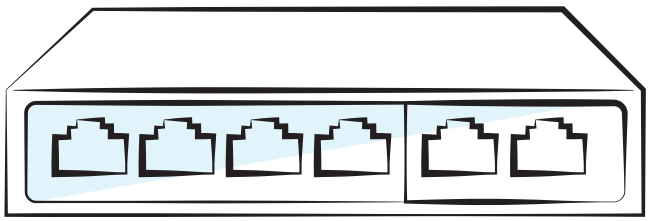
SK

Používateľská príručka
4-portový prepínač

Gigabit PoE

BCS-L-SP04G02G



www.bcs.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

Aktualizácia: 11.02.2022

ÚVOD

VŠEOBECNÉ INFORMÁCIE

Tento návod popisuje funkcie a obsluhu HDCVI kamery (ďalej len „zariadenie“)

BEZPEČNOSTNÉ INŠTRUKCIE

V návode môžu byť zahrnuté nasledujúce slová s definovaným významom.

Heslo	Význam
NEBEZPEČENSTVO!	Označuje potenciálne vysoký stupeň nebezpečenstva, ktorý môže mať za následok vážne poškodenie zdravia alebo smrť.
VÝSTRAHA!	Označuje potenciálne stredný alebo nízky stupeň rizika, ktorý by mohol viesť k strednému alebo nízkemu poškodeniu zdravia.
POZOR!	Označuje potenciálne nebezpečenstvo, ktoré by mohlo viesť k poškodeniu majetku, strate údajov, zníženiu výkonu zariadenia alebo iným neočakávaným výsledkom.
POZNÁMKA	Navrhuje spôsoby riešenia problému alebo úspory času.

HISTÓRIA REVÍZIE

Verzia	Obsah revízie	Dátum vydania
V.1.0.1	Aktualizovaný predhovor	November 2020

INFORMÁCIA O OCHRANE OSOBNÝCH ÚDAJOV

Ako používateľ zariadenia alebo správca údajov môžete zhromažďovať osobné údaje iných ľudí, ako je tvár, odtlačky prstov, registračné číslo auta, e-mailová adresa, telefónne číslo, GPS atď. Musíte dodržiavať miestne zákony a nariadenia o ochrane osobných údajov, aby ste chránili legitímne práva a záujmy iných vykonávaním opatrení, ktoré zahŕňajú, ale nie sú obmedzené na: poskytnutie jasnej a viditeľnej identifikácie na informovanie dotknutej osoby o existencii kontrolovanej oblasti a zabezpečenie primeraného kontaktu.

O TEJTO PRÍRUČKE

- Návod slúži len na informačné účely. V prípade nesúladu medzi návodom a skutočným produktom má prednosť skutočný produkt.
- Nie sme zodpovední za žiadne straty spôsobené konaním, ktoré nie je v súlade s pokynmi.
- Príručka bude aktualizovaná podľa najnovších zákonov a nariadení v príslušnej jurisdikcii. Podrobnosti nájdete v papierovej príručke, na disku CD-ROM, v kóde QR alebo na našej oficiálnej webovej stránke. V prípade rozporu medzi papierovou príručkou a elektronickou verziou má prednosť elektronická verzia.
- Všetky dizajny a softvér sa môžu zmeniť bez predchádzajúceho písomného upozornenia. Aktualizácie produktu môžu spôsobiť určité rozdiely medzi skutočným produktom a manuálom. Ak chcete získať najnovší program a dodatočnú dokumentáciu, kontaktujte zákaznícky servis.
- Stále môžu existovať odchýlky v špecifikáciách, funkčných a prevádzkových popisoch alebo chyby tlače. Ak máte nejaké pochybnosti alebo spor, pozrite si naše konečné vysvetlenie.
- Aktualizujte softvér čítačky alebo vyskúšajte iný populárny čítací softvér, ak sa príručka nedá otvoriť (vo formáte PDF).
- Všetky ochranné známky, registrované ochranné známky a názvy spoločností v tejto príručke sú majetkom príslušných vlastníkov.
- Navštívte našu webovú stránku, kontaktujte dodávateľa alebo zákaznícky servis, ak sa pri používaní zariadenia vyskytne nejaký problém.
- V prípade akýchkoľvek pochybností alebo kontroverzií si pozrite naše záverečné vysvetlenie.

DÔLEŽITÉ BEZPEČNOSTNÉ OPATRENIA A UPOZORNENIA

Pokyny vám pomôžu správne používať náš produkt. Aby ste predišli akémukoľvek nebezpečenstvu a materiálnym škodám, pred použitím produktu si pozorne prečítajte pokyny a dôrazne odporúčame, aby ste si ich uschovali pre budúce použitie.

PREVÁDZKOVÉ POŽIADAVKY

- Nevystavujte zariadenie priamemu slnečnému žiareniu a chráňte ho pred teplom.
- Zariadenie neinštalujte vo vlhkom prostredí a vyhýbajte sa prachu a sadzi.
- Uistite sa, že je jednotka namontovaná vodorovne a nainštalujte ju na pevný a rovný povrch, aby nedošlo k pádu.
- Zabráňte striekaniu tekutín na zariadenie. Na zariadenie neumiestňujte predmety naplnené kvapalinou, aby ste zabránili vniknutiu kvapaliny do zariadenia.
- Zariadenie inštalujte v dobre vetranej miestnosti. Neblokujte ventilačný otvor zariadenia.
- Zariadenie používajte s menovitým vstupným a výstupným napätím.
- Nerozoberajte zariadenie bez odborných pokynov.
- Preprava, používanie a skladovanie zariadenia by sa malo uskutočňovať iba v rámci povolených rozsahov vlhkosti a teploty.

POŽIADAVKY NA NAPÁJANIE

- Batériu používajte správne, aby ste predišli požiaru, výbuchu a iným nebezpečenstvám
- Vymeňte batériu za batériu rovnakého typu.
- Používajte miestne odporúčaný napájací kábel v rámci menovitých špecifikácií.
- Použite štandardný AC adaptér. Za problémy spôsobené neštandardným napájacím adaptérom nemôžeme prevziať žiadnu zodpovednosť.
- Napájací zdroj by mal spĺňať požiadavku SELV. Používajte napájací adaptér kompatibilný s Limited Power Source v súlade s normou IEC60950 1. Skontrolujte štítok zariadenia.
- Použite ochranu GND pre zariadenie typu I.
- Spínač je odpájacie zariadenie. Pre ľahkú manipuláciu ho držte pod uhlom.

OBSAH

1. OPIS PRODUKTU

1.1 PREDSTAVENIE PRODUKTU/ÚVOD

4-portový gigabitový prepínač je typ komerčného prepínača vrstvy 2, ktorý podporuje úplný gigabitový prístup. Poskytuje 4 ethernetové porty 10/100/1000 Mb/s a 2 uplink porty 10/100/1000 Mb/s.

1.2 FUNKCIE

Všeobecné vlastnosti:

- Komerčný prepínač 2. vrstvy.
- Podporuje IEEE802.3, IEEE802.3u, IEEE802.3ab a IEEE80 2.3×.
- Automatické štúdium a usporiadanie MAC, veľkosť tabuľky MAC je 2K.
- Samoprispôsobenie MDI / MDIX
- Podporuje 10/100/1000 Mb/s RJ45 porty, samoprispôsobenie podporuje štandardy napájania IEEE802.3af a IEEE802.3at.
- Uzavreté v kovovom obale.
- Napájanie DC 48V 57V.
- Port 1 podporuje napájacie zdroje Hi Po E 60 W.

1.3 POUŽITIE

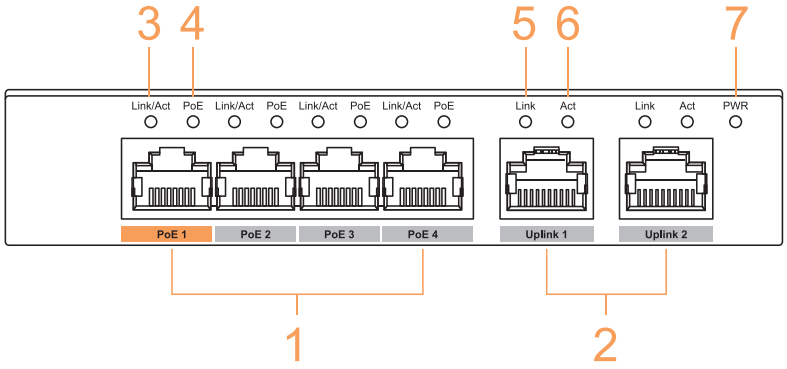
Typický príklad sieťových interakcií je znázornený na obrázku 1-1

Nákres 1-1 Použitie

2. ŠTRUKTÚRA ZARIADENIA

2.1 PREDNÝ PANEL

Predný panel je zobrazený na nákrese 2-1



Nákres 2-1 Panel zariadenia

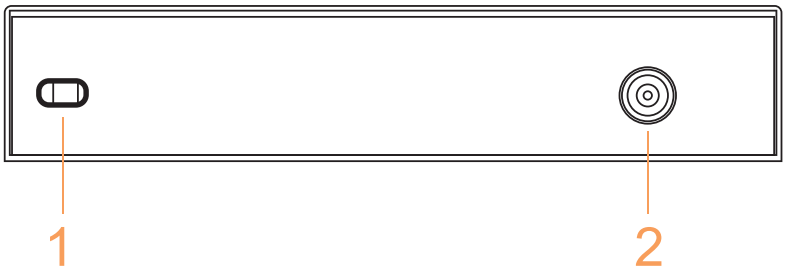
Opis predného panela ukazuje tabuľka 2-1

Nr.	Funkcia	Funkcia
1	PoE1 PoE4	10/100 Mb/s alebo 10/100/1000 Mb/s 4 samoprispôsobiteľné napájacie porty PoE
2	Uplink 1, Uplink 2	10/100 Mb/s alebo 10/100/1000 Mb/s 2 samostatne sa prispôsobujúce uplink porty
3	Ukazovateľ napájania	On: Zapnuté Off: Vypnuté
4	Indikátor stavu spojenia s jedným portom	Wskaźnik stanu pojedynczego portu PoE
5	Link	Wskaźnik stanu łącza portu uplink
6	Act	Wskaźnik stanu transmisji danych portu uplink
7	PWR	Wskaźnik mocy

Tabuľka 2-1 Panel zariadenia

2.2 ZADNÝ PANEL

Zadný panel je zobrazený na nákrese 2-2



Nákres 2-2 Panel zariadenia

Opis predného panela ukazuje tabuľka 2-2

Nr.	Názov	Opis
1	Uzamykací otvor zámku	Zamknúť spínač
2	Napájací port	Podporuje DC 48V 57V

Tabuľka 2-2 Opis zadného panelu

2.3 NAPÁJANIE POE

- Jeden gigabitový port RJ45 (podporuje štandardy IEEE802.3af, IEEE802.3at a 60W Hi PoE napájanie.
- Tri gigabitové porty RJ45 (PoE2 PoE4) podporujú štandardné napájanie IEEE802.3af a IEEE802.3at.

3. PRÍLOHA – ODPORÚČANIA PRE KYBERNETICKÚ BEZPEČNOSŤ

Kybernetická bezpečnosť je viac než len módne slovo: je to niečo, čo platí pre akékoľvek zariadenie pripojené k internetu. IP video dohľad nie je imúnny voči kybernetickým hrozbám, no ak podniknete základné kroky na ochranu a posilnenie vašich sietí a zariadení, budú menej zraniteľné voči útokom. Nižšie je niekoľko tipov a odporúčaní, ako vytvoriť bezpečnejší bezpečnostný systém.

POVINNÉ OPATRENIA, KTORÉ JE POTREBNÉ PRIJAŤ NA ZABEZPEČENIE ZÁKLADNÉHO ZABEZPEČENIA SIETE ZARIADENÍ.

1. Používajte silné heslá

Zapoznaj się z następującymi sugestiami dotyczącymi ustawiania haseł:

- Pozrite si nasledujúce návrhy na nastavenie hesiel:
- Dĺžka by nemala byť kratšia ako 8 znakov;
- Zahrňte aspoň dva typy znakov; typy znakov zahŕňajúce veľké a malé písmená, čísla a symboly;
- Nezadávajte ako heslo názov účtu alebo názov účtu naopak;
- Nepoužívajte po sebe idúce znaky ako 123, abc atď;
- Nepoužívajte rovnaké znaky ako 111, aaa atď.;

2. Aktualizujte firmvér a klientsky softvér včas

- Podľa priemyselného štandardného postupu vám odporúčame aktualizovať firmvér vášho hardvéru (ako je NVR, DVR, IP kamera atď.), aby ste sa uistili, že váš systém je vybavený najnovšími bezpečnostnými opravami. Keď je zariadenie pripojené k verejnej sieti, odporúča sa zapnúť funkciu „automatická kontrola aktualizácií“, aby ste získali najnovšie informácie o aktualizáciách firmvéru vydaných výrobcom.
- Odporúčame vám stiahnuť a používať najnovšiu verziu klientskeho softvéru.

UŽITOČNÉ ODPORÚČANIA NA ZLEPŠENIE ZABEZPEČENIA SIETE ZARIADENÍ:

1. Fyzická ochrana

Odporúčame vám fyzicky chrániť váš hardvér, najmä úložné zariadenia. Napríklad umiestnite zariadenie do špeciálnej počítačovej miestnosti a skrinky a aplikujte dobre vykonanú kontrolu prístupu a správu kľúčov, aby ste zabránili neoprávnenému personálu vykonávať fyzické činnosti, ako je poškodenie zariadenia, neoprávnené pripojenie vymeniteľného zariadenia (ako je USB flash disk , sériový port) atď.

2. Pravidelňe meňte heslá

Odporúčame vám, aby ste si heslá pravidelne menili, aby ste znížili riziko uhádnutia alebo prelomenia.

3. Nastavte a aktualizujte heslá, resetujte informácie včas.

Zariadenie podporuje funkciu obnovenia hesla. Včas nastavte súvisiace informácie o obnovení hesla, vrátane emailu koncového používateľa a otázok o ochrane hesla. Ak sa informácie zmenia, musia byť včas revidované. Pri nastavovaní otázok na ochranu hesla sa odporúča nepoužívať tie, ktoré sa dajú ľahko uhádnuť.

4. Zapnite blokovanie účtu

Funkcia uzamknutia účtu je predvolene zapnutá a odporúčame vám ju nechať zapnutú, aby ste sa uistili, že je váš účet bezpečný. Ak sa útočník pokúsi prihlásiť viackrát s nesprávnym heslom, príslušný účet a zdrojová IP adresa budú zablokované.

5. Zmeňte predvolené porty HTTP a porty inných služieb

Odporúčame zmeniť predvolené porty HTTP a porty iných služieb na ľubovoľnú sadu čísel medzi 1024 a 65535, čím sa zníži riziko, že okoloidúci budú môcť uhádnuť, ktoré porty používate.

6. Povoľte HTTPS

Odporúčame vám povoliť protokol HTTPS na návštevu webovej služby cez zabezpečený komunikačný kanál.

7. Povoľte whitelist

Odporúčame vám povoliť funkciu whitelistu, aby ste zabránili komukoľvek okrem ľudí s konkrétnymi IP adresami v prístupe k vášmu systému.

8. Naviazanie MAC adresy

Odporúčame vám prepojiť IP a MAC adresu brány so zariadením, čím sa zníži riziko spoofingu ARP.

9. Priraďte účty a povolenia rozumným spôsobom.

Podľa vašich obchodných a manažérskych požiadaviek pridávajte používateľov rozumne a priraďte im minimálny súbor povolení.

10. Vypnite nepotrebné služby a vyberte bezpečné režimy

Ak to nie je potrebné, odporúča sa vypnúť niektoré služby ako SNMP, SMTP, UPnP atď., aby sa znížilo riziko.

Dôrazne sa odporúča, aby ste v prípade potreby používali núdzové režimy vrátane, ale nie výlučne, nasledujúcich služieb:

- SNMP: Vyberte SNMP v3 a nakonfigurujte silné šifrovacie a autentifikačné heslá.
- SMTP: Zvoľte TLS pre prístup k poštovému serveru.
- FTP: Vyberte SFTP a nastavte silné heslá.
- Prístupový bod AP: Vyberte režim šifrovania WPA2 PSK a nastavte silné heslá.

11. Šifrovaný prenos audia a videa

Ak je obsah audio a video dát veľmi dôležitý alebo citlivý, odporúčame použiť funkciu šifrovaného prenosu, aby ste znížili riziko krádeže audio a video dát počas prenosu.

Poznámka: šifrovaný prenos spôsobí určité zníženie výkonu.

12. Bezpečný audit

- Kontrola online používateľov: Odporúčame vám pravidelne sledovať online používateľov, aby ste skontrolovali, či nie je zariadenie prihlásené neoprávnene.
- Skontrolujte protokol hardvéru: zobrazením protokolov môžete zistiť adresy IP, ktoré boli použité na prihlásenie do zariadení, a ich kľúčové operácie.

13. Sieťový denník

V dôsledku obmedzenej úložnej kapacity hardvéru je uchovávaný protokol obmedzený. Ak potrebujete uchovávať protokolovanie dlhší čas, odporúča sa zapnúť funkciu sieťového denníka, aby ste sa uistili, že vaše kritické denníky sú synchronizované so serverom sieťových denníkov na účely sledovania.

14. Vytvorte bezpečné sieťové prostredie

Ak chcete lepšie chrániť svoj hardvér a znížiť potenciálne kybernetické hrozby, odporúčame:

- Vypnite funkciu mapovania portov smerovača, aby ste zabránili priamemu prístupu k intranetovým zariadeniam z externej siete.
- Sieť by mala byť rozdelená a izolovaná podľa skutočných potrieb siete. Ak neexistujú žiadne komunikačné požiadavky medzi týmito dvoma podsieťami, odporúča sa použiť VLAN, sieť GAP a ďalšie technológie na rozdelenie siete, aby sa dosiahol efekt izolácie siete.
- Nakonfigurujte prístupový autentifikačný systém 802.1x a znížite riziko neoprávneného prístupu do súkromných sietí.

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

Aktualizácia: 11.02.2022