



**PROGRAM
REGIONALNY**
NARODOWA STRATEGIA SPÓJNOŚCI



UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2007-2013. Projekt jest również współfinansowany z budżetu Samorządu Województwa Śląskiego, Miasta Katowice, Ministerstwa Nauki i Szkolnictwa Wyższego, Uniwersytetu Ekonomicznego w Katowicach, Uniwersytetu Śląskiego w Katowicach.

CENTRUM INFORMACJI NAUKOWEJ I BIBLIOTEKA AKADEMICKA

www.ciniba.us.edu.pl lub www.ciniba.ae.katowice.pl

RU/DW/134/11

Załącznik nr 2

Opis przedmiotu zamówienia

nr indeksu 30021

1. Założenia wstępne.

System dostępu bezprzewodowego będzie stanowił rozszerzenie sieci LAN, przy czym ta metoda dostępu pozycjonowana jest do konkretnych grup użytkowników i urządzeń końcowych. W szczególności należy wymienić tu podział na trzy grupy:

- WiFi External - dostęp do sieci publicznej dla każdego użytkownika znajdującego się w zasięgu sieci bezprzewodowej,
- WiFi Internal Readers – dostęp dla użytkowników zewnętrznych zweryfikowanych w jednym z kilku systemów LDAP,
- WiFi Internal Job – dostęp dla urządzeń zautentykowanych poprzez autentykację użytkownika w AD lub przy pomocy adresu MAC urządzenia.

Niezbędne jest aby system dostępu bezprzewodowego oparty był o technologie ustandaryzowane, zapewniające obsługę możliwie szerokiego spektrum urządzeń klienckich.

Dodatkowo w drugim etapie, przewiduje się implementację usług rozszerzonych, takich jak:

- monitorowanie pasma radiowego pod kątem obecności nieautoryzowanych urządzeń,
- lokalizacja i neutralizacja nieautoryzowanych urządzeń bezprzewodowych,

- monitorowanie lokalizacji wybranych urządzeń i zasobów.

Sieć bezprzewodowa musi zatem zapewniać:

- objęcie zasięgiem radiowym wyznaczonego obszaru Biblioteki, w szczególności części współdzielonych, sal konferencyjnych, czytelní, oraz w drugim etapie obszarów magazynowych nie objętych tym postępowaniem;
- wysoką skalowalność, gwarantującą zarówno możliwość zagęszczenia punktów dostępowych, jak też zapewnienia wysokiej wydajności,
- automatyzację zarządzania spektrum radiowym,
- wysoki poziom bezpieczeństwa,
- możliwość wirtualizacji (obsługi wielu segmentów sieci),
- oparcie o standardy branżowe.

2. Analiza technologiczna.

Lokalizacja punktów dostępowych.

Gęstość rozmieszczenia punktów dostępowych ma być zróżnicowana w zależności od typów obszarów – w miejscach rzadko uczęszczanych (typu pomieszczenia techniczne) zasięg sieci będzie pozwalał na korzystanie ze znacznie mniejszej liczby urządzeń , podczas gdy strefy uczęszczane (hole, czytelní, sale konferencyjne) mają posiadać typy i zagęszczenie punktów dostępowych umożliwiające uzyskanie optymalnej wydajności. Dopuszczalny jest montaż punktów dostępowych oraz anten na suficie podwieszanym. Do podłączenia punktów dostępowych należy w pierwszej kolejności wykorzystać istniejące punkty łączeniowe umieszczone na suficie.

Uwaga: Specyfika sieci bezprzewodowych powoduje, iż rozmieszczenie projektowe będzie musiało być na etapie przedimplementacyjnym zweryfikowane przez przeprowadzenie pomiarów propagacji sygnału.

Wyróżnione zostały trzy typy punktów dostępowych:

- *Typ I o maksymalnie wysokiej wydajności* , są to punkty dostępowe 3x3 MIMO zgodne ze standardem 802.11a/b/g/n posiadające dwa moduły radiowe (2,4GHz i 5GHz), o wbudowanych lub zewnętrznych antenach posiadające funkcjonalność monitorowania środowiska radiowego obsługujące hole, czytelní, sale konferencyjne, o przepustowości przynajmniej 300Mbps,

- *Typ II o wysokiej wydajności*, są to punkty dostępowe 2x2 MIMO zgodne ze standardem 802.11a/b/g/n posiadające dwa moduły radiowe (2,4GHz i 5GHz), posiadające funkcjonalność monitorowania środowiska radiowego, o wbudowanych antenach obsługujące pozostałe pomieszczenia o dużej liczbie użytkowników, o przepustowości przynajmniej 300 Mbps,
- *Typ III o standardowej wydajności (przewidziane do instalacji w drugim etapie)* , są to punkty dostępowe 2x2 MIMO zgodne ze standardem 802.11a/b/g/n posiadające przynajmniej jeden moduł radiowy (2,4GHz lub 5GHz), posiadające funkcjonalność monitorowania środowiska radiowego, o wbudowanych lub zewnętrznych antenach, obsługujące pomieszczenia o mniejszej ilości użytkowników (np. pomieszczenia techniczne).

Wszystkie zastosowane punkty dostępowe mają posiadać mechanizmy zwiększania czułości odbiorczej przez korelację sygnałów z kilku anten i odbiorników.

3. Standardy transmisji.

Wybudowana sieć bezprzewodowa ma być w pełni zgodna ze standardem 802.11n umożliwiającym uzyskanie przepustowości sieci rzędu 300Mbps. Wszystkie punkty dostępowe typu I i typu II mają posiadać możliwość jednoczesnej pracy w dwóch zakresach częstotliwości: 2,4GHz i 5GHz. Wszystkie urządzenia mają posiadać certyfikację zgodności WiFi Alliance. Biorąc pod uwagę charakterystykę użytkowników systemu, część transmisji będzie się odbywać bez ochrony kryptograficznej, jednak dla grup wewnętrznych (np. dostęp do aplikacji) konieczne jest zapewnienie autoryzacji i ochrony kryptograficznej. Należy użyć standardu 802.11i/WPA2 w wersji Enterprise. Używa on ram autoryzacyjnych zgodnych z 802.1x i szyfrowania AES-CCMP. Jest to aktualnie najsilniejszy standardowy mechanizm ochronny transmisji bezprzewodowej WiFi.

Wybudowana sieć bezprzewodowa ma umożliwiać kreowanie przynajmniej 32 segmentów sieciowych w oparciu o oddzielne SSID (identyfikator segmentu sieci bezprzewodowej), które na poziomie kontrolerów mają być mapowane do odpowiednich segmentów sieci LAN oraz wspierać najpopularniejszy używany aktualnie standard – 802.11e/WMM.

4. Zarządzanie systemem.

Zamawiający wymaga, aby sieć dostępu bezprzewodowego została wybudowana w oparciu o przynajmniej jeden kontroler WLAN z możliwością rozbudowy w drugim etapie o kolejne kontrolery, które będą pracowały redundantnie z wcześniej dostarczonymi kontrolerami. Taka architektura ma zapewnić:

- Konfigurację sieci bezprzewodowej z jednego miejsca, w oparciu o szablony konfiguracyjne
- Koordynację i automatyzację zarządzania pasmem radiowym (automatyczny dobór kanałów i mocy nadajników, optymalizację pokrycia)
- Wyeliminowanie pojedynczego punktu awarii systemu (po rozbudowie w drugim etapie) – w przypadku awarii kontrolera jego rolę ma przejąć kontroler zapasowy, w przypadku awarii punktu dostępowego sąsiednie urządzenia mają zwiększyć moc nadawczą w celu wyeliminowania obszaru bez pokrycia
- Możliwość implementacji usług dodatkowych (po rozbudowie w drugim etapie), takich jak: lokalizacji zasobów i klientów, wykrywania i neutralizacji nieautoryzowanych urządzeń.

System kontroli punktów dostępowych ma być zbudowany zgodnie ze standardami, w oparciu o protokół CAPWAP.

5. Topologia.

System dostępu bezprzewodowego ma zostać zbudowany w oparciu o centralny moduł kontrolny zapewniający wysoką dostępność. Punkty dostępowe mają być rozmieszczone zgodnie z wykonanym na podstawie wykonanych pomiarów zrealizowanym w ramach tego zamówienia i zatwierdzonym przez Zamawiającego projektem i dołączone do przełączników dostępowych za pomocą łączy miedzianych 1Gbps. Zasilanie punktów dostępowych ma być realizowane przez kabel Ethernet z dostarczonych przez Wykonawcę zasilaczy lub jeśli będzie to możliwe bezpośrednio z portów przełączników posiadanych przez Zamawiającego, a w przypadku punktów dostępowych o poborze mocy przekraczającym standard 802.3af za każdym razem za pomocą dedykowanego zasilacza dodatkowego.

6. Wymagania techniczne dla rozwiązań.

Dla zapewnienia jednolitości i możliwości prostej rozbudowy wszystkie elementy z których zbudowany ma być system dostępu bezprzewodowego muszą być w pełni kompatybilne (kontroler, punkt dostępowy, system zarządzania) tj. każdy z elementów użytych do budowy systemu musi mieć publicznie dostępne świadectwa kompatybilności wystawione przez producenta pozostałych użytych w systemie komponentów. W przypadku użycie komponentów od tego samego producenta nie są one potrzebne.

Kontroler/y WLAN

- urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
 - zarządzanie politykami bezpieczeństwa

- wykrywanie intruzji
 - zarządzanie pasmem radiowym
 - zarządzanie mobilnością
 - zarządzanie jakością transmisji
- kontroler WLAN musi łączyć w jednym fizycznym urządzeniu funkcjonalności:
- kontrolera sieci bezprzewodowej,
 - urządzenia zapory ogniowej (ang. Statefull firewall) dla co najmniej 96 punktów dostępowych w chwili dostawy,
 - możliwość pracy jako VPN gateway (możliwość rozbudowy o funkcję VPN IPsec),
- zarządzanie zgodnie z protokołem CAPWAP (RFC 5415) min. 96-ma punktami
- dostępowymi,
- należy dostarczyć kontroler wraz z licencjami pozwalającymi na zrealizowanie opisanych poniżej funkcjonalności,
- możliwość rozbudowy obsługiwanej przez kontroler liczby punktów dostępowych do min. 128 jedynie przez dołożenie licencji,
- min. 4 interfejsy GE dual mode (10/100/1000Base-T i slot 1000BaseX SFP) z możliwością agregacji pasma –wyposażenie w 4 moduły światłowodowe multimodowe,
- możliwość obsługi co najmniej 2048 użytkowników przez pojedynczy kontroler,
- możliwość obsługi co najmniej 512 wyniesionych punktów dostępowych (poza siecią lokalną, oddzielonych siecią WAN, wyposażonych w funkcjonalność lokalnej zapory ogniowej),
- możliwość obsługi minimum 128000 aktywnych sesji zapory ogniowej,
- wydajność dla usługi zapory ogniowej co najmniej na poziomie 4Gbps,
- wydajność dla szyfrowania ruchu AES CBC 256 na poziomie co najmniej 8 Gbps,
- wydajność dla szyfrowania ruchu AES-CCM na poziomie co najmniej 4Gbps,
- obsługa 64000 adresów MAC,
- zarządzanie pasmem radiowym punktów dostępowych
- automatyczna adaptacja do zmian w czasie rzeczywistym
 - optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
 - dynamiczne przydzielanie kanałów radiowych
 - wykrywanie, eliminacja i unikanie interferencji

- równoważenie obciążenia punktów dostępowych (rozkład użytkowników pomiędzy punkty dostępowe i poszczególne moduły radiowe)
- obsługa mechanizmów optymalizacji ruchu multicast – IGMP snooping
- obsługa mechanizmów związanych z bezpieczeństwem i kontrolą:
 - 802.11i, WPA2, WPA, WEP,
 - 802.1x z EAP (EAP-PEAP, EAP-TLS, EAP dla usług AAA, EAP-TTLS)
 - weryfikacja tożsamości nadawcy na zasadzie per-packet,
 - autentykacja w oparciu o definiowany portal Web,
 - autentykacja w oparciu o MAC, SSID, lokalizację,
 - konfigurowalne polityki dla użytkowników typu „gość”,
 - wsparcie pracy w trybie wielu usług SSID dla wielu sieci WLAN,
 - współpraca z mechanizmami zaawansowanej kontroli dostępu do sieci (typu NAC, NAP lub równoważne) – wymuszanie polityki dostępu na poziomie kontrolera,
 - wsparcie dla serwerów RADIUS, TACACS+ oraz LDAP,
 - współpraca z przynajmniej pięcioma serwerami autentykacji,
 - selekcja serwera RADIUS w oparciu o SSID,
 - funkcjonalność lokalnej bazy użytkowników,
 - możliwość profilowania użytkowników
 - przydział sieci VLAN,
 - minimum 128 interfejsów VLAN IP,
 - aplikowanie polityk bezpieczeństwa w czasie rzeczywistym, bez restartów usługi lub urządzenia,
 - jednoczesne wsparcie dla sieci WLAN scentralizowanych (kampusowych) oraz wyniesionych (zdalnych),
 - funkcjonalność zapory ogniowej (stateful firewall), aplikowana do poszczególnych użytkowników lub portów,
 - obsługa translacji adresów NAT,
 - wykrywanie i zabezpieczanie przed atakami TCP, ICMP Denial of Service,
- urządzenie ma wspierać następujące funkcjonalności związane z usługami sieci WLAN:
 - obsługa transmisji danych oraz głosu przez jeden SSID,

- mechanizm zapewnienia jakości usług QoS oparty o VFC (voice flow classification),
 - 802.11e WMM, U-APSD, T-SPEC,
 - architektura DiffServ, 802.1p QoS,
 - CAC – Call Admission Control – z wykorzystaniem VFC,
 - kontrakty na pasmo dostępne w oparciu o użytkownika lub rolę (grupę użytkowników),
 - możliwość jednoczesnego monitorowania (nasłuchu) spektrum radiowego oraz obsługi użytkowników końcowych,
 - równoważenie (load-balancing) w oparciu o ilość użytkowników zarejestrowanych na dany punkt dostępowy lub użycie pasma,
 - wykrywanie „dziur” oraz przestrzeni zakłóceń (interferencji) w pokryciu zasięgiem, mechanizm automatycznego i dynamicznego przeciwdziałania tego typu zjawiskom,
 - usługi lokalizacyjne dla użytkowników końcowych, RFID,
 - przełączanie w warstwie 2 i 3,
 - VLAN mobility dla warstwy 2,
 - wbudowany serwer DHCP oraz funkcjonalność DHCP relay,
 - możliwość budowy redundantnych klastrów VRRP N+1
- urządzenie powinno wspierać następujące funkcjonalności związane z wykrywaniem i przeciwdziałaniem nadużyciom:
- możliwość uruchomienia wybranych punktów dostępowych w trybie monitorowania spektrum radiowego ,
 - wykrywanie wrogich punktów dostępowych oraz wizualizacji ich lokalizacji,
 - automatyczne klasyfikowanie wykrytego zagrożenia (wrogie punkty dostępowe, urządzenie powodujące zakłócenia w sieci, urządzenie nieuwierzytelnione itp.),
 - wykrywanie i blokowanie sieci typu Ad-hoc,
 - wykrywanie udostępniania sieci WLAN przez użytkowników końcowych, tzw. bridging,
 - zabezpieczenie przed atakami typu DoS dla punktów dostępowych, wykrywanie ataków typu Floyd, Airjack, fałszywych punktów dostępowych,
 - elastyczne definiowanie nowych sygnatur ataków w sieci bezprzewodowej,
- urządzenie powinno wspierać następujące funkcjonalności związane z szyfrowaniem ruchu sieciowego (po zastosowaniu opcjonalnej licencji):

- zestawianie tuneli IPSec VPN typu site-to-site, także z urządzeniami innych producentów,
 - terminowanie połączeń VPN site-to-client w oparciu o L2TP/IPSec dla użytkowników MSWindows,
 - terminowanie połączeń VPN w oparciu o XAUTH/PPTP,
 - współpraca z serwerami RADIUS oraz LDAP dla tunelowania VPN,
 - wsparcie mechanizmów autentykacji PAP, CHAP, MS-CHAP, MS-CHAPv2,
 - sprzętowe szyfrowanie DES, 3DES, AES, MPPE,
 - szyfrowanie połączeń point-to-point w warstwie 2,
- urządzenie powinno dysponować następującymi certyfikatami:
- FCC part 15 Class A CE,
 - znak CE,
 - EN 55022 ClassA
- możliwość instalacji w szafie rack 19" (wymagane wyposażenie montażowe).

Punkt dostępowy Typu I

- Punkt dostępowy współpracujący bezbłędnie z kontrolerem będącym przedmiotem przetargu.
- Minimum dwa moduły radiowe z możliwością jednoczesnej pracy,
- Praca w standardzie 802.11a/n oraz 802.11b/g/n, zintegrowane anteny 3x3MIMO dual-band o zysku co najmniej 3,0dBi dla pasma 2.4GHz oraz 5.0dBi dla pasma 5GHz lub możliwość podłączenia w wybranych punktach dedykowanych anten zewnętrznych,
- Współpraca z zasilaniem 802.3af PoE oraz 802.3at PoE+ oraz możliwość podłączenia zewnętrznego zasilania 5V DC,
- Interfejsy: dwa porty 10/100/1000 RJ-45 (Dual homing) z funkcjonalnością auto MDI/MDX,
- Dedykowany port konsoli,
- Urządzenie musi wspierać następujące standardy:
 - Technologie:
 - 802.11b: Direct-Sequence Spread-Spectrum (DSSS)
 - 802.11a/g/n: Orthogonal Frequency Division Multiplexing (OFDM)
 - 802.11n High-Throughput (HT) support: HT 20/40

- 802.11n Packet Aggregation: A-MPDU, A-MSDU
- Modulacje:
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM
- Prędkości transmisyjne:
 - 802.11b: 1, 2, 5.5, 11
 - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - 802.11n: MCS0 to MCS15 (6.5 Mb/s to 300 Mb/s)
- Możliwość pracy w trybie punktu dostępowego, monitora RF (monitorowania fal radiowych) lub obu tych trybach jednocześnie,
- możliwość identyfikacji zakłóceń i interferencji w środowisku radiowym, w tym również urządzeń takich jak kuchenki mikrofalowe, urządzenia Bluetooth, DECT, możliwość identyfikacji źródła zakłócenia, możliwość zlokalizowanie go na mapie,
- Automatyczne zarządzanie mocą nadawania oraz pokrycia zasięgiem (ARM),
- Inkrementacja mocy nadawania co 0.5 dBm,
- Wsparcie minimum 32 SSID na punkt dostępowy,
- VLAN load balancing,
- Call Admission Control ,
- Wsparcie dla wireless multimedia QoS (WMM),
- Filtrowanie ruchu multicast,
- Funkcja oszczędzania energii (U-APSD),
- Klasyfikacja ruchu, rezerwacja pasma (T-SPEC/TCLAS),
- Możliwość regulacji mocy sygnału przez system zarządzania,
- Waga urządzenia nie większa niż 0.5kg,
- Certyfikacja dla regulacji:
 - FCC Part 15,
 - Znak CE,
 - EN 300 328,
 - EN 301 893,
 - EN 301 489,
 - Dyrektywy 1995/5/EC, 72/23/EEC,
 - UL/IEC/EN 60950,
- liczba dostarczonych, skonfigurowanych i zainstalowanych punktów dostępowych Typu I nie powinna być mniejsza niż 40 sztuk w tym 20 sztuk z antenami zewnętrznymi. Wszystkie punkty dostępowe powinny zostać dostarczone wraz z dedykowanymi zestawami montażowymi.

Punkt dostępowy Typu II

- Punkt dostępowy współpracujący bezbłędnie z kontrolerem będącym przedmiotem przetargu.
- Minimum dwa moduły radiowe z możliwością jednoczesnej pracy,
- Praca w standardzie 802.11a/n oraz 802.11b/g/n, zintegrowane anteny 2x2 MIMO dual-band o zysku co najmniej 2.5dBi dla pasma 2.4GHz oraz 4.0dBi dla pasma 5GHz,
- Współpraca z zasilaniem 802.3af PoE oraz 802.3at PoE+ oraz możliwość podłączenia zewnętrznego zasilania 12V DC,
- Maksymalne zużycie mocy na nie większe niż 13W,
- Interfejsy 10/100/1000 RJ-45 z funkcjonalnością auto MDI/MDX,
- Dedykowany port konsoli,
- Urządzenie musi wspierać następujące standardy:
 - o Technologie:
 - 802.11b: Direct-Sequence Spread-Spectrum (DSSS)
 - 802.11a/g/n: Orthogonal Frequency Division Multiplexing (OFDM)
 - 802.11n High-Throughput (HT) support: HT 20/40
 - 802.11n Packet Aggregation: A-MPDU, A-MSDU
 - o Modulacje:
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM
 - o Prędkości transmisyjne:
 - 802.11b: 1, 2, 5.5, 11
 - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - 802.11n: MCS0 to MCS15 (6.5 Mb/s to 300 Mb/s)
- Możliwość pracy w trybie punktu dostępowego, monitora RF (monitorowania fal radiowych) lub obu tych trybach jednocześnie,
- możliwość identyfikacji zakłóceń i interferencji w środowisku radiowym, w tym również urządzeń takich jak kuchenki mikrofalowe, urządzenia Bluetooth, DECT, możliwość identyfikacji źródła zakłócenia, możliwość zlokalizowanie go na mapie,
- Automatyczne zarządzanie mocą nadawania oraz pokrycia zasięgiem (ARM),
- Inkrementacja mocy nadawania co 0.5 dBm,
- Wsparcie minimum 32 SSID na punkt dostępowy,

- VLAN load balancing,
- Call Admission Control ,
- Wsparcie dla wireless multimedia QoS (WMM),
- Filtrowanie ruchu multicast,
- Funkcja oszczędzania energii (U-APSD),
- Klasyfikacja ruchu, rezerwacja pasma (T-SPEC/TCLAS),
- Zabezpieczenie fizyczne przed kradzieżą punktu mocowania,
- Możliwość regulacji mocy sygnału przez system zarządzania,
- Wymiary zewnętrzne urządzenia nie większe niż: 135 x 135 x 45 [mm],
- Waga urządzenia nie większa niż 0.3kg,
- Certyfikacja dla regulacji:
 - FCC Part 15,
 - Znak CE,
 - EN 300 328,
 - EN 301 893,
 - EN 301 489,
 - Dyrektywy 1995/5/EC, 72/23/EEC,
 - UL/IEC/EN 60950,
- Liczba dostarczonych, skonfigurowanych i zainstalowanych punktów dostępowych Typu II nie powinna być mniejsza niż 40 sztuk. Wszystkie punkty dostępowe powinny zostać dostarczone wraz z dedykowanymi zestawami montażowymi.

Punkt dostępowy Typu III

- Punkt dostępowy współpracujący bezbłędnie z kontrolerem będącym przedmiotem przetargu.
- Minimum jeden moduł radiowy,
- Praca w standardzie 802.11a/n lub 802.11b/g/n, zintegrowane anteny 2x2 MIMO o zysku co najmniej 2.5dBi dla pasma 2.4GHz oraz 5.0dBi dla pasma 5GHz lub możliwość podłączenia dedykowanych zewnętrznych anten,
- Współpraca z zasilaniem 802.3af PoE oraz 802.3at PoE+ oraz możliwość podłączenia zewnętrznego zasilania 12V DC,
- Maksymalne zużycie mocy na nie większe niż 11W,
- Interfejsy 10/100/1000 RJ-45 z funkcjonalnością auto MDI/MDX,

- Dedykowany port konsoli,
- Urządzenie musi wspierać następujące standardy:
 - Technologie:
 - 802.11b: Direct-Sequence Spread-Spectrum (DSSS)
 - 802.11a/g/n: Orthogonal Frequency Division Multiplexing (OFDM)
 - 802.11n High-Throughput (HT) support: HT 20/40
 - 802.11n Packet Aggregation: A-MPDU, A-MSDU
 - Modulacje:
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM
 - Prędkości transmisyjne:
 - 802.11b: 1, 2, 5.5, 11
 - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - 802.11n: MCS0 to MCS15 (6.5 Mb/s to 300 Mb/s)
- Możliwość pracy w trybie punktu dostępowego, monitora RF (monitorowania fal radiowych) lub obu tych trybach jednocześnie,
- możliwość identyfikacji zakłóceń i interferencji w środowisku radiowym, w tym również urządzeń takich jak kuchenki mikrofalowe, urządzenia Bluetooth, DECT, możliwość identyfikacji źródła zakłócenia, możliwość zlokalizowanie go na mapie,
- Automatyczne zarządzanie mocą nadawania oraz pokrycia zasięgiem (ARM),
- Inkrementacja mocy nadawania co 0.5 dBm,
- Wsparcie minimum 32 SSID na punkt dostępowy,
- VLAN load balancing,
- Call Admission Control ,
- Wsparcie dla wireless multimedia QoS (WMM),
- Filtrowanie ruchu multicast,
- Funkcja oszczędzania energii (U-APSD),
- Klasyfikacja ruchu, rezerwacja pasma (T-SPEC/TCLAS),
- Możliwość regulacji mocy sygnału przez system zarządzania,
- Wymiary zewnętrzne urządzenia nie większe niż: 135 x 135 x 45 [mm],

- Waga urządzenia nie większa niż 0.3kg,
- Certyfikacja dla regulacji:
 - FCC Part 15,
 - Znak CE,
 - EN 300 328,
 - EN 301 893,
 - EN 301 489,
 - Dyrektywy 1995/5/EC, 72/23/EEC,
 - UL/IEC/EN 60950,

Punkty dostępne Typu III są przewidziane w drugim etapie i system ma być z nimi zgodny. W swojej ofercie Wykonawca zobowiązany jest do wskazania typu urządzeń spełniających warunki opisane powyżej.

System zarządzania WLAN- przewidziany w drugim etapie nie objęty tym postępowaniem (wymagania dotyczące przyszłych prac integracyjno - wdrożeniowych)

Wymagania ogólne dla systemu zarządzania rozwiązaniem sieci bezprzewodowej:

- aplikacja instalowana na serwerze sprzętowym umożliwiającą centralne zarządzanie rozwiązaniem sieci bezprzewodowej (punktami dostępowymi, kontrolerami),
- monitorowanie w czasie rzeczywistym użytkowników, sesji i urządzeń z zaznaczeniem wysycenia pasma, siły sygnału radiowego, QoS,
- przechowywanie logów przez 2 lata,
- wykrywanie wrogich punktów dostępowych w sieci bezprzewodowej oraz przewodowej i wskazanie prawdopodobnego miejsca wykrycia m.in. poprzez triangulację sygnału,
- automatyzacja i dystrybucja wymiany wersji oprogramowania urządzeń,
- wizualizacja mapy pokrycia/zasięgu sygnału sieci bezprzewodowej,
- wizualizacja alertów i błędów wraz z możliwością dostosowywania parametrów progów i parametrów wyzwalających,
- możliwość zapewnienia funkcjonalności failover one-to-many,
- wykrywanie urządzeń przy pomocy protokołów: SNMP, http, CDP,
- czasowe sprawdzanie konfiguracji punktów dostępowych względem poprawności zdefiniowanej polityki.

System zarządzania WLAN jest przewidziany do instalacji w drugim etapie. Jeśli jest to uzasadnione merytorycznie Zamawiający dopuszcza dostawę przez Wykonawcę systemu skonfigurowanego wg powyższych założeń.

7. Wymagania gwarancyjno – serwisowe

- Wszystkie dostarczone komponenty sprzętowe i programowe muszą być fabrycznie nowe i pochodzić z oficjalnego źródła dystrybucji na terenie Polski.
- Wymagany jest 36 miesięczny serwis gwarancyjny na wszystkie dostarczone urządzenia w następującym zakresie:
 - przyjmowanie zgłoszeń w godzinach od 8:00-16:00 w dni robocze,
 - naprawa lub wymiana na miejscu kontrolera WLAN w następny dzień roboczy od pisemnego zgłoszenia awarii (faxem lub mailem),
 - naprawa lub wymiana na miejscu (wraz ze zdjęciem uszkodzonego i powieszeniem sprawnego) punktu dostępowego WLAN w czasie do pięciu dni roboczych od pisemnego zgłoszenia awarii (faxem lub mailem),
 - bezpośredni dostęp do wsparcia technicznego producenta sprzętu
 - prawo do bezpłatnej aktualizacji oprogramowania systemowego
- Serwis gwarancyjny musi być oparty na świadczeniach gwarancyjnych producenta.