TEMAT:	**PROJEKT MODERNIZACJI SIECI KOMPUTEROWEJ W BIURACH RZECZNIKA PRAW OBYWATELSKICH**
ADRES:	**BIURO RPO** **AL. SOLIDARNOŚCI 77** **00-090 WARSZAWA**
INWESTOR:	**BIURO RPO; AL. SOLIDARNOŚCI 77; 00-090 WARSZAWA**
STADIUM PROJEKTU:	**PROJEKT WYKONAWCZY**
DATA OPRACOWANIA:	**WRZESIEŃ 2018**

Spis treści

1. Spis rysunków

L.P	Tytuł rysunku	Nr Rys.
1	Ulica Długa rzut parteru część A	**01**
2	Ulica Długa rzut parteru część B	**02**
3	Ulica Długa rzut parteru część C	**03**
4	Ulica Długa rzut I piętra część A	**04**
5	Ulica Długa rzut I piętra część B	**05**
6	Ulica Długa rzut I piętra część C	**06**
7	Ulica Długa rzut II piętra część A	**07**
8	Ulica Długa rzut II piętra część B	**08**
9	Ulica Długa rzut II piętra część C	**09**
10	Ulica Długa rzut III piętra część A	**10**
11	Ulica Solidarności rzut Parteru	**11**
12	Ulica Solidarności rzut I Piętra	**12**
13	Ulica Solidarności rzut II Piętra	**13**
14	Ulica Solidarności rzut III Piętra	**14**
15	Ulica Solidarności rzut IV Piętra	**15**

2. Zakres projektu

Przedmiotem niniejszego opracowania jest projekt modernizacji sieci komputerowej w Biurach RPO mieszczących się w Warszawie, Katowicach, Gdańsku i Wrocławiu. Opracowanie to obejmuje budowę infrastruktury teletechnicznej i dostawę urządzeń sieciowy wraz z oprogramowaniem w Biurach RPO zlokalizowanych w Warszawie oraz dostawę urządzeń sieciowych dla Biur RPO zlokalizowanych w Katowicach, Gdańsku i Wrocławiu. Projekt opracowano zgodnie ze wskazówkami i zaleceniami Inwestora, z uwzględnieniem wymagań użytkownika co do elastyczności systemu, standardów nowoczesnych urządzeń do transmisji danych oraz zgodnymi ze Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

3. Podstawy opracowania

Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym są normy okablowania strukturalnego.

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+A2:2015 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości
- PN-EN 50174-2:2010/A1:2011+A2:2015 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków
- PN-EN 50174-3:2014 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków
- IEC 61935-1:2015 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards;

- PN-EN 50310:2016 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym

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

4. Wymagania ogólne

- W obu Biurach RPO w Warszawie należy dostarczyć po dwa, połączone ze sobą, przełączniki rdzeniowe. Prędkość połączenia pomiędzy przełącznikami 2x100Gb QSFP;
- Przełączniki rdzeniowe mają być wyposażone w 24 porty z możliwością zamontowania portów 10Gb GIBIC
- Wszystkie przełączniki dostępowe mają być w wersji PoE+;
- Każdy z przełączników dostępowych przeznaczony do instalacji w lokalizacjach Solidarności i Długa musi mieć możliwość zamontowania 2x10Gb GIBIC;
- W ramach dostawy przełączników należy dostarczyć oprogramowanie do zarządzania przełącznikami i kontrolowania urządzeń podłączanych do sieci oraz analizy ruchu w sieci;
- Dla uzyskania jednolitej gwarancji i poprawnego działania oprogramowania do zarządzania urządzeniami sieciowymi i kontrolą urządzeń, przełączniki rdzeniowe, przełączniki dostępowe, AP oraz oprogramowanie ma być tego samego producenta;
- Należy dostarczyć i zainstalować 10 x AP w pomieszczeniach Biura RPO zgodnie z ustaleniami z inwestorem na etapie realizacji;
- Podłączenie AP do infrastruktury sieciowej należy wykonać okablowaniem min KAT6A FFTP;
- Wszystkie elementy pasywne składające się na światłowodową część okablowania strukturalnego 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;

- Dla uzyskania pełnej kompatybilności i wysokiego bezpieczeństwa działania, blokady portów RJ45, USB, LC mają być tego samego producenta co pozostała część okablowania światłowodowego;
- Minimalne wymagania elementów miedzianego okablowania strukturalnego pod względem wydajności to Kategoria 6_A (komponenty)/ Klasa E_A (podstawowa wydajność całego systemu) i zapewnienie możliwości transmisji 10Gigabit Ethernet 802.3an;
- Światłowodowe okablowanie strukturalne w obu Biurach RPO zlokalizowanych w Warszawie należy wykonać w min kategorii OM3. Włókna światłowodowe należy zakończyć złączami LC.
- Główne punkty dystrybucyjny jak i pośrednie są zlokalizowane w zaznaczonym na rzutach pomieszczeniach, ewentualne zmiany lokalizacji punktów dystrybucyjnych mają być uwzględnione na etapie wykonawczym oraz zaznaczone w dokumentacji powykonawczej;
- Miedziane okablowanie ma być realizowane poprzez ekranowane moduły gniazd RJ45 kat. 6_A składające się z dwóch elementów, posiadających zacisk ekranu kabla (360^o);
- Do czasu przełączenia na nową sieć strukturalną, obie instalacje powinny być czynne, stąd demontaż okablowania musi odbywać być sukcesywnie po wykonaniu stosownych przełączeń na nową instalację;
- Okablowanie miedziane dla AP ma zapewnić poprawne działanie transmisji danych przy wykorzystaniu PoE+ zgodnie z IEEE 802.3at-2009 oraz w przyszłości 4PPoE zgodnie z IEEE 802.3bt. W związku z tym wymagane jest przeprowadzenie rozszerzonych testów certyfikujących okablowanie miedziane co opisano szczegółowo w dziale Odbiór i pomiary sieci;
- 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");
- W ramach realizacji inwestycji należy dostarczyć vouchery na szkolenia certyfikowane przez producenta dostarczonych urządzeń sieciowych i oprogramowania dla 4 administratorów (ważność voucher'ów - 6 miesięcy);

5. Instalacja teletechniczna (opis technologii)

5.1 Szkielet światłowodowy

5.1.1 Prowadzenie okablowania szkieletowego

Światłowodowe okablowanie zostanie rozprowadzone w dwóch Biurach RPO zlokalizowanych w Warszawie przy ulicy Al. Solidarności 77 oraz przy ulicy Długiej 23/25. Przy układaniu okablowania światłowodowego pomiędzy punktami dystrybucyjnymi należy wykorzystać: istniejące koryta kablowe, przebicia pomiędzy piętrami i przebicia pomiędzy pomieszczeniami. Jeżeli ze względów technicznych nie będzie możliwości ułożenia kabla światłowodowego należy ten fakt zgłosi do Inwestora i Projektanta w celu uzyskania zgody na inne ułożenia kabla światłowodowego.

5.1.2 Połączenia pomiędzy punktami dystrybucyjnymi

W ramach realizacji należy wykonać następujące połączenia światłowodowe między punktami dystrybucyjnymi:

- w Biurze RPO zlokalizowanym przy Al. Solidarności 77
    a. z GPD1(p.2.17) do PD1(korytarz) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
    b. z GPD1(p.2.17) do PD2(korytarz) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
    c. z GPD1(p.2.17) do PD3(korytarz) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
    d. z GPD1(p.2.17) do PD4(korytarz) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
    e. z GPD1(p.2.17) do PD Konferencyjna(p.1.18) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)

- w Biurze RPO zlokalizowanym przy ulicy Długiej 23/25
    a. z GPD2(p.110) do PD10A(p.10A) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)

b. z GPD2(p.110) do PD7(p.7) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
c. z GPD2(p.110) do PD130(p.130) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
d. z GPD2(p.110) do PD301(p.301) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
e. z GPD2(p.110) do PD236(p.236) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
f. z GPD2(p.110) do PD219(p.219) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)
g. z GPD2(p.110) do PD118C(p.118C) (kabel światłowodowy OM3, 12 włókien, zakończony z obu stron złączami LC; montaż w panelu światłowodowym 1U)

5.1.3 Wymagania techniczne i funkcjonalne dla elementów okablowania światłowodowego

Panel światłowodowy

W głównych punktach dystrybucyjnych GPD1 i GPD2 należy zastosować modularny panel światłowodowy o wysokości 1U z montażem w szafie 19" wyposażony w 12 uniwersalnych półek. Biorąc pod uwagę możliwość dalszej rozbudowy sieci oraz modernizacji kolejnych urządzeń aktywnych należy zastosować panel spełniający poniższe wymagania:

a. Pojemność panela 1U - 144 złącza LC simplex lub 72 złącza LC duplex w wersji spawanej lub dla kabli gotowych zakończonych złączami LC
b. Ze względu na możliwość migracji urządzeń aktywnych do wyższych prędkości panel światłowodowy musi mieć możliwość montażu różnych kaset w konfiguracjach 1xMPO(12)/4xLCduplex, 3xMPO(12)/12xLCduplex dla połączeń 40GB, 1xMPO(24)/12xLCduplex, 2xMPO(12)/2x6LCduplex – uniwersalne zastosowanie
c. Dostępne kategorie światłowodów dla kaset OM3/ OM4/ OS2
d. Panel 1U ma umożliwiać montaż dowolnej konfiguracji wysuwanych półek z możliwością uzyskania maksymalnie 72 zakończeń LCduplex w różnych konfiguracjach
e. Na etapie realizacji należy zastosować kasety na 12 spawów dla włókna OM3

W pośrednich punktach dystrybucyjnych należy zastosować modularny panel światłowodowy 1U (z możliwością montażu do 4 płytek/kaset wyposażonych w adaptery LC/SC/ST/MPO), wyposażony w płytkę z 6 adapterami LC duplex. Panel ma być przystosowany do zainstalowania minimum 12 włókien światłowodowych OM3 zakończonych złączami LC. Ze względów na możliwość wystąpienia dalszych rekonfiguracji połączeń światłowodowych pomiędzy punktami dystrybucyjnymi, panel ma mieć możliwość wykonania i zamontowania do 96 spawów ze złączami LC na wysokości 1U dla włókien OM3/OM4/OM5/OS1/OS2.

Kabel światłowodowy
Do połączeń pomiędzy punktami dystrybucyjnymi należy zastosować kabel światłowodowy 12 włóknowy OM3. Klasa niepalności dla kabla światłowodowego min: Dca s2 d2 a1. Ze względu na ograniczone miejsce w korytach kablowych należy zastosować kabel nie przekraczający 6,5mm średnicy, z użytkowym promieniem gięcia nie większym niż 75mm, instalacyjnym promieniem gięcia nie większym niż 130mm. Zakresy temperaturowy w jakiej może być użytkowany kabel światłowodowy to od minus 20^{o}C do plus 70^{o}C. Osłona kabla LSZH / LSHF-FR / FRNC zgodnie z EN 50290-2-27. Zgodność z normami: IEC 60332-1-2, IEC 60332-3-24, IEC 60754-2, IEC 61034.

Szafy dystrybucyjne
W szafach dystrybucyjnych należy zainstalować osprzęt połączeniowy oraz sprzęt aktywny.

Uwaga
Lokalizacja szaf w budynku została pokazana na rysunkach dołączonych do projektu. Dokładne zestawienie wyposażenia szaf oraz zestawienie ilościowe sprzętu instalowanego w szafach znajduje się w zestawieniu materiałowym.
Rozmieszczenie sprzętu w szafach należy ustalić z zamawiającym na etapie instalacji. 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.

5.1.4 Zestawienie materiałowe dla szkieletowych połączeń światłowodowych

Opis	Ilość Suma

Panel FO 1U na 12 kaset dla GPD1/2	2 szt.
Kaseta dla panela do GPD1/2 OM3	12 szt.
Mocowanie kabla dla panel FO w GPD1/2	2 szt.
Panel FO 1U dla pośrednich punktów dystrybucyjnych	12 szt.
Wyposażenie panela FO	12 szt.
Tacka na spawy	12 szt.
Płytka z adapterami FO LC	12 szt.
Prowadnica kabla FO	12 szt.
Pigtail OM3 1metr LC	144 szt.
Kabel światłowodowy OM3 12 włókien Dca	600 metrów
Kabel krosowy OM3 1metr LC duplex	20 szt.
Kabel krosowy OM3 2metr LC duplex	20 szt.
Kabel krosowy OM3 3metr LC duplex	8 szt.
Blokada portów USB (10 sztuk)	10 kpl.
Blokada portów USB (5 sztuk)	7 kpl.
Blokada portów RJ45 (10 sztuk)	10 kpl.

5.2 Urządzenia sieciowe i oprogramowanie

5.2.1 Przełącznik rdzeniowy/szkieletowy

Podstawowe

1. Przełącznik wyposażony w 24 porty SFP+
2. Przełącznik wyposażony w 1 port 10Gb/40Gb QSFP+
3. Przełącznik wyposażony w 2 porty 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28
4. Pamięć operacyjna: min. 4 GB pamięci DRAM
5. Wyposażony w dysk SSD o pojemności min. 32GB.
6. Obsługa sieci wirtualnych IEEE 802.1Q tworzonych przez użytkownika – min. 4092
7. Przełącznik wyposażony w port konsolowy RJ-45
8. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
9. Przełącznik wyposażony w port Micro-USB Typu A
10. Wysokość urządzenia 1U
11. Bufor pakietów minimum 12MB
12. Obsługa przepływu powietrza w przełączniku: przód-tył / tył przód, definiowane poprzez zastosowanie odpowiednich modułów wentylatorów i zasilaczy.
13. Tablica MAC adresów min. 272K
14. Nieblokująca architektura o wydajności przełączania 880Gbps
15. Urządzenie wyposażone w procesor czterordzeniowy pracujący z częstotliwością 2.4GHz
16. Ilość obsługiwanych wpisów LPM 256K dla IPv4
17. Ilość wpisów LPM 128K dla IPv6

18. Przełącznik wyposażony w dwa modularne, wewnętrzne zasilacze, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika.
19. Przełącznik wyposażony w cztery moduły wentylatorów zapewniający pełną redundancję.
20. Możliwość sformowania stosu z 8 urządzeń
21. Możliwość sformowania stosu o prędkości 400Gbps przy wykorzystaniu dwóch portów 100GB Full Duplex.
22. Możliwość instalacji zasilaczy o mocy 1100W każdy
23. Możliwość sformowania stosu z innymi modelami przełączników tego samego producenta
24. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
26. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci
27. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
28. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
29. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
30. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
31. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
32. Obsługa Q-in-Q IEEE 802.1ad
33. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
34. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
35. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
36. Gwarancja realizowana przez min. 5 lat, NBD

Obsługa mechanizmów:

1. Wsparcie dla Flexible Universal Forwarding Tables (UFT) lub równoważnego
2. Obsługa VxLAN Tunneling End Point (VTEP)
3. Obsługa DCBx Data Center Bridging Exchange Protocol
4. Obsługa Priority Flow Control (PFC)
5. Obsługa - Enhanced Transmission Selection (ETS)

Bezpieczeństwo

6. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
7. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
8. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
9. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
10. Obsługa Guest VLAN dla IEEE 802.1x
11. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
12. Obsługa Identity Management
13. Wbudowana obrona procesora urządzenia przed atakami DoS
14. Obsługa TACACS+
15. Obsługa RADIUS Authentication (RFC 2138)
16. Obsługa RADIUS Accounting (RFC 2139)
17. RADIUS and TACACS+ per-command Authentication
18. 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
19. Możliwość wyłączenia MAC learning
20. Obsługa SNMPv1/v2/v3
21. Klient SSH2
22. 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
23. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    d. Adres MAC źródłowy i docelowy plus maska
    e. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    f. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    g. Numery portów źródłowych i docelowych TCP, UDP
    h. Zakresy portów źródłowych i docelowych TCP, UDP
    i. Identyfikator sieci VLAN - VLAN ID
    j. Flagi TCP
    k. Obsługa fragmentów
24. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika

25. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
26. Obsługa bezpiecznego transferu plików SCP/SFTP
27. Obsługa DHCP Option 82
28. Obsługa IP Security - Gratuitous ARP Protection
29. Obsługa IP Security – Trusted DHCP Server
30. Obsługa IP Security – DHCP Secured ARP/ARP Validation
31. Ograniczanie przepustowości (rate limiting) na portach wyjściowych

Obsługa Multicastów

1. Statyczne przyłączanie do grupy Multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM
5. Obsługa PIM-SSM
6. Obsługa PIM snooping
7. Obsługa Multicast VLAN Registration - MVR
8. Obsługa IGMP v1 - RFC 1112
9. Obsługa IGMP v2 - RFC 2236
10. Obsługa IGMP v3 - RFC 3376
11. Obsługa IGMP v1/v2/v3 snooping
12. Możliwość konfiguracji statycznych tras dla Routingu Multicastów
13. Ilość grup Multicast min. 4k
14. Ilość wpisów Multicast min. 68k

Bezpieczeństwo sieciowe

1. Możliwość konfiguracji portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP - RFC 2338
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
8. Obsługa G.8032 v1/v2
9. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
10. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników

Zarządzanie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
2. Obsługa synchronizacji czasu NTP
3. Zarządzanie przez SNMP v1/v2/v3
4. Zarządzanie przez przeglądarkę WWW – protokół http i https
5. Możliwość zarządzania przez protokół XML
6. Telnet Serwer/Klient dla IPv4 / IPv6
7. SSH2 Serwer/Klient dla IPv4 / IPv6
8. Ping dla IPv4 / IPv6
9. Traceroute dla IPv4 / IPv6
10. Obsługa SYSLOG z możliwością definiowania wielu serwerów
11. Sprzętowa obsługa sFlow
12. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)

Obsługa RMON2 (RFC 2021

Inne:

1. Możliwość rozszerzenia funkcjonalności o MPLS poprzez wymianę oprogramowania lub licencję. Wymagane wsparcie dla następujących funkcjonalności: MPLS/VPLS, MPLS/VPWS, LDP, RSVP-TE, Fast Reroute
2. Obsługa skryptów CLI
3. Obsługa funkcji TCL/Tk w skryptach CL
4. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
5. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
6. Przełącznik ma by wyposażony w dwa zasilacze o mocy min. 765 W każdy oraz 4 wentylatory

5.2.2 Przełącznik dostępowy Typ I

1. Przełącznik posiadający 48 porty 10/100/1000BASE-T POE+
2. Przełącznik posiadający 4 porty 10GbE SFP+ w tym dwa z obsługą modułów optycznych LRM
3. Brak portów typu COMBO (Dual Personality)
4. Dwa porty SFP+ z obsługą modułów optycznych LRM
5. Wysokość urządzenia 1U
6. Budżet POE do podziału dla urządzeń 370W
7. Nieblokująca architektura o wydajności przełączania min. 176 Gb/s
8. Szybkość przełączania min. 130.9 Milionów pakietów na sekundę
9. Tablica MAC adresów min. 16k
10. Wsparcie dla ramek Jumbo Frames

11. Obsługa Quality of Service, IEEE 802.1p
12. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
13. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
14. Obsługa CDPv2
15. Obsługa Remote Switch Port Analyzer (RSPAN)
16. Możliwość zarządzania przełącznikiem za pomocą systemu zarządzania z poziomu chmury obsługującego polityki oraz mechanizmy kontroli dostępu NAC.
17. Obsługa mechanizmu Zero-touch provisioning z poziomu chmury oraz lokalnego systemu zarządzania
18. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management
19. Wbudowany port pozwalający na podłączenie zewnętrznego redundantnego zasilacza RPS
20. Możliwość monitoringu pakietów
21. Zarządzenie z WEB GUI
22. Obsługa TACACS+ (RFC 1492)
23. Obsługa klienta RADIUS RFC 2865
24. Obsługa RADIUS Accounting RFC 2866
25. Obsługa SSH 1.5 oraz 2.0
    a. RFC 4252: SSH authentication protocol
    b. RFC 4253: SSH transport layer protocol
    c. RFC 4254: SSH connection protocol
    d. RFC 4251: SSH protocol architecture
    e. RFC 4716: SECSH public key file format
    f. RFC 4419: Diffie-Hellman group exchange
26. Obsługa SSL 3.0 oraz TLS 1.0
    a. RFC 2246: Protokół TLS, wersja 1.0
    b. RFC 2818: HTTP over TLS
    c. RFC 3268: AES
27. Obsługa MIB-ów SNMP
    a. IEEE 802.1x MIB (IEEE 802.1-PAEMIB 2004 Revision)
    b. IEEE 802.3ad MIB (IEEE 802.3-ADMIB)
    c. IANAifType-MIB
    d. RFC 1213 – MIB II
    e. RFC 1493 – Bridge MIB
    f. RFC 1612 – DNS resolver MIB extensions
    g. RFC 2233 – Interfaces group MIB - SMI v2
    h. RFC 2613 – SMON MIB
    i. RFC 2618 – RADIUS authentication client MIB
    j. RFC 2620 – RADIUS accounting MIB
    k. RFC 2674 – VLAN MIB
    l. RFC 2737 – Entity MIB version 2
    m. RFC 2819 – RMON groups 1, 2, 3, and 9
    n. RFC 2863 – IF-MIB

o. RFC 4022 – TCP-MIB
p. RFC 4113 – UDP-MIB
q. RFC 2096 – IP forwarding table MIB
r. RFC 3636 – MAU MIB
s. RFC 3289 – Informacje zarządzania architektury DiffServ (read only)

28. Obsługa routingu statycznego
29. Obsługa IEEE 802.3x —Flow control
30. Obsługa Multicast VLAN Registration (MVR)
31. Obsługa Independent VLAN Learning (IVL)
32. Obsługa Multi-Switch Link Access Group (MLAG). Połączenie link aggregation do dwóch niezależnych przełączników.
33. Obsługa RFC 4541 (IGMP)
34. Obsługa minimum 4 instancji MSTP
35. Obsługa dynamicznego routing IPv4 (RFC 2453 RIP v2)
36. Obsługa statycznego routingu IPv6, do 64 tras
37. Możliwość tworzenia stosu urządzeń. Stos zarządzany za pomocą jednego adresu IP
38. Obsługa Policy-Based Routing
39. Obsługa Listy kontroli dostępu ACL do 10 na port
40. Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie:
    a. Czasu
    b. Źródłowego i docelowego adresu IP
    c. TCP/UDP źródłowy i docelowy
    d. Rodzaju protokołu IP
    e. EtherType
    f. IEE 802.1p
    g. Źródłowy i docelowy adres MAC
    h. Vlan id
41. Zakres temperatury pracy 0-50 °C
42. Możliwość pracy przy wilgotności od 10% do 95%
43. Urządzenie 1U oraz maksimum 26 cm głębokości
44. Obsługa skryptów CLI
45. Urządzenie wyposażone w oryginalny kabel zasilania
46. Gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia

5.2.3 Przełącznik dostępowy Typ II

1. Przełącznik posiadający 24 porty 10/100/1000BASE-T POE+
2. Przełącznik posiadający 2 porty 1GBE SFP
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 52 Gb/s
5. Szybkość przełączania min. 38.7 Milionów pakietów na sekundę

6. Tablica MAC adresów min. 16k
7. Budżet POE do podziału dla urządzeń 185W
8. Wsparcie dla ramek Jumbo Frames
9. Obsługa Quality of Service, IEEE 802.1p
10. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
11. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
12. Obsługa CDPv2
13. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
14. Możliwość monitoringu pakietów
15. Obsługa GVRP – Dynamic VLAN registration
16. Obsługa GMRP – Dynamic L2 multicast registration
17. Obsługa TACACS+ (RFC 1492)
18. Obsługa klienta RADIUS RFC 2865
19. Obsługa RADIUS Accounting RFC 2866
20. Obsługa SSH 1.5 oraz 2.0
    a. RFC 4252: SSH authentication protocol
    b. RFC 4253: SSH transport layer protocol
    c. RFC 4254: SSH connection protocol
    d. RFC 4251: SSH protocol architecture
    e. RFC 4716: SECSH public key file format
    f. RFC 4419: Diffie-Hellman group exchange for the SSH transport layer protocol
21. Obsługa routing statycznego minimum 60 tras
22. Obsługa IEEE 802.3x —Flow control
23. Obsługa Multicast VLAN Registration (MVR)
24. Obsługa Independent VLAN Learning (IVL)
25. Obsługa Multi-Switch Link Access Group (MLAG). Połączenie link aggregation do dwóch niezależnych przełączników.
26. Obsługa RFC 4541 (IGMP)
27. Obsługa protokołu MSTP minimum 4 instancje
28. Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie:
    a. Czasu
    b. Źródłowego i docelowego adresu IP
    c. TCP/UDP źródłowy i docelowy
    d. Rodzaju protokołu IP
    e. EtherType
    f. IEE 802.1p
    g. Źródłowy i docelowy adres MAC
    h. Vlan id
29. Zakres temperatury pracy 0-40 °C
30. Procesor o architekturze 32-bit o częstotliwości pracy minimum 400 MHz
31. Pamięć DRAM minimum 512 MB
32. Pamięć Flash minimum 128 MB

33. Urządzenie umożliwiające integrację z systemem zarządzania z poziomu chmury
34. Obsługa skryptów CLI
35. Gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia

5.2.4 Przełącznik dostępowy Typ III

1. Przełącznik posiadający 48 porty 10/100/1000BASE-T POE+
2. Przełącznik posiadający 4 porty 1GBE SFP
3. Wysokość urządzenia 1U
4. Budżet POE do podziału dla urządzeń 370W
5. Nieblokująca architektura o wydajności przełączania min. 104 Gb/s
6. Szybkość przełączania min. 77.4 Milionów pakietów na sekundę
7. Tablica MAC adresów min. 16k
8. Wsparcie dla ramek Jumbo Frames
9. Obsługa Quality of Service, IEEE 802.1p
10. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
11. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
12. Obsługa CDPv2
13. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
14. Możliwość monitoringu pakietów
15. Obsługa TACACS+ (RFC 1492)
16. Obsługa klienta RADIUS RFC 2865
17. Obsługa RADIUS Accounting RFC 2866
18. Obsługa SSH 1.5 oraz 2.0
    a. RFC 4252: SSH authentication protocol
    b. RFC 4253: SSH transport layer protocol
    c. RFC 4254: SSH connection protocol
    d. RFC 4251: SSH protocol architecture
    e. RFC 4716: SECSH public key file format
    f. RFC 4419: Diffie-Hellman group exchange for the SSH transport layer protocol
19. Obsługa routing statycznego
20. Obsługa IEEE 802.3x —Flow control
21. Obsługa Multicast VLAN Registration (MVR)
22. Obsługa Independent VLAN Learning (IVL)
23. Obsługa Multi-Switch Link Access Group (MLAG). Połączenie link aggregation do dwóch niezależnych przełączników.
24. Obsługa RFC 4541 (IGMP)
25. Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie:
    a. Czasu
    b. Źródłowego i docelowego adresu IP

c. TCP/UDP źródłowy i docelowy
d. Rodzaju protokołu IP
e. EtherType
f. IEE 802.1p
g. Źródłowy i docelowy adres MAC
h. Vlan id

26. Zakres temperatury pracy 0-40 °C
27. Obsługa skryptów CLI
28. Gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia

5.2.5 Access Point – sieć WiFi

1. Punkt dostępowy z dwoma wbudowanymi, niezależnymi od siebie, modułami radiowymi dla komunikacji IEEE 802.11ac Wave 2/a/n (5 GHz) i 802.11 b/g/n (2,4GHz)
2. Punkt dostępowy zasilany poprzez POE zgodnie ze standardem IEEE 802.11af oraz IEEE 802.11at
3. 8 wbudowanych anten dookólnych w konfiguracji 4:4 MIMO
4. Anteny o uzysku 5dBi dla 5GHz oraz 3 dBi dla 2.4GHz
5. Charakterystyka modułów radiowych 29dBm dla 5GHz oraz 27dBm dla 2.4GHz
6. Obsługa do trzech urządzeń MU-MIMO w danej chwili
7. Punkt dostępowy musi oferować wydajność przewodową na poziomie 90.000 pakietów na sekundę.
8. Musi realizować maksymalną przepustowość Throughput na poziomie 2.5 Gbps
9. Obsługa do 480 użytkowników. (240 na moduł radiowy)
10. Punkt dostępowy musi mieć możliwość pracy w trybie pół-autonomicznym i realizować w ten sposób, niezależnie od kontrolera, zadania związane z inteligentnym szyfrowaniem, bezpieczeństwem, filtrowaniem, zarządzaniem łącznością radiową i QoS.
11. Musi obsługiwać funkcje egzekwowania polityk i ograniczania przepustowości w punkcie dostępowym.
12. Przełącznik musi obsługiwać polityki na portach Ethernet
13. Punkt dostępowy musi jednocześnie obsługiwać ruch tunelowany i mostowany.
14. Punkt dostępowy musi obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń.
15. Punkt dostępowy musi realizować funkcję samo-naprawy i samo-formowania sieci kratowej (*self-healing* i *self-forming*).
16. Punkt dostępowy musi obsługiwać instalację typu plug&play.

17. Punkt dostępowy musi posiadać funkcję analizy widma łączności radiowej i wyszukiwania w nim wzorców xorr
18. Punkt dostępowy musi mieć możliwość takiego skonfigurowania by zapewniać równoważenie obciążenia i sterowanie pasmem.
19. Punkt dostępowy musi wspierać standard IEEE 802.11h dla dynamicznej kontroli kanału.
20. Punkt dostępowy musi obsługiwać do 16 SSID (8 na każdy moduł radiowy).
21. Zarządzanie łącznością radiową w ramach punktów dostępowych - *RF Management,* musi obsługiwać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (*Transmit Power Control*).
22. Zarządzanie łącznością radiową w ramach punktów dostępowych - *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.
23. Punkty dostępowe muszą obsługiwać protokoły 802.11e, w tym WMM oraz U-APSD.
24. Punkt dostępowy musi zapewniać wsparcie dla minimum 30 połączeń typu Voice (802.11b, G711, R>80)
25. Punkt dostępowy musi umożliwiać rozdystrybuowaną oraz z zcentralizowaną architekturę przepływu danych w ramach tego samego SSID
26. Możliwość zarządzania urządzeniem za pomocą systemu zarządzania siecią i kontroli dostępu (NAC) z poziomu chmury
27. Urządzenie musi łączyć się z chmurą i systemem zarzadzania bez jakiejkolwiek konfiguracji (out of box)
28. Możliwość przejścia z zarządzania z poziomu chmury na lokalny bez konieczności zmiany oprogramowania punktu dostępowego
29. Gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia

5.2.6 Kontroler – sieć WiFi

1. Obsługa w środowisku wirtualnym VMware ESXi lub Hyper-V
2. Obsługa do 525 punktów dostępowych
3. Obsługa do 1,050 punktów dostępowych w trybie wysokiej dostępności
4. Obsługa do 4000 użytkowników
5. Obsługa 2 interfejsów Ethernet (wirtualnych)
6. Architektura systemu oferuje następujące możliwości przesyłania danych WLAN w sieci przewodowej:
   - a) Routowany na kontrolerze: Kontroler WLAN w tym trybie pracuje jak

klasyczny router warstwy 3 i trasuje ruch klientów WLAN w sieci przewodowej
- b) Mostowany na kontrolerze: W tym przypadku kontroler WLAN pracuje jak most warstwy 2, kieruje cały ruch warstwy 2 do zdefiniowanej sieci VLAN w ramach infrastruktury przewodowej
- c) Mostowany na punkcie dostępowym: W tym trybie ruch WLAN jest w punkcie dostępowym na warstwie 2 kierowany bezpośrednio do zdefiniowanej sieci VLAN

7. Wszystkie dostępne typy punktów dostępowych wchodzące w skład rozwiązania WLAN muszą obsługiwać jednocześnie te 3 możliwości przesyłania danych
8. Musi istnieć możliwość zmiany metody przesyłania ruchu przed i po uwierzytelnianiu dla każdej sesji klienckiej
9. Poniższe ustawienia muszą być możliwe w ramach sesji klienckiej SSID:
   - indywidualne reguły filtrowania
   - przypisywanie VLAN
   - QoS według użytkownika/ aplikacji
   - ograniczenia szerokości pasma wchodzącego i wychodzącego
   - topologia (routowany na kontrolerze, mostowany na kontrolerze, mostowany na punkcie dostępowym)
10. Architektura bezpieczeństwa wykorzystująca IEEE 802.1X dla klientów WLAN
11. Obsługa RADIUS ze wstępnym uwierzytelnianiem oraz PMK Caching (Pairwise Master Key) z czasami przełączania poniżej 50 ms (roaming); Możliwość stosowania certyfikatów zgodnych z X.509
12. Architektura umożliwia połączenie ze sobą dwóch kontrolerów w trybie HA (wysoka dostępność).
13. Wsparcie dla VPN, wideo oraz VoIP, z szybkim roamingiem oraz obsługą co najmniej 5 profili QoS, również w roamingu warstwy 3.
14. Obsługa CAC – Call Admission Control. CAC sprawdza czy mogą być zestawione nowe połączenia na punkcie dostępowym, nie wpływając na jakość dotychczasowych połączeń.
15. Równoważenie obciążenia dla klientów
16. Możliwość ograniczania ruchu multicast dla każdej sieci.
17. Obsługa QBSS (Informacja o zbyt dużym obciążeniu zostanie przekazania klientowi, dla obsługi inteligentnego roamingu
18. Obsługa UAPSD (Unscheduled Automatic Power Save Delivery)
19. Funkcja FCA (Flexible Client Access) zwiększająca prędkość transmisji klientów 11n w sieci z urządzeniami 11a/b/g

20. Obsługa równoważenia obciążenia punktów dostępowych w celu efektywnego rozdziału ruchu pomiędzy klientami WLAN
21. Funkcja oszczędzania energii zmniejszająca zużycie prądu, w czasie gdy w punkcie dostępowym nie jest zarejestrowany żaden klient.
22. Obsługa funkcji Band Preference dla automatycznego przenoszenia klientów w paśmie 5GHz.

Portal dla gości

23. Zintegrowany, kompleksowy system obsługi gości:
    - Możliwość stworzenia własnej strony logowania
    - Szablony ticketów
    - Lokalne zarządzanie kontami
    - Oddzielny portal do administracji ticketami
24. Opcjonalna realizacja dostępu dla gości przez uwierzytelnianie w ramach portalu Captive portal oraz ograniczanie dostępu dla nieuwierzytelnionych klientów.
25. Edytor HTML pozwalający na dostosowanie portalu dla gości

Konfiguracja

26. Kreator konfiguracji dla podstawowych ustawień, wysokiej dostępności i usług WLAN
27. Funkcjonowanie i konfiguracja punktów dostępowych w strukturach sieciowych warstwy 2 i 3
28. Obsługa reguł filtrowania wg. użytkownika, interfejsu i punktu dostępowego dla wszystkich architektur systemowych – routowany na kontrolerze, mostowany na kontrolerze, mostowany na punkcie dostępowym
29. Obsługa Opportunistic Key Caching (OKC) dla szybszego i bezpieczniejszego roamingu
30. Obsługa Wireless Distribution System (WDS)
31. Obsługa Dynamic Meshing dla automatycznej budowy i pracy rozproszonego systemu WDS
32. Kompleksowe narzędzia diagnostyczne. Informacje statystyczne na temat wykorzystania sieci, przypisanych klientów, użytkowników, stan (oraz błędy) interfejsów radiowych i Ethernetowych punktów dostępowych; Raporty są widoczne przez graficzny interfejs użytkownika, eksportowane do HTML lub dostępne przez SNMPv2
33. Dostęp do administracji jest zabezpieczanych przez RADIUS i rejestrowany
34. Sterowanie z poziomu kontrolera inteligentnymi funkcjami łączności radiowej, takimi jak monitorowanie każdego kanału, dynamiczna

zmiana kanału na wypadek zakłóceń oraz automatyczne zwalnianie kanałów, gdy źródło zakłóceń przestanie być aktywne

35. Rozpoznawanie i uzupełnianie niedostatecznie pokrytych łącznością radiową obszarów powstałych na skutek awarii punktu dostępowego, dzięki automatycznemu dopasowywaniu mocy nadawczej
36. Białe i czarne listy adresów MAC

Zarządzanie

37. Zarządzanie wszystkimi funkcjami przez:
    - Interfejs przeglądarki (HTTP/HTTPs)
    - SNMP V1, V2.c,V3
    - CLI (Telnet / SSH)
    - Oprogramowanie systemowe
38. Obsługa IP v4 i v6
39. Szyfrowane przesyłanie informacji zarządzania pomiędzy punktami dostępowymi a centralnym systemem przełączania WLAN, przy zastosowaniu IPSEC, IKEv2, AES i protokołów szyfrowania Diffie-Hellman
40. Enkapsulacja pakietów przez protokół tunelowania CAPWAP
41. Centralne konfigurowanie i aktualizowanie oprogramowania punktów dostępowych, wraz z automatyczną pierwszą konfiguracją (zero-touch)
42. Panel sterowania pozwalający na sprawdzenie funkcjonowania systemu
43. Wprowadzenie nowego, nieznanego punktu dostępowego tylko po podaniu numeru seryjnego.
44. Definiowanie wirtualnych usług sieciowych dla mapowania metod uwierzytelniania oraz grupowo kontrolowanych zestawów reguł w oparciu o RADIUS
45. Wirtualne usługi sieciowe, punkty dostępowe oraz zestawy reguł muszą być przypisywane zależnie od lokalizacji
46. Punkty dostępowe są aktywne tylko po przypisaniu co najmniej jednej usługi sieci wirtualnych
47. Blokowanie ruchu klientów wewnątrz WLAN
48. Autonomicznie trasowane podsieci IP, każda z oddzielną usługą DHCP
49. Obsługa OSPF V2
50. Opcjonalna obsługa istniejących punktów dostępowych pochodzących od innych dostawców, na zarezerwowanym porcie
51. Wykrywanie fałszywych punktów dostępowych i ochrona przed nimi
52. Integracja jednolitego zarządzania sieciami LAN i WLAN, w celu globalnego wprowadzania polityk oraz centralnego zabezpieczania sieci, konfigurowania i dystrybucji firmware.

53. Obsługa funkcji przechwytywania pakietów w czasie rzeczywistym – bezpośrednie śledzenia ruchu 802.11 na punktach dostępowych oraz jego ocena w Wireshark
54. Wygenerowane przez RADIUS ID tuneli muszą być przetłumaczone na reguły filtrów w celu adaptacji scenariuszy RFC3580

Niezawodność

55. Ogólna wysoka dostępność rozwiązania może być zabezpieczona przez redundantną parę kontrolerów oraz krótkie cykle odpytywania punktów dostępowych
56. W wypadku wystąpienia awarii wszystkie punkty dostępowe przypisane do pary kontrolerów są obsługiwane przez sprawne urządzenie.
57. Szybka konwergencja (Fast Failover) bez utraty istniejących połączeń głosowych i transmisji danych
58. Punkty dostępowe pracują także w tzw. Trybie Branch Office, niezależnie od połączenia z kontrolerem (lokalne mostowanie ruchu na warstwie 2)
59. W trybie Branch Office zapytania uwierzytelniające 802.1X i MAC mogą być kierowane do lokalnego serwera RADIUS
60. W trybie Branch Office grupom do 32 punktów dostępowych może być zapewniony niezależny od kontrolera roaming.

5.2.7 Oprogramowanie do zarządzania przełącznikami i NAC

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
   a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
   b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową
3. Aplikacja zarządzająca musi obsługiwać minimum 25 urządzeń (adresów IP)
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników.
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje

na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego

6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
    a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości
    b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów
    c. konfiguracji sieci VLAN

d. konfiguracji protokołu routingu OSPF

24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https
25. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość obsługi urządzeń sieciowych różnych producentów
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie
        i) źródłowy i docelowy adres MAC
        ii) źródłowy i docelowy adres IP
        iii) źródłowy i docelowy adres IP podsieci
        iv) źródłowy i docelowy port TCP/UDP
        v) źródłowy i docelowy zakres portów TCP/UDP
        vi) typ protokołu
        vii) pole IP TOS
    b. przydziału parametrów QoS
        i) priorytety
        ii) ograniczenia przepustowości

c. przydziału użytkownika do wskazanej sieci VLAN
d. przekierowania ruchu do zewnętrznego systemu analizującego pakiety

32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych
34. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
    b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
    c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
    d. generowanie raportów
35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
        i) adres IP kontrolera
        ii) liczba obsługiwanych klientów
        iii) szczytowe wartości zajmowanego pasma
        iv) wersja oprogramowania
    d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
        i) adres IP punktu dostępowego
        ii) MAC adres punktu dostępowego
        iii) wersja oprogramowania
        iv) typ punktu dostępowego
        v) kanały pracy poszczególnych interfejsów radiowych

vi) szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych

e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
   i) adres IP klienta
   ii) MAC adres klienta
   iii) nazwa użytkownika
   iv) nazwa punktu dostępowego, do którego dołączony jest użytkownik
   v) BSSID, do którego dołączony jest użytkownik
   vi) SSID, do którego dołączony jest użytkownik
f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
   i) zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
   ii) zaznaczenie kanałów pracy urządzeń
   iii) lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci z zapewnieniem widzialności następujących informacji:
   a. adresu MAC
   b. adresu IP
   c. nazwy komputera
   d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
   e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
   f. adres IP urządzenia, do którego dołączony jest klient.
   g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
   h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
   i. nazwa przydzielonej polityki bezpieczeństwa.
37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
42. System zapewniający widoczność zautoryzowanych klientów jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 250 punktów dostępowych oraz min. 25 przełączników sieciowych
43. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.
    a. Analiza danych o przepływie(mirror)
    b. Analiza danych NetFlow
    c. Możliwość analizy minimum 50 tyś przepływów na minutę
    d. Rozpoznawanie co najmniej 7000 aplikacji
    e. Baza danych z 13000 sygnatur
    f. Modyfikowalny zestaw sygnatur, tworzenie własnych
    g. Analiza opóźnienia w całej sieci w oparciu o TCP
    h. Analiza wykorzystania zasobów w oparciu o aplikacje
    i. Analiza wykorzystania aplikacji, celów i opóźnienia w podziale na poszczególnych użytkowników
    j. Panel sterowania umożliwiający przeglądanie informacji o klientach, serwerach, paśmie, przepływach i opóźnieniu
    k. Ekran prezentujący największe zużycie pasma dla użytkowników i serwerów i aplikacji
    l. Panel sterowania wyświetlający pasmo przypisane do grup aplikacji
    m. Różne modele wizualizacji danych: wykres kołowy, drzewo, mapa bąbelkowa, itp.

44. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.
45. System zarządzania musi być objęty rocznym wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.

5.2.8 Zakres wdrożenia urządzeń sieciowych i oprogramowania

Dostarczone przełączniki należy zainstalować w szafach rack wskazanych przez zamawiającego. Punkty dostępowe należy zainstalować w odpowiednich miejscach by pokryć zasięgiem pomieszczenia wskazane przez zamawiającego (sugerowane wykonanie Site Survey). Jeśli kontroler WLAN, oprogramowanie zarządzające przełącznikami oraz kontroli dostępu do sieci) zostanie dostarczony w formie maszyny wirtualnej należy go zainstalować w zasobach udostępnionych przez zamawiającego. Należy stworzyć co najmniej dwie polityki bezpieczeństwa dostępu do sieci przewodowej i bezprzewodowej (dla pracowników oraz gości) i uruchomić je na dostarczonych przełącznikach oraz punktach dostępowych. System należy zintegrować z kontrolerem Acive Directory posiadanym przez zamawiającego. Oprogramowanie do zarządzania siecią należy uruchomić zgodnie z wytycznymi zamawiającego. Wraz ze sprzętem należy dostarczyć niezbędne licencje, które umożliwią uzyskanie oczekiwanej funkcjonalności.

5.2.9 Zestawienie materiałowe

Opis	Ilość Suma
Przełącznik rdzeniowy/szkieletowy (dwa zasilacze, cztery wentylatory, dwa kable zasilające, kabel stackujący)	4 szt.
Przełącznik typ I	27 szt.
Przełącznik typ II	2 szt.
Przełącznik typ III	2 szt.
Punkt dostępowy	10 szt.
Kontroler WLAN 10 licencji na punkty dostępowe	1 szt.
Oprogramowanie do zarządzania siecią i kontrolą dostępu do sieci	1 szt.
Kabel stackujący	19 szt.
Moduł światłowodowy 10Gb/s SR	40 szt.

6. Wymagania gwarancyjne

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 światłowodowego wraz z kablami krosowymi, szkieletowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, pigtaile, wieszaki, 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.

Gwarancja na urządzenia aktywne ma spełniać poniższe warunki:

- przełącznik rdzeniowy – gwarancja realizowana przez min. 5 lat, NBD;
- przełącznik dostępowy – gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia
- Access Point – gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia
- Oprogramowanie ma zostać dostarczone z rocznym wsparciem technicznym ze strony producenta aktywnym, nie wcześniej niż, od momentu podpisania protokołów odbioru instalacji bez uwag;

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 lub oficjalnego przedstawiciela na Polskę systemu.
Zbudowana infrastruktura kablowa ma być ostatecznie fizycznie sprawdzona przez producenta lub oficjalnego przedstawiciela na Polskę 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 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, osoby te muszą uczestniczyć w nadzorowaniu prac 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 światłowodowe, panele krosowe, kable krosowe, blokady portów) 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.

7. 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.

8. 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 50346:2004/A2:2010. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego.

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 wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX-5000);
- Pomiary dla systemu należy wykonać w konfiguracji pomiarowej kanału łącza stałego (Channel-link) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego;
- Pomiary sieci miedzianej należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1 z rozszerzeniem parametrów o rezystancję niezrównoważenia (dla 4PPoE):
    - Klasa E_A dla wszystkich torów transmisyjnych;
- Protokół pomiarowy każdego toru transmisyjnego poziomego miedzianego ma zawierać:
    - mapę połączeń;
    - długość połączeń i rezystancje par;
    - rezystancję niezrównoważenia
    - 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 może być wyznaczone za pomocą miernika spadku mocy optycznej lub reflektometru;
- Pomiar tłumienia mocy optycznej należy wykonać przy wykorzystaniu metody wtrąceniowej z 3 kablami referencyjnymi lub 1 kablem referencyjnym;
- Przy pomiarze reflektometrem należy użyć rozbiegówki oraz dobiegówki w celu zapewnienia analizy całego tory transmisyjnego i określenia jakości wszystkich złączy;
- Niezależnie od użytego sprzętu pomiarowego kompletny pomiar tłumienia każdego dupleksowego toru transmisyjnego powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien:
  - od punktu A do punktu B w oknie 850nm i 1300nm (MM)
  - od punktu B do punktu A w oknie 850nm i 1300nm (MM)
- Na raportach pomiarów powinna znaleźć się informacja opisująca wielkość marginesu transmisyjnego (inaczej zapasu, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej mierzonej wielkości);

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.

9. 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 Inwestorem i 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.

10. Alternatywne propozycje

Uwaga: Zgodnie z zasadami zamówień publicznych można zastosować materiały i rozwiązania równoważne, to jest w żadnym stopniu nie obniżające standardu, parametrów technicznych 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 materiałów o innych parametrach technicznych, funkcjonalnych, użytkowych, gwarancyjnych, musi do oferty dołączyć listę zamienionych materiałów, jak również wszelkie dokumenty pozwalającej Komisji Przetargowej ocenić zgodność z wymaganiami SIWZ i dokumentacji projektowej wraz z załącznikami. W sytuacjach niejasnych zmawiający może wystąpić do oferenta o przedstawienie próbek zaoferowanych materiałów okablowania strukturalnego wraz z dokonaniem pomiarów oraz zaprezentowanie działania funkcjonalności urządzeń sieciowych oraz oprogramowania wymaganych przez zamawiającego, w siedzibie u zamawiającego, zgodnych z wytycznymi zawartymi w projekcie, przed podpisaniem umowy i w terminie wyznaczonym przez zamawiającego.