WLAN CONCEPTS

Titlul Modulului	Obiectivul Modulului
Introducere în Rețelele Fără Fir	Descrierea tehnologiei și standardelor WLAN.
Componente ale rețelelor WLAN	Descrierea componentelor unei infrastructuri WLAN.
Operații WLAN	Explicarea modului în care tehnologia fără fir permite funcționarea WLAN.
Operațiuni CAPWAP	Explicarea modului în care un WLC utilizează CAPWAP pentru a gestiona mai multe AP-uri.
Managementul Canalului	Descrierea managementului canalului într-un WLAN.
Amenințările WLANurilor	Descrierea amenințărilor la adresa rețelelor WLAN.
Securizarea WLANurilor	Descrierea mecanismelor de securitate WLAN.

Control and Provisioning of Wireless Access Points.

12.1.1 - BENEFICIILE REȚELELOR WIRELESS

O rețea LAN fără fir (WLAN) este un tip de rețea fără fir care este utilizată în mod obișnuit în case, birouri și medii de campus. Rețelele trebuie să sprijine oamenii care sunt în mișcare. Oamenii se conectează folosind computere, laptopuri, tablete și telefoane inteligente. Există multe infrastructuri de rețea diferite care oferă acces la rețea, cum ar fi rețele LAN cu fir, rețele de furnizori de servicii și rețele de telefonie mobilă. Dar WLAN-ul este cel care face posibilă mobilitatea în mediul de acasă și de afaceri.

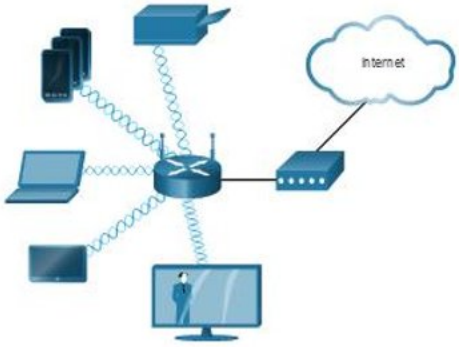
În întreprinderile cu o infrastructură wireless existentă, pot exista economii de costuri oricând se schimbă echipamentul sau când se mută un angajat într-o clădire, se reorganizează echipamente sau un laborator sau când se mută în locații temporare sau locații de proiect. O infrastructură fără fir se poate adapta nevoilor și tehnologiilor în schimbare rapidă.

12.1.2 - TIPURI DE REȚELE FĂRĂ FIR

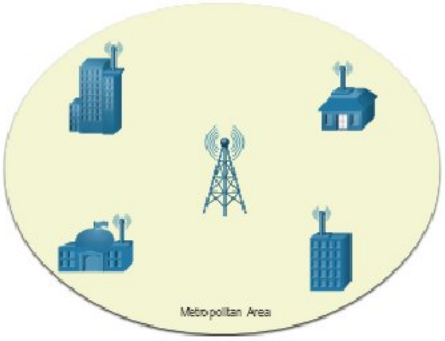
Rețelele fără fir se bazează pe standardele Institute of Electrical and Electronics Engineers (IEEE) și pot fi clasificate în general în patru tipuri principale: WPAN, WLAN, WMAN și WWAN.

1. ***Rețele fără fir personal-zonă (WPAN)*** *- Utilizează transmițătoare cu putere redusă pentru o rețea cu rază scurtă de acțiune, de obicei între 20 și 30 de picioare (6 până la 9 metri). Dispozitivele bazate pe Bluetooth și ZigBee sunt utilizate în mod obișnuit în WPAN. WPAN-urile se bazează pe standardul 802.15 și pe o frecvență radio de 2,4 GHz.*

2. ***LAN fără fir (WLAN)*** - *Utilizează transmițătoare pentru a acoperi o rețea de dimensiuni medii, de obicei până la 300 de picioare. Rețelele WLAN sunt potrivite pentru utilizare într-o casă, birou și chiar într-un mediu de campus. Rețelele WLAN se bazează pe standardul 802.11 și pe o frecvență radio de 2,4 GHz sau 5 GHz.*



3. ***Wireless MANs (WMAN)*** - *Utilizează transmițătoare pentru a furniza servicii fără fir pe o zonă geografică mai mare. WMAN-urile sunt potrivite pentru a oferi acces wireless la un oraș metropolitan sau un anumit district. WMAN-urile folosesc frecvențe specifice licențiate.*



4. ***Rețele wireless pe suprafață largă (WWAN)*** - *Utilizează transmițătoare pentru a oferi acoperire pe o zonă geografică extinsă. WWAN-urile sunt potrivite pentru comunicații naționale și globale. WWAN-urile folosesc, de asemenea, frecvențe specifice licențiate.*

12.1.3 - TEHNOLOGII FĂRĂ FIR

Tehnologia wireless folosește spectrul radio fără licență pentru a trimite și a primi date. Spectrul fără licență este accesibil oricui are un router wireless și tehnologie wireless în dispozitivul pe care îl folosește.

A. ***Bluetooth*** - Un standard IEEE 802.15 WPAN care utilizează un proces de împerechere a dispozitivelor pentru a comunica pe distanțe de până la 300 ft. (100 m). Poate fi găsit în dispozitive inteligente de acasă, conexiuni audio, automobile și alte dispozitive care necesită o conexiune la distanță scurtă. Există două tipuri de radio Bluetooth:

A.1 Bluetooth Low Energy (BLE) - Acesta acceptă mai multe tehnologii de rețea, inclusiv topologia mesh pentru dispozitive de rețea la scară largă.

A.2 Bluetooth Basic Rate/Enhanced Rate (BR/EDR) - Acesta acceptă topologii punct la punct și este optimizat pentru streaming audio.

B. WiMAX (Worldwide Interoperability for Microwave Access) - WiMAX este o alternativă la conexiunile de internet prin cablu în bandă largă, concurând cu DSL și cablu. Cu toate acestea, este utilizat de obicei în zonele care nu sunt încă conectate la un furnizor DSL sau de cablu. Este un standard IEEE 802.16 WWAN care oferă acces la bandă largă fără fir de mare viteză de până la 30 mile (50 km). WiMAX funcționează într-un mod similar cu Wi-Fi, dar la viteze mai mari, pe distanțe mai mari și pentru un număr mai mare de utilizatori. Utilizează o rețea de turnuri WiMAX care sunt similare cu turnurile de telefoane mobile. Transmițătoarele WiMAX și transmițătoarele celulare pot împărți spațiu pe același turn, așa cum se arată în figură.

C. Banda largă celulară - Cellular 4G/5G sunt rețele mobile fără fir utilizate în principal de telefoanele celulare, dar pot fi utilizate în automobile, tablete și laptopuri. Rețelele celulare sunt rețele cu acces multiplu care transportă atât comunicații de date, cât și de voce. Un site celular este creat de un turn celular care transmite semnale într-o zonă dată. Site-urile de interconectare celulară formează rețeaua celulară. Cele două tipuri de rețele celulare sunt Global System for Mobile (GSM) și Code Division Multiple Access (CDMA). GSM este recunoscut la nivel internațional, în timp ce CDMA este utilizat în principal în SUA.

Rețeaua mobilă de generația a 4-a (4G) este rețeaua mobilă actuală. 4G oferă viteze de 10 ori mai mari decât rețelele 3G anterioare. Noul 5G deține promisiunea de a oferi viteze de 100 de ori mai mari decât 4G și de a conecta mai multe dispozitive la rețea decât oricând.

D. Bandă largă prin satelit - Oferă acces la rețea la site-uri la distanță prin utilizarea unei antene satelit direcționale care este aliniată cu un anumit satelit geostaționar pe orbita Pământului. De obicei, este mai scump și necesită o linie vizuală clară. De obicei, este folosit de proprietarii de case din mediul rural și de întreprinderile în care cablul și DSL nu sunt disponibile.

12.1.4 - STANDARDE 802.11

Lumea comunicațiilor fără fir este vastă. Cu toate acestea, pentru anumite competențe legate de locul de muncă, dorim să ne concentrăm asupra aspectelor specifice ale Wi-Fi. Cel mai bun loc pentru a

începe este cu standardele IEEE 802.11 WLAN. Aceste standarde definesc modul în care frecvențele radio sunt utilizate pentru legăturile fără fir. Majoritatea standardelor specifică că dispozitivele fără fir au o antenă pentru a transmite și a primi semnale fără fir pe frecvența radio specificată (2,4 GHz sau 5 GHz). Unele dintre standardele mai noi care transmit și recepționează la viteze mai mari necesită ca punctele de acces (AP) și clienții fără fir să aibă mai multe antene folosind tehnologia cu intrări multiple și ieșiri multiple (MIMO). MIMO folosește mai multe antene atât ca transmițător, cât și ca receptor pentru a îmbunătăți performanța comunicațiilor. Pot fi utilizate până la opt antene de transmisie și recepție pentru a crește debitul.

De-a lungul anilor au fost dezvoltate diverse implementări ale standardului IEEE 802.11. Tabelul evidențiază aceste standarde.

IEEE WLAN Standard	Radio Frequency	Description
802.11	2.4 GHz	○ *viteze de până la 2 Mbps*
802.11a	5 GHz	• viteze de până la 54 Mbps • zonă mică de acoperire • mai puțin eficient la penetrarea structurilor clădirilor • nu este interoperabil cu 802.11b și 802.11g
802.11b	2.4 GHz	▪ *viteze de până la 11 Mbps* ▪ *rază mai mare decât 802.11a* ▪ *mai capabil să pătrundă în structurile clădirii*
802.11g	2.4 GHz	➢ viteze de până la 54 Mbps ➢ compatibil cu 802.11b cu o lățime de bandă redusă
802.11n	2.4 GHz 5 GHz	○ *ratele de date variază de la 150 Mbps la 600 Mbps, cu o distanță de până la 70 m (230 picioare)* ○ *AP-urile și clienții fără fir necesită mai multe antene folosind tehnologia MIMO compatibil cu dispozitivele 802.11a/b/g cu rate de date limitate*
802.11ac	5 GHz	• oferă rate de date de la 450 Mbps la 1,3 Gbps (1300 Mbps) folosind tehnologia MIMO • Pot fi acceptate până la opt antene compatibil cu dispozitivele 802.11a/n cu rate de date limitate
802.11ax	2.4 GHz 5 GHz	▪ *cel mai recent standard lansat în 2019* ▪ *cunoscut și sub numele de Wi-Fi 6 sau High-Efficiency Wireless (HEW)* ▪ *oferă o eficiență energetică îmbunătățită, rate de date mai mari, capacitate crescută și se ocupă de multe dispozitive conectate* ▪ *în prezent funcționează folosind 2,4 GHz și 5 GHz, dar va folosi 1 GHz și 7 GHz când acele frecvențe vor deveni disponibile* ▪ *Pentru mai multe informații pe internet* ***Wi-Fi Generation 6***

12.1.5 - FRECVENȚE RADIO

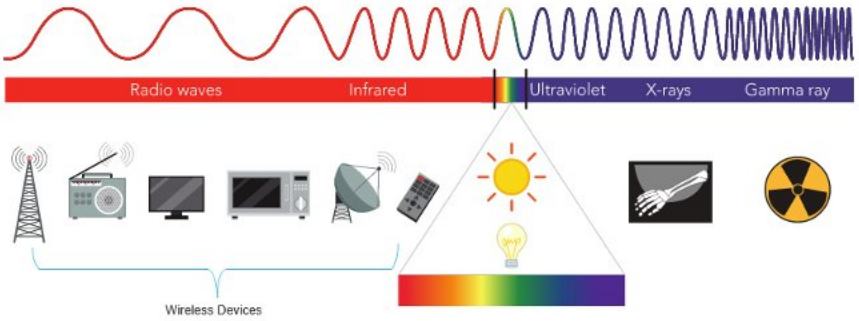
Toate dispozitivele fără fir funcționează în domeniul undelor radio din spectrul electromagnetic. Rețelele WLAN funcționează în banda de frecvență de 2,4 GHz și în banda de 5 GHz. Dispozitivele

LAN fără fir au transmițătoare și receptoare reglate la frecvențe specifice din domeniul undelor radio, așa cum se arată în figură. Mai exact, următoarele benzi de frecvență sunt alocate rețelelor LAN fără fir 802.11:

i. ***2,4 GHz (UHF) - 802.11b/g/n/ax***

ii. ***5 GHz (SHF) - 802.11a/n/ac/ax***

Spectrul Electromagnetic.



12.1.6 - ORGANIZAȚII PENTRU STANDARDE WIRELESS

Standardele asigură interoperabilitatea între dispozitivele care sunt fabricate de diferiți producători. Pe plan internațional, cele trei organizații care influențează standardele WLAN sunt ITU-R, IEEE și Wi-Fi Alliance.

a) ***Uniunea Internațională a Telecomunicațiilor (ITU)*** *- reglementează alocarea spectrului de frecvențe radio și a orbitelor sateliților prin ITU-R. ITU-R înseamnă ITU Radiocommunication Sector.*

b) ***Institute of Electrical and Electronics Engineers (IEEE)*** *- specifică modul în care o frecvență radio este modulată pentru a transporta informații. Menține standardele pentru rețelele locale și metropolitane (MAN) cu familia de standarde IEEE 802 LAN/MAN. Standardele dominante din familia IEEE 802 sunt 802.3 Ethernet și 802.11 WLAN.*

c) ***Wi-Fi Alliance*** *- este o asociație comercială globală, non-profit, dedicată promovării creșterii și acceptării rețelelor WLAN. Este o asociație de furnizori al cărei obiectiv este să îmbunătățească interoperabilitatea produselor care se bazează pe standardul 802.11 prin certificarea furnizorilor pentru conformitatea cu normele din industrie și aderarea la standarde.*

12.2.2 - NIC-URI WIRELESS

Implementările wireless necesită cel puțin două dispozitive care au un transmițător radio și un receptor radio reglate la aceleași frecvențe radio:

a. ***Dispozitive finale cu NIC-uri wireless***

b. ***Un dispozitiv de rețea, cum ar fi un router fără fir sau un AP fără fir***

Pentru a comunica fără fir, laptopurile, tabletele, telefoanele inteligente și chiar și cele mai recente automobile includ NIC-uri wireless integrate care încorporează un transmițător/receptor radio. Cu toate acestea, dacă un dispozitiv nu are o NIC wireless integrată, atunci poate fi utilizat un adaptor wireless USB, așa cum se arată în figură.

Notă: Multe dispozitive fără fir uzuale nu au antene vizibile. Sunt încorporate în smartphone-uri, laptop-uri și routere wireless de acasă.

Adaptor USB wireless

12.2.3 - ROUTER WIRELESS PENTRU ACASĂ

Tipul de dispozitiv de infrastructură cu care se asociază și se autentifică un dispozitiv final variază în funcție de dimensiunea și cerințele rețelei WLAN.

De exemplu, un utilizator casnic interconectează în mod obișnuit dispozitivele fără fir folosind un router fără fir mic, așa cum se arată în figură. Routerul wireless servește ca:

1. ***Punct de acces*** *- Acesta oferă acces wireless 802.11a/b/g/n/ac.*
2. ***Comutator*** *- Acesta oferă un comutator Ethernet cu patru porturi, full-duplex, 10/100/1000 pentru a interconecta dispozitivele cu fir.*
3. ***Router*** *- Acesta oferă un gateway implicit pentru conectarea la alte infrastructuri de rețea, cum ar fi internetul*.

Un router wireless este implementat în mod obișnuit ca un dispozitiv de acces wireless pentru întreprinderi mici sau rezidențiale. Routerul fără fir își face publicitate serviciilor fără fir prin trimiterea de semnalizatoare care conțin identificatorul de set de servicii partajat (SSID). Dispozitivele descoperă wireless SSID-ul și încearcă să se asocieze și să se autentifice cu acesta pentru a accesa rețeaua locală și internetul.

Majoritatea routerelor wireless oferă, de asemenea, funcții avansate, cum ar fi acces de mare viteză, suport pentru streaming video, adresare IPv6, calitatea serviciului (QoS), utilitare de configurare și porturi USB pentru conectarea imprimantelor sau unităților portabile.

În plus, utilizatorii casnici care doresc să-și extindă serviciile de rețea pot implementa extensii de gamă Wi-Fi. Un dispozitiv se poate conecta fără fir la extender, ceea ce îi sporește comunicațiile pentru a fi repetate la routerul wireless.

12.2.4 - PUNCTE DE ACCES WIRELESS

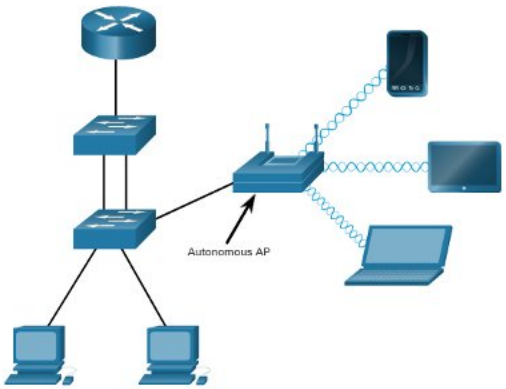
În timp ce extenderiile sunt ușor de configurat și configurat, cea mai bună soluție ar fi instalarea unui alt punct de acces wireless pentru a oferi acces wireless dedicat dispozitivelor utilizatorului. Clienții wireless își folosesc NIC-ul wireless pentru a descoperi AP-urile din apropiere care își fac publicitate SSID-ul. Clienții încearcă apoi să se asocieze și să se autentifice cu un AP. După ce au fost autentificați, utilizatorii wireless au acces la resursele rețelei. AP-urile Cisco Meraki Go sunt prezentate în figură.

12.2.5 - CATEGORII DE AP

AP-urile pot fi clasificate fie ca AP autonome, fie AP-uri bazate pe controler.

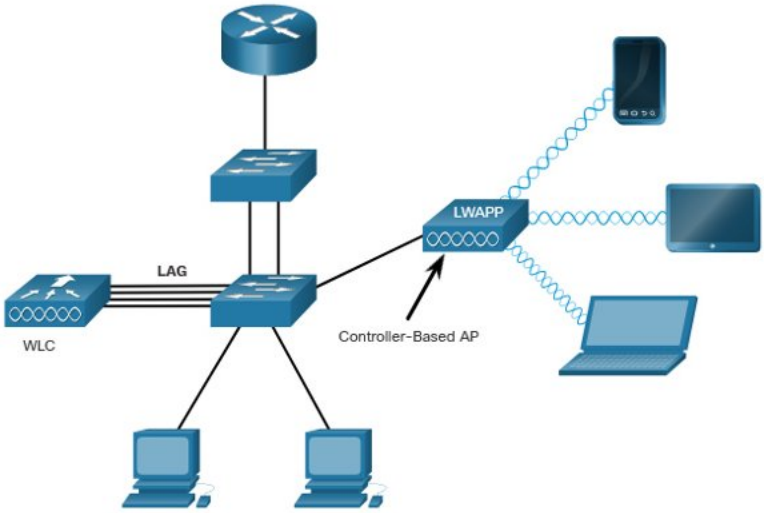
B. ***AP-uri autonome*** *- Acestea sunt dispozitive autonome configurate folosind o interfață de linie de comandă sau o interfață grafică, așa cum se arată în figură. AP-urile autonome sunt utile în situațiile în care sunt necesare doar câteva AP-uri în organizație. Un router de acasă este un exemplu de AP autonom deoarece întreaga configurație AP se află pe dispozitiv. Dacă cerințele wireless cresc,*

ar fi necesare mai multe AP-uri. Fiecare AP ar funcționa independent de alte AP și fiecare AP ar necesita configurație și management manual. Acest lucru ar deveni copleșitor dacă ar fi nevoie de multe AP-uri.



B. ***AP-uri bazate pe controler*** *- Aceste dispozitive nu necesită configurație inițială și sunt adesea numite AP-uri ușoare (LAP-uri). LAP-urile folosesc protocolul Lightweight Access Point (LWAPP) pentru a comunica cu un controler WLAN (WLC), așa cum se arată în figura următoare. AP-urile bazate pe controler sunt utile în situațiile în care sunt necesare multe AP-uri în rețea. Pe măsură ce se adaugă mai multe AP, fiecare AP este configurat și gestionat automat de WLC.*

Se poate observa în figură că WLC are patru porturi conectate la infrastructura de comutare. Aceste patru porturi sunt configurate ca un grup de agregare a legăturilor (LAG) pentru a le combina. La fel ca modul în care funcționează EtherChannel, LAG oferă redundanță și echilibrare a sarcinii. Toate porturile de pe switch care sunt conectate la WLC trebuie să fie trunchiate și configurate cu EtherChannel activat. Cu toate acestea, LAG nu funcționează exact ca EtherChannel. WLC nu acceptă Protocolul de agregare porturi (PaGP) sau Protocolul de control al agregarii de legături (LACP).



12.2.6 - ANTENE WIRELESS

Majoritatea AP-urilor de clasă business necesită antene externe pentru a le face unități pe deplin funcționale.

i. *Antenele omnidirecționale precum cea prezentată în figură oferă o acoperire la 360 de grade și sunt ideale în case, zone deschise de birouri, săli de conferințe și zone exterioare.*

ii. *Antenele direcționale concentrează semnalul radio într-o direcție dată. Acest lucru îmbunătățește semnalul către și de la AP în direcția în care este îndreptată antena. Aceasta oferă o putere mai puternică a semnalului într-o direcție și o putere redusă a semnalului în toate celelalte direcții. Exemple de antene direcționale Wi-Fi includ antene Yagi și antene parabolice.*

iii. *Multiple Input Multiple Output (MIMO) folosește mai multe antene pentru a crește lățimea de bandă disponibilă pentru rețelele wireless IEEE 802.11n/ac/ax. Pot fi utilizate până la opt antene de transmisie și recepție pentru a crește debitul.*

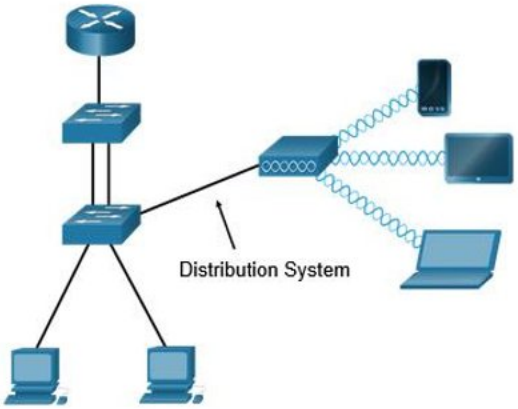
12.3.1 - FUNCȚIONARE WLAN

12.3.2 - 802.11 MODURI DE TOPOLOGII FĂRĂ FIR

Rețelele LAN fără fir pot găzdui diverse topologii de rețea. Standardul 802.11 identifică două moduri principale de topologie fără fir: modul Ad-hoc și modul Infrastructură. Tethering-ul este, de asemenea, un mod folosit uneori pentru a oferi acces rapid wireless.

1. ***Modul ad hoc*** *- Acesta este atunci când două dispozitive se conectează fără fir într-un mod peer-to-peer (P2P) fără a utiliza AP-uri sau routere wireless. Exemplele includ clienții fără fir care se conectează direct între ei folosind Bluetooth sau Wi-Fi Direct. Standardul IEEE 802.11 se referă la o rețea ad-hoc ca un set de servicii de bază independent (IBSS).*

2. ***Modul infrastructură*** *- Acesta este atunci când clienții wireless se interconectează printr-un router wireless sau un AP, cum ar fi în rețele WLAN. AP-urile se conectează la infrastructura de rețea folosind sistemul de distribuție cu fir, cum ar fi Ethernet.*



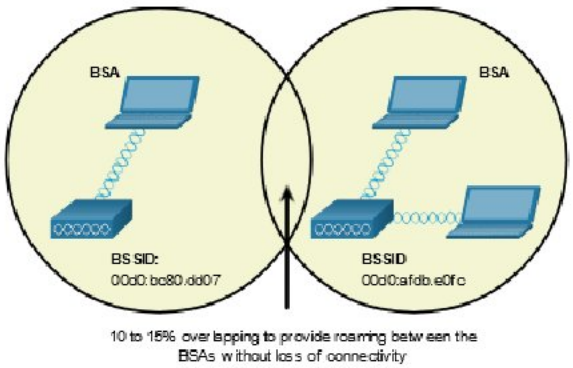
3. ***Tethering*** *- O variație a topologiei ad-hoc este atunci când un telefon inteligent sau o tabletă cu acces la date celulare este activată pentru a crea un hotspot personal. Această caracteristică este uneori denumită tethering. Un hotspot este de obicei o soluție rapidă temporară care permite unui telefon inteligent să ofere serviciile wireless ale unui router Wi-Fi. Alte dispozitive se pot asocia și autentifica cu telefonul inteligent pentru a utiliza conexiunea la internet.*

12.3.3 - BSS ȘI ESS

Modul infrastructură definește două blocuri de topologie: un set de servicii de bază (BSS) și un set de servicii extins (ESS).

1. ***Set de servicii de bază (Basic Service Set)-*** Un BSS constă dintr-un singur AP care interconecta toți clienții wireless asociați. Două BSS sunt prezentate în figură. Cercurile descriu zona de acoperire pentru BSS, care este numită Zona de servicii de bază (BSA). Dacă un client wireless se mută din BSA, acesta nu mai poate comunica direct cu alți clienți wireless din BSA.

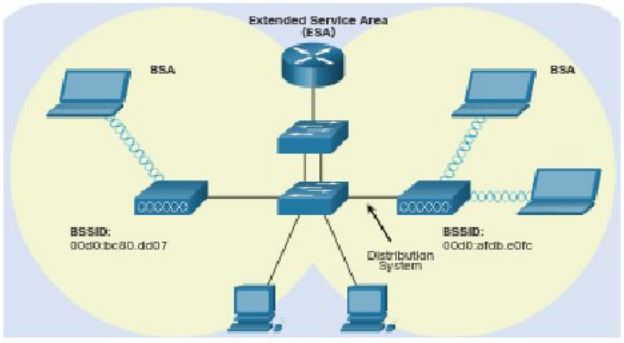
Adresa MAC Layer 2 a AP este utilizată pentru a identifica în mod unic fiecare BSS, care este numit Basic Service Set Identifier (BSSID). Prin urmare, BSSID este numele formal al BSS și este întotdeauna asociat cu un singur AP.



2. ***Set de servicii extinse (Extended Service Set)*** - Când un singur BSS oferă o acoperire insuficientă, două sau mai multe BSS-uri pot fi conectate printr-un sistem de distribuție comun (DS) într-un ESS. Un ESS este uniunea a două sau mai multe BSS-uri interconectate printr-un DS cu fir. Fiecare ESS este identificat printr-un SSID și fiecare BSS este identificat prin BSSID-ul său.

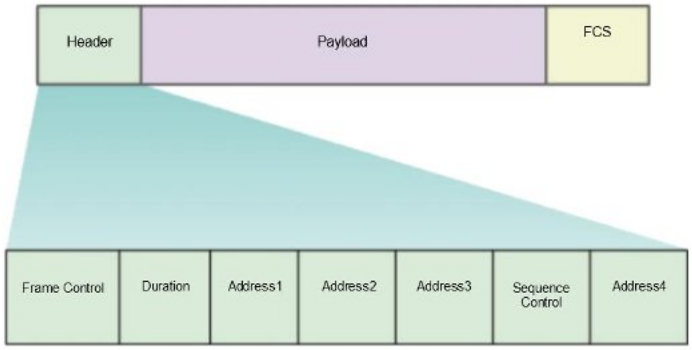
Clienții wireless dintr-un BSA pot comunica acum cu clienții wireless dintr-un alt BSA din cadrul aceluiași ESS. Clienții fără fir mobil în roaming se pot muta de la un BSA la altul (în cadrul aceluiași ESS) și se pot conecta fără probleme.

Zona dreptunghiulară din figură ilustrează zona de acoperire în care membrii unui ESS pot comunica. Această zonă se numește Extended Service Area (ESA).



12.3.4 - STRUCTURA CADRULUI 802.11

Se poate reaminti că toate cadrele Layer 2 constau dintr-un antet, sarcină utilă și secțiune Frame Check Sequence (FCS). Formatul de cadru 802.11 este similar cu formatul de cadru Ethernet, cu excepția faptului că conține mai multe câmpuri, așa cum se arată în figură.



Toate cadrele wireless 802.11 conțin următoarele câmpuri:

1. ***Frame Control*** - Acesta identifică tipul de cadru wireless și conține subcâmpuri pentru versiunea protocolului, tipul de cadru, tipul de adresă, managementul energiei și setările de securitate.
2. ***Durată*** - Aceasta este de obicei folosită pentru a indica durata rămasă necesară pentru a primi următoarea transmisie de cadru.

De pe un dispozitiv wireless:

i. **Address 1 Receiver Address** - *adresa MAC a AP-ului*.
ii. **Adresa 2 Transmitter Address** - *adresa MAC a expeditorului.*
iii. **Adresa 3 SA/DA/BSSID** - *adresa MAC a destinației care ar putea fi un dispozitiv fără fir sau un dispozitiv cu fir.*

De la AP:

a. Address 1 Receiver Address - adresa MAC a expeditorului.

b. Address 2 Transmitter Address - adresa MAC a AP-ului.

c. Adresa 3 SA/DA/BSSID - adresa MAC a destinatiei wireless.

d. Controlul secvenței - Acesta conține informații pentru a controla secvențierea și cadrele fragmentate.

e. Adresa4 - Aceasta lipsește de obicei deoarece este utilizată numai în modul ad-hoc.

f. Sarcină utilă - Acesta conține datele pentru transmitere.

g. FCS - Acesta este utilizat pentru controlul erorilor de nivel 2.

12.3.5 - CSMA/CA

WLAN-urile sunt configurații media partajate, semi-duplex. Half-duplex înseamnă că un singur client poate transmite sau recepționa la un moment dat. Media partajată înseamnă că toți clienții wireless pot transmite și primi pe același canal radio. Acest lucru creează o problemă deoarece un client wireless nu poate auzi în timp ce trimite, ceea ce face imposibilă detectarea unei coliziuni.

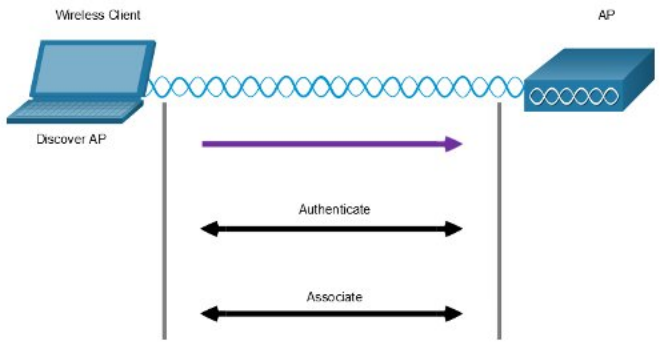
Pentru a rezolva această problemă, rețelele WLAN utilizează accesul multiplu de detectare a transportatorului cu evitarea coliziunilor (CSMA/CA) ca metodă pentru a determina cum și când să trimită date în rețea. Un client wireless face următoarele:

1. *Ascultă canalul pentru a vedea dacă este inactiv, ceea ce înseamnă că simte că nu există niciun alt trafic în prezent pe canal. Canalul este numit și purtător.*
2. *Trimite un mesaj de solicitare de trimitere (RTS) către AP pentru a solicita acces dedicat la rețea.*
3. *Primește un mesaj clar pentru trimitere (CTS) de la AP care acordă acces pentru trimitere.*
4. *Dacă clientul wireless nu primește un mesaj CTS, acesta așteaptă o perioadă de timp aleatorie înainte de a reporni procesul.*
5. *După ce primește CTS, transmite datele.*
6. *Toate transmisiile sunt confirmate. Dacă un client wireless nu primește o confirmare, presupune că a avut loc o coliziune și repornește procesul.*

12.3.6 - ASOCIEREA CLIENTULUI WIRELESS ȘI AP

Pentru ca dispozitivele wireless să comunice printr-o rețea, acestea trebuie mai întâi să se asocieze cu un AP sau un router fără fir. O parte importantă a procesului 802.11 este descoperirea unui WLAN și, ulterior, conectarea la acesta. Dispozitivele fără fir finalizează următorul proces în trei etape, așa cum se arată în figură:

A. ***Descoperirea unui AP wireless***
B. ***Autentificare cu AP***
C. ***Asocierea cu AP***



Pentru a avea o asociere de succes, un client wireless și un AP trebuie să convină asupra unor parametri specifici. Parametrii trebuie apoi configurați pe AP și ulterior pe client pentru a permite negocierea unei asocieri de succes.

i.***SSID*** -Numele SSID apare în lista de rețele wireless disponibile pe un client. În organizațiile mai mari care utilizează mai multe VLAN-uri pentru a segmenta traficul, fiecare SSID este mapat la un VLAN. În funcție de configurația rețelei, mai multe AP-uri dintr-o rețea pot partaja un SSID comun.

ii.***Parolă*** - Aceasta este necesară de la clientul wireless pentru a se autentifica la AP.

iii.Mod de rețea - Se referă la standardele WLAN 802.11a/b/g/n/ac/ad. AP-urile și routerele wireless pot funcționa într-un mod mixt, ceea ce înseamnă că pot accepta simultan clienții care se conectează prin mai multe standarde.

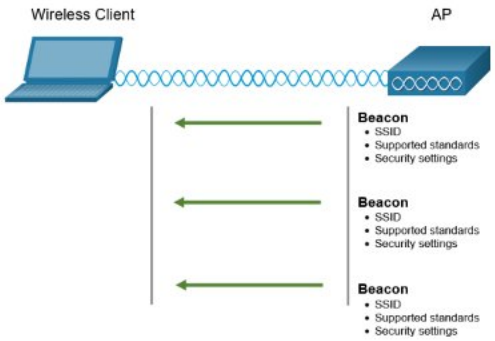
iv.***Mod de securitate*** - Se referă la setările parametrilor de securitate, cum ar fi WEP, WPA sau WPA2. Activați întotdeauna cel mai înalt nivel de securitate acceptat.

v.***Setări canal*** - Se referă la benzile de frecvență utilizate pentru a transmite date fără fir. Routerele și AP-urile fără fir pot scana canalele de frecvență radio și pot selecta automat o setare de canal adecvată. Canalul poate fi setat și manual dacă există interferențe cu un alt AP sau dispozitiv wireless.

12.3.7 - MODURI DE DESCOPERIRE PASIV ȘI ACTIVE

Dispozitivele wireless trebuie să descopere și să se conecteze la un AP sau un router wireless. Clienții wireless se conectează la AP folosind un proces de scanare (sondare). Acest proces poate fi pasiv sau activ.

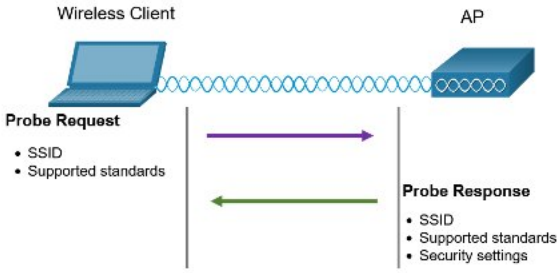
1. PASSIVE MODE - În modul pasiv, AP-ul își face reclamă în mod deschis serviciul trimițând periodic cadre de semnalizare care conțin SSID-ul, standardele acceptate și setările de securitate. Scopul principal al balizei este de a permite clienților fără fir să învețe ce rețele și punctele de acces sunt disponibile într-o anumită zonă. Acest lucru permite clienților fără fir să aleagă ce rețea și AP să folosească.



2. ACTIVE MODE - În modul activ, clienții wireless trebuie să cunoască numele SSID-ului. Clientul wireless inițiază procesul prin difuzarea unui cadru de solicitare a sondei pe mai multe canale.

Solicitarea probei include numele SSID și standardele acceptate. AP-urile configurate cu SSID vor trimite un răspuns de probă care include SSID-ul, standardele acceptate și setările de securitate. Modul activ poate fi necesar dacă un AP sau un router wireless este configurat să nu difuzeze cadre de semnalizare.

Un client wireless ar putea trimite, de asemenea, o cerere de sondă fără un nume SSID pentru a descoperi rețelele WLAN din apropiere. AP-urile configurate pentru a difuza cadre de baliză ar răspunde clientului fără fir cu un răspuns de probă și vor furniza numele SSID. AP-urile cu caracteristica SSID de difuzare dezactivată nu răspund.



OPERAȚIUNI CAPWAP

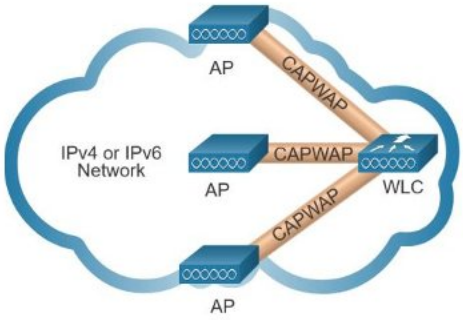
12.4.1 – CAPWAP

În ultimul subiect am aflat despre funcționarea WLAN. Acum vom afla despre controlul și furnizarea punctelor de acces fără fir (CAPWAP).

12.4.2 - INTRODUCERE ÎN CAPWAP

CAPWAP este un protocol standard IEEE care permite unui WLC să gestioneze mai multe AP-uri și WLAN-uri. CAPWAP este, de asemenea, responsabil pentru încapsularea și redirecționarea traficului clientului WLAN între un AP și un WLC.

CAPWAP se bazează pe LWAPP, dar adaugă securitate suplimentară cu Datagram Transport Layer Security (DTLS). CAPWAP stabilește tuneluri pe porturile UDP (User Datagram Protocol). CAPWAP poate funcționa fie prin IPv4, fie IPv6, așa cum se arată în figură, dar utilizează IPv4 în mod implicit. IPv4 și IPv6 folosesc ambele porturi UDP 5246 și 5247. Portul 5246 este pentru mesajele de control CAPWAP utilizate de WLC pentru a gestiona AP-ul. Portul 5247 este folosit de CAPWAP pentru a încapsula pachetele de date care călătoresc către și de la clienții wireless. Cu toate acestea, tunelurile CAPWAP folosesc diferite protocoale IP în antetul pachetului. IPv4 utilizează protocolul IP 17, iar IPv6 utilizează protocolul IP 136.



12.4.3 – DIVIZAREA ARHITECTURII MAC

O componentă cheie a CAPWAP este conceptul de control al accesului media divizat (MAC). Conceptul MAC split CAPWAP realizează toate funcțiile efectuate în mod normal de AP-urile individuale și le distribuie între două componente funcționale:

1. ***Funcții AP MAC***
2. ***Funcții WLC MAC***

Tabelul prezintă câteva dintre funcțiile MAC efectuate de fiecare.

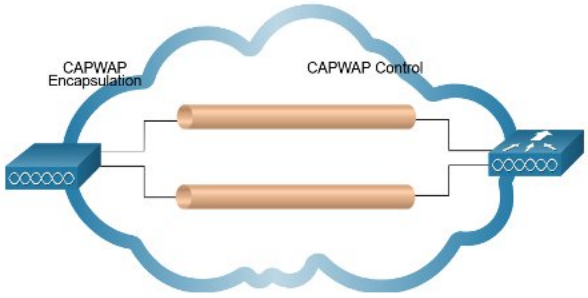
Funcții AP MAC	**Funcții WLC MAC**
Răspunsuri la balize și sondă	Autentificare
Confirmări de pachete și retransmisii	Asocierea și reasociere clienților de roaming
Așezarea cadrelor și prioritizarea pachetelor	Translatarea cadrelor în alte protocoale
Criptarea și decriptarea datelor la nivel MAC	Terminarea traficului 802.11 pe o interfață cu fir

12.4.4 - CRIPTARE DTLS

DTLS este un protocol care oferă securitate între AP și WLC. Le permite să comunice folosind criptarea și previne interceptarea sau manipularea.

DTLS este activat implicit pentru a securiza canalul de control CAPWAP, dar este dezactivat implicit pentru canalul de date, așa cum se arată în figură. Tot traficul de gestionare și control CAPWAP schimbat între un AP și WLC este criptat și securizat în mod implicit pentru a oferi confidențialitate a planului de control și pentru a preveni atacurile Man-In-the-Middle (MITM).

Criptarea datelor CAPWAP este opțională și este activată pe AP. Criptarea datelor necesită instalarea unei licențe DTLS pe WLC înainte de a fi activată pe un AP. Când este activat, tot traficul clientului WLAN este criptat la AP înainte de a fi redirecționat către WLC și invers.



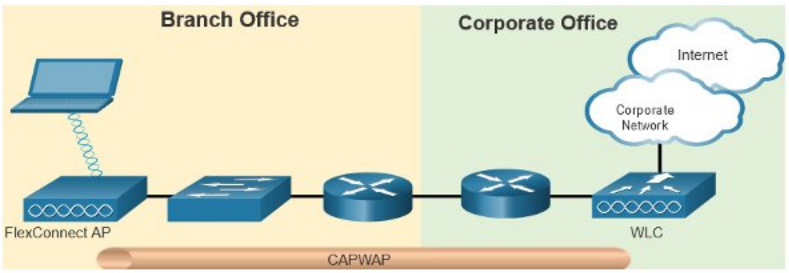
12.4.5 - AP-URI FLEXCONNECT

FlexConnect este o soluție wireless pentru implementări de filiale și birouri de la distanță. Vă permite să configurați și să controlați punctele de acces dintr-o sucursală de la biroul corporativ printr-o legătură WAN, fără a instala un controler în fiecare birou.

Există două moduri de operare pentru FlexConnect AP.

1. ***Mod conectat*** - WLC este accesibil. În acest mod, FlexConnect AP are conectivitate CAPWAP cu WLC și poate trimite trafic prin tunelul CAPWAP, așa cum se arată în figură. WLC își îndeplinește toate funcțiile CAPWAP.

2. ***Modul autonom*** - WLC este inaccesibil. FlexConnect a pierdut sau nu a reușit să stabilească conectivitatea CAPWAP cu WLC-ul său. În acest mod, un AP FlexConnect poate asuma unele dintre funcțiile WLC, cum ar fi comutarea locală a traficului de date client și efectuarea locală de autentificare a clientului.



MANAGEMENTUL CANALULUI

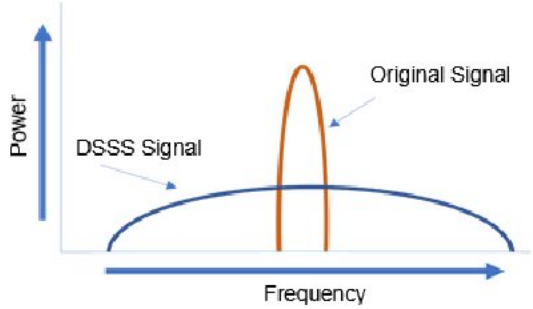
12.5.1 - SATURAȚIA CANALULUI DE FRECVENȚĂ

Dispozitivele LAN fără fir au transmițătoare și receptoare reglate pe anumite frecvențe ale undelor radio pentru a comunica. O practică comună este ca frecvențele să fie alocate ca intervale. Astfel de intervale sunt apoi împărțite în intervale mai mici numite canale.

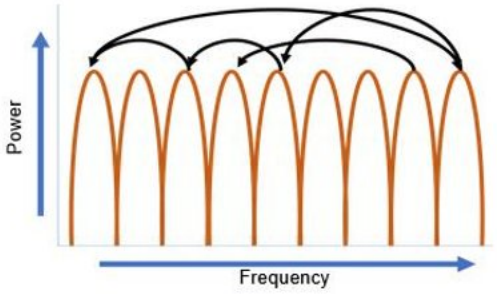
Dacă cererea pentru un anumit canal este prea mare, este posibil ca acel canal să devină suprasaturat. Saturația mediului wireless degradează calitatea comunicației. De-a lungul anilor, au fost create o serie de tehnici pentru a îmbunătăți comunicarea fără fir și a atenua saturația. Aceste tehnici atenuează saturația canalului utilizând canalele într-un mod mai eficient.

A. ***Direct-Sequence Spread Spectrum (DSSS)*** - Aceasta este o tehnică de modulație concepută pentru a răspândi un semnal pe o bandă de frecvență mai mare. Tehnicile cu spectru extins au fost dezvoltate în timpul războiului pentru a îngreuna inamicii să intercepteze sau să blocheze un semnal de comunicare. Face acest lucru prin răspândirea semnalului pe o frecvență mai largă care ascunde efectiv vârful vizibil al semnalului, așa cum se arată în figură. Un receptor configurat corect poate

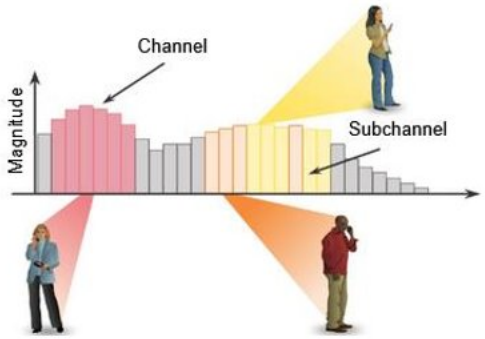
inversa modulația DSSS și poate reconstrui semnalul original. DSSS este utilizat de dispozitivele 802.11b pentru a evita interferențele de la alte dispozitive care folosesc aceeași frecvență de 2,4 GHz.



B. ***Frequency-Hopping Spread Spectrum (FHSS)*** - Acesta se bazează pe metode cu spectru împrăștiat pentru a comunica. Transmite semnale radio prin comutarea rapidă a unui semnal purtător între multe canale de frecvență. Cu FHSS, emițătorul și receptorul trebuie să fie sincronizate pentru a „ști" la ce canal să sară. Acest proces de salt de canale permite o utilizare mai eficientă a canalelor, scăzând congestionarea canalului. FHSS a fost folosit de standardul original 802.11. Walkie-talki-urile și telefoanele fără fir de 900 MHz folosesc, de asemenea, FHSS, iar Bluetooth utilizează o variantă de FHSS.



C. ***Orthogonal Frequency-Division Multiplexing (OFDM)*** - Acesta este un subset de multiplexare cu diviziune de frecvență în care un singur canal folosește mai multe sub-canale pe frecvențe adiacente. Sub-canalele dintr-un sistem OFDM sunt precis ortogonale între ele, ceea ce permite sub-canalelor să se suprapună fără interferențe. OFDM este utilizat de o serie de sisteme de comunicații, inclusiv 802.11a/g/n/ac. Noul 802.11ax folosește o variantă a OFDM numită Orthogonal frequency-division multiaccess (OFDMA).



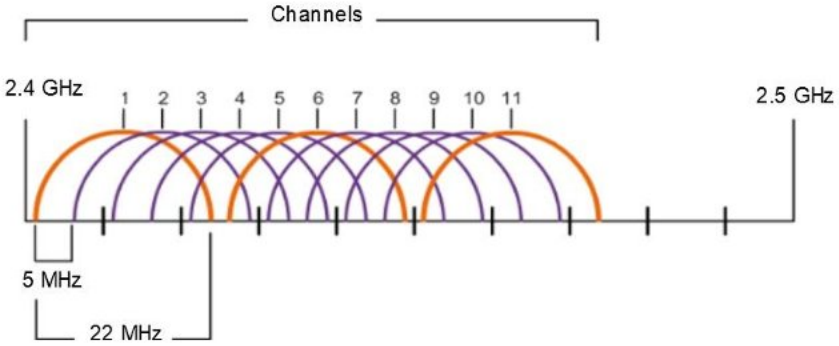
12.5.2 - SELECTAREA CANALULUI

O bună practică pentru rețelele WLAN care necesită mai multe AP-uri este utilizarea canalelor care nu se suprapun. De exemplu, standardele 802.11b/g/n operează în spectrul de la 2,4 GHz până la 2,5 GHz. Banda de 2,4 GHz este subdivizată în mai multe canale. Fiecare canal are o lățime de bandă de 22 MHz și este separat de canalul următor cu 5 MHz. Standardul 802.11b identifică 11 canale pentru America de Nord, așa cum se arată în figură (13 în Europa și 14 în Japonia).

Notă: Se pot căuta pe internet canale de 2,4 GHz pentru a afla mai multe despre variațiile pentru diferite țări.

Figura arată 11 canale care au o lățime de 22 MHz și 5 MHz între fiecare. Spectrul este între 2,2 GHz și 2,5 GHz.

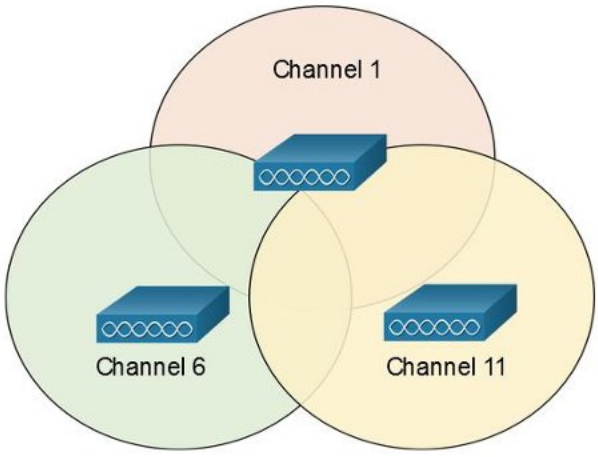
Canale suprapuse de 2,4 GHz în America de Nord



Interferența apare atunci când un semnal se suprapune pe un canal rezervat unui alt semnal, provocând posibile distorsiuni. Cea mai bună practică pentru rețelele WLAN de 2,4 GHz care necesită mai multe AP-uri este utilizarea canalelor care nu se suprapun, deşi majoritatea AP-urilor moderne vor face acest lucru automat. Dacă există trei AP-uri adiacente, utilizați canalele 1, 6 și 11, așa cum se arată în figură.

Figura arată trei AP-uri folosind canalele 1, 6 și 11.

Canale fără suprapunere de 2,4 GHz pentru 802.11b/g/n

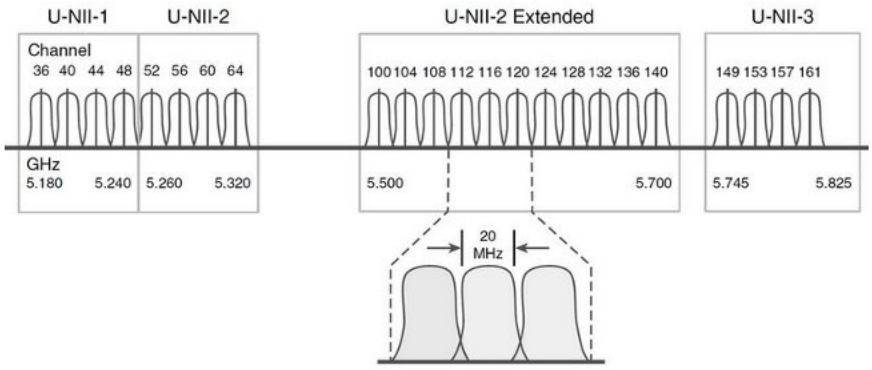


Pentru standardele de 5 GHz 802.11a/n/ac, există 24 de canale. Banda de 5 GHz este împărțită în trei secțiuni. Fiecare canal este separat de canalul următor cu 20 MHz. Figura arată toate cele 24 de canale fără licență ale Infrastructurii Naționale de Informații (U-NNI) 24 pentru banda de 5 GHz. Deși există o ușoară suprapunere la cozile frecvenței fiecărui canal, canalele nu interferează unul cu celălalt. Wireless de 5 GHz poate oferi o transmisie de date mai rapidă pentru clienții fără fir din rețelele fără fir foarte populate, datorită cantității mari de canale wireless care nu se suprapun.

Notă: Se pot căuta pe internet canale de 5 GHz pentru a afla mai multe despre variațiile pentru diferite țări.

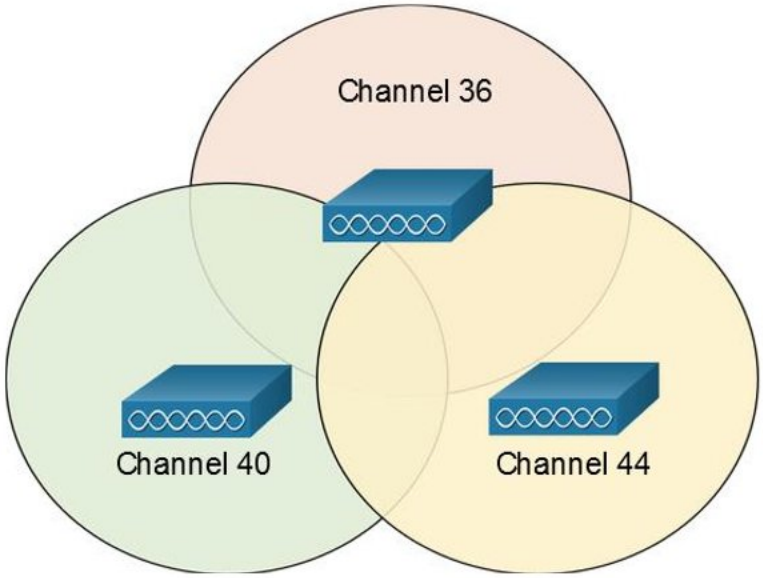
Figura arată 8 canale care au 20 MHz între fiecare. Spectrul este între 5150 MHz și 5350 MHz.

Primele opt canale de 5 GHz care nu interferează



Ca și în cazul rețelelor WLAN de 2,4 GHz, se vor alege canale care nu interferează atunci când se configurează mai multe AP-uri de 5 GHz care sunt adiacente unul altuia, așa cum se arată în figură.

Figura arată trei AP-uri folosind canalele 36, 48 și 60.



12.5.3 - Planificarea unei implementări WLAN

Numărul de utilizatori acceptați de un WLAN depinde de aspectul geografic al unității, inclusiv de numărul de corpuri și dispozitive care pot încăpea într-un spațiu, de ratele de date pe care utilizatorii se așteaptă să le utilizeze, de utilizarea canalelor care nu se suprapun de către mai multe AP-uri într-un ESS și setările de putere de transmisie.

Când se va planifica locația AP-urilor, aria de acoperire circulară aproximativă este importantă (așa cum se arată în figură), dar există câteva recomandări suplimentare:

Dacă AP-urile vor folosi cablurile existente sau dacă există locații în care AP-urile nu pot fi plasate, aceste locații vor fi notate pe hartă.

Se vor reține toate sursele potențiale de interferență care pot include cuptoare cu microunde, camere video fără fir, lumini fluorescente, detectoare de mișcare sau orice alt dispozitiv care utilizează gama de 2,4 GHz.

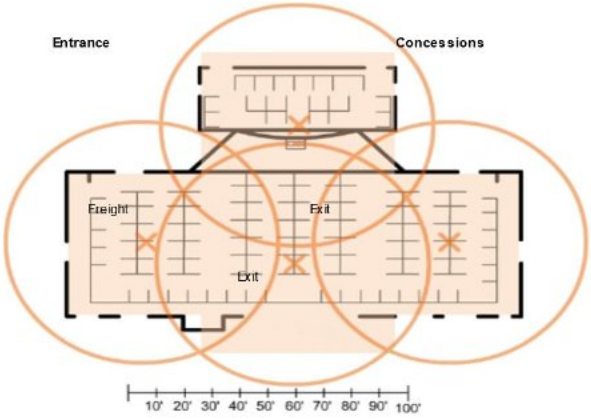
AP-urile vor fi poziționate deasupra obstacolelor.

Dacă este posibil, AP-urile vor fi poziționate vertical lângă tavan în centrul fiecărei zone de acoperire.

AP-urile vor fi poziționate în locații în care se așteaptă să se afle utilizatorii. De exemplu, sălile de conferințe sunt de obicei o locație mai bună pentru AP-uri decât un hol.

Dacă o rețea IEEE 802.11 a fost configurată pentru modul mixt, clienții wireless pot experimenta viteze mai lente decât cele normale pentru a accepta standardele wireless mai vechi.

Când se va estima aria de acoperire așteptată a unui AP, se va realiza că această valoare variază în funcție de standardul WLAN sau de amestecul de standarde care sunt implementate, de natura unității și de puterea de transmisie pentru care este configurat AP. Este foarte important, ca întotdeauna să fie consultate specificațiile pentru AP atunci când se vor planifica zonele de acoperire.



AMENINȚĂRI LA REȚELELE WLAN

12.6.1 - AMENINȚĂRI LA REȚELELE WLAN

Subiectele anterioare au acoperit componentele și configurația WLAN. La acest pas vor fi învățate amenințările la WLAN.

12.6.2 - PREZENTARE GENERALĂ A SECURITĂȚII FĂRĂ FIR

Un WLAN este deschis oricui se află în raza de acțiune a unui AP și a acreditărilor corespunzătoare pentru a se asocia cu acesta. Cu o NIC wireless și cunoștințe despre tehnicile de cracare, un atacator poate să nu fie nevoit să intre fizic la locul de muncă pentru a obține acces la un WLAN.

Atacurile pot fi generate de persoane din afară, angajați nemulțumiți și chiar neintenționat de către angajați. Rețelele wireless sunt susceptibile în mod specific la mai multe amenințări, inclusiv:

a) ***Interceptarea datelor*** *- Datele wireless ar trebui să fie criptate pentru a preveni citirea lor de către cei care interceptează.*

b) ***Intruziuni fără fir*** *- Utilizatorii neautorizați care încearcă să acceseze resursele rețelei pot fi descurajați prin tehnici eficiente de autentificare.*

c) ***Atacurile de respingere a serviciului (DoS)*** *- Accesul la serviciile WLAN poate fi compromis fie accidental, fie rău intenționat. Există diverse soluții în funcție de sursa atacului DoS.*

d) ***AP-uri neautorizate*** *- AP-urile neautorizate instalate de un utilizator bine intenționat sau în scopuri rău intenționate pot fi detectate folosind un software de management.*

12.6.3 – ATACURILE DE TIP DOS

Atacurile de tip DoS wireless pot fi rezultatul:

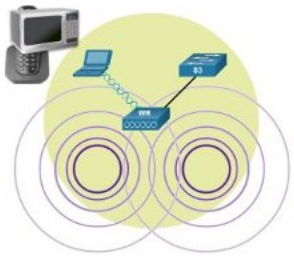
i. ***Dispozitive configurate incorect*** - Erorile de configurare pot dezactiva WLAN-ul. De exemplu, un administrator ar putea modifica accidental o configurație și dezactiva rețeaua, sau un intrus cu privilegii de administrator ar putea dezactiva în mod intenționat un WLAN.

ii. ***Un utilizator rău intenționat*** - care interferează în mod intenționat cu comunicația wireless - Scopul lor este de a dezactiva complet rețeaua wireless sau până la punctul în care niciun dispozitiv legitim nu poate accesa mediul.

iii. ***Interferențe accidentale*** - WLAN-urile sunt predispuse la interferențe de la alte dispozitive fără fir, inclusiv cuptoare cu microunde, telefoane fără fir, monitoare pentru copii și multe altele, așa cum se arată în figură. Banda de 2,4 GHz este mai predispusă la interferențe decât banda de 5 GHz.

Pentru a minimiza riscul unui atac DoS din cauza dispozitivelor configurate necorespunzător și a atacurilor rău intenționate, toate dispozitivele vor fi întărite, vor fi păstrate parolele în siguranță, vor fi create copii de rezervă și se va asigura că toate modificările de configurare sunt încorporate în afara orelor de program.

Va fi monitorizat WLAN-ul pentru orice probleme accidentale de interferență și le va rezolva pe măsură ce apar. Deoarece banda de 2,4 GHz este utilizată de alte tipuri de dispozitive, banda de 5 GHz ar trebui utilizată în zonele predispuse la interferențe.

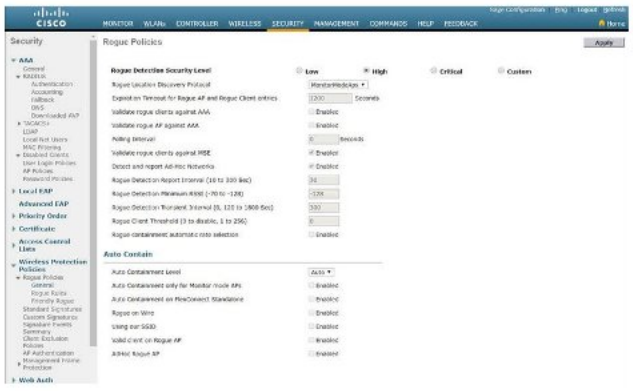


12.6.4 - PUNCTE DE ACCES NECINSTITE (ROGUE)

Un AP necinstit este un AP sau un router wireless care a fost conectat la o rețea corporativă fără autorizare explicită și împotriva politicii corporative. Oricine are acces la sediu poate instala (în mod rău intenționat sau nu) un router wireless ieftin care poate permite accesul la o resursă de rețea sigură. Odată conectat, AP-ul necinstiți poate fi folosit de către un atacator pentru a captura adrese MAC, pentru a captura pachete de date, pentru a obține acces la resursele rețelei sau pentru a lansa un atac de tip man-in-the-middle.

Un hotspot de rețea personală ar putea fi, de asemenea, utilizat ca un AP necinstit. De exemplu, un utilizator cu acces securizat la rețea permite gazdei Windows autorizate să devină un AP Wi-Fi. Procedând astfel, se eludează măsurile de securitate și alte dispozitive neautorizate pot accesa acum resursele rețelei ca dispozitiv partajat.

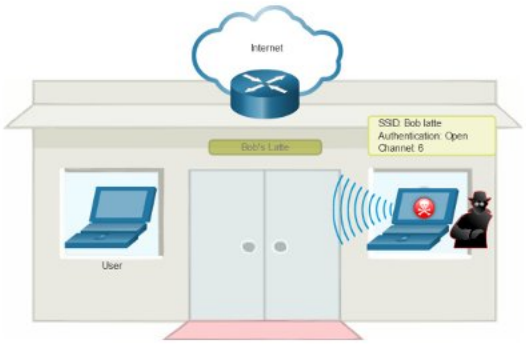
Pentru a preveni instalarea de AP-uri necinstite, organizațiile trebuie să configureze WLC-urile cu politici AP-uri neautorizate, așa cum se arată în figură, și să utilizeze software de monitorizare pentru a monitoriza în mod activ spectrul radio pentru AP-uri neautorizate.



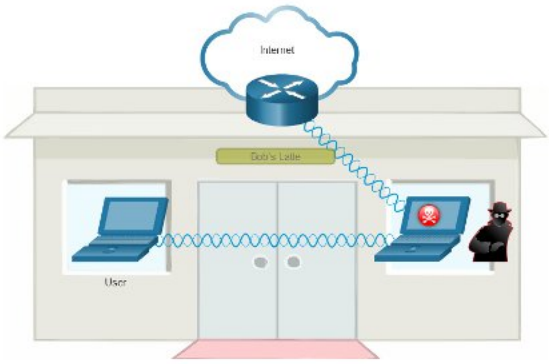
12.6.5 - MAN-IN-THE-MIDDLE

Într-un atac man-in-the-middle (MITM), hackerul este poziționat între două entități legitime pentru a citi sau modifica datele care trec între cele două părți. Există multe moduri prin care se poate crea un atac MITM.

Un atac popular MITM wireless se numește atacul „evil twin AP", în care un atacator introduce un AP necinstit și îl configurează cu același SSID ca un AP legitim, așa cum se arată în figură. Locațiile care oferă Wi-Fi gratuit, cum ar fi aeroporturile, cafenelele și restaurantele, sunt locuri deosebit de populare pentru acest tip de atac datorită autentificării deschise.



Clienții wireless care încearcă să se conecteze la un WLAN vor vedea două AP-uri cu același SSID care oferă acces wireless. Cei din apropierea AP-ului necinstiți găsesc semnalul mai puternic și cel mai probabil se asociază cu acesta. Traficul utilizatorului este acum trimis către AP-ul necinstiți, care, la rândul său, captează datele și le transmite către AP-ul legitim, așa cum se arată în figură. Traficul returnat de la AP-ul legitim este trimis către AP-ul necinstiți, capturat și apoi redirecționat către utilizatorul care nu bănuiește. Atacatorul poate fura parolele utilizatorului, informațiile personale, poate obține acces la dispozitivul său și poate compromite sistemul.



Blocarea unui atac precum un atac MITM depinde de sofisticarea infrastructurii WLAN și de vigilența în monitorizarea activității în rețea. Procesul începe cu identificarea dispozitivelor legitime pe WLAN. Pentru a face acest lucru, utilizatorii trebuie să fie autentificați. După ce toate dispozitivele legitime sunt cunoscute, rețeaua poate fi monitorizată pentru dispozitive sau trafic anormal.

SECURIZAREA REȚELELOR WLAN

12.7.1 - SECURIZAREA REȚELELOR WLAN

Subiectul anterior a explicat amenințările WLAN.

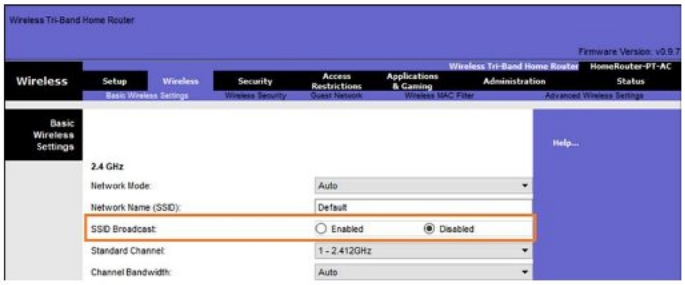
- Ce se va face pentru a securiza WLAN-ul este întrebarea ?

12.7.2 - ASCUNDEREAREA SSID ȘI FILTRAREA ADRESELOR MAC

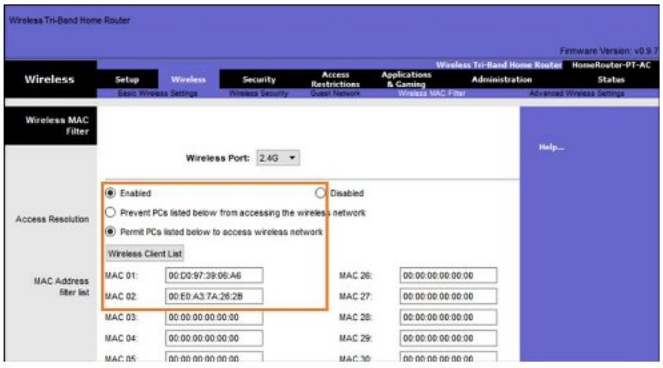
Semnalele wireless pot călători prin materie solidă, cum ar fi tavane, podele, pereți, în afara casei sau în spațiul de birou. Fără măsuri de securitate stricte, instalarea unui WLAN poate fi echivalentul cu porturile Ethernet peste tot, chiar și în exterior.

Pentru a aborda amenințările de a menține intrușii fără fir și de a proteja datele, au fost utilizate două funcții de securitate timpurii și sunt încă disponibile pe majoritatea routerelor și AP-urilor: descuamarea SSID și filtrarea adreselor MAC.

A. ***Ascunderea SSID*** - AP-urile și unele routere wireless permit dezactivarea cadrului de baliză SSID, așa cum se arată în figură. Clienții wireless trebuie să configureze manual SSID-ul pentru a se conecta la rețea.



B. ***Filtrarea adreselor MAC*** - Un administrator poate permite sau interzice manual clienților accesul wireless pe baza adresei lor fizice hardware MAC. În figură, routerul este configurat să permită două adrese MAC. Dispozitivele cu adrese MAC diferite nu se vor putea conecta la WLAN de 2,4 GHz.



12.7.3 - METODE DE AUTENTIFICARE ORIGINALE PENTRU 802.11

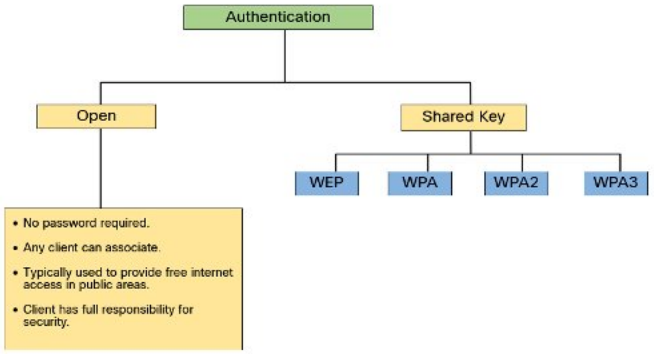
Deși aceste două caracteristici ar descuraja majoritatea utilizatorilor, realitatea este că nici descuamarea SSID și nici filtrarea adreselor MAC nu ar descuraja un intrus viclean. SSID-urile sunt

ușor de descoperit chiar dacă AP-urile nu le difuzează și adresele MAC pot fi falsificate. Cel mai bun mod de a securiza o rețea fără fir este utilizarea sistemelor de autentificare și criptare.

Au fost introduse două tipuri de autentificare cu standardul original 802.11:

1. ***Autentificare în sistem deschis*** - Orice client wireless ar trebui să se poată conecta cu ușurință și ar trebui să fie utilizat numai în situații în care securitatea nu prezintă niciun motiv de îngrijorare, cum ar fi cele care oferă acces gratuit la internet, cum ar fi cafenele, hoteluri și în zone îndepărtate. Clientul wireless este responsabil pentru asigurarea securității, cum ar fi utilizarea unei rețele private virtuale (VPN) pentru a se conecta în siguranță. VPN-urile oferă servicii de autentificare și criptare. VPN-urile depășesc domeniul de aplicare al acestui subiect.
2. ***Autentificare cu cheie partajată*** - Oferă mecanisme, cum ar fi WEP, WPA, WPA2 și WPA3 pentru a autentifica și cripta datele între un client wireless și AP. Cu toate acestea, parola trebuie să fie pre-partajată între ambele părți pentru a se conecta.

Următoarea diagramă rezumă aceste metode de autentificare.



12.7.4 - METODE DE AUTENTIFICARE A CHEII PARTAJATE

Există patru tehnici de autentificare a cheii partajate disponibile, așa cum este descris în tabel. Până când disponibilitatea dispozitivelor WPA3 devine omniprezentă, rețelele wireless ar trebui să utilizeze standardul WPA2.

Authentication Method	Description
Wired Equivalent Privacy (WEP)	Specificația originală 802.11 concepută pentru a securiza datele folosind metoda de criptare Rivest Cipher 4 (RC4) cu o cheie statică. Cu toate acestea, cheia nu se schimbă niciodată la schimbul de pachete. Acest lucru îl face ușor de piratat. WEP nu mai este recomandat și nu trebuie utilizat niciodată.
Wi-Fi Protected Access (WPA)	Un standard Wi-Fi Alliance care utilizează WEP, dar securizează datele cu algoritmul de criptare Temporal Key Integrity Protocol (TKIP) mult mai puternic. TKIP schimbă cheia pentru fiecare pachet, ceea ce face mult mai dificilă piratarea.

Authentication Method	Description
WPA2	WPA2 este standardul actual al industriei pentru securizarea rețelelor wireless. Utilizează Advanced Encryption Standard (AES) pentru criptare. În prezent, AES este considerat cel mai puternic protocol de criptare.
WPA3	Următoarea generație de securitate Wi-Fi. Toate dispozitivele compatibile cu WPA3 folosesc cele mai recente metode de securitate, nu permit protocoale vechi învechite şi necesită utilizarea cadrelor de management protejate (PMF). Cu toate acestea, dispozitivele cu WPA3 nu sunt încă disponibile.

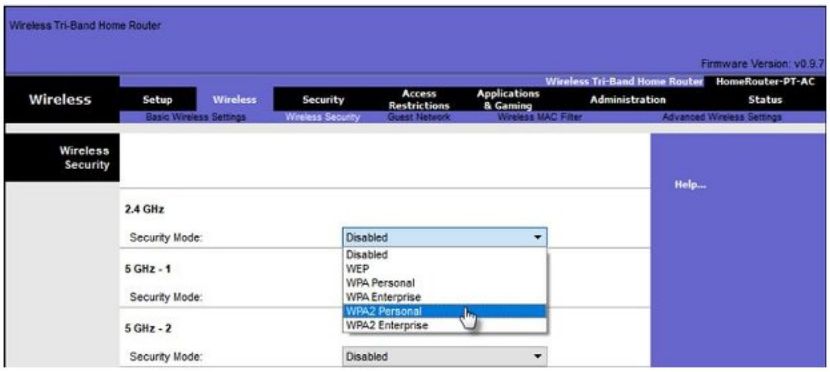
12.7.5 - AUTENTIFICAREA UNUI UTILIZATOR ACASĂ

Routerele de acasă au de obicei două opțiuni pentru autentificare: WPA şi WPA2. WPA2 este cel mai puternic dintre cele două. Figura arată opțiunea de a selecta una dintre cele două metode de autentificare WPA2:

i. ***Personal*** - Destinat pentru rețelele de acasă sau de birouri mici, utilizatorii se autentifică folosind o cheie pre-partajată (PSK). Clienții wireless se autentifică cu routerul wireless folosind o parolă pre-partajată. Nu este necesar un server special de autentificare.

ii. ***Enterprise*** - Destinat rețelelor de întreprindere, dar necesită un server de autentificare RADIUS (Remote Authentication Dial-In User Service). Deşi mai complicat de configurat, oferă securitate suplimentară. Dispozitivul trebuie să fie autentificat de serverul RADIUS şi apoi utilizatorii trebuie să se autentifice folosind standardul 802.1X, care utilizează protocolul de autentificare extensibil (EAP) pentru autentificare.

În figură, administratorul configurează routerul wireless cu autentificare personală WPA2 pe banda de 2,4 GHz.



12.7.6 - METODE DE CRIPTARE

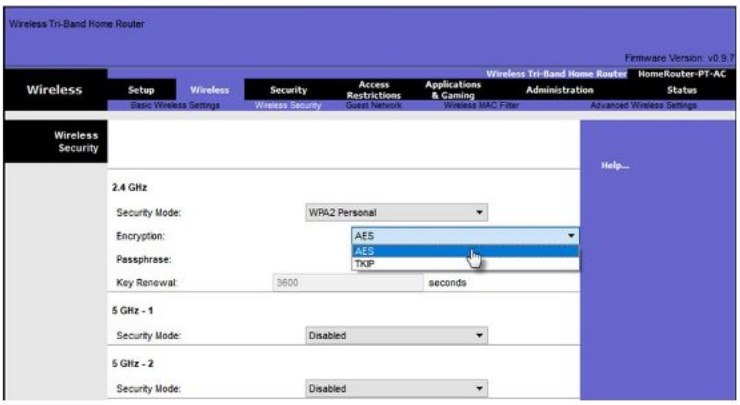
Criptarea este folosită pentru a proteja datele. Dacă un intrus a capturat date criptate, nu ar putea să le descifreze într-un interval de timp rezonabil.

Standardele WPA şi WPA2 utilizează următoarele protocoale de criptare:

1. ***Temporal Key Integrity Protocol (TKIP)*** - TKIP este metoda de criptare folosită de WPA. Oferă suport pentru echipamentele WLAN vechi, abordând defectele originale asociate cu metoda de criptare 802.11 WEP. Utilizează WEP, dar criptează încărcătura utilă de Layer 2 folosind TKIP și efectuează o verificare a integrității mesajului (MIC) în pachetul criptat pentru a se asigura că mesajul nu a fost modificat.

2. ***Advanced Encryption Standard (AES)*** - AES este metoda de criptare folosită de WPA2. Este metoda preferată, deoarece este o metodă mult mai puternică de criptare. Utilizează modul Counter Cipher cu Block Chaining Message Authentication Code Protocol (CCMP) care permite gazdelor de destinație să recunoască dacă biții criptați și necriptați au fost modificați.

În figură, administratorul configurează routerul wireless pentru a utiliza WPA2 cu criptare AES pe banda de 2,4 GHz.



12.7.7 - AUTENTIFICARE LA NIVEL DE ÎNTREPRINDERI

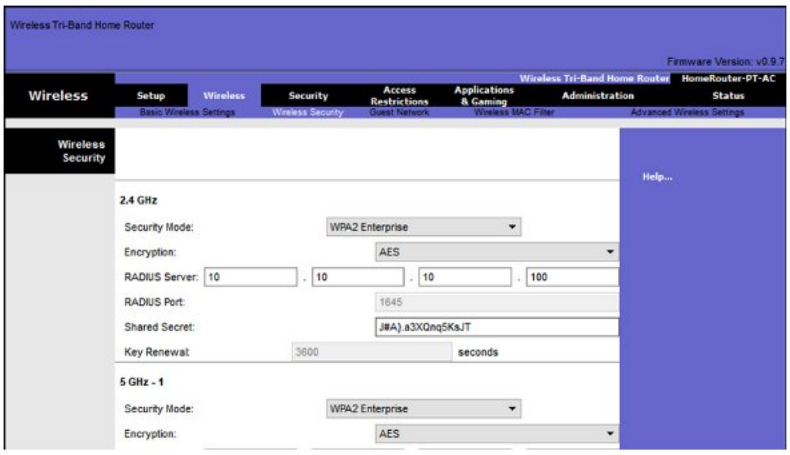
În rețelele care au cerințe de securitate mai stricte, este necesară o autentificare sau autentificare suplimentară pentru a acorda clienților fără fir un astfel de acces. Alegerea modului de securitate Enterprise necesită un server RADIUS de autentificare, autorizare și contabilitate (AAA).

a. ***Adresa IP a serverului RADIUS*** - Aceasta este adresa accesibilă a serverului RADIUS.

b. ***Numere de port UDP*** - Porturile UDP 1812 atribuite oficial pentru autentificare RADIUS și 1813 pentru contabilitate RADIUS, dar pot funcționa și folosind porturile UDP 1645 și 1646, așa cum se arată în figură.

c. ***Cheie partajată*** - Folosită pentru a autentifica AP-ul cu serverul RADIUS.

În figură, administratorul configurează routerul wireless cu autentificare WPA2 Enterprise folosind criptarea AES. Adresa IPv4 a serverului RADIUS este configurată, de asemenea, cu o parolă puternică pentru a fi utilizată între routerul wireless și serverul RADIUS.



Cheia partajată nu este un parametru care trebuie configurat pe un client wireless. Este necesar doar pe AP pentru a se autentifica cu serverul RADIUS. Autentificarea și autorizarea utilizatorilor sunt gestionate de standardul 802.1X, care oferă o autentificare centralizată, bazată pe server, a utilizatorilor finali.

Procesul de conectare 802.1X utilizează EAP pentru a comunica cu serverul AP și RADIUS. EAP este un cadru pentru autentificarea accesului la rețea. Poate oferi un mecanism de autentificare securizat și poate negocia o cheie privată securizată care poate fi apoi utilizată pentru o sesiune de criptare fără fir folosind criptarea TKIP sau AES.

12.7.8 - WPA3

La momentul elaborării materialului pentru curs, dispozitivele care acceptă autentificarea WPA3 nu erau disponibile. Cu toate acestea, WPA2 nu mai este considerat sigur. WPA3, dacă este disponibil, este metoda recomandată de autentificare 802.11. WPA3 include patru caracteristici:

WPA3-Personal

WPA3-Enterprise

Rețele deschise

Incorporarea Internetului lucrurilor (IoT).

1. ***WPA3-Personal*** - În WPA2-Personal, actorii amenințărilor pot asculta „strângerea de mână” dintre un client wireless și AP și pot folosi un atac de forță brută pentru a încerca să ghicească PSK. WPA3-Personal zădărnicește acest atac utilizând Simultaneous Authentication of Equals (SAE), o caracteristică specificată în IEEE 802.11-2016. PSK-ul nu este niciodată expus, ceea ce face imposibil ca actorul amenințării să ghicească.

2. ***WPA3-Enterprise*** - WPA3-Enterprise utilizează încă autentificarea 802.1X/EAP. Cu toate acestea, necesită utilizarea unei suite criptografice de 192 de biți și elimină amestecarea protocoalelor de securitate pentru standardele 802.11 anterioare. WPA3-Enterprise aderă la Suita Commercial

National Security Algorithm (CNSA) care este utilizată în mod obișnuit în rețelele Wi-Fi de înaltă securitate.

3. ***Rețele deschise*** - Rețelele deschise în WPA2 trimit traficul utilizatorului în text clar, neautentificat. În WPA3, rețelele Wi-Fi deschise sau publice încă nu folosesc nicio autentificare. Cu toate acestea, folosesc Opportunistic Wireless Encryption (OWE) pentru a cripta tot traficul wireless.

4. ***Onboarding IoT*** - Deși WPA2 a inclus Wi-Fi Protected Setup (WPS) pentru a integra rapid dispozitivele fără a le configura mai întâi, WPS este vulnerabil la o varietate de atacuri şi nu este recomandat. În plus, dispozitivele IoT sunt de obicei fără cap, ceea ce înseamnă că nu au GUI încorporat pentru configurare și au nevoie de orice modalitate ușoară de a se conecta la rețeaua wireless. Protocolul de furnizare a dispozitivelor (DPP) a fost conceput pentru a răspunde acestei nevoi. Fiecare dispozitiv fără cap are o cheie publică codificată. Cheia este de obicei ștampilată pe exteriorul dispozitivului sau a ambalajului acestuia ca un cod de răspuns rapid (QR). Administratorul de rețea poate scana codul QR și poate monta rapid la bordul dispozitivului. Deși nu face parte strict din standardul WPA3, DPP va înlocui WPS în timp.

CONFIGURARE WLAN

13.0.1 - MODUL

13.0.2 - SE VA ÎNVĂȚA ÎN ACEST MODUL

Titlul Modulului	Obiectivul Modulului
Remote Site WLAN Configuration	*Configurarea unui WLAN pentru a accepta un site la distanță.*
Configurarea unui WLAN de bază cu WLC	Configurarea unui WLAN WLC pentru a utiliza interfața de gestionare și autentificarea WPA2 PSK.
Configurarea unui WLAN WPA2 Enterprise cu WLC	Configurarea unui WLAN WLC pentru a utiliza o interfață VLAN, un server DHCP și autentificare WPA2 Enterprise.
Depanarea problemelor WLAN	Depanarea problemelor comune de configurare wireless.

REMOTE SITE WLAN CONFIGURATION

13.1.1 - CONFIGURAREA WIRELESS NETWORK

13.1.2 - ROUTERELE FĂRĂ FIR

Lucrătorii de la distanță, sucursalele mici și rețelele de acasă folosesc adesea un birou mic și un router de acasă. Aceste routere sunt uneori numite router integrat deoarece includ de obicei un comutator pentru clienții cu fir, un port pentru o conexiune la internet (uneori etichetat „WAN”) și componente wireless pentru accesul clienților fără fir, așa cum se arată pentru Cisco Meraki MX64W în figură. . Pentru restul acestui modul, routerele mici de birou și de acasă sunt denumite routere fără fir.

Figura arată partea din spate a unui mic router de birou sau de acasă. Routerul are două antene, câte una pe fiecare parte. În stânga, există un buton de resetare. Lângă butonul de resetare există patru porturi pentru conectarea dispozitivelor LAN. Apoi există un port pentru conexiunea WAN și, în sfârșit, butonul de pornire și portul pentru cablul de alimentare.

Cisco Meraki MX64W

Pentru exemplificare va fi creată o topologie care să ilustreze conexiunea fizică a unui laptop cu fir la routerul wireless, care este apoi conectat la un modem prin cablu sau DSL pentru conectivitate la internet.

Figura trebuie să ilustreze conexiunea fizică a unui laptop cu fir la routerul wireless, care este apoi conectat la un modem prin cablu sau DSL pentru conexiune la internet. Conectat la partea din spate a computerului desktop este o legătură care merge la un router fără fir, iar de la routerul fără fir există o legătură către modemul de bandă largă. Modemul de bandă largă are o conexiune serială la Internet, ilustrată de un nor.

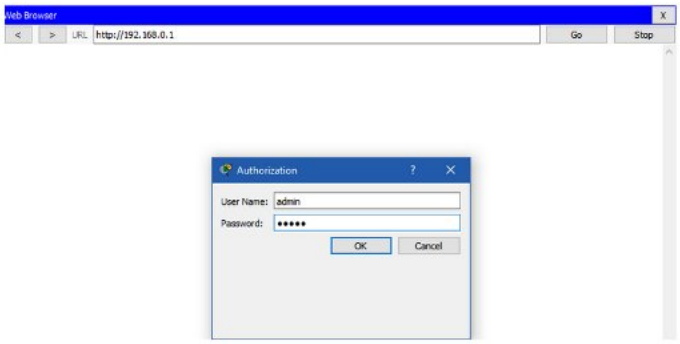
Router wireless Broadband Modem Internet - Aceste routere wireless oferă de obicei securitate WLAN, servicii DHCP, traducere integrată a adresei de nume (NAT), calitate a serviciului (QoS), precum și o varietate de alte caracteristici. Setul de caracteristici va varia în funcție de modelul de router.

Notă: Configurarea modemului prin cablu sau DSL se face de obicei de către reprezentantul furnizorului de servicii, fie la fața locului, fie de la distanță, printr-o prezentare pe telefon.

13.1.3 - CONECTAREA LA ROUTERUL WIRELESS

Cele mai multe routere wireless sunt gata de service imediat. Sunt preconfigurate pentru a fi conectate la rețea și pentru a oferi servicii. De exemplu, routerul wireless folosește DHCP pentru a furniza automat informații de adresare dispozitivelor conectate. Cu toate acestea, adresele IP implicite ale routerului fără fir, numele de utilizator și parolele pot fi găsite cu ușurință pe internet. Doar va fi introdusă expresia de căutare „adresă IP implicită a routerului wireless” sau „parole implicite a routerului fără fir” pentru a vedea o listă a multor site-uri web care oferă aceste informații. De exemplu, numele de utilizator și parola pentru routerul wireless din figură sunt „admin”. Prin urmare, prima prioritate ar trebui să fie modificarea acestor valori implicite din motive de securitate.

Pentru a obține acces la GUI de configurare a routerului fără fir, va fi deschis un browser web. În câmpul de adresă, va fi introdusă adresa IP implicită pentru routerul wireless. Adresa IP implicită poate fi găsită în documentația livrată cu routerul wireless sau se poate căuta pe internet. Figura arată adresa IPv4 192.168.0.1, care este o valoare implicită comună pentru mulți producători. O fereastră de securitate solicită autorizarea pentru a accesa GUI al routerului. Cuvântul admin este folosit în mod obișnuit ca nume de utilizator și parolă implicite. Din nou, se poate verifica documentația routerului wireless sau se poate căuta pe internet.

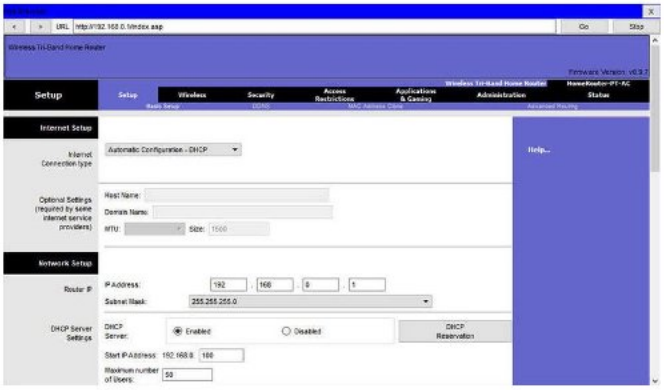


13.1.4 - CONFIGURAREA DE BAZĂ A REȚELEI

Configurarea de bază a rețelei include următorii pași:

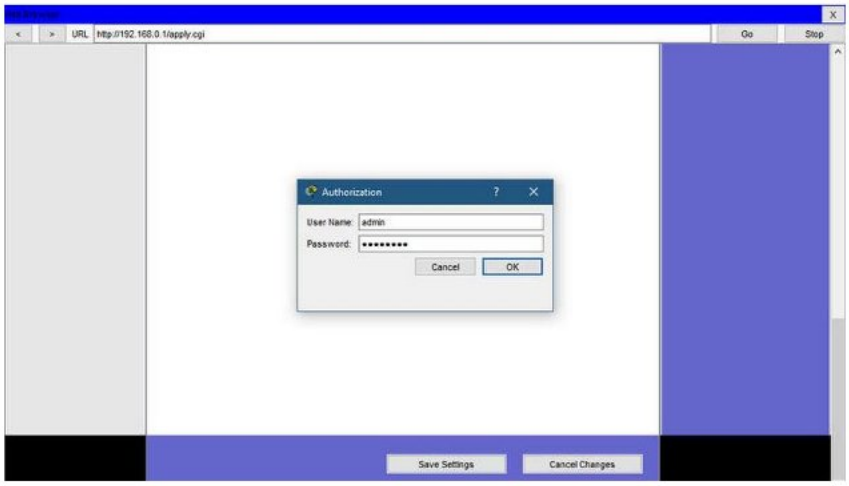
1. ***Conectarea la router dintr-un browser web.***
2. ***Schimbarea parolei administrative implicite.***
3. ***Conectare cu noua parolă administrativă.***
4. ***Modificarea adreselor implicite DHCP IPv4.***
5. ***Reînnoirea adresei IP.***
6. ***Conectarea la router cu noua adresă IP***.

1. ***Conectarea la router dintr-un browser web -*** *După conectare, se deschide o interfață grafică. GUI va avea file sau meniuri pentru a ajuta la navigarea la diferite sarcini de configurare a routerului. De multe ori este necesar să fie salvate setările modificate într-o fereastră înainte de a trece la o altă fereastră. La acest pas, cea mai bună practică este să se facă modificări la setările implicite.*

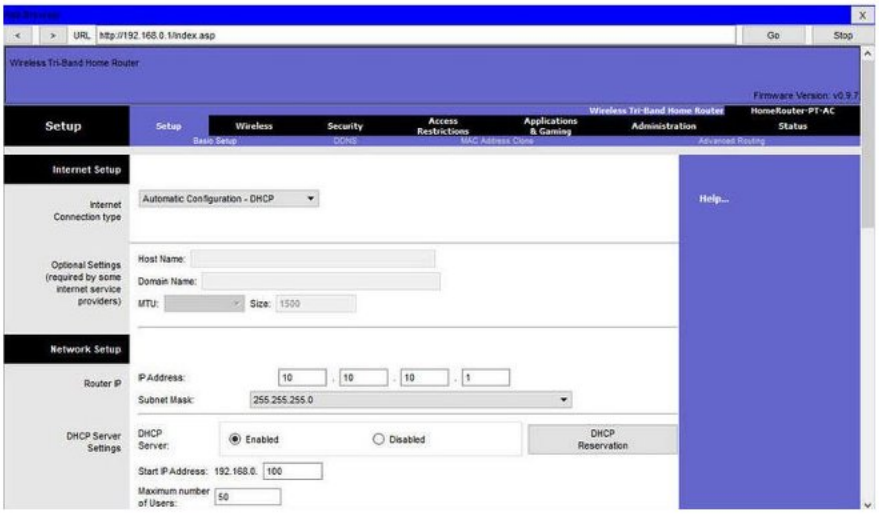


2. ***Schimbarea parolei administrative implicite -*** *Pentru a schimba parola de conectare implicită, va fi găsită porțiunea de administrare a GUI a routerului. În acest exemplu, a fost selectată fila Administrare. Aici poate fi schimbată parola routerului. Pe unele dispozitive, cum ar fi cel din exemplu, se poate schimba doar parola. Numele de utilizator rămâne admin sau oricare ar fi numele de utilizator implicit pentru configurarea routerului.*

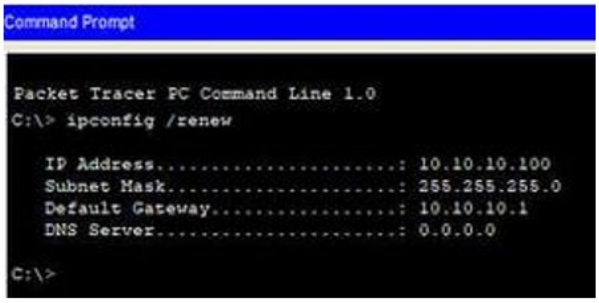
3. ***Conectare cu noua parolă administrative*** *– După ce va fi salvată noua parolă, routerul wireless va solicita din nou autorizarea. Se va introduce numele de utilizator și noua parolă, așa cum se arată în exemplu.*



4. ***Modificarea adreselor implicite DHCP IPv4*** *– Se va schimba adresa IPv4 implicită a routerului. Cea mai bună practică este utilizarea adresei IPv4 private în interiorul rețelei. Adresa IPv4 10.10.10.1 este folosită în exemplu, dar poate fi ales orice adresă IPv4 privată.*



5. ***Reînnoirea adresei IP -*** *Când se va face clic pe salvare, se va pierde temporar accesul la routerul wireless. Se va deschide o fereastră de comandă și se va reînnoi adresa IP cu comanda ipconfig /renew, așa cum se arată în exemplu.*



6. ***Conectarea la router cu noua adresă IP*** *- Se va introduce noua adresă IP a routerului pentru a recâștiga accesul la GUI de configurare a routerului, așa cum se arată în exemplu. Acum va fi gata să se continue configurarea routerului pentru acces wireless.*

13.1.5 - CONFIGURAREA DE BAZĂ A REȚELELOR FĂRĂ FIR

Configurarea de bază fără fir include următorii pași:

A. Vizualizarea setărilor implicite WLAN.

B. Schimbarea modului de rețea.

C. Configurarea SSID-ului.

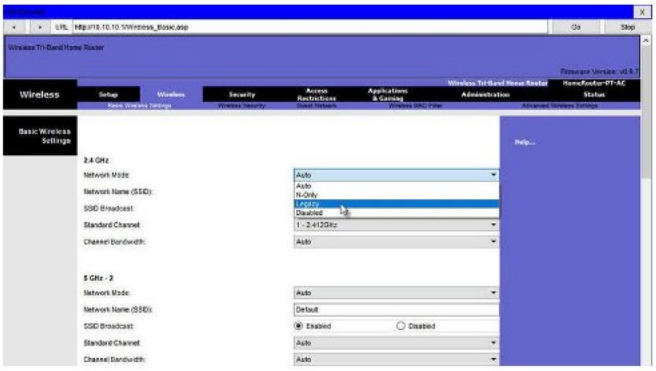
D. Configurarea canalului.

E. Configurarea modului de securitate.

F. Configurarea expresiei de acces.

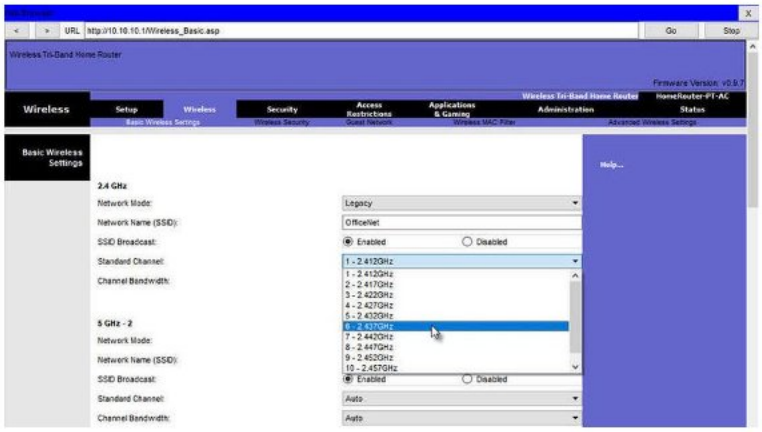
A. Vizualizarea setărilor implicite WLAN - *Ieșit din cutie înseamnă de la furnizor, un router wireless oferă acces fără fir la dispozitive folosind un nume și o parolă de rețea fără fir implicite. Numele rețelei se numește Service Set Identified (SSID). Se vor găsi setările de bază wireless pentru router pentru a modifica aceste valori implicite, așa cum se arată în exemplu.*

B. *Schimbarea modului de rețea -* *Unele routere wireless permit selectarea standardului 802.11 de implementat. Exemplul arată că „Legacy" a fost selectat. Aceasta înseamnă că dispozitivele wireless care se conectează la routerul wireless pot avea instalate o varietate de NIC-uri wireless. Routerele wireless de astăzi configurate pentru modul vechi sau mixt acceptă cel mai probabil 802.11a, 802.11n și 802.11ac NIC.*

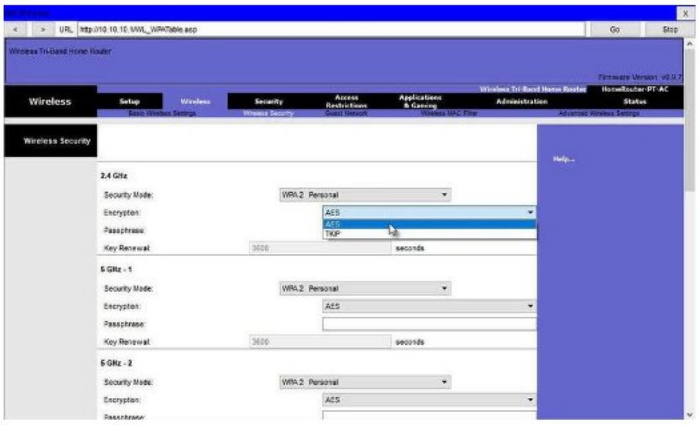


C. *Configurarea SSID-ului* *– La acest pas va fi atribuit un SSID rețelelor WLAN. OfficeNet este utilizat în exemplu pentru toate cele trei rețele WLAN (al treilea WLAN nu este afișat). Routerul wireless își anunță prezența trimițând emisiuni care își anunță SSID-ul. Acest lucru permite gazdelor wireless să descopere automat numele rețelei wireless. Dacă transmisia SSID este dezactivată, va trebui introdus manual SSID-ul pe fiecare dispozitiv wireless care se conectează la WLAN.*

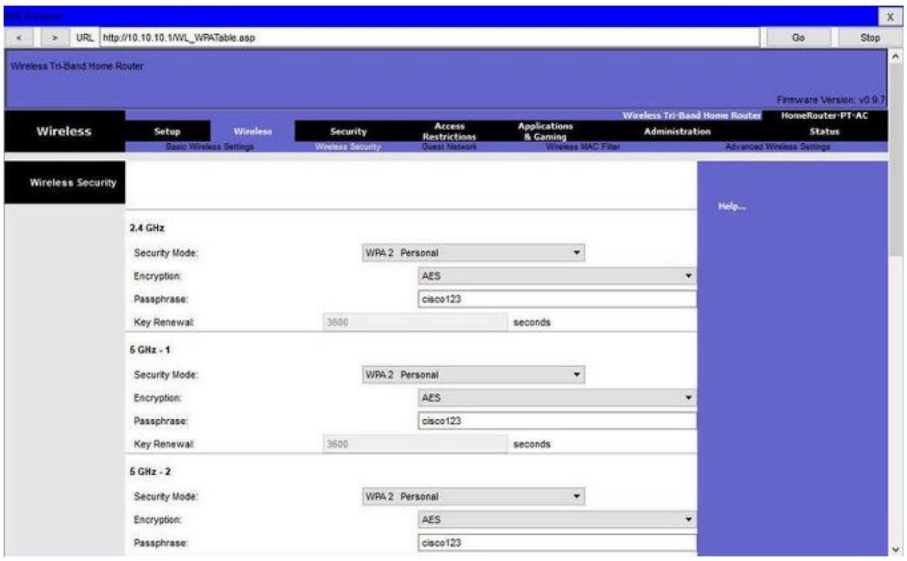
D. *Configurarea canalului -* *Dispozitivele configurate cu același canal în banda de 2,4 GHz se pot suprapune și provoca distorsiuni, încetinind performanța wireless și pot întrerupe conexiunile la rețea. Soluția pentru evitarea interferențelor este configurarea canalelor care nu se suprapun pe routerele wireless și punctele de acces care sunt aproape unul de celălalt. În mod specific, canalele 1, 6 și 11 nu se suprapun. În exemplu, routerul wireless este configurat să utilizeze canalul 6*



E. *Configurarea modului de Securitate –* *Venit direct de la producator, un router wireless poate să nu aibă securitate WLAN configurată. În exemplu, versiunea personală a Wi-Fi Protected Access versiunea 2 (WPA2 Personal) este selectată pentru toate cele trei rețele WLAN. WPA2 cu criptare Advanced Encryption Standard (AES) este în prezent cel mai puternic mod de securitate.*

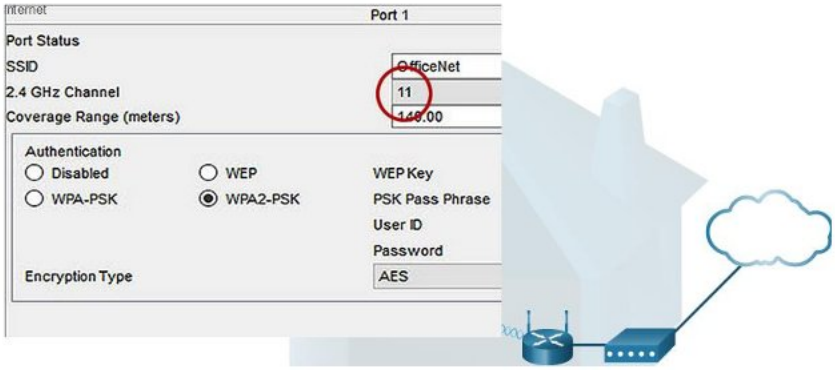


F. *Configurarea expresiei de acces* *- WPA2 personal folosește o expresie de acces pentru a autentifica clienții wireless. WPA2 personal este mai ușor de utilizat într-un mediu mic de birou sau acasă, deoarece nu necesită un server de autentificare. Organizațiile mai mari implementează WPA2 enterprise și solicită clienților wireless să se autentifice cu un nume de utilizator și o parolă.*



13.1.6 - CONFIGURAREA UNEI REȚELE MESH FĂRĂ FIR

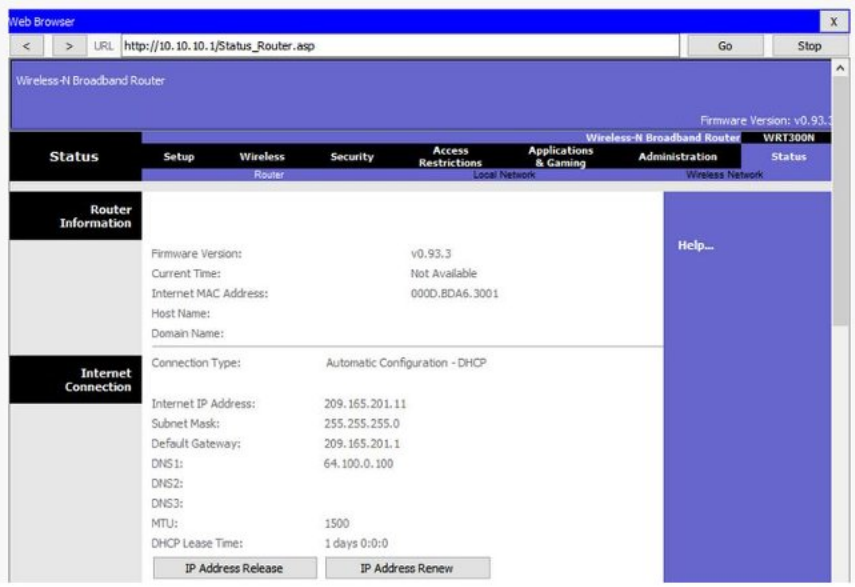
Într-o rețea mică de birou sau de acasă, un router wireless poate fi suficient pentru a oferi acces fără fir tuturor clienților. Cu toate acestea, dacă se dorește, se poate extinde raza de acțiune dincolo de aproximativ 45 de metri în interior și 90 de metri în exterior, se pot adăuga și puncte de acces wireless. După cum se arată în rețeaua rețea fără fir din figură, două puncte de acces sunt configurate cu aceleași setări WLAN din exemplul nostru anterior. Se poate observa că aici canalele selectate sunt 1 și 11, astfel încât punctele de acces să nu interfereze cu canalul 6 configurat anterior pe routerul wireless.



Extinderea unui WLAN într-un mic birou sau acasă a devenit din ce în ce mai ușoară. Producătorii au simplificat crearea unei rețele de plasă fără fir (WMN) prin intermediul aplicațiilor pentru smartphone. Se poate cumpăra sistemul, se dispersează punctele de acces, se conectează, se descarcă aplicația și se configurează WMN-ul în câțiva pași. Se poate căuta pe internet „cel mai bun sistem de rețea wi-fi mesh” pentru a găsi recenzii despre ofertele curente.

13.1.7 - NAT PENTRU IPV4

Pe un router wireless, dacă va fi căutată o pagină precum pagina `Status` prezentată în figură, vor fi găsite informațiile de adresare IPv4 pe care routerul le folosește pentru a trimite date pe internet. Se poate observa că adresa IPv4 este 209.165.201.11 este o rețea diferită de adresa 10.10.10.1 atribuită interfeței LAN a routerului. Toate dispozitivele de pe LAN-ul routerului vor primi adrese atribuite cu prefixul 10.10.10.



Adresa IPv4 209.165.201.11 este rutabilă public pe internet. Orice adresă cu 10 în primul octet este o adresă IPv4 privată și nu poate fi direcționată pe internet. Prin urmare, routerul va folosi un proces numit Network Address Translation (NAT) pentru a converti adrese IPv4 private în adrese IPv4 rutabile prin internet. Cu NAT, o adresă IPv4 sursă privată (locală) este tradusă într-o adresă publică (globală). Procesul este invers pentru pachetele primite. Routerul este capabil să traducă multe adrese IPv4 interne în adrese publice, utilizând NAT.

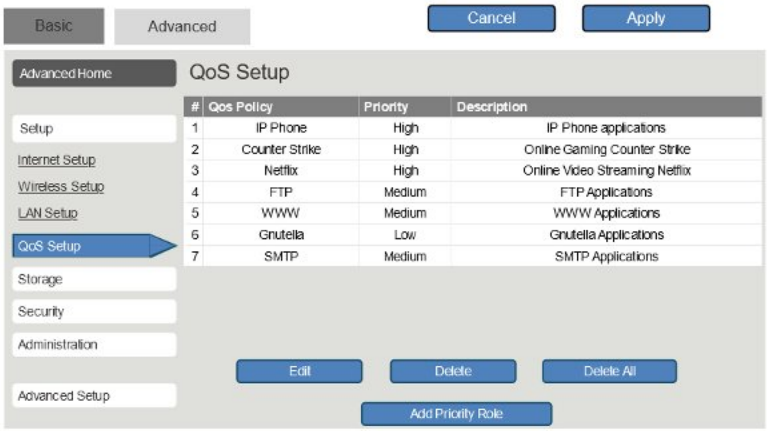
Unii ISP-uri folosesc adresarea privată pentru a se conecta la dispozitivele clienților. Cu toate acestea, în cele din urmă, traficul generat va părăsi rețeaua furnizorului și va fi direcționat pe internet. Pentru a vedea adresele IP pentru orice dispozitiv, prin căutarea pe internet „care este adresa mea IP". Se va putea face acest lucru pentru alte dispozitive din aceeași rețea și va vedea că toate partajează aceeași adresă IPv4 publică. NAT face acest lucru posibil prin urmărirea numerelor portului sursă pentru fiecare sesiune stabilită de un dispozitiv. Dacă ISP-ul are IPv6 activat, atunci va vedea o adresă IPv6 unică pentru fiecare dispozitiv.

13.1.8 - QUALITY OF SERVICE

Multe routere wireless au o opțiune pentru configurarea Calității Serviciului (QoS). Prin configurarea QoS, se poate garanta că anumite tipuri de trafic, cum ar fi vocea și video, au prioritate

față de traficul care nu este la fel de sensibil la timp, cum ar fi e-mailul și navigarea pe web. Pe unele routere wireless, traficul poate fi prioritizat și pe anumite porturi.

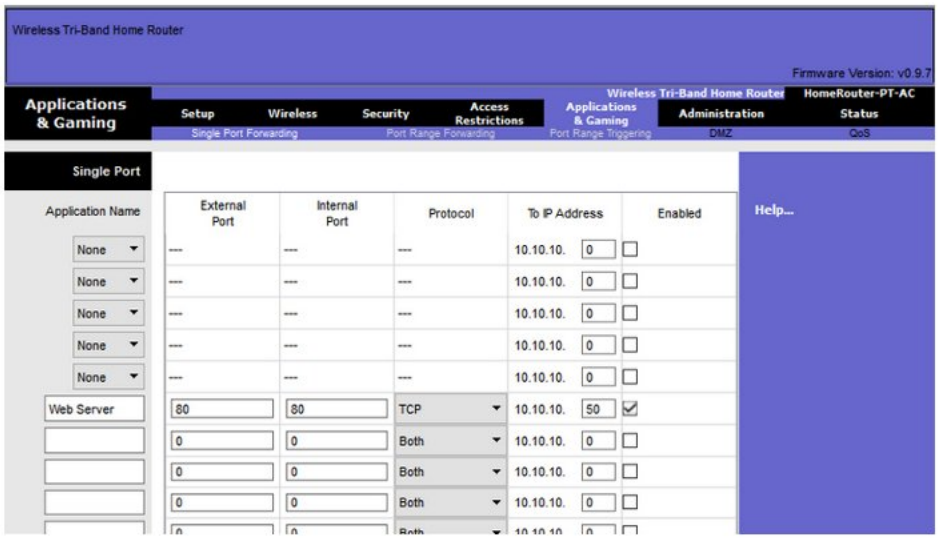
Figura este o machetă simplificată a unei interfețe QoS bazată pe o GUI Netgear. De obicei, se vor găsi setările QoS în meniurile avansate. Dacă va fi disponibil un router wireless, este important să fie investigate setările QoS. Uneori, acestea pot fi listate sub „controlul lățimii de bandă" sau ceva similar. Cel mai ușor este să fie consultată documentația routerului wireless sau să fie căutată pe internet „setări qos" pentru marca și modelul routerului.



13.1.9 - Port Forwarding

Routerele wireless blochează de obicei porturile TCP și UDP pentru a preveni accesul neautorizat în și în afara unei rețele LAN. Cu toate acestea, există situații în care anumite porturi trebuie deschise pentru ca anumite programe și aplicații să poată comunica cu dispozitive din rețele diferite. Redirecționarea portului este o metodă bazată pe reguli de direcționare a traficului între dispozitive din rețele separate.

Când traficul ajunge la router, acesta determină dacă traficul ar trebui să fie redirecționat către un anumit dispozitiv pe baza numărului portului găsit cu traficul. De exemplu, un router poate fi configurat să redirecționeze portul 80, care este asociat cu HTTP. Când routerul primește un pachet cu portul de destinație 80, routerul redirecționează traficul către serverul din interiorul rețelei care deservește paginile web. În figură, redirecționarea portului este activată pentru portul 80 și este asociată cu serverul web la adresa IPv4 10.10.10.50.



Declanșarea portului permite routerului să transmită temporar date prin porturile de intrare către un anumit dispozitiv. Puteți utiliza declanșarea portului pentru a redirecționa date către un computer numai atunci când un interval de porturi desemnat este utilizat pentru a face o solicitare de ieșire. De exemplu, un joc video poate folosi porturile de la 27000 la 27100 pentru conectarea cu alți jucători. Acestea sunt porturile de declanșare. Un client de chat poate folosi portul 56 pentru a conecta aceiași jucători, astfel încât aceștia să poată interacționa între ei. În acest caz, dacă există trafic de jocuri pe un port de ieșire în intervalul de porturi declanșat, traficul de chat de intrare pe portul 56 este redirecționat către computerul care este utilizat pentru a juca jocul video și a discuta cu prietenii. Când jocul se termină și porturile declanșate nu mai sunt utilizate, portul 56 nu mai are voie să trimită trafic de orice tip către acest computer.