Wprowadzenie do konfiguracji sieci bezprzewodowej.

ZAGADNIENIA

1. Z czego składa się infrastruktura sieci bezprzewodowych?
2. W jakich trybach mogą pracować sieci bezprzewodowe?
3. Jakie standardy dotyczą sieci bezprzewodowych?
4. Jak skonfigurować bezprzewodową kartę sieciową?
5. W jaki sposób zabezpieczyć sieć bezprzewodową przed podsłuchem?
6. Jakie standardy szyfrowania danych używane są w sieciach bezprzewodowych?

****

Obecnie jest więcej urządzeń bezprzewodowych niż przewodowych. Około 10 lat temu większość biur miała tylko komputery stacjonarne i niektóre inne urządzenia sieciowe, takie jak drukarki. Wszystkie były połączone przewodami. Obecnie wielu użytkowników ma laptopa, smartfona i tablet. To trzy urządzenia bezprzewodowe dla każdego użytkownika. Szybkość łączności bezprzewodowej znacznie wzrosła, zbliżając się do bezprzewodowej sieci Gigabit.

Bezprzewodowa sieć **lokalna WLAN** (*Wireless Local Area Network*) jest to sieć, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów. Do przesyłania danych pomiędzy urządzeniami wykorzystuje się fale radiowe. Zakres częstotliwości fal radiowych wykorzystywany w sieciach WIAN nie podlega koncesjonowaniu i dlatego można go używać bez żadnych zezwoleń. Jednak w paśmie tym występują znaczne zakłócenia pochodzące od innych urządzeń, np. kuchenek mikrofalowych, telefonów bezprzewodowych itp.

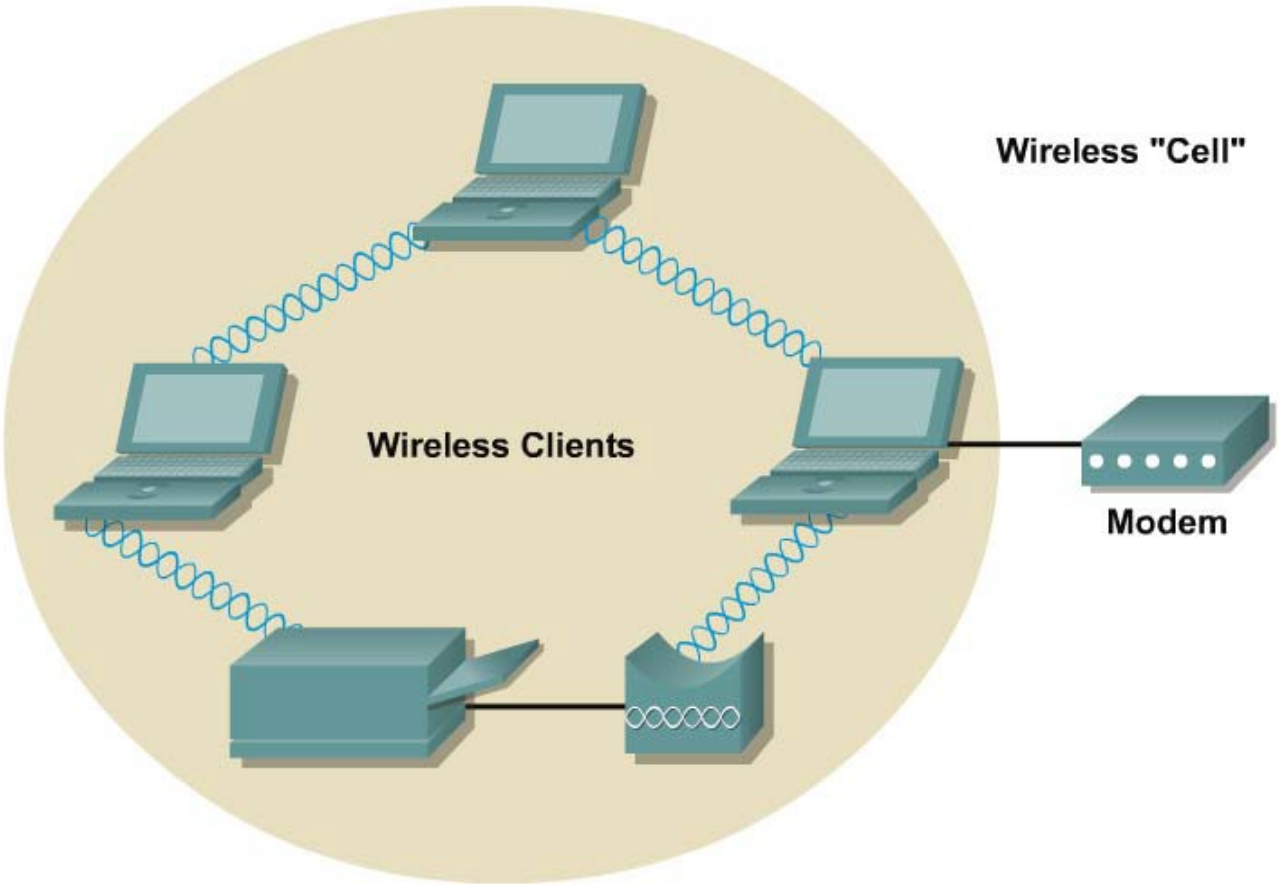
Infrastruktura sieci bezprzewodowych:

- **karty sieciowe** - najczęściej typu PCI, PCIExpress, ExpressCard, USB, PCMCIA, ale też wbudowanych w urządzenia przenośne, takie jak laptopy, smartfony, itp.;
- **punkty dostępowe** (Access Point) - pełnią rolę bezprzewodowych koncentratorów w sieciach pracujących w trybie infrastruktury;
- **anteny**
- **kable, złącza** itp.

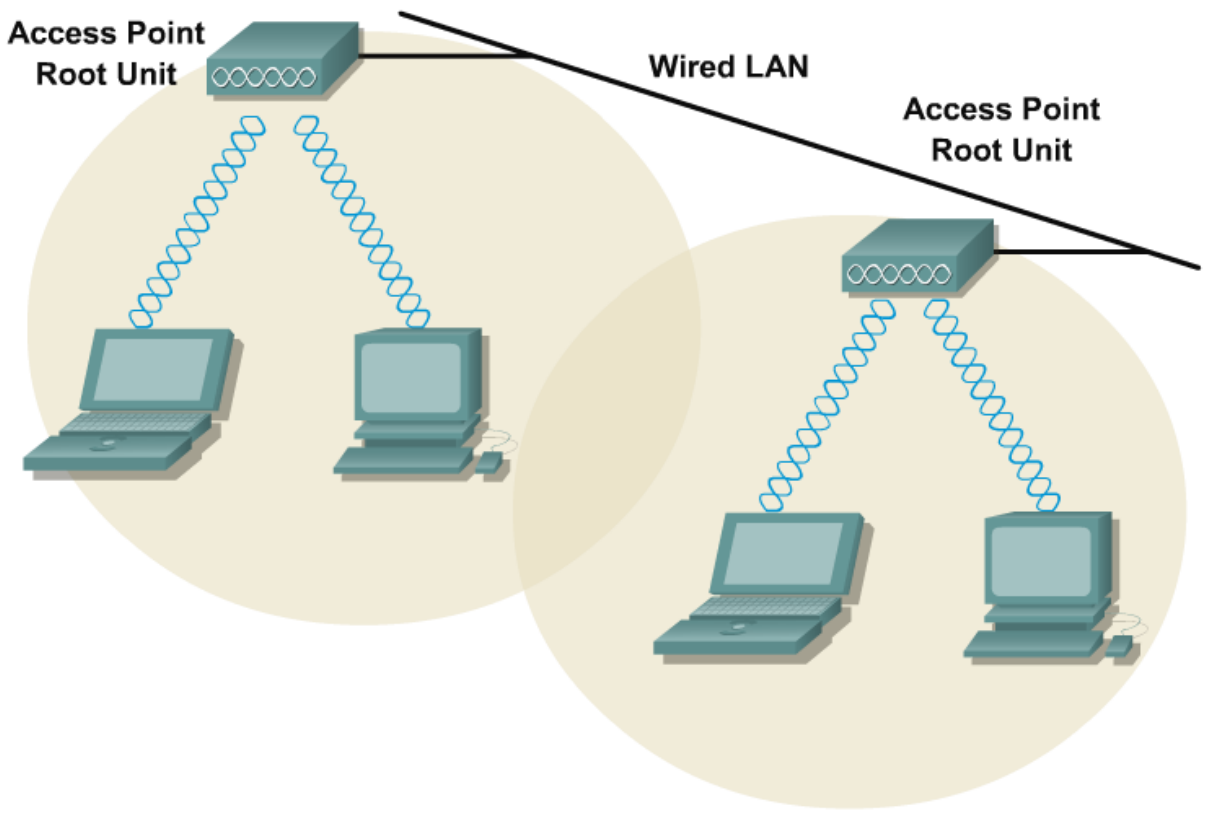
****

Tryby sieci bezprzewodowych:

- **tryb ad hoc** - małe sieci bezprzewodowe - urządzenia komunikują się bezpośrednio ze sobą,



- **tryb infrastruktury -** dla większych sieci przewidziano, w którym urządzenia komunikują się ze sobą za pośrednictwem punktów dostępowych.



****

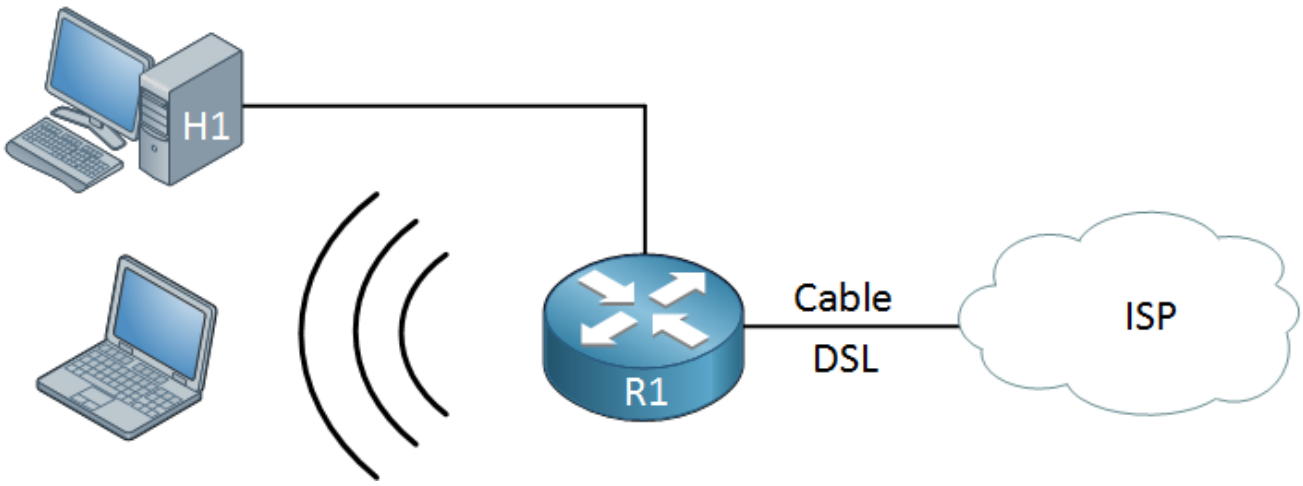
Standardy sieci WLAN, - opisuje dokument IEEE 802.11 - różnią się częstotliwościami pracy, prędkościami przesyłania danych i sposobem kodowania sygnału.

- **802.11a** - standard wykorzystuje pasmo częstotliwości w zakresie 5,15-5,35 GHz oraz 5,725-5,825 GHz. Obejmuje 8 kanałów przeznaczonych do pracy w budynkach oraz 4 przeznaczone do pracy między dwoma punktami (point-to-point). Praca na wyższych częstotliwościach powoduje zmniejszenie zasięgu w porównaniu z innymi sieciami o około połowę. Maksymalna prędkość transmisji w tym standardzie wynosi 54 Mb/s. Wadą jest brak zgodności z innymi standardami.
- **802.11b** - używa pasma w częstotliwości 2,4 GHz (od 2400 do 2485 MHz), osiągając maksymalną prędkości 11 Mb/s w promieniu 46 m w pomieszczeniach zamkniętych i 96 na otwartych przestrzeniach. Pasmo częstotliwości podzielone jest na 14 kanałów o szerokości 22 MHz, częściowo zachodzących na siebie (tylko trzy kanały nie pokrywają się w swoich zakresach). W Polsce można wykorzystywać tylko kanały od l do 13.
- - **802.11g** - standard ten używa tego samego pasma częstotliwości, co 802.11b. Umożliwia transmisję danych z prędkością 54 Mb/s. Standard ten jest w pełni zgodny z 802.11b.
- - **802.11n** - w zależności od rozwiązania (zastosowanych anten) pozwala na przesyłanie plików z prędkością teoretyczną - od 150 do 600 Mb/s. Standard „n" może działać na częstotliwości zarówno 2,4 GHz, jak i 5 GHz (jednak większość urządzeń potrafi pracować tylko w paśmie 2,4 GHz). Standard obsługuje technologię **Multiple Input Multiple Output** - (MIMO) wykorzystującą wiele anten do nadawania/odbioru sygnału (sygnał jest nadawany z kilku źródeł i odbierany przez kilka odbiorników). Ponadto urządzenia 802.11n potrafią wykorzystywać wiele kanałów transmisyjnych do stworzenia jednego połączenia, co teoretycznie dodatkowo zwiększa dostępną prędkość transmisji. Starsze urządzenia obsługujące jedynie standard „b" lub „g" mogą współpracować z urządzeniem działającym w standardzie „n", jednak w takiej sytuacji nast ępuje przełączenie na wolniejsze tempo standardu „b" lub „g".
- **802.11ac** – maksymalny transfer danych 7 Gb/s (co najmniej 1 Gb/s), częstotliwość sygnału 5GHz
- TGp (przyszłość **802.11p**) - Grupa zadaniowa przyjmująca 802.11 do użytku w samochodach. Początkowe użycie prawdopodobnie będzie standardowym protokołem stosowanym do pobierania opłat drogowych.
- TGr (przyszłość **802.11r**) - Ulepszenia wydajności roamingu.
- TG (przyszłe **802.11**) - Grupa zadań ulepszająca 802.11 do wykorzystania jako technologia sieci kratowej.
- TGT (w przyszłości **802.11T**) - Grupa zadań projektująca specyfikację testu i pomiaru dla 802.11. Jego wynik będzie niezależny, stąd wielka litera.
- TGu (przyszłość **802.11u**) - Grupa zadań modyfikująca 802.11, aby pomóc w współpracy z innymi technologiami sieciowymi.

****

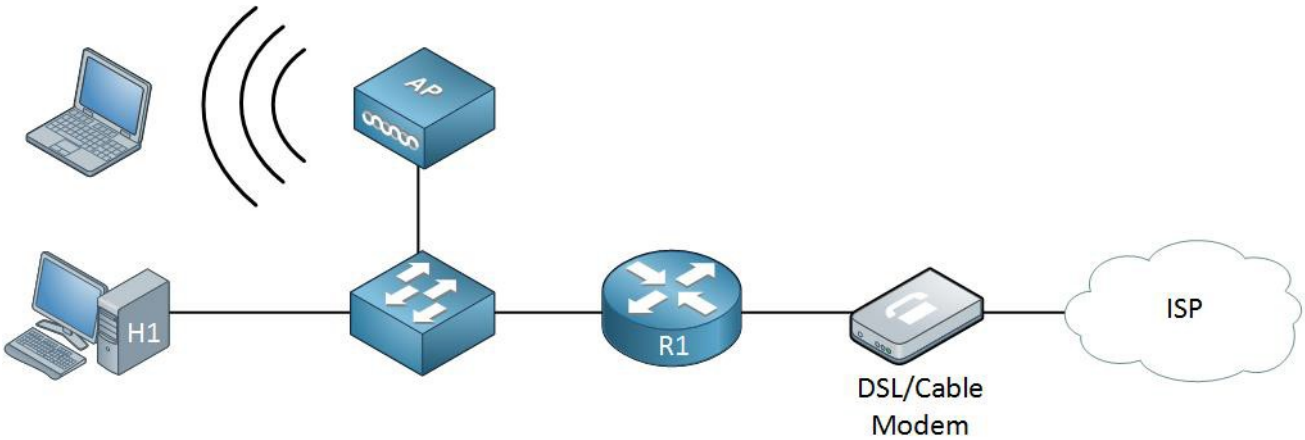
Bezprzewodowa sieć LAN SOHO

Twój router w domu prawdopodobnie ma takie same możliwości jak ten poniżej:



Jest on podłączony do Twojego dostawcy usług internetowych za pośrednictwem kabla lub DSL, a może światłowodu. Ma kilka portów Ethernet do podłączenia komputerów i anteny dla użytkowników bezprzewodowych. W rzeczywistości wszystkie te elementy są wbudowane w jedno urządzenie:
Przełącznik Ethernet + Bezprzewodowy punkt dostępu + (Modem kablowy lub DSL) + Router

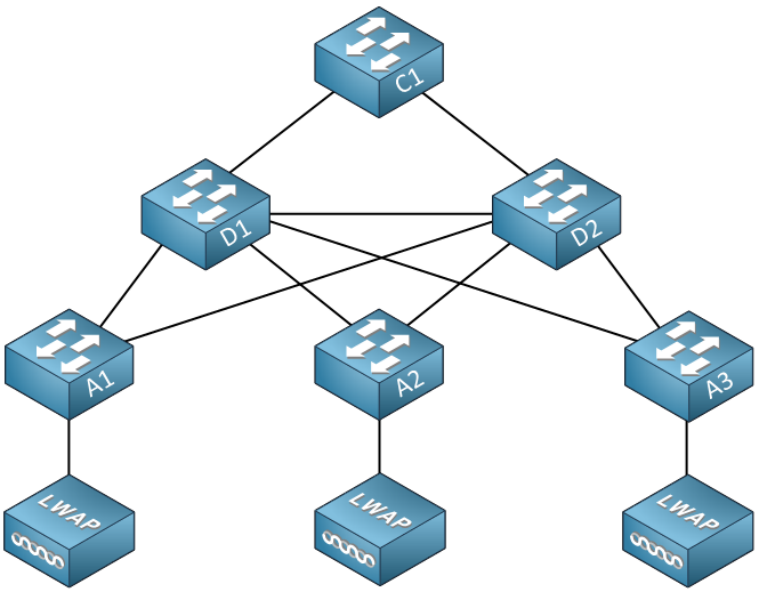
Jeśli rozłożysz wszystko na części, wygląda to tak:



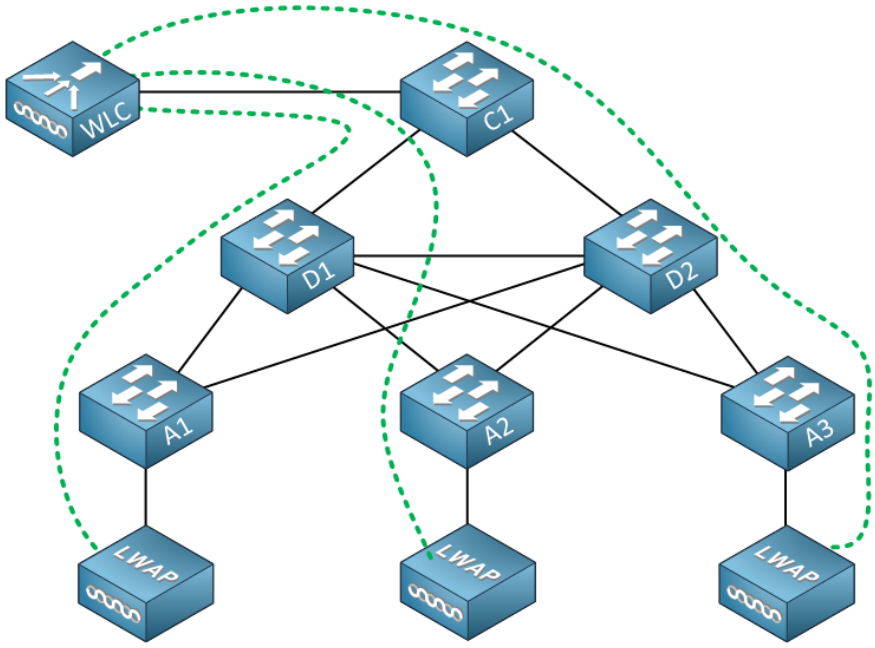
W takich małych sieciach punkt dostępowy robi wszystko sam. Nazywamy to autonomicznym punktem dostępu. Korzysta z protokołów 802.11 do komunikacji z klientami bezprzewodowymi i korzysta z Ethernetu po stronie sieci LAN.

Enterprise Wireless LAN

Kiedy patrzymy na duże sieci Enterprise, pojedynczy punkt dostępu nie wystarczy. Wyobraź sobie sieć z setkami lub tysiącami użytkowników. Spacerując po biurze, nie chcesz rozłączać się za każdym razem, gdy telefon przełącza się z jednego punktu dostępu do drugiego. Chcesz mieć stabilne połączenie bezprzewodowe, gdziekolwiek jesteś. Płynne przełączanie z jednego punktu dostępu do drugiego nazywa się **roamingiem**.
Pojedynczy punkt dostępu ma również ograniczoną przepustowość. Jeśli masz salę konferencyjną ze 100 użytkownikami, pojedynczy punkt dostępu może nie być w stanie zapewnić wszystkim wystarczającej przepustowości.
Ponieważ używamy sieci bezprzewodowej dla naszych użytkowników, musi ona być blisko naszych użytkowników. Dlatego punkty dostępu znajdują się w warstwie dostępu do sieci, podobnie jak komputery i drukarki:



Nadal jest jeden problem. Załóżmy, że masz połączenie z punktem dostępu i zaczynasz chodzić po biurze, telefon przełączy się na inny punkt dostępu. Skąd ten drugi punkt dostępu wie, że jesteś już uwierzytelniony w sieci? Możesz ponownie uwierzytelnić, ale spowoduje to zerwanie połączenia ... nie jest to dobry pomysł.
Aby rozwiązać ten problem, współpracujemy z kontrolerami bezprzewodowej sieci LAN:



Wszystkie zadania zarządzania są przenoszone z punktów dostępu do kontrolera bezprzewodowej sieci LAN. Zajmuje się uwierzytelnianiem, roamingiem, tworzeniem nowych sieci bezprzewodowych itp. Punkty dostępu są odpowiedzialne tylko za przekazywanie ruchu, nazywamy je **LWAP (Light Weight Access Point)**.

Aby to osiągnąć, cały ruch musi być wysyłany z punktów dostępu do kontrolera bezprzewodowej sieci LAN. Odbywa się to za pomocą tuneli zwanych **CAPWAP (kontrola i udostępnianie bezprzewodowych punktów dostępowych)**. Zielone kropkowane linie to tunele CAPWAP między punktami dostępowymi i WLC.

Mamy teraz jedną dużą sieć bezprzewodową. Jeśli utworzysz nową sieć bezprzewodową (SSID), zostanie ona przekazana do wszystkich punktów dostępu. Roaming również nie stanowi problemu, ponieważ cały ruch jest przekazywany do WLC.

****

Przed przyłączeniem komputera do sieci bezprzewodowej należy skonfigurować bezprzewodową kartę sieciową. Jeżeli w sieci bezprzewodowej będzie działał serwer DHCP, to karta będzie mogła otrzymać adres IP i inne dane niezbędne do prawidłowej pracy w sieci. Jeżeli serwera DHCP w sieci nie będzie, to wszystkie dane należy przypisać karcie ręcznie.

Przykład 1

Konfigurowanie bezprzewodowej karty sieciowej

W tym przykładzie zostanie skonfigurowana bezprzewodowa karta sieciowa w systemie Windows 10. Inne systemy, np. Linux i starsze wersje systemu Windows, posiadają inne narzędzia służące do konfigurowania sieci bezprzewodowych. Jeżeli dane konfiguracyjne mają być przypisane do karty w sposób statyczny, należy wykonać następujące czynności:

l. Zainstalować kartę i niezbędne sterowniki lub upewnić się, że zostały one poprawnie zainstalowane.
2. W panelu sterowania wybrać *Sieć i Internet*, a następnie *Centrum sieci i udostępniania*.
3. W oknie *Centrum sieci i udostępniania* wybrać polecenie *Zmień ustawienia karty sieciowej*.
4. W oknie *Połączenia sieciowe* kliknąć prawym klawiszem myszy ikonę symbolizującą konfigurowaną kartę i wybrać polecenie *Właściwości*.
5. Z rozwijanej listy wybrać *Protokół internetowy w wersji 4 (TCP/ IPv4)* i kliknąć przycisk *Właściwości*.
6. W odpowiednie pola wprowadzić dane konfiguracyjne:
• adres IP,
• maskę podsieci,
• bramę domyślną,
• adresy serwerów DNS (preferowanego i alternatywne go).
7. Kliknąć przycisk OK.
8. Upewnić się za pomocą polecenia ipconfig /all, że dane konfiguracyjne zostały wprowadzone poprawnie.

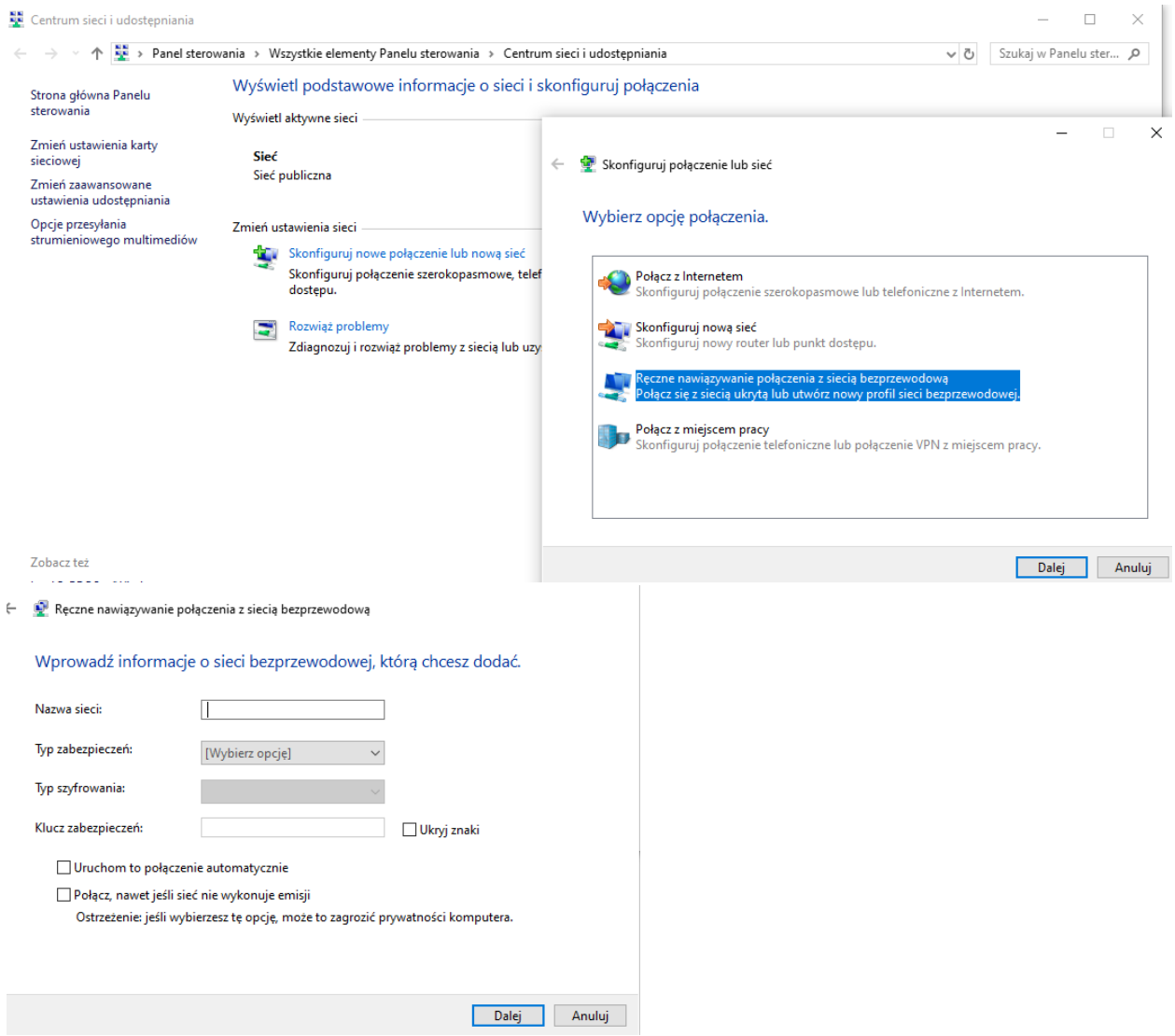
Sieć w trybie **ad hoc** charakteryzuje się zdecentralizowaną strukturą, w której przyłączone urządzenia mogą pełnić funkcje zarówno klientów, jak i punktów dostępowych. Do przekazywania danych nie jest wymagana żadna infrastruktura sieciowa, ponieważ pakiety dostarczane są bezpośrednio do odbiorcy. Sieci tego typu budowane są zazwyczaj na krótko i później demontuje się je. Wykorzystywane są np. do połączenia laptopa ze smartfonem lub tabletem. W Windows 10 w stworzeniu sieci ad hoc pomaga kreator, który prowadzi użytkownika przez cały proces konfiguracji.

Przykład 2

Konfigurowanie sieci ad hoc.

W tym przykładzie zostanie skonfigurowana sieć ad-hoc w systemie Windows 10. Inne systemy, np. Linux i starsze wersje systemu Windows posiadają inne narzędzia służące do konfigurowania sieci bezprzewodowych.
Sieci ad hoc najczęściej budowane są jako rozwiązania tymczasowe, wykorzystywane do przesyłania plików pomiędzy dwoma urządzeniami. Ze względu na tymczasowość sieci na ogół tworzy się sieci niezabezpieczone przed dostępem osób nieuprawnionych.

Tu zbudowana zostanie niezabezpieczona sieć w trybie ad hoc. Należy jednak pamiętać, że rozwiązanie to nie zapewnia bezpieczeństwa i może być stosowane tylko w wyjątkowych przypadkach, gdy przesyłane dane nie wymagają ochrony.



****

Sieci bezprzewodowe są narażone na podsłuch danych w znacznie większym stopniu niż sieci kablowe. Wynika to z faktu, że fale elektromagnetyczne rozchodzą się w całej przestrzeni, a każdy, kto znajdzie się w zasięgu rozprzestrzeniania się fal, może je odbierać (pod warunkiem, że posiada odpowiednie urządzenia). Aby zabezpieczyć sieć przed dostępem osób nieuprawnionych, należy zastosować następujące procedury:

1. Zmiana domyślnego loginu i hasła dostępowego - wszystkie inne zabezpieczenia będą nieskuteczne, jeśli każdy będzie mógł załogować się na naszym routerze i przejąć nad nim kontrolę. Listę domyślnych haseł routerów można znaleźć w internecie.

2. **Umożliwienie zarządzania tylko przez kabel** - wyłączenie możliwości logowania się do punktu dostępowego przez sieć bezprzewodową ogranicza dostęp do zarządzania urządzeniem tylko dla użytkowników podłączonych kablem.

3. **Ograniczenie mocy nadawania** - pozwoli na ograniczenie zasięgu sieci tylko do niezbędnego obszaru, np. mieszkania, a sieć będzie niedostępna dla sąsiadów znajdujących się poza zasięgiem.

4. Dobór umiejscowienia punktu dostępowego - punkt dostępowy można w miarę możliwości instalować w środku mieszkania oraz ograniczyć moc nadawania, tak aby jego zasięg obejmował jedynie mieszkanie. Innym możliwym rozwiązaniem jest zastosowanie specjalnych anten sektorowych o ograniczonym obszarze pokrycia terenu.

5. Wyłączenie identyfikatora sieci - każda sieć bezprzewodowa posiada unikatowy identyfikator SSID (*Serwer Set IDentifier*). Identyfikator SSID jest wysyłany przez każde urządzenie, np. punkt dostępowy. Na podstawie tej nazwy urządzenia wykrywają sieci w swoim otoczeniu i mogą rozpocząć procedurę przyłączenia do sieci. Punkty dostępowe i routery standardowo używają jako identyfikatora swojej nazwy, np. linksys. Dobrą praktyką jest zmiana identyfikatora na inną - jeżeli potencjalny włamywacz wie, jaki jest typ punktu dostępowego, to jego zadanie jest ułatwione. Można również wyłączyć wysyłanie identyfikatora SSID - sieć stanie się niewidoczna dla typowych narzędzi. Przyłączyć się do sieci będą mogli tylko ci użytkownicy, którzy znaj ą SSID. Zabezpieczenie to jest niewystarczające, gdyż istnieje wiele specjalistycznych programów, które są w stanie odczytać SSID, nawet jeżeli jego wysyłanie jest wyłączone np.: WiFi Analizer.
6. Włączenie filtrowania adresów MAC - każda karta bezprzewodowa posiada unikatowy adres fizyczny MAC. Na jego podstawie punkt dostępowy może rozpoznać, czy jest to legalny użytkownik sieci czy intruz. Punkt dostępowy może mieć zdefiniowaną listę adresów MAC urządzeń, które powinny uzyska ć dostęp do sieci (biała lista) i urządzeń, którym należy zabronić dostępu (czarna lista). Niestety, metoda filtrowania adresów MAC w obecnych czasach nie spełnia swojego zadania, ponieważ bardzo łatwo obejść to zabezpieczenie przez podmianę adresu MAC przez włamywacza. Mimo wszystko warto ją stosować.
7. Włączenie szyfrowania danych - brak szyfrowania sprawia, że nasze dane (loginy, hasła, numery kart) są przesyłane w sieci w sposób umożliwiający ich łatwe przechwycenie przez osoby trzecie.

Spośród wymienionych wyżej metod zwiększenia bezpieczeństwa sieci bezprzewodowych największe znaczenie praktyczne ma szyfrowanie danych.

****

Standardy zabezpieczenia danych:

1. WEP - (Wired Equivalent Privacy) - do ochrony danych w standardzie WE P wykorzystuje się algorytm RC4, który jest symetrycznym szyfrem strumieniowym z kluczem poufnym. Podczas szyfrowania metodą RC4 zostaje wykonana operacja różnicy symetrycznej XOR na bitach klucza i danych, której efektem jest szyfrogram. W celu odkodowania wiadomości odbiorca musi użyć tego samego klucza, który został u żyty do zaszyfrowania wiadomości. W WEP stosowane są klucze o długości 64 lub 128 bitów (klucz składa się z 40 lub 104 bitów klucza i z tzw. wektora inicjalizującego o długości 24 bitów). W standardzie WEP oferowane są klucze poufne o długości 40 bitów, ponieważ w momencie opracowywania standardu prawo Stanów Zjednoczonych nie pozwalało na wykorzystywanie klucza dłuższego niż 40 bitów.

Obecnie metoda WEP jest uznawana za niewystarczającą i powinna być stosowana tylko w przypadku, gdy urządzenia nie obsługują standardu WPA.

2. WPA - (WiFi Protected Access) - wykorzystuje protokoły TKIP (Temporal Key Integrity Protocol) oraz uwierzytelnienie EAP (Extensible Authentication Protocol). Został wprowadzony jako standard przejściowy pomiędzy WEP a WPA2. Zwiększenie bezpieczeństwa użytkowników sprzętu następuje bez konieczności wymiany sprzętu - wystarczy zmienić sterownik w karcie sieciowej lub firmware w punktach dostępowych.

Tryby WPA:

• **Enterprise** - używa serwera RADIUS, który przydziela klucze odpowiednim użytkownikom.

Konieczność autoryzacji

Do konieczności autoryzacji klientów radiowych dołączających się do punktów dostępowych (AP) nie trzeba chyba nikogo przekonywać. Każdemu zależy na zabezpieczeniu dostępu do sieci bezprzewodowej. Można stosować do tego celu szyfrowanie połączenia. Jednak nie zawsze jest to konieczne a może zmniejszyć przepustowość łącz radiowych. Dla WISP najistotniejsze jest zabezpieczenie przed nieuprawnionym dostępem do sieci bezprzewodowej. Stąd szyfrowanie jest zbędne i wystarczy autoryzacja urządzeń radiowych z wykorzystaniem adresów MAC. Jednak w dużych sieciach bezprzewodowych, gdzie istnieje wiele punktów dostępowych, kłopotliwe jest zarządzanie tablicą autoryzowanych adresów MAC na każdym AP osobno. Dlatego przydatna staje się możliwość scentralizowanego zarządzania.

Niektóre typy punktów dostępowych umożliwiają autoryzację z wykorzystaniem zewnętrznego serwera RADIUS. Co to daje? Informacje o autoryzowanych urządzeniach przechowywane są w jednym miejscu. Dlatego zarządzanie staje się łatwiejsze i elastyczniejsze. Po jednorazowym wpisaniu adresu MAC urządzenia klienckiego możliwe jest łączenie się urządzenia z każdym AP korzystającym z serwera RADIUS.

• **Personal** - wszystkie podłączone stacje wykorzystują jeden klucz dzielony przypisywany ręcznie przez administratora (PSK - *Pre-Shared Key*).

3. WPA2 - (WiFi Protected Access) - zawiera poprawki eliminujące wszystkie znalezione luki w zabezpieczeniach WEP i WPA. W porównaniu z W PA wykorzystuje dynamiczne klucze o długości 128 bitów i automatycznie je dystrybuuje. Wykorzystuje algorytm szyfrowania AES. Jest zalecany do stosowania w sieciach bezprzewodowych.

****

PODSUMOWANIE

****

Dziesięć przykazań zabezpieczenia sieci WLAN.

1. Wyłącz rozgłaszanie komunikatów SSID na AP.
   Dzięki temu przypadkowy podsłuchiwacz nie pozna od razu nazwy sieci, co odsieje większość przypadkowych ciekawskich.
2. Włącz szyfrowanie WEP z kluczem 128 bitów.
   Zmusi to włamywacza do spędzenia na łamaniu klucza co najmniej kilkadziesiąt minut, a to powinno zniechęcić 99% podsłuchiwaczy.
3. Jeśli z powodów technicznych albo organizacyjnych nie możesz używać kluczy 128-bitowych, korzystaj choćby z kluczy 40-bitowych. Rezultat będzie podobny, bo podsłuchiwacz nie wie, jaki klucz jest używany. Włącz WEP dla wszystkich klientów. Nawet jedno niezabezpieczone połączenie może ujawnić włamywaczowi wiele informacji, dzięki którym będzie w stanie przełamywać kolejne zabezpieczenia.
4. Traktuj identyfikatory SSID jak hasła. Nawet jeśli masz wyłączone rozgłaszanie SSID, jest wiele programów błyskawicznie odgadujących proste SSID na podstawie słownika. Przypadkowy SSID (np. Iey2ohgu) nie jest trudny do wpisania, a bardzo wydłuża zgadywanie albo w ogóle je uniemożliwia.

5. Stosuj trudne do zgadnięcia hasła WEP. Teoretycznie hasło dla 40-bitowego klucza WEP powinno mieć ok. 20 znaków, a dla 128-bitowego - niemal 85 znaków (wiele urządzeń dopuszcza nawet hasła do 128 znaków), stosuj minimum hasła 10-znakowe.
6. Nie zapomnij o zabezpieczeniu koncentratora WLAN. Większość AP udostępnia usługi telnet, SNMP z prostym hasłem fabrycznym lub bez hasła. Pozwala to włamywaczowi bez wysiłku poznać hasła WEP i konfigurację sieci.
7. Od czasu do czasu testuj bezpieczeństwo swojej sieci. Sprawdzaj, czy nie pojawiły się nieautoryzowane stacje, czy w sieci nie pojawiają się nieszyfrowane pakiety i czy ESSID nie "wycieka" przez którąś ze stacji roboczych lub AP.
8. Nie podłączaj AP bezpośrednio do okablowania strukturalnego lub serwera. Zabezpiecz dostęp do sieci wewnętrznej za pomocą zapory firewall. W razie włamania do WLAN cała podsieć będzie pod kontrolą intruza.
9. Jeśli w sieci WLAN są przesyłane ważne dane, które nie powinny wydostać się na zewnątrz, oprócz włączenia WEP rozważ niezależne od niego tunelowanie VPN wykorzystujące sprawdzony, bezpieczny protokół IPsec.
10. Rada na koniec: korzystajmy ze wszystkich dostępnych zabezpieczeń, na które możemy sobie pozwolić - również tych najprostszych. Pamiętajmy, że 90% skutecznych włamań do sieci WLAN jest rezultatem braku jakichkolwiek zabezpieczeń.