

Niezarządzalny switch PoE Fast Ethernet

Podręcznik użytkownika








Wstęp

Instrukcja ta przedstawia podstawowe funkcje i budowę niezarządzalnego switcha Fast Ethernet wyposażonego w porty PoE.

Instrukcje bezpieczeństwa

W instrukcji mogą pojawić się następujące słowa lub znaki ostrzegawcze o określonym znaczeniu.

 ZAGROŻENIE	Oznacza wysokie zagrożenie, które może prowadzić do śmierci lub poważnych obrażeń.
 WAŻNE OSTRZEŻENIE	Oznacza średnie bądź niskie zagrożenie, które może prowadzić do mniej poważnych obrażeń.
 OSTRZEŻENIE	Oznacza niskie zagrożenie, które może prowadzić do zniszczenia urządzenia, utraty danych, zmniejszenia wydajności lub innych nieprzewidzianych rezultatów.
 WSKAZÓWKA	Pozwala rozwiązać problem lub oszczędzić czas
 NOTATKA	Dodatkowe informacje rozszerzające zakres informacji.

Historia zmian

Wersja	Zmiany	Data wydania
V1.0.0	Wydanie pierwsze	Lipiec 2020

Informacje o podręczniku

- Niniejszy podręcznik ma charakter wyłącznie referencyjny. W razie rozbieżności między podręcznikiem a urządzeniem obowiązuje faktyczna nazwa elementów interfejsu urządzenia.
- Firma Dahua nie ponosi odpowiedzialności za jakiegokolwiek straty poniesione wskutek nieprzestrzegania zaleceń zawartych w niniejszym podręczniku.
- Niniejszy podręcznik będzie aktualizowany zgodnie z nowymi przepisami i regulacjami obowiązującymi w danych regionach. Szczegółowe informacje dostępne są w wersji drukowanej podręcznika, na płycie CD-ROM, po zeskanowaniu kodu QR oraz na oficjalnej stronie Dahua. W razie rozbieżności między wersją drukowaną a elektroniczną podręcznika obowiązuje wersja elektroniczna.
- Wszystkie projekty oraz oprogramowanie mogą zostać zmienione bez wcześniejszego powiadomienia na piśmie. Aktualizacje produktów mogą skutkować powstaniem różnic między produktami a treścią podręcznika. Aby uzyskać najnowsze informacje dotyczące oprogramowania oraz dokumentację uzupełniającą, skontaktuj się z działem obsługi klienta.
- Dokument może zawierać nieścisłości techniczne, rozbieżności w zakresie funkcji i działania produktów, a także błędy w druku. W razie wątpliwości obowiązują finalne wyjaśnienia dostarczone przez firmę.
- Zaktualizuj oprogramowanie do otwierania plików PDF lub zainstaluj inny, popularny program, jeśli nie możesz otworzyć podręcznika(w formacie PDF).

- Wszystkie znaki towarowe, zastrzeżone znaki towarowe oraz nazwy firm wymienione w niniejszym podręczniku należą do ich prawowitych właścicieli.
- W razie jakichkolwiek problemów z użytkowaniem urządzenia odwiedź naszą stronę internetową, skontaktuj się z dostawcą lub działem obsługi klienta.
- W razie wątpliwości obowiązują finalne wyjaśnienia dostarczone przez firmę.

Ważne informacje i ostrzeżenia

Niniejsza instrukcja pomoże Ci szybko zaznajomić się z urządzeniem. Aby zmniejszyć ryzyko niebezpieczeństwa i szkód materialnych przeczytaj dokładnie niniejszy podręcznik zanim zaczniesz używać urządzenia, i zachowaj go na przyszłość.

Wymogi operacyjne

- Nie umieszczaj ani nie montuj urządzenia w miejscu wystawionym na światło słoneczne lub w pobliżu źródła ciepła.
- Umieść urządzenie w miejscu, w którym nie będzie narażone na wilgoć, pył lub sadzę.
- Zamontuj urządzenie w pozycji poziomej i na stabilnym podłożu, aby zapobiegać upadkom.
- Nie wylewaj płynów na urządzenie ani nie umieszczaj na nim przedmiotów zawierających płyny. Ma to na celu ochronę urządzenia przed działaniem płynów, które mogą spowodować uszkodzenie komponentów wewnętrznych.
- Zamontuj urządzenie w dobrze wentylowanym miejscu i nie blokuj jego otworów wentylacyjnych.
- Urządzenie powinno być wykorzystywane wyłącznie z przewidzianym dla niego zasilaczem, podłączanym do gniazda zasilającego o podanych parametrach.
- Nie rozmontowuj samodzielnie urządzenia.
- Urządzenie należy transportować, użytkować oraz przechowywać w dozwolonym przedziale wilgotności i temperatur.

Bezpieczeństwo elektryczne

- Niewłaściwe użytkowanie akumulatora może doprowadzić do wybuchu lub pożaru.
- Wymieniając akumulator, upewnij się, że jest on tego samego typu co stosowany dotychczas. Postępuj zgodnie z instrukcjami, aby pozbyć się zużytego akumulatora.
- Używaj przewodów zasilających zalecanych w Twoim regionie oraz spełniających wymogi mocy znamionowej.
- Używaj zasilacza dołączonego do urządzenia. Używanie innego zasilacza może doprowadzić do obrażeń ciała lub uszkodzenia urządzenia.
- Źródło zasilania musi spełniać wymogi standardu bezpieczeństwa dla instalacji niskonapięciowych (SELV) oraz normy IEC60950-1. Pamiętaj, że wymogi dotyczące zasilania podane są na etykiecie urządzenia.
- Podłącz urządzenie (klasa izolacji typu I) do uziemionego gniazda zasilania.
- Przewód zasilający daje się odłączyć od urządzenia. Podczas użytkowania należy zachowywać kąt umożliwiający obsługę urządzenia

Spis treści

Wstęp	I
Ważne informacje i ostrzeżenia	II
Spis treści.....	III
1 Przegląd produktu	1
1.1 Opis.....	1
1.2 Właściwości	1
2 Budowa urządzenia	2
2.1 18-Portowy niezarządzalny switch Fast Ethernet	2
2.2 26-Portowy niezarządzalny switch Fast Ethernet	4
3 Instalacja i podłączenie.....	6
3.1 Instalacja.....	6
3.1.1 Instalacja desktop.....	6
3.1.2 Instalacja w szafie RACK.	6
3.2 Uruchamianie urządzenia.....	7
3.3 Podłączanie kabla sieciowego LAN.....	7
Zalecenia dotyczące cyberbezpieczeństwa	8

1 Przegląd produktu.

1.1 Opis

Niezarządzalny switch Fast Ethernet z 16 lub 24 portami PoE 10/100Mbps oraz dwoma portami Gigabit Ethernet uplink Combo.

Używa technologii „przechowaj i prześlij” w połączeniu z dynamiczną alokacją pamięci aby zapewnić efektywną komunikację na każdym porcie. Wsparcie dla kontroli przepływu zapobiega stratom pakietów podczas nadawania i odbierania. Kompatybilny z trzema środowiskami sieciowymi 10 Base-T, 100 Base-TX and 1000 Base-T automatycznie dopasowuje prędkość transmisji 10/100/1000 Mbps. Porty optyczne (SFP) do komunikacji na duże odległości przy użyciu włókien światłowodowych. Wsparcie dla standardów zasilania PoE IEEE802.3af i IEEE802.3at. Porty 1 i 2 wspierają Hi-PoE. Seria switchy zaprojektowana do łatwego użycia w sieciach domowych i biurowych.

1.2 Właściwości

Podstawowe właściwości

- Wsparcie dla standardów IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3az oraz IEEE802.3ab
- Kontrolę przepływu trybie pełnego duplex (standard IEEE802.3x) oraz pół-duplex dla pakietów zwrotnych
- Port 1 i 2 – wsparcie dla Hi-PoE.
- 2 gigabitowe porty optyczne uplink
- Technologia przechowaj i prześlij
- Auto-negocjacja prędkości transmisji dla portów UTP
- Automatyczna aktualizacja tablicy MAC adresów
- Obsługuje MDI / samoadaptacyjny MDIX
- Metalowa obudowa
- Funkcja PD alive
- Transmisja do 250m
- Funkcja QoS dla portów VIP
- Funkcja izolacji portów

Właściwości indywidualne

- 18-Portowy switch niezarządzalny Fast Ethernet : 16 × 10/100 Mbps portów RJ45 oraz 2porty Gigabit Ethernet uplink Combo, wbudowany zasilacz
- 26-Portowy switch niezarządzalny Fast Ethernet : 24 × 10/100 Mbps portów RJ45 oraz 2porty Gigabit Ethernet uplink Combo, wbudowany zasilacz

2 Budowa urządzenia

2.1 18-Portowy niezarządzalny switch Fast Ethernet

Rys. 2-1 - Panel przedni



Tabela 2-1 Opis panelu przedniego

Nr	Nazwa	Opis
1	Porty RJ45 PoE	Port 1-2 : 2x 10/100 Mbps RJ45, Hi-PoE Port 3-16 : 14 x 10/100 Mbps RJ45, PoE
2	Porty Uplink Combo	2x 10/100/1000 Mbps RJ45 lub 2x1000Mbps SFP
3	Przełączniki DIP	Użyj przełączników do wł./wył. następujących funkcji: PD alive – sprawdzanie aktywności urządzenia (kamery IP) Extend mode – zwiększenie odległości transmisji do 250m z prędkością 10Mbps VIP Port- Porty 1-8 są portami VIP, przy włączonej funkcji dane tych portów są przesyłane w pierwszej kolejności. Port Isolation – Porty PoE izolowane pomiędzy sobą, transmisja jedynie pomiędzy portami PoE i uplink.
4	Wskaźnik zasilania PoE	Wskazuje aktualny stan zasilania PoE
5	Wskaźnik statusu portu	Wskazuje aktualny stan połączenia portu RJ45
6	Wskaźnik PoE	Wskazuje stan zasilania PoE portu RJ45
7	Wskaźnik portów Uplink	Wskazuje stan połączenia portów Uplink
8	Wskaźnik stanu urządzenia	Wskaźnik zasilania i stanu urządzenia

Tabela 2-2 Opis wskaźników

Wskaźnik	Kolor wskaźnika	Stan	Opis
PWR	Zielony	Włączony	Zasilanie włączone
		Wyłączony	Zasilanie wyłączone
Wskaźnik PoE	Zielony	Włączony	Zasilanie PoE używane
		Wyłączony	Zasilanie PoE nieużywane
Wskaźnik statusu portu	Zielony	Wyłączony	Port nie podłączony
		Włączony	Port podłączony
		Miga	Port odbiera lub wysyła dane
Wskaźnik zasilania PoE	Zielony	Włączony	Pobór prądu przez wszystkie urządzenia PoE $\leq 50\%$
	Zielony, żółty	Zielony i żółty włączony	$50\% <$ Pobór prądu przez wszystkie urządzenia PoE $\leq 80\%$
	Zielony, żółty, czerwony	Zielony, żółty i czerwony włączony	Pobór prądu przez wszystkie urządzenia PoE $> 80\%$
Wskaźnik systemu	Zielony	Włączony	System uruchomiony
		Wyłączony	System nieuruchomiony

Rys. 2-2 - Panel tylny



Tabela 2-3 Opis panelu tylnego

Nr	Nazwa	Opis
1	Włącznik	Włączanie i wyłączanie urządzenia
2	Gniazdo zasilania	Podłączenie zasilania 100-240VAC
3	Złącze uziemienia	Podłączenie uziemienia, szyny wyrównawczej

2.2 26-Portowy niezarządzalny switch Fast Ethernet

Rys. 2-3 - Panel przedni

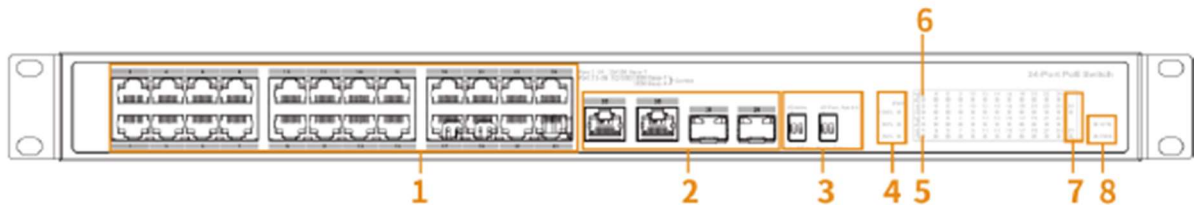


Tabela 2-4 Opis panelu przedniego

Nr	Nazwa	Opis
1	Porty RJ45 PoE	Port 1-2 : 2x 10/100 Mbps RJ45, Hi-PoE Port 3-16 : 14 x 10/100 Mbps RJ45, PoE
2	Porty Uplink Combo	2x 10/100/1000 Mbps RJ45 lub 2x1000Mbps SFP
3	Przełączniki DIP	Użyj przełączników do wł./wył. następujących funkcji: PD alive – nadzorowanie aktywności urządzenia (kamery IP) Extend mode – zwiększenie odległości transmisji do 250m z prędkością 10Mbps VIP Port- Porty 1-8 są portami VIP, przy włączonej funkcji dane tych portów są przesyłane w pierwszej kolejności. Port Isolation – Porty PoE izolowane pomiędzy sobą, transmisja jedynie pomiędzy portami PoE i uplink.
4	Wskaźnik zasilania PoE	Wskazuje aktualny stan zasilania PoE
5	Wskaźnik statusu portu	Wskazuje aktualny stan połączenia portu RJ45
6	Wskaźnik PoE	Wskazuje stan zasilania PoE portu RJ45
7	Wskaźnik portów Uplink	Wskazuje stan połączenia portów Uplink
8	Wskaźnik stanu urządzenia	Wskaźnik zasilania i stanu urządzenia

Tabela 2-5 Opis wskaźników

Wskaźnik	Kolor wskaźnika	Stan	Opis
PWR	Zielony	Włączony	Zasilanie włączone
		Wyłączony	Zasilanie wyłączone
Wskaźnik PoE	Zielony	Włączony	Zasilanie PoE używane
		Wyłączony	Zasilanie PoE nieużywane
Wskaźnik statusu portu	Zielony	Wyłączony	Port nie podłączony
		Włączony	Port podłączony
		Miga	Port odbiera lub wysyła dane
Wskaźnik zasilania PoE	Zielony	Włączony	Pobór prądu przez wszystkie urządzenia PoE $\leq 50\%$
	Zielony, żółty	Zielony i żółty włączony	$50\% < \text{Pobór prądu przez wszystkie urządzenia PoE} \leq 80\%$
	Zielony, żółty, czerwony	Zielony, żółty i czerwony włączony	Pobór prądu przez wszystkie urządzenia PoE $> 80\%$
Wskaźnik systemu	Zielony	Włączony	System uruchomiony
		Wyłączony	System nieuruchomiony

Rys. 2-4 - Panel tylny



Tabela 2-6 Opis panelu tylnego

Nr	Nazwa	Opis
1	Włącznik	Włączanie i wyłączanie urządzenia
2	Gniazdo zasilania	Podłączenie zasilania 100-240VAC
3	Złącze uziemienia	Podłączenie uziemienia, szyny wyrównawczej

3 Instalacja i podłączenie

3.1 Instalacja

3.1.1 Instalacja desktop

Urządzenie można zainstalować/położyć na stabilnym biurku w pobliżu źródła zasilania. Upewnić się, że jest wystarczająca przestrzeń wentylacyjna do rozpraszania ciepła.1 Instalacja na biurku

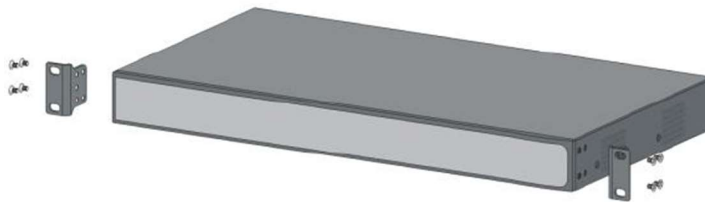
3.1.2 Instalacja w szafie RACK.

Urządzenie można zainstalować w 11-calowym stelażu RACK w standardzie EIA.

Krok 1 Sprawdź uziemienie szafy i upewnij się, że stelaż jest stabilny.

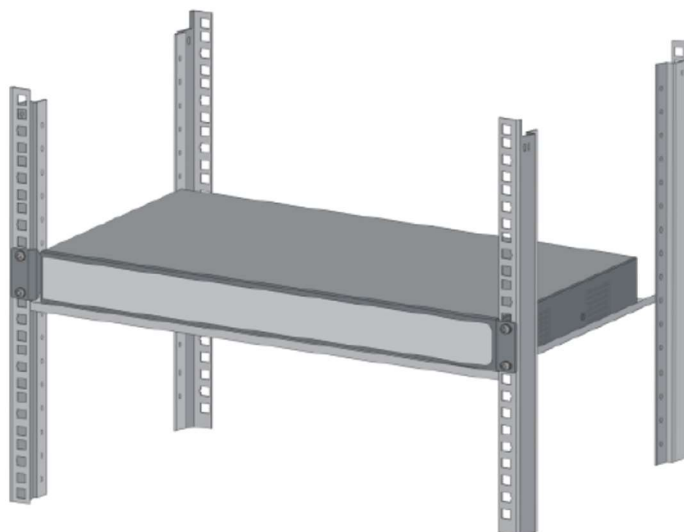
Krok 2 Przymocuj wsporniki za pomocą śrub po obu stronach panelu bocznego urządzenia.

Rys. 3-1 – montaż wsporników



Krok 3 Przykręć urządzenia do stelaża przy pomocy śrub.

Rys. 3-2 – montaż urządzenia do stelaża RACK



3.2 Uruchamianie urządzenia

Krok 1 Podłącz jeden koniec przewodu zasilającego do portu zasilania na panelu tylnym urządzenie, a następnie podłącz drugi koniec do gniazda zasilającego

Krok 2 Sprawdź, czy świeci się wskaźnik zasilania (PWR) urządzenia, jeśli tak oznacza to że zasilanie zostało podłączone prawidłowo.

3.3 Podłączanie kabla sieciowego LAN.

Podłącz jeden koniec kabla sieciowego do urządzenia obsługującego PoE, a drugi koniec do dowolnego Port RJ45 urządzenia. Maksymalna odległość między urządzeniem a IPC wynosi około 100 metrów. Po pomyślnym nawiązaniu połączenia odpowiedni port przełącznika działa normalnie.

Zalecenia dotyczące cyberbezpieczeństwa

Cyberbezpieczeństwo to coś więcej niż modny slogan. To realna kwestia dotycząca każdego urządzenia podłączonego do internetu. Systemy monitoringu wideo również są narażone na cyberataki, ale podjęcie choćby podstawowych kroków w celu zwiększenia ochrony sieci i urządzeń wyraźnie zmniejsza takie ryzyko. Poniżej przedstawiono kilka wskazówek i zaleceń firmy Dahua na temat tego, jak podnieść poziom bezpieczeństwa swojego systemu zabezpieczeń.

Obowiązkowe działania do podjęcia celem zapewnienia podstawowego bezpieczeństwa urządzeń sieciowych:

1. Wybieraj silne hasła

- Oto kilka sugestii dotyczących haseł:
- Hasło musi mieć przynajmniej 8 znaków;
- Hasło powinno składać się z co najmniej dwóch rodzajów znaków, takich jak wielkie i małe litery, cyfry i znaki specjalne;
- Hasło nie powinno zawierać nazwy konta (również w odwróconej kolejności);
- Hasło nie powinno składać się z ciągu następujących po sobie znaków, takich jak 123, abc itp.; Hasło nie powinno składać się z ciągu tych samych znaków, np. 111, aaa itp.;

2. Aktualizuj oprogramowanie sprzętowe i klienckie na czas

- Zgodnie ze standardowymi procedurami w branży technologicznej zalecamy aktualizowanie oprogramowania sprzętowego urządzeń (NVR, DVR, kamer IP itp.) celem zapewnienia, że system jest aktualny oraz zostały zainstalowane najnowsze łatki i poprawki. Jeśli sprzęt podłączony jest do sieci publicznej, zalecamy włączenie funkcji automatycznego sprawdzania aktualizacji, tak aby otrzymywać na bieżąco informacje o aktualizacjach oprogramowania sprzętowego udostępnianych przez producenta.
- Zalecamy pobranie i używanie najnowszej wersji oprogramowania klienckiego

Zalecane działania nakierowane na zwiększenie bezpieczeństwa urządzenia w sieci:

1. Zabezpieczenia fizyczne

Zalecamy stosowanie fizycznych zabezpieczeń sprzętu, w szczególności urządzeń pamięci masowej. Warto na przykład umieścić sprzęt w specjalnym pomieszczeniu komputerowym lub szafce oraz wdrożyć odpowiednio skonfigurowaną kontrolę dostępu za pomocą uprawnień i kluczy, aby zapobiegać sytuacjom, w których nieuprawnieni członkowie personelu mogą mieć kontakt ze sprzętem, uszkadzając go lub podłączając nośniki zewnętrzne (jak dyski flash USB, urządzenia podłączane przez port szeregowy itp.).

2. Regularnie zmieniaj hasła

Sugerujemy regularną zmianę haseł, aby ograniczać ryzyko, że zostaną one odgadnięte lub złamane.

3. Skonfiguruj i terminowo aktualizuj informacje dotyczące resetowania hasła

Urządzenie obsługuje funkcję resetowania hasła. Dodaj w odpowiednim terminie informacje potrzebne do resetu hasła, takie jak adres e-mail użytkownika oraz pytania do hasła. Jeśli informacje ulegną zmianie, upewnij się, że zostaną na czas zmodyfikowane w systemie. Sugerujemy, aby przy ustawianiu pytań zabezpieczających do hasła nie używać takich, na które odpowiedzi są łatwe do odgadnięcia.

4. Włącz blokadę konta

Funkcja blokowania konta jest domyślnie włączona i zalecamy, aby tak ją pozostawić celem zapewnienia bezpieczeństwa konta. W przypadku wielokrotnych nieudanych prób zalogowania dane konto oraz źródłowy adres IP zostaną zablokowane.

5. Zmień domyślne porty HTTP i inne

Sugerujemy zmianę domyślnych portów HTTP i innych portów na wybraną liczbę z przedziału od 1024 do 65535. Zmniejsza to ryzyko, że osobom z zewnątrz uda się zgadnąć, których portów używasz.

6. Włącz obsługę protokołu HTTPS

Sugerujemy włączenie obsługi protokołu HTTPS, tak aby komunikacja z witryną odbywała się za pośrednictwem bezpiecznego kanału.

7. Włącz białą listę

Sugerujemy włączenie funkcji białej listy, co uniemożliwi osobom z innymi niż wskazane adresami IP uzyskanie dostępu do systemu. Upewnij się, że adres IP Twojego komputera oraz adresy IP urządzeń dodatkowych zostały dodane do białej listy.

8. Zastosuj wiązanie adresów MAC

Zalecamy powiązanie adresów IP i MAC bramy z urządzeniem, ograniczając w ten sposób ryzyko ataków typu ARP spoofing.

9. Rozsądnie przydzielaj konta i uprawnienia

Użytkowników należy dodawać w sposób rozsądny, w oparciu o wymogi biznesowe i z zakresu zarządzania, oraz należy przyznawać im minimalne wymagane uprawnienia.

10. Wyłącz zbędne usługi i używaj trybów bezpieczeństwa

Celem ograniczenia ryzyka zaleca się wyłączenie zbędnych usług, takich jak SNMP, SMTP, UPnP itp. Jeśli są one niezbędne, zalecamy korzystanie z trybów bezpieczeństwa między innymi dla następujących usług:

- SNMP: wybierz SNMP v3 i ustaw silne hasła szyfrowania i uwierzytelniania.
- SMTP: wybierz protokół TLS jako metodę dostępu do serwera poczty.
- FTP: wybierz SFTP i ustaw silne hasła.
- Hotspot z punktem dostępu: wybierz tryb szyfrowania WPA2-PSK i ustaw silne hasła.

11. Szyfrowanie przesyłanych sygnałów audio i wideo

Jeśli przesyłane treści audio lub wideo są szczególnie ważne bądź wrażliwe, zalecamy korzystanie z funkcji szyfrowania transmisji, która ogranicza ryzyko wykradzenia danych podczas przesyłania. Przypomnienie: szyfrowanie transmisji spowoduje obniżenie jej prędkości.

12. Bezpieczeństwo audytów

- Sprawdzaj użytkowników online: sugerujemy regularne kontrole użytkowników online celem sprawdzenia, czy urządzenia bez odpowiednich uprawnień nie są zalogowane.
- Sprawdzaj dziennik systemu: sprawdzając dzienniki, możesz zidentyfikować adresy IP używane do logowania się do Twoich urządzeń oraz wykonane najważniejsze czynności.

13. Dziennik sieciowy

Ze względu na ograniczoną pamięć masową urządzenia przechowywany dziennik ma ograniczony rozmiar. Jeśli potrzebujesz utrzymywać dziennik przez dłuższy czas, zalecamy włączenie funkcji dziennika sieciowego celem zapewnienia, że dzienniki o znaczeniu krytycznym będą synchronizowane z serwerem dziennika sieciowego na potrzeby śledzenia.

14. Stwórz bezpieczne środowisko sieciowe

W celu zapewnienia wyższego poziomu bezpieczeństwa sprzętowi oraz ograniczenia potencjalnego ryzyka wystąpienia cyberataków zalecamy:

- Wyłączenie funkcji mapowania portów w routerze, aby wyeliminować możliwość bezpośredniego dostępu do urządzeń w sieci intranet z sieci zewnętrznej.
- Sieć powinna być podzielona na odizolowane od siebie podsieci w zależności od faktycznych potrzeb. Jeśli poszczególne podsieci nie muszą się ze sobą komunikować, sugerujemy użycie sieci VLAN, network GAP lub innych technologii do podziału sieci celem zapewnienia efektu izolacji.
- Stwórz system uwierzytelniania 802.1x celem ograniczenia ryzyka nieuprawnionego dostępu do sieci prywatnych.
- Zaleca się włączenie zapory sieciowej lub skonfigurowania listy dostępu blokowanych i dozwolonych urządzeń tak aby zmniejszyć ryzyko ataku na urządzenia w sieci.