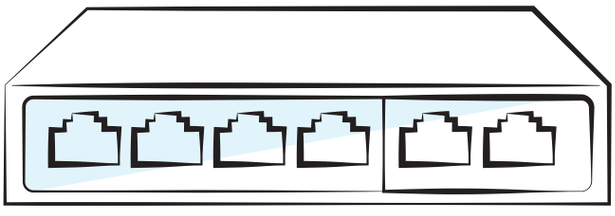
PL

Instrukcja obsługi
4-portowego przełącznika
Gigabit PoE

BCS-L-SP04G02G(II)



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

Wersja podręcznika: 2.05

TYTUŁEM WSTĘPU

INFORMACJE OGÓLNE

Niniejsza instrukcja przedstawia cechy i strukturę 4-portowego przełącznika Gigabit PoE, (zwanego dalej „Urządzeniem").

INSTRUKCJE BEZPIECZEŃSTWA

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

Hasła ostrzegawcze	Znaczenie
OSTRZEŻENIE!	Wskazuje na wysokie potencjalne zagrożenie, które, jeśli się go nie uniknie, spowoduje śmierć lub poważne obrażenia.
PRZESTROGA!	Wskazuje na średnie lub niskie potencjalne zagrożenie, które, jeśli się go nie uniknie, może spowodować lekkie lub umiarkowane obrażenia.
UWAGA!	Wskazuje na potencjalne ryzyko, które, jeśli się go nie uniknie, może spowodować uszkodzenie mienia, utratę danych, obniżenie wydajności lub nieprzewidywalne skutki.
NOTA	Zawiera dodatkowe informacje jako wyróżnienie i uzupełnienie tekstu.

HISTORIA ZMIAN

Wersja	Treść wersji	Data wydania
V.1.0.1	Zaktualizowana przedmowa	Listopad 2020

INFORMACJA O OCHRONIE PRYWATNOŚCI

Jako użytkownik urządzenia lub administrator danych możesz zbierać dane osobowe innych osób, takie jak twarz, odciski palców, numer rejestracyjny samochodu, adres e-mail, numer telefonu, GPS i tak dalej. Musisz przestrzegać lokalnych przepisów i regulacji dotyczących ochrony prywatności, aby chronić uzasadnione prawa i interesy innych osób, wdrażając środki, które obejmują między innymi: zapewnienie jasnej i widocznej identyfikacji w celu poinformowania osoby, której dane dotyczą, o istnieniu obszaru nadzorowanego i zapewnienie adekwatnego kontaktu.

O INSTRUKCJI

- Instrukcja ma jedynie charakter informacyjny. W przypadku niezgodności między instrukcją a rzeczywistym produktem, pierwszeństwo ma produkt rzeczywisty.
- Nie odpowiadamy za jakiekolwiek straty spowodowane działaniami niezgodnymi z instrukcją.
- Podręcznik będzie aktualizowany zgodnie z najnowszymi przepisami i regulacjami w powiązanych regionach. Aby uzyskać szczegółowe informacje, zapoznaj się z instrukcją papierową, płytą CD-ROM, kodem QR lub naszą oficjalną stroną internetową. W przypadku niezgodności między instrukcją papierową a wersją elektroniczną, wersja elektroniczna ma pierwszeństwo.
- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez wcześniejszego pisemnego powiadomienia. Aktualizacje produktu mogą powodować pewne różnice między rzeczywistym produktem a instrukcją. Prosimy o kontakt z obsługą klienta w celu uzyskania najnowszego programu i dodatkowej dokumentacji.
- Nadal mogą występować odchylenia w danych technicznych, opisach funkcji i operacji lub błędy w druku. W przypadku jakichkolwiek wątpliwości lub sporów zapoznaj się z naszym ostatecznym wyjaśnieniem.
- Zaktualizuj oprogramowanie czytnika lub wypróbuj inne popularne oprogramowanie czytnika, jeśli nie można otworzyć instrukcji (w formacie PDF).
- Wszystkie znaki towarowe, zarejestrowane znaki towarowe i nazwy firm w podręczniku są własnością ich odpowiednich właścicieli.
- Odwiedź naszą stronę internetową, skontaktuj się z dostawcą lub obsługą klienta, jeśli wystąpi jakikolwiek problem podczas korzystania z urządzenia.
- W przypadku jakichkolwiek wątpliwości lub kontrowersji prosimy zapoznać się z naszym ostatecznym wyjaśnieniem.

WAŻNE ZABEZPIECZENIA I OSTRZEŻENIA

Instrukcja pomoże właściwie korzystać z naszego produktu. Aby uniknąć niebezpieczeństw i szkód materialnych, przeczytaj uważnie instrukcję przed użyciem produktu i zdecydowanie zalecamy zachowanie jej na przyszłość.

WYMAGANIA OPERACYJNE

- Nie wystawiaj urządzenia bezpośrednio na działanie promieni słonecznych i trzymaj z dala od ciepła.
- Nie instaluj urządzenia w wilgotnym środowisku i unikaj kurzu i sadzy.
- Upewnij się, że urządzenie jest zamontowane poziomo i zainstaluj urządzenie na solidnej i płaskiej powierzchni, aby uniknąć upadku.
- Unikaj rozpryskiwania cieczy na urządzeniu. Nie umieszczaj na urządzeniu przedmiotów wypełnionych cieczą, aby uniknąć przedostania się cieczy do urządzenia.
- Zainstaluj urządzenie w dobrze wentylowanym pomieszczeniu. Nie blokuj otworu wentylacyjnego urządzenia.
- Używaj urządzenia przy znamionowym napięciu wejściowym i wyjściowym.
- Nie demontuj urządzenia bez fachowej instrukcji.
- Transport, użytkowanie i przechowywanie urządzenia powinno mieć miejsce tylko w dozwolonych zakresach wilgotności i temperatury.

WYMAGANIA DOTYCZĄCE ZASILANIA

- Używaj baterii we właściwy sposób, aby uniknąć pożaru, eksplozji i innych niebezpieczeństw
- Wymień baterię na baterię tego samego typu.
- Używaj lokalnie zalecanego przewodu zasilającego w granicach znamionowych specyfikacji.
- Użyj standardowego zasilacza. Nie ponosimy żadnej odpowiedzialności za jakiekolwiek problemy spowodowane przez niestandardowy zasilacz.
- Zasilacz powinien spełniać wymóg SELV. Używaj zasilacza zgodnego z Limited Power Source, zgodnie z normą IEC60950 1. Zapoznaj się z etykietą urządzenia.
- Zastosuj ochronę GND dla urządzenia typu I.
- Łącznik jest urządzeniem odłączającym. Trzymaj go pod kątem, aby ułatwić obsługę.

SPIS TREŚCI

1. OPIS PRODUKTU

1.1 WPROWADZENIE/WSTĘP DO PRODUKTU

4-portowy przełącznik gigabitowy to typ komercyjnego przełącznika warstwy 2, który obsługuje pełny dostęp gigabitowy. Zapewnia 4 porty Ethernet 10/100/1000 Mb / s oraz 2 porty uplink 10/100/1000 Mb / s.

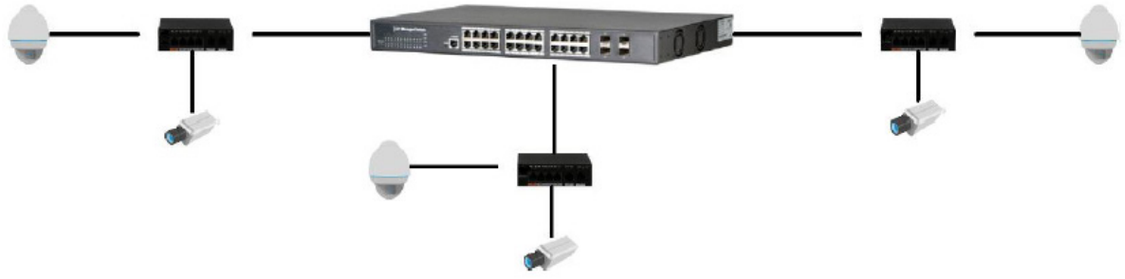
1.2 FUNKCJE

Cechy Ogólne:

- Komercyjny przełącznik warstwy 2.
- Obsługuje standardy IEEE802.3, IEEE802.3u, IEEE802.3ab i IEEE80 2.3x.
- Automatyczne badanie i starzenie się MAC, rozmiar tablicy MAC wynosi 2K.
- Samoadaptacja MDI / MDIX
- Obsługa portów RJ45 s 10/100/1000 Mb / s samodostosowujące się obsługuje standardy zasilania IEEE802.3af i IEEE802.3at.
- Zamknięty w metalowej obudowie.
- Zasilanie DC 48 V 57 V.
- Port 1 obsługuje zasilacze Hi P o E 60 W.

1.3 TYPOWE ZASTOSOWANIE

Typową scenę interakcji sieciowych przedstawiono na rysunku 1-1

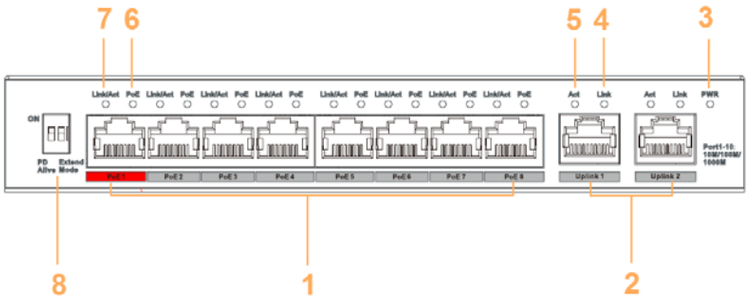


Rysunek 1-1 Zastosowanie

2. STRUKTURA URZĄDZENIA

2.1 PRZEDNI PANEL

Panel przedni pokazano na rysunku 2-1



Rysunek 2-1 Panel urządzenia

Opis panelu przedniego zawiera Tabela 2-1

Nr	Funkcja	Funkcja
1	PoE1 PoE4	10/100 Mb/s lub 10/100/1000 Mb/s 4 samodostosowujace się porty zasialnia PoE.
2	Uplink 1, Uplink 2	10/100 Mb/s lub 10/100/1000 Mb/s 2 samodostosowujace się porty uplink
3	Wskaźnik zasilania	On: Włączone Off: Wyłączone
4	Wskaźnik stanu pojedyńczego portu link	On: urzadzenie podłączone Off: urządzenie niepodłączone
5	Wskaźnik stanu transmisji danych portu uplink	Miga: transmisja danych w toku Wył: brak transmisji
6	Wskaźnik statusu portu PoE	On: Zasilanie PoE Off: Brak zasilania PoE
7	Wskaźnik transmisji danych lub podłączenia pojedyńczego portu	On: Urządzenie podłączone Off: Urządzenie niepodłączone Miga: transmisja danych w toku
8	Przełącznik DIP	PD Alive: Po wykryciu zawieszenia urządzenia, funkcja ponownie uruchamia urządzenie Extend Mode: Wydłuża zasieg transmisji do 250m obniżając prędkosc transmisji do 10 Mb/s
9	Przełącznik DIP	Wybierz Default lub Extend Mode zmieniajac ustawienie przełącznika Extend Mode: Extend Mode: Wydłuża zasieg transmisji do 250m obniżając prędkosc transmisji do 10 Mb/s
10	Wskaźnik prędkości transmisji portu	On: 100 Mb/s lub 1000 Mb/s Off: 10 Mb/s

Tabela 2-1 Panel urządzenia

2.2 PANEL TYLNY

Panel tylny pokazano na rysunku 2-2

Rysunek 2-1 Panel urządzenia

Opis panelu tylnego zawiera Tabela 2-2

Nr	Nazwa	Opis
1	GND	Uziemienie
2	Otwór zamka blokującego	Zablokuj przełącznik.
2	Port zasilania	Obsługuje DC 48 V 57 V.

Tabela 2-2 Opis panelu tylnego

2.3 ZASILANIE POE

- Jeden gigabitowy port RJ45 (obsługuje standardy IEEE802.3af, IEEE802.3at i zasilacz Hi PoE 60 W.
- Trzy gigabitowe porty RJ45 (PoE2 PoE4) obsługują standardowe zasilanie IEEE802.3af i IEEE802.3at.

3. ZAŁĄCZNIK – ZALECENIA DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo to coś więcej niż modne hasło: to coś, co dotyczy każdego urządzenia podłączonego do internetu. Nadzór wideo IP nie jest odporny na cyberzagrożenia, ale podjęcie podstawowych kroków w celu ochrony i wzmocnienia sieci i urządzeń sieciowych sprawi, że będą one mniej podatne na ataki. Poniżej znajduje się kilka wskazówek i zaleceń, jak stworzyć bardziej bezpieczny system bezpieczeństwa.

OBOWIĄZKOWE DZIAŁANIA, KTÓRE NALEŻY PODJĄĆ W CELU ZAPEWNIENIA PODSTAWOWEGO BEZPIECZEŃSTWA SIECI SPRZĘTU.

1. Używaj silnych haseł

Zapoznaj się z następującymi sugestiami dotyczącymi ustawiania haseł:

- Długość nie powinna być mniejsza niż 8 znaków;
- Uwzględnij co najmniej dwa typy znaków; typy znaków obejmują wielkie i małe litery, cyfry i symbole;
- Nie podawaj nazwy konta ani nazwy konta w odwrotnej kolejności;
- Nie używaj ciągłych znaków, takich jak 123, abc itp .;
- Nie używaj zachodzących na siebie znaków, takich jak 111, aaa itp .;

2. Aktualizuj oprogramowanie sprzętowe i oprogramowanie klienta na czas

- Zgodnie ze standardową procedurą w branży technologicznej, zalecamy aktualizowanie oprogramowania sprzętowego sprzętu (takiego jak NVR, DVR, kamera IP itp.), Aby upewnić się, że system jest wyposażony w najnowsze poprawki bezpieczeństwa i poprawki. Gdy urządzenie jest podłączone do sieci publicznej, zaleca się włączenie funkcji „automatycznego sprawdzania dostępności aktualizacji" w celu uzyskania aktualnych informacji o aktualizacjach oprogramowania sprzętowego wydanych przez producenta.
- Sugerujemy pobranie i używanie najnowszej wersji oprogramowania klienckiego.

POMOCNE ZALECENIA DOTYCZĄCE POPRAWY BEZPIECZEŃSTWA SIECI SPRZĘTU:

1. Ochrona fizyczna

Sugerujemy zapewnienie fizycznej ochrony sprzętu, zwłaszcza urządzeń pamięci masowej. Na przykład umieść sprzęt w specjalnym pomieszczeniu komputerowym i szafce i zastosuj dobrze wykonaną kontrolę dostępu i zarządzanie kluczami, aby uniemożliwić nieupoważnionemu personelowi wykonywanie fizycznych działań, takich jak uszkodzenie sprzętu, nieautoryzowane podłączenie sprzętu wymiennego (takiego jak dysk flash USB, port szeregowy) itp.

2. Regularnie zmieniaj hasła

Sugerujemy regularne zmienianie haseł, aby zmniejszyć ryzyko odgadnięcia lub złamania.

3. Ustaw i aktualizuj hasła, Resetuj informacje w odpowiednim czasie.

Urządzenie obsługuje funkcję resetowania hasła. Urządzenie obsługuje funkcję resetowania hasła. Skonfiguruj powiązane informacje dotyczące resetowania hasła na czas, w tym skrzynkę pocztową użytkownika końcowego i pytania dotyczące ochrony hasłem. Jeśli informacje ulegną zmianie, należy je w odpowiednim czasie zmodyfikować. Podczas ustawiania pytań dotyczących ochrony hasła zaleca się, aby nie używać tych, które można łatwo odgadnąć.

4. Włącz blokadę konta

Funkcja blokady konta jest domyślnie włączona i zalecamy jej pozostawienie, aby zagwarantować bezpieczeństwo konta. Jeśli osoba atakująca spróbuje zalogować się kilkakrotnie przy użyciu nieprawidłowego hasła, odpowiednie konto i źródłowy adres IP zostaną zablokowane.

5. Zmień domyślne porty HTTP i inne porty usług

Sugerujemy zmianę domyślnych portów HTTP i innych portów usług na dowolny zestaw liczb z zakresu od 1024 do 65535, zmniejszając ryzyko, że osoby postronne będą w stanie odgadnąć, których portów używasz.

6. Włącz HTTPS

Sugerujemy włączenie protokołu HTTPS, aby odwiedzać usługę sieci Web za pośrednictwem bezpiecznego kanału komunikacji.

7. Włącz białą listę

Sugerujemy włączenie funkcji białej listy, aby uniemożliwić wszystkim, z wyjątkiem osób o określonych adresach IP, dostęp do systemu.

8. Wiązanie adresu MAC

Zalecamy powiązanie adresu IP i MAC bramy z urządzeniem, zmniejszając w ten sposób ryzyko fałszowania ARP.

9. Przypisuj konta i uprawnienia w rozsądny sposób.

Zgodnie z wymaganiami biznesowymi i zarządczymi rozsądnie dodawaj użytkowników i przypisz im minimalny zestaw uprawnień.

10. Wyłącz niepotrzebne usługi i wybierz bezpieczne tryby

Jeśli nie jest to potrzebne, zaleca się wyłączenie niektórych usług, takich jak SNMP, SMTP, UPnP itp., Aby zmniejszyć ryzyko.

W razie potrzeby zdecydowanie zaleca się korzystanie z bezpiecznych trybów, w tym między innymi następujących usług:

- SNMP: Wybierz SNMP v3 i skonfiguruj silne hasła szyfrowania i hasła uwierzytelniania.
- SMTP: Wybierz TLS, aby uzyskać dostęp do serwera skrzynki pocztowej.
- FTP: wybierz SFTP i ustaw silne hasła.
- Punkt dostępu AP: Wybierz tryb szyfrowania WPA2 PSK i ustaw silne hasła.

11. Szyfrowana transmisja audio i wideo

Jeśli zawartość danych audio i wideo jest bardzo ważna lub wrażliwa, zalecamy użycie funkcji transmisji szyfrowanej, aby zmniejszyć ryzyko kradzieży danych audio i wideo podczas transmisji.

Przypomnienie: szyfrowanie transmisji spowoduje pewny spadek wydajności.

12. Bezpieczny audyt

- Sprawdzaj użytkowników online: sugerujemy regularne monitorowanie użytkowników online, aby sprawdzić, czy urządzenie jest zalogowane bez autoryzacji.
- Sprawdź dziennik sprzętu: przeglądając dzienniki, możesz poznać adresy IP, które były używane do logowania się na urządzeniach i ich kluczowe operacje.

13. Dziennik sieci

Ze względu na ograniczoną pojemność przechowywania sprzętu, przechowywany dziennik jest ograniczony. Jeśli musisz zapisywać dziennik przez długi czas, zaleca się włączenie funkcji dziennika sieciowego, aby zapewnić synchronizację dzienników krytycznych z serwerem dzienników sieci w celu śledzenia.

14. Zbuduj bezpieczne środowisko sieciowe

Aby lepiej zapewnić bezpieczeństwo sprzętu i zmniejszyć potencjalne zagrożenia cybernetyczne, zalecamy:

- Wyłącz funkcję mapowania portów routera, aby uniknąć bezpośredniego dostępu do urządzeń intranetowych z sieci zewnętrznej.
- Sieć powinna być podzielona na partycje i odizolowana zgodnie z rzeczywistymi potrzebami sieci. Jeśli nie ma wymagań dotyczących komunikacji między dwiema podsieciami, sugeruje się użycie VLAN, GAP sieci i innych technologii do podziału sieci, aby uzyskać efekt izolacji sieci.
- Skonfiguruj system uwierzytelniania 802.1x a ccess, aby zmniejszyć ryzyko nieautoryzowanego dostępu do sieci prywatnych.

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