetworzy wszystkie TC-BPDU razem, po odebraniu pierwszego pakietu TC-BPDU, a następnie zresetuje czas.
Krok 6	**spanning-tree bpduguard** (Opcjonalnie) Włącz BPDU Protect. Zaleca się włączenie funkcji na portach końcowych. Porty końcowe w drzewie rozpinającym służą do łączenia się z urządzeniami końcowymi i, w standardowej sytuacji, nie otrzymują pakietów BPDU. Otrzymywanie BPDU przez porty końcowe może wskazywać na atak. Funkcja BPDU Protect służy do ochrony przełącznika przed takim zagrożeniem. Przy włączonej funkcji porty końcowe po otrzymaniu pakietu BPDU będą odrzucane, a sytuacja zostanie zaraportowana administratorowi. Jedynie administrator może przywrócić poprzedni stan portów.

Krok 7	**spanning-tree bpdufilter** (Opcjonalnie) Włącz lub wyłącz BPDU Filter. Zaleca się włączenie funkcji na portach końcowych. Przy włączonej funkcji BPDU filter port nie odbiera i nie przekazuje pakietów BPDU, ale rozsyła własne BPDU. BPDU Filter pozwala zapobiegać atakom na przełącznik (tak samo, jak funkcja BPDU Protect).
Krok 8	**spanning-tree bpduflood** (Opcjonalnie) Włącz funkcję BPDU Forward. Funkcja działa jedynie przy globalnym wyłączeniu funkcji drzewa rozpinającego. Funkcja jest domyślnie włączona. Przy włączonej funkcji BPDU forward, mimo wyłączonej funkcji Spanning Tree, port może nadal przesyłać BPDU drzewa rozpinającego.
Krok 9	**show spanning-tree interface-security** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*] [bpdufilter | bpduguard | bpduflood | loop | root | tc] (Opcjonalnie) Sprawdź dane ochrony portów. *port:* Określ numer portu. *lagid:* Określ ID grupy LAG.
Krok 10	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji Loop Protect, Root Protect, BPDU Filter i BPDU Protect na porcie 1/0/3:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#spanning-tree guard loop

Switch(config-if)#spanning-tree guard root

Switch(config-if)#spanning-tree bpdufilter

Switch(config-if)#spanning-tree bpduguard

Switch(config-if)#show spanning-tree interface-security gigabitEthernet 1/0/3

Interface	BPDU-Filter	BPDU-Guard	Loop-Protect	Root-Protect	TC-Protect	BPDU-Flood
Gi1/0/3	Enable	Enable	Enable	Enable	Disable	Enable

Switch(config-if)#end

Switch#copy running-config startup-config

Część 12

Konfiguracja LLDP

ROZDZIAŁY

1 LLDP

1.1 Obsługiwane funkcje

Przełącznik obsługuje protokoły LLDP i LLDP-MED.

Protokół LLDP umożliwia urządzeniom lokalnym kapsułkowanie swoich adresów zarządzania, ID i innych informacji do jednostki danych LLDP (LLDPDU) i okresowe rozgłaszanie tej LLDPDU urządzeniom sąsiadującym. Urządzenia te przechowują otrzymane LLDPDU w standardowych bazach danych MIB (Management Information Base), co umożliwia dostęp do tych informacji poprzez NMS (Network Management System) za pomocą protokołu zarządzania, takiego jak SNMP (Simple Network Management Protocol).

LLDP-MED umożliwia urządzeniom sieciowym przesyłanie swoich informacji, w tym m. in. o Auto VoIP, czy też o pojemności PoE (Power over Ethernet), do urządzeń końcowych (np. telefonów IP) w celu automatycznej konfiguracji. Urządzenia końcowe odbierają informacje o Auto VoIP, kończą proces automatycznej konfiguracji i przesyłają ruch głosowy z żądaną konfiguracją, co może zapewnić preferencyjne traktowanie tego ruchu głosowego.

2 Konfiguracja LLDP

Wykonaj poniższe kroki, aby skonfigurować funkcję LLDP:

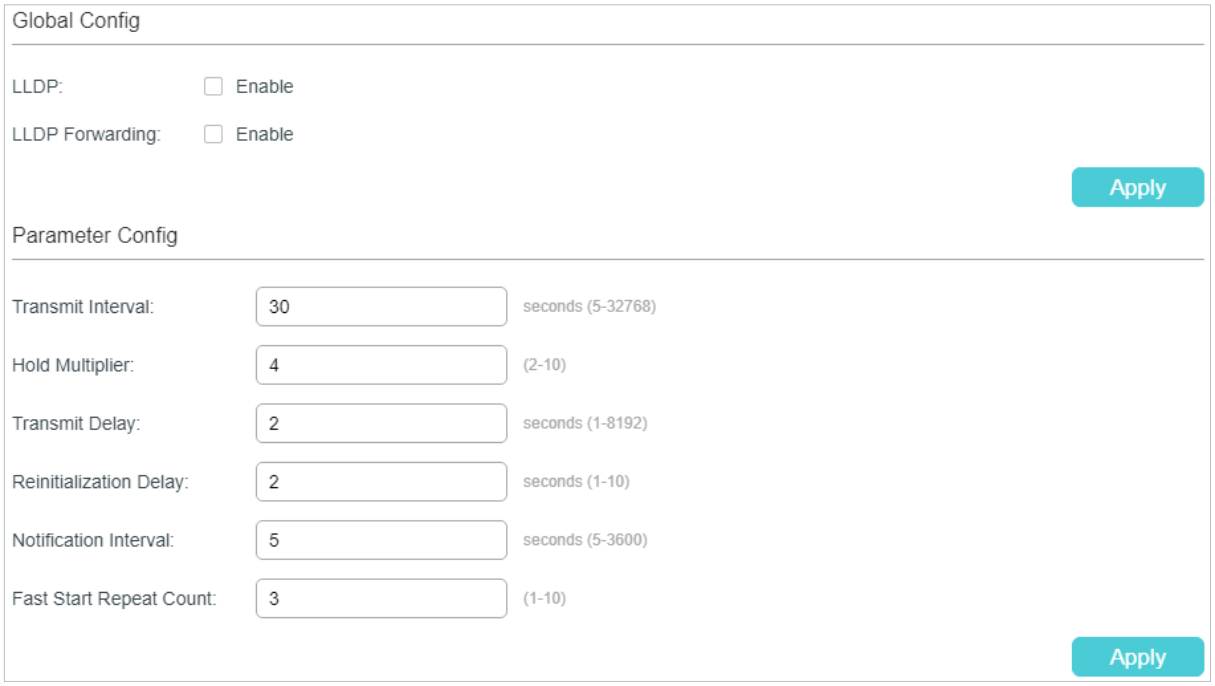
1) Skonfiguruj funkcję LLDP globalnie.
2) Skonfiguruj funkcję LLDP dla portu.

2.1 Przez GUI

2.1.1 Globalna konfiguracja LLDP

Wybierz z menu **L2 FEATURES > LLDP** > **LLDP Config** > **Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna



Wykonaj poniższe kroki, aby skonfigurować globalnie funkcję LLDP.

1) W sekcji **Global Config** włącz LLDP. Możesz także włączyć przekierowywanie komunikatów LLDP przez przełącznik, gdy funkcja LLDP jest wyłączona. Kliknij **Apply**.

LLDP	Włącz globalnie funkcję LLDP.
LLDP Forwarding	(Opcjonalnie) Włącz przekierowywanie komunikatów LLDP przez przełącznik, gdy funkcja LLDP jest wyłączona.

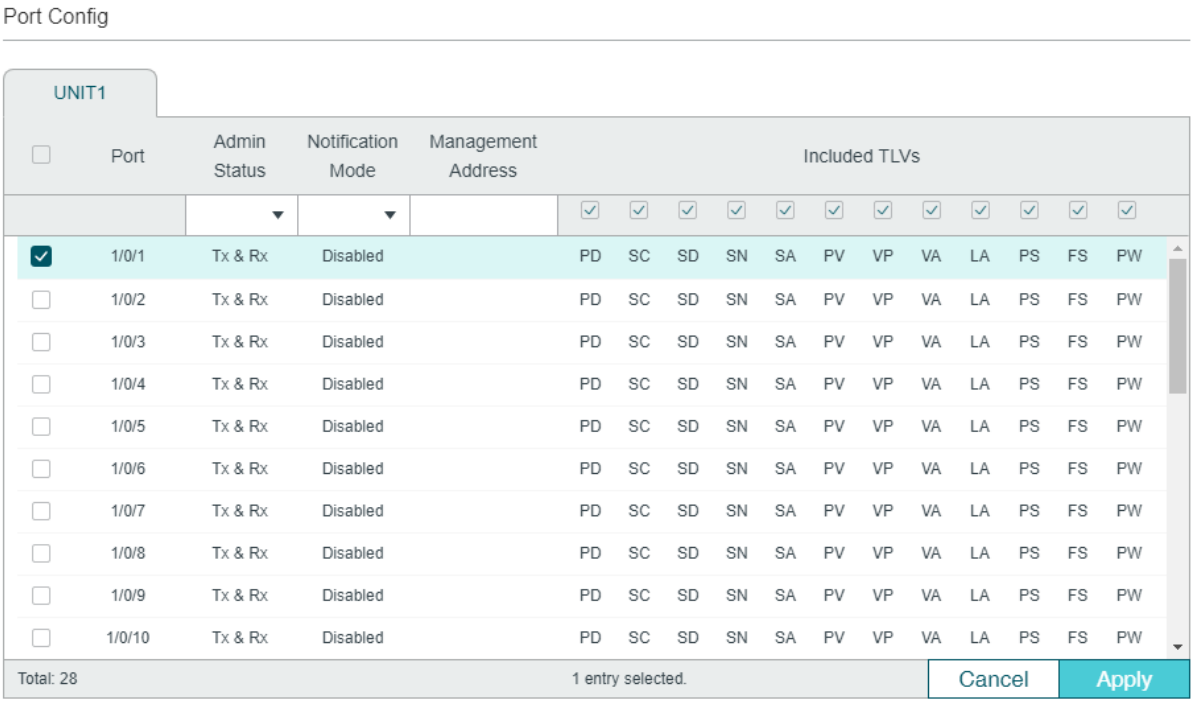
2) W sekcji **Parameter Config** skonfiguruj parametry LLDP. Kliknij **Apply**.

Transmit Interval	Podaj interwał kolejnych pakietów LLDP, które są cyklicznie wysyłane z urządzenia lokalnego do urządzeń sąsiadujących. Wartością domyślną jest 30 sekund.
Hold Multiplier	Ten parametr jest mnożnikiem interwału transmisji, który określa rzeczywistą wartość TTL (Time To Live) użytą w pakiecie LLDP. TTL to czas, przez który urządzenie sąsiadujące powinno przechowywać odebrany pakiet LLDP przed jego odrzuceniem. Wartością domyślną jest 4. TTL= Hold Multiplier * Transmit Interval.
Transmit Delay	Określ czas opóźnienia, po którym stan portów zmieni się na „Disable", aż do momentu ponownej próby inicjalizacji. Wartością domyślną są 2 sekundy.
Reinitialization Delay	Określ czas opóźnienia, po którym stan portów zmieni się na „Disable", aż do momentu ponownej próby inicjalizacji. Wartością domyślną są 2 sekundy.
Notification Interval	Podaj interwał w sekundach pomiędzy kolejnymi komunikatami Trap, które są cyklicznie wysyłane z urządzenia lokalnego do NMS. Wartością domyślną jest 5.
Fast Start Repeat Count	Określ liczbę pakietów LLDP, którą port lokalny ma wysyłać po jego zmianie stanu administracyjnego z Disable (lub Rx_Only) na Tx&RX (lub Tx_Only). Wartością domyślną jest 3. W tym przypadku urządzenie lokalne skróci Transmit Interval pakietów LLDP do 1 sekundy, aby mogły być szybko wykrywane przez urządzenia sąsiadujące. Po wysłaniu określonej liczby pakietów LLDP, Transmit Interval zostanie przywrócony do podanej wcześniej wartości.

2.1.2 Konfiguracja LLDP dla portów

Wybierz z menu **L2 FEATURES > LLDP** > **LLDP Config** > **Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja portów



Wykonaj poniższe kroki, aby skonfigurować funkcję LLDP dla interfejsu.

1) Wybierz jeden lub kilka portów do konfiguracji.
2) Skonfiguruj Admin Status i Notification Mode dla portu.

Admin Status	Ustaw stan dla portu, aby określić jego działania względem pakietów LLDP. Tx&Rx: Port wysyła i odbiera pakiety LLDP. Rx_Only: Port tylko odbiera pakiety LLDP. Tx_Only: Port tylko wysyła pakiety LLDP. Disable: Port nie wysyła i nie odbiera pakietów LLDP.
Notification Mode	(Opcjonalnie) Zezwól przełącznikowi na przesyłanie komunikatów trap do NMS, gdy informacje o urządzeniach sąsiadujących, połączonych z tym portem, ulegają zmianie.
Management Address	Podaj adres IP zarządzania portu, o którym urządzenie sąsiadujące ma być poinformowane. Wartość 0.0.0.0 oznacza, że port poda urządzeniu sąsiadującemu swój domyślny adres zarządzania.

3) Wybierz kodowania TLV (Type-length-value) zawarte w pakietach LLDP, zgodnie ze swoimi oczekiwaniami.

Included TLVs	Skonfiguruj kodowania TLV, zawarte w wychodzących pakietach LLDP. Przełącznik obsługuje następujące kodowania TLV: PD: Służy do rozgłaszania opisu portu zdefiniowanego przez stację LAN IEEE 802. SC: Służy do rozgłaszania obsługiwanych funkcji i informacji czy te funkcje są włączone. SD: Służy do rozgłaszania opisu systemu, zawierającego pełną nazwę i identyfikator wersji sprzętowej, system operacyjny oprogramowania i oprogramowanie sieciowe. SN: Służy do rozgłaszania nazwy systemowej. SA: Służy do rozgłaszania adresu zarządzania urządzeniem lokalnym, aby urządzenie mogło być zarządzane przez SNMP. PV: Służy do rozgłaszania ID VLAN-u 802.1Q portu. VP: Służy do rozgłaszania ID protokołu VLAN-u portu. VA: Służy do rozgłaszana nazwy VLAN-u, do którego przynależy port. LA: Służy do rozgłaszania informacji, czy łącze jest zdolne agregacji, czy łącze jest aktualnie w trakcie procesu agregacji, a także o identyfikatorze portu, gdy podlega agregacji. PS: Służy do rozgłaszania atrybutów portu, w tym możliwości dupleksu i przepływności wysyłającego węzła LAN IEEE 802.3, który jest podłączony do nośnika fizycznego, aktualnych ustawień dupleksu i przepływności wysyłającego węzła LAN IEEE 802.3 oraz informacji, czy te ustawienia są wynikiem autonegocjacji podczas inicjacji łącza, czy ręcznej czynności zastępowania. FS: Służy do rozgłaszania maksymalnego rozmiaru ramki zaimplementowanego adresu MAC i fizycznej warstwy ochronnej (PHY). PW: Służy do rozgłaszania możliwości obsługi PoE na porcie.

4) Kliknij **Apply**.

2.2 Przez CLI

2.2.1 Konfiguracja globalna

Włącz funkcję LLDP na przełączniku i skonfiguruj parametry LLDP.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**lldp** Włącz funkcję LLDP na przełączniku.

Krok 3	**lldp forward_message** (Opcjonalnie) Zezwól przełącznikowi na przesyłanie komunikatów LLDP, gdy funkcja LLDP jest wyłączona.
Krok 4	**lldp hold-multiplier** *multiplier* (Opcjonalnie) Podaj czas, przez który urządzenie sąsiadujące powinno przechowywać odebrany pakiet LLDP przed jego odrzuceniem. Ten parametr jest mnożnikiem interwału transmisji, który określa rzeczywistą wartość TTL (Time To Live) użytą w pakiecie LLDP. TTL= Hold Multiplier * Transmit Interval. *multiplier:* Podaj hold-multiplier. Prawidłowe wartości wahają się od 2 do 10, a wartością domyślną jest 4.
Krok 5	**lldp timer { tx-interval** *tx-interval* **| tx-delay** *tx-delay* **| reinit-delay** *reinit-delay* **| notify-interval** *notify-interval* **| fast-count** *fast-count* **}** (Opcjonalnie) Skonfiguruj czasy przesyłania pakietów LLDP. *tx-interval:* Podaj interwał kolejnych pakietów LLDP, które są cyklicznie wysyłane z urządzenia lokalnego do urządzeń sąsiadujących. *tx-delay:* Podaj czas oczekiwania przed wysłaniem kolejnego pakietu LLDP do urządzeń sąsiadujących. Wartością domyślną są 2 sekundy. *reinit-delay:* Podaj czas oczekiwania przed wysłaniem kolejnego pakietu LLDP do urządzeń sąsiadujących. Wartością domyślną są 2 sekundy. *notify-interval:* Podaj interwał w sekundach pomiędzy kolejnymi komunikatami Trap, które są cyklicznie wysyłane z urządzenia lokalnego do NMS. Wartością domyślną jest 5. *fast-count:* Podaj liczbę pakietów przesyłanych przez port lokalny, gdy jego stan administracyjny ulega zmianie. Wartością domyślną jest 3.
Krok 6	**show lldp** Przejrzyj informacje LLDP.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji następujących parametrów: lldp timer=4, tx-interval=30 sekund, tx-delay=2 sekund, reinit-delay=3 sekund, notify-iInterval=5 sekund, fast-count=3.

Switch#configure

Switch(config)#lldp

Switch(config)#lldp hold-multiplier 4

Switch(config)#lldp timer tx-interval 30

Switch(config)#lldp timer tx-delay 2

Switch(config)#lldp timer reinit-delay 3

Switch(config)#lldp timer notify-interval 5

Switch(config)#lldp timer fast-count 3

Switch(config)#show lldp

LLDP Status: Enabled

LLDP Forward Message: Disabled

Tx Interval: 30 seconds

TTL Multiplier: 4

Tx Delay: 2 seconds

Initialization Delay: 2 seconds

Trap Notification Interval: 5 seconds

Fast-packet Count: 3

LLDP-MED Fast Start Repeat Count: 4

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja portów

Wybierz porty i skonfiguruj ich Admin Status, Notification Mode i TLVs zawarte w pakietach LLDP.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**lldp receive** (Opcjonalnie) Ustaw ten tryb dla portu, aby odbierać pakiety LLDP. Opcja jest domyślnie włączona.
Krok 4	**lldp transmit** (Opcjonalnie) Ustaw ten tryb dla portu, aby wysyłać pakiety LLDP. Opcja jest domyślnie włączona.

Krok 5	**lldp snmp-trap** (Opcjonalnie) Włącz tryb powiadomień na porcie. Włączenie opcji spowoduje, że urządzenie lokalne będzie wysyłać komunikaty trap do NMS, gdy zmienią się informacje o urządzeniu sąsiadującym. Domyślnie opcja jest wyłączona.
Krok 6	**lldp tlv-select** (Opcjonalnie) Skonfiguruj kodowania TLV zawarte w wychodzących pakietach LLDP. Domyślnie pakiety wychodzące LLDP zawierają wszystkie kodowania TLV.
Krok 7	**show lldp interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Przejrzyj konfigurację LLDP portu.
Krok 8	**end** Powróć do trybu uprzywilejowanego (priviledged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji portu 1/0/1. Port może odbierać i wysyłać pakiety LLDP, jego tryb wysyłania komunikatów ma status enabled, a wychodzące pakiety LLDP zawierają wszystkie TLVs.

Switch#configure

Switch(config)#lldp

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#lldp receive

Switch(config-if)#lldp transmit

Switch(config-if)#lldp snmp-trap

Switch(config-if)#lldp tlv-select all

Switch(config-if)#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status: TxRx

SNMP Trap: Enabled

TLV	Status
---	------
Port-Description	Yes
System-Capability	Yes

System-Description	Yes
System-Name	Yes
Management-Address	Yes
Port-VLAN-ID	Yes
Protocol-VLAN-ID	Yes
VLAN-Name	Yes
Link-Aggregation	Yes
MAC-Physic	Yes
Max-Frame-Size	Yes
Power	Yes

Switch(config-if)#end

Switch#copy running-config startup-config

3 Konfiguracja LLDP-MED

Wykonaj poniższe kroki, aby skonfigurować funkcję LLDP-MED:

1) Włącz funkcję LLDP globalnie i skonfiguruj parametry LLDP dla portów.
2) Skonfiguruj globalnie liczbę wysyłanych pakietów LLDP-MED.
3) Włącz i skonfiguruj funkcję LLDP-MED na porcie.

Wskazówki dotyczące konfiguracji

Protokół LLDP-MED jest stosowany wraz z Auto VoIP w celu wdrożenia dostępu VoIP. Oprócz konfiguracji funkcji LLDP-MED konieczna jest także konfiguracja Auto VoIP. Szczegółowe informacje znajdziesz w części *Konfiguracja QoS*.

3.1 Przez GUI

3.1.1 Globalna konfiguracja LLDP

Włącz LLDP globalnie i skonfiguruj parametry LLDP dla portów. Szczegółowe informacje o konfiguracji LLDP znajdziesz w rozdziale *Konfiguracja LLDP*.

3.1.2 Globalna konfiguracja LLDP-MED

Wybierz z menu **L2 FEATURES > LLDP Config** > **LLDP-MED Config** > **Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja parametrów LLDP-MED

Skonfiguruj Fast Start Count i wyświetl aktualną klasę urządzenia. Kliknij **Apply**.

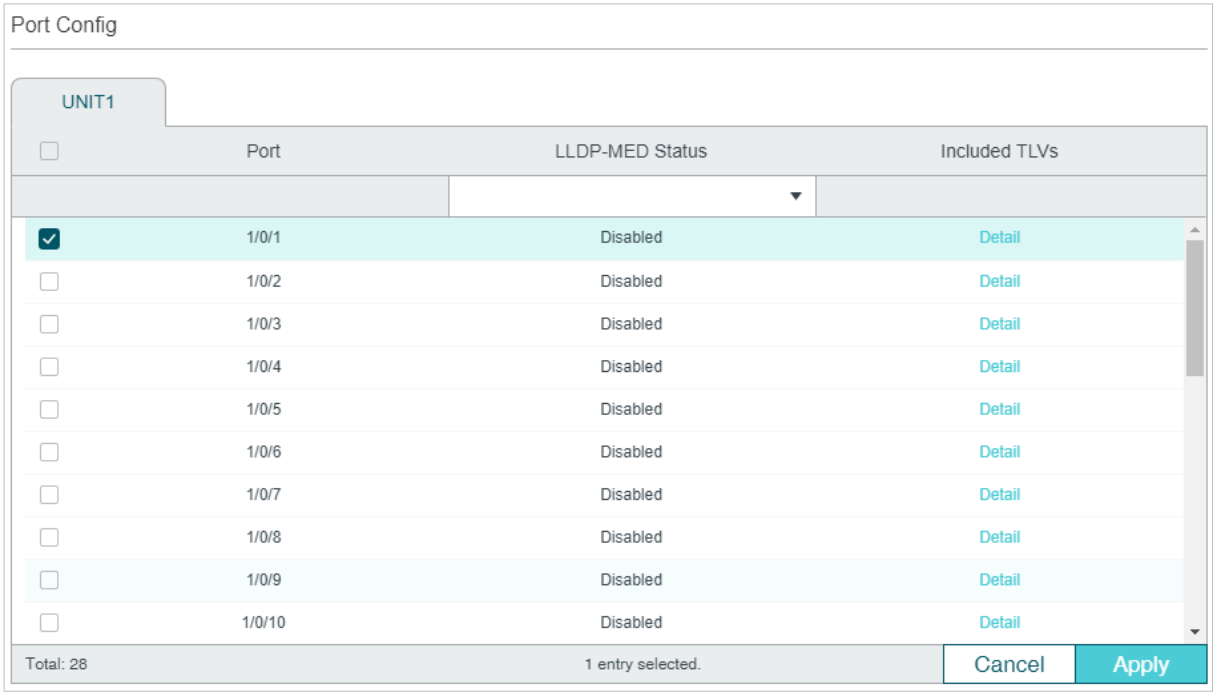
Fast Start Repeat Count	Podaj liczbę kolejnych pakietów LLDP-MED, które przełącznik wysyła, gdy odbiera pakiety LLDP-MED z sąsiadujących urządzeń końcowych. Wartością domyślną jest 4. Gdy przełącznik po raz pierwszy otrzyma pakiety LLDP-MED od sąsiadujących urządzeń końcowych, prześle określoną liczbę pakietów LLDP-MED z informacjami o LLDP-MED. Po tym wydarzeniu, transmit interval zostanie przywrócony do podanej wcześniej wartości.

Device Class	Aktualna klasa urządzenia. LLDP-MED definiuje dwie klasy urządzeń: Network Connectivity Device i Endpoint Device. Przełącznik jest Network Connectivity device.

3.1.3 Konfiguracja LLDP-MED dla portów

Wybierz z menu **L2 FEATURES > LLDP** > **LLDP-MED Config** > **Port Config**, aby wyświetlić poniższą stronę.

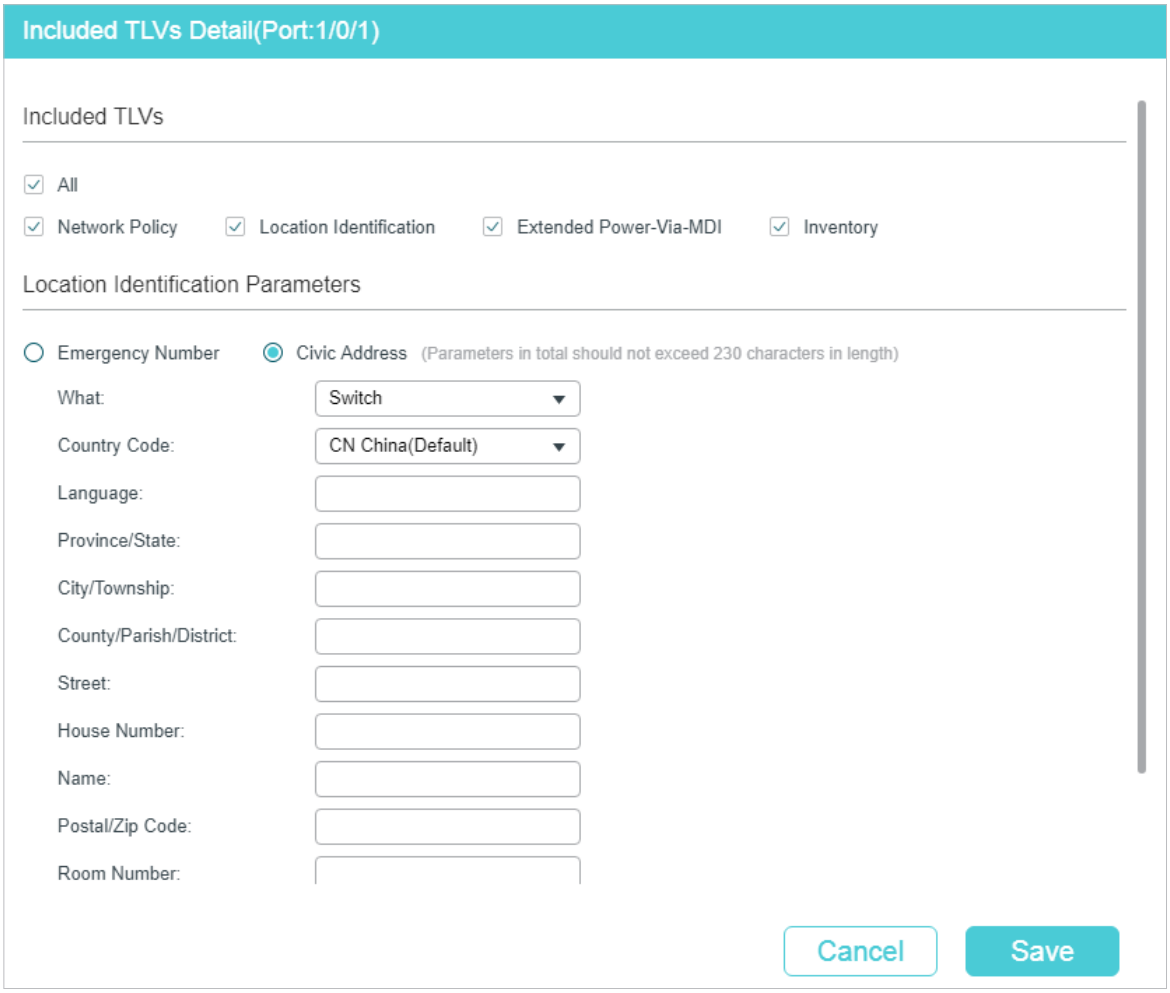
Rys. 3-2 Konfiguracja portów LLDP-MED



Wykonaj poniższe kroki, aby włączyć LLDP-MED:

1) Wybierz porty i włącz dla nich LLDP-MED. Kliknij **Apply**.
2) Kliknij **Detail**, aby wyświetlić poniższą stronę. Skonfiguruj kodowania TLV zawarte w wychodzących pakietach LLDP. Jeżeli zaznaczysz **Location Identification**, musisz ustawić Emergency Number lub wybrać Civic Address, aby skonfigurować szczegółowe informacje. Kliknij **Apply**.

Rys. 3-3 Konfiguracja portów LLDP-MED - informacje szczegółowe



Network Policy	Służy do rozgłaszania konfiguracji VLAN-u i powiązanych atrybutów warstwy 2 i warstwy 3 portu do urządzeń końcowych.
Location Identification	Służy do przypisywania urządzeniom końcowym informacji o identyfikatorze lokalizacji. Jeżeli opcja jest zaznaczona, możesz skonfigurować numer alarmowy i szczegółowe informacje o urządzeniu końcowym w części Location Identification Parameters.
Extended Power-Via-MDI	Służy do rozgłaszania szczegółowych informacji o PoE, w tym o priorytetyzacji dostarczanej energii i o stanie zasilania pomiędzy urządzeniami końcowymi LLDP-MED a urządzeniami Network Connectivity.
Inventory	Służy do rozgłaszania informacji o inwentarzu. Zestaw TLV zawiera siedem podstawowych kodowań TLV inwentarzu zarządzania, tj. wersję sprzętową TLV, wersję firmware'u TLV, wersję oprogramowania TLV, numer seryjny TLV, nazwę producenta TLV, nazwę modelu TLV i Asset ID TLV.
Emergency Number	Skonfiguruj numer awaryjny, aby móc zadzwonić do CAMA lub PSAP. Numer powinien składać się z 10-25 znaków.

Civic Address	Skonfiguruj adres urządzenia audio w formacie adresu zdefiniowanym przez IETF. What: Określ rolę urządzenia lokalnego, serwera DHCP, przełącznika lub urządzenia końcowego LLDP-MED. Country Code: Podaj kod kraju zgodny z ISO 3166, np. CN, US. Language, Province/State etc.: Uzupełnij pozostałe informacje.

3.2 Przez CLI

3.2.1 Konfiguracja globalna

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**lldp** Włącz funkcję LLDP na przełączniku.
Krok 3	**lldp med-fast-count** *count* (Opcjonalnie) Podaj liczbę kolejnych ramek LLDP-MED, które urządzenie lokalne wysyła, gdy mechanizm fast start jest aktywowany. Urządzenie lokalne wysyła określoną liczbę pakietów LLDP z informacjami LLDP-MED. *count:* Prawidłowe wartości wahają się od 1 do 10. Wartością domyślną jest 4.
Krok 4	**show lldp** Przejrzyj informacje o LLDP.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania LLDP-MED fast count jako 4:

Switch#configure

Switch(config)#lldp

Switch(config)#lldp med-fast-count 4

Switch(config)#show lldp

LLDP Status: Enabled

Tx Interval: 30 seconds

TTL Multiplier: 4

Tx Delay: 2 seconds

Initialization Delay: 2 seconds

Trap Notification Interval: 5 seconds

Fast-packet Count: 3

LLDP-MED Fast Start Repeat Count: 4

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Konfiguracja portów

Zaznacz porty, włącz LLDP-MED i wybierz kodowania TLV (Type-length-value) zawarte w wychodzących pakietach LLDP, zgodnie ze swoimi oczekiwaniami.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**lldp med-status** (Opcjonalnie) Włącz LLDP-MED na porcie. Domyślnie funkcja jest wyłączona.
Krok 4	**lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }** (Opcjonalnie) Skonfiguruj kodowania TLV, zawarte w wychodzących pakietach LLDP. Domyślnie wychodzące pakiety LLDP zawierają wszystkie kodowania TLV. Jeżeli zaznaczysz LLDP-MED Location TLV, skonfiguruj poniższe parametry: **lldp med-location {emergency-number** *identifier* **| civic-address [language** *language* **| province-state** *province-state* **| lci-county-name** *county* **| lci-city** *city* **| street** *street* **| house-number** *house-number* **| name** *name* **| postal-zipcode** *postal-zipcode* **| room-number** *room-number* **| post-office-box** *post-office-box* **| additional** *additional* **| country-code** *country-code* **| what { dhcp-server | endpoint | switch }] }** Skonfiguruj lokalizację kodowania TLV LLDP-MED zawartą w pakietach wychodzących LLDP. Służy ona do przypisywania informacji o identyfikatorze lokalizacji do urządzeń końcowych. *identifier:* Skonfiguruj numer awaryjny, aby móc zadzwonić do CAMA lub PSAP. Numer powinien składać się z 10-25 znaków. *language, province-state, county.etc:* Skonfiguruj adres w formacie adresu zdefiniowanym przez IETF.

Krok 5	**show lldp interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Przejrzyj konfigurację LLDP portu.
Krok 6	**end** Powróć do trybu uprzywilejowanego (priviledged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania LLDP-MED na porcie 1/0/1 i konfiguracji kodowań TLV LLDP-MED zawartych w wychodzących pakietach LLDP.

Switch(config)#lldp

Switch(config)#lldp med-fast-count 4

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#lldp med-status

Switch(config-if)#lldp med-tlv-select all

Switch(config-if)#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status: TxRx

SNMP Trap: Enabled

TLV Status

--- ------

Port-Description Yes

System-Capability Yes

System-Description Yes

System-Name Yes

Management-Address Yes

Port-VLAN-ID Yes

Protocol-VLAN-ID Yes

VLAN-Name Yes

Link-Aggregation Yes

MAC-Physic Yes

Max-Frame-Size Yes

Power Yes

LLDP-MED Status: Enabled

TLV Status

--- ------

Network Policy Yes

Location Identification Yes

Extended Power Via MDI Yes

Inventory Management Yes

Switch(config)#end

Switch#copy running-config startup-config

4 Przeglądanie ustawień LLDP

Ten rozdział przedstawia możliwe sposoby przeglądania ustawień LLDP na urządzeniu lokalnym.

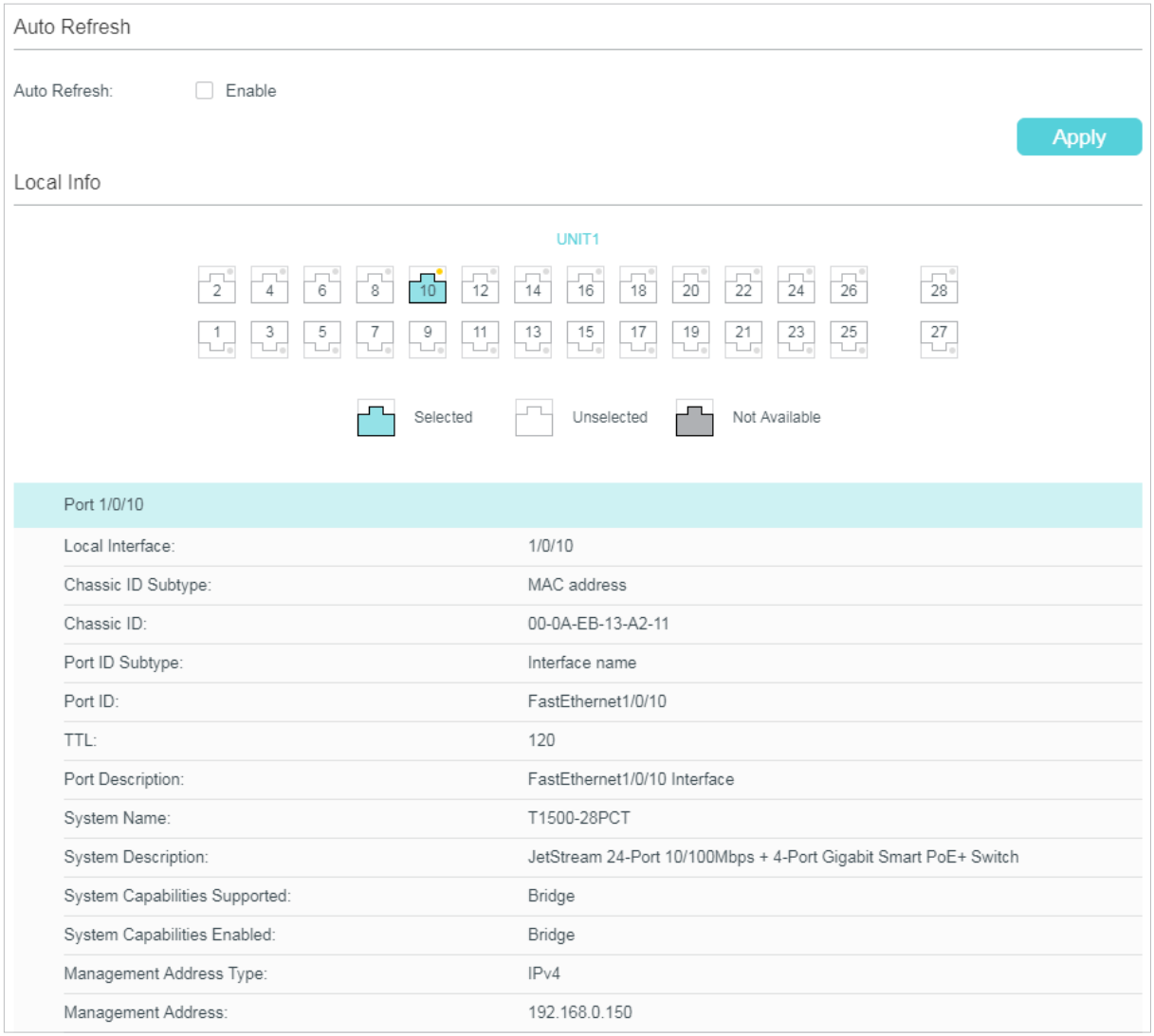
4.1 Przez GUI

4.1.1 Przeglądanie informacji urządzenia o LLDP

- Przeglądanie informacji lokalnych

Wybierz z menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Local Info**, aby wyświetlić poniższą stronę.

Rys. 4-1 Informacje lokalne



Wykonaj poniższe kroki, aby uzyskać dostęp do informacji lokalnych:

1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
2) W sekcji **Local Info** wybierz port i wyświetl informacje o powiązanym z nim urządzeniu lokalnym.

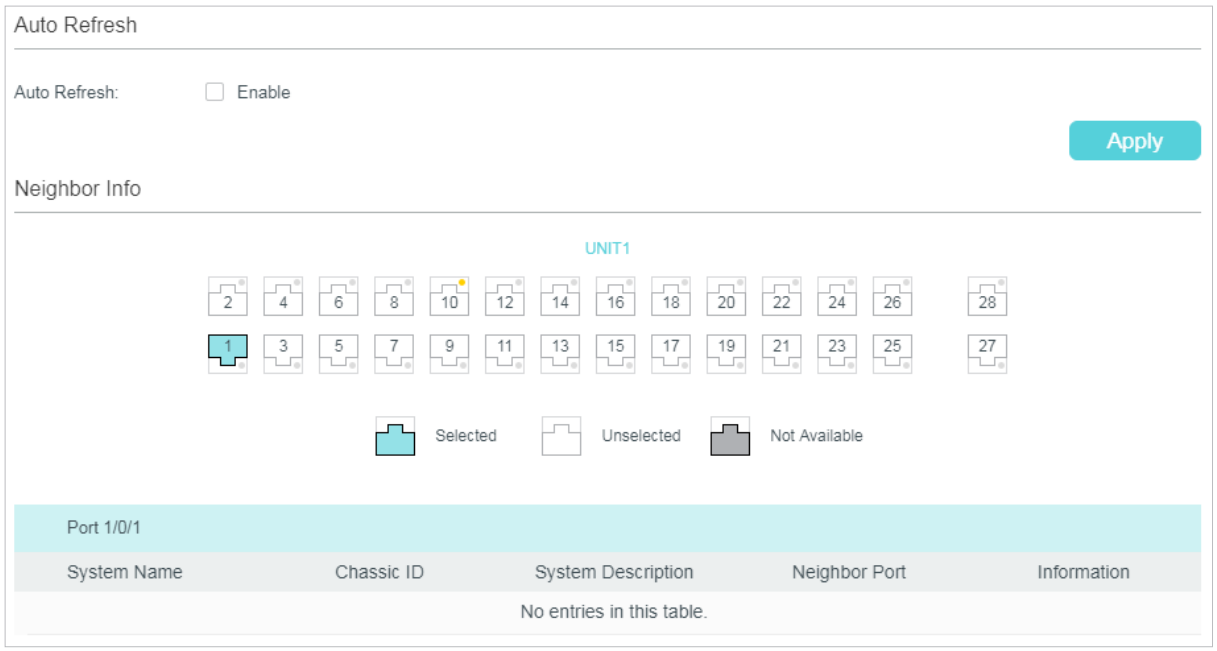
Local Interface	ID portu lokalnego.
Chassis ID Subtype	Typ ID obudowy.
Chassis ID	Wartość ID obudowy.
Port ID Subtype	Typ ID portu.
Port ID	Wartość iD portu.
TTL	Podaj czas w sekundach, przez który urządzenie sąsiadujące powinno przechowywać odebraną informację przed jej odrzuceniem.
Port Description	Opis portu lokalnego.
System Name	Nazwa systemowa urządzenia lokalnego.
System Description	Opis systemowy urządzenia lokalnego.
System Capabilities Supported	Obsługiwane możliwości systemu lokalnego.
System Capabilities Enabled	Podstawowe funkcje urządzenia lokalnego.
Management Address Type	Typ adresu IP zarządzania urządzenia lokalnego.
Management Address	Adres IP zarządzania urządzenia lokalnego.
Management Address Interface Type	Typ numerowania interfejsu, który jest stosowany do ustalania ID interfejsu.
Management Address Interface ID	ID interfejsu, który służy identyfikowaniu określonego interfejsu, powiązanego z adresem MAC urządzenia lokalnego.
Management Address OID	OID (Object Identifier) urządzenia lokalnego. Wartość równa 0 oznacza, że nie ma OID.
Port VLAN ID(PVID)	PVID portu lokalnego.
Port And Protocol VLAN ID(PPVID)	PPVID portu lokalnego.

Port And Protocol Supported	Informacja, czy urządzenie lokalne obsługuje funkcję portu i protokołu VLAN.
Port And Protocol VLAN Enabled	Stan funkcji portu i protokołu VLAN.
VLAN Name of VLAN 1	Nazwa VLAN 1 dla urządzenia lokalnego.
Protocol Identify	Protokół zalecany przez urządzenie lokalne.
Auto-negotiation Supported	Informacja, czy urządzenie lokalne obsługuje auto negocjację.
Auto-Negotiation Enable	Stan auto negocjacji urządzenia lokalnego.
OperMau	Pole OperMau (opcjonalne Mau) TLV, skonfigurowane przez urządzenie lokalne.
Link Aggregation Supported	Informacja, czy urządzenie lokalne obsługuje agregację łączy.
Link Aggregation Enabled	Stan agregacji łączy urządzenia lokalnego.
Aggregation Port ID	ID portu agregacji urządzenia lokalnego.
Power Port Class	Klasa portu zasilającego urządzenia lokalnego.
PSE Power Supported	Informacja, czy urządzenie lokalne obsługuje zasilanie PSE.
PSE Power Enabled	Stan zasilania PSE urządzenia lokalnego.
PSE Pairs Control Ability	Informacja, czy można kontrolować pary PSE dla urządzenia lokalnego.
Maximum Frame Size	Maksymalny rozmiar ramki obsługiwany przez urządzenie lokalne.

Przeglądanie informacji o urządzeniach sąsiadujących

Wybierz z menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Neighbor Info**, aby wyświetlić poniższą stronę.

Rys. 4-2 Informacje o urządzeniach sąsiadujących



Wykonaj poniższe kroki, aby wyświetlić informacje o urządzeniach sąsiadujących:

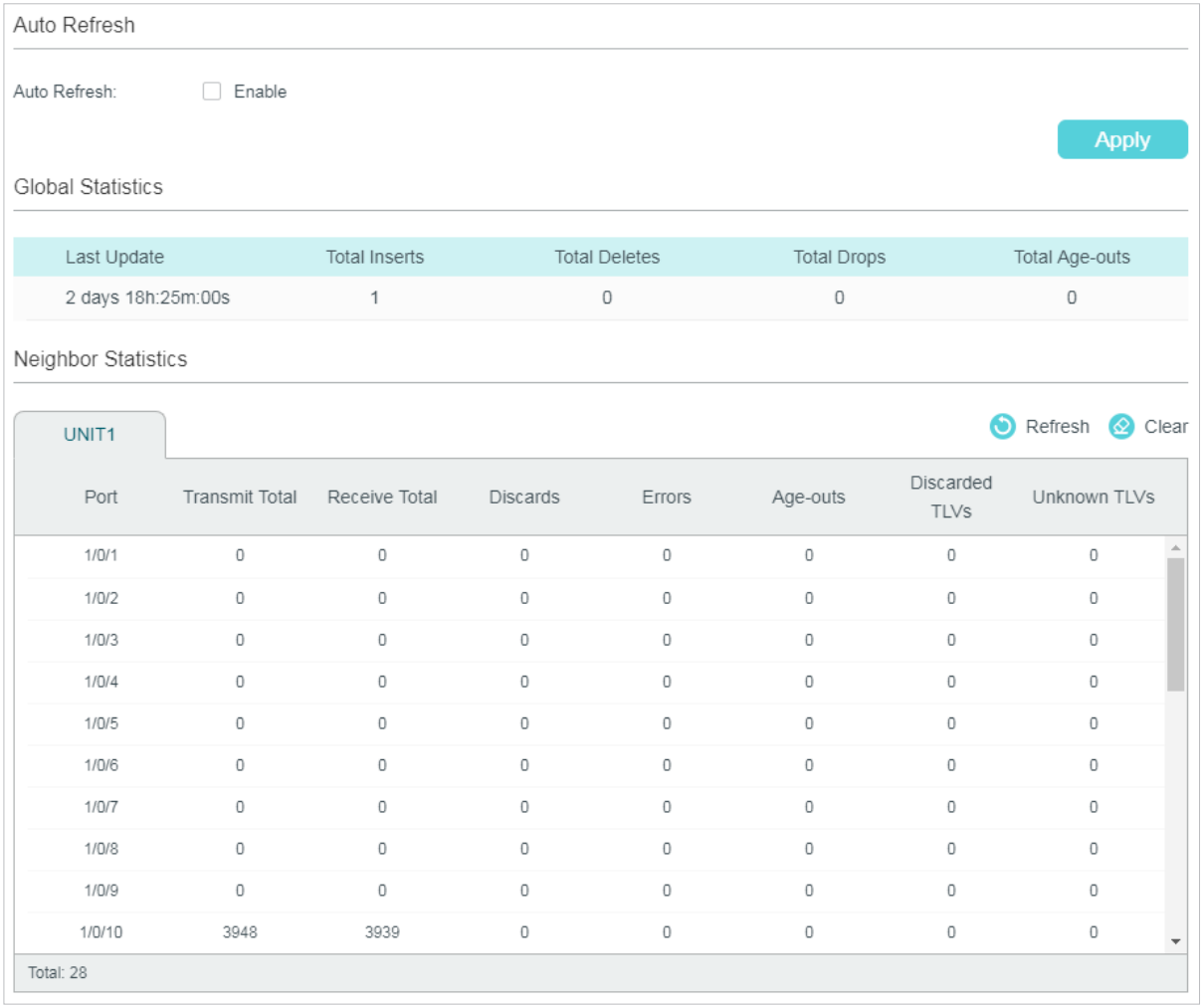
1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
2) W sekcji **Nieghbor Info** wybierz port i wyświetl informacje o powiązanym z nim urządzeniu sąsiadującym.

System Name	Nazwa systemowa urządzenia sąsiadującego.
Chassis ID	ID obudowy urządzenia sąsiadującego.
System Description	Opis systemowy urządzenia sąsiadującego.
Neighbor Port	ID portu urządzenia sąsiadującego, które jest podłączone do portu lokalnego.
Information	Kliknij, aby wyświetlić informacje szczegółowe o urządzeniu sąsiadującym.

4.1.2 Przeglądanie statystyk LLDP

Wybierz z menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Statistics Info**, aby wyświetlić poniższą stronę.

Rys. 4-3 Statystyki



Wykonaj poniższe kroki, aby wyświetlić statystyki LLDP:

1) IW sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
2) W sekcji **Global Statistics** wyświetl globalne statystyki urządzenia lokalnego.

Last Update	Czas ostatniej aktualizacji statystyk.
Total Inserts	Całkowita liczba urządzeń sąsiadujących po ostatniej aktualizacji.
Total Deletes	Liczba urządzeń sąsiadujących, usuniętych przez urządzenie lokalne. Port usuwa urządzenie sąsiadujące, gdy jest wyłączony lub wartość TTL pakietów LLDP przesyłanych do urządzenia sąsiadującego wynosi 0.
Total Drops	Liczba urządzeń sąsiadujących, odrzuconych przez urządzenie lokalne. Każdy z portów może nauczyć się maksymalnie 80 urządzeń sąsiadujących. Każde kolejne urządzenie będzie odrzucane.

Total Age-outs	Liczba urządzeń sąsiadujących, które straciły ważność na urządzeniu lokalnym.

3) W sekcji **Neighbors Statistics** możesz wyświetlić statystyki portu.

Transmit Total	Całkowita liczba pakietów LLDP przesłanych na porcie.
Receive Total	Całkowita liczba pakietów LLDP odebranych na porcie.
Discards	Całkowita liczba pakietów LLDP odrzuconych przez port.
Errors	Całkowita liczba błędnych pakietów LLDP odebranych na porcie.
Age-outs	Liczba podłączonych do portu urządzeń sąsiadujących, które utraciły ważność.
TLV Discards	Całkowita liczba kodowań TLV odrzuconych przez port po otrzymaniu pakietów LLDP.
TLV Unknowns	Całkowita liczba nieznanych kodowań TLV, zawartych w otrzymanych pakietach LLDP.

4.2 Przez CLI

■ Przeglądanie informacji lokalnych

show lldp local-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Wyświetla szczegółowe informacje LLDP o określonym porcie lub o wszystkich portach na urządzeniu lokalnym.

■ Przeglądanie informacji o urządzeniu sąsiadującym

show lldp neighbor-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Wyświetla informacje o urządzeniu sąsiadującym, które jest podłączone do portu.

■ Przeglądanie statystyk LLDP

show lldp traffic interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Wyświetla statystyki wybranego portu na urządzeniu lokalnym.

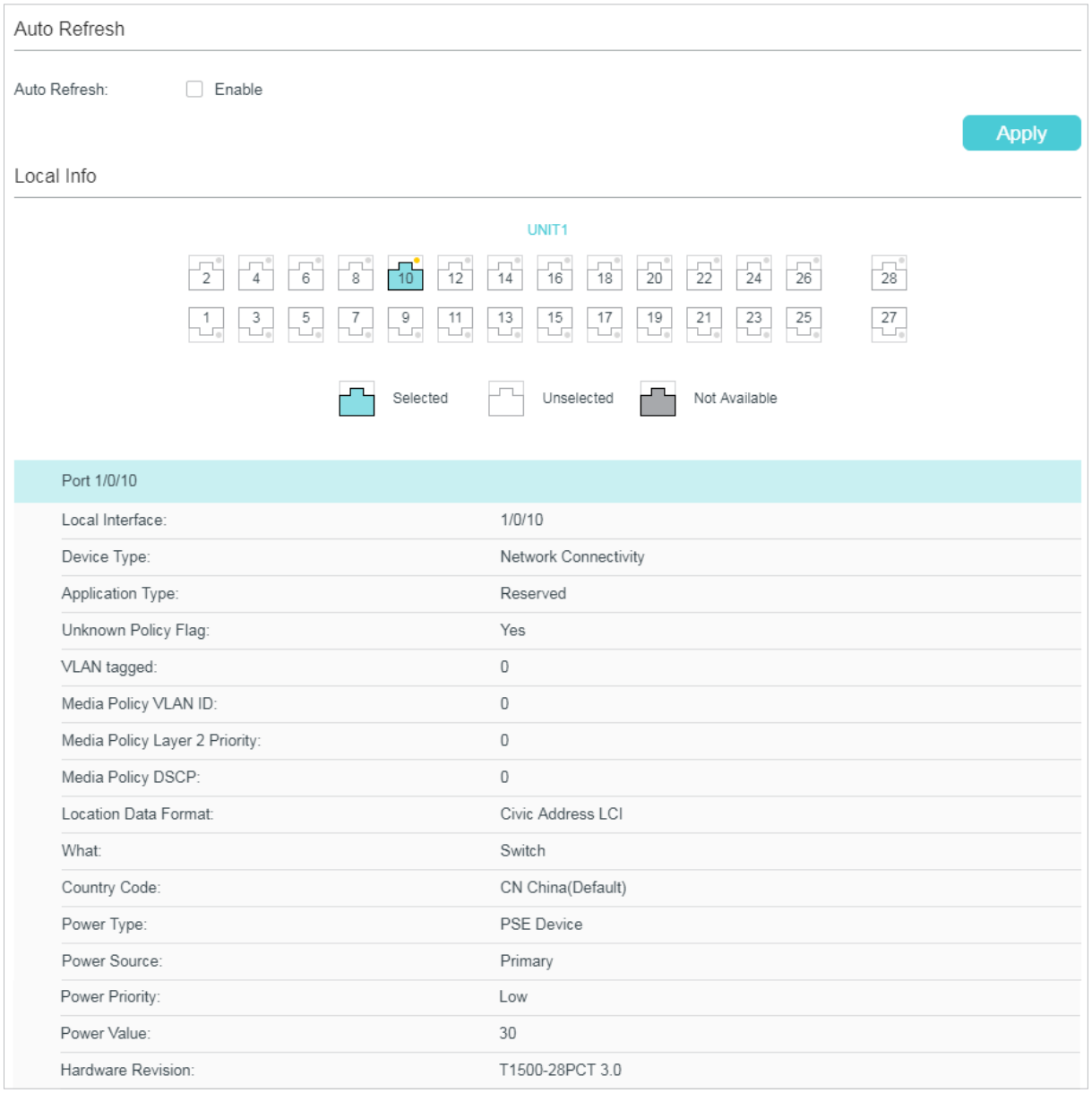
5 Przeglądanie ustawień LLDP-MED

5.1 Przez GUI

Wybierz z menu **L2 FEATURES** > **LLDP** > **LLDP-MED Config** > **Local Info**, aby wyświetlić poniższą stronę.

- Przeglądanie informacji lokalnych

Rys. 5-1 Informacje lokalne o LLDP-MED



Port 1/0/10	
Local Interface:	1/0/10
Device Type:	Network Connectivity
Application Type:	Reserved
Unknown Policy Flag:	Yes
VLAN tagged:	0
Media Policy VLAN ID:	0
Media Policy Layer 2 Priority:	0
Media Policy DSCP:	0
Location Data Format:	Civic Address LCI
What:	Switch
Country Code:	CN China(Default)
Power Type:	PSE Device
Power Source:	Primary
Power Priority:	Low
Power Value:	30
Hardware Revision:	T1500-28PCT 3.0

Wykonaj poniższe kroki, aby wyświetlić informacje lokalne o LLDP-MED:

1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
2) W sekcji **LLDP-MED Local Info** wybierz porty i wyświetl ustawienia LLDP-MED.

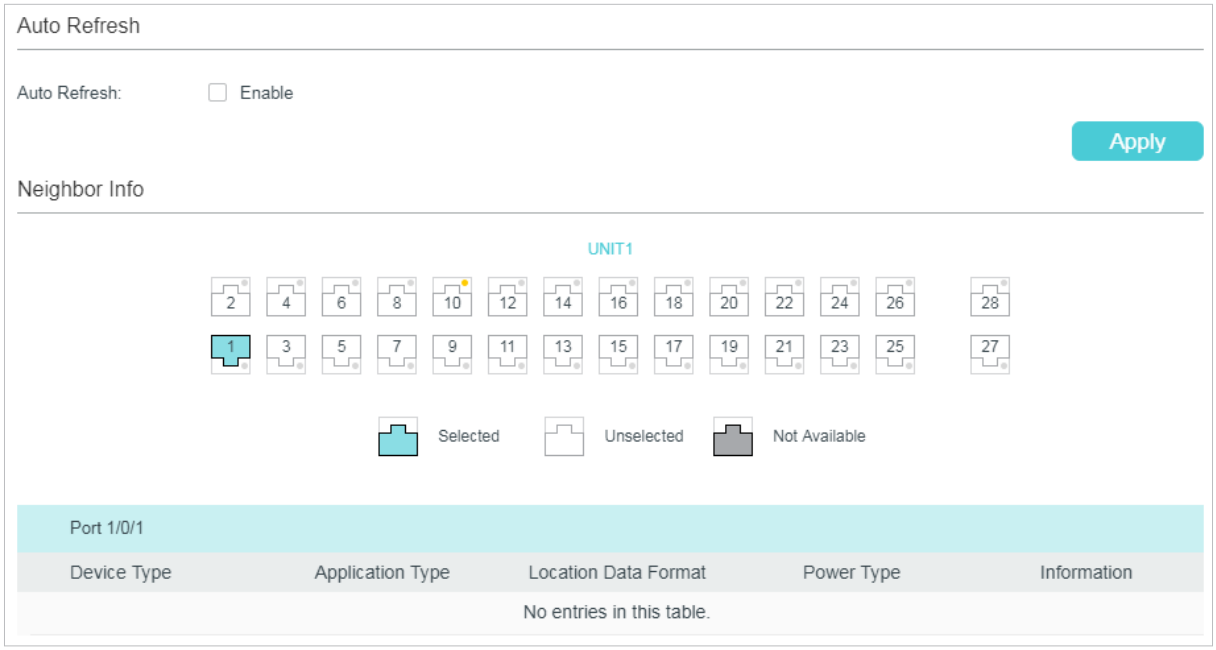
Local Interface	ID portu lokalnego.
Device Type	Typ urządzenia lokalnego, definiowanego przez LLDP-MED.LLDP-MED.
Application Type	Obsługiwane zastosowania urządzenia lokalnego.
Unknown Policy Flag	Ustawienia nieznanej lokalizacji zawartej w polityce sieciowej TLV.
VLAN tagged	Typ tagu VLAN aplikacji, tagowany lub nietagowany.
Media Policy VLAN ID	ID 802.1Q VLAN portu.
Media Policy Layer 2 Priority	Priorytet warstwy 2, stosowany dla określonego zastosowania.
Media Policy DSCP	Wartość DSCP, stosowana dla określonego zastosowania.
Location Data Format	Format danych identyfikatora lokalizacji urządzenia lokalnego.
What	Typ urządzenia lokalnego.
Country Code	Kod kraju urządzenia lokalnego.
Power Type	Informacja, czy urządzenie lokalne jest urządzeniem PSE czy PD。
Power Source	Źródło zasilania urządzenia lokalnego.
Power Priority	Priorytet zasilania urządzenia lokalnego to priorytet energii elektrycznej, która dostarczana jest przez urządzenia PD lub priorytet energii elektrycznej, dostarczanej przez urządzenia PSE.
Power Value	Moc wymagana od urządzenia PD lub dostarczana przez urządzenie PSE.
Hardware Revision	Wersja sprzętowa urządzenia lokalnego.
Firmware Revision	Wersja firmware'u urządzenia lokalnego.
Software Revision	Wersja oprogramowania urządzenia lokalnego.
Serial Number	Numer seryjny urządzenia lokalnego.

Manufacturer Name	Nazwa producenta urządzenia lokalnego.
Model Name	Model urządzenia lokalnego.
Asset ID	Asset ID urządzenia lokalnego.

■ Przeglądanie informacji o urządzeniach sąsiadujących

Wybierz z menu **L2 FEATURES** > **LLDP** > **LLDP-MED Config** > **Neighbor Info**, aby wyświetlić poniższą stronę.

Rys. 5-2 Informacje LLDP-MED urządzeń sąsiadujących



Wykonaj poniższe kroki, aby wyświetlić informacje LLDP-MED urządzeń sąsiadujących:

1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
2) W sekcji **Nieghbor Info** wybierz port i wyświetl informacje o powiązanym z nim urządzeniu sąsiadującym.

Device Type	Typ LLDP-MED urządzenia sąsiadującego.
Application Type	Typ zastosowań urządzenia sąsiadującego.
Location Data Format	Typ lokalizacji urządzenia sąsiadującego.
Power Type	Typ zasilania urządzenia sąsiadującego.
Information	Kliknij, aby wyświetlić szczegółowe informacje LLDP-MED urządzenia sąsiadującego.

5.2 Przez CLI

Przeglądanie informacji lokalnych

show lldp local-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Wyświetla szczegółowe informacje LLDP określonego portu lub wszystkich portów na urządzeniu lokalnym.

Przeglądanie informacji o urządzeniu sąsiadującym

show lldp neighbor-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Wyświetla informacje o urządzenie sąsiadującym, które jest połączone z portem.

Przeglądanie statystyk LLDP

show lldp traffic interface { fastEthernet *port* **| gigabitEthernet** *port* **| tengigabitEthernet** *port* **}**

Wyświetla statystyki wybranych portów.

Część 13

Konfiguracja usługi DHCP

ROZDZIAŁY

1 DHCP

1.1 Obsługiwane funkcje

Obsługiwane przez przełącznik funkcje DHCP to DHCP Relay i DHCP L2 Relay.

DHCP Relay

DHCP Relay służy do przetwarzania i przekazywania pakietów DHCP między różnymi podsieciami lub sieciami VLAN.

Klient DHCP wysyła pakiety żądania DHCP (DHCP Request) w celu pozyskania adresu IP. Przesyłanie pakietów broadcastowych zawsze ograniczone jest do jednego LAN, jeżeli więc serwer DHCP i klient nie należą do tego samego LAN, klient nie ma możliwości uzyskania adresu IP z serwera DHCP. Każdy LAN powinien zatem być wyposażony w serwer DHCP, co zwiększa koszty budowy sieci i stanowi utrudnienie w centralnym zarządzaniu siecią.

Funkcja DHCP Relay stanowi rozwiązanie problemu. Urządzenie z DHCP Relay pełni funkcję agenta przekazywania i przesyła pakiety DHCP między klientami DHCP i serwerami DHCP w różnych sieciach LAN. Dzięki temu klienci DHCP z różnych sieci LAN mogą dzielić jeden serwer DHCP.

Funkcja DHCP Relay obsługuje opcję 82 (Option 82) i DHCP VLAN Relay.

- Option 82

Dzięki opcji 82 przełącznik może rejestrować dane lokalizacyjne klienta DHCP. Przełącznik może dodać opcję 82 do pakietu żądania DHCP i przesłać pakiet do serwera DHCP. Serwer DHCP z obsługą opcji 82 może ustawić strategię rozdziału adresów IP i inne parametry, zapewniając bardziej elastyczny sposób rozdziału adresów.

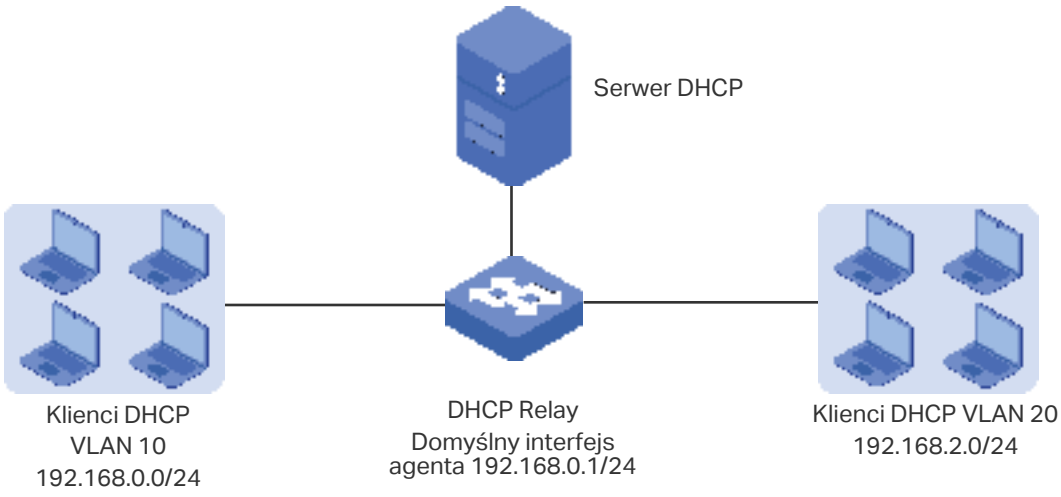
- DHCP VLAN Relay

DHCP VLAN Relay umożliwia klientom z różnych sieci VLAN pozyskiwanie adresów IP z serwera DHCP przy wykorzystaniu jednego adresu IP interfejsu agenta.

Dzięki DHCP VLAN Relay możesz ustawić VLAN interface 1 (domyślny interfejs zarządzania VLAN)jako domyślny interfejs agenta dla wszystkich sieci VLAN. Przełącznik wpisze adres IP domyślnego interfejsu agenta w pole adresu IP agenta przekazywania pakietów DHCP ze wszystkich sieci VLAN.

Jak przedstawiono na poniższym rysunku, do VLAN 10 i VLAN 20 nie przypisano żadnych adresów. Przełącznik wykorzystuje adres IP domyślnego interfejsu agenta (192.168.0.1/24) w celu zaaplikowania o adresy IP dla klientów obu sieci, VLAN 10 i VLAN 20. W rezultacie serwer DHCP przypisze adresy IP na 192.168.0.0/24 (ta sama podsieć co adres IP domyślnego interfejsu agenta) klientom obu sieci, VLAN 10 i VLAN 20.

Rys. 1-1 Scenariusz DHCP VLAN Relay



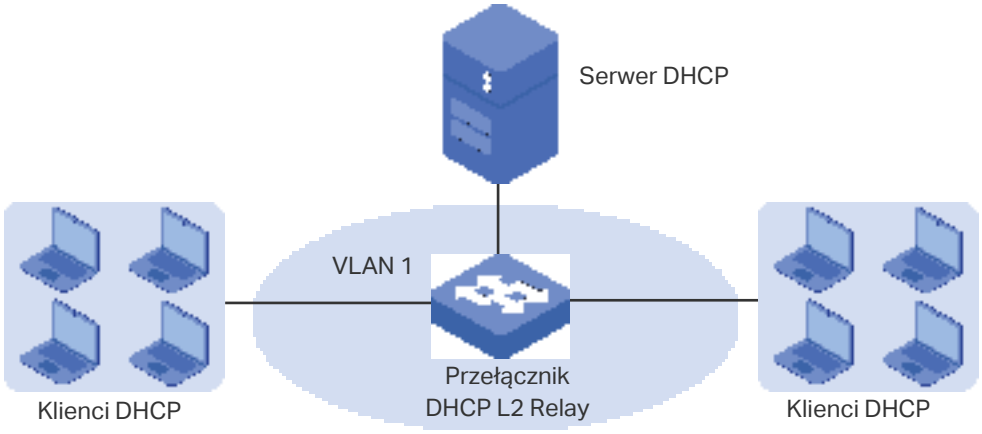
Uwaga:

W przełącznikach serii T1500 tylko interfejs zarządzania VLAN może być ustawiony jako domyślny interfejs agenta przekazywania.

DHCP L2 Relay

W przeciwieństwie do DHCP relay, DHCP L2 Relay wykorzystywany jest w sytuacji, gdy serwer DHCP i klient znajdują się w jednej sieci VLAN. Dzięki DHCP L2 Relay poza standardowym przypisywaniem adresów IP klientom z serwera DHCP, przełącznik może również rejestrować dane lokalizacyjne klienta DHCP za pomocą opcji 82. Przełącznik może dodać opcję 82 do pakietu żądania DHCP i przekazać pakiet do serwera DHCP. Serwer DHCP z obsługą opcji 82 może ustawić strategię rozdziału adresów IP i inne parametry, zapewniając bardziej elastyczny sposób rozdziału adresów.

Rys 1-2 Scenariusz DHCP L2 Relay



2 Konfiguracja DHCP Relay

Aby przeprowadzić konfigurację DHCP Relay, postępuj zgodnie z poniższymi krokami.

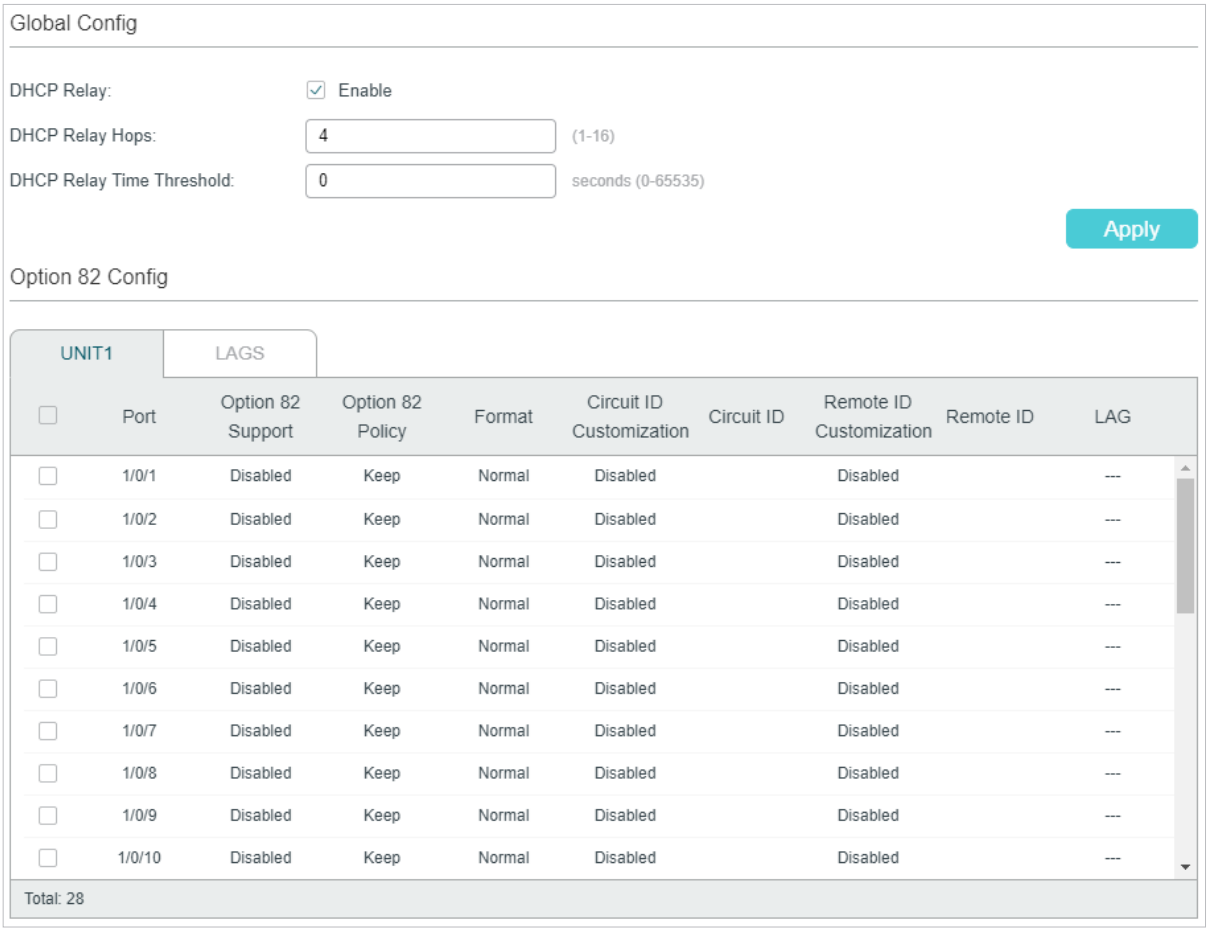
1) Włącz DHCP Relay. W razie konieczności skonfiguruj Opcję 82.
2) Wyznacz serwer DHCP na interfejsie lub w sieci VLAN.

2.1 Przez GUI

2.1.1 Włączanie DHCP Relay i konfiguracja Opcji 82

Wybierz menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config**, aby załadować następującą stronę.

Rys. 2-1 Włączanie DHCP Relay i konfiguracja Opcji 82



Aby włączyć opcję DHCP Relay i skonfigurować Opcję 82, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Global Config** włącz DHCP Relay globalnie i skonfiguruj przeskoki przekaźnika i próg czasu. Kliknij **Apply**.

DHCP Relay	Włącz DHCP Relay globalnie.
DHCP Relay Hops	Wyznacz przeskoki DHCP relay. DHCP Relay Hops to maksymalna liczba przeskoków (DHCP Relay agent), w których mogą być przekazywane pakiety DHCP. Jeżeli liczba przeskoków pakietu będzie większa, niż ustawiona w tym miejscu wartość, pakiet zostanie odrzucony.
DHCP Relay Time Threshold	Wyznacz prób czasu przekaźnika DHCP. Wartość powinna wynosić od 0 do 65535 sekund. Czas przekaźnika DHCP to czas, który upłynął od kiedy klient rozpoczął pozyskiwanie adresu i proces odnowy. Jeżeli czas jest dłuższy niż ustawiona w tym miejscu wartość, pakiet DHCP zostanie odrzucony przez przełącznik. Wartość 0 oznacza, że przełącznik nie będzie sprawdzać tego obszaru pakietów DHCP.

2) (Opcjonalnie) W sekcji **Option 82 Config** skonfiguruj opcję 82.

Option 82 Support	Zaznacz, czy chcesz włączyć opcję 82. Opcja jest domyślnie wyłączona. Opcja 82 wykorzystywana jest do zapisu lokalizacji DHCP klienta, portu Ethernet, VLAN itd. Jeżeli chcesz zapisać aktualną lokalizację klienta, możesz włączyć opcję 82 na urządzeniu przekaźnikowym, znajdującym się najbliżej niego.
Option 82 Policy	Wybierz działanie dla pola opcji 82 pakietów żądania DHCP. **Keep (zachowaj)**: Oznacza zachowanie pola opcji 82. **Replace (zastąp)**: Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i ID portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Relay, które odbiera pakiety żądania DHCP. **Drop (odrzuć)**: Oznacza odrzucanie pakietów zawierających pole opcji 82.
Format	Wybierz format pola wartości podopcji opcji 82. **Normal:** Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość). **Private:** Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.
Circuit ID Customization	Włącz lub wyłącz Customization of Option 82 (dostosowywanie opcji 82). Jeżeli funkcja jest włączona, należy skonfigurować dane opcji 82 ręcznie. Jeżeli funkcja jest wyłączona, przełącznik automatycznie skonfiguruje VLAN ID i ID portu, który odbiera pakiety DHCP jako circuit ID.
Circuit ID	Wprowadź zindywidualizowany circuit ID, składający się z maks. 64 znaków. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.
Remote ID Customization	Włącz lub wyłącz przełącznik w celu zdefiniowania pola Remote ID – podopcji opcji 82. Jeżeli jest włączone, możesz ręcznie skonfigurować zdalny ID. Jeżeli jest wyłączone, przełącznik automatycznie skonfiguruje adres MAC przełącznika jako zdalny ID.

Remote ID	Wprowadź zindywidualizowany zdalny ID, składający się z maks. 64 znaków. Ustawienia zdalnego ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.

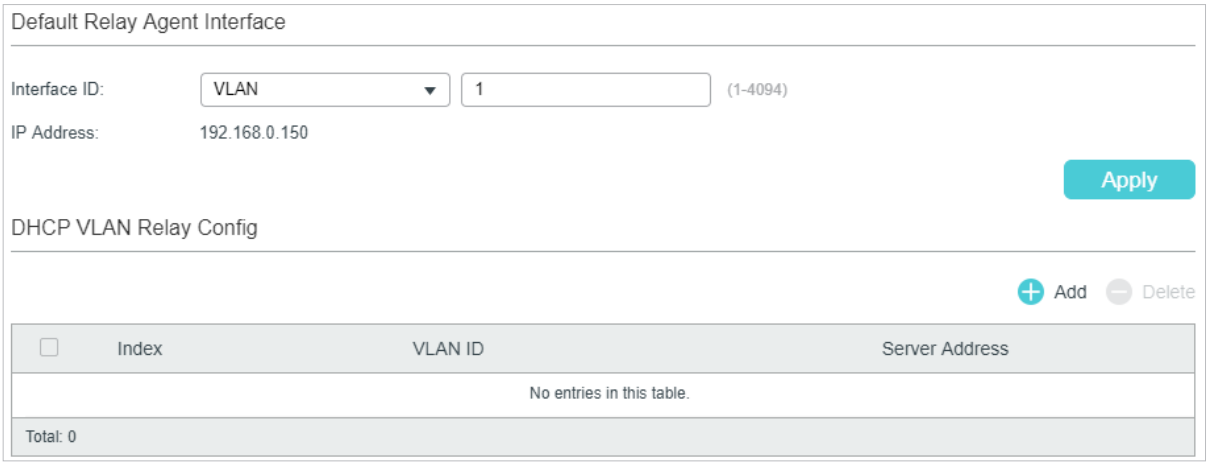
3) Kliknij **Apply**.

2.1.2 Konfiguracja DHCP VLAN Relay

DHCP VLAN Relay wykorzystywany jest dla klientów w sieciach VLAN, ale nie posiada interfejsu warstwy trzeciej jako bramy do pozyskiwania adresów IP z serwera DHCP, który nie należy do tej samej podsieci co klienci.

Wybierz menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay**, aby załadować następującą stronę.

Rys. 2-2 Wyznacz Serwer DHCP dla sieci VLAN

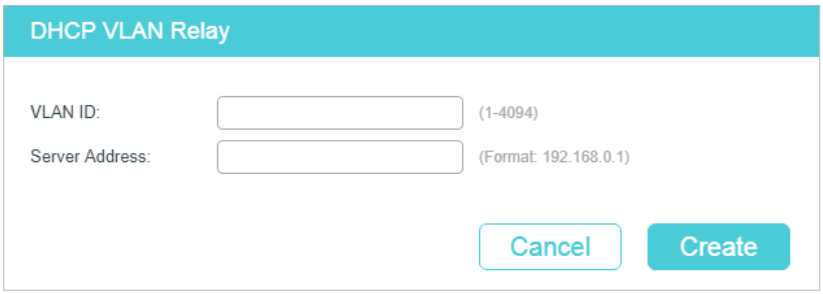


Aby wyznaczyć Serwer DHCP dla wybranej sieci VLAN, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Default Relay Agent Interface** ustaw VLAN zarządzający (domyślnie jest to VLAN 1) jako domyślny interfejs agenta przekazywania. Przełącznik poda jej adres IP do pola adresu IP agenta przekazywania w pakietach DHCP po zapytaniu o adresy IP z serwera DHCP. Kliknij **Apply**.

Interface ID	Określ typ i ID interfejsu, który będzie ustawiony jako domyślny interfejs agenta przekazywania. Na domyślny interfejs agenta przekazywania ustawić możesz każdy z interfejsów warstwy 3. Serwer DHCP przypisze adresy IP w tej samej podsieci co interfejs agenta przekazywania do klientów, którzy wykorzystują ten interfejs agenta przekazywania do ubiegania się o adresy IP.
IP Address	Informuje o adresie IP interfejsu.

2) W sekcji **DHCP VLAN Relay Config** kliknij Add, aby załadować następującą stronę.



Określ, do której sieci VLAN należą klienci i adres IP serwera DHCP. Kliknij **Create**.

VLAN ID	Określ sieć VLAN, w której klienci mogą pozyskać adresy IP z serwera DHCP.
Server Address	Wpisz adres IP serwera DHCP.

2.2 Przez CLI

2.2.1 Włączanie DHCP Relay

Aby włączyć DHCP Relay i skonfigurować odpowiednie parametry, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**service dhcp relay** Włącz DHCP Relay.
Krok 3	**show ip dhcp relay** Sprawdź ustawienia DHCP Relay.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (Privileged EXEC Mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie DHCP Relay, konfigurację przeskoków przekaźnika na 5 i konfigurację czasu przekaźnika na 10 sekund:

Switch#configure

Switch(config)#service dhcp relay

Switch(config)#show ip dhcp relay

DHCP relay state: enabled

.....

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 (Opcjonalnie) Konfiguracja opcji 82

Aby skonfigurować opcję 82, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ip dhcp relay information option** Włącz funkcję opcji 82 na porcie.
Krok 4	**ip dhcp relay information strategy {** keep | replace | drop **}** Wybierz działanie dla pola opcji 82 pakietów żądania DHCP z hosta. Dostępne są poniższe działania. keep**(zachowaj)**: Oznacza zachowanie pola opcji 82. replace (zastąp): Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i numer portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Snooping, które odbiera pakiety żądania DHCP. drop**(odrzuć)**: Oznacza odrzucanie pakietów zawierających pole opcji 82.
Krok 5	**ip dhcp relay information format {** normal | private **}** Wybierz format pola wartości podopcji opcji 82. normal: Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość). private: Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.
Krok 6	**ip dhcp relay information circuit-id** *string* Skonfiguruj circuit ID. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne. *string:* Wprowadź circuit ID, składający się z maks. 64 znaków.

Krok 7	**ip dhcp relay information remote-id** *string* Skonfiguruj remote ID. (zdalny ID). Ustawienia remote ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne. *string:* Wprowadź remote ID, składający się z maks. 64 znaków.
Krok 8	**show ip dhcp relay information interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Sprawdź konfigurację opcji 82 portu.
Krok 9	**end** Wróć do trybu użytkownika uprzywilejowanego (Privileged EXEC Mode).
Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie opcji 82 na porcie 1/0/7 i konfigurację strategii na replace (zastąp), formatu na normal, circuit-id jako VLAN 20 i remote-id jako Host1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#ip dhcp relay information option

Switch(config-if)#ip dhcp relay information strategy replace

Switch(config-if)#ip dhcp relay information format normal

Switch(config-if)#ip dhcp relay information circut-id VLAN20

Switch(config-if)#ip dhcp relay information remote-id Host1

Switch(config-if)#show ip dhcp relay information interface gigabitEthernet 1/0/7

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	Remote ID	LAG
---	---	---	---	---	---	---
Gi1/0/7	Enable	Replace	Normal	VLAN20	Host1	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Konfiguracja DHCP VLAN Relay

Aby skonfigurować DHCP VLAN Relay, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2	Wejdź w tryb konfiguracji interfejsu VLAN. **interface vlan** *vlan-id* *vlan-id*: **Wyznacz interfejs** VLAN. Obsługiwana jest jedynie VLAN 1 (VLAN zarządzający).
Krok 3	**ip dhcp relay default-interface** Ustaw interfejs management VLAN (VLAN zarządzający) jako domyślny interfejs agenta przekazywania.
Krok 4	**ip dhcp relay vlan** *vid* **helper-address** *ip-address* Określ VLAN ID i serwer DHCP. *vid*: Wprowadź ID VLAN, w której hosty mogą dynamicznie pozyskiwać IP z serwera DHCP. *ip-address*: Wprowadź adres IP serwera DHCP.
Krok 5	**exit** Wróć do trybu konfiguracji globalnej.
Krok 6	**show ip dhcp relay** Sprawdź ustawienia DHCP Relay.
Krok 7	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC Mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie interfejsu VLAN 1 (VLAN zarządzający) na domyślny interfejs agenta przekazywania i wyznaczenie serwera DHCP przez wpisanie adresu serwera jako 192.168.1.8 na VLAN 10:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)# ip dhcp relay default-interface

Switch(config-if)#exit

Switch(config)#ip dhcp relay vlan 10 **helper-address** 192.168.1.8

Switch(config)#show ip dhcp relay

...

DHCP VLAN relay helper address is configured on the following vlan:

vlan Helper address

---------- --------------

VLAN 10 192.168.1.8

Switch(config)#end

Switch#copy running-config startup-config

3 Konfiguracja DHCP L2 Relay

Aby przeprowadzić konfigurację DHCP L2 Relay, postępuj zgodnie z poniższymi krokami.

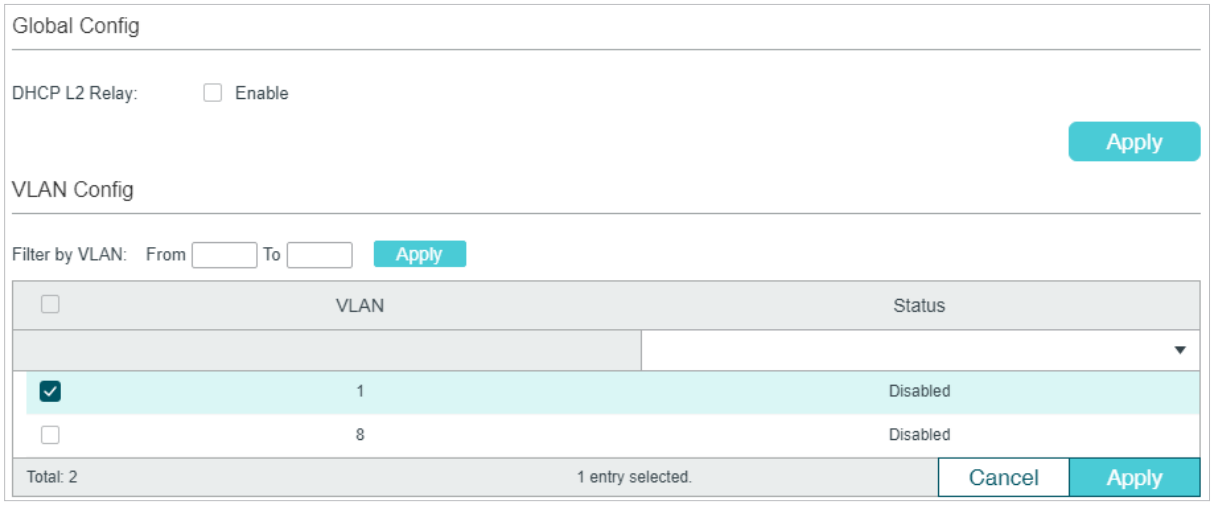
1) Włącz DHCP L2 Relay.
2) Skonfiguruj opcję 82 dla portów.

3.1 Przez GUI

3.1.1 Włączanie DHCP L2 Relay

Wybierz menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Global Config**, aby załadować następującą stronę.

Rys. 3-1 Włączanie DHCP L2 Relay



Aby włączyć DHCP L2 Relay globalnie dla wybranej sieci VLAN, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Global Config** włącz globalnie DHCP L2 Relay. Kliknij **Apply**.

DHCP L2 Relay	Włącz DHCP Relay globalnie.

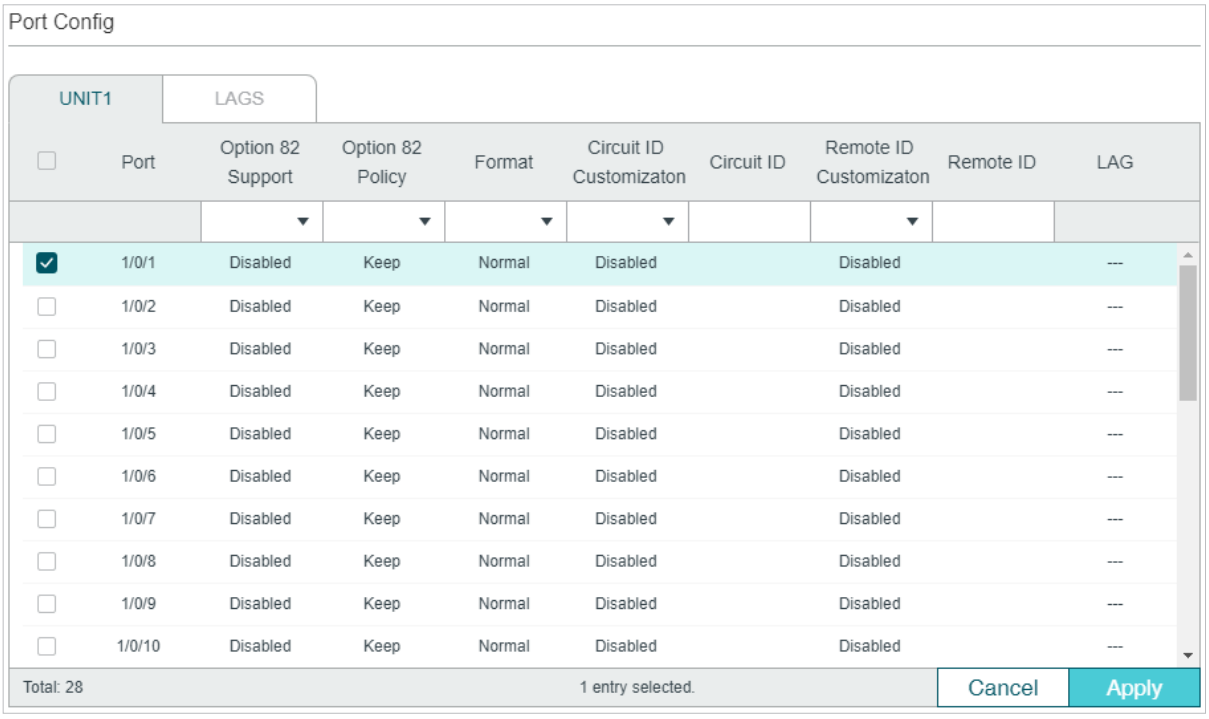
2) W sekcji **VLAN Config** włącz DHCP L2 Relay dla wybranej sieci VLAN. Kliknij **Apply**.

VLAN	Informuje o VLAN ID.
Status (Stan)	Włącz DHCP L2 Relay dla wybranej sieci VLAN.

3.1.2 Konfiguracja opcji 82 dla portów

Wybierz menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Port Config**, aby załadować następującą stronę.

Rys. 3-2 Konfiguracja opcji 82 dla portów



Aby włączyć DHCP Relay i skonfigurować opcję 82, postępuj zgodnie z poniższymi krokami:

1) Wybierz jeden port lub więcej portów, aby skonfigurować na nich opcję 82.

Option 82 Support	Zaznacz, czy chcesz włączyć opcję 82. Opcja jest domyślnie wyłączona. Opcja 82 wykorzystywana jest do zapisu lokalizacji DHCP klienta, portu Ethernet, VLAN itd. Jeżeli chcesz zapisać aktualną lokalizację klienta, możesz włączyć opcję 82 na urządzeniu przekaźnikowym, znajdującym się najbliżej niego.
Option 82 Policy	Wybierz działanie dla pola opcji 82 pakietów żądania DHCP. **Keep (zachowaj)**: Oznacza zachowanie pola opcji 82. **Replace (zastąp)**: Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i ID portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Relay, które odbiera pakiery żądania DHCP. **Drop (odrzuć)**: Oznacza odrzucanie pakietów zawierających pole opcji 82.
Format	Wybierz format pola wartości podopcji opcji 82. **Normal:** Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość). **Private:** Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.

Circuit ID Customization	Włącz lub wyłącz Customization of Option 82 (dostosowywanie opcji 82). Jeżeli funkcja jest włączona, należy skonfigurować dane opcji 82 ręcznie. Jeżeli funkcja jest wyłączona, przełącznik automatycznie skonfiguruje VLAN ID i ID portu, który odbiera pakiety DHCP jako circuit ID.
Circuit ID	Wprowadź zindywidualizowany circuit ID, składający się z maks. 64 znaków. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.
Remote ID Customization	Włącz lub wyłącz przełącznik w celu zdefiniowania pola Remote ID – podopcji opcji 82. Jeżeli jest włączone, możesz ręcznie skonfigurować zdalny ID. Jeżeli jest wyłączone, przełącznik automatycznie skonfiguruje adres MAC przełącznika jako zdalny ID.
Remote ID	Wprowadź zindywidualizowany zdalny ID, składający się z maks. 64 znaków. Ustawienia zdalnego ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.

2) Kliknij **Apply**

3.2 Przez CLI

3.2.1 Włączanie DHCP Relay

Aby włączyć DHCP L2 Relay, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip dhcp l2relay** Włącz DHCP L2 Relay.
Krok 3	**ip dhcp l2relay vlan** *valn-list* Włącz DHCP L2 Relay dla wybranych sieci VLAN. *vlan-list:* Wyznacz VLAN, który będzie włączany przez DHCP L2 relay.
Krok 5	**show ip dhcp l2relay** Sprawdź konfigurację DHCP Relay.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (Privileged EXEC Mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Następujący przykład prezentuje włączanie DHCP L2 Relay globalnie i dla VLAN 2:

Switch#configure

Switch(config)#ip dhcp l2relay

Switch(config)#ip dhcp l2relay vlan 2

Switch(config)#show ip dhcp l2relay

Global Status: Enable

VLAN ID: 2

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Konfiguracja opcji 82 dla portów

Aby skonfigurować opcję 82, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ip dhcp l2relay information option** Włącz funkcję opcji 82 na porcie.
Krok 4	**ip dhcp l2relay information strategy {** keep | replace | drop **}** Wybierz działanie dla pola opcji 82 pakietów żądania DHCP z hosta. Dostępne są poniższe działania. keep **(zachowaj)**: Oznacza zachowanie pola opcji 82. replace (zastąp): Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i numer portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Snooping, które odbiera pakiety żądania DHCP. drop **(odrzuć)**: Oznacza odrzucanie pakietów zawierających pole opcji 82.
Krok 5	**ip dhcp l2relay information format {** normal | private **}** Wybierz format pola wartości podopcji opcji 82. normal: Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość). private: Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.

Krok 6	**ip dhcp l2relay information circuit-id** *string* Skonfiguruj circuit ID. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne. *string:* Wprowadź circuit ID, składający się z maks. 64 znaków.
Krok 7	**ip dhcp l2relay information remote-id** *string* Skonfiguruj remote ID. (zdalny ID). Ustawienia remote ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne. *string:* Wprowadź remote ID, składający się z maks. 64 znaków.
Krok 8	**show ip dhcp l2relay information interface { fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Sprawdź konfigurację opcji 82 portu.
Krok 9	**end** Wróć do trybu użytkownika uprzywilejowanego (Privileged EXEC Mode).
Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Następujący przykład prezentuje włączanie opcji 82 na porcie 1/0/7 i konfigurację strategii na replace (zastąp), formatu na normal, circuit-id na VLAN20 i remote-id na Host1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#ip dhcp l2relay information option

Switch(config-if)#ip dhcp l2relay information strategy replace

Switch(config-if)#ip dhcp l2relay information format normal

Switch(config-if)#ip dhcp l2relay information circut-id VLAN20

Switch(config-if)#ip dhcp l2relay information remote-id Host1

Switch(config-if)#show ip dhcp l2relay information interface gigabitEthernet 1/0/7

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	Remote ID	LAG
---	---	---	---	---	---	---
Gi1/0/7	Enable	Replace	Normal	VLAN20	Host1	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

Część 14

Konfiguracja QoS

ROZDZIAŁY

1 Konfiguracja usług Class of Service

Konfigurując usługi class of service możesz:

- skonfigurować priorytetyzację portu;
- skonfigurować priorytetyzację 802.1p;
- skonfigurować priorytetyzację DSCP;
- dostosować ustawienia harmonogramu.

Wskazówki dotyczące konfiguracji

- Wybierz tryb priorytetyzacji, któremu porty ufają, zgodnie z wymaganiami sieci.

  Port może korzystać tylko z jednego trybu priorytetyzacji do klasyfikacji pakietów przychodzących. Przełącznik obsługuje trzy tryby priorytetyzacji: priorytetyzacja portu, priorytetyzacja 802.1P i priorytetyzacja DSCP.

  - Priorytetyzacja portu

  W tym trybie przełącznik przydziela pakietom priorytety, zgodnie z ich portami odbierającymi, bez względu na pole lub typ pakietu.

  - Priorytetyzacja 802.1P

  Standard 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI wahają się od 0 do 7. Priorytetyzacja 802.1P przydziela pakietom priorytet w oparciu o wartość PRI.

  W tym trybie przełącznik przydziela priorytety tylko pakietom z tagiem VLAN, bez względu na nagłówek IP pakietów.

  - Priorytetyzacja DSCP

  Priorytetyzacja DSCP ustala priorytety pakietów w oparciu o pole ToS (Type of Service) w nagłówku IP. RFC2474 określa pole ToS w nagłówku IP pakietu poprzez pole DS. Pierwsze sześć bitów (bit 0 - bit 5) pola DS stanowi priorytet DSCP. Wartości DSCP wahają się od 0 do 63.

  W tym trybie przełącznik przydziela priorytety tylko pakietom IP.

- Określ mapowanie 802.1p do kolejek, zgodnie ze swoimi wymagniami.

  W wypadku priorytetyzacji 802.1p pakiety będą przesyłane bezpośrednio, zgodnie z mapowaniem 802.1p do kolejek.

  W wypadku priorytetyzacji portu i priorytetyzacji DSCP, będą one w pierwszej kolejności mapowane do priorytetu 802.1p, a następnie mapowane zgodnie z mapowaniem 802.1p do kolejek.

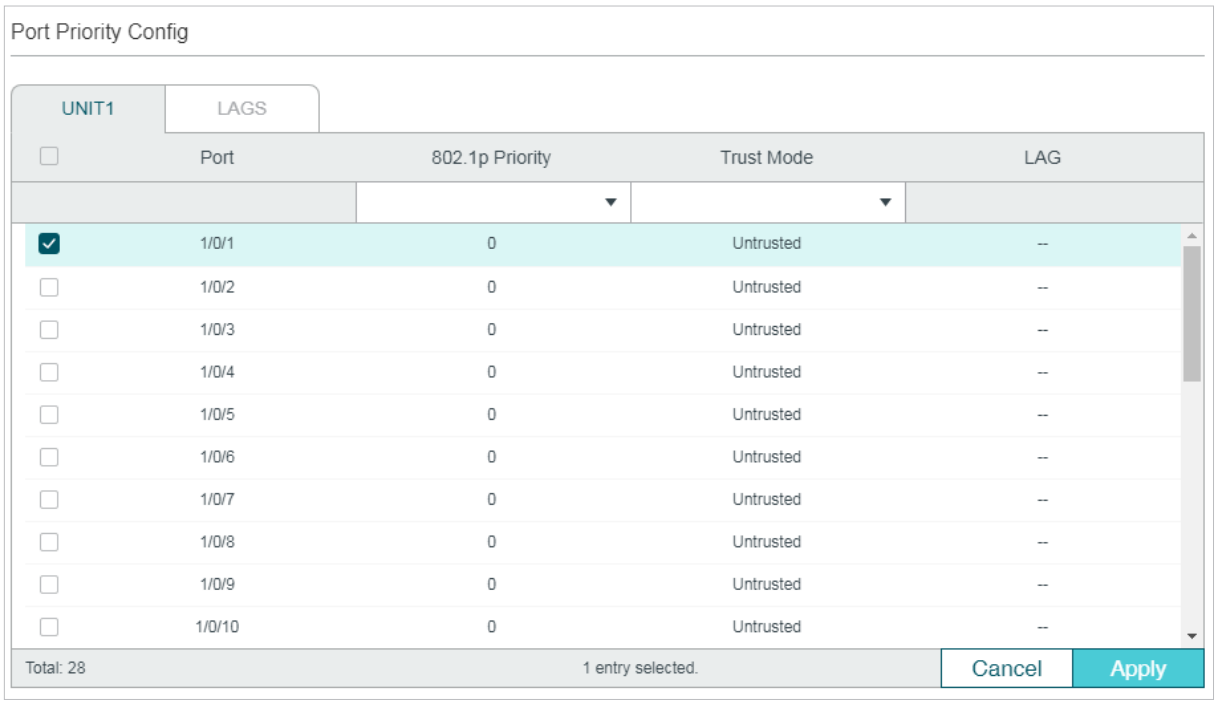
1.1 Przez GUI

1.1.1 Konfiguracja priorytetyzacji portu

- Konfiguracja Trust Mode i Port to 802.1p Mapping

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 1-1 Konfiguracja Trust Mode i Port to 802.1p Mapping



Wykonaj poniższe kroki, aby skonfigurować parametry priorytetyzacji portu:

1) Wybierz porty, dostosuj priorytetyzację 802.1p i ustaw trust mode jako Untrusted.

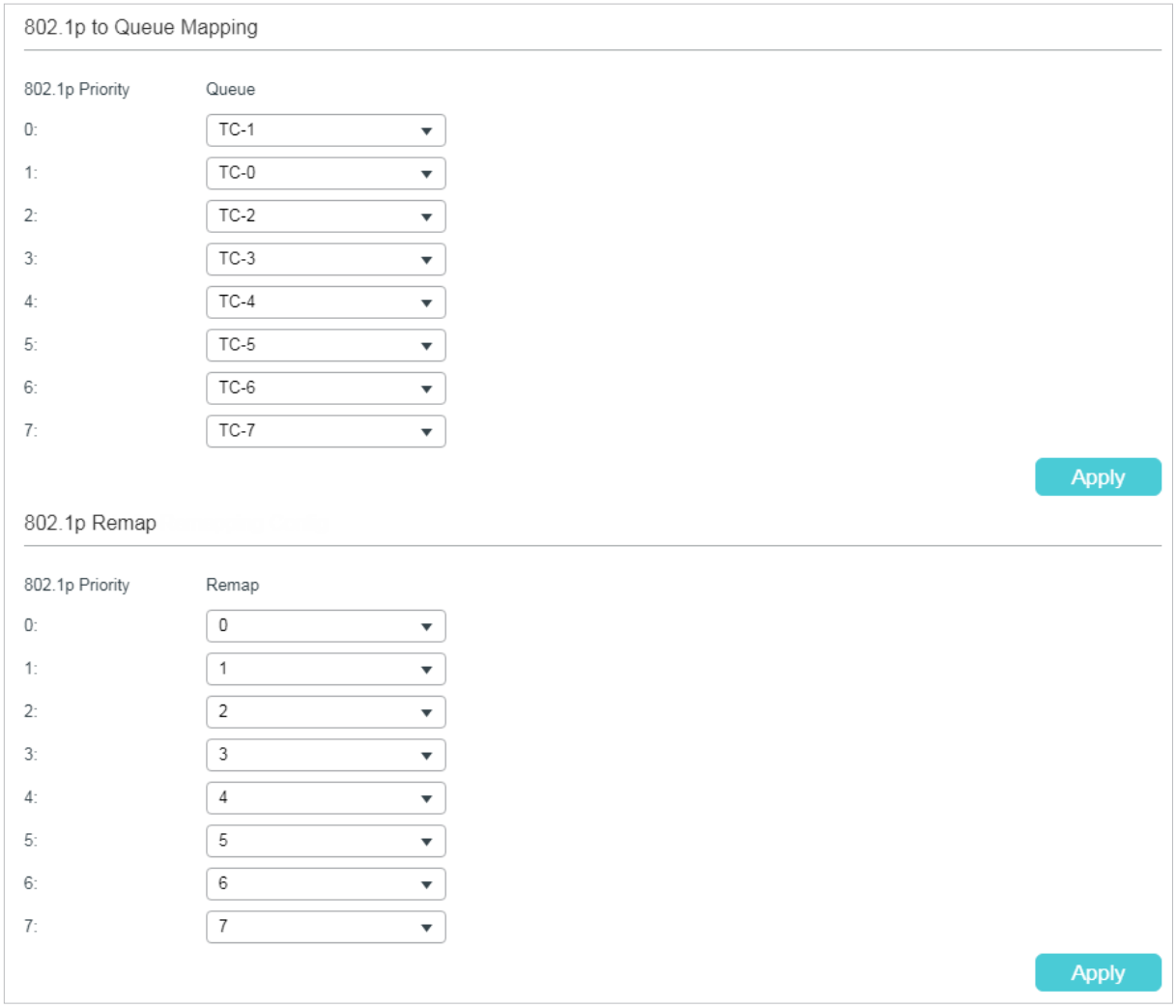
802.1p Priority	Wybierz dla portu mapowanie portu do priorytetu 802.1p. Pakiety przychodzące są w pierwszej kolejności mapowanie do priorytetu 802.1p na podstawie mapowania portu do 802.1p, następnie do kolejek TC w oparciu o mapowanie 802.1p do kolejek. Pakiety nietagowane z jednego portu będą mieć przydzieloną wartość priorytetu 802.1p, zgodnie z mapowaniem priorytetyzacji portu do priorytetu 802.1p.
Trust Mode	Ustaw ten tryb jako Untrusted. W trym trybie pakiety będą przetwarzane zgodnie z konfiguracją priorytetyzacji portu.

2) Kliknij **Apply**.

Konfiguracja mapowania 802.1p do kolejek

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 1-2 Konfiguracja mapowania 802.1p do kolejek



W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

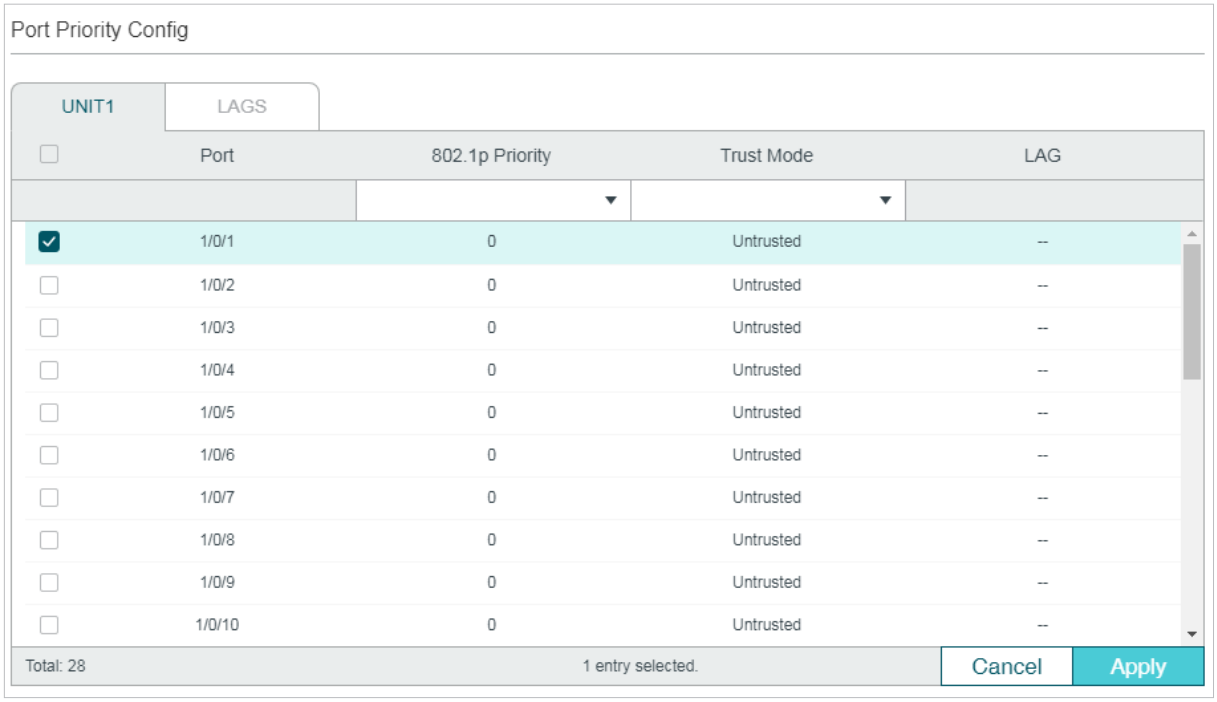
802.1p Priority	Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service.
Queue	Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce.

1.1.2 Konfiguracja priorytetyzacji 802.1p

Konfiguracja Trust Mode

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 1-3 Konfiguracja Trust Mode



Wykonaj poniższe kroki, aby skonfigurować trust mode:

1) Wybierz porty i ustaw trust mode jako Trust 802.1p.

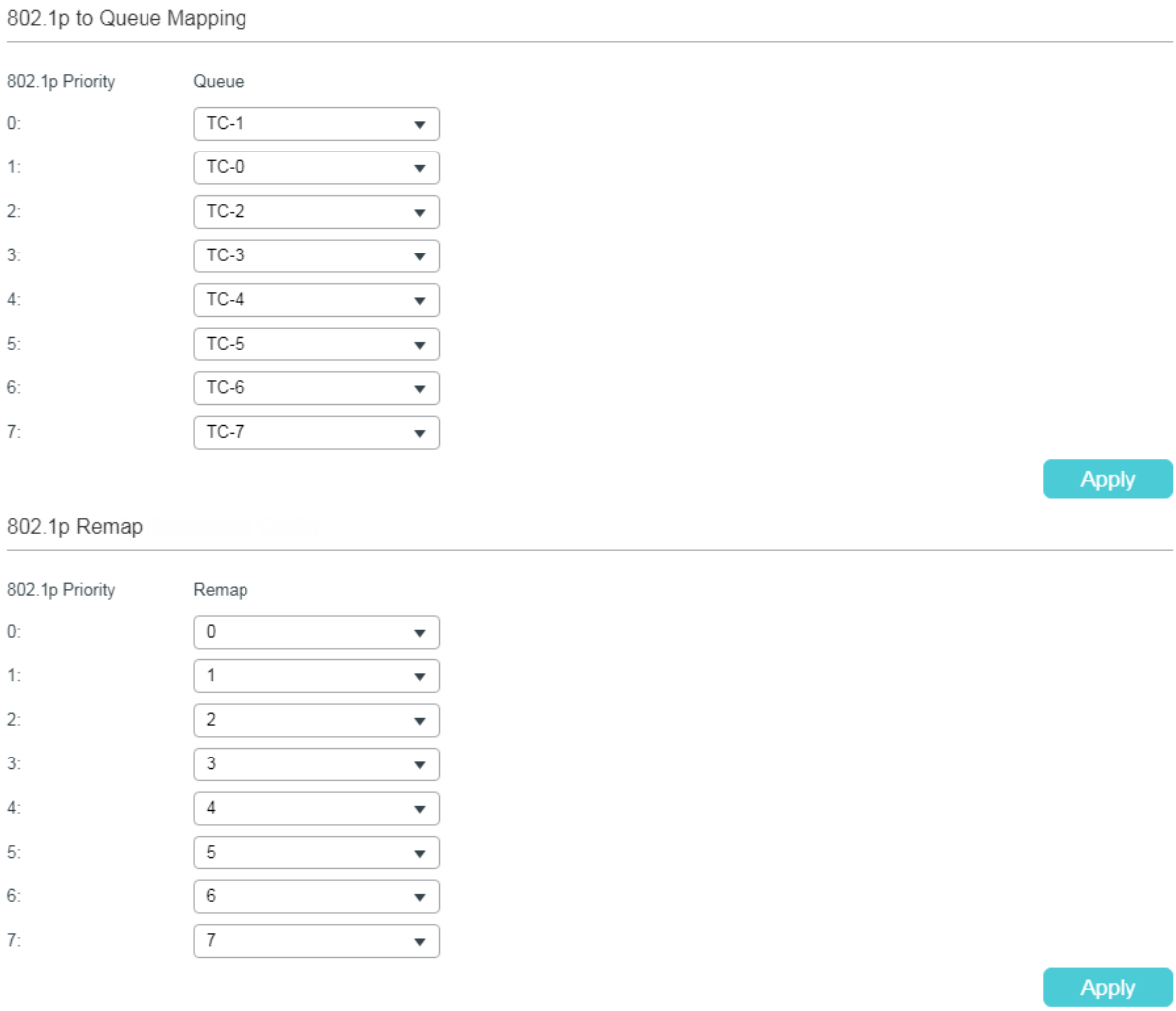
Trust Mode	Ustaw ten tryb jako Trust 802.1p. W tym trybie pakiety tagowane będą przetwarzane zgodnie z konfiguracją priorytetyzacji 802.1p, a pakiety nietagowane zgodnie z konfiguracją priorytetyzacji portu.

2) Kliknij **Apply**.

Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 1-4 Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p



Wykonaj poniższe kroki, aby skonfigurować parametry priorytetyzacji 802.1p:

1) W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

802.1p Priority	Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service. Standard IEEE 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI są określane priorytetem 802.1p i wykorzystywane do określania priorytetu pakietów warstwy 2. Ta funkcja wymaga pakietów z tagiem VLAN.
Queue	Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce.

2) (Opcjonalnie) W sekcji **802.1p Remap** skonfiguruj 802.1p na mapowania 802.1p i kliknij **Apply**.

802.1p Priority	Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service. Standard IEEE 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI są określane priorytetem 802.1p i wykorzystywane do określania priorytetu pakietów warstwy 2. Ta funkcja wymaga pakietów z tagiem VLAN.
Remap	Wybierz priorytety 802.1p, do których oryginalne priorytety 802.1p będą remapowane. Remapowanie 802.1p służy modyfikacji priorytetów 802.1p pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami 802.1p, zmieni wartość priorytetów 802.1p zgodnie z mapą.

Uwaga:

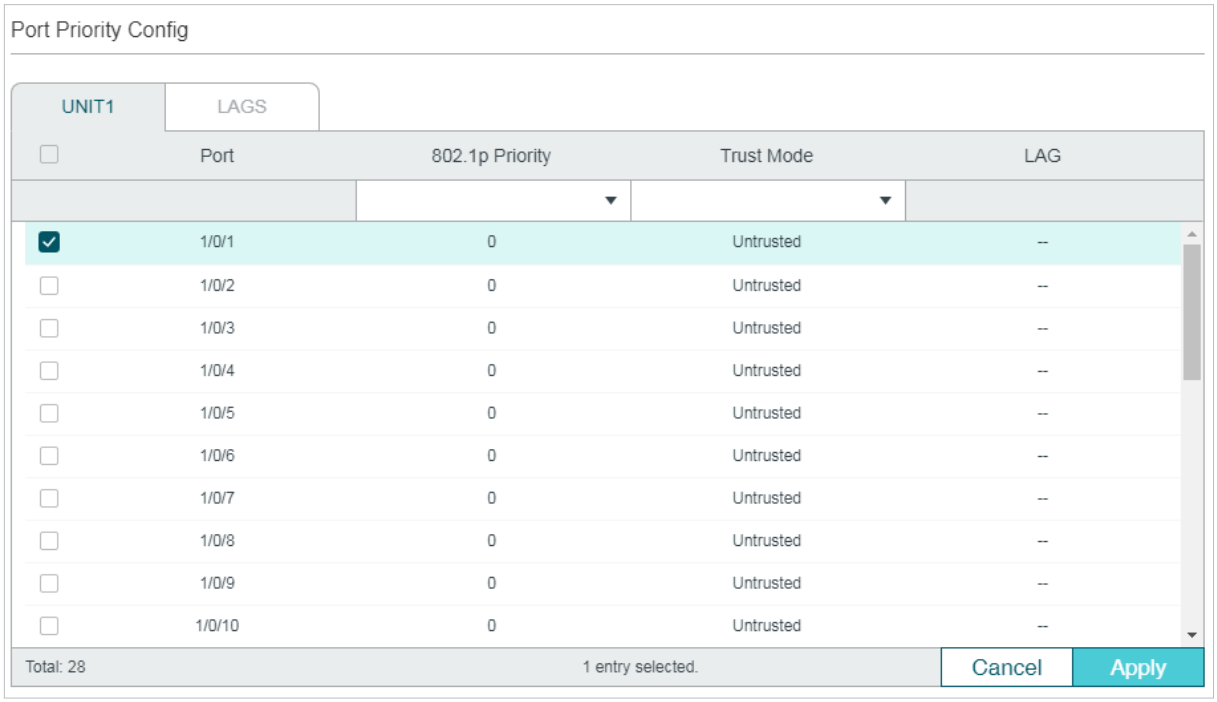
W trybie Trust 802.1p pakietom nietagowanym zostanie przydzielony priorytet 802.1p w oparciu o mapowanie portu do 802.1p i zostaną one przesłane zgodnie z mapowaniem 802.1p do kolejek.

1.1.3 Konfiguracja priorytetyzacji DSCP

■ Konfiguracja Trust Mode

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 1-5 Konfiguracja Trust Mode



Wykonaj poniższe kroki, aby skonfigurować trust mode:

1) Wybierz porty i ustaw trust mode jako Trust DSCP.

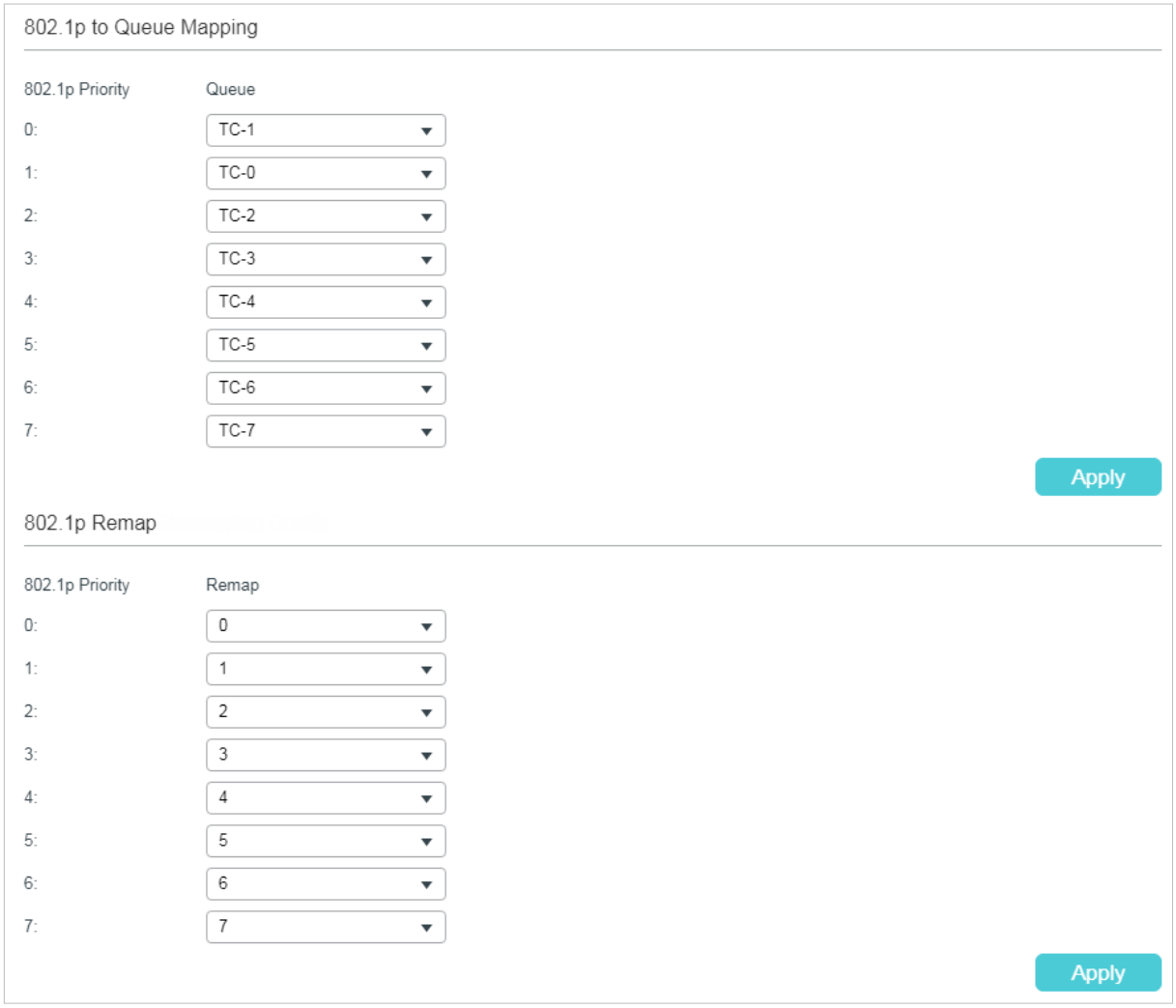
Trust Mode	Ustaw ten tryb jako Trust DSCP. W tym trybie pakiety IP będą przetwarzane zgodnie z konfiguracją priorytetyzacji DSCP, a pakiety non-IP zgodnie z konfiguracją priorytetyzacji portu.

2) Kliknij **Apply**.

Konfiguracja mapowania 802.1p do kolejek

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 1-6 Konfiguracja mapowania 802.1p do kolejek



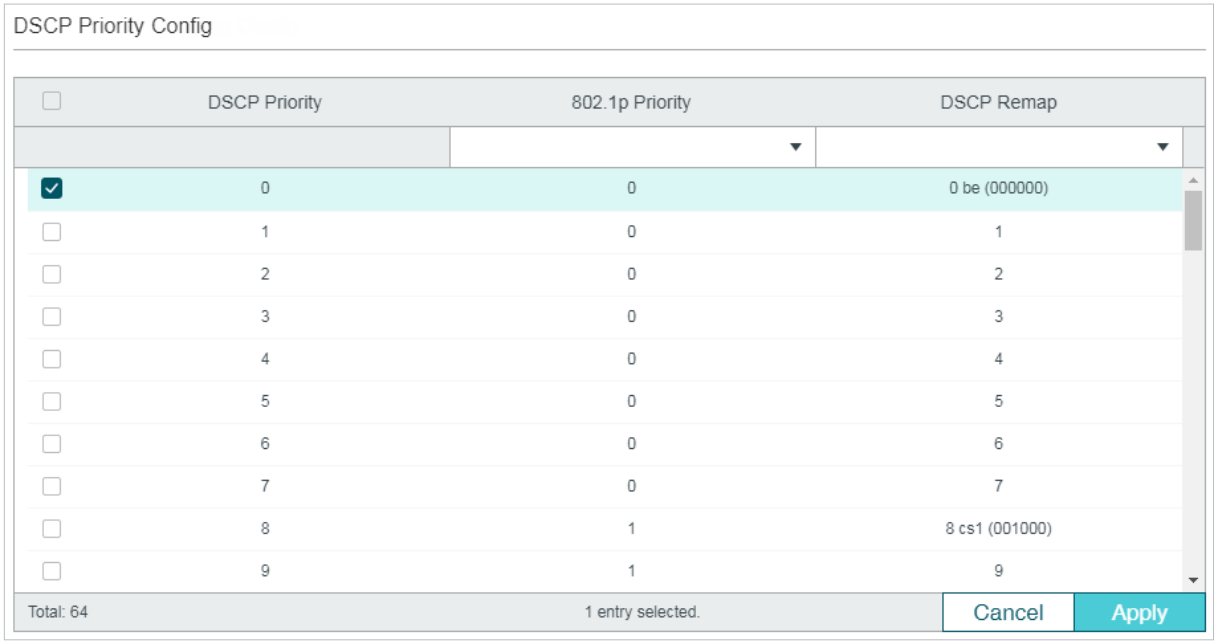
W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

802.1p Priority	Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service.
Queue	Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce.

■ Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP

Wybierz z menu **QoS > Class of Service >DSCP Priority**, aby wyświetlić poniższą stronę.

Rys. 1-7 Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP



Wykonaj poniższe kroki, aby skonfigurować priorytetyzację DSCP:

1) W sekcji **DSCP Priority Config** skonfiguruj mapowanie 802.1p i remapowanie DSCP.

DSCP Priority	Wartość priorytetu DSCP. Priorytetyzacja DSCP służy klasyfikacji pakietów w oparciu o wartość DSCP i mapowaniu ich do różnych kolejek. ToS (Type of Service) to część nagłówka IP, a DSCP wykorzystuje pierwsze sześć bitów ToS do ustalanie priorytetów pakietów IP. Wartości DSCP wahają się od 0 do 63.
802.1p Priority	Określ mapowanie DSCP do 802.1p. Pakiety przychodzące są najpierw mapowane do priorytetu 802.1p, w oparciu o mapowania DSCP do 802.1p, a następnie do kolejek TC, zgodnie z mapowaniami 802.1p do kolejek. Nietagowanym pakietom IP z żądaną wartością DSCP będą nadawane wartości priorytetów 802.1p, zgodnie z mapowaniem DSCP do 802.1p.
DSCP Remap	(Opcjonalnie) Wybierz priorytet DSCP, do którego oryginalny priorytet DSCP zostanie zremapowany. Gdy przełącznik wykryje pakiety z żądaną wartością DSCP, zmieni wartość pakietów DSCP zgodnie z mapą.

2) Kliknij **Apply**.

Uwaga:

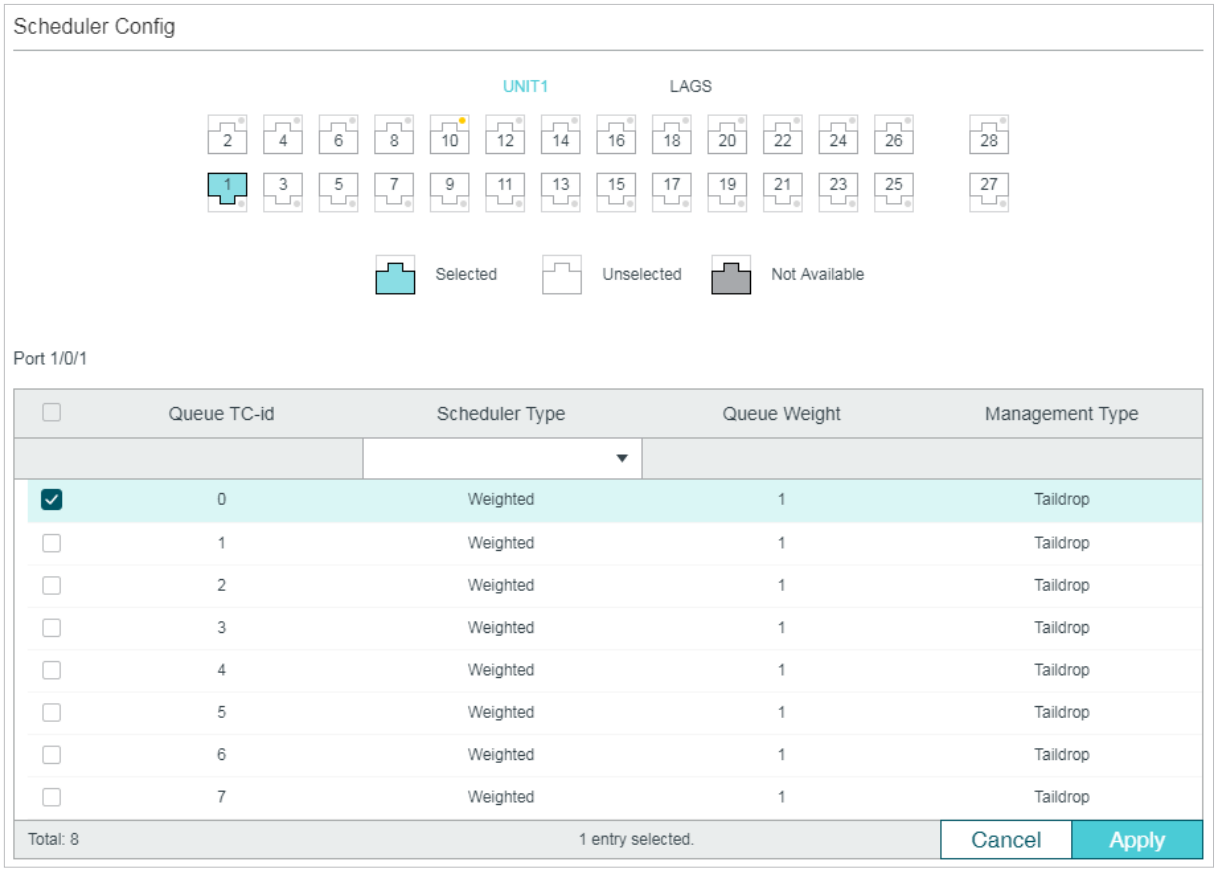
W trybie Trust DSCP pakietom non-IP zostanie nadany priorytet 802.1p w oparciu o mapowanie portu do 802.1p i zostaną one przesłane zgodnie z mapowaniem 802.1p do kolejek.

1.1.4 Konfiguracja ustawień harmonogramu

Dostosuj ustawienia harmonogramu, aby kontrolować sekwencję przesyłania różnych kolejek TC w przypadku przeciążenia.

Wybierz z menu **QoS > Class of Service > Scheduler Settings,** aby wyświetlić poniższą stronę.

Rys. 1-8 Konfiguracja ustawień harmonogramu



Wykonaj poniższe kroki, aby skonfigurować tryb harmonogramu:

1) W sekcji **Scheduler Config** wybierz port.
2) Wybierz kolejki i skonfiguruj parametry.

Queue TC-id	ID kolejki priorytetyzacji.
Scheduler Type	Wybierz typ harmonogramu dla danej kolejki. W przypadku przeciążenia sieci, kolejka ruchu wychodzącego określi sekwencję przesyłania pakietów zgodnie z wybranym typem. **Strict:** W tym trybie kolejka ruchu wychodzącego skorzysta z SP (Strict Priority) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, ruch będzie przesyłany ściśle według priorytetów kolejek. Kolejka o wyższym poziomie priorytetu wykorzystuje całą przepustowość. Pakiety w kolejkach o niższym poziomie priorytetu są wysyłane tylko wtedy, gdy kolejka o wyższym poziomie priorytetu jest pusta. **Weighted:** W tym trybie kolejka ruchu wychodzącego skorzysta z WRR (Weighted Round Robin) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, cały ruch będzie przesyłany, ale przepustowość sieci zostanie przydzielona kolejkom na podstawie wagi kolejek.

Queue Weight	Określ wagę danę kolejki. Ta wartość może być ustawiona tylko w trybie Weighted. Prawidłowe wartości wahają się od 1 do 127.
Management Type	Typ zarządzania kolejek. Przełącznik obsługuje tryb Taildrop. Gdy przesyłany ruch przekroczy limit, nadmiarowy ruch zostanie odrzucony.

3) Kliknij **Apply**.

Uwaga:

Funkcja ACL Redirect sprawia, że przełącznik mapuje wszystkie pakiety, który spełniają reguły ACL do nowej kolejki TC, niezależnie od ustawień relacji mapowań, które zostały skonfigurowane w tej sekcji.

1.2 Przez CLI

1.2.1 Konfiguracja priorytetyzacji portu

- Konfiguracja Trust Mode i mapowania portu do 802.1p

Wykonaj poniższe kroki, aby skonfigurować trust mode i mapowanie portu do 802.1p:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Wybierz trust mode dla portu. Domyślnym trybem jest untrust. Poniższe polecenie ustawia trust mode jako untrust. *untrust:* Ustawia dla portu tryb untrust. W tym trybie pakiety będą przetwarzane zgodnie z konfiguracją priorytetyzacji portu.
Krok 4	**qos port-priority {***dot1p-priority***}** Wybierz dla portu mapowanie portu do priorytetu 802.1p. Pakiety przychodzące są w pierwszej kolejności mapowanie do priorytetu 802.1p na podstawie mapowania portu do 802.1p, następnie do kolejek TC w oparciu o mapowanie 802.1p do kolejek. Pakiety nietagowane z jednego portu będą mieć przydzieloną wartość priorytetu 802.1p, zgodnie z mapowaniem priorytetyzacji portu do priorytetu 802.1p. *dot1p-priority:* Uzupełnij priorytet 802.1p wartością z przedziału 0 - 7. Wartością domyślną jest 0.
Krok 5	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź konfigurację trust mode dla portów.

Krok 6	**show qos port-priority interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź mapowania portu do 802.1p.
Krok 7	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

■ Konfiguracja mapowania 802.1p do kolejek

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej
Krok 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority:* Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7. *tc-queue:* Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.
Krok 3	**show qos cos-map** Sprawdź mapowanie 802.1p do kolejek.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako untrust, mapowania portu 1/0/1 do priorytetu 1 802.1p i mapowania priorytetu 1 802.1p do TC3:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode untrust

Switch(config-if)#qos port-priority 1

Switch(config-if)#exit

Switch(config)#qos cos-map 1 3

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

```
Port       Trust Mode      LAG
--------   ---------       --------
Gi1/0/1    untrust         N/A
```

Switch(config)#show qos port-priority interface gigabitEthernet 1/0/1

```
Port       CoS Value       LAG
--------   ---------       --------
Gi1/0/1    CoS  1          N/A
```

Switch(config)#show qos cos-map

```
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value |0     |1    |2     |3     |4     |5     |6    |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC              |TC0 |TC3 |TC2  |TC3  |TC4 |TC5  |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja priorytetyzacji 802.1p

- Konfiguracja Trust Mode

Wykonaj poniższe kroki, aby skonfigurować trust mode:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej

Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Wybierz trust mode dla portu. Domyślnie ustawiony jest tryb untrust. Za pomocą poniższego polecenia ustawimy trust mode jako dot1p. *dot1p:* Ustawia tryb portów jako dot1p. W tym trybie pakiety tagowane będą przetwarzane zgodnie z konfiguracją priorytetyzacji 802.1p, a pakiety nietagowane zgodnie z konfiguracją priorytetyzacji portu.
Krok 4	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź trust mode portów.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

■ Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek i remapowanie 802.1p:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej
Krok 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiednich kolejkach. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority:* Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7. *tc-queue:* Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.
Krok 3	**qos dot1p-remap {***dot1p-priority***} {***new-dot1p-priority***}** (Opcjonalnie) Określ mapowania 802.1p do 802.1p. Remapowanie 802.1p służy modyfikacji priorytetów 802.1p pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami 802.1p, zmieni wartość priorytetów 802.1p zgodnie z mapą. Domyślnie oryginalny priorytet 802.1p o wartości 0 jest mapowany do priorytetu 802.1p o wartości 0, oryginalny priorytet 802.1p o wartości 1 jest mapowany do priorytetu 802.1p o wartości 1, itd. *dot1p-priority:* Podaj oryginalny priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7. *new-dot1p-priority:* Podaj nowy priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.

Krok 4	**show qos cos-map** Sprawdź mapowania 802.1p do kolejek.
Krok 5	**show qos dot1p-remap** Sprawdź mapowania 802.1p do 802.1p.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

W trybie Trust 802.1p pakietom nietagowanym będą przydzielane priorytety 802.1p w oparciu o mapowanie portu do 802.1p i będą one przesyłane zgodnie z mapowaniem 802.1p do kolejek.

Poniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako dot1p, mapowanie priorytetu 3 802.1p do TC4 i konfigurację mapowania oryginalnego priorytetu 1 802.1p do priorytetu 3 802.1p:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode dot1p

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

Switch(config)#qos dot1p-remap 1 3

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

```
Port       Trust Mode      LAG
--------   ---------       --------
Gi1/0/1    trust 802.1P    N/A
```

Switch(config)#show qos cos-map

```
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value  |0     |1     |2     |3     |4     |5     |6    |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC             |TC0  |TC1  |TC2  |TC4  |TC4  |TC5  |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#show qos dot1p-remap

Dot1p Value	0	**1**	2	3	4	5	6	7	LAG
Dot1p Remap	0	**3**	2	3	4	5	6	7	N/A

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Konfiguracja priorytetyzacji DSCP

■ Konfiguracja Trust Mode

Wykonaj poniższe kroki, aby skonfigurować trust mode:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**qos trust mode {***untrust* **|** *dot1p* **|** *dscp***}** Wybierz trust mode dla portu. Domyślnym trybem jest untrust. Poniższe polecenie ustawia trust mode jako dscp. *dscp:* Ustawia tryb portu jako dscp. W tym trybie pakiety IP będą przetwarzane zgodnie z konfiguracją priorytetyzacji DSCP, a pakiety non-IP zgodnie z konfiguracją priorytetyzacji portu.
Krok 4	**show qos trust interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź trust mode portów.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

■ Konfiguracja mapowania 802.1p do kolejek

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej

Krok 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiednich kolejkach. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority:* Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7. *tc-queue:* Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.
Krok 3	**show qos cos-map** Sprawdź mapowania 802.1p do kolejek.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

■ Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP Remp

Wykonaj poniższe kroki, aby skonfigurować mapowanie DSCP do 802.1p i remapowanie DSCP:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej
Krok 2	**qos dscp-map {***dscp-value-list***} {***dot1p-priority***}** Określ mapowanie DSCP do 802.1p. Pakiety przychodzące są najpierw mapowane do priorytetu 802.1p, w oparciu o mapowania DSCP do 802.1p, a następnie do kolejek TC, zgodnie z mapowaniami 802.1p do kolejek. Nietagowanym pakietom IP z żądaną wartością DSCP będą nadawane wartości priorytetów 802.1p, zgodnie z mapowaniem DSCP do 802.1p. Domyślnie priorytety 0-7 DSCP są mapowanie do priorytetu 802.1p o wartości 0, priorytety 8-15 DSCP są mapowane do priorytetu 802.1p o wartości 1, itd. *dscp-value-list:* Podaj listę wartości DSCP w formacie “1-3,5,7”. Prawidłowe wartości wahają się od 0 do 63. *dot1p-priority:* Określ priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.
Krok 3	**qos dscp-remap {***dscp-value-list***} {***dscp-remap-value***}** (Opcjonalnie) Określ mapowania DSCP do DSCP. Remapowanie DSCP służy modyfikacji priorytetów DSCP pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami DSCP, zmieni wartość priorytetów DSCP zgodnie z mapą. Domyślnie oryginalny priorytet DSCP o wartości 0 jest mapowany do priorytetu DSCP o wartości 0, oryginalny priorytet DSCP o wartości 1 jest mapowany do priorytetu DSCP o wartości 1, itd. *dscp-value-list:* Podaj listę oryginalnych priorytetów w formacie “1-3,5,7”. Prawidłowe wartości wahają się od 0 do 63. *dscp-remap-value:* Podaj nowy priorytet DSCP. Prawidłowe wartości wahają się od 0 do 63.

Krok 4	**show qos dscp-map** Sprawdź mapowania DSCP do kolejek.
Krok 5	**show qos dscp-remap** Sprawdź mapowania DSCP do DSCP.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

W trybie Trust DSCP pakietom non-IP będą przydzielane priorytety 802.1p w oparciu o mapowanie portu do 802.1p i będą one przesyłane zgodnie z mapowaniem 802.1p do kolejek.

Poniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako dscp, mapowanie priorytetu 3 802.1p do TC4, mapowanie priorytetów 1-3,5,7 DSCP do priorytetu 3 802.1p i konfigurację mapowania oryginalnego priorytetu 9 DSCP do priorytetu 5 DSCP:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos trust mode dscp

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

Switch(config)#qos dscp-map 1-3,5,7 3

Switch(config)#qos dscp-remap 9 5

Switch(config)#show qos trust interface gigabitEthernet 1/0/1

```
Port        Trust Mode     LAG
--------    ---------      ------
Gi1/0/1     trust DSCP     N/A
```

Switch(config)#show qos cos-map

```
---------------+-----+-----+-----+-----+-----+-----+----+----
Dot1p Value |0     |1    |2    |3    |4    |5    |6   |7
---------------+-----+-----+-----+-----+-----+-----+----+----
TC              |TC0 |TC1 |TC2 |TC4 |TC4 |TC5 |TC6 |TC7
---------------+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#show qos dscp-map

DSCP:	0	**1**	**2**	**3**	4	**5**	6	**7**
DSCP to 802.1P	0	**3**	**3**	**3**	0	**3**	0	**3**

DSCP:	8	9	10	11	12	13	14	15
DSCP to 802.1P	1	1	1	1	1	1	1	1

DSCP:	16	17	18	19	20	21	22	23
DSCP to 802.1P	2	2	2	2	2	2	2	2

DSCP:	24	25	26	27	28	29	30	31
DSCP to 802.1P	3	3	3	3	3	3	3	3

DSCP:	32	33	34	35	36	37	38	39
DSCP to 802.1P	4	4	4	4	4	4	4	4

DSCP:	40	41	42	43	44	45	46	47
DSCP to 802.1P	5	5	5	5	5	5	5	5

DSCP:	48	49	50	51	52	53	54	55
DSCP to 802.1P	6	6	6	6	6	6	6	6

DSCP:	56	57	58	59	60	61	62	63
DSCP to 802.1P	7	7	7	7	7	7	7	7

Switch(config)#show qos dscp-remap

DSCP:	0	1	2	3	4	5	6	7
DSCP remap value	0	1	2	3	4	5	6	7

DSCP:	8	**9**	10	11	12	13	14	15

```
DSCP remap value  8   5   10  11  12  13  14  15
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             16  17  18  19  20  21  22  23
DSCP remap value  16  17  18  19  20  21  22  23
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             24  25  26  27  28  29  30  31
DSCP remap value  24  25  26  27  28  29  30  31
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             32  33  34  35  36  37  38  39
DSCP remap value  32  33  34  35  36  37  38  39
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             40  41  42  43  44  45  46  47
DSCP remap value  40  41  42  43  44  45  46  47
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             48  49  50  51  52  53  54  55
DSCP remap value  48  49  50  51  52  53  54  55
                  ----- ----- ----- ----- ----- ----- ----- -----
DSCP:             56  57  58  59  60  61  62  63
DSCP remap value  56  57  58  59  60  61  62  63
                  ----- ----- ----- ----- ----- ----- ----- -----
```

Switch(config-if)#end

Switch#copy running-config startup-config

1.2.4 Konfiguracja ustawień harmonogramu

Wykonaj poniższe kroki, aby dostosować ustawienia harmonogramu, w celu kontroli sekwencji przesyłania różnych kolejek TC w przypadku przeciążenia sieci.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.

Krok 3	**qos queue** *tc-queue* **mode {**sp **|** wrr**} [weight** *weight***]** Wybierz typ harmonogramu dla danej kolejki. W przypadku przeciążenia sieci, kolejka ruchu wychodzącego określi sekwencję przesyłania pakietów zgodnie z wybranym typem. Domyślnie ustawionym trybem jest wrr, a wagą wszystkich kolejek wartość 1. *tc-queue*: Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7. sp: W tym trybie kolejka ruchu wychodzącego skorzysta z SP (Strict Priority) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, ruch będzie przesyłany ściśle według priorytetów kolejek. Kolejka o wyższym poziomie priorytetu wykorzystuje całą przepustowość. Pakiety w kolejkach o niższym poziomie priorytetu są wysyłane tylko wtedy, gdy kolejka o wyższym poziomie priorytetu jest pusta. wrr: W tym trybie kolejka ruchu wychodzącego skorzysta z WRR (Weighted Round Robin) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, cały ruch będzie przesyłany, ale przepustowość sieci zostanie przydzielona kolejkom na podstawie wagi kolejek. *weight*: Określ wagę danę kolejki. Ta wartość może być ustawiona tylko w trybie wrr. Prawidłowe wartości wahają się od 1 do 127.
Krok 4	**show qos queue interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź ustawienia harmonogramu.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Funkcja ACL Redirect sprawia, że przełącznik mapuje wszystkie pakiety, który spełniają reguły ACL do nowej kolejki TC, niezależnie od ustawień relacji mapowań, które zostały skonfigurowane w tej sekcji. .

Poniższy schemat przedstawia przykładową konfigurację ustawień harmonogramu dla portu 1/0/1. Tryb harmonogramu TC1 zostanie skonfigurowany na tryb sp, tryb harmonogramu TC4 na tryb wrr, a waga kolejki na 5.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#qos queue 1 **mode** sp

Switch(config-if)#qos queue 4 **mode** wrr **weight** 5

Switch(config-if)#show qos queue interface gigabitEthernet 1/0/1

Gi1/0/1----LAG: N/A

Queue Schedule Mode Weight

----- ---------- -----

TC0	WRR	1
TC1	Strict	N/A
TC2	WRR	1
TC3	WRR	1
TC4	WRR	5
TC5	WRR	1
TC6	WRR	1
TC7	WRR	1

Switch(config-if)#end

Switch#copy running-config startup-config

2 Konfiguracja kontroli przepustowości

Konfiguracja kontroli przepustowości umożliwia:

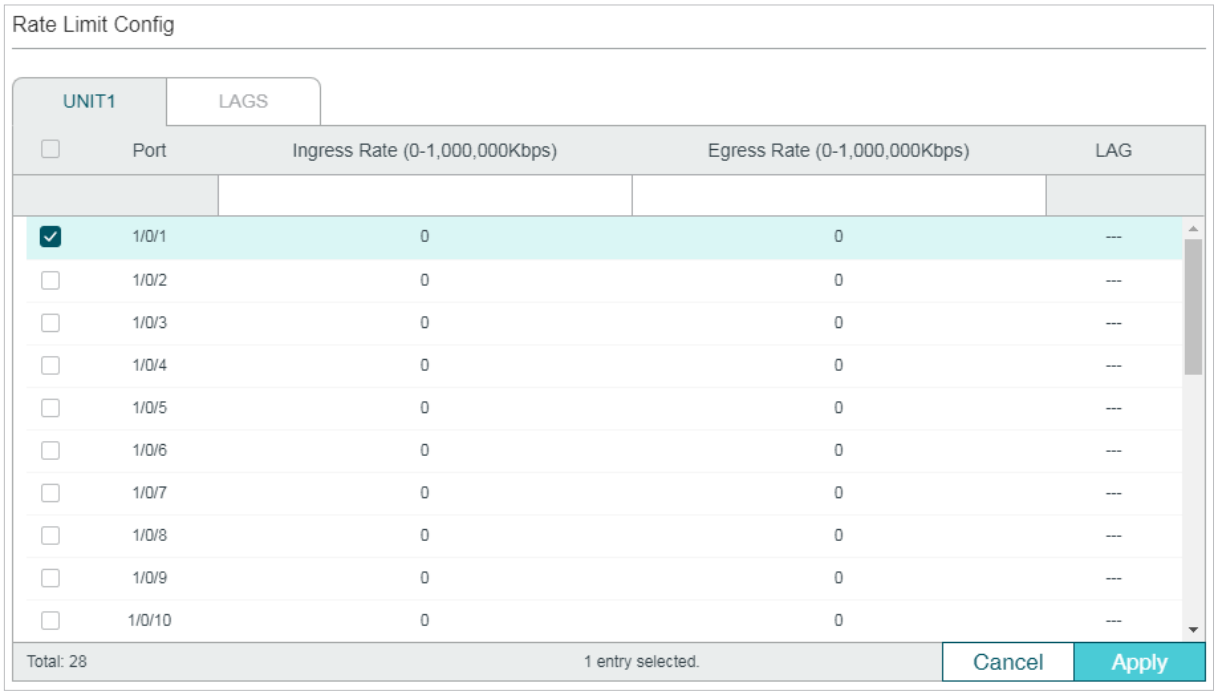
- Konfigurację limitu prędkości
- Konfigurację Storm Control

2.1 Przez GUI

2.1.1 Konfiguracja limitu prędkości

Wybierz z menu **QoS > Bandwidth Control > Rate Limit**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja limitu prędkości



Wykonaj poniższe kroki, aby skonfigurować funkcję limitu prędkości:

1) Wybierz porty i skonfiguruj górny limit prędkości odbierania i wysyłania pakietów.

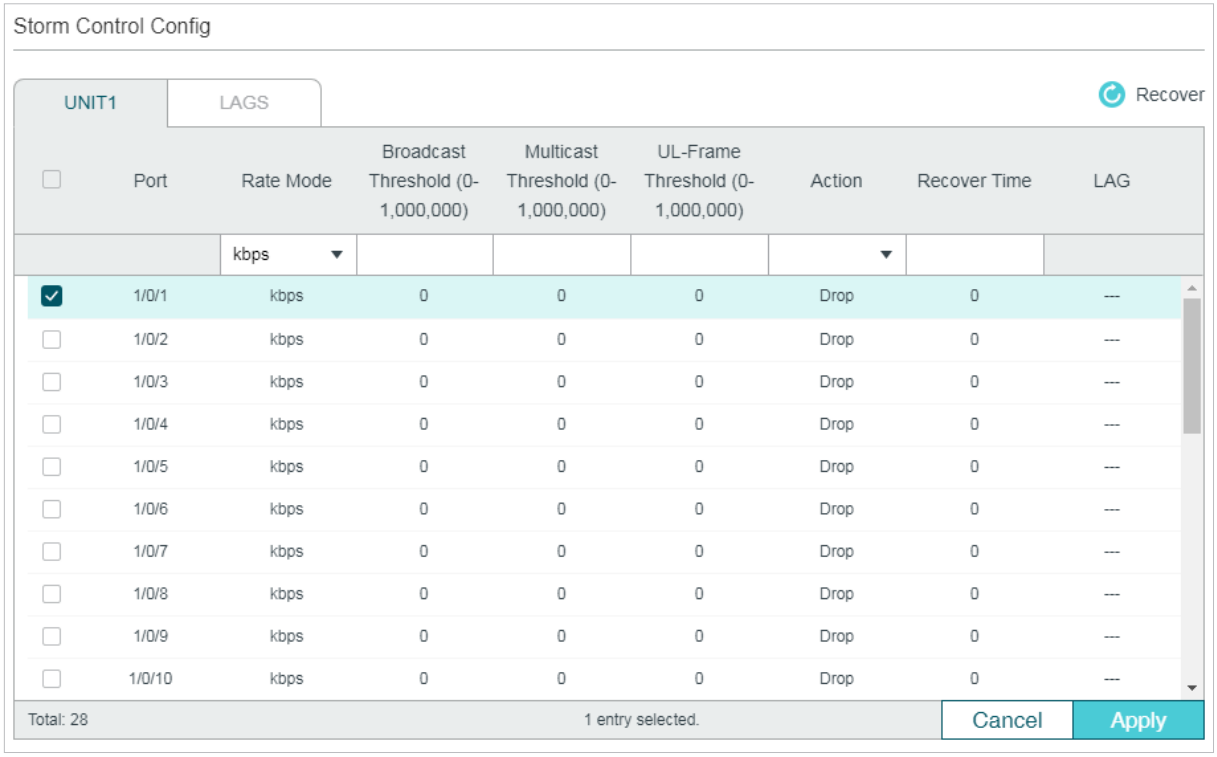
Ingress Rate (0-1,000,000Kbps)	Skonfiguruj górny limit prędkości odbierania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 kb/s, a 0 oznacza, że limit prędkości na wejściu jest wyłączony.
Egress Rate (0-1,000,000Kbps)	Skonfiguruj przepustowość wysyłania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 Kb/s, a 0 oznacza, że limit prędkości na wyjściu jest wyłączony.

2) Kliknij **Apply**.

2.1.2 Konfiguracja Storm Control

Wybierz z menu **QoS > Bandwidth Control > Storm Control,** aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja Storm Control



Wykonaj poniższe kroki, aby skonfigurować funkcje Storm Control:

1) Wybierz port i skonfiguruj górny limit prędkości przesyłania pakietów broadcast, pakietów multicast i ramek unknown unicast (UL-frames).

Rate Mode	Wybierz tryb prędkości dla progu transmisji broadcast, progu transmisji mutlicastowej i progu UL-Frame na danym porcie. **kbps:** Przełącznik ograniczy maksymalną prędkość w kilobitach na sekundę dla określonych rodzajów ruchu. **ratio:** Przełącznik ograniczy przydzielanie przepustowości dla określonych rodzajów ruchu.
Broadcast Threshold (0-1,000,000)	Podaj górny limit prędkości odbierania pakietów broadcast. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji broadcast jest wyłączony. Transmisja broadcast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.
Multicast Threshold (0-1,000,000)	Podaj górny limit prędkości odbierania pakietów multicast. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji multicastowej jest wyłączony. Transmisja multicastowa, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.

UL-Frame Threshold (0-1,000,000)	Podaj górny limit prędkości odbierania UL-frames. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji unknown unicast jest wyłączony. Transmisja unknown unicast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.
Action	Wybierz działanie, które podejmie przełącznik, gdy transmisja przekroczy ustawiony limit. **Drop:** Działanie odrzucające. Port odrzuci kolejne pakiety, gdy transmisja przekroczy dozwolony limit. **Shutdown:** Działanie wyłączające. Port zostanie wyłączony, gdy transmisja przekroczy dozwolony limit.
Recover Time	Podaj czas do przywrócenia portu. Uzupełnienie tej wartości możliwe jest tylko, gdy ustawionym działaniem jest Shutdown. Prawidłowe wartości wahają się od 0 do 3600 sekund. Gdy port zostaje wyłączony, ponownie może być uruchomiony dopiero, gdy upłynie czas do przywrócenia portu. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie, więc trzeba go włączyć ręcznie.

2) Kliknij **Apply**.

Uwaga:

Rate limit / storm control powinny mieć tą samą wartość dla portów z tej samej grupy agregacji łączy, aby agregacja portów powiodła się.

2.2 Przez CLI

2.2.1 Konfiguracja limitu prędkości

Wykonaj poniższe kroki, aby skonfigurować górny limit prędkości odbierania i wysyłania pakietów na porcie:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.

Krok 3	**bandwidth {ingress** *ingress-rate* **| egress** *egress-rate***}** Skonfiguruj górny limit prędkości odbierania i wysyłania pakietów na porcie. *ingress-rate:* Skonfiguruj górny limit prędkości odbierania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 kb/s. *egress-rate:* Skonfiguruj przepustowość wysyłania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 Kb/s.
Krok 4	**show bandwidth interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź limit prędkości na wejściu/wyjściu dla przesyłania pakietów na porcie lub w grupie agregacji łączy. Jeżeli żaden port lub LAG nie zostanie podany, polecenie pokaże górny limit prędkości na wejściu/wyjściu dla wszystkich portów lub grup agregacji łączy.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację prędkości na wejściu do wartości 5120 kb/s prędkości na wyjściu do wartości 1024 Kb/s dla portu 1/0/5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#bandwidth ingress 5120 **egress** 1024

Switch(config-if)#show bandwidth interface gigabitEthernet 1/0/5

Port	IngressRate(Kbps)	EgressRate(Kbps)	LAG
---	---	---	---
Gi1/0/5	5120	1024	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja Storm Control

Wykonaj poniższe kroki, aby skonfigurować górny limit prędkości przesyłania pakietów broadcast, pakietów multicast i ramek unknown unicast na porcie:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej

Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 3	**storm-control rate-mode {**kbps **|** ratio**}** Wybierz tryb prędkości dla progu transmisji broadcast, progu transmisji mutlicastowej i progu UL-Frame na danym porcie. kbps: Przełącznik ograniczy maksymalną prędkość w kilobitach na sekundę dla określonych rodzajów ruchu. ratio: Przełącznik ograniczy przydzielanie przepustowości dla określonych rodzajów ruchu.
Krok 4	**storm-control broadcast** *rate* Podaj górny limit prędkości odbierania pakietów broadcast. Transmisja broadcast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action. *rate*: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.
Krok 5	**storm-control multicast** *rate* Podaj górny limit prędkości odbierania pakietów multicast. Transmisja multicastowa, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action. *rate*: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.
Krok 6	**storm-control unicast** *rate* Podaj górny limit prędkości odbierania UL-frames. Transmisja unknown unicast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action. *rate*: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.
Krok 7	**storm-control exceed {**drop **|** shutdown**} [recover-time** *time***]** Wybierz działanie i podaj czas do przywrócenia portu. Przełącznik podejmie to działanie, gdy transmisja przekroczy ustawiony limit. Domyślnym ustawieniem jest drop. drop**:** Działanie odrzucające. Port odrzuci kolejne pakiety, gdy transmisja przekroczy dozwolony limit. shutdown**:** Działanie wyłączające. Port zostanie wyłączony, gdy transmisja przekroczy dozwolony limit. *time*: Podaj czas do przywrócenia portu. Uzupełnienie tej wartości możliwe jest tylko, gdy ustawionym działaniem jest Shutdown. Prawidłowe wartości wahają się od 0 do 3600 sekund. Gdy port zostaje wyłączony, ponownie może być uruchomiony dopiero, gdy upłynie czas do przywrócenia portu. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie, więc trzeba go włączyć ręcznie.

Krok 8	**storm-control recover** (Opcjonalnie) Przywróć port ręcznie. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie. Musisz wtedy skorzystać z tego polecenia, aby przywrócić port ręcznie.
Krok 9	**show storm-control interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Sprawdź ustawienia storm control portu lub grupy agregacji łączy. Jeżeli żaden port lub LAG nie zostanie podany, polecenie pokaże ustawienia storm control dla wszystkich portów lub grup agregacji łączy.
Krok 10	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania górnego limitu prędkości dla pakietów broadcast jako 1024 kb/s, działania jako shutdown i czasu do przywrócenia portu jako 10 dla portu 1/0/5:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

T2600G-28TS(config-if)#storm-control rate-mode kbps

T2600G-28TS(config-if)#storm-control broadcast 1024

T2600G-28TS(config-if)#storm-control exceed shutdown **recover-time** 10

T2600G-28TS(config-if)#show storm-control interface gigabitEthernet 1/0/5

Port	Rate Mode	BcRate	McRate	UlRate	Exceed	Recover Time	LAG
Gi1/0/5	kbps	1024	0	0	shutdown	10	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3 Konfiguracja Voice VLAN

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji Voice VLAN:

1) Utwórz 802.1Q VLAN
2) Skonfiguruj adresy OUI
3) Skonfiguruj globalnie Voice VLAN
4) Dodaj porty do Voice VLAN-u

Wskazówki dotyczące konfiguracji

- Przed konfiguracją voice VLAN konieczne jest utworzenie 802.1Q VLAN dla transmisji głosowej. Szczegółowe informacje o konfiguracji 802.1Q VLAN znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.
- VLAN 1 jest domyślnym VLAN-em i nie można go skonfigurować do Voice VLAN-u.
- Tylko jeden VLAN może być Voice VLAN-em na przełączniku.

3.1 Przez GUI

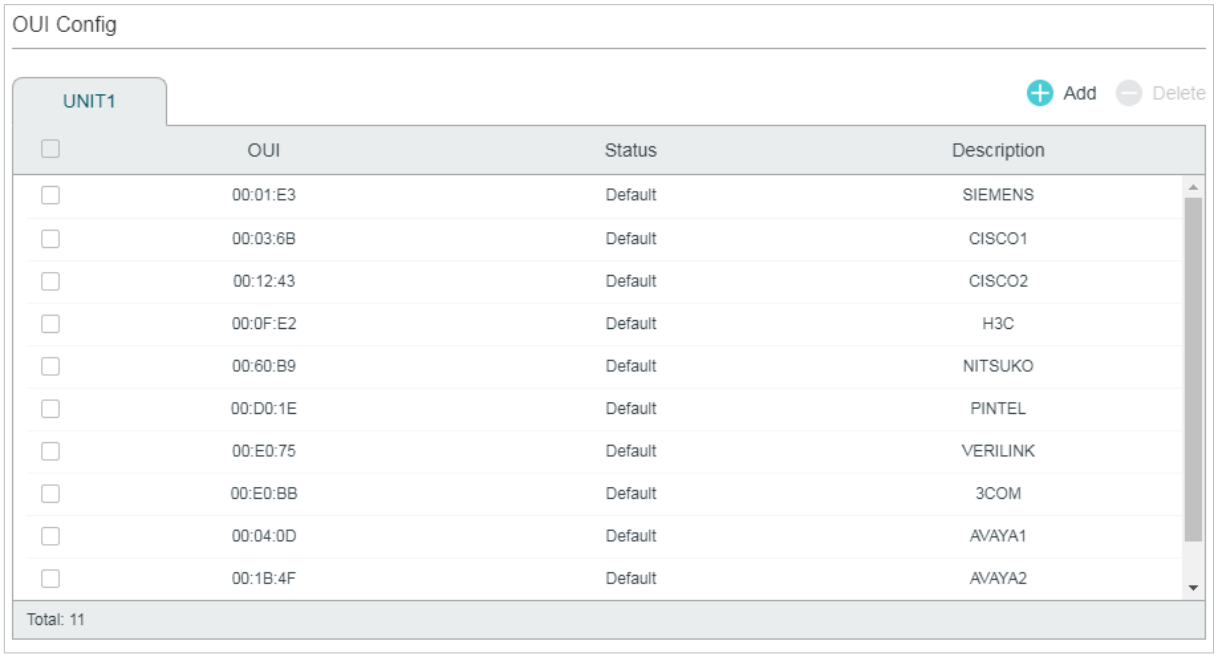
3.1.1 Konfiguracja adresów OUI

Adres OUI pełni rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Przełącznik wykorzystuje ten adres to identyfikowania pakietów voice.

Jeżeli w tabeli OUI nie ma adresu OUI twojego urządzenia głosowego, dodaj nowy adres OUI do tabeli.

Wybierz z menu **QoS > Voice VLAN > OUI Config**, aby wyświetlić poniższą stronę.

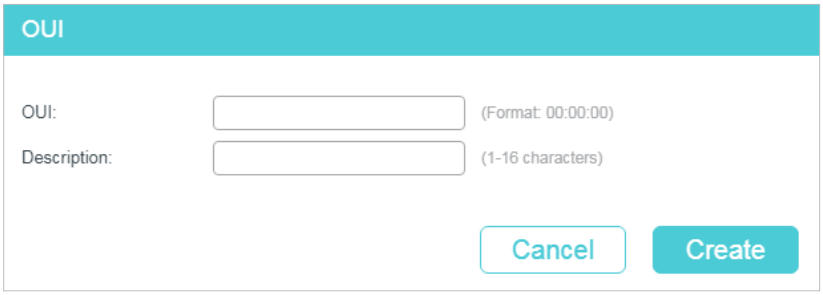
Rys. 3-1 Konfiguracja adresów OUI



Wykonaj poniższe kroki, aby skonfigurować adresy OUI:

1) Kliknij Add, aby wyświetlić poniższą stronę.

Rys. 3-2 Tworzenie wpisu OUI



2) Podaj adres OUI i uzupełnij opis.

OUI	Podaj adres OUI swojego urządzenia głosowego. Adres OUI potrzebny jest przełącznikowi do identyfikacji pakietów voice. Adres OUI to 24 pierwsze bity adresu MAC, pełniące rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Jeżeli źródłowy adres MAC pakietu jest zgodny z adresami OUI z listy OUI, przełącznik klasyfikuje pakiet jako pakiet voice i nadaje mu priorytet w transmisji.
Description	Uzupełnij opis adresu OUI dla jego łatwiejszej identyfikacji.

3) Kliknij **Create**.

3.1.2 Konfiguracja globalna Voice VLAN

Wybierz z menu **QoS > Voice VLAN > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja globalna Voice VLAN

Wykonaj poniższe kroki, aby skonfigurować globalnie Voice VLAN:

1) Włącz funkcję Voice VLAN i skonfiguruj parametry.

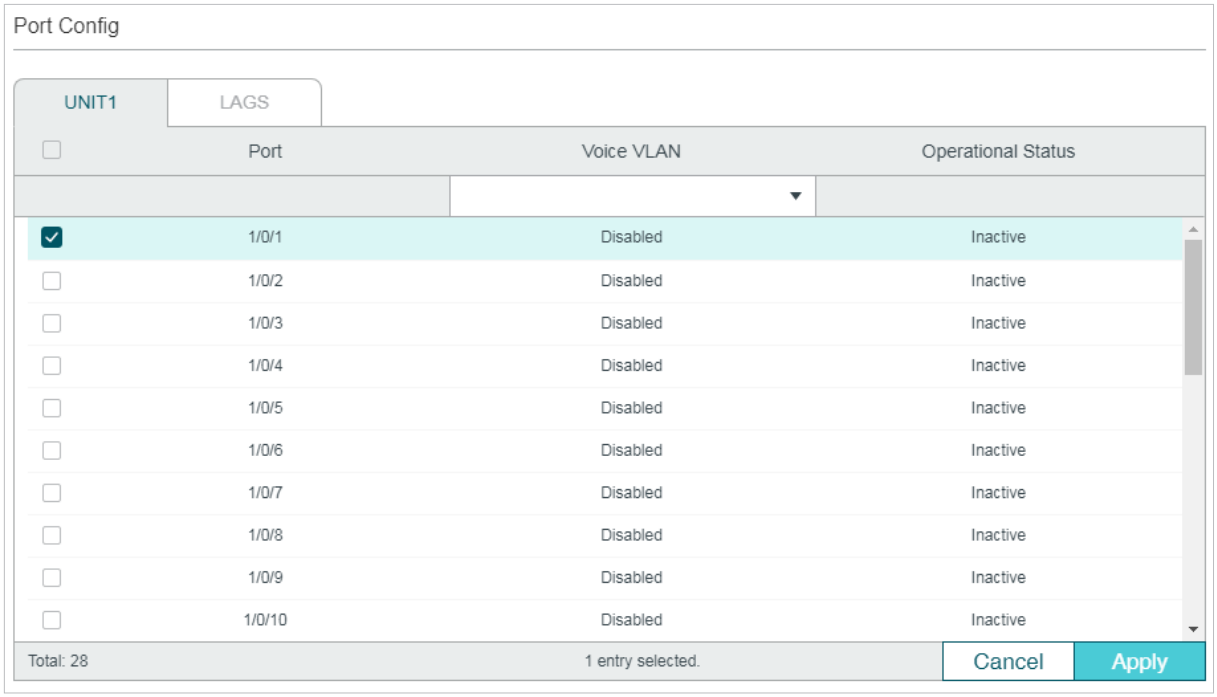
VLAN ID	Podaj ID 802.1Q VLAN, aby ustawić 802.1Q VLAN jako Voice VLAN.
Priority	Wybierz priorytet, który zostanie przypisany pakietom voice, pamiętając, że im wyższa wartość, tym wyższy priorytet. Tryb harmonogramu priorytetu IEEE 802.1p możesz skonfigurować poprzez usługę Class of Service, jeżeli to konieczne.

2) Kliknij **Apply**.

3.1.3 Dodawanie portów do Voice VLAN

Wybierz z menu **QoS > Voice VLAN > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-4 Dodawanie portów do Voice VLAN



Wykonaj poniższe kroki, aby skonfigurować globalnie Voice VLAN:

1) Wybierz porty i zaznacz Enable w polu Voice VLAN.

Voice VLAN	Zaznacz Enable, aby włączyć funkcję Voice VLAN na portach i dodaj wybrane porty do Voice VLAN.

Optional Status	Stan Voice VLAN na danym porcie. **Active:** Funkcja Voice VLAN jest włączona na porcie. **Inactive:** Funkcja Voice VLAN jest wyłączona na porcie.

2) Kliknij **Apply**.

3.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Voice VLAN:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**show voice vlan oui-table** Sprawdź czy adres OUI twojego urządzenia głosowego znajduje się w tabeli OUI. Adres OUI potrzebny jest przełącznikowi do identyfikacji pakietów voice. Adres OUI to 24 pierwsze bity adresu MAC, pełniące rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Jeżeli źródłowy adres MAC pakietu jest zgodny z adresami OUI z listy OUI, przełącznik klasyfikuje pakiet jako pakiet voice i nadaje mu priorytet w transmisji.
Krok 3	**voice vlan oui** *oui-prefix* **oui-desc** *string* Jeżeli w tabeli OUI nie ma adresu OUI twojego urządzenia głosowego, dodaj nowy adres OUI do tabeli. *oui-prefix*: Podaj adres OUI swojego urządzenia głosowego w formacie XX:XX:XX. *string*: Uzupełnij opis adresu OUI dla jego łatwiejszej identyfikacji. Opis może zawierać maksymalnie 16 znaków.
Krok 4	**voice vlan** *vid* Włącz funkcję Voice VLAN i ustaw 802.1Q VLAN jako Voice VLAN. *vid:* Podaj ID 802.1Q VLAN, aby ustawić 802.1Q VLAN jako Voice VLAN.
Krok 5	**voice vlan priority** *pri* Wybierz priorytet, który zostanie przypisany pakietom voice. *pri:* Wybierz priorytet, który zostanie przypisany pakietom voice, pamiętając, że im wyższa wartość, tym wyższy priorytet. Prawidłowe wartości wahają się od 0 do 7, a wartością domyślną jest 7. Tryb harmonogramu priorytetu IEEE 802.1p możesz skonfigurować poprzez usługę Class of Service, jeżeli to konieczne.
Krok 6	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Uruchom tryb konfiguracji interfejsu.
Krok 7	**voice vlan** Włącz funkcję Voice VLAN na portach i dodaj wybrane porty do Voice VLAN.

Krok 8	**show voice vlan interface** Przejrzyj konfigurację Voice VLAN.
Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób otwierania tabeli OUI, ustawiania VLAN 8 jako Voice VLAN, ustawiania priorytetu jako 6 i włączania funkcji Voice VLAN na porcie 1/0/3:

Switch#configure

Switch(config)#show voice vlan oui-table

00:01:E3 Default SIEMENS

00:03:6B Default CISCO1

00:12:43 Default CISCO2

00:0F:E2 Default H3C

00:60:B9 Default NITSUKO

00:D0:1E Default PINTEL

00:E0:75 Default VERILINK

00:E0:BB Default 3COM

00:04:0D Default AVAYA1

00:1B:4F Default AVAYA2

00:04:13 Default SNOM

Switch(config)#voice vlan 8

Switch(config)#voice vlan priority 6

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#voice vlan

Switch(config-if)#show voice vlan interface

Voice VLAN ID 8

Priority 6

Interface Voice VLAN Mode Operational Status LAG

--- --- --- ---

Gi1/0/1	disabled	Down	N/A
Gi1/0/2	disabled	Down	N/A
Gi1/0/3	enabled	Up	N/A
Gi1/0/4	disabled	Down	N/A
Gi1/0/5	disabled	Down	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

4 Konfiguracja Auto VoIP

Wskazówki dotyczące konfiguracji

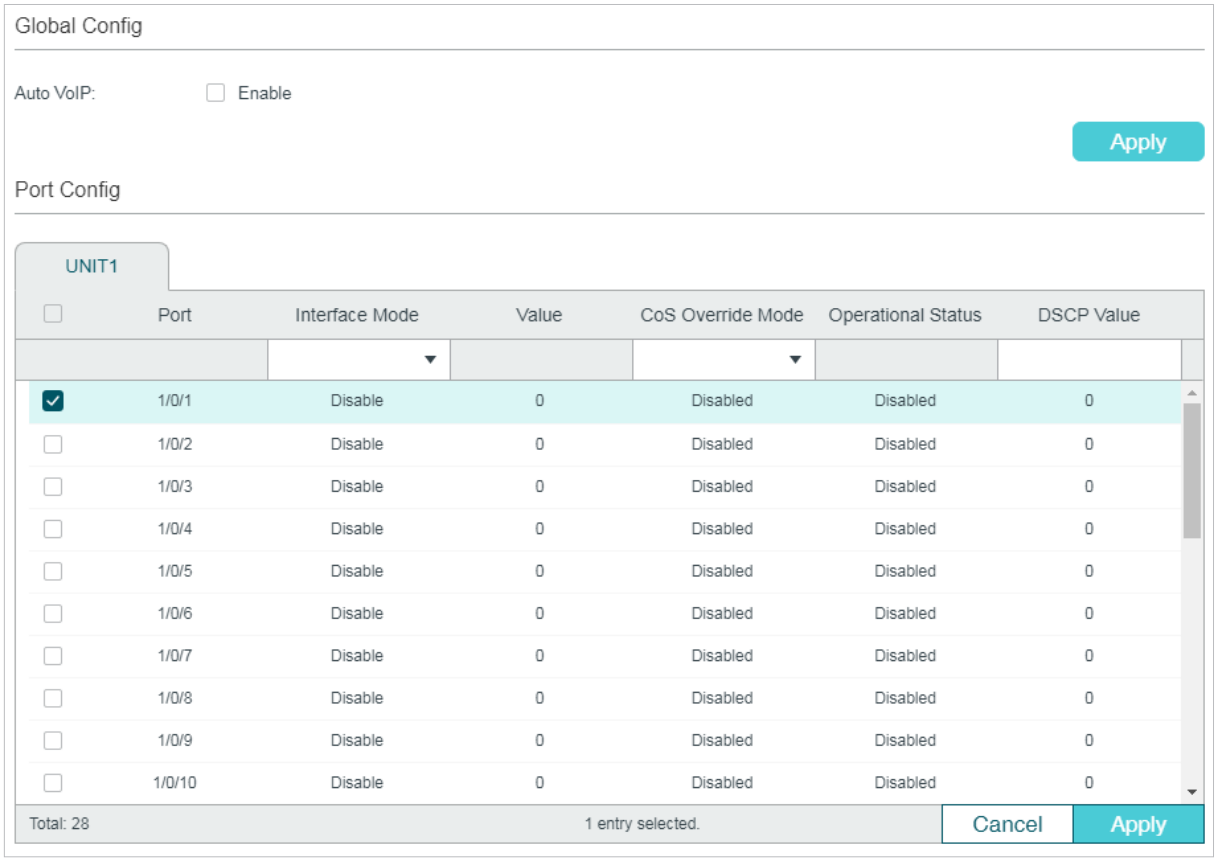
- Przed konfiguracją Auto VoIP konieczne jest włączenie LLDP-MED na portach i konfiguracja odpowiednich parametrów. Szczegółowe informacje o konfiguracji LLDP-MED znajdują się w rozdziale *Konfiguracja LLDP*.

- Funkcja Auto VoIP zapewnia elastyczne rozwiązania do optymalizacji transmisji głosowej. Może współpracować z innymi funkcjami, takimi jak VLAN i Class of Service, aby odpowiednio przetwarzać pakiety voice. Wszystkie te funkcje możesz skonfigurować stosownie do swoich potrzeb.

4.1 Przez GUI

Wybierz z menu **QoS > Auto VoIP**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja Auto VoIP



Wykonaj poniższe kroki, aby skonfigurować adresy OUI:

1) W sekcji **Global Config** włącz globalnie funkcję Auto VoIP.
2) W sekcji **Port Config** wybierz porty i skonfiguruj ich parametry.

Interface Mode	Wybierz tryb interfejsu dla portu. **Disable:** Wyłącz funkcję Auto VoIP na danym porcie. **None:** Zezwól urządzeniom głosowym na korzystanie z własnych ustawień do transmisji głosowej. **VLAN ID:** Urządzenia głosowe będą wysyłać pakiety voice z wybranym tagiem VLAN. Jeżeli wybierzesz ten tryb, uzupełnij pole VLAN ID. Ponadto, musisz także skonfigurować 802.1Q VLAN, aby odpowiednie porty mogły normalnie przesyłać pakiety. **Dot1p:** Urządzenia głosowe będą wysyłać pakiety voice z wybranym priorytetem 802.1p. Jeżeli wybierzesz ten tryb, ustaw priorytet 802.1p w polu Value. Ponadto, musisz także skonfigurować usługę Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetem 802.1p. **Untagged:** Urządzenia głosowe będą wysyłać nietagowane pakiety voice.
Value	Uzupełnij wartość ID VLAN lub priorytetu 802.1p dla portu, zgodnie z ustawieniami trybu interfejsu.
CoS Override Mode	Włącz lub wyłącz tryb zastępowania usługi Class of Service. **Enabled:** Włącz zastępowanie CoS. Przełącznik będzie ignorować priorytety 802.1p w pakietach voice, bezpośrednio umieszczając je w kolejce TC-5. **Disabled:** Wyłącz zastępowanie CoS. Przełącznik będzie umieszczać pakiety voice w kolejkach TC zgodnie z priorytetami 802.1p pakietów.
Operational Status	Stan działania funkcji Voice VLAN na poziomie interfejsu. Aby funkcja działała poprawnie, włącz Voice VLAN zarówno globalnie, jak i na poziomie interfejsu.
DSCP Value	Podaj wartość priorytetu DSCP. Urządzenie głosowe będzie przesyłać pakiety z odpowiednią wartością DSCP. Ponadto, możesz także skonfigurować Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetami DSCP.

3) Kliknij **Apply**.

4.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Auto VoIP:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**auto-voip** Uruchom globalnie Auto VoIP.

Krok 3 **interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}**

Uruchom tryb konfiguracji interfejsu.

Krok 4 Wybierz tryb interfejsu dla portu.

no auto-voip

Gdy ustawisz tryb interfejsu jako disabled, funkcja Auto VoIP będzie wyłączona na danym porcie.

auto-voip none

Gdy ustawisz tryb interfejsu jako none, przełącznik zezwoli urządzeniom głosowym na korzystanie z własnych ustawień do transmisji głosowej.

auto-voip *vlan-id*

Gdy ustawisz tryb interfejsu jako VLAN ID, urządzenia głosowe będą wysyłać pakiety voice z wybranym tagiem VLAN. Jeżeli wybierzesz ten tryb, uzupełnij pole VLAN ID. Prawidłowe wartości wahają się od 1 do 4093.

Ponadto, musisz także skonfigurować 802.1Q VLAN, aby odpowiednie porty mogły normalnie przesyłać pakiety

auto-voip dot1p *dot1p*

Gdy ustawisz tryb interfejsu jako dot1p, urządzenia głosowe będą wysyłać pakiety voice z wybranym priorytetem 802.1p. Jeżeli wybierzesz ten tryb, ustaw priorytet 802.1p w polu Value. Prawidłowe wartości wahają się od 0 do 7.

Ponadto, musisz także skonfigurować usługę Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetem 802.1p.

auto-voip untagged

Gdy ustawisz tryb interfejsu jako untagged, urządzenia głosowe będą wysyłać nietagowane pakiety voice.

Krok 5 **auto-voip data priority {**trust **|** untrust**}**

Włącz lub wyłącz tryb zastępowania usługi Class of Service. Domyślnie ustawioną opcją jest trust, co oznacza, że zastępowanie Class of Service jest wyłączone.

trust: W tym trybie przełącznik będzie umieszczać pakiety voice w kolejkach TC zgodnie z priorytetami 802.1p pakietów.

untrust: W tym trybie przełącznik będzie ignorować priorytety 802.1p w pakietach voice, bezpośrednio umieszczając je w kolejce TC-5.

Krok 6 **auto-voip dscp** *value*

Podaj wartość priorytetu DSCP. Urządzenie głosowe będzie przesyłać pakiety z odpowiednią wartością DSCP.

IPonadto, możesz także skonfigurować Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetami DSCP.

value: Uzupełnij wartość priorytetu DSCP. Prawidłowe wartości wahają się od 0 do 63, a wartością domyślną jest 0.

Krok 7	**show auto-voip** Sprawdź globalny stan Auto VoIP.
Krok 8	**show auto-voip interface** Przejrzyj konfigurację Auto VoIP dla portów.
Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania trybu interfejsu jako dot1p, priorytetu 802.1p jako 4, priorytetu DSCP jako 10 i włączania trybu zastępowania CoS dla portu 1/0/3:

Switch#configure

Switch(config)#auto-voip

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#auto-voip dot1p 4

Switch(config-if)#auto-voip dscp 10

Switch(config-if)#auto-voip data priority untrust

Switch(config-if)#show auto-voip

Administrative Mode: Enabled

Switch(config-if)#show auto-voip interface

Interface.Gi1/0/1

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/2

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/3

Auto-VoIP Interface Mode. Enabled

Auto-VoIP Priority. 4

Auto-VoIP COS Override. True

Auto-VoIP DSCP Value. 10

Auto-VoIP Port Status. Enabled

...

Switch(config-if)#end

Switch#copy running-config startup-config

Część 15

Konfiguracja Access Security

ROZDZIAŁY

1 Access Security

Obsługiwane funkcje

Access Control

Funkcja ta służy do kontrolowania dostępu użytkowników do przełącznika w oparciu o adres IP, adres MAC lub port.

HTTP

Funkcja opiera się na protokole HTTP. Może udzielić użytkownikom dostęp lub odmówić dostępu do przełącznika przez przeglądarkę sieciową.

HTTPS

Funkcja opiera się na protokołach SSL lub TLS, pracujących w warstwie transportowej. Wspiera security access (zabezpieczenie dostępu) przez przeglądarkę sieciową.

SSH

Funkcja opiera się na protokole SSH, protokole zabezpieczeń ustawionym w warstwie aplikacji i w warstwach transportowych. Funkcja z SSH jest podobna do połączenia telnet, może jednak zapewnić bezpieczeństwo informacji i silne uwierzytelnianie.

Telnet

Funkcja opiera się na protokole Telnet, objętym protokołem TCP/IP. Wykorzystując Telnet, użytkownicy mogą zdalnie logować się do przełącznika.

2 Konfiguracja Access Security

Z konfiguracją zabezpieczeń dostępu (Access Security) możliwa jest:

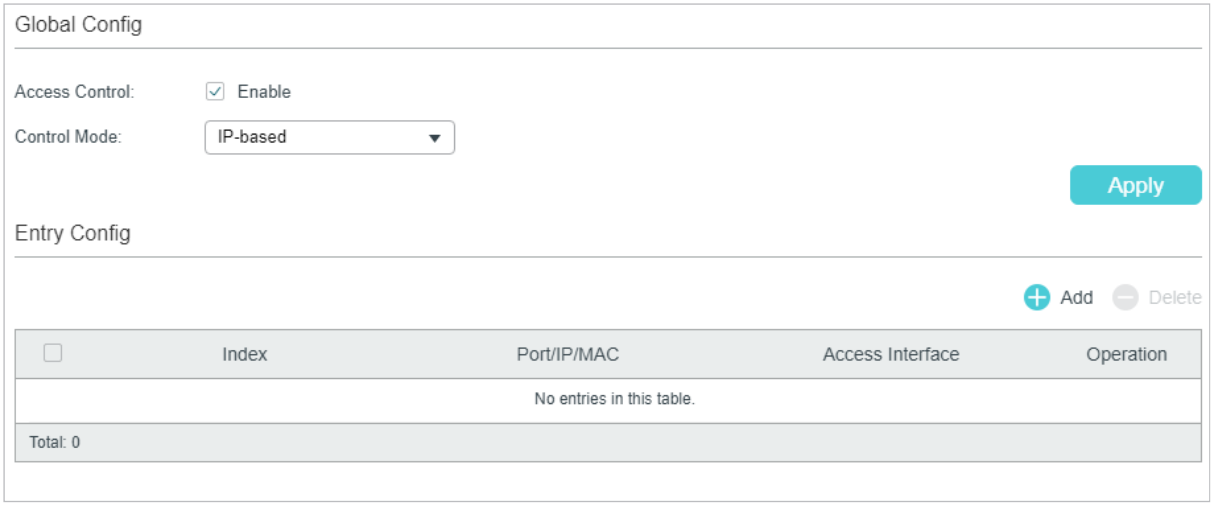
- konfiguracja funkcji Access Control;
- konfiguracja funkcji HTTP;
- konfiguracja funkcji HTTPS;
- konfiguracja funkcji SSH;
- konfiguracja funkcji Telnet.

2.1 Przez GUI

2.1.1 Konfiguracja funkcji Access Control

Wybierz menu **SECURITY** > **Access Security** > **Access Control**, aby załadować następującą stronę.

Rys. 2-1 Konfiguracja funkcji Access Control

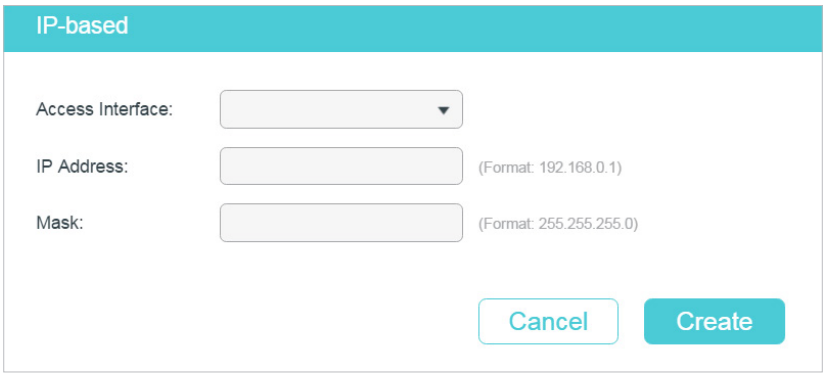


1) W sekcji **Global Config** włącz Access Control, wybierz jeden tryb kontroli i kliknij **Apply**.

Control Mode	Wybierz tryb kontroli dla użytkowników, by mogli logować się do strony zarządzania. **IP-based (w oparciu o IP)**: Dostęp do przełącznika mają jedynie użytkownicy z IP mieszczącym się w ustawionym tu zakresie. **MAC-based (w oparciu o MAC)**: Dostęp do przełącznika mają jedynie użytkownicy z ustawionym tu adresem MAC. **Port-based (w oparciu o port)**: Dostęp do przełącznika mają jedynie użytkownicy podłączeni do wyznaczonych w tym miejscu portów.

2) W sekcji **Entry Table** kliknij Add, aby dodać wpis dla funkcji Access Control.
W przypadku wybrania trybu I**P-based** pojawi się następujące okno.

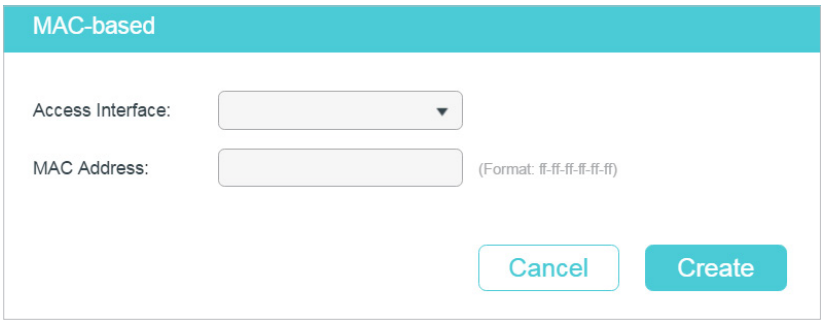
Rys. 2-2 Konfiguracja wpisu Access Control - tryb IP Based



Access Interface	Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika. **SNMP**: Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS. **Telnet**: Typ połączenia umożliwiający użytkownikom logowanie zdalne. **SSH**: Typ połączenia bazujący na protokole SSH. **HTTP**: Typ połączenia bazujący na protokole HTTP. **HTTPS**: Typ połączenia bazujący na protokole SSL. **Ping**: Protokół komunikacyjny służący do testowania połączenia sieci.
IP Address/ Mask	Wprowadź adres IP i maskę, aby określić zakres IP. Jedynie użytkownicy z IP w tym zakresie mają dostęp do przełącznika.

W przypadku wybrania trybu **MAC-based** pojawi się następujące okno.

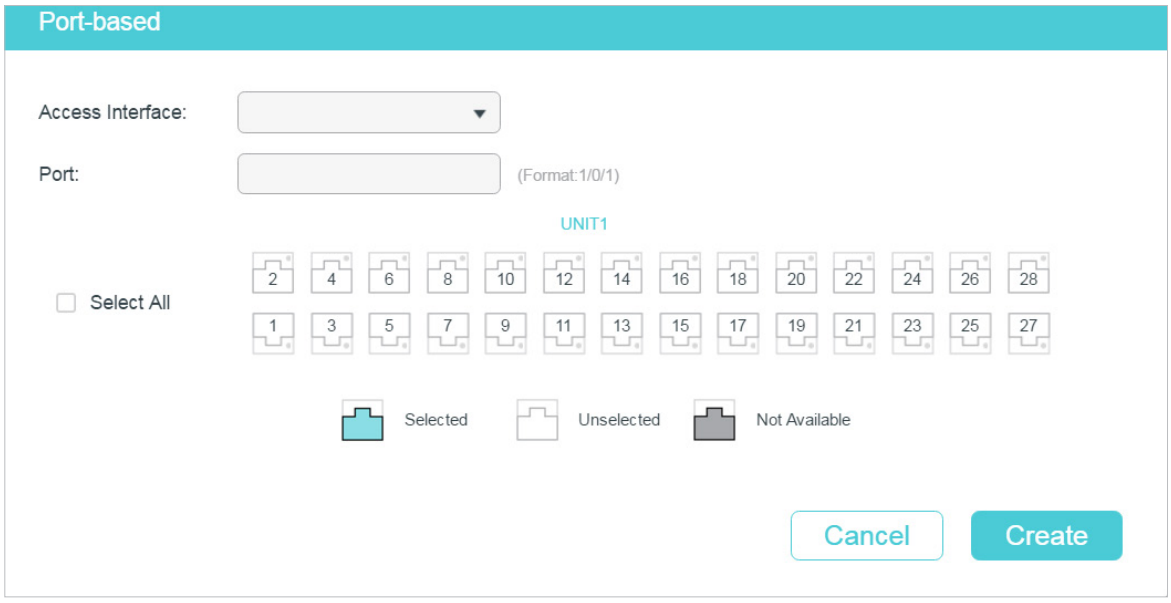
Rys. 2-3 Konfiguracja wpisu Access Control - tryb MAC Based



Access Interface	Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika. **SNMP**: Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS. **Telnet**: Typ połączenia umożliwiający użytkownikom logowanie zdalne. **SSH**: Typ połączenia bazujący na protokole SSH. **HTTP**: Typ połączenia bazujący na protokole HTTP. **HTTPS**: Typ połączenia bazujący na protokole SSL. **Ping**: Protokół komunikacyjny służący do testowania połączenia sieci.
MAC Address	Określ adres MAC. Tylko użytkownicy z poprawnym adresem MAC mają dostęp do przełącznika.

W przypadku wybrania trybu **Port-based** pojawi się następujące okno.

Rys. 2-4 Konfiguracja wpisu Access Control Entry - tryb Port Based



Access Interface	Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika. **SNMP**: Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS. **Telnet**: Typ połączenia umożliwiający użytkownikom logowanie zdalne. **SSH**: Typ połączenia bazujący na protokole SSH. **HTTP**: Typ połączenia bazujący na protokole HTTP. **HTTPS**: Typ połączenia bazujący na protokole SSL. **Ping**: Protokół komunikacyjny służący do testowania połączenia sieci.

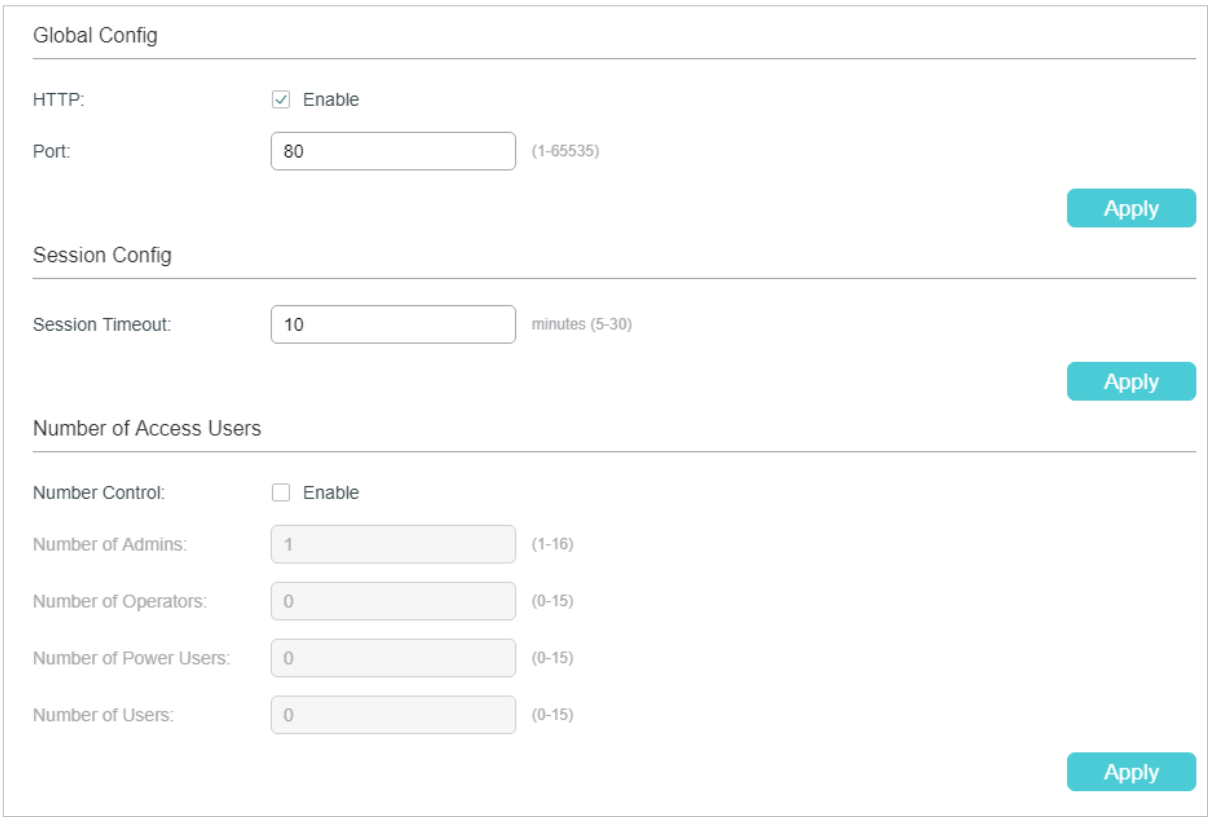
Port	Wybierz co najmniej jeden port do konfiguracji. Jedynie użytkownicy podłączeni do tych portów mają dostęp do przełącznika.

3) Kliknij **Create**. Wyświetlą się utworzone wpisy w **Entry Table**.

2.1.2 Konfiguracja funkcji HTTP

Wybierz menu **SECURITY** > **Access Security** > **HTTP Config**, aby załadować następującą stronę.

Rys. 2-5 Konfiguracja funkcji HTTP



1) W sekcji **Global Control** włącz funkcję HTTP, wyznacz port wykorzystywany w HTTPi kliknij **Apply, aby włączyć funkcję** HTTP.

HTTP	Funkcja HTTP opiera się na protokole HTTP. Funkcja umożliwia użytkownikom zarządzanie przełącznikiem przez przeglądarkę sieciową.
Port	Określ numer portu dla usługi HTTP.

2) W sekcji **Session Config** określ Session Timeout i kliknij **Apply**.

Session Timeout	Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu.

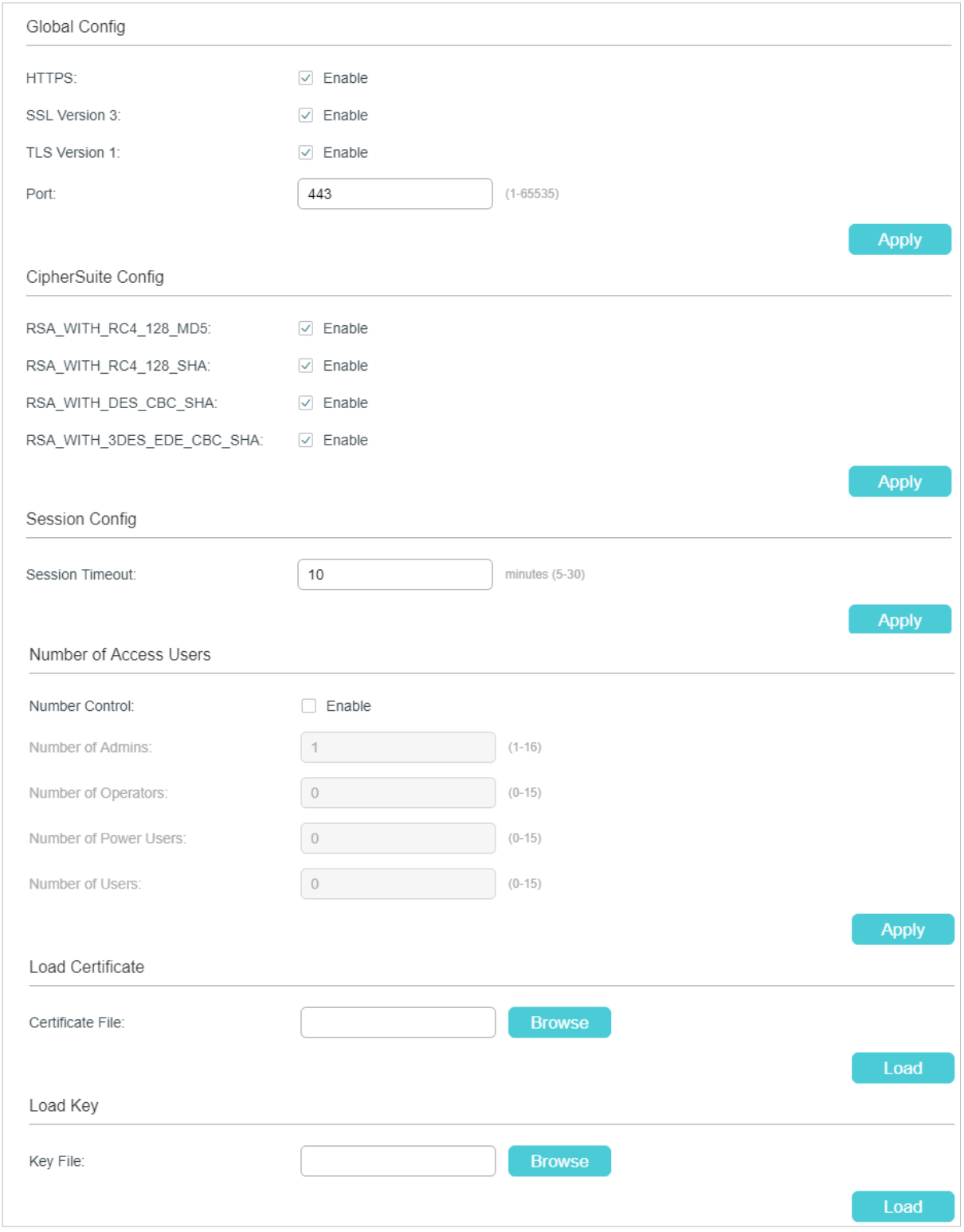
3) W sekcji **Number of Access Users** włącz funkcję Number Control, określ następujące parametry i kliknij **Apply**.

Number Control	Włącz lub wyłącz Number Control. Włączona funkcja umożliwi ci kontrolowanie liczby użytkowników logujących się w tym samym czasie do strony zarządzającej. Całkowita liczba użytkowników nie powinna przekraczać 16.
Number of Admins	Określ maks. liczbę użytkowników z poziomem dostępu Admin.
Number of Operators	Określ maks. liczbę użytkowników z poziomem dostępu Operator.
Number of Power Users	Określ maks. liczbę użytkowników z poziomem dostępu Power User.
Number of Users	Określ maks. liczbę użytkowników z poziomem dostępu User.

2.1.3 Konfiguracja funkcji HTTPS

Wybierz menu **SECURITY** > **Access Security** > **HTTPS Config**, aby załadować następującą stronę.

Rys. 2-6 Konfiguracja funkcji HTTPS



1) W sekcji **Global Config** włącz funkcję HTTPS, wybierz obsługiwany przez przełącznik protokół i wyznacz port do HTTPS. Kliknij **Apply**.

HTTPS	Włącz lub wyłącz funkcję HTTPS. Funkcja HTTPS opiera się na protokole SSL lub TLS. Funkcja zapewnia bezpieczne połączenie między klientem a przełącznikiem.
SSL Version 3	Włącz lub wyłącz na przełączniku protokół SSL Version 3. SSL to protokół transportowy. Może dostarczyć uwierzytelnianie serwera, szyfrowanie i integralność komunikatów, zapewniając bezpieczne połączenie HTTP.
TLS Version 1	Włącz lub wyłącz na przełączniku protokół TLS Version 1. TLS to protokół transportowy, będący uaktualnieniem SSL. TLS obsługuje inny algorytm szyfrowania niż SSL, nie jest więc z nim kompatybilny. TLS może obsługiwać bardziej bezpieczne połączenie.

2) W sekcji **CipherSuite Config** wybierz algorytm, który chcesz włączyć i kliknij **Apply**.

RSA_WITH_ RC4_128_MD5	Wymiana kluczy z szyfrowaniem 1-bitowym RC4 i algorytmem MD5 dla skrótu wiadomości.
RSA_WITH_ RC4_128_SHA	Wymiana kluczy z szyfrowaniem 128-bitowym RC4 i SHA dla skrótu wiadomości.
RSA_WITH_ DES_CBC_SHA	Wymiana kluczy z DES-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości.
RSA_ WITH_3DES_ EDE_CBC_SHA	Wymiana kluczy z 3DES i DES-EDE3-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości.

3) W sekcji **Session Config** określ Session Timeout i kliknij **Apply**.

Session Timeout	Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu

4) W sekcji **Number of Access Users** włącz funkcję Number Control, określ następujące parametry i kliknij **Apply**.

Number Control	Włącz lub wyłącz Number Control. Włączona funkcja umożliwi ci kontrolowanie liczby użytkowników logujących się w tym samym czasie do strony zarządzającej. Całkowita liczba użytkowników nie powinna przekraczać 16.
Number of Admins	Określ maks. liczbę użytkowników z poziomem dostępu Admin.
Number of Operators	Określ maks. liczbę użytkowników z poziomem dostępu Operator.
Number of Power Users	Określ maks. liczbę użytkowników z poziomem dostępu Power User.

Number of Users	Określ maks. liczbę użytkowników z poziomem dostępu User.

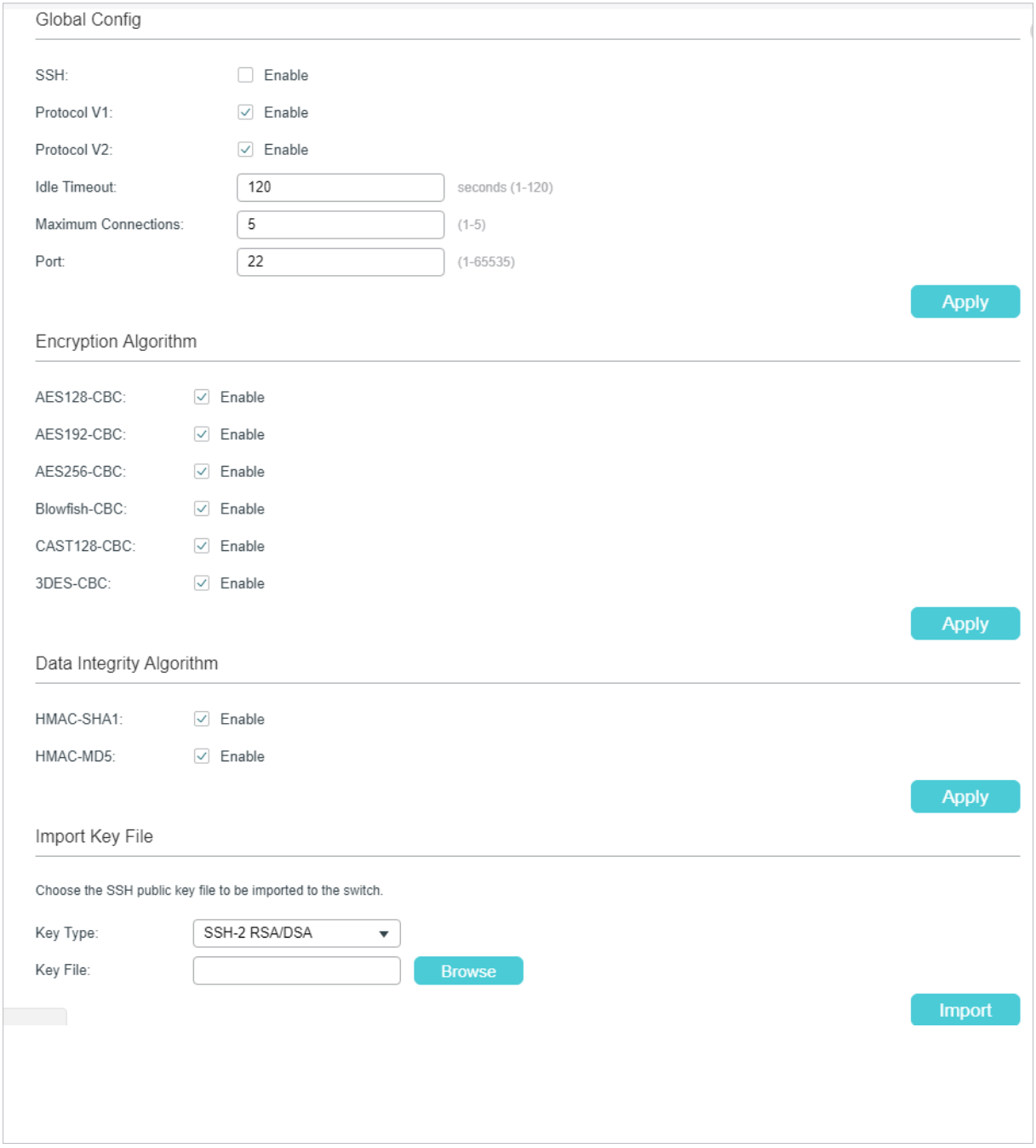
5) W sekcji **Load Certificate** i **Load Key** pobierz certyfikat i klucz.

Certificate File	Wybierz certyfikat, który chcesz pobrać na przełącznik. Certyfikat musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować, w przeciwnym razie połączenie HTTPS nie zadziała.
Key File	Wybierz klucz, który chcesz pobrać na przełącznik. Klucz musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować, w przeciwnym razie połączenie HTTPS nie zadziała.

2.1.4 Konfiguracja funkcji SSH

Wybierz menu **SECURITY** > **Access Security** > **SSH Config**, aby załadować następującą stronę.

Rys. 2-7 Konfiguracja funkcji SSH



1) W sekcji **Global Config** wybierz **Enable**, aby włączyć funkcję SSH i określ następujące parametry.

SSH	Wybierz **Enable**, aby włączyć funkcję SSH. SSH to protokół pracujący w warstwie aplikacji i w warstwie transportowej. Moze zapewnić bezpieczne zdalne połączenie z urządzeniem. SSH jest lepszą gwarancją bezpieczeństwa niż protokół Telnet, ponieważ posiada silne szyfrowanie.

Protocol V1	Wybierz **Enable** aby włączyć SSH w wersji 1.
Protocol V2	Wybierz **Enable** aby włączyć SSH w wersji 2.
Idle Timeout	Określ okres czasu bezczynności. Po wygaśnięciu czasu bezczynności system automatycznie zwolni połączenie.
Maximum Connections	Określ maks. liczbę połączeń z serwerem SSH. Jeżeli liczba połączeń osiągnie określony limit, nie powstaną nowe połączenia.
Port	Wyznacz port wykorzystywany do SSH.

2) W sekcji **Encryption Algorithm** włącz algorytm szyfrowania, który ma być obsługiwany przez przełącznik i kliknij **Apply**.
3) W sekcji **Data Integrity Algorithm** włącz algorytm integralności, który ma być obsługiwany przez przełącznik i kliknij **Apply**.
4) W sekcji **Import Key File** z rozwijanej listy wybierz typ klucza i kliknij **Browse**, aby pobrać plik wybranego klucza.

Key Type	Wybierz typ klucza. Algorytm odpowiedniego typu wykorzystywany jest zarówno do generowania klucza, jak i do uwierzytelniania.
Key File	Wybierz klucz publiczny do pobrania na przełącznik. Długość klucza pobranego pliku wynosi od 512 do 3072 bitów.

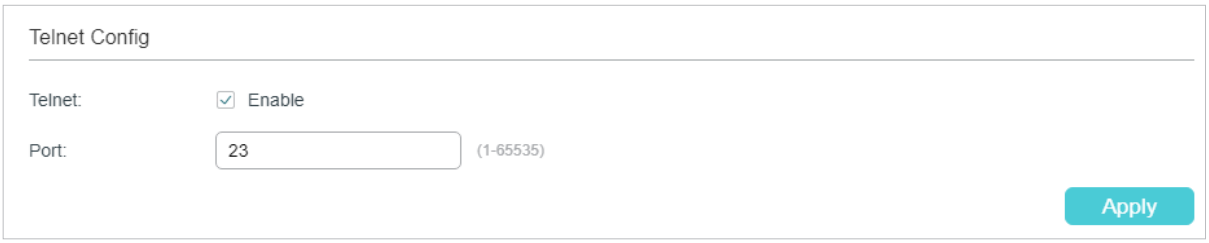
Uwaga:

Pobieranie pliku klucza zajmuje wiele czasu. Czekaj, nie wykonując żadnych działań.

2.1.5 Konfiguracja funkcji Telnet

Wybierz menu **SECURITY** > **Access Security** > **Telnet Config**, aby załadować następującą stronę.

Rys. 2-8 Konfiguracja funkcji Telnet



Włącz Telnet i kliknij **Apply**.

Telnet	Wybierz **Enable**, aby włączyć funkcję Telnet. Funkcja opiera sie na protokole Telnet, objętym protokołem TCP/IP. Dzięki niej użytkownicy mogą zdalnie logować się do przełącznika.
Port	Wyznacz port wykorzystywany przez Telnet.

2.2 Przez CLI

2.2.1 Konfiguracja Access Control

Aby skonfigurować funkcję kontroli dostępu, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych adresów IP. **user access-control ip-based enable** Skonfiguruj tryb kontroli jako IP-based. **user access-control ip-based {** *ip-addr ip-mask* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Dostęp do przełącznika mają jedynie użytkownicy z IP mieszczącym się w ustawionym tu zakresie. *ip-addr*:Wyznacz adres IP dla użytkownika. *ip-mask*: Wyznacz maskę podsieci użytkownika. **[** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Wybierz jaki typ dostępu do przełącznika mają użytkownicy. Domyślnie, wszystkie typy dostępu są włączone. Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych adresów MAC: **user access-control mac-based enable** Skonfiguruj tryb kontroli jako MAC-based. **user access-control mac-based {** *mac-addr* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Tylko użytkownicy z wyznaczonymi tu adresami MAC mają dostęp do przełącznika. *mac-addr*: Wyznacz adres MAC użytkownika. **[** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Wybierz jaki typ dostępu do przełącznika mają użytkownicy. Domyślnie, wszystkie typy dostępu są włączone. Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych portów: **user access-control port-based enable** Skonfiguruj tryb kontroli jako Port-based. **user access-control port-based interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Dostęp do przełącznika mają jedynie użytkownicy podłączeni do wyznaczonych w tym miejscu portów. *port-list*: Sporządź listę portów Ethernet port w formacie 1/0/1-4. Możesz wyznaczyć maks. 5 portów.

Krok 3	**show user configuration** Sprawdź dane ustawień bezpieczeństwa informacji uwierzytelniania użytkowników i interfejsu dostępu.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie typu kontroli dostępu na IP-based. Ustaw adres IP jako 192.168.0.100, maskę podsieci jako 255.255.255.255 i włącz na przełączniku obsługę snmp, telnet, http i https.

Switch#configure

Switch(config)#user access-control ip-based enable

Switch(config)#user access-control ip-based 192.168.0.100 255.255.255.255 snmp telnet http https

Switch(config)#show user configuration

User authentication mode: IP based

Index	IP Address	Access Interface
1	192.168.0.100/32	SNMP Telnet HTTP HTTPS

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja funkcji HTTP

Aby skonfigurować funkcję HTTP, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip http server** Włącz funkcję HTTP. Funkcja jest domyślnie włączona.
Krok 3	**ip http session timeout** *minutes* Określ czas Session Timeout (czas wygasania sesji). Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu. *minutes*: Określ czas wygasania sesji, od 5 do 30 minut. Wartość domyślna to 10.

Krok 4	**ip http max-users** *admin-num operator-num poweruser-num user-num* Określ maks. liczbę użytkowników, którzy mogą łączyć się z serwerem HTTP. Całkowita liczba użytkowników nie powinna przekraczać 16. *admin-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Admin. Wartość powinna wynosić od 1 do 16. *operator-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Operator. Wartość powinna wynosić od 1 do 15. *poweruser-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Power User. Wartość powinna wynosić od 1 do 15. *user-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu User. Wartość powinna wynosić od 1 do 15.
Krok 5	**show ip http configuration** Sprawdź dane konfiguracyjne serwera HTTP(status, session timeout, access-control, max-user number, idle-timeout itd.).
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie czasu wygasania sesji na 9, maks. liczby adminów na 6, maks. liczby operatorów na 2, maks. liczby użytkowników zaawansowanych na 2 i maks. liczby użytkowników na 2.

Switch#configure

Switch(config)#ip http server

Switch(config)#ip http session timeout 9

Switch(config)#ip http max-user 6 2 2 2

Switch(config)#show ip http configuration

HTTP Status:	Enabled
HTTP Port:	80
HTTP Session Timeout:	9
HTTP User Limitation:	Enabled
HTTP Max Users as Admin:	6
HTTP Max Users as Operator:	2
HTTP Max Users as Power User:	2
HTTP Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Konfiguracja funkcji HTTPS

Aby skonfigurować funkcję HTTPS, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip http secure-server** Włącz funkcję HTTPS. Funkcja jest domyślnie włączona.
Krok 3	**ip http secure-protocol { [** ssl3 **] [** tls1 **] }** Skonfiguruj, aby włączyć na przełączniku obsługę odpowiedniego protokołu. Domyślnie przełącznik obsługuje SSLv3 i TLSv1. ssl3: Włącz protokół SSL w wersji 3. SSL to protokół transportowy. Może dostarczyć uwierzytelnianie serwera, szyfrowanie i integralność komunikatów, zapewniając bezpieczne połączenie HTTP. tls1: Włącz protokół TLS w wersji. TLS to protokół transportowy, będący uaktualnieniem SSL. TLS obsługuje inny algorytm szyfrowania niż SSL, nie jest więc z nim kompatybilny. TLS może obsługiwać bardziej bezpieczne połączenie.
Krok 4	**ip http secure-ciphersuite { [3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] }** Włącz odpowiedni mechanizm szyfrowania. Domyślnie, wszystkie typy są włączone. **3des-ede-cbc-sha**: Wymiana kluczy z 3DES i DES-EDE3-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości. **rc4-128-md5**: Wymiana kluczy z szyfrowaniem 128-bitowym RC4 i algorytmem MD5 dla skrótu wiadomości. **rc4-128-sha**: Wymiana kluczy z szyfrowaniem 128-bitowym RC i SHA dla skrótu wiadomości. **des-cbc-sha**: Wymiana kluczy z DES-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości.
Krok 5	**ip http secure-session timeout** *minutes* Określ czas Session Timeout (czas wygasania sesji). Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu. *minutes*: Określ czas wygasania sesji, od 5 do 30 minut. Wartość domyślna to 10.

Krok 6	**ip http secure-max-users** *admin-num operator-num poweruser-num user-num* Określ maks. liczbę użytkowników, którzy mogą łączyć się z serwerem HTTP. Całkowita liczba użytkowników nie powinna przekraczać 16. *admin-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Admin. Wartość powinna wynosić od 1 do 16. *operator-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Operator. Wartość powinna wynosić od 1 do 15. *poweruser-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Power User. Wartość powinna wynosić od 1 do 15. *user-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu User. Wartość powinna wynosić od 1 do 15.
Krok 7	**ip http secure-server download certificate** *ssl-cert* **ip-address** *ip-addr* Pobierz na przełącznik wybrany certyfikat z serwera TFTP. *ssl-cert*: Ustaw nazwę certyfikatu SSL, od 1 do 25 znaków. Certyfikat musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować. *ip-addr*: Określ adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.
Krok 8	**ip http secure-server download key** *ssl-key* **ip-address** *ip-addr* Pobierz na przełącznik wybrany klucz z serwera TFTP. *ssl-key*: Ustaw nazwę pliku klucza zapisanego w serwerze TFTP. Klucz musi mieć kodowanie BASE64. *ip-addr*: Ustaw adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.
Krok 9	**show ip http secure-server** Sprawdź konfigurację globalną HTTPS.
Krok 10	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację funkcji HTTPS. Włącz protokoły SSL3 i TLS1. Włącz mechanizm szyfrowania 3des-ede-cbc-sha. Ustaw czas wygasania sesji na 15, maks. liczbę adminów na 2, maks. liczbę operatorów na 2, maks. liczbę użytkowników zaawansowanych na 2, maks. liczbę użytkowników na 2. Pobierz certyfikat nazwany ca.crt i klucz z nazwą ca.key z serwera TFTP z adresem IP 192.168.0.100.

Switch#configure

Switch(config)#ip http secure-server

Switch(config)#ip http secure-protocol ssl3 tls1

Switch(config)#ip http secure-ciphersuite 3des-ede-cbc-sha

Switch(config)#ip http secure-session timeout 15

Switch(config)#ip http secure-max-users 2 2 2 2

Switch(config)#ip http secure-server download certificate ca.crt **ip-address** 192.168.0.100

Start to download SSL certificate.....

Download SSL certificate OK.

Switch(config)#ip http secure-server download key ca.key **ip-address** 192.168.0.100

Start to download SSL key.....

Download SSL key OK.

Switch(config)#show ip http secure-server

HTTPS Status:	Enabled
HTTPS Port:	443
SSL Protocol Level(s):	ssl3 tls1
SSL CipherSuite:	3des-ede-cbc-sha
HTTPS Session Timeout:	15
HTTPS User Limitation:	Enabled
HTTPS Max Users as Admin:	2
HTTPS Max Users as Operator:	2
HTTPS Max Users as Power User:	2
HTTPS Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Konfiguracja funkcji SSH

Aby skonfigurować funkcję SSH, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip ssh server** Włącz funkcję SSH. Funkcja jest domyślnie wyłączona.

Krok 3	**ip ssh version {** v1 | v2 **}** Skonfiguruj, aby włączyć na przełączniku obsługę odpowiedniego protokołu. Domyślnie przełącznik obsługuje SSHv1 i SSHv3. v1 | v2: Wybierz, aby włączyć odpowiedni protokół.
Krok 4	**ip ssh timeout** *value* Określ okres czasu bezczynności. Po wygaśnięciu czasu bezczynności system automatycznie zwolni połączenie. *value*: Wprowadź wartość wygasania czasu, między 1 a 120 sekund. Wartość domyślna to 20 sekund.
Krok 5	**ip ssh max-client** *num* Określ maks. liczbę połączeń z serwerem SSH. Jeżeli liczba połączeń osiągnie określony limit, nie powstaną nowe połączenia. *num*: Wprowadź liczbę połączeń, od 1 do 5. Wartość domyślna to 5.
Krok 6	**ip ssh algorithm {** AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 **}** Włącz odpowiedni algorytm. Domyślnie wszystkie typy są włączone. AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC: Określ algorytm szyfrowania, który ma być obsługiwany przez przełącznik. HMAC-SHA1 | HMAC-MD5: Określ algorytm integralności danych, który ma być obsługiwany przez przełącznik.
Krok 7	**ip ssh download {** v1 | v2 **}** *key-file* **ip-address** *ip-addr* Wybierz typ pliku klucza i pobierz na przełącznik wybrany plik z serwera TFTP. v1 | v2: Wybierz typ klucza. Algorytm odpowiedniego typu wykorzystywany jest zarówno do generowania klucza, jak do uwierzytelniania. *key-file*: Ustaw nazwę pliku klucza zapisanego w serwerze TFTP. Upewnij się, że długość klucza pobranego pliku wynosi od 512 do 3072 bitów. *ip-addr*: Ustaw adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.
Krok 8	**show ip ssh** Sprawdź konfigurację globalną SSH.
Krok 9	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Pobieranie pliku klucza zajmuje wiele czasu. Czekaj, nie wykonując żadnych działań.

Poniższy przykład prezentuje konfigurację funkcji SSH. Ustaw wersję 1 i 2 SSH. Włącz algorytm szyfrowania AES128-CBC i Cast128-CBC. Włącz algorytm integralności danych HMAC-MD5. Wybierz typ klucza SSH-2 RSA/DSA.

Switch(config)#ip ssh server

Switch(config)#ip ssh version v1

Switch(config)#ip ssh version v2

Switch(config)#ip ssh timeout 100

Switch(config)#ip ssh max-client 4

Switch(config)#ip ssh algorithm AES128-CBC

Switch(config)#ip ssh algorithm Cast128-CBC

Switch(config)#ip ssh algorithm HMAC-MD5

Switch(config)#ip ssh download v2 publickey **ip-address** 192.168.0.100

Start to download SSH key file.....

Download SSH key file OK.

Switch(config)#show ip ssh

Global Config:

SSH Server: Enabled

Protocol V1: Enabled

Protocol V2: Enabled

Idle Timeout: 100

MAX Clients: 4

Port: 22

Encryption Algorithm:

AES128-CBC: Enabled

AES192-CBC: Disabled

AES256-CBC: Disabled

Blowfish-CBC: Disabled

Cast128-CBC: Enabled

3DES-CBC: Disabled

Data Integrity Algorithm:

HMAC-SHA1: Disabled

HMAC-MD5: Enabled

Key Type: SSH-2 RSA/DSA

Key File:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: “dsa-key-20160711”

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Konfiguracja funkcji Telnet

Aby włączyć funkcję Telnet, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**telnet enable** Włącz funkcję telnet. Funkcja jest domyślnie włączona.
Krok 3	**telnet port** *port* Wyznacz port wykorzystywany przez Telnet, w zakresie od 1 do 65535.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Część 16

Konfiguracja AAA

ROZDZIAŁY

1 Konfiguracja AAA

Funkcja AAA umożliwia przetwarzanie uwierzytelniania lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+. Aby zapewnić stabilność systemu uwierzytelniania, możesz równocześnie skonfigurować wiele serwerów i metod uwierzytelniania. W tym rozdziale dowiesz się jak skonfigurować kompleksowo procesy uwierzytelniania w AAA.

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji:

1) Dodaj serwery.
2) Skonfiguruj grupy serwerów.
3) Skonfiguruj listę metod.
4) Skonfiguruj listę opcji AAA.
5) Skonfiguruj konto logowania i hasło dostępu.

Wskazówki dotyczące konfiguracji

Poniżej wyjaśnione są podstawowe pojęcia i mechanizm działania AAA:

- Domyślne ustawienie AAA

Domyślnie funkcja AAA jest włączona i nie można jej wyłączyć.

- Grupa serwera

Serwery korzystające z tego samego protokołu mogą być dodane do jednej grupy serwerów. Serwery w tej grupie będą uwierzytelniać dostęp użytkowników w takiej kolejności, w jakiej zostały dodane. Serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie w normalnych okolicznościach. Jeżeli jednak ten pierwszy serwer przestanie działać lub nie będzie odpowiadać na żądanie uwierzytelnienia dostępu, funkcję uwierzytelniania przejmie drugi serwer, itd.

- Lista metod

Za metodę uznawana jest m.in. grupa serwerów, czy też uwierzytelnianie lokalne. Listę metod może tworzyć wiele metod. Do uwierzytelniania dostępu użytkownika przełącznik korzysta z pierwszej metody na liście, a jeżeli ta metoda zawiedzie, przełącznik korzysta z kolejnej metody. Proces ten trwa, dopóki dostęp użytkownika nie zostanie uwierzytelniony lub do wyczerpania zdefiniowanych metod. Jeżeli proces uwierzytelniania się powiedzie lub jeżeli serwer bezpieczeństwa lub przełącznik lokalny odmówi dostępu użytkownikowi, proces uwierzytelniania zatrzyma się i kolejne metody nie będą wykorzystane.

Dostępne są dwa typy listy metod: lista metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika oraz lista metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.

- Lista opcji AAA

Przełącznik obsługuje następujące opcje dostępu: Telnet, SSH i HTTP. Dla każdej opcji można wybrać skonfigurowaną listę metod uwierzytelniania.

1.1 Przez GUI

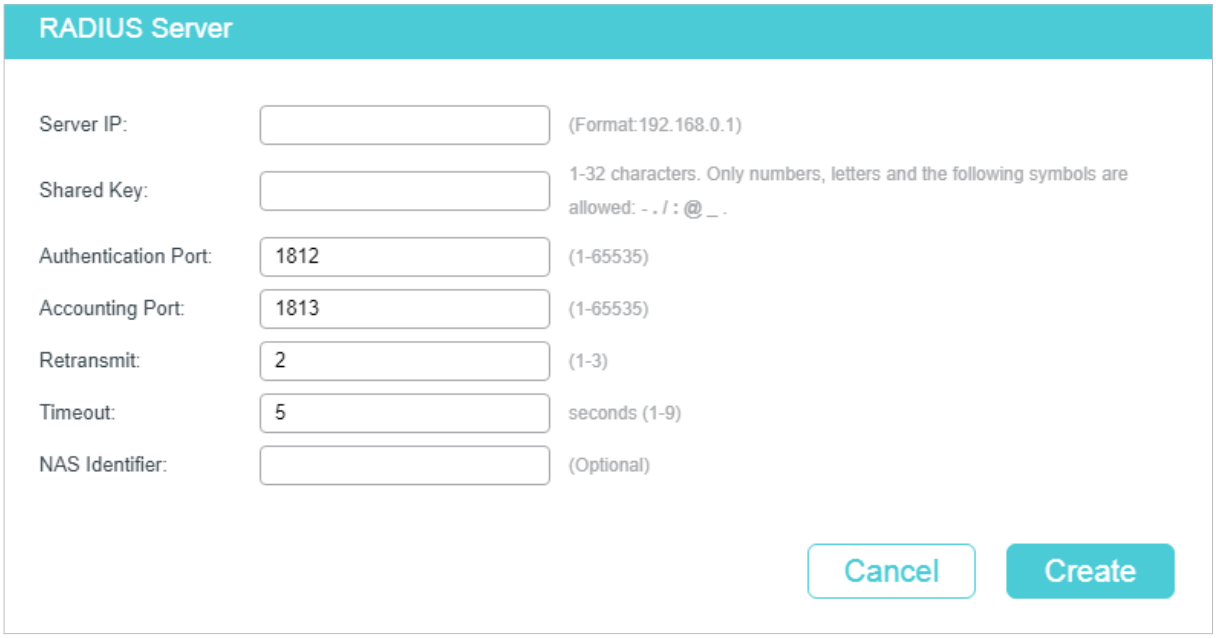
1.1.1 Dodawanie serwerów

Na przełączniku możesz dodać jeden lub kilka serwerów RADIUS/TACACS+ do uwierzytelniania. Jeżeli dodasz kilka serwerów, serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie użytkowników starających się uzyskać dostęp do przełącznika. Kolejne serwery są serwerami zapasowymi, na wypadek awarii pierwszego serwera.

- Dodawanie serwera RADIUS

Wybierz z menu **SECURITY > AAA > RADIUS Config** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 1-1 Konfiguracja serwera RADIUS



Wykonaj poniższe kroki, aby dodać serwer RADIUS:

1) Skonfiguruj poniższe parametry.

Server IP	Podaj adres IP serwera z protokołem bezpieczeństwa RADIUS.
Shared Key	Podaj wspólny klucz zabezpieczeń serwera RADIUS i przełącznika. Serwer RADIUS i przełącznik korzystają z ciągu klucza do szyfrowania haseł i wymiany komunikatów.

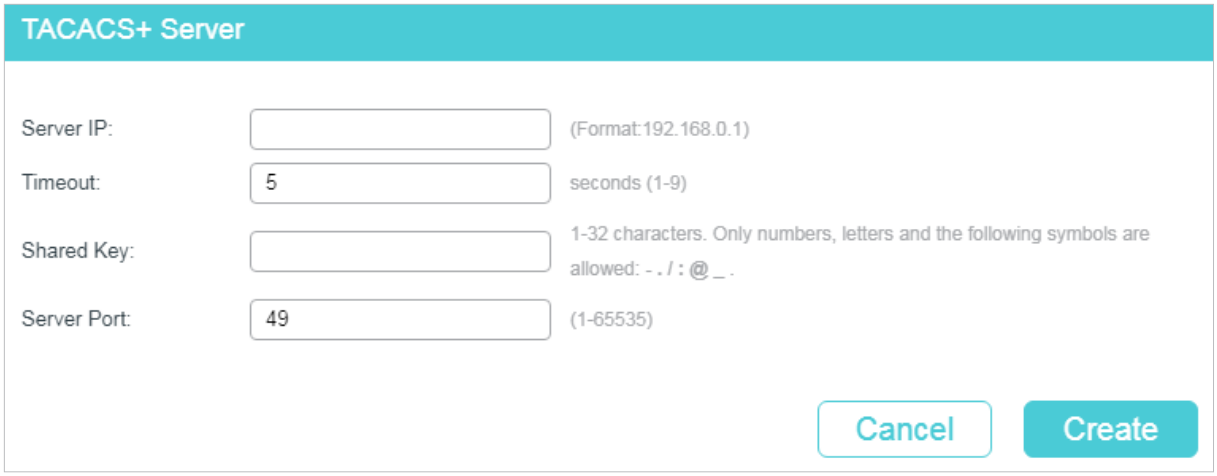
Authentication Port	Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań uwierzytelniania. Domyślnym ustawieniem jest 1812.
Accounting Port	Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań rozliczania. Domyślną wartością jest 1813. Port ten zwykle stosuje się dla funkcji 802.1x.
Retransmit	Określ ile razy żądanie ma być wysłane do serwera, gdy serwer nie odpowiada. Domyślnym ustawieniem jest 2.
Timeout	Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Domyślnym ustawieniem jest 5 sekund.
NAS Identifier	Podaj nazwę NAS (Network Access Server), która zostanie umieszczona w pakiecie RADIUS dla łatwiejszej identyfikacji. Nazwa musi zawierać od 1 do 31 znaków. Domyślną wartością jest adres MAC przełącznika. Zasadniczo NAS określa sam przełącznik.

2) Kliknij **Create,** aby dodać serwer RADIUS na przełączniku.

■ Dodawania serwera TACACS+

Wybierz z menu **SECURITY > AAA > TACACS+ Config** i kliknij Add, aby wyświetlić poniższą stronę.

Rys. 1-2 Konfiguracja serwera TACACS+



Wykonaj poniższe kroki, aby dodać serwer TACACS+:

1) Skonfiguruj poniższe parametry.

Server IP	Podaj adres IP serwera z protokołem bezpieczeństwa TACACS+.
Timeout	Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Domyślnym ustawieniem jest 5 sekund.
Shared Key	Podaj wspólny klucz zabezpieczeń serwera TACACS+ i przełącznika. Serwer TACACS+ i przełącznik korzystają z ciągu klucza do szyfrowania haseł i wymiany komunikatów.

Server Port	Określ port TCP stosowany na serwerze TACACS+ dla AAA. Domyślnym ustawieniem jest 49.

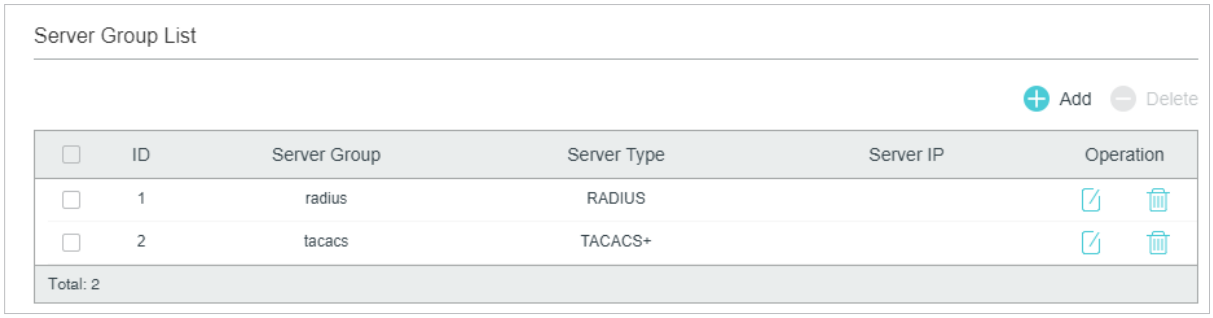
2) Kliknij **Create,** aby dodać serwer TACACS+ na przełączniku.

1.1.2 Konfiguracja grup serwerów

Przełącznik ma dwie wbudowane grupy serwerów, jeden dla serwerów RADIUS, a drugi dla serwerów TACACS+. Serwery korzystające z tego samego protokołu są automatycznie dodawane do domyślnej grupy serwerów. Możesz dodawać nowe grupy serwerów, jeżeli uznasz to za potrzebne.

Wybierz z menu **SECURITY > AAA > Server Group**, aby wyświetlić poniższą stronę.

Rys. 1-3 Dodaj nową grupę serwera



Na liście są dwie domyślne grupy serwerów. Możesz je edytować lub wykonać poniższe kroki, aby skonfigurować nową grupę serwerów:

1) Kliknij Add , aby pojawiło się poniższe okno.

Rys. 1-4 Dodawanie grupy serwerów

Skonfiguruj poniższe parametry:

Server Group	Podaj nazwę grupy serwerów.
Server Type	Wybierz typ serwera dla grupy. Dostępne są dwie opcje: RADIUS i TACACS+.
Server IP	Wybierz adres IP serwera, który zostanie dodany do grupy serwerów.

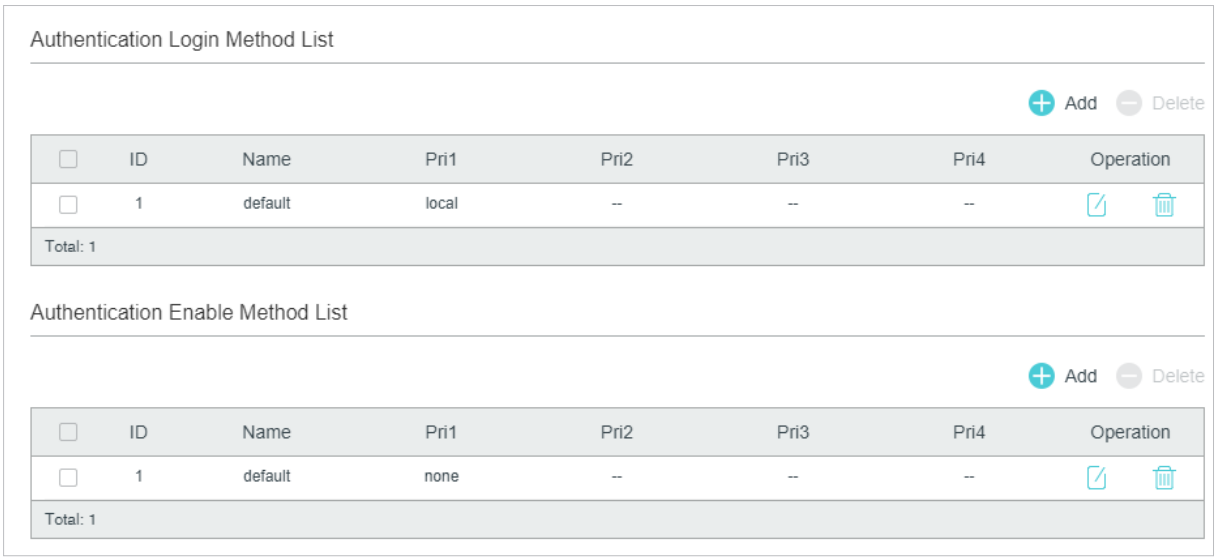
2) Kliknij **Create**.

1.1.3 Konfiguracja listy metod

Lista metod opisuje metody uwierzytelniania i kolejność, w jakiej są używane do uwierzytelniania dostępu użytkowników. Przełącznik obsługuje listę metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika i oraz listę metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.

Wybierz z menu **SECURITY > AAA > Method List**, aby wyświetlić poniższą stronę.

Rys. 1-5 Lista metod

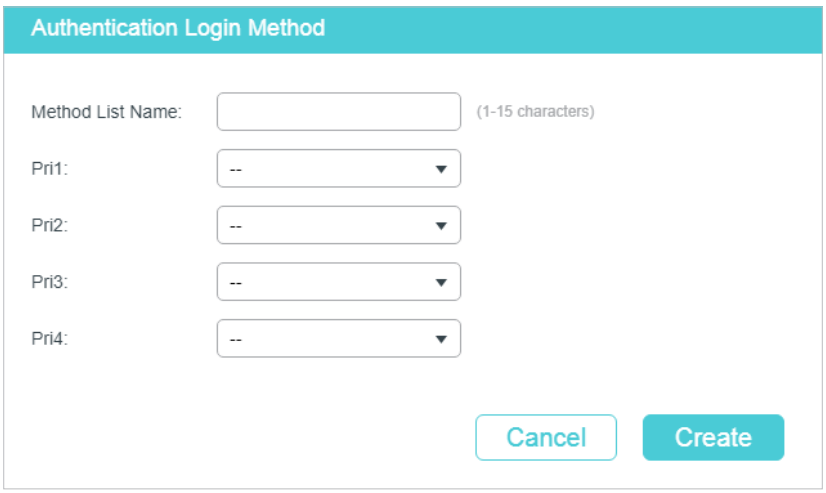


Dostępne są odpowiednio dwie domyślne metody dla uwierzytelniania logowania i uwierzytelniania dostępu.

Możesz edytować domyślne metody lub wykonać poniższe kroki, aby dodać nową metodę:

1) Kliknij Add w sekcji **Authentication Login Method List** lub **Authentication Enable Method List**, aby dodać odpowiedni typ list metod. Pojawi się poniższe okno.

Rys. 1-6 Dodaj nową metodę



Skonfiguruj parametry dla metody, którą chcesz dodać.

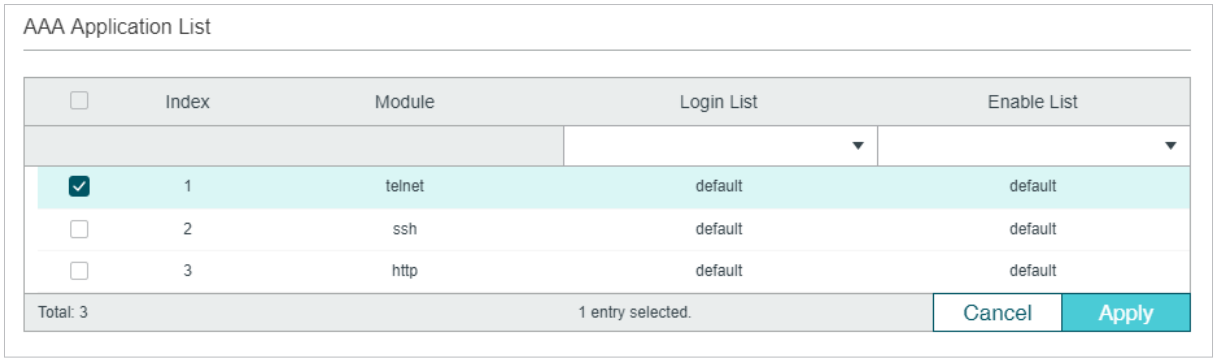
Method List Name	Podaj nazwę metody.
Pri1- Pri4	Ustal kolejność metod uwierzytelniania. Metoda o priorytecie 1 posłuży do uwierzytelniania dostępu użytkownika jako pierwsza, metoda o priorytecie 2 jako kolejna, gdy poprzednia metoda zawiedzie, itd. **local**: Skorzystaj z lokalnej bazy danych przełącznika do uwierzytelniania. **none**: Brak uwierzytelniania. **radius**: Skorzystaj ze zdalnego serwera/grup serwerów RADIUS. **tacacs**: Skorzystaj ze zdalnego serwera/grup serwerów TACACS+. **Other user-defined server groups**: Skorzystaj z grup serwerów zdefiniowanych przez użytkownika.

2) Kliknij **Create**, aby dodać nową metodę.

1.1.4 Konfiguracja listy aplikacji AAA

Wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę.

Rys. 1-7 Konfiguracja listy aplikacji



Wykonaj poniższe kroki, aby skonfigurować listę aplikacji AAA.

1) W sekcji **AAA Application List** wybierz opcję dostępu i skonfiguruj listę logowania i listę dostępu.

Module	Konfigurowalne protokoły na przełączniku: telnet, ssh i http.
Login List	Wybierz skonfigurowaną uprzednio listę metod logowania. Pozwoli ona uwierzytelniać użytkowników, którzy starają się zalogować na przełącznik.
Enable List	Wybierz skonfigurowaną uprzednio listę metod dostępu. Pozwoli ona uwierzytelniać użytkowników, którzy chcą uzyskać uprawnienia administratora.

2) Kliknij **Apply**.

1.1.5 Konfiguracja konta logowania i hasła dostępu

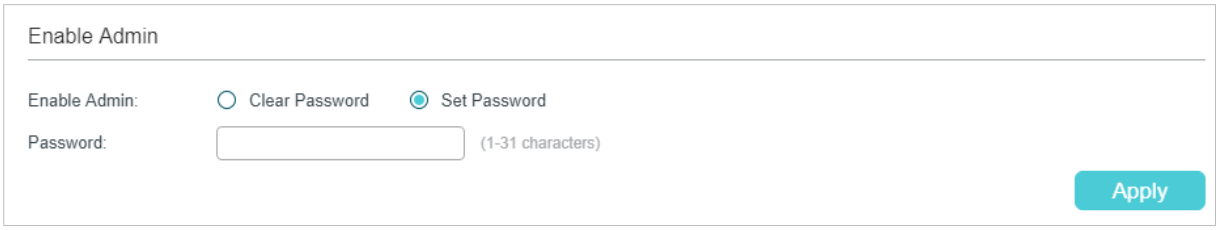
Konto logowania i hasło dostępu można skonfigurować lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+.

- Na przełączniku

Lokalną nazwę użytkownika i hasło logowania można skonfigurować na stronie zarządzania kontami użytkowników. Szczegółowe informacje znajdziesz w rozdziale *Zarządzanie systemem*.

Aby skonfigurować lokalne hasło dostępu do uzyskania uprawnień administratora, wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę.

Rys. 1-8 Konfiguracja hasła dostępu



Dostępne są dwie opcje: **Clear Password** i **Set Password**. Możesz zdecydować czy hasło dostępu będzie wymagane od gości starających się uzyskać uprawnienia administratora. Kliknij **Apply**.

Wskazówka: Zalogowani goście mogą wpisać lokalne hasło dostępu, aby uzyskać uprawnienia administratora.

- Na serwerze

Użytkownicy konta utworzonych poprzez serwer RADIUS/TACACS+ mogą tylko przeglądać ustawienia i informacje sieciowe bez hasła dostępu.

Zasady konfiguracji na serwerze są następujące:

- W przypadku konfiguracji uwierzytelniania logowaniem, na serwerze można utworzyć więcej niż jedno konto logowania. Ponadto, można także dostosować nazwę użytkownika i hasło.

- W przypadku konfiguracji hasła dostępu:

  Na serwerze RADIUS nazwą użytkownika musi być **$enable$**, ale hasło dostępu jest konfigurowalne. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

  Na serwerze TACACS+ ustaw hasło logowania w pliku konfiguracyjnym, wpisując wartość “enable 15“. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

1.2 Przez CLI

1.2.1 Dodawanie serwerów

Na przełączniku możesz dodać jeden lub kilka serwerów RADIUS/TACACS+ do uwierzytelniania. Jeżeli dodasz kilka serwerów, serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie użytkowników starających się uzyskać dostęp do przełącznika. Kolejne serwery są serwerami zapasowymi, na wypadek awarii pierwszego serwera.

- Dodawania serwera RADIUS

Wykonaj poniższe kroki, aby dodać serwer RADIUS na przełączniku:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**radius-server host** *ip-address* **[auth-port** *port-id* **] [acct-port** *port-id* **] [timeout** *time* **] [retransmit** *number* **] [nas-id** *nas-id* **] key {** [0] *string* **|** 7 *encrypted-string* **}** Dodaj serwer RADIUS i skonfiguruj odpowiednie parametry. **host** *ip-address*: Podaj adres IP serwera z protokołem RADIUS. **auth-port** *port-id*: Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań uwierzytelniania. Domyślnym ustawieniem jest 1812. **acct-port** *port-id:* Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań rozliczania. Domyślną wartością jest 1813. Port ten zwykle stosuje się dla funkcji 802.1x. **timeout** *time*: Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Prawidłowe wartości wahają się od 1 do 9 sekund, a domyślnym ustawieniem jest 5 sekund. **retransmit** *number*: Określ ile razy żądanie ma być wysłane do serwera, gdy serwer nie odpowiada. Prawidłowe wartości wahają się od 1 do 3, a domyślnym ustawieniem jest 2. **nas-id** *nas-id*: Podaj nazwę NAS (Network Access Server), która zostanie umieszczona w pakiecie RADIUS dla łatwiejszej identyfikacji. Nazwa musi zawierać od 1 do 31 znaków. Domyślną wartością jest adres MAC przełącznika. Zasadniczo NAS określa sam przełącznik. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Podaj wspólny klucz zabezpieczeń. 0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego, o stałej długości. Domyślnym ustawieniem jest 0. *string* jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. *encrypted-string* to klucz szyfrowania symetrycznego, o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej.
Krok 3	**show radius-server** Przejrzyj ustawienia serwera RADIUS.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób dodawania serwera RADIUS na przełączniku. Ustawionym adresem IP serwera będzie 192.168.0.10, portem uwierzytelniania 1812, wspólnym kluczem 123456, czasem oczekiwania 8 sekund, a liczbą ponownych wysłań żądania 3.

Switch#configure

Switch(config)#radius-server host 192.168.0.10 **auth-port** 1812 **timeout** 8 **retransmit** 3 **key** 123456

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.10	1812	1813	5	2	000AEB132397	123456

Switch(config)#end

Switch#copy running-config startup-config

■ Dodawanie serwera TACACS+

Wykonaj poniższe kroki, aby dodać serwer TACACS+ na przełączniku:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**tacacs-server host** *ip-address* **[port** *port-id* **] [timeout** *time* **] [key {** [0] *string* **|** 7 *encrypted-string* **}]** Dodaj serwer RADIUS i skonfiguruj odpowiednie parametry. **host** *ip-address*: Podaj adres IP serwera z protokołem TACACS+. **port** *port-id*: Podaj numer portu docelowego UDP na serwerze TACAS+ dla żądań uwierzytelniania. Domyślnym ustawieniem jest 49. **timeout** *time*: Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Prawidłowe wartości wahają się od 1 do 9 sekund, a domyślnym ustawieniem jest 5 sekund. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Podaj wspólny klucz zabezpieczeń. 0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego, o stałej długości. Domyślnym ustawieniem jest 0. *string* jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. *encrypted-string* to klucz szyfrowania symetrycznego, o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej.
Krok 3	**show tacacs-server** Przejrzyj ustawienia serwera TACACS+.

Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób dodawania serwera TACACS+ na przełączniku. Ustawionym adresem IP serwera będzie 192.168.0.20, portem uwierzytelniania 49, wspólnym kluczem 123456, a czasem oczekiwania 8 sekund.

Switch#configure

Switch(config)#tacacs-server host 192.168.0.20 **auth-port** 49 **timeout** 8 **key** 123456

Switch(config)#show tacacs-server

Server Ip	Port	Timeout	Shared key
192.168.0.20	49	8	123456

Switch(config)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja grup serwerów

Przełącznik ma dwie wbudowane grupy serwerów, jeden dla serwerów RADIUS, a drugi dla serwerów TACACS+. Serwery korzystające z tego samego protokołu są automatycznie dodawane do domyślnej grupy serwerów. Możesz dodawać nowe grupy serwerów, jeżeli uznasz to za potrzebne.

Dwie domyślne grupy serwerów nie mogą być usunięte, ani edytowane. Wykonaj poniższe kroki, aby dodać grupę serwerów:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**aaa group {** radius | tacacs **}** *group-name* Utwórz grupę serwerów. radius | tacacs: Podaj typ grupy. *group-name*: Podaj nazwę grupy.
Krok 3	**server** *ip-address* Dodaj istniejące serwery do grup serwerów. *ip-address*: Podaj adres IP serwera, który ma być dodany do grupy.

Krok 4	**show aaa group** [*group-name*] Przejrzyj ustawienia grup serwerów.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Step 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia grupy serwera RADIUS o nazwie RADIUS1 i dodawania do grupy dwóch istniejących serwerów RADIUS, których adresami IP są odpowiednio 192.168.0.10 i 192.168.0.20.

Switch#configure

Switch(config)#aaa group radius RADIUS1

Switch(aaa-group)#server 192.168.0.10

Switch(aaa-group)#server 192.168.0.20

Switch(aaa-group)#show aaa group RADIUS1

192.168.0.10

192.168.0.20

Switch(aaa-group)#end

Switch#copy running-config startup-config

1.2.3 Konfiguracja listy metod

Lista metod opisuje metody uwierzytelniania i kolejność, w jakiej są używane do uwierzytelniania dostępu użytkowników. Przełącznik obsługuje listę metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika i oraz listę metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.

Wykonaj poniższe kroki, aby skonfigurować listę metod:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**aaa authentication login {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Skonfiguruj listę metod logowania. *method-list*: Podaj nazwę listy metod. *method1/method2/method3/method4*: Ustal kolejność metod uwierzytelniania. Metoda o priorytecie 1 posłuży do uwierzytelniania dostępu użytkownika jako pierwsza, metoda o priorytecie 2 jako kolejna, gdy poprzednia metoda zawiedzie, itd. Metodami domyślnymi są radius, tacacs, local i none. None oznacza brak uwierzytelniania logowania użytkowników.
Krok 3	**aaa authentication enable {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Skonfiguruj listę metod hasła dostępu. *method-list*: Podaj nazwę listy metod. *method1/method2/method3/method4*: Ustal kolejność metod uwierzytelniania. Metodami domyślnymi są radius, tacacs, local i none. None oznacza brak uwierzytelniania dla użytkowników, którzy chcą uzyskać uprawnienia administratora.
Krok 4	**show aaa authentication** [login | enable] Przejrzyj ustawienia listy metod.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia listy metod logowania o nazwie Login1 i ustawiania method 1 jako domyślnej grupy serwerów RADIUS i method 2 jako local.

Switch#configure

Switch(config)##aaa authentication login Login1 radius local

Switch(config)#show aaa authentication login

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Login1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

Poniższy schemat przedstawia przykładowy sposób tworzenia listy metod hasła dostępu o nazwie Enable1 i ustawiania method 1 jako domyślnej grupy serwerów RADIUS i method 2 jako local.

Switch#configure

Switch(config)##aaa authentication enable Enable1 radius local

Switch(config)#show aaa authentication enable

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Enable1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

1.2.4 Konfiguracja listy aplikacji AAA

Możesz skonfigurować listy metod uwierzytelniania poprzez następujące aplikacje dostępu: Telnet, SSH i HTTP.

- Telnet

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z Telnet:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**line telnet** Uruchom tryb konfiguracji łącza.
Krok 3	**login authentication {** *method-list* **}** Powiąż listę metod logowania z Telnet. *method-list*: Podaj nazwę listy metod logowania.
Krok 4	**enable authentication {** *method-list* **}** Powiąż listę metod hasła dostępu z Telnet. *method-list*: Podaj nazwę listy metod hasła dostępu.
Krok 5	**show aaa global** Przejrzyj ustawienia list aplikacji.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z Telnet.

Switch#configure

Switch(config)#line telnet

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

Module	Login List	Enable List
Telnet	Login1	Enable1
Ssh	default	default
Http	default	default

Switch(config-line)#end

Switch#copy running-config startup-config

- SSH

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z SSH:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**line ssh** Uruchom tryb konfiguracji łącza.
Krok 3	**login authentication {** *method-list* **}** Powiąż listę metod logowania z SSH. *method-list*: Podaj nazwę listy metod logowania.
Krok 4	**enable authentication {** *method-list* **}** Powiąż listę metod hasła dostępu z SSH. *method-list*: Podaj nazwę listy metod hasła dostępu.
Krok 5	**show aaa global** Przejrzyj ustawienia list aplikacji.
Krok 6	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z SSH.

Switch#configure

Switch(config)#line ssh

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

Module	Login List	Enable List
Telnet	default	default
Ssh	Login1	Enable1
Http	default	default

Switch(config-line)#end

Switch#copy running-config startup-config

- HTTP

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z HTTP:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip http login authentication {** *method-list* **}** Powiąż listę metod logowania z HTTP. *method-list*: Podaj nazwę listy metod logowania.
Krok 3	**ip http enable authentication {** *method-list* **}** Powiąż listę metod hasła dostępu z HTTP. *method-list*: Podaj nazwę listy metod hasła dostępu.
Krok 4	**show aaa global** Przejrzyj ustawienia list aplikacji.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z HTTP:

Switch#configure

Switch(config)#ip http login authentication Login1

Switch(config)#ip http enable authentication Enable1

Switch(config)#show aaa global

Module	Login List	Enable List
Telnet	default	default
Ssh	default	default
Http	Login1	Enable1

Switch(config)#end

Switch#copy running-config startup-config

1.2.5 Konfiguracja konta logowania i hasła dostępu

Konto logowania i hasło dostępu można skonfigurować lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+.

- Na przełączniku

Lokalną nazwę użytkownika i hasło logowania można skonfigurować na stronie zarządzania kontami użytkowników. Szczegółowe informacje znajdziesz w rozdziale *Zarządzanie systemem*.

Wykonaj poniższe kroki, aby skonfigurować lokalne hasło dostępu do uzyskania uprawnień administratora:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**enable admin password {** [0] *password* **|** 7 *encrypted-password* **}** Ustaw hasło dostępu. To polecenia korzysta z szyfrowania symetrycznego. 0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego o stałej długości. Domyślnym ustawieniem jest 0. *password* jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. *encrypted-password* to klucz szyfrowania symetrycznego o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej. **enable admin secret {** [0] *password* **|** 5 *encrypted-password* **}** Ustaw hasło dostępu. To polecenia korzysta z szyfrowania MD5. 0 i 5 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 5 oznacza szyfrowanie MD5 o stałej długości. Domyślnym ustawieniem jest 0. *password* jest ciągiem 1 - 31 znaków alfanumerycznych lub symboli. *encrypted-password* jest hasłem szyfrowanym MD5 o stałej długości, które można skopiować z pliku konfiguracyjnego innego przełącznika.

Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

- Na serwerze

Użytkownicy konta utworzonych poprzez serwer RADIUS/TACACS+ mogą tylko przeglądać ustawienia i informacje sieciowe bez hasła dostępu.

Zasady konfiguracji na serwerze są następujące:

- W przypadku konfiguracji uwierzytelniania logowaniem, na serwerze można utworzyć więcej niż jedno konto logowania. Ponadto, można także dostosować nazwę użytkownika i hasło.

- W przypadku konfiguracji hasła dostępu:

  Na serwerze RADIUS nazwą użytkownika musi być **$enable$**, ale hasło dostępu jest konfigurowalne. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

  Na serwerze TACACS+ ustaw hasło logowania w pliku konfiguracyjnym, wpisując wartość “enable 15”. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

Wskazówka: Korzystając z polecenia **enable-admin** zalogowani goście mogą podać hasło dostępu i uzyskać uprawnienia administratora.

Część 17

Konfiguracja 802.1x

ROZDZIAŁY

1 Konfiguracja 802.1x

Aby przeprowadzić konfigurację 802.1x, postępuj zgodnie z poniższymi krokami.

1) Skonfiguruj serwer RADIUS.
2) Skonfiguruj 802.1x globalnie.
3) Skonfiguruj 802.1x na portach.

Dodatkowo możesz sprawdzić stan wystawcy uwierzytelnienia.

Wytyczne konfiguracyjne

Uwierzytelnianie 802.1x i funkcja Port Security nie mogą być jednocześnie włączone. Przed włączeniem uwierzytelniania 802.1x upewnij się, że funkcja Port Security jest wyłączona.

1.1 Przez GUI

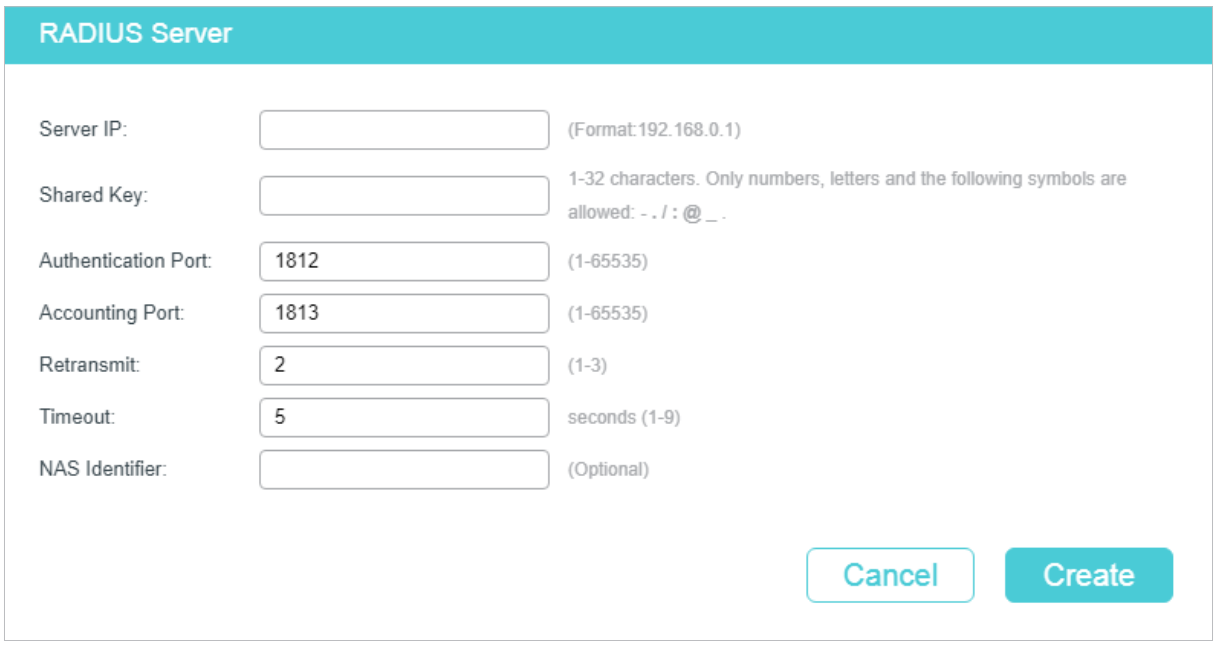
1.1.1 Konfiguracja serwera RADIUS

Skonfiguruj parametry i grupę serwera RADIUS.

- Dodawanie serwera RADIUS

Wybierz menu **SECURITY > AAA > RADIUS Config** i kliknij Add , aby załadować następującą stronę.

Rys. 1-1 Dodawanie serwera RADIUS



Aby dodać serwer RADIUS, postępuj zgodnie z poniższymi krokami:

1) Skonfiguruj parametry serwera RADIUS.

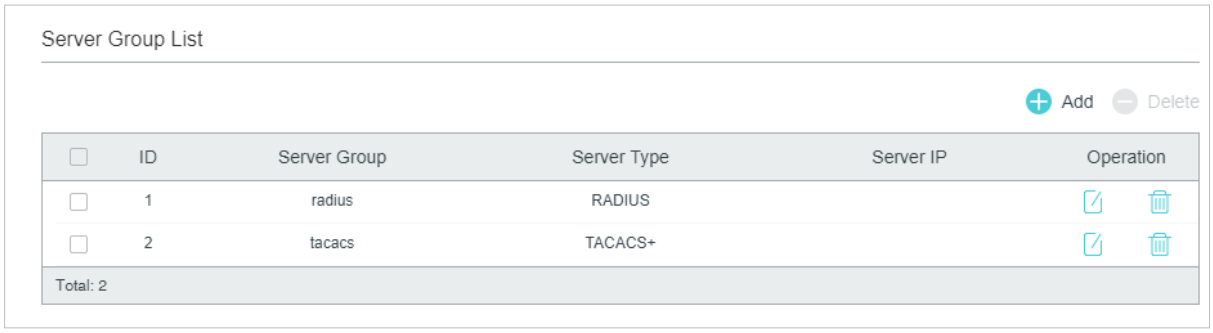
Server IP	Wprowadź adres IP serwera obsługującego protokół RADIUS.
Shared Key	Wprowadź klucz wspólny dla serwera RADIUS i przełącznika. Serwer RADIUS i przełącznik wykorzystują ciąg klucza do szyfrowania haseł i wymiany odpowiedzi.
Authentication Port	Wyznacz na serwerze RADIUS port docelowy UDP do żądań uwierzytelniania. Ustawienie domyślne to 1812.
Accounting Port	Wyznacz na serwerze RADIUS port docelowy UDP do żądań rozliczania. Ustawienie domyślne to 1813.
Retransmit	Wyznacz, ile razy ponawiane będzie wysyłanie żądania na serwer w przypadku braku odpowiedzi serwera. Ustawienie domyślne to 2.
Timeout	Wyznacz, ile czasu przełącznik będzie czekał na odpowiedź serwera przed ponownym wysłaniem żądania. Ustawienie domyślne to 5 s.
NAS Identifier	Ustaw nazwę NAS (Network Access Server), która będzie zawarta w pakietach RADIUS w celu identyfikacji. Nazwa powinna zawierać od 1 do 31 znaków. Domyślnie jako nazwa ustawiony jest adres MAC przełącznika. Zwykle serwer NAS sam identyfikuje przełącznik.

2) Kliknij **Apply**.

■ Konfiguracja grupy serwera RADIUS

Wybierz menu **SECURITY > AAA > Server Group**, aby załadować następującą stronę.

Rys. 1-2 Dodawanie grupy serwera

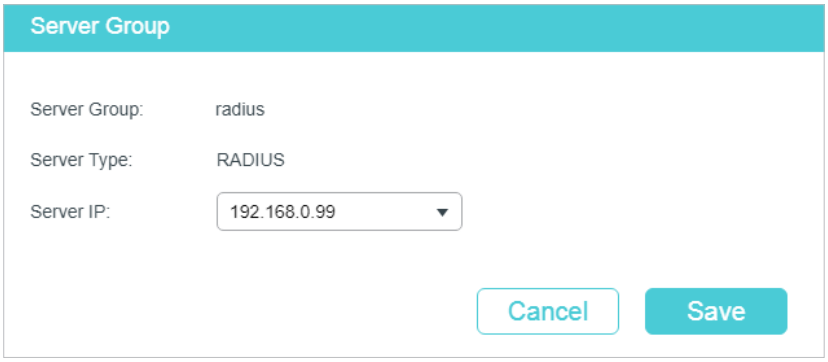


Aby dodać serwer RADIUS do grupy serwera, postępuj zgodnie z poniższymi krokami:

1) Kliknij , aby edytować domyślną grupę serwera RADIUS lub kliknij Add , aby dodać nową grupę serwera.

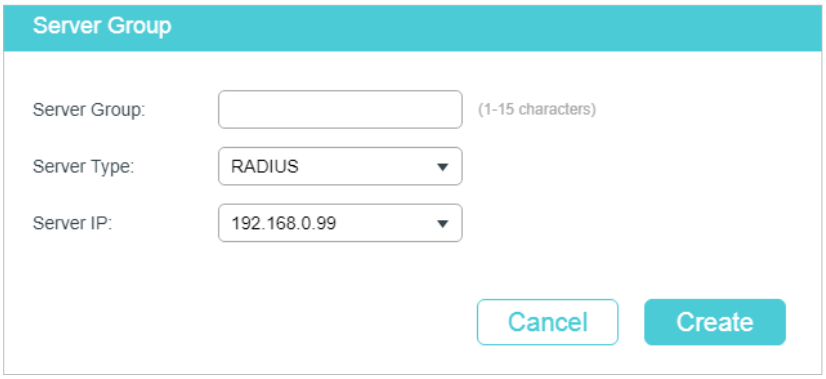
W przypadku kliknięcia pojawi się następujące okno. Wybierz serwer RADIUS i kliknij **Save**.

Rys. 1-3 Edytowanie grupy serwera



W przypadku kliknięcia Add pojawi się następujące okno. Ustaw nazwę grupy serwera, wybierz typ serwera jako RADIUS i wybierz adres IP serwera RADIUS. Kliknij **Save**.

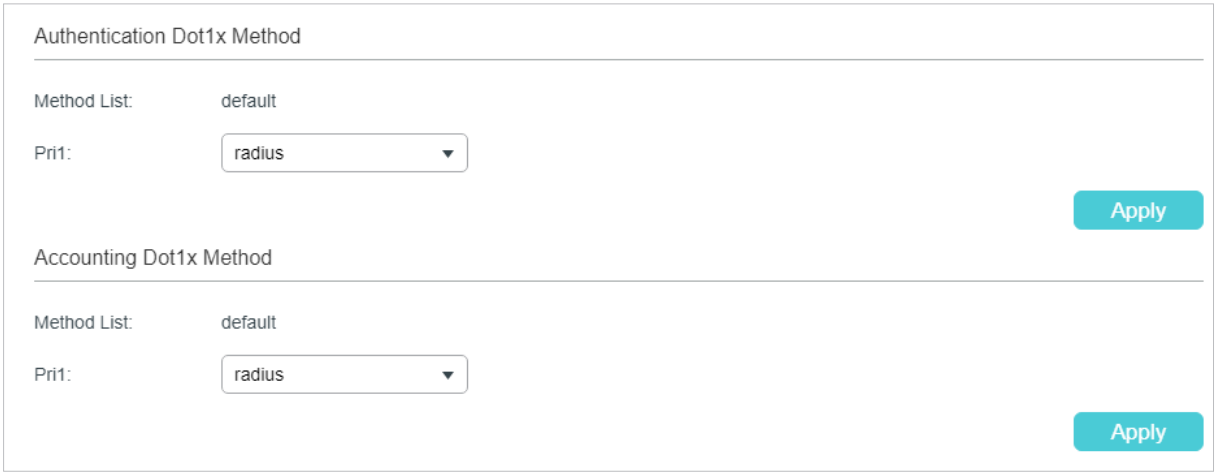
Rys. 1-4 Dodawanie grupy serwera



■ Konfiguracja listy Dot1x

Wybierz menu **SECURITY > AAA > Dot1x List**, aby załadować następującą stronę.

Rys. 1-5 Konfiguracja listy Dot1x



Aby skonfigurować grupy serwera RADIUS do uwierzytelniania 802.1x i rozliczania:

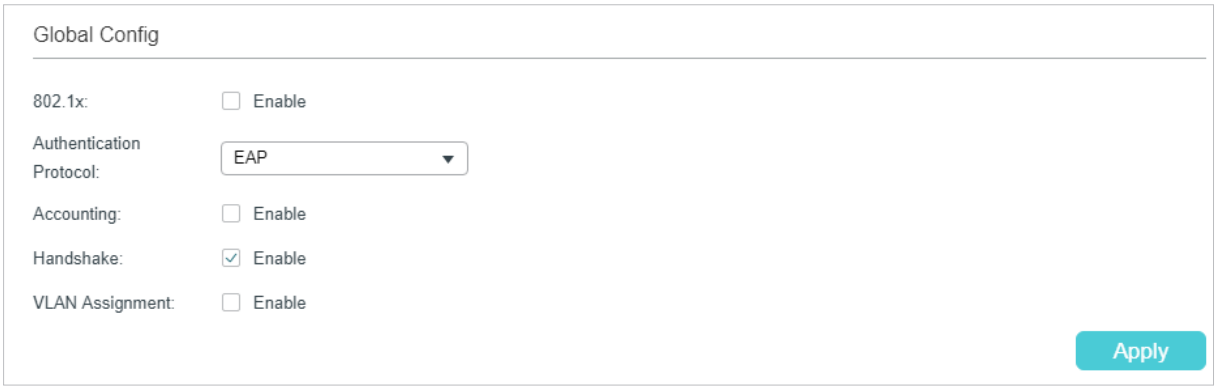
1) W sekcji **Authentication Dot1x Method** z rozwijanej listy Pri1 wybierz grupę serwera RADIUS do uwierzytelniania i kliknij **Apply**.

2) W sekcji **Accounting Dot1x Method** z rozwijanej listy Pri1 wybierz grupę serwera RADIUS do rozliczania i kliknij **Apply**.

1.1.2 Konfiguracja globalna 802.1x

Wybierz menu **SECURITY > 802.1x > Global Config**, aby załadować następującą stronę.

Rys. 1-6 Konfiguracja globalna



Aby skonfigurować globalne parametry 802.1x, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Global Config** skonfiguruj następujące parametry.

802.1x	Włącz lub wyłącz 802.1x globalnie.
Auth Protocol	Wybierz protokół uwierzytelniania 802.1x. **PAP**: System uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem i klientem. Przekazywanie pakietów EAP (Extensible Authentication Protocol) jest zakończane na przełączniku, a pakiety EAP konwertowane są do innych pakietów protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania. **EAP**: System uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem i klientem. Pakiety EAP z danymi uwierzytelniania są kondensowane w pakietach zaawansowanego protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania.
Accounting	Włącz lub wyłącz funkcję rozliczania 802.1x.
Handshake	Włącz lub wyłącz funkcję Handshake. Funkcja służy do wykrywania stanu połączenia między TP-Link 802.1x Client i przełącznikiem. Wyłącz funkcję Handshake, jeżeli korzystasz z innych oprogramowań niż TP-Link 802.1x Client.

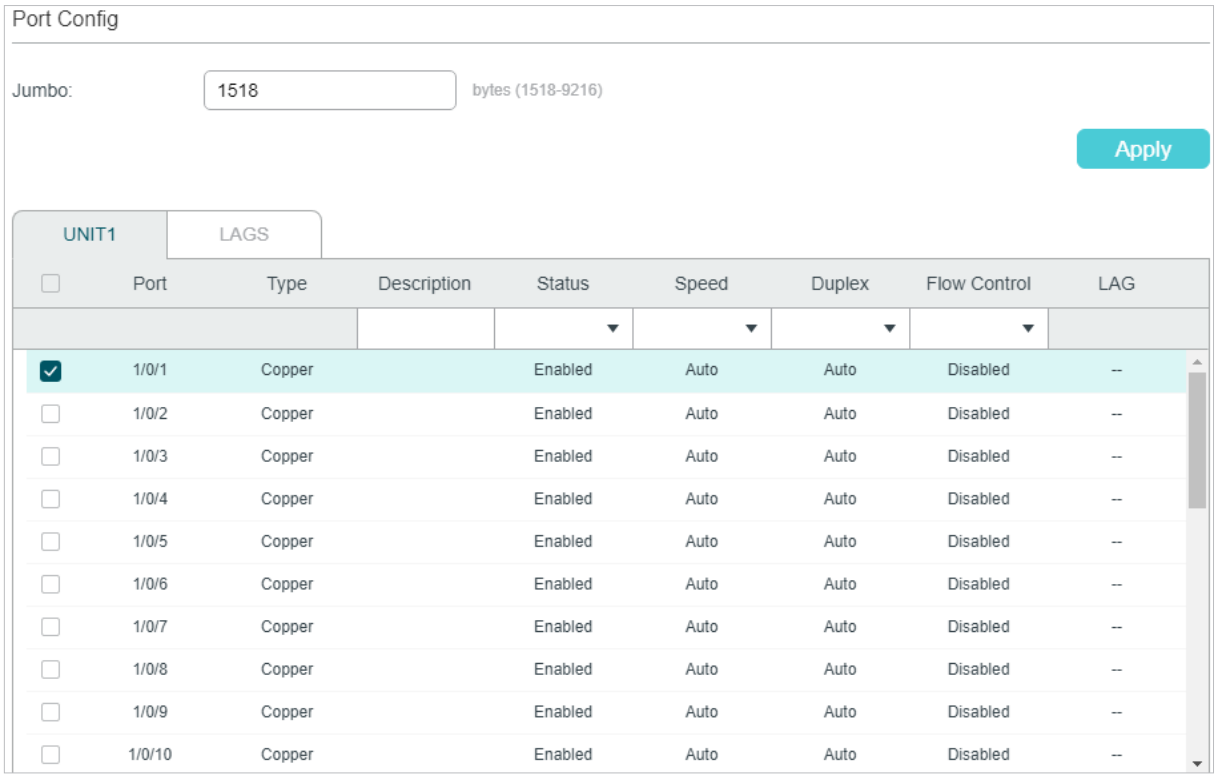
VLAN Assignment	Włącz lub wyłącz funkcję przydziału VLAN 802.1x. Przydział VLAN 802.1x to technologia umożliwiająca serwerowi RADIUS wysłanie przydziału VLAN do portu po jego uwierzytelnieniu. Jeżeli przypisanego VLAN nie ma na przełączniku, przełącznik automatycznie utworzy powiązany VLAN, doda do niego port uwierzytelniania i zmieni PVID oparty na przydzielonym VLAN. Jeżeli przydzielony VLAN istnieje na przełączniku, zamiast tworzyć nowy VLAN, przełącznik bezpośrednio doda port uwierzytelniania do powiązanego VLAN i zmieni PVID. Jeżeli serwer RADIUS nie dostarczy żadnego VLAN lub jeżeli uwierzytelnianie 802.1x jest wyłączone, port po pomyślnym uwierzytelnieniu pozostanie w swojej sieci VLAN.

2) Kliknij **Apply**.

1.1.3 Konfiguracja 802.1x na portach

Wybierz menu **SECURITY > 802.1x > Port Config**, aby załadować następującą stronę.

Rys. 1-7 Konfiguracja portu



Aby skonfigurować uwierzytelnianie 802.1x na wybranym porcie, postępuj zgodnie z poniższymi krokami:

1) Wybierz co najmniej jeden port i skonfiguruj następujące parametry:

Status	Włącz uwierzytelnianie 802.1x na porcie.

MAB	Zaznacz, czy chcesz połączyć na porcie funkcję MAB (MAC-Based Authentication Bypass). Przy włączonej funkcji MAB przełącznik automatycznie wysyła do serwera uwierzytelniania ramkę żądania dostępu RADIUS z adresem MAC klienta ustawionym jako nazwa użytkownika i hasło. Konieczna jest konfiguracja serwera RADIUS z danymi do uwierzytelniania klienta. Możesz włączyć tę funkcję na portach IEEE 802.1x podłączonych do urządzenia bez obsługi 802.1x. Dla przykładu, większość drukarek, telefonów IP i faksów nie obsługuje 802.1x. *Note:* MAB nie zadziała, jeżeli włączony jest Guest VLAN.
Guest VLAN	Ustaw ID dla Guest VLAN. 0 oznacza, że Guest VLAN jest wyłączony. Skonfigurowany VLAN musi być istniejącym VLAN 802.1Q. Przy włączonej funkcji Guest VLAN port ma dostęp do zasobów w sieci VLAN dla gości, nawet jeżeli port nie został jeszcze uwierzytelniony. Jeżeli guest VLAN jest wyłączony, a port nie został uwierzytelniony, port nie ma dostępu do zasobów LAN.
Port Control	Wybierz tryb ochrony portu. Domyślnie ustawiony jest tryb Auto. **Auto**: Jeżeli wybierzesz tę opcję, port będzie miał dostęp do sieci tylko po uwierzytelnieniu. **Force-Authorized**: Jeżeli wybierzesz tę opcję, port nie będzie musiał być uwierzytelniony, żeby mieć dostęp do sieci. **Force-Unauthorized**: Jeżeli wybierzesz tę opcję, port nie będzie mógł zostać uwierzytelniony.
Port Method	Wybierz strategię portu. Domyślnie ustawiona jest opcja MAC Based. **MAC Based**: Wszyscy klienci podłączeni do portu muszą być uwierzytelnieni. **Port Based**: Jeżeli jeden klient podłączony do portu jest uwierzytelniony, inni klienci mogą łączy się z LAN bez uwierzytelniania.
Maximum Request (1-9)	Wyznacz maks. liczbę prób wysłania pakietu uwierzytelniania. Wartość powinna wynosić od 1 do 9. Wartość domyślna to 3 razy.
Quiet Period (1-999)	Wyznacz czas trwania Quiet Period. Wartość powinna wynosić od 1 do 999 sekund. Czas domyślny to 10 sekund. Quiet Period rozpoczyna się po błędzie uwierzytelniania. Jest to czas, w którym przełącznik nie przetwarza żądań uwierzytelniania od tego samego klienta.
Supplicant Timeout (1-9)	Wyznacz maks. czas, przez który przełącznik czeka na odpowiedź klienta. Wartość powinna wynosić od 1 do 9 sekund. Wartość domyślna to 3 sekundy. Jeżeli w wyznaczonym czasie przełącznik nie otrzyma od klienta żadnej odpowiedzi, ponownie wyśle żądanie.

Authorized	Informacja o tym, czy port jest uwierzytelniony, czy nie.
LAG	Informacja do której grupy LAG należy port.

2) Kliknij **Apply**.

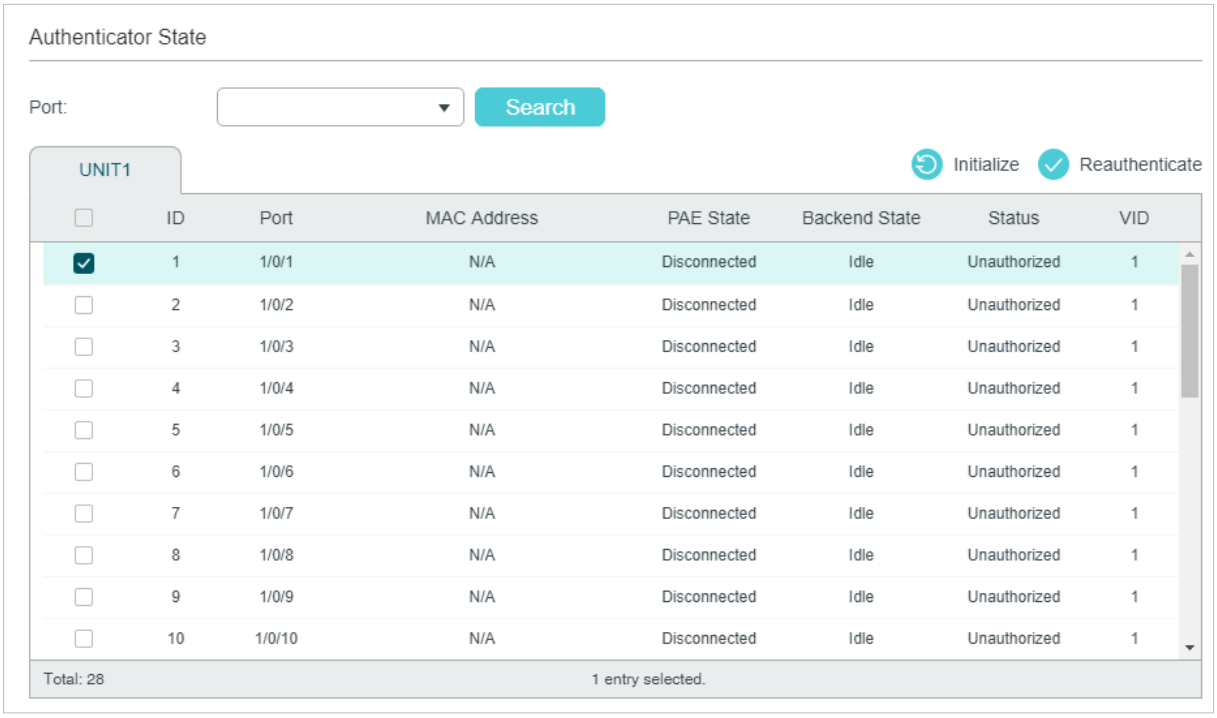
Uwaga:

Jeżeli port należy do grupy LAG, nie można włączyć jego funkcji uwierzytelniania 802.1x. Analogicznie, port z włączonym uwierzytelnianiem 802.1x nie może być dodany do grupy LAG.

1.1.4 Sprawdzanie stanu wystawcy uwierzytelnienia

Wybierz menu **SECURITY > 802.1x > Authenticator State**, aby załadować następującą stronę.

Rys.1-8 Sprawdzanie stanu wystawcy uwierzytelnienia



Na tej stronie możesz sprawdzić stan uwierzytelniania każdego portu.

Port	Informacja o numerze portu.
MAC Address	Informacja o adresie MAC uwierzytelnionego urządzenia. Jeżeli wybraną strategią portu jest Port Based (w oparciu o port), adres MAC pierwszego uwierzytelnionego urządzenia będzie wyświetlał się z sufiksem „p".
PAE State	Informacja o aktualnym stanie maszyny stanów uwierzytelniania PAE. Dostępne wartości to: Initialize (Inicjuj), Disconnected (Rozłączony), Connecting (Łączenie), Authenticating (Uwierzytelnianie), Authenticated (Uwierzytelniony), Aborting (Przerywanie), Held (Utrzymany), ForceAuthorized i ForceUnauthorized.

Backend State	Informacja o bieżącym stanie maszyny stanów backendu uwierzytelniania. Dostępne wartości to: Request (żądanie), Response (odpowiedź), Success (powodzenie), Fail (niepowodzenie), Timeout (koniec czasu), Initialize (inicjowanie) i Idle (bezczynność).
Status	Informacja o tym, czy port jest uwierzytelniony, czy nie.
VLAN ID	Informacja o VLAN ID przypisanym przez wystawcę uwierzytelnienia do urządzenia suplikującego, jeżeli powiązany port jest uwierzytelniony. Jeżeli powiązany port nie jest uwierzytelniony i dostępny jest Guest VLAN ID, wyświetlony zostanie Guest VLAN ID.

1.2 Przez CLI

1.2.1 Konfiguracja serwera RADIUS

Aby skonfigurować serwer RADIUS, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**radius-server host** *ip-address* **[auth-port** *port-id* **] [acct-port** *port-id* **] [timeout** *time* **] [retransmit** *number* **] [nas-id** *nas-id* **] key {** [0] *string* **|** 7 *encrypted-string* **}** Dodaj serwer RADIUS i odpowiednio skonfiguruj powiązane parametry. **host** *ip-address*: Wpisz adres IP serwera obsługującego protokół RADIUS. **auth-port** *port-id*: Wyznacz port docelowy UDP na serwerze RADIUS do żądań uwierzytelniania. Port domyślny to 1812. **acct-port** *port-id:* Wyznacz port docelowy UDP na serwerze RADIUS do żądań rozliczania. Port domyślny to 1813. Z reguły funkcja rozliczania nie jest wykorzystywana w zarządzaniu kontem uwierzytelniania. **timeout** *time*: Wyznacz, ile czasu przełącznik będzie czekał na odpowiedź serwera przed ponownym wysłaniem żądania. Wartość powinna wynosić od 1 do 9 sekund. Ustawienie domyślne to 5 s. **retransmit** *number*: Wyznacz, ile razy ponawiane będzie wysyłanie żądania na serwer w przypadku braku odpowiedzi serwera. Wartość powinna wynosić od 1 do 3. Ustawienie domyślne to 2. **nas-id** *nas-id:* Określ nazwę NAS (Network Access Server), która będzie zawarta w pakietach RADIUS w celu identyfikacji. Nazwa powinna zawierać od 1 do 31 znaków. Domyślnie jako nazwa ustawiony jest adres MAC przełącznika. Z reguły NAS sam wskazuje na przełącznik. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Wprowadź klucz wspólny. 0 i 7wykluczają wybieranie trybu szyfrowania. 0 oznacza, że wybrany zostanie klucz nieszyfrowany. 7 oznacza, że zastosowany zostanie klucz szyfrowany symetrycznie o stałej długości. Domyślny typ szyfrowania to 0. *string* jest to klucz wspólny dla przełącznika i serwera, składający się z maks. 32 znaków. *encrypted-string* to klucz szyfrowany symetrycznie o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Klucz lub klucz zaszyfrowany skonfigurowany w tym miejscu zostanie wyświetlony w formie zaszyfrowanej.

Krok 3	**aaa group** radius *group-name* Utwórz grupę serwera RADIUS. radius: Ustaw typ grypy na radius. *group-name*: Ustaw nazwę grupy.
Krok 4	**server** *ip-address* Dodaj istniejące serwery do grupy serwera. *ip-address*: Ustaw adres IP serwera, który będzie dodany do grupy.
Krok 5	**exit** Wróć do trybu konfiguracji globalnej.
Krok 6	**aaa authentication dot1x default** { *method* } Wybierz grupę RADIUS do uwierzytelniania 802.1x. *method:* Wyznacz grupę RADIUS do uwierzytelniania 802.1x. **aaa accounting dot1x default** { *method* } Wybierz grupę RADIUS do rozliczania 802.1x. *method:* Wybierz grupę RADIUS do rozliczania 802.1x. *Note*: Jeżeli dostępne są liczne serwery RADIUS, zaleca się dodanie ich do innych grup serwera, oddzielnie do uwierzytelniania i rozliczania.
Krok 7	**show radius-server** (Opcjonalnie) Sprawdź ustawienia serwera RADIUS.
Krok 8	**show aaa group** [*group-name*] (Opcjonalnie) Sprawdź ustawienia grupy serwera.
Krok 9	**show aaa authentication** dot1x (Opcjonalnie) Sprawdź listę strategii uwierzytelniania.
Krok 10	**show aaa accounting** dot1x (Opcjonalnie) Sprawdź listę strategii rozliczania.
Krok 11	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode)
Krok 12	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Następny przykład prezentuje włączanie AAA, dodawanie serwera RADIUS do grupy serwera nazwanej radius1 i zastosowanie tej grupy serwera do uwierzytelniania 802.1x. Adres IP serwera RADIUS to 192.168.0.100; klucz wspólny to 123456; port uwierzytelniania to 1812; port rozliczania to 1813.

Switch#configure

Switch(config)#radius-server host 192.168.0.100 **auth-port** 1812 **acct-port** 1813 **key** 123456

Switch(config)#aaa group radius radius1

Switch(aaa-group)#server 192.168.0.100

Switch(aaa-group)#exit

Switch(config)#aaa authentication dot1x default radius1

Switch(config)#aaa accounting dot1x default radius1

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.100	1812	1813	5	2	000AEB132397	123456

Switch(config)#show aaa group radius1

192.168.0.100

Switch(config)#show aaa authentication dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#show aaa accounting dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja globalna 802.1x

Aby skonfigurować 802.1x globalnie, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**dot1x system-auth-control** Włącz uwierzytelnianie 802.1x globalnie.

Krok 3	**dot1x auth-protocol** { pap | eap } Konfiguracja protokołu uwierzytelniania 802.1x. pap: Wyznacz PAP jako protokół uwierzytelniania. W przypadku wybrania tej opcji system uwierzytelniania 802.1x wykorzystuje pakiety EAP (Extensible Authentication Protocol) do wymiany informacji między przełącznikiem, a klientem. Przekazywanie pakietów EAP jest zakończane na przełączniku, a pakiety EAP konwertowane są do innych pakietów protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania eap: Wyznacz EAP jako protokół uwierzytelniania. W przypadku wybrania tej opcji system uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem, a klientem. Pakiety EAP z danymi uwierzytelniania są kondensowane w pakietach zaawansowanego protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania.
Krok 4	**dot1x accounting** (Opcjonalnie) Włącz funkcję rozliczania.
Krok 5	**dot1x handshake** (Opcjonalnie) Włącz funkcję Handshake. Funkcja służy do wykrywania stanu połączenia między TP-Link 802.1x Client i przełącznikiem. Wyłącz funkcję Handshake, jeżeli korzystasz z innych oprogramowań niż TP-Link 802.1x Client.
Krok 6	**dot1x vlan-assignment** (Opcjonalnie) Włącz lub wyłącz funkcję przydziału VLAN 802.1x. Przydział VLAN 802.1x to technologia umożliwiająca serwerowi RADIUS wysłanie przydziału VLAN do portu po jego uwierzytelnieniu. Jeżeli przypisanego VLAN nie ma na przełączniku, przełącznik automatycznie utworzy powiązany VLAN, doda do niego port uwierzytelniania i zmieni PVID oparty na przydzielonym VLAN. Jeżeli przydzielony VLAN istnieje na przełączniku, zamiast tworzyć nowy VLAN, przełącznik bezpośrednio doda port uwierzytelniania do powiązanego VLAN i zmieni PVID. Jeżeli serwer RADIUS nie dostarczy żadnego VLAN lub jeżeli uwierzytelnianie 802.1x jest wyłączone, port po pomyślnym uwierzytelnieniu pozostanie w swojej sieci VLAN.
Krok 7	**show dot1x global** (Opcjonalnie) Sprawdź ustawienia globalne 802.1x.
Krok 8	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Następujący przykład prezentuje włączanie uwierzytelniania 802.1x, ustawianie PAP na metodę uwierzytelniania i zachowanie ustawień domyślnych dla pozostałych parametrów:

Switch#configure

Switch(config)#dot1x system-auth-control

Switch(config)#dot1x auth-protocol pap

Switch(config)#show dot1x global

802.1X State: Enabled

Authentication Protocol: PAP

Handshake State: Enabled

802.1X Accounting State: Disabled

802.1X VLAN Assignment State: Disabled

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Konfiguracja 802.1x na portach

Aby skonfigurować port, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu. *port:* Wprowadź ID postu do konfiguracji.
Krok 3	**dot1x** Włącz uwierzytelnianie 802.1x dla portu.
Krok 4	**dot1x mab** Włącz na porcie funkcję MAB (MAC-Based Authentication Bypass). Przy włączonej funkcji MAB przełącznik automatycznie wysyła do serwera uwierzytelniania ramkę żądania dostępu RADIUS z adresem MAC klienta ustawionym jako nazwa użytkownika i hasło. Konieczna jest konfiguracja serwera RADIUS z danymi do uwierzytelniania klienta. Możesz włączyć tę funkcję na portach IEEE 802.1x podłączonych do urządzenia bez obsługi 802.1x. Dla przykładu, większość drukarek, telefonów IP i faksów nie obsługuje 802.1x. *Note:* MAB nie zadziała, jeżeli włączony jest Guest VLAN.

Krok 5	**dot1x guest-vlan** *vid* (Opcjonalnie) Skonfiguruj na porcie VLAN dla gości (Guest VLAN). *vid:* Określ ID sieci VLAN, która będzie skonfigurowana jako VLAN dla gości. Wartość powinna mieścić się pomiędzy 0 a 4094. 0 oznacza, że Guest VLAN jest wyłączony na porcie. Skonfigurowany VLAN musi być istniejącym VLAN 802.1Q. Klienci w sieci VLAN dla gości mają dostęp tylko do zasobów z wybranych sieci VLAN. *Note*: Aby korzystać z Guest VLAN, typ kontroli portu powinien by ustawiony jako port-based.
Krok 6	**dot1x port-control** { auto | authorized-force | unauthorized-force } Skonfiguruj tryb kontroli dla portu. Domyślnie ustawiony jest tryb auto. auto: Jeżeli wybierzesz tę opcję, port będzie miał dostęp do sieci tylko po uwierzytelnieniu. authorized-force: Jeżeli wybierzesz tę opcję, port nie będzie musiał być uwierzytelniony, żeby mieć dostęp do sieci. unauthorized-force: Jeżeli wybierzesz tę opcję, port nie będzie mógł zostać uwierzytelniony.
Krok 7	**dot1x port-method** { mac-based | port-based } Skonfiguruj typ kontroli portu. Domyślnie ustawiona jest opcja MAC Based. mac-based **(w oparciu o MAC)**: Wszyscy klienci podłączeni do portu muszą być uwierzytelnieni. port-based **(w oparciu o port)**: Jeżeli jeden klient podłączony do portu jest uwierzytelniony, inni klienci mogą łączy się z LAN bez uwierzytelniania.
Krok 8	**dot1x max-req** *times* Wyznacz maks. liczbę prób wysłania przez klienta pakietu uwierzytelniania. *times:* Maks. liczba prób wysłania pakietu uwierzytelniania przez klienta. Wartość powinna wynosić od 1 do 9. Wartość domyślna to 3 razy.
Krok 9	**dot1x quiet-period** [time] (Opcjonalnie) Wyznacz czas trwania Quiet Period dla uwierzytelniania 802.1x i skonfiguruj Quiet Period. time: Ustaw wartość Quiet Period między 1 a 999 sekund. Wartość domyślna to 10 sekund. Quiet Period rozpoczyna się po błędzie uwierzytelniania. Jest to czas, w którym przełącznik nie przetwarza żądań uwierzytelniania od tego samego klienta.

Krok 10	**dot1x timeout supp-timeout** *time* Skonfiguruj Supplicant Timeout (przekroczenie czasu dla suplikanta). *time:* Wyznacz maks. czas, przez który przełącznik czeka na odpowiedź klienta. Wartość powinna wynosić od 1 do 9 sekund. Wartość domyślna to 3 sekundy. Jeżeli w wyznaczonym czasie przełącznik nie otrzyma od klienta żadnej odpowiedzi, ponownie wyśle żądanie.
Krok 11	**show dot1x interface [fastEthernet** *port* **|gigabitEthernet** *port* **| ten-gigabitEthernet** *port***]** (Opcjonalnie) Sprawdź ustawienia uwierzytelniania 802.1x authentication na porcie. *port:* Wprowadź ID portu do konfiguracji. Jeżeli nie wyznaczony zostanie konkretny port, przełącznik wyświetli ustawienia wszystkich portów.
Krok 12	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 13	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie uwierzytelniania 802.1x na porcie 1/0/2, konfigurację typu kontroli na port-based i zachowanie ustawień domyślnych dla pozostałych parametrów.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#dot1x

Switch(config-if)#dot1x port-method port-based

Switch(config-if)#show dot1x interface gigabitEthernet 1/0/2

Port	State	MAB State	GuestVLAN	PortControl	PortMethod
Gi1/0/2	disabled	disabled	0	auto	port-based

MaxReq	QuietPeriod	SuppTimeout	Authorized	LAG
3	10	3	unauthorized	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

1.2.4 Sprawdzanie stanu wystawcy uwierzytelnienia

Możesz sprawdzić stan wystawcy uwierzytelnienia. W razie konieczności możesz też zainicjować lub powtórzyć uwierzytelnianie wybranego klienta:

Krok 1	**show dot1x auth-state [interface fastEthernet** *port* **| interface gigabitEthernet** *port***]** Informacja o stanie wystawcy uwierzytelnienia.
Krok 2	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 3	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Wejdź w tryb konfiguracji interfejsu. *port:* Wpisz ID portu do konfiguracji.
Krok 4	**dot1x auth-init [mac** *mac-address* **]** Zainicjuj wybranego klienta. Aby mieć dostęp do sieci, klient musi dostarczyć poprawne dane, by powtórnie przejść przez proces uwierzytelniania. *mac-address:* Wpisz adres MAC aklienta, który będzie nieuwierzytelniony.
Krok 5	**dot1x auth-reauth [mac** *mac-address* **]** Uwierzytelnij na nowo wybranego klienta. *mac-address:* Wpisz adres MAC klienta, który będzie powtórnie uwierzytelniony.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Część 18

Konfiguracja Port Security

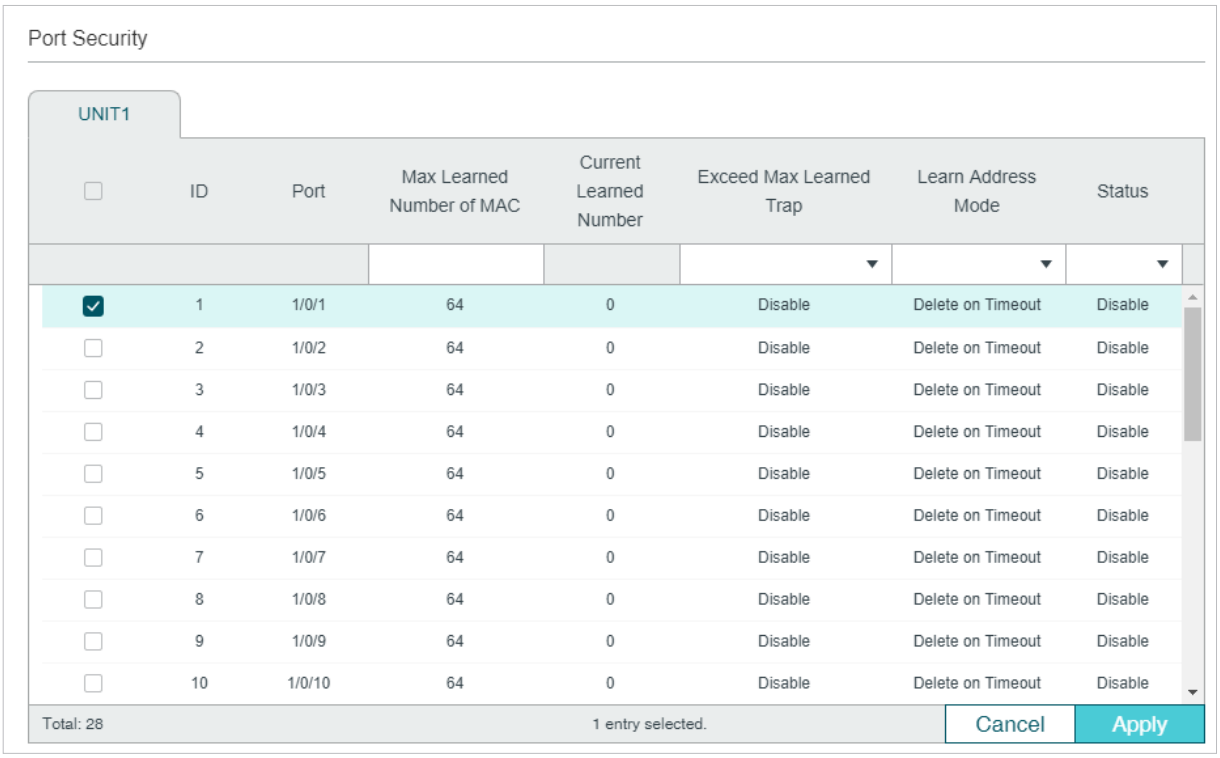
ROZDZIAŁY

1 Konfiguracja Port Security

1.1 Przez GUI

Wybierz z menu **SECURITY > Port Security,** aby wyświetlić poniższą stronę.

Rys. 1-1 Port Security



Wykonaj poniższe kroki, aby skonfigurować Port Security:

1) Wybierz jeden lub kilka portów i skonfiguruj poniższe parametry.

Port	Numer portu.
Max Learned Number of MAC	Podaj maksymalną liczbę adresów MAC, które mogą być zapamiętane na porcie. Gdy liczba zapamiętanych adresów MAC osiągnie ustalony limit, port przerwie zapamiętywanie. Ta wartość musi mieścić się w przedziale 0 - 64.
Current Learned MAC	Aktualna liczba adresów MAC, które zostały zapamiętane na porcie.
Exceed Max Learned Trap	Gdy włączysz tę opcję, w przypadku przekroczonego limitu zapamiętanych adresów MAC na określonym porcie, do hosta zarządzającego zostanie wysłane powiadomienie.

Learn Address Mode	Wybierz tryb zapamiętywania adresów MAC na porcie. Dostępne są trzy tryby: **Delete on Timeout**: Przełącznik usunie adresy MAC, które nie są używane lub aktualizowane przed terminem utraty ważności. To ustawienie jest domyślnie włączone. **Delete on Reboot**: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną usunięte po restarcie przełącznika. **Permanent**: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną zachowane nawet po restarcie przełącznika.
Status	Wybierz stan Port Security spośród trzech typów: **Drop**: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie i odrzuci pakiety z adresami MAC, które nie zostały zapamiętane. **Forward**: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie, ale prześle pakiety z adresami MAC, które nie zostały zapamiętane. **Disable**: Limit nie jest aktywny na porcie, dlatego przełącznik stosuje się do pierwotnych reguł przekazywania. To ustawienie jest domyślnie włączone.

2) Kliknij **Apply**.

Uwaga:

- Funkcji Port Security nie można włączyć na portach należących do LAG, a port o włączonej funkcji Port Security nie może być dodany do LAG.
- Włączenie w tym samym czasie Port Security i 802.1x na jednym porcie nie jest możliwe.

1.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Port Security:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Uruchom tryb konfiguracji interfejsu.

Krok 3	**mac address-table max-mac-count { [max-number** *num***] [exceed-max-learned** enable | disable**] [mode** { dynamic | static | permanent } **] [status** { forward | drop | disable } **]}** Włącz funkcję Port Security na porcie i skonfiguruj odpowiednie parametry. *num*: Maksymalna liczba adresów MAC, które mogą być zapamiętane na porcie. Prawidłowa wartość musi mieścić się w przedziale 0 - 64. Wartością domyślną jest 64. **exceed-max-learned:** Gdy włączysz tę opcję, w przypadku przekroczonego limitu zapamiętanych adresów MAC na określonym porcie, do hosta zarządzającego zostanie wysłane powiadomienie. enable: Włącz exceed-max-learned. disable: Wyłącz exceed-max-learned. **mode**: Tryby zapamiętywania adresów MAC na porcie. Dostępne są trzy tryby: dynamic: Przełącznik usunie adresy MAC, które nie są używane lub aktualizowane przed terminem utraty ważności. static: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną usunięte po restarcie przełącznika. permanent: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną zachowane nawet po restarcie przełącznika. **status**: Stan funkcji Port Security. Domyślnie funkcja jest wyłączona. drop: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie i odrzuci pakiety z adresami MAC, które nie zostały zapamiętane. forward: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie, ale prześle pakiety z adresami MAC, które nie zostały zapamiętane. disable: Limit nie jest aktywny na porcie, dlatego przełącznik stosuje się do pierwotnych reguł przekazywania. To ustawienie jest domyślnie włączone.
Krok 4	**show mac address-table max-mac-count interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Przejrzyj ustawienia Port Security i aktualnie zapamiętanych adresów MAC na porcie.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

- Funkcji Port Security nie można włączyć na portach należących do LAG, a port o włączonej funkcji Port Security nie może być dodany do LAG.
- Włączenie w tym samym czasie Port Security i 802.1x na jednym porcie nie jest możliwe.

Poniższy schemat przedstawia przykładowy sposób ustawiania maksymalnej liczby adresów MAC, które mogą być zapamiętane na porcie 1/0/1 jako 30, włączania opcji exceed-max-leaned, ustawiania trybu jako permanent i stanu jako drop:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#mac address-table max-mac-count max-number 30 **exceed-max-learned** enable **mode** permanent **status** drop

Switch(config-if)#show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Port	Max-learn	Current-learn	Exceed Max Limit	Mode	Status
----	---------	-----------	----------	------	--------
Gi1/0/1	30	0	disable	permanent	drop

Switch(config-if)#end

Switch#copy running-config startup-config

Część 19

Konfiguracja ACL

ROZDZIAŁY

1 Konfiguracja ACL

1.1 Przez GUI

1.1.1 Konfiguracja zakresu czasu

Działanie niektórych usług i funkcji opartych na ACL (Access Control List) może musieć być ograniczone do wyznaczonego zakresu czasu. W takim przypadku należy skonfigurować zakres czasu działania ACL. Więcej szczegółów dotyczących konfiguracji zakresu czasu znajdziesz w rozdziale *Zarządzanie systemem*.

1.1.2 Tworzenie ACL

Możesz utworzyć różne typy ACL i zdefiniować reguły w oparciu o źródłowy adres MAC lub IP, docelowy adres MAC lub IP, typ protokołu, numer portu itd.

MAC ACL: MAC ACL wykorzystuje źródłowy i docelowy adres MAC do czynności dopasowywania.

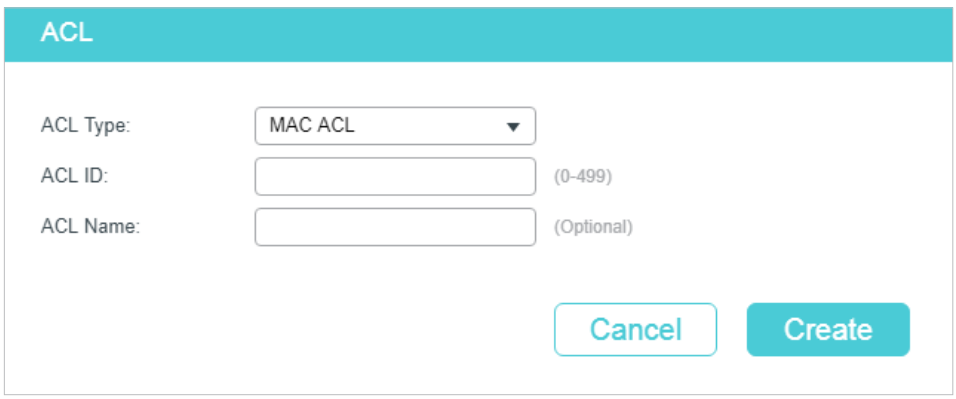
IP ACL: IP ACL wykorzystuje źródłowy i docelowy adres IP, protokoły IP itd. do czynności dopasowywania.

Combined ACL: Łączona ACL wykorzystuje do czynności dopasowywania źródłowe i docelowe adresy MAC i IP.

IPv6 ACL: IPv6 ACL wykorzystuje do czynności dopasowywania źródłowe i docelowe adresy IPv6.

Wybierz menu **SECURITY > ACL > ACL Config** i kliknij Add, aby załadować następującą stronę.

Rys. 1-1 Tworzenie ACL



Aby utworzyć ACL, postępuj zgodnie z poniższymi krokami.

1) Wybierz typ ACL i wpisz numer do identyfikacji ACL.

2) (Opcjonalnie) Przypisz nazwę do ALC.

3) Kliknij **Create**.

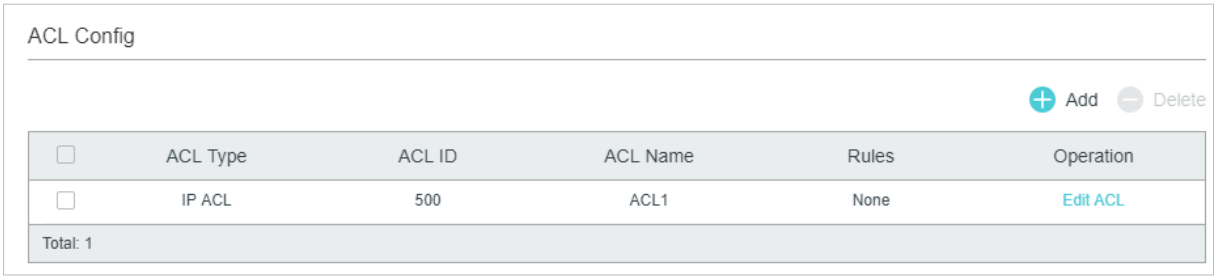
Uwaga:

Obsługiwany typ ACL i zakres ID różni się dla różnych modeli przełącznika. Należy kierować się informacją wyświetlaną na ekranie.

1.1.3 Konfiguracja reguł ACL

Utworzone ACL wyświetlane będą na stronie **SECURITY > ACL > ACL Config**.

Rys. 1-2 Edycja ACL



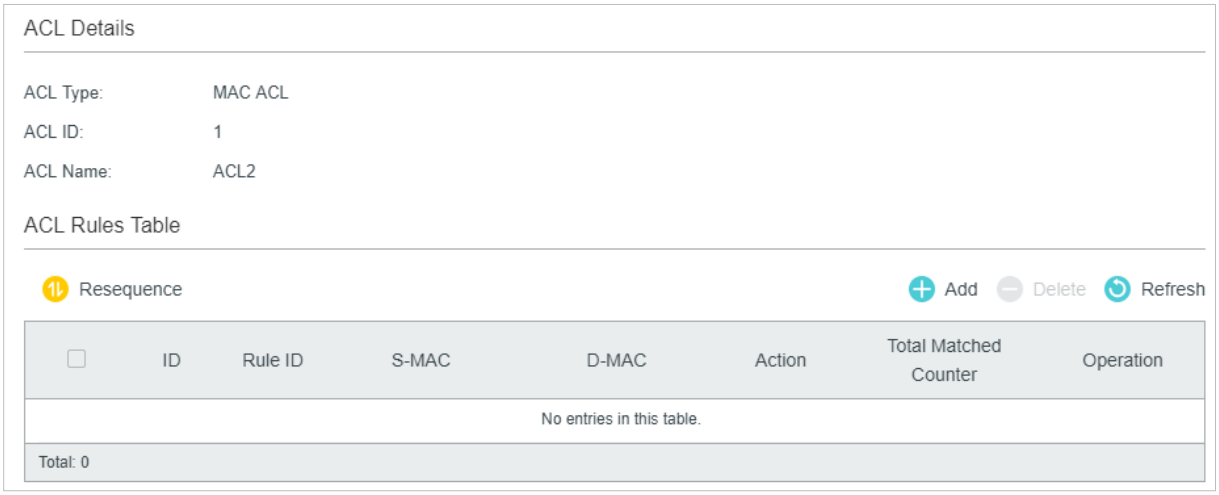
Aby skonfigurować reguły danej listy, kliknij **Edit ACL** w kolumnie **Operation**.

Następujące sekcje wprowadzają zagadnienie konfiguracji MAC ACL, IP ACL, Combined ACL i IPv6 ACL.

• Konfiguracja Reguły MAC ACL

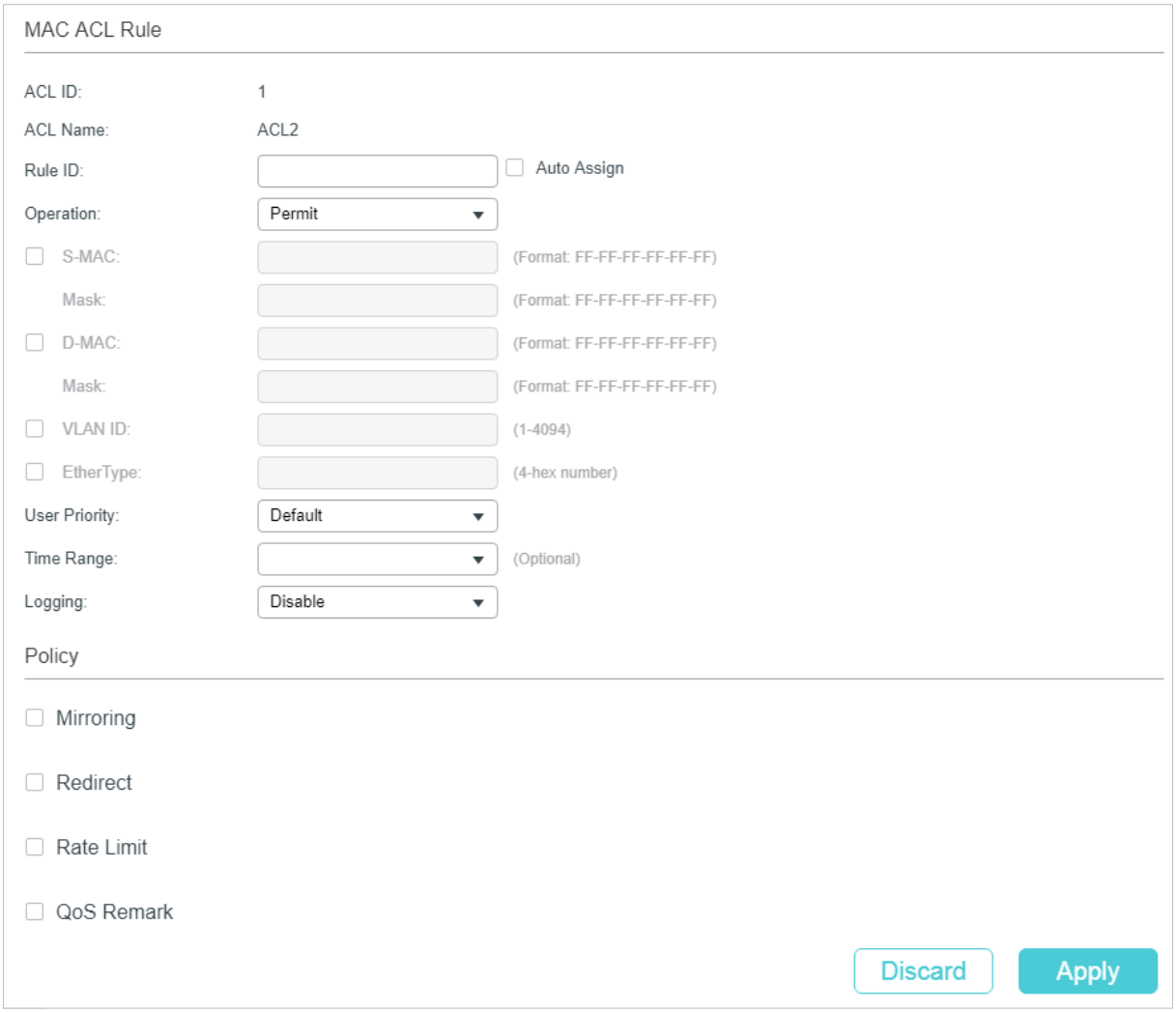
Kliknij **Edit ACL** przy wpisie MAC ACL, aby załadować następującą stronę.

Rys. 1-3 Konfiguracja Reguły MAC ACL



W sekcji **ACL Rules Table** kliknij Add, a pojawi się następujące okno.

Rys. 1-4 Konfiguracja Reguły MAC ACL



Aby skonfigurować regułę MAC ACL, postępuj zgodnie z poniższymi krokami:

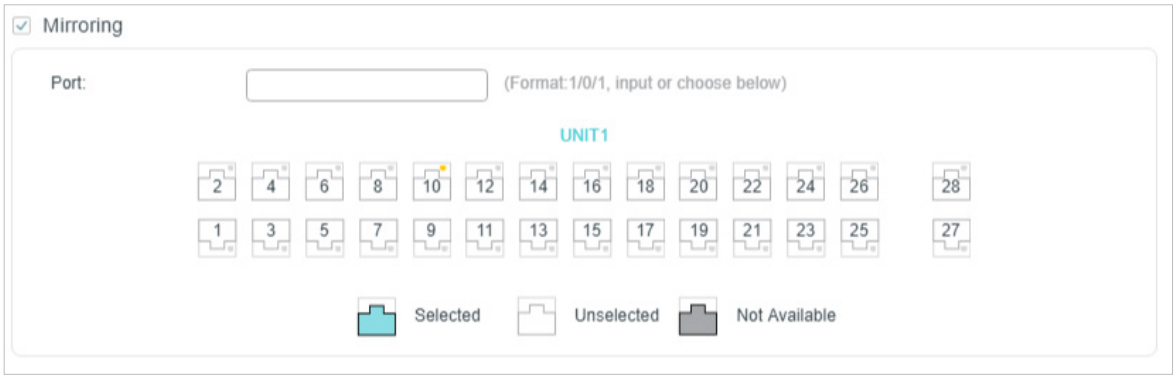
1) W sekcji **MAC ACL Rule** skonfiguruj następujące parametry.

Rule ID	Wpisz numer ID, aby umożliwić identyfikację reguły. Numer nie powinien być taki sam, jak jakikolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.
Operation	Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły. **Permit**: Jeżeli dopasowane pakiety mają być przekazywane. **Deny**: Jeżeli dopasowane pakiety mają być odrzucane.
S-MAC/Mask	Wpisz źródłowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
D-MAC/Mask	Wpisz docelowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
VLAN ID	Wpisz numer ID sieci VLAN, do której zastosowanie będzie miała ACL.

EtherType	Określ EtherType, który będzie dopasowany, używając 4 liczb szesnastkowych.
User Priority	Określ User Priority, który zostanie dopasowany.
Time Range	Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie **SYSTEM > Time Range**.
Logging	Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table.

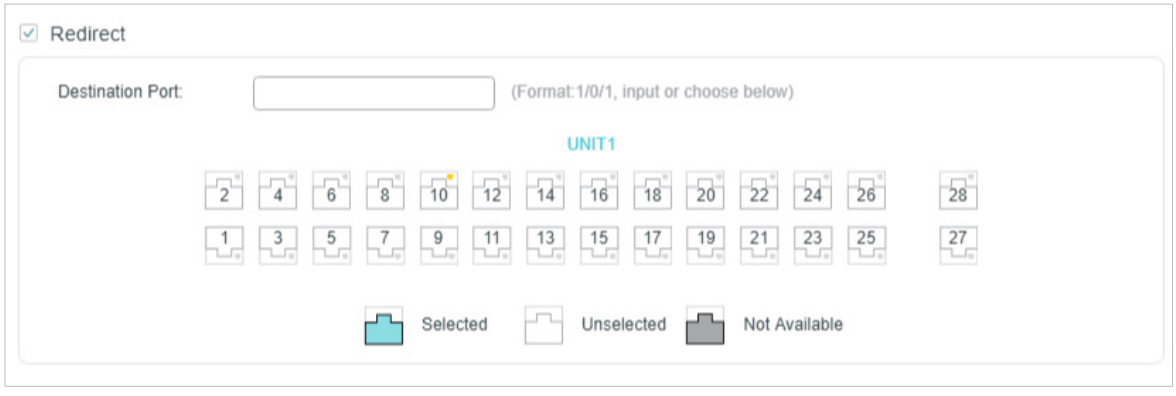
2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, na którym kopiowane będą pakiety.

Rys. 1-5 Konfiguracja funkcji Mirroring



3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego przekierowywane będą pakiety.

Rys. 1-6 Konfiguracja funkcji Redirect

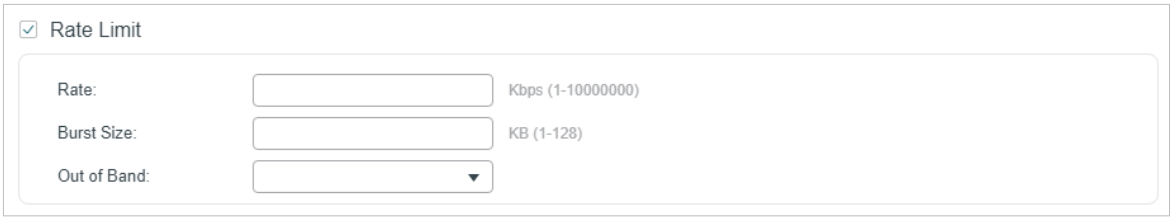


Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli funkcja została włączona, skonfiguruj powiązane parametry.

Rys. 1-7 Konfiguracja funkcji Rate Limit



Rate	Wyznacz prędkość transmisji dopasowanych pakietów.
Burst Size	Określ maks. dopuszczalną liczbę bitów na sekundę.
Out of Band	Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem. **None:** Pakiety będą przekazywane normalnie. **Drop:** Pakiety będą odrzucane.

5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 1-8 Konfiguracja QoS Remark

DSCP	Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.
Local Priority	Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.
802.1p Priority	Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.

6) Kliknij **Apply**.

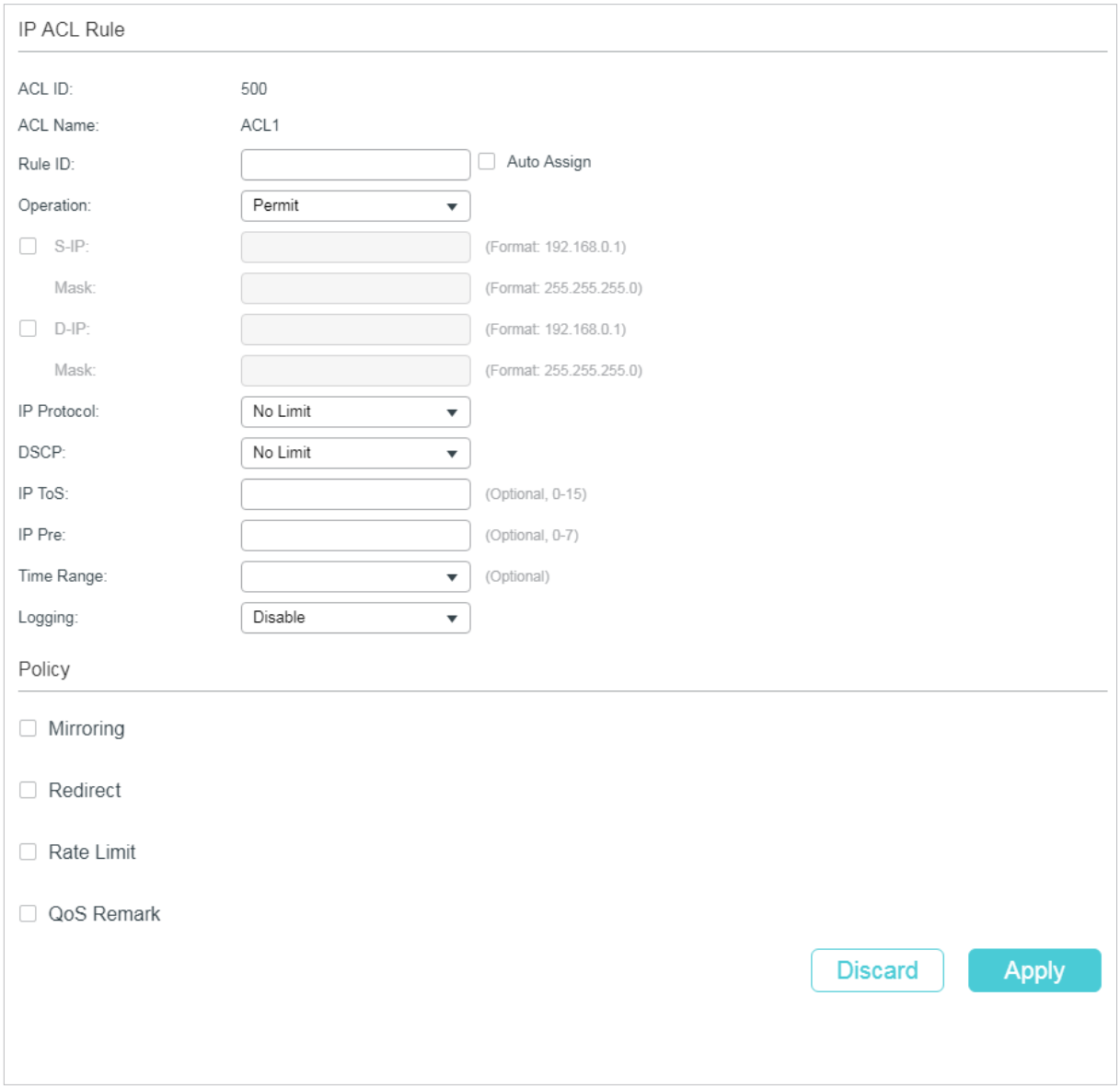
•Konfiguracja Reguły IP ACL

Kliknij **Edit ACL** dla wpisu IP ACL, aby załadować następującą stronę.

Rys. 1-9 Konfiguracja Reguły IP ACL

W sekcji **ACL Rules Table** kliknij Add i pojawi się następujące okno.

Rys. 1-10 Konfiguracja Reguły IP ACL



Aby skonfigurować regułę IP ACL, postępuj zgodnie z poniższymi krokami:

1) W sekcji **IP ACL Rule** skonfiguruj następujące parametry:

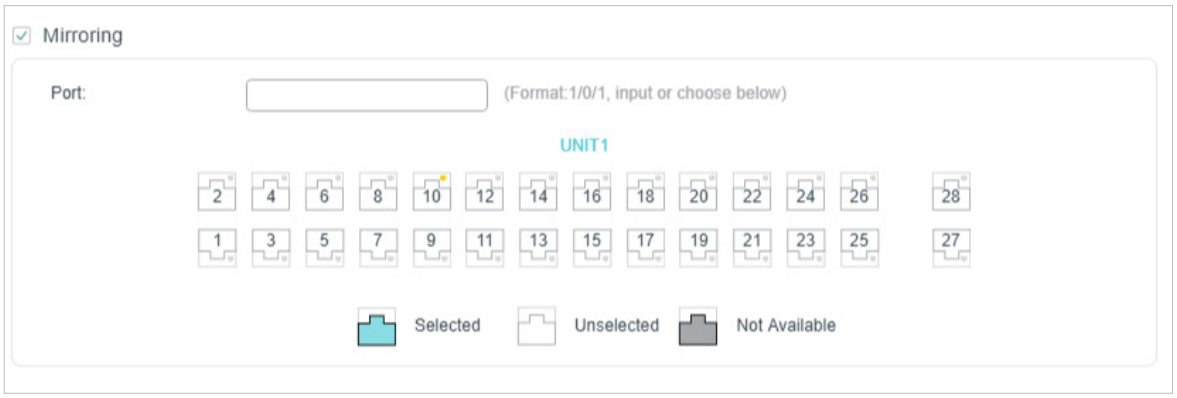
Rule ID	Wpisz numer ID, aby umożliwić identyfikację reguły. Numer nie powinien być taki sam, jak numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.
Operation	Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły. **Permit**: Jeżeli dopasowane pakiety mają być przekazywane. **Deny**: Jeżeli dopasowane pakiety mają być odrzucane.

Fragment	W przypadku wybrania tej opcji, reguła zostanie zastosowana do pakietów całego fragmentu z wyjątkiem ostatniego pakietu fragmentu w grupie pakietów fragmentu.
S-IP/Mask	Wprowadź źródłowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
D-IP/Mask	Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
IP Protocol	Wybierz z rozwijanej listy typ protokołu. Ustawienie domyślne to No Limit, co oznacza, że dopasowywane będą pakiety wszystkich protokołów. Można również wybrać opcję User-defined, aby odpowiednio dostosować protokół IP.
TCP Flag	W przypadku wybrania protokołu TCP dostępna jest opcja konfiguracji TCP Flag, funkcji służącej do działań dopasowywania reguły. Dostępnych jest sześć flag, z czego każda posiada trzy opcje: *, 0 i 1. Domyślnie ustawiona jest opcja *, wskazująca na to, że flaga nie jest wykorzystywana do działań dopasowywania. **URG (urgent)**: Flaga oznaczania jako pilne. **ACK (acknowledge)**: Flaga potwierdzania. **PSH (push)**: Flaga wymuszania przesyłu. **RST (reset)**: Flaga resetu. **SYN (synchronize)**: Flaga synchronizacji. **FIN (finish)**: Flaga zakańczania.
S-Port / D-Port	Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego z maską. **Wartość**: Wyznacz numer portu**.** **Maska**: Wyznacz maskę portu, używając 4 cyfr szesnastkowych.
DSCP	Określ wartość DSCP do dopasowania, między 0 a 63. Ustawienie domyślne to No Limit.
IP ToS	Określ wartość ToS adresu IP do dopasowania, między 0 a 15. Ustawienie domyślne to No Limit.
IP Pre	Określ wartość IP Precedencedo dopasowania, między 0 a 7. Ustawienie domyślne to No Limit.
Time Range	Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie **SYSTEM > Time Range**.

Logging	Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table.

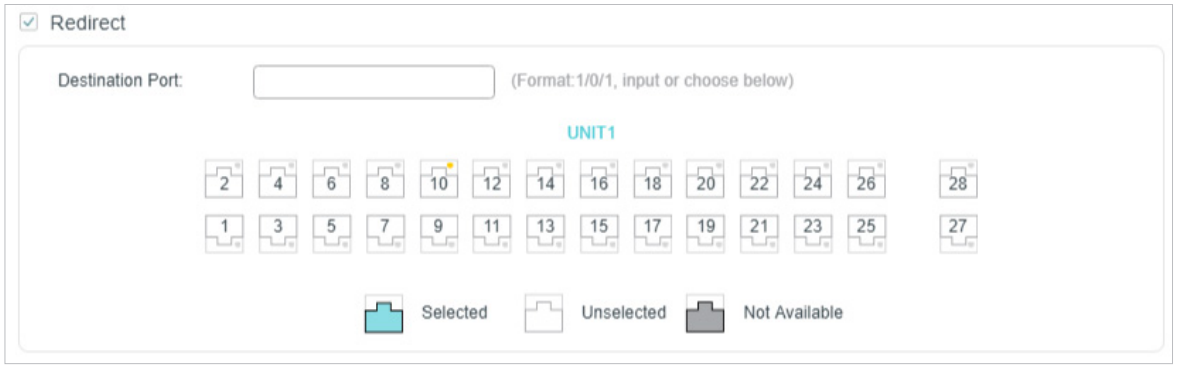
2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja ta jest włączona, należy wybrać port docelowy, na którym kopiowane będą pakiety.

Rys. 1-11 Konfiguracja funkcji Mirroring



3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego przekierowywane będą pakiety.

Rys. 1-12 Konfiguracja funkcji Redirect

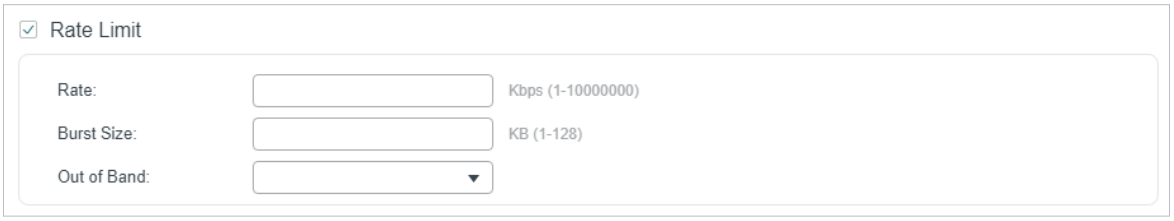


Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. W przypadku włączenia funkcji, należy skonfigurować następujące parametry.

Rys. 1-13 Konfiguracja funkcji Rate Limit



Rate	Wyznacz prędkość transmisji dopasowanych pakietów.
Burst Size	Określ maks. dopuszczalną liczbę bitów na sekundę.
Out of Band	Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem. **None:** Pakiety będą przekazywane normalnie. **Drop:** Pakiety będą odrzucane.

5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 1-14 Konfiguracja funkcji QoS Remark

DSCP	Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.
Local Priority	Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.
802.1p Priority	Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.

6) Kliknij **Apply**.

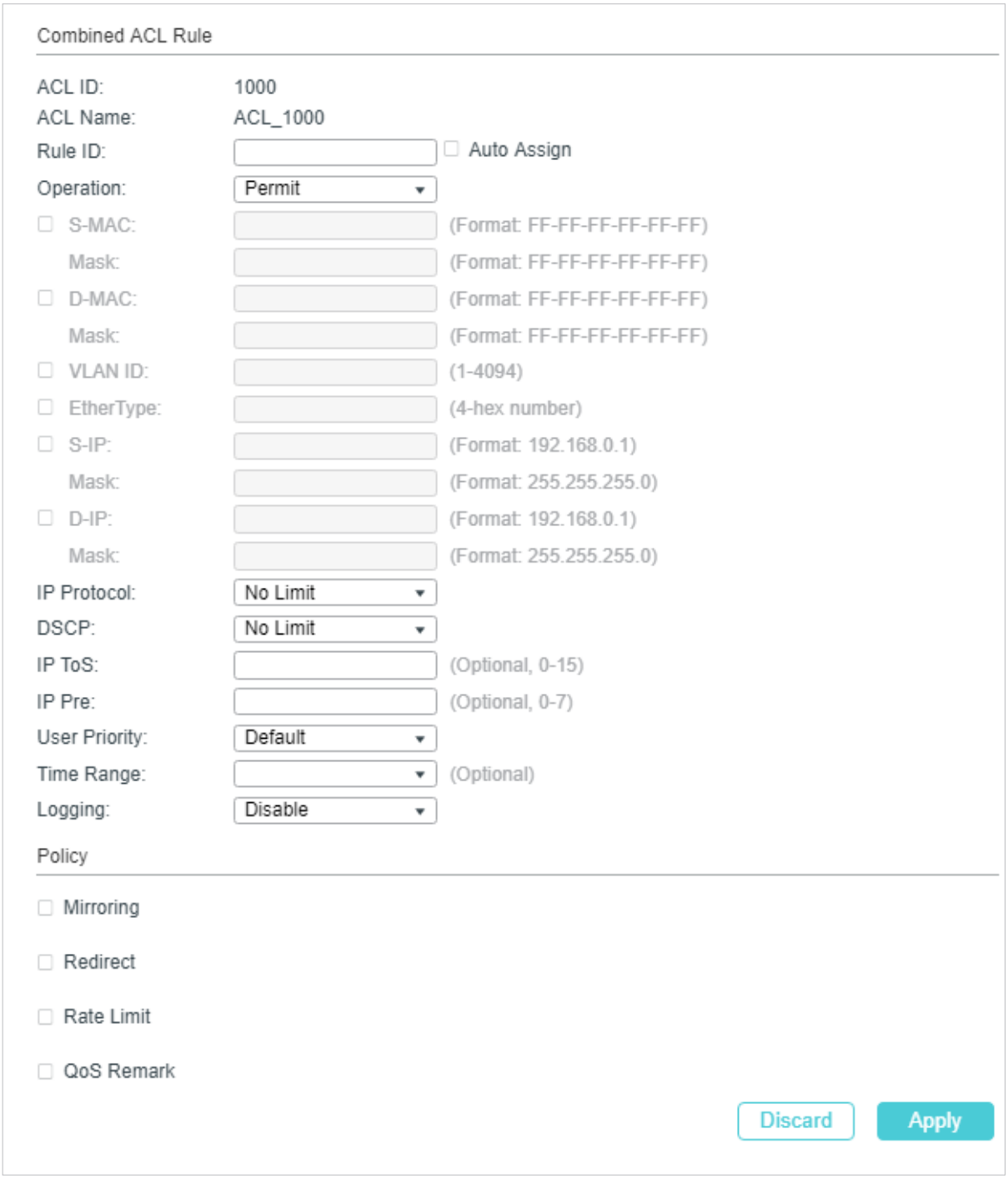
• Konfiguracja łączonej reguły ACL

Kliknij **Edit ACL** dla wpisu Combined ACL, aby załadować następującą stronę.

Rys. 1-15 Konfiguracja łączonej reguły ACL

W sekcji **ACL Rules Table** kliknij Add, a pojawi się następujące okno.

Rys. 1-16 Konfiguracja łączonej reguły ACL



Aby skonfigurować łączoną regułę ACL, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Combined ACL Rule** skonfiguruj następujące parametry:

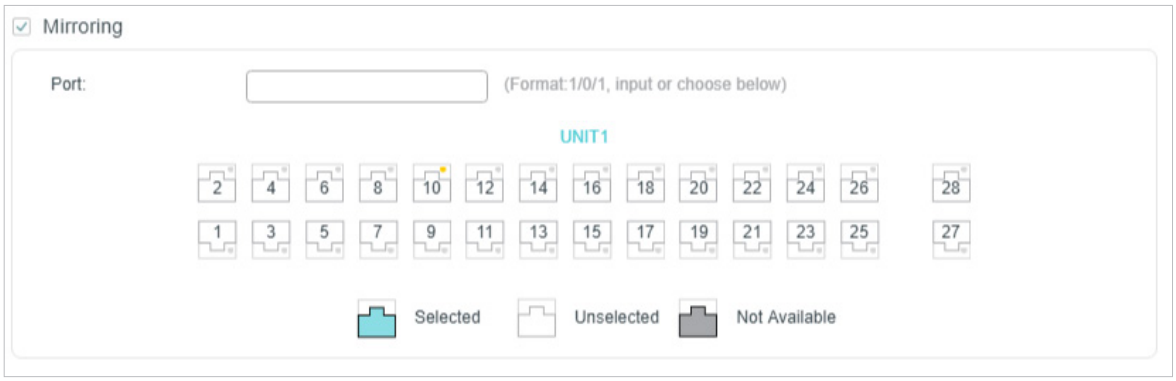
Rule ID	Wpisz numer ID, aby umożliwić identyfikację reguły. Numer nie powinien być taki sam, jak jakikolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.

Operation	Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły. **Permit:** Jeżeli dopasowane pakiety mają być przekazywane. **Deny**: Jeżeli dopasowane pakiety mają być odrzucane.
S-MAC/Mask	Wprowadź źródłowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
D-MAC/Mask	Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
VLAN ID	Wprowadź numer ID sieci VLAN, do której zastosowanie będzie miała ACL.
EtherType	Określ EtherType, który będzie dopasowany, używając 4 liczb szesnastkowych.
S-IP/Mask	Wprowadź źródłowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
D-IP/Mask	Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
IP Protocol	Wybierz z rozwijanej listy typ protokołu. Ustawienie domyślne to No Limit, co oznacza, że dopasowywane będą pakiety wszystkich protokołów. Można również wybrać opcję User-defined, aby odpowiednio dostosować protokół IP.
TCP Flag	W przypadku wybrania protokołu TCP dostępna jest opcja konfiguracji TCP Flag, funkcji służącej do działań dopasowywania reguły. Dostępnych jest sześć flag, z czego każda posiada trzy opcje: *, 0 i 1. Domyślnie ustawiona jest opcja *, wskazująca na to, że flaga nie jest wykorzystywana do działań dopasowywania. **URG (urgent)**: Flaga oznaczania jako pilne. **ACK (acknowledge)**: Flaga potwierdzania. **PSH (push)**: Flaga wymuszania przesyłu. **RST (reset)**: Flaga resetu. **SYN (synchronize)**: Flaga synchronizacji. **FIN (finish)**: Flaga zakańczania.
S-Port / D-Port	Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego z maską. **Wartość:** Wyznacz numer portu**.** **Maska**: Wyznacz maskę portu, używając 4 cyfr szesnastkowych.
DSCP	Określ wartość DSCP do dopasowania, między 0 a 63. Ustawienie domyślne to No Limit.
IP ToS	Określ wartość ToS adresu IP do dopasowania, między 0 a 15. Ustawienie domyślne to No Limit.
IP Pre	Określ wartość IP Precedence dopasowania, między 0 a 7. Ustawienie domyślne to No Limit.

User Priority	Wyznacz User Priority do dopasowania.
Time Range	Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie **SYSTEM > Time Range**.
Logging	Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table.

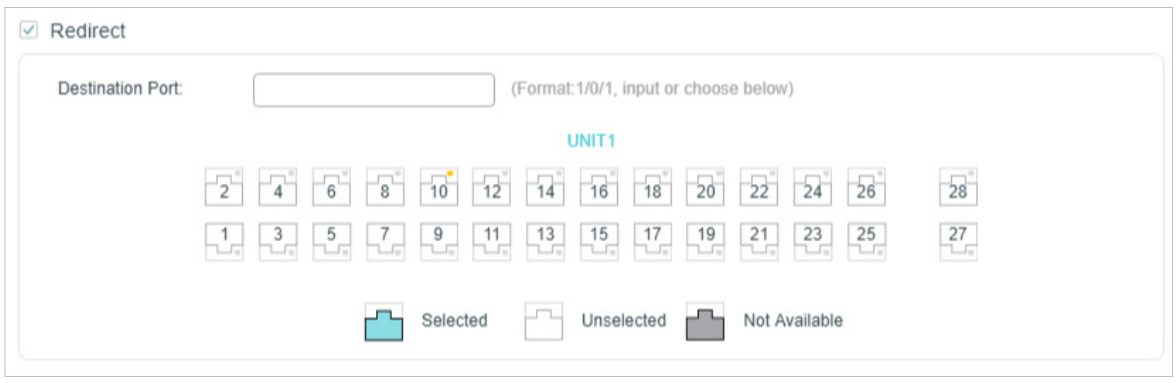
2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego pakiety będą kopiowane.

Rys. 1-17 Konfiguracja funkcji Mirroring



3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, na który przekierowywane będą pakiety.

Rys.1-18 Konfiguracja funkcji Redirect

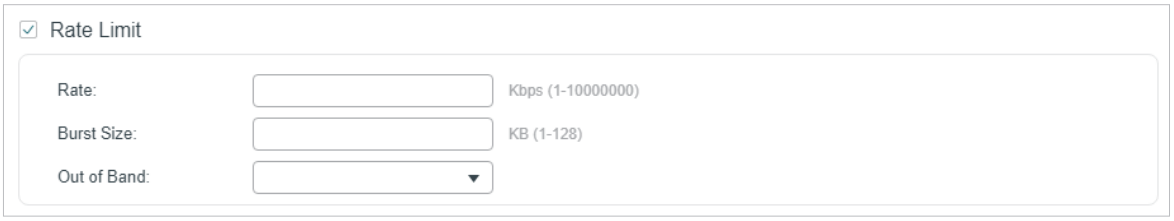


Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry.

Rys. 1-19 Konfiguracja funkcji Rate Limit



Rate	Wyznacz prędkość transmisji dopasowanych pakietów.
Burst Size	Określ maks. dopuszczalną liczbę bitów na sekundę.
Out of Band	Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem. **None:** Pakiety będą przekazywane normalnie. **Drop:** Pakiety będą odrzucane.

5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 1-20 Konfiguracja funkcji QoS Remark

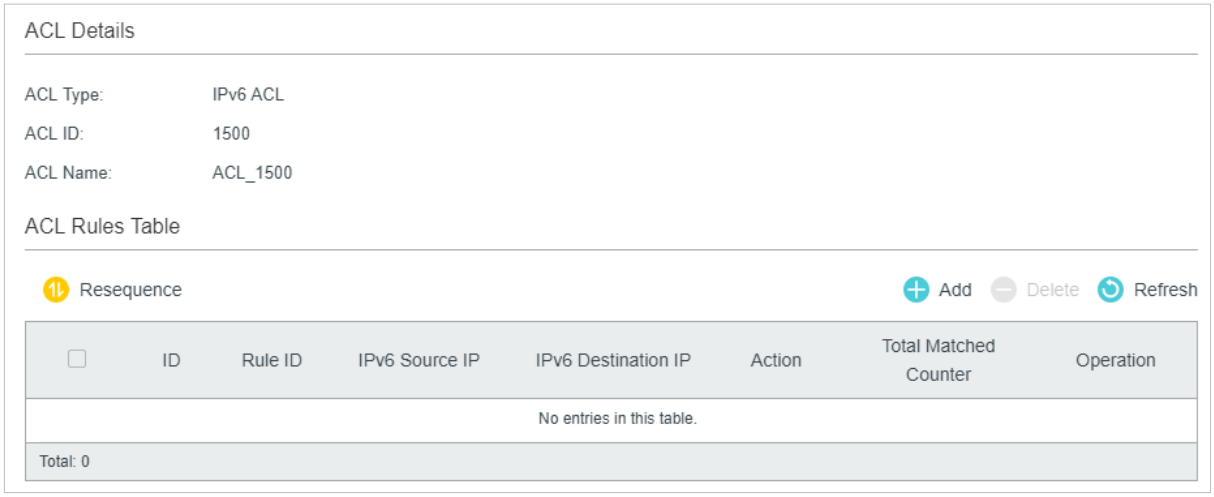
DSCP	Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.
Local Priority	Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.
802.1p Priority	Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.

6) Kliknij **Apply**.

• Konfiguracja reguły IPv6 ACL

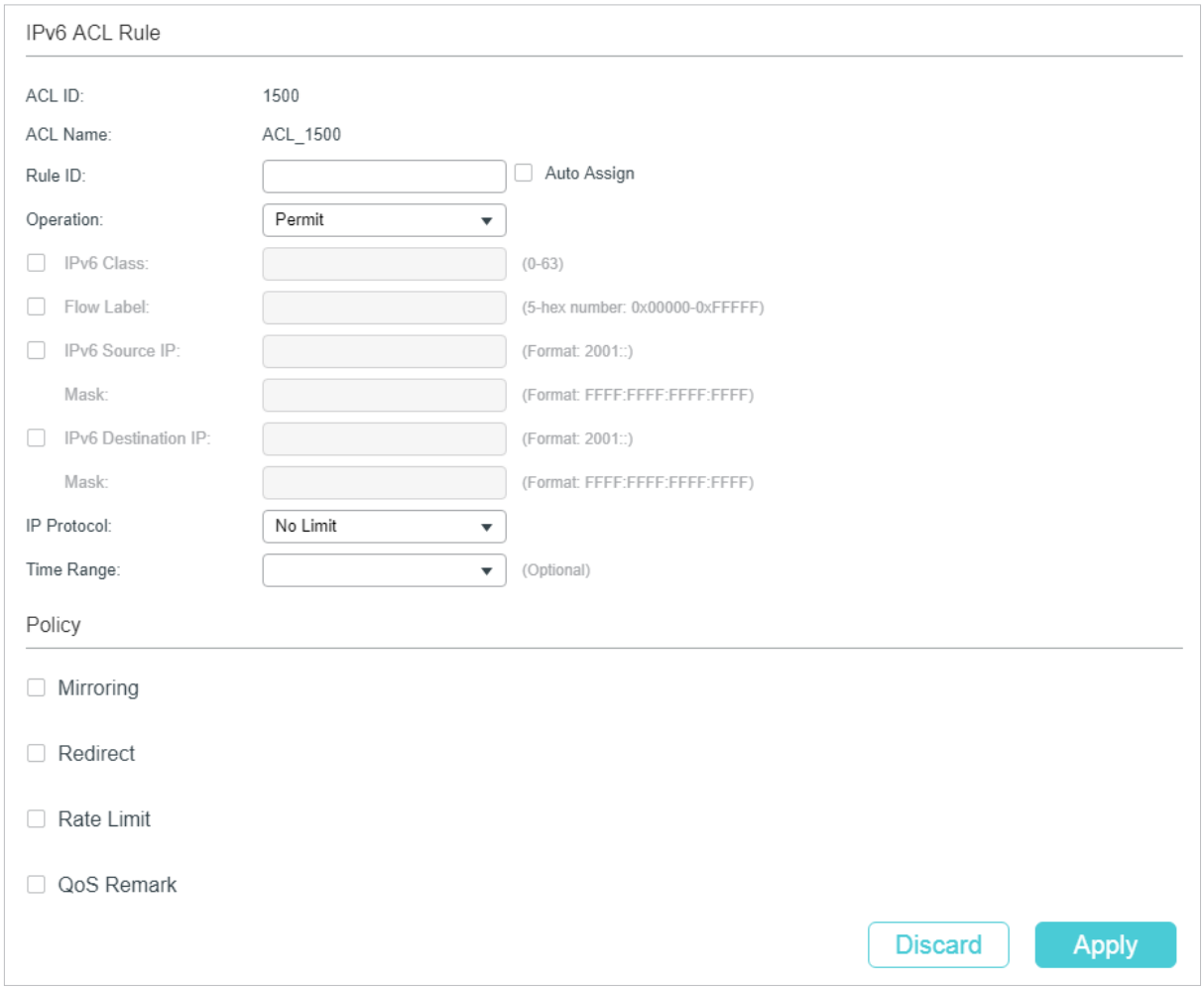
Kliknij **Edit ACL** dla wpisu IPv6 ACL, aby załadować następującą stronę.

Rys. 1-21 Konfiguracja reguły IPv6 ACL



W sekcji **ACL Rules Table** kliknij Add , a pojawi się następujące okno.

Rys. 1-22 Konfiguracja reguły IPv6 ACL



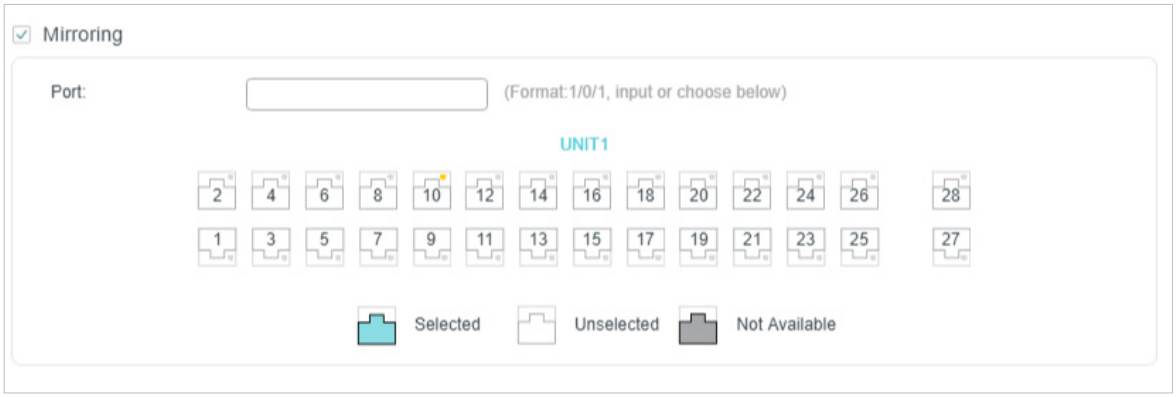
Aby skonfigurować regułę IPv6 ACL, postępuj zgodnie z poniższymi krokami:

1) IW sekcji **IPv6 ACL Rule** skonfiguruj następujące parametry.

Rule ID	Wpisz numer ID, aby umożliwić identyfikację reguły. Numer nie powinien być taki sam, jak jakikolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.
Operation	Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły. **Permit**: Jeżeli dopasowane pakiety mają być przekazywane. **Deny**: Jeżeli dopasowane pakiety mają być odrzucane.
IPv6 Class	Wyznacz wartość klasy IPv6 do dopasowania. Przełącznik sprawdzi pole klasy nagłówka IPv6.
Flow Label	Wyznacz wartość Flow Label do dopasowania.
IPv6 Source IP	Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.
Mask	Maska jest wymagana, jeżeli podany jest źródłowy adres IPv6. Wpisz maskę w pełnym formacie (np. FFFF:FFFF:0000:FFFF). Maska adresu IP wyznacza, które bity w źródłowym adresie IPv6 mają być dopasowane do reguły. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
IPv6 Destination IP	Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.
Mask	Maska jest wymagana, jeżeli podany jest docelowy adres IPv6. Wpisz maskę w pełnym formacie (np. FFFF:FFFF:0000:FFFF). Maska adresu IP wyznacza, które bity w źródłowym adresie IP mają być dopasowane do reguły. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.
IP Protocol	Wybierz z rozwijanej listy typ protokołu. **No Limit:** Dopasowane będą pakiety wszystkich protokołów. **UDP:** Wyznacz port źródłowy i docelowy do dopasowania pakietu UDP. **TCP**: Wyznacz port źródłowy i docelowy do dopasowania pakietu TCP. **User-defined**: Możesz dowolnie dostosować protokół IP.
S-Port / D-Port	Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego.
Time Range	Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie **SYSTEM > Time Range**.

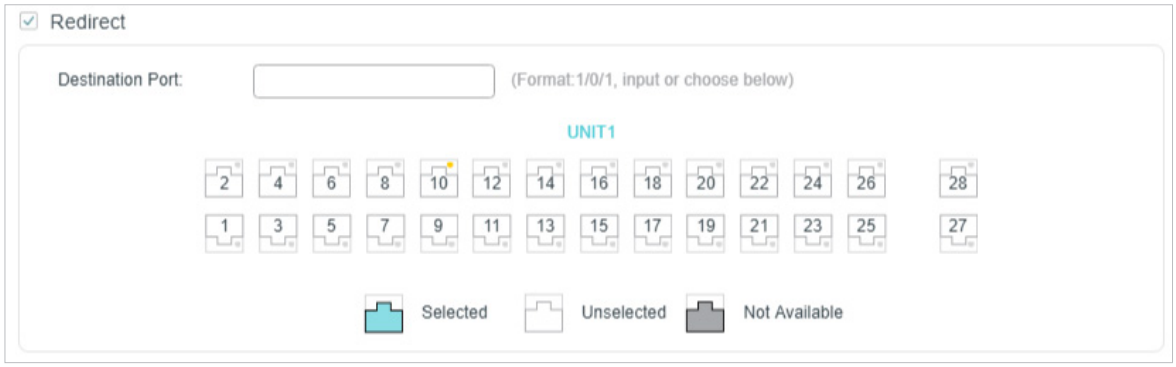
2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, wybierz port docelowy, na który kopiowane będą pakiety.

Rys. 1-23 Konfiguracja funkcji Mirroring



3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego pakiety będą przekierowywane.

Rys. 1-24 Konfiguracja funkcji Redirect

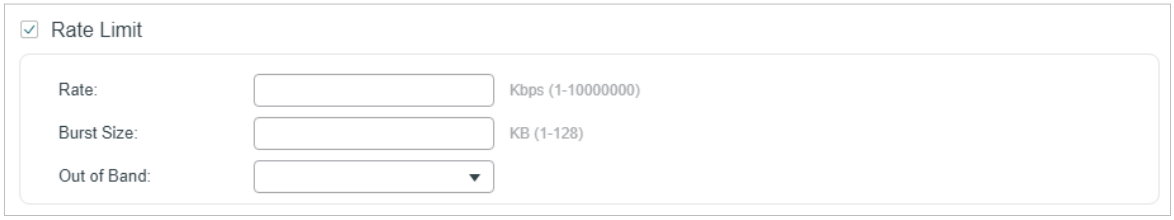


Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy skonfigurować powiązane parametry.

Rys. 1-25 Konfiguracja funkcji Rate Limit

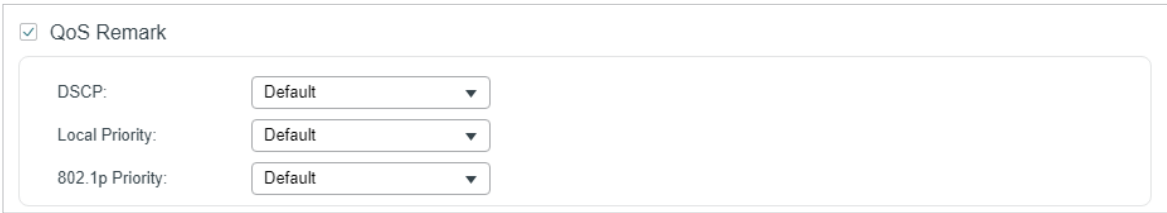


Rate	Wyznacz prędkość transmisji dopasowanych pakietów.
Burst Size	Określ maks. dopuszczalną liczbę bitów na sekundę.

Out of Band	Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem. **None:** Pakiety będą przekazywane normalnie. **Drop:** Pakiety będą odrzucane.

5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 1-26 Konfiguracja funkcji QoS Remark



DSCP	Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.
Local Priority	Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.
802.1p Priority	Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.

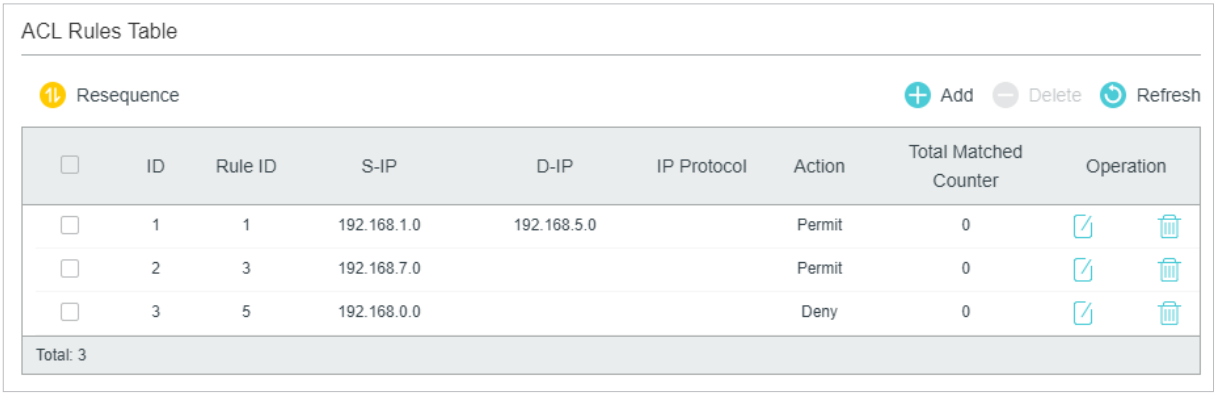
6) Kliknij **Apply**.

Wyświetlanie reguł ACL

Reguły ACL wymienione są w kolejności rosnącej ID reguły. Przełącznik dopasowuje otrzymany pakiet do reguł według ich kolejności. Jeżeli pakiet jest dopasowany do reguły, przełącznik przerywa proces dopasowywania i wykonuje działanie wyznaczone przez regułę.

Kliknij **Edit ACL** przy utworzonym przez ciebie wpisie, a wyświetli się tablica reguł**.** Jako przykład pokazana jest tablica reguł IP ACL.

Rys. 1-27 Podgląd tablicy reguł ACL Rules



Tutaj możesz wyświetlać i edytować reguły ACL. Możesz również kliknąć **Resequence**, aby zmienić kolejność reguł, podając ID pierwszej reguły (Start Rule ID) i wartość krokową.

1.1.4 Konfiguracja wiązania ACL

Możesz powiązać ACL z potrem lub siecią VLAN. Pakiety odebrane na porcie lub w sieci VLAN będą dopasowane i przetworzone zgodnie z regułami ACL. ACL zacznie działać dopiero po powiązaniu jej z portem lub siecią VLAN.

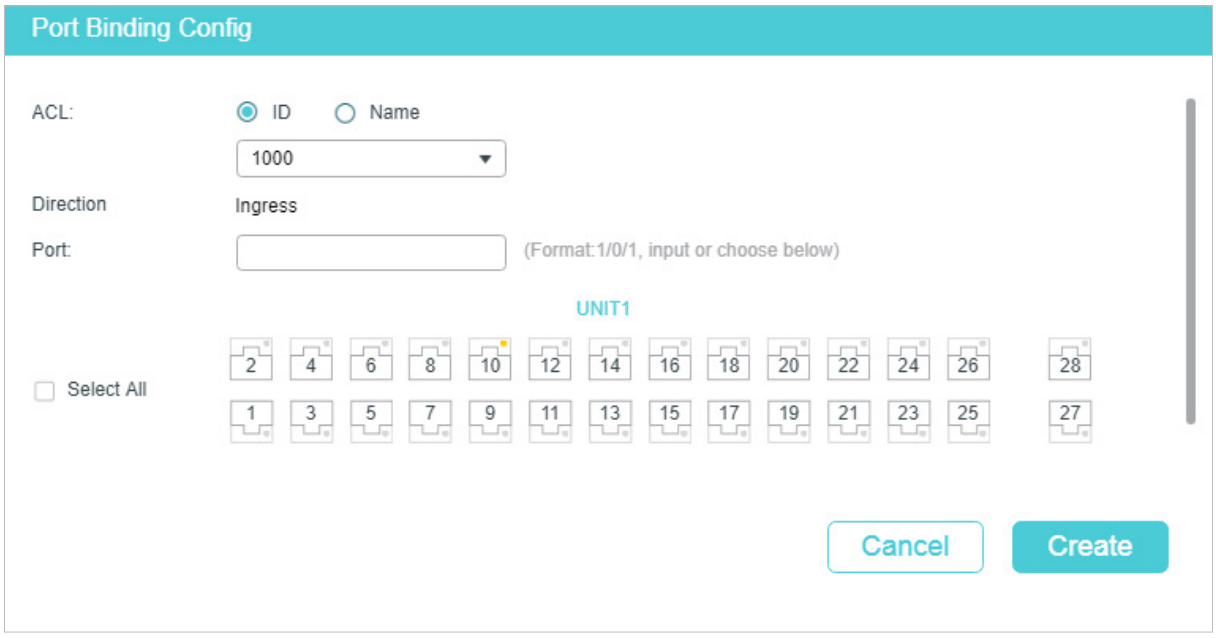
Uwaga:

- Różne typy ACL nie mogą być powiązane z tym samym portem lub siecią VLAN.
- Liczne ACL tego samego typu mogą być powiązane z tym samym portem lub siecią VLAN. Przełącznik dopasowuje odebrane pakiety wykorzystując listy ACL, zgodnie z kolejnością. Im wcześniej ACL została powiązana, tym większy ma priorytet.

■ Wiązanie ACL z portem

Wybierz menu **SECURITY > ACL > ACL Binding > Port Binding** i kliknij Add , aby załadować następującą stronę.

Rys. 1-28 Wiązanie ACL z portem



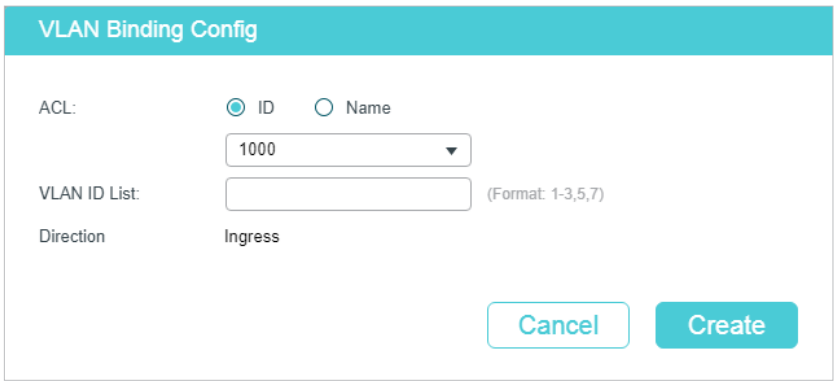
Aby powiązać ACL z portem, postępuj zgodnie z poniższymi krokami.

1) Wybierz ID lub Nazwę, wykorzystywane do dopasowywania ACL. Następnie wybierz ACL z rozwijanej listy.
2) Wyznacz port do wiązania.
3) Kliknij **Create**.

- Wiązanie ACL z VLAN

Wybierz menu **SECURITY > ACL > ACL Binding > VLAN Binding**, aby załadować następującą stronę.

Rys. 1-29 Wiązanie ACL z VLAN



Aby powiązać ACL z VLAN, postępuj zgodnie z poniższymi krokami:

1) Wybierz ID lub Nazwę, wykorzystywane do dopasowywania ACL. Następnie wybierz ACL z rozwijanej listy.
2) Wprowadź ID sieci VLAN do wiązania.
3) Kliknij **Create**.

1.2 Przez CLI

1.2.1 Konfiguracja zakresu czasu

Niektóre usługi lub funkcje bazujące na ACL mogą wymagać ograniczenia ich działania do wyznaczonego zakresu czasu. W tym przypadku możesz skonfigurować zakres czasu ACL. Więcej szczegółów dotyczących konfiguracji zakresu czasu znajdziesz w rozdziale *Zarządzanie systemem*.

1.2.2 Konfiguracja ACL

Aby utworzyć ACL różnego typu i skonfigurować reguły ACL, postępuj zgodnie z poniższymi krokami.

Możesz zdefiniować reguły w oparciu o źródłowy adres MAC lub IP, docelowy adres MAC lub IP, typ protokołu, numer portu itd.

- **MAC ACL**

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2	**access-list create** *acl-id* **[name** *acl-name***]** Utwórz MAC ACL. *acl-id*: Wprowadź ACL ID. ID mieści się w zakresie od 0 do 499. *acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.
Krok 3	**access-list mac** *acl-id-or-name* **rule** { auto | *rule-id* } { deny | permit } **logging** {enable | disable} [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**type** ether-type] [**pri** *dot1p-priority*] [**vid** *vlan-id*] [**tseg** *time-range-name*] Dodaj regułę MAC ACL. *acl-id-or-name*: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę. *auto:* ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund. *rule-id*: Przypisz ID do reguły. deny | permit: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadky wybrania funkcji Permit pakiety będą przekazywane. **logging** {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap). *source-mac*: Wprowadź źródłowy adres MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF. *source-mac-mask*: Wprowadź maskę źródłowego adresu MAC. Jest to konieczne w przypadku wprowadzenia źródłowego adresu MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF. *destination-mac*: Wprowadź docelowy adres MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF. *destination-mac-mask*: Wprowadź maskę docelowego adresu MAC. Jest to konieczne w przypadku wprowadzenia docelowego adresu MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF. ether-type: Wyznacz typ Ethernet, używając 4 cyfr szesnastkowych. *dot1p-priority*: Priorytet użytkownika wynosi od 0 do 7. Ustawienie domyślne to No Limit. *vlan-id*: VLAN ID wynosi od 1 do 4094. *time-range-name*: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.
Krok 4	**exit** Wróć do trybu konfiguracji globalnej.
Krok 5	**show access-list** [*acl-id-or-name*] Wyświetl aktualną konfigurację ACL. *acl-id-or-name*: Numer ID i nazwa ACL.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).

Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie MAC ACL 50 i konfigurację reguły 5 (Rule 5) do przesyłania pakietów (permit) o źródłowym adresie MAC 00:34:A2:D4:34:B5:

Switch#configure

Switch(config)#access-list create 50

Switch(config-mac-acl)#access-list mac 50 **rule** 5 **permit logging** disable **smac** 00:34:A2:D4:34:B5 **smask** FF:FF:FF:FF:FF:FF

Switch(config-mac-acl)#exit

Switch(config)#show access-list 50

MAC access list 50 name: ACL_50

rule 5 permit logging disable smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

■ IP ACL

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**access-list create** *acl-id* **[name** *acl-name***]** Utwórz IP ACL. *acl-id*: Wprowadź ACL ID. ID wynosi od 500 do 999. *acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.

Krok 3 **access-list ip** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**frag** {enable | disable}] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]

Dodaj reguły do ACL.

acl-id-or-name: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.

auto: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

rule-id: Przypisz ID do reguły.

deny | permit: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadky wybrania funkcji Permit pakiety będą przekazywane.

logging {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

sip-address: Wprowadź źródłowy adres IP.

sip-address-mask: Wprowadź maskę źródłowego adresu IP. Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

dip-address: Wprowadź docelowy adres IP.

dip-address-mask: Wprowadź maskę docelowego adresu IP. Jest to konieczne w przypadku wprowadzenia docelowego adresu IP.

dscp-value: Wysnacz wartość DSCP, między 0 a 63.

tos-value: Wyznacz wartość ToS adresu IP do dopasowania, między 0 a 15.

pre-value: Wyznacz wartość IP Precedence do dopasowania, między 0 a 7.

frag {enable | disable}*:* Włącz lub wyłącz dopasowywanie pakietów podzielonych na fragmenty. Funkcja jest domyślnie wyłączona. Jeżeli funkcja jest włączona, reguła będzie miała zastosowanie do wszystkich pakietów podzielonych na fragmenty i zawsze dopuści przekazywanie ostatniego fragmetu pakietu.

protocol: Wyznacz numer protokołu, między 0 a 255.

s-port-number: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu źródłowego.

s-port-mask: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu źródłowego, używając 4 cyfr szesnastkowych.

d-port-number: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu docelowego.

d-port-mask: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu docelowego, używając 4 cyfr szesnastkowych.

tcpflag: W przypadku ustawienia na protokół TCP należy wyznaczyć wartość flagi, używając liczb binarnych lub * (np. 01*010*). Ustawnienie domyślne to *, oznaczające, że flaga nie zostanie dopasowana.

Dostępne flagi to URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) and FIN (Finish Flag).

time-range-name: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.

Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie IP ACL 600, konfigurację Rule 1 na przesyłanie (permit) pakietów o źródłowym adresie IP 192.168.1.100:

Switch#configure

Switch(config)#access-list create 600

Switch(config)#access-list ip 600 **rule** 1 **permit logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 600

IP access list 600 name: ACL_600

rule 1 permit logging disable sip 192.168.1.100 smask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

Łączona ACL

Krok 1 **configure**

Wejdź w tryb konfiguracji globalnej.

Krok 2 **access-list create** *acl-id* **[name** *acl-name***]**

Utwórz Combined ACL (łączoną ACL).

acl-id: Wprowadź ACL ID. ID wynosi od 1000 do 1499.

acl-name: Wprowadź nazwę, aby umożliwić identyfikację ACL.

Krok 3 **access-list combined** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**smac** *source-mac-address* **smask** *source-mac-mask*] [**dmac** *dest-mac-address* **dmask** *dest-mac-mask*] [**vid** *vlan-id*] [**type** *ether-type*] [**pri** *priority*] [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]

Dodaj reguły do ACL.

acl-id-or-name: Wprowadź ID lub nazwę ACL, go której chcesz dodać regułę.

auto: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

rule-id: Przypisz ID do reguły.

deny | permit: kreśl, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadky wybrania funkcji Permit pakiety będą przekazywane.

logging {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

source-mac-address: Wprowadź źródłowy adres MAC.

source-mac-mask: Wprowadź maskę źródłowego adresu MAC.

dest-mac-address: Wprowadź docelowy adres MAC

dest-mac-mask: Wprowadź maskę docelowego adresu MAC. Jest to konieczne w przypadku wprowadzenia docelowego adresu MAC.

vlan-id: VLAN ID wynosi od 1do 4094.

ether-type: Wyznacz typ Ethernet, używając 4 cyfr szesnastkowych.

priority: Priorytet użytkownika wynosi od 0 do 7. Ustawienie domyślne to No Limit.

sip-address:Wprowadź źródłowy adres IP.

sip-address-mask: Wprowadź maskę źródłowego adresu IP. Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

dip-address: Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

dip-address-mask: Wprowadź maskę docelowego adresu IP. Jest to konieczne w przypadku wprowadzenia docelowego adresu IP.

dscp-value: Wyznacz wartość DSCP między 0 a 63.

tos-value: Wyznacz wartość ToS adresu IP do dopasowania, miedzy 0 a 15.

	protocol: Wyznacz numer protokołu, między 0 an255. *s-port-number:* W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu źródłowego. *s-port-mask:* W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu źródłowego, używając 4 cyfr szesnastkowych. *d-port-number:* W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu docelowego. *d-port-mask:* W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu docelowego, używając 4 cyfr szesnastkowych. *tcpflag:* W przypadku ustawienia na protokół TCP należy wyznaczyć wartość flagi, używając liczb binarnych lub * (np. 01*010*). Ustawnienie domyślne to *, oznaczające, że flaga nie zostanie dopasowana. Dostępne flagi to URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) i FIN (Finish Flag). *time-range-name*: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie Combined ACL 1100 i konfigurację Rule 1 (reguły 1) odrzucania pakietów o źródłowym adresie IP 192.168.3.100 in VLAN 2:

Switch#configure

Switch(config)#access-list create 1100

Switch(config)#access-list combined 1100 **logging** disable **rule** 1 **permit vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 2600

Combined access list 2600 name: ACL_2600

rule 1 permit logging disable vid 2 sip 192.168.3.100 sip-mask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

■ IPv6 ACL

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2 **access-list create** *acl-id* **[name** *acl-name***]**

Utwórz IPv6 dla ACL.

acl-id: Wprowadź ID listy ACL. ID mieści się w zakresie od 1500 do 1999.

acl-name: Wprowadź nazwę, aby umożliwić identyfikację ACL.

Krok 3 **access-list ipv6** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*]

Dodaj reguły do ACL.

acl-id-or-name: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.

auto: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

rule-id: Przypisz ID do reguły.

deny | permit: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadky wybrania funkcji Permit pakiety będą przekazywane.

logging {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

class-value: Wyznacz wartość klasy do dopasowania, w zakresie od 0 do 63.

flow-label-value: Wyznacz wartość Flow Label do dopasowania

source-ip-address: Wpisz źródłowy adres IP. Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.

source-ip-mask: Wprowadź maskę źródłowego adresu IP. Maska jest wymagana, jeżeli podany został źródłowy adres IPv6. Wprowadź maskę w pełnym formacie (np. ffff:ffff:0000:ffff). Maska wyznacza, które bity w źródłowym adresie IPv6 będą dopasowywane do reguły.

destination-ip-address: Wpisz docelowy adres IP. Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.

destination-ip-mask: Wprowadź maskę docelowego adresu IP. Maska jest wymagana, jeżeli podany został źródłowy adres IPv6. Wprowadź maskę w pełnym formacie (np. ffff:ffff:0000:ffff). Maska wyznacza, które bity w źródłowym adresie IPv6 będą dopasowywane do reguły.

source-port-number: Wprowadź port źródłowy TCP/UDP, jeżeli wybrany został protokół TCP/UDP.

destination-port-number: Wprowadź port docelowy TCP/UDP, jeżeli wybrany został protokół TCP/UDP.

Krok 4 **end**

Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).

Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie IPv6 listy ACL 1600 i konfigurację Rule 1 do odrzucania pakietów o adresie źródłowym IPv6 CDCD:910A:2222:5498:8475:1111:3900:2020:

Switch#configure

Switch(config)#access-list create 1600

Switch(config)#access-list ipv6 1600 **rule** 1 **deny logging** disable **sip** CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

Switch(config)#show access-list 1600

IPv6 access list 1600 name: ACL_1600

rule 1 deny logging disable sip cdcd:910a:2222:5498:8475:1111:3900:2020 sip-mask ffff:ff

ff:ffff:ffff

Switch(config)#end

Switch#copy running-config startup-config

Zmiana kolejności reguł

Możesz zmienić kolejność reguł, podając ID pierwszej reguły (Start Rule ID) i wartość krokową.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**access-list resequence** *acl-id-or-name* **start** *start-rule-id* **Krok** *rule-id-Krok-value* Zmień kolejność reguł na wybranej ACL. *acl-id-or-name*: Wpisz ID lub nazwę ACL. *start-rule-id*:Wpisz pierwszy ID reguły. *rule-id-Krok-value*: Wprowadź wartość krokową.
Krok 3	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje zmianę kolejności reguł ACL MAC 100: ustawianie pierwszego ID reguły na 1 i ustawianie wartości krokowej na 10:

Switch#configure

Switch(config)#access-list resequence 100 **start** 1 **Krok** 10

rule 11 permit logging disable vid 18

rule 21 permit logging disable dmac aa:cc:ee:ff:dd:33 dmask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Strategie konfiguracji

Strategie konfiguracji umożliwiają dalsze przetwarzanie dopasowanych pakietów poprzez takie działania jak mirroring, ograniczanie prędkości, przekierowywanie lub zmiana priorytetu.

Postępuj zgodnie z poniższymi krokami, aby skonfigurować strategie dla reguły ACL: .

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**access-list action** *acl-id-or-name* **rule** *rule-id* Skonfiguruj strategie dla reguły ACL. *acl-id-or-name*: Wprowadź ID lub nazwę ACL. *rule-id*: Wprowadź ID reguły ACL.

Krok 3	**redirect interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Opcjonalnie) Ustaw strategię na przekierowywanie dopasowanych pakietów do wybranego portu. *port*: Port docelowy, do którego przekierowywane będą pakiety. Ustawienie domyślne to All (wszystkie). **s-mirror interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Opcjonalnie) Ustaw strategię na kopiowanie (mirroring) dopasowanych pakietów na wybranym porcie. *port*: Port docelowy, na którym kopiowane będą pakiety. **s-condition rate** *rate* **burst** *burst-size* **osd** { **none | discard** } (Opcjonalnie) Ustaw strategię na monitorowanie prędkości dopasowanych pakietów. *rate*: Ustaw prędkość między 1 a 1000000 kb/s. *burst-size*: Określ maks. dopuszczalną liczbę bajtów na sekundę, od 1 do 128. **osd**: Wpisz „none" (brak) lub „discard" (odrzucaj) jako działanie, które ma być podejmowane względem pakietów, których prędkość przekracza granicę wyznaczonego zakresu. Ustawienie domyślne to None. **qos-remark** [**dscp** *dscp*] [**priority** *pri*] [**dot1p** *pri*] (Opcjonalnie) Wyznacz strategię oznaczania priorytetu dopasowanych pakietów. *dscp*: Wyznacz region DSCP dla pakietów danych. Wartość wynosi od 0 do 63. **priority** *pri*: Wyznacz priorytet lokalny dla pakietów danych. Wartość wynosi od 0 do 7. **dot1p** *pri:* Wyznacz priorytet 802.1p dla pakietów danych. Wartość wynosi od 0 do 7.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Przekierowywanie dopasowanych pakietów do portu 1/0/4 w regule 1 ACL MAC 10:

Switch#configure

Switch(config)#access-list action 10 rule 1

Switch(config-action)#redirect interface gigabitEthernet 1/0/4

Switch(config-action)#exit

Switch(config)#show access-list 10

MAC access list 10 name: ACL_10

rule 5 permit logging disable action redirect Gi1/0/4

Switch(config)#end

Switch#copy running-config startup-config

1.2.4 Konfiguracja wiązania ACL

Możesz powiązać ACLz portem lub siecią VLAN. Pakiety odebrane na porcie lub w sieci VLAN będą dopasowane i przetworzone zgodnie z regułami ACL. ACL zacznie działać dopiero po powiązaniu jej z portem lub siecią VLAN.

Uwaga:

- Różne typy ACL nie mogą być powiązane z tym samym portem lub siecią VLAN.
- Liczne ACL tego samego typu mogą być powiązane z tym samym portem lub siecią VLAN. Przełącznik dopasowuje odebrane pakiety wykorzystując listy ACL, zgodnie z kolejnością. Im wcześniej ACL została powiązana, tym większy ma priorytet.

Aby powiązać ACL z portem lub VLAN, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**access-list bind** *acl-id-or-name* **interface** { [**vlan** *vlan-list*] | [**fastEthernet** *port-list*] | [**gigabitEthernet** *port-list* | [**ten-gigabitEthernet** *port-list*] } Powiąż ACL z portem lub VLAN. *acl-id-or-name*: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę. *vlan-list*: Wyznacz ID lub listę ID sieci VLAN, którą(-e) chcesz powiązać z ACL. Wartość powinna wynosić między 1 a 4094, np. 2-3,5. *port-list*: Wyznacz numer lub listę portu Ethernet, który chcesz powiązać z ACL.
Krok 3	**show access-list bind** Sprawdź ustawienia wiązania ACL.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje wiązanie ACL 1 z portem 3 i VLAN 4:

Switch#configure

Switch(config)#show access-list bind

ACL ID	ACL NAME	Interface/VID	Direction	Type
-----	----------	------------	-------	----
1	ACL_1	Gi1/0/3	Ingress	Port
1	ACL_1	4	Ingress	VLAN

Switch(config)#end

Switch#copy running-config startup-config

1.2.5 Wyświetlanie liczby dopasowanych pakietów ACL

Za pomocą poniższego polecenia możesz wyświetlić liczbę dopasowanych pakietów każdej ACL, w trybie użytkownika uprzywilejowanego i w każdym innym trybie.

show access-list *acl-id-or-name* **counter**

Wyświetl liczbę dopasowanych pakietów wybranej ACL.

acl-id-or-name: Podaj ID lub nazwę ACL do wyświetlenia.

Część 20

Konfiguracja IMPB IPv4

ROZDZIAŁY

1 IMPB IPv4

1.1 Obsługiwane funkcje

Wiązanie IP-MAC

Funkcja ta służy do dodawania wpisów wiązania. Wpisy wiązania mogą być konfigurowane ręcznie lub wyuczane przez ARP scanning (skanowanie ARP) lub DHCP snooping. Funkcje ARP Detection i IPv4 Source Guard bazują na wpisach wiązania IP-MAC.

ARP Detection

W rozbudowanej sieci wdrażanie protokołu ARP wiąże się z dużym zagrożeniem dla bezpieczeństwa samej sieci. Sieć często narażona jest na ataki opierające się na fałszowaniu danych (ARP cheating), np. imitowanie bramy sieciowej, podawanie błędnej bramy sieciowej czy błędnego terminala hosta oraz na ataki ARP flooding, polegające na wypełnianiu pamięci przełącznika błędnymi informacjami. Funkcja ARP Detection może ochronić sieć przed atakami ARP.

- Zapobieganie atakom ARP Cheating

Bazując na wpisach wiązania adresów IP i MAC, funkcję ARP Detection można skonfigurować tak, by wykrywała pakiety ARP i filtrowała te nielegalne w celu ochrony sieci przed atakami fałszowania ARP (ARP cheating).

- Zapobieganie atakom ARP Flooding

Aby zapobiec atakom ARP Flooding możesz ograniczyć prędkość odbierania przez port legalnych pakietów ARP.

IPv4 Source Guard

Funkcja IPv4 Source Guard służy do filtrowania pakietów IPv4 w oparciu o tablicę wiązania IP-MAC. Przekazywane są jedynie pakiety zgodne z regułami wiązania.

2 Konfiguracja wiązania IP-MAC

Wpisy wiazania IP-MAC można dodawać trzema sposobami.

- Wiązanie ręczne
- Przez ARP Scanning
- Przez DHCP Snooping

Dodatkowo można wyświetlać, wyszukiwać i edytować wpisy na tablicy wiązania (Binding Table).

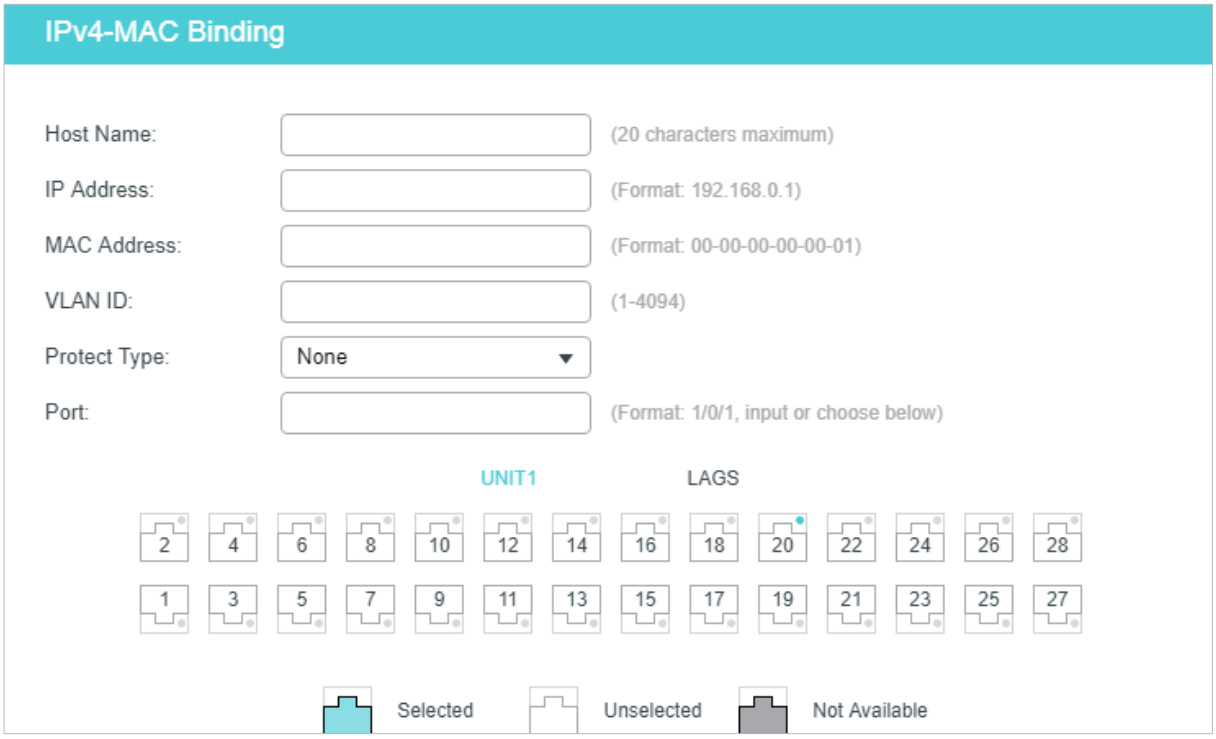
2.1 Przez GUI

2.1.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IP, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wybierz z menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** i kliknij Add , aby załadować następującą stronę.

Rys. 2-1 Wiązanie ręczne



Aby ręcznie utworzyć wpis wiązania IP-MAC, postępuj zgodnie z poniższymi krokami.

1) Wprowadź następujące informacje, aby określić hosta.

Host Name	Wprowadź nazwę, aby umożliwić identyfikację hosta.
IP Address	Wprowadź adres IP.
MAC Address	Wprowadź adres MAC.
VLAN ID	Wprowadź VLAN ID.

2) Wybierz typ ochrony wpisu.

Protect Type	Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje: **None**: Wpis nie będzie zastosowany do żadnej funkcji. **ARP Detection**: Wpis zostanie zastosowany do funkcji ARP Detection. **IP Source Guard**: Wpis zostanie zastosowany do funkcji IPv4 Source Guard. **Both**: Wpis zostanie zastosowany do obu funkcji.

3) Wpisz lub wybierz port podłączony do tego hosta.

4) Kliknij **Apply**.

2.1.2 Wiązanie wpisów przez ARP Scanning

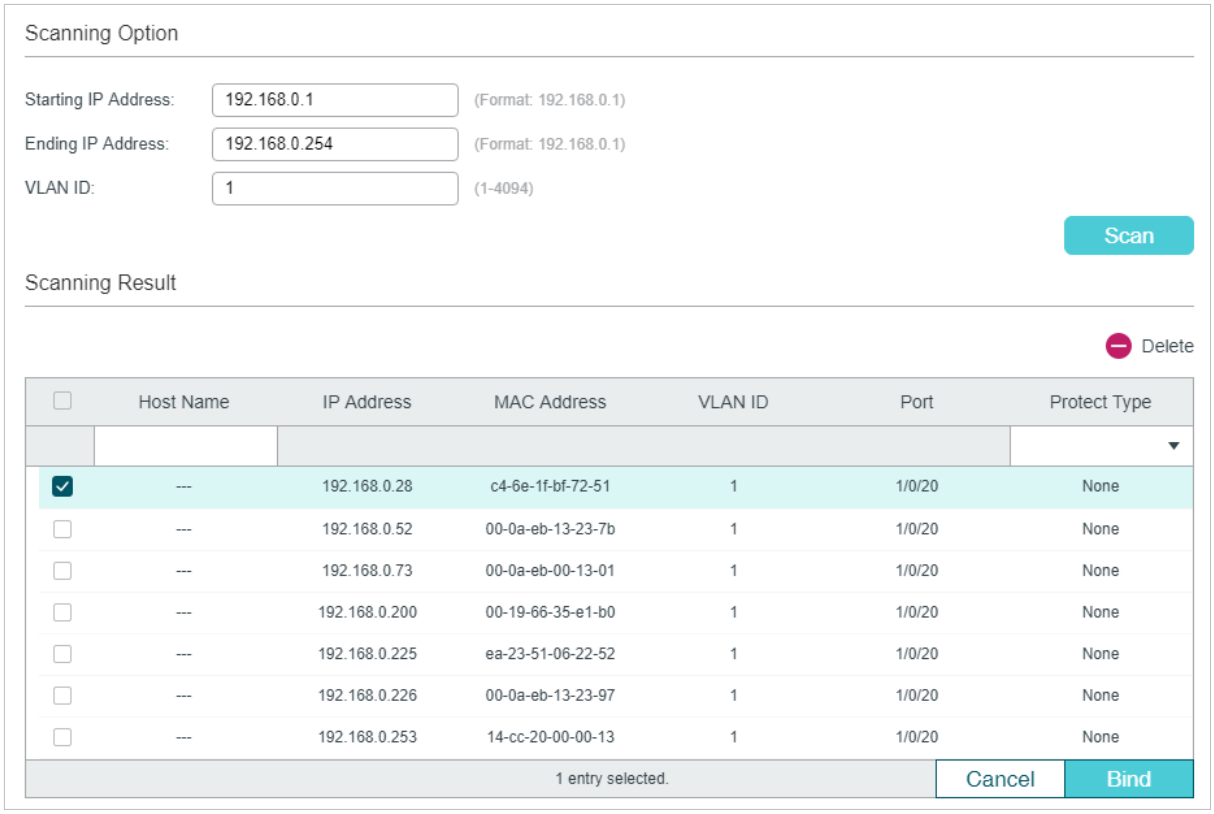
Przy włączonej funkcji ARP Scanning przełącznik wysyła do hostów pakiety żądania ARP wybranego pola IP. W przypadku otrzymania pakiet odpowiedzi ARP przełącznik może pozyskać adres IP, adres MAC, VLAN ID i numer portu podłączonego do hosta. Możesz dogodnie powiązać wpisy.

Uwaga:

Przed włączeniem tej funkcji upewnij się, że sieć jest bezpieczna, i że aktualnie nie występują ataki ARP na hosty. W przeciwnym wypadku możesz uzyskać błędne wpisy wiązania IP-MAC. Jeżeli sieć jest atakowana, zaleca się przeprowadzenie ręcznego wiązania wpisów.

Wybierz menu **SECURITY > IPv4 IMPB > IP-MAC Binding > ARP Scanning**, aby załadować następującą stronę.

Rys. 2-2 ARP Scanning



Aby skonfigurować wiązanie IP-MAC przez ARP scanning, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Scanning Option** wyznacz zakres adresu IP i VLAN ID. Następnie kliknij **Scan,** aby przeskanować wpisy w wyznaczonym zakresie adresu IP i VLAN.

Starting IP Address/Ending IP Address	Wyznacz zakres IP, wpisując początkowy i końcowy adres IP.
VLAN ID	Wyznacz VLAN ID.

2) W sekcji **Scanning Result** wybierz co najmniej jeden wpis i skonfiguruj odpowiednie parametry. Następnie kliknij **Bind**.

Host Name	Wprowadź nazwę, aby umożliwić identyfikację hosta.
IP Address	Informacja o adresie IP.
MAC Address	Informacja o adresie MAC.
VLAN ID	Informacja o VLAN ID.
Port	Informacja o numerze portu.

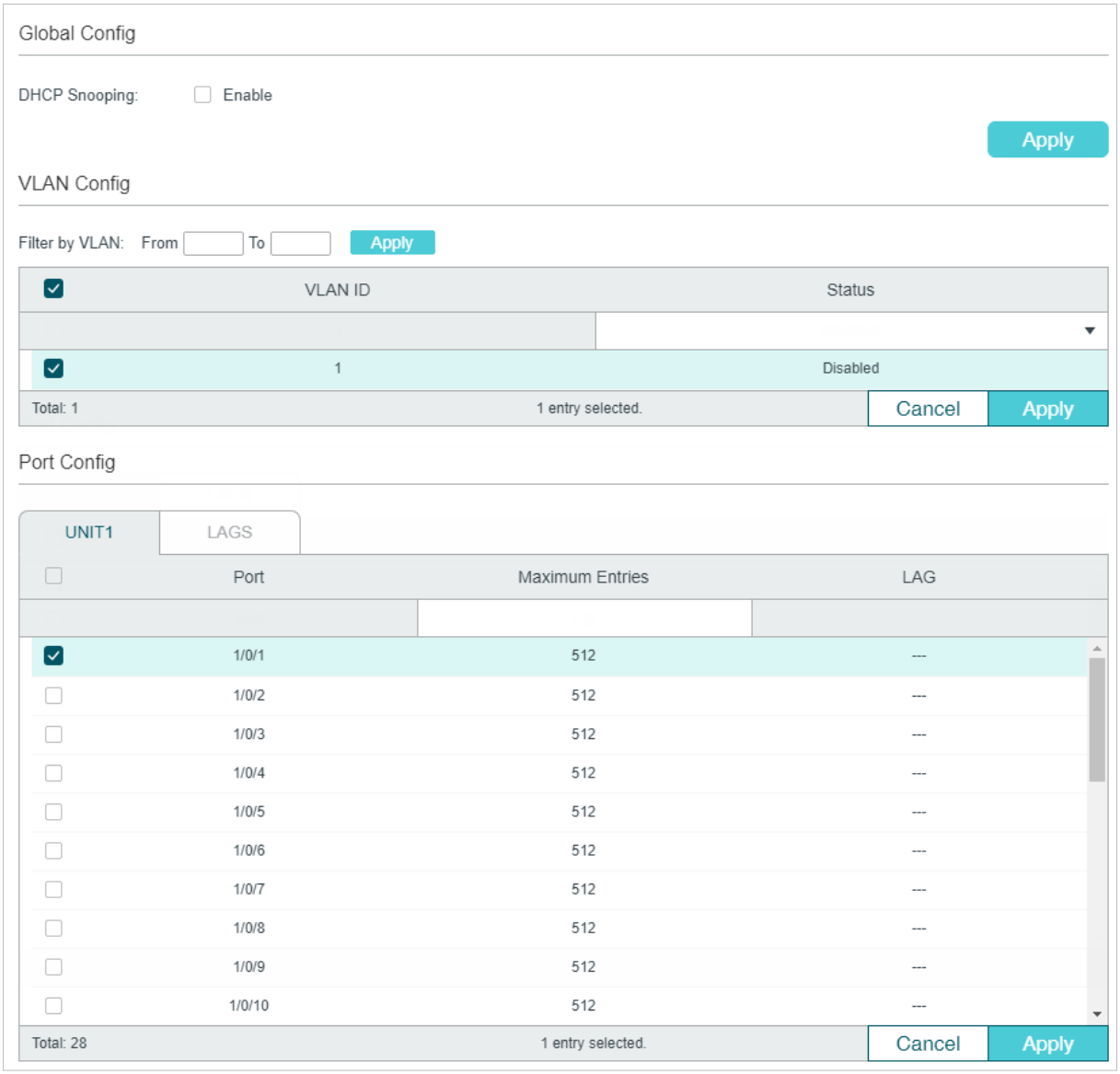
Protect Type	Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje: **None**: Wpis nie będzie zastosowany do żadnej funkcji. **ARP Detection**: Wpis zostanie zastosowany do funkcji ARP Detection. **IP Source Guard**: Wpis zostanie zastosowany do funkcji IPv4 Source Guard. **Both**: Wpis zostanie zastosowany do obu funkcji.

2.1.3 Wiązanie wpisów przez DHCP Snooping

Przy włączonej funkcji DHCP Snooping przełącznik może monitorować proces przyjmowania przez host adresu IP i zarejestrować adres IP, adres MAC, VLAN ID i numer portu podłączonego do hosta.

Wybierz menu **SECURITY > IPv4 IMPB > IP-MAC Binding > DHCP Snooping**, aby załadować następującą stronę.

Rys. 2-3 DHCP Snooping



Aby skonfigurować wiązanie IP-MAC przez DHCP Snooping, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Global Config** włącz DHCP Snooping globalnie. Kliknij **Apply**.

2) W sekcji **VLAN Config** włącz DHCP Snooping w sieci VLAN lub w kilku sieciach VLAN. Kliknij **Apply**.

VLAN ID	Informacja o VLAN ID.
Status	Włącz lub wyłącz DHCP Snooping w sieci VLAN.

3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCP Snooping. Kliknij **Apply**.

Port	Informacja o numerze portu.
Maximum Entries	Skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCP snooping.
LAG	Informacja o grupie LAG, do której należy port.

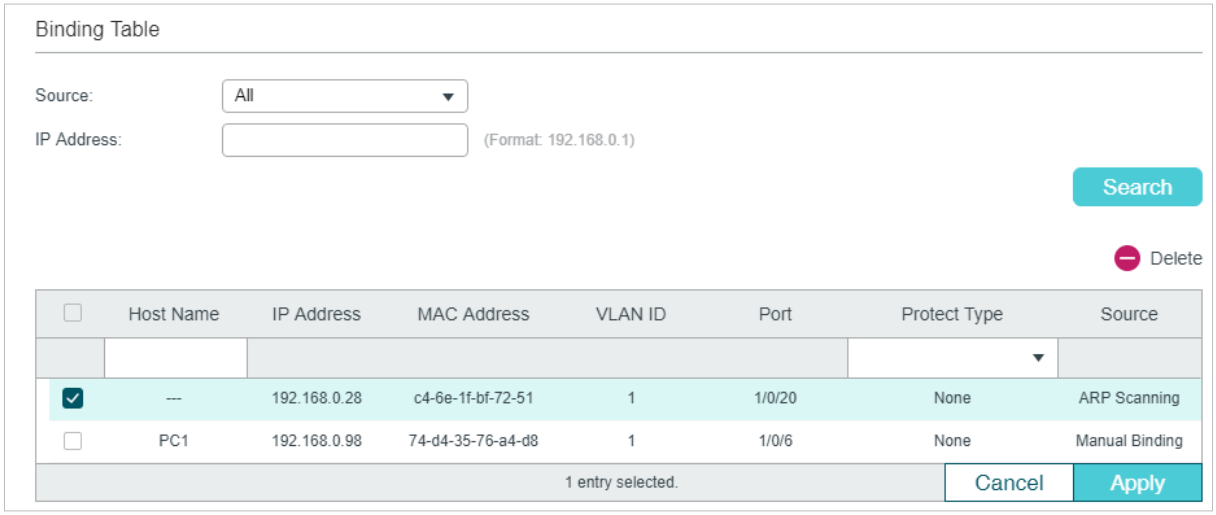
4) Wyuczone wpisy będą wyświetlane na tablicy wiązania (Binding Table). Aby wyświetlać lub edytować wpisy, idź do **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table**.

2.1.4 Wyświetlanie wpisów wiązania

Na tablicy wiązania (Binding Table) możesz wyświetlić, wyszukać lub edytować wybrane wpisy wiązania.

Wybierz menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table**, aby załadować następującą stronę.

Rys. 2-4 Binding Table



Możesz ustawić kryteria wyszukiwania wpisów.

Source	Wybierz źródło wpisu i kliknij **Search**. **All**: Wyświetlanie wpisów ze wszystkich źródeł. **Manual Binding**: Wyświetlanie wpisów powiązanych ręcznie. **ARP Scanning**: Wyświetlanie wpisów wiązania wyuczonych z ARP Scanning. **DHCP Snooping**: Wyświetlanie wpisów wiązania wyuczonych z DHCP Snooping.
IP	Wpisz adres IP i kliknij **Search, aby wyszukać konkretny wpis**.

Dodatkowo wybierz co najmniej jeden wpis, aby edytować nazwę hosta i typ ochrony. Kliknij **Apply**.

Host Name	Wpisz nazwę, aby umożliwić identyfikację hosta.

IP Address	Informacja o adresie IP.
MAC Address	Informacja o adresie MAC.
VLAN ID	Informacja o VLAN ID.
Port	Informacja o numerze portu.
Protect Type	Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje: **None**: Wpis nie będzie zastosowany do żadnej funkcji. **ARP Detection**: Wpis zostanie zastosowany do funkcji ARP Detection. **IP Source Guard**: Wpis zostanie zastosowany do funkcji IPv4 Source Guard. **Both**: Wpis zostanie zastosowany do obu funkcji.
Source	Informacja o źródle wpisu.

2.2 Przez CLI

Wiązanie wpisów przez ARP scanning nie jest obsługiwane przez CLI. Poniższe sekcje opisują, w jaki sposób powiązać wpisy ręcznie i przez DHCP Snooping oraz jak wyświetlać wpisy wiązania.

2.2.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IP, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Aby ręcznie powiązać wpisy, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2	**ip source binding** *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **} {** none | arp-detection | ip-verify-source | both **}** Ręcznie powiąż nazwę hosta, adres IP, adres MAC, VLAN ID i numer portu hosta oraz skonfiguruj typ ochrony hosta. *hostname*: Wyznacz nazwę hosta, składającą się z maks. 20 znaków. *ip-addr*: Wpisz adres IP hosta. *mac-addr*: Wpisz adres MAC hosta w formacie xx:xx:xx:xx:xx:xx. *vlan-id*: Wpisz VLAN ID hosta. *port*: Wpisz numer portu, do którego podłączony jest host. none | arp-detection | ip-verify-source | both: Wyznacz typ ochrony wpisu. „None" oznacza, że wpis nie będzie zastosowany do żadnej funkcji; „arp-detection" oznacza, że wpis zostanie zastosowany do funkcji ARP Detection; „ip-verify-source" oznacza, że wpis zostanie zastosowany do IPv4 Source Guard.
Krok 3	**show ip source binding** Sprawdź wpis wiązania.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje wiązanie wpisu z nazwą hosta host1, adresem IP 192.168.0.55, adresem MAC 74:d4:35:76:a4:d8, VLAN ID 10, portem numer 1/0/5 i włączanie dla wpisu funkcji ARP detection.

Switch#configure

Switch(config)#ip source binding host1 192.168.0.55 74:d4:35:76:a4:d8 **vlan** 10 **interface gigabitEthernet** 1/0/5 arp-detection

Switch(config)#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	host1	192.168.0.55	74:d4:35:76:a4:d8	10	Gi1/0/5	ARP-D	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Wiązanie wpisów przez DHCP Snooping

Aby powiązać wpisy przez DHCP Snooping, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip dhcp snooping** Włącz DHCP Snooping globalnie.
Krok 3	**ip dhcp snooping vlan** *vlan-range* Włącz DHCP Snooping w wyznaczonym VLAN. *vlan-range:* Wprowadź zakres VLAN w formacie 1-3, 5.
Krok 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 5	**ip dhcp snooping max-entries** *value* Skonfiguruj maks. liczbę wpisów wiązania, których port może nauczyć się przez DHCP snooping. *value:* Wpisz maks. dopuszczalną liczbę wpisów. Wartość powinna wynosić od 0 do 512.
Krok 6	**show ip dhcp snooping** Sprawdź konfigurację globalną DHCP Snooping.
Krok 7	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje globalne włączanie DHCP Snooping we VLAN 5 i ustawianie maks. liczby wpisów wiązania, których może nauczyć się port 1/0/1 przez DHCP snooping na100:

Switch#configure

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 5

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp snooping max-entries 100

Switch(config-if)#show ip dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--------- ---------- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Wyświetlanie wpisów wiązania

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji, możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia.

show ip source binding

Wyświetl dane wpisów wiązania (nazwa hosta, adres IP, adres MAC, VLAN ID, numer portu, typ ochrony).

3 Konfiguracja funkcji ARP Detection

Aby przeprowadzić konfigurację funkcji ARP Detection, wykonaj poniższe kroki:

1) Dodaj wpisy wiązania IP-MAC.
2) Włącz ARP Detection.
3) Skonfiguruj ARP Detection na portach.
4) Sprawdź statystyki ARP.

3.1 Przez GUI

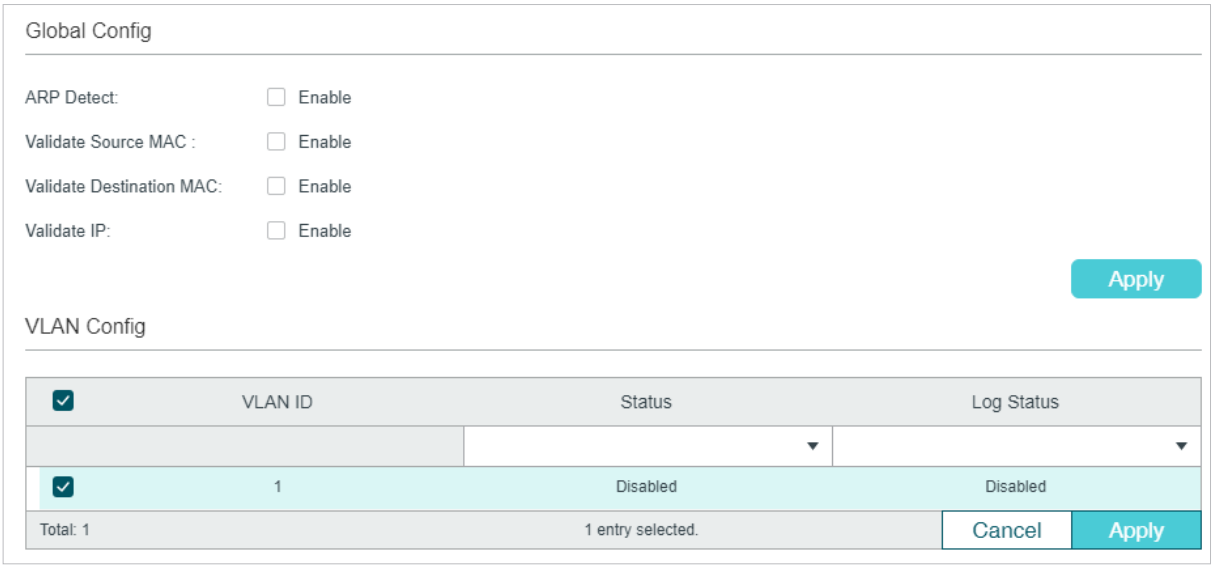
3.1.1 Dodawanie wpisów wiązania IP-MAC

Funkcja ARP Detection polega na wykrywaniu przez przełącznik pakietów ARP w oparciu o wpisy wiązania na tablicy wiązania IP-MAC (IP-MAC Binding Table.) Przed konfiguracją funkcji ARP Detection należy przeprowadzi konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

3.1.2 Włączanie funkcji ARP Detection

Wybierz menu **SECURITY > IPv4 IMPB > ARP Detection > Global Config**, aby załadować następującą stronę.

Rys. 3-1 Konfiguracja globalna ARP Detection



Aby włączyć ARP Detection, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Global Config** włącz ARP Detection i skonfiguruj powiązane parametry. Kliknij **Apply**.

ARP Detect	Włącz lub wyłącz ARP Detection globalnie.
Validate Source MAC	Możesz włączyć na przełączniku sprawdzanie, czy przy odbieraniu pakietu ARP źródłowy adres MAC i adres MAC nadawcy są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.
Validate Destination MAC	Możesz włączyć na przełączniku sprawdzanie, czy podczas odbierania pakietu odpowiedzi ARP docelowy adres MAC i źródłowy adres MAC są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.
Validate IP	Możesz włączyć na przełączniku sprawdzanie, czy adres IP nadawcy wszystkich pakietów ARP i docelowy adres IP pakietów odpowiedzi ARP są legalne. Nielegalne pakiety ARP, takie jak adresy broadcast, adresy multicast, adresu klasy E, adresy loopback (127.0.0.0/8) i adres 0.0.0.0., zostaną odrzucone.

2) W sekcji **VLAN Config** włącz ARP Detection w wybranych sieciach VLAN. Kliknij **Apply**.

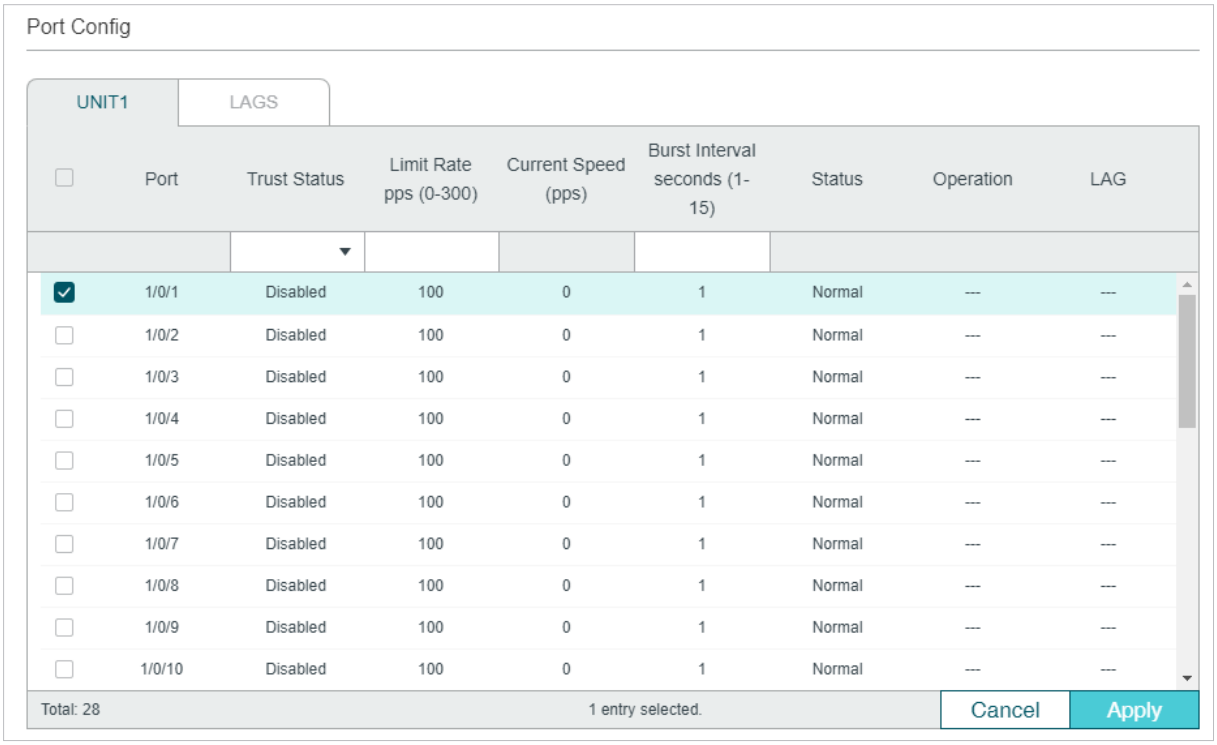
VLAN ID	Informacja o VLAN ID.
Status	Włącz lub wyłącz ARP Detection w sieci VLAN.

Log Status	Włącz lub wyłącz w sieci VLAN Log Feature (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ARP będzie generował zapis.

3.1.3 Konfiguracja funkcji ARP Detection na portach

Wybierz menu **SECURITY > IPv4 IMPB > ARP Detection >Port Config**, aby załadować następującą stronę.

Rys 3-2 ARP Detection na porcie



Aby skonfigurować ARP Detection na portach, postępuj zgodnie z poniższymi krokami.

1) Wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry.

Trust Status	Włącz lub wyłącz dla tego portu status portu zaufanego. Na porcie zaufanym pakiety ARP przekierowywane są bezpośrednio, bez sprawdzania. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.
Limit Rate	Wyznacz maks. liczbę pakietów ARP, które mogą być odbierane na porcie na jedną sekundę.
Current Speed	Informacja o aktualnej prędkości odbierania pakietów ARP na porcie.

Burst Interval	Wyznacz zakres czasu. Jeżeli prędkość otrzymywanych pakietów ARP osiągnie górną granicę tego zakresu, port zostanie zamknięty.
Status	Informacja o stanie ataku ARP: **Normal**: Przekierowywanie pakietów ARP na porcie przebiega normalnie. **Down:** Prędkość przekazywania legalnych pakietów ARP przekracza wyznaczoną wartość. Port zostanie zamknięty za 300 sekund. Aby na nowo uaktywnić port, kliknij przycisk Recovery.
Operation	Jeżeli stan zmieni się na Down, pojawi się przycisk **Recover**. Możesz kliknąć ten przycisk, aby przywrócić port do normalnego stanu.
LAG	Informacja o grupie LAG, do której należy port.

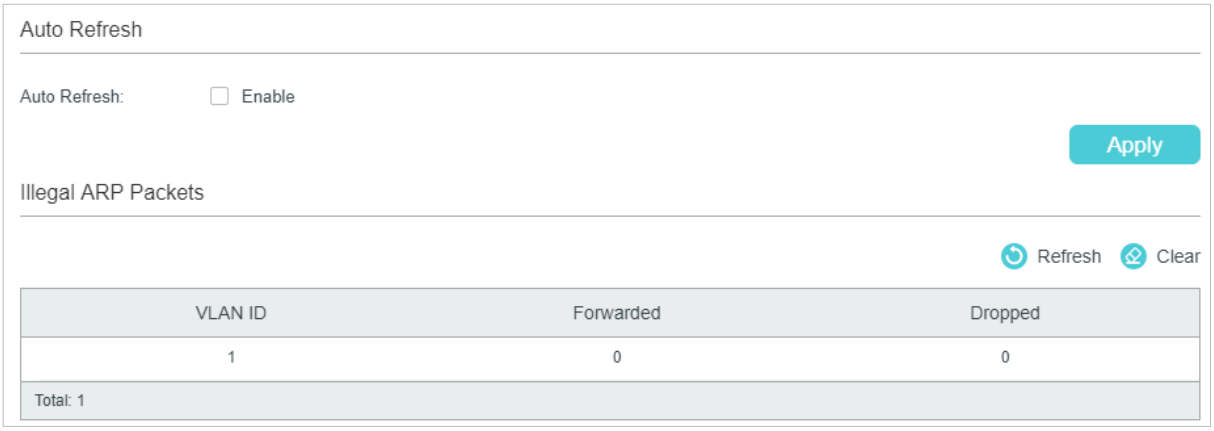
2) Kliknij **Apply**.

3.1.4 Wyświetlanie statystyk ARP

Możesz zobaczyć liczbę nielegalnych pakietów ARP otrzymanych przez każdy port. Ułatwi to zlokalizowanie przyczyny wadliwego działania sieci i podjęcie odpowiednich środków dla zabezpieczenia sieci.

Wybierz menu **SECURITY > IPv4 IMPB > ARP Detection > ARP Statistics**, aby załadować następującą stronę.

Rys. 3-3 Statystyki ARP



W sekcji **Auto Refresh** możesz włączyć funkcję automatycznego odświeżania i wyznaczy odstęp czasu, w którym strona internetowa będzie automatycznie odświeżana.

W sekcji **Illegal ARP Packet** możesz sprawdzić liczbę nielegalnych pakietów ARP w każdej sieci VLAN.

VLAN ID	Informacja o VLAN ID.
Forwarded	Informacja o liczbie przekazanych pakietów ARP w tej sieci VLAN.

Dropped	Informacja o liczbie odrzuconych pakietów ARP w tej sieci VLAN.

3.2 Przez CLI

3.2.1 Dodawanie wpisów wiązania IP-MAC

Funkcja ARP Detection polega na wykrywaniu przez przełącznik pakietów ARP w oparciu o wpisy wiązania na tablicy wiązania IP-MAC (IP-MAC Binding Table.) Przed konfiguracją funkcji ARP Detection należy przeprowadzi konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

3.2.2 Włączanie funkcji ARP Detection

Aby włączyć funkcję ARP Detection, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ip arp inspection** Włącz funkcję ARP Detection globalnie.
Krok 3	**ip arp inspection validate {** src-mac | dst-mac | ip **}** Skonfiguruj na przełączniku sprawdzanie adresów IP lub adresów MAC otrzymanych pakietów. src-mac: Włącz na przełączniku sprawdzanie podczas odbierania pakietu ARP, czy źródłowy adres MAC i adres MAC nadawcy są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony. dst-mac: Włącz na przełączniku sprawdzanie podczas odbierania pakietu odpowiedzi ARP, czy docelowy adres MAC i źródłowy adres MAC są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony. ip: Włącz na przełączniku sprawdzanie, czy adres IP nadawcy wszystkich pakietów ARP i docelowy adres IP pakietów odpowiedzi ARP są legalne. Nielegalne pakiety ARP, takie jak adresy broadcast, adresy multicast, adresy klasy E, adresy loopback (127.0.0.0/8) i adres 0.0.0.0., zostaną odrzucone
Krok 4	**ip arp inspection vlan** *vlan-list* Włącz ARP Detection na co najmniej jednej istniejącej sieci VLAN 802.1Q. *vlan-list*: Wpisz VLAN ID. Format to 1,5-9.

Krok 5	**ip arp inspection vlan** *vlan-list* **logging** (Opcjonalnie) Włącz funkcję Log feature (funkcja rejestru zdarzeń, aby przełącznik po odrzuceniu nielegalnego pakietu ARP generował zapis. *vlan-list*: Wpisz VLAN ID. Format to 1,5-9.
Krok 6	**show ip arp inspection** Sprawdź ustawienia ARP Detection.
Krok 7	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie globalne ARP Detection na VLAN 2 i włączanie na przełączniku sprawdzania przy odbieraniu pakietów, czy ARP źródłowy adres MAC i adres MAC nadawcy są takie same:

Switch#configure

Switch(config)#ip arp inspection

Switch(config)#ip arp inspection validate src-mac

Switch(config)#ip arp inspection vlan 2

Switch(config)#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Disable

Verify IP: Disable

Switch(config)#show ip arp inspection vlan

VID	Enable status	Log Status
----	----------	----------
1	Disable	Disable
2	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Konfiguracja funkcji ARP Detection na portach

Aby skonfigurować funkcję ARP Detection na portach, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ip arp inspection trust** Ustaw port jako zaufany, który nie będzie objęty działaniem funkcji ARP Detection. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.
Krok 4	**ip arp inspection limit-rate** *value* Wyznacz maks. liczbę pakietów ARP, które mogą być odbierane na porcie na jedną sekundę. *value:* Wyznacz wartość maksymalną. Wartość powinna wynosić od 0 do 300 p/s (pakiety na sekundę); wartość domyślna to 100.
Krok 5	**ip arp inspection burst-interval** *value* Wyznacz zakres czasu. Jeżeli prędkość otrzymywanych pakietów ARP osiągnie górną granicę tego zakresu, port zostanie zamknięty. *value:* Wyznacz zakres czasu, między 1 a 15 sekund. Wartość domyślna to 1 sekunda.
Krok 6	**show ip arp inspection interface** Sprawdź konfigurację i stan portu.
Krok 7	**show ip arp inspection vlan** Sprawdź konfigurację i stan sieci VLAN.
Krok 8	**ip arp inspection recover** (Opcjonalnie) Porty, których prędkość odbierania pakietów przekroczyła wyznaczony limit można przywrócić do stanu Normal za pomocą tego polecenia.
Krok 9	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawienie portu 1/02 jako zaufany, ustawienie limitu prędkości na 20 p/s i zakresu czasu (burst interval) na porcie 1/0/2 na 2 sekundy:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip arp inspection trust

Switch(config-if)#ip arp inspection limit-rate 20

Switch(config-if)#ip arp inspection burst-interval 2

Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2

Interface	Trust state	limit Rate(pps)	Current speed(pps)	Burst Interval	Status	LAG
---	---	---	---	---	---	---
Gi1/0/2	Enable	20	0	2	---	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

The following example shows how to restore the port 1/0/1 that is in Down status to Normal status:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip arp inspection recover

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Wyświetlanie statystyk ARP

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji ,możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia.

show ip arp inspection statistics

Wyświetl statystyki ARP dla każdego portu (liczba przekazanych pakietów ARP, liczba odrzuconych pakietów ARP).

4 Konfiguracja funkcji IPv4 Source Guard

Aby przeprowadzić konfigurację IPv4 Source Guard, wykonaj poniższe kroki:

1) Dodaj wpis wiązania IP-MAC.
2) Skonfiguruj funkcję IPv4 Source Guard.

4.1 Przez GUI

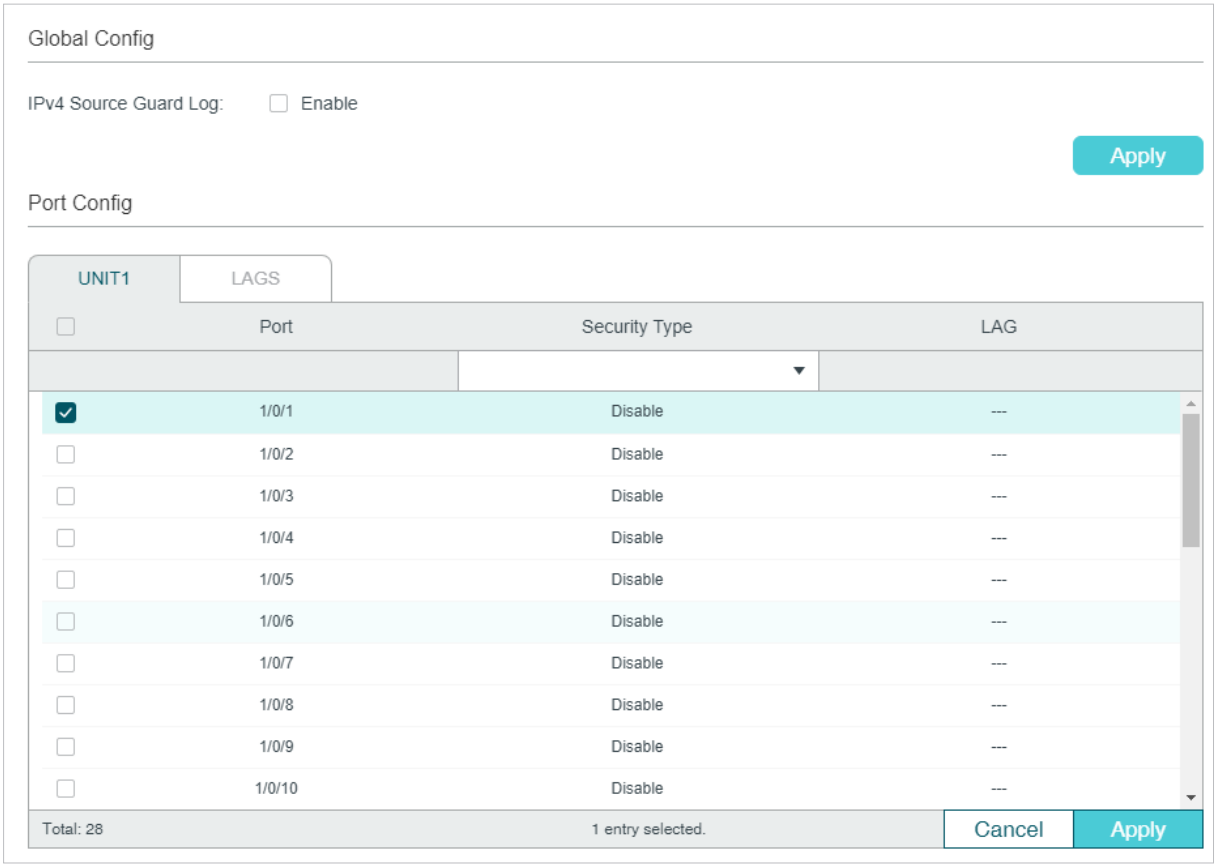
4.1.1 Dodawanie wpisów wiązania IP-MAC

Funkcja IPv4 Source Guard polega na filtrowaniu przez przełącznik pakietów, które nie są dopasowane do reguł tabeli wiązania IPv4-MAC. Przed konfiguracją funkcji ARP Detection należy więc przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

4.1.2 Konfiguracja funkcji IPv4 Source Guard

Wybierz menu **SECURITY > IPv4 IMPB > IPv4 Source Guard**, aby załadować następującą stronę.

Rys.4-1 Konfiguracja funkcji IPv4 Source Guard



Aby skonfigurować funkcję IPv4 Source Guard, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Global Config** section zdecyduj, czy chcesz włączyć funkcję Log. Kliknij **Apply**.

IPv4 Source Guard Log	Włącz lub wyłącz funkcję IPv4 Source Guard Log (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ARP będzie generował zapis.

2) W sekcji **Port Config** skonfiguruj tryb ochrony portów i kliknij A**pply**.

Port	Informacja o numerze portu.

Security Type	Wybierz tryb ochrony na porcie dla pakietów IPv4. Dostępne są następujące opcje: **Disable:** Funkcja IP Source Guard jest wyłączona na porcie. **SIP+MAC**: Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane. **SIP**: Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane.
LAG	Informacja o grupie LAG, do której należy port.

4.2 Przez CLI

4.2.1 Dodawanie wpisów wiązania IP-MAC

Funkcja IPv4 Source Guard polega na filtrowaniu przez przełącznik pakietów, które nie są dopasowane do reguł tabeli wiązania IPv4-MAC. Przed konfiguracją funkcji ARP Detection należy więc przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

4.2.2 Konfiguracja funkcji IPv4 Source Guard

Aby skonfigurować funkcję IPv4 Source Guard, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ip verify source {** sip+mac | sip **}** Włącz IP Source Guard dla pakietów IPv4. sip+mac*:* Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane. sip*:* Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane.
Krok 4	**show ip verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** Sprawdź konfigurację IP Source Guard dla pakietów IPv4.

Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie IPv4 Source Guard na porcie1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip verify source sip+mac

Switch(config-if)#show ip verify source interface gigabitEthernet 1/0/1

Port Security-Type LAG

---- ---------- ----

Gi1/0/1 SIP+MAC N/A

Switch(config-if)#end

Switch#copy running-config startup-config

Część 21

Konfiguracja IMPB IPv6

ROZDZIAŁY

1 IMPB IPv6

1.1 Obsługiwane funkcje

Wiązanie IPv6-MAC

Funkcja służy do dodawania wpisów wiązania. Wpisy wiązania mogą być konfigurowane ręcznie lub wyuczone przez funkcje ND Snooping lub DHCPv6 snooping. ND Detection i IPv6 Source Guard bazują na wpisach wiązania IPv6-MAC.

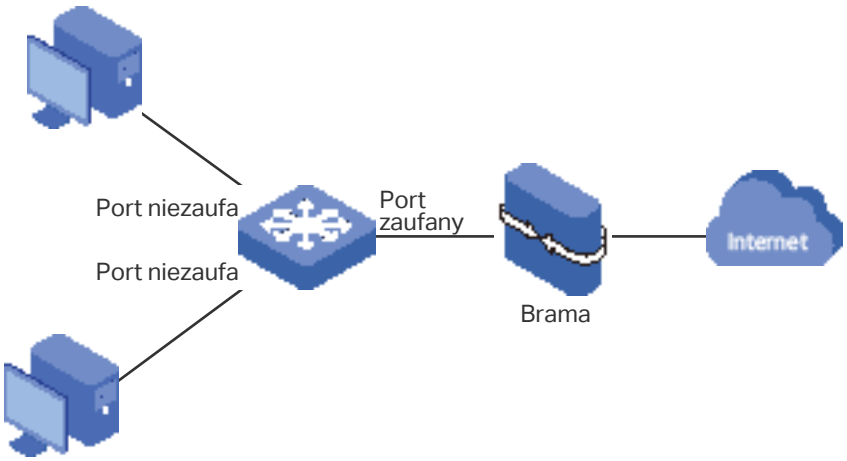
ND Detection

Ze względu na brak mechanizmu zabezpieczającego, protokół IPv6 ND (Neighbor Discovery) może być z łatwością wykorzystywany przez podmiot atakujący. Funkcja ND detection wykorzystuje wpisy z tablicy wiązania IPv6-MAC do filtrowania sfałszowanych pakietów ND i zapobiegania atakom ND.

Topologia wdrażania ND Detection zaprezentowana jest na poniższym schemacie. Port podłączony do bramy powinien być skonfigurowany jako zaufany, pozostałe porty nie powinny mieć ustawionego trybu zaufania. Poniżej przedstawiono zasady przekierowywania pakietów ND:

- Wszystkie pakiety ND odebrane na porcie zaufanym będą przekierowywane bez sprawdzania.
- Pakiety RS (Router Solicitation) i NS (Neighbor Solicitation) bez wyznaczonych adresów IPv6, jak np. pakiet RS do żądania adresu IPv6 i pakiet NS do wykrywania podwójnych adresów, nie będą sprawdzane na żadnym z dwóch typów portów.
- Pakiety RA (Router Advertisement) i RR (Router Redirect) odebrane na porcie niezaufanym będą bezpośrednio odrzucane. Pozostałe pakiety ND będą sprawdzane. Przełącznik użyje tablicy wiązania IPv6-MAC do porównania adresu IPv6, adresu MAC, VLAN ID i portu odbierającego między wpisem i pakietem ND. W przypadku znalezienia dopasowania, pakiet ND uznawany jest za legalny, pakiet zostanie więc przekierowany. W przypadku braku dopasowania, pakiet ND uznawany jest za nielegalny; pakiet zostanie więc odrzucony.

Rys. 1-1 Topologia sieci ND Detection



IPv6 Source Guard

Funkcja IPv6 Source Guard służy do filtrowania pakietów IPv6 w oparciu o tablicę wiązania IPv6-MAC. Przekierowywane są jedynie pakiety zgodne z regułami wiązania.

2 Konfiguracja wiązania IPv6-MAC

Wpisy wiązania IPv6-MAC można dodawać trzema sposobami:

- Wiązanie ręczne
- Przez ND Snooping
- Przez DHCPv6 Snooping

Dodatkowo można wyświetlać, wyszukiwać i edytować wpisy na tablicy wiązania (Binding Table).

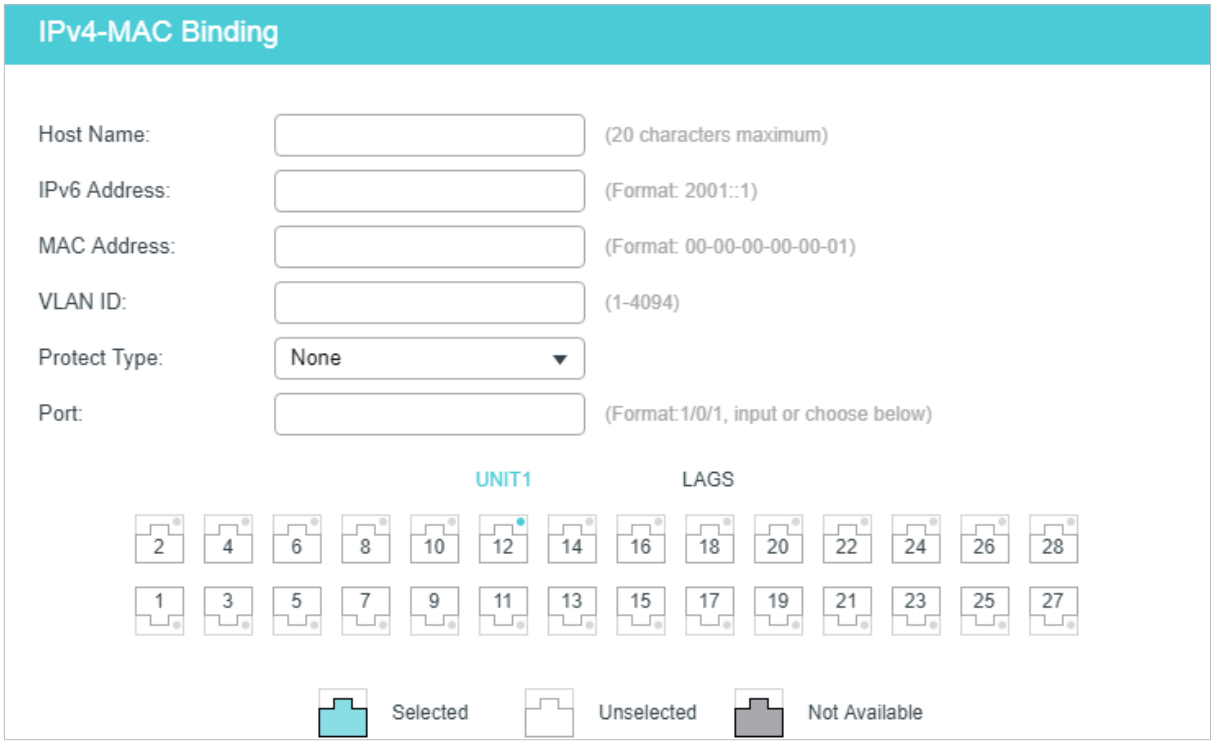
2.1 Przez GUI

2.1.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IPv6, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wybierz menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** i kliknij Add , aby załadować następującą stronę.

Rys. 2-1 Wiązanie ręczne



Aby ręcznie utworzyć wpis wiązania IPv6-MAC, postępuj zgodnie z poniższymi krokami.

1) Wprowadź następujące informacje, aby określić host.

Host Name	Wprowadź nazwę, aby umożliwić identyfikację hosta.
IP Address	Wprowadź adres IP.
MAC Address	Wprowadź adres MAC.
VLAN ID	Wprowadź VLAN ID.

2) Wybierz typ ochrony wpisu.

Protect Type	Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje: **None**: Wpis nie będzie zastosowany do żadnej funkcji. **ND Detection**: Wpis zostanie zastosowany do funkcji ND Detection. **IPv6 Source Guard**: Wpis zostanie zastosowany do funkcji IPv6 Source Guard. **Both**: Wpis zostanie zastosowany do obu funkcji.

3) Wpisz lub wybierz port podłączony do tego hosta.

4) Kliknij **Apply**.

2.1.2 Wiązanie wpisów przez ND Snooping

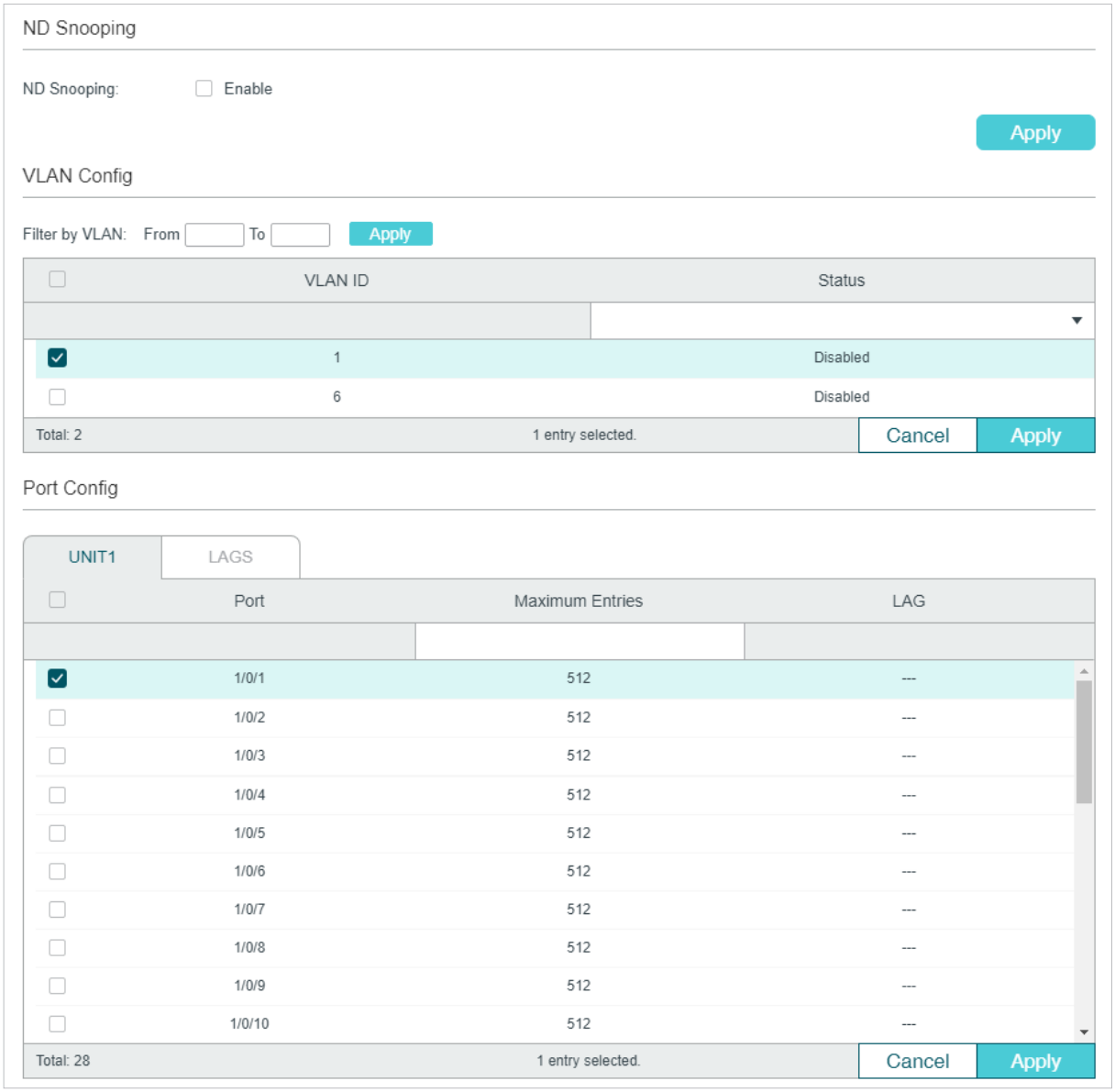
Przy włączonej funkcji ND Snooping przełącznik monitoruje pakiety ND i zapisuje adresy IPv6, adresy MAC, VLAN ID i numery portów połączonych z hostami IPv6. Możesz dogodnie powiązać wpisy.

Uwaga:

Przed włączeniem tej funkcji upewnij się, że sieć jest bezpieczna, i że aktualnie nie występują ataki ND na hosty. W przeciwnym wypadku możesz uzyskać błędne wpisy wiązania IPv6-MAC. Jeżeli sieć jest atakowana, zaleca się przeprowadzenie ręcznego wiązania wpisów.

Wybierz menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > ND Snooping**, aby załadować następującą stronę.

Rys. 2-2 ND Snooping



Aby skonfigurować wiązanie IPv6-MAC przez ND Snooping, postępuj zgodnie z poniższymi krokami.

1) W sekcji **ND Snooping** włącz ND Snooping i kliknij **Apply**.
2) W sekcji **VLAN Config** wybierz co najmniej jeden VLAN i włącz ND Snooping. Kliknij **Apply**.

VLAN ID	Informacja o VLAN ID.
Status (Stan)	Włącz lub wyłącz ND Snooping w sieci VLAN.

3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów, których port może wyuczyć się przez ND snooping. Kliknij **Apply**.

Port	Informacja o numerze portu.
Maximum Entries (Maks. liczba wpisów)	Skonfiguruj maks. liczbę wpisów, których port może wyuczyć się przez ND snooping..
LAG	Informacja o grupie LAG, do której należy port.

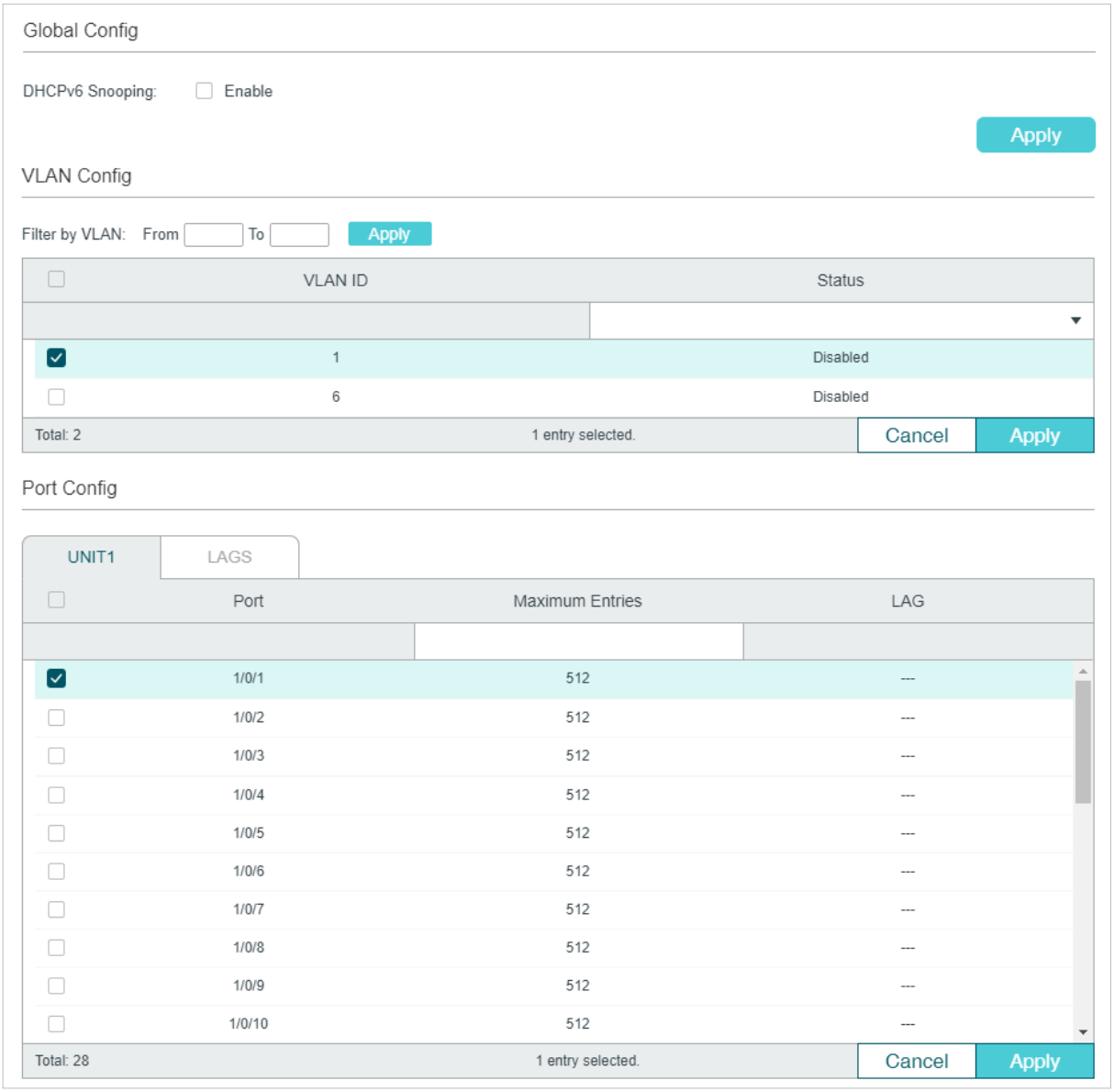
4) Wyuczone wpisy będą wyświetlane na tablicy wiązania (Binding Table). Aby wyświetlać lub edytować wpisy, idź do **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table**.

2.1.3 Wiązanie wpisów przez DHCPv6 Snooping

Przy włączonej funkcji DHCPv6 Snooping przełącznik może monitorować proces przyjmowania przez host adresu IP i zarejestrować adres IPv6, adres MAC, VLAN ID i numer portu podłączonego do hosta.

Wybierz menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > DHCPv6 Snooping**, aby załadować następującą stronę.

Rys. 2-3 DHCPv6 Snooping



Aby skonfigurować wiązanie IPv6-MAC przez DHCPv6 Snooping, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Global Config** włącz DHCPv6 Snooping globalnie. Kliknij **Apply**.

2) W sekcji **VLAN Config** włącz DHCPv6 Snooping w sieci VLAN lub w kilku sieciach VLAN. Kliknij **Apply**.

VLAN ID	Informacja o VLAN ID.
Status	Włącz lub wyłącz DHCPv6 Snooping w sieci VLAN.

3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCPv6 Snooping. Kliknij **Apply**.

Port	Informacja o numerze portu.
Maximum Entries	Skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCPv6 snooping.
LAG	Informacja o grupie LAG, do której należy port.

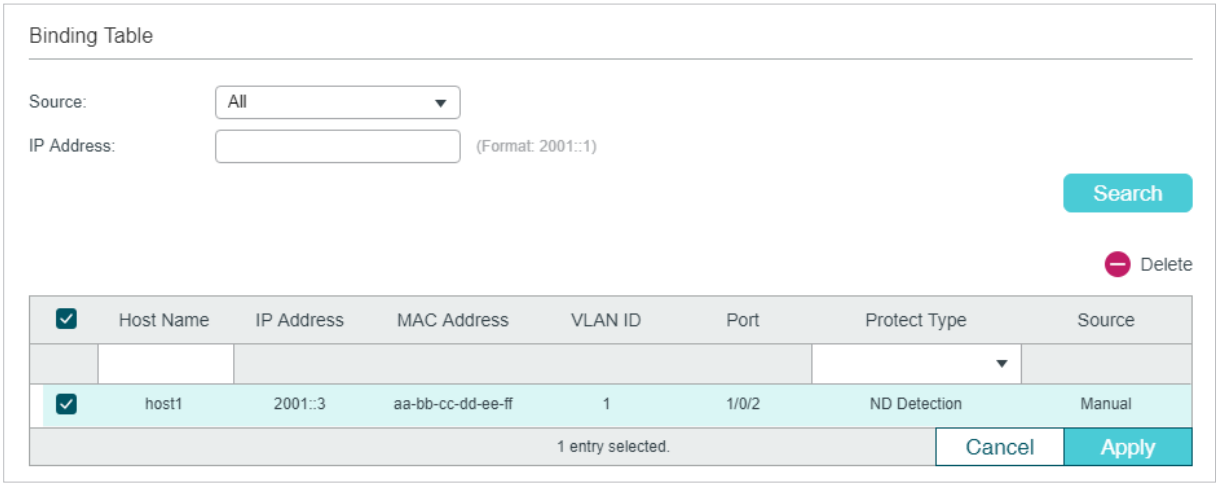
4) Wyuczone wpisy będą wyświetlane na tablicy wiązania (Binding Table). Aby wyświetlać lub edytować wpisy, idź do **SECURITY > IPv6 IMPB > IP-MAC Binding > Binding Table**.

2.1.4 Wyświetlanie wpisów wiązania

Na tablicy wiązania (Binding Table) możesz wyświetlić, wyszukać lub edytować wybrane wpisy wiązania.

Wybierz menu **SECURITY > IPv6 IMPB > IP-MAC Binding > Binding Table**, aby załadować następującą stronę.

Rys. 2-4 Binding Table



Możesz ustawić kryteria wyszukiwania wpisów.

Source	Wybierz źródło wpisu i kliknij **Search**. **All**: Wyświetlanie wpisów ze wszystkich źródeł. **Manual Binding**: Wyświetlanie wpisów powiązanych ręcznie. **ND Snooping**: Wyświetlanie wpisów wiązania wyuczonych z ND Snooping. **DHCPv6 Snooping**: Wyświetlanie wpisów wiązania wyuczonych z DHCP Snooping.
IP	Wpisz adres IP i kliknij **Search**, aby wyszukać konkretny wpis**.**

Dodatkowo wybierz co najmniej jeden wpis, aby edytować nazwę hosta i typ ochrony. Kliknij **Apply**.

Host Name	Wpisz nazwę, aby umożliwić identyfikację hosta.

IP Address	Informacja o adresie IPv6.
MAC Address	Informacja o adresie MAC.
VLAN ID	Informacja o VLAN ID.
Port	Informacja o numerze portu.
Protect Type	Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje: **None (żadna)**: Wpis nie będzie zastosowany do żadnej funkcji. **ND Detection**: Wpis zostanie zastosowany do funkcji ND Detection. **IPv6 Source Guard**: Wpis zostanie zastosowany do funkcji IP Source Guard. **Both (obie)**: Wpis zostanie zastosowany do obu funkcji.
Source	Informacja o źródle wpisu.

2.2 Przez CLI

Poniższe sekcje prezentują, jak powiązać wpisy ręcznie, przez ND Snooping i przez DHCP Snooping, oraz jak wyświetlać wpisy wiązania.

2.2.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IPv6, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Aby ręcznie powiązać wpisy, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ipv6 source binding** *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **} {** none | nd-detection | ipv6-verify-source | both **}** Ręcznie powiąż nazwę hosta, adres IP, adres MAC, VLAN ID i numer portu hosta oraz skonfiguruj typ ochrony hosta. *hostname*: Wyznacz nazwę hosta, składającą się z maks. 20 znaków. *ipv6-addr*: Wpisz adres IPv6 hosta. *mac-addr*: Wpisz adres MAC hosta w formacie xx:xx:xx:xx:xx:xx. *vlan-id*: Wpisz VLAN ID hosta. *port*: Wpisz numer portu, do którego podłączony jest host. none | nd-detection | ipv6-verify-source | both: Wyznacz typ ochrony wpisu. „None" oznacza, że wpis nie będzie zastosowany do żadnej funkcji; „nd-detection" oznacza, że wpis zostanie zastosowany do funkcji ND Detection; „ipv6-verify-source" oznacza, że wpis zostanie zastosowany do IP Source Guard; „Both" oznacza, że wpis będzie zastosowany do obu funkcji
Krok 3	**show ip source binding** Sprawdź wpis wiązania.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje wiązanie wpisu z nazwą hosta host1, adresem IPv6 2001:0:9d38:90d5::34, adresem MAC AA-BB-CC-DD-EE-FF, VLAN ID 10, portem numer 1/0/5 i włączanie dla wpisu funkcji ND Detection.

Switch#configure

Switch(config)#ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff **vlan** 10 **interface gigabitEthernet** 1/0/5 nd-detection

Switch(config)#show ipv6 source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Source
-	----	-------	--------	---	----	---	------
1	host1	2001:0:9d38:90d5::34	aa:bb:cc:dd:ee:ff	10	Gi1/0/5	ND-D	Manual

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Wiązanie wpisów przez ND Snooping

Aby powiązać wpisy przez ND Snooping, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ipv6 nd snooping** Włącz ND Snooping globalnie.
Krok 3	**ipv6 nd snooping vlan** *vlan-range* Włącz ND Snooping w wyznaczonym VLAN. *vlan-range:* Wpisz zakres VLAN w formacie 1-3, 5.
Krok 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Wejdź w tryb konfiguracji interfejsu.
Krok 5	**ipv6 nd snooping max-entries** *value* Skonfiguruj maks. liczbę wpisów wiązania ND, których port może nauczyć się przez ND snooping. *value:* Wpisz maks. dopuszczalną liczbę wpisów wiązania ND, których port może nauczyć się przez ND snooping. Wartość powinna wynosić od 0 do 1024, wartość domyślna to 1024.
Krok 6	**show ipv6 nd snooping** Sprawdź konfigurację globalną IPv6 ND Snooping
Krok 7	**show ipv6 nd snooping interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Sprawdź konfigurację IPv6 ND Snoopingna wyznaczonym porcie.
Krok 8	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje globalne włączanie ND Snooping we VLAN 1.

Switch#configure

Switch(config)#ipv6 nd snooping

Switch(config)#ipv6 nd snooping vlan 1

Switch(config)#show ipv6 nd snooping

Global Status: Enable

VLAN ID: 1

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the maximum number of entries that can be learned on port 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 nd snooping max-entries 1000

Switch(config-if)#show ipv6 nd snooping interface gigabitEthernet 1/0/1

Interface	max-entries	LAG
---	---	---
Gi1/0/1	1000	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Wiązanie wpisów przez DHCPv6 Snooping

Aby powiązać wpisy przez DHCP Snooping, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ipv6 dhcp snooping** Włącz DHCPv6 Snooping globalnie.
Krok 3	**ipv6 dhcp snooping vlan** *vlan-range* Włącz DHCPv6 Snooping w wyznaczonym VLAN. *vlan-range:* Wpisz zakres VLAN w formacie 1-3, 5.
Krok 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 5	**ipv6 dhcp snooping max-entries** *value* Skonfiguruj maks. liczbę wpisów wiązania, których port może nauczyć się przez DHCPv6 snooping. *value:* Wpisz maks. dopuszczalną liczbę wpisów. Wartość powinna wynosić od 0 do 512.

Krok 6	**show ip dhcp snooping** Sprawdź konfigurację globalną DHCPv6 Snooping.
Krok 7	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 8	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje globalne włączanie DHCPv6 Snooping we VLAN 5 i ustawianie maks. liczby wpisów wiązania, których może nauczyć się port 1/0/1 przez DHCPv6 snooping na 100:

Switch#configure

Switch(config)#ipv6 dhcp snooping

Switch(config)#ipv6 dhcp snooping vlan 5

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 dhcp snooping max-entries 100

Switch(config-if)#show ipv6 dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ipv6 dhcp snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--------- ---------- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Wyświetlanie wpisów wiązania

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji ,możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia.

show ipv6 source binding Wyświetl dane wpisów wiązania (nazwa hosta, adres IP, adres MAC, VLAN ID, numer portu, typ ochrony).

3 Konfiguracja funkcji ND Detection

Aby przeprowadzić konfigurację ND Detection, postępuj zgodnie z poniższymi krokami:

1) Dodaj wpis wiązania IPv6-MAC.
2) Włącz ND Detection.
3) Skonfiguruj ND Detection na portach.
4) Sprawdź statystyki ND.

3.1 Przez GUI

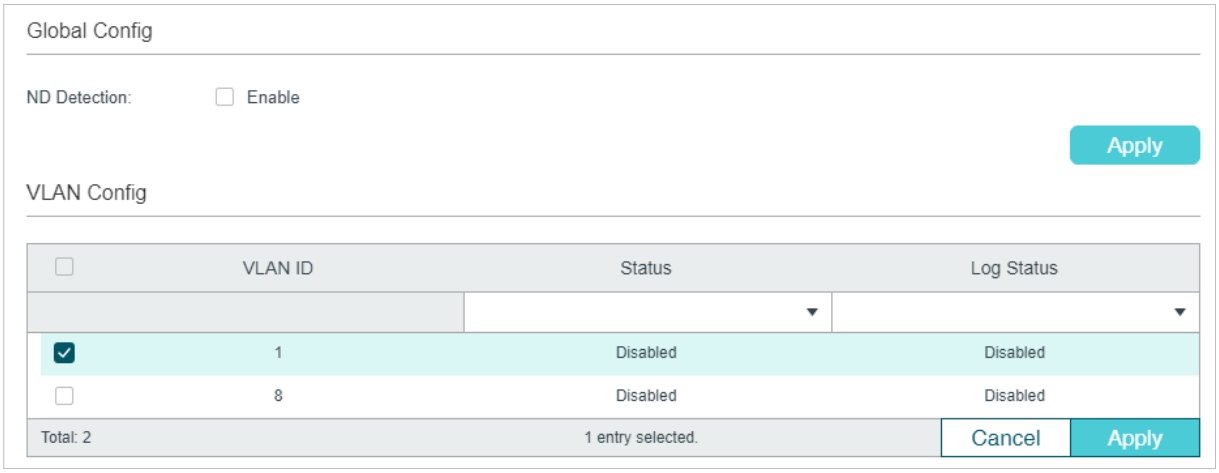
3.1.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzi konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

3.1.2 Włączanie funkcji ND Detection

Wybierz menu **SECURITY > IPv6 IMPB > ND Detection > Global Config**, aby załadować następującą stronę.

Rys. 3-1 Globalna konfiguracja ND Detection



Aby włączyć ND Detection, postępuj zgodnie z poniższymi krokami

1) W sekcji **Global Config** włącz ND Detection i skonfiguruj powiązane parametry. Kliknij **Apply**.

ND Detection	Włącz lub wyłącz ND Detection globalnie.

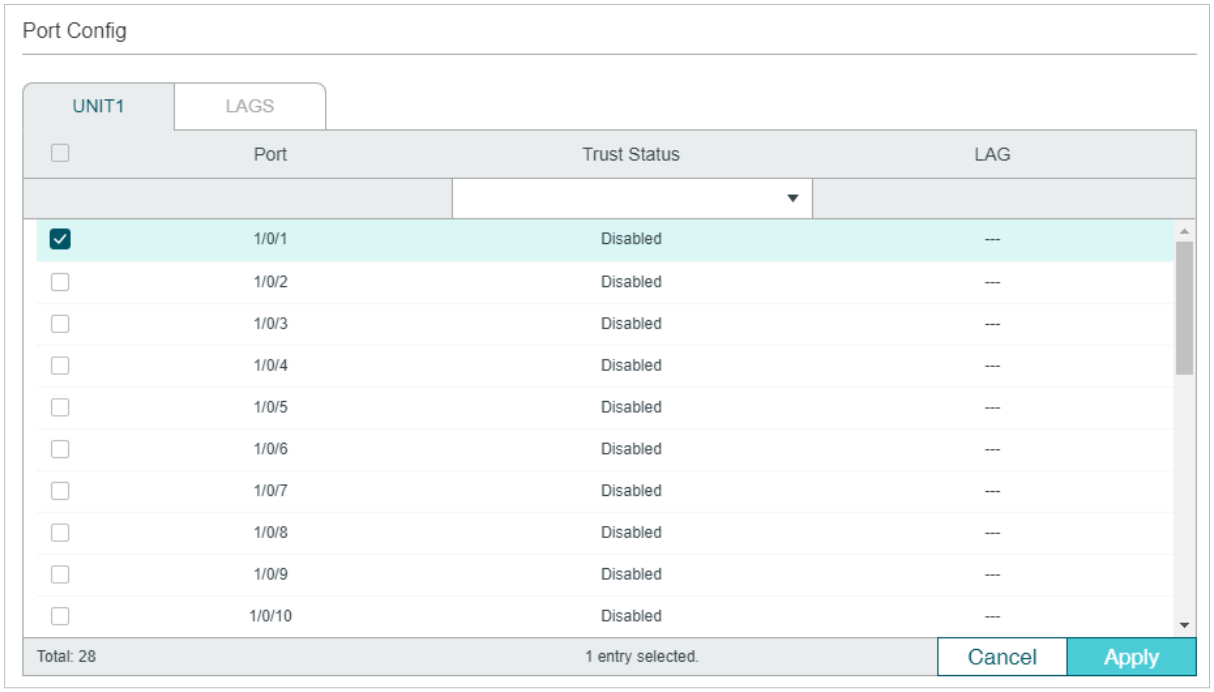
2) W sekcji **VLAN Config** włącz ND Detection w wybranych VLAN. Kliknij **Apply**.

VLAN ID	Informacja o VLAN ID.
Status	Włącz lub wyłącz ND Detection w sieci VLAN.
Log Status	Włącz lub wyłącz w sieci VLAN Log Feature (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ND będzie generował zapis.

3.1.3 Konfiguracja ND Detection na portach

Wybierz menu **SECURITY > IPv6 IMPB > ND Detection >Port Config**, aby załadować następując stronę.

Rys. 3-2 ND Detection na porcie



Aby skonfigurować ND Detection na portach, postępuj zgodnie z poniższymi krokami.

1) Wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry.

Port	Informacja o numerze portu.
Trust Status	Włącz lub wyłącz dla tego portu status portu zaufanego. Na porcie zaufanym pakiety ARP przekierowywane są bezpośrednio, bez sprawdzania. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.
LAG	Informacja o grupie LAG, do której należy port..

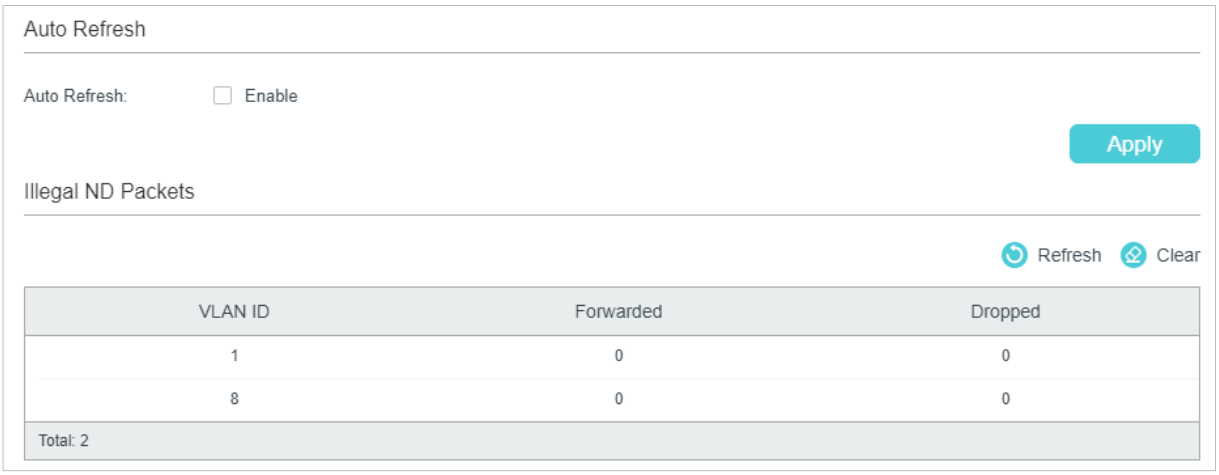
2) Kliknij **Apply**.

3.1.4 Wyświetlanie statystyk ND

Możesz zobaczyć liczbę nielegalnych pakietów ND otrzymanych przez każdy port. Ułatwi to zlokalizowanie przyczyny wadliwego działania sieci i podjęcie odpowiednich środków dla zabezpieczenia sieci.

Wybierz menu **SECURITY > IPv6 IMPB > ND Detection > ND Statistics**, aby załadować następującą stronę.

Rys. 3-3 Statystyki ND



W sekcji **Auto Refresh** możesz włączyć funkcję automatycznego odświeżania i wyznaczy odstęp czasu, w którym strona internetowa będzie automatycznie odświeżana.

W sekcji **Illegal ND Packet** możesz sprawdzić liczbę nielegalnych pakietów ND w każdej sieci VLAN.

VLAN ID	Informacja o VLAN ID.
Forwarded	Informacja o liczbie przekazanych pakietów ND w tej sieci VLAN.
Dropped	Informacja o liczbie odrzuconych pakietów ND w tej sieci VLAN.

3.2 Przez CLI

3.2.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzi konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

3.2.2 Włączanie funkcji ND Detection

Aby włączyć funkcję ND Detection, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**ipv6 nd detection** Włącz funkcję ND Detection globalnie.
Krok 3	**ipv6 nd detection vlan** *vlan-range* Włącz ND Detection w wybranej sieci VLAN. *vlan-range:* Wpisz zakres VLAN w formacie 1-3, 5.
Krok 4	**ipv6 nd detection vlan** *vlan-range* **logging** (Opcjonalnie) Włącz funkcję Log feature (funkcja rejestru zdarzeń, aby przełącznik po odrzuceniu nielegalnego pakietu ND generował zapis. *vlan-range:* Wpisz zakres VLAN w formacie 1-3, 5.
Krok 5	**show ipv6 nd detection** Sprawdź ustawienia globalne ND Detection.
Krok 6	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje globalne włączanie ND Detection we VLAN 1:

Switch#configure

Switch(config)#ipv6 nd detection

Switch(config)#ipv6 nd detection vlan 1

Switch(config)#show ipv6 nd detection

Global Status: Enable

Switch(config)#show ipv6 nd detection vlan

VID	Enable status	Log Status
1	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Konfiguracja funkcji ND Detection na portach

Aby skonfigurować funkcję ND Detection na portach, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ipv6 nd detection trust** Ustaw port jako zaufany, który nie będzie objęty działaniem funkcji ND Detection. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.
Krok 4	**show ipv6 nd detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Sprawdź globalną konfigurację ND Detection na porcie.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację portu 1/0/1 jako zaufanego.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 nd detection trust

Switch(config-if)#show ipv6 nd detection interface gigabitEthernet 1/0/1

Interface Trusted LAG

--------- ------- ---

Gi1/0/1 Enable N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Wyświetlanie statystyk ND

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji ,możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia.

show ipv6 nd detection statistics

Wyświetl statystyki ND dla każdego portu (liczba przekazanych pakietów ND, liczba odrzuconych pakietów ND).

4 Konfiguracja funkcji IPv6 Source Guard

Aby przeprowadzić konfigurację IPv6 Source Guard, postępuj zgodnie z poniższymi krokami:

1) Dodaj wpis wiązania IP-MAC.
2) Skonfiguruj funkcję IPv6 Source Guard.

4.1 Przez GUI

4.1.1 Dodawanie wpisów wiązania IPv6-MAC

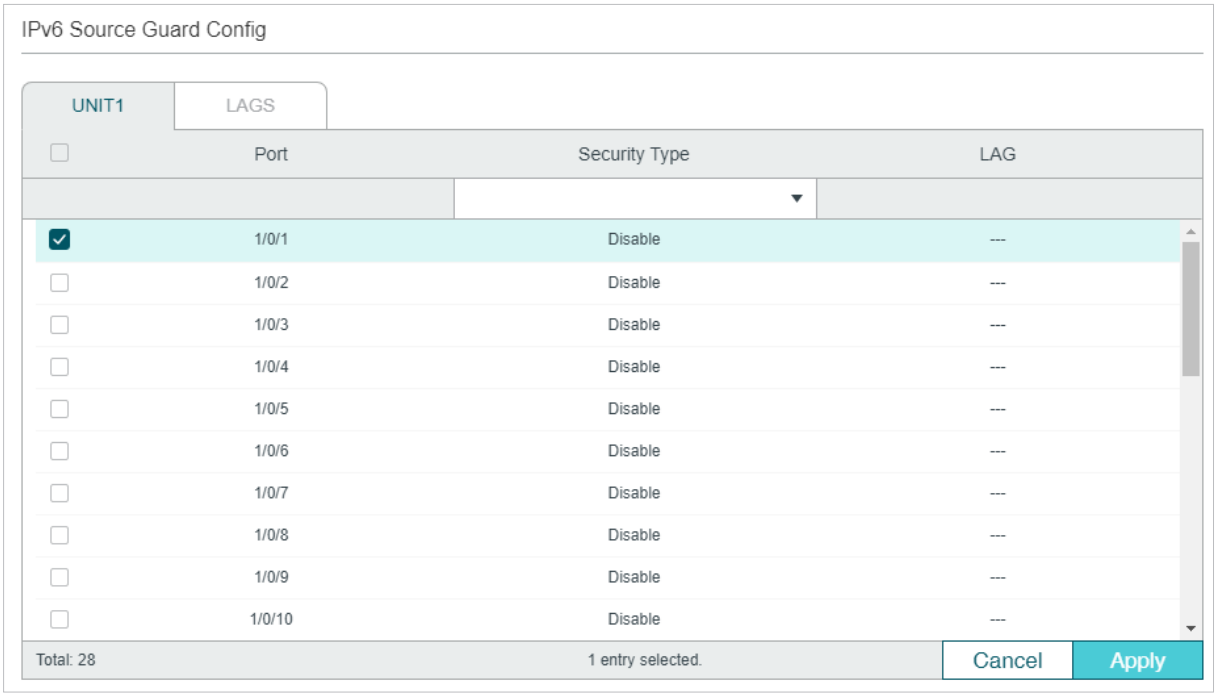
Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzi konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

4.1.2 Konfiguracja funkcji IPv6 Source Guard

Przed konfiguracją funkcji IPv6 Source Guard należy skonfigurować szablon (SDM template) jako EnterpriseV6.

Wybierz menu **SECURITY > IPv6 IMPB > IPv6 Source Guard**, aby załadować następującą stronę.

Rys. 4-1 Konfiguracja IPv6 Source Guard



Aby skonfigurować IPv6 Source Guard, postępuj zgodnie z poniższymi krokami:

1) Wybierz co najmniej jeden port i skonfiguruj typ ochrony.

Port	Informacja o numerze portu.
Security Type	Wybierz tryb ochrony na porcie dla pakietów IPv6. Dostępne są następujące opcje: **Disable (wył.):** Funkcja IP Source Guard jest wyłączona na porcie. **SIP+MAC**: Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane. **SIP**: Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6 i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane.
LAG	Informacja o grupie LAG, do której należy port.

2) Kliknij **Apply**.

4.2 Przez CLI

4.2.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzi konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

4.2.2 Konfiguracja funkcji IPv6 Source Guard

Przed konfiguracją funkcji IPv6 Source Guard należy skonfigurować szablon (SDM template) jako EnterpriseV6.

Aby skonfigurować IPv6 Source Guard, postępuj zgodnie z poniższymi krokami:

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Wejdź w tryb konfiguracji interfejsu.
Krok 3	**ipv6 verify source {** sipv6+mac | sipv6 **}** Włącz IP Source Guard dla pakietów IPv6. sipv6+mac*:* Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane.
Krok 4	**show ipv6 verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** Sprawdź konfigurację IP Source Guard dla pakietów IPv6.
Krok 5	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji IPv6 Source Guard na porcie 1/0/1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 verify source sipv6+mac

Switch(config-if)#show ipv6 verify source interface gigabitEthernet 1/0/1

Switch(config-if)#show ipv6 verify source interface gigabitEthernet 1/0/1

Port Security-Type LAG

---- ---------- ----

Gi1/0/1 SIPv6+MAC N/A

Switch(config-if)#end

Switch#copy running-config startup-config

Część 22

Konfiguracja filtrowania DHCP

ROZDZIAŁY

1 Konfiguracja filtrowania DHCPv4

Wykonaj poniższe kroki, aby przeprowadzić konfigurację filtrowania DHCPv4:

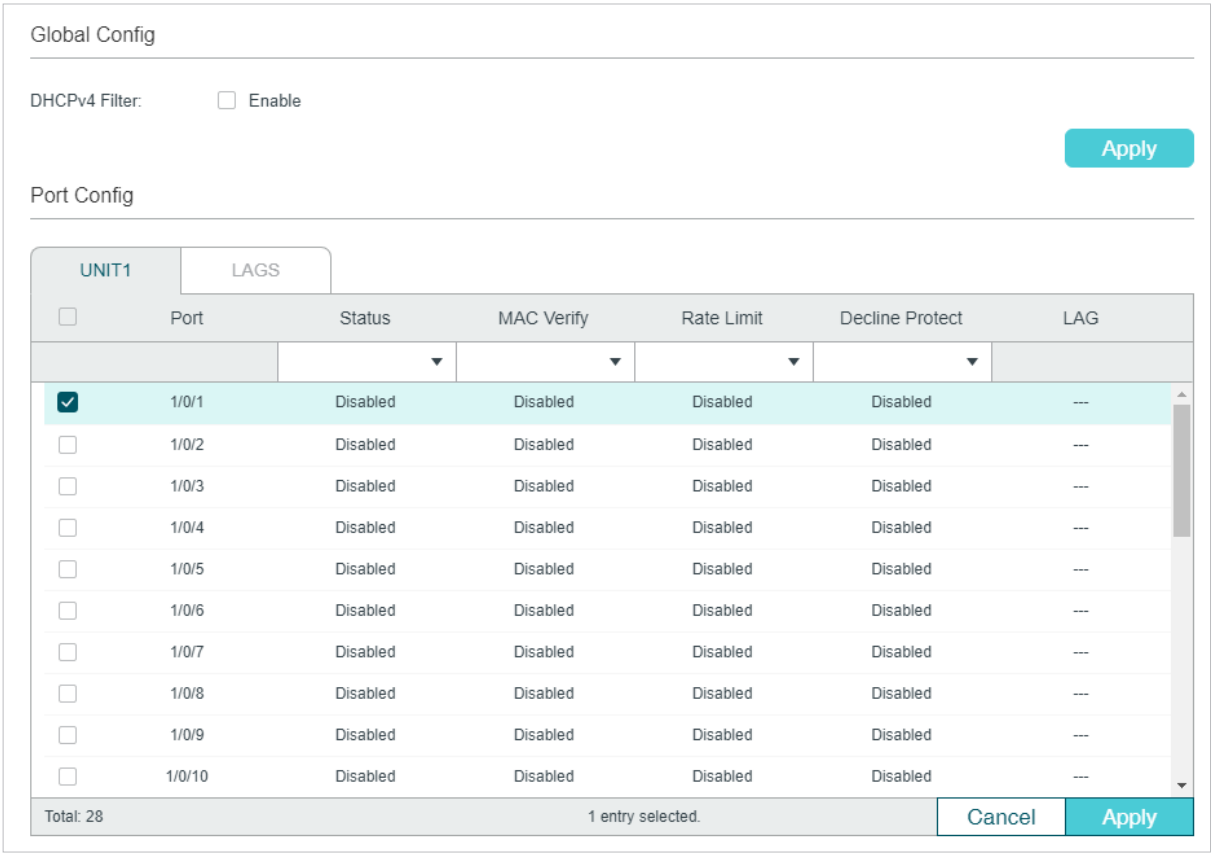
1) Skonfiguruj podstawowe parametry filtrowania DHCPv4.
2) Skonfiguruj legalne serwery DHCPv4.

1.1 Przez GUI

1.1.1 Konfiguracja podstawowych parametrów filtrowania DHCPv4

Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config,** aby wyświetlić poniższą stronę.

Rys. 1-1 Podstawowa konfiguracja filtrowania DHCPv4



Wykonaj poniższe kroki, aby skonfigurować podstawowe ustawienia filtrowania DHCPv4:

1) W sekcji **Global Config** włącz globalnie DHCPv4.
2) W sekcji **Port Config** wybierz jeden lub kilka portów i skonfiguruj ich parametry.

Port	Numer portu.

Status	Włącz lub wyłącz funkcję filtrowania DHCPv4 na porcie.
MAC Verify	Włącz lub wyłącz funkcję weryfikacji adresów MAC. Pakiet DHCPv4 składa się z dwóch pól, które zawierają adres MAC hosta. Weryfikacja adresów MAC polega na porównaniu dwóch pól pakietu DHCPv4 i odrzuceniu pakietu, których pola się od siebie różnią. Zapobiega to wyczerpywaniu się źródła adresów IP na serwerze DHCPv4 przez fałszywe adresy MAC.
Rate Limit	Zaznacz, aby włączyć funkcję ograniczania przesyłu pakietów i ustalić maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.
Decline Protect	Zaznacz, aby włączyć tę funkcję i ustalić maksymalną liczbę odrzuconych pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.
LAG	LAG, do którego należy port.

3) Kliknij **Apply**.

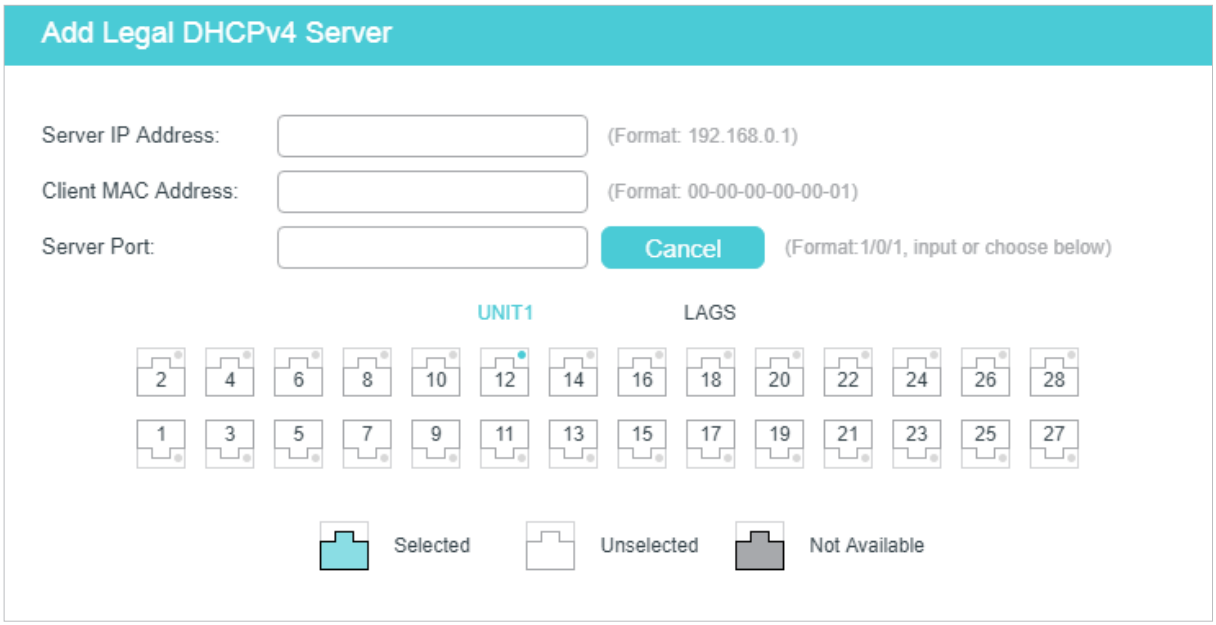
Uwaga:

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

1.1.2 Konfiguracja legalnych serwerów DHCPv4

Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 1-2 Dodawanie legalnego serwera DHCPv4



Wykonaj poniższe kroki, aby dodać legalny serwer DHCPv4:

1) Skonfiguruj poniższe parametry:

Server IP Address	Podaj adres IP legalnego serwera DHCPv4.
Client MAC Address	(Opcjonalnie) Podaj adres MAC klienta DHCP. Pozostawienie tego pola pustego oznacza wybór wszystkich klientów DHCP.
Server Port	Wybierz port, z którym legalny serwer DHCPv4 jest połączony.

2) Kliknij **Create**.

1.2 Przez CLI

1.2.1 Konfiguracja podstawowych parametrów filtrowania DHCPv4

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry filtrowania DHCPv4:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip dhcp filter** Włącz globalnie filtrowanie DHCPv4.
Krok 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 4	**ip dhcp filter** Włącz filtrowanie DHCPv4 na porcie.
Krok 5	**ip dhcp filter mac-verify** Włącz funkcję weryfikacji adresów MAC. Pakiet DHCPv4 składa się z dwóch pól, które zawierają adres MAC hosta. Weryfikacja adresów MAC polega na porównaniu dwóch pól pakietu DHCPv4 i odrzuceniu pakietu, których pola się od siebie różnią. Zapobiega to wyczerpywaniu się źródła adresów IP na serwerze DHCPv4 przez fałszywe adresy MAC.
Krok 6	**ip dhcp filter limit rate** *value* Włącz funkcję ograniczania przesyłu pakietów i ustal maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane. *value:* Podaj wartość limitu przesyłanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.

Krok 7	**ip dhcp filter decline rate** *value* Włącz funkcję limitu odrzucania pakietów i ustal maksymalną liczbę odrzuconych pakietów, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane. *value:* Podaj wartość limitu odrzucanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.
Krok 8	**show ip dhcp filter** Przejrzyj globalną konfigurację filtrowania DHCPv4.
Krok 9	**show ip dhcp filter interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*] Przejrzyj konfigurację filtrowania DHCPv4 na porcie.
Krok 10	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 11	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania filtrowania DHCPv4, włączania filtrowania DHCPv4, funkcji weryfikacji adresów MAC, ustawiania limitu przesyłanych pakietów jako 10 p/s i odrzucanych pakietów jako 20 p/s na porcie 1/0/1:

Switch#configure

Switch(config)#ip dhcp filter

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp filter

Switch(config-if)#ip dhcp filter mac-verify

Switch(config-if)#ip dhcp filter limit rate 10

Switch(config-if)#ip dhcp filter decline rate 20

Switch(config-if)##show ip dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface state MAC-Verify Limit-Rate Dec-rate LAG

| --- | --- | --- | --- | --- | --- |
| Gi1/0/1 | Enable | Enable | 10 | 20 | N/A |

Switch(config-if)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja legalnych serwerów DHCPv4

Wykonaj poniższe kroki, aby skonfigurować legalne serwery DHCPv4:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip dhcp filter server permit-entry server-ip** *ipAddr* **client-mac** macAddr **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Utwórz wpis dla legalnego serwera DHCPv4. *ipAddr*: Podaj adres IP legalnego serwera DHCPv4. macAddr : Podaj adres MAC klienta DHCP. Wartość “all” oznacza wszystkie adresy MAC klientów. *port-list* | *port-channel-id*: Określ port, z którym legalny serwer DHCPv4 jest połączony.
Krok 3	**show ip dhcp filter server permit-entry** Przejrzyj ustawienia legalnego serwera DHCPv4.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu dla legalnego serwera DHCPv4, którego adres IP wynosi 192.168.0.100, a numerem połączonego portu jest 1/0/1 bez przydzielonego adresu MAC klienta:

Switch#configure

Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface gigabitEthernet** 1/0/1

Switch(config)#show ip dhcp filter server permit-entry

Server IP	Client MAC	Interface
192.168.0.100	all	Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

2 Konfiguracja filtrowania DHCPv6

Wykonaj poniższe kroki, aby przeprowadzić konfigurację filtrowania DHCPv6:

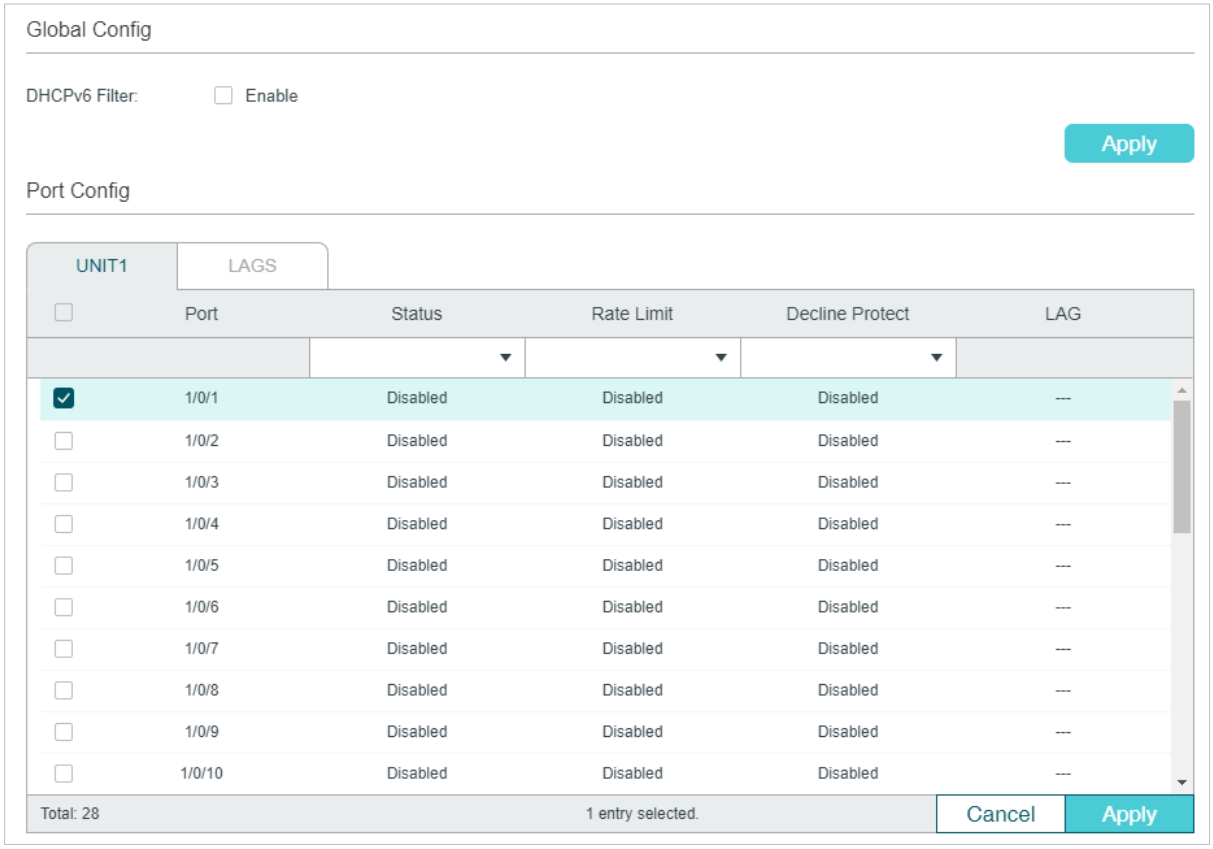
1) Skonfiguruj podstawowe parametry filtrowania DHCPv6.
2) Skonfiguruj legalne serwery DHCPv6.

2.1 Przez GUI

2.1.1 Konfiguracja podstawowych parametrów filtrowania DHCPv6

Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config,** aby wyświetlić poniższą stronę.

Rys. 2-1 Podstawowa konfiguracja filtrowania DHCPv6



Wykonaj poniższe kroki, aby skonfigurować podstawowe ustawienia filtrowania DHCPv6:

3) W sekcji **Global Config** włącz globalnie DHCPv6.
4) W sekcji **Port Config** wybierz jeden lub kilka portów i skonfiguruj ich parametry.

Port	Numer portu.

Status	Włącz lub wyłącz funkcję filtrowania DHCPv6 na porcie.
Rate Limit	Zaznacz, aby włączyć funkcję ograniczania przesyłu pakietów i ustalić maksymalną liczbę pakietów DHCPv6, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.
Decline Protect	Zaznacz, aby włączyć tę funkcję i ustalić maksymalną liczbę odrzuconych pakietów DHCPv6, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.
LAG	LAG, do którego należy port.

5) Kliknij **Apply**.

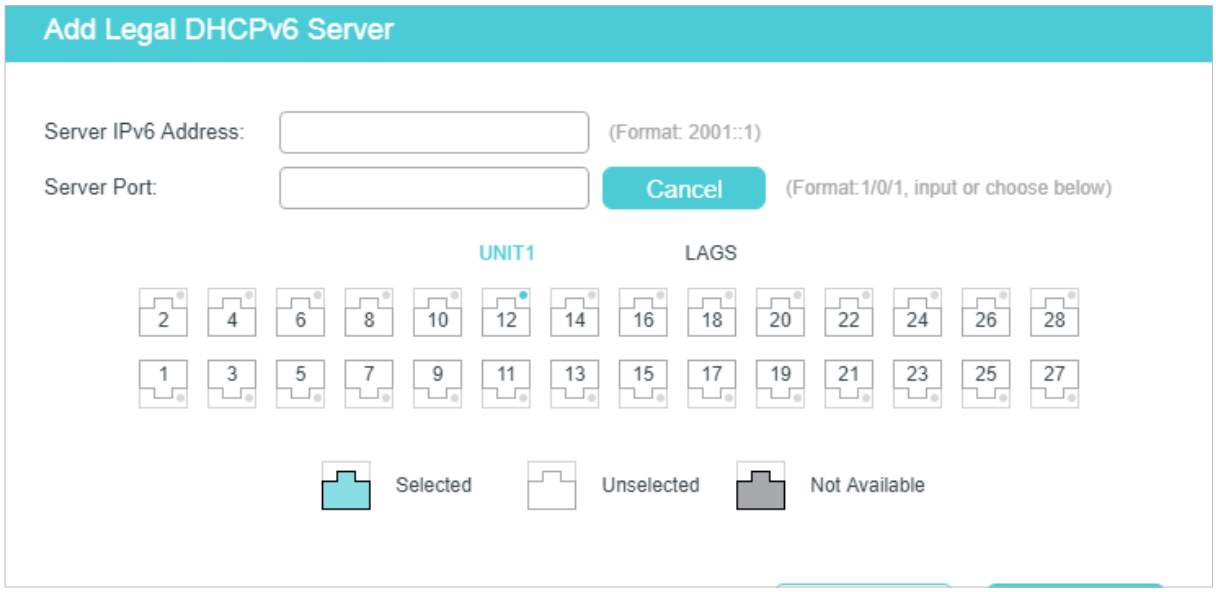
Note:

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

2.1.2 Konfiguracja legalnych serwerów DHCPv6

Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 2-2 Dodawanie legalnego serwera DHCPv6



Wykonaj poniższe kroki, aby dodać legalny serwer DHCPv6:

1) Skonfiguruj poniższe parametry:

Server IPv6 Address	Podaj adres IP legalnego serwera DHCPv6.
Server Port	Wybierz port, z którym legalny serwer DHCPv6 jest połączony.

2) Kliknij **Create**.

2.2 Przez CLI

2.2.1 Konfiguracja podstawowych parametrów filtrowania DHCPv6

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry filtrowania DHCPv6:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ipv6 dhcp filter** Włącz filtrowanie DHCPv6 globalnie.
Krok 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Uruchom tryb konfiguracji interfejsu.
Krok 4	**ipv6 dhcp filter** Włącz filtrowanie DHCPv6 na porcie.
Krok 5	**ipv6 dhcp filter limit rate** *value* Włącz funkcję ograniczania przesyłu pakietów i ustal maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane. *value:* Podaj wartość limitu przesyłanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.
Krok 6	**ipv6 dhcp filter decline rate** *value* Włącz funkcję limitu odrzucania pakietów i ustal maksymalną liczbę odrzuconych pakietów, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane. *value:* Podaj wartość limitu odrzucanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.
Krok 7	**show ipv6 dhcp filter** Przejrzyj globalną konfigurację filtrowania DHCPv6.
Krok 8	**show ipv6 dhcp filter interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Przejrzyj konfigurację filtrowania DHCPv6 na porcie.
Krok 9	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 10	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Uwaga:

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania filtrowania DHCPv6, włączania filtrowania DHCPv6, ustawiania limitu przesyłanych pakietów jako 10 p/s i odrzucanych pakietów jako 20 p/s na porcie 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 dhcp filter

Switch(config-if)#ipv6 dhcp filter limit rate 10

Switch(config-if)#ipv6 dhcp filter decline rate 20

Switch(config-if)##show ipv6 dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface	state	Limit-Rate	Dec-rate	LAG
---	---	---	---	---
Gi1/0/1	Enable	10	20	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Konfiguracja legalnych serwerów DHCPv6

Wykonaj poniższe kroki, aby skonfigurować legalne serwery DHCPv6:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**ipv6 dhcp filter server permit-entry server-ip** *ipAddr* **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Utwórz wpis dla legalnego serwera DHCPv6. *ipAddr*: Podaj adres IP legalnego serwera DHCPv6. *port-list* | *port-channel-id*: Określ port, z którym legalny serwer DHCPv6 jest połączony.
Krok 3	**show ip dhcp filter server permit-entry** Przejrzyj ustawienia legalnego serwera DHCPv6.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu dla legalnego serwera DHCPv4, którego adresem IP jest 2001::54, a numerem połączonego portu 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 **interface gigabitEthernet** 1/0/1

Switch(config)#show ipv6 dhcp filter server permit-entry

Server IP Interface

---------- ---------

2001::54 Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

Część 23

Konfiguracja DoS Defend

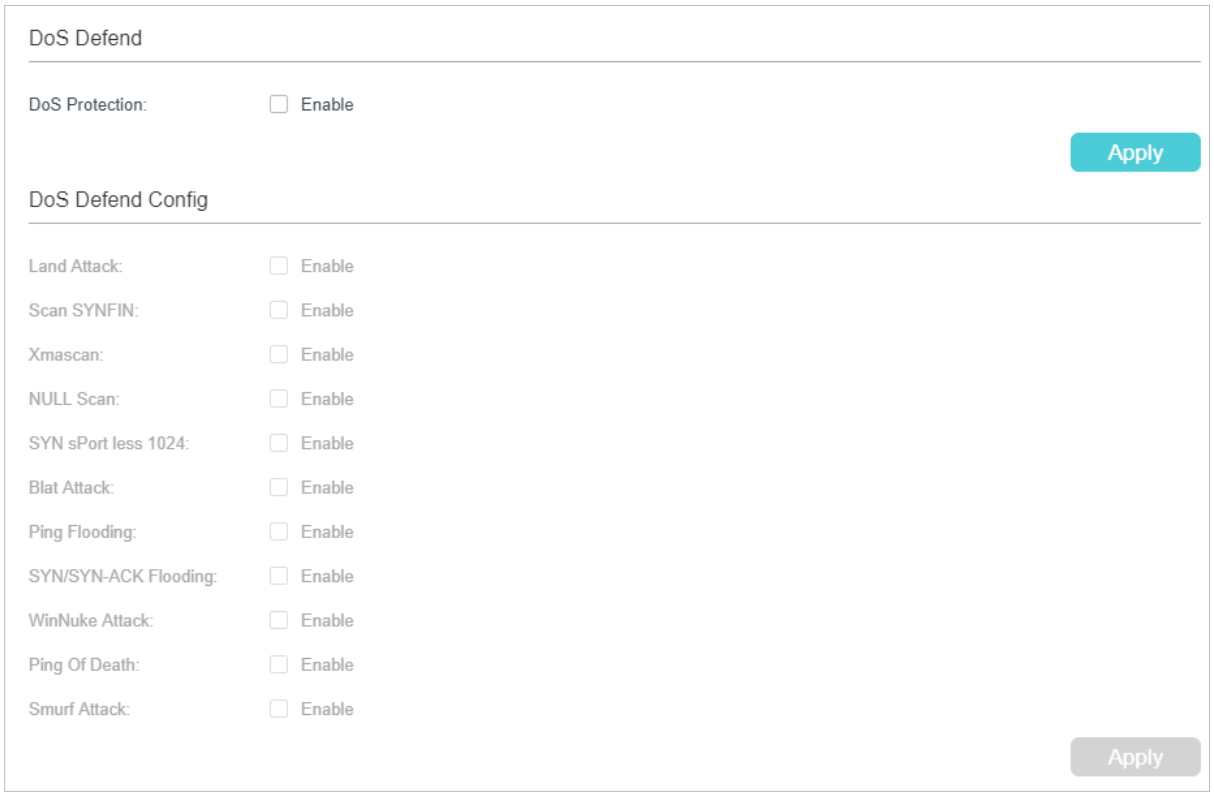
ROZDZIAŁY

1 Konfiguracja ochrony przed atakami DoS

1.1 Przez GUI

Wybierz z menu **SECURITY > DoS Defend**, aby wyświetlić poniższą stronę.

Rys. 1-1 Ochrona przed atakami DoS



Wykonaj poniższe kroki, aby skonfigurować Ochronę przed atakami DoS:

1) W sekcji **DoS Defend** włącz DoS Protection i kliknij **Apply**.
2) W sekcji **DoS Defend Config** wybierz jeden lub kilka typów ochrony, stosownie do wymagań, i kliknij **Apply**. Poniższa tabela zawiera wszystkie typy ataków DoS.

Land Attack	Strona atakująca wysyła określony fałszywy pakiet SYN (synchroniczny) do hosta docelowego. Ponieważ zarówno źródłowy adres IP, jak i docelowy adres IP pakietu SYN mają pełnić rolę adresu IP hosta, host bezskutecznie będzie starać się nawiązać połączenie ze stroną atakującą.
Scan SYNFIN	Strona atakująca wysyła pakiet z ustawioną flagą SYN oraz flagą FIN o wartości 1. Flaga SYN wysyła do hosta żądanie nawiązania połączenia, natomiast flaga FIN żąda przerwania połączenia. Zatem pakiet tego typu jest nielegalny.
Xmascan	Strona atakująca wysyła nielegalny pakiet z indeksem TCP oraz flagami FIN, URG i PSH o wartości 1.

NULL Scan	Strona atakująca wysyła nielegalny pakiet ze swoim indeksem TCP i wszystkimi polami kontrolnymi ustawionymi do wartości 0. Podczas trwającego połączenia TCP oraz transmisji danych wszystkie pola kontrolne o wartości 0 są klasyfikowane jako nielegalne.
SYN sPort less 1024	Strona atakująca wysyła nielegalne pakiety z ustawionymi flagami TCP SYN o wartości 1 oraz portem źródłowym o numerze niższym niż 1024.
Blat Attack	Strona atakująca wysyła nielegalny pakiet z tym samym portem źródłowym i docelowym w warstwie 4 oraz flagą URG o wartości 1. Podobnie jak w przypadku Land Attack, działanie systemu atakowanego hosta jest ograniczone, ponieważ host bezskutecznie stara się nawiązać połączenie ze stroną atakującą.
Ping Flooding	Strona atakująca przeciąża system docelowy wysyłanymi pakietami ping, tworząc burzę broadcastową, która uniemożliwia systemowi poprawną komunikację.
SYN/SYN-ACK Flooding	Strona atakująca korzysta ze sfałszowanego adresu IP do wysyłania pakietów żądań TCP do serwera. Po otrzymaniu pakietów żądań serwer odpowiada poprzez pakiety SYN-ACK. Ze względu na to, że adres IP jest sfałszowany, serwer nie otrzyma żadnej odpowiedzi. Dlatego serwer będzie kontynuować wysyłanie pakietów SYN-ACK. Jeżeli strona atakująca przeciąży zasoby sieciowe wysyłaniem sfałszowanych pakietów żądań, także żądania legalnych klientów będą odrzucane.
WinNuke Attack	Ze względu na to, że system operacyjny z błędami nie może poprawnie przetwarzać flagi URG (Urgent Pointer) pakietów TCP, strona atakująca wysyła ten typ pakietów do portu 139 (NetBIOS) hosta z błędami systemu operacyjnego, co skutkuje zawieszeniem systemu i wyświetleniem niebieskiego ekranu.
Ping of Death	Strona atakująca wysyła nieprawidłowe pakiety ping, większe niż 65535 bajtów, aby spowodować awarię systemu komputera docelowego.
Smurf Attack	Smurf attack to rozproszony atak DoS, w którym duża liczba pakietów ICMP (Internet Control Message Protocol) ze sfałszowanym adresem IP jest przesyłana na adres rozgłoszeniowy sieci. Większość urządzeń w sieci będzie domyślnie wysyłała odpowiedzi na źródłowy adres IP atakowanej ofiary. Jeżeli liczba urządzeń, które wysyłają odpowiedzi na te pakiety jest duża, łącze atakowanego komputera zostanie przeciążone.

3) Kliknij **Apply**.

1.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować ochronę przed atakami DoS:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**ip dos-prevent** Włącz globalnie funkcję ochrony przed atakami DoS.

Krok 3 **ip dos-prevent type {** land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf **}**

Skonfiguruj jeden lub kilka typów ochrony, stosownie do wymagań. Poniżej znajdują się objaśnienia wszystkich typów ataków DoS.

land: Strona atakująca wysyła określony fałszywy pakiet SYN (synchroniczny) do hosta docelowego. Ponieważ zarówno źródłowy adres IP, jak i docelowy adres IP pakietu SYN mają pełnić rolę adresu IP hosta, host bezskutecznie będzie starać się nawiązać połączenie ze stroną atakującą.

scan-synfin: Strona atakująca wysyła pakiet z ustawioną flagą SYN oraz flagą FIN o wartości 1. Flaga SYN wysyła do hosta żądanie nawiązania połączenia, natomiast flaga FIN żąda przerwania połączenia. Zatem pakiet tego typu jest nielegalny.

xma-scan: Strona atakująca wysyła nielegalny pakiet z indeksem TCP oraz flagami FIN, URG i PSH o wartości 1.

null-scan: Strona atakująca wysyła nielegalny pakiet ze swoim indeksem TCP i wszystkimi polami kontrolnymi ustawionymi do wartości 0. Podczas trwającego połączenia TCP oraz transmisji danych wszystkie pola kontrolne o wartości 0 są klasyfikowane jako nielegalne.

port-less-1024: Strona atakująca wysyła nielegalne pakiety z ustawionymi flagami TCP SYN o wartości 1 oraz portem źródłowym o numerze niższym niż 1024.

blat: Strona atakująca wysyła nielegalny pakiet z tym samym portem źródłowym i docelowym w warstwie 4 oraz flagą URG o wartości 1. Podobnie jak w przypadku Land Attack, działanie systemu atakowanego hosta jest ograniczone, ponieważ host bezskutecznie stara się nawiązać połączenie ze stroną atakującą.

ping-flood: Strona atakująca przeciąża system docelowy wysyłanymi pakietami ping, tworząc burzę broadcastową, która uniemożliwia systemowi poprawną komunikację.

syn-flood: Strona atakująca korzysta ze sfałszowanego adresu IP do wysyłania pakietów żądań TCP do serwera. Po otrzymaniu pakietów żądań serwer odpowiada poprzez pakiety SYN-ACK. Adres IP jest sfałszowany, stąd serwer nie otrzyma żadnej odpowiedzi i serwer będzie kontynuować wysyłanie pakietów SYN-ACK. Jeżeli strona atakująca przeciąży zasoby sieciowe fałszywymi pakietami żądań, żądania legalnych klientów będą odrzucane.

win-nuke: Ze względu na to, że system operacyjny z błędami nie może poprawnie przetwarzać flagi URG (Urgent Pointer) pakietów TCP, strona atakująca wysyła ten typ pakietów do portu 139 (NetBIOS) hosta z błędami systemu operacyjnego, co skutkuje zawieszeniem systemu i wyświetleniem niebieskiego ekranu.

ping-of-death: Strona atakująca wysyła nieprawidłowe pakiety ping, większe niż 65535 bajtów, aby spowodować awarię systemu komputera docelowego.

smurf: Smurf attack to rozproszony atak DoS, w którym duża liczba pakietów ICMP (Internet Control Message Protocol) ze sfałszowanym adresem IP jest przesyłana na adres rozgłoszeniowy sieci. Większość urządzeń w sieci będzie domyślnie wysyłała odpowiedzi na źródłowy adres IP atakowanej ofiary. Jeżeli liczba urządzeń, które wysyłają odpowiedzi na te pakiety jest duża, łącze atakowanego komputera zostanie przeciążone.

Krok 4 **show ip dos-prevent**

Przejrzyj ustawienia ochrony DoS.

Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania typu ochrony DoS o nazwie land:

Switch#configure

Switch(config)#ip dos-prevent

Switch(config)#ip dos-prevent type land

Switch(config)#show ip dos-prevent

DoS Prevention State: Enabled

Type Status

---- ------

Land Attack Enabled

Scan SYNFIN Disabled

Xmascan Disabled

NULL Scan Disabled

SYN sPort less 1024 Disabled

Blat Attack Disabled

Ping Flooding Disabled

SYN/SYN-ACK Flooding Disabled

WinNuke Attack Disabled

Smurf Attack Disabled

Ping Of Death Disabled

Switch(config)#end

Switch#copy running-config startup-config

Część 24

Monitorowanie systemu

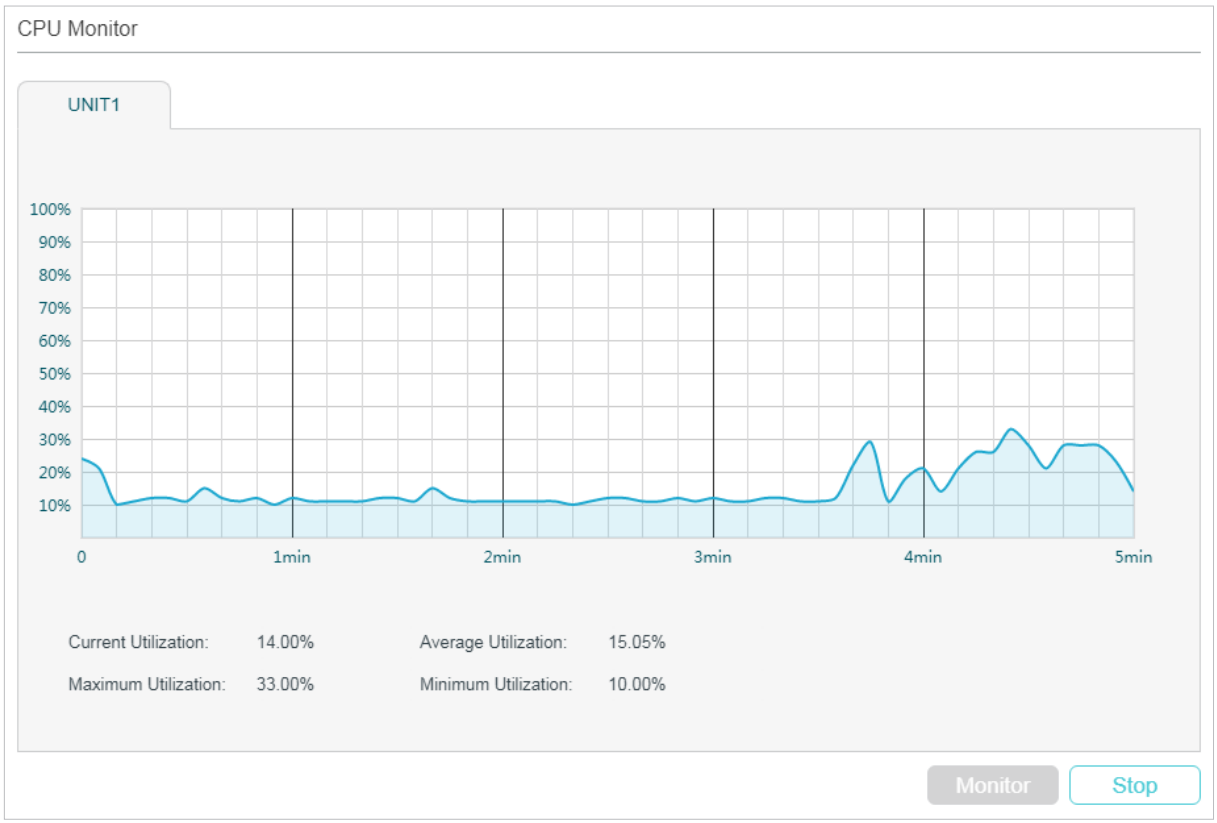
ROZDZIAŁY

1 Monitorowanie procesora

1.1 Przez GUI

Wybierz z menu **MAINTENANCE > System Monitor > CPU Monitor**, aby wyświetlić poniższą stronę.

Rys. 1-1 Monitorowanie procesora



Kliknij **Monitor**, aby włączyć na przełączniku monitorowanie i wyświetlanie co 5 sekund stopnia zużycia procesora.

1.2 Przez CLI

Korzystając z poniższego polecenia w trybie uprzywilejowanym (privileged EXEC mode) lub w każdym innym trybie konfiguracji możesz wyświetlić zużycie procesora:

show cpu-utilization

Zobacz zużycie procesora przełącznika sprzed ostatnich 5 sekund, 1 minuty i 5 minut.

Poniższy schemat przedstawia przykładowy sposób monitorowania procesora:

Switch#show cpu-utilization

Unit | CPU Utilization

No. | Five-Seconds One-Minute Five-Minutes

------+----------

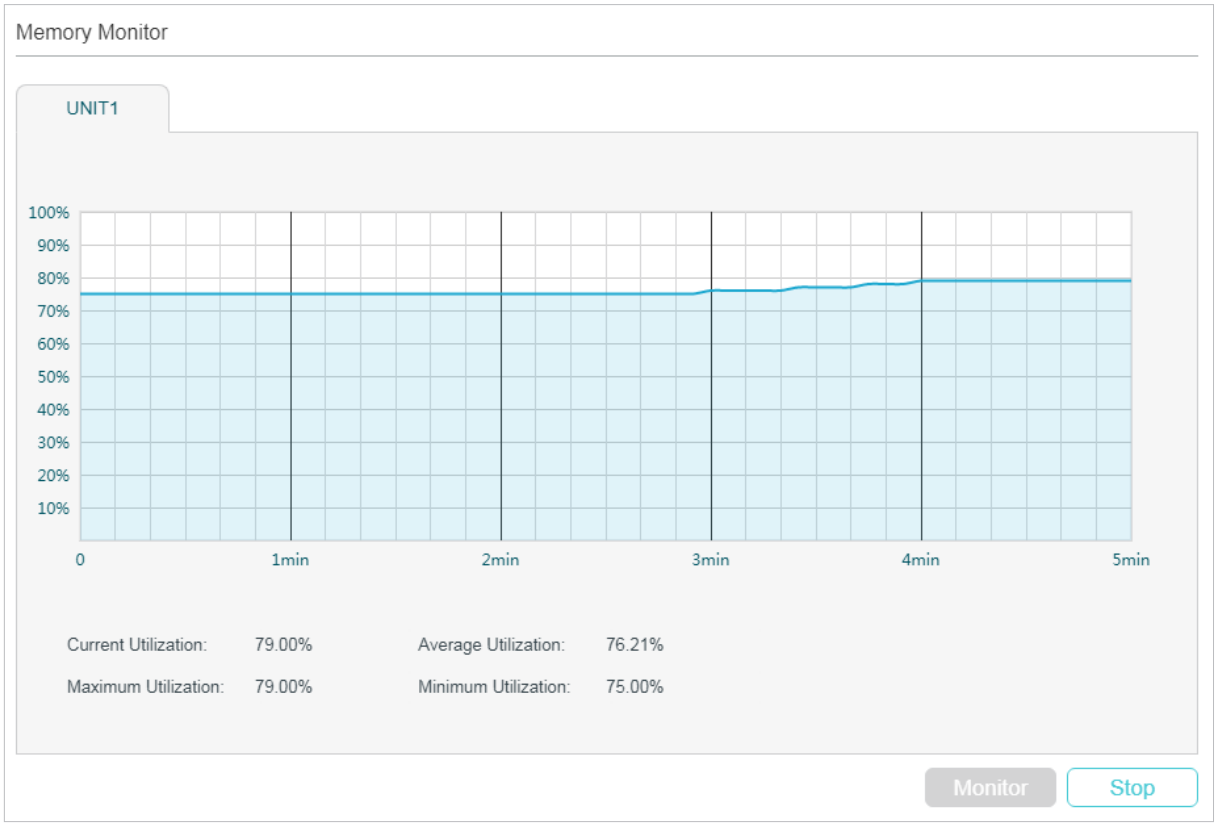
1 | 13% 13% 13%

2 Monitorowanie pamięci

2.1 Przez GUI

Wybierz z menu **MAINTENANCE > System Monitor > Memory Monitor**, aby wyświetlić poniższą stronę.

Rys. 2-1 Monitorowanie pamięci



Kliknij **Monitor,** aby włączyć na przełączniku monitorowanie i wyświetlanie co 5 sekund stopnia zużycia pamięci.

2.2 Przez CLI

Korzystając z poniższego polecenia w trybie uprzywilejowanym (privileged EXEC mode) lub w każdym innym trybie konfiguracji możesz wyświetlić zużycie pamięci:

show memory-utilization

Zobacz aktualne zużycie pamięci przełącznika.

Poniższy schemat przedstawia przykładowy sposób monitorowania pamięci:

Switch#show memory-utilization

```
Unit   |   Current Memory Utilization
------+--------------------------
1      |   74%
```

Część 25

Monitorowanie ruchu

ROZDZIAŁY

1 Monitorowanie ruchu

Funkcja monitorowania ruchu umożliwia analizę ruchu na każdym porcie poprzez dostęp do dokładnych zestawień i statystyk ruchu danych.

1.1 Przez GUI

Wybierz z menu **MAINTENANCE > Traffic Monitor,** aby wyświetlić poniższą stronę.

Rys. 1-1 Podsumowanie ruchu danych

Wykonaj poniższe kroki, aby zobaczyć zestawienia ruchu dla każdego portu:

1) Włącz automatyczne odświeżanie (**Auto Refresh**) lub kliknij **Refresh**, aby na bieżąco analizować zestawienia ruchu.

Auto Refresh:	Włączenie tej opcji umożliwia przełącznikowi automatyczne odświeżanie zestawień ruchu.
Refresh Interval:	Podaj interwał odświeżania zestawień ruchu przez przełącznik.

2) W sekcji **Traffic Summary** kliknij **UNIT1,** aby zobaczyć informacje o portach fizycznych, a następnie kliknij **LAGS**, aby wyświetlić informacje o grupach agregacji łączy (LAG).

Packets Rx:	Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane.
Packets Tx:	Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane.
Octets Rx:	Liczba oktetów odebranych na porcie. Błędne oktety są uwzględniane.
Octets Tx:	Liczba oktetów przesyłanych na porcie. Błędne oktety są uwzględniane.

Aby wyświetlić szczegółowe statystyki danych dla portu, kliknij **Statistics** po prawej stronie pozycji.

Rys. 1-2 Statystyki ruchu

Received:	Szczegółowe informacje o odebranych pakietach. Broadcast: Liczba prawidłowych pakietów broadcast odebranych na porcie. Błędne ramki nie są uwzględniane. Multicast: Liczba prawidłowych pakietów multicast odebranych na porcie. Błędne ramki nie są uwzględniane. Unicast: Liczba prawidłowych pakietów unicast odebranych na porcie. Błędne ramki nie są uwzględniane. Jumbo: Liczba prawidłowych pakietów jumbo odebranych na porcie. Błędne ramki nie są uwzględniane. Alignment Errors: Liczba odebranych pakietów, których FCS (Frame Check Sequence) ma niezintegrowany oktet (Alignment Error). Rozmiar pakietu musi mieścić się w przedziale 64 - 1518 bajtów. Undersize Packets: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych), krótszych niż 64 bajty. 64-Octets Packets: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych) o rozmiarze 64 bajtów. 65-to-127-Octects Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 65 do 127 bajtów długości. 128-to-255-Octects Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 128 do 255 bajtów długości. 256-to-511-Octects Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 256 do 511 bajtów długości. 512-to-1023-Octects Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości. 1023-to-1518-Octects Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości. Pkts: Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane. Bytes: Liczba bajtów odebranych na porcie. Błędne pakiety nie są uwzględniane.
Sent:	Szczegółowe informacje o pakietach wysłanych. Broadcast: Liczba prawidłowych pakietów broadcast przesłanych na porcie. Błędne ramki nie są uwzględniane. Multicast: Liczba prawidłowych pakietów multicast przesłanych na porcie. Błędne ramki nie są uwzględniane. Unicast: Liczba prawidłowych pakietów unicast przesłanych na porcie. Błędne ramki nie są uwzględniane. Pkts: Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane. Bytes: Liczba bajtów przesłanych na porcie. Błędne pakiety nie są uwzględniane. Collisions: Liczba kolizji na porcie w trybie półdupleksu podczas przesyłania pakietów.

1.2 Przez CLI

Korzystając z poniższego polecenia w trybie uprzywilejowanym (privileged EXEC mode) lub w każdym innym trybie konfiguracji możesz wyświetlić informacje o ruchu na każdym porcie lub w grupie agregacji łączy (LAG):

show interface counters [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]**

port-channel-id : Numer grupy LAG.

Jeżeli nie podasz żadnego numeru portu, ani numeru grupy, wyświetlą się informacje o wszystkich portach i grupach.

Te informacje uwzględniają:

Tx Collisions: Liczba kolizji na porcie podczas przesyłania pakietów.

Tx Ucast / Tx Mcast / Tx Bcast / Tx Jumbo: Liczba prawidłowych pakietów unicast / multicast / broadcast / jumbo przesłanych na porcie. Błędne ramki nie są uwzględniane.

Tx Pkts: Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane.

Tx Bytes: Liczba bajtów przesłanych na porcie. Błędne pakiety nie są uwzględniane.

Rx Ucast / Rx Mcast / Rx Bcast / Rx Liczba prawidłowych pakietów unicast / multicast / broadcast / jumbo odebranych na porcie. Błędne ramki nie są uwzględniane.

Rx Alignment: Liczba odebranych pakietów, których FCS (Frame Check Sequence) ma niezintegrowany oktet (Alignment Error). Rozmiar pakietu musi mieścić się w przedziale 64 - 1518 bajtów.

Rx UnderSize: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych), krótszych niż 64 bajty.

Rx 64Pkts: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych) o rozmiarze 64 bajtów.

Rx 65-127Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 65 do 127 bajtów długości.

Rx 128-255Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 128 do 255 bajtów długości.

Rx 256-511Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 256 do 511 bajtów długości.

Rx 512-1023Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.

Rx 1024-1518Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.

Rx Pkts: Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane.

Rx Bytes: Liczba bajtów odebranych na porcie. Błędne pakiety nie są uwzględniane.

Część 26

Mirroring ruchu

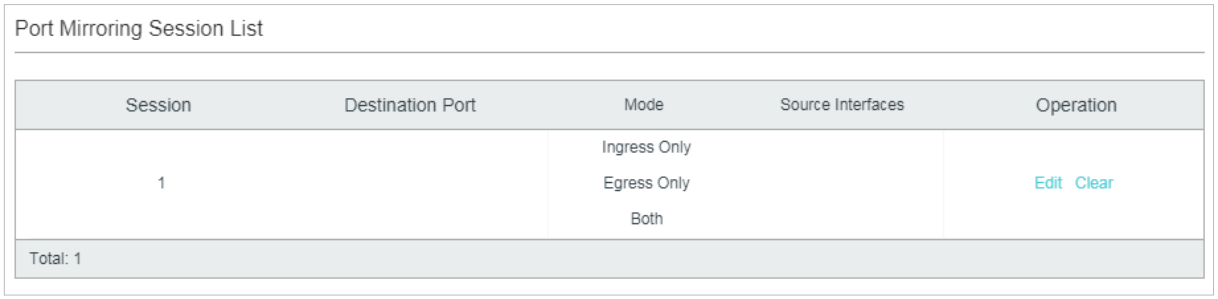
ROZDZIAŁY

1 Mirroring

1.1 Przez GUI

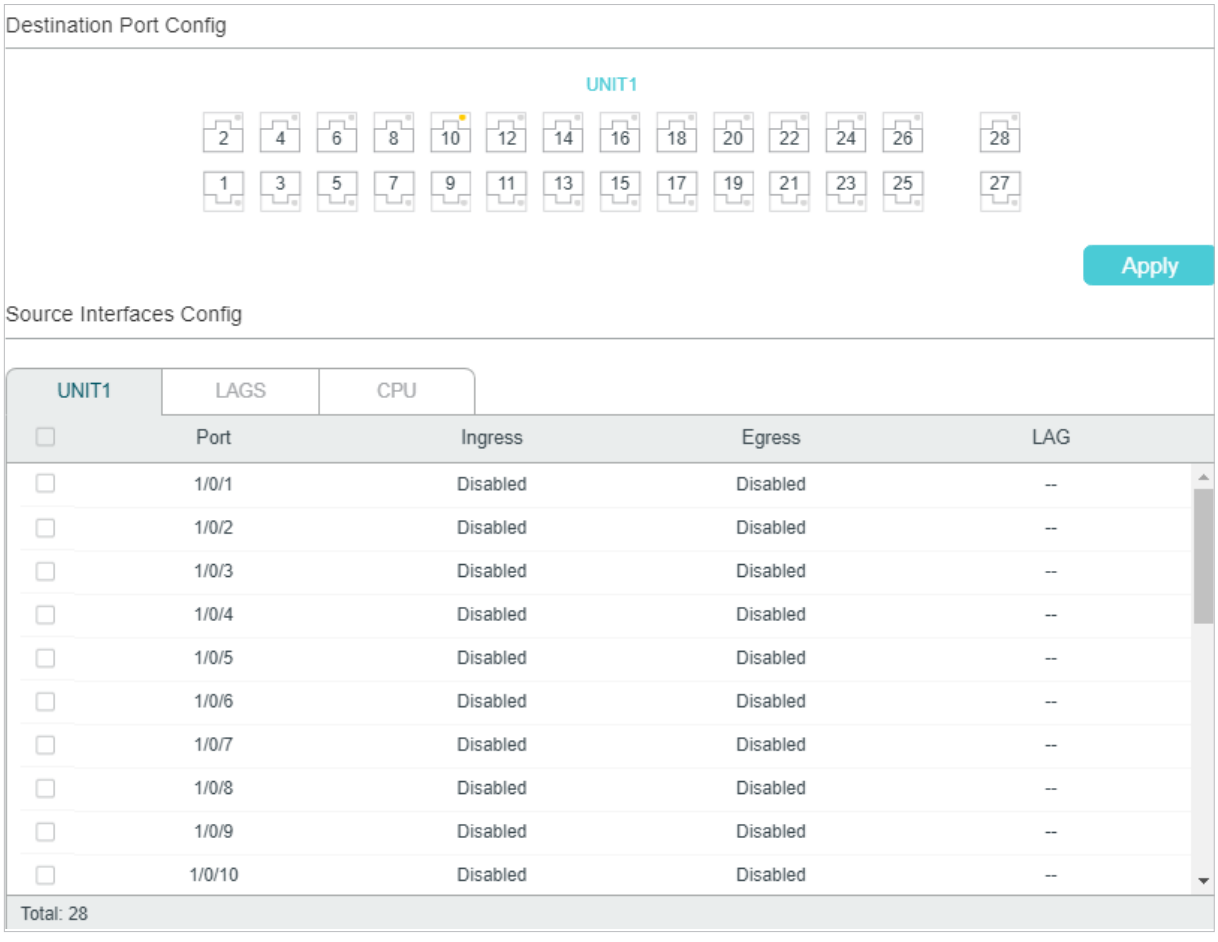
Wybierz z menu **MAINTENANCE > Mirroring**, aby wyświetlić poniższą stronę.

Rys. 1-1 Lista sesji Port Mirroring



Powyższy rysunek przedstawia sesję mirroring. Nie można utworzyć żadnej dodatkowej sesji. Kliknij **Edit,** aby skonfigurować tą sesję mirroring tak jak na poniższej stronie.

Rys. 1-2 Konfiguracja sesji mirroring



Wykonaj poniższe kroki, aby skonfigurować sesję mirroring:

1) W sekcji **Destination Port Config** wybierz port docelowy dla sesji mirroring i kliknij **Apply**.
2) W sekcji **Source Interfaces Config** wybierz interfejsy źródłowe i kliknij **Apply**. Ruch przesyłany przez interfejsy źródłowe będzie kopiowany do portu źródłowego. Dostępne są trzy typy interfejsów źródłowych: port, LAG i CPU. Wybierz jeden lub kilka typów, stosownie do swoich wymagań.

UNIT1	Ustaw interfejsy źródłowe, wybierając określone porty. Przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez port.
LAGS	Ustaw interfejsy źródłowe, wybierając określone grupy agregacji łącza. Przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez LAG.
CPU	Jeżeli wybierzesz ten typ, przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez procesor.
Ingress	Jeżeli włączysz tę opcję, pakiety odebrane przez odpowiedni interfejs (port, LAG lub CPU) zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest włączona.
Egress	Jeżeli włączysz tę opcję, pakiety przesłane przez odpowiedni interfejs (port, LAG lub CPU) zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest wyłączona.

Uwaga:

- Porty przynależące do LAG nie mogą być portami docelowymi ani źródłowymi.
- Ten sam port nie może być równocześnie portem docelowym i źródłowym.

1.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować mirroring.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**monitor session** *session_num* **destination interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port***}** Włącz funkcję port mirror i ustaw port docelowy. *session_num:* Numer sesji monitorowania. Jedyną dozwoloną wartością jest 1. *port*: Numer portu docelowego. Dla sesji monitorowania można podać tylko jeden port docelowy.

Krok 3	**monitor session** *session_num* **source { cpu** *cpu_numbr* **| interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}}** *mode* Ustaw interfejsy monitorowania, wybierając określone porty lub grupy agregacji łącza. *session_num*: Numer sesji monitorowania. Jedyną dozwoloną wartością jest 1. *cpu_number*: Numer procesora. Jedyną dozwoloną wartością jest 1. *port-list*: Lista portów źródłowych. Można wybrać wiele opcji. *mode*: Tryb monitorowania. Dostępne są trzy opcje: **rx**, **tx** i **both**: **rx**: Pakiety przychodzące na port źródłowy będą kopiowane na port docelowy. **tx**: Pakiety wychodzące na porcie źródłowym będą kopiowane na port docelowy. **both**: Zarówno pakiety przychodzące, jak i wychodzące na porcie źródłowym mogą być skopiowane na port docelowy. *Note:* Możesz skonfigurować dowolną liczbę typów interfejsów źródłowych (ports, LAGs i CPU), stosownie do wymagań.
Krok 4	**show monitor session** Przejrzyj konfigurację Port Mirroring.
Krok 5	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 6	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób kopiowania odebranych i wysłanych pakietów na porcie 1/0/1,2,3 i procesora CPU na port 1/0/10.

Switch#configure

Switch(config)#monitor session 1 **destination interface gigabitEthernet** 1/0/10

Switch(config)#monitor session 1 **source interface gigabitEthernet** 1/0/1-3 both

Switch(config)#monitor session 1 **source cpu** 1 both

Switch(config)#show monitor session

Monitor Session: 1

Destination Port: Gi1/0/10

Source Ports(Ingress): Gi1/0/1-3

Source Ports(Egress): Gi1/0/1-3

Source CPU(Ingress): cpu1

Source CPU(Egress): cpu1

Switch(config-if)#end

Switch#copy running-config startup-config

Część 27

Konfiguracja DLDP

ROZDZIAŁY

1 Konfiguracja DLDP

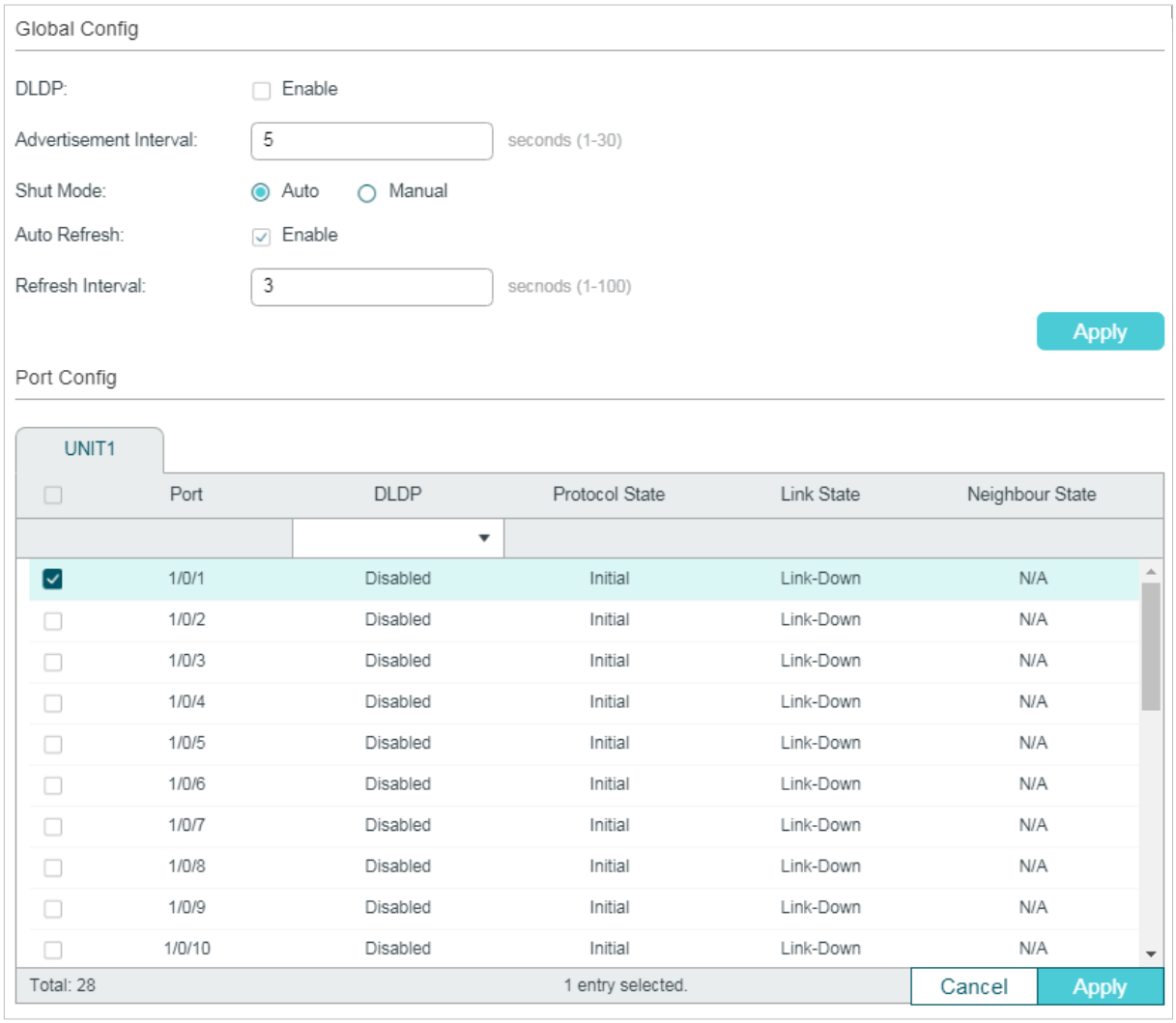
Wskazówki dotyczące konfiguracji

- Port obsługujący DLDP nie może wykryć łącza jednokierunkowego, jeżeli jest podłączony do portu nieobsługującego DLDP innego przełącznika.
- Aby wykrywać łącza jednokierunkowe, upewnij się, że technologia DLDP jest włączona po obu stronach łącza.

1.1 Przez GUI

Wybierz z menu **MAINTENANCE > DLDP**, aby wyświetlić poniższą stronę.

Rys. 1-1 Konfiguracja DLDP



Wykonaj poniższe kroki, aby skonfigurować DLDP:

1) W sekcji **Global Config** włącz DLDP i skonfiguruj odpowiednie parametry. Kliknij **Apply**.

DLDP State	Włącz lub wyłącz globalnie DLDP.
Advertisement Interval	Skonfiguruj interwał wysyłania pakietów powiadamiających. Prawidłowe wartości wahają się od 1 do 30 sekund, a wartością domyślną jest 5 sekund.
Shut Mode	Wybierz sposób zamknięcia portu, gdy wykryte zostanie łącze jednokierunkowe: **Auto**: Gdy na porcie zostanie wykryte łącze jednokierunkowe, DLDP wygeneruje dzienniki i pułapki, a następnie zamknie port, a DLDP na tym porcie wyłączy się. **Manual**: Gdy na porcie zostanie wykryte łącze jednokierunkowe, DLDP wygeneruje dzienniki i pułapki. Następnie użytkownicy będą mogli ręcznie zamknąć porty łącza jednokierunkowego.
Auto Refresh	Po zaznaczeniu tej opcji przełącznik będzie automatycznie odświeżać informacje o DLDP.
Refresh Interval	Ustaw częstotliwość odświeżania informacji o DLDP. Prawidłowe wartości wahają się od 1 do 100 sekund, a wartością domyślną są 3 sekundy.

2) W sekcji **Port Config** wybierz co najmniej jeden port, włącz DLDP i kliknij **Apply**. W tabeli pojawią się informacje o DLDP.

DLDP	Włącz lub wyłącz DLDP na porcie.
Protocol State	Stan protokołu DLDP. **Initial**: DLDP jest wyłączony. **Inactive**: DLDP jest włączony, ale łącze nie działa. **Active**: DLDP jest włączony i łącze działa lub wpisy o urządzeniach sąsiadujących na tym urządzeniu są puste. **Advertisement**: Nie wykryto łącza jednokierunkowego (urządzenie ustanowiło dwukierunkowe połączenia ze wszystkimi urządzeniami sąsiadującymi) lub DLDP pozostało w stanie Active dłużej niż 5 sekund. **Probe**: Po przejściu w ten stan urządzenie wyśle pakiety sondujące, aby sprawdzić czy łącze jest jednokierunkowe. Port wchodzi w ten stan ze stanu Active, jeżeli odbierze pakiet od nieznanego urządzenia sąsiadującego. **Disable**: Wykryto łącze jednokierunkowe.
Link State	Stan łącza. **Link-Down**: Łącze nie jest aktywne. **Link-Up**: Łącze jest aktywne.

Neighbour State	Stan urządzenia sąsiadującego. **Unknown**: Trwa wykrywanie łącza. **Unidirectional**: Łącze pomiędzy portem a urządzeniem sąsiadującym jest jednokierunkowe. **Bidirectional**: Połączenie pomiędzy portem a urządzeniem sąsiadującym jest dwukierunkowe.

1.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować DLDP:

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**dldp** Włącz globalnie DLDP.
Krok 3	**dldp interval** *interval-time* Skonfiguruj interwał wysyłania pakietów powiadamiających na portach, które są w stanie powiadomień. *interval-time*: Podaj wartość interwału. Prawidłowe wartości wahają się od 1 do 30 sekund, a wartością domyślną jest 5 sekund.
Krok 3	**dldp shut-mode** { auto | manual } Skonfiguruj tryb wyłączania DLDP po wykryciu łącza jednokierunkowego. auto: Przełącznik automatycznie zamyka porty, gdy wykryte zostanie łącze jednokierunkowe. manual: Przełącznik wysyła powiadomienie, gdy wykryte zostanie łącze jednokierunkowe. Następnie użytkownicy mogą ręcznie zamknąć porty łącza jednokierunkowego.
Krok 4	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***}** Uruchom tryb konfiguracji globalnej.
Krok 5	**dldp** Włącz DLDP na wybranym porcie.
Krok 6	**show dldp** Przejrzyj globalną konfigurację DLDP.
Krok 7	**show dldp interface** Przejrzy konfigurację DLDP portów.

Krok 8	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania DLDP, ustawiania interwału DLDP jako 10 sekund i trybu wyłączania DLDP jako auto.

Switch#configure

Switch(config)#dldp

Switch(config)#dldp interval 10

Switch(config)#dldp shut-mode auto

Switch(config)#show dldp

DLDP Global State: Enable

DLDP Message Interval: 10

DLDP Shut Mode: Auto

Switch(config)#end

Switch#copy running-config startup-config

Poniższy schemat przedstawia przykładowy sposób włączania DLDP na porcie 1/0/1.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#dldp

Switch(config-if)#show dldp interface

Port	DLDP State	Protocol State	Link State	Neighbor State
----	----------	--------------	----------	--------------
Gi1/0/1	Enable	Inactive	Link-Down	N/A
Gi1/0/2	Disable	Initial	Link-Down	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

Część 28

Konfiguracja SNMP i RMON

ROZDZIAŁY

1 Konfiguracja SNMP

Aby przeprowadzić proces konfiguracji SNMP, wybierz wersję SNMP zgodnie z wymaganiami sieci i obsługą oprogramowania NMS, a następnie wykonaj poniższe kroki:

- Wybierając SNMPv1 lub SNMPv2c

1) Włącz SNMP.
2) Utwórz widok SNMP dla zarządzanych obiektów.
3) Utwórz społeczność (community), wybierz widok dostępu i odpowiednie uprawnienia dostępu.

- Wybierając SNMPv3

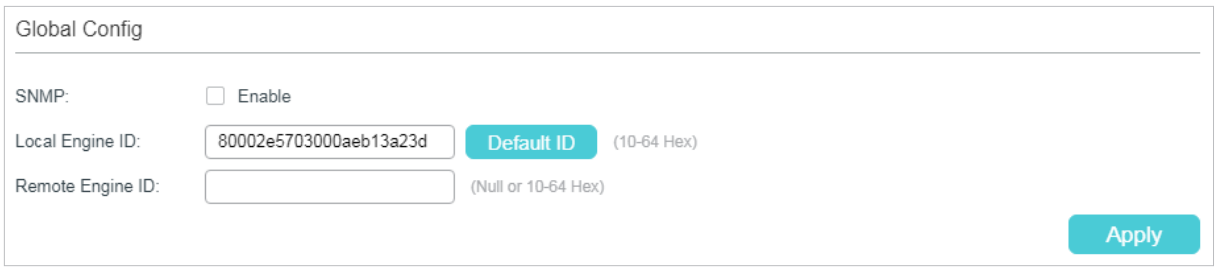
1) Włącz SNMP.
2) Utwórz widok SNMP dla zarządzanych obiektów.
3) Utwórz grupę SNMP i określ prawa dostępu.
4) Utwórz użytkowników SNMP i skonfiguruj tryb uwierzytelniania, tryb ochrony prywatności i odpowiednia hasła.

1.1 Przez GUI

1.1.1 Włączanie SNMP

Wybierz z menu **MAINTENANCE > SNMP > Global Config**, aby wyświetlić poniższą stronę.

Rys. 1-1 Konfiguracja globalna



Wykonaj poniższe kroki, aby skonfigurować globalnie SNMP:

1) W sekcji **Global Config** włącz SNMP i skonfiguruj lokalny i zdalny engine ID.

SNMP	Włącz lub wyłącz globalnie SNMP.

Local Engine ID	Ustaw engine ID lokalnego agenta SNMP (przełącznika) używając od 10 do 64 znaków szesnastkowych. Domyślnie przełącznik generuje engine ID korzystając z PEN firmy TP-LINK (80002e5703) i własnego adresu MAC. Lokalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP. Agent SNMP ma tylko jeden silnik SNMP, dlatego za pomocą lokalnego engine ID można jednoznacznie zidentyfikować agenta SNMP.
Remote Engine ID	Ustaw ID zdalnego menadżera SNMP, używając od 10 do 64 znaków szesnastkowych. Jeżeli nie jest potrzebny żaden zdalny menedżer SNMP, możesz pozostawić to pole puste. Zdalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP urządzenia zdalnego, które otrzymuje od przełącznika komunikaty inform.

2) Kliknij **Apply**.

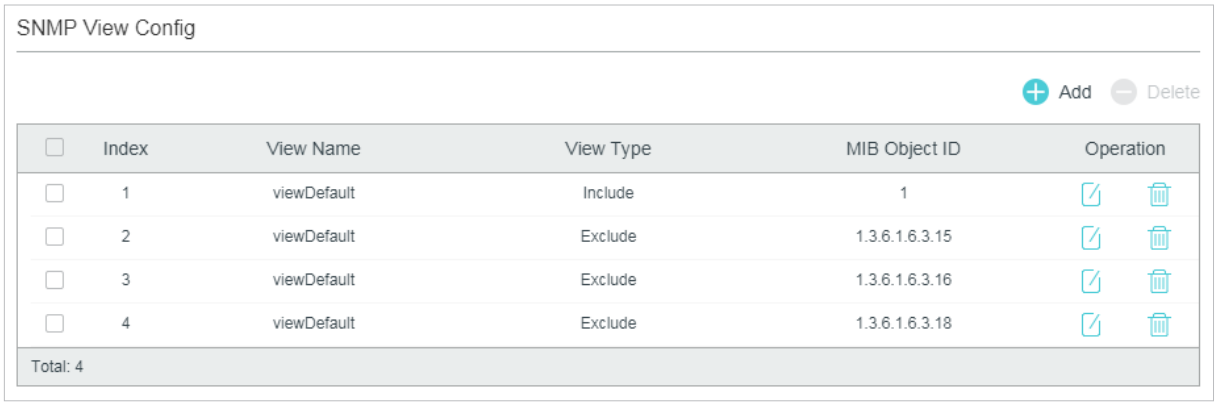
Uwaga:

- Engine ID musi zawierać parzystą liczbę znaków.
- Zmiana wartości engine ID SNMP ma istotne konsekwencje. W wersji SNMPv3 hasło użytkownika jest konwertowane na kryptograficzną funkcję skrótu MD5 lub SHA w oparciu o hasło i ID silnika. Gdy wartość engine ID ulega zmianie, przełącznik automatycznie usuwa wszystkich lokalny użytkowników SNMPv3, ponieważ ich algorytm kryptograficzny traci ważność. Tak samo wszyscy zdalni użytkownicy SNMPv3 są usuwani, gdy wartość zdalnego engine ID ulega zmianie.

1.1.2 Tworzenie widoku SNMP

Wybierz z menu **MAINTENANCE > SNMP > Global Config**, aby wyświetlić poniższą stronę.

Rys. 1-2 Konfiguracja widoku SNMP

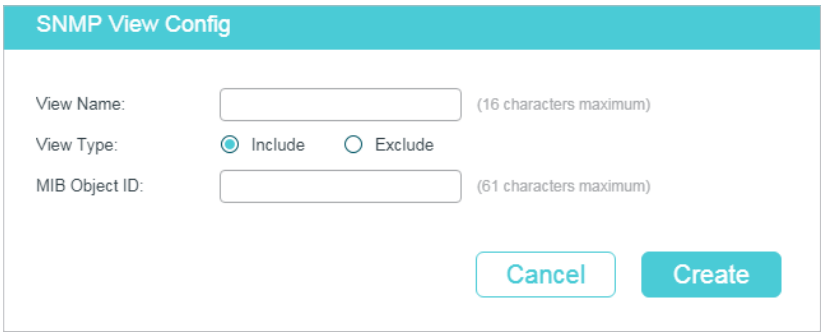


NMS zarządza obiektami bazy MIB w oparciu o widok SNMP. Widok SNMP jest podzbiorem bazy MIB. System zapewnia domyślny widok o nazwie viewDefault, ale możesz także tworzyć inne widoki SNMP, stosownie do wymagań.

Wykonaj poniższe kroki, aby skonfigurować widok SNMP:

1) Kliknij Add , aby wyświetlić poniższą stronę. Podaj nazwę widoku oraz wybierz typ widoku i obiekt bazy MIB, który będzie powiązany z widokiem.

Rys. 1-3 Tworzenie widoku SNMP



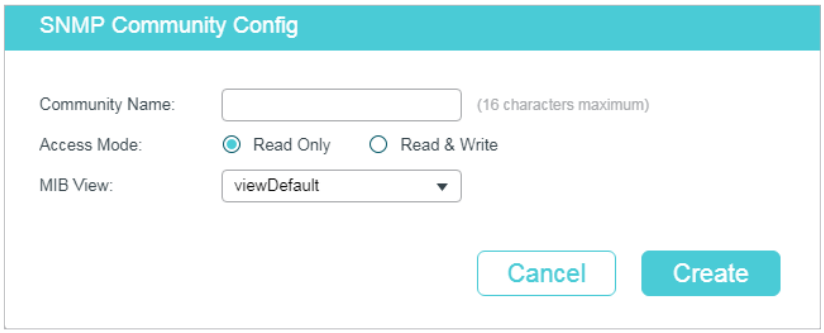
View Name	Podaj nazwę widoku wpisując od 1 do 16 znaków. W pełni skonfigurowany widok składa się z obiektów bazy MIB o tej samej nazwie widoku.
View Type	Ustaw, które obiekty bazy MIB mają należeć do widoku. Domyślnie obiekt należy do widoku. **Include:** NMS może wyświetlać lub zarządzać funkcją wskazaną przez obiekt. **Exclude:** NMS nie może wyświetlać ani zarządzać funkcją wskazaną przez obiekt.
MIB Object ID	Wpisz identyfikator obiektu (OID) bazy MIB, aby określić funkcję urządzenia. Podanie OID bazy MIB określa wszystkie child OIDs. Szczegółowe reguły ID znajdują się w bazach MIB powiązanych z urządzeniami.

2) Kliknij **Create**.

1.1.3 Tworzenie społeczności SNMP (SNMP v1/v2c)

Wybierz z menu **MAINTENANCE > SNMP > SNMP v1/v2c** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 1-4 Tworzenie społeczności SNMP



1) Podaj nazwę społeczności, określ uprawnienia dostępu i powiązany widok.

Community Name	Skonfiguruj nazwę społeczności, która będzie pełnić rolę hasła dostępu dla NMS do obiektów bazy MIB w agencie SNMP przełącznika.

Access Mode	Wybierz tryb dostępu do powiązanego widoku. Domyślnym ustawieniem jest read-only. **Read Only:** NMS może wyświetlać, ale nie może zmieniać parametrów określonego widoku. **Read & Write:** NMS może wyświetlać i zmieniać parametry określonego widoku.
MIB View	Wybierz widok SNMP, który zezwala na dostęp społeczności. Domyślnym widokiem jest viewDefault.

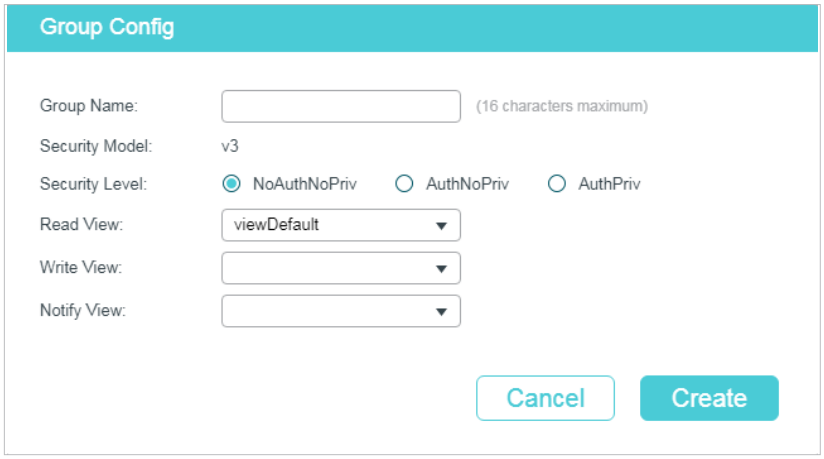
2) Kliknij **Create**.

1.1.4 Tworzenie grupy SNMP (SNMP v3)

Utwórz grupę SNMP i skonfiguruj odpowiednie parametry.

Wybierz z menu **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** i kliknij Add , aby wyświetlić poniższą stronę.

Rys, 1-5 Tworzenie grupy SNMP



Wykonaj poniższe kroki, aby utworzyć grupę SNMP:

1) Podaj nazwę grupy, a następnie ustaw poziom zabezpieczeń oraz widok odczytu, zapisu i powiadomień.

Group Name	Podaj nazwę grupy SNMP używając od 1 do 16 znaków. Identyfikator grupy składa się z nazwy grupy, modelu zabezpieczeń i poziomu zabezpieczeń. Grupy o tym samym identyfikatorze uznawane są za te same grupy.
Security Model	Model zabezpieczeń. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.

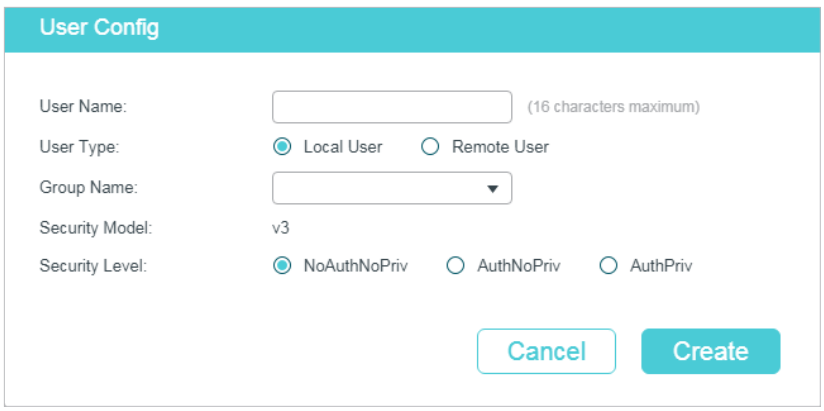
Security Level	Ustaw poziom zabezpieczeń dla grupy SNMPv3. Domyślnym ustawieniem jest NoAuthNoPriv. **NoAuthNoPriv:** Pakiety nie są sprawdzane ani szyfrowane, ponieważ nie zastosowano trybu uwierzytelniania ani trybu ochrony prywatności. **AuthNoPriv:** Pakiety są sprawdzane w trybie uwierzytelniania, ale nie są szyfrowane, ponieważ nie zastosowano trybu ochrony prywatności. **AuthPriv:** Zastosowano tryb uwierzytelniania i tryb ochrony prywatności, dlatego pakiety są sprawdzane i szyfrowane.
Read View	Wybierz ten widok, aby zezwolić na wyświetlanie parametrów przez NMS. Modyfikowanie ich przez NMS nie będzie jednak możliwe. Wybór widoku jest konieczny dla każdej grupy. Widokiem domyślnym jest viewDefault. Zmiana parametrów widoku możliwa jest tylko w widoku zapisu.
Write View	Wybierz ten widok, aby zezwolić na zmianę parametrów przez NMS. Wyświetlanie ich przez NMS nie będzie jednak możliwe. Widokiem domyślnym jest none. Widok zapisu wymaga włączenia widoku odczytu.
Notify View	Wybierz ten widok, aby zezwolić na wysyłanie powiadomień do NMS.

2) Kliknij **Create**.

1.1.5 Tworzenie użytkowników SNMP (SNMP v3)

Wybierz z menu **MAINTENANCE > SNMP > SNMP v3 > SNMP User** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 1-6 Tworzenie użytkownika SNMP



Wykonaj poniższe kroki, aby utworzyć użytkownika SNMP:

1) Podaj nazwę użytkownika, typ użytkownika i grupę, do której należy użytkownik. Następnie skonfiguruj poziom zabezpieczeń.

User Name	Podaj nazwę użytkownika SNMP używając od 1 do 16 znaków. Nazwy użytkowników nie mogą się powtarzać.

User Type	Wybierz typ użytkownika, aby określić jego lokalizację. Domyślnym ustawieniem jest Local User. **Local User:** Użytkownik korzysta z lokalnego silnika, który jest agentem SNMP przełącznika. **Remote User:** Użytkownik korzysta z NMS. Ze względu na to, że zdalny engine ID i hasło użytkownika są używane do obliczania skrótu uwierzytelniania i ochrony prywatności, przed skonfigurowaniem użytkownika zdalnego należy ustawić zdalny engine ID.
Group Name	Wybierz grupę, do której należy użytkownik. Użytkownicy o tej samej nazwie grupy, modelu zabezpieczeń i poziomie zabezpieczeń będą należeć do tej samej grupy.
Security Model	Model zabezpieczeń. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.
Security Level	Ustaw poziom zabezpieczeń dla grupy SNMPv3. Poziomy zabezpieczeń od najwyższego do najniższego układają się następująco: NoAuthNoPriv, AuthNoPriv, AuthPriv. Ustawieniem domyślnym jest NoAuthNoPriv. Poziom zabezpieczeń użytkownika nie powinien być niższy niż grupy, do której należy. **NoAuthNoPriv:** Do uwierzytelnienia dostępu wymagana jest nazwa użytkownika. Brak szyfrowania. **AuthNoPriv:** Pakiety są sprawdzane w trybie uwierzytelniania, ale nie są szyfrowane, ponieważ nie zastosowano trybu ochrony prywatności. **AuthPriv:** Zastosowano tryb uwierzytelniania i tryb ochrony prywatności, dlatego pakiety są sprawdzane i szyfrowane.

2) Jeżeli wybierzesz **AuthNoPriv** lub **AuthPriv**, musisz odpowiednio ustawić tryb uwierzytelniania lub tryb ochrony prywatności. W innym wypadku pomiń ten krok.

Authentication Mode	Jeżeli wybierzesz AuthNoPriv lub AuthPriv, skonfiguruj tryb uwierzytelniania i hasło. Do wyboru są dwa tryby uwierzytelniania: **MD5:** Uwierzytelniaj za pomocą algorytmu HMAC-MD5. **SHA:** Uwierzytelniaj za pomocą algorytmu SHA (Secure Hash Algorithm). Algorytm SHA zapewnia wyższy poziom bezpieczeństwa niż algorytm MD5.
Authentication Password	Ustaw hasło uwierzytelniające.
Privacy Mode	Jeżeli wybierzesz AuthPriv, skonfiguruj tryb ochrony prywatności i hasło szyfrowania. Przełącznik używa algorytmu DES (Data Encryption Standard) do szyfrowania.
Privacy Password	Ustaw hasło szyfrowania.

3) Kliknij **Create**.

1.2 Przez CLI

1.2.1 Włączanie SNMP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server** Włączanie SNMP.
Krok 3	**snmp-server engineID** {[**local** *local-engineID*] [**remote** *remote-engineID*]} Skonfiguruj lokalny engine ID i zdalny engine ID. *local-engineID:* Ustaw engine ID lokalnego agenta SNMP (przełącznika) używając od 10 do 64 znaków szesnastkowych. Domyślnie przełącznik generuje engine ID korzystając z PEN firmy TP-LINK (80002e5703) i własnego adresu MAC. Lokalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP. Agent SNMP ma tylko jeden silnik SNMP, dlatego za pomocą lokalnego engine ID można jednoznacznie zidentyfikować agenta SNMP. *remote-engineID:* Ustaw ID zdalnego menadżera SNMP używając od 10 do 64 znaków szesnastkowych. Identyfikator musi zawierać parzystą liczbę znaków. Zdalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP urządzenia zdalnego, które otrzymuje od przełącznika komunikaty inform. *Note:* Zmiana wartości engine ID SNMP ma istotne konsekwencje. W wersji SNMPv3 hasło użytkownika jest konwertowane na kryptograficzną funkcję skrótu MD5 lub SHA w oparciu o hasło i ID silnika. Gdy wartość engine ID ulega zmianie, przełącznik automatycznie usuwa wszystkich lokalny użytkowników SNMPv3, ponieważ ich algorytm kryptograficzny traci ważność. Tak samo wszyscy zdalni użytkownicy SNMPv3 są usuwani, gdy wartość zdalnego engine ID ulega zmianie.
Krok 4	**show snmp-server** Przejrzyj globalne ustawienia SNMP.
Krok 5	**show smnp-server engineID** Sprawdź engine ID SNMP.
Krok 6	**end** Powróć do trzybu uprzywilejowanego (privileged EXEC mode).
Krok 7	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania SNMP i ustawiania 123456789a jako zdalnego engine ID:

Switch#configure

Switch(config)#snmp-server

Switch(config)#snmp-server engineID remote 123456789a

Switch(config)#show snmp-server

SNMP agent is enabled.

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad value errors

0 General errors

0 Response PDUs

0 Trap PDUs

Switch(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Switch(config)#end

Switch#copy running-config startup-config

1.2.2 Tworzenie widoku SNMP

Podaj identyfikator obiektu (OID) widoku, aby określić zarządzane obiekty.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**snmp-server view** *name mib-oid* {include | exclude} Skonfiguruj widok. *name:* Podaj nazwę widoku wpisując 1 - 16 znaków. Możesz dodać wiele wpisów z powiązanymi obiektami bazy MIB. W pełni skonfigurowany widok składa się z obiektów bazy MIB o tej samej nazwie widoku. *mib-oid:* Podaj identyfikator obiektu bazy MIB używając od 1 do 61 znaków. include | exclude: Określ typ widoku. Include oznacza, że obiekty widoku mogą być zarządzane przez NMS, natomiast exclude wyklucza zarządzanie obiektów przez NMS.
Krok 3	**show snmp-server view** Wyświetla tabelę widoków.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji zezwolenia na zarządzanie wszystkimi funkcjami przez NMS dla widoku. Nazwą widoku będzie View:

Switch#configure

Switch(config)#snmp-server view View 1 include

Switch(config)#show snmp-server view

No. View Name Type MOID

--- ---------- ------- ----

1 viewDefault include 1

2 viewDefault exclude 1.3.6.1.6.3.15

3 viewDefault exclude 1.3.6.1.6.3.16

4 viewDefault exclude 1.3.6.1.6.3.18

5 View include 1

Switch(config)#end

Switch#copy running-config startup-config

1.2.3 Tworzenie społeczności SNMP (SNMP v1/v2c)

W przypadku SNMPv1 i SNMPv2c nazwa społeczności, pełniąc rolę hasła, będzie używana do uwierzytelniania dostępu.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server community** *name* { read-only | read-write } [*mib-view*] Skonfiguruj społeczność. *name:* Podaj nazwę grupy używając od 1 do 16 znaków. *read-only | read-write:* Wybierz uprawnienia dostępu dla społeczności. Read-only oznacza, że NMS może wyświetlać, ale nie może zmieniać parametrów widoku, natomiast read-write oznacza, że NMS może zarówno wyświetlać, jak i zmieniać parametry. *mib-view:* Wybierz widok, aby zezwolić społeczności na dostęp. Nazwa może zawierać od 1 do 61 znaków. Domyślnym widokiem jest viewDefault.
Krok 3	**show snmp-server community** Wyświetla wpisy społeczności.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania społeczności SNMP. Nazwą społeczności będzie nms-monitor, a NMS będzie mieć zezwolenie na wyświetlanie i zmianę parametrów widoku View:

Switch#configure

Switch(config)#snmp-server community nms-monitor read-write View

Switch(config)#show snmp-server community

Index	Name	Type	MIB-View
-----	----------	----------	--------
1	nms-monitor	read-write	View

Switch(config)#end

Switch#copy running-config startup-config

1.2.4 Tworzenie grupy SNMP (SNMPv3)

Utwórz grupę SNMP i ustaw kontrolę dostępu użytkownika za pomocą widoków odczytu, zapisu i powiadomień. Ustaw także tryby uwierzytelniania i ochrony prywatności, aby zabezpieczyć komunikację między NMS a zarządzanymi urządzeniami.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server group** *name* [**smode** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] Utwórz grupę SNMP. *name:* Podaj nazwę grupy SNMP używając od 1 do 16 znaków. Identyfikator grupy składa się z nazwy grupy, modelu zabezpieczeń i poziomu zabezpieczeń. Grupy o tym samym identyfikatorze uznawane są za te same grupy. v3: Skonfiguruj model zabezpieczeń dla grupy. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa. noAuthNoPriv | authNoPriv | authPriv: Wybierz poziom zabezpieczeń spośród noAuthNoPriv (brak uwierzytelniania i szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania), authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Jeżeli wybranym modelem zabezpieczeń jest wersja 1 lub wersja 2, poziom zabezpieczeń nie może być skonfigurowany. *read-view:* Gdy ustawisz widok odczytu, NMS będzie mógł wyświetlać parametry określonego widoku. *write-view:* Gdy ustawisz widok zapisu, NMS będzie mógł zmieniać parametry określonego widoku. Pamiętaj, że widok zapisu wymaga włączenia widoku odczytu. *notify-view:* Gdy ustawisz widok powiadomień. NMS będzie mógł otrzymywać powiadomienia dotyczące określonego widoku od agenta.
Krok 3	**show snmp-server group** Wyświetla wpisy grupy SNMP.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia grupy SNMPv3 o nazwie nms1, ustawiania zabezpieczeń na poziomie authPriv, oraz widoku odczytu i powiadomień jako View1:

Switch#configure

Switch(config)#snmp-server group nms1 **smode** v3 **slev** authPriv **read** View1 **notify** View1

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
---	--------	------------	----------	------------	------------	------------
1	nms1	v3	authPriv	View1		View1

Switch(config)#end

Switch#copy running-config startup-config

1.2.5 Tworzenie użytkowników SNMP (SNMPv3)

Skonfiguruj użytkowników grupy SNMP. Użytkownicy należący do grupy korzystają z tego samego poziomu zabezpieczeń i uprawnień dostępu co grupa.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server user** *name* { local | remote } *group-name* [**smode** v3] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**cmode** { none | MD5 | SHA }] [**cpwd** *confirm-pwd*] [**emode** { none | DES }] [**epwd** *encrypt-pwd*] Skonfiguruj użytkowników grupy SNMP. *name:* Wprowadź nazwę użytkownika, wpisując od 1 do 16 znaków. local | remote*:* Wybierz typ użytkownika. Typ Local oznacza, że użytkownik połączony jest z silnikiem lokalnym SNMP, natomiast remote oznacza, że użytkownika jest połączony z silnikiem zdalnym SNMP. Ze względu na to, że zdalny engine ID i hasło użytkownika są używane do obliczania skrótu uwierzytelniania i ochrony prywatności, przed skonfigurowaniem użytkownika zdalnego należy ustawić zdalny engine ID. *group-name:* Podaj nazwę grupy, do której należy użytkownik. Grupę określa jej nazwa oraz tryb i poziom zabezpieczeń. v3*:* Skonfiguruj tryb zabezpieczeń dla użytkownika. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.. noAuthNoPriv | authNoPriv | authPriv*:* Ustaw poziom zabezpieczeń dla grupy. Poziomy zabezpieczeń od najwyższego do najniższego układają się następująco: noAuthNoPriv (brak uwierzytelniania i brak szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania) i authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Poziom zabezpieczeń użytkownika nie powinien być niższy niż grupy, do której należy. none | MD5 | SHA: Wybierz algorytm uwierzytelniania. Algorytm SHA zapewnia wyższy poziom bezpieczeństwa niż algorytm. Domyślnym ustawieniem jest none. *confirm-pwd:* Ustaw hasło uwierzytelniające, używając od 1 do 16 znaków, z wykluczeniem znaków zapytania i spacji. To hasło będzie wyświetlane w pliku konfiguracyjnym pod postacią szyfru symetrycznego. none | DES*:* Wybierz tryb ochrony prywatności. None oznacza brak ustawień prywatności, natomiast DES wskazuje na użycie szyfrowania DES. Domyślnym ustawieniem jest none. *encrypt-pwd:* Ustaw hasło ochrony prywatności, używając od 1 do 16 znaków, z wykluczeniem znaków zapytania i spacji. To hasło będzie wyświetlane w pliku konfiguracyjnym pod postacią szyfru symetrycznego.
Krok 3	**show snmp-server user** Przejrzyj informacje o użytkownikach SNMP.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia użytkownika SNMP i dodawania go do grupy nms1. Nazwą użytkownika będzie admin, typem remote user, trybem zabezpieczeń SNMPv3, poziomem zabezpieczeń authPriv, algorytmem uwierzytelniania SHA, hasłem uwierzytelniającym 1234, algorytmem ochrony prywatności DES, a hasłem ochrony prywatności 1234:

Switch#configure

Switch(config)#snmp-server user admin remote nms1 **smode** v3 **slev** authPriv **cmode** SHA **cpwd** 1234 **emode** DES **epwd** 1234

Switch(config)#show snmp-server user

No.	U-Name	U-Type	G-Name	S-Mode	S-Lev	A-Mode	P-Mode
---	------	------	------	------	-----	------	------
1	admin	remote	nms1	v3	authPriv	SHA	DES

Switch(config)#end

Switch#copy running-config startup-config

2 Konfiguracja powiadomień

Po włączeniu powiadomień przełącznik będzie mógł wysyłać powiadomienia do NMS o ważnych zdarzeniach związanych z pracą urządzenia. Ułatwia to monitorowanie i zarządzanie NMS.

Wykonaj poniższe kroki, aby skonfigurować powiadomienia SNMP:

1) Skonfiguruj informacje o hostach NMS.
2) Włącz SNMP trap.

Wskazówki dotyczące konfiguracji

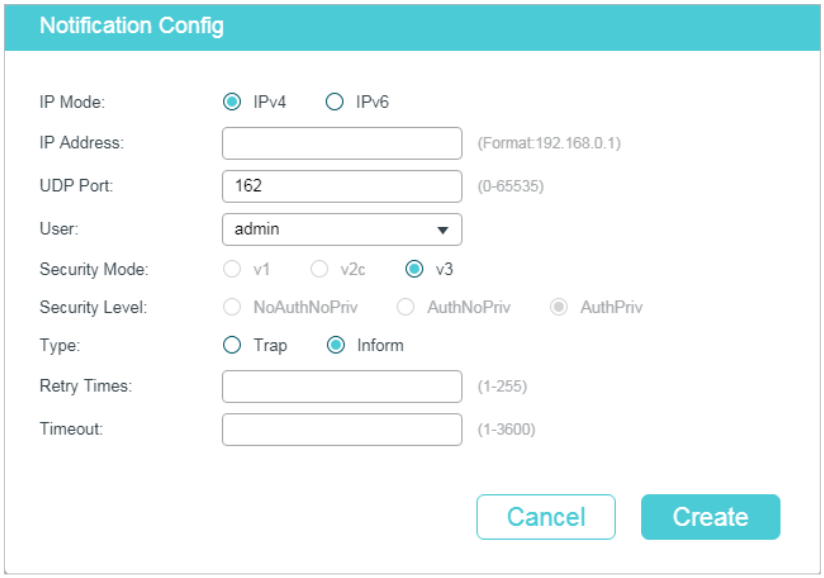
Aby komunikację między przełącznikiem a NMS była możliwa, upewnij się, że przełącznik i NMS wykrywają się nawzajem.

2.1 Przez GUI

2.1.1 Konfiguracja informacji o hostach NMS

Wybierz z menu **MAINTENANCE > SNMP > Notification > Notification Config** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 2-1 Dodawanie hosta NMS



Wykonaj poniższe kroki, aby dodać hosta NMS:

1) Wybierz tryb IP zgodny z otoczeniem sieciowym i podaj adres IP hosta NMS oraz port UDP, który odbiera powiadomienia.

IP Mode	Wybierz tryb IP dla hosta NMS.
IP Address	Jeżeli wybranym **IP Mode** jest IPv4, podaj adres IPv4 dla hosta NMS. Jeżeli wybranym **IP Mode** jest IPv6, podaj adres IPv6 dla hosta NMS.
UDP Port	Wybierz port UDP na hoście NMS do odbierania powiadomień. Portem domyślnym jest 162. W celu zapewnienia bezpieczeństwa komunikacji zalecamy zmianę numeru portu pod warunkiem, że komunikacja na innych portach UDP nie zostanie zakłócona.

2) Podaj nazwę użytkownika lub nazwę społeczności, z której korzysta host NMS i skonfiguruj tryb i poziom zabezpieczeń, w zależności od ustawień użytkownika lub społeczności.

User Name	Podaj nazwę użytkownika lub społeczności, z której korzysta host NMS.
Security Mode	Jeżeli w polu User Name podałeś nazwę społeczności (stworzoną dla SNMPv1/v2c), trybem zabezpieczeń musi być v1 lub v2c. Jeżeli w polu User Name podałeś nazwę użytkownika (stworzoną dla SNMPv3), trybem zabezpieczeń będzie v3. Host NMS powinien korzystać z odpowiedniej wersji SNMP.
Security Level	Jeżeli Security Level to v3, pole pokazuje poziom zabezpieczeń użytkownika.

3) Wybierz typ powiadomień w oparciu o wersję SNMP. Jeżeli wybierzesz typ Inform, musisz także ustawić limit wysyłanych komunikatów oraz limit czasu oczekiwania.

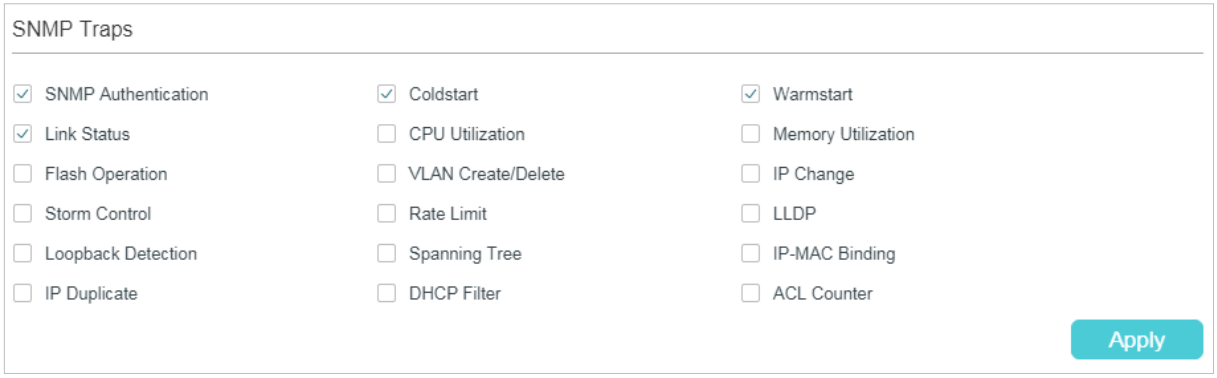
Type	Wybierz typ powiadomień dla hosta NMS. Obsługiwanym typem dla SNMPv1, jest trap. Dla SNMPv2c i SNMPv3 dostępne są typy trap oraz inform. Trap: Przełącznik wysyła komunikaty Trap do hosta NMS po wystąpieniu określonych zdarzeń. Gdy host NMS otrzymuje komunikat Trap, nie wysyła odpowiedzi do przełącznika. Zatem przełącznik nie może stwierdzić, czy komunikat został odebrany, czy nie i komunikaty, które nie zostały odebrane, nie zostaną wysłane ponownie. Inform: Przełącznik wysyła komunikaty Inform do hosta NMS po wystąpieniu określonych zdarzeń. Gdy host NMS otrzymuje komunikat Inform, wysyła odpowiedź do przełącznika. Jeśli przełącznik nie otrzyma odpowiedzi w ustalonym limicie czasu oczekiwania, ponownie wysyła komunikat Inform. Zatem komunikaty Inform są bardziej przewidywalne niż komunikaty Trap.
Retry	Ustaw limit wysyłanych komunikatów Inform. Jeżeli przełącznik nie otrzyma odpowiedzi od hosta NMS w ustalonym limicie czasu oczekiwania, ponownie wyśle komunikat Inform. Przełącznik zaprzestanie wysyłania komunikatów Inform po osiągnięciu ustalonego limitu.
Timeout	Ustaw czas oczekiwania przełącznika na odpowiedź od hosta NMS po przesłaniu komunikatu Inform.

4) Kliknij **Create**.

2.1.2 Włączanie SNMP Traps

Wybierz menu **MAINTENANCE > SNMP > Notification > Trap Config,** aby wyświetlić poniższą stronę.

Rys. 2-2 Włączanie SNMP Traps



Na stronie znajduje się lista obsługiwanych komunikatów Trap. Wykonaj poniższe kroki, aby włączyć lub wyłączyć wybrane komunikaty Trap:

1) Wybierz komunikaty Trap, które chcesz włączyć, w zależności od swoich wymagań.

SNMP Authentication	Ma zastosowanie, gdy uwierzytelnianie otrzymanego żądania SNMP kończy się niepowodzeniem.
Coldstart	Wskazuje na inicjalizację SNMP spowodowaną ponowną inicjalizacją systemu przełącznika. Komunikat trap jest wysyłany po restarcie przełącznika.
Warmstart	Wskazuje, że funkcja SNMP jest ponownie inicjalizowana na przełączniku z niezmienioną konfiguracją fizyczną. Komunikat trap jest wysyłany, gdy SNMP zostanie wyłączony i ponownie włączony po pełnej konfiguracji i włączeniu SNMP.
Link Status	Ma zastosowanie, gdy przełącznik wykrywa zmianę stanu łącza.
CPU Utilization	Ma zastosowanie, gdy wykorzystanie procesora przekracza ustawiony limit. Domyślnym limitem dla przełącznika jest 80%.
Memory Utilization	Ma zastosowanie, gdy wykorzystanie pamięci przekracza 80%.
Flash Operation	Ma zastosowanie, gdy pamięć flash ulega zmianie poprzez takie działania, jak tworzenie kopii zapasowej, reset, aktualizacja firmware'u, import konfiguracji. .
VLAN Create/Delete	Ma zastosowanie, gdy określone VLAN-y zostaną pomyślnie utworzone lub usunięte.
IP Change	Monitoruje zmiany adresu IP wszystkich interfejsów. Komunikat trap jest wysyłany, gdy adres IP interfejsu ulegnie zmianie.
Storm Control	Monitoruje, czy wskaźnik storm osiągnął ustawiony limit. Komunikat trap jest wysyłany, gdy funkcja jest włączona, a ramki broadcast/multicast/unknown-unicast są wysłane na port niezgodnie z ustawionym limitem.

Rate Limit	Monitoruje przekroczenie limitu ustawionej przepustowości. Komunikat trap jest wysyłany, gdy opcja Rate Limit jest włączona, a pakiety są wysyłane na port niezgodnie z ustawionym limitem.
LLDP	Wskazuje na zmiany w topologii LLDP. Komunikat trap jest wysyłany, gdy nowe urządzenie zdalne, podłączone do portu lokalnego lub urządzenia zdalnego, traci połączenie lub zostaje podłączone do innego portu.
Loopback Detection	Ma zastosowanie, gdy przełącznik wykryje połączenie loopback lub, gdy połączenie loopback zostanie usunięte.
Spanning Tree	Wskazuje na zmiany spanning tree. Komunikat trap jest wysyłany, gdy stan portu ulega zmianie z non-forwarding do forwarding lub na odwrót. Port odbiera pakiet z flagą TC lub pakiet TCN.
PoE	Tylko dla urządzeń z obsługą funkcji PoE. Wszystkie komunikaty trap odnoszą się do PoE , tj.: **Over-max-pwr-budget**: Ma zastosowanie, gdy całkowita moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć przełącznik PoE. **Port-pwr-change**: Ma zastosowanie, gdy port zaczyna dostarczać energię lub wyłącza zasilanie urządzeń. **Port-pwr-deny**: Ma zastosowanie, gdy przełącznik wyłącza zasilanie urządzeń PD na portach o niskim priorytecie. Gdy całkowita moc wymagana przez podłączone urządzenia PD przekroczy limit mocy systemowej, przełącznik wyłącza urządzenia PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń PD. **Port-pwr-over-30w**: Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przekracza 30W. **Port-pwr-overload**: Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć port. **Port-short-circuit**: Ma zastosowanie, gdy na porcie zostanie wykryte zwarcie. **Thermal-shutdown**: Ma zastosowanie, gdy układ PSE przegrzeje się. Przełącznik automatycznie wyłącza w tej sytuacji zasilanie.
IP-MAC Binding	Ma zastosowanie w następujących sytuacjach: funkcja inspekcji ARP jest włączona i przełącznik odbiera nielegalny pakiet ARP; funkcja IPv4 Source Guard jest włączona i przełącznik odbiera nielegalny pakiet IP.
IP Duplicate	Ma zastosowanie, gdy przełącznik wykrywa konflikt adresów IP.
DHCP Filter	Ma zastosowanie, gdy funkcja filtrowania DHCPv4 jest włączona i przełącznik odbiera pakiety DHCP z nielegalnego serwera DHCP.
ACL Counter	Monitoruje informacje o dopasowaniach ACL, w tym o ID dopasowań ACL, ID reguł oraz liczbie dopasowań pakietów. Włączenie tej opcji oraz funkcji **Logging** w ustawieniach reguł ACL sprawi, że przełącznik będzie sprawdzać informacje o dopasowaniach ACL co 5 minut i przesyłać komunikaty trap SNMP w przypadku zmian.

2) Kliknij **Apply**.

2.2 Przez CLI

2.2.1 Konfiguracja informacji o hostach NMS

Skonfiguruj parametry hostów NMS i mechanizm obsługi pakietów.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server host** *ip udp-port user-name* [**smode** { v1 | v2c | v3 }] [**slev** {noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform}] [**retries** *retries*] [**timeout** *timeout*] Skonfiguruj parametry hosta NMS i mechanizm obsługi pakietów. *ip:* Podaj adres IP hosta NMS w adresacji IPv4 lub IPv6. Upewnij się, że możliwa jest komunikacja dla podanych adresów IP hosta NMS i przełącznika. *udp-port:* Wybierz port UDP na hoście NMS do odbierania powiadomień. Portem domyślnym jest 162. W celu zapewnienia bezpieczeństwa komunikacji zalecamy zmianę numeru portu pod warunkiem, że komunikacja na innych portach UDP nie zostanie zakłócona. *user-name:* Podaj nazwę hosta NMS. Gdy host NMS korzysta z SNMPv1 lub SNMPv2c wprowadź Community Name; gdy host NMS korzysta z SNMPv3, wprowadź User Name grupy SNMP. v1 | v2c | v3: Wybierz tryb zabezpieczeń, z których korzysta użytkownik, spośród następujących opcji: SNMPv1, SNMPv2c, SNMPv3. Host NMS powinien korzystać z takiej samej wersji SNMP. noAuthNoPriv | authNoPriv | authPriv: Wybierz poziom zabezpieczeń spośród noAuthNoPriv (brak uwierzytelniania i szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania), authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Jeżeli wybranym modelem zabezpieczeń jest wersja 1 lub wersja 2, poziom zabezpieczeń nie może być skonfigurowany. trap | inform: Wybierz typ powiadomień dla hosta NMS. Obsługiwanym typem dla SNMPv1, jest trap. Dla SNMPv2c i SNMPv3 dostępne są typy trap oraz inform. Gdy host NMS otrzymuje komunikat Trap, nie wysyła odpowiedzi do przełącznika. Zatem przełącznik nie może stwierdzić, czy komunikat został odebrany, czy nie i komunikaty, które nie zostały odebrane, nie zostaną wysłane ponownie. Gdy host NMS otrzymuje komunikat Inform, wysyła odpowiedź do przełącznika. Jeżeli przełącznik nie otrzyma odpowiedzi w ustalonym limicie czasu oczekiwania, ponownie wysyła komunikat Inform. Zatem komunikaty Inform są bardziej przewidywalne niż komunikaty Trap. *retries:* Ustaw limit wysyłanych komunikatów Inform, wybierając wartość z przedziału 1 - 255 (domyślnie 3). Jeżeli przełącznik nie otrzyma odpowiedzi od hosta NMS w ustalonym limicie czasu oczekiwania, ponownie wyśle komunikat Inform. Przełącznik zaprzestanie wysyłania komunikatów Inform po osiągnięciu ustalonego limitu. *timeout:* Ustaw czas oczekiwania przełącznika na odpowiedź od hosta NMS po przesłaniu komunikatu Inform, wybierając wartość z przedziału 1 - 3600 sekund (domyślnie 100 sekund).

Krok 3	**show snmp-server host** Przejrzyj informacje o hoście.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania 192.30.1.222 jako adresu IP hosta NMS, portu 162 jako portu UDP, admin jako nazwy używanej przez hosta NMS, SNMPv3 jako trybu zabezpieczeń, authPriv jako poziomu zabezpieczeń, Inform jako typu powiadomień, 3 jako limitu wysyłanych komunikatów oraz 100 sekund jako czasu oczekiwania na odpowiedź:

Switch#configure

Switch(config)#snmp-server host 192.30.1.222 162 admin **smode** v3 **slev** authPriv **type** inform **retries** 3 **timeout** 100

Switch(config)#show snmp-server host

No.	Des-IP	UDP	Name	SecMode	SecLev	Type	Retry	Timeout
---	------	-----	----	-------	------	----	-----	-------
1	192.30.1.222	162	admin	v3	authPriv	inform	3	100

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Włączanie SNMP Traps

Przełącznik obsługuje wiele komunikatów trap SNMP, w tym standardowe trap SNMP,trap ACL i trap VLAN. Wybierz komunikaty Trap, które chcesz włączyć, w zależności od swoich wymagań.

- Globalne włączanie standardowych komunikatów trap SNMP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**snmp-server traps snmp [** linkup | linkdown | warmstart | coldstart | auth-failure **]** Włącz wybrane komunikaty trap SNMP. Bez podania parametrów polecenie włącza wszystkie standardowe komunikaty trap SNMP. Domyślnie włączone są wszystkie standardowe komunikaty trap SNMP. linkup: Wskazuje na zmianę stanu portu z linkdown do linkup i ma zastosowanie po podłączeniu urządzenia do portu. linkdown: Wskazuje na zmianę stanu portu z linkup do linkdown i ma zastosowanie po odłączeniu urządzenia od portu. warmstart: Wskazuje, że funkcja SNMP jest ponownie inicjalizowana na przełączniku z niezmienioną konfiguracją fizyczną. Komunikat trap jest wysyłany, gdy SNMP zostanie wyłączony i ponownie włączony po pełnej konfiguracji i włączeniu SNMP. coldstart: Wskazuje na inicjalizację SNMP spowodowaną ponowną inicjalizacją systemu przełącznika. Komunikat trap jest wysyłany po restarcie przełącznika. auth-failure: Ma zastosowanie, gdy uwierzytelnianie otrzymanego żądania SNMP kończy się niepowodzeniem.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji na przełączniku przesyłania komunikatów trap linkup:

Switch#configure

Switch(config)#snmp-server traps snmp linkup

Switch(config)#end

Switch#copy running-config startup-config

■ Globalne włączanie rozszerzonych komunikatów trap SNMP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2	**snmp-server traps** { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory } Włącz wybrane komunikaty trap SNMP. Domyślnie włączone są wszystkie rozszerzone komunikaty trap SNMP. rate-limit: Monitoruje przekroczenie limitu ustawionej przepustowości. Komunikat trap jest wysyłany, gdy opcja Rate Limit jest włączona, a pakiety są wysyłane na port niezgodnie z ustawionym limitem. cpu: Monitoruje stan obciążenia procesora przełącznika. Ma zastosowanie, gdy wykorzystanie procesora przekracza ustawiony limit. Domyślnym limitem dla przełącznika jest 80%. flash: Ma zastosowanie, gdy pamięć flash ulega zmianie poprzez takie działania, jak tworzenie kopii zapasowej, reset, aktualizacja firmware'u, import konfiguracji. lldp remtableschange: Powiadomienie lldp RemTablesChange jest wysyłane, gdy wartość lldp StatsRemTableLastChangeTime ulega zmianie. Może być stosowany przez hosta NMS do wysyłania table maintenance polls systemów zdalnych LLDP. lldp topologychange: Wskazuje na zmiany w topologii LLDP. Komunikat trap jest wysyłany, gdy nowe urządzenie zdalne, podłączone do portu lokalnego lub urządzenia zdalnego, traci połączenie lub zostaje podłączone do innego portu. loopback-detection: Ma zastosowanie, gdy przełącznik wykryje połączenie loopback lub, gdy połączenie loopback zostanie usunięte. storm-control: Funkcja monitoruje sieciowe burze rozgłoszeniowe. System wygeneruje komunikat trap, gdy liczba pakietów broadcast lub multicast osiągnie ustawiony limit. spanning-tree: Wskazuje na zmiany spanning tree. Komunikat trap jest wysyłany, gdy stan portu ulega zmianie z non-forwarding do forwarding lub na odwrót. Port odbiera pakiet z flagą TC lub pakiet TCN. memory: Monitoruje zużycie pamięci. Ma zastosowanie, gdy wykorzystanie pamięci przekracza 80%.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap bandwidth-control:

Switch#configure

Switch(config)#snmp-server traps bandwidth-control

Switch(config)#end

Switch#copy running-config startup-config

Globalne włączanie komunikatów trap VLAN

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server traps vlan** [create | delete] Włącz wybrane komunikaty trap VLAN. Bez podania parametrów polecenie włącza wszystkie komunikaty trap VLAN. Domyślnie komunikaty trap VLAN są wyłączone. create: Ma zastosowanie po pomyślnym utworzeniu określonych VLAN-ów. delete: Ma zastosowaniu po pomyślnym usunięciu określonych VLAN-ów.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania wszystkich komunikatów trap VLAN SNMP na przełączniku:

Switch#configure

Switch(config)#snmp-server traps vlan

Switch(config)#end

Switch#copy running-config startup-config

Globalne włączanie komunikatów trap ochrony SNMP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server traps security** { dhcp-filter | ip-mac-binding } Włącz wybrane komunikaty trap ochrony. Domyślnie wszystkie komunikaty trap są wyłączone. dhcp-filter: Ma zastosowanie, gdy funkcja filtrowania DHCPv4 jest włączona i przełącznik odbiera pakiety DHCP z nielegalnego serwera DHCP. ip-mac-binding: Ma zastosowanie, gdy funkcja inspekcji ARP jest włączona i przełącznik odbiera nielegalny pakiet ARP lub funkcja IPv4 Source Guard jest włączona i przełącznik odbiera nielegalny pakiet IP.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania komunikatów trap dla filtrowania DHCP na przełączniku:

Switch#configure

Switch(config)#snmp-server traps security dhcp-filter

Switch(config)#end

Switch#copy running-config startup-config

■ Globalne włączanie komunikatów trap ACL

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server traps security acl** Włącz komunikaty trap ACL. Domyślnie opcja jest wyłączona. Trap monitoruje informacje o dopasowaniach ACL, w tym o ID dopasowań ACL, ID reguł oraz liczbie dopasowań pakietów. Włączenie tej opcji oraz funkcji **Logging** w ustawieniach reguł ACL sprawi, że przełącznik będzie sprawdzać informacje o dopasowaniach ACL co 5 minut i przesyłać komunikaty trap SNMP w przypadku zmian.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania komunikatów trap ACL:

Switch#configure

Switch(config)#snmp-server traps acl

Switch(config)#end

Switch#copy running-config startup-config

■ Globalne włączanie komunikatów trap IP

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server traps ip** { change | duplicate } Włącz komunikaty trap IP. Domyślnie wszystkie komunikaty trap IP są wyłączone. change: Włącz komunikaty zmian IP SNMP. Trap monitoruje zmiany adresu IP wszystkich interfejsów. Komunikat trap jest wysyłany, gdy adres IP interfejsu ulegnie zmianie. duplicate: Włącz komunikaty duplikatów IP SNMP. Trap ma zastosowanie, gdy przełącznik wykrywa konflikt adresów IP.

Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode)..
Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap dla zmian adresów IP:

Switch#configure

Switch(config)#snmp-server traps ip change

Switch(config)#end

Switch#copy running-config startup-config

■ Globalne włączanie komunikatów trap PoE SNMP

Uwaga:

Tylko urządzenia T1500G-10PS, T1500G-10MPS i T1500-28PCT obsługują komunikaty trap PoE.

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**snmp-server traps power** [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown] Włącz komunikaty trap PoE. Bez podania parametrów polecenie włącza wszystkie komunikaty trap PoE. Domyślnie wszystkie komunikaty trap PoE są wyłączone. over-max-pwr-budget: Ma zastosowanie, gdy całkowita moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć przełącznik PoE. port-pwr-change: Ma zastosowanie, gdy port zaczyna dostarczać energię lub wyłącza zasilanie urządzeń. port-pwr-deny: Ma zastosowanie, gdy przełącznik wyłącza zasilanie urządzeń PD na portach o niskim priorytecie. Gdy całkowita moc wymagana przez podłączone urządzenia PD przekroczy limit mocy systemowej, przełącznik wyłącza urządzenia PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń PD. port-pwr-over-30w: Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przkeracza 30W. port-pwr-overload: Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć port. port-short-circuit: Ma zastosowanie, gdy na porcie zostanie wykryte zwarcie. thermal-shutdown: Ma zastosowanie, gdy układ PSE przegrzeje się. Przełącznik automatycznie wyłącza w tej sytuacji zasilanie.
Krok 3	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 4	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku wszystkich komunikatów trap PoE:

Switch#configure

Switch(config)#snmp-server traps power

Switch(config)#end

Switch#copy running-config startup-config

- Włączanie komunikatów trap o stanie łącza dla portów

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Skonfiguruj powiadomienia trap na określonych portach. *port/port-list:* Numer lub lista portów Ethernet dla powiadomień trap.
Krok 3	**snmp-server traps link-status** Włącz komunikaty trap o stanie łącza. Mają zastosowanie, gdy przełącznik wykrywa zmianę stanu łącza. Domyślnie opcja jest wyłączona.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode)..
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap o zmianie stanu łącza:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#snmp-server traps link-status

Switch(config-if)#end

Switch#copy running-config startup-config

3 RMON

RMON (Remote Network Monitoring) to standard uzupełniający SNMP. Służy do badania ilości przesyłanych danych. RMON ogranicza ruch pomiędzy NMS a urządzeniami zarządzalnymi, co jest wygodnym rozwiązaniem w przypadku dużych środowisk sieciowych.

RMON uwzględnia dwa aspekty: NMS oraz agentów działających na każdym urządzeniu sieciowym. NMS to zwykle host obsługujący oprogramowanie zarządzające agentami urządzeń sieciowych. Agentem jest zwykle przełącznik lub router, który zbiera statystyki ruchu (takie jak całkowita liczba pakietów segmentu sieci w określonym przedziale czasowym lub całkowita liczba prawidłowych pakietów wysyłanych do hosta). W oparciu o protokół SNMP, NMS zbiera dane sieciowe poprzez komunikację z agentami. Jednakże NMS nie może pozyskać wszystkich danych z bazy MIB RMON ze względu na ograniczone zasoby urządzenia. Zasadniczo NMS może uzyskać informacje tylko o czterech następujących grupach: Statistics (Statystyki), History (Historia), Event (Zdarzenie) i Alarm.

- **Statistics:** Zbiera statystyki portu Ethernet (takie jak całkowita wartość odebranych bajtów, całkowita liczba pakietów broadcast oraz całkowita liczba pakietów o określonym rozmiarze) w ramach interfejsu.
- **History:** Zapisuje Historię statystyk portów Ethernet w określonych interwałach sondowania.
- **Event:** Określa działanie, które zostanie podjęte, gdy Alarm wywoła Zdarzenie. Działanie może polegać na wygenerowaniu pozycji dziennika lub komunikatu trap SNM.
- **Alarm:** Monitoruje określony obiekt bazy MIB przez ustalony czas, wyzwala zdarzenie o określonej wartości (próg wzrostu lub próg spadku).

4 Konfiguracja RMON

Konfiguracja RMON umożliwia:

- Konfigurację Statystyk.
- Konfigurację Historii.
- Konfigurację Zdarzeń.
- Konfigurację Alarmu.

Wskazówki dotyczące konfiguracji

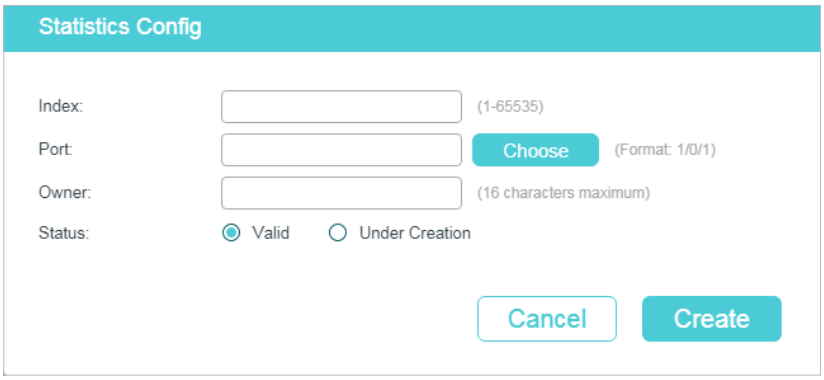
Aby mieć pewność, że NMS poprawnie odbiera powiadomienia, skonfiguruj najpierw SNMP i powiadomienia SNMP.

4.1 Przez GUI

4.1.1 Konfiguracja Statystyk

Wybierz z menu **MAINTENANCE > SNMP > RMON > Statistics** i kliknij Add , aby wyświetlić poniższą stronę.

Rys. 4-1 Dodawanie pozycji do Statystyk



Wykonaj poniższe kroki, aby skonfigurować Statystyki:

1) Podaj numer identyfikacyjny pozycji, monitorowany port i nazwę właściciela wpisu. Ustaw dla pozycji stan Valid lub Under Creation.

Index	Podaj numer identyfikacyjny pozycji.
Port	Kliknij **Choose,** aby wybrać port Ethernet, który ma być monitorowany lub podaj numer portu w formacie 1/0/1.
Owner	Podaj nazwę właściciela pozycji, używając od 1 do 16 znaków.

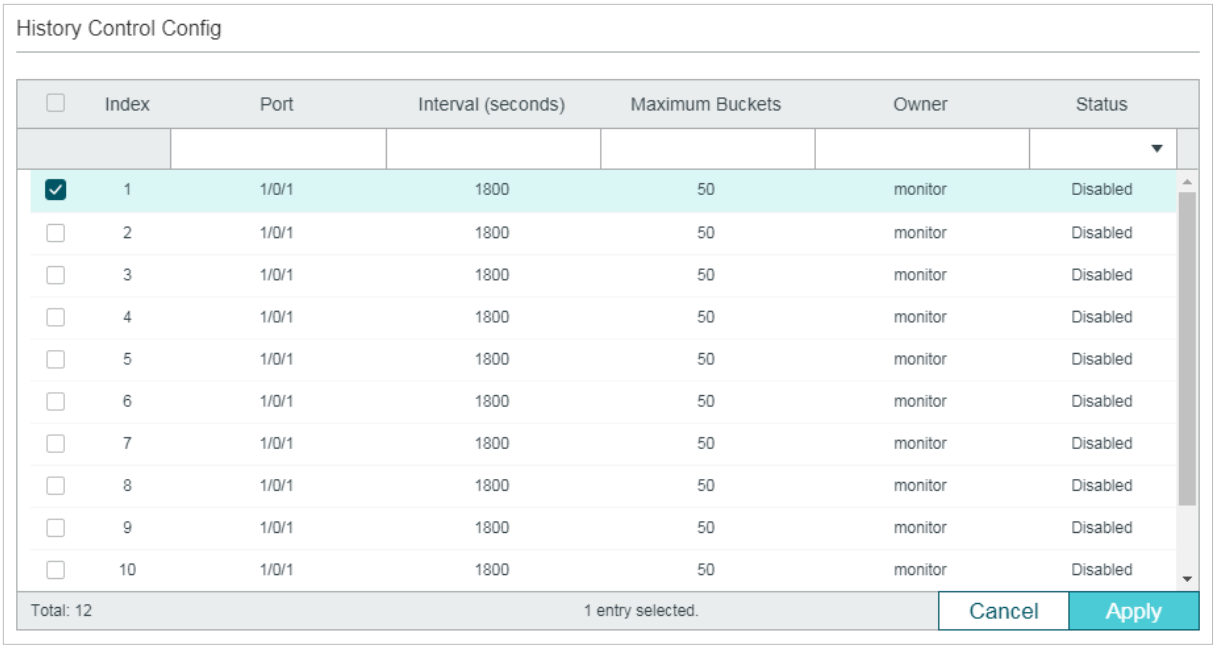
Status	Ustaw stan wpisu, wybierając spośród opcji Valid i Under Creation. Domyślnym ustawieniem jest Valid, które powoduje, że przełącznik automatycznie zaczyna zbierać statystyki z portu Ethernet dla tej pozycji. **Valid**: Pozycja została utworzona i jest aktywna. **Under Creation**: Pozycja została utworzona, ale nie jest aktywna.

2) Kliknij **Create**.

4.1.2 Konfiguracja Historii

Wybierz z menu **MAINTENANCE > SNMP > RMON > History**, aby wyświetlić poniższą stronę.

Rys. 4-2 Konfiguracja wpisu Historii



Wykonaj poniższe kroki, aby skonfigurować grupę Historii:

1) Wybierz pozycję Historii i wybierz monitorowany port.

Index	Numer identyfikacyjny wpisu Historii. Maksymalnie można dodać 12 pozycji.
Port	Podaj numer portu, który ma być monitorowany, w formacie 1/0/1.

2) Ustaw częstotliwość próbkowania i maksymalną liczbę wyników dla wpisu Historii.

Interval (seconds)	Ustal częstotliwość próbkowania. Prawidłowe wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund. Każdy wpis Historii ma swoje własne ustawienia czasu. W przypadku monitorowanego portu przełącznik pobiera informacje o pakietach i generuje wynik w ramach każdego interwału.

Maximum Buckets	Ustaw maksymalną liczbę wpisów Historii. Gdy liczba wpisów przekroczy limit, najwcześniejsza pozycja zostanie nadpisana. Prawidłowe wartości wahają się od 10 do 130, a wartością domyślną jest 50.

3) Podaj nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

Owner	Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.
Status	Włącz lub wyłącz pozycję. Domyślnie pozycja jest wyłączona. **Enable**: Pozycja jest włączona. **Disable**: Pozycja jest wyłączona.

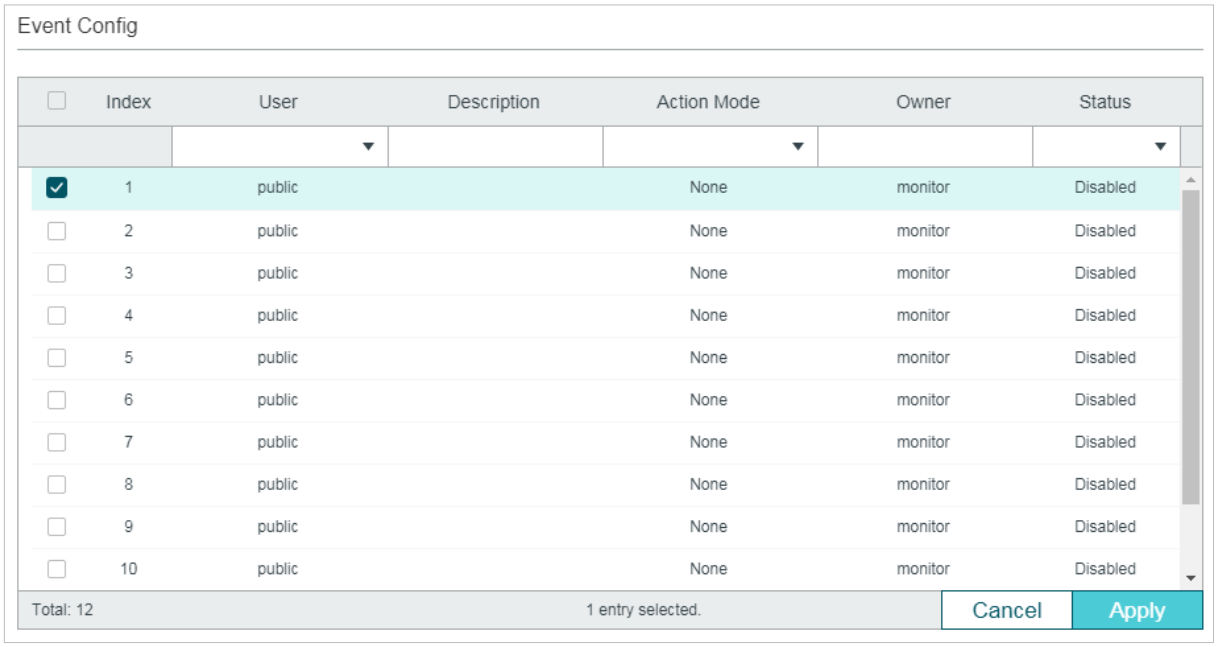
Uwaga:

Aby zmiana parametrów wpisu Historii była możliwa, pozycja musi być włączona. W przeciwnym razie zmiany nie zostaną wprowadzone.

4.1.3 Konfiguracja Zdarzeń

Wybierz z menu **MAINTENANCE > SNMP > RMON > Event**, aby wyświetlić poniższą stronę.

Rys. 4-3 Konfiguracja wpisu Zdarzeń



Wykonaj poniższe kroki, aby skonfigurować grupę Zdarzeń:

1) Wybierz wpis Zdarzeń i ustaw dla pozycji użytkownika SNMP.

Index	Numer identyfikacyjny wpisu Zdarzenia. Maksymalnie można dodać 12 pozycji.

User	Wybierz nazwę użytkownika lub nazwę społeczności SNMP dla pozycji. Nazwa powinna się zgadzać z wcześniejszymi ustawieniami SNMP.

2) Uzupełnij opis zdarzenia i działanie, które należy podjąć po wywołaniu zdarzenia.

Description	Wprowadź krótki opis tego zdarzenia, aby ułatwić jego identyfikację.
Action Mode	Określ działanie, które podejmie przełącznik po wywołaniu zdarzenia. **None**: Brak działania. Opcja jest domyślnie włączona. **Log**: Przełącznik rejestruje zdarzenie w dzienniku, a NMS, aby otrzymywać powiadomienia, powinien inicjować żądania. **Notify**: Przełącznik przesyła powiadomienia do NMS. **Log & Notify**: Przełącznik rejestruje zdarzenie w dzienniku i przesyła powiadomienia do NMS.

3) Uzupełnij nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

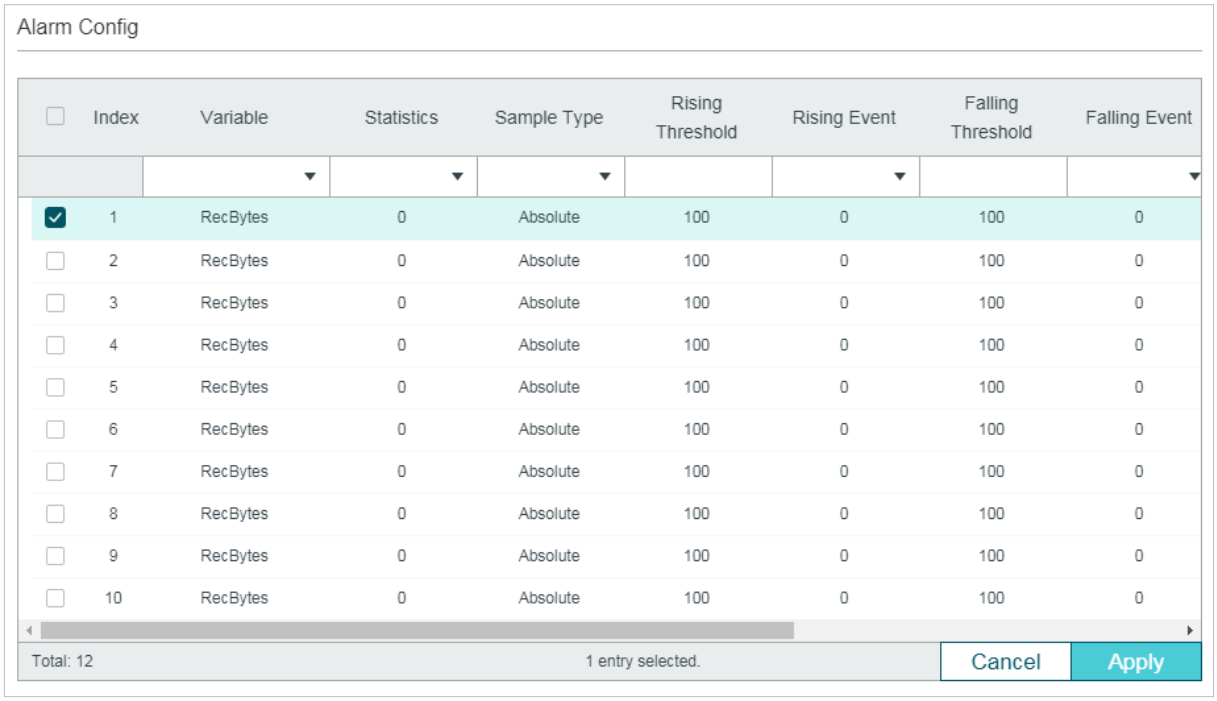
Owner	Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.
Status	Włącz lub wyłącz pozycję. Domyślnie pozycja jest wyłączona. **Enable**: Pozycja jest włączona. **Disable**: Pozycja jest wyłączona.

4.1.4 Konfiguracja Alarmu

Przed rozpoczęciem konfiguracji dostosuj ustawienia Statystyk i Zdarzeń, ponieważ wpisy Alarmu muszą być zgodne z wcześniej skonfigurowanymi wpisami Statystyk i Zdarzeń.

Wybierz z menu **MAINTENANCE > SNMP > RMON > Alarm**, aby wyświetlić poniższą stronę.

Rys. 4-4 Konfiguracja wpisu Alarmu



Wykonaj poniższe kroki, aby skonfigurować grupę Alarmu:

1) Wybierz wpisy Alarmu i zmienne, które będą monitorowane, a następnie powiąż wpisy z pozycjami Statystyk.

Index	Numer identyfikacyjny wpisu Alarmu. Maksymalnie można dodać 12 pozycji.
Variable	Wybierz zmienne, które będę kontrolowane. Przełącznik będzie monitorować wybrane zmienne cyklicznie i reagować w ustalony sposób na uruchomienia alarmu. Domyślnie wybraną zmienną jest RecBytes. **RecBytes**: Łącznie odebrane bajty. **RecPackets**: Łącznie odebrane pakiety. **BPackets**: Całkowita liczba pakietów broadcast. **MPackets**: Całkowita liczba pakietów multicast. **CRC&Align ERR**: Pakiety o wielkości od 64 do 1518 bajtów, zawierające błąd FCS lub błąd wyrównania. **Undersize**: Pakiety mniejsze niż 64 bajty. **Oversize**: Pakiety większe niż 1518 bajtów. **Jabbers**: Pakiety wysyłane po wystąpieniu kolizji portów. **Collisions**: Czasy kolizji w segmencie sieci. **64, 65-127, 128-255, 256-511, 512-1023, 1024-10240**: Łączna liczba pakietów o określonym rozmiarze.

Statistics	Powiąż wpis Alarmu z wpisem Statystyk. Przełącznik będzie monitorować określoną zmienną wpisu Statystyk.

2) Wybierz typ próbkowania, próg wzrostu i spadku, odpowiedni tryb działania dla zdarzenia oraz typ alarmu dla wpisu.

Sample Type	Wybierz metodę próbkowania dla określonej zmiennej Domyślnym ustawieniem jest absolute. **Absolute**: Porównuje wartość próbkowania z ustawionym progiem. **Delta**: Przełącznik oblicza różnicę pomiędzy wartościami próbkowania bieżącego i poprzedniego cyklu, a następnie porównuje tą różnicę z ustawionym progiem.
Rising Threshold	Ustaw próg wzrost dla zmiennej. Gdy wartość próbkowania przekroczy ustawiony próg, system uruchomi odpowiednie zdarzenie (**Rising Event**). Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.
Rising Event	Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania przekroczy ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.
Falling Threshold	Ustaw prób spadku dla zmiennej. Gdy wartość próbkowania będzie niższa niż ustawiony próg, system uruchomi odpowiednie zdarzenie (**Falling Event).** Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.
Falling Event	Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania będzie niższa niż ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.
Alarm Type	Określ typ alarmu dla wpisu. Domyślnym typem alarmu jest all. **Rising**: Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania przekracza ustawiony próg wzrostu. **Falling**: Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania jest niższa od ustawionego progu spadku. **All**: Alarm uruchamiany jest, gdy wartość próbkowania przekracza ustawiony próg wzrostu lub jest niższa od ustawionego progu spadku.

3) Podaj nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

Interval (seconds)	Ustaw interwał próbkowania. Poprawne wartości wynoszą od 10 do 3600 sekund, a wartość domyślna to 1800 sekund.
Owner	Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.

Status	Włącz lub wyłącz wpis. Domyślnie pozycja jest wyłączona. **Enable**: Wpis jest włączony. **Disable**: Wpis jest wyłączony.

4.2 Przez CLI

4.2.1 Konfiguracja Statystyk

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**rmon statistics** *index* **interface interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**owner** *owner-name*] [**status** { underCreation | valid }] Skonfiguruj wpisy Statystyk RMON. *index:* Uzupełnij ID wpisu Statystyk wartością z przedziału 1 - 65535 w formacie 1-3 lub 5. *port:* Wprowadź numer portu w formacie 1/0/1, aby przypisać go do wpisu. *owner-name:* Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor. underCreation | valid: Ustaw stan wpisu. UnderCreation oznacza, że wpis został utworzony, ale nie jest aktywny, natomiast Valid oznacza, że wpis został utworzony i jest aktywny. Domyślnym ustawieniem jest valid. Stan Valid oznacza, że przełącznik automatycznie zaczyna zbierać statystyki z portu Ethernet dla tej pozycji Statystyk.
Krok 3	**show rmon statistics** [*index*] Wyświetla wpisy Statystyk i ich ustawienia. *index:* Wpisz numery identyfikacyjne wpisów Statystyk, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 65535.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisów Statystyk na przełączniku do monitorowania odpowiednio portu 1/0/1 oraz portu 1/0/2. Właścicielem obu wpisów będzie monitor, a wartością stanu Valid:

Switch#configure

Switch(config)#rmon statistics 1 **interface gigabitEthernet** 1/0/1 **owner** monitor **status** valid

Switch(config)#rmon statistics 2 **interface gigabitEthernet** 1/0/2 **owner** monitor **status** valid

Switch(config)#show rmon statistics

Index	Port	Owner	State
-----	----	-----	-----
1	Gi1/0/1	monitor	valid
2	Gi1/0/2	monitor	valid

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 Konfiguracja Historii

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Step 2	**rmon history** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**interval** *seconds*] [**owner** *owner-name*] [**buckets** *number*] Konfiguracja wpisów Historii RMON. *index:* Uzupełnij numer identyfikacyjny wpisu Historii wartością z przedziału 1 - 12 w formacie 1-3 lub 5. *port:* Wprowadź numer portu w formacie 1/0/1, aby przypisać go do wpisu. *seconds:* Ustaw częstotliwość próbkowania. Wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund. *owner-name:* Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor. *number:* Ustaw maksymalną liczbę wpisów Historii. Gdy liczba wpisów przekroczy limit, najwcześniejsza pozycja zostanie nadpisana. Prawidłowe wartości wahają się od 10 do 130, a wartością domyślną jest 50.
Krok 3	**show rmon history** [*index*] Wyświetla skonfigurowany wpis Historii i jego ustawienia. *index:* Wpisz numery identyfikacyjne wpisów Historii, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).

Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową sposób tworzenia wpisu Historii na przełączniku do monitorowania portu 1/0/1. Wartością częstotliwości próbkowania będzie 100 sekund, maksymalną liczbą wpisów 50, a właścicielem monitor:

Switch#configure

Switch(config)#rmon history 1 **interface gigabitEthernet** 1/0/1 **interval** 100 **owner** monitor **buckets** 50

Switch(config)#show rmon history

Index	Port	Interval	Buckets	Owner	State
1	Gi1/0/1	100	50	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

4.2.3 Konfiguracja Zdarzeń

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.
Krok 2	**rmon event** *index* [**user** *user-name*] [**description** *description*] [**type** { none | log | notify | log-notify }] [**owner** *owner-name*] Konfiguracja wpisów Zdarzeń RMON. *index:* Uzupełnij numer identyfikacyjny wpisu Zdarzeń wartością z przedziału 1 - 12 w formacie 1-3 lub 5. *user-name:* Wybierz nazwę użytkownika lub nazwę społeczności SNMP dla pozycji. Nazwa powinna się zgadzać z wcześniejszymi ustawieniami SNMP. Domyślna nazwa to public. *description:* Wprowadź krótki opis dla wpisu, używając od 1 do 16 znaków. Domyślnie opis jest pusty. none | log | notify | log-notify: Określ działanie, które podejmie przełącznik po wywołaniu zdarzenia. Domyślnie ustawionym typem jest none. None oznacza brak działania, log oznacza, że przełącznik rejestruje zdarzenie, notify oznacza, że przełącznik wysyła powiadomienia do NMS, a log-notify oznacza, że przełącznik rejestruje zdarzenie i wysyła powiadomienia do NMS. *owner-name:* Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.

Krok 3	**show rmon event** [*index*] Wyświetla skonfigurowany wpis Zdarzeń i jego ustawienia. *index:* Wpisz numery identyfikacyjne wpisów Zdarzeń, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu Zdarzeń na przełączniku. Nazwą użytkownika będzie admin, typem zdarzenia Notify (przełącznik przesyła powiadomienia do NMS), a właścicielem monitor:

Switch#configure

Switch(config)#rmon event 1 **user** admin **description** rising-notify **type** notify **owner** monitor

Switch(config)#show rmon event

Index	User	Description	Type	Owner	State
1	admin	rising-notify	Notify	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

4.2.4 Konfiguracja Alarmu

Krok 1	**configure** Uruchom tryb konfiguracji globalnej.

Krok 2 **rmon alarm** *index* **stats-index** *sindex* [**alarm-variable** { revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-10240}] [**s-type** {absolute | delta}] [**rising-threshold** *r-hold*] [**rising-event-index** *r-event*] [**falling-threshold** *f-hold*] [**falling-event-index** *f-event*] [**a-type** {rise | fall | all}] [**owner** *owner-name*] [**interval** *interval*]

Skonfiguruj wpisy Alarmu RMON.

index: Uzupełnij numer identyfikacyjny wpisu Alarmu wartością z przedziału 1 - 12 w formacie 1-3 lub 5.

sindex: Ustaw numery identyfikacyjne powiązanych wpisów Statystyk (od 1 do 65535).

revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65- 127 | 128-255 | 256-511 | 512-1023 | 1024-10240: Wybierz zmienne, które będę kontrolowane. Przełącznik będzie monitorować wybrane zmienne cyklicznie i reagować w ustalony sposób na uruchomienia alarmu. Domyślnie wybraną zmienną jest revbyte.

revbyte oznacza łącznie odebrane bajty; revpkt oznacza łącznie odebrane pakiety; bpkt oznacza całkowitą liczbę pakietów broadcast. mpkt oznacza całkowitą liczbę pakietów multicast; crc-align oznacza pakiety o wielkości od 64 do 1518 bajtów, zawierające błąd FCS lub błąd wyrównania; undersize oznacza pakiety mniejsze niż 64 bajty; oversize oznacza pakiety większe niż 1518 bajty; jabber oznacza pakiety wysyłane po wystąpieniu kolizji portów; collision oznacza Czasy kolizji w segmencie sieci; 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-10240 oznacza łączną liczbę pakietów o określonym rozmiarze.

absolute | delta: Wybierz metodę próbkowania dla określonej zmiennej Domyślnym ustawieniem jest absolute. W trybie absolute przełącznik porównuje wartość próbkowania z ustawionym progiem; w trybie delta przełącznik oblicza różnicę pomiędzy wartościami próbkowania bieżącego i poprzedniego cyklu, a następnie porównuje tą różnicę z ustawionym progiem.

r-hold: Ustaw próg wzrost dla zmiennej. Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.

r-event: Podaj numer identyfikacyjny wpisu Zdarzenia (od 1 do 12), które będzie uruchamiane, gdy wartość próbkowania przekroczy ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.

f-hold: Ustaw prób spadku dla zmiennej. Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.

f-event: Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania będzie niższa niż ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.

rise | fall | all: Określ typ alarmu. Domyślnym ustawieniem jest all. Rise oznacza, że Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania przekracza ustawiony próg wzrostu. Fall oznacza, że alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania jest niższa od ustawionego progu spadku. All oznacza, że alarm uruchamiany jest, gdy wartość próbkowania przekracza ustawiony próg wzrostu lub jest niższa od ustawionego progu spadku.

owner-name: Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.

interval: Ustaw częstotliwość próbkowania. Wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund.

Krok 3	**show rmon alarm** [*index*] Wyświetla skonfigurowany wpis Alarmu i jego ustawienia. *index:* Wpisz numery identyfikacyjne wpisów Alarmu, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5.
Krok 4	**end** Powróć do trybu uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu Alarmu do monitorowania BPackets na przełączniku. ID powiązanego wpisu Statystyk będzie 1, typem próbkowania Absolute, progiem wzrostu 3000, numerem identyfikacyjnym powiązanego wpisu zdarzenia dla wzrostu 1, progiem spadku 2000, numerem identyfikacyjnym powiązanego zdarzenia dla spadku 2, typem alarmu all, interwałem powiadomień 10 sekund, a właścicielem wpisu monitor:

Switch#configure

Switch(config)#rmon alarm 1 **stats-index** 1 **alarm-variable** bpkt **s-type** absolute **rising-threshold** 3000 **rising-event-index** 1 **falling-threshold** 2000 **falling-event-index** 2 **a-type** all **interval** 10 **owner** monitor

Switch(config)#show rmon alarm

Index-State: 1-Enabled

Statistics index: 1

Alarm variable: BPkt

Sample Type: Absolute

RHold-REvent: 3000-1

FHold-FEvent: 2000-2

Alarm startup: All

Interval: 10

Owner: monitor

Switch(config)#end

Switch#copy running-config startup-config

Część 29

Diagnostyka urządzenia i sieci

ROZDZIAŁY

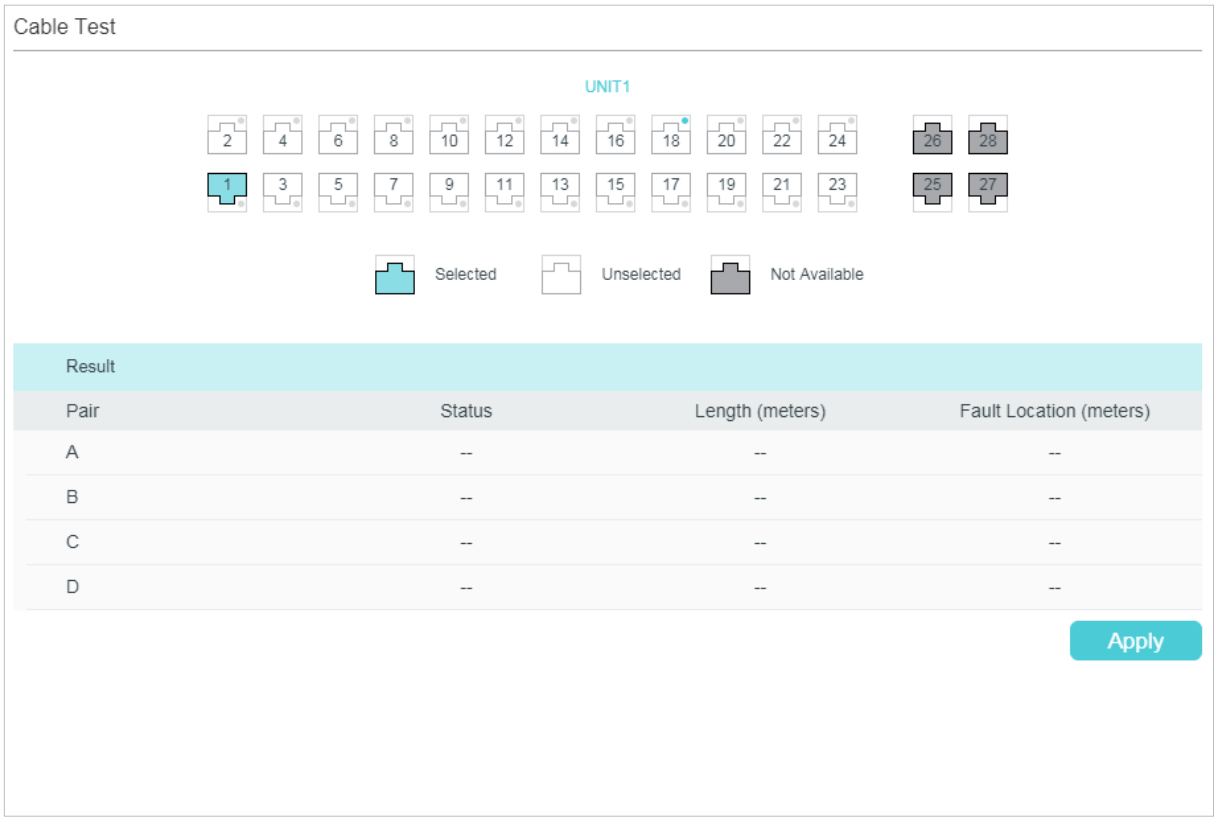
1 Diagnostyka urządzenia

Diagnostyka urządzenia polega na testowaniu kabli. Funkcja umożliwia rozwiązywanie problemów związanych ze stanem połączenia, długością kabla czy lokalizacją usterki.

1.1 Przez GUI

Wybierz menu **MAINTENANCE > Device Diagnostics**, aby załadować następującą stronę.

Rys. 1-1 Diagnostyka kabla



Aby sprawdzić stan kabla, postępuj zgodnie z poniższymi krokami.

1) Wybierz port do przeprowadzenia testu i kliknij **Apply**.
2) Sprawdź wyniki testu w sekcji **Result**.

Pair	Informacja o numerze pary.

Status	Informacja o stanie kabla. Dostępne opcje to: normal, closed, open i crosstalk. **Normal**: Kabel jest podłączony normalnie (standardowo). **Closed**: Nieprawidłowy kontakt przewodów w kablu spowodował zwarcie w obwodzie. **Open**: Do drugiego końca nie jest podłączone żadne urządzenie, co spowodowało błąd połączenia. **Crosstalk**: Niedopasowanie rezystencji spowodowane słabą jakością kabla.
Length	Jeżeli stan kabla to Normal, w tym miejscu wyświetlana jest informacja o zakresie długości kabla.
Fault Location	Jeżeli stan kabla to Short, Close lub Crosstalk, w tym miejscu wyświetlana jest informacja o odległości między portem a lokalizacją usterki.

1.2 Przez CLI

W trybie użytkownika uprzywilejowanego (privileged EXEC mode) tak jak w każdym innym trybie konfiguracji za pomocą poniższego polecenia sprawdzić można stan połączenia kabla podłączonego do przełącznika.

show cable-diagnostics interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Wyświetl wyniki diagnostyki kabla podłączonego portu Ethernet.

port: Wpisz numer portu w formacie 1/0/1, aby sprawdzić wyniki testu kabla.

show cable-diagnostics careful interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Wyświetl wyniki diagnostyki kabla podłączonego portu Ethernet. Po przeprowadzeniu szczegółowego testu kabli, przełącznik będzie testował jedynie kabel dla portu ze statusem tzw. łącza w dół.

port: Wpisz numer portu w formacie 1/0/1, aby sprawdzić wyniki testu kabla.

Poniższy przykład prezentuje sprawdzanie wyników diagnostyki kabla portu 1/0/2:

Switch#show cable-diagnostics interface gigabitEhternet 1/0/2

Port	Pair	Status	Length	Error
Gi1/0/2	Pair-A	Normal	2 (+/- 10m)	---
	Pair-B	Normal	2 (+/- 10m)	---
	Pair-C	Normal	0 (+/- 10m)	---
	Pair-D	Normal	2 (+/- 10m)	---

2 Diagnostyka sieci

Funkcja diagnostyki sieci polega na testowaniu Ping i testowaniu Tracert. Możesz przeprowadzić test połączenia z hostami zdalnymi lub z bramami, od przełącznika do punktu docelowego.

Funkcja diagnostyki sieci (Network Diagnostics) umożliwia:

- rozwiązywanie problemów przez testowanie Ping,
- rozwiązywanie problemów przez testowanie Tracert.

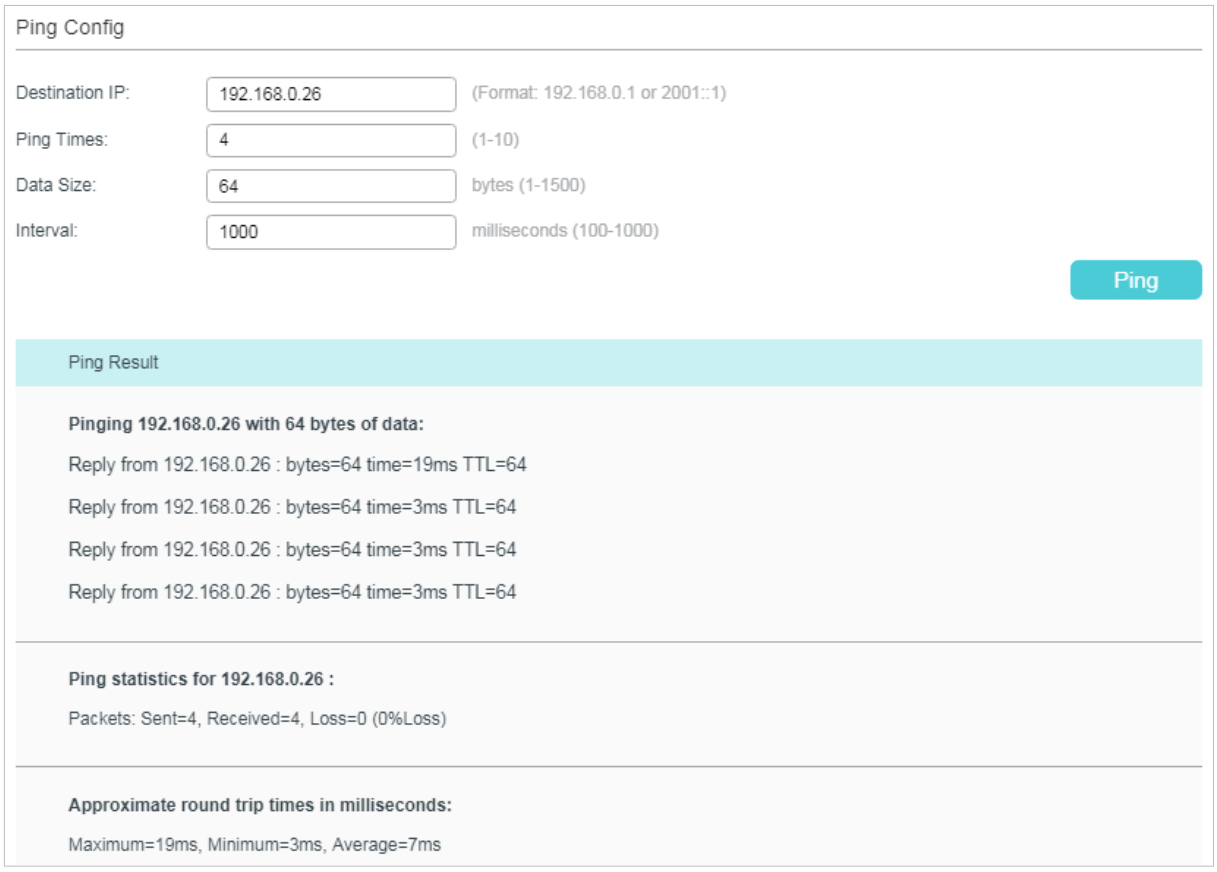
2.1 Przez GUI

2.1.1 Rozwiązywanie problemów przez testowanie Ping

Możesz wykorzystać narzędzie Ping do przetestowania połączenia ze zdalnymi hostami.

Wybierz menu **MAINTENANCE > Network Diagnostics > Ping**, aby załadować następującą stronę.

Rys. 2-1 Rozwiązywanie problemów przez testowanie Ping



Aby sprawdzić stan połączenia między przełącznikiem a innym urządzeniem w sieci, postępuj zgodnie z poniższymi krokami.

1) W sekcji **Ping Config** wpisz adres IP urządzenia docelowego w teście Ping, ustaw dowolnie wartość Ping times, rozmiar danych oraz interwał i kliknij **Ping, aby rozpocząć test**.

Destination IP	Wpisz adres IP węzła docelowego w teście Ping. Obsługiwane są adresy IPv4 i IPv6.
Ping Times	Wpisz, ile razy dane testowe będą przesłane do testowania Ping. Zaleca się zachowanie wartości domyślnej, wynoszącej 4.
Data Size	Wpisz rozmiar danych wysłanych do testowania Ping. Zaleca się zachowanie wartości domyślnej, wynoszącej 64 bajty.
Interval	Wyznacz odstęp czasu, w którym wysyłane będą pakiety żądania ICMP. Zaleca się zachowanie wartości domyślnej, wynoszącej 1000 milisekund.

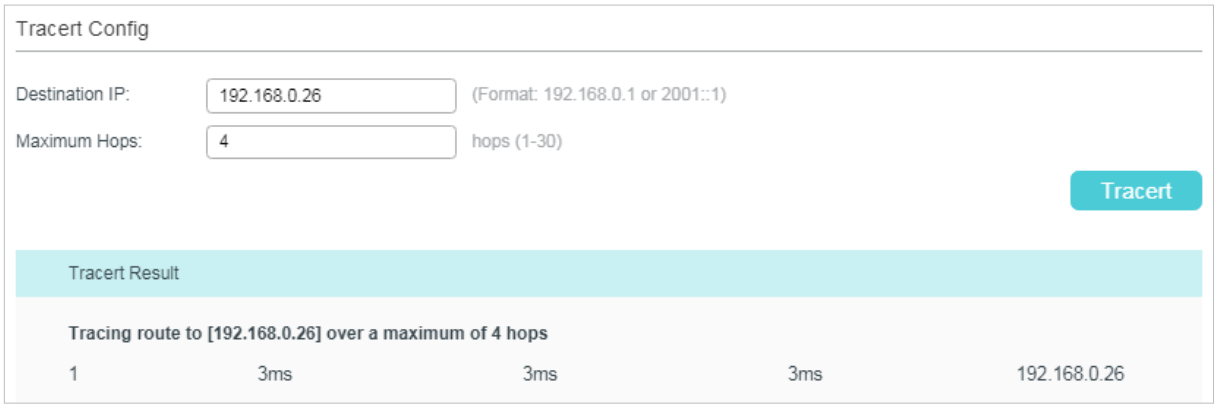
2) W sekcji **Ping Result** sprawdź wyniki testu.

2.1.2 Rozwiązywanie problemów przez testowanie Tracert

Możesz wykorzystać narzędzie Tracert to odszukania ścieżki między przełącznikiem a punktem docelowym i przetestowania połączenia między przełącznikiem i routerami wzdłuż ścieżki.

Wybierz menu **MAINTENANCE > Network Diagnostics > Tracert**, aby załadować następującą stronę.

Rys. 2-2 Rozwiązywanie problemów przez testowanie Tracert



Aby sprawdzić połączenie między przełącznikiem i routerami wzdłuż ścieżki od źródła do punktu docelowego, postępuj zgodnie z poniższymi krokami:

1) W sekcji **Tracert Config** wpisz adres IP punktu docelowego, ustaw maks. liczbę przeskoków i kliknij **Tracert**, aby rozpocząć test.

Destination IP	Wpisz adres IP urządzenia docelowego. Obsługiwane są IPv4 i IPv6.

Maximum Hops	Wpisz maks. liczbę przeskoków na ścieżce, przez które mogą przejść dane testowe.

2) W sekcji **Tracert Result** sprawdź wyniki testu.

2.2 Przez CLI

2.2.1 Konfiguracja testu Ping

W trybie użytkownika uprzywilejowanego (privileged EXEC mode) za pomocą poniższego polecenia sprawdzić można stan połączenia między przełącznikiem a węzłem sieci.

ping [ip | ipv6 **] {** *ip_addr* **} [-n** *count* **] [-l** *size* **] [-i** *interval* **]**

Przetestuj połączenie między przełącznikiem a urządzeniem docelowym.

ip: Wymagany typ adresu IP do testu Ping to IPv4.

ipv6: Wymagany typ adresu IP do testu Ping to IPv6.

ip_addr: Adres IP węzła docelowego w teście Ping. Jeżeli nie ustawiono parametru ip/ipv6, obsługiwane będą zarówno adresy IPv4, jak i IPv6d (np. 192.168.0.100 lub fe80::1234).

count: Wyznacz, ile razy wysyłane będą dane to testu Ping. Wartość powinna wynosić od 1 do 10 razy; wartość domyślna to 4.

size: Wpisz rozmiar danych wysłanych do testowania Ping. Wartość powinna wynosić między 1 a 1500 bajtów; wartosc domyślna to 64 bajty

interval: Wyznacz odstęp czasu, w którym wysyłane będą pakiety żądania ICMP. Wartość powinna wynosić między 100 a 1000 milisekund; wartość domyślna to 1000 milisekund

Poniższy przykład prezentuje testowanie połączenia między przełącznikiem a urządzeniem docelowym o adresie IP 192.168.0.10, wyznaczanie wartości Ping Times na 3, rozmiaru danych na 1000 bajtów i interwału na 500 milisekund:

Switch#ping ip 192.168.0.10 **-n** 3 **-l** 1000 **-i** 500

Pinging 192.168.0.10 with 1000 bytes of data :

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Ping statistics for 192.168.0.10:

Packets: Sent = 3 , Received = 3 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms , Maximum = 0ms , Average = 0ms

2.2.2 Konfiguracja testu Tracert

W trybie użytkownika uprzywilejowanego (privileged EXEC mode) za pomocą poniższego polecenia sprawdzić można stan połączenia między przełącznikiem a routerami wzdłuż ścieżki od źródła do punktu docelowego.

tracert [ip | ipv6] *ip_addr* [*maxHops*]

Sprawdź połączenie bram wzdłuż ścieżki od źródła do punktu docelowego.

ip: Wymagany typ adresu IP do testu Tracert to IPv4.

ipv6: Wymagany typ adresu IP do testu Tracert to IPv6.

ip_addr: Wpisz adres IP urządzenia docelowego. Jeżeli nie ustawiono parametru ip/ipv6, obsługiwane będą zarówno adresy IPv4, jak i IPv6d (np. 192.168.0.100 lub fe80::1234).

maxHops: Określ maks. liczbę przeskoków na ścieżce, przez które mogą przejść dane testowe, między 1 a 30; wartość domyślna to 4 przeskoki.

Poniższy przykład prezentuje testowanie połączenia miedzy przełącznikiem a urządzeniem sieciowym o adresie IP 192.168.0.100. Maks. liczba przeskoków to 2:

Switch#tracert 192.168.0.100 2

Tracing route to 192.168.0.100 over a maximum of 2 hops

1 8 ms 1 ms 2 ms 192.168.1.1

2 2 ms 2 ms 2 ms 192.168.0.100

Trace complete.

Część 30

Konfiguracja dzienników systemowych

ROZDZIAŁY

1 Konfiguracja dzienników systemowych

Na konfigurację dzienników systemowych składają się:

- konfiguracja dzienników lokalnych;
- konfiguracja dzienników zdalnych;
- tworzenie kopii zapasowych dzienników;
- wyświetlanie tablicy dzienników.

Wskazówki dotyczące konfiguracji

Zdarzenia systemowe klasyfikuje się przez przypisywanie ich do jednego z ośmiu poziomów. Im niższy poziom zdarzenia, tym mniej poważne, niebezpieczne jest zdarzenie. Komunikaty poziomów 0-4 świadczą o pogorszeniu działania przełącznika. W przypadku komunikatu o zdarzeniu należy podjąć sugerowane działanie.

Tabela 1-1 Poziomy zdarzeń

Komunikaty	Poziom	Opis	Przykład
Emergencies	0	System nie działa i konieczny jest restart przełącznika.	Usterki oprogramowania wpływające na działanie przełącznika.
Alerts	1	Należy natychmiastowo podjąć odpowiednie działania.	Wykorzystanie pamięci osiągnęło wyznaczony limit.
Critical	2	Należy natychmiastowo podjąć odpowiednie działania lub przeprowadzić analizę przyczyn.	Wykorzystanie pamięci osiągnęło próg ostrzegawczy.
Errors	3	Błędne działania lub niestandardowe przetwarzanie, które nie wpłyną na kolejne działania. Powinny jednak zostać przeanalizowane.	Wprowadzono błędne polecenie lub hasło.
Warnings	4	Warunki, które mogą spowodować błąd przetwarzania i które powinny być odnotowane.	Wykryto błędne pakiety protokołu.
Notifications	5	Standardowe, ale istotne warunki.	Zastosowano polecenie zamknięcia portu.
Informational	6	Standardowe komunikaty informacyjne.	Zastosowano polecenie wyświetlania.
Debugging	7	Komunikaty z poziomu śledzenia, które możesz zignorować.	Standardowe informacje operacyjne.

1.1 Przez GUI

1.1.1 Konfiguracja dzienników lokalnych

Wybierz menu **MAINTENANCE > Logs > Local Logs**, aby załadować następującą stronę.

Rys. 1-1 Konfiguracja dzienników lokalnych

Aby skonfigurować dzienniki lokalne, postępuj zgodnie z poniższymi krokami:

1) Wybierz kanał i skonfiguruj odpowiedni poziom istotności zdarzenia oraz stan kanału.

Channel	Dzienniki lokalne zawierają 2 kanały: Log buffer (bufor dziennika) i Log file (plik dziennika). Bufor dziennika wskazuje RAM do zapisywania dzienników systemowych. Kanał jest domyślnie włączony. Informacje z buforu dziennika wyświetlane są na stronie **MAINTENANCE > Logs > Logs Table**. Po restarcie przełącznika dane zostaną utracone. Plik dziennika wskazuje na sektor pamięci flash do zapisywania dzienników systemowych. Informacje zapisane w pliku dziennika nie zostaną utracone po restarcie przełącznika i mogą być wyeksportowane na stronie **MAINTENANCE > Logs > Back Up Logs**.
Severity	Ustaw poziom istotności komunikatu zdarzenia zapisanego na wybranym kanale. Zapisywane będą tylko komunikaty o tym samym co wyznaczony tu poziom lub o niższym poziomie istotności. Istnieje osiem poziomów istotności, oznaczonych od 0 do 7. Im niższy poziom, tym istotniejsza jest wiadomość.
Status	Włącz lub wyłącz kanał.
Sync-Periodic	Domyślnie dane dziennika są natychmiastowo zapisywane w buforze dziennka i synchronizowane w pliku dziennika raz na 24 godziny. W razie konieczności możesz zmodyfikować częstotliwość synchronizacji dziennika, używając CLI.

2) Kliknij **Apply**.

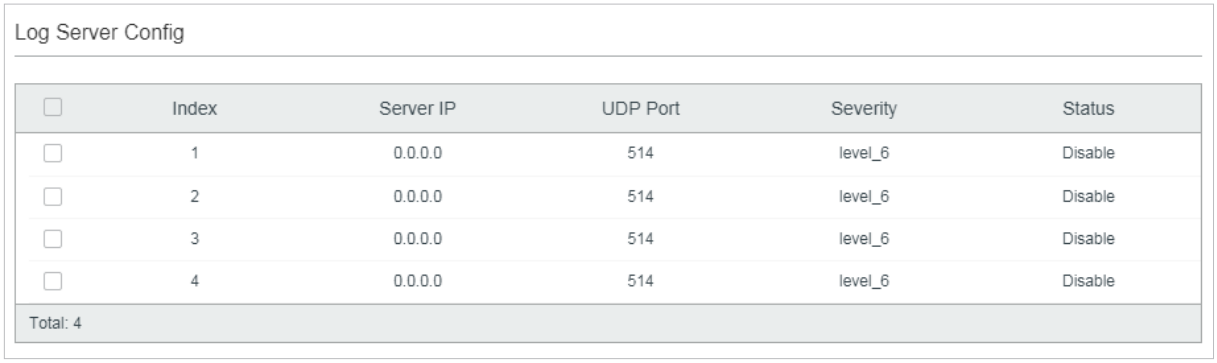
1.1.2 Konfiguracja dzienników zdalnych

Możesz skonfigurować otrzymywanie dzienników systemowych przełącznika na maks. czterech hostach. Hosty te nazywane są Log Servers (Serwery dzienników). Po wygenerowaniu komunikatu dziennika przełącznik będzie przekazywał komunikat do

serwerów. Aby wyświetlić dzienniki, serwery powinny obsługiwać oprogramowanie dziennika serwera zgodne ze standardem dzienników systemowych.

Wybierz menu **MAINTENANCE > Logs > Remote Logs**, aby załadować następującą stronę.

Rys. 1-2 Konfiguracja dzienników zdalnych



Aby skonfigurować dane serwerów dzienników zdalnych, postępuj zgodnie z poniższymi krokami.

1) Wybierz wpis do włączenia serwera, następnie ustaw adres IP serwera i poziom istotności zdarzenia.

Server IP	Wyznacz adres IP serwera dziennika.
UDP Port	Informacja o porcie UDP, wykorzystywanym przez serwer do odbierania komunikatów dziennika. Do wysyłania komunikatów dziennika przełącznik wykorzystuje standardowy port 514.
Severity	Określ poziom istotności komunikatów dziennika wysyłanych na wybrany serwer dziennika. Zapisywane będą tylko komunikaty o tym samym lub o niższym poziomie istotności.
Status	Włącz lub wyłącz serwer dziennika.

2) Kliknij **Apply**.

1.1.3 Tworzenie kopii zapasowych dzienników

Wybierz menu **MAINTENANCE > Logs > Back Up Logs**, aby załadować następującą stronę.

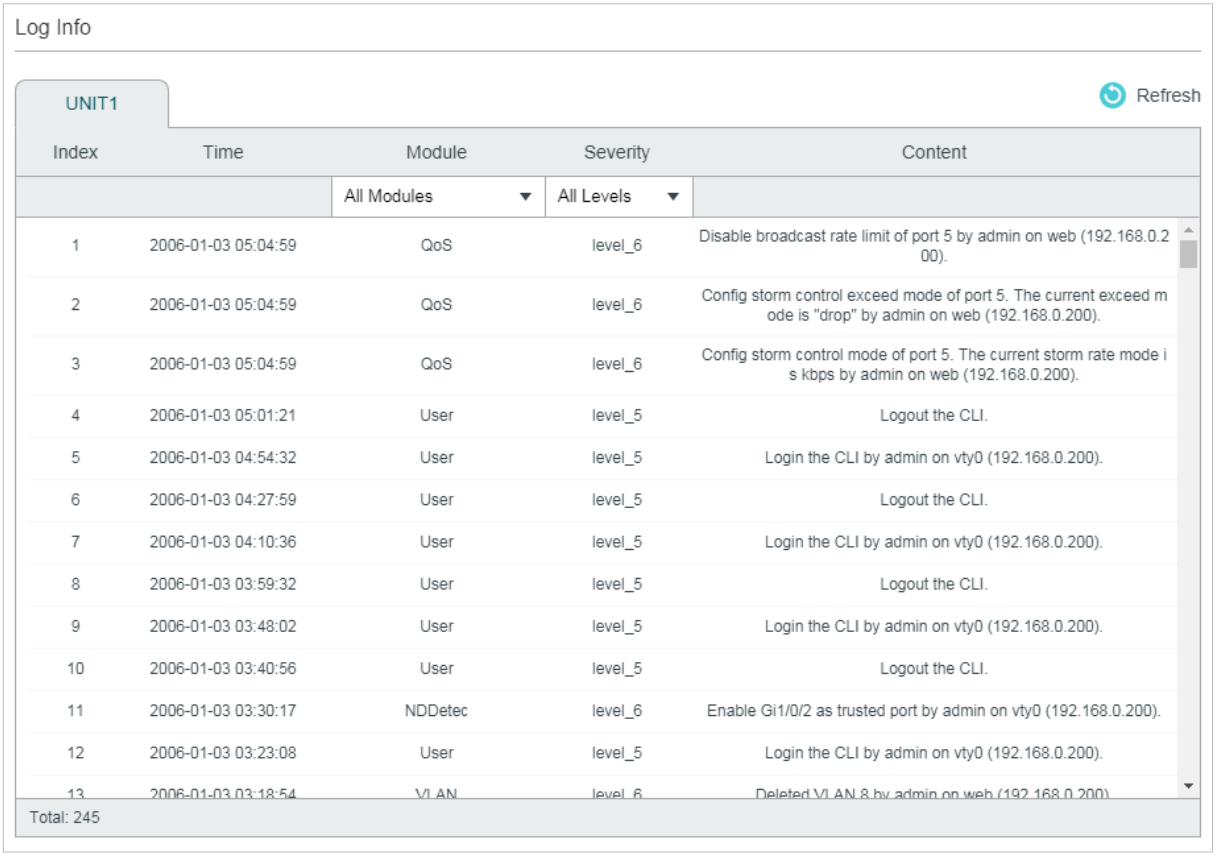
Rys. 1-3 Tworzenie kopii zapasowej pliku dziennika

Kliknij **Back Up Logs**, aby zapisać dzienniki systemowe jako plik na twoim komputerze. W przypadku awarii systemu przełącznika, możesz sprawdzić plik do rozwiązywania problemów.

1.1.4 Wyświetlanie tablicy dzienników

Wybierz menu **MAINTENANCE > Logs > Log Table**, aby załadować następującą stronę.

Rys. 1-4 Wyświetlanie tablicy dzienników



Wybierz blok i poziom istotności, aby wyświetlić odpowiednie dane dziennika.

Time	Informacja o czasie, w którym wystąpiło zdarzenie dziennika. Aby poznać dokładny czas zdarzenia, należy skonfigurować czas systemu na stronie zarządzania **SYSTEM > System Info > System Time**.
Module	Z rozwijanej listy wybierz blok, aby wyświetlić odpowiednie dane dziennika.
Severity	Wybierz poziom istotności. Wyświetlane będą tylko komunikaty o tym samym lub o niższym poziomie istotności.
Content	Szczegółowe dane zdarzenia dziennika.

1.2 Przez CLI

1.2.1 Konfiguracja dzienników lokalnych

Aby skonfigurować dzienniki lokalne, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.
Krok 2	**logging buffer** Skonfiguruj przełącznik tak, aby zapisywał komunikaty systemowe w buforze dziennika. Bufor dziennika wskazuje RAM do zapisywania dzienników systemowych. Po restarcie przełącznika dane w buforze dziennika zostaną utracone. Możesz wyświetlić dzienniki za pomocą polecenia show logging buffer.
Krok 3	**logging buffer level** */level* Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane w buforze. *level*: Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. Zapisywane będą tylko zdarzenia o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 6. Oznacza to, że w buforze dziennika zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 6.
Krok 4	**logging file flash** Skonfiguruj przełącznik tak, by komunikaty systemowe zapisywane były w pliku dziennika. Plik dziennika wskazuje na sektor pamięci flash do zapisywania dzienników systemowych. Informacje zapisane w pliku dziennika nie zostaną utracone po restarcie przełącznika. Możesz wyświetlić dzienniki za pomocą polecenia **show logging flash**.
Krok 5	**logging file flash frequency** { **periodic** *periodic* | **immediate** } Ustaw częstotliwość, z jaką synchronizowane będą dzienniki systemowe z bufora dziennika w sektorze pamięci flash. *periodic*: Wyznacz częstotliwość, między 1 a 48 godzin. Domyślnie synchronizacja przeprowadzana jest raz na 24 godziny. **immediate**: Plik dziennika systemowego w buforze będzie natychmiastowo synchronizowany w sektorze pamięci flash. Opcja ta oznacza, że częste działania w obszarze flash nie są zalecane.
Krok 6	**logging file flash level** */level* Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane w sektorze flash. *level*: Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. W sektorze flash zapisywane będą tylko komunikaty zdarzeń o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 3. Oznacza to, że w sektorze flash zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 3.
Krok 7	**show logging local-config** Sprawdź dane konfiguracyjne dzienników lokalnych.
Krok 8	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).

Krok 9	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację na przełączniku dzienników lokalnych. W buforze dziennika zapisywane będą komunikaty z poziomów 0-5, komunikaty z poziomów 0-2 będą synchronizowane w sektorze flash raz na 10 godzin:

Switch#configure

Switch(config)#logging buffer

Switch(config)#logging buffer level 5

Switch(config)#logging file flash

Switch(config)#logging file flash frequency periodic 10

Switch(config)#logging file flash level 2

Switch(config)#show logging local-config

Channel	Level	Status	Sync-Periodic
-------	-----	------	-------------
Buffer	5	enable	Immediately
Flash	2	enable	10 hour(s)
Console	5	enable	Immediately
Monitor	5	enable	Immediately

Switch(config)#end

Switch#copy running-config startup-config

1.2.2 Konfiguracja dzienników zdalnych

Możesz skonfigurować otrzymywanie dzienników systemowych przełącznika na maks. czterech hostach. Hosty te nazywane są Log Servers (Serwery dzienników). Po wygenerowaniu komunikatu dziennika przełącznik będzie przekazywał komunikat do serwerów. Aby wyświetlić dzienniki, serwery powinny obsługiwać oprogramowanie dziennika serwera zgodne ze standardem dzienników systemowych.

Aby skonfigurować dziennik zdalny, postępuj zgodnie z poniższymi krokami.

Krok 1	**configure** Wejdź w tryb konfiguracji globalnej.

Krok 2	**logging host index** *idx host-ip level* Skonfiguruj host zdalny, który będzie odbierał dzienniki systemowe przełącznika. Taki host nazywany jest Log Server (Serwer dziennika). Za pomocą serwera dziennika możesz zdalnie monitorować ustawienia i status działania przełącznika. *idx*: Wpisz indeks serwera dziennika. Przełącznik może obsługiwać maks. 4 serwery dziennika. *host-ip*: Wpisz adres IP serwera dziennika. *level*: Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane na serwerze dziennika. Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. Zapisywane będą tylko komunikaty zdarzeń o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 6. Oznacza to, że zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 6.
Krok 3	**show logging loghost** [*index*] Sprawdź dane konfiguracyjne serwera dziennika. *index*: Wpisz indeks serwera dziennika, aby wyświetlić odpowiednie dane konfiguracyjne. Jeżeli nie zostanie wyznaczona żadna wartość, wyświetlone zostaną dane wszystkich hostów dziennika.
Krok 4	**end** Wróć do trybu użytkownika uprzywilejowanego (privileged EXEC mode).
Krok 5	**copy running-config startup-config** Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie na przełączniku dziennika zdalnego, włączanie dziennika serwera 2, ustawianie jego adresu IP na 192.168.0.148 i włączenie wysyłania na serwer komunikatów zdarzeń z poziomów 0-5:

Switch#configure

Switch(config)# logging host index 2 192.168.0.148 5

Switch(config)# show logging loghost

Index	Host-IP	Severity	Status
-----	-------	--------	------
1	0.0.0.0	6	disable
2	192.168.0.148	5	enable
3	0.0.0.0	6	disable
4	0.0.0.0	6	disable

Switch(config)#end

Switch#copy running-config startup-config