**Nr postępowania: 23 Z TP 22**

Załącznik nr 1 do SWZ

*Nazwa i adres Wykonawcy* ..............................

**Opis przedmiotu zamówienia**

**Dostawa urządzeń do rozbudowy sieci bezprzewodowej wraz z wykonaniem okablowania strukturalnego w budynkach Kujawsko - Pomorskiego Centrum Pulmonologii w Bydgoszczy**

CPV o nr: 32400000-7

|  |  |  |
| --- | --- | --- |
| Zestawienie ilościowe | | |
| 1. | Przełącznik 48p 10/100/1000BASE-T oraz  4p 1/10gigabitowe SFP+ | 6 szt. |
| 2. | Punkt dostępowy | 64 szt. |
| 3. | Zestaw montażowy punktu dostępowego | 64 szt. |
| 4. | Kontroler sieci bezprzewodowej | 1 szt. |
| 5. | Roczne wsparcie na kontroler bezprzewodowy z serwisem sprzętu i ewentualną wymianą następny dzień roboczy. Wsparcie telefoniczne 24x7, uaktualnienia oprogramowania | 1 lic. |
| 6. | Licencje kontrolera na obsługę punktów dostępowych | 86 lic |
| 7. | Obsługa serwisowa Licencji kontrolera na obsługę punktów dostępowych | 86 lic. |
| 8. | Kabel S/FTP kat.7A | 6 km |
| 9. | Gniazdo do zakończenia okablowania strukturalnego z obudową do montażu natynkowego 45x45, bez ramki i wkładki | 64 szt. |
| 10. | Wkładka ekranowana 1xRJ45 kat.6A ISO, do zakończeń okablowania strukturalnego przy punktach dostępowych | 64 szt. |
| 11. | Panel krosowy 24 port HD, kpl. bez wkładek,2U, RAL9005 | 8 szt. |
| 12. | Wkładka ekranowana 1xRJ45 do panela krosowego kat.6A ISO, | 64 szt. |
| 13. | Zaślepka gniazda w panelu krosowym (kolor czarny) | 34 szt. |
| 14. | Kabel krosowy S/FTP LSZH kat.6A ISO RJ45 biały 1.5m | 128 szt. |

**I. Szczegółowe wymagania dla przełącznika 48p (6 sztuk):**

|  |  |  |
| --- | --- | --- |
| Lp | Parametry | Parametr graniczny |
|  | Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+) | Tak |
|  | Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy | Tak |
|  | Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) | Tak |
|  | Wydajność: minimum 98 Mp/s | Tak |
|  | Bufor pakietów: minimum 12 MB | Tak |
|  | Minimum 4GB pamięci operacyjnej | Tak |
|  | Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash). | Tak |
|  | Dedykowany port konsoli USB | Tak |
|  | Port USB 2.0 (niezależny od portu konsoli USB) | Tak |
|  | Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W. Pobór mocy (bez PoE) nie może być większy niż 50W. | Tak |
|  | Wielkość tablicy routingu: minimum 500 wpisów IPv4, 500 wpisów IPv6 | Tak |
|  | Wielkość tablicy ARP co najmniej 1000 wpisów, wielkość tablicy ND co najmniej 500 wpisów | Tak |
|  | Tablica adresów MAC o wielkości minimum 8000 pozycji | Tak |
|  | Obsługa Jumbo Frames co najmniej 9198 bajtów | Tak |
|  | Obsługa sFlow lub Netflow | Tak |
|  | Obsługa REST API | Tak |
|  | Obsługa RMON (minimum grupy 1,2,3 i 9) | Tak |
|  | Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN | Tak |
|  | Obsługa protokołu MVRP | Tak |
|  | Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne | Tak |
|  | Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) | Tak |
|  | Obsługa Secure FTP lub SCP | Tak |
|  | Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) | Tak |
|  | Obsługa SNTPv4 lub NTP | Tak |
|  | Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping) | Tak |
|  | Obsługa protokołów rutingu: ruting statyczny | Tak |
|  | Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup) | Tak |
|  | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) | Tak |
|  | Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) | Tak |
|  | Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting | Tak |
|  | Obsługa uwierzytelniania użytkowników zgodna z 802.1x | Tak |
|  | Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS | Tak |
|  | Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera | Tak |
|  | Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie | Tak |
|  | Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ | Tak |
|  | Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+ | Tak |
|  | Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), | Tak |
|  | Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) | Tak |
|  | Obsługa list kontroli dostępu (ACL) | Tak |
|  | Zakres pracy od 0 do 45°C | Tak |
|  | Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 32 cm. | Tak |
|  | Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania | Tak |
|  | Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. | Tak |
|  | Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. | Tak |

**II. Szczegółowe wymagania dla kontrolera sieci bezprzewodowej:**

|  |  |  |
| --- | --- | --- |
| Lp. | Parametry | Parametr graniczny |
|  | Kontroler musi zarządzać siecią bezprzewodową złożoną z 86 punktów dostępowych z możliwością rozbudowy do 256 punktów dostępowych | Tak |
|  | Kontroler musi obsługiwać posiadane przez Zamawiającego punkty dostępowe Aruba AP207, AP505 oraz punkty dostępowe opisane w tym dokumencie w pkt III | Tak |
|  | Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall) | Tak |
|  | Musi posiadać funkcje VPN Gateway | Tak |
|  | Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym. | Tak |
|  | Kontroler musi umożliwiać pracę w klastrze HA | Tak |
|  | Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych. | Tak |
|  | Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania | Tak |
|  | Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jedne kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom. | Tak |
|  | Kontroler musi posiadać następujące parametry sieciowe:   1. możliwość wdrożenia w warstwie 2 i 3 ISO/OSI, 2. wsparcie dla sieci VLAN w tym również trunk 802.1q 3. wbudowany serwer DHCP 4. obsługa SNMPv2, SNMPv3 5. routing dynamiczny OSPF | Tak |
|  | Kontroler sieci WLAN musi obsługiwać co najmniej:   * 1. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST, DES, 3DES, AES-CBC   2. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze   3. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit   4. Autoryzację dostępu użytkowników:      1. Typy uwierzytelnienia: IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal”, 802.1X i MAC      2. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia      3. Wsparcie dla autoryzacji, minumum: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC      4. Musi umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal”      5. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)      6. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym      7. Uwierzytelnienie oraz autoryzacja musi być możliwe przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.   5. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.   6. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu   7. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia | Tak |
|  | Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:   * 1. Integracja jednoczesnej transmisji danych i głosu   2. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p   3. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)   4. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika   5. Ograniczenie pasma dla poszczególnych aplikacji   6. Ograniczenie pasma dla poszczególnych SSID | Tak |
|  | Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API. | Tak |
|  | Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal) | Tak |
|  | Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni) | Tak |
|  | Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:   * 1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe   2. Stałe monitorowanie pasma oraz usług   3. Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi   4. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma   5. Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie   6. Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)   7. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału   8. Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w   9. Integracja z systemami RFID - wymagane jest wbudowane stosowne API | Tak |
|  | Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:   * 1. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia   2. Kopiowanie (mirroring) sesji   3. Szczegółowe logi (per pakiet) do późniejszej analizy   4. ALG (Application Layer gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera   5. Translacja źródłowa, docelowa adresów IP   6. Identyfikacja i blokowanie ataków DoS   7. Obsługa protokołu GRE   8. hDeep packet inspection (DPI)   9. Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie). | Tak |
|  | Kontroler musi mieć wbudowany serwer VPN, charakteryzujący się następującymi parametrami, nie mniej niż:   * 1. Site-to-site oraz client-site VPN   2. Terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP   3. Obsługa tokenów   4. Wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu: PAP CHAP, MS-CHAP, MS-CHAP2   5. Wsparcie dla algorytmów kryptograficznych: DES, 3DES, AES przy wykorzystaniu dedykowanych układów scalonych kontrolera | Tak |
|  | Kontroler musi posiadać funkcję systemu WIDS/ WIPS (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie). Moduł WIPS musi posiadać co najmniej następujące funkcje:   * 1. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.   2. Identyfikacja i możliwość blokowania sieci Adhoc   3. Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging   4. Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler   5. Identyfikacja błędów konfiguracji klientów WLAN   6. Identyfikacja podszywania się pod autoryzowane punkty dostępowe | Tak |
|  | Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie). | Tak |
|  | Kontroler musi mieć możliwość wprowadzenia klasyfikacji treści przeglądanych przez użytkowników stron www (np. przemoc, hazard itp.) oraz określenia ich reputacji. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie, dostęp do bazy treści może być oferowany w formie subskrypcji, o ile dostępna jest ona na co najmniej 10 lat bez konieczności jej odnawiania) | Tak |
|  | Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli. | Tak |
|  | Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA | Tak |
|  | Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:   * 1. Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 256   2. Liczba jednocześnie obsługiwanych adresów MAC nie mniej niż 8000   3. Liczba aktywnych sesji zapory sieciowej nie mniej niż 1000000,   4. przepustowość nie mniej niż (duże pakiety) 12Gbps   5. Liczba obsługiwanych BSSID nie mniej niż 8192   6. Liczba jednoczesnych sesji IPSEC nie mniej niż 4000   7. Minimum 2 porty 10GBASE-X ze stykiem definiowanym przez SFP+   8. Minimum 4 porty gigabitowe w standardzie 10/100/1000BaseT   9. Minimum 4 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT)   10. 1 interfejs konsoli (mini USB/RJ-45)   11. Minimum 1 port USB 2.0   12. Zużycie energii nie większe niż 110W   13. Pełna obsługa standardu 802.1Q – 4094 tagów sieci VLAN | Tak |
|  | Dla kontrolera wymagana zgodność z normami CE | Tak |
|  | Minimum roczna gwarancja producenta obejmująca wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 8x5 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. | Tak |

Z kontrolerem muszą być dostarczone licencje dla minimum 86 Punktów Dostępowych (Access Pointów) z wsparciem technicznym minimum na 12 miesięcy.

Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), o ile nie wyspecyfikowano inaczej, nie dopuszcza się licencji czasowych i subskrypcji.

**III. Minimalne wymagania dla punktu dostępowego (64 sztuki):**

|  |  |  |
| --- | --- | --- |
| Lp. | Parametry | Parametr graniczny |
|  | Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax. | Tak |
|  | Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej | Tak |
|  | Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:   1. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https 2. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki 3. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. | Tak |
|  | Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:   1. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego 2. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny 3. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe 4. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję 5. Tworzenie klastra do 130 urządzeń | Tak |
|  | Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP | Tak |
|  | Punkt dostępowy musi mieć możliwość pracy jako analizator widma | Tak |
|  | W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa | Tak |
|  | W system musi być wbudowany serwer DHCP | Tak |
|  | W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów | Tak |
|  | Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:   1. EAP-TLS 2. PEAP-MSCHAPv2 3. PEAP-GTC 4. TTLS-MSCHAPv2 | Tak |
|  | Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP | Tak |
|  | Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID | Tak |
|  | Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN | Tak |
|  | Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:   1. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania 2. Zewnętrzny portal WWW | Tak |
|  | Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT | Tak |
|  | Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne | Tak |
|  | Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:   1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe 2. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu 3. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma 4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału 5. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz 6. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g) 7. Wsparcie dla 802.11d oraz 802.11h 8. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane | Tak |
| Tak |
|  | Minimalizacja interferencji związanych z sieciami 3G/4G LTE | Tak |
|  | Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej | Tak |
|  | Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 6dBm) | Tak |
|  | Obsługa roamingu klientów w warstwie 2 | Tak |
|  | Obsługa monitoringu przez SNMP | Tak |
|  | Obsługa logowania na zewnętrznym serwerze SYSLOG | Tak |
|  | W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci | Tak |
|  | W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci | Tak |
|  | Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:   * 1. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością   2. Wykorzystanie pasma   3. Ilość klientów korzystających z systemu/interferujących   4. Ilość ramek wejściowych/wyjściowych dla każdego radia   5. Ilość odrzuconych/błędnych ramek/s dla każdego radia   6. Szum tła dla każdego radia   7. Wyświetlanie logów systemowych | Tak |
|  | Punkt dostępowy musi posiadać co najmniej 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz | Tak |
|  | Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax | Tak |
|  | Praca w trybie SU MIMO 2X2:2 dla 5GHz | Tak |
|  | Specyfikacja radia 802.11a/n/ac/ax:   1. Obsługiwana technologia OFDM oraz OFDMA 2. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM 3. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm 4. Prędkości transmisji: 5. Od 6,5 Mbps do 400 Mbps dla 802.11n 6. Od 6,5 Mbps do 1000 Mbps dla 802.11ac 7. Od 3,6 Mbps do 574 Mbps dla 802.11ax (2,4GHz) 8. Od 3,6 Mbps do 1200 Mbps dla 802.11ax (5GHz) 9. Obsługa HT – kanały 20/40MHz dla 802.11n 10. Obsługa VHT – kanały 20/40/80 dla 802.11ac 11. Obsługa HE – kanały 20/40/80 dla 802.11ax 12. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz 13. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac 14. Wsparcie dla: 15. MRC (Maximal ratio combining) 16. CDD/CSD (Cyclic delay/shift diversity) 17. STBC (Space-time block coding) 18. LDPC (Low-density parity check) 19. Technologia TxBF | Tak |
|  | Specyfikacja radia 802.11b/g/n/ax:   1. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA 2. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM 3. Moc transmisji konfigurowalna przez administratora | Tak |
|  | Punkt dostępowy musi posiadać co najmniej:   1. 1 interfejs 100/1000BaseT 2. z funkcją auto-sensing link oraz MDI/MDX 3. z funkcją PoE/PoE+ 4. ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE) 5. interfejs konsoli RS-232 (RJ-45) lub USB 6. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli) 7. przycisk przywracający konfigurację fabryczną 8. slot zabezpieczający Keningston | Tak |
|  | Parametry pracy urządzenia:   1. Temperatura otoczenia (zakres minimalny): 0-50 º C 2. Wilgotność (zakres minimalny): 5% - 92% 3. Obsługiwane standardy:    1. Ethernet IEEE 802.3 / IEEE 802.3u    2. Power-over-Ethernet IEEE 802.3af    3. Wireless IEEE 802.11a/b/g/n/ac/ax 4. Znak CE 5. EN 60601-1-1, EN60601-1-2 | Tak |
|  | Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE oraz przy pomocy lokalnego zasilacza DC (zasilacz nie musi być dołączony) | Tak |
|  | Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac | Tak |
|  | Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. | Tak |
|  | Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni | Tak |
|  | Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik o nie gorszych parametrach. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu. | Tak |

Urządzenia musza być wspierane przez posiadane przez Zamawiającego oprogramowanie HPE IMC Standard Software Platform.

W związku z tym, że gwarancja HPE na produkt HPE Networking jest dostępna wyłącznie dla

pierwotnych użytkowników końcowych działających w dobrej wierze, którzy nabyli produkt za

pośrednictwem autoryzowanego kanału dystrybucji HPE, Zamawiający zastrzega sobie prawo do sprawdzenia bezpośrednio u polskiego przedstawiciela producenta właściwego statusu Wykonawcy na etapie oceny ofert. Brak odpowiedniego statusu będzie oznaczał, że oferowany przedmiot zamówienia nie będzie pochodził z autoryzowanego kanału dystrybucji, co oznacza, że Zamawiający nie nabędzie praw gwarancyjnych oferowanych przez producenta sprzętu. Będzie to jednoznaczne z zaoferowaniem przedmiotu zamówienia niezgodnego z OPZ, a tym samym skutkować odrzuceniem oferty.

Dostawa musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Unii Europejskiej. Dostarczone urządzenia muszą być fabrycznie nowe, nie eksploatowane w żaden sposób oraz nie wykorzystywane w celach prezentacyjnych lub ekspozycyjnych, a ponadto nie mogą pochodzić z odsprzedaży.

Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień gwarancyjnych.

**IV. Standard i gwarancja na system okablowania strukturalnego**

Okablowanie strukturalne na potrzeby punktów dostępowych (Access Pointów) należy wykonać w oparciu o system okablowania strukturalnego posiadanego przez Zamawiającego (Użytkownika) m.in. w blokach C i D Szpitala. Wykonana instalacja ma zostać włączona w zakres gwarancji udzielonej przez producenta na system okablowania strukturalnego w budynkach Kujawsko - Pomorskiego Centrum Pulmonologii w Bydgoszczy.

Gwarancja na system okablowania strukturalnego ma spełniać poniższe warunki:

1. 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);
2. ma obejmować całość okablowania miedzianego wraz z kablami krosowymi i przyłączeniowymi oraz innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda RJ45, wieszaki, szafy itp.;
3. minimalny czas trwania 25 lat ma być udzielany na oficjalnych warunkach, ogólnie znanych i opublikowanych;
4. gwarancja ma być udzielona przez producenta okablowania bezpośrednio Inwestorowi/Użytkownikowi.

Producent systemu okablowania w swojej gwarancji systemowej ma zapewniać:

1. gwarancję materiałową (w przypadku wykrycia wady lub usterki fabrycznej, produkty wadliwe zostaną naprawione bądź wymienione);
2. gwarancję parametrów łącza/kanału (parametry łączy stałych bądź kanałów będą przewyższać wskazaną klasę okablowania w ciągu trwania całego okresu gwarancyjnego);
3. 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

Wykonawca ma posiadać aktualną umowę zawartą bezpośrednio z producentem okablowania regulującą uprawnienia, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi.

Wykonawca ma posiadać i przedstawić Inwestorowi (lub Użytkownikowi końcowemu) dyplomy ukończenia kursów kwalifikacyjnych, przez zatrudnionych pracowników w zakresie:

1. instalacji;
2. pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń;
3. 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 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, panele krosowe, kable krosowe) 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.

1. Lokalizacja poszczególnych gniazd na potrzeby punktów dostępowych (Access Pointów), została wskazana na rzutach przekazanych przez Zamawiającego (załącznik nr 3 do projektu umowy). Miejsca instalacji to budynki przy ulicach Meysnera 9 i Seminaryjnej 1 w Bydgoszczy. Gniazda nad sufitem podwieszanym należy montować w puszkach 45x45mm natynkowych mocowanych do stropu lub ścian.
2. Okablowanie poziome ma być zbudowane w oparciu o kabel ekranowany S/FTP kat. 7A (1000 MHz) w osłonie zewnętrznej klasy B2ca

* Wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z normą PN-EN 50173-1;
* Wszystkie łącza okablowania poziomego zakańczane na kablu kat.7A mają zapewniać:

W momencie instalacji systemu w osprzęcie połączeniowym ma być zapewniony dostęp do gniazda RJ45 o wydajności kat.6A;

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/IEC11801 lub EN50173-1: RJ45, ARJ45, TERA złącze F.

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,

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,

* System ma zapewniać możliwość wielokrotnej zmiany typu gniazda, jego kategorii oraz współdzielenie 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, wymiany osprzętu (płyty czołowe), ponownego wykonywania pomiarów oraz instalowania dodatkowych elementów w postaci paneli krosowych i płyt czołowych w punktach logicznych.

Nie dopuszcza się stosowania gniazd i wtyków z niestandardowymi interfejsami (takimi, do których nie ma referencji w dokumentach z Rozdziału V.

**Administracja i dokumentacja**

Wszystkie kable muszą 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 panelu 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 ma być zgodne z normą PN-EN 50346 A1+A2. 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 informacje 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 wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX5000);

pomiary sieci miedzianej należy wykonać w konfiguracji pomiarowej łącza stałego na zgodność z ISO/IEC11801 lub EN50173-1 - Klasa EA dla wszystkich torów transmisyjnych.

pomiary kabli krosowych RL i NEXT;

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.

protokół pomiarowy każdego kabla krosowego miedzianego ma zawierać:

mapę połączeń;

RL;

NEXT.

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.

Zamawiający oświadcza, że posiada system Commscope AMP CO Ultra z wykorzystaniem kabla kategorii 7A