Normy europejskie dotyczące ogólnych wymagań oraz specyficznych dla środowiska biurowego:

- PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne
- PN-EN 50173-2:2008/A1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe

Dodatkowe normy europejskie związane z planowaniem powołane w projekcie:

- PN-EN 50174-1:2010/A1:2011 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości
- PN-EN 50174-2:2010/A1:2011 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków
- PN-EN 50174-3:2014-02 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków
- PN-EN 50346:2004/A2:2010 Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania
- ISO/IEC 14763-3:2014 Implementation and operation of customer premises cabling - Part 3: Testing of optical fibre cabling
- PN-EN 50310:2016 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym

Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami opisanymi w dokumentacji projektowej, a jeśli którykolwiek z dokumentów normalizacyjnych uległ aktualizacji wg nowych aktualnych wymagań.

Wymagania ogólne dotyczące okablowania strukturalnego

- Ilość stanowisk roboczych wynika ze wskazówek Użytkownika końcowego, przy czym ich ostateczna i precyzyjna lokalizacja powinna być ustalona z wykonawcą okablowania przed rozpoczęciem prac;
- Maksymalna długość kabla instalacyjnego (tzw. łącza stałego) nie może przekroczyć 90 metrów;
- Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu 25-letniej gwarancji udzielonej bezpośrednio przez w/w producenta;
- Minimalne wymagania elementów okablowania komputerowego pod względem wydajności to Kategoria 6_A (komponenty)/ Klasa E_A (podstawowa wydajność całego systemu) i zapewnienie możliwości transmisji 10Gigabit Ethernet 802.3an, zaś docelowa wydajność każdego kanału transmisyjnego zbudowanego z kabli miedzianych to Klasa F_A;
- Liczba i rozmieszczenie stanowisk roboczych przyjęto na podstawie informacji podanych w trakcie wizji lokalnej przez Użytkownika/Inwestora. W trakcie realizacji, ostateczna lokalizacja gniazd logicznych w pomieszczeniach (bez zmiany ich liczby) powinna być ustalona pomiędzy Użytkownikiem, a Wykonawcą;
- Okablowanie strukturalne w budynków obsługiwane jest przez Punkty Dystrybucyjne;
- Punkty dystrybucyjne są zlokalizowane w zaznaczonych na rzutach miejscach, ewentualne zmiany lokalizacji punktów dystrybucyjnych mają być uwzględnione na etapie wykonawczym oraz zaznaczone w dokumentacji powykonawczej;

- Okablowanie strukturalne ma być prowadzone podwójnie ekranowanym kablem typu S/FTP (PiMF) 7_A w powłoce zewnętrznej LSFRZH;
- Punkty końcowe PEL oparte zostały na uniwersalnym ekranowanym gnieździe teleinformatycznym (z możliwością wymiany interfejsu końcowego w postaci wkładki, bez zmian w trwałym zakończeniu kabla na złączu) w uchwycie do osprzętu np. Mozaik (45x45);
- System ma pozwalać na rozbudowę ilości gniazd (interfejsów) końcowych bez konieczności instalacji nowych kabli oraz bez ponownej terminacji kabla na złączu;
- System ma zapewniać możliwość wielokrotnej zmiany typu gniazda, jego kategorii oraz współdzielenia kabla dla wielu aplikacji przy czym czynności te mają być wykonywane samodzielnie przez Użytkownika bez ingerowania w rozszycie kabla na osprzęcie połączeniowym bez potrzeby ponownego zarabiania gniazd, ponownego wykonywania pomiarów oraz instalowania dodatkowych elementów w postaci paneli krosowych i płyt czołowych w punktach logicznych.
- System ma pozwalać na zmianę wydajności (kategorii, klasy okablowania) na odpowiednią (zarówno w górę jak i w dół), jedynie poprzez zmianę wkładek końcowych – bez zmian kabla transmisyjnego i bez zmian w jego stałym zakończeniu;
- Nie dopuszcza się stosowania gniazd i wtyków z niestandardowymi interfejsami (takimi, do których nie ma referencji w dokumentach z Rozdziału 3).
- Wszystkie łącza okablowania poziomego mają zapewniać:
  - Możliwości transmisyjne do minimum klasy FA co ma być potwierdzone certyfikatem pomiarowym wydanym na kanał lub łącze przez akredytowane niezależne laboratorium (np. Delta, GHMT) oraz powykonawczo pomiarami wykonanymi na obiekcie z gniazdem kat.7A.
  - Możliwość zmiany typu gniazda na inny znajdujący się w normach ISO/IEC 11801 EN50173-1: RJ45, ARJ45, TERA złącze FA.
  - Możliwość zmiany kategorii gniazd na kat. 5, kat.6, kat.6_A i kat.7_A
  - Gniazda wymienne muszą występować w minimum 3 kolorach np. biały, czarny, beżowy
  - Możliwość współdzielenia jednego kabla dla kilku aplikacji w następujących konfiguracjach:
    - 2 x Fast Ethernet z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6A,
    - 2 x ISDN z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6A,
    - Fast Ethernet + ISDN z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6A,
    - Gigabit Ethernet + ISDN z wykorzystaniem gniazd RJ45,
    - 2 x telefon analogowy + Fast Ethernet z wykorzystaniem gniazd RJ45,
    - 4 x telefon analogowy z wykorzystaniem gniazd RJ45 kat.3,
    - 1 x telefon analogowy + 1x Fast Ethernet + 1x CATV z wykorzystaniem gniazd RJ45 i złącza F,
    - 1x TERA o wydajności Kat.7A
- W momencie instalacji należy zapewnić w punktach logicznych dostęp do gniazd 1xRJ45 kategorii $6_{A;}$
- Pomiędzy punktami dystrybucyjnymi należy zrealizować okablowanie szkieletowe światłowodowe klasy OF 300:
  - Punkty Dystrybucyjne w obrębie sieci należy połączyć kablem światłowodowym jednomodowym OS2 8x9/125/250µm w luźnej tubie, w osłonie ULSZH oraz kablem wielomodowym OM3 8x50/125/250µm w luźnej tubie, w osłonie ULSZH;
- Wszystkie złącza światłowodowe muszą być wypolerowane w fabrycznym procesie produkcyjnym;
- Połączenia dla linii telefonicznych analogowych należy zrealizować następująco:

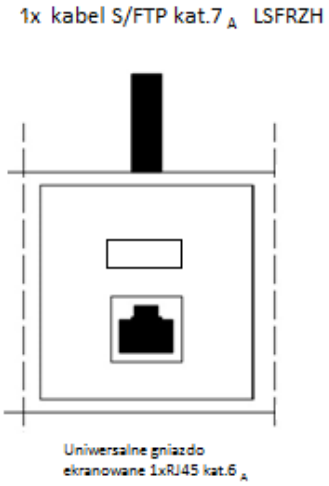
- W budynku pomiędzy Punktami Dystrybucyjnymi poprowadzić kabel U/UTP kat. 3, 50 par w osłonie LSZH;

- Środowisko, w którym będzie instalowany osprzęt kablowy jest środowiskiem biurowym i zostało ono sklasyfikowane jako $M_1I_1C_1E_2$ wg. specyfikacji środowiska instalacji okablowania (MICE) – zgodnie z PN-EN 50173-1:2011;
- Na całość zainstalowanego okablowania ma być udzielona gwarancja bezpośrednio przez producenta na okres minimum 25 lat (szczegółowy opis zawarty w dziale „Gwarancja oraz wymagania dotyczące kompetencji").

Instalacja teletechniczna (opis technologii)

Konfiguracja punktu logicznego

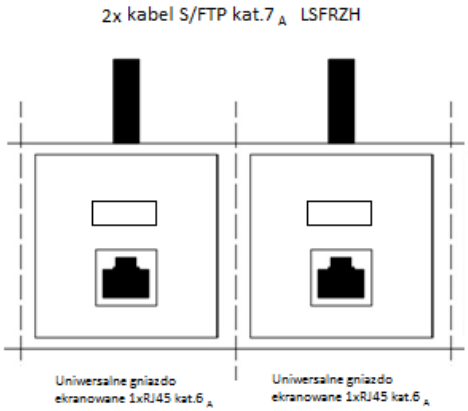
Do Punktu Logicznego w konfiguracji 1 doprowadzić 1 kabel S/FTP kat.7A, który należy zakończyć w osprzęcie połączeniowym z zamontowanym wymiennym gniazdem RJ45 kat.6A. Gniazda zasilające mogą być umieszczone z obu stron gniazd PL2.



Punkt Logiczny 1 z jednym wymiennym gniazdem ekranowanym 1xRJ45 kat.6_A .

Kable okablowania poziomego mają być zakończone w zestawach gniazd, zwanych dalej punktami logicznymi (PL). Zestawy gniazd mają być zgodne ze standardem uchwytu osprzętu elektroinstalacyjnego typu Mosaic 45. Ostateczna lokalizacja powinna być ustalona z Użytkownikiem.

Do Punktu Logicznego w konfiguracji 2 (2xPL1) doprowadzić 2 kable S/FTP kat.7A, które należy zakończyć w osprzęcie połączeniowym z zamontowanym wymiennym gniazdem RJ45 kat.6A. Gniazda zasilające mogą być umieszczone z obu stron gniazd PL2.



Punkt Logiczny 2 z dwoma wymiennymi gniazdami ekranowanymi 1xRJ45 kat.6_A .

Okablowanie poziome

Należy stosować kable w powłokach LSFRZH. Przy prowadzeniu tras kablowych zachować bezpieczne odległości od innych instalacji. W przypadku traktów, gdzie kable sieci teleinformatycznej i zasilającej biegną razem i równolegle do siebie, należy zachować odległość (rozdział) między instalacjami (szczególnie zasilającą i logiczną), co najmniej 10mm lub stosować metalowe przegrody. Wielkość separacji dla trasy kablowej jest obliczona dla przypadku kabli S/FTP 7A. Zakłada się, że ilość obwodów elektrycznych 230V 50Hz max 16A nie będzie większa niż 15.

Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 8mm (co determinuje maksymalną średnicę żyły na 23AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej.

Instalacja ma być poprowadzona ekranowanym kablem konstrukcji S/FTP z osłoną zewnętrzną LSFRZH. Ekran takiego kabla ma być zrealizowany na dwa sposoby:

1. w postaci jednostronnie laminowanej folii aluminiowej oplatającej każdą parę transmisyjna (w celu redukcji oddziaływań miedzy parami)
2. w postaci wspólnej siatki okalającej dodatkowo wszystkie pary (skręcone razem między sobą) – w celu redukcji wzajemnego oddziaływania kabli pomiędzy sobą.

Taka konstrukcja pozwala osiągnąć najwyższe parametry transmisyjne, zmniejszenie przesłuchu NEXT i PSNEXT oraz zmniejszyć poziom zakłóceń od kabla. Pozwala także w dużym stopniu poprawić odporność na zakłócenia zarówno wysokich, jak i niskich częstotliwości. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze obowiązujące specyfikacje.

Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min. 1500MHz dla kabla kat.7A.

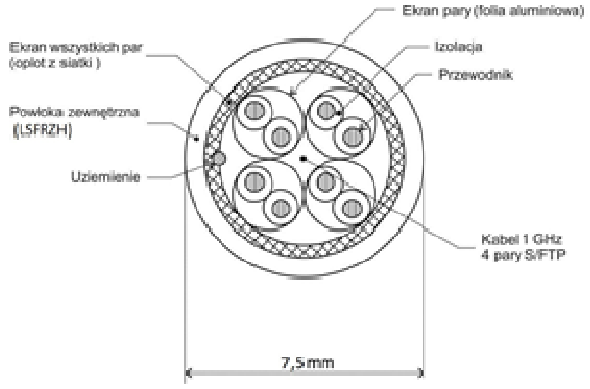
W celu zagwarantowania najwyższej jakości połączenia przede wszystkim powtarzalnych parametrów, wszystkie złącza, zarówno w gniazdach końcowych jak i panelach muszą być zarabiane za pomocą standardowych narzędzi instalacyjnych tj. zgodnych ze standardem złącza 110 lub LSA+. Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym (umieszczonych w zestawach instalacyjnych) nie może być większy niż 6 mm.

Kabel ten ma spełniać wymagania stawiane komponentom Kategorii 7A przez obowiązujące specyfikacje norm, równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania.

Wymagania dla kabla (S/FTP Kat.7_A)

Budowa kabla	S/FTP (zgodnie z rysunkiem)
Wydajność kabla	Kategoria 7_A wg. ISO/IEC 11801; EN 50173-1 z charakterystykami rozszerzonymi do częstotliwości 1500MHz
Certyfikat	Producent musi dostarczyć certyfikat wydany przez laboratorium

	potwierdzający jego charakterystyki na kategorię 7_A
Normy dotyczące palności	IEC 60332-1, IEC 60754-1, IEC 60754-2, IEC 61034-2
Tłumienie sprzężenia	Min. 85dB
Średnica zewnętrzna kabla	max.7,5 mm
Średnica żyły	23AWG (Φ 0.54 – 0.61mm)
Waga	max 68 kg/km
Temperatura podczas instalacji	Minimum przedział 0ºC do +50ºC
Osłona zewnętrzna:	LSFRZH, LSZH-FR



Budowa kabla kat. 7_A S/FTP

Wymagania dla parametrów transmisyjnych kabla przy częstotliwościach kluczowych:

Częstotliwość	**Tłumienie**	**PSNEXT**	**RL**
[MHz]	[dB]	[dB]	[dB]
100	17	102	40
250	27	102	34
600	46	92	25
1000	58	85	18
1500	79	82	13

Kable miedzianego okablowania poziomego należy zakończyć na panelach krosowych prostych o wysokości montażowej 1U i pojemności do 24 gniazd. Każdy port ma mieć możliwość oddzielnego opisu i oznaczenia poprzez system kolorowych ikon. Panel ma być wyposażony w tylny wspornik w celu ułożenia i zamocowania do niego kabli, oraz zacisk uziemiający. Panele mają być wyposażone w gniazda RJ45 tego samego typu co w punktach dostępowych Użytkownika (punktach logicznych).

Panele uniwersalne powinny posiadać zintegrowane prowadnice na kable oraz odpowiednią ilość portów wyposażonych w uniwersalne ekranowane złącza modularne umieszczone w zamkniętej, ekranowanej obudowie (szczelna elektromagnetycznie klatka Faraday'a. Dzięki takiej konstrukcji w uniwersalnym złączu modularnym można umieścić dowolne wymienne wkładki, o odpowiedniej wydajności (kategorii okablowania) i z odpowiednim interfejsem końcowym. Panele uniwersalne powinny posiadać 24 porty na wysokości 2U. W fazie projektowej (uruchomienia instalacji) należy skonfigurować porty w panelu tak, aby spełniały obecne wymagania kategorii 6A/klasy EA – wykorzystując w gniazdach wkładki 1xRJ45 kat.6A (uniwersalne).

Kable krosowe miedziane

Kable obszaru roboczego (przyłączane do stacji użytkownika), jak i krosowe (w szafie kablowej) mają być wykonane z linki ekranowanej S/FTP 600MHz. Wtyk złącza RJ45 ma posiadać szczelną

elektromagnetycznie osłonę ekranowaną, tak aby zapewnić kontakt elektryczny z obudową ekranowanych gniazd RJ45 po całym obwodzie złącza. Wymaga się standardowej sekwencji rozszycia kabla T568B (preferowana) lub T568A. Osłona zewnętrzna kabli ma być typu LSZH.

Wszystkie kable obszaru roboczego i krosowe mają być fabrycznie wykonane i testowane. Wszystkie komponenty składowe: wtyki, kabel mają być wyprodukowane i trwale oznaczone przez tego samego producenta co cały system okablowania. Dodatkowo kable krosowe miedziane mają być zgodne ze specyfikacją Kat.6_A. Wymagane jest aby kable krosowe były wykonane fabrycznie z linki ekranowanej typu S/FTP, posiadającej osłonę LSZH.

Okablowanie szkieletowe światłowodowe

Okablowanie szkieletowe ma zapewnić kanały transmisyjne o dużej przepustowości łączące poszczególne punkty dystrybucyjne sieci ze sobą.

Dobór nośników ma zapewnić minimalizację zakłóceń elektromagnetycznych oraz maksymalną uniwersalność w uruchamianiu różnorodnych protokołów transmisyjnych.

Szkielet budynkowy należy wykonać z użyciem kabla światłowodowego wielomodowego kategorii OM3 oraz kabla światłowodowego jednomodowego kategorii OS2. We wszystkich panelach krosowych światłowodowych wielomodowych i jednomodowych należy zastosować interfejs typu LC.

Wymagania dla kabla wielomodowego 12 włóknowego OM3

Budowa	12 włókien światłowodowych konstrukcja luźnej tuby wyłącznie elementy dielektryczne
Kolory włókien	Zgodna z EN50174-1
Palność Emisja dymów Emisja gazów żrących	IEC 60332 część 1 oraz 3 IEC 60334 część 1 oraz 2 IEC 6074 część 1
Osłona zewnętrzna	LSZH z odpornością min. 180min próby ogniowej
Średnica zewnętrzna kabla	Max. 7,9 mm
Waga	Max. 56 kg/km
Promień gięcia	Min. 115 mm
Max tłumienność 850nm	2,4dB/km
Max tłumienność 1300nm	0,6 dB/km

Wymagania transmisyjne dotyczące charakterystyki włókien FO MM

Typ włókna	Szerokość pasma [MHz x km]		Tłumienność [dB/km]	
	850 nm	1300 nm	850 nm	1300 nm
OM3	≥ 1500	≥ 500	≤ 2,4	≤ 0,6

Włókna wielomodowe należy po obu stronach toru transmisyjnego zakończyć pigtailami – połączenie należy wykonać w technologii spawania. Pigtaile muszą być wykonane z włókna światłowodowego o średnicy rdzenia 50 µm spełniającego wymagania kategorii OM3 w buforze 900µm fabrycznie zakończone interfejsem LC z ceramiczną ferrulą i fabrycznie pomierzone. Każdy pigtail musi być zapakowany osobno i posiadać nadruk z informacją o indywidualnych wartościach pomiarowych.
Tłumienność wtrąceniowa nie może przekraczać 0,3dB natomiast strata sygnału odbitego powinna być wyższa od 30dB.

Wymagania dla kabla jednomodowego 12 włóknowego OS2

Budowa	12 włókien światłowodowych konstrukcja luźnej tuby wyłącznie elementy dielektryczne
Kolory włókien	Zgodna z EN50174-1

Palność Emisja dymu Emisja gazów trujących	IEC 60332 część 1 oraz 3 IEC 61034 część 1 oraz 2 IEC 60754 część 1
Osłona zewnętrzna	ULSZH
Średnica zewnętrzna kabla	Max. 6,4 mm
Waga	Max. 48 kg/km
Promień gięcia	Min. 130 mm
Naprężenia podczas instalacji	max. 1250 N
Odporność na zgniecenia	1000N

Wymagania transmisyjne dotyczące charakterystyki włókien FO SM

Typ włókna	Tłumienność [dB/km]		
	1310 nm	1380-1386 nm	1550 nm
OS2	≤ 0,34	≤ 0,34	≤ 0,22

Włókna jednomodowe należy po obu stronach toru transmisyjnego zakończyć pigtailami – połączenie należy wykonać w technologii spawania. Pigtaile muszą być wykonane z włókna światłowodowego o średnicy rdzenia 9 µm spełniającego wymagania kategorii OS2 w buforze 900 µm fabrycznie zakończone interfejsem LC z ceramiczną ferrulą.

Tłumienność wtrąceniowa nie może przekraczać 0,3dB, natomiast strata sygnału odbitego powinna być wyższa od 45 dB.

Kable krosowe światłowodowe
Światłowodowe kable krosowe muszą być wykonane fabrycznie, maszynowo polerowane, fabrycznie przetestowane i posiadać protokoły badań dla każdego kabla oddzielnie. Kable krosowe muszą być fabrycznie zakończone z obu stron interfejsem typu LC, z ceramiczną ferullą i być wykonane z włókna światłowodowego o średnicy rdzenia 9 µm lub 50 µm w zależności od zastosowanego kabla światłowodowego . Każdy kabel musi być zapakowany osobno i posiadać nadruk z informacją o indywidualnych wartościach pomiarowych.

Tłumienność wtrąceniowa nie może przekroczyć 0,3dB natomiast strata sygnału odbitego powinna być wyższa niż 35dB dla kabli MM oraz tłumienność wtrąceniowa nie może przekroczyć 0,3dB natomiast strata sygnału odbitego powinna być wyższa niż 45dB dla kabli SM. Kabel musi działać w zakresie temperatur od -10^{o}C do +60^{o}C.

Ze względu na parametry optyczne i geometryczne, niedopuszczalne jest stosowanie kabli krosowych zarabianych i polerowanych ręcznie.

Panel krosowy okablowania szkieletowego
Należy zastosować panele o wysokości 1U o konstrukcji umożliwiającej montaż w szafie z rozstawem szyn mocujących 19” oraz montaż adapterów światłowodowych LC typu duplex.
Ze względu na niezawodność połączeń światłowodowych oraz jego serwisowanie wymaga się aby:

- Budowa i wyposażenie panela zapewniały zabezpieczenie interfejsów światłowodowych przed kurzem, tj. mają być stosowane zatyczki do adapterów;
- Panel posiadał przepusty lub inne wyposażanie zapewniające trwałe mocowanie kabla światłowodowego na obudowie panela;
- Panel ma posiadać odpowiednie elementy służące do prowadzenia oraz składowania zapasu włókien światłowodowych (krzyżak zapasu włókien, przepusty kablowe);
- Panel ma mieć konstrukcję szufladową, tj. wysuwaną i wyjmowaną tacę na której jest mocowany kabel;

Okablowanie telefoniczne

Połączenie pomiędzy Punktami Dystrybucyjnymi znajdującymi się w pomieszczeniach serwerowni ma być zrealizowane za pomocą kabla telefonicznego U/UTP kat.3 50 parowego. W każdej szafie

dystrybucyjnej zaplanowano wykorzystanie systemu okablowania poziomego oraz paneli telefonicznych. Połączenie dwóch krosownic sygnałów daje rozwiązanie, które realizuje potrzebę skierowania sygnału telefonicznego do odpowiedniego gniazda końcowego przez proste połączenie odpowiednich portów obydwu paneli kablem krosowym. Panel telefoniczny – krosownica telefoniczna z interfejsem RJ45 (50 portów). Każdy panel telefoniczny ma mieć wysokość montażową 1U i zawierać zintegrowaną prowadnicę, umożliwiającą przymocowanie kabli mających zakończenie na panelu.

Dodatkowo do Punktu Dystrybucyjnego PPD1 (pomieszczenie 26) doprowadzony zostanie kabel wieloparowy z budynku Wydziału Inżynierii Elektrycznej i Komputerowej.

Punkty dystrybucyjne

Szafy dystrybucyjne
W szafach dystrybucyjnych należy zainstalować osprzęt połączeniowy oraz sprzęt aktywny.
Szafy mają posiadać stopień ochrony przynajmniej IP20 zgodnie z PN 92/E-08106 /EN 60 529 / IEC 529.

Uwaga
Lokalizacja szaf w budynku została pokazana na podkładach dołączonych do projektu. Sprzęt należy instalować zgodnie z rozmieszczeniem zaproponowanym na przykładowym rysunku dołączonym do projektu. Okablowanie poziome oraz szkieletowe należy wprowadzać do szafy od dołu, przez przepust szczotkowy umieszczony w cokole lub od góry poprzez otwór powstały przez wyciągnięcie dekla maskującego. W określonych przypadkach należy zbudować trasę kablową tak, aby kable nie były narażone na uszkodzenia wynikające z długotrwałych naprężeń.

W szafach bezwzględnie należy zostawiać zapas instalacyjny kabla.

Wymagania dla szaf
- Wysokość 24U, szerokość 800mm oraz głębokość 1000 mm;
- Sześć pionowych profili / słupów montażowych o rozstawie 19”;
- Drzwi przednie jednoskrzydłowe perforowane i perforowane po bokach z możliwością montażu prawo- i lewostronnego, z zamkiem i klamką;
- Ściany boczne i tylna zdejmowane;
- Perforacja u dołu szafy na wszystkich ścianach;
- 4 „belki poziome” mocowane do zewnętrznego stelaża szafy po 2 z każdej strony przeznaczone do mocowania kabli skrętkowych, z możliwością instalacji dodatkowych belek;
- Wszystkie elementy rozłączne tj. drzwi, ściany boczne itd. mają posiadać linki uziemiające;
- W dachu i podstawie otwory pod zainstalowanie paneli wentylacyjnych/zaślepek z włókniną oraz otwory umożliwiające wprowadzenie kabli liniowych od góry;
- Dół szafy wypełniony panelami zaślepiającymi otwory do wprowadzenia kabli od dołu;
- Otwór o wysokości min. 3U i szerokości min 450mm znajdujące się w dolnej części tylnej ściany szafy;
- Szafa ma posiadać nóżki regulowane lub możliwość zastosowania kół jezdnych;
- Szafa musi być wypoziomowana.

Organizacja połączeń kablowych dla szaf
- Komfortowy dostępu do każdego łącza tak, aby mieć kontrolę nad wszystkimi elementami całego pasywnego systemu okablowania;
- Zachowanie ułożenia kabli podczas normalnego użytkowania oraz w trakcie reorganizacji;
- Minimalny promień zagięcia zainstalowanych kabli połączeniowych (miedzianych). Redukcja naprężenia kabli i ich zagęszczenia oraz lepsze zarządzanie kablami z uwzględnieniem prowadzenia kabli krosowych (ograniczenie stosowania wieszaków i organizatorów poziomych które zabierają wysokość montażową „U” w szafie);
- Podniesienie pojemności i gęstości połączeń w punkcie dystrybucyjnym poprzez zastosowanie prowadnic przednich otwieranych i zamykanych na zamek gumowy o wysokościach 1U, 4U, (w zależności od potrzeb).

Uwaga: Przed montażem paneli krosowych wraz z prowadnicami przednimi należy sprawdzić czy do pełnego zamknięcia drzwi szafy, nie jest konieczne cofnięcie stelaży montażowych 19”.

Urządzenia aktywne

Zasadniczym celem zadania jest stworzenie spójnego systemu infrastruktury informatycznej będą szafy wyposażona w.

Wyposażenie szafy (PD) powinno składać się będzie z:
- 2 przełączników 24 portowych,
- 1 przełącznika 24 portowego z POE+,
- 3 panelów uniwersalnych 24 port.,
- 1 panel światłowodowy LC 24 port. OM3
- listwa zasilająca
- wentylator

Aby zagwarantować pełną kompatybilność całego systemu wszystkie jego komponenty muszą pochodzić od jednego producenta. Zapewni to jeden punkt zgłaszanie ewentualnych usterek bądź problemów konfiguracyjnych oraz spójne warunku świadczenia gwarancji oraz wsparcia serwisowego.

W/w przełączniki muszą być dostosowane do inteligentnego zarządzania indywidualnymi połączeniami użytkowników, urządzeń i aplikacji, jak również do dostarczenia widoczności i zarządzania dla rozwiązywania problemów z połączeniami, określenia położenia urządzeń i zapewnienia ochrony danych.

W każdym z punktów dystrybucyjnych (PD) przełączniki powinny być połączone w stos, aby uprościć ich konfigurację oraz zoptymalizować zarządzanie nimi. Ze względu na dużą ilość przesyłanych danych i wymaganą dużą wydajność, przepustowość przełącznika w stosie powinna wynosić minimum 160 Gbps. Zapewni to w płynność przesyłanych danych oraz zminimalizuje ryzyko wystąpienia wąskich gardeł.
Połącznie pomiędzy PD ma zostać zrealizowane za pomocą redundantnych łączy światłowodowych z przepustowością minimum 160Gbps.

Należy wykonać sieć strukturalną w taki sposób, aby mogła podołać wszelkim wyzwaniom związanym z współczesnym bezpieczeństwem urządzeń i użytkowników. Powinno to zostać zapewnione poprzez możliwość wdrożenia nowoczesnych standardów bezpieczeństwa i widoczności w sieci zarówno urządzeń, jak i użytkowników znajdujących się w niej wraz z możliwością egzekwowania bezpiecznego dostępu do infrastruktury dla użytkowników nie będących na stałe podłączonych do infrastruktury (dostęp gościnny).
Ponadto system powinien zarządzać wszystkimi urządzeniami (LAN/WLAN) za pomocą jednej aplikacji co znacząco usprawni działanie działu IT.

Zestawienie ilościowe urządzeń aktywnych sieci LAN

Lp.	Ilość szt.	
Szafy PD (11 kpl)		
1.	2x11=**22**szt.	Przełącznik 24 portowy
2.	1x11=**11**szt.	Przełącznik 24 portowy z PoE
3.	3x11=**33**szt.	Kable połączeniowe stack
4.	6x11=**66**szt.	Wkładki SFP+ SR 10Gbs LC MMF
5.	3x11=**33**szt.	Wkładki SFP+ SR 10Gbs LC SMF
6.	3x11=**33**szt.	Panel uniwersalny 24 portowy
7.	1x11=**11**szt.	Panel światłowodowy LC 24 portowy
Urządzenia WLAN		
8.	1	Kontroler sieci WLAN wraz z odpowiednią ilością licencji
9.	11	Wewnętrzne Access Point 802.11abgn/ac Wave 2, 4x4:4 MIMO
Aplikacje do zarządzania i bezpieczeństwa		
10.	1	System zarządzania urządzeniami sieciowymi
11.	1	System kontroli dostępu do sieci – Network Access Control

Ogólna charakterystyka i wymagania techniczne dla urządzeń aktywnych sieci

Zaprojektowano lokalne punkty dystrybucyjne (PD), które połączone są ze sobą za pomocą linków światłowodowych.

Przy doborze urządzeń zastosowano następujące wytyczne:

-do przełączników w PD podłączone zostaną urządzenia oraz punkty dostępowe obsługujące technologię 802.11ac, które z racji przesyłania dużej ilości danych wymagają zapewnienia odpowiednio wydajnych przełączników;

-połączenia pomiędzy PD – z uwagi na podłączenie dużej ilości urządzeń przesyłających mnóstwo danych oraz spełniających najnowsze standardy, bardzo wydajnych punktów dostępowych, zapewniono odpowiednią przepustowość pomiędzy PD – połączenie pomiędzy nimi winno wynosić minimum 160Gbps;

-przełączniki oraz punkty dostępowe muszą zapewniać skuteczną ochronę sieci przed atakami i innymi zagrożeniami, dlatego zdefiniowane przez Administratorów za pomocą systemu zarządzania polityki bezpieczeństwa organizacji powinny być egzekwowane również na tych urządzeniach. Dodatkowo, aby ułatwić konfigurację oraz zwiększyć bezpieczeństwo, polityki bezpieczeństwa organizacji powinny być tworzone z jednego panelu administracyjnego zarówno dla sieci przewodowej LAN, jak i bezprzewodowej WLAN - zwiększy to elastyczność konfiguracji oraz sprawi, że diagnostyka zagrożeń w sieci stanie się bardziej skuteczna.

-punkty dostępowe muszą spełniać najnowsze standardy związane z wydajnością, w tym technologię 802.11ac Wave 2 oraz technologię MIMO, a także bezpieczeństwem sieciowym

-system sieci bezprzewodowej WLAN powinien oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych, muszą być dostępne zarówno funkcje wykrywania, raportowania, jak i automatycznego zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom WLAN usługi transmisji danych

-systemem kontroli dostępu objęci muszą zostać wszyscy użytkownicy sieci przewodowej, jak również sieci bezprzewodowej. Sieć bezprzewodowa musi być obsługiwana analogicznie jak przewodowa, gwarantując co najmniej ten sam poziom bezpieczeństwa i zarządzania.

-system zarządzania powinien udostępniać narzędzia graficznej prezentacji urządzeń sieciowych (dedykowana aplikacja lub interfejs przeglądarkowy), oraz mieć możliwość lokacji systemów końcowych podłączonych do sieci, zarówno przewodowej LAN, jak i bezprzewodowej WLAN (lokacja oparta o triangulację z podglądem przemieszczania się terminala w czasie) na zaimportowanych planach budynków Zamawiającego.

Wymagania ogólne dla systemu zarządzania siecią

System zarządzania siecią musi umożliwiać objęcie swoim działaniem wszystkich urządzeń (LAN/WLAN) dostarczanych w ramach postępowania. Musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.

Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 5 lat.

Zamawiający określa wymagania minimalne dla systemu zarządzania siecią:

Funkcjonalność

-Musi umożliwiać zbieranie statystyk co najmniej z wykorzystaniem SNMP lub RMON.
-Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji
-Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci (LAN/WLAN)
-Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN
-Musi udostępniać narzędzia automatycznej identyfikacji urządzeń instalowanych w sieci
-Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II
-Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent
-Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć
-Musi udostępniać narzędzia graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia
-Musi mieć możliwość lokacji systemów końcowych podłączonych do sieci bezprzewodowej WLAN opartej o triangulację z podglądem przemieszczania się terminala w czasie
-Musi mieć możliwość dodawanie własnych planów pięter, wyświetlanie symulacji pokrycia zasięgiem sieci bezprzewodowej z możliwością podglądu wykorzystanych kanałów 802.11

Architektura

-System musi umożliwiać w momencie dostawy zarządzanie minimum 5 urządzeniami sieciowymi rozumianymi jako adres IP (przełącznik/stos/kontroler WLAN/brama NAC itp.) i 50 punktami dostępowymi, z opcją rozbudowy do minimum 20 adresów IP i 200 AP poprzez zakup licencji.
-Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej LAN, jak i bezprzewodowej WLAN będącymi przedmiotem tego postępowania
-Musi posiadać dedykowane API pozwalające na integrację systemu zarządzania z urządzeniami innych producentów np. urządzeniem Firewall
-Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych profili bezpieczeństwa na urządzeniach sieci przewodowej i bezprzewodowej

Bezpieczeństwo

-Musi mieć możliwość definiowania profili bezpieczeństwa w oparciu o następujące parametry:
a. ograniczanie poziomu pasma,
b. ograniczanie liczby nowych połączeń sieciowych,
c. ustalanie pierwszeństwa ruchu w oparciu o mechanizmy QoS warstw 2 i 3,
d. nadawanie tagów pakietom, celem poddawania kwarantannie poszczególnych portów lub sieci VLAN i/lub uruchamianie wcześniej zdefiniowanych działań

-Musi umożliwiać powiązanie profilu bezpieczeństwa w jeden funkcjonalny zestaw reguł obejmujący:
a. użytkowników,
b. protokoły,
c. sieci VLAN,
d. porty

-Musi posiadać możliwość wdrażania profili bezpieczeństwa w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której profile zostaną rozesłane do wszystkich urządzeń
-Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone profile bezpieczeństwa, włączając w to zdolność do powiadamiania systemu FireWall o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform)

-Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji
-Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności musi obsługiwać uwierzytelnianie oparte o 802.1X, RADIUS oraz MAC
-Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p
-Musi umożliwiać przypisywanie reguł filtrowania warstw L2-L4 oraz QoS na w warstwach L2-L4 (DSCP i 802.1p) dla każdego użytkownika na porcie przełącznika i grupie portów.

Narzędzia administracyjne

-Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB
-Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych profili bezpieczeństwa w razie potrzeby
-Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego
-Musi udostępniać narzędzie dla automatyzacji uaktualniania oprogramowania i zmian konfiguracyjnych w urządzeniach sieciowych.
-Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie
-Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń
-Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania
-Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury
System zarządzania siecią musi posiadać widok danych uzyskanych przez system kontroli dostępu - NAC.
-Musi umożliwiać diagnozowanie problemów sieciowych i wydajności oraz widzianych w sieci przepływów i aplikacji stanowiąc interfejs gromadzący dane o warstwie aplikacji z systemu analityki opartej o protokół NetFlow.

Raportowanie

-Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych widoków sieci
-Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID)
-Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia
-Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń
-Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych

Network Access Control (NAC).

System kontroli dostępu musi umożliwiać objęcie swoim działaniem wszystkich urządzeń (LAN/WLAN) dostarczanych w ramach postępowania. Musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji.
Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 5 lat.

Zamawiający określa wymagania minimalne dla systemu kontroli dostępu:
Funkcjonalność

-System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i do sieci bezprzewodowej WLAN z wykorzystaniem standardu 802.1X, adresu MAC urządzenia i formularza webowego.
-System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) 802.1X opartych o złożone i wielowarunkowe reguły profili bezpieczeństwa.
-System powinien aktywnie uniemożliwiać dostęp do sieci nieautoryzowanych użytkowników.

-System powinien współpracować z rozwiązaniem Microsoft NAP (Network Access Protection).
-Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
-Musi zapewniać możliwość powiadamiania poprzez Syslog oraz pocztę elektroniczną o sytuacjach krytycznych.
-System musi umożliwiać wysyłanie powiadomień mailowych z wykorzystaniem protokołu SMTP.
-System musi posiadać wewnętrzną bazę użytkowników. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych przy pomocy interfejsu programistycznego RESTful API lub równoważne.
-Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania i autoryzacji podłączanych systemów końcowych.
-Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP.
-Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

Profilowanie urządzeń

-System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMP.
-System musi umożliwiać dodawanie rozpoznanych urządzeń do grupy.
-System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. Musi istnieć możliwość przyznania określonego dostępu na podstawie informacji o urządzeniu dla co najmniej 500 urządzeń.
-System musi rozpoznawać co najmniej następujące rodzaje urządzeń:

a. urządzenia z systemem Android,
b. Apple iPad, Apple iPhone, Apple iPod,
c. drukarki,
d. telefony IP,
e. stacja robocza z systemem Microsoft Windows,
f. stacja robocza z systemem MAC OS,
g. stacja robocza z systemem Linux.

Architektura

1. System kontroli dostępu musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych i/lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu. W momencie dostawy na co najmniej dwóch serwerach fizycznych i/lub wirtualnych.
-System musi umożliwiać uruchomienie wszystkich elementów funkcjonalnych na jednym fizycznym lub wirtualnym serwerze, Zamawiający dopuszcza rozwiązanie gdzie zarządzanie i monitorowanie systemu zostanie zainstalowane na dedykowanej do tego maszynie wirtualnej.
-System musi umożliwiać realizację wysokiej dostępności poszczególnych elementów funkcjonalnych typu 1:1 lub N+1.
-System kontroli dostępu (NAC) musi być rozwiązaniem typu out-of-band, które może być zarządzane przez jedną centralną aplikację. Wszystkie urządzenia typu NAC Gateway powinny być zarządzane i monitorowane z jednej, centralnej konsoli.
-System w chwili uruchomienia musi umożliwiać obsługę co najmniej 500 urządzeń równocześnie podłączonych do sieci lokalnej LAN lub sieci bezprzewodowej WLAN.
-Rozwiązanie powinno wspierać możliwość rozbudowy do min. 2000 sesji autoryzacyjnych poprzez dodanie do systemu odpowiednich licencji (bez potrzeby rozbudowy systemu o dodatkowe serwery fizyczne lub wirtualne).
-Na cele przyszłej rozbudowy wymaga się, aby system umożliwiał rozbudowę licencyjną o funkcjonalność skanowania systemów końcowych (z wykorzystaniem oprogramowania typu agent i bez niego) dla potrzeb procesów oceniania, kwarantanny i korygowania podłączanych systemów końcowych
-Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 5 lat.

Zarządzanie systemem

-System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową lub dedykowaną aplikację.
-System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników oraz zewnętrzne repozytorium użytkowników.
-System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania.
-System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych.

Zarządzanie dostępem gościnnym

-System musi umożliwiać realizację dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN przy pomocy portalu webowego. Formularz musi obsługiwać co najmniej następujące przeglądarki: Microsoft IE, Mozilla Firefox, Safari.
-Rozwiązanie musi posiadać funkcję portalu rejestracyjnego (captive portal), aby zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT, wraz z możliwością sponsorowania dostępu takie jak sponsorowanie email wraz z portalem dla sponsorów służący do zatwierdzania rejestracji gości.

<u>Wymagania szczegółowe dla urządzeń typu Przełącznik 24 portowy</u>

Wymagania podstawowe

1. Przełącznik posiadający minimum następującą liczbę i rodzaj portów:
   a. 24 portów 10/100/1000BASE-T wspierających IEEE 802.3az (Energy Efficient Ethernet)
   b. 4 porty 1/10 GBASE-X SFP+
   c. 2 porty 40 GBASE-X QSFP+
   d. Port szeregowy oraz port do zarządzania przełącznikiem typu out-of-band
   e. Gniazdo USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika
2. Wysokość urządzenia 1U
3. Przełącznik w chwili dostawy musi posiadać dwa wbudowane, redundantne zasilacze AC 230V, ale dostępne do zamontowania w przełączniku muszą być również zasilacze na prąd stały DC.
4. Przełącznik musi posiadać wymienny zestaw wentylatorów zapewniających chłodzenie przód-tył, tył-przód (wymagane dostarczenie przód-tył).
5. Zarówno zasilacze jak i wentylatory muszą mieć możliwość wymiany podczas pracy urządzenia (hot-swap),
6. Nieblokująca architektura o wydajności przełączania min. 335 Gb/s
7. Szybkość przełączania min. 250 Milionów pakietów na sekundę
8. Średnie opóźnienia na portach maksimum 4 µs (pakiety 64 bitowe)
9. Możliwość łączenia do 8 przełączników w stos z przepustowością minimum 160Gbps. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych
10. Tablica MAC adresów min. 96k
11. Pamięć operacyjna: min. 1GB pamięci DRAM
12. Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 4MB
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
14. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
15. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
16. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
17. Możliwość monitorowania zajętości CPU
18. Obsługa IP Flow Information Export (IPFIX)
19. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla L2 VPN i L3 VPN (np. poprzez dodatkową licencję)

Obsługa Routingu IPv4

20. Pojemność tabeli routingu min. 12000 wpisów
21. Routing statyczny
22. Obsługa routingu dynamicznego IPv4

a. RIPv1/v2
b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
c. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla BGPv4 (np. poprzez dodatkową licencję)
d. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla IS-IS (np. poprzez dodatkową licencję)
e. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla MPLS, VPLS i H-VPLS (np. poprzez dodatkową licencję)

23. Policy Based Routing dla IPv4

Obsługa Routingu IPv6

24. Pojemność tabeli routingu min. 6000 wpisów
25. Routing statyczny
26. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję)
    c. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla MBGP (np. poprzez dodatkową licencję)
    d. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla IS-IS (np. poprzez dodatkową licencję)
27. Policy Based Routing dla IPv6

Obsługa Multicastów

28. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
29. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
30. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla PIM-SM, PIM-DM, PIM-SSM, MSDP i Anycast RP (np. poprzez dodatkową licencję)

Bezpieczeństwo

31. Obsługa Network Login
    a. IEEE 802.1x
    b. Web-based Network Login
    c. MAC based Network Login
32. Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants)
33. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
34. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
35. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
36. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
37. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
38. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
    d. możliwość wyłączenia MAC learning
39. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection

c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

40. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
41. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
42. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

Bezpieczeństwo sieciowe

43. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
44. Obsługa STP, RSTP, MSTP, PVST+
45. Obsługa EAPS (RFC 3619) oraz G.8032
46. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 16 portów
47. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

48. Zarządzanie przez SNMP v1/v2/v3
49. Obsługa SYSLOG z możliwością definiowania wielu serwerów
50. Sprzętowa obsługa sFlow
51. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

Inne

52. Wsparcie dla OpenFlow
53. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
54. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

<u>Wymagania szczegółowe dla urządzeń typu Przełącznik 24 portowy z POE</u>

Wszystkie zapisy dotyczące urządzeń typu Przełącznik 24 portowy i dodatkowo:

1. Przełącznik musi posiadać wbudowane redundantne zasilacze zapewniające budżet mocy POE na poziomie 1440W
2. Musi gwarantować dostarczenie 30W mocy równocześnie na wszystkich 48 portach 10/100/1000BASE-T oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.

<u>Kontroler sieci WLAN</u>

Kontroler sieci WLAN musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 36 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji. W przypadku rozwiązania sprzętowego – wymiana uszkodzonego sprzętu musi zostać wykonana następnego dnia roboczego po zgłoszeniu awarii.

Architektura

1. Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 5 punktów dostępowych. Kontroler musi umożliwiać docelową rozbudowę do minimum 125 punktów dostępowych poprzez zakup dodatkowych licencji.
2. Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym tunelowanie ruchu z AP do kontrolera i lokalnego terminowania do sieci przewodowej na poziomie AP (mechanizmy te muszą być dostępne do skonfigurowania w obrębie tego samego kontrolera, per SSID)

Captive Portal

3. Kontroler sieci WLAN musi przekierowywać użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)
4. Musi posiadać zintegrowany (w kontrolerze), logicznie wydzielony portal dostępowy (Captive Portal), dowolnie konfigurowany przez administratora, z wykorzystaniem wbudowanych narzędzi edycyjnych

5. Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN z wykorzystaniem autentykacji 802.1x
6. Możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta
7. Captive Portal musi dawać dostęp Gościom do zasobów sieci Internet w dedykowanym VLAN-nie (Sieć Gości), nie dopuszczając Gości do zasobów wewnętrznych Zamawiającego (Intranet).
8. Możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
9. Możliwość profilowania użytkowników – co najmniej przydział: sieci VLAN, list kontroli dostępu (ACL), mechanizmów QoS, 802.1p, oraz ograniczanie pasma per użytkownik

Bezpieczeństwo

10. Musi obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o 802.1p
11. Musi umożliwiać automatyczną ochronę kryptograficzną (AES) ruchu pomiędzy punktem dostępowym, a Kontrolerem WLAN.
12. System musi obsługiwać kreowanie polityk bezpieczeństwa w obrębie jednego SSID (przypisywanie indywidualnych parametrów obsługi ruchu poszczególnym użytkownikom VLAN, QoS, ACL, ograniczenie pasma), bez konieczności segmentacji przez dedykowane SSID. Rozwiązanie powinno w ten sposób zmniejszyć konieczność uruchomienia wielu SSID do realizowania różnych funkcjonalności (minimalizacja utylizacji pasma radiowego)

Zarządzanie

13. Musi umożliwiać zarządzanie poprzez ssh, https, snmpv3 oraz dedykowaną aplikację do zarządzania.
14. Wraz z rozwiązaniem wymaga się dostarczenia rozwiązania do zarządzania i monitorowania kilkoma kontrolerami sieci WLAN – centralny interfejs graficzny.
15. Musi umożliwiać optymalizację wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany).
16. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie, bez interwencji użytkownika.
17. System zarządzania łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
18. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11ag oraz 802.11n. (rozwiązanie Airtime fairness, np. ClientLink lub równoważne). System zarządzania łącznością radiową – typu RRM (Radio Resource Management) - RF Management musi wspierać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control) oraz obsługa Dynamic Frequency Selection (DFS).
19. Kontroler musi zapewniać zarządzanie oparte o graficzny interfejs użytkownika, lokalny uruchomiony na kontrolerze WLAN.
20. Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika – dla celów Captive Portal.

System WIPS/WIDS

21. Kontroler musi oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych co oznacza, że muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom sieci bezprzewodowej usługi transmisji danych.
22. Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS, z kilku kontrolerów WLAN jednocześnie.

Inne

23. System musi posiadać certyfikat 802.11n WiFi dla kompatybilności w sieciach WLAN.
24. Możliwość redundancji rozwiązania (N+1)

25. Kontroler WLAN powinien współpracować z punktami dostępowymi, zcentralizowanym systemem zarządzania siecią LAN/WLAN będącymi przedmiotem niniejszego postępowania

Punkt dostępowy sieci WLAN

Pasma robocze

1. Punkty dostępowe muszą posiadać min. 2 moduły radiowe i obsługiwać równolegle dwa pasma częstotliwości: 802.11ac/a/n (5 GHz) i 802.11b/g/n (2,4 GHz).

Interfejsy fizyczne

2. Punkty dostępowe muszą być wyposażone w 2 porty 10/100/1000 BASE-T RJ-45

Standardy sieciowe

3. Zgodność z DFS2 (Dynamic Frequency Selection)
4. Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence,
5. Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC)
6. Obsługa do 16 SSID (8 na częstotliwość radiową),
7. Obsługa minimum 450 użytkowników jednocześnie,
8. RADIUS Authentication & Accounting,
9. Płynny roaming pomiędzy podsieciami IP i pomiędzy wieloma kontrolerami,
10. Wsparcie dla protokołu IEEE 802.1p prioritization, IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP,
11. Wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS,
12. Mechanizmy: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2,
13. Mechanizm izolacji klientów na poziomie L2,
14. Mechanizmy IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP),
15. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g, 802.11n oraz 802.11ac.

Anteny

16. Muszą posiadać min. 8 anten wewnętrznych.

Tryby pracy

17. Tryb działania radio WLAN: Client access, Local mesh, Packet capture, WDS,
18. Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza,
19. Obsługa technologii 802.11ac Wave 2 i praca w technice transmisji wieloantenowej MIMO 4x4:4
20. Obsługa 802.11n z przepływnością do co najmniej 800Mbps i 802.11ac z przepływnością do co najmniej 1,7Gbps
21. Jednoczesna obsługa ruchu tunelowanego i mostowanego,
22. Wszystkie punkty dostępowe muszą mieć możliwość pracy w formie sensorów sieci.
23. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera.

Funkcje zarządzania

24. Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF (Radio Frequency) Management niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu.
25. Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału
26. Możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej,

Bezpieczeństwo

27. Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane przy pomocy technologii AES minimum 128 bit,
28. Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń,
29. Obsługa standardów uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x,
30. Punkt dostępowy musi wspierać szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera,
31. Możliwość pracy w architekturze bezpieczeństwa opartej na rolach, zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, aplikowane względem użytkownika i aplikacji,
32. Funkcje egzekwowania przypisanych ról i ograniczania przepustowości muszą być osiągalne na poziomie punktu dostępowego,
33. Przypisywanie ról klientom musi odbywać się bez konieczności segmentacji przez dedykowane SSID.

WIPS

34. Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS,
35. Punkt dostępowy musi oferować funkcje WIPS/WIDS, działające bez wpływu na poziom świadczonych usług sieciowych, muszą być dostępne zarówno funkcje wykrywania, jak i zmniejszania zagrożeń, gdy punkt dostępowy świadczy innym klientom Wi-FI usługi transmisji danych,
36. Kategorie zagrożeń WIDS/WIPS, które należy wykrywać i raportować:
    a. Analizy widma – zakłócenia pochodzące ze źródeł innych niż WiFi,
    b. Aktywna obserwacja
    c. Atak Packet Injection (wtryskiwanie pakietów) – atakujący wprowadza swoje pakiety w transmisję danych pomiędzy dwoma urządzeniami, dzięki temu urządzenia traktują te złośliwe pakiety, tak jakby pochodziły z autoryzowanego urządzenia,
    d. Atak Denial of Service (skierowany na stację końcową) – zalewanie stacji końcowej komunikatami uwierzytelniania lub anulowania uwierzytelniania
37. Kategorie zagrożeń WIDS/WIPS, które należy wykrywać, raportować i zmniejszać:
    a. Honeypot
    b. Wrogi punkt dostępu (ang. Rogue AP) – punkt dostępowy podłączony do autoryzowanej sieci, pomimo braku upoważnienia do tego,
    c. Fałszywy punkt dostępu (ang. Spoofing AP) – urządzenie posługujące się BSSID (adres MAC) w rzeczywistości należącym do innego, autoryzowanego punktu dostępowego,
    d. Aktywne łamanie szyfrowania (ang. Active Encryption Cracking) – atak typu chop-chop i fragmentaryczny,
    e. Atak Denial of Service (skierowany na punkt dostępu)

Wymagania gwarancyjne dla sieci strukturalnej

Gwarancja na system okablowania strukturalnego ma spełniać poniższe warunki:

- gwarancja ma być jednolitą bezpłatną usługą serwisową świadczoną przez producenta okablowania (tj. bez ponoszenia jakichkolwiek kosztów w przyszłości związanych z przeglądami, serwisowaniem czy innymi pracami związanymi z naprawą i powtórną instalacją wadliwych elementów);
- ma obejmować całość okablowania miedzianego oraz telefonicznego wraz z kablami krosowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda RJ45, adaptery światłowodowe, pigtaile, wieszaki, szafy itp.;
- minimalny czas trwania 25 lat ma być udzielany na oficjalnych warunkach, ogólnie znanych i opublikowanych;
- gwarancja ma być udzielona przez producenta okablowania bezpośrednio Inwestorowi/Użytkownikowi.

Obowiązki producenta okablowania
Producent systemu okablowania w swojej gwarancji systemowej ma zapewniać:

- gwarancję materiałową (w przypadku wykrycia wady lub usterki fabrycznej, produkty wadliwe zostaną naprawione bądź wymienione);
- gwarancję parametrów łącza/kanału (parametry łączy stałych bądź kanałów będą przewyższać wskazaną klasę okablowania w ciągu trwania całego okresu gwarancyjnego);
- gwarancję aplikacji (protokoły sieciowe współczesne i stworzone w przyszłości, które zaprojektowane były lub będą dla systemów okablowania danej klasy będą działać poprawnie w ciągu całego okresu gwarancyjnego.

Instalacja ma być nadzorowana w trakcie budowy przez inżynierów ze strony producenta.
Zbudowana infrastruktura kablowa ma być ostatecznie fizycznie sprawdzona przez producenta przed wystawieniem certyfikatu gwarancyjnego pod kątem technicznym, funkcjonalnym oraz estetycznym. Użytkownik/Inwestor musi otrzymać raport, potwierdzający sprawdzenie instalacji oraz ma prawo uczestniczyć w procesie jej weryfikacji.

Obowiązki instalatora
W celu ujawnienia procedury, jak również zapoznania Użytkownika/Inwestora z prawami, obowiązkami i ograniczeniami gwarancji, wykonawca ma posiadać aktualną umowę zawartą bezpośrednio z producentem okablowania regulującą uprawnienia, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi.

Wykonawca przed rozpoczęciem prac związanych z zakresem okablowania strukturalnego ma dostarczyć Zamawiającemu potwierdzenie faktu rozpoczęcia budowy instalacji wystawione przez producenta.

Wykonawca ma posiadać dyplomy ukończenia kursów kwalifikacyjnych, przez zatrudnionych pracowników w zakresie:

- instalacji;
- pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń;
- projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania;

W przypadku jeśli wykonawca na etapie oferty korzysta z uprawnień osób trzecich, dokumenty te muszą uczestniczyć w nadzorze zadania lub być na każde wezwanie na etapie realizacji.

Powyższe kursy mają znajdywać się w oficjalnej ofercie producenta.

Dokumenty mają być przedstawione Zamawiającemu przed podpisaniem umowy.

Dostarczone elementy pasywne (kable miedziane i światłowodowe, panele krosowe, kable krosowe, panele telefoniczne, szafy wraz z wyposażeniem) składające się na system okablowania strukturalnego muszą być oznaczone nazwą lub znakiem firmowym tego samego producenta okablowania i pochodzić z jednolitej oferty rynkowej, będącej kompletnym systemem w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania gwarancji w/w producenta.

Administracja i dokumentacja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, zarówno od strony gniazda PL, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach telekomunikacyjnych w obszarach roboczych oraz na panelach krosowych.

Konwencja oznaczeń okablowania poziomego:
X / **Y**/ **C**/
gdzie:
X – identyfikator szafy,
Y – numer panela krosowego,
C – numer portu w panelu.

Odbiór i pomiary sieci

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest spełnienie wszystkich poniższych warunków:

- wykonanie instalacji w sposób prawidłowy, zgodny ze sztuką, wymaganiami i obowiązującymi normami oraz z zachowaniem estetyki prac;
- wykonanie kompletu pomiarów;
- opracowanie i przekazanie dokumentacji powykonawczej Inwestorowi;
- uzyskanie gwarancji systemowej producenta okablowania.

Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346 A1+A2. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą ISO/IEC 14763-3:2014. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada analizy parametrów, według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualną kalibrację/legalizację (tj. certyfikat potwierdzający dokładność jego wskazań, wydany przez serwis producenta).

Na raportach pomiarowych muszą się znaleźć informacja dotyczące ustawień sprzętu pomiarowego (norma, typ kabla itp.), nazwa mierzonego łącza oraz wyniki pomiarów wraz z zapasami w stosunku do limitów z norm. Każdy wynik musi być jednoznacznie opisany jako poprawny lub niepoprawny.

Pomiary okablowania miedzianego

- Analizator okablowania wykorzystany do pomiarów sieci miedzianej musi charakteryzować się przynajmniej V klasą dokładności dla klasy F_A wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX5000);
- Pomiary dla systemu należy wykonać w konfiguracji pomiarowej kanału (Channel) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego;
- Pomiary sieci miedzianej należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1:
  - Klasa F_A dla wszystkich torów transmisyjnych.
- Protokół pomiarowy każdego toru transmisyjnego poziomego miedzianego ma zawierać:
  - mapę połączeń;
  - długość połączeń i rezystancje par;
  - opóźnienie propagacji oraz różnicę opóźnień propagacji;
  - tłumienie;
  - NEXT i PS NEXT w dwóch kierunkach;
  - ACR-F i PS ACR-F w dwóch kierunkach;
  - ACR-N i PS ACR-N w dwóch kierunkach;
  - RL w dwóch kierunkach.

Pomiary okablowania światłowodowego

- Tłumienie światłowodowego toru transmisyjnego ma być wyznaczone za pomocą reflektometru;
- Przy pomiarze reflektometrem należy użyć rozbiegówki oraz dobiegówki w celu określenia jakości wszystkich złączy;
- Kompletny pomiar każdego dupleksowego toru transmisyjnego powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien (chyba że typ złącza uniemożliwia taką procedurę):
  - od punktu A do punktu B w oknie 850nm i 1300nm (MM);
  - od punktu B do punktu A w oknie 850nm i 1300nm (MM);
  - od punktu A do punktu B w oknie 1310nm i 1550nm (SM);
  - od punktu B do punktu A w oknie 1310nm i 1550nm (SM).

Zawartość dokumentacji powykonawczej

Po zakończeniu prac instalatorskich należy wykonać i przekazać Użytkownikowi końcowemu dokumentacje powykonawczą, która ma zawierać:

- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli,
- Rysunki z oznaczeniami poszczególnych szaf, paneli krosowych i portów,

- Lokalizację przebić przez ściany i podłogi.

Uwagi końcowe

Trasy prowadzenia okablowania poziomego zostały skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną oraz ogólną instalacją elektryczną, instalacją centralnego ogrzewania, wody, kanalizacji, itp., Jeżeli w trakcie realizacji nastąpią zmiany prowadzenia tras instalacji okablowania oraz lokalizacji Punktów Logicznych lub wystąpią konflikty z innymi instalacjami, należy ustalić poprawione rozprowadzenie tras kablowych w porozumieniu z Projektantem.
Należy uziemić zgodnie obowiązującymi przepisami wszystkie metalowe korytka, drabinki kablowe, szafy kablowe wraz z osprzętem oraz inne urządzenia sieciowe, które zgodnie z instrukcją ich montażu tego wymagają.
Wszystkie materiały wprowadzone do robót muszą być nowe, nieużywane, najnowszych aktualnych wzorów.

Alternatywne propozycje

Uwaga: Zgodnie z zasadami zamówień publicznych można zastosować materiały i rozwiązania równoważne, to jest w żadnym stopniu nie obniżające standardu i nie zmieniające zasad oraz rozwiązań technicznych przyjętych w projekcie, a tym samym nie powodujące konieczności przeprojektowania jakichkolwiek elementów infrastruktury ani nie pozbawiające Użytkownika żadnych wydajności, funkcjonalności użyteczności opisanych lub wynikających z dokumentacji projektowej.

Jeżeli oferent zdecyduje się na zastosowanie rozwiązania alternatywnego, powinien do oferty dołączyć listę zamienionych materiałów, jak również wszelkie dokumenty pozwalającej Komisji Przetargowej ocenić zgodność z wymaganiami SIWZ i dokumentacji projektowej wraz z załącznikami.

Objaśnienia

PL = Punkt Logiczny

SFTP = kabel skrętkowy 4 parowy z indywidualnie ekranowanymi w postaci jednostronnie laminowanej folii parami transmisyjnymi i wspólnym ekranem wszystkich par w postaci siatki miedzianej, kat.7A, w powłoce zewnętrznej niepalnej LSFRZH

LSFRZH (ang. *Low Smog Flame Retardent Zero Halogen*) – osłona zewnętrzna kabla