

Spis treści:

Tom I:

1. Przedmiot opracowania.....	3
2. Podstawa opracowania.....	3
3. Zakres projektu.....	3
4. Przyjęte założenia.....	3
5. Stan projektowany.....	3
6. Uwagi końcowe.....	18
7. Rysunki.	19

Tom II:

1. Raport Budynki A, B, C, D, H.
2. Raport Budynek Pralni i Kuchni.
3. Raport Budynek Wielofunkcyjny
4. Raport Budynek Bakteriologii
5. Raport Budynek Kotłownii

1. Przedmiot opracowania

Przedmiotem opracowania jest wykonanie sieci bezprzewodowej WiFi na terenie budynków WSS w Elblągu oraz dla potrzeb lądowiska.

2. Podstawa opracowania.

Podstawą opracowania dokumentacji jest:

- zlecenie na wykonanie dokumentacji projektowej,
- uzgodnienia z inwestorem,
- uzgodnienia międzybranżowe,
- aktualne przepisy i normy,
- przeprowadzone badania i symulacja poprawności działania łączności radiowej

Projekty związane:

- projekt budowlany budowy Data Center WSZ w Elblągu,
- projekt budowlany pn.: „Logiczna sieć komputerowa wraz z dedykowanym zasilaniem” opracowanym przez firmę Przedsiębiorstwo Elektroniczne DAMIR S.C.

3. Zakres projektu.

Budowa sieci bezprzewodowej WiFi obejmuje:

- montaż urządzeń dostępu bezprzewodowego (Access Point - AP),
- montaż okablowania telekomunikacyjnego pomiędzy AP a punktem dostępowym sieci teleinformatycznej (szafy PD),
- montaż przełączników sieciowych dostępowych w szafach PD,
- montaż kontrolerów sieci WiFi,
- instalacja systemu zarządzania infrastrukturą aktywną.

4. Przyjęte założenia.

Na terenie WSS w Elblągu wykonana zostanie sieć szkieletowa wraz z serwerownią zgodnie z projektami:

- projekt budowy Data Center WSZ w Elblągu,
- projekt pn.: „Logiczna sieć komputerowa wraz z dedykowanym zasilaniem” opracowanym przez firmę Przedsiębiorstwo Elektroniczne DAMIR S.C.

Zakłada się, że w głównych ciągach komunikacyjnych zachowane będą zabudowy sufitów oraz nie zmieni się aranżacja pomieszczeń w sposób istotny, tzn. wymagający ponownej symulacji poprawności działania sieci WiFi.

5. Stan projektowany.

Sieć bezprzewodowa musi być oparta na standardach: 802.11a/b/g/n/ac. Obecnie najlepszym rozwiązaniem jest koncepcja oparta o kontroler oraz punkty dostępowe. Poza umożliwieniem dostępu do zasobów sieciowych dla użytkowników oraz gości możliwe jest wykorzystanie sieci bezprzewodowej WiFi również zorganizowania przenośnej telefonii IP.

Przełączniki WLAN to kontrolery stworzone z myślą o zaawansowanych usługach WLAN. Przełączniki będą posiadały te same zaawansowane funkcjonalności i najlepsze zabezpieczenia w swojej klasie, a także obsługę wymagających funkcjonalności takich

jak Voice over WLAN (VoWLAN). Ponadto powinny cechować się uproszczoną instalacją, monitorowaniem i rozwiązywaniem problemów infrastruktury WLAN. Przełączniki agregują ruch punktów dostępowych, przetwarzają go i przenoszą do sieci.

Wymagane funkcje systemu łączności bezprzewodowej:

- obsługa dużego ruchu generowanego przez wydajne sieci IEEE 802.11n i ac;
- możliwość wdrożenia jako dodatkowej warstwy w już istniejącej sieci, bez przerywania jej działania;
- uproszczony nadzór poprzez minimalizację liczby elementów sieci;
- analiza przestrzeni radiowej i wykorzystanie samo dostrajających się punktów dostępowych, co pozwala na tworzenie sieci z nadzorem w czasie rzeczywistym;
- integracja sieci bezprzewodowej i systemu wykrywania oraz zapobiegania wtargnięciom do sieci obniżająca koszty tworzenia i działania sieci bezprzewodowej;
- wgląd w przyczyny zakłóceń radiowych dzięki wbudowanemu analizatorowi spektrum;
- uniemożliwienie niepowołanym osobom połączenie z siecią firmy, dający bezpieczny dostęp gościom, pracownikom i kontrahentom;
- zabezpieczenia oparte na profilach;
- możliwość śledzenia położenia użytkowników, w celu poprawy jakości informacji na temat ich dostępności;
- możliwość śledzenia zasobów ze znacznikami WiFi na terenie WSS;
- mechanizmy QoS poprawiające jakość komunikacji głosowej takie jak: WMM, DSCP, CAC;
- wydłużona żywotności baterii poprzez protokoły U-APSD;
- wbudowany wysokiej klasy firewall;
- zapewnienie ciągłości komunikacji przy przełączaniu się między punktami dostępowymi;
- wbudowaną technologię certyfikatów cyfrowych aplikacji pozwalającą na identyfikację zaszyfrowanych protokołów transmisji głosu i wideo i zastosowanie QoS;
- porty USB w przełącznikach WLAN, do których można podłączyć nośniki danych lub drukarki; urządzenia te będą dostępne z dowolnego miejsca;
- obsługa łączności 3G umożliwia błyskawiczne utworzenie sieci w przypadku braku łączności kablowej (np. DSL), służąca jako zabezpieczenie na wypadek awarii głównego łącza;
- wysoka wydajność;
- skalowalna architektura;
- scentralizowane przełączanie w sieci WLAN;
- dynamiczne zarządzanie częstotliwościami;
- zintegrowana bezprzewodowa ochrona przed intruzami;
- zintegrowana analiza spektrum;
- ochrona ukierunkowana na użytkownika ze stateful firewallem;
- certyfikaty cyfrowe aplikacji;
- QoS, wydłużona żywotność baterii, płynny roaming dla urządzeń transmitujących głos;
- wbudowany serwer drukarek i plików



PROJEKT SYSTEMU WIFI NA TERENIE WSZ W GU

Warstwa dostępową będą stanowiły urządzenia o stałej konfiguracji z 48 portów 1 Gigabit Ethernet (GigE) Ethernet i min. 4 porty 10 Gigabit Ethernet (GigE) uplink. Dzięki optymalizacji skalowania, elastyczności i niskiemu poborowi prądu przełączniki będą gwarantowały wysoką dostępność, automatyczną ochronę, prostotę zarządzania i energooszczędny charakter sieci. Wydajność w aplikacjach obsługujących musi odbywać się w czasie rzeczywistym dla głosu, danych i treści wideo w konwergentnych sieciach o wymaganej skalowalności. System powinien gwarantować oszczędne zarządzanie energią, obniżenie kosztów utrzymania i całkowitego kosztu posiadania TCO dzięki niskiemu poborowi mocy oraz dynamicznemu rozdzielaniu Power over Ethernet (PoE) dostarczającego moc tylko urządzeniom, które jej potrzebują. System posiada automatyczną konfigurację przełącznika oraz kompleksową obsługę przez virtual LAN (VLAN).

Wymagania dla przełączników dostępowych.

- -

PROJEKT SYSTEMU WIFI NA TERENIE WSZ W ELBLĄGU

- możliwość przechowywania min. 12 wersji konfiguracji w plikach tekstowych w pamięci Flash;
- możliwość monitorowania zajętości CPU;
- lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring);
- wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem.

Parametry obsługi Routingu IPv4:

- sprzętowa obsługa routingu IPv4 – forwarding;
- pojemność tabeli routingu typowa dla przełącznika brzegowego min. 480 wpisów;
- routing statyczny;
- obsługa routingu dynamicznego IPv4: RIPv1/v2, OSPFv2 (możliwość rozszerzenia przez licencję oprogramowania);

Parametry obsługi Routingu IPv6

- sprzętowa obsługa routingu IPv6 – forwarding;
- pojemność tabeli routingu typowa dla przełącznika brzegowego min. 240 wpisów;
- routing statyczny;
- obsługa routingu dynamicznego IPv4: RIPv1/v2, OSPFv2 (możliwość rozszerzenia przez licencję oprogramowania);
- obsługa MLDv1 (Multicast Listener Discovery version 1);
- obsługa MLDv2 (Multicast Listener Discovery version 2);

Parametry obsługi Multicastów

- filtrowanie IGMP;
- obsługa Multicast VLAN Registration – MVR;
- obsługa IGMP v1/v2/v3 snooping;

Parametry bezpieczeństwa.

- obsługa Network Login
 - IEEE 802.1x - RFC 3580
 - Web-based Network Login
 - MAC based Network Login
- obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
- możliwość integracji funkcjonalności Network Login z Microsoft NAP;
- przydział sieci VLAN, ACL/QoS podczas logowania Network Login;
- obsługa Guest VLAN dla IEEE 802.1x;
- obsługa funkcjonalności przechwytywanie autoryzacji użytkowników;
- obsługa Identity Management;
- wbudowana obrona procesora urządzenia przed atakami DoS;
- obsługa TACACS+ (RFC 1492);
- obsługa RADIUS Authentication (RFC 2138);
- obsługa RADIUS Accounting (RFC 2139);
- RADIUS and TACACS+ pcr-command Authentication;
- bezpieczeństwo MAC adresów;
- ograniczenie liczby MAC adresów na porcie;
- zatrzaśnięcie MAC adresu na porcie;
- możliwość wpisania statycznych MAC adresów na port/vlan;

- możliwość wyłączenia MAC learning;
- obsługa SNMPv1/v2/v3;
- funkcja Klient SSH2;
- zabezpieczenie przełącznika przed atakami DoS:
 - Networks Ingress Filtering RFC 2267
 - SYN Attack Protection
 - zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania;
- listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:
 - adres MAC źródłowy i docelowy plus maska
 - adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
 - protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
 - numery portów źródłowych i docelowych TCP, UDP
 - zakresy portów źródłowych i docelowych TCP, UDP
 - identyfikator sieci VLAN – VLAN ID
 - flagi TCP
 - obsługa fragmentów
- wwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika;
- możliwość konfiguracji min. 2000 reguł na wejściu i 500 reguł na wyjściu;
- 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. – możliwość rozszerzenia przez licencję oprogramowania;
- obsługa bezpiecznego transferu plików SCP/SFTP;
- obsługa DHCP Option 82;
- obsługa IP Security - Gratuitous ARP Protection, Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation, IP Source Guard
- ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s;

Parametry bezpieczeństwa sieciowego.

- możliwość konfiguracji portu głównego i zapasowego;
- Obsługa:
 - STP (Spanning Tree Protocol) IEEE 802.1D
 - RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
 - MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
 - PVST+
 - EAPS (Ethernet Automatic Protection Switching) RFC 3619
 - G.8032
 - Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
 - MLAG - połączenie Link Aggregation do dwóch niezależnych przełączników,
 - LACP w ramach MLAG



PROJEKT SYSTEMU WIFI NA TERENIE WSZ W ELBLĄGU

Parametry zarządzania.

- obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
- obsługa synchronizacji czasu NTP
- zarządzanie przez SNMP v1/v2/v3
- zarządzanie przez przeglądarkę WWW – protokół http i https
- możliwość zarządzania poprzez protokół XML
- telnet Serwer/Klient dla IPv4 / IPv6
- SSH2 Serwer/Klient dla IPv4 / IPv6
- Ping dla IPv4 / IPv6
- Traceroute dla IPv4 / IPv6
- obsługa SYSLOG z możliwością definiowania wielu serwerów
- sprzętowa obsługa sFlow
- obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
- obsługa RMON2 (RFC 2021)

Inne parametry

- obsługa skryptów CLI
- obsługa funkcji TCL/Tk w skryptach CLI
- obsługa skryptów Python
- możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
- wsparcie dla OpenFlow – poprzez rozszerzenie licencji
- obsługa AVB (Audio Video Bridging) – poprzez rozszerzenie licencji
- możliwość zarządzania przełącznikiem z tabletów iPad i tabletów pracujących pod systemem Android
- możliwość uruchamiania skryptów ręcznie, o określonym czasie lub co wskazany okres czasu na podstawie wpisów w logu systemowym;

Cechy funkcjonalne.

- 48 portów 10/100/100 POE
- Stakowanie min 7 urządzeń
- 1 Console port
- 4 porty 10G SFP+

Wymagania dla bezprzewodowych punktów dostępowych AP

Jako punkty dostępowe accesspoint projektowane są urządzenia o minimalnych parametrach:

- standard sieci: 802.11 a/b/g/n/ac
- radio dwuzakresowe 2,4 i 5 GHz
- zasilanie PoE
- wbudowane anteny o wysokiej wydajności, zaprojektowane, aby maksymalizować wzmocnienie i minimalizować interferencje,

Wymaga się od punktów dostępowych AP pełnej obsługi funkcjonalności opisanej przy kontrolerze WiFi.

Urządzenia montowane na zewnątrz budynku do obsługi lądowiska dla helikopterów będą spełniały dodatkowo następujące wymagania środowiskowe:

- zakres temperatury pracy: -40°C do +60°C,



PROJEKT SYSTEMU WiFi NA TERENIE WSZ W ELBLĄGU

- odporność na wilgoć: IP 67

Wymagania dla kontrolera sieci WiFi.

- kontroler bezprzewodowy zarządzający min. 600 punktami dostępowymi z możliwością rozszerzenia do obsługi min. 1000 punktów dostępowych;
 - obsługa min. 8000 jednoczesnych użytkowników;
 - instalacja w szafie Rack 19”;
 - dwa odporne na awarie zasilacze AC 230V;
 - min. 2 porty 10/100/1000BASE-T oraz min 2 porty SFP+ pozwalające na dołączenie do sieci przewodowej w redundantny sposób z wykorzystaniem Link Aggregation IEEE 802.3ad;
 - dedykowany port 10/100/1000BASE-T dla zarządzania;
 - możliwość pracy w klastrze odpornym na awarię składającym się z min. dwóch kontrolerów i obsługujących w takiej konfiguracji do min. 1000 punktów dostępowych;
 - obsługa sieci VLAN zgodnych z IEEE 802.1Q;
 - automatyczne wykrywanie nowych punktów dostępowych;
 - zarządzany przez przeglądarkę www bez konieczności instalacji Java;
 - zarządzany przez SNMPv1/v2/v3 oraz SSHv2;
 - obsługa:
 - RADIUS authentication oraz RADIUS accounting;
 - 802.11i, WPA, WPA2, TKIP oraz AES
 - IEEE 802.1x
 - autentykacji: EAP-TLS, EAP-TTLS, PEAP, EAP-MD5 oraz EAP-SIM.
 - przesyłanie danych z sieci WLAN do sieci przewodowej w następujących architekturach:
 - routing na kontrolerze – kontroler pracuje w trybie klasycznego routera i zapewnia routing klientów sieci bezprzewodowej do sieci przewodowej,
 - bridging na kontrolerze – kontroler zapewnia przełączanie ruchu z sieci bezprzewodowej do wskazanej sieci wirtualnej przewodowej dołączonej do kontrolera,
 - bridging na punkcie dostępowym – w tym trybie ruch z sieci bezprzewodowej jest kierowany bezpośrednio do wskazanej sieci wirtualnej przyłączonej bezpośrednio do punktu dostępowego;
- Wszystkie punkty dostępowe muszą zapewniać realizację wskazanych powyżej architektur przesyłania danych wraz z możliwością ich zmiany przed uwierzytelnieniem i po uwierzytelnieniu dla każdego klienta.
- możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:
 - indywidualne reguły filtrowania
 - przypisanie sieci VLAN
 - QoS
 - ograniczenia transmisji wejściowej i wyjściowej
 - wyboru topologii (routowana na kontrolerze, bridging na kontrolerze, bridging na punkcie dostępowym)
 - możliwość tworzenia sieci wirtualnej dla wskazanego protokołu np. Bonjour. Klienci dołączeni do różnych sieci wirtualnych muszą mieć możliwość połączenia

PROJEKT SYSTEMU WIFI NA TERENIE WSZ W ELBLĄGU

się np. z rzutnikiem dołączonym do innej sieci wirtualnej np. w celu wyświetlenia prezentacji na projektorze obsługującym protokół Bonjour lub inny;

- obsługa portalu dla gości oraz dedykowaną stroną www dla tworzenia kont dla gości przez niewykwalifikowany personel;
- możliwość autoryzacji gości w oparciu o portal www znajdujący się na kontrolerze, a po autoryzacji zapewniać dostęp klienta do sieci przewodowej i wskazanej sieci wirtualnej w miejscu podłączenia punktu dostępowego.
- edytor html pozwalający na modyfikację portalu dla gości;
- możliwość drukowania strony zawierającej informacje o danych logowania dla gościa;
- obsługa wstępnego uwierzytelniania (Pre-Authentication)
- routing między sieciami wirtualnymi oraz zapewniać obsługę protokołu OSPF
- obsługa funkcjonalności Proxy ARP;
- konfiguracja oraz monitorowanie wszystkich dostarczonych punktów bezprzewodowych;
- automatyczna, centralna aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera;
- możliwość potwierdzania adaptacji punktów dostępowych przez administratora;
- graficzny interfejs użytkownika dostępny przez stronę www zawierający następujące informacje:
 - liczba dołączonych do kontrolera punktów dostępowych z podziałem na punkty dostępowe pracujące prawidłowo i niepracujące, ale zaadoptowane do kontrolera,
 - liczba obsługiwanych klientów bezprzewodowych na poszczególnych punktach dostępowych,
 - liczba obsługiwanych klientów z podziałem na standard przyłączonego urządzenia – np. IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac,
 - wykaz klientów bezprzewodowych z podziałem na SSID oraz punkty dostępowe. Wykaz klientów bezprzewodowych musi zawierać MAC adres klienta końcowego, przydzielony adres IP, identyfikator SSID, typ autentykacji (np. EAP/WPA), standard np. IEEE 802.11g, poziom odbieranego sygnału np. -50 dBm, nazwa użytkownika jeśli dołączenie nastąpiło z wykorzystaniem IEEE 802.1x lub jako gościa z podaniem nazwy użytkownika, czas połączenia;
- możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej.
- autoryzacja użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID;
- autoryzacja użytkowników w serwerze RADIUS w imieniu punktów dostępowych. Musi również istnieć możliwość konfiguracji grupy punktów dostępowych, które będą odpytywać serwer RADIUS lokalnie bez pośrednictwa kontrolera;
- przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580;

PROJEKT SYSTEMU WIFI NA TERENIE WSZ W ELBLĄGU

- przydzielanie polityki zawierającej QoS (Quality of Service), list kontroli dostępu ACL. Przydzielane polityki muszą być realizowane na punktach dostępowych w przypadku ruchu, który jest wpuszczany do sieci bezpośrednio na punkcie dostępowym;
- roaming pomiędzy punktami dostępowymi;
- funkcjonalność oszczędzania energii UAPSD (Unscheduled Automatic Power Save Delivery);
- musi informować o zbyt dużym obciążeniu i informacja ta może być przekazywana klientowi dla obsługi inteligentnego roamingu;
- obsługa funkcjonalności FCA (Flexible Client Access) zwiększającą prędkość transmisji klientów IEEE 802.11n w sieci z urządzeniami IEEE 802.11/a/b/g;
- obsługa funkcjonalności CAC (Call Admission Control), pozwalającą na sprawdzenie, czy zestawienie nowego połączenia telefonii VoIP nie wpłynie na jakość dotychczasowych połączeń;
- obsługa preferencji pasma polegającą na automatycznym przenoszeniu klientów na pasmo 5 GHz;

Okablowanie strukturalne

Sieć okablowania strukturalnego należy wykonać z wykorzystaniem certyfikowanego systemu okablowania strukturalnego. Minimalny okres gwarancji udzielonej przez producenta okablowania to 20 lat. Wszystkie elementy toru transmisyjnego (miedzianego i światłowodowego) powinny pochodzić od jednego producenta, który udzieli systemowej gwarancji niezawodności na sieć zainstalowaną przez certyfikowanego instalatora. Wymóg pochodzenia poszczególnych komponentów obowiązuje, co najmniej w takim zakresie elementów, jaki wyznaczył producent instalowanego okablowania, jako warunek uzyskania certyfikatu rozszerzonej gwarancji niezawodności.

Wykonawca sieci strukturalnej musi posiadać stosowny certyfikat producenta systemu uprawniający do uzyskania wydłużonej gwarancji producenta. Po zakończonych pracach, niezależnie od wymagań producenta, należy przedstawić zamawiającemu protokoły pomiarów wszystkich linków stałych wraz z elektroniczną wersją źródłową plików z urządzeń pomiarowych. Wszystkie połączenia muszą spełniać wymagania normatywne dla klas linków określonych w dokumentacji

Pomiędzy gniazdami (1xRJ45 cat.6A) punktów dostępowych AP a punktami dystrybucyjnymi okablowania szkieletowego (PD) należy wykonać połączenia miedziane klasy EA zgodnie z EN 50173. Do tego celu należy stosować komponenty kategorii 6A ekranowanej. W punktach PD dla okablowania miedzianego należy zastosować panele krosowe kątowe, umożliwiające prowadzenie patchcordów bezpośrednio na boki szafy bez dodatkowego panela porządkującego.

Po wykonaniu instalacji okablowania strukturalnego wykonawca powinien przeprowadzić odpowiednie testy i pomiary poświadczające, że okablowanie poziome spełnia standardy kategorii 6 / Klasy E, zgodnie z wymogami zawartymi w normach i ewentualne inne wymagania konieczne do wystawienia certyfikatu gwarancyjnego przez producenta okablowania. Należy sprawdzić zgodność struktury okablowania z wymaganiami norm w tym zakresie.

Minimalne wymagania dla elementów okablowania strukturalnego

1. Panel krosowy RJ45 miedziany.

- panel modułowy o wysokości 1U, z możliwością instalacji 24 modułów RJ45 ekranowanych
- listwa/ grzebień automatycznie uziemiający moduły
- moduły RJ45 montowane pod kątem - wyprowadzenie przewodów bezpośrednio na boki panela
- system umożliwiający szybki montaż i demontaż a także wyposażenia panela w boczne organizery kabli
- etykiety opisowe w centralnej części oraz na bokach panela

2. Moduł RJ45

- spełnia wymagania dla linków klasy EA wg ISO/IEC 11801:2011 Ed2.2 oraz wymagania dla kategorii 6A wg IEC 60603-7-51 i ANSI/TIA-568-C.2
- wykonanie ekranowane
- moduł jednoelementowy, terminacja kabla oraz montaż w panelu - beznarzędziowy
- samoregulujący styk ekranu dla dowolnej grubości kabla

4. Kabel FFTP kategorii 6A

- 4 pary 550MHz, AWG23.
- zgodny z EN50173, ISO/IEC 11801:2011 Ed 2.2
- FFTP ekranowanie: wspólna folia dla par i kabla
- drut uziemiający na całej długości kabla
- płaszcz LSZH
- parametry dla 500MHz straty odbicia nie gorsze niż 17,3dB; tłumienie nie gorsze niż 45,3dB; przesłuch NEXT nie gorszy niż 54,8dB, PS NEXT nie gorszy niż 51,8dB

Minimalny zakres obowiązkowych testów obejmuje pomiary łączy stałych (Permanent Link) w odniesieniu do wartości granicznych parametrów wg normy ISO/IEC 11801 lub EN 50173:

- Poprawność i ciągłość wykonanych połączeń
- Straty odbiciowe RL
- Tłumienność wtrąceniowa
- Zmniejszenie przesłuchu zbliżnego NEXT pomiędzy dwiema parami
- Sumaryczne zmniejszenie przesłuchu zbliżnego (PSNEXT)
- Współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu pomiędzy dwiema parami (ACR)
- Sumaryczny współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu (PSACR)
- Zmniejszenie przesłuchu zdalnego skorygowane w odniesieniu do długości linii transmisyjnej (ELFEXT) pomiędzy dwiema parami Sumaryczne zmniejszenie przesłuchu zdalnego skorygowane w odniesieniu do długości linii transmisyjnej (PSELFEXT)
- Rezystancja pętli stałoprądowej
- Opóźnienie propagacji
- Różnica opóźnień propagacji.

Instalacje okablowania w obrębie serwerowni układane będą w :

- metalowych kanałach siatkowych: szerokości 200 mm, wysokości 60 mm (typu KDS200H60), umieszczonych nad sufitami podwieszanymi,
- listwach kablowych PCV montowanych natynkowo poza przestrzenią nad sufitem podwieszanym lub w miejscach wskazanych na załączonych rysunkach również w przestrzeni międzysufitowej.

Elementy konstrukcyjne prowadzenia okablowania będą mocowane do stropów, ścian oraz sufitów za pomocą kołków rozporowych. Kanały po zamontowaniu nie będą wymagać dodatkowych prac związanych z ich wykończeniem, ponieważ przewidziano instalację elementów rozgałęziających, zmieniających kąt i poziom prowadzenia kanałów oraz elementy łączące. Kanały należy instalować tak, aby stanowiły jeden ciąg (wszystkie przewody powinny być na całej długości ukryte w kanałach). Kanały metalowe należy podłączyć do uziemienia budynku.

Rodzaje kanałów oraz sposób ich układania określono na planach instalacji.

Nie dopuszcza się łączenia kanałów i koryt w sposób niezgodny z zaleceniami producenta i bez elementów wykańczających trasy kablowe (łączniki kanałów, redukcje, luki itp.) Przejścia poza strefy pożarowe muszą być uszczelnione masą ogniochronną. Trasy kablowe teletechniczne powinny być ułożone nad innymi instalacjami sanitarnymi i energetycznymi.

System zarządzania infrastrukturą aktywną

W zakresie projektu jest oprogramowanie zarządzające urządzeniami aktywnymi oraz siecią bezprzewodową na terenie WSS w Elblągu. System powinien działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.

Wymagania funkcjonalne:

- zarządzanie siecią dla minimum 25 jednoczesnych użytkowników;
- możliwość uruchomienia zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego;
- definiowanie wielopoziomowych dostępu do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników;
- integracja autoryzacji użytkowników za pomocą LDAP i/lub Radius;
- wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze;
- praca na protokołach: SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
- możliwość tworzenia 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;
- przyjmowanie trapów SNMP oraz przekierowywania ich do innych systemów;
- wbudowana przeglądarka SNMP MIB;
- kompilowanie SNMP MIB różnych producentów;

PROJEKT SYSTEMU WIFI NA TERENIE WSZ W ELBLĄGU

- zarządzanie urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
- wskazywanie dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych;
- automatyczna reakcja na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu;
- wbudowany Syslog serwer;
- wbudowany BootP serwer;
- wsparcie dla protokołów IPv4 oraz IPv6;
- automatyczna realizacja backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera;
- automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora;
- tworzenie przez administratora grup urządzeń oraz portów na urządzeniach;
- wizualizacja sieci z uwzględnieniem:
 - połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości,
 - stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów,
 - konfiguracji sieci VLAN,
 - konfiguracji protokołu routingu OSPF,
- możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https;
- możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
 - adres IP urządzenia,
 - adresu MAC urządzenia,
 - nazwy urządzenia,
 - wersji oprogramowania,
 - wersji bootrom,
 - lokalizacji urządzenia,
 - danych kontaktowych administratora,
 - numeru seryjnego.
- centralne zarządzanie konfiguracjami urządzeń sieciowych, w tym:
 - automatyczna okresowa realizacja backup'u konfiguracji urządzeń o wskazanym czasie,
 - odtworzenie wskazanej konfiguracji urządzenia,
 - porównywanie różnic we wskazanych tekstowych plikach konfiguracyjnych,
 - obsługa urządzeń sieciowych różnych producentów;
- możliwość aktualizacji oprogramowania na urządzeniach sieciowych, w tym zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie;
- historia zmian konfiguracji oraz oprogramowania na urządzeniach;
- tworzenie raportów wykorzystywanych portów urządzeń sieciowych;

PROJEKT SYSTEMU WiFi NA TERENIE WSZ W ELBLĄGU

- definiowanie polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem podziału użytkowników na grupy np. Administracja, Finanse, Goście, Zarząd itp.;
- wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
 - 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).
 - 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).
 - wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
 - generowanie raportów
- Aplikacja zarządzająca musi zapewniać zarządzania siecią bezprzewodową.
 - musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
 - 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
 - musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
 - adres IP kontrolera
 - liczba obsługiwanych klientów
 - szczytowe wartości zajmowanego pasma
 - wersja oprogramowania
 - musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
 - adres IP punktu dostępowego
 - MAC adres punktu dostępowego
 - wersja oprogramowania
 - typ punktu dostępowego
 - kanały pracy poszczególnych interfejsów radiowych
 - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
 - Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
 - adres IP klienta
 - MAC adres klienta
 - nazwa użytkownika
 - nazwa punktu dostępowego, do którego dołączony jest użytkownik

PROJEKT SYSTEMU WiFi NA TERENIE WSZ W ELBLĄGU

- BSSID, do którego dołączony jest użytkownik
 - SSID, do którego dołączony jest użytkownik
- Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
 - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
 - zaznaczenie kanałów pracy urządzeń
 - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
- Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością z zapewnieniem widzialności następujących informacji:
 - adresu MAC
 - adresu IP
 - nazwy komputera
 - typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
 - nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
 - adres IP urządzenia, do którego dołączony jest klient.
 - 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.
 - typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
 - nazwa przydzielonej polityki bezpieczeństwa.
- System zarządzania tożsamością 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.;
 - możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa;
 - 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;
 - możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci;
 - zbieranie informacji dotyczących:
 - liczby urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
 - liczby urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.

PROJEKT SYSTEMU WiFi NA TERENIE WSZ W ELBLĄGU

- liczby urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
- liczby urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
- liczby urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
- liczbę użytkowników min. 12 000 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 1000 punktów dostępowych oraz min. 250 przełączników sieciowych
- możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7
- wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.
- integrację systemu zarządzania z systemami firewall takimi jak: Palo Alto i Fortinet.
- 3 letni wsparcie serwisowe producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24/7.

ZESTAWIENIE PODSTAWOWYCH MATERIAŁÓW

L.p.	Opis	Ilość	j.m.
1	Urządzenia łączności bezprzewodowej Access Point WiFi wewnętrzne	445	kpl
2	Urządzenia łączności bezprzewodowej Access Point WiFi zewnętrzne	3	kpl
3	Przełączniki sieciowe dostępne	34	kpl
4	Kontrolery sieci WiFi	2	kpl
5	Koryta siatkowe typu KDS200H60	2410	m
6	Listwy elektroinstalacyjne	3360	m
7	Kabel FFTP 4x2x0,5 kat.6A	22790	m
8	Panele krosowe 24xRJ45	34	kpl
9	Gniazda zakończeniowe 1xRJ45	445	kpl
10	Oprogramowanie zarządzające	1	Kpl

6. Uwagi końcowe.

System został zaprojektowany na podstawie przeprowadzonych badań propagacji fal radiowych oraz symulacji poprawności działania.

Zmiana parametrów urządzeń lub ich lokalizacji wymaga:

- zgody projektanta,
- przeprowadzenia nowych badań propagacji fal radiowych,
- przeprowadzenie nowej symulacji zgodnie z załączonym do projektu raportem.

7. Rysunki.

1. Schemat sieci WiFi	rys. T-1
2. Rzut - Budynek A Niski Parter	rys. T_A-1, skala 1:100
3. Rzut - Budynek A Wysoki Parter	rys. T_A-2, skala 1:100
4. Rzut - Budynek A I Piętro	rys. T_A-3, skala 1:100
5. Rzut - Budynek A II Piętro	rys. T_A-4, skala 1:100
6. Rzut - Budynek A III Piętro	rys. T_A-5, skala 1:100
7. Rzut - Budynek A IV Piętro	rys. T_A-6, skala 1:100
8. Rzut - Budynek A V Piętro	rys. T_A-7, skala 1:100
9. Rzut - Budynek A VI Piętro	rys. T_A-8, skala 1:100
10. Rzut - Budynek B Niski Parter	rys. T_B-1, skala 1:100
11. Rzut - Budynek B Wysoki Parter	rys. T_B-2, skala 1:100
12. Rzut - Budynek B I Piętro	rys. T_B-3, skala 1:100
13. Rzut - Budynek C Niski Parter	rys. T_C-1, skala 1:100
14. Rzut - Budynek C Wysoki Parter	rys. T_C-2, skala 1:100
15. Rzut - Budynek C I Piętro	rys. T_C-3, skala 1:100
16. Rzut - Budynek D Niski Parter	rys. T_D-1, skala 1:100
17. Rzut - Budynek D Wysoki Parter	rys. T_D-2, skala 1:100
18. Rzut - Budynek D I Piętro	rys. T_D-3, skala 1:100
19. Rzut - Budynek H Niski Parter	rys. T_H-1, skala 1:100
20. Rzut - Budynek H Wysoki Parter	rys. T_H-2, skala 1:100
21. Rzut - Budynek H I Piętro	rys. T_H-3, skala 1:100
22. Rzut - Budynek P+K Niski Parter	rys. T_PK-1, skala 1:100
23. Rzut - Budynek P+K Wysoki Parter	rys. T_PK-2, skala 1:100
24. Rzut - Budynek Wielofunkcyjny Niski Part	rys. T_Wf-1, skala 1:100
25. Rzut - Budynek Wielofunkcyjny Wysoki Parter	rys. T_Wf-2, skala 1:100
26. Rzut - Budynek Wielofunkcyjny I Piętro	rys. T_Wf-3, skala 1:100
27. Rzut - Budynek Wielofunkcyjny II Piętro	rys. T_Wf-4, skala 1:100
28. Rzut - Budynek Wielofunkcyjny III Piętro	rys. T_Wf-5, skala 1:100
29. Rzut – Tunel od strony bud. Wielofunkcyjnego	rys. T_Wf-6, skala 1:500
30. Rzut – Tunel od strony bud. P+K	rys. T_Wf-7, skala 1:500
31. Rzut – Budynek Bakteriologii	rys. T-BB-1, skala 1:100