Opracowanie zawiera:

Załączniki:

ZE.1) Uprawnienia budowlane projektanta
ZE.2) Zaświadczenie o przynależności projektanta do PIIB
ZE.3) Uprawnienia budowlane sprawdzającego
ZE.4) Zaświadczenie o przynależności sprawdzającego do PIIB
ZE.5) Oświadczenie projektanta
ZE.6) Oświadczenie sprawdzającego
ZE.7) Schemat LAN archiwalny

Rysunki:

ZGL_PW_TT_PL_	01	Rzut instalacji przyzywowej – Parter
ZGL_PW_TT_PL_	02	Rzut instalacji przyzywowej – Piętro +1
ZGL_PW_TT_PL_	03	Rzut instalacji przyzywowej – Piętro +2
ZGL_PW_TT_PL_	04	Rzut instalacji przyzywowej – Piętro +3
ZGL_PW_TT_PL_	05	Rzut instalacji przyzywowej – Piętro +4
ZGL_PW_TT_PL_	06	Rzut instalacji zabezpieczeń – Piwnica
ZGL_PW_TT_PL_	07	Rzut instalacji zabezpieczeń – Parter
ZGL_PW_TT_PL_	08	Rzut instalacji zabezpieczeń – Piętro +1
ZGL_PW_TT_PL_	09	Rzut instalacji zabezpieczeń – Piętro +2
ZGL_PW_TT_PL_	10	Rzut instalacji zabezpieczeń – Piętro +3
ZGL_PW_TT_PL_	11	Rzut instalacji zabezpieczeń – Piętro +4
ZGL_PW_TT_PL_	12	Rzut instalacji zabezpieczeń – Nadbudówka
ZGL_PW_TT_PL_	13	Rzut instalacji LAN i RTV – Piwnica
ZGL_PW_TT_PL_	14	Rzut instalacji LAN i RTV – Parter
ZGL_PW_TT_PL_	15	Rzut instalacji LAN i RTV – Piętro +1
ZGL_PW_TT_PL_	16	Rzut instalacji LAN i RTV – Piętro +2
ZGL_PW_TT_PL_	17	Rzut instalacji LAN i RTV – Piętro +3
ZGL_PW_TT_PL_	18	Rzut instalacji LAN i RTV – Piętro +4
ZGL_PW_TT_PL_	19	Rzut instalacji LAN i RTV – Dach
ZGL_PW_TT_PL_	20	Rzut instalacji LAN PZT
ZGL_PW_TT_PL_	21	Rzut systemu kolejkowego – Parter
ZGL_PW_TT_PL_	22	Rzut systemu kolejkowego – Piętro +4
ZGL_PW_TT_SC_	01	Schemat instalacji przyzywowej
ZGL_PW_TT_SC_	02	Schemat systemu kontroli dostępu
ZGL_PW_TT_SC_	03	Schemat monitoringu CCTV
ZGL_PW_TT_SC_	04	Schemat instalacji videodomofonowej
ZGL_PW_TT_SC_	05	Schemat instalacji LAN
ZGL_PW_TT_SC_	06	Elewacja szafy LAN LPD.B1 - Piwnica
ZGL_PW_TT_SC_	07	Elewacja szafy LAN LPD.0 - Parter
ZGL_PW_TT_SC_	08	Elewacja szafy LAN LPD.1 - Piętro 1
ZGL_PW_TT_SC_	09	Elewacja szafy LAN LPD.1 - Piętro 2
ZGL_PW_TT_SC_	10	Elewacja szafy LAN LPD.1 - Piętro 3
ZGL_PW_TT_SC_	11	Elewacja szafy LAN LPD.1 - Piętro 4
ZGL_PW_TT_SC_	12	Schemat systemu kolejkowego na parterze

1. OPIS TECHNICZNY OGÓLNY

1.1 Przedmiot opracowania

Przedmiotem niniejszego opracowania jest projekt przebudowy i rozbudowy oraz rozmieszczenia oddziałów szpitalnych w budynku L, Szpitala Uniwersyteckiego w Zielonej Górze Sp. z o.o., ul. Zyty 26, 65-046 Zielona Góra Działka nr ew. 61/9, w zakresie instalacji teletechnicznych.

1.2 Zakres opracowania

Przewiduje się zaprojektowanie następujących elementów instalacji i systemów:

- instalację teleinformatyczną
- instalację przyzywową,
- kontrolę dostępu,
- monitoring CCTV,
- telewizję RTV,
- system kolejkowy.

1.3 Podstawa opracowania

Projekt niniejszy opracowano na podstawie:

a) aktualnych podkładów architektonicznych,
b) założeń technologicznych,
c) zaleceń, uzgodnień i wytycznych Inwestora,
d) wytycznych z branży sanitarnej,
e) uzgodnień międzybranżowych,
f) obowiązujących przepisów i Polskich Norm

1.4 Przepisy i normy powołane

- *Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie, Dz.U. Nr 75 poz. 690 z późniejszymi zmianami*
- *Ustawa z dnia 7 lipca 1994 r. Prawo budowlane, Dz.U. 1994 Nr 89 poz.414*
- *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U. 1994 Nr24 poz. 83*
- *Ustawa z dnia 21 grudnia 2000 r. o dozorze technicznym, Dz.U. 2000 Nr 122 poz. 1321*
- *Ustawa z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz. U. nr 92, poz. 881*
- *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów Dz. U. z 2010 Nr 109 poz. 719*
- *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010r. zmieniające rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania, Dz. U. nr 85 z 2010 r. poz. 553 z dnia 27 kwietnia 2010 r.*
- *Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej. (tekst jednolity Dz.U.2018 poz. 620)*

Przewiduje się, że wszystkie urządzenia i materiały nie odpowiadające wymogom zawartym w w/w rozporządzeniach, przepisach i normach nie zostaną przyjęte do użycia w obiekcie. W przypadku

nieuprawnionego zainstalowania, ich demontażem, usunięciem i zastąpieniem zostanie obarczony Wykonawca.

W przypadku, gdy w trakcie trwania budowy wejdą w życie nowe przepisy i rozporządzenia, Wykonawca zobowiązany będzie do pisemnego powiadomienia o w/w fakcie Inwestora, Generalnego projektanta, Architekta, oraz Kierownika robót jak i do stosowania się do nich.

Materiały nie znormalizowane oraz te, które nie odpowiadają wyżej wyszczególnionym wymogom będą stanowić przedmiot opinii technicznej wydanej przez stosowne władze.

1.5 Priorytety ważności przepisów, norm i uzgodnień

Przyjęto następujący priorytet ważności przepisów, norm i uzgodnień:

- rozporządzenia właściwych Ministrów,
- normy powołane przez stosowne przepisy do obowiązkowego stosowania,
- rozporządzenia władz lokalnych,
- przepisy organów kontrolnych,
- postanowienia i decyzje wydane w stosunku do danego obiektu,
- normy i przepisy powołane przez projektanta do zastosowania,
- zasady wiedzy technicznej,
- uzgodnienia z rzeczoznawcą d/s p.poż.,
- uzgodnienia z rzeczoznawcą d/s bhp,
- uzgodnienia z Inwestorem,
- wytyczne Inwestora,
- wytyczne technologiczne,
- wytyczne branżowe,
- opisy wszystkich branż.

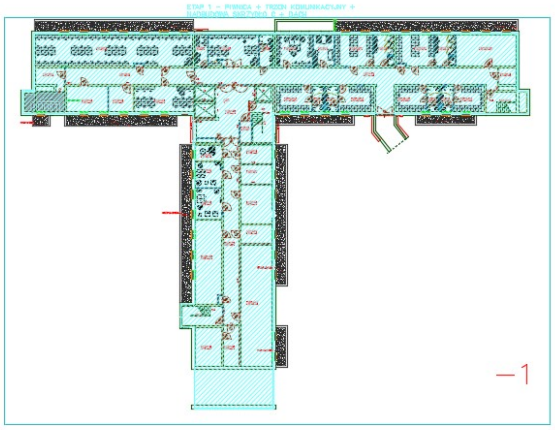
Wszędzie stosowane jest kryterium wg którego wymagania stawiane dla każdej z instalacji są na poziomie takim na jakim są wymagania wyższe z grupy wymagań inwestora, oraz przepisów i norm.

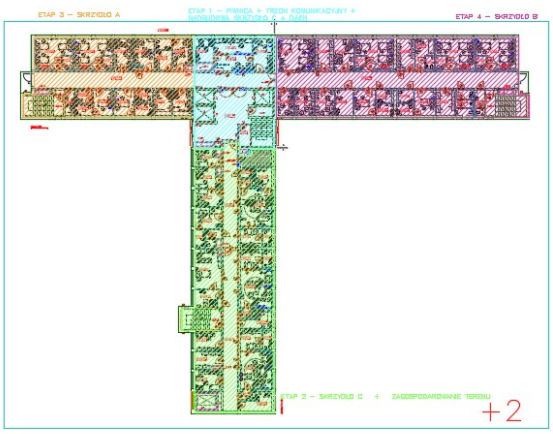
2. MATERIAŁY REFERENCYJNE

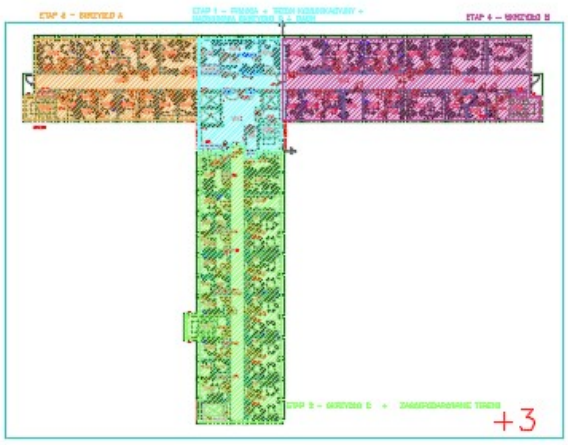
Projekt opracowany został na materiałach referencyjnych, jednak dopuszcza się stosowanie materiałów innych dostawców o parametrach nie gorszych od zaproponowanych. Inwestor zastrzega, że instalacje teletechniczne należy powiązać z systemami istniejącymi wbudowanymi na zmodernizowanym parterze.

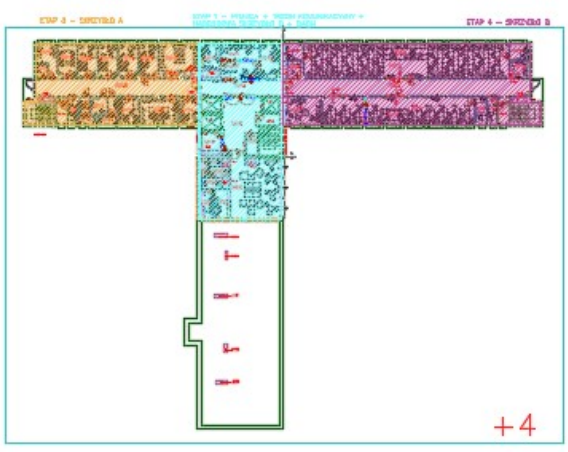
3. ETAPOWANIE INWESTYCJI

Zakłada się wykonanie etapowania Inwestycji, z podziałem na cztery etapy:
ETAP – 1 – PIWNICA + TRZON KOMUNIKACYJNY + NADBUDOWA SKRZYDŁA C
ETAP – 2 – SKRZYDŁO C + ZAGOSPODAROWANIE TERENU
ETAP – 3 – SKRZYDŁO A
ETAP – 4 – SKRZYDŁO B
Zgodnie z diagramem poniżej.









Na każdym etapie generalny wykonawca, musi przekazać system sprawny, funkcjonujacy, umożliwajacy jego poprawną prace. Każdy kolejny etap należy wykonać jako rozbudowa systemu istniejącego.

- monitoring CCTV – etap pierwszy obejmować musi połączenie systemu między piętrami, oraz kamery zgodnie z etapowaniem pokazanym na schemacie systemu oraz zakresami zaznaczonymi powyżej.
- kontrola dostępu – etap pierwszy obejmować musi połączenie systemu między piętrami, oraz drzwi zgodnie z etapowaniem pokazanym na schemacie systemu oraz zakresami zaznaczonymi powyżej
- system wideodomofonowy – cały system do wykonania w pierwszym etapie
- system kolejkowy – system na parterze, wykonać w drugim etapie, system na czwartej kondygnacji wykonać w pierwszym etapie
- system przyzywowy – etap pierwszy obejmować musi połączenie systemu między piętrami, wykonanie centralki głównej, oraz bramek na piętrach, podział na etapy pokazany na schemacie systemu oraz zaznaczony powyżej.
- instalacja RTV – w zakresie pierwszego podłączenia systemu do istniejącej anteny, wyprowadzenie sygnału do budynku U oraz pozostałych budynku, wykonanie szkieletu instalacji między piętrami wraz ze skrzynką rozgałęźną sygnału. Uwaga: skrzynka rozgałęźna dostosowana do podłączenia wszystkich gniazd, również tych z kolejnych etapów. Etapowanie rozprowadzenia instalacji zgodnie z etapowaniem remontu w budynku.
- instalacja LAN – w zakresie prac pierwszego etapu: połączenie z systemem CCTV, wykonanie podłączenia z budynkiem Centrum Matki Zdrowia i Dziecka, wykonanie dodatkowych światłowodów pomiędzy szafami. W zakresie pierwszego etapy dostawa i podłączenie kompletnej szafy na parterze, dostawa kompletnej szafy na kondygnacji +4, wraz z przełożeniem do niej przełączników zgodnie z ZGL_PW_TT_SC_11 (z istniejących szaf na kondygnacjach parteru, oraz pięter). W zakresie prac pierwszego etapu wymiana przełączników dedykowanych dla Wifi na D-Link 3630PC POE zgodnie z rysunkami elewacji, na wszystkich kondygnacjach oraz przełącznik DXS-3600-32S/SI w LPD.0. W każdym z etapów generalny wykonawca wyposaży szafy w niezbędną ilość organizerów, patch paneli i przełączników tak aby szafy były kompletne w swym wyposażeniu. Etapowanie rozprowadzenia instalacji zgodnie z etapowaniem remontu w budynku.

4. DEMONTAŻE

W zakresie wykonawcy prac wykonanie instalacji teletechnicznych istniejących. Instalacje demontować w taki sposób, aby nie przerwać ciągłości instalacji obsługujących przestrzenie przewidziane do wykonania w kolejnych etapach.

5. INSTALACJA TELEFONICZNA I KOMPUTEROWA

Instalację komputerową logiczną wykonać w oparciu o istniejącą infrastrukturę z uwzględnieniem rozbudowy w oparciu o urządzenia kompatybilne z istniejącymi rozwiązaniami.
Uwaga: wszystkie punkty WiFi zamontować odtworzeniowo, GW zdemontuje urządzenia, zabezpieczy na czas budowy a następnie ponownie zamontuje. Przed demontażem, należy zweryfikować, działanie anteny, sporządzić protokół z ilości sprawnych urządzeń, w przypadku uszkodzenia urządzenia, wymiana na koszt GW.
Wszystkie gniazda zakończyć na patch panelach kat. 6A w szafach LPD, w ramach realizacji Inwestycji należy wykorzystać istniejące okablowanie strukturalne wykonane w latach 2016-2017. Ilość skrętek wyprowadzonych na poszczególnych piętrach zgodnie z załącznikiem nr 7 do dokumentacji. Stan instalacji należy określić jako „dobry – działający poprawnie”, GW na własne ryzyko powinien oszacować ilość okablowania do wykorzystania, w celu obniżenia kosztów realizacji.
Centralę telefoniczną rozbudować o dwa dodatkowe moduły w celu powiększenia bazy wolnych numerów na projektowane stanowiska.

1.6 Lokalizacja lokalnych punktów dystrybucyjnych

Przewiduje się zlokalizowanie szaf w pomieszczeniach technicznych, w holu pomiędzy klatką schodową a windami. Na każdej kondygnacji przewiduje się jedną szafę LPD.
W celu wykonania instalacji IT zakłada się:

- wykorzystanie 4 szaf istniejących oraz dwóch nowych projektowanych
- częściowe wykorzystanie urządzeń zlokalizowanych w szafach, (reszta urządzeń w dostawie GW)
- przełożenie części urządzeń tak, aby uniknąć sytuacji montażu urządzeń aktywnych niekompatybilnych z już istniejącymi.

1.7 Wymagania ogólne dotyczące systemu okablowania strukturalnego

System okablowania strukturalnego ma zapewnić warstwę fizyczną dla przesyłu wszystkich aplikacji zaprojektowanych dla okablowania kat. 6a F/FTP według najnowszych standardów PN-EN 50173, ISO/IEC 11801, ANSI/TIA/EIA 568-B.2. Dla zapewnienia elastyczności, system musi umożliwiać swobodną rozbudowę, oraz rekonfigurację.

Wszystkie komponenty systemu muszą spełniać wymagania co najmniej kategorii 6a w celu uzyskania odpowiednio dużych marginesów bezpieczeństwa parametrów transmisyjnych.
Okablowanie strukturalne instalowane w obiekcie musi posiadać certyfikaty, wydane przez niezależne laboratorium badawcze Delta, potwierdzające zgodność z wymienionymi normami okablowania strukturalnego, w zakresie pojedynczych komponentów, łącza Permanent Link oraz testu „de-embedded”. Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001 i posiadać certyfikat, w zakresie produkcji, projektowania i serwisowania swojego systemu.
Instalacja okablowania strukturalnego musi zostać wykonywana przez instalatora posiadającego ważne uprawnienia i certyfikat wydany przez producenta okablowania.

Na zainstalowany, przez certyfikowanego instalatora, system okablowania strukturalnego zostanie wydany certyfikat 20-letniej gwarancji niezawodności. W przypadku udzielenia gwarancji przez wykonawcę instalacji, producent okablowania jest zobligowany do wydania certyfikatu zapewniającego reasekurację gwarancji udzielonej przez wykonawcę. Reasekuracja obejmuje okres, na jaki wykonawca udzielił gwarancji.

1.8 Wymagania ogólne dotyczące szaf RACK IT

Instalację należy sprowadzić do szaf na poszczególnych piętrach.

Do LPD.0 należy dołożyć Switch typu III w celu zapewnienia redundancji do poszczególnych pięter.
Szafy należy rozbudować o dodatkowe elementy aktywne i pasywne zgodnie z widokami elewacji szaf.

Szafy wyposażyć, w urządzenia, osprzęt i okablowanie niezbędne do poprawnego funkcjonowania:

- odpowiednią ilość patchpaneli RJ45,
- odpowiednią ilość paneli porządkujących,
- listwę zasilającą RACK,
- sprzęt aktywny zapewniający działanie projektowanych PEL,
- odpowiednią ilość switchy TYP I,
- odpowiednią ilość switchy TYP II,
- odpowiednią ilość kabli stack
- moduły SFP+ tego samego producenta co przełączniki – po 2szt. na każdą szafę
- patchcordy światłowodowe 1m MM LC-LC

Szafy wyposażyć w odpowiednią ilość patchcordów zapewniających skrosowanie wszystkich gniazd RJ45 pomiędzy patchpanelami a switchami w każdej szafie, oraz odpowiednią ilość patchord do połączenia wszystkich RJ-45 we wszystkich projektowanych PEL pomiędzy PEL a urządzeniami końcowymi (PEL 3xRJ45=3 patchcordy do szafy+3 patchcordy do PEL)

Wszystkie szafy muszą stanowić kompletny system, wyposażone we wszystkie urządzenia niezbędne do ich funkcjonowania (w tym w urządzenia aktywne)

1.9 Połączenia pomiędzy szafami

Pomiędzy szafą LPD na parterze a szafami LPD.1, LPD.2, LPD.3 – wykonane są połączenia światłowodowe: 6xOM3, 2xFTP
Połączenia te należy pozostawić bez zmian.
Analogiczne połączenia należy wykonać dla szaf zlokalizowanej w piwnicy LPD.B1 oraz na czwartek kondygnacji LPD.4.

Należy wykonać połączenie światłowodowe jednomodowe 48J pomiędzy szafą LPD.0 a serwerownią w budynku Centrum Zdrowia Matki i Dziecka.
Dodatkowo w szafie LPD.0 należy zamontować dodatkowy switch TYPU III i wykonać dodatkowe połączenia światłowodem 6xOM3 do każdej z szaf LPD.B1, LPD.1, LPD.2, LPD.3, LPD.4. Dla switcha typ III należy również dostarczyć 4 moduły jednomodowe SFP+, 2 moduły stackujące wraz z kablem stackującym. Całość od jednego producenta.

1.10 Wytyczne ilości gniazd RJ45

Ilości punktów LAN zgodnie z rzutem instalacji teletechnicznych.
W pomieszczeniach biurowych, zabiegowych, badań, dyżurkach i innych powinny zostać zainstalowane punkty PEL składające się z trzech gniazd logicznych i trzech gniazd elektrycznych (3xRJ45+3x230V) + dodatkowe gniazdo telefoniczne.
Gniazda RJ45 w kolumnach, dedykowane dla urządzeń technicznych, technologii ilość wg wytycznych technologicznych dla poszczególnych pomieszczeń, wskazane zostały na rzutach.
Dodatkowo zakłada się wykonanie gniazd teletechnicznych dla:
- anten WiFi;
- gazów medycznych
- instalacji przyzywowej
- systemu kolejkowego
- części urządzeń sanitarnych.

Wszystkie te urządzenia zostaną wpięte w sieć LAN.
Monitoring CCTV – będzie posiadał dedykowane switche CCTV, okablowanie dla tych urządzeń wykonane będzie wg projektu monitoringu CCTV.

Do sieci LAN wpięte będą:

- UPS
- Centralna bateria
- Analizatory parametrów sieci
- W celu odczytu parametrów technicznych

Linie zakończyć na patchapnelach kat 6a w szafie RACK, danej kondygnacji.

Dla połączeń wychodzących na zewnątrz budynku stosować kable żelowane.

1.11 Zasilanie urządzeń IT

Wszystkie szafy LAN zasilane będą z sieci zasilania gwarantowanego, rezerwowanej zasilaczem bezprzerwowym UPS i agregatem.
Access Pointy WiFi – zasilanie PoE

1.12 Wytyczne dla urządzeń aktywnych

Zgodnie z wymaganiami Inwestora, dla urządzeń aktywnych należy zapewnić funkcjonalność jak poniżej w celu zapewnienia kompatybilności z urządzeniami już istniejącymi w szafach LPD zlokalizowanych w obiekcie.

Switch TYP I:
Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 24.
Porty na moduły światłowodowe SFP (IEEE 802.3z) z możliwością instalacji modułów 1000Base-SX/LX/LH/ZX - liczba portów co najmniej 4. Dopuszcza się, aby porty SFP były dzielone z portami 1000Base-T.
Porty SFP powinny umożliwiać obsługę również modułów SFP 100Base-FX (IEEE 802.3u).

Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).
Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu.
Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+.
Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego oraz dedykowany port Ethernet do zarządzania Out-of-Band, a także w port umożliwiający podłączenie zewnętrznych czujników zdarzeń, których wyzwolenie spowoduje wysłanie powiadomienia SNMP i port umożliwiający podłączenie zewnętrznego elementu wykonawczego wyzwalanego po wystąpieniu alarmu.
Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 9 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 80 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie.
Urządzenie powinno być zasilane napięciem AC 230V. Musi istnieć możliwość użycia dodatkowego zasilacza nadmiarowego.
Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s.
Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji).
Pojemność tablicy MAC powinna wynosić nie mniej, niż 69600 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 1020 wpisów statycznych.
Dostępna pamięć RAM powinna wynosić nie mniej, niż 1024 MB. Pamięć Flash - nie mniej niż 1024 MB.
Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 12280 B.
Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 4 MB.
Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza.
Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza.
Przełącznik powinien posiadać ochronę przeciwprzepięciową na portach miedzianych co najmniej do 6 kV.
Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 300000 godzin.

Funkcjonalności warstwy 2
Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 8190 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych.
Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 4090 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych.
Powinna istnieć możliwość uwierzytelnienia klienta przed dostarczeniem mu strumienia Multicast.

Urządzenie powinno umożliwiać konfigurację filtrów dla protokołu IGMP ograniczających adresy IPv4 grup multicast do których poszczególni klienci mogą się przyłączać.
Urządzenie powinno umożliwiać również konfigurację filtrów dla protokołu MLD ograniczających adresy grup IPv6 multicast do których poszczególni klienci mogą się przyłączać.
Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 64 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN.
Dodatkowo, urządzenie powinno umożliwiać skonfigurowanie portu zapasowego, który zostanie aktywowany w przypadku awarii połączenia poprzez port podstawowy.
Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej.
Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP.
Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 2. Sprzęt powinien obsługiwać co najmniej 26 jednocześnie skonfigurowanych pierścieni.
Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6.
Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP) oraz kopiowania ruchu na port monitorujący znajdujący się w innym przełączniku.
Urządzenie powinno umożliwiać dostarczanie ruchu na wiele portów fizycznych na których obecne są te same adresy IP i MAC co pozwala na bezpośrednie przyłączenie klastrów serwerów posługujących się pojedynczym wirtualnym adresem IP i MAC.
Urządzenie powinno umożliwiać tunelowanie ruchu kontrolnego L2, w tym protokołów GVRP i STP oraz protokołów CDP i VTP (01-00-0C-CC-CC-CC i 01-00-0C-CC-CC-CD).

Obsługa sieci VLAN
Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu i pozwalać na tworzenie tzw. podwójnych VLANów.
Parametry podwójnego tagowania powinny być konfigurowalne przez administratora.
Powinna być też możliwość tworzenia specjalnych sieci VLAN dla przenoszenia ruchu typu multicast i rozdzielenia tak przenoszonego ruchu na klientów żądających przyłączenia do danej grupy multicast. Urządzenie powinno umożliwić utworzenie co najmniej 5 takich sieci VLAN.
Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.
Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 3070 wpisów MAC dla takiej sieci VLAN.

Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane.
Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów.
Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.

Funkcjonalności warstwy 3
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów.
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 256 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 256 takich interfejsów.
Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika (urządzenie powinno umożliwić konfigurację co najmniej 8 instancji takiego interfejsu).
Musi istnieć możliwość skonfigurowania interfejsu, który będzie odrzucać cały kierowany do niego ruch (interfejs Null).
Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN.
Przełącznik musi posiadać funkcjonalność Gratuitous ARP.
Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci.
Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych).
Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 96 pule adresów IP oraz wspierającego protokół IPv6. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP.
Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6.
Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 32K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych.
Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 32760 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 16384 takich tras dla IPv6.
Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 16380 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 7168 takich tras dla IPv6.
Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 510 takich tras) oraz dla IPv6 (co najmniej 250 tras).
Urządzenie musi umożliwiać tunelowanie ruchu IPv6 w IPv4 (ISATAP, 6to4).
Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP).
Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu.
Urządzenie powinno wspierać także funkcję uRPF (Unicast Reverse Path Forwarding) kontrolującą, czy nadchodzący pakiet IP posiada adres źródłowy IP znajduje się w tablicy routingu.

Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng.
Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6.

Quality of Service
Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.
Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu.
W przypadku wykrycia ruchu iSCSI, urządzenie powinno również być w stanie obsługiwać ten ruch ze skonfigurowanym dla niego priorytetem, WRR, WDRR.
Urządzenie powinno obsługiwać tzw. CIR z minimalną granulacją nie mniejszą, niż 64 kb/s.
Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb.
Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s.
Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 8 kb/s.

Filtrowanie ruchu
Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika.
Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.

Funkcje bezpieczeństwa
Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12288 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie.
Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony.

Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika.
Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.
Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników.
Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.
Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.
Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.
Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP.
Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.
Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).
Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS.
Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.
Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.
Przełącznik powinien umożliwiać filtrowanie pakietów kontrolnych L3 (np. IGMP-Query, PIM, DVMRP) i nie dopuszczanie ich do wnętrza sieci.
Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 2 pps), Multicast (z krokiem minimalnym co najwyżej 2 pps), Broadcast (z krokiem minimalnym co najwyżej 2 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.
Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.

Zarządzanie
Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.
Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.
Zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną.

Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia.
Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6.
W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3.
Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6.
Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow.
Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731 - w tym pomiar opóźnienia (Delay Measurement) i strat (Loss Measurement) na badanej ścieżce.
Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta.
Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych.
Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu.
Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.
Przełącznik powinien posiadać wbudowanego klienta SMTP.
Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN.
Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6 oraz musi wspierać protokół synchronizacji czasu zgodny z IEEE1588.
Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.
Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6.
Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6.
Interfejs WWW przełącznika powinien umożliwiać graficzne monitorowanie ruchu na portach fizycznych urządzenia, a także umożliwiać przeglądanie tablicy adresów MAC.
Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.
Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.
Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.
Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.
Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji.

Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.
Powinna istnieć możliwość automatycznego ponownego uruchomienia urządzenia o określonym czasie lub w określonym horyzoncie czasowym.
Przełącznik powinien wspierać zarządzanie przez zewnętrzny kontroler zgodnie ze standardem OpenFlow 1.3.
Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).
Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.

Pozostałe
Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.

Switch TYP II

Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) z zasilaniem PoE zgodnym z IEEE 802.3at - liczba portów co najmniej 24.
Porty na moduły światłowodowe SFP (IEEE 802.3z) z możliwością instalacji modułów 1000Base-SX/LX/LH/ZX - liczba portów co najmniej 4. Dopuszcza się, aby porty SFP były dzielone z portami 1000Base-T.
Porty SFP powinny umożliwiać obsługę również modułów SFP 100Base-FX (IEEE 802.3u).
Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).
Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu.
Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+.
Musi istnieć możliwość uruchamiania zasilania PoE na portach sterowana kalendarzem.
Urządzenie musi umożliwiać aktywne monitorowanie podłączonego urządzenia klienckiego PoE i w przypadku wykrycia jego braku wyłączać, a następnie ponownie włączać zasilanie na porcie.
Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego oraz dedykowany port Ethernet do zarządzania Out-of-Band, a także w port umożliwiający podłączenie zewnętrznych czujników zdarzeń, których wyzwolenie spowoduje wysłanie powiadomienia SNMP i port umożliwiający podłączenie zewnętrznego elementu wykonawczego wyzwalanego po wystąpieniu alarmu.
Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 9 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 80 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie.

Urządzenie powinno być zasilane napięciem AC 230V. Musi istnieć możliwość użycia dodatkowego zasilacza nadmiarowego.
Przełącznik musi zapewniać budżet mocy dla urządzeń PoE na poziomie co najmniej 370 watów. Konstrukcja układu zasilania musi umożliwiać jednoczesne korzystanie z zasilacza podstawowego oraz nadmiarowego w celu zwiększenia maksymalnej mocy, która może być dostarczana do urządzenia do co najmniej 740 watów.
Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s.
Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji).
Pojemność tablicy MAC powinna wynosić nie mniej, niż 69600 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 1020 wpisów statycznych.
Dostępna pamięć RAM powinna wynosić nie mniej, niż 1024 MB. Pamięć Flash - nie mniej niż 1024 MB.
Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 12280 B.
Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 4 MB.
Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -3 stopni Celsjusza.
Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 48 stopni Celsjusza.
Przełącznik powinien posiadać ochronę przeciwprzepięciową na portach miedzianych co najmniej do 6 kV.
Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 250000 godzin.

Funkcjonalności warstwy 2
Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 8190 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych.
Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 4090 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych.
Powinna istnieć możliwość uwierzytelnienia klienta przed dostarczeniem mu strumienia Multicast.
Urządzenie powinno umożliwiać konfigurację filtrów dla protokołu IGMP ograniczających adresy IPv4 grup multicast do których poszczególni klienci mogą się przyłączać.
Urządzenie powinno umożliwiać również konfigurację filtrów dla protokołu MLD ograniczających adresy grup IPv6 multicast do których poszczególni klienci mogą się przyłączać.
Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 64 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN.
Dodatkowo, urządzenie powinno umożliwiać skonfigurowanie portu zapasowego, który zostanie aktywowany w przypadku awarii połączenia poprzez port podstawowy.
Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej.
Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP.
Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.

Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 2. Sprzęt powinien obsługiwać co najmniej 26 jednocześnie skonfigurowanych pierścieni.
Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6.
Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP) oraz kopiowania ruchu na port monitorujący znajdujący się w innym przełączniku.
Urządzenie powinno umożliwiać dostarczanie ruchu na wiele portów fizycznych na których obecne są te same adresy IP i MAC co pozwala na bezpośrednie przyłączenie klastrów serwerów posługujących się pojedynczym wirtualnym adresem IP i MAC.
Urządzenie powinno umożliwiać tunelowanie ruchu kontrolnego L2, w tym protokołów GVRP i STP oraz protokołów CDP i VTP (01-00-0C-CC-CC-CC i 01-00-0C-CC-CC-CD).

Obsługa sieci VLAN
Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu i pozwalać na tworzenie tzw. podwójnych VLANów.
Parametry podwójnego tagowania powinny być konfigurowalne przez administratora.
Powinna być też możliwość tworzenia specjalnych sieci VLAN dla przenoszenia ruchu typu multicast i rozdzielenia tak przenoszonego ruchu na klientów żądających przyłączenia do danej grupy multicast. Urządzenie powinno umożliwić utworzenie co najmniej 5 takich sieci VLAN.
Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.
Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 3070 wpisów MAC dla takiej sieci VLAN.
Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane.
Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów.
Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.

Funkcjonalności warstwy 3
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów.
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 256 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 256 takich interfejsów.

Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika (urządzenie powinno umożliwić konfigurację co najmniej 8 instancji takiego interfejsu).
Musi istnieć możliwość skonfigurowania interfejsu, który będzie odrzucać cały kierowany do niego ruch (interfejs Null).
Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN.
Przełącznik musi posiadać funkcjonalność Gratuitous ARP.
Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci.
Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych).
Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 96 pule adresów IP oraz wspierającego protokół IPv6. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP.
Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6.
Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 32K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych.
Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 32760 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 16384 takich tras dla IPv6.
Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 16380 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 7168 takich tras dla IPv6.
Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 510 takich tras) oraz dla IPv6 (co najmniej 250 tras).
Urządzenie musi umożliwiać tunelowanie ruchu IPv6 w IPv4 (ISATAP, 6to4).
Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP).
Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu.
Urządzenie powinno wspierać także funkcję uRPF (Unicast Reverse Path Forwarding) kontrolującą, czy nadchodzący pakiet IP posiada adres źródłowy IP znajduje się w tablicy routingu.
Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng.
Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6.

Quality of Service
Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.
Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu.

W przypadku wykrycia ruchu iSCSI, urządzenie powinno również być w stanie obsługiwać ten ruch ze skonfigurowanym dla niego priorytetem, WRR, WDRR.
Urządzenie powinno obsługiwać tzw. CIR z minimalną granulacją nie mniejszą, niż 64 kb/s.
Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb.
Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s.
Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 8 kb/s.

Filtrowanie ruchu
Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika.
Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.

Funkcje bezpieczeństwa
Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12288 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie.
Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony.
Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika.
Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.
Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników.
Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.
Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.
Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.

Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP.
Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.
Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).
Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS.
Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.
Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.
Przełącznik powinien umożliwiać filtrowanie pakietów kontrolnych L3 (np. IGMP-Query, PIM, DVMRP) i nie dopuszczanie ich do wnętrza sieci.
Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 2 pps), Multicast (z krokiem minimalnym co najwyżej 2 pps), Broadcast (z krokiem minimalnym co najwyżej 2 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.
Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.

Zarządzanie
Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.
Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.
Zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną.
Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia.
Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6.
W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3.
Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6.
Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow.
Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731 - w tym pomiar opóźnienia (Delay Measurement) i strat (Loss Measurement) na badanej ścieżce.

Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta.
Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych.
Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu.
Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.
Przełącznik powinien posiadać wbudowanego klienta SMTP.
Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN.
Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6 oraz musi wspierać protokół synchronizacji czasu zgodny z IEEE1588.
Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.
Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6.
Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6.
Interfejs WWW przełącznika powinien umożliwiać graficzne monitorowanie ruchu na portach fizycznych urządzenia, a także umożliwiać przeglądanie tablicy adresów MAC.
Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.
Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.
Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.
Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.
Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji.
Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.
Powinna istnieć możliwość automatycznego ponownego uruchomienia urządzenia o określonym czasie lub w określonym horyzoncie czasowym.
Przełącznik powinien wspierać zarządzanie przez zewnętrzny kontroler zgodnie ze standardem OpenFlow 1.3.
Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).
Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.

Pozostałe
Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.

Switch TYP III

Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).
Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu.
Sprzęt powinien umożliwiać zainstalowanie co najmniej 24 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+.
Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego oraz dedykowany port Ethernet do zarządzania Out-of-Band.
Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 4 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 480 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie.
Urządzenie powinno być zasilane napięciem AC 230V. Musi istnieć możliwość użycia dodatkowego zasilacza nadmiarowego.
Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 960 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 714 Mp/s.
Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji).
Pojemność tablicy MAC powinna wynosić nie mniej, niż 131000 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 1020 wpisów statycznych.
Dostępna pamięć RAM powinna wynosić nie mniej, niż 2048 MB. Pamięć Flash - nie mniej niż 1024 MB.
Urządzenie powinno być wyposażone w dodatkowy slot dla karty SD. Powinna istnieć możliwość obsadzenia karty o pojemności co najmniej 32 GB.
Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 13310 B.
Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 9 MB.
Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż 0 stopni Celsjusza.
Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 45 stopni Celsjusza.
Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 130000 godzin.

Funkcjonalności warstwy 2
Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 4090 grup multicast w tym możliwość utworzenia co najmniej 1024 grup statycznych.

Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 4090 grup multicast w tym możliwość utworzenia co najmniej 1024 grup statycznych.
Urządzenie powinno umożliwiać konfigurację filtrów dla protokołu IGMP ograniczających adresy IPv4 grup multicast do których poszczególni klienci mogą się przyłączać.
Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s w tym co najmniej 64 instancji MSTP. Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN.
Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej.
Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 12 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP.
Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED.
Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 2. Sprzęt powinien obsługiwać co najmniej 14 jednocześnie skonfigurowanych pierścieni.
Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6.
Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko kierowanego do określonego adresu IP) oraz kopiowania ruchu na port monitorujący znajdujący się w innym przełączniku.
Urządzenie powinno umożliwiać dostarczanie ruchu na wiele portów fizycznych na których obecne są te same adresy IP i MAC co pozwala na bezpośrednie przyłączenie klastrów serwerów posługujących się pojedynczym wirtualnym adresem IP i MAC.
Urządzenie powinno umożliwiać tunelowanie ruchu kontrolnego L2, w tym protokołów GVRP i STP oraz protokołów CDP i VTP (01-00-0C-CC-CC-CC i 01-00-0C-CC-CC-CD).

Obsługa sieci VLAN
Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu i pozwalać na tworzenie tzw. podwójnych VLANów.
Parametry podwójnego tagowania powinny być konfigurowalne przez administratora.
Powinna być też możliwość tworzenia specjalnych sieci VLAN dla przenoszenia ruchu typu multicast i rozdzielenia tak przenoszonego ruchu na klientów żądających przyłączenia do danej grupy multicast. Urządzenie powinno umożliwić utworzenie co najmniej 5 takich sieci VLAN.
Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 8190 wpisów MAC dla takiej sieci VLAN.
Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane.
Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów.

Przełącznik powinien umożliwiać realizację funkcji Super VLAN.
Powinna istnieć możliwość liczenia w pakietach przepływającego przez VLAN ruchu.

Funkcjonalności warstwy 3
Urządzenie powinno posiadać funkcjonalność IGMP w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 4090 grup multicast.
Przełącznik powinien umożliwiać tworzenie statycznych wpisów dla protokołu IGMP - co najmniej 1024 takich wpisów.
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów.
Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 254 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 254 takich interfejsów.
Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika (urządzenie powinno umożliwić konfigurację co najmniej 8 instancji takiego interfejsu).
Musi istnieć możliwość skonfigurowania interfejsu, który będzie odrzucać cały kierowany do niego ruch (interfejs Null).
Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN.
Przełącznik musi posiadać funkcjonalność Gratuitous ARP.
Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych).
Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 32 pule adresów IP oraz wspierającego protokół IPv6.
Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 8K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych.
Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 1020 takich tras) oraz dla IPv6 (co najmniej 510 tras).
Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4 oraz dla IPv6.
Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. Tablica sprzętowa multicast powinna umożliwiać przechowywanie co najmniej 2040 wpisów.

Quality of Service
Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.
Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR.
Urządzenie powinno obsługiwać tzw. CIR z minimalną granulacją nie mniejszą, niż 64 kb/s.
Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED.
Przełącznik powinien posiadać obsługę powiadamiania o kongestii zgodnie z IEEE 802.1Qau, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb i posiadać wsparcie dla alokowania przepustowości pomiędzy klasami ruchu zgodnie ze standardem 802.1Qaz.

Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s oraz umożliwiać gwarantowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s.
Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 8 kb/s.

Filtrowanie ruchu
Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika, a także umożliwiać tworzenie statystyk dla ACL i mieć możliwość uruchamiania reguł ACL wg kalendarza.
Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.

Funkcje bezpieczeństwa
Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12K takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie.
Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony.
Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika.
Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.
Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników.
Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.
Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.
Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.
Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP.
Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, z dodatkową możliwością przypisania pary IP-MAC do

pojedynczego portu lub grupy portów przełącznika, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.
Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).
Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.
Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.
Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.
Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 2 pps), Multicast (z krokiem minimalnym co najwyżej 2 pps), Broadcast (z krokiem minimalnym co najwyżej 2 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.
Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.

Zarządzanie
Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.
Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.
Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia.
Zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną.
Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia.
Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6.
W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3.
Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6.
Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow.
Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731.
Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta.
Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych.
Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu.
Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.

Przełącznik powinien posiadać wbudowanego klienta SMTP.
Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN.
Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6.
Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.
Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.
Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6.
Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6.
Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.
Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.
Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.
Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji.
Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.
Powinna istnieć możliwość automatycznego ponownego uruchomienia urządzenia o określonym czasie lub w określonym horyzoncie czasowym.
Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).
Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.

Dodatkowo:
urządzenie musi być wyposażone w odpowiedni moduł oraz kabel umożliwiający połączenie w stos niezawodnościowy z posiadanym przez Zamawiającego urządzeniem DXS-3600

Pozostałe
Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.
Sprzęt powinien być objęty dożywotnią gwarancją oraz dodatkowo przez minimum 5 lat po zakończeniu jego produkcji.

1.13 Kable krosowe RJ45

Zadaniem kabli krosowych RJ45 jest połączenie łączy okablowania poziomego zakończonych na panelu rozdzielczym z portami RJ45 urządzeń aktywnych lub z portami centrali telefonicznej. W projekcie należy zastosować kable krosowe ze świetlną identyfikacją połączeń, które zapewnią:

- Transmisję danych dla urządzeń Ethernet działających z przepływnością 10Gb/s. Należy zastosować kabel o wydajności kategorii 6a ekranowane.
- Idealne dopasowanie do łączy okablowania poziomego, dlatego należy użyć kabli krosowych tego samego systemu okablowania strukturalnego, co pozostałe elementy łączy okablowania. W celu wyeliminowanie braku ciągłości w łączach wynikających z niepełnej kompatybilności mechanicznej i elektrycznej nie dopuszcza się użyci kabli krosowych innego producenta.
- Szybką i łatwą lokalizację połączeń w punkcie dystrybucyjnym dzięki świetlnej identyfikacji połączeń. Po podświetleniu jednego końca kabla krosowego zapali się drugi koniec kabla, wskazując połączone porty RJ45 w switchu i na panelu rozdzielczym, przy czym proces ten nie wymaga wypięcia wtyków kabla z portów RJ45. Identyfikacja musi odbywać się za pośrednictwem plastikowych włókien światłowodowych znajdujących się wewnątrz kabla. Nie należy stosować rozwiązań, w których identyfikacja odbywa się za pośrednictwem impulsów elektrycznych przesyłanych wewnątrz kabla i układów elektronicznych (typu diody LED), ponieważ generują one zakłócenia, które powodują błędy w transmisji danych użytkowych, a poza tym w czasie eksploatacji ujawnia się w nich brak ciągłości połączeń w układach podświetlania LED i wadliwe działanie.
- Kolorystyczne oznaczanie wtyków, w zależności od przeznaczenia kabla. Kolorowe identyfikatory należy nakładać na wtyki RJ45
- Zabezpieczenie wtyku RJ45 przed przypadkowym wypięciem. Kolorowe klipsy nakładane na wtyki RJ45 musza mieć taki kształt, aby chroniły nosek wtyku RJ45 przed przyciśnięciem i wypięciem. Rozłączenie połączenia musi być możliwe dopiero w momencie wypięcia klipsa ochronnego.
- Elastyczną i wygodna w układaniu konstrukcję wykonana z 4-parowego kabla skrętkowego typu linka.

1.14 Trasy kablowe

Kable należy prowadzić w dedykowanych do tego celu trasach kablowych:

- Okablowanie w pionie między kondygnacjami należy układać w szachtach kablowych i mocować je do drabin kablowych.
- Okablowanie układane w poziomie należy instalować w korytach kablowych lub kanałach kablowych. W głównych trasach kablowych należy stosować podwieszane koryta kablowe metalowe wykonane z blachy perforowanej, które instaluje się w przestrzeni sufitowej.
- Kable skrętkowe i światłowodowe okablowania poziomego instalowane pod tynkiem należy układać w rurach osłonowych z tworzywa sztucznego. Nie należy prowadzić kabli telekomunikacyjnych i zasilających w tej samej rurze osłonowej.
- Połączenia wykonywane na zewnątrz budynków należy realizować przy wykorzystaniu dedykowanej kanalizacji teletechnicznej.

1.15 Pomiary instalacji okablowania strukturalnego

Po wykonaniu instalacji okablowania strukturalnego wykonawca musi przeprowadzić odpowiednie pomiary sprawdzające (certyfikacyjne), wszystkich łączy miedzianych skrętkowych i światłowodowych, potwierdzające, iż wykonane okablowanie strukturalne spełnia wymagania norm. Pomiary należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO

11801 lub EN 50173. Wyniki wszystkich pomiarów muszą być pozytywne. Pomiary należy wykonać przyrządem w pełni sprawnym, posiadającym ważny certyfikat potwierdzający przejście procesu kalibracji u producenta, co będzie potwierdzeniem poprawności jego wskazań. Do dokumentacji powykonawczej należy dołączyć wymieniony certyfikat kalibracji oraz raport z wynikami pomiarów wszystkich łączy okablowania skrętkowego i światłowodowego.

1.16 Dokumentacja powykonawcza

Po wykonaniu instalacji wykonawca jest zobowiązany do sporządzenia dokumentacji powykonawczej, która będzie zawierała:

- Opis instalacji, przedstawiający architekturę systemu oraz charakterystykę rozwiązań technicznych zastosowanych w systemie okablowania.
- Listę produktów, z ilościami, wykorzystanych do budowy sieci okablowania strukturalnego.
- Schemat oznaczeń łączy miedzianych i światłowodowych.
- Podkłady budowlana z zaznaczeniem: łączy, punktów przyłączeniowych użytkowników oraz punktów dystrybucyjnych.
- Schemat blokowy instalacji.
- Rysunki przedstawiające wyposażenie punktów dystrybucyjnych.
- Pozytywne wyniki pomiarów wszystkich łączy wg normy EN 50173 lub ISO/IEC 11801.
- Certyfikat potwierdzający ważność kalibracji przyrządu, którym wykonano pomiary

6. INSTALACJA PRZYZYWOWA

W obiekcie zainstalowany zostanie system przyzywowy, objęte nim będą pomieszczeniach chorych i sale obserwacyjne, oraz łazienki, pomieszczenia zgodnie z informacją zawartą w części rysunkowej.

System będzie umożliwiał zdalne informowanie obsługi i szybką możliwość reakcji.

Przewiduje się wykonanie niezależnych sygnałów na każdym oddziale.

5.1 Zakres projektu

System ma być w pełni zgodny z wymaganiami opisanymi w normie DIN VDE 0834. Systemem przywoławczym zostaną objęte pokoje chorych, toalety (połączone z pokojami chorych oraz korytarzowe). Punty pielęgniarskie zostaną wyposażone w stacje pielęgniarskie.

System przywoławczy ma zostać zrealizowany w oparciu o sieć LON oraz działać na zasadzie ‘rozporoszonej inteligencji’, gdzie wszystkie urządzenia elektroniczne tworzą samodzielne ‘węzły’ z własnymi procesorami i oprogramowaniem. Nie może wystąpić ‘jeden punkt awarii’, który mógłby mieć wpływ na cały system, dzięki czemu zapewniona zostanie niezawodność systemu i pewność, że pojedyncze punkty awarii zostaną łatwo zlokalizowane, a awarie usunięte.

Przywołania powinny być sygnalizowane za pomocą lampek nad drzwiami od pomieszczenia, z którego nastąpiło wezwanie. W przypadku zaznaczenia obecności na terminalu komunikacyjnym lub panelu z przyciskiem przywołania, kasowania/obecności z brzęczykiem, urządzenia powinny mieć możliwość emitowania sygnału akustycznego informującego o wezwaniu asekuracji z pomieszczenia w którym są zainstalowane oraz w przypadku wezwań z pochodzących z innych pomieszczeń. Dodatkowo informacja o wezwaniu oraz jego lokalizacja z dokładnością co do łóżka pacjenta (w przypadku pokoju), co do pomieszczenia (w przypadku łazienki) musi być wyświetlana na stacjach pielęgniarskich w punktach pielęgniarskich. Stacje pielęgniarskie, na których zaznaczona jest obecność powinny również emitować sygnał akustyczny informujący o wezwaniu.

5.2 Funkcjonalność

Magistrala systemu powinna zostać wykonana w oparciu o przewód JY(St)Y 4x2x0,8 o średnicy żyły 0,8mm. Elementy peryferyjne powinny zostać połączone za pomocą przewodu JY(St)Y 4x2x0,6. Zasilacz systemu z UPS powinien zostać zabudowany w dedykowanej obudowie i podłączony przewodem NYM-O 2x1,5 mm² bezpośrednio do sieci poprzez zabezpieczone bezpiecznikiem odgałęzienie. Podłączenie za pomocą wtyczki do gniazdka nie jest dozwolone. Zasilacz ma dostarczać do systemu bezpieczne napięcie typu SELV DC. Podtrzymanie UPS ma zapewnić ciągłe działanie systemu w przypadku awarii zasilania sieciowego. System przywoławczy będzie posiadał pełne monitorowanie, a awarie sprzętowe będą zapisywane przez oprogramowanie rejestrujące oraz sygnalizowane na odpowiednio zaprogramowanych urządzeniach z wyświetlaczami. Monitorowanie awarii ma objąć całą instalację, wszystkie podłączone urządzenia i punkty przywołania. Bramki tcp/ip oraz serwer powinien być podłączone do przełącznika za pomocą kabla lan.

Kabel magistrali głównej musi być prowadzony w przestrzeni sufitu podwieszanego w korytach kablowych. Kable systemu przywoławczego nie mogą być układane we wspólnych kanałach, rurkach lub wiązkach kablowych z przewodami instalacji zasilającej. Jeżeli przewody zasilające i systemu przywoławczego układane są obok siebie na odległości mniejszej niż 1 m należy zachować minimum 10 cm odległości między przewodami obu instalacji. Jeżeli odległość przewyższa 1 m należy zachować odstęp minimum 30 cm między przewodami obu instalacji. Przewody magistrali głównej mogą wykorzystywać te same trasy kablowe, co kable sieci strukturalnej. Kable wychodzące od poszczególnych węzłów do elementów peryferyjnych należy prowadzić w elastycznych rurach osłonowych, podtynkowo.

Przy łóżkach pacjentów (w wyznaczonych miejscach w panelach medycznych) mają zostać zainstalowane panele z przyciskami przywołania oraz gniazdem pod manipulator. Panel musi posiadać diodę potwierdzającą

wciśnięcie przycisku. Dioda przycisku przywołania powinna być cały czas lekko podświetlona w celu ułatwienia lokalizacji przycisku. Lokalizacja panelu powinna umożliwić swobodny dostęp do przycisku przywołania przez pacjenta. Dodatkowo każde łóżko powinno zostać wyposażone w manipulator o kablu długości minimum 3 metry. Zarówno wtyczka kabla jak i gniazdo w panelu muszą zostać wykonane w sposób umożliwiający wielokrotne wypinanie i wpinanie manipulatora pod różnym kątem. Manipulator musi być wyposażony w czerwony przycisk przywołania, wyraźnie odróżniający się od pozostałych przycisków. Przycisk musi posiadać wbudowaną diodę LED ułatwiającą lokalizacje manipulatora. Dodatkowo manipulator musi być wyposażony w żółty przycisk umożliwiający sterowaniem oświetleniem przy łóżku pacjenta. W celu poprawy bezpieczeństwa poza wezwaniem za pomocą przycisku, również wypięcie manipulatora z gniazda powinno generować alarm. Na ścianie przy każdym z łóżek musi znajdować się uchwyt służący do odkładania manipulatora.

Na ścianie pokoju przy wejściu oraz przy wejściu do łazienki znajdującej się na korytarzu musi zostać zainstalowany panel z przyciskami przywołania, kasowania/obecności z brzęczykiem służący do kasowania wezwań z tych pomieszczeń oraz zaznaczania obecności w pomieszczeniu przez pielęgniarkę, umożliwiający wezwanie dodatkowego personelu w razie potrzeby. Oba przyciski muszą posiadać diody potwierdzające wciśnięcie przycisku. Dodatkowo dioda przycisku przywołania powinna być cały czas lekko podświetlona w celu ułatwienia lokalizacji przycisku. W określonych pomieszczeniach zainstalowane zostaną terminale komunikacyjne spełniające podobne funkcje jak w przypadku panelu z przyciskiem przywołania, kasowania/obecności z brzęczykiem.

Na ścianie łazienki połączonej z pokojem, przy wejściu musi zostać zainstalowany panel z przyciskami przywołania, kasowania służący do kasowania wezwań z tego pomieszczenia oraz umożliwiający wezwanie lekarza w razie potrzeby. Oba przyciski muszą posiadać diody potwierdzające wciśnięcie przycisku. Dodatkowo dioda przycisku przywołania powinna być cały czas lekko podświetlona w celu ułatwienia lokalizacji przycisku.

Panele z linką pociągową powinny być instalowane na ścianach toalety, tak aby zwisająca linka pociągowa była dostępna z poziomu toalety oraz podłogi. Linka musi być koloru czerwonego i posiadać dwa trójkątne uchwyty na różnych wysokościach. Linka musi być wykonana w taki sposób, aby zerwać się pod obciążeniem większym niż 3,5 kg. Linka oraz uchwyty pociągowe muszą być wykonane z materiału zawierającego dodatki zwalczające drobnoustroje. Ma to zapobiec uduszeniu w przypadku zaplątania w linkę. Panel musi posiadać diodę potwierdzająca pociągnięcie linki. Panele pociągowe obok kabin natryskowych muszą zostać zainstalowane co najmniej 20 cm powyżej najwyższej możliwej lokalizacji głowicy natryskowej i posiadać stopień ochrony IP66.

Wszystkie panele mają być typu modułowego, aby ułatwić zmianę wykorzystania w razie potrzeby. Przyciski przywołania mają być odpowiednio oznaczone symbolami i/lub tekstem w sposób umożliwiający pacjentom i personelowi szybkie ustalenie ich funkcji i używanie ich po podstawowym szkoleniu. Oznakowanie ma znajdować się na przyciskach, a nie na panelach w celu zapewnienia zamienności i elastyczności. Przyciski mają być kolorowe w celu ułatwienia identyfikacji ich funkcji. Przyciski przywołania pielęgniarki przez pacjenta mają być czerwone. W przypadku przycisków wezwania umieszczonych na panelach medycznych: białe z czerwonym symbolem z możliwością zamiany na czerwone. Przyciski przywołania personelu przez personel (awaryjne) – również czerwone. W przypadku przycisków umieszczonych na panelach medycznych białe z czerwonym symbolem z możliwością wymiany na czerwone. Przyciski kasowania oraz obecności mają być koloru zielonego.

Stacje pielęgniarskie powinny zostać zainstalowane w punktach pielęgniarskich. Ich zadaniem jest wyświetlanie informacji o wezwaniach, wiadomościach, przechowanych wezwaniach i obecnościach. Kolor wyświetlacza musi zmieniać się w zależności od kategorii danego wezwania. Cała stacja pielęgniarska musi być wykonany z materiału antybakteryjnego. Klawiatura musi być wykonana w formie membrany, w celu ułatwienia czyszczenia. Stacja pielęgniarska musi być wyposażona w port mini USB służący do wgrywania oprogramowania bezpośrednio do urządzenia. Na wyświetlaczu powinny również wyświetlać się informację o usterkach systemu i ich lokalizacjach. Wyświetlacz musi posiadać możliwość konfiguracji przycisków na wyświetlaczu dotykowym.

Obudowy paneli przywołania, obecności/kasowania z brzęczykiem; przywołania, kasowania; pociągowych; przyłóżkowych; manipulatorów; terminali komunikacyjnych; stacji pielęgniarskich oraz lampek LED muszą być wykonane z materiału zawierającego dodatki zwalczające drobnoustroje.

Wszystkie zdarzenia w systemie muszą być rejestrowane przy pomocy oprogramowania rejestrującego i zapisywane w postaci bazy danych na przewidzianym do tego celu serwerze znajdującym się w pomieszczeniu teletechnicznym. Oprogramowanie musi zapisywać dokładny czas oraz lokalizację zdarzeń w systemie. Oprogramowanie musi umożliwiać eksport danych do arkusza kalkulacyjnego.

Wezwania pacjent-personel

Wezwanie pielęgniarki może zostać zainicjowane z poziomu łóżka, pomieszczenia lub łazienki za pomocą czerwonego przycisku na panelu, czerwonego przycisku na manipulatorze lub czerwonego przycisku pociągowego. Powinno to spowodować następującą sekwencję zdarzeń:

Zapala się LED-owa lampka potwierdzająca

Zapala się czerwony segment lampy znajdującej się na korytarzu nad drzwiami do pokoju(w przypadku wezwania pochodzącego z pokoju).

Zapala się biały segment lampy znajdującej się na korytarzu nad drzwiami do pokoju (w przypadku wezwania pochodzącego z łazienki połączonej z pokojem).

Zapala się biały i czerwony segment lampy znajdującej się na korytarzu nad drzwiami do łazienki (w przypadku wezwania pochodzącego z łazienki na korytarzu).

Rozlega się sygnał akustyczny (1 sekunda sygnału akustycznego na 14 sekund przerwy, zgodnie z zaleceniami VDE 0834) na stacjach pielęgniarskich i w pomieszczeniach gdzie zaznaczona jest obecność pielęgniarki z wyjątkiem pomieszczenia z którego pochodzi wezwanie.

Stacje pielęgniarskie z zaznaczoną obecnością wyświetlają wiadomość tekstową podającą dokładną lokalizację przywołania.

Personel udający się do aktywnego wezwania ma wcisnąć zielony przycisk „obecności” znajdujący się przy wejściu do pomieszczenia, z którego pochodzi wezwanie. Powinno to spowodować następującą sekwencję zdarzeń:

Zapala się zielony segment lampy znajdującej się na korytarzu nad drzwiami do pomieszczenia sygnalizując obecność pielęgniarki.

Zapalenie LED-owej lampki potwierdzającej związanej z aktywnym przyciskiem obecności pielęgniarki.

Wciśnięcie zielonego przycisku „obecności” w pokoju oraz toalecie znajdującej się na korytarzu powoduje że kasowane są wezwania w tych pomieszczeniach:

Gaśnie czerwony segment lampy znajdującej się na korytarzu nad drzwiami do pokoju (w przypadku wezwania pochodzącego z pokoju).

Gaśnie biały i czerwony segment lampy znajdującej się na korytarzu nad drzwiami do łazienki (w przypadku wezwania pochodzącego z łazienki na korytarzu).

Tekst wezwania znika z wyświetlaczy stacji pielęgniarskich.

Sygnały akustyczne przestają być nadawane na stacjach pielęgniarskich.

Wezwania z łazienki połączonej z pokojem kasowane są za pomocą zielonego przycisku kasującego zainstalowanego wewnątrz łazienki.

Jeśli wizyta personelu wystarcza do zaspokojenia wymagań pacjenta, wychodząc z pokoju pielęgniarka powinna wcisnąć zielony przycisk „obecności”. Powinno to spowodować następującą sekwencję zdarzeń:

Gaśnie zielony segment lampy znajdującej się korytarzu nad drzwiami do pomieszczenia.

Gaśnie lampka potwierdzająca związana z aktywnym przyciskiem obecności pielęgniarki.

Znika wiadomość tekstowa wskazująca na obecność w pomieszczeniu wyświetlana na wyświetlaczach stacji pielęgniarskich.

Wezwania personel-personel (Asekuracja)

Po wciśnięciu przez pielęgniarkę zielonego przycisku „obecności”, kolejne wciśnięcie czerwonego przycisku wezwania powinno spowodować:

Pulsujący sygnał akustyczny (1 sekundę włączony, 1 sekundę wyłączony), na stacjach pielęgniarskich i w pomieszczeniach gdzie zaznaczona jest obecność pielęgniarki.

Miganie czerwonego segmentu lampy na korytarzu nad drzwiami do pomieszczenia (1 sekundę włączony, 1 sekundę wyłączony)

Zapala się biały segment lampy znajdującej się na korytarzu nad drzwiami do pomieszczenia (w przypadku wezwania pochodzącego z łazienki)

Zapalenie LED-owej lampki potwierdzającej związanej z urządzeniem przywołującym

Zielony segment lampy znajdujący się na korytarzu nad drzwiami do pomieszczenia nadal się świeci.

Stacje pielęgniarskie z zaznaczoną obecnością wyświetlają wiadomość tekstową podającą dokładną lokalizację przywołania

Wezwanie pomocy przez pielęgniarkę ma priorytet nad standardowym przywołaniem pacjent-personel, które są aktualnie aktywne i są wyświetlane na stacjach pielęgniarskich w pierwszej kolejności. Jeśli interwencja jest wystarczająca do udzielenia wsparcia, personel ma nacisnąć zielony przycisk kasujący znajdujący się przy drzwiach do pokoju lub toalety. Powinno to spowodować:

Gaśnie czerwony segment lampy znajdującej się na korytarzu nad drzwiami do pokoju (w przypadku wezwania z pokoju)

Gaśnie biały segment lampy znajdującej się na korytarzu nad drzwiami do pokoju (w przypadku wezwania pochodzącego z łazienki).

Gaśnie biały i czerwony segment lampy znajdującej się na korytarzu nad drzwiami do łazienki (w przypadku wezwania pochodzącego z łazienki na korytarzu)

Tekst wezwania znika z wyświetlaczy stacji pielęgniarskich.

Sygnały akustyczne przestają być nadawane na stacjach pielęgniarskich.

Następnie wychodząc z pokoju personel powinien wcisnąć zielony przycisk „obecności”. Powinno to spowodować następującą sekwencję zdarzeń:

Gaśnie zielony segment lampy znajdującej się na korytarzu nad drzwiami do pomieszczenia.

Gaśnie lampka potwierdzająca związana z aktywnym przyciskiem obecności personelu.

Znika wiadomość tekstowa wskazująca na obecność w pomieszczeniu wyświetlana na wyświetlaczach stacji pielęgniarskich.

6. SYSTEM KONTROLI DOSTĘPU

6.1 Ogólny opis systemu kontroli dostępu

System kontroli dostępu za pomocą czytników kart oraz zamków szyfrowych. Projektowany system umożliwia swobodne poruszanie się uprawnionych pracowników po strefach objętych systemem kontrolą oraz stanowi zabezpieczenie elektroniczne obiektu i znajdującego się w mienia i dóbr niematerialnych dając jednocześnie dostęp osobom uprawnionym.

Wszystkie przejścia kontrolowane jednostronnie za pomocą czytników kart, z jednej strony drzwi znajduje się czytnik kart a z drugiej przycisk otwierania drzwi. Ponadto wszystkie drzwi kontrolowane posiadają awaryjne przyciski otwierania drzwi na wypadek pożaru. Kontrola dostępu na wypadek pożaru zwalniana jest również za pomocą modułów systemu SSP.

Jednostronnie kontrolowane przejście zbudowane jest z następujących elementów:

- elektrorygiel
- jeden czytnik online
- kontaktron
- samozamykacz drzwiowy
- przycisk otwierania drzwi
- awaryjny przycisk otwierania drzwi

Kontrolą dostępu planuje się objąć następujące pomieszczenia:

- rejestrację,
- pokoje lekarskie i personelu
- gabinety zabiegowe
- wszystkie gabinety badań lekarskich na poziomie poradni i oddziału
- szatnie personelu
- wszystkie pomieszczenia techniczne.

6.2 Elementy instalacji

Instalacja kontroli dostępu składa się z czytników kart zbliżeniowych, do których są podłączone zwory, przycisk wyjścia i czujnik magnetyczny kontrolujący drzwi.

6.3 Montaż czytników kart

Projekt przewiduje użycie czytników kart z metalową obudową. Czytniki kart należy montować na wysokości 120 cm od podłogi i unikać montażu na powierzchniach metalowych.

7. INSTALACJA MONITORINGU CCTV

Obiekt zostanie objęty monitoringiem. W budynku przewiduje się wykonanie:

- monitoringu bezpieczeństwa obiektu
- monitoringu parametrów życiowych pacjentów

Monitoring oparty o systemy cyfrowe w technologii IP. Podgląd obrazu z kamer będzie możliwy na dowolnym komputerze podłączonym do sieci komputerowej. Sygnał z kamer doprowadzony będzie do rejestratorów, zlokalizowanych w pomieszczeniach LPD na piętrach. Dobór odpowiedniej ilości rejestratorów, do podłączenia wszystkich kamer, na etapie projektu wykonawczego.

Lokalizacja kamer bezpieczeństwa obiektu:

- ciągi komunikacyjne
- schody
- wejścia/wyjścia z budynku
- windy

Lokalizacja kamer parametrów życiowych – zgodnie z rzutem

Zapis monitoringu przechowywany przez minimum 30 dni.

ZASILANIE SYSTEMU

Urządzenia rejestrujące umieszczone w szafie strukturalnej należy zasilić napięciem 230V. Zasilanie kamer zostanie zrealizowane jako PoE wykorzystując do tego celu odpowiednie switche.

Okablowanie w kategorii 6A F/FTP.

8. INSTALACJA WIDEODOMOFONOWA

Instalację wideodomofonową zaprojektowano z wykorzystaniem systemu IP realizującego cyfrową transmisję danych w całej instalacji bez potrzeby wykorzystywania modulacji sygnału przez co jest ona odporna na występujące zakłócenia.

Połączenia urządzeń instalacji w obrębie budynku należy wykonać przewodem typu FTP kat. 6 4x2x0,5mm ułożonym, w zależności od warunków, odpowiednio w korytkach instalacyjnych i/lub w rurkach ochronnych pod tynkiem.

Monitory IP zasilane są za pomocą PoE w standardzie 802.3af. Zasilanie realizowane za pomocą PoE pozwala na zasilanie urządzenia i przesył danych za pomocą jednego przewodu.

Dla systemu instalacji wideodomofonowej przewiduje się dedykowany switch w szafie Rack wiszącej przeznaczonej dla instalacji zabezpieczeń, zlokalizowanej na każdym piętrze w pomieszczeniu teletechnicznym.

Panele wejściowe zlokalizowane przed wejściem na oddział na każdym piętrze w taki sposób aby uniknąć wejście na oddział osobą nieupoważnionym. Panele odbiorcze zlokalizowane w punktach pielęgniarskich.

9. INSTALACJA RTV

Dla projektowanego obiektu wykonana zostanie Instalacje RTV płatnej w salach chorych i bezpłatnej dla lekarzy. Telewizory są uruchamiane poprzez urządzenia dostępowe – umożlwiające dostęp do usług płatnej TV Szpitalnej.

9.1 Sposób wykonania instalacji

Instalacje montować:

- W korytarzu w zabudowanych sufitach
- Kable dystrybucyjne w szachtach kablowych
- Montaż urządzeń wykonać zgodnie z dołączonymi do sprzętu DTR.

9.2 Zasilanie

Zasilanie zgodnie z projektem instalacji elektrycznych.

10. SYSTEM KOLEJKOWY

10.1 Funkcjonalność systemu

- system musi umożliwiać samodzielne zmienianie przez Inwestora m.in. liczby i nazw kategorii oraz grup usług,
- system musi umożliwiać samodzielne przydzielanie przez Inwestora poszczególnych stanowisk do dowolnie wybranych kategorii usług,
- każde stanowisko musi mieć możliwość obsługi więcej niż jednej kategorii usług,
- system powinien mieć możliwość nadawania priorytetów dla danych usług na poszczególnych stanowiskach (min. 3 poziomy priorytetów),
- system musi pracować w ramach sieci LAN,
- system musi umożliwiać podgląd pracy systemu osobom odpowiedzialnym za nadzór bez konieczności opuszczania swoich miejsc pracy, w ramach sieci LAN,
- zarządzanie (zmiana parametrów) i monitoring systemu powinien odbywać się centralnie za pośrednictwem przeglądarki internetowej z dowolnej stacji komputerowej w ramach sieci LAN,
- system powinien być w pełni elastyczny pod względem rozbudowy o dodatkowe urządzenia (automaty biletowe, ekrany stanowiskowe, ekrany zbiorcze),
- system powinien zapewniać możliwość rozbudowy bez dodatkowych kosztów:
- - o dodatkowe kategorie i/lub grupy usług reprezentowane oddzielnym przyciskiem na automacie biletowym,
- - o dodatkowe wirtualne konsole przywoławcze w postaci oprogramowania,
- system powinien odtwarzać aktualny stan kolejki po czasowym zaniku napięcia w sieci zasilającej,
- możliwość ustawienia dowolnej godziny, o której resetowany jest stan kolejki, ponadto system powinien posiadać możliwość ręcznego zresetowania stanu kolejki w dowolnym momencie przez upoważnioną osobę,
- system powinien mieć możliwość uruchomienia komunikacji audio (tzw. gong lub wyczytywanie przywoływanego biletu) bez dodatkowych kosztów rozbudowy,
- program sterujący pracą systemu kolejkowego powinien móc funkcjonować uniwersalnie w środowisku windows i linux,
- system musi zapewnić możliwość zmiany w dowolnym momencie funkcji poszczególnych stanowisk,
- system musi umożliwiać dowolny transfer klientów pomiędzy różnymi kategoriami spraw bez konieczności ponownego pobierania biletu oraz możliwość przerwania na pewien czas obsługi danego klienta i obsługiwania w czasie tej przerwy innych klientów,
- powinna istnieć możliwość samodzielnego określenia w systemie ilościowego lub czasowego limitu wydawania biletów do poszczególnych kategorii usług,
- powinna istnieć możliwość samodzielnego zablokowania wydawania biletów do poszczególnych kategorii usług w dowolnym momencie przez uprawnionego pracownika za pośrednictwem konsoli przywoławczej,
- system w całości powinien obsługiwać język polski włącznie ze znakami diakrytycznymi,
- system powinien mieć możliwość obsługi 3 dowolnych tłumaczeń językowych na automacie biletowym oraz realizować przywołania audio w tych 3 językach,
- system powinien posiadać możliwość wykupienia dodatkowej licencji na otwarte API wraz z dokumentacją techniczną w języku polskim do integracji z zewnętrznymi systemami (np. z systemem bazo-danowym placówki),

- system powinien mieć możliwość realizacji obsługi w ramach kolejności przybycia jak i w ramach umówionych wizyt,
- system powinien posiadać możliwość wykupienia dodatkowej licencji na umawianie wizyt za pośrednictwem strony internetowej jak i ręcznie przez pracowników w placówce,
- system powinien posiadać możliwość wykupienia dodatkowej licencji na publikację wybranych danych na stronie internetowej Inwestora (np. ilość oczekujących osób w poszczególnych kategoriach usług),
- system musi mieć możliwość opcjonalnego uruchomienia modułu „Badania Satysfakcji Klientów” poprzez agregowanie statystyk z mobilnych urządzeń, na których Klient może ocenić w 3 stopniowej skali zadowolenie z obsługi, moduł zarządzany jest z tego samego panelu co cały system,
- system musi mieć możliwość opcjonalnego uruchomienia modułu wyświetlania na monitorach stanowiskowych grafiku pracy pracowników w poszczególnych pokojach, dane wyświetlane są automatycznie z harmonogramu poszczególnych pracowników, moduł zarządzany jest z tego samego panelu co cały system,
- system musi mieć możliwość opcjonalnego uruchomienia modułu kalendarza do umawiania wizyt na nadchodzące dni, dodatkowo musi istnieć możliwość wystawienia na stronie internetowej Inwestora pluginu html lub php do samodzielnego umawiania wizyt przez Klientów, moduł zarządzany jest z tego samego panelu co cały system,
- możliwość ustawiania tzw. „inteligentnych limitów biletów”, które wstrzymują wydawanie biletów danego dnia jeśli szacowany czas obsługi wykracza poza czas pracy,
- możliwość sprawdzania historii obsługi wygenerowanych biletów.

10.2 Moduł raportów

- możliwość podglądu stanu kolejki w czasie rzeczywistym,
- możliwość eksportu raportu do plików Excel, CSV, XML, PDF,
- dostęp tylko dla osób uprawnionych (logowanie zabezpieczone hasłem),
- dostęp powinien odbywać się centralnie za pośrednictwem przeglądarki internetowej z dowolnej stacji komputerowej w ramach sieci LAN,
- możliwość generowania raportów dziennych oraz w wyznaczonych okresach,
- możliwość raportowania po stanowiskach, użytkownikach i usługach,
- statystyka czasu oczekiwania na obsługę (średniego , maks. i min.),
- statystyka czasu obsługi (średniego , maks. i min.),
- statystyka pobranych biletów, anulowanych, przekierowanych,

10.3 Komunikacja systemu

Instalacje systemu kolejkowego należy wpiąć do lokalnej sieci LAN

10.4 Zasilanie urządzeń

Zasilanie urządzeń – z instalacji 230V AC, doprowadzenie zasilania wg projektu branży elektrycznej.

10.5 Elementy systemu

Automat biletowy

- każdy automat biletowy musi być wyposażony w monitor dotykowy min. 19”,
- nakładka dotykowa powinna być wykonana w technologii umożliwiającej zabezpieczenie matrycy monitora odpornym szkłem,
- pobranie biletu z automatu biletowego będzie się odbywało przez dotknięcie odpowiedniego pola na ekranie monitora dotykowego, na którym będzie znajdował się opis usługi,
- automat powinien być wyposażony w przemysłową drukarkę termiczną o szer. biletów min. 570 mm oraz z automatycznym odcinaczem papieru,
- drukarka powinna działać na zwykłym papierze do kas fiskalnych bez wymaganej dodatkowej perforacji
- Inwestor powinien mieć możliwość redagowania informacji umieszczanych na drukowanych przez automat biletach,
- automat powinien mieć opcjonalną możliwość generowania wirtualnych biletów (wyświetlanych na monitorze automatu bez wydruku biletu),

  bilety powinny móc zawierać poniższe informacje:

  - nazwa i adres organizacji,
  - data i godzina wydania biletu,
  - ilość osób oczekujących w kolejce,
  - przewidywany czas oczekiwania,
  - logo, mapki i inne obrazki,
  - dowolne informacje tekstowe,

- Personalizacja: logo Klienta w formie naklejki,
- Komunikacja: LAN,
- Zasilanie: 230V,
- Montaż: wolnostojący lub przymocowany na kołki do podłoża,
- Materiał: stal (opcjonalnie stal nierdzewna),
- Kolor: szary (opcjonalnie paleta RAL),
- Zabezpieczony dostęp na zamek z wkładką patentową,
- Wandaloodporna konstrukcja,
- Otwory rewizyjne do wszystkich komponentów,
- Wymiana papieru powinna być możliwa z frontu automatu,
- Możliwość zdalnego serwisu.
- Konsola przywoławcza w wersji oprogramowania
- logowanie do konsoli zabezpieczone hasłem,
- aplikacja komputerowa instalowana na systemach typu Windows 7 SP1, 8.1, 10,
- możliwość zmiany przez użytkownika kategorii obsługiwanych kolejek,
- możliwość ustawienia opcji „zawsze na wierzchu,
- możliwość ponownego wezwania Klienta,
- możliwość przywołania Klienta po numerze jego biletu,
- transfer Klienta do innej kolejki,

- podgląd ilości Klientów oczekujących w kolejce,
- podgląd ilości Klientów oczekujących w innych kolejkach,
- możliwość anulowania danego biletu,
- możliwość wstrzymania obsługi danego biletu i wskazanie czasu po którym będzie przywrócony do obsługi,
- możliwość ręcznego wybrania Klienta w kolejce,
- licencja bezterminowa, bez ograniczenia ilości instalacji,
- możliwość uruchomienia konsoli w wersji Web bez dodatkowych kosztów.

Wyświetlacze stanowiskowe

- wyświetlacze stanowiskowe (służące do wyświetlania numeru obsługiwanego aktualnie klienta) muszą wyświetlać przynajmniej cztery znaki reprezentujące przywoływany bilet oraz wyświetlać nazwę i numer stanowiska.
- muszą także mieć możliwość wyświetlania informacji z każdej grupy usług tak, aby zmiana litery symbolizującej grupę usług i numer klienta odbywała się automatycznie w zależności od tego, z jakiej grupy przywoływany jest klient.
- Wyświetlacze powinny być monitorami LCD wykonanymi w technologii led o przekątnej ekranu min. 15”, a maksymalnie 21”.
- min. rozdzielczość monitora to 1366x768 px,
- monitor powinien być przystosowany do pracy ciągłej w trybie min. 12h/7,
- monitor powinien być wyposażony w player z systemem Android 5.1 lub nowszym do obsługi aplikacji kolejkowej,
- Jasność: min. 200 cd/m2,
- Kontrast: min. 700:1,
- Kolor: czarny,
- Komunikacja: LAN, WiFi,
- Zasilanie: 230V,

Wyświetlacze główne

- wyświetlacz główny służy do wyświetlania informacji systemowych takich jak aktualnie obsługiwany numer w grupach oraz dowolnych informacji dotyczących np. działalności placówki itp.
- informacja na monitorze musi mieć możliwość wyświetlania loga i nazwy placówki, przywoływanych biletów do dowolnej ilości obsługiwanych kategorii usług oraz treści multimedialnych,
- monitor powinien być wyposażony w player z systemem Android 5.1 lub nowszym do obsługi aplikacji kolejkowej,
- oprogramowanie wraz z playerem Android obsługujące wyświetlane treści na monitorze musi umożliwiać publikację takich źródeł jak: pliki video (mp4), pliki graficzne (jpg, png, bmp),
- możliwość przygotowania listy odtwarzanych multimediów,
- wyświetlacze powinny być monitorami LCD wykonanymi w technologii led o przekątnej ekranu min. 32”, a maksymalnie 65”.
- min. rozdzielczość monitora to 1920x1080 px
- monitor powinien być przystosowany do pracy ciągłej w trybie min. 12h/7,
- Jasność: min. 300 cd/m2,
- Kontrast: min. 1000:1,

- Auto włącznik i wyłącznik,
- Kolor: czarny,
- Komunikacja: LAN, WiFi,
- Zasilanie: 230V,
- Wbudowane głośniki, możliwość generowania przywołań audio.

Oprogramowanie systemu

- program sterujący pracą systemu kolejkowego powinien funkcjonować uniwersalnie w środowisku windows lub linux wg potrzeb,
- system musi być sterowany w trybie on-line przez komputer włączony w sieć komputerową Inwestora,
- system musi mieć możliwość pracy w sieci, w celu przekazywania on-line pełnych informacji o postępie załatwiania interesantów, pracy stanowisk itp. oraz możliwość wydruków raportów statystycznych,
- system musi zapewnić poprzez sieć komputerową możliwość zdalnego diagnozowania oraz dokonywania zmiany konfiguracji ustawień systemu w obszarze obsługi klientów; usługa zdalnego dostępu powinna posiadać funkcje zabezpieczenia, uniemożliwiające dokonywania zmian przez osoby nieupoważnione.
- panel administracyjny i konfiguracyjny powinien być dostępny z poziomu przeglądarki internetowej w ramach sieci LAN Zamawiającego,
- możliwość budowania bibliotek multimediów,
- baza użytkowników z min. 3 rolami uprawnień (pracownik, manager, administrator).

UWAGA SYSTEM KOLEJKOWY – MUSI BYĆ KOMPATYBILNY Z SYSTEM ZAINSTALOWANYM NA PARTERZE CZĘŚCI NIEMODERNIZOWANEJ.

11. USZCZELNIENIA POŻAROWE

Wszelkie przepusty i oddzielenia stref pożarowych będą musiały posiadać odporność ogniową równą odporności tego oddzielenia.

Stosowane będą przegrody i uszczelnienia produkcji renomowanych firm, np. PROMAT, takie jak:

- masa uszczelniająca pęczniejąca – uszczelnienia pojedynczych kabli oraz wiązek kabli, do uszczelnienia przejść przez stropy (szachty) i przebicia poziome,
- poduszki ochronne pęczniejące – uszczelnienia tras kablowych i dużych przejść instalacyjnych
- zaprawa murarska – uszczelnienia przejść przez ściany i stropy,

Zastosowane materiały ogniochronne muszą być atestowane i montowane zgodnie z instrukcją producenta.

12. WYTYCZNE DO BEZPIECZEŃSTWA I OCHRONY ZDROWIA

Ze względu na specyfikę obiektu podczas realizacji zadania projektowego wymagane jest bezwzględne stosowanie się do zasad BHP dotyczących bezpieczeństwa pracy na wysokości podczas realizacji projektu.

Strefy robót na wysokościach powinny być odpowiednio oznaczone i odgrodzone, a pracownicy powinni posiadać odpowiednie zabezpieczenia.

Pracownicy zatrudnieni przy robotach budowlanych i montażowych w zakresie instalacji elektrycznych i teletechnicznych powinni być przeszkoleni pod względem bezpieczeństwa i higieny pracy stosownie do rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 roku „w sprawie szczegółowych zasad szkolenia w dziedzinie bezpieczeństwa i higieny pracy” (Dz. U. Nr 62, poz. 1405), oraz posiadać aktualne badania lekarskie stwierdzające możliwość wykonywania prac na wysokości.

Na całym terenie robót obowiązywać będzie nakaz noszenia kasków ochronnych dla wszystkich pracowników i służb dozoru.

Przebywanie na terenie budowy osób trzecich będzie mogło odbywać się jedynie po wydaniu zezwolenia przez kierownika budowy i pod nadzorem osoby upoważnionej do przebywania na terenie.

Realizacje projektu należy wykonać zgodnie z projektem, przepisami i normami branżowymi, oraz przepisami p.poż, bezpieczeństwa i higieny pracy mając na względzie zasady bezpieczeństwa i ochrony zdrowia, zawarte w przepisach wydanych na podstawie art. 21a, ust.4 ustawy z dnia 7 lipca 1994 roku – Prawo Budowlane (Dz. U. z 2000r. Nr 106, poz. 1126, z późniejszymi zmianami) ze szczególnym uwzględnieniem zasad określonych w ROZPORZADZENIU MINISTRA INFRASTRUKTURY z dnia 6 lutego 2003 roku „w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych” (Dz. U,. z 2003 roku, nr 47, poz. 401).

Wszelkie roboty powinny być wykonywane zgodnie z wymogami Ministra Budownictwa i Przemysłu „w sprawie bhp i przy robotach budowlano montażowych i rozbiórkowych” z dnia 28 marca 1972 roku (Dz. U. nr 13, poz. 93), oraz wymogami Rozporządzenia Ministra Infrastruktury z 06.02.2003 roku „w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych” (Dz. U. Nr 47, poz. 401).

Dodatkowo zwraca się uwagę na obowiązki wynikające z Ustawy Prawo Budowlane;

1. Zgodnie z zapisem Art. 42, ust. 1 Inwestor jest obowiązany zapewnić objęcie kierownictwa budowy (rozbiórki) lub określonych robót budowlanych, oraz nadzoru nad robotami przez osobę posiadającą uprawnienia budowlane w odpowiedniej specjalności.

2. Zgodnie z zapisem Art. 41, ust. 4 Inwestor jest zobowiązany zawiadomić o zamierzonym terminie rozpoczęcia robót budowlanych, na które jest wymagane pozwolenie na budowę właściwy organ oraz projektanta sprawującego nadzór nad zgodnością realizacji budowy z projektem, co najmniej 7 dni przed ich rozpoczęciem, dołączając na piśmie oświadczenie kierownika budowy (robót), stwierdzające sporządzenie plany bezpieczeństwa i ochrony zdrowia oraz przyjęcie obowiązku kierowania budową (robotami budowlanymi), a także zaświadczenie, o którym mowa w Art. 12 ust. 7 Ustawy.

3. Zgodnie z zapisem Art. 42, ust.2 pkt. 2 Kierownik budowy (robót) jest obowiązany umieścić na budowie (…), w widocznym miejscu, tablice informacyjną, oraz ogłoszenie zawierające dane dotyczące zasad bezpieczeństwa pracy i ochrony zdrowia; (…).

13. ZGODNOŚĆ ZASTOSOWANYCH MATERIAŁÓW Z PRZEPISAMI LOKALNYMI

Zastosowane materiały i urządzenia będą musiały posiadać stosowane atesty wymagane przepisami lokalnymi. Wykonawca będzie zobowiązany do przedłożenia do nadzoru budowy stosownych dokumentów przed ich zamówieniem i instalacją w obiekcie.

14. UWAGI KOŃCOWE

Całość prac należy wykonać zgodnie z obowiązującymi przepisami i normami.
Wykonawca jest zobowiązany do zapoznania się z DTR każdego urządzenia, przed jego zamontowaniem i uruchomieniem.

Wykonawca jest zobowiązany do sporządzenia nieodpłatnie dokumentacji powykonawczej.
Wszystkie zmiany na etapie realizacji w stosunku do zapisów w projekcie powinny zostać zawarte w dokumentacji powykonawczej w formie potwierdzonych podpisem uzgodnień.
Wszelkie zmiany materiałowe, zmiany tras prowadzenia kabli i warunków wykonania instalacji powinny zostać skonsultowane z projektantem, ew. inspektorem nadzoru, a końcowe ustalenia zmian powinny zostać zawarte w postaci potwierdzonej pisemnie notatki i załączone do dokumentacji powykonawczej.
Dokumentacja powykonawcza musi zostać dostarczona do Inwestora przed odbiorem technicznym.

Po wykonaniu instalacji w obiekcie należy, przed zgłoszeniem do odbioru, przeprowadzić pomiary i próby montażowe, zgodnie z wytycznymi Polskich Norm. Protokoły badań i pomiarów należy dołączyć do dokumentacji powykonawczej.

Wszystkie prace oraz pomiary musza zostać wykonane przez osoby posiadająca odpowiednie przeszkolenie potwierdzone stosownymi certyfikatami – SEP E, SEP D.

15. KLAUZULA OPRACOWANIA

Opracowanie jest zgodne z umową i kompletne z punktu widzenia celu, któremu ma służyć. Wraz z podpisaniem przez obie strony protokołu odbioru końcowego dokumentacji bez zastrzeżeń, Projektant w ramach wynagrodzenia określonego w umowie przenosi na Zamawiającego autorskie prawa majątkowe oraz prawa zależne do przedmiotu umowy oraz do każdej jego części, bez ograniczeń czasu, terytorium, wersji językowych, sposobu, form i środków eksploatacji na wszystkich polach eksploatacji znanych w dniu zawarcia umowy.

Projekt został wykonany zgodnie z obowiązującymi przepisami budowlanymi, Polskimi Normami, oraz zasadami wiedzy technicznej. Projekt opracowano zgodnie z udostępnionymi danymi do wykonania pracy, oraz z uwzględnieniem aktualnych przepisów na dzień przekazania projektu Zamawiającemu. W całościowej formie zawartej w opracowaniu nadaje się do wykonania instalacji objętej projektem.
Integralną częścią całego opracowania jest opis wraz z rysunkami w postaci rzutów i schemat instalacji zgodnie z zamieszczonym zestawieniem w spisie treści.

Wykorzystanie opracowania w kolejnych fazach procesu inwestycyjnego - szczególnie po upływie 12 miesięcy od daty jego wykonania - wymagać będzie sprawdzenia i ewentualnej weryfikacji danych oraz zastosowanych rozwiązań technicznych pod kątem obowiązujących wówczas przepisów.

16. ZAŁĄCZNIKI I RYSUNKI