Przełącznik Ethernet (zarządzany)

Podręcznik użytkownika

wersja 1.0.0

Wprowadzenie

Informacje ogólne

W tym podręczniku przedstawiono procedury wykonywane w interfejsie internetowym przełącznika RTL (zwanego dalej „przełącznikiem"). Można wyświetlać i konfigurować ustawienia przełącznika oraz zarządzać nimi przy użyciu jego interfejsu internetowego.

Zalecenia dotyczące bezpieczeństwa

W podręczniku mogą być używane hasła ostrzegawcze zdefiniowane w poniższej tabeli.

Hasła ostrzegawcze	Znaczenie
ZAGROŻENIE	Oznacza poważne zagrożenie, które może spowodować poważny uszczerbek na zdrowiu, a nawet zgon, jeżeli nie zostaną podjęte działania zaradcze.
OSTRZEŻENIE	Oznacza średnie lub nieznaczne zagrożenie, które może spowodować drobny lub umiarkowany uszczerbek na zdrowiu, jeżeli nie zostaną podjęte działania zaradcze.
PRZESTROGA	Oznacza potencjalne zagrożenie, które może spowodować zniszczenie mienia, utratę danych, obniżenie wydajności lub nieoczekiwane skutki, jeżeli nie zostaną podjęte działania zaradcze.
PORADA	Ułatwia rozwiązywanie problemów lub zaoszczędzenie czasu.
UWAGA	Dodatkowe informacje potwierdzające lub uzupełniające treść podręcznika.

Często używane funkcje

Ikona/ustawienie	Opis
	Edycja elementu.
lub **Usuń** (Delete)	Usuwanie elementów pojedynczo lub zbiorczo.
lub	Włączanie lub wyłączanie elementów pojedynczo lub zbiorczo.
Odśwież (Refresh) lub **Automatycznie odświeżanie** (Auto Refresh)	Odświeżanie lub automatyczne odświeżanie informacji.

Historia wersji

Wersja	Zakres zmian	Data wydania
wersja 1.0.0	Pierwsze wydanie.	sierpień 2024

Opis podręcznika

- Podręcznik jest tylko źródłem informacji referencyjnych. Rzeczywisty wygląd produktu może różnić się nieznacznie od przedstawionego w podręczniku.
- Nie ponosimy odpowiedzialności za straty wynikające z użycia produktu w sposób niezgodny z podręcznikiem.

- Podręcznik będzie aktualizowany zgodnie z najnowszymi przepisami i rozporządzeniami, obowiązującymi w danej jurysdykcji. Aby uzyskać więcej informacji, skorzystaj z drukowanego podręcznika użytkownika, naszej płyty CD-ROM, skanu kodu QR lub naszej oficjalnej witryny internetowej. Podręcznik jest tylko źródłem informacji referencyjnych. Między elektroniczną wersją podręcznika a jego drukowaną wersją mogą występować nieznaczne różnice.
- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez wcześniejszego, pisemnego powiadomienia. Aktualizacje produktu mogą powodować rozbieżności między rzeczywistym produktem a informacjami podanymi w podręczniku. Aby otrzymać najnowsze oprogramowanie lub dokumentację pomocniczą, należy skontaktować się z działem obsługi klienta.
- Mogą wystąpić błędy w druku lub rozbieżności w opisie funkcji, operacji i danych technicznych. Wątpliwości lub kwestie sporne będą rozstrzygane zgodnie z decyzją firmy.
- Jeżeli nie można otworzyć podręcznika elektronicznego (w formacie PDF), należy uaktualnić oprogramowanie przeglądarki lub użyć innego popularnego programu obsługującego ten format.
- Wszystkie znaki towarowe, zastrzeżone znaki towarowe i nazwy firm, użyte w tym podręczniku, są własnością odpowiednich firm.
- Jeżeli wystąpią problemy z użytkowaniem urządzenia, należy skorzystać z naszej witryny internetowej albo skontaktować się z dostawcą lub działem obsługi klienta.
- Zastrzegamy sobie prawo do podejmowania ostatecznej decyzji rozstrzygającej wszelkie wątpliwości i kwestie sporne.

Spis treści

1 Logowanie

1.1 Inicjowanie przełącznika

Wymagania wstępne

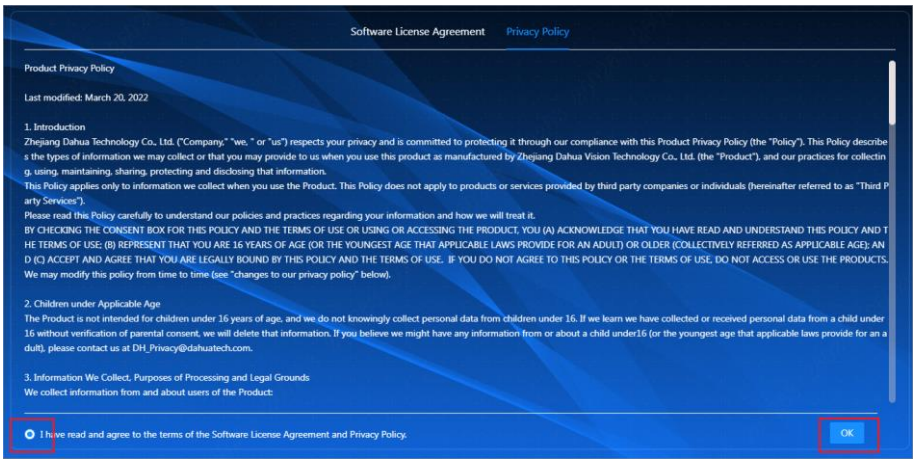
Przed zalogowaniem upewnij się, że przełącznik i urządzenie konfiguracyjne są połączone, a ich zasilanie jest włączone.

Procedura

Krok 1 Uruchom przeglądarkę IE, wprowadź adres IP przełącznika (domyślnie 192.168.1.110) na pasku adresu, a następnie naciśnij klawisz Enter.

Krok 2 Przeczytaj dokumenty „**Umowa licencyjna użytkownika oprogramowania**" (Software License Agreement) i „**Zasady ochrony prywatności**" (Privacy Policy) i zaznacz pole wyboru „**Potwierdzam przeczytanie i akceptację dokumentów Umowa licencyjna użytkownika oprogramowania i Zasady ochrony prywatności**" (I have read and agree to the terms of the Software License Agreement and Privacy Policy), a następnie kliknij przycisk **OK**.

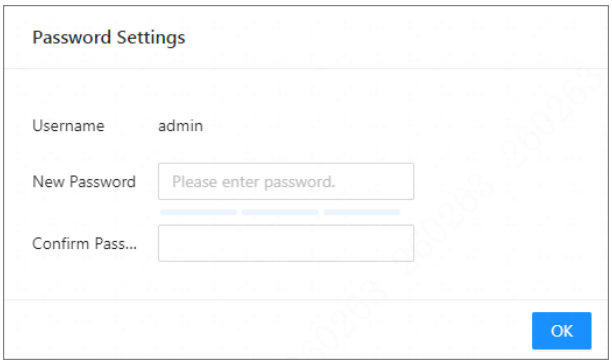
Rysunek 1-1 Zasady ochrony prywatności



Krok 3 Skonfiguruj hasło.

Domyślną nazwą użytkownika jest „admin”.

Rysunek 1-2 Konfigurowanie hasła



Krok 4 Kliknij przycisk **OK**.

1.2 Logowanie

Wymagania wstępne

Przed zalogowaniem upewnij się, że spełnione są następujące warunki:

- Skonfigurowano już adres IP przełącznika. Domyślny adres IP sieci VLAN1 to 192.168.1.110.
- Komputer jest połączony z siecią i otrzymuje od przełącznika odpowiedzi na polecenie Ping.

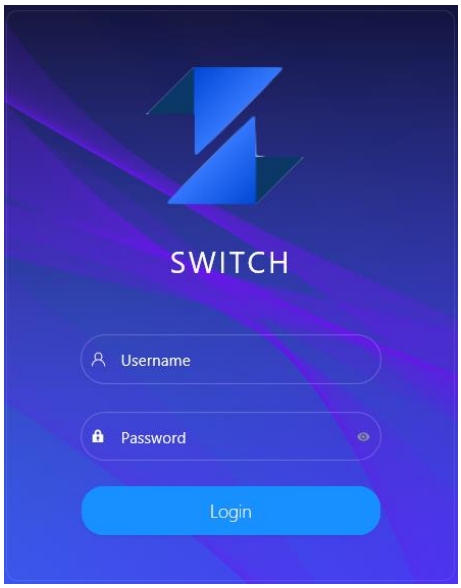
Procedura

Krok 1 Wprowadź adres IP (domyślnie 192.168.110) przełącznika na pasku adresu przeglądarki internetowej, a następnie naciśnij klawisz Enter.

Krok 2 Wprowadź nazwę użytkownika i hasło.

Krok 3 Kliknij przycisk **Zaloguj** (Login).

Rysunek 1–3 Logowanie



- Zmień hasło po pierwszym zalogowaniu. Hasło musi składać się z 8–32 niepustych znaków należących do co najmniej dwóch z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne (z wyjątkiem ' " ; : &).

Rysunek 1-4 Strona główna

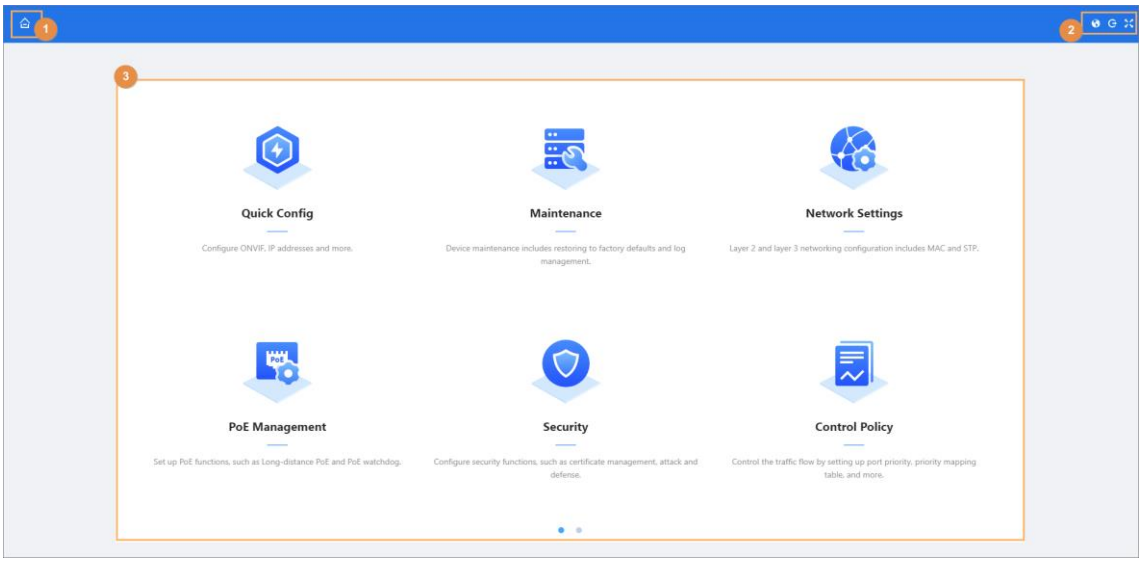


Tabela 1-1 Opis strony głównej

Nr	Nazwa	Opis
1		Powrót do strony głównej.
2		Przełączanie języków systemu. Obsługiwanych jest wiele języków.
		Wylogowanie użytkownika i powrót do strony logowania.
		Wyświetlanie strony internetowej w trybie pełnego ekranu.
3	Wyświetlanie stanu (Status Display)	Wyświetlanie w czasie rzeczywistym informacji o stanie przełącznika.
	Szybka konfiguracja (Quick Config)	Szybkie konfigurowanie ustawień takich jak funkcja ONVIF lub adres IP.
	Konserwacja (Maintenance)	Konfigurowanie ustawień konserwacji oraz przywracanie fabrycznych ustawień domyślnych i zarządzanie dziennikami.
	Ustawienia sieciowe (Network Settings)	Konfigurowanie ustawień sieci takich jak ustawienia adresów MAC i protokołu STP.
	Zarządzanie PoE (PoE Management)	Konfigurowanie ustawień zasilania PoE takich jak Duży zasięg PoE (Long-distance PoE) i PoE Watchdog.
	Zabezpieczenia (Security)	Konfigurowanie ustawień zabezpieczeń, łącznie z zarządzaniem certyfikatami, atakami i obroną.

Nr	Nazwa	Opis
	Zasady sterowania (Control Policy)	Konfigurowanie ustawień przepływu ruchu, łącznie z ustawieniem priorytetu portów i tabelą mapowania priorytetów
	Uwierzytelnianie (Authentication)	Konfigurowanie zarządzania uwierzytelnianiem, łącznie z 802.1x i RADIUS.

2 Szybka konfiguracja

Można wyświetlać informacje o systemie i skonfigurować ustawienia przełącznika, takie jak funkcja ONVIF i adres IP. Zrzuty ekranu używane w podręczniku służą wyłącznie do celów referencyjnych i mogą różnić się od rzeczywistego wyglądu stron.

2.1 Konfigurowanie ustawień ogólnych

Można wyświetlać i konfigurować ustawienia ogólne, takie jak nazwa, adres IP, maska podsieci i brama domyślna.

Procedura

Krok 1 Wybierz **Szybka konfiguracja > Ogólne** (Quick Config > General).

Krok 2 Można wyświetlać i konfigurować ogólne informacje dotyczące przełącznika.

Krok 3 (Opcjonalnie) Kliknij przycisk , aby włączyć funkcję DHCP.

Należy rozważnie korzystać z tej funkcji. Po włączeniu funkcji DHCP router lub serwer DHCP połączony z przełącznikiem automatycznie przydziela adres IP dla przełącznika. Pierwotny adres IP nie umożliwia dostępu do interfejsu internetowego.

Rysunek 2-1 Informacje ogólne

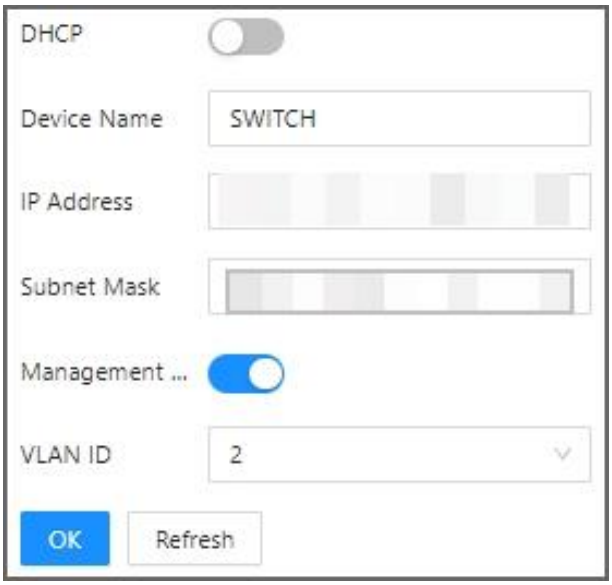


Tabela 2-1 Opis informacji ogólnych

Ustawienie	Opis
DHCP	Umożliwia włączanie funkcji DHCP. Po włączeniu funkcji DHCP nowy adres IP zostanie automatycznie uzyskany i przydzielony. Przed przypisaniem nowego adresu IP stosowany jest domyślny adres IP 192.168.1.110.
Nazwa urządzenia (Device Name)	Bieżąca nazwa urządzenia. Można zmienić nazwę.

Ustawienie	Opis
Adres IP (IP address)	Bieżący adres IP. Można ręcznie konfigurować to ustawienie.
Maska podsieci (Subnet Mask)	Umożliwia wprowadzenie maski podsieci
Sieć VLAN zarządzana (Managed VLAN)	Po włączeniu funkcji **Sieć VLAN zarządzana** (Managed VLAN) dostęp do interfejsu internetowego można uzyskać tylko przy użyciu sieci VLAN zarządzanej.
Identyfikator VLAN ID	Bieżący identyfikator VLAN ID zarządzany

2.2 Informacje o portach

Można wyświetlać informacje takie jak port, typ, stan łącza, szybkość/dupleks, użycie sieci VLAN, RX i TX oraz typ nośników przełącznika.

Procedura

Krok 1 Wybierz **Szybka konfiguracja > Informacje o portach** (Quick Config > Port Info).

Krok 2 Wyświetl informacje o portach przełącznika.

Rysunek 2-2 Informacje o portach

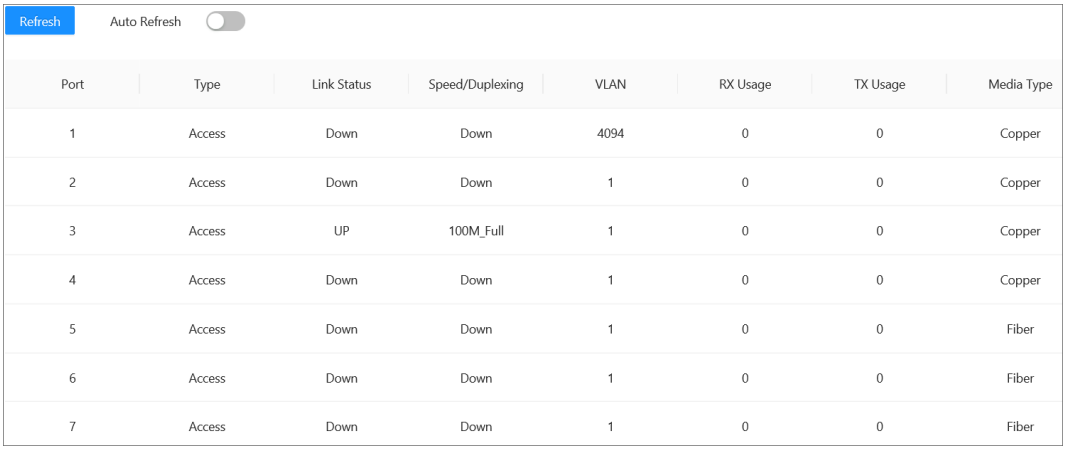


Tabela 2–2 Opis informacji o portach

Ustawienie	Opis
Port	Wszystkie porty przełącznika
Opis (Description)	Ustaw opis portu. Można używać cyfr, liter (wielkość liter nie jest uwzględniana) i znaków specjalnych. Można użyć maksymalnie 16 niepustych znaków. Domyślnie brak opisu.
Typ (Type)	Dostępne są trzy typy: **Dostęp** (Access), **Hybrydowy** (Hybrid) i **Magistrala** (Trunk).
Stan łącza (Link status)	Obsługiwane są dwa stany: **Aktywny** (Up) i **Nieaktywny** (Down). ● Aktywny: Port jest połączony. ● Nieaktywny: Port nie jest połączony lub połączenie nie powiodło się.
Szybkość/dupleks (Speed/Duplexing)	● Online: Szybkość portu i tryb dupleksu ● Offline: Wyświetlane jest ustawienie **Nieaktywny** (Down).

Ustawienie	Opis
VLAN	Sieć VLAN portu. Domyślnie VLAN1.
Użycie odbiornika (RX usage)	Wyświetla użycie odbiornika
Użycie nadajnika (TX usage)	Wyświetla użycie nadajnika
Typ nośnika (Media type)	Dostępne są dwa typy: **Przewód miedziany** (Copper) i **Światłowód** (Fiber). ● Przewód miedziany: Złącze RJ-45 ● Światłowód: Złącze światłowodowe

Powiązane działania

- Kliknij przycisk **Odśwież** (Refresh), aby ręcznie odświeżyć informacje o portach.
- Kliknij przycisk obok etykiety **Automatyczne odświeżanie** (Auto Refresh), aby włączyć automatyczne odświeżanie.

2.3 Funkcja ONVIF

Wybierz **Szybka konfiguracja > Informacje o portach** (Quick Config > Port Info), aby wyświetlić informacje o portach przełącznika.

Kliknij przycisk , aby włączyć funkcję ONVIF. Włączenie tej funkcji powoduje wyświetlenie wszystkich portów i stanu połączeń przełącznika.

- Zielony port: Prawidłowe połączenie
- Jasnoniebieski port: Brak połączenia lub usterka połączenia

Liczba portów jest zależna od modelu. Poniższy rysunek służy wyłącznie do celów referencyjnych. Aby uzyskać więcej informacji, należy skorzystać z dokumentacji danego produktu.

Rysunek 2-3 Informacje ONVIF

Tabela 2-3 Opis portów

Nazwa	Opis
Port	Numer portu
Opis	Opis portu

Nazwa	Opis
Typ portu (Port Type)	Dostępne są trzy typy: **Dostęp** (Access), **Hybrydowy** (Hybrid) i **Magistrala** (Trunk).
Stan łącza (Link Status)	Obsługiwane są dwa stany: **Aktywny** (Up) i **Nieaktywny** (Down). ● Aktywny: Port jest połączony. ● Nieaktywny: Port nie jest połączony lub połączenie nie powiodło się.
Stan sterowania przepływem (Flow Control Status)	Umożliwia sprawdzenie stanu funkcji sterowania przepływem.
Szybkość/dupleks (Speed/Duplexing)	● Online: Szybkość portu i tryb dupleksu ● Offline: Wyświetlane jest ustawienie **Nieaktywny** (Down).
VLAN	Sieć VLAN portu. Domyślnie VLAN1.
PoE	Pobór mocy zasilania PoE ● Przełączniki non-PoE nie obsługują tej funkcji. ● Liczba portów PoE jest zależna od modelu. Aby uzyskać więcej informacji, należy skorzystać z dokumentacji danego produktu.
Użycie odbiornika (RX usage)	Bieżąca szybkość odbioru podzielona przez rzeczywistą szybkość wynegocjowaną dla danego okresu (zazwyczaj pięciu minut)
Użycie nadajnika (TX usage)	Bieżąca szybkość nadawania podzielona przez rzeczywistą szybkość wynegocjowaną dla danego okresu (zazwyczaj pięciu minut)
Typ nośnika (Media Type)	Dostępne są dwa typy: **Przewód miedziany** (Copper) i **Światłowód** (Fiber). ● Przewód miedziany: Złącze RJ-45 ● Światłowód: Złącze światłowodowe

2.4 Wyświetlanie informacji o kamerach internetowych i rejestratorach NVR

Wybierz **Szybka konfiguracja > Kamery IP i rejestratory NVR** (Quick Config > IPC&NVR), aby wyświetlić informacje dotyczące kamer IP, rejestratorów NVR i innych urządzeń podłączonych do przełącznika.

3 Ustawienia sieci

3.1 Konfigurowanie portów

Informacje wstępne

Można skonfigurować ustawienia portów, między innymi takie jak szybkość/dupleks lub sterowanie przepływem. Ustawienia portów wpływają bezpośrednio na ich funkcjonowanie.
Należy skonfigurować ustawienia zależnie od potrzeb.

Interfejs internetowy jest zależny od urządzenia. Aby uzyskać więcej informacji, należy sprawdzić ustawienia na danej stronie.

Procedura

Krok 1 Wybierz **Ustawienia sieci > Porty** (Network Settings > Port).

Krok 2 Można wyświetlać i konfigurować ustawienia.

Rysunek 3-1 Ustawienia portów

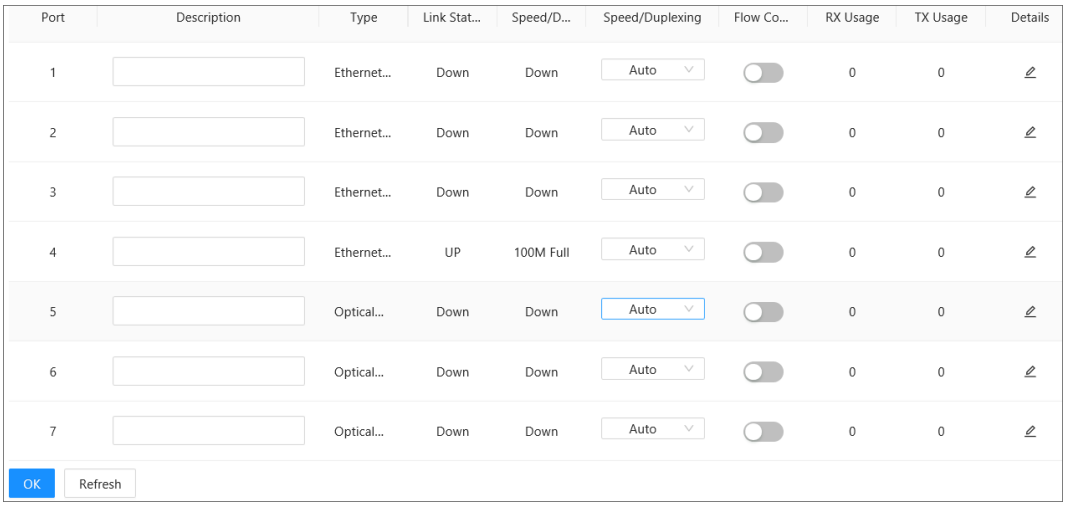


Tabela 3-1 Opis ustawień portów

Ustawienie	Opis
Port	Wszystkie porty przełącznika
Opis (Description)	Wprowadź opis portu. Opis może składać się z maksymalnie 16 znaków. Dozwolone są tylko cyfry, litery i następujące znaki specjalne: . _ -. Pierwszym znakiem musi być litera, a ostatnim znakiem nie może być znak specjalny.

Ustawienie	Opis
Typ nośnika (Media Type)	Wyświetla dwa rodzaje typu mediów, obejmuje dwa typy: **Przewód miedziany** (Copper) i **Światłowód** (Fiber). ● Przewód miedziany: Złącze Ethernet. ● Światłowód: Złącze optyczne
Stan łącza (Link status)	Obsługiwane są dwa stany: **Aktywny** (Up) i **Nieaktywny** (Down). ● Aktywny: Port jest połączony. ● Nieaktywny: Port nie jest połączony lub połączenie nie powiodło się.
Stan szybkości/dupleksu (Speed/Duplexing Status)	● Online: Szybkość portu i tryb dupleksu ● Offline: Wyświetlane jest ustawienie **Nieaktywny** (Down).
Szybkość/dupleks (Speed/Duplexing)	Ustaw szybkość i tryb dupleksu **Brak , Auto, Półdupleks 10M, Pełny dupleks 10M, Półdupleks 100M, Pełny dupleks 100M lub** (Down, Auto, 10M Half, 10M Full, 100M Half, 100M Full) **Pełny dupleks 1000M** (1000M Full). W przypadku złączy zespolonych ustawiona jest szybkość/dupleks **Auto**.
Sterowanie przepływem (Flow control)	Kliknij ikonę , aby włączyć lub wyłączyć tę funkcję.
Użycie odbiornika (RX usage)	Wyświetla użycie odbiornika
Użycie nadajnika (TX usage)	Wyświetla użycie nadajnika
Szczegóły (Details)	● Całkowita wartość RX i TX dla każdego portu. Można odświeżyć lub wyczyścić szczegółowe informacje dotyczące każdego portu. ● Liczba bajtów z błędami

Krok 3 Kliknij przycisk **OK**.

3.2 Konfigurowanie funkcji EEE

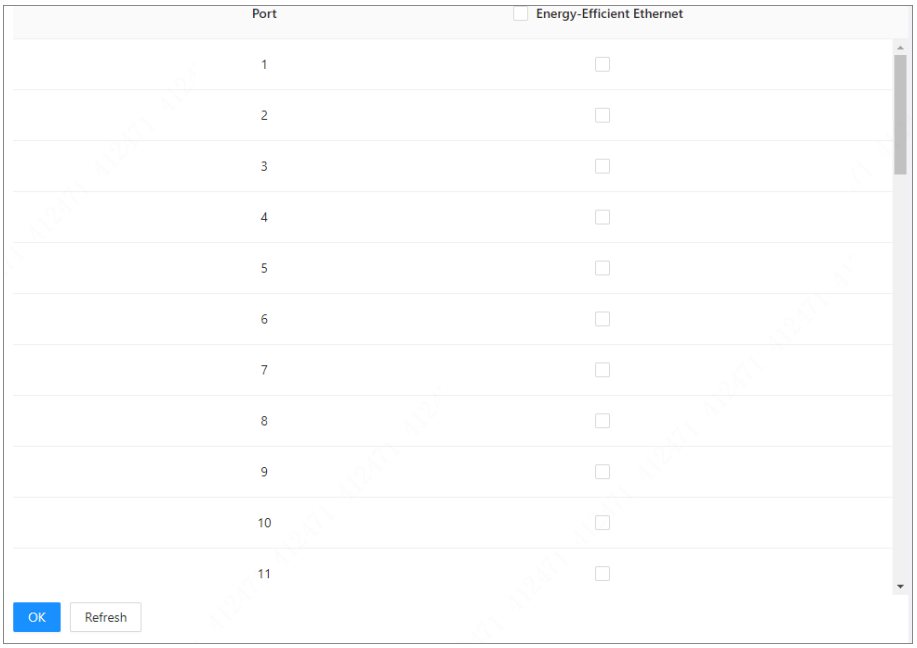
Włącz funkcję Energooszczędny Ethernet (EEE, Energy-Efficient Ethernet).

Procedura

Krok 1 Wybierz **Ustawienia sieci > Funkcja EEE** (Network Settings > EEE).

Krok 2 Zaznacz pole wyboru portu, aby włączyć funkcję **Energooszczędny Ethernet** (Energy-Efficient Ethernet), a następnie kliknij przycisk **OK**, aby zapisać konfigurację.

Rysunek 3-2 Funkcja EEE



3.3 Konfigurowanie sieci VLAN

3.3.1 Definicja sieci VLAN

Logicznie można podzielić sieć LAN (Local Area Network) na wiele podsieci. Każda podsieć ma własny obszar rozgłaszania: wirtualną sieć LAN (VLAN). Sieć VLAN jest oddzielona od sieci LAN w sposób bardziej logiczny niż sprzętowy w celu utworzenia izolowanego obszaru rozgłaszania w sieci VLAN.

3.3.2 Zalety sieci VLAN

- Zwiększanie wydajności sieci. Pakiety rozgłoszeniowe są przesyłane w sieci VLAN, dlatego można efektywne kontrolować burzę rozgłoszeniową, zmniejszać użycie przepustowości sieci i zwiększać wydajność przetwarzania sieciowego.
- Ulepszanie zabezpieczeń sieciowych. Przełączniki w różnych sieciach VLAN nie mogą uzyskać dostępu do siebie wzajemnie, a hosty w różnych sieciach VLAN nie mogą komunikować się ze sobą. Aby przekazać wiadomość, konieczne jest użycie routera lub przełącznika trójwarstwowego.
- Uproszczenie zarządzania siecią. Host wirtualnej grupy roboczej nie jest ograniczony do jednego obszaru sprzętowego, co ułatwia zarządzanie siecią i tworzenie grup roboczych dla użytkowników w różnych obszarach.

3.3.3 Sieć VLAN oparta na portach

Dostępne są następujące typy portów: **Dostęp** (Access), **Magistrala** (Trunk) i **Hybrydowy** (Hybrid).

- Dostęp: Port należy do sieci VLAN i służy do połączenia z portem komputerowym.
- Magistrala: Port umożliwia przechodzenie wielu sieci VLAN, odbieranie i wysyłanie wiadomości wielu sieci VLAN oraz łączenie przełączników.
- Hybrydowy: Port umożliwia przechodzenie wielu sieci VLAN, odbieranie i wysyłanie wiadomości wielu sieci VLAN oraz łączenie przełączników i komputera.

3.3.4 Dodawanie sieci VLAN

Informacje wstępne

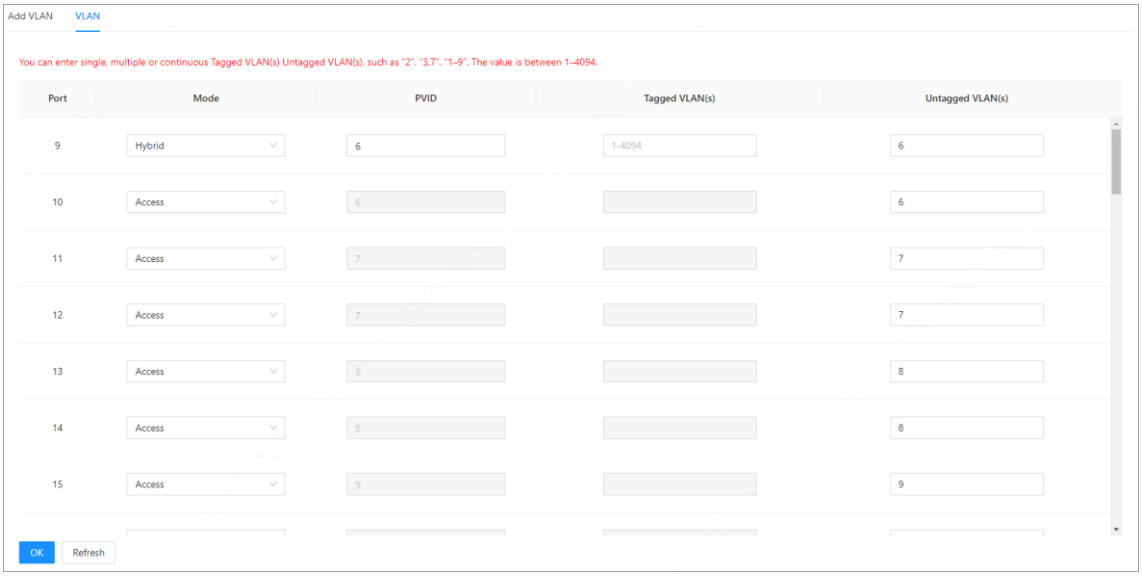
Można dodać port do sieci VLAN. Domyślnie wybrana jest sieć VLAN1.

Nie można włączyć równocześnie funkcji izolacji portów i VLAN. Włączenie jednej z tych funkcji powoduje automatyczne wyłączenie drugiej funkcji. Zachowaj ostrożność.

Procedura

Krok 1 Wybierz **Ustawienia sieci > VLAN** (Network Settings > VLAN).

Rysunek 3-3 Ustawienia sieci VLAN



Krok 2 Na stronie **Dodawanie sieci VLAN** (Add VLAN) kliknij przycisk **Dodaj** (Add), a następnie wprowadź identyfikator **VLAN ID** i **Opis** (Description).

Rysunek 3-4 Dodawanie sieci VLAN

Krok 3 Kliknij przycisk **OK**.

Nie można usunąć sieci VLAN1.

Powiązane działania

- Kliknij przycisk , aby edytować sieć VLAN.
- Kliknij przycisk , aby usunąć sieć VLAN.

3.3.5 Konfigurowanie sieci VLAN portu

Można konfigurować ustawienia portu VLAN.

Rysunek 3-5 Konfigurowanie sieci VLAN

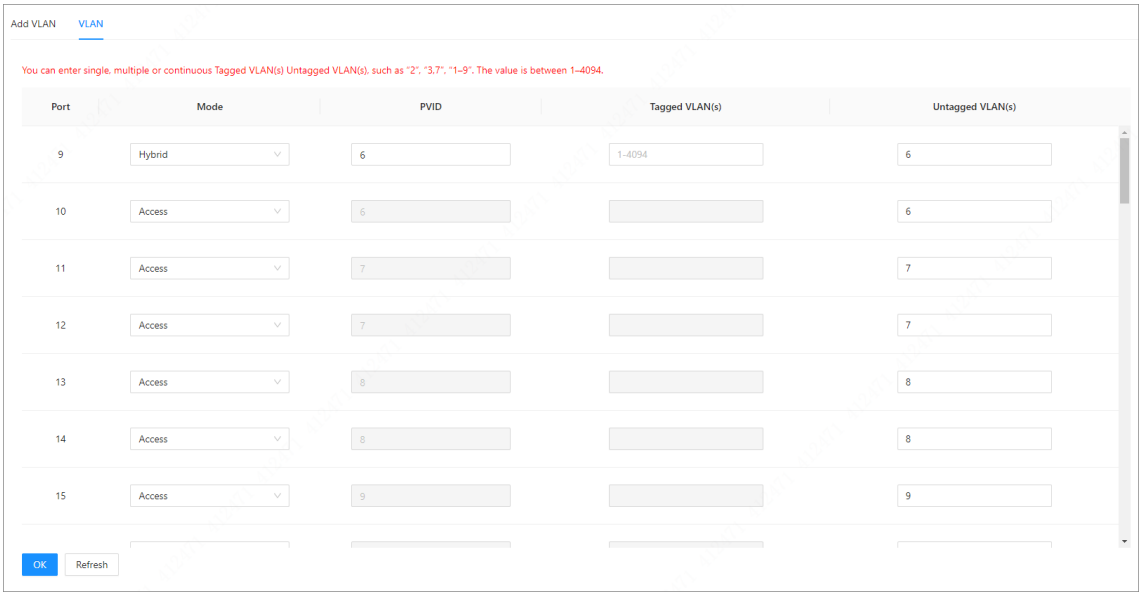


Tabela 3-2 Ustawienia konfiguracji sieci VLAN portu

Ustawienie	Opis
Port	Wszystkie porty przełącznika
Tryb (Mode)	Dostępne są trzy tryby: **Dostęp** (Access), **Hybrydowy** (Hybrid) i **Magistrala** (Trunk). ● Dostęp: Należy do jednej sieci VLAN. Używane zazwyczaj do podłączania złączy komputerów. ● Magistrala: Umożliwia przechodzenie wielu sieci VLAN. Odbieranie i wysyłanie wielu pakietów VLAN. Zazwyczaj używane do łączenia przełączników. ● Hybrydowy: Umożliwia przechodzenie wielu sieci VLAN. Odbieranie i wysyłanie wielu pakietów VLAN. Używane do łączenia przełączników lub przełączników z komputerami.
Oznakowane sieci VLAN (Tagged VLAN)	Skonfiguruj identyfikator VLAN ID dla portu, który może być oznakowany podczas wysyłania pakietów.
Nieoznakowane sieci VLAN (Untagged VLAN)	Skonfiguruj identyfikator VLAN ID dla portu, który może być nieoznakowany podczas wysyłania pakietów.

Tabela 3-3 Porównanie przetwarzania ramek

<table>
<tr><th>Typ portu</th><th>Przetwarzanie ramek nieoznakowanych</th><th>Przetwarzanie ramek oznakowanych</th><th>Przesyłanie ramek</th></tr>
<tr><td>Dostęp (Access)</td><td>Odebranie ramki nieoznakowanej i dodanie do niej znacznika z domyślnym identyfikatorem VLAN ID.</td><td>● Akceptacja ramki oznakowanej, jeżeli jej identyfikator VLAN ID jest zgodny z domyślnym identyfikatorem VLAN ID.
● Odrzucenie ramki oznakowanej, jeżeli jej identyfikator VLAN ID różni się od domyślnego identyfikatora VLAN ID.</td><td>Po usunięciu znacznika PVID ramka jest przesyłana.</td></tr>
<tr><td rowspan="2">Magistrala (Trunk)</td><td rowspan="3">● Dodanie znacznika z domyślnym identyfikatorem VLAN ID do ramki nieoznakowanej i akceptacja ramki, jeżeli interfejs zezwala na domyślny identyfikator VLAN ID.
● Dodanie znacznika z domyślnym identyfikatorem VLAN ID do ramki nieoznakowanej i odrzucenie ramki, jeżeli interfejs nie akceptuje domyślnego identyfikatora VLAN ID.</td><td rowspan="3">● Akceptacja ramki oznakowanej, jeżeli jej identyfikator VLAN ID jest dozwolony rzez interfejs.
● Odrzucenie ramki oznakowanej, jeżeli jej identyfikator VLAN ID został odrzucony przez interfejs.</td><td>● Jeżeli identyfikator VLAN ID ramki jest zgodny z domyślnym identyfikatorem VLAN ID, który jest dozwolony przez interfejs, urządzenie usuwa znacznik i przesyła ramkę.
● Jeżeli identyfikator VLAN ID ramki różni się od domyślnego identyfikatora VLAN ID, ale jest dozwolony przez interfejs, urządzenie przesyła ramkę bezpośrednio.</td></tr>
<tr><td>Hybrydowy (Hybrid)</td><td>Jeżeli identyfikator VLAN ID jest dozwolony przez interfejs, ramka jest przesyłana. Interfejs można skonfigurować do przesyłania ramek ze znacznikami.</td></tr>
</table>

3.4 Konfigurowanie interfejsu VLANIF

Informacje wstępne

Interfejs logiczny trzeciej warstwy VLANIF jest najczęściej używany do implementowania komunikacji w trzeciej warstwie między hostami w różnych sieciach VLAN w różnych segmentach sieci.

Każdy interfejs VLANIF reprezentuje sieć VLAN. Po skonfigurowaniu adresu IP dla interfejsu VLANIF pełni on funkcję bramy hostów użytkowników w danej sieci VLAN i przekazuje pakiety w segmentach sieci w trzeciej warstwie.

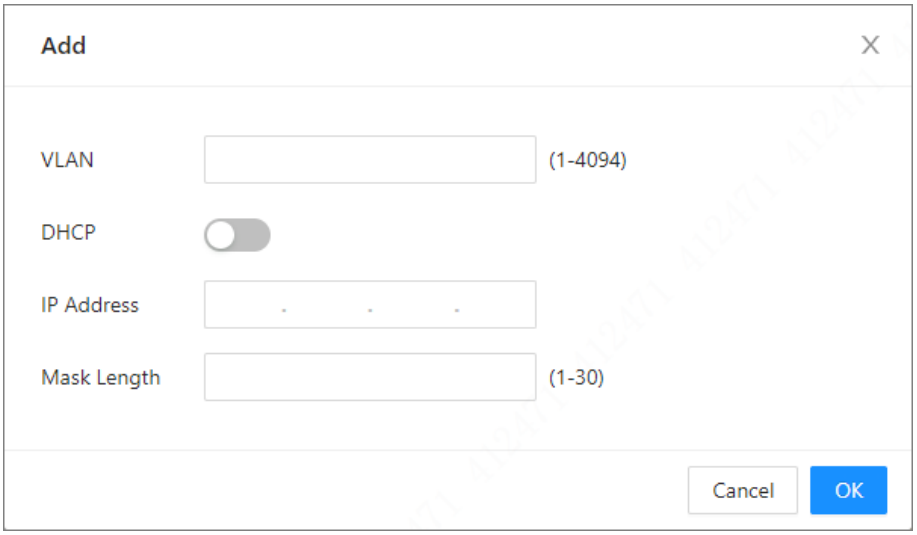
Procedura

Krok 1 Wybierz **Ustawienia sieci > VLANIF** (Network Settings > VLANIF).

Krok 2 Kliknij przycisk **Dodaj** (Add), wprowadź numer sieci **VLAN**, a następnie włącz funkcję **DHCP** dla portu z ustawieniem **Dynamiczny** (Dynamic) opcji **Tryb** (Mode).

Gdy funkcja **DHCP** jest wyłączona, należy wprowadzić ustawienia **Adres IP** (IP Address) i **Długość maski** (Mask Length).

Rysunek 3-6 Dodawanie interfejsu VLANIF



Powiązane działania

- Usuwanie interfejsu VLANIF: Wybierz sieć VLAN, a następnie kliknij przycisk **Usuń** (Delete) lub .
- Odświeżanie ustawień: Kliknij przycisk **Refresh** (Odśwież), aby odświeżyć ustawienia sieci VLAN.

3.5 Konfigurowanie adresu IP i routingu

Można wprowadzić adres IP i ustawienia routingu przełącznika.

Procedura

Krok 1 Wybierz **Ustawienia sieci > Adres IP i routing** (Network Settings > IP & Routing).

Krok 2 Na karcie **Ustawienia routingu** (Routing Settings) kliknij przycisk **Dodaj** (Add), a następnie skonfiguruj ustawienia.

Niektóre modele obsługują tylko routing domyślny. Aby uzyskać więcej informacji, należy skorzystać z dokumentacji danego produktu.

Rysunek 3-7 Ustawienia routingu

Tabela 3-4 Opis ustawień routingu

Ustawienie	Opis
Sieć (Network)	Wprowadź adres docelowy lub sieć docelową do identyfikacji pakietów IP.
Długość maski (Mask Length)	Ustaw segment do identyfikacji przełącznika docelowego lub routera z adresem docelowym.
Następny skok (Next Hop)	Ustaw adres następnego skoku routera.

Powiązane działania

- Usuwanie routingu: Wybierz sieć VLAN i routing, a następnie kliknij przycisk **Usuń** (Delete) lub .
- Odświeżanie ustawień: Kliknij przycisk **Refresh** (Odśwież), aby odświeżyć ustawienia routingu.

3.6 Konfigurowanie funkcji ERPS

Protokół ERPS, zdefiniowany przez Międzynarodową Unię Telekomunikacyjną (International Telecommunication Union – Telecommunication Standardization Sector, ITU-T) umożliwia eliminację pętli w drugiej warstwie. Zazwyczaj łącza redundantne są używane w sieci przełączanej Ethernet, takiej jak sieć pierścieniowa, jako łącza zapasowe i zapewniają większą niezawodność sieci. Użycie łączy redundantnych może jednak powodować zapętlenie, burze rozgłoszeniowe i bezużyteczność tabel adresów MAC. Powoduje to pogorszenie jakości komunikacji, a nawet przerwy w dostępności usług komunikacyjnych. Protokół ERPS zapobiega burzom rozgłoszeniowym, implementuje szybkie przełączanie ruchu w sieci, w której występują pętle, zapewnia szybką

konwergencję i niezawodność klasy operatora, a także umożliwia komunikację wszystkich urządzeń obsługujących protokół ERPS w sieci pierścieniowej.

Niektóre modele nie obsługują funkcji ERPS. Aby uzyskać więcej informacji, należy skorzystać z dokumentacji danego produktu.

3.6.1 Ustawienia funkcji ERPS

Procedura

Krok 1 Wybierz **Ustawienia sieci > ERPS** (Network Settings > ERPS).

Krok 2 Na karcie **ERPS** kliknij przycisk **Dodaj** (Add), aby dodać instancję ERPS.

Krok 3 Skonfiguruj ustawienia, a następnie kliknij przycisk **OK**.

Rysunek 3-8 Dodawanie instancji ERPS

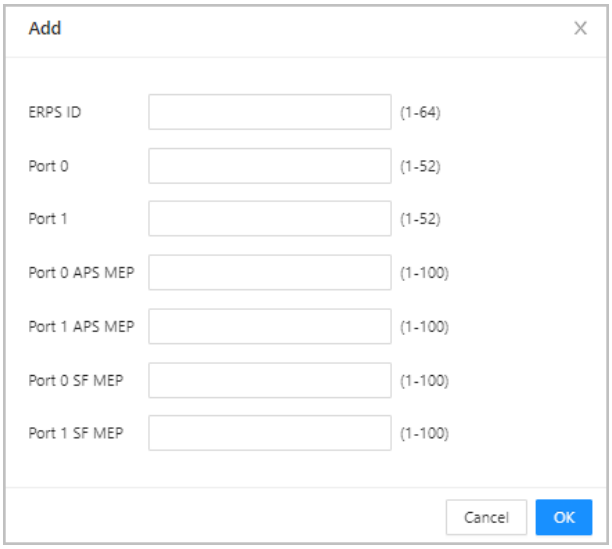


Tabela 3-5 Opis ustawień

Ustawienie	Opis
ERPS ID	Identyfikator instancji ERPS
Port 0	Dwa porty przełącznika dodane do instancji ERPS.
Port 1	
Instancja MEP APS portu 0 (Port 0 APS MEP)	● Instancja MEP BPDU portu ERPS. ● Powiąż instancję MEP monitorowania portu ERPS. Instancja MEP APS portu 0 jest taka sama jak instancja MEP SF portu 0. Instancja MEP APS portu 1 jest taka sama jak instancja MEP SF portu 1.
Instancja MEP APS portu 1 (Port 1 APS MEP)	
Instancja MEP SF portu 0 (Port 0 SF MEP)	
Instancja MEP SF portu 1 (Port 1 SF MEP)	

3.6.2 Ustawienia MEP

Instancja MEP (Maintenance Entity Group End Point) jest częścią pierścienia ERPS. Węzeł oznacza urządzenie przełączające drugiej warstwy dodane do pierścienia ERPS. Do każdego pierścienia ERPS można dodać maksymalnie dwa porty w każdym węźle.

Procedura

Krok 1 Wybierz **Ustawienia sieci > ERPS** (Network Settings > ERPS).

Krok 2 Na karcie **MEP** kliknij przycisk **Dodaj** (Add), aby dodać instancję MEP.

Krok 3 Skonfiguruj ustawienia MEP.

Krok 4 Kliknij przycisk **OK.**

Rysunek 3-9 Dodawanie instancji MEP

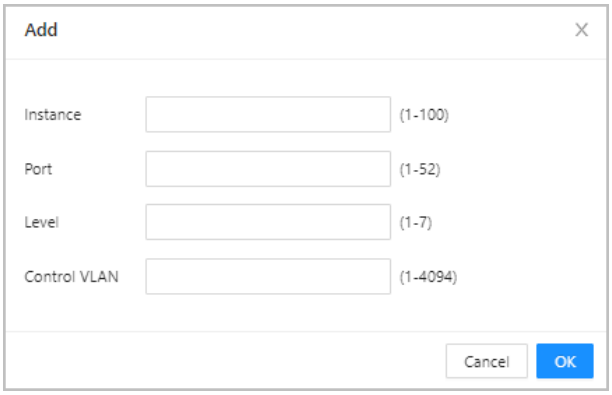


Tabela 3-6 Opis ustawień MEP

Ustawienie	Opis
Instancja (Instance)	Numer instancji MEP
Port	Numer portu MEP
Poziom (Level)	Poziom konserwacji Zalecamy ustawienie „0”.
Sieć VLAN sterowania (Control VLAN)	Identyfikator ID sieci VLAN sterowania w segmencie SEP.

3.7 Konfigurowanie monitorowania IGMP

Monitorowanie IGMP (Internet Group Management Protocol Snooping) jest mechanizmem ograniczania multiemisji, uruchamianym na urządzeniu drugiej warstwy, umożliwiającym zarządzanie multiemisją i kontrolowanie jej. Analizując odebrane pakiety IGMP, urządzenie drugiej warstwy, wykonujące zadania związane z monitorowaniem IGMP, tworzy mapowanie między portem a adresem MAC multiemisji i przekazuje dane multiemisji zgodnie z tym mapowaniem.

Procedura

Krok 1 Wybierz **Ustawienia sieci > Monitorowanie IGMP** (Network Settings > IGMP Snooping).

Krok 2 Kliknij przycisk obok etykiety **Monitorowanie IGMP** (IGMP Snooping), aby włączyć tę funkcję.

Krok 3 Kliknij przycisk obok etykiety **Pozostawiaj wiadomości grupy IGMP** (IGMP Leave Group Messages), aby włączyć tę funkcję.

- Włączenie funkcji: Po włączeniu tej funkcji przełącznik pozostawia niezarejestrowane wiadomości grupy. Użycie przepustowości będzie mniejsze, a szybkość przekazywania będzie większa.
- Wyłączenie funkcji: Niezarejestrowane wiadomości grupy są emitowane w sieci VLAN. Użycie przepustowości będzie większe, a szybkość przekazywania będzie mniejsza.

Należy pamiętać o włączeniu opcji **Pozostawiaj wiadomości grupy IGMP** (IGMP Leave Group Messages) zapewniającej prawidłowe funkcjonowanie multiemisji.

Krok 4 Kliknij przycisk **OK**.

3.8 Konfigurowanie funkcji STP

Protokół STP (Spaning Tree Protocol) tworzy logiczną topologię dla sieci LAN bez pętli. Blokowane są redundantne łącza między urządzeniami sieciowymi i zachowywane jest pojedyncze aktywne łącze między nimi, co umożliwia eliminację pętli.

Protokoły STP, RSTP i MSTP zapewniają następujące funkcje:

- STP: Protokół zarządzania w warstwie łączy danych umożliwia wykrywanie i eliminowanie pętli w sieci warstwy drugiej. Konwergencja topologii sieci jest jednak powolna.
- RSTP: Ulepszona wersja protokołu STP zapewniająca szybką konwergencję topologii sieci. Jednak zarówno RSTP, jak i STP mają wadę, która powoduje, że wszystkie sieci VLAN w określonej sieci LAN mają to samo drzewo rozpinające.
- MSTP: Wirtualna tabela mapowania sieci VLAN, w której identyfikatory VLAN ID są powiązane z instancjami drzewa rozpinającego. Ponadto protokół MSTP dzieli sieć przełączającą na wiele regionów, z których każdy ma wiele wzajemnie niezależnych instancji drzewa rozpinającego. W przeciwieństwie do protokołów STP i RSTP, protokół MSTP zapewnia wiele redundantnych ścieżek przekazywania danych. Ponadto implementowane jest równoważenie obciążenia sieci VLAN.

3.8.1 Funkcja STP

Informacje wstępne

Gdy włączona jest funkcja drzewa rozpinającego, nie można korzystać z aplikacji iLinkView.

Procedura

Krok 1 Wybierz **Ustawienia sieci > STP** (Network Settings > STP).

Krok 2 Kliknij obok **STP**, aby włączyć funkcję STP.

Krok 3 Wybierz tryb roboczy.

Krok 4 Kliknij przycisk **Zaawansowane** (Advanced), a następnie skonfiguruj ustawienia zaawansowane.

Rysunek 3-10 Konfiguracja STP

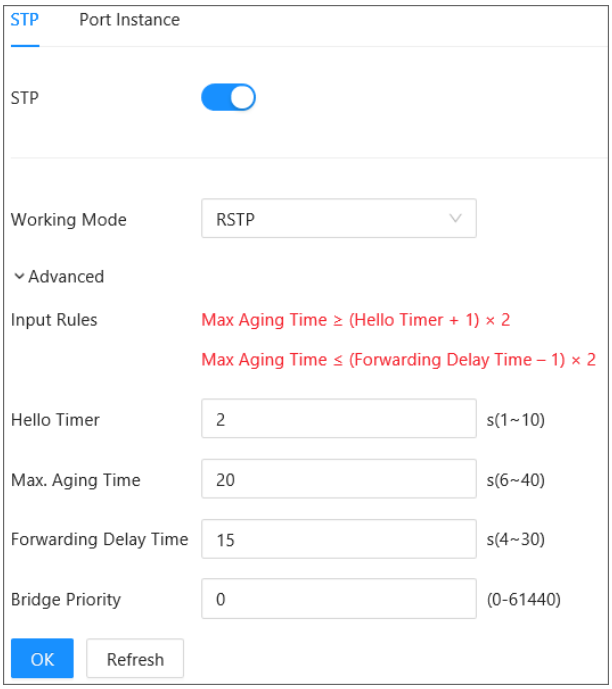


Tabela 3-7 Opis ustawień zaawansowanych

Ustawienie	Opis
STP	Podstawowy protokół drzewa rozpinającego.
RSTP	Ulepszona wersja protokołu STP zapewniająca szybką konwergencję topologii sieci.
Czasomierz powitania (Hello Timer)	Okres wysyłania BPDU przez mostek główny. Ten czas mieści się w zakresie od 1 do 10 sek.
Maks. czas wygasania (Max. Aging Time)	Czas wygasania bieżącej jednostki BPDU. Ten czas mieści się w zakresie od 6 do 40 sekund.
Opóźnienie przekazywania (Forwarding Delay Time)	Czas pozostawania mostka w stanie monitorowania i analizowania po wprowadzeniu zmiany w topologii. Ten czas mieści się w zakresie od 4 od 30 sekund.
Priorytet mostka (Bridge Priority)	Zakres wartości 0–61440.

3.8.2 Instancje portów

Procedura

Krok 1 Wybierz **Ustawienia sieci > STP > Instancje portów** (Network Settings > STP > Port Instance).

Krok 2 Wprowadź ustawienia **Priorytet** (Priority) i **Koszt ścieżki głównej** (Root Path Cost) każdego portu.

- Ustawienie **Priorytet** (Priority) ma zakres od 0 do 240 i musi być całkowitą wielokrotnością liczby 16.
- Domyślne ustawienie **Priorytetu** (Priority) to 128.

Rysunek 3-11 Instancje portów

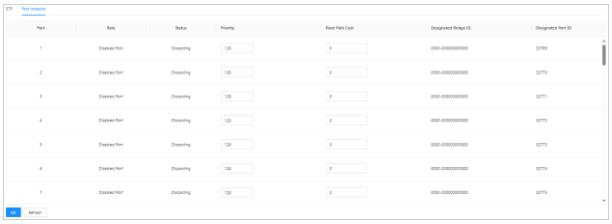


Tabela 3-8 Opis ustawień instancji portów

Ustawienie	Opis
Role (Rola)	Podstawowa funkcja STP
Stan (Status)	Ulepszona wersja protokołu STP zapewniająca szybką konwergencję topologii sieci.
Priorytet (Priority)	Priorytet portu
Koszt ścieżki głównej (Root Path Cost)	Koszt ścieżki głównej portu
Wskazany identyfikator mostka (Designated Bridge ID)	Wskazany identyfikator mostka portu
Wskazany identyfikator portu (Designated Port ID)	Wskazany identyfikator portu

3.9 Konfigurowanie agregacji łączy

Informacje wstępne

Agregacja łączy umożliwia utworzenie logicznego portu reprezentującego wiele sprzętowych złączy przełącznika. Wiele łączy w tej samej grupie można uznać za łącze logiczne o większej przepustowości.

Po agregacji porty w tej samej grupie mogą współdzielić przepływ komunikacji, aby zwiększyć przepustowość. Ponadto porty w tej samej grupie mogą wspierać się wzajemnie i dynamicznie w celu zwiększenia niezawodności łącza.

- Agregacja łączy wyklucza się wzajemnie z trybem STP, monitorowaniem IGMP i trybem 802.1x. Gdy tryb STP jest włączony, nie można skonfigurować agregacji łączy. Przed skonfigurowaniem agregacji łączy należy wyłączyć tryb STP.
- Nie zalecamy implementowania konfiguracji i zaawansowanych funkcji dla portów używanych do agregacji łączy.
- Agregację łączy można podzielić na agregację statyczną i LACP. Zgodnie z ogólną zasadą urządzenia równorzędne z agregacją łączy to przełącznik i adapter sieciowy.
- Tylko porty z tą samą szybkością, dupleksem, dużym zasięgiem i konfiguracją VLAN mogą należeć do tej samej grupy agregacji.

Procedura

Krok 1 Wybierz **Ustawienia sieci > Agregacja łączy** (Network Settings > Link Aggregation).

Krok 2 Kliknij przycisk **Dodaj** (Add).

Krok 3 Wybierz opcję **Numer grupy agregacji** (Aggregation Group No).

Krok 4 Wybierz opcję **Tryb grupy agregacji** (Aggregation Group Mode), a następnie kliknij przycisk **OK**.

Dostępne są następujące tryby grupy agregacji: Statyczny (Static), Aktywny LACP (LACP active) i Pasywny LACP (LACP passive).

- Statyczny: Tryb statyczny jest też zwany ręcznym. Konieczne jest ręczne utworzenie interfejsu Eth-Trunk i dodanie interfejsów członkowskich. Protokół LACP jest wyłączony.
- Aktywny LACP: Konieczne jest ręczne utworzenie interfejsu Eth-Trunk i dodanie interfejsów członkowskich. W porównaniu z trybem statycznym wybór interfejsu jest konfigurowany przez protokół LACP. W tym trybie interfejs aktywnie prowadzi negocjacje. W tym trybie interfejs inicjuje negocjacje z innymi interfejsami, wysyłając jednostki LACPDU.
- Pasywny LACP: Tworzone są interfejsy Eth-Trunk, a interfejsy członkowskie są dodawane przez protokół LACP. W tym trybie interfejs pasywnie uczestniczy w negocjowaniu. W tym trybie interfejs odpowiada na odbierane jednostki LACPDU, ale nie inicjuje negocjacji LACPDU.

Krok 5 Wybierz porty do dodania, a następnie kliknij przycisk **OK**.

Krok 6 Skonfiguruj ustawienie **Klucz operacyjny** (Operational Key).

- Agregację łączą można skonfigurować pod warunkiem, że opcję **Tryb grupy agregacji** (Aggregation Group Mode) skonfigurowano z ustawieniem LACP.
- Zakres wartości 1–65535.

Krok 7 Wybierz dla opcji **Limit czasu** (Timeout) ustawienie **Długi limit czasu** (Long Timeout) lub **Krótki limit czasu** (Short Timeout).

Krok 8 Kliknij przycisk **OK**.

Rysunek 3-12 Agregacja łączy

3.10 Konfigurowanie protokołu SNMP

SNMP (Simple Network Management Protocol) jest standardowym protokołem zarządzania siecią w Internecie i jest powszechnie stosowany do uzyskiwania dostępu do urządzeń i zarządzania nimi. Funkcje protokołu SNMP są następujące:

- Inteligentne zarządzanie urządzeniami sieciowymi. Korzystając z sieciowej platformy zarządzania opartej na protokole SNMP, administrator sieci może sprawdzać stan uruchomienia i ustawienia urządzeń sieciowych, konfigurować ustawienia, wyszukiwać błędy, diagnozować usterki, a następnie zaplanować wydajność i wygenerować raport.
- Protokół SNMP umożliwia zarządzanie urządzeniami o różnych cechach sprzętowych. Protokół SNMP zapewnia tylko podstawową bibliotekę funkcji. Zapewnia on niezależność zadań zarządzania i cech sprzętowych od technologii sieciowej zarządzanych urządzeń, dlatego umożliwia zarządzanie urządzeniami różnych producentów.

Sieć protokołu SNMP zapewnia dwa komponenty: system NMS i agenta.

- System zarządzania siecią (NMS, Network Management System) jest menedżerem w sieci protokołu SNMP, zapewniającym łatwy w użyciu interfejs człowiek-maszyna, ułatwiający administratorowi wykonywanie większości zadań związanych z zarządzaniem siecią.
- Agent jest zarządzaną rolą w sieci protokołu SNMP, odbierającą i obsługującą pakiety żądań z systemu NMS. W niektórych sytuacjach zagrożenia, takich jak zmiana stanu portu, agent może aktywnie wysyłać pakiety alarmowe do systemu NMS.

3.10.1 Konfigurowanie protokołu SNMP V1 i V2

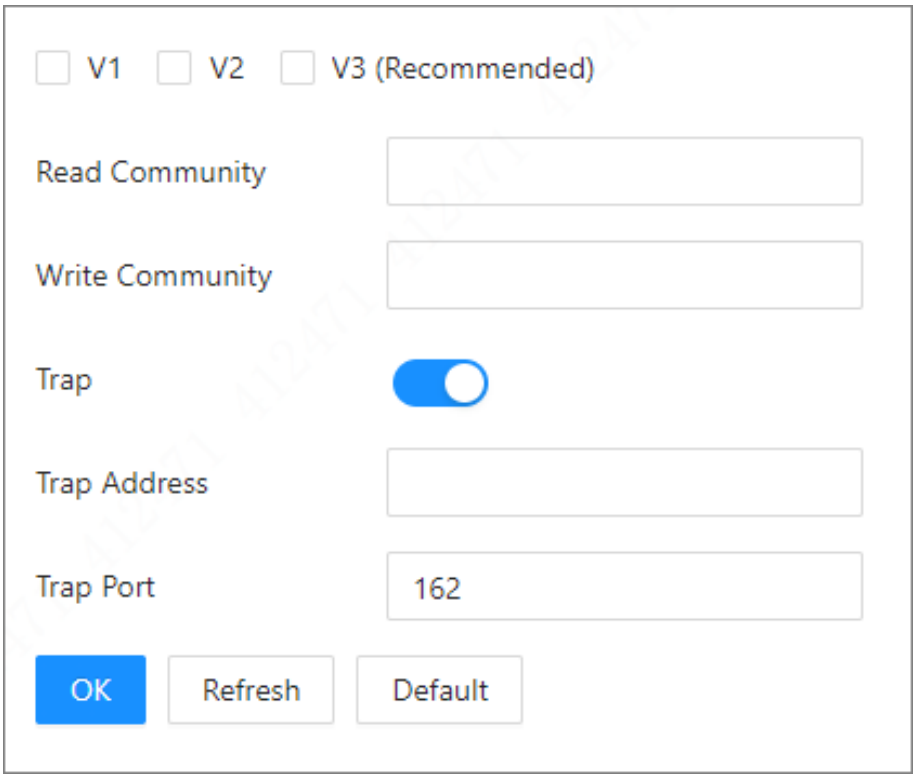
Procedura

Krok 1 Wybierz **Ustawienia sieci > SNMP** (Network Settings > SNMP).

Krok 2 Wybierz wersję **V1** lub **V2**.

Krok 3 Skonfiguruj ustawienia takie jak **Wspólnota odczytu** (Read Community), **Wspólnota zapisu** (Write Community), **Adres pułapka** (Trap Address) i **Port pułapka** (Trap Port).

Rysunek 3-13 Funkcja SNMP



Krok 4 Kliknij przycisk **OK**.

3.10.2 Konfigurowanie protokołu SNMP V3

Procedura

Krok 1 Wybierz **Ustawienia sieci > SNMP** (Network Settings > SNMP).

Krok 2 Wybierz wersję **V3**.

Krok 3 Skonfiguruj ustawienia.

Rysunek 3-14 Protokół SNMP V3

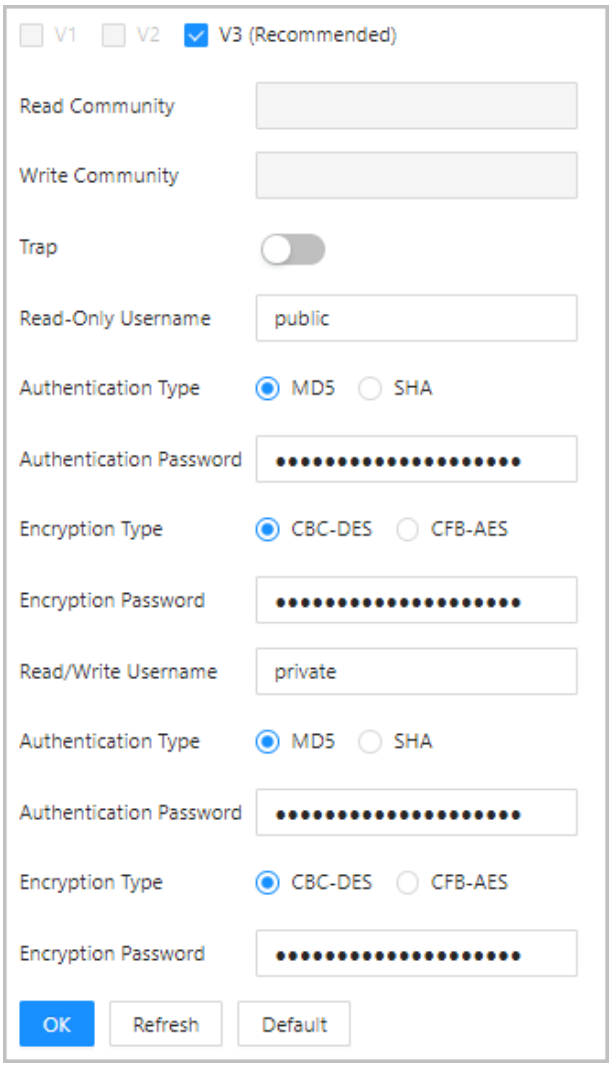


Tabela 3-9 Opis ustawień funkcji SNMP

Ustawienie	Opis
Wspólnota odczytu (Read community)	Wspólnota odczytu obsługiwana przez programy agentów.
Wspólnota zapisu (Write community)	Wspólnota zapisu obsługiwana przez programy agentów.
Adres pułapka (Trap address)	Adres docelowy informacji pułapek wysłanych przez program agenta.
Port pułapka (Trap port)	Port docelowy informacji pułapek wysłany przez program agenta.
Nazwa użytkownika tylko do odczytu (Read-only username)	Skonfiguruj nazwę użytkownika przeznaczoną tylko do odczytu. Dotyczy tylko wersji V3.
Typ uwierzytelniania (Authentication type)	Skonfiguruj tryb uwierzytelniania, gdy ustawiono poziom zabezpieczeń **Uwierzytelnianie bez szyfrowania** (Authentication no encryption) lub **Uwierzytelnianie i szyfrowanie** (Authentication and encryption). Dostępne są tryby uwierzytelniania **MD5** i **SHA**.
Hasło uwierzytelniania (Authentication password)	Skonfiguruj hasło uwierzytelniania.

Ustawienie	Opis
Typ szyfrowania (Encryption type)	Skonfiguruj tryb szyfrowania, gdy ustawiono tryb uwierzytelniania **Uwierzytelnianie i szyfrowanie** (Authentication and encryption).
Hasło szyfrowania (Encryption password)	Skonfiguruj hasło szyfrowania, gdy ustawiono tryb uwierzytelniania **Uwierzytelnianie i szyfrowanie** (Authentication and encryption).
Nazwa użytkownika do odczytu/zapisu (Read/Write username)	Skonfiguruj nazwę użytkownika przeznaczoną do odczytu i zapisu.

Krok 4 Kliknij przycisk **OK**.

3.11 Konfigurowanie tabeli MAC

W tabelach MAC (Media Access Control) zapisywane są powiązania adresów MAC z portami oraz informacje dotyczące między innymi sieci VLAN, do której należy port. Gdy urządzenie przekazuje pakiet, wyszukuje dla niego adres docelowy w tabeli MAC. Jeżeli docelowy adres MAC pakietu jest podany w tabeli MAC, pakiet jest przesyłany bezpośrednio przez powiązany port wskazany w tabeli. Jeżeli docelowy adres MAC pakietu nie jest podany w tabeli MAC, urządzenie używa trybu rozgłaszania do przekazania pakietu do wszystkich portów z wyjątkiem portu odbiorczego w sieci VLAN.

3.11.1 Dodawanie tabeli MAC

Procedura

Krok 1 Wybierz **Ustawienia sieci > Tabela MAC** (Network Settings > MAC Table).

Krok 2 Na karcie **Tabela MAC** (MAC Table) kliknij przycisk **Dodaj** (Add).

Krok 3 Skonfiguruj adres MAC, VLAN i port.

Na przykład powiąż adres MAC 00:00:00:00:00:01 z portem 3 w sieci VLAN2.

Krok 4 Kliknij przycisk **OK**.

Rysunek 3-15 Dodawanie tabeli MAC

Powiązane działania

Rys. 3-16 Powiązane procedury

- Usuwanie statycznego adresu MAC: Wybierz adres MAC, a następnie kliknij przycisk **Usuń** (Delete).

- Odświeżanie listy adresów MAC: Kliknij przycisk **Odśwież** (Refresh) lub włącz opcję **Automatyczne odświeżanie** (Auto Refresh).
- Czyszczenie dynamicznego adresu MAC: Kliknij przycisk **Wyczyść dynamiczny adres MAC** (Clear Dynamic MAC).
- Wyszukiwanie adresu MAC i portu: Wprowadź adres MAC lub numer portu w prawym górnym rogu, a następnie kliknij przycisk **Wyszukaj** (Search).

3.11.2 Filtrowanie MAC portu

Informacje wstępne

Po włączeniu filtrowania MAC portu urządzenia o poniższych adresach MAC mogą komunikować się z portem.

- Urządzenia z listy dozwolonych adresów MAC
- Adresy MAC przełączane do trybu statycznego z dynamicznego

Po włączeniu filtrowania MAC port nie może uzyskać dostępu do adresu zarządzania lub logowania.

Procedura

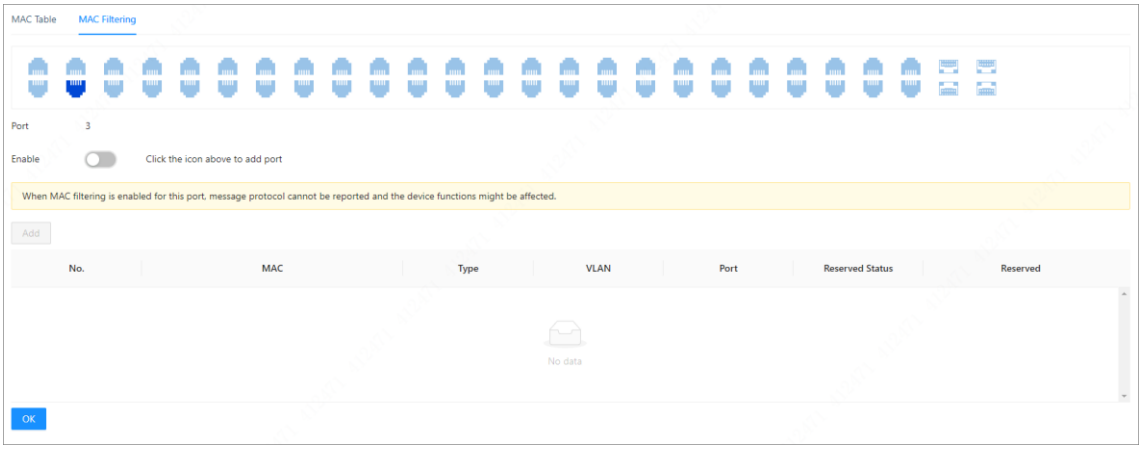
Krok 1 Wybierz **Ustawienia sieci > Tabela MAC** (Network Settings > MAC Table).

Krok 2 Na karcie **Filtrowanie MAC** (MAC Filtering) wybierz port, a następnie kliknij przycisk , aby włączyć funkcję filtrowania.

Krok 3 Skonfiguruj filtrowanie MAC portu.

- Przełącz z trybu dynamicznego do statycznego.
  1. Wybierz jeden rekord, a następnie wybierz przycisk obok etykiety **Zarezerwowane** (Reserved).
  2. Kliknij przycisk **OK**.
     Typ zostanie zmieniony z **Dynamiczny** (Dynamic) na **Statyczny** (Static).
     Statyczne urządzenia MAC mogą prawidłowo komunikować się z portem.
- Utwórz listę dozwolonych MAC.
  1. Kliknij przycisk **Dodaj** (Add).
  2. Skonfiguruj adres MAC i sieć VLAN.
  3. Kliknij przycisk **OK**.

Rysunek 3-17 Filtrowanie MAC



3.12 Konfigurowanie funkcji LLDP

Protokół LLDP (Link Layer Discovery Protocol) jest standardowym sposobem odnajdywania warstw łącza. Umożliwia on tworzenie głównych funkcji, adresów zarządzania, numerów urządzeń i numerów portów jako wartości TLV (Type Length Value), umieszczanie ich w jednostce LLDPDU (Link Layer Discovery Protocol Data Unit) i udostępnianie sąsiedniemu urządzeniu. Sąsiednie urządzenie przechowuje odebrane informacje w standardowej bazie danych zarządzania (MIB, Management Information Base), aby umożliwić systemowi zarządzania siecią sprawdzanie i ocenę stanu komunikacji łącza.

Procedura

Krok 1 Wybierz **Ustawienia sieci > LLDP** (Network Settings > LLDP).

Krok 2 Na karcie **Zdalne urządzenie LLDP** (LLDP Remote Device) wyświetlane są informacje o zdalnym urządzeniu LLDP.

Rysunek 3-18 Zdalne urządzenie LLDP

4 Zarządzanie PoE

Korzystając z funkcji PoE, urządzenie może używać przewodów sieciowych do podłączania zewnętrznych urządzeń PD (Powered Device) w celu zdalnego zasilania przez elektryczne złącza Ethernet. Funkcja PoE umożliwia centralne zasilanie i ułatwia wykonywanie kopii zapasowych. Złącza sieciowe nie wymagają zewnętrznego zasilania i wymagają tylko jednego przewodu sieciowego. Urządzenie jest zgodne ze standardami IEEE 802.3af, IEEE 802.3at i IEEE 802.3bt i wyposażone w uniwersalne złącze zasilania. Można go używać w telefonach internetowych, punktach dostępu (AP, Access Point) sieci bezprzewodowych, ładowarkach przenośnych, czytnikach kart kredytowych, kamerach sieciowych i urządzeniach do zbierania danych.

- Przełączniki non-PoE nie obsługują tej funkcji.
- Tylko niektóre modele przełączników PoE są zgodne ze standardem IEEE 802.3at. Pojedynczy port BT zapewnia moc maksymalnie 90 W. Aby uzyskać więcej informacji, należy skorzystać z dokumentacji danego produktu.

4.1 Konfigurowanie ustawień PoE

Wybierz **Zarządzanie PoE** > **Ustawienia PoE** (PoE Management > PoE Settings). Można skonfigurować ustawienia zasilania, stan zasilania, stan portu i sterowanie.

Procedura

Krok 1 W obszarze **Ustawienia zasilania** (Power Settings) można wyświetlić łączną moc czterech portów oraz skonfigurować moc zarezerwowaną i alarmową.

Krok 2 W obszarze **Stan zasilania** (Power Status) wyświetlany jest pobór mocy, pozostała moc i moc zarezerwowana.

Krok 3 W obszarze **Stan portu i sterowanie** (Port Status and Control) wybierz z listy pozycję **Zarządzanie PoE** (PoE Management), aby włączyć lub wyłączyć zasilanie PoE danego portu.

Krok 4 Kliknij przycisk **OK**.

Rysunek 4-1. Ustawienia zasilania PoE

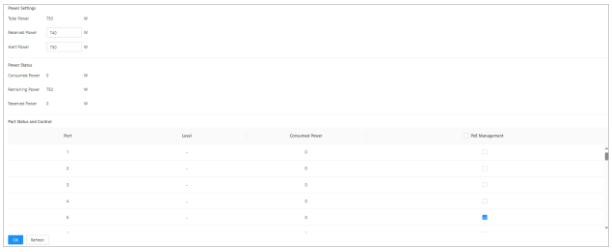


Tabela 4-1 Opis ustawień zasilania PoE

Ustawienie		**Opis**
Ustawienia zasilania	Łączna moc (Total power)	Łączna moc PoE

Ustawienie		Opis
(Power settings)	Moc zarezerwowana (Reserved power)	Skonfiguruj zarezerwowaną moc PoE.
	Moc alarmowa (Alert Power)	Skonfiguruj alarmową moc PoE.
Stan zasilania (Power status)	Pobór mocy (Consumed power)	Bieżący pobór mocy PoE przez wszystkie porty
	Pozostała moc (Remaining power)	Bieżąca pozostała moc PoE
	Moc zarezerwowana (Reserved power)	Moc PoE niedostępna do użytku. Moc zarezerwowana = Łączna moc – Przeciążenie.
Stan portów i sterowanie (Port status and control)	Poziom (Level)	Poziom mocy dla urządzeń terminalowych. Ustawienia poziomu mocy zasilania należą do zakresu 0–8, a standardowy poziom Hi-PoE to „5+”.
	Pobór mocy (Consumed power)	Bieżący pobór mocy PoE przez odpowiedni pojedynczy port
	Zarządzanie PoE (PoE management)	Wybierz ustawienie **Włącz** (Enable) lub **Wyłącz** (Disable). ● Po wybraniu ustawienia **Wyłącz** (Disable) system nie zasila urządzeń PD (Powered Device) i nie rezerwuje zasilania dla tych urządzeń. ● Wybranie ustawienia **Włącz** (Enable) portu PoE nie może powodować przeciążenia zasilania PoE. Jeżeli ten warunek nie zostanie spełniony, nie można włączyć funkcji PoE portu PoE. ● Domyślnie zasilanie PoE portów PoE jest wyłączone. ● Przeciążenie PSE: Gdy łączny pobór mocy przez wszystkie porty przekracza maksymalną moc PSE, system zgłasza przeciążenie PSE.

4.2 Konfigurowanie stałego zasilania PoE

Procedura

Krok 1 Wybierz **PoE Management > Stałe zasilanie PoE** (PoE Management > Perpetual PoE).

Krok 2 Kliknij przycisk , aby włączyć funkcję **Włącz na stałe** (Global Enable).

Krok 3 Kliknij przycisk **OK**, aby zapisać konfigurację.

4.3 Konfigurowanie dużego zasięgu PoE

Informacje wstępne

Włączenie funkcji Duży zasięg PoE (Long Distance PoE) umożliwia zwiększenie zasięgu transmisji ze 100 m do 250 m przy równoczesnym zmniejszaniu szybkości transmisji ze 100 Mb/s do 10 Mb/s.

Tryb większego zasięgu (Extend Mode) umożliwia transmisję z portu PoE na odległość 250 m przy równoczesnym zmniejszaniu szybkości transmisji do 10 Mb/s. Rzeczywisty zasięg transmisji jest zależny od poboru mocy przez podłączone urządzenia oraz typu i stanu przewodów.

Procedura

Krok 1 Wybierz **Zarządzanie PoE > Duży zasięg PoE** (PoE Management > Long Distance PoE).

Krok 2 Kliknij przycisk odpowiedniego portu, aby włączyć duży zasięg PoE.

Krok 3 Kliknij przycisk **OK**.

Rysunek 4-2 Duży zasięg PoE

4.4 Wyświetlanie statystyk zdarzeń PoE

Wybierz **Zarządzanie PoE > Statystyki zdarzeń PoE** (PoE Management > PoE Event Statistics), aby wyświetlić statystyki zdarzeń PoE.

Tabela 4-2 Opis statystyk zdarzeń PoE

Ustawienie	Opis
Przeciążenie (Overload)	Pojedynczy port jest uruchamiany po przekroczeniu progowego natężenia prądy portu.
Zwarcie (Short circuited)	Gdy mikroukład zasilający wysyła zasilanie do portu, następuje jego zwarcie.
Rozłączenie DC (DC disconnect)	Wyłączenie zasilania pojedynczego portu
Zwarcie podczas uruchamiania (Short circuit during startup)	Gdy mikroukład zasilający wysyła zasilanie, następuje zwarcie.

Ustawienie	Opis
Zabezpieczenie termiczne (Overheat protection)	Pojedynczy port jest uruchamiany po przekroczeniu wartości progowej temperatury mikroukładu zasilającego..

4.5 Konfigurowanie energooszczędnego zasilania PoE

Energooszczędne zasilanie PoE umożliwia zmniejszenie poboru mocy przy zachowaniu pełnej zgodności z istniejącym wyposażeniem.

Procedura

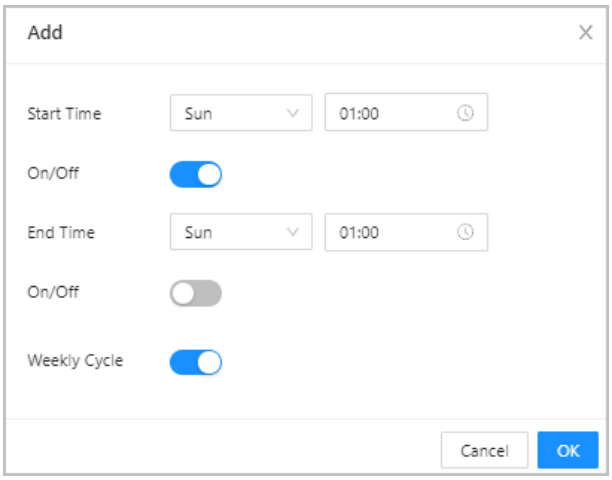
Krok 1 Wybierz **Zarządzanie PoE > Energooszczędne zasilanie PoE** (PoE Management > Green PoE).

Krok 2 Dodaj ustawienia **Godzina początkowa** (Start Time) i **Godzina końcowa** (End Time).

Krok 3 Wybierz port, a następnie kliknij przycisk , aby włączyć energooszczędne zasilanie PoE.

Krok 4 Kliknij przycisk **OK**.

Rysunek 4-3 Energooszczędne zasilanie PoE



4.6 Konfigurowanie wymuszania zasilania PoE

Informacje wstępne

Po włączeniu funkcji Wymuś PoE (Force PoE) port wymusza zasilanie urządzenia PD, nawet wówczas, gdy urządzenie podłączone do portu nie spełnia wymagań. Zachowaj ostrożność.

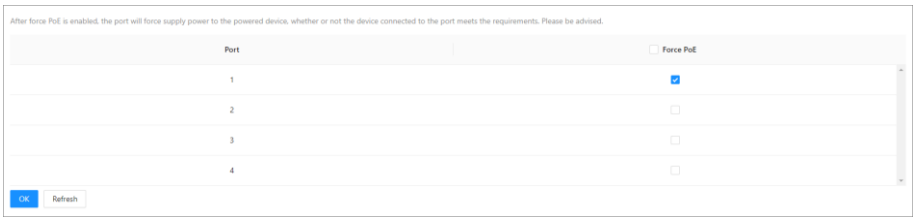
Procedura

Krok 1 Wybierz **Zarządzanie PoE > Wymuś PoE** (PoE Management > Force PoE).

Krok 2 Kliknij przycisk odpowiedniego portu, aby włączyć energooszczędne zasilanie PoE.

Krok 3 Kliknij przycisk **OK**.

Rysunek 4-4 Wymuś zasilanie PoE



4.7 Konfigurowanie funkcji PoE Watchdog

Informacje wstępne

Korzystając z funkcji PoE Watchdog, można co 60 sekund monitorować zasilane urządzeń PD (Powered Device) i utrzymywać je w trybie online. W przypadku braku transmisji danych następuje automatyczne wyłączenie zasilanie portu i jego ponowne uruchomienie.

Nie można równocześnie włączyć funkcji **Wymuś PoE** (Force PoE) i **PoE Watchdog**.

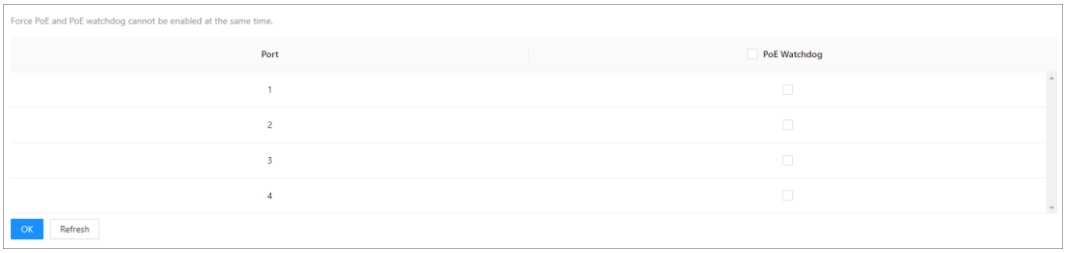
Procedura

Krok 1 Wybierz **Zarządzanie PoE > PoE Watchdog** (PoE Management > PoE watchdog).

Krok 2 Kliknij przycisk odpowiedniego portu, aby włączyć monitorowanie PoE.

Krok 3 Kliknij przycisk **OK**.

Rysunek 4-5 Monitorowanie PoE



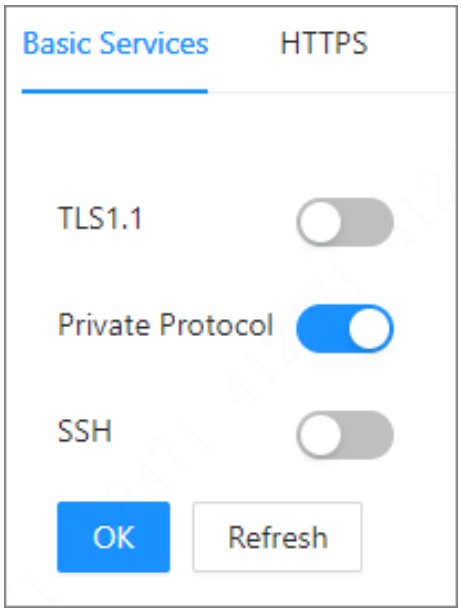
5 Zabezpieczenia

5.1 Usługi podstawowe

5.1.1 Konfigurowanie podstawowych usług

Protokół bezpiecznej warstwy transportu (TLS) gwarantuje poufność i integralność danych podczas komunikacji aplikacji. Ten protokół składa się z dwóch warstw: rejestrowania i uzgadniania TLS. Protokół TLS1.1 używa jednak słabego algorytmu szyfrowania. Zalecamy wyłączenie tej opcji.
Protokół prywatny jest niepublikowanym protokołem. Zalecamy wyłączenie tej opcji.
Protokoły zabezpieczeń SSH i Secure Shell są oparte na warstwie aplikacji. SSH jest niezawodnym protokołem zapewniającym bezpieczeństwo zdalnych sesji logowania i innych usług sieciowych. Użycie funkcji SSH skutecznie zapobiega nieautoryzowanemu ujawnieniu informacji podczas zdalnego zarządzania.

Rysunek 5-1 Usługi podstawowe



5.1.2 Konfigurowanie funkcji HTTPS

Protokół HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) opisuje usługi przy użyciu zabezpieczeń TLS (Transport Layer Security). Protokół HTTPS zapewnia usługę sieci Web oraz usługi dostępu ONVIF i RTSP.

Procedura

Krok 1 Wybierz **Zabezpieczenia > HTTPS** (Zabezpieczenia > HTTPS).

Krok 2 (Opcjonalnie) Na karcie **Usługi podstawowe** (Basic Services) kliknij przycisk , aby włączyć zabezpieczenia TLS1.1 zależnie od potrzeb, a następnie kliknij przycisk **OK**.

Domyślnie interfejs internetowy obsługuje tylko zabezpieczenia TLS1.2. Jeżeli konieczne jest użycie protokołu TLS1.1, należy włączyć funkcję TLS1.1 w interfejsie internetowym. Należy pamiętać, że korzystanie z protokołu TLS1.1 jest związane z zagrożeniami. Należy wyłączyć funkcję TLS1.1, aby zapobiec nieoczekiwanym zagrożeniom.

Krok 3 Na karcie **HTTPS** kliknij przycisk , aby włączyć funkcję HTTPS.

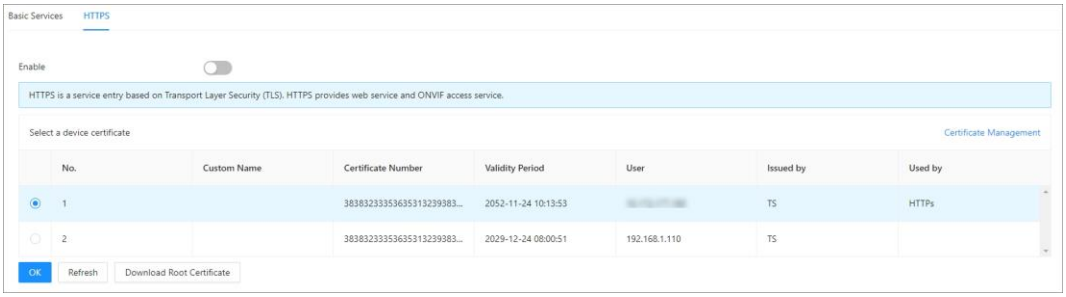
Krok 4 Wybierz certyfikat urządzenia.

Krok 5 Wybierz łącze **Zarządzanie certyfikatami** (Certificate Management), aby wyświetlić stronę **Certyfikat CA** (CA Certificate).

Więcej informacji podano w sekcji „5.2. Konfigurowanie certyfikatu. Urzędu certyfikacji".

Krok 6 Kliknij przycisk **OK**.

Rysunek 5-2 Konfigurowanie funkcji HTTPS



5.2 Konfigurowanie certyfikatu urzędu certyfikacji

5.2.1 Instalowanie certyfikatu urządzenia

Certyfikat urządzenia jest dowodem jego legalności. Na przykład certyfikat urządzenia jest weryfikowany podczas dostępu do urządzenia przy użyciu przeglądarki i protokołu HTTPS.

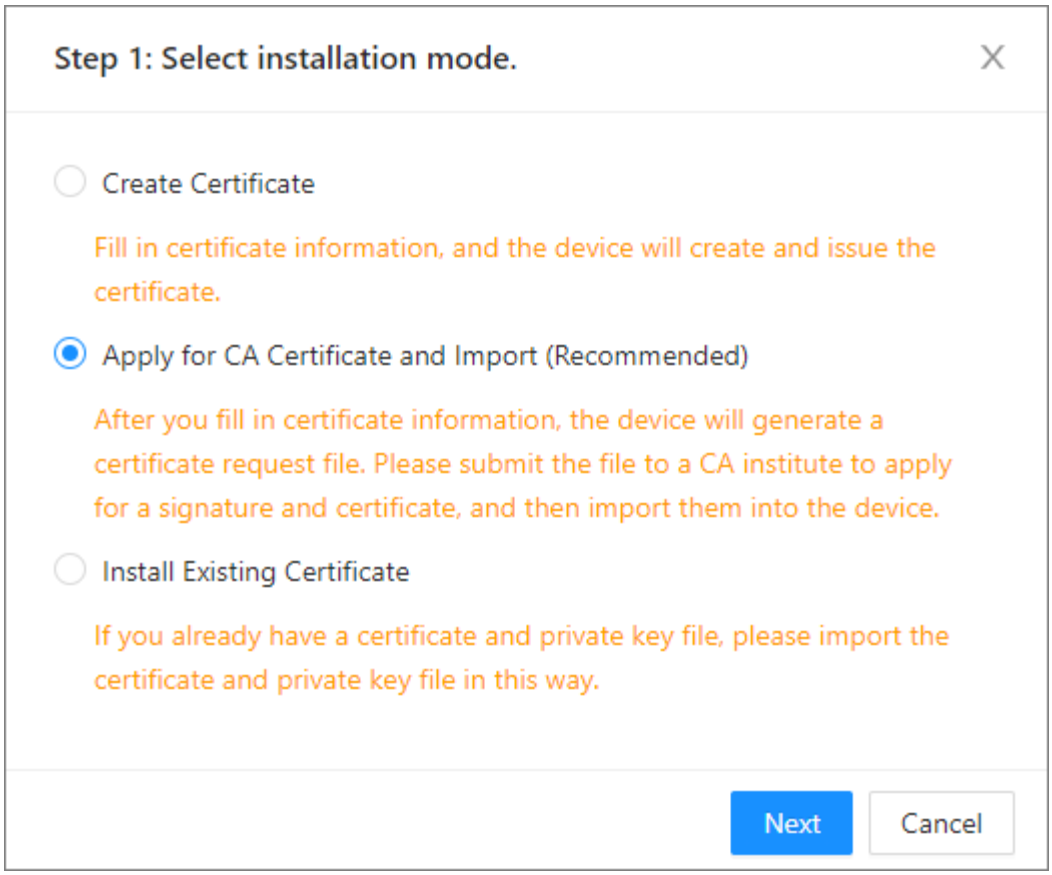
Procedura

Krok 1 Wybierz **Zabezpieczenia > Certyfikat urzędu certyfikacji > Certyfikat urządzenia** (Security > CA Certificate > Device Certificate).

Krok 2 Na karcie **Certyfikat urządzenia** (Device Certificate) kliknij przycisk **Zainstaluj certyfikat urządzenia** (Install Device Certificate).

Krok 3 Wybierz tryb instalacji zależnie od potrzeb.

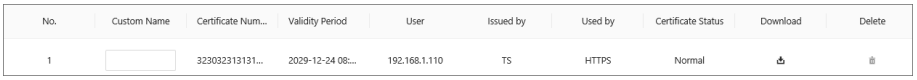
Rysunek 5-3 Wybór trybu instalacji



Krok 4 Wprowadź informacje o certyfikacie, a następnie kliknij opcję **Stwórz i zainstaluj certyfikat** (Create and install certificate), **Stwórz i pobierz** (Create and Download) i **Importuj i instaluj** (Import and Install).

Krok 5 (Opcjonalnie) Kliknij przycisk **Wejdź do trybu edycji** (Enter Edit Mode), aby edytować ustawienie **Nazwa niestandardowa** (Custom Name), a następnie kliknij przycisk **Zapisz konfigurację** (Save Config).

Rysunek 5-4 Edytowanie certyfikatu



Powiązane działania

- Pobieranie certyfikatu: Kliknij przycisk .
- Usuwanie certyfikatu: Kliknij przycisk .

5.2.2 Instalowanie certyfikatów zaufanego urzędu certyfikacji

Informacje wstępne

Certyfikat zaufanego urzędu certyfikacji (CA, Certification Authority) jest używany do weryfikowania legalności hosta. Na przykład zostanie zainstalowany certyfikat urzędu certyfikacji dla przełącznika, umożliwiający uwierzytelnianie 802.1x.

Obsługiwane jest tylko instalowanie certyfikatu podrzędnego urzędu certyfikacji.

Procedura

Krok 1 Wybierz **Zabezpieczenia > Certyfikat urzędu certyfikacji** (Security > CA Certificate).

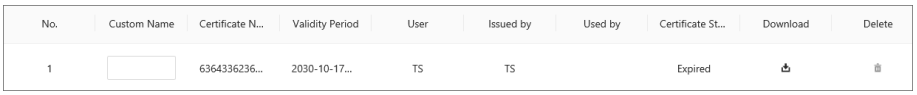
Krok 2 Na karcie **Certyfikaty zaufanych urzędów certyfikacji** (Trusted CA Certificates) kliknij przycisk **Instaluj certyfikat zaufany** (Install Trusted Certificate).

Krok 3 Kliknij przycisk **Przeglądaj** (Browse), a następnie kliknij przycisk **OK**.

Rysunek 5-5 Instalowanie certyfikatu zaufanego

Krok 4 (Opcjonalnie) Kliknij przycisk **Włącz tryb edycji** (Enter Edit Mode), aby edytować ustawienie **Nazwa niestandardowa** (Custom Name), a następnie kliknij przycisk **Zapisz konfigurację** (Save Config).

Rysunek 5-6 Edytowanie certyfikatu



Powiązane działania

- Pobieranie certyfikatu: Kliknij przycisk .
- Usuwanie certyfikatu: Kliknij przycisk .

5.3 Konfigurowanie ochrony przed atakiem

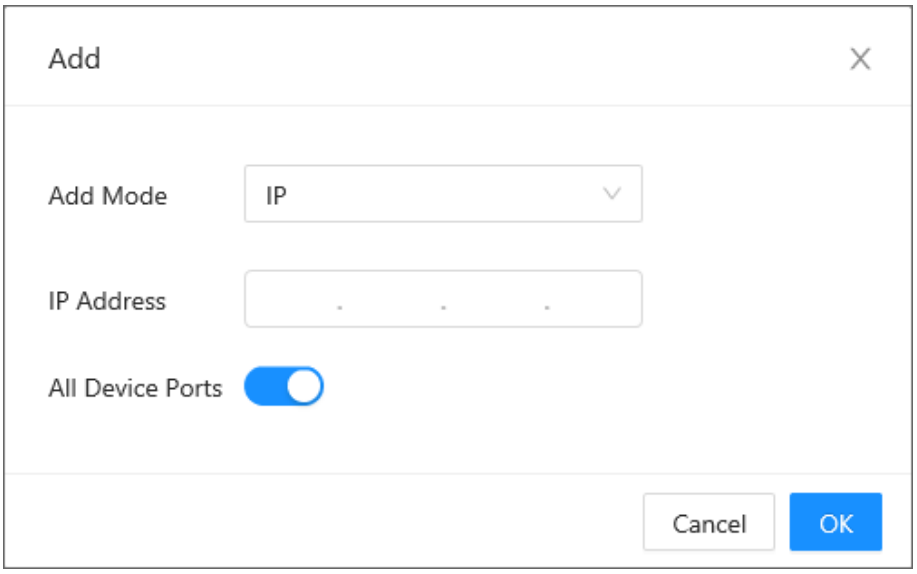
5.3.1 Konfigurowanie zapory

Procedura

Krok 1 Wybierz **Zabezpieczenia > Ochrona przed atakami** (Security > Attack Defense).

Krok 2 Na karcie **Zapora** (Firewall) kliknij przycisk **Wszystko** (All), aby zezwolić hostom źródłowym na dostęp do wszystkich portów urządzenia z dowolnych adresów IP/MAC.
Kliknij przycisk **Lista dozwolonych** (Allowlist), aby wyświetlić listę adresów IP/MAC hostów źródłowych uprawnionych do dostępu do odpowiednich portów urządzenia, a następnie kliknij przycisk **Dodaj** (Add), aby dodać hosty do listy dozwolonych.

Rysunek 5-7 Dodawanie do listy dozwolonych



Kliknij przycisk **Lista zabronionych** (Blocklist), aby wyświetlić listę adresów IP/MAC hostów źródłowych, które nie są uprawnione do dostępu do odpowiednich portów urządzenia przy użyciu połączenia sieciowego. Kliknij przycisk **Dodaj** (Add), aby dodać hosty do listy zabronionych.

Rysunek 5-8 Dodawanie do listy zabronionych

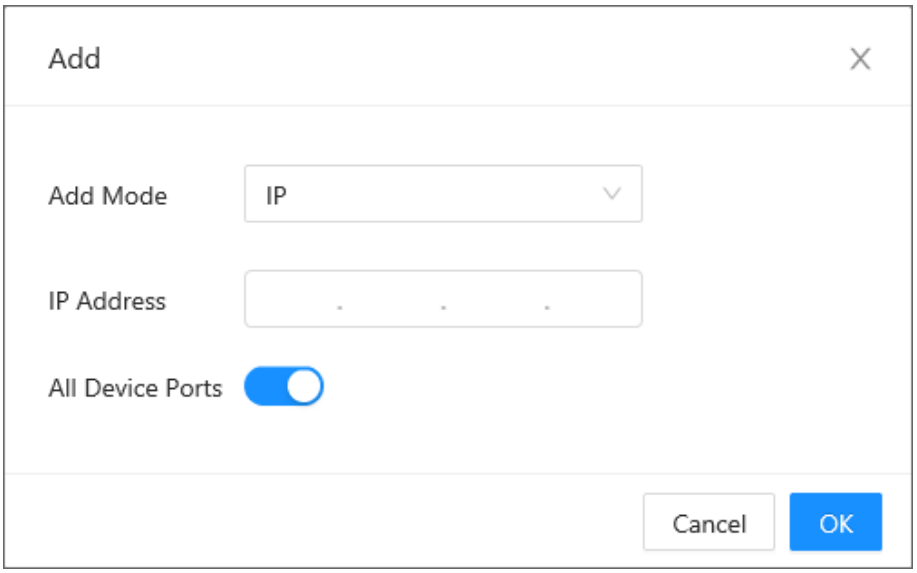


Tabela 5-1 Zapora

Ustawienie	Opis
Wszystko (All)	Hosty źródłowe mogą uzyskać dostęp do wszystkich portów urządzenia z dowolnych adresów IP/MAC.
Lista dozwolonych (Allowlist)	Tylko hosty źródłowe, których adresy IP/MAC uwzględniono na tej liście, mogą uzyskać dostęp do odpowiednich portów urządzenia.
Lista zabronionych (Blocklist)	Hosty źródłowe, których adresy IP/MAC uwzględniono na tej liście, nie są uprawnione do dostępu do odpowiednich portów urządzenia.

Krok 3 Kliknij przycisk **OK**.

5.3.2 Konfigurowanie ochrony przed atakiem DoS

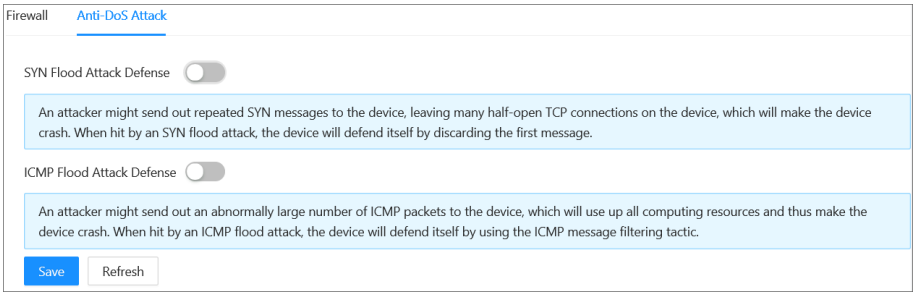
Procedura

Krok 1 Wybierz **Zabezpieczenia > Ochrona przed atakami** (Security > Attack Defense).

Krok 2 Na karcie **Ochrona przez atakiem DoS** (Anti-DoS Attack) kliknij przycisk , aby włączyć różne funkcje ochrony zależnie od potrzeb.

Krok 3 Kliknij przycisk **Zapisz** (Save).

Rysunek 5-9 Ochrona przed atakiem DoS



5.4 Konfigurowanie izolacji portów

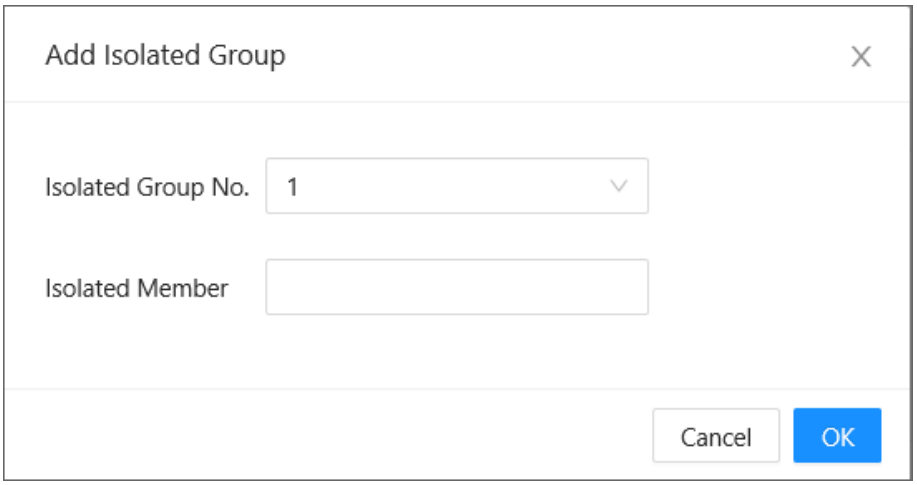
Izolowanie portów zapewnia drugą warstwę rozdzielającą wiadomości. Wystarczy dodać port do grupy izolowanej, aby rozdzielić dane drugiej warstwy między portami w tej grupie. Funkcja izolowania portów zapewnia użytkownikom bezpieczniejsze i bardziej wszechstronne rozwiązanie sieciowe.

Procedura

Krok 1 Wybierz **Zabezpieczenia > Izolowanie portów** (Security > Port Isolation).

Krok 2 Kliknij przycisk **Dodaj** (Add).

Rysunek 5-10 Dodawanie grupy izolowanej



Krok 3 Wybierz ustawienia **Nr grupy izolowanej** (Isolated Group No) i **Członek izolowany** (Isolated Member), a następnie kliknij przycisk **OK**.

Powiązane działania

- Edytowanie grupy izolowanej: Kliknij przycisk .
- Czyszczenie grupy izolowanej: Kliknij przycisk .

6 Zasady sterowania

6.1 Konfigurowanie priorytetów portów

Informacje wstępne

Domyślnie do połączeń głosowych 802.1p i DSCP sieci VLAN przypisywany jest priorytet odpowiednio 6 i 46. Można dynamicznie konfigurować priorytety 802.1p i DSCP w celu planowania różnych usług głosowych.

- Priorytet połączeń 802.1p jest reprezentowany przez wartość pola PRI, zawierającego trzy bity, w każdej ramce 802.1Q VLAN. To pole określa priorytet transmisji pakietów danych przy przeciążeniu urządzenia przełączającego.
- Wartość DSCP jest reprezentowana przez sześć bitów w polu typu usługi (ToS, Type of Service) w nagłówku pakietu protokołu IPv4. Wartości DSCP, jako sygnalizacja dla usługi DiffServ, są używane do gwarantowania jakości usług (QoS) w sieciach protokołu Internetu (IP). Kontroler ruchu w bramie sieciowej wykonuje operacje tylko na podstawie informacji przekazywanych przy użyciu sześciu bitów.

Procedura

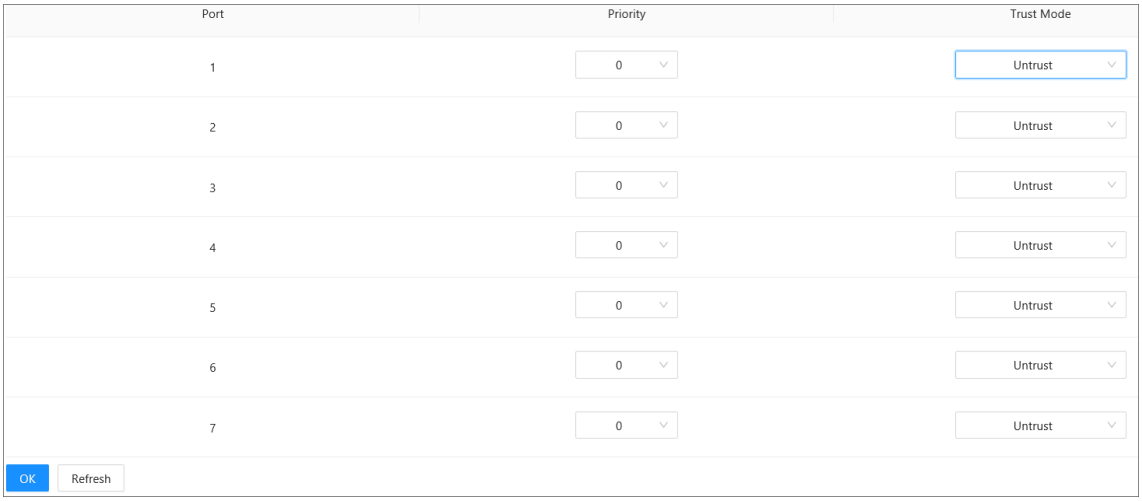
Krok 1 Wybierz **Zasady sterowania** > **Priorytety portów** (Control Policy > Port Priority).

Krok 2 Wybierz ustawienia **Priorytet** (Priority) i **Tryb zaufania** (Tryb zaufania).

Dostępne są cztery ustawienia trybu zaufania: **Niezaufane** (Untrust), **802.1P**, **DSCP** oraz **DSCP i 802.1P**.

Krok 3 Kliknij przycisk **OK**.

Rysunek 6-1 Konfigurowanie priorytetów portów



6.2 Konfigurowanie tabeli mapowania priorytetów

Procedura

Krok 1 Wybierz **Zasady sterowania > Tabela mapowania priorytetów** (Control Policy > Priority Mapping Table).

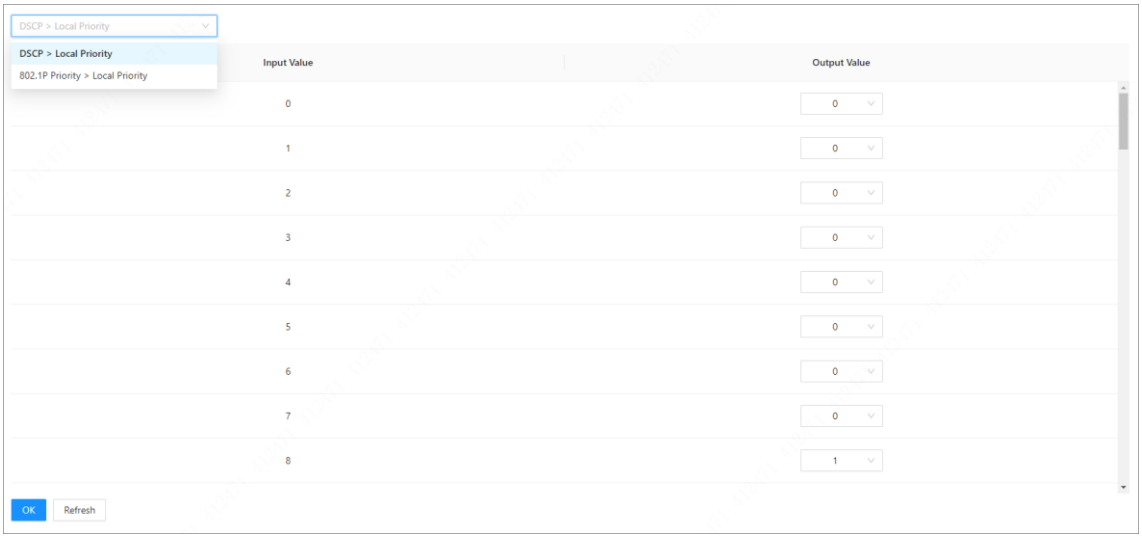
Krok 2 Wybierz **DSCP > Priorytet lokalny** (DSCP > Local Priority) lub **802.1p > Priorytet lokalny** (802.1p > Local Priority).

Krok 3 Wybierz ustawienie **Wartość wyjściowa** (Output Value).

Wartość wejściowa i wartość wyjściowa są zależne od trybu.

Krok 4 Kliknij przycisk **OK**.

Rysunek 6-2 Mapowanie priorytetów



6.3 Konfigurowanie planowania kolejek

Informacje wstępne

- PQ: Kolejkowanie priorytetowe. Metoda PQ polega na porządkowaniu pakietów zgodnie z priorytetami w kolejności malejącej. Pakiety w kolejkach o niższym priorytecie mogą być planowane dopiero po zaplanowaniu wszystkich pakietów o wyższym priorytecie.
- WRR: Ważony algorytm karuzelowy. Metoda WRR polega na umieszczaniu pakietów przez urządzenie w kolejkach zgodnie z przypisanymi wagami. Po jednej rundzie planowania wagi wszystkich kolejek są zmniejszane o 1. Nie można zaplanować kolejki, której waga została zmniejszona do 0.

Procedura

Krok 1 Wybierz **Zasady sterowania > Planowanie kolejek** (Control Policy > Queue Scheduling).

Krok 2 Wybierz ustawienie **Algorytm kolejki** (Queue Algorithm).

W trybie WRR waga kolejki priorytetowej wynosi Kolejka0:Kolejka1:Kolejka2:Kolejka3=1:2:4:8.

Krok 3 Kliknij przycisk **OK**.

Rysunek 6-3 Planowanie kolejek

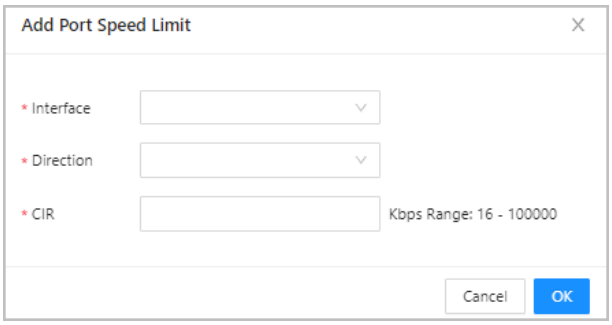
6.4 Konfigurowanie limitów szybkości portów

Procedura

Krok 1 Wybierz **Zasady sterowania > Limity szybkości portów** (Control Policy > Port Speed Limit).

Krok 2 Kliknij przycisk **Dodaj** (Add).

Rysunek 6-4 Dodawanie limitów szybkości portów



Krok 3 Wprowadź ustawienia **Interfejs** (Interface), **Kierunek** (Direction) i **CIR**.

- Dostępne są następujące ustawienia **Kierunku** (Direction): **Przychodzący** (In) i **Wychodzący** (Out).
- Reguła wejściowa dla ustawienia CIR: Zakres 16–100000 (musi być wielokrotnością całkowitą 16).

Krok 4 Kliknij przycisk **OK**.

6.5 Konfigurowanie kontroli burzy rozgłoszeniowej

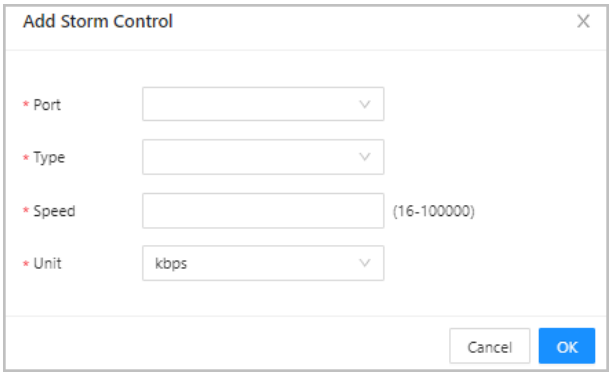
Ramki rozgłoszeniowe w sieci są przekazywane w sposób ciągły, co utrudnia prawidłową komunikację i znacznie zmniejsza wydajność sieci. Ograniczając przepływy rozgłoszeniowe portu i odrzucając ramki rozgłoszeniowe, gdy przepływ przekroczy określoną wartość progową, można zmniejszyć ryzyko burzy rozgłoszeniowej i zapewnić prawidłowe funkcjonowanie sieci.

Procedura

Krok 1 Wybierz **Zasady sterowania** > **Kontrola burzy rozgłoszeniowej** (Control Policy > Storm Control).

Krok 2 Kliknij przycisk **Dodaj** (Add).

Rysunek 6-5 Dodawanie kontroli burzy rozgłoszeniowej



Krok 3 Wprowadź ustawienia **Port**, **Typ** (Type) i **Szybkość** (Speed).

Krok 4 Kliknij przycisk **OK**.

7 Uwierzytelnianie

7.1 Konfigurowanie funkcji 802.1x

Protokół uwierzytelniania sieciowego 802.1X umożliwia otwarcie portów dostępu do sieci, gdy organizacja uwierzytelni tożsamość użytkownika i autoryzuje go do dostępu do sieci.

Procedura

Krok 1 Kliknij przycisk obok etykiety **Włącz** (Enable), aby włączyć magazyn NAS (Network Attached Storage).

Krok 2 Wybierz ustawienie **Stan portu** (Port Status).

Dostępne są następujące ustawienia stanu: **Auto**, **Wymuś nieautoryzowane** (Force unAuthorized) i **Wymuś autoryzowane** (Force Authorized).

Rysunek 7-1 Konfigurowanie funkcji 802.1x

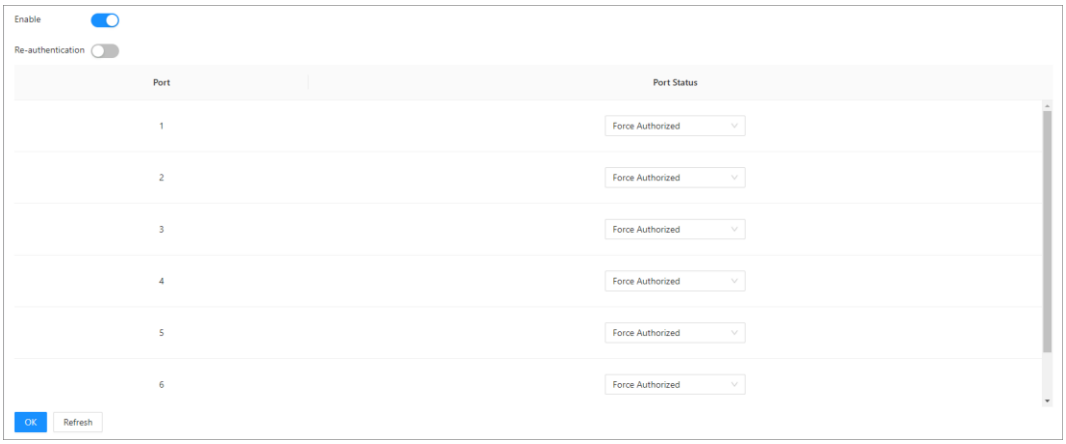


Tabela 7-1 Opis ustawień 802.1x

Ustawienie	Opis
Auto	Port automatycznie konfiguruje stan zgodnie z wynikami uwierzytelniania.
Wymuś nieautoryzowane (Force unAuthorized)	● Port jest zawsze nieautoryzowany, dlatego użytkownicy nie mogą uwierzytelniać się. ● Urządzenie nie świadczy usług uwierzytelniania dla użytkowników korzystających z tego portu.
Wymuś autoryzowane (Force Authorized)	Port jest zawsze autoryzowany, a użytkownicy mogą uzyskać dostęp do zasobów sieciowych bez uwierzytelniania.

Krok 3 Kliknij przycisk **OK**.

7.2 Konfigurowanie funkcji RADIUS

Informacje wstępne

Popularny protokół RADIUS (Remote Authentiation Diall-In User Service) obsługujący uwierzytelnianie AAA (Authentication, Authorization and Accounting).

RADIUS jest protokołem interakcji informacyjnej o konstrukcji rozproszonej i C/S. Umożliwia on ochronę sieci przed nieautoryzowanym dostępem. Ten protokół jest używany w sieciach zezwalających na dostęp zdalny, w których jest wymagany wyższy poziom bezpieczeństwa. Protokół określa format pakietów RADIUS i mechanizm przesyłania wiadomości. Protokół UDP jest używany jako warstwa transportu do hermetyzacji pakietów RADIUS.

RADIUS początkowo był protokołem uwierzytelniania AAA przeznaczonym tylko dla użytkowników połączeń telefonicznych. Rozwój dostępu użytkowników spowodował dostosowanie protokołu RADIUS do różnych metod dostępu, takich jak Ethernet i ADSL. Ten protokół zapewnia dostęp do serwerów poprzez uwierzytelnienie i autoryzację oraz zbieranie rekordów użycia źródeł sieciowych przy użyciu funkcji rejestrowania.

Procedura

Krok 1 Wybierz **Uwierzytelnianie > RADIUS** (Authentication > RADIUS).

Rysunek 7-2 Funkcja RADIUS

Krok 2 Kliknij przycisk **Dodaj** (Add).

Rysunek 7-3 Dodawanie instancji RADIUS

Krok 3 Skonfiguruj ustawienia **Adres IP**, **Port** i **Klucz** (Key).

Krok 4 Kliknij przycisk **OK**.