Cisco Systems Poland

Sieci Bezprzewodowe

W Jednostkach Samorządu Terytorialnego

Cisco Systems Poland
Al. Jerozolimskie 146C
Warszawa, 02-305
Polska
http://www.cisco.pl

Spis treści

1. Wstęp

Zainteresowanie klientów rozwiązaniami w zakresie sieci bezprzewodowych **WLAN** (Wireless LAN) stale rośnie i to praktycznie w każdym segmencie rynku, niezależnie od branży i wielkości firmy czy instytucji. WLAN oferuje użytkownikom nieznaną dotychczas mobilność, wpływające na zwiększenie efektywności i wydajności oraz na lepszą organizację pracy. W małych jednostkach sieć bezprzewodowa może nawet całkowicie zastąpić kablową sieć stacjonarną; podobnie w halach magazynowych, salach sklepowych i innych pomieszczeniach, w których doprowadzenie sieci przewodowej byłoby zbyt kosztowne czy trudne technicznie. Jednak najczęściej WLAN wdrażany jest jako uzupełnienie sieci stacjonarnej - zwłaszcza w takich miejscach, jak sale konferencyjne, pokoje spotkań, itp.

Sieci bezprzewodowe WLAN 802.11b wykorzystują fale radiowe w zakresie częstotliwości od 2.412 do 2.472GHz (wg norm ETSI) do przesyłania informacji z jednego punktu do drugiego bez użycia medium fizycznego. Dzięki wydanemu w sierpniu 2002r. rozporządzeniu Ministerstwa Infrastruktury w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia - Dziennik Ustaw nr 138 poz. 1162 - rozwój i wprowadzanie tej technologii na polski rynek jest możliwy bez żadnych ograniczeń. To samo rozporządzenie umożliwiło korzystanie bez pozwolenia z urządzeń pracujących w standardzie 802.11a w paśmie 5GHz.

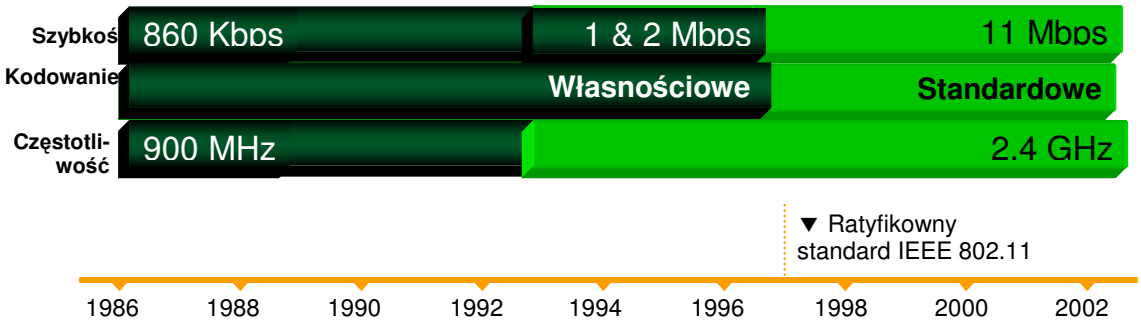
Obecnie sieci bezprzewodowe wkraczają w fazę wielkiego rozkwitu. Znajdują one zastosowanie w wielu dziedzinach życia codziennego. Pojawiają się wszędzie tam, gdzie dostęp do sieci nie może ograniczać swobody przemieszczania się. Łatwość i szybkość instalacji WLAN to główny czynnik ich popularności. Tam, gdzie na dużych powierzchniach konieczne jest zapewnienie łączności, zaś wykonanie okablowania jest kosztowne i trudne do realizacji, chętnie budowane są bezprzewodowe sieci lokalne.
Technologia ta z powodzeniem stosowana jest również:

- w bibliotekach,
- salach wykładowych,
- mobilnych pracowniach komputerowych.

Z WLAN korzystają uczniowie i studenci dysponujący komputerami przenośnymi. Dla tego typu użytkownika sieć bezprzewodowa jest naturalnym środowiskiem nauki i pracy. Ponadto w wielu sytuacjach sieci bezprzewodowe są jedynym możliwym do zastosowania sposobem zapewnienia transmisji. Na przykład obiekty zabytkowe, w których często zlokalizowane są szkoły lub instytucje publiczne, gdzie niejednokrotnie wykonanie okablowania strukturalnego jest niemożliwe bez odpowiednich zezwoleń. W większości przypadków uzyskanie pozwoleń jest bardzo kosztowne, a więc wykorzystanie sieci bezprzewodowych ma w tym przypadku silne uzasadnienie ekonomicznie.

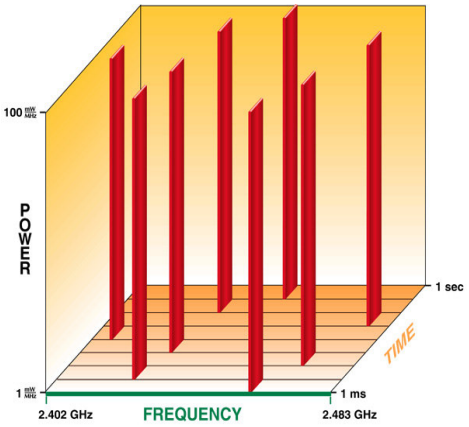
2. Szkic technologiczny

Technologie umożliwiające transmisję danych drogą radiową są znane już od wielu lat. Jednak dopiero wprowadzenie w roku 1997 przez Institute of Electrical and Electronics Engineers (IEEE) standardu 802.11 spowodowało znaczący przełom w tej dziedzinie. Spośród mnogości rozwiązań stosowanych przez różnych producentów wyłoniła się spójna definicja podstawowych elementów bezprzewodowych sieci lokalnych. Wraz z pojawieniem się tego standardu można było zaobserwować znaczne ożywienie na rynku urządzeń do budowy Wireless LAN.

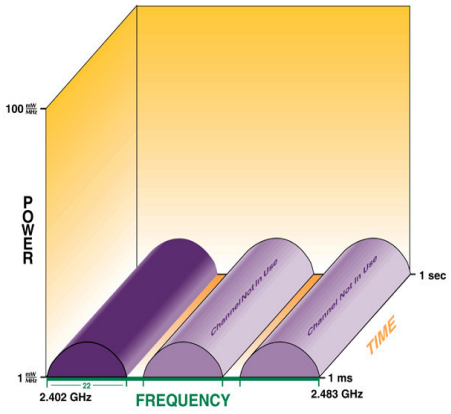


Wychodząc naprzeciw oczekiwaniom użytkowników w roku 1999 IEEE wprowadziło rozszerzenie do standardu 802.11 oznaczone 802.11b. Najważniejszą jego częścią jest zmiana sposobu transmisji radiowej. Powszechnie stosowana do tej pory modulacja określana skrótem FHSS (Frequency-Hopping Spread Spectrum), która pozwalała na transmisję z maksymalną prędkością 2Mb/s została wyparta przez DSSS (Direct Sequence Spread Spectrum) oferującą transmisję z szybkością do 11Mb/s. Jakkolwiek FHSS posiada kilka niezaprzeczalnych zalet, na przykład stosunkowo dużą odporność na interferencje spowodowane sąsiedztwem kilku systemów pracujących jednocześnie, to jednak wydaje się, że wprowadzenie standardu 802.11b definitywnie zamknęło rozdział historii związany z tą technologią.

Skokowa zmiana częstotliwości (Frequency Hopping)



Sekwencja bezpośrednia (Direct Sequence)



Z kolei obecny od 2002 roku standard 802.11g zaczyna wypierać rozwiązania 802.11b. Nowy standard wprowadzając bardziej zaawansowane metody kodowania sygnału radiowego pozwala na uzyskanie transmisji z szybkością do 54Mb/s. Jednocześnie urządzenia 802.11g są wstecznie zgodne z urządzeniami 802.11b, dzięki czemu możliwa jest bezproblemowa współpraca urządzeń zgodnych z każdym z powyższych standardów.

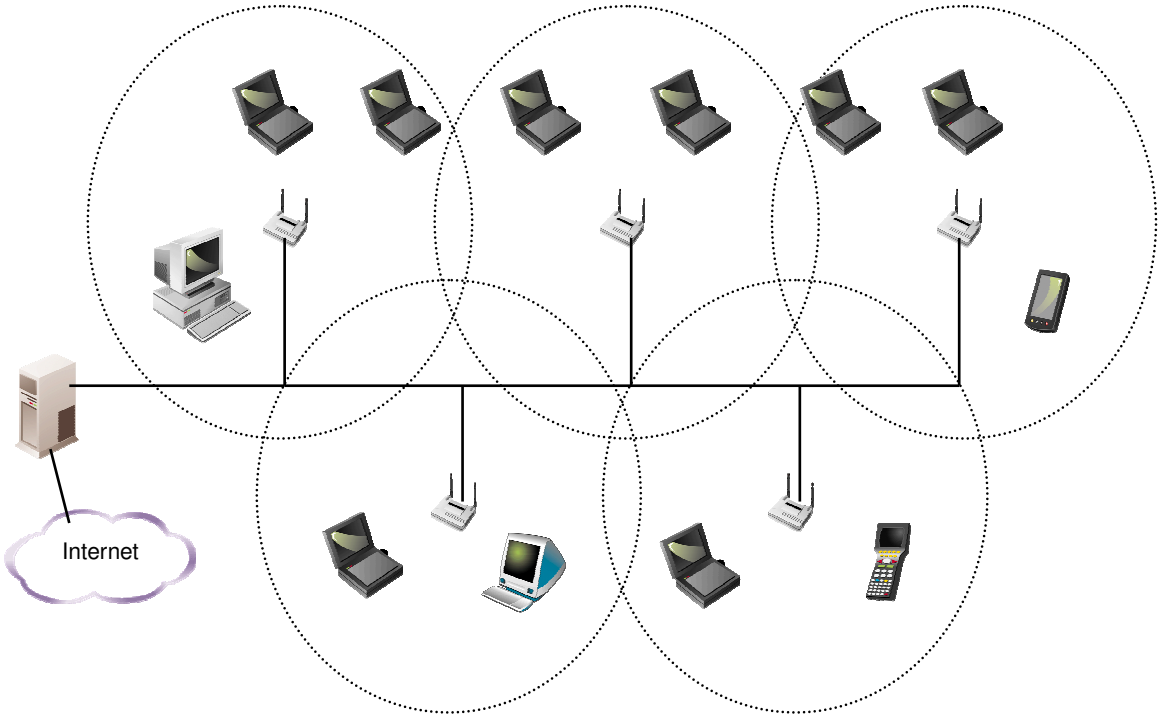
Poza standardami operującymi w paśmie 2.4GHz istnieje również standard 802.11a w paśmie 5GHz. Zaletą tego rozwiązania jest szybkość transmisji na poziomie 54Mb/s oraz mniej zatłoczone pasmo.

Standardy 802.11a/b/g są obecnie technologiami wzajemnie się uzupełniającymi, czego najlepszym dowodem są bezprzewodowe punkty dostępowe Cisco Aironet 1200, które mogą pracować jednocześnie w obu dostępnych pasmach 802.11.

Sieci bezprzewodowe zasadniczo możemy podzielić na dwie grupy:

- Sieci lokalne, czyli takie, które zastępują bądź rozszerzają istniejącą strukturę LAN,
- Sieci typu LAN-to-LAN, których zadaniem jest połączenie drogą radiową dwóch lub więcej odległych systemów. W tym celu stosowane są najczęściej tak zwane mostki bezprzewodowe (Wireless Bridge).

Pierwsze z wymienionych struktur budowane są w oparciu o bezprzewodowe punkty dostępowe (*ang. Access Point*). Zadaniem takiego punktu jest koncentracja ruchu od klientów, którymi mogą być zarówno komputery PC, jak i małe podręczne urządzenia bezprzewodowe takie, jak na przykład czytniki kodów kreskowych czy PDA. Punkty dostępowe łączone są ze sobą w przeważającej większości za pośrednictwem tradycyjnej, kablowej sieci LAN. Jednak możliwe do zrealizowania są rozwiązania, w których punkty dostępowe komunikują się ze sobą drogą radiową - w takich przypadkach mamy do czynienia z tak zwanym bezprzewodowym repeaterem.

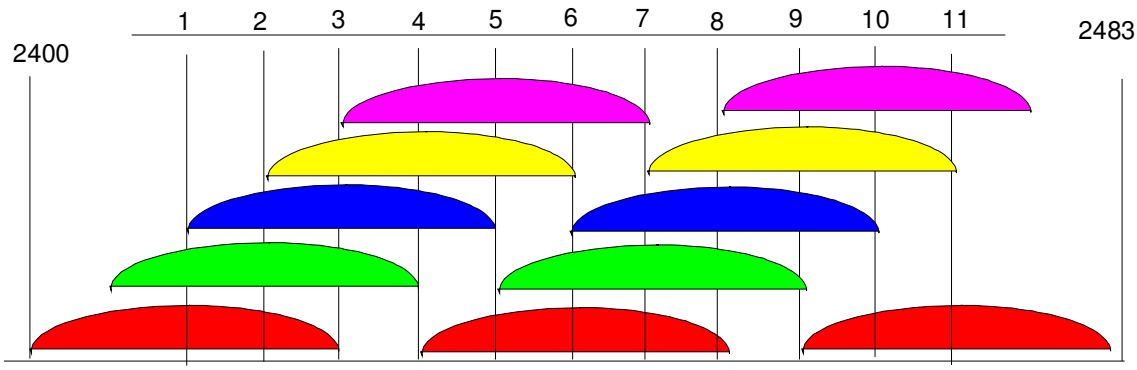


Rys. Topologia bezprzewodowej sieci WLAN.

Zaprojektowanie prostej bezprzewodowej sieci lokalnej nie powinno przysparzać wielu kłopotów. Instalacja pojedynczego punktu dostępowego Cisco Aironet sprowadza się do kilku łatwych do wykonania czynności typu „plug and play". Bardziej skomplikowanym zadaniem jest zaprojektowanie dużej sieci wymagającej zastosowania wielu punktów dostępowych. W tym miejscu warto zwrócić uwagę na pewne aspekty związane z transmisją radiową w technice rozpraszania widma z wykorzystywaniem sekwencji bezpośredniej (DSSS).

W metodzie tej do transmisji danych wykorzystuje się trzynaście[1] kanałów o szerokości 22 MHz każdy, które rozkładają się w paśmie od 2412 MHz do 2472 MHz.

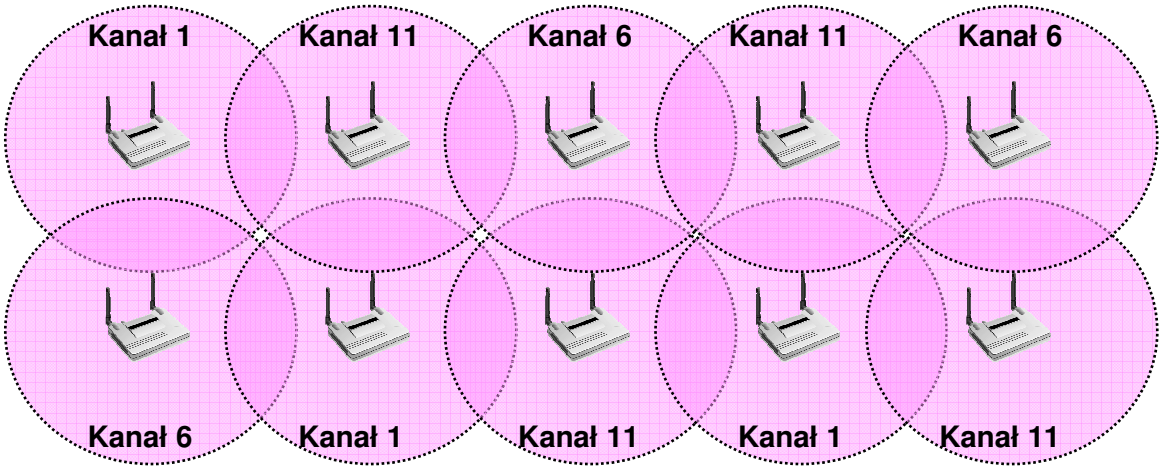
[1] 13 kanałów wg norm ETSI, 11 wg norm FCC



Rys. Podział pasma 2.4GHz na kanały

Większość z 11 kanałów znajduje się w bardzo bliskim sąsiedztwie, co może powodować ich nakładanie się, a tym samym wzajemne zakłócanie. Aby uniknąć takiego niekorzystnego oddziaływania należy tak dobrać kanały sąsiadujących ze sobą punktów dostępowych, aby ich częstotliwości nie zachodziły na siebie. W systemie Aironet zalecane jest stosowanie kanałów 1, 6 i 11, które są oddalone od siebie, na tyle że jednoczesna transmisja przy ich użyciu nie wywołuje interferencji, co przedstawia poniższy rysunek.

Stosując się do tej zasady możemy zaprojektować dowolnej wielkości sieć LAN. Dzięki wykorzystaniu funkcji roamingu, czyli możliwości przemieszczania się klienta sieci bezprzewodowej pomiędzy punktami dostępowymi bez utraty połączenia, uzyskujemy praktycznie nieograniczoną swobodę pracy w dowolnym miejscu pokrywanego falami radiowymi obszaru.

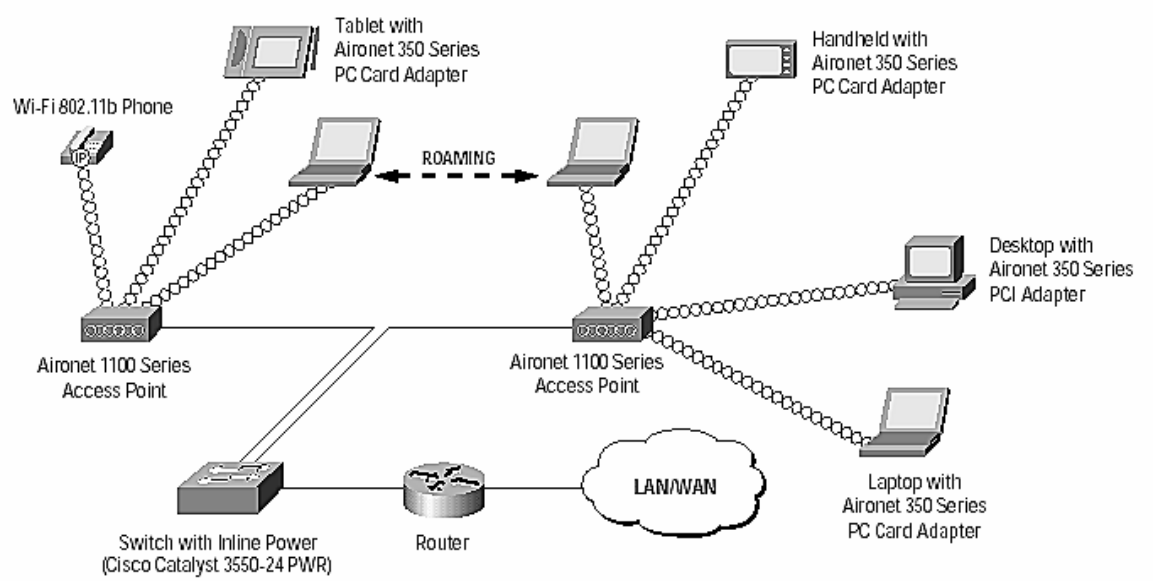


Rys. Przykładowe pokrycie obszaru nienakładającymi się kanałami w paśmie 2.4GHz.

Taką funkcjonalność (tzw. roaming) szczególnie cenią sobie osoby, których charakter pracy wymaga ciągłego przemieszczania się. W tradycyjnych sieciach lokalnych, gdzie występuje element związania z miejscem pracy w postaci kabla sieciowego, mobilność pracownika wprowadza wiele zamieszania oraz dodatkowe koszty. Koszty te wiążą się z

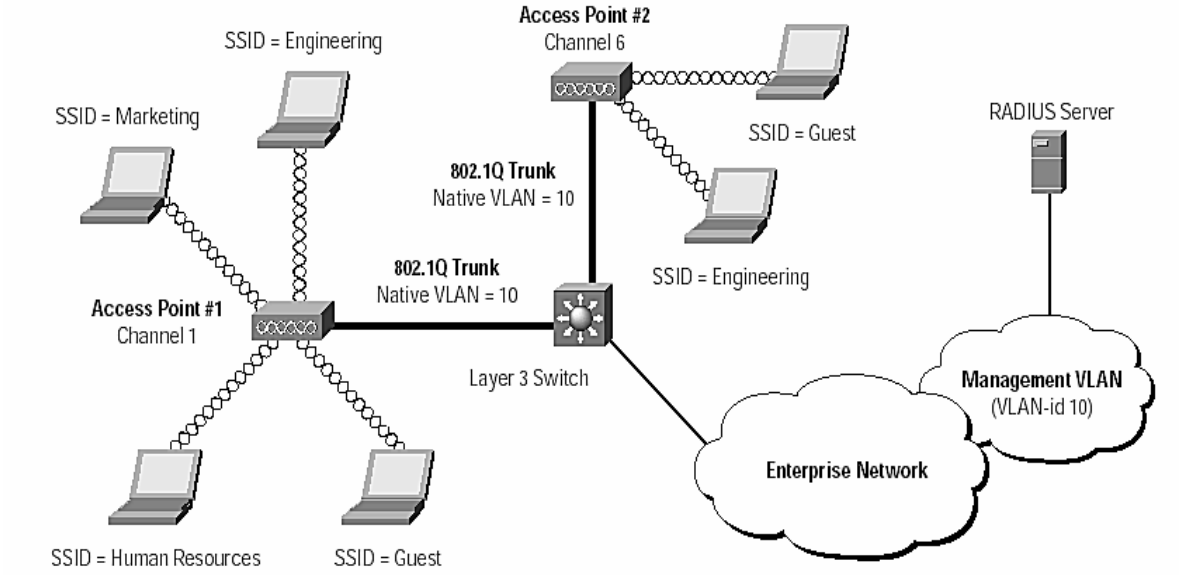
koniecznością posiadania dużej ilości gniazd dostępowych w wielu różnych pomieszczeniach, co większości przypadków jest bardzo mało efektywne i drogie. Dzięki technologii bezprzewodowej można tą niekorzystną sytuację w dużym stopniu ograniczyć lub całkowicie wyeliminować.

Mobilność wypływająca z funkcjonalności bezprzewodowych sieci LAN jest szeroko wykorzystywana we wszelkiego typu instalacjach na dużych powierzchniach. Wszędzie tam, gdzie niezbędne jest zapewnienie łączności na dużym obszarze, gdzie użytkownik znajduje się w ciągłym ruchu i nie może podlegać ograniczeniom „tradycyjnych" technologii.



Nowoczesne bezprzewodowe punkty dostępowe takie, jak Cisco Aironet 1100 i 1200 pozwalają na obsługę zaawansowanych technologii sieciowych, jak np. VLAN (Virtual Local Area Network), QoS (Quality of Service) oraz proxy Mobile IP - znanych z rozwiązań korporacyjnych, a także obsługę hot-standby czy funkcji równoważenia obciążenia umożliwiające wdrażanie Cisco Aironet 1100 zarówno w dużych sieciach, jak i w małych biurach.

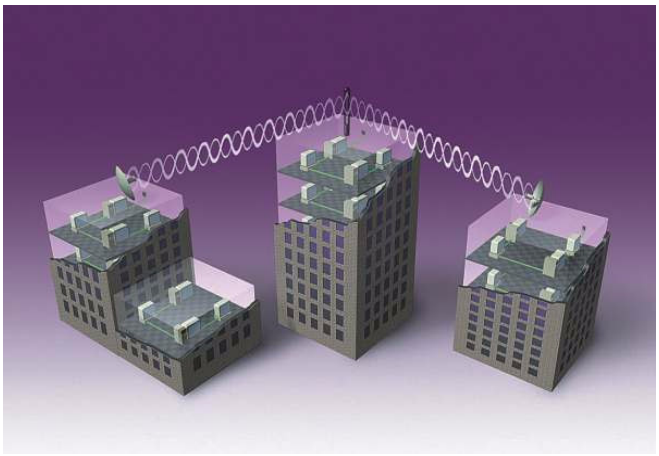
Bezprzewodowe punkty dostępowe Cisco Aironet są w stanie obsłużyć do 16 VLAN-ów (rys. powyżej), co umożliwia zróżnicowanie praw dostępu, usług, zasad korzystania oraz poziomu bezpieczeństwa czy QoS. Wykorzystanie VLAN umożliwia oddzielenie ruchu gości, chwilowo tylko przebywających w biurze od ruchu pracowników, a także wyodrębnienie pakietów głosowych o najwyższym priorytecie. Ruch do/z AP o różnym poziomie bezpieczeństwa może trafiać do różnych VLAN-ów z przydzielonymi różnymi regułami bezpieczeństwa. Na przykład w szkole wyższej można zabezpieczeń ruch generowany przez wykładowców i administrację oraz oddzielić go od ruchu generowanego przez studentów korzystających z tej samej infrastruktury bezprzewodowej.



Cisco Aironet wykorzystuje mechanizmy QoS 802.1p do nadawania pakietom różnych priorytetów już na samym brzegu sieci. Ruch wrażliwy na opóźnienia, taki, jak transmisja głosu czy video, może otrzymać wyższy priorytet niż zwykła transmisja danych. Umożliwia to bardziej efektywne wykorzystanie pasma i zwiększenie przepustowości sieci. W przyszłości uaktualnienie oprogramowania lub wymiana modułu radiowego umożliwi przejście na nowe standardy np. standard QoS 802.11e, który ma standaryzować mechanizmy QoS w ramach sieci 802.11.

Obsługa priorytetów transmisji głosowych we współpracy z bezprzewodowymi telefonami IP zgodnymi z 802.11b umożliwia korzystanie z technologii voice-over-wireless-LAN.

Kolejne z wymienionych typów bezprzewodowych sieci to połączenia typu LAN-to-LAN czyli, w wolnym tłumaczeniu, połączenia sieć – sieć.



Przy tego typu rozwiązaniach mamy do czynienia z nieco innymi wymaganiami oraz warunkami pracy. O wyborze danego rozwiązania decyduje przede wszystkim zasięg

oraz maksymalna możliwa do uzyskania przepustowość. Ponieważ połączenia tego rodzaju stanowią najczęściej alternatywę dla linii dzierżawionych, ich przepustowość powinna być, co najmniej na zbliżonym poziomie.

Produkty Cisco mają w tym zakresie bardo dobre parametry. Maksymalne zasięgi bezprzewodowych mostków sięgają kilkudziesięciu kilometrów, a przepustowości, jakie można uzyskać w pewnych konfiguracjach oscylują w granicach 33Mb/s.

Do zaprojektowanie połączenia pomiędzy sieciami LAN wymagana jest większa wiedza niż w przypadku instalacji WLAN na małych powierzchniach. Rozważając taką instalację należy zwrócić uwagę na kilka elementów.

Po pierwsze - właściwy dobór urządzeń: mostków, anten, przewodów łączących anteny z mostkami, złączy itp.

Patch Wall

Mast Mount

Mast Mount
High Gain

Yagi Mast

Solid Dish

Cisco w swojej ofercie ma kilkanaście rodzajów anten różniących się pod względem wielkości, kierunku oddziaływania, skuteczności oraz, w zależności od wymagań, miejsca montażu.

Podczas projektowania radiowego łącza LAN-to-LAN należy mieć na uwadze fakt, że do skutecznej transmisji, anteny łączonych systemów muszą znajdować się w polu widzenia. W pewnych warunkach pociąga to za sobą konieczność stosowania masztów, aby wynosząc anteny na większą wysokość zapewnić im lepszą „widzialność". Należy pamiętać, że na widoczność anten - czyli również na transmisję - mają wpływ takie elementy, jak: krzywizna ziemi, ukształtowanie terenu, drzewa, góry, etc. Wszystkie one powinny być uwzględnione na etapie projektowym.

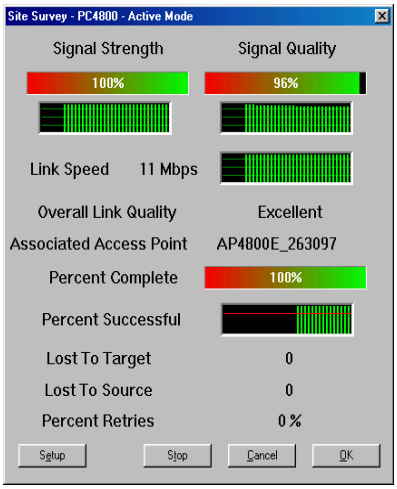
3. Planowanie sieci bezprzewodowych WLAN

Bez względu na to jakiego rodzaju sieć bezprzewodową zamierzamy zbudować, Wiereless LAN bądź LAN-to-LAN, ważne jest, aby na etapie projektowym przeprowadzić tak zwane **planowanie radiowe**.

Planowanie radiowe jest to proces, na który składa się szereg praktycznych testów i pomiarów wykonanych w miejscu planowanej instalacji. Ma ono na celu sprawdzenie jak system będzie zachowywał się w rzeczywistych warunkach, w których będzie funkcjonować. Dzięki rozpoznaniu przeprowadzonemu w miejscu docelowej instalacji uzyskujemy również informacje na temat pokrycia fal radiowych na danym obszarze, co ma wpływ na uzyskiwane przepustowości w WLAN.
Właściwie przeprowadzone planowanie radiowe powinno dać również odpowiedź na pytania:

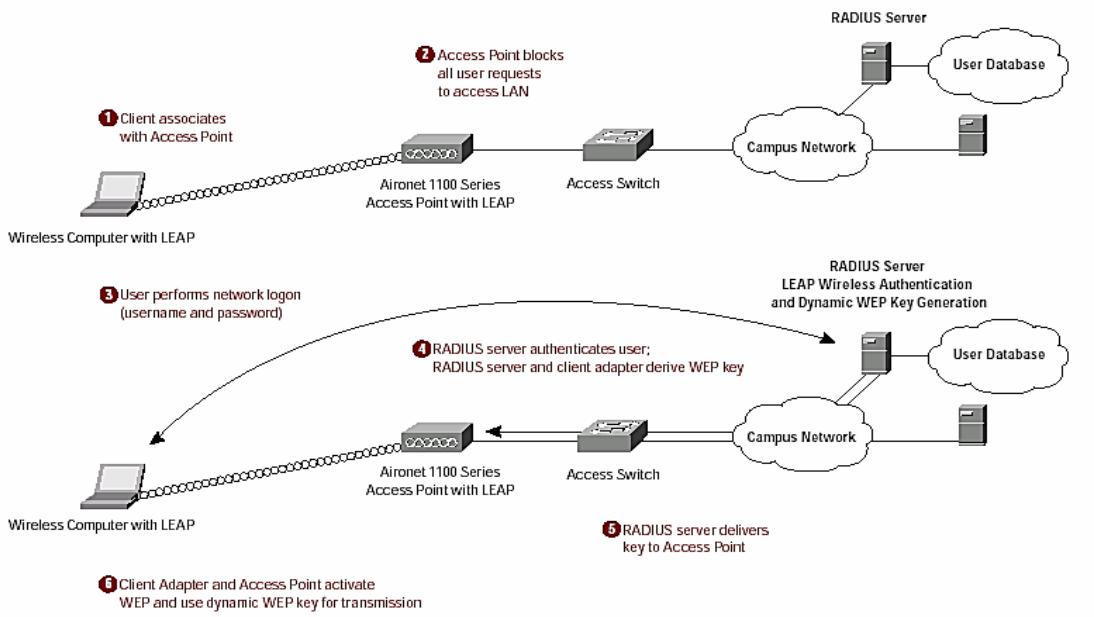
- ile punktów dostępowych należy zastosować, aby zapewnić łączność na określonej powierzchni,
- jak należy dobrać kanały radiowe, aby zminimalizować wpływ nakładania się częstotliwości,
- jaka ilość użytkowników będzie obsługiwana przez jeden punkt dostępowy,
- jakiego typu anteny należy zastosować,
- gdzie wystepują potencjalne źródła zakłóceń (kuchenki mikrofalowe, inne systmy radiowe, itp.).

Wykonanie prostego planowania radiowego nie należy do czynności skomplikowanych. Dodatkowym ułatwieniem jest dołączone do urządzeń Aironet Cisco bezpłatnie, oprogramowanie przeznaczone do tego celu. Jego interfejs graficzny, w przejrzysty sposób dostarcza wielu informacji np. na temat mocy sygnału radiowego, jego jakości, uzyskiwanych przepustowości.



4. Bezpieczeństwo sieci bezprzewodowych

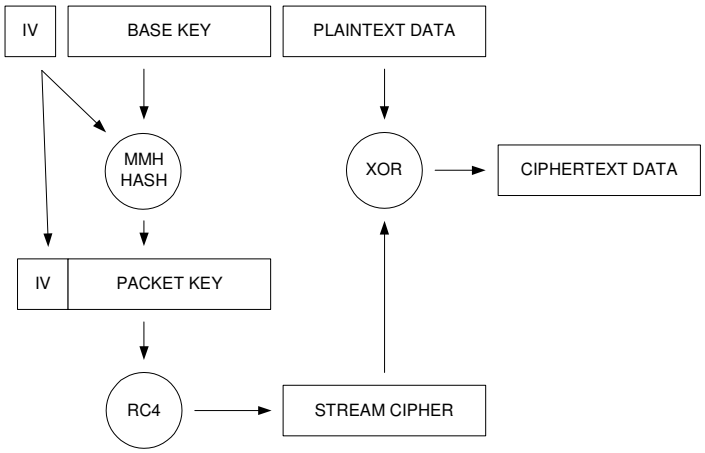
We współczesnych bezprzewodowych sieciach lokalnych bardzo duży nacisk kładzie się na bezpieczeństwo transmisji. Ponieważ systemy te w przeważającej większości wykorzystywane są jako rozszerzenia tradycyjnych sieci LAN, w których mamy do czynienia z wymianą wielu poufnych informacji, muszą one adresować również ten aspekt transmisji. Potencjalne niebezpieczeństwo związane ze stosowaniem bezprzewodowych sieci LAN wynika z faktu, że fale radiowe rozchodzą się w atmosferze w sposób niekontrolowany. Oznacza to, że teoretycznie każdy, kto posiada bezprzewodową kartę sieciową może niemal bezkarnie dołączyć się do dowolnego systemu posiadającego bezprzewodowe punkty dostępowe. Problem ten nie został jednak pominięty i w celu zapewnienia ochrony transmisji wprowadzono szyfrowanie na bazie protokołu WEP (Wired Equivalent Privacy). WEP jest protokołem symetrycznym, co w praktyce oznacza, że do kodowania i dekodowania informacji wykorzystywany jest ten sam klucz. W protokole WEP można dostrzec wiele podobieństw do powszechnie znanego DES. Podobnie jak on WEP wykorzystuje dwa rodzaje klucza 40 bitowy oraz 128 bitowy. Istotnym elementem związanym z transmisją szyfrowaną przy użyciu protokołu WEP jest sposób zarządzania kluczami szyfracyjnymi. Statyczna definicja jednego lub więcej kluczy stanowi poważną lukę w systemie. Przechwycenie takiego klucza w jakikolwiek sposób, może umożliwić nieautoryzowany dostęp do sieci, która na pierwszy rzut oka wydawała się bezpieczna. Podobnie, jak w przypadku technologii DSSS Cisco jako pierwsze zaproponowało rozwiązanie problemu statycznie zdefiniowanych kluczy szyfracyjnych. Technologia ta, oparta na standardzie IEEE 802.1X, wykorzystuje do uwierzytelniania użytkowników protokół Extensible Authentication Protocol (EAP) (rys).



Cisco Wireless Security Suite współpracuje z szeroką gamą urządzeń końcowych wykorzystując wszystkie typy uwierzytelniań zawarte w normie 802.1X, włączając w to EAP Cisco Wireless (LEAP), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) oraz protokoły pracujące na bazie EAP-TLS - Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) oraz EAP-Subscriber

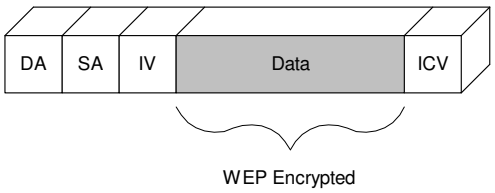
Identity Module (EAP-SIM). Do centralnego zarządzania polityką bezpieczeństwa i dostępem użytkowników do zasobów sieciowych może być wykorzystanych wiele serwerów RADIUS obsługujących te same mechanizmy uwierzytelniania użytkowników. Integralną częścią Cisco Wireless Security Suite są również takie rozszerzenia standardu, jak - Temporal Key Integrity Protocol (TKIP), per-packet key hashing, message integrity check (MIC) oraz broadcast key rotation:

- WEP Key Hashing zapobiegający przechwyceniu klucza jednorazowego i dokonaniu tzw. session hijacking

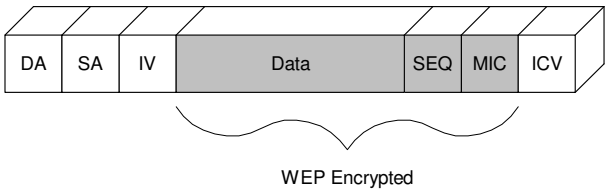


- Message Integrity Check – dodatkowe pole dodane do części szyfrowanej WEP pozwalające na określenie przynależności pakietu do sesji

WEP Frame - No MIC



WEP Frame - MIC

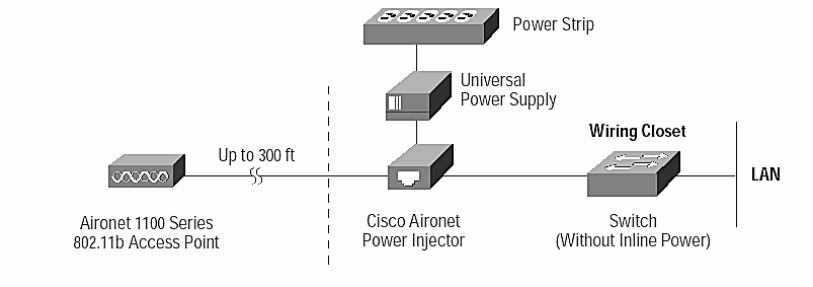


5. Portfolio produktów Cisco dla sieci WLAN w Jednostkach Samorządu Terytorialnego

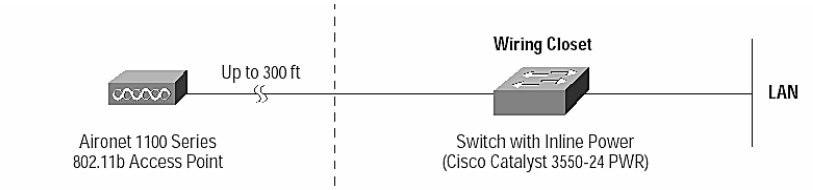
Punkt dostępowy serii Cisco Aironet 1200 oferuje największe możliwości oraz elastyczność konfiguracji sprzętowej. Cechą wyróżniającą go spośród innych produktów jest radio – urządzenie może pracować zarówno zgodnie ze standardem 802.11b/g jak i 802.11a (opcjonalnie lub jednocześnie) dzięki możliwości zabudowania jednocześnie dwóch modułów radiowych – jeden pracujący w pasmie 2.4GHz a drugi w pasmie 5GHz. Ponadto AP1200 można wyposażyć w dowolnego rodzaju antenę, co pozwala odpowiednio kształtować zasięg i pokrycie sieci bezprzewodowej w danym obszarze.

Urządzenie to zostało również wzbogacone o szereg funkcji pozwalających na zwiększenie bezpieczeństwa w sieciach WLAN, jak również poprawę jakości usług w dostępie bezprzewodowym Jednocześnie po stronie odbiorczej dokonano wielu modyfikacji zwiększających czułość, co pozwala na znaczne wydłużenie dystansu.

Z punktu widzenia instalacji bezprzewodowych punktów dostępowych istotny jest sposób zasilania urządzeń. Zasilanie podawane jest za pośrednictwem kabla ethernet. Jest on w pełni zgodny z produktami Cisco posiadającymi funkcjonalność „in-line power" (rys.)



Rys. Cisco Aironet 1200/1100 zasilany poprzez sieć Ethernet z opcjonalnym Inline Power Injector



Rys. Cisco Aironet 1200/1100 zasilany dzięki przełącznikom Cisco Catalyst z funkcjonalnością in-line power

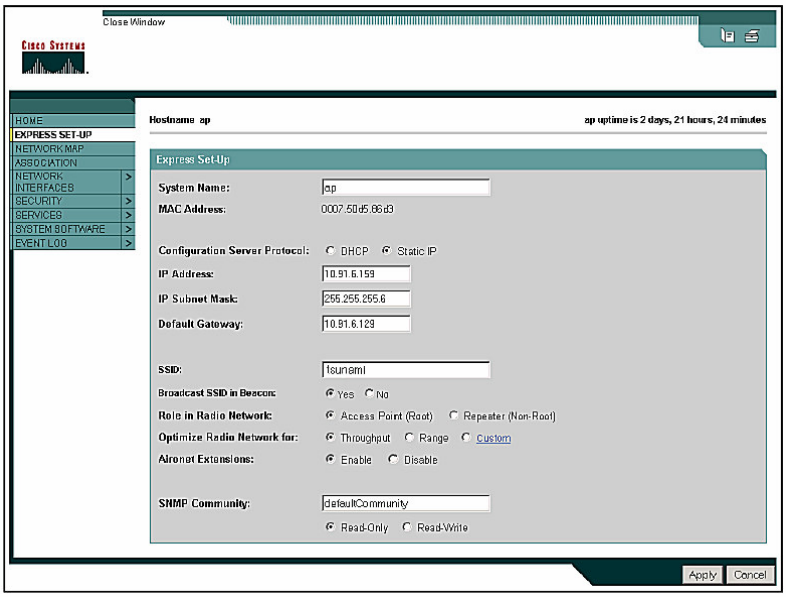
Wraz z wprowadzeniem serii 1200 pojawiła się nowa wersja systemu operacyjnego. Oprogramowanie to zawiera szereg nowych możliwości, takich, jak choćby wspomniany wcześniej sposób identyfikacji użytkowników bazujący na nazwie użytkownika i haśle oraz mechanizm przydzielania kluczy szyfracyjnych dla każdej pojedynczej sesji.

Do przechowywania informacji o użytkownikach wykorzystywany jest serwer Cisco Secure ACS 3.2, który ma wbudowany serwer RADIUS wraz z rozszerzeniem EAP. Ponadto, w nowym systemie zaimplementowane zostały mechanizmy umożliwiające efektywne filtrowanie ruchu na bazie protokołów TCP/IP.

Cisco Aironet 1100 to idealne rozwiązanie dla nowo powstających lokalizacji oraz jako rozszerzenie już istniejącej sieci. Zapas mocy procesora oraz dodatkowa pamięć umożliwia obsługę przyszłych wersji oprogramowania i standardów komunikacyjnych. Klienci mogą również wymienić moduł nadajnika radiowego 802.11b na obsługujący wyższe prędkości w standardzie 802.11g. Rozwiązanie Cisco Aironet 1100 jest urządzeniem wyposażonym w identyczne funkcje oprogramowania, jak AP 1200.

Cisco Aironet 1100 jest wyposażony w pojedynczy moduł radiowy w standardzie 802.11b z możliwością rozbudowy, zintegrowaną antenę dipolową oraz nowoczesny system montażu umożliwiający łatwą instalację w dowolnej orientacji oraz w różnych pomieszczeniach.

Intuicyjny interfejs graficzny umożliwia zarządzanie punktami dostępowymi Cisco Aironet 1100/1200 za pomocą przeglądarki webowej. Nowoczesny interfejs graficzny ułatwia proces instalacji, konfiguracji i diagnostyki urządzenia. Cisco Aironet 1100/1200 może być również zarządzany poprzez dobrze znany interfejs znakowy (CLI).



Najnowszym produktem w ofercie bezprzewodowych punktów dostępowych Cisco jest Aironet 1300 Outdoor Access Point/Bridge. Urządzenie to pracuje w standardzie 802.11g dzięki czemu umożliwia transmisję z szybkością do 54Mb/s a jednocześnie pozwala na współpracę ze stacjami klienckimi 802.11b. AP 1300 może pełnić jednocześnie funkcje punktu dostępowego dla sieci LAN oraz mostka bezprzewodowego dla połączeń LAN-to-LAN. Dzięki odpornej na warunki atmosferyczne obudowie

urządzenie to może być instalowane na zewnątrz budynków i pracować w zakresie temperatur od -30 do +55 stopni Celsjusza.

Dodatkowe nowe funkcje wprowadzone wraz z AP 1300 to m.in.:

- Automatyczny wybór kanału pracy – dzięki wbudowanemu analizatorowi pasma urządzenie automatycznie wybiera do pracy najmniej zajęty kanał pasma 2.4GHz,
- Narzędzia ułatwiające instalację i konfigurację – specjalny tryb pracy, w którym nie ma potrzeby korzystania z żadnego komputera by odpowiednio ustawić i skierować urządzenia pracujące w trybie mostka LAN-to-LAN. Diody LED umieszczone na obudowie pokazują informację o sile odbieranego sygnału,
- Dostosowanie parametrów transmisji do odległości – mechanizm ten pozwala automatycznie dobrać parametry sposobu transmisji bezprzewodowej Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) na podstawie skonfigurowanej odległości między mostkami bezprzewodowymi,
- Łączenie pakietów – dla lepszego wykorzystania dostępnego pasma AP 1300 potrafi łączyć małe pakiety w większe porcje informacji.

Aironet 1300 Outdoor Accenss Point/Bridge

Istotne znaczenie ma także zarządzanie systemem składającym się w wielu urządzeń bezprzewodowych. Cisco posiada w swojej ofercie rozwiązanie WLSE (Wireless LAN Solution Engine). Rozwiązanie to jest narzędziem programowym posadowionym na dedykowanej platformie sprzętowej. Pozwala na zarządzanie wszystkimi urządzeniami bezprzewodowymi instalowanymi w sieci w zakresie:

- Zapewnienia bezpieczeństwa sieci:
  - Monitoring i sprawdzanie spójności polityki bezpieczeństwa na wszystkich urządzeniach;
  - Generowanie alarmów przy naruszeniach polityki bezpieczeństwa;
  - Powiadamianie administratora przy naruszeniach polityki bezpieczeństwa – E-mail, syslog, SNMP trap,
- Ułatwiania konfiguracji:
  - Monitoring i sprawdzanie spójności konfiguracji na wszystkich urządzeniach;

- Scentralizowana dystrybucja oprogramowania systemowego;
- Automatyczna konfiguracja nowych urządzeń w sieci z zastosowaniem wzorca przygotowanego przez administratora;
- Tworzenie archiwów konfiguracji do 4 wersji wstecz: Automatycznie i "na żądanie",

- Monitorowania urządzeń oraz optymalizacji ruchu na łączach WAN:
  - Monitoring obciążenia wszystkich urządzeniach;
  - Możliwość obsługi progów ruchu (thresholds) na portach Ethernet oraz portach radiowych;
  - Możliwość uruchomienia mechanizmów mających na celu zmniejszenie/kontrolę obciążenia na łączach WAN (np. polling).

Zastosowanie tego rodzaju rozwiązań pozwala traktować zestaw urządzeń WLAN jako potencjalnie kompletne rozwiązanie.

6. Przyszłość sieci bezprzewodowych

Technologie wykorzystywane obecnie przez bezprzewodowe sieci lokalne są obecnie stabilne. Standard IEEE 802.11b liczy sobie już kilka lat, a jednak ciągle trwają prace nad nowymi technologiami umożliwiającymi szybszą i bezpieczniejszą transmisję. Dostępny jest już standard 802.11g, lecz ze względu na to, że urządzenia dostępne są na rynku od niedawna, większość kart klienckich obecnie używanych to karty 802.11b. W dobie konwergencji, kiedy w sieciach komputerowych coraz częściej mamy do czynienia nie tylko z transmisją danych ale również z transmisją głosu (Voice over IP), WLAN muszą sprostać i temu wyzwaniu.

Jednym z kluczowych elementów związanych z transmisją głosu w sieciach służących do transmisji danych jest zapewnienie odpowiedniej gwarancji pasma oraz priorytetu. W tym celu pracuje się nad odpowiednim mechanizmem znakowania pakietów tak, aby możliwe było ich rozróżnienie i odpowiednie traktowanie w zależności od przenoszonych informacji.

Powołano szereg grup roboczych pracujących nad rozszerzeniami standardu 802.11 m.in. o takie elementy jak:

- Zagwarantowanie jakości usług w sieciach bezprzewodowych (802.11e),
- Zapewnienie bezpieczeństwa w WLAN (802.11e docelowo 802.11i, znane również jako WPA),
- Dynamiczne zarządzanie częstotliwościami radiowymi i mocą nadajnika (802.11h).

Transmisja danych drogą radiową postrzegana jest obecnie przez wielu specjalistów jako kierunek rozwoju obecnych sieci LAN. Już dzisiaj pracuje się nad urządzeniami umożliwiającymi transmisje danych z szybkościami 100Mb/s. Jakkolwiek możemy spodziewać się dalszej ekspansji tych technologii to wydaje się, że w obliczu takich standardów, jak Gigabit Ethernet pozostaną one, tak jak do tej pory, głównie technologiami dostępowymi dla użytkowników końcowych.

7. Aplikacje sieciowe WLAN w Jednostkach Samorządu Terytorialnego

Poprzednie rozdziały opisujące warstwę technologiczną nie wskazują jednoznacznie aplikacji możliwych do zrealizowania z wykorzystaniem urządzeń bezprzewodowych. Do najpopularniejszych aplikacji WLAN stosowanych w Jednostkach Samorządu Terytorialnego zaliczamy:

A. Połączenia międzybudynkowe,
B. Hotspoty,
C. Pokrycie siecią bezprzewodową sal konferencyjnych, sal spotkań etc.

A. Połączenie międzybudynkowe

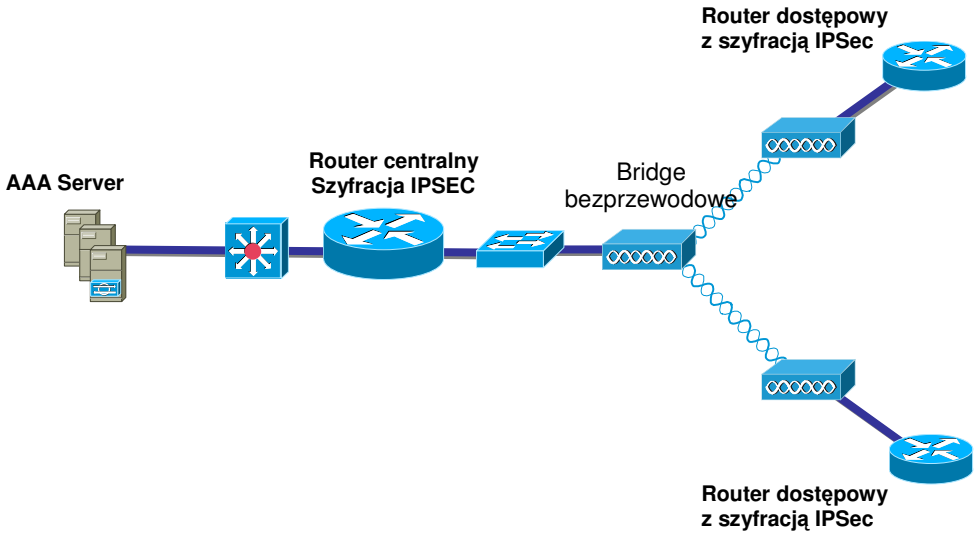
Dla realizacji połączeń między budynkami stosowane są urządzenia bridge. Przy projektowaniu tego typu sieci należy sprawdzać tzw, „widzialność" obiektów. Poszczególne obiekty nie mogą być zasłonięte przez inne budynki, drzewa etc. Zasięg połączeń tego typu zależy od zastosowanych anten oraz mocy nadawczej bridge'a. Aby zachować zgodność z normami ETSI należy zakładać zasięg tego typu rozwiązań na poziomie około 2-3km. Nie oznacza to, że dystans ten jest gwarantowany. W przypadku nieoptymalnego doboru anten wynikającego z różnych uwarunkowań lokalnych zasięg ten może być mniejszy. Z drugiej strony, w optymalnej konfiguracji zasięgi te mogą być większe.

Korzystając z urządzeń pracujących w paśmie otwartym – a takim jest pasmo pracy urządzeń 802.11b/g - należy pamiętać, że pasmo to jest współdzielone z innymi użytkownikami. Oznacza to, że choć technologia umożliwia transfery z przepustowościami 54Mbps, to obecność innych użytkowników może znacząco obniżyć dostępne pasmo.

Drugim istotnym zagadnieniem jest bezpieczeństwo. Analizując bezpieczeństwo sieci bezprzewodowych należy zaznaczyć kilka aspektów:

- Uwierzytelnianie,
- Zapewnienie Integralności przesyłanych danych,
- Zapewnienie poufności przesyłanych danych.

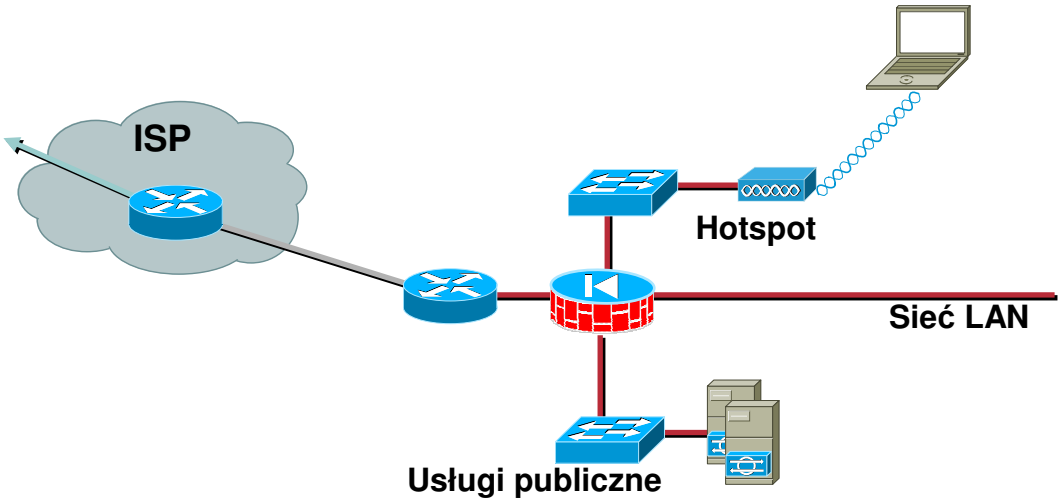
Ze względu na regulacje prawne związane z otwartością pasma 2.4-2.485GHZ dla użytku publicznego, niemożliwe jest przeciwdziałanie funkcjonowania innych Access Point'ów na tym obszarze. Również udowodnienie ataków jest wyjątkowo trudne. Dlatego dla połączeń międzybudynkowych stosuje się topologię typową dla budowy sieci rozległych WAN. Dla zapewnienia integralności i poufności przesyłanych danych zaleca się stosowanie w każdej lokalizacji routerów szyfrujących IPSec. Wykorzystanie routerów z funkcjonalnością zwiększenia poziomu bezpieczeństwa sieci ma dodatkowe zalety. Należy do nich zaliczyć np. tak ważną rzecz jak zachowanie lokalnej adresacji sieci i korzystanie z NAT na routerach. Ma to ogromne znaczenie w lokalizacjach gdzie stosowana jest aplikacja z „pełnym" klientem, który z kolei może być mocno powiązany w adresem sieciowym (adresem IP) serwera. Również izolacja problemów jest zdecydowanie łatwiejsza w takiej strukturze. Przykładowy schemat realizacji takiego zadania zamieszczono poniżej:



Do tego zadania należy przewidywać zastosowanie bridge'y Aironet 1300.

B. HotSpot

Hotspoty są coraz częściej stosowanym sposobem realizacji dostępu do sieci globalnej. Hostpoty internetowe pojawiły się już w najbardziej eksponowanych miejscach największych miast Polski. Realizacja dostępu do internetu wymaga jednak kilku dodatkowych elementów. Ważnym jest określenie, czy usługa taka ma być bezpłatna czy też ma być usługą płatną, ale nieprzynoszącą zysku JST (opłata pokrywa koszty funkcjonowania hotspotu). Jednak w obu przypadkach stosowane są jednak te same urządzenia bezprzewodowe. Dla realizacji tej aplikacji stosuje się typowe punkty dostępowe (access points). Bardzo ważnym aspektem jest stosowanie rozwiązań pozwalających na swobodną pracę użytkownikom, bez konieczności wymuszania na nich dodatkowych funkcji lub narzędzi. Przykładowo pokrycie obszaru rynku miejskiego z punktu dostępowego umieszczonego na budynku JST oddalonego o 500m, od tegoż rynku, nie ma sensu. Chociaż możliwe jest zastosowanie anten realnie pokrywających zakładany obszar to typowe urządzenia klientów mają zdecydowanie mniejszy zasięg. Zatem taka konfiguracja jest praktycznie bezużyteczna jako hotspot. Hotspot zatem jest realizowany przez punkt dostępowy lub ich grupę. Urządzenia te są przyłączone kablowo do sieci komputerowej na dedykowany segment firewalla lub też bezpośrednio do segmentu realizującego połączenie pomiędzy firewallem a routerem internetowym. W tym drugim przypadku trzeba jednak zarezerwować publiczne adresy IP (bez translacji adresowej NAT) dla klientów hotspotów, a to jest nieefektywne i przez to bardzo rzadko stosowane rozwiązanie.



W przypadku realizacji aplikacji gdzie usługa dostępu do internetu jest usługą płatną należy pomiędzy segmentem WLAN a firewallem przewidzieć dodatkowe urządzenie pozwalające na identyfikację użytkownika i „pobieranie opłat". Forma płatności może być różna – od dokonania opłaty przez kartę kredytową, poprzez „zdrapkę" na stałym dostępie abonamentowym skończywszy. W takim rozwiązaniu można dopuścić darmową komunikację z JST – dostęp do Hotspota pozwala wówczas na skorzystanie z aplikacji e-urzędu bez możliwości wyjścia na zewnętrz i korzystania z globalnej sieci Internet.

C. Pokrycie siecią bezprzewodową obszarów wewnątrz budynków.

Jest to najprawdopodobniej najprostsza aplikacja do zrealizowania w systemach sieci bezprzewodowych. Mimo, że wszystko jest pozornie proste nie można zapominać o kilku aspektach. Do najistotniejszych należy zaliczyć:

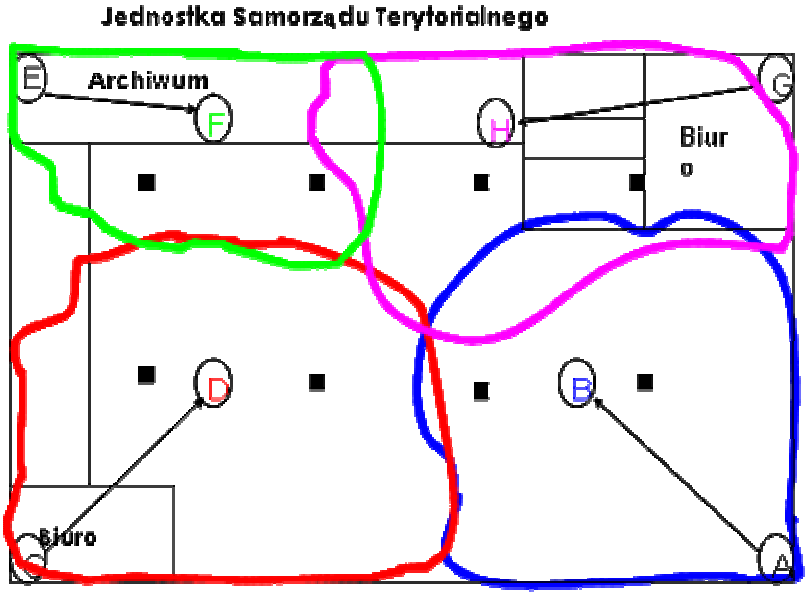
- Dokładne określenia zasięgu punktów dostępowych,
- Przydział kanałów (w 802.11b),
- Funkcje roamingowe,
- Bezpieczeństwo sieci.

Przydział kanałów oraz funkcje roamingowe zostały dokładniej opisane w poprzednich rozdziałach

Projektując sieć WLAN wewnątrz budynku należy bezwzględnie przeprowadzić tzw. Site Survey polegający na ustawieniu punktów dostępowych w wytypowanych miejscach, a następnie sprawdzanie zasięgu w budynku. Można do tego celu wykorzystać standardowe oprogramowanie dostarczane przez Cisco z punktami bezprzewodowymi.

Należy zwrócić uwagę na fakt, że na zasięg mają wpływ zarówno grube ściany budynków (część JST mieści się z zabytkowych budynkach gdzie grubość ścian odbiega od obecnych standardów), jak i ekrany metalowe (takim ekranem może być np. grupa metalowych szafek w archiwum).

Obraz pokrycia obiektu sygnałem bardzo rzadko składa się z obszarów kolistych (jak by sugerował model nadawania z anteny dookólnej)



Bezpieczeństwo sieci bezprzewodowych to także bardzo istotne zagadnienie. Standard 802.11 w pierwotnej, a zarazem najczęściej używanej wersji nie jest przygotowany do realizacji funkcji bezpieczeństwa. Początkowo uważany za mechanizm bezpieczeństwa SSID (Service Set Identifier) jest de facto wykorzystywany do logicznej separacji VLANów. Pomimo tego, że można wyłączyć rozpowszechnianie własnego SSID,

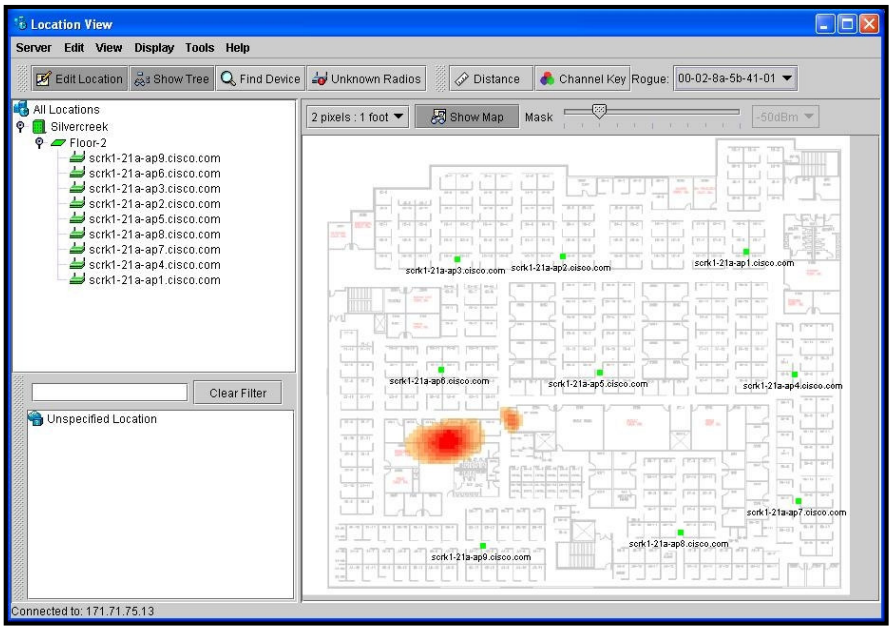
dotyczy to tylko tzw. ramek beacon. W dowolnej innej ramce SSID jest on przesyłany, co powoduje, że jego podsłuchanie nie jest zadaniem trudnym.

Zachowanie poufności transmisji jest również bardzo trudne w przypadku zastosowania standardowych mechanizmów. WEP (Wired Equivalent Privacy) oparty jest na symetrycznym szyfrowaniu RC4, gdzie stosowane są statyczne, wspólne klucze (ang. *pre-shared keys*). Klucz jest łączony z 24-bitowym losowym wektorem inicjalizującym (IV). WEP jest obarczony szeregiem wad. Przede wszystkim wektor IV jest wysyłany niezaszyfrowany, co powoduje że klucz można odtworzyć na podstawie analizy statystycznej kilku milionów ramek (atak statyczny z zastosowaniem narzędzi takich jak Airsnort). WEP nie ma również wbudowanego automatycznego mechanizmu zmiany klucza. Pozostaje, zatem manualna zmiana kluczy, które w dłuższej perspektywie czasowej, czy zastosowaniu większej ilości Access Point'ów po prostu jest niemożliwe do opanowania. Fakt współdzielenia klucza przez wszystkie urządzenia powoduje, iż w przypadku kradzieży klienta (stacji roboczej, laptopa etc.), należy liczyć się z tym, że atakujący zna klucz do całej sieci.

Jak łatwo zauważyć, ograniczenie zabezpieczeń do stosowania typowych dostępnych narzędzi może doprowadzić do utraty kontroli nad siecią, a także do utraty kontroli nad przechowywanymi informacjami. Bardzo ciekawą obserwacją jest fakt, że przy bardzo rygorystycznym stosowaniu instrukcji kancelaryjnych dotyczących rozdzielenia sieci internetowej i wewnętrznej oraz jednoczesnym korzystaniu z Access Point'ów w typowej konfiguracji poziom bezpieczeństwa jest o wiele niższy aniżeli przy stosowaniu jednej sieci komputerowej oraz sieci bezprzewodowej z dodatkowymi elementami bezpieczeństwa.

Bardzo ważnym aspektem zarządzania siecią bezprzewodową w budynkach jest też wykrywanie intruzów – obcych Access Point'ów, które z jednej strony mogą służyć do nasłuchiwania, z drugiej zaś mogą „mylić" klientów, którzy zamiast podłączyć się do sieci własnej będą nadawać od „obcego" AP. Identyfikacja obcych AP jest możliwa przez porównanie parametrów odbieranych ramek ze znanymi sąsiadami zaś dzięki BSSID możliwe jest określenie portu przełącznika, do którego jest on wpięty (jeżeli jest to. np. AP używany przez urzędnika). Jeżeli obcy AP nie jest wpięty do żadnego kontrolowanego przez administratora przełącznika możliwe jest określenie jego położenia przez tzw. triangulację radiową (sprawdzenie mocy sygnału).

Unikalną cechę systemu zarządzania sieciami bezprzewodowymi w wykonaniu Cisco jest graficzna prezentacja miejsca instalacji obcego AP.



W lepiej zabezpieczanych systemach transmisji bezprzewodowej stosuje się szyfrację IPSec. W tym rozwiązaniu bezpośrednio za przełącznikiem agregującym ruch z punktów dostępowych (wydzielona sieć) znajduje się VPN Concentrator. Urządzenie VPN Concentrator zbiera sesje szyfrowane IPSec od użytkowników korzystających z sieci bezprzewodowej. Sama stacja robocza musi mieć zainstalowane oprogramowanie klienta sieci VPN. Zaleca się też, aby miała zintegrowane oprogramowanie osobistego firewalla (ang. *Personal Firewall*). Access Point powinien w tym modelu przyjmować tylko pakiety szyfrowane (filtracja poprzez listy dostępowe konfigurowane na punkcie dostępowym).

Podsumowując – zbudowanie sieci WLAN wymaga szczególnie dobrego przygotowania projektu. Nawet, jeżeli dziś przewidywany jest tylko pojedynczy access point należy patrzeć na to zagadnienie szerzej, z wizją całościowego rozwiązania. Brak takiego spojrzenia może powodować implikacje, które na dziś są już widoczne (opisane powyżej), rzutujące np. na bezpieczeństwo danych osobowych w JST.

8. Podsumowanie

Sieci bezprzewodowe są dzisiaj jedną z najszybciej rozwijających się technologii sieciowych. Pojawiają się tam, gdzie dotychczas nie było możliwości dotarcia drogą kablową.

W spontanicznych działaniach mających na celu poprawę istniejącego stanu połączeń nie należy jednak zapominać o zachowaniu kontroli. Dotyczy to zarówno systemów bezprzewodowych dla połączeń między budynkami, jak również systemów instalowanych wewnątrz obiektów JST. Kontrola nad sieciami bezprzewodowymi objawia się poprzez zachowanie odpowiedniego poziomu bezpieczeństwa, kontrolę dostępu do medium (w sieciach wewnątrz budynków), priorytetyzację danych, pełne zarządzanie, wykrywanie „pirackich" punktów dostępowych etc.

Warto też przygotowywać systemy sieciowe WLAN z wizją końcowej ich postaci – pozwoli to uniknąć niepożądanych efektów w przyszłości.