Universitatea Politehnica Bucuresti

Facultatea de Electronica, Telecomunicatii si Tehnologia Informatiei

Securitatea rețelelor WLAN

Studenți : Taifas Ștefania
Lupe Bogdan
Haidu Marius
Grupa : 443 A

Ianuarie 2014

Cuprins

1. Infrastructura WLAN - Taifas Stefania - 443A
1.1 Generalități
1.2 Notiuni si configuratii posibile
1.3.Componentele retelei
1.3.1 Setul serviciului de baza (BSS - Basic Service Set)
1.3.2 Sistemul de distribuire (DS)
1.4 Semnalele si performantele retelelor WLAN
1.4.1 Semnale Wireless
1.4.2 Potenţialul unei reţele WLAN şi utilitatea acesteia
1.4.3 Standarde WLAN
1.4.4 Raza de acţiune a unei reţele wireless
1.4.5 Propagarea undelor radio
1.5 Avantaje/Dezavantaje ale retelelor WLAN
1.6 Standardul IEEE 802.11
1.6.1 Introducere
1.6.2 Rata de transfer
1.6.3. Aria de acoperire
1.7 Bluetooth
1.7.1 Istoric
1.7.2 Caracteristici generale
1.7.3. Principiile Bluetooth

2. Mecanisme de securitate: IEEE 802.11 – Lupe Bogdan – 443A
2.1 WIRED EQUIVALENT PRIVACY (WEP)
2.1.1 Slăbiciuni ale WEP
2.1.2 IEEE 802.1x
2.1.3 Extensible Authentication Protocol (EAP)
2.2 WI-FI PROTECTED ACCESS (WPA)
2.2.1. Temporal Key Integrity Protocol (TKIP)
2.2.2 Michael Message Integrity Check (MIC)
2.3 IEEE 802.11I
2.3.1 Counter Mode with CBC-MAC Protocol (CCMP)
2.3.2 WRAP
2.3.3 WPA2
2.4 Comparații și recomandări

3. ENTERPRISE ARCHITECTURE DESIGN – Haidu Marius – 443A
3.1 VIRTUAL PRIVATE NETWORKS
3.2 APPLICATION ENCRYPTION
3.3 Concluzii

4. Bibliografie

Retele WLAN

1.Infrastructura

1.1 Generalitati

Wi-Fi este o marca inregistrata de Wi-Fi Alliance pentru a descrie tehnologia WLAN(wireless local area networks) bazata pe standardul IEEE 802.11.
O retea wireless **(Wi-Fi) WLAN** este o retea fara fir, locala, extinsa pe arii limitate, in functie de echipamentele folosite si de puterea acestora, prin care se poate face transfer de date si internet folosind undele radio.

Trebuie stiut ca Wi-Fi, prescurtarea de la "Wireless Fidelity", reprezinta o categorie de produse compatibile cu standardele WLAN (Wireless Local Area Networks) bazate pe protocoale IEEE 802.11. Noile standarde care au precedat specificatiile 802.11, cum ar fi 802.16 (WiMAX), fac parte din retelele actuale si ofera multe imbunatatiri, de la arii mari de acoperire pana la viteze mari de transfer.

Diferentele intre o retea terestra si o retea wireless radio sunt multiple si reprezinta beneficii in favoarea retelelor wireless:

- Spre deosebire de alte sisteme radio, Wi-Fi foloseste un spectru de frecvente radio care nu au nevoie de licenta deci nu necesita aprobare pentru utilizare.
- Se permite dezvoltarea variata a unei retele locale WLAN fara utilizarea cablurilor, reducand costurile necesare dezvoltarii retelei si evitand diferite obstacole in implementarea retelei (locuri inaccesibile, care nu pot fi cablate).).
- Multe retele Wi-Fi suporta roaming, permitand unui client sa se mute dintr-un punct de acces in altul in aceeasi cladire, sau zona geografica.
- Wi-Fi este un standard global, clientii Wi-Fi putand lucra in diferite tari de pe glob.
- Posibilitati variate de conectare a utilizatorului final, prin intermediul placilor Wi-Fi PCMCIA, PCI, USB sau a variatelor sisteme Wi-Fi 802.11b sau 802.11g integrate in majoritatea notebook-urilor moderne.

A fost proiectata pentru a fi folosita pentru diferite dispozitive mobile cum ar fi laptopuri, dar si pentru multe alte servicii incluzand servicii de Internet si voce sau servicii pentru conectarea televizoarelor, camerelor digitale sau DVD playerelor.

Reteaua wireless are drept componenta principala un echipament care se numeste Punct de Acces. El este un releu care emite si recepteaza unde radio catre, respectiv de la dispozitivele din raza sa de actiune.

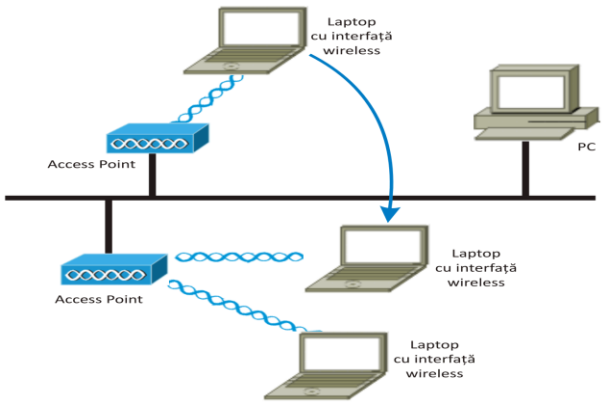
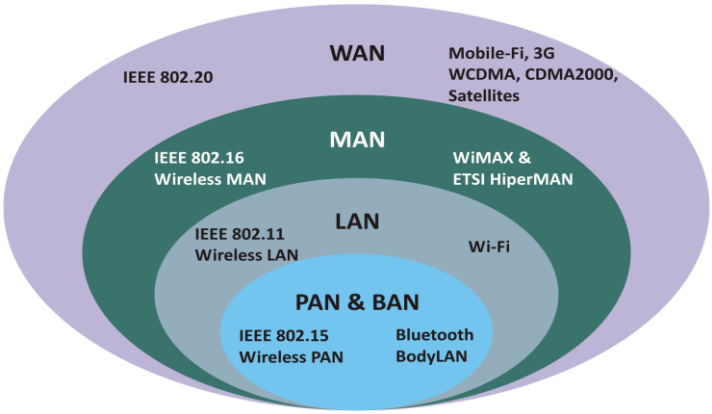


Fig.1 Retea wireless

Figura urmatoare prezinta regasirea standardul WiFi intr-o asezare globala a standardelor wireless :



1.2 Notiuni si configuratii posibile

In WLAN unitatea adresabila este o statie (STA), destinatie a mesajului si care, in general, nu este o locatie fixa. Nivelul fizic este diferit fata de cel al retelelor cu fire:

- utilizeaza un mediu de transmisiune care nu are margini absolute, dincolo de care tranceiverele n-ar fi capabile sa receptioneze;
- nu este protejat impotriva unor semnale externe;
- comunicatia se desfasoara pe un mediu mult mai putin fiabil decât cel cu fire;
- are topologii dinamice;
- lipsa unei conectivitati totale (nu orice statie poate "auzi" oricare alta statie);
- are proprietati de propagare variabile in timp si asimetrice.

Standardul IEEE 802.11 permite interoperabilitatea sistemelor WLAN, acestea putand fi interconectate cu retele de tipul IEEE 802.3 (Ethernet) sau IEEE 802.5 (token-ring).

Elementul de baza este celula acoperita de un echipament similar statiei de baza din comunicatiile mobile numita, aici, Punct de Acces (AP – Acces Point).

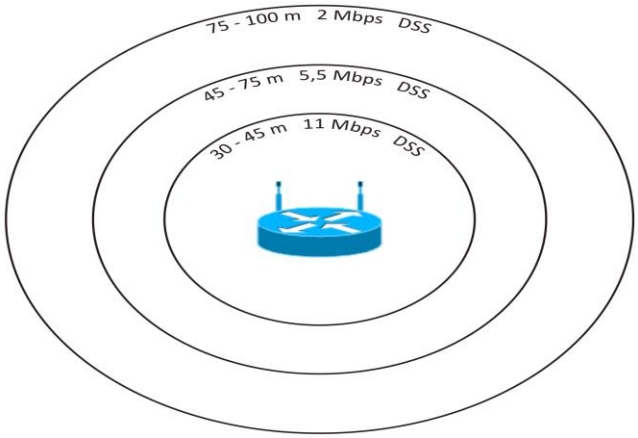


Fig. 3: Acoperirea cu semnal de la un Access Point

DSS = Digital Spread Spectrum

Raza de actiune a fiecarui punct de acces radio determina o celula sau in termenii IEEE 802.11 un BSS (Basic Service Set).

Mai multe celule sunt conectate intre ele, printr-o retea de distributie, realizata de obicei prin cablu, formând un ESS (Extended Service Set) sau un domeniu.

In acest domeniu un calculator mobil (un client) se poate deplasa de la o celula la alta fara a pierde conexiunea cu reteaua. Aceasta este semnificatia termenului de roaming.

In acest scop statia mobila:

- va monitoriza permanent calitatea legaturii cu celula folosita.
- va incepe cautarea de noi celule atunci când calitatea comunicatiei scade sub un prag prestabilit
- va folosi un ID diferit in fiecare celula, acesta fiind impus de catre sistem.

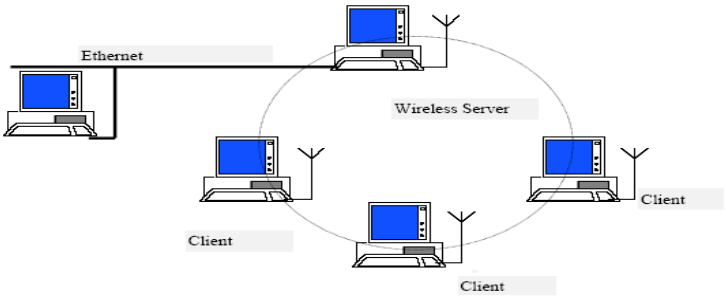


Fig.4 Statii client si server wireless

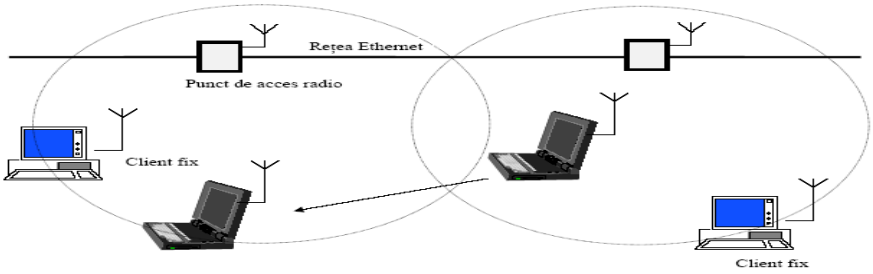


Fig.5 Retea cu mai multe celule

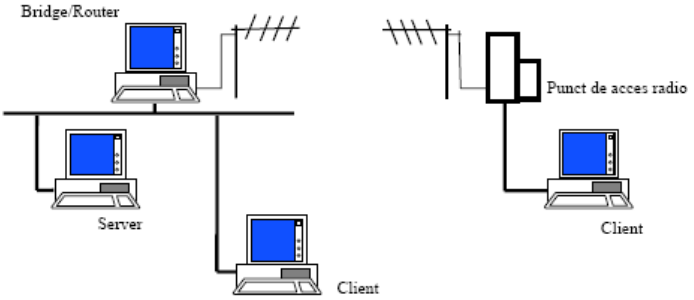


Fig.6 Retea locala folosind un ruter wireless

1.3 Componentele retelei

1.3.1 Setul serviciului de baza (BSS - Basic Service Set)

Din cauza limitarilor privind nivelul fizic (acoperire radio), retelele wireless care trebuie sa acopere distante geografice rezonabile pot fi compuse din blocuri de baza. Blocul de baza este numit setul serviciului de baza (BSS). In figura de mai jos sunt prezentate doua BSS, compuse fiecare din doua statii, forma ovala indicând, simbolic, aria acoperita, in care statiile membre ale BSS pot ramâne in comunicatie. Daca o statie iese din aceasta arie, ea nu mai poate comunica cu celelalte statii membre ale aceluiasi BSS.

Fig.7 Seturile serviciului de baza

Conform standardului 802.11 se disting doua tipuri de retele locale:

- retele ad-hoc;
- retele infrastructurale

Un BSS independent (IBSS - Independent BSS) reprezinta cel mai semnificativ tip de baza al retelei IEEE 802.11. O retea IEEE 802.11 minima poate fi formata din numai doua statii. In figura de mai sus sunt prezentate doua IBSS. Deoarece acest tip de retea IEEE 802.11 se formeaza

adesea fara o planificare, numai pentru un interval de timp cât este necesara, mai este numita retea ad hoc.

Asocierea dintre o STA si un BSS este dinamica: statia poate fi alimentata, nealimentata, poate iesi din aria de acoperire BSS sau poate intra in aceasta arie. Pentru ca o statie sa devina membru al unei infrastructuri BSS, ea trebuie sa devina "asociata". Aceasta asociere este dinamica si implica utilizarea serviciului sistemului de distribuire (DSS - Distribution System Service).

1.3.2 Sistemul de distribuire (DS)

Pentru unele retele comunicatia directa statie - statie nu este posibila din cauza distantei. In aceste cazuri un BSS, in loc sa fie independent, poate fi o componenta a unei retele extinse, formata din mai multe BSS, elementul utilizat pentru a le interconecta fiind numit sistem de distribuire (figura 8).

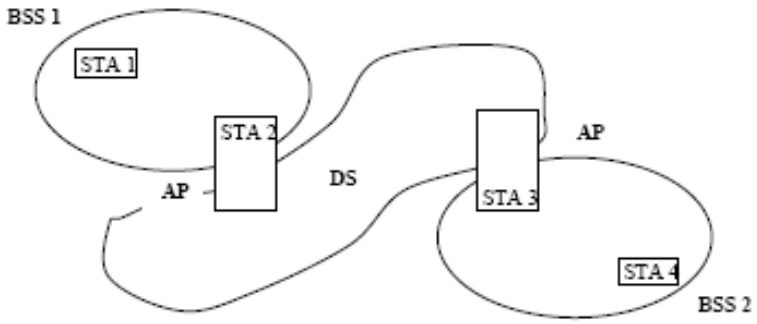


Fig.8 Sisteme de distributie si puncte de acces

Sistemul de distribuire furnizeaza serviciile logice necesare integrarii mai multor BSS. Un punct de acces (AP - Acces point) este o statie care asigura accesul la DS, furnizând serviciile DS si functionând si ca o statie. Datele sunt transferate intre un BSS si un DS prin intermediul unui AP. Toate punctele de acces (AP) sunt, de asemenea, statii (STA), deci ele sunt entitati adresabile. Un DS si mai multe BSS formeaza o retea wireless, de marime si complexitate arbitrare. O astfel de retea este numita setul serviciului extins (ESS - Extended Service Set). Un concept important este ca o retea ESS este vazuta de subnivelul LLC la fel cum este vazuta o retea IBSS. Statiile din cadrul unei retele ESS pot comunica si statiile mobile se pot deplasa de la un BSS la altul (in aceeasi retea ESS) in mod transparent fata de LLC. In standardul IEEE 802.11 nu se mentioneaza nimic in legatura cu locatiile fizice relative ale BSS - urilor (ele se pot suprapune partial, pot fi disjuncte, distantele intre BSS - uri nu sunt limitate).

c) Integrarea cu celelalte retele locale (cablate)

Pentru conectarea cu alte tipuri de retele locale (cu fire) este utilizat un portal, componenta logica arhitecturala reprezentând punctul logic prin care unitatile de date ale serviciului MAC dintr-o retea locala cu fire sunt transferate in arhitectura IEEE 802.11 (in sistemul de distribuire) si invers (figura 9). Este posibil ca un echipament sa functioneze simultan ca un AP si ca un portal; acesta poate fi cazul când un DS este implementat din componentele LAN IEEE 802. Portalul interconecteaza mediul de transmisiune al sistemului de distribuire si cel al LAN cu fir.

1.4 Semnalele si performantele retelelor WLAN

1.4.1 Semnale Wireless

Semnalele wireless sunt transportate prin aer de undele electromagnetice. Spectrul de frecvenţe radio este un continuum al undelor electromagnetice folosite pentru date şi comunicaţii de voce. Reţelele care transmit semnale prin atmosfera prin frecvenţă radio (RF) sunt cunoscute sub numele de reţele wireless sau reţele WLAN (wireless LAN).

Spectrul de semnale al retelelor Wireless este reprezentat in urmatoarea figura:

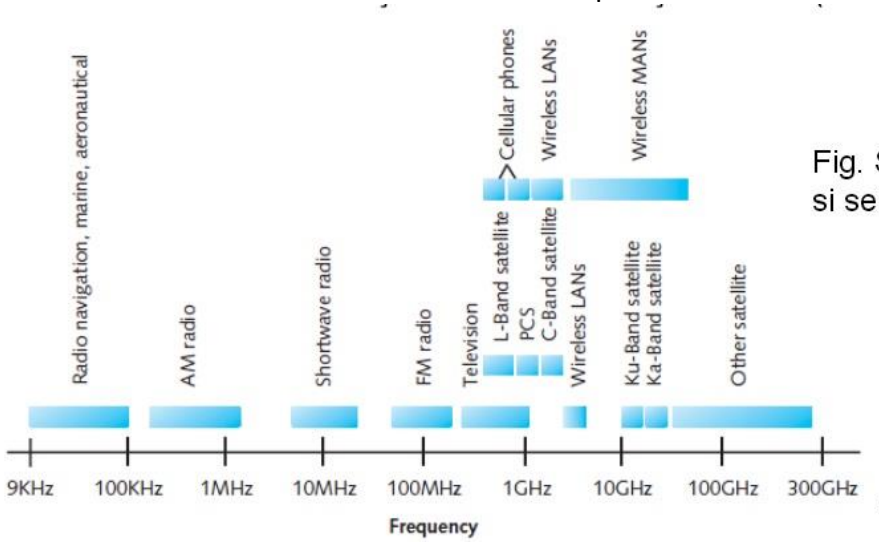


Fig. Spectrul *wireless* si serviciile Wireless

[Network+ Guide to Networks, Tamara Dean]

Propagarea semnalului se face in felul urmator:

- Ideal : in linie dreapta de la emitator la destinatar
- Reflection
- Diffraction : cauzata de obstacole ca obiecte cu margini ascutite
- Scattering : cauzata de intalnirea cu un obiect care are dimensiuni mici in comparatie cu lungimea de unda a semnalulu sau poate fi determinata de rugozitatea unei suprafete; pentru semnalele care sunt trasnsmise in aer liber ploaia, ceata, ninsoarea pot provoca acest efect.

1.4.2Potenţialul unei reţele WLAN şi utilitatea acesteia

- acces fără fir la o reţea locală, fie acasă, la birou, etc.

  acces fără fir la internet într-un spaţiul public (hotspot); în aeroporturi, gări, cafenele etc.

- conexiune wireless point-2-point (conectarea reţelelor LAN, telemetrie, control de la distanţă, monitorizare de la distanţă)
- acces wireless la internet (atât în oraşe cât şi în zona rurală)
- legături pentru comunicaţii de urgenţă (redundanţă wireless pentru conexiunile pe cablu)

1.4.3Standarde WLAN

Vom prezenta soluţii conforme cu următoarele trei standarde:

- 802.11a - în banda de 5 GHz: 5.150 - 5.350 GHz şi 5.470 - 5.725 GHz, rată de transfer de până la 54 Mbps;
- 802.11b - în banda de 2.4 GHz: 2.4 - 2.483 GHz, rată de transfer de până la 11 Mbps;
- 802.11g - în banda de 2.4 GHz: 2.4 - 2.483 GHz, rată de transfer de până la 54 Mbps;

Sunt utilizate şi alte standarde, precum:

- 802.11f - IAPP - Inter Obiective Access Protocol - cooperare între puncte de acces;
- 802.11i - standard care defineneşte noi metode de securitate în reţelele wireless;
- 802.11n - standard pentru transmiterea de conţinut multimedia folosind tehnologia MIMO, viteze de până la 300 Mbps;
- 802.11e - standard ce defineşte QoS - asigură calitatea serviciilor wireless;
- 802.16 - standardul WiMax pentru reţelele wireless de mare capacitate.

1.4.4Raza de acţiune a unei reţele wireless

Trebuie înţeles faptul că raza de acţiune a unei reţele fără fir depinde de o mulţime factori; putem influenţa doar câţiva dintre aceştia. Raza de acţiune a unei reţele wireless depinde de:

1. Factori care depind de echipamentele folosite:

- puterea de ieşire (este specificată de către producător),
- atenuarea pe cablu (depinde de lungimea şi tipul cablului),
- câştigul antenelor (specificat de către producător),
- sensibilitatea dispozitivelor (specificată de către producător).

2. Factori externi:

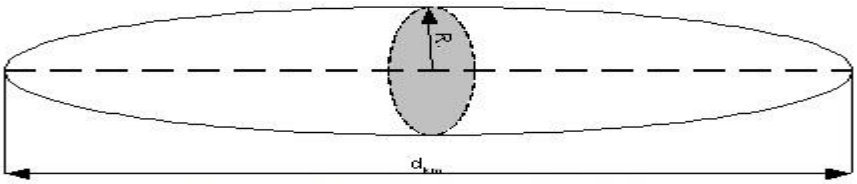
- atenuarea dintre antene (poate fi estimată folosindu-se modelul FSL);
- interferenţa cu alte dispozitive (nu poate fi prevăzută - o marjă de siguranţă suplimentară trebuie să fie dată pentru compensarea acesteia),
- influenţa unor bariere fizice (pereţi, podele, copaci, etc.)

1.4.5Propagarea undelor radio

Zona Fresnel

Zona Fresnel este unul dintre cele mai importante concepte legate de propagarea undelor electromagnetice, fiind indispensabilă pentru evaluarea parametrilor oricărei conexiuni radio. Este o zonă de acţiune intensă pentru transmiterea energiei electromagnetice. Utilizând o secţiune longitudinală aceasta se prezintă ca o elipsă iar dacă se foloseşte o secţiune transversală, zona Fresnel are forma unui cerc. Raza acestuia este o funcţie ce depinde de distanţele antenelor până la acel punct,

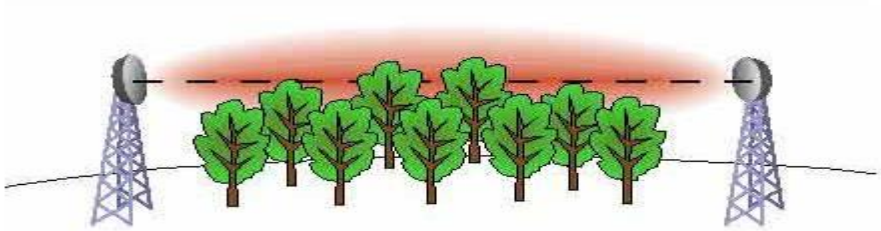
cu o valoare maximă la mijlocul distanţei dintre antene. Este o zonă de spaţiu importantă deoarece cea mai mare parte a energiei semnalului traversează această zonă Fresnel I.



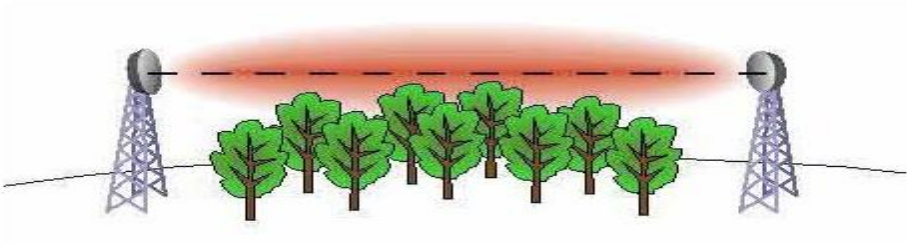
Forma zonei Fresnel R_1 este raza zonei I.

$$R_1 = 17{,}3\sqrt{\frac{d_{1km}\,d_{2km}}{d_{km}\,f_{GHz}}}$$ [m]; Unde:

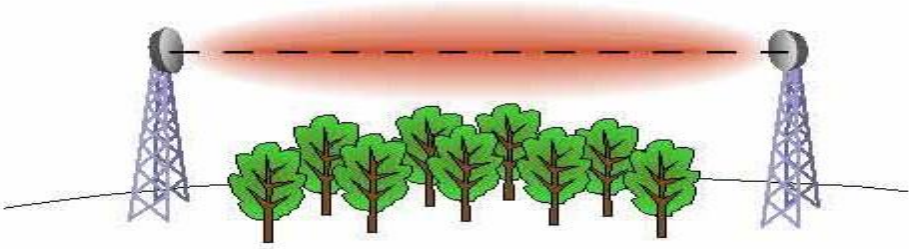
- $d_{km} = d_{1km}+d_{2km}$, este distanţa în km dintre stâlpi
- d_{1km} - distanţa în km până la prima antenă
- d_{2km} - distanţa în km până la a doua antenă



ıtene amplasate greşit. *Nu este îndeplinită cerinţa de vizibilitate mutuală. Legătura radio nu funcţionează.*



Un alt exemplu de instalare efectuată eronat. *Existenţa unei obstrucţii fizice în prima zonă Fresnel va duce la funcţionarea incorectă a conexiunii radio.*



Antene montate corect. *Vizibilitatea mutuală a antenelor şi lipsa barierelor fizice. Conexiunea va funcţiona corespunzător.*

În practică, absenţa obstacolelor în **60% din zona Fresnel I** face ca puterea conexiunii radio să sufere pierderi minimale.

Lungimea legăturii radio [km]	60% din raza zonei Fresnel I ($0.6R_1$ [m])	
	2.4 GHz	5 GHz
0.1	1.1	0.7
0.2	1.5	1.0
0.5	2.4	1.6
1	3.4	2.3
2	4.7	3.3
3	5.8	4.0
4	6.7	4.6
5	7.5	5.2
6	8.2	5.7
7	8.9	6.1
8	9.5	6.6
9	10.1	7.0
10	10.6	7.3

Raza zonei Fresnel I în funcţie de lungimea conexiunii,
pentru sisteme care funcţionează în banda de 2.4 GHz, respectiv 5 GHz (tabel).

Curbura Pământului

În cazul distanţelor mai mari de câţiva kilometri, este necesar să se ia în calcul şi curbura pământului. Pentru o distanţă de 5 km între antene, înălţimea obstacolului din centru creşte cu 1 m (marime numită factor de curbură) iar pentru o distanţă de 10 km, obstacolul creşte cu încă 4 m. Antenele ar trebui montate puţin peste înălţimea minimă care satisface condiţia:

Înălţimea antenelor *= înălţimea celui mai mare obstacol de pe traseu + 0.6R* $_1$ *+ factorul de curbură*

Pentru distanţe mai lungi, vor fi necesare calcule mult mai precise, bazate pe curba hipsografică a terenului ţinând cont şi de efectele de refracţie şi multiplele reflexii ale undei.

Atenuarea cauzată de ploaie şi gaze

Aceste fenomene sunt bine înţelese şi este cunoscut faptul ca pot influenţa negativ o conexiune radio, în practică, ele sunt inofensive pentru sistenele WLAN din 2,4 GHz şi 5 GHz.

Modelul FSL şi atenuarea în aer

Una dintre principalele problemele care apar în proiectarea unei conexiuni radio pentru uz în mediul exterior, este calculul atenuării între emiţător şi receptor. În acest scop se poate folosi modelul FSL. Este un model de calcul a atenuării unelor electromagnetice care se propagă în aer şi porneşte de la următoarele ipoteze:

- nu există nici un obstacol între emiţător şi receptor,
- undele reflectate nu influenţează receptorul,
- prima zonă Fresnel nu este obstrucţionată,
- interferenţele exterioare şi fading-ul semnalului nu sunt considerate.

Atenuarea de spaţiu liber este definită ca reducerea puterii semnalului cauzată de dispersia sferică în atmosferă a undelor radio.

FSL pentru frecvenţa de 2.4 GHz este determinat:

Lp [dB] = 100 + 20log10 D, unde D este distanţa

FSL pentru frecvenţa de 5.4 GHz este determinat:

Lp [dB] = 106 + 20log10 D, unde D este distanţa

Atenuarea de spaţiu liber şi de regula 6dB

Intensitatea semalului radio va scădea pe distanţa propagării acestuia în atmosferă. Determinarea atenuării semnalului radio este urmatoarea etapă în procesul de proiectare.

Distanţa [km]	Atenuarea [dB]	
	2.4 GHz	5 GHz
0.1	80.4	86.4
0.2	86.4	92.4
0.5	94.4	100.4
1	100.4	106.4

2	106.4	112.4
3	109.9	116.0
4	112.4	118.5
5	114.4	120.4
6	116.0	122.0
7	117.3	123.3
8	118.5	124.5
9	119.5	125.5
10	120.4	126.4

Regula 6 dB, în engleză "6dB rule" precizează că o dublare a distanţei de propagare creşte atenuarea semnalului cu 6 dB. Regula este valabilă şi în sens invers, adică o înjumătăţire a distanţei scade atenuarea cu 6dB. Este o regulă simplă care se poate memora foarte uşor. Este suficient să vă amintiţi că în banda de **2.4 GHz, atenuarea la distanţa de 1 km este de 100 dB.**

Deci, folosind regula 6 dB, vom obţine pentru distanţele de 2, 4 şi 8 km, atenuări de 106, 112 şi respectiv 118 dB. Pentru 500 m, 250 m şi 125 m, atenuarea va fi de 94, 88 şi bineînţeles 82 dB. Regula 6 dB se poate folosi şi pentru banda de 5 GHz şi nu numai, dar, atenuarea în banda de 5 GHz pe distanţa de 1 km va fi de 106 dB.

Alte modele de propagare a energiei electromagnetice

În instalaţii profesionale, inginerii utilizează modele extrem de sofisticate, dezvoltate pentru medii şi condiţii specifice:

- model de propagare cu zona Fresnel blocată
- model de propagare, care consideră inclusiv atenuarea pereţilor din interiorul clădirilor

1.5 Avantaje/Dezavantaje ale retelelor WLAN

Retelele wireless sunt utilizate acolo unde distanta este o problema sau din punct de vedere al costurilor sau al performantei este mai eficienta. Un avantaj al retelelor wireless este ca nu necesita cablari sau diferite amenajari, iar extinderea retelei se face foarte rapid si usor.

Avantaje:

- mobilitatea utilizatorilor;
- instalarea rapida;
- flexibilitatea;
- extensibilitatea
- reconfigurare usoara a retelei

Dezavantaje:

Exista insa si dezavantaje in cazul retelelor wireless. Pe langa cea mai usoara utilizare si cea mai mare flexibilitate, o retea wireless este totodata si cea mai expusa din punct de vedere al vulnerabilitatii la interceptari neautorizate.

La nivelul fizic, oricine poate sa acceseze o retea wireless. Nu este nevoie sa tai cabluri, pentru ca mediul de propagare al datelor este aerul. Ele pot trece prin ferestre, la fel de bine cum pot trece si prin peretii subtiri din birourile obisnuite. Din fericire, nu este suficient in general sa ai acces la nivelul fizic pentru a obtine si accesul efectiv la retea, deoarece producatorii echipamentelor de comunicatii au conceput modalitati de criptare a informatiilor, care sa le faca inaccesibile intrusilor. Securitatea retelelor wireless este un punct de discutie foarte aprins, deoarece din motive de necunostinta a utilizatorilor sau de neprofesionalism al administratorilor, ori pentru a permite conectarea usoara, aceste caracteristici de protectie nu sunt intotdeauna activate.

Un alt mare dezavantaj al retelelor wireless il reprezinta faptul ca acestea au o banda redusa cu un mediu de transmisie half-duplex si o stabilitate a conexiunii redusa.

1.6 Standardul IEEE 802.11

1.6.1 Introducere

Standardul a fost elaborat de IEEE în anii 1990, prima versiune a lui fiind definitivată în 1997. Acea versiune nu mai este folosită de implementatori, versiunile mai noi și îmbunătățite 802.11a/b/g fiind publicate între 1999 și 2001. Din 2004 se lucrează la o nouă versiune, intitulată 802.11n și care, deși nu a fost definitivată, este deja implementată de unii furnizori de echipamente

Odata cu lansarea lui in anul 1999 standardul IEEE 802.11 a devenit un standard de referinta pentru retelele wireless, oferind mobilitate si conectivitate la preturi relativ reduse.

Limitările standardului provin din mediul fără fir folosit, care face ca rețelele IEEE 802.11 să fie mai lente decât cele cablate, de exemplu Ethernet dar și din folosirea benzii de frecvență de 2,4 GHz, împărțită în 12 canale care se suprapun parțial două câte două. Limitările date de consumul mare de energie, precum și de reglementările privind puterea electromagnetică emisă, nu permit arii de acoperire mai mari de câteva sute de metri, mobilitatea în cadrul acestor rețele fiind restrânsă. Cu toate acestea au apărut și unele tehnologii care permit legături fără fir bazate pe standardul 802.11 între două puncte fixe aflate la distanțe de ordinul sutelor de kilometri. Din punct de vedere al securității, IEEE și Wi-Fi Alliance recomandă utilizarea standardului de securitate 802.11i, respectiv a schemei WPA2. Standardul IEEE 802.11 descrie protocoale de comunicație aflate la nivelul gazdă-rețea al Modelului TCP/IP, respectiv la nivelurile fizic și legătură de date ale Modelului OSI. Aceasta înseamnă că implementările IEEE 802.11 trebuie să primească pachete de la protocoalele de la nivelul rețea (IP) și să se ocupe cu transmiterea lor, evitând eventualele coliziuni cu alte stații care doresc să transmită.

802.11 face parte dintr-o familie de standarde pentru comunicațiile în rețele locale, elaborate de IEEE, și din care mai fac parte standarde pentru alte feluri de rețele, inclusiv standardul 802.3, pentru Ethernet. Cum Ethernet era din ce în ce mai popular la jumătatea anilor 1990, s-au depus eforturi ca noul standard să fie compatibil cu acesta, din punctul de vedere al transmiterii pachetelor.

Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	540 Mbps	~50 m

Familia de protocoale 802.11

1.6.2 Rata de transfer

Ratele de transfer ale standardului 802.11 au fost, la început (anii 1997-1999), de ordinul megabiților pe secundă, într-o perioadă în care rețelele Ethernet, cablate, ofereau rate de ordinul zecilor și sutelor de megabiți pe secundă. În anul 2012, sunt disponibile pe scară largă echipamente Ethernet Gigabit, apărând chiar și echipamente ce transferă date prin cablu la 10 Gbps, în timp ce rețelele 802.11g ating rate de transfer de 56 Mbps, iar noul standard 802.11n își propune să atingă 450 Mbps. Din punctul de vedere al ratei de transfer, din cauza caracteristicilor adesea imprevizibile ale mediului, cum ar fi zgomote electromagnetice provenite din diverse sursesau fenomene atmosferice (ceață, fenomene electrice și electrostatice), rețelele Wi-Fi rămân în urma celor cablate. Totuși, rețelele 802.11 sunt cele mai rapide rețele fără fir, singurele care se pot compara ca rată de transfer cu rețelele locale cablate.

1.6.3 Aria de acoperire

O limitare importantă a rețelelor Wi-Fi o constituie aria de acoperire. Ea depinde mult de capabilitățile antenelor dispozitivelor și de topografia particulară a zonei pe care urmărește rețeaua să o acopere. Plantele absorb radiațiile electromagnetice, și astfel instalarea unei rețele într-o zonă împădurită (cum ar fi un parc) limitează aria de acoperire a acesteia. Pereții de beton reflectă puternic undele radio, instalarea unei rețele într-o clădire aducând astfel limitarea numărului de camere ce poate fi acoperit de o singură celulă. În interiorul clădirilor, un punct de acces cu o antenă de dimensiuni mici și un preț accesibil poate acoperi o rază de aproximativ 32 m, iar în exterior, același punct de acces poate ajunge la 95 m. Aria de acoperire poate fi și mai restrânsă în cazul folosirii benzii de 5 GHz în locul celei de 2,4 GHz (mai zgomotoasă, dar în care se poate acoperi o arie mai mare). Transmisiunea la cea mai mare distanță cu ajutorul unor dispozitive Wi-Fi a fost realizată, folosind antene puternice și semnale

direcționate, de Ermanno Pietrosemoli de la *Escuela Latinoamerica de Redes*, care a transferat 3 MB de date între vârfurile El Aguila și Platillon din Venezuela, aflate la o distanță de 382 km.

1.7 Bluetooth

1.7.1 Istoric

Bluetooth este un standard deschis (specificaţiile sale tehnice sunt accesibile oricui) destinat comunicaţiilor radio pe distanţe scurte. Introdus de compania Ericcson în 1994, Bluetooth a fost rapid adoptat deIBM, Nokia, Intel şi Toshiba care împreună cu Ericsson, au format Bluetooth Special Interest Group – un grup de lucru axat pe îmbunătăţirea acestei tehnologii. Bluetooth a fost standardizat prin standardul IEEE 802.15.1-2002.3. Bluetooth operează în banda de frecvenţe 2400 – 2483,5 MHz, bandă ce poate fi utilizată de oricine fără a deţine licenţă de operare. Tot în această bandă operează şi standardul wireless IEEE 802.11b/g.

1.7.2 Caracteristici generale

Bluetooth este utilizat în multe domenii pentru realizarea unor reţele wireless de tip peer to peer – P2P, în care pot fi conectate cu uşurinţă o varietate de dispozitive cum ar fi: telefoane mobile, laptop-uri, imprimante, tastaturi, echipamente auto, dispozitive medicale, senzori, etc. Prin intermediul acestor reţele pot fi transferate în general date sau semnal vocal.

Aceasta tehnologie a fost proiectata si dezvoltata pentru transmiterea datelor pe distante mici (aprox. 10m) ceea ce implica un consum mic de energie.Astfel aceasta tehnologie este ideala pentru echipamente portabile de mici dimenisuni care de obicei functioneaza pe baterie.Printr-o retea bluetooth se pot transmite atat date cat si semnale de tip voce.

Standardurile Bluetooth în ordinea apariţiei:
Bluetooth 1.2 – Noiembrie 2003;
Bluetooth 2.0 + EDR (Enhanced Data Rate)– Noiembrie 2004;
Bluetooth 2.1 + EDR – Iulie 2007;
Bluetooth 3.0 + HS (High Speed) – Aprilie 2009;
Bluetooth 4.0 LE (Low Energy);

1.7.3 Principiile Bluetooth

Bluetooth foloseşte tehnologia radio cu salt de frecvenţă - FHSS (Frequency Hopping Spread Spectrum), tehnologie ce presupune utilizarea după un algoritm de salt predefinit, a mai multor frecvenţe discrete dintr-un set dat. FHSS are proprietatea de a reduce puternic interferenţele şi erorile de transmisie.

Bluetooth 1.2 şi 2.1, utilizează 79 canale radio cu banda de 1 MHz ce sunt schimbate de 1600 de ori pe secundă pentru legăturile de voce/date şi de 3200 de ori pe secundă atunci când se efectuează scanarea spectrului pentru descoperirea altor dispozitive. Un canal este utilizat 625 microsecunde, după care se efectuează saltul conform secvenţei pseudoaleatoare. Pentru a reduce consumul şi pentru a putea emite în raza maximă pentru care este proiectat dispozitivul respectiv, puterea semnalului utilizat în reţelele Bluetooth este adaptivă, ceea ce înseamnă că, nivelul acesteia depinde de condiţiile de propagare. Fiecare dispozitiv poate determina nivelul semnalului recepţionat astfel încât, poate cere altor dispozitive din reţea să

scadă sau să crească puterea relativă a semnalului emis pentru a fi atinsă o recepţie optimă. Puterea adaptivă şi saltul de frecvenţă fac ca tehnologia Bluetooth să fie mult mai greu de interceptat în raport cu o tehnologie în frecvenţă fixă cum este IEEE 802.11b/g.

Funcţie de puterea emisă şi implicit a razei maxime de acţiune, dispozitivele Bluetooth sunt grupate în trei clase:

Bluetooth Clasa 1-distanţa maximă de acţiune de până la 100 m, puterea emisă 100 mW, dispozitive din această clasă – adaptoare USB, puncte de acces

Bluetooth Clasa 2-distanţa maximă de acţiune de până la 10 m, puterea emisă 2,5 mW, dispozitive din această clasă – telefoane mobile, adaptoare Bluetooth

Bluetooth Clasa 3-distanţa maximă de acţiune de până la 1 m, puterea emisă 1 mW, dispozitive din această clasă – adaptoare Bluetooth

Dispozitivele Bluetooth suportă mai multe viteze de transmisie funcţie de standard-ul în care funcţionează. Deoarece toate standardele sunt concepute în ideea compatibilităţii cu versiunile precedente, orice dispozitiv Bluetooth va putea comunica cu un altul dar cu o restricţie legată de viteza de transfer.Dispozitivele Bluetooth 1.1 şi 1.2 suportă viteze de transmisie de până la 1 Mbps – standardul BR (Basic Rate) utilizând modulaţia GFSK.Incepand cu standardul 2.0 viteza de transfer a crescut la 3 Mbps - EBR (Enhanced Basic Rate) datorită modulaţiei 8DPSK.

Dispozitivele Bluetooth în standardul 3.0 – High Speed ating viteze de transfer de până la 24 Mbps folosind modulaţia OFDM.Standardul Bluetooth 4.0 LE (Low Energy) permite viteze de transfer de până la 1 Mpbs şi raze de acţiune cu până la 30 % mai mari folosind puteri de emisie de 10 ori mai mici decât standardele 1.1, 1.2 şi 2.1.

2. Mecanisme de securitate: IEEE 802.11

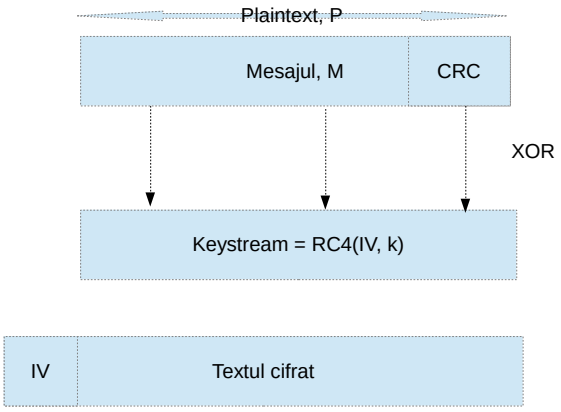
Standardul IEEE 802.11 a fost pentru prima dată introdus în 1997 pentru a oferi conexiuni fără fir pe distanțe limitate. Originalul 802.11 opera în gama de 900 MHz și furniza rate de transfer de până la 2 Mbps. IEEE a introdus un număr de extensii la standardul 802.11, în special 802.11a, 802.11b, 802.11g. O comparație a diferitelor protocoale 802.11 este prezentată mai jos.

	802.11a	802.11b	802.11g
Banda de frecventa	5 GHz UNII	2.4 GHz ISM	2.5 GHz ISM
Tipul de modulatie	OFDM	DSSS	DSSS sau OFDM
Numărul de canale de date	12	3	3
Transfer (max)	54 Mbps	10 Mbps	54 Mbps
Acoperire	50 m	100 m	100 m
Interoperabilitate	Doar 802.11a	Compatibil cu 802.11g	Compatibil cu 802.11b (totuși, performațele se reduc la 802.11b)

2.1 WIRED EQUIVALENT PRIVACY (WEP)

IEEE 802.11 specifică un standard de securitate cunoscut sub numele de WEP pentru a furniza securitate rețelelelor fără fir. Vom detalia WEP pentru a oferi o mai bună înțelegere a limitărilor sale, și modul în care aceste limitări vor fi remediate prin protocoalele WPA și IEEE 802.11i. WEP a fost proiectat pentru a oferi securitate în rețeaua wireless la un nivel echivalent cu rețelele cablate. Principalele 3 obiective de securitate pentru WEP sunt: [Borisov 2002]

Confidențialitatea: Prevenirea interceptării folosind un sistem de criptare bazat pe cifrul pe flux RC4. Accesul controlat: Protejarea acesului la o infrastructură wireless prin solicitarea utilizatorului să demonstreze cunoașterea unei chei secrete k (comun cunoscută sub numele de cheie WEP). Această cheie este partajată între toți utilizatorii legitimi ai rețelei WLAN. Integritatea datelor : Pentru a preveni manipularea frauduloasă a mesajelor transmise, printr-o sumă de control CRC-32



Procesul de criptare WEP

O descriere a procesului de criptare folosit în WEP:

Presupunem că utilizatorul are cheia secretă corectă k pentru a accesa rețeaua. Procesul criptarii unui mesaj generat de utilizator M este următorul:

Pasul 1: Se calculează o sumă de control ciclică redundantă de 32 biți (CRC) pentru Mesajul M. CRC-ul este lipit la mesajul M pentru a forma un mesaj P de tip text clar.

Etapa 2: Un keystream RC4 este generat prin utilizarea cheii secrete k și un vector de inițializare(IV) ca intrări. IV este utilizat pentru a se asigura că pachetele de date ulterioare sunt criptate cu diferite keystreams, chiar dacă este utilizată aceeași cheie secretă.

Pasul 3: RC4 keystream este EXCLUSIVE-ORed (XOR) cu mesajul plaintext P, pentru a genera textul cifrat C.

Pasul 4: IV este concatenat cu textul cifrat, și întregul cadru este transmis. IV nu este criptat și este transmis în clar.

Pasul 5: Când sosește cadrul mesajului la destinatar (o altă gazdă pe rețeaua fără fir care posedă, de asemenea, cheia secretă k), IV este extras din cadru. IV este folosit împreună cu cheia comună secretă K pentru a genera keystream-ul RC4 original. Textul clar original P este apoi recuperat prin efectuarea unui XOR de către textul cifrat și keystream.

Pasul 6: Gazda destinatară efectuează o verificare de integritate prin calcularea sumei de control pentru mesajul primit, și comparând-o cu suma de control CRC primită. Mesajul trece de verificarea integrității în cazul în care cele două sume de control sunt identice. Dacă sumele de control sunt diferite, mesajul este considerat a fi compromis și va fi eliminat.

Diferiți parametri utilizați în mecanismul WEP

Parametrii	Proprietăți
Cheie secretă k - cheie WEP	40 biți (folosit în vechile sisteme WEP) 104 biți (standardul curent)
Vector de inițializare, IV	24 biți
Sumă de control pentru integritate	CRC de 32 biți
Algoritm de criptare	Cifru pe flux RC4

2.1.1 Slăbiciuni ale WEP

Mecanismul WEP a intrat sub control intens pe parcursul ultimilor ani, din cauza defectelor sale de securitate inerente. [Borisov 2002] a demonstrat că WEP eșuează în realizarea obiectivelor sale de securitate de confidențialitate, integritate și controlul accesului. Pe baza cercetărilor, WEP s-a dovedit a fi nesigur din cauza punerii în aplicare necorespunzătoare a algoritmului RC4 și utilizarea sumei de control CRC 32 pentru integritatea datelor. Problemele cheie ale WEP sunt rezumate după cum urmează:

1 . Integritatea

Suma de control CRC 32 nu oferă integritate puternică mesajului. A fost demonstrat că un atacator poate modifica conținutul unui pachet de mesaj , precum și suma de control CRC - 32 de corespunzătoare , chiar fără să știe secretul cheii de criptare .

2 . Autentificarea

Mecanismul de autentificare utilizat în WEP este un simplu sistem "provocare și răspuns" bazat pe faptul că un utilizator cunoaște un secret comun. În cazul WEP , aceast secret comun este cheia WEP, care este împărțită între toți utilizatorii rețelei wireless. Problema cu utilizarea de autentificare WEP este că utilizatorii nu pot fi identificați și autentificați în mod individual, deoarece oricine are cheia WEP i se va acorda acces. O altă problemă cu WEP este că nu acceptă autentificare reciprocă. Prin urmare, un utilizator nu poate contesta și autentifica un punct de acces la rețea și nu poate fi sigur că se conectează la o rețea legitimă.

3.Confidențialitatea

WEP nu protejează confidențialitatea ca urmare a punerii în aplicare necorespunzătoare a algoritmului RC4. Managementul prost al cheilor, precum și reutilizarea IV poate permite atacatorilor să spargă cheia WEP în cazul în care un număr suficient de pachetele sunt captate („sniffed") și colectate de pe undele radio. Odată ce cheia WEP este spartă , decriptarea informațiilor transmise în rețeaua wireless devine banală. Au fost dezvoltate instrumente care exploată punctele slabe WEP și pot fi liber descărcate prin intermediul Internetului . Exemple de asemenea instrumente sunt AirSnort (disponibil la http://airsnort.shmoo.com) și WEPCrack (disponibil la http://wepcrack.sourceforge.net).

WEP poate fi atacat chiar dacă fiecare utilizator are o cheie distinctă. Din moment ce cheile sunt în general stabile pentru perioade lungi de timp, standardul WEP recomandă (dar nu impune) ca IV-ul să fie schimbat la fiecare pachet pentru a evita atacul de tip reutilizare asupra şirului cheie. Din nefericire, multe plăci 802.11 pentru calculatoarele portabile resetează IV la 0 când placa este introdusă în calculator şi apoi îl incrementează cu 1 la fiecare pachet trimis. Cum utilizatorii scot şi apoi reinserează frecvent aceste plăci, pachetele cu valori mici pentru IV sunt destul de obişnuite. Dacă cineva poate să colecteze mai multe pachete trimise de acelaşi utilizator, care au aceeaşi valoare pentru IV (care este trimis în clar cu fiecare pachet), atunci poate să calculeze XOR între două valori de text clar şi poate astfel să spargă cifrul. Dar, chiar dacă placa 802.11 alege o valoare aleatoare pentru fiecare pachet, IV are doar 24 de biţi, astfel încât după ce au fost trimise 2^{24} pachete, va trebui ca valorile să fie refolosite. Mai rău, folosind valori aleatoare pentru IV, numărul probabil de pachete care trebuie trimise înainte ca acelaşi număr să fie folosit de două ori este în jur de 5000, datorită atacului de tip „ziua de naştere"*. Ca urmare, dacă cineva ascultă pentru câteva minute, acea persoana este aproape sigură că va captura două pachete cu acelaşi IV şi aceeaşi cheie. Efectuând operaţia XOR între cele două texte cifrate, ea este capabilă să obţină combinaţia XOR dintre textele în clar. Această secvenţă de biţi poate fi atacată în diferite moduri pentru a descoperi textele în clar. Cu mai multă muncă, şirul cheie pentru acel IV poate fi obţinut de asemenea. Atacatorul poate continua să lucreze în acest mod pentru a realiza un dicţionar de şiruri cheie pentru diferite IV. Odată spart un IV, toate pachetele trimise cu acesta în viitor (dar şi în trecut) pot fi complet decriptate. Mai

mult, deoarece IV-rile sunt folosite aleator, odată ce acea persoana a determinat o pereche (IV, şircheie) validă, ea o poate folosi pentru a genera toate pachetele pe care le doreşte şi astfel, să intervină activ în comunicaţie. Teoretic, un receptor ar putea observa că dintr-o dată un număr mare de pachete au toate acelaşi IV, dar WEP permite acest lucru şi oricum nimeni nu verifică acest lucru. În sfârşit, CRC-ul nu valorează prea mult, deoarece este posibil ca persoana (atacatorul) să modifice încărcătura utilă şi apoi să facă schimbările corespunzătoare în CRC, fără a trebui măcar să elimine criptarea. Pe scurt, spargerea securităţii 802.11 este destul de evidentă, şi nici măcar nu am enumerat toate atacurile pe care le-au găsit Borisov et. al. În august 2001, la o lună după ce a fost prezentată lucrarea lui Borisov et. al, a fost publicat un alt atac devastator asupra WEP (Fluhrer et. al, 2001). Acesta a găsit slăbiciuni criptografice chiar în RC4. Fluhrer et. al au descoperit că multe dintre chei au proprietatea că este posibilă deducerea câtorva dintre biţii cheii din şirul-cheie. Dacă acest atac este pus în aplicare repetat, este posibilă deducerea întregii chei cu un efort modest. Fiind înclinaţi mai mult către teorie, Fluhrer et. al nu au încercat efectiv să spargă vreun LAN 802.11. În contrast, când un student la cursurile de vară şi doi cercetători de la AT&T Labs au aflat despre atacul lui Fluhrer et. al, s-au decis să îl încerce într-un caz real (Stubblefield et. al, 2002). Într-o săptămână ei au spart prima lor cheie de 128 de biţi dintr-un LAN 802.11 de producţie şi cea mai mare parte a săptămânii a fost de fapt dedicată căutării celei mai ieftine plăci de reţea 802.11, obţinerii permisiunii de a o cumpăra, instalării şi testării ei. Programarea a durat efectiv doar două ore. Când şi-au anunţat rezultatele, CNN a emis o ştire intitulată „Un spărgător de rutină sparge criptarea comunicaţiilor fără fir", în care nişte guru din industrie au încercat să minimalizeze rezultatele lor, spunând că ceea ce au făcut ei a fost trivial, date fiind rezultatele lui Fluhrer. Chiar dacă această observaţie este tehnic adevărată, rămâne faptul că eforturile combinate ale acestor două echipe au demonstrat o scăpare fatală în WEP şi 802.11. În 7 Septembrie, 2001, IEEE a răspuns faptului că WEP era atunci complet spartă printr-o declaraţie scurtă cu şase puncte care pot fi rezumate grosier în felul următor:

1. Noi v-am spus că securitatea WEP nu era mai bună decât cea a Ethernet-ului.
2. O ameninţare mult mai mare este să uiţi complet să activezi securitatea.
3. Încercaţi să folosiţi altă securitate (de ex., securitatea nivelului transport)
4. Versiunea următoare, 802.11i, va avea o securitate mai bună.
5. Certificările ulterioare vor impune folosirea 802.11i.
6. Vom încerca să ne dăm seama ce se poate face până când apare 802.11i.

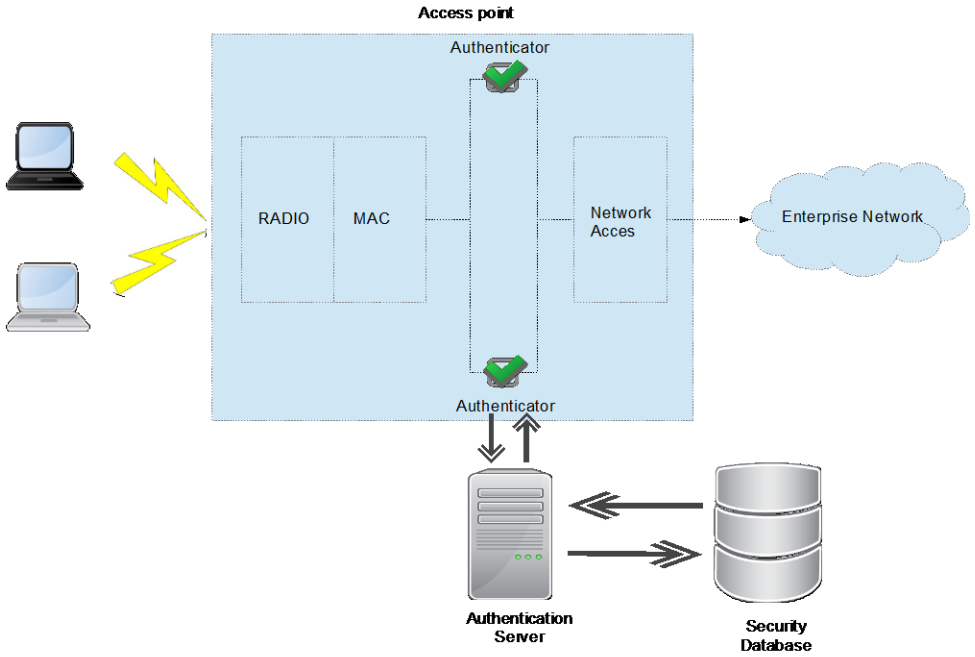
2.1.2 IEEE 802.1x

IEEE 802.1x este un protocol pe bază de port care oferă autentificare și autorizare pentru ambele rețele cu fir sau fără fir. A fost inclus în standardul 802.11 pentru a remedia deficiențele în procesele de autentificare utilizate în WEP. IEEE 802.1x a fost ratificat în iunie 2001, și este în prezent suportat de multe carduri 802.11 și punctele de acces. (Specificația este disponibil la http://www.ieee802.org/1/pages/802.1x.html).

Principiul de funcționare : 802.1x definește trei entități în procesul de autentificare [Edney și Arbaugh 2004]:

- Supplicant (Solicitant) - entitate care dorește să se conecteze la o rețea adică un client wireless.

• Authenticator (Autentificator) - entitate care controlează accesul la rețea. În caz de rețele WLAN, aceasta se referă la un punct de acces.
• Server de autentificare - entitate care ia decizia de autorizare.
O prezentare generală a procesul de autentificare utilizat în 802.1x:



Un autentificator este creat împreună cu un port logic pentru fiecare supplicant care solicită accesul la rețea. Autentificatorul controlează accesul la resursele rețelei, prin utilizarea de switchuri logice în punctul de acces. În mod implicit, switch-urile logice sunt în poziție deschisă. Un dispozitiv wireless trebuie să prezinte credențialele (cum ar fi user ID-ul și parola) la autentificator, care, la rândul său, transmite aceste mesaje serverului de autentificare. Serverul de autentificare folosește credențialele oferite de dispozitivul wireless și determină dacă acordă accesul. Dacă accesul este acordat, comutatorul logic care controlează conexiunea pentru dispozitivul wireless va fi închis permițând astfel accesul la rețea. 802.1x încearcă să protejeze rețeaua de atacurile de la toate nivelele superioare prin securizarea nivelului Acces la mediu. 802.1X permite și alte funcții pe lângă blocarea accesului stațiilor neautentificate:

–Poate urmări locația utilizatorilor (de exemplu AP-ul sau switch-ul de unde s-au conectat)

–Poate contabiliza și taxa activitatea clientului autentificat (pentru servicii de ISP)

–Poate permite doar accesul la anumite părți din rețeaua fizică în funcție de nivelul de acces al clientului

Procesul de autentificare 802.1X include mai multe tipuri de trafic

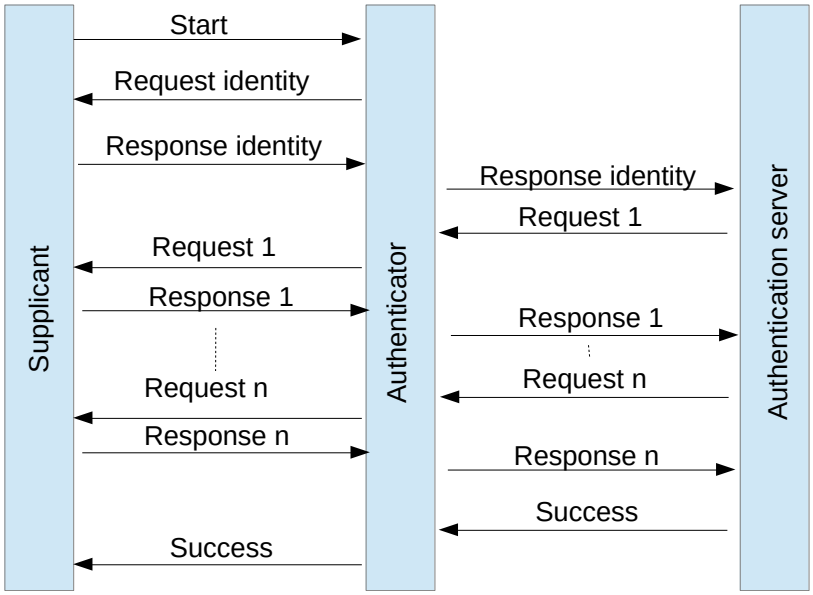
•Între solicitator și autentificator: EAPOL – Funcționează direct peste nivelul 2 (sunt suportate 802.3 și 802.11)

•Între autentificatorși serverul de autentificare: RADIUS – Protocol de nivel aplicație ce funcționează peste UDP

2.1.3 Extensible Authentication Protocol (EAP)

802.1x este destinat să ofere autentificare puternică, controlul accesului și controlul gestiunii cheilor, care nu sunt furnizate în WEP. 802.1x se bazează pe EAP sau mai precis EAP peste Local Area Networks (EAPOL). EAP este un protocol de mesaje care furnizează comunicații și schimburi de mesaje între diferite părți în procesului de autentificare. EAP nu specifică tipul de metodă de autentificare utilizată. Cu toate acestea, diferite metode de autentificare au fost implementate să lucreze cu EAP, inclusiv Kerberos, chei publice/private, precum și biometrice.

Fluxul de mesaje EAP(general) în procesul de autentificare(din [Edney & Arbaugh 2004]):



Secvența de autentificare EAP generală este prezentată în figură. Un solicitant începe procesul de autentificare prin trimiterea unui mesaj EAP-Start la autentificator. La primirea mesajului EAP-Start, autentificatorul răspunde cu un mesaj EAP- Cerere de identitate pentru a determina identitatea solicitantului. Solicitantul trimite informațiile sale de identitate folosind mesajul EAP (Response Identity message) care este transmis de către autentificatoru pentru serverul de autentificare. Serverul de autentificare inițiază o serie de cereri pentru solicitant, care oferă răspunsuri la fiecare cerere. Serverul de autentificare verifică răspunsurile primite de la solicitant, și returnează un mesaj de succes la autentificator dacă răspunsurile sunt corecte. La primirea mesajului de succes de la serverul de autentificare, autentificatorul acordă acces solicitantului. Cele mai multe aplicații actuale utilizează metoda EAP-TLS (una dintre metodele EAP) pentru autentificare cu un server de autentificare. EAP-TLS (Extensible Authentication Protocol Transport Layer Security) folosește un mecanism pe bază de certificat pentru a efectua autentificarea reciprocă și schimbul de chei, și este în general considerată a fi cea mai puternica metodă de EAP. Din moment ce EAP-TLS utilizează certificate, PKI trebuie să fie suportat în rețeaua enterprise. Serverul de autentificare este de obicei un server RADIUS-based (Remote *Authentication* in Dial-In User Service). Cu toate acestea, 802.1x nu specifică RADIUS ca

serverul de autentificare implicit, și alte servere de autentificare pot fi folosite atât timp cât serverele suportă EAP.

2.2 WI-FI PROTECTED ACCESS (WPA)

WPA este un mecanism, interoperabil, bazat pe standarde dezvoltatat de către Wi-Fi Alliance.
Scopul WPA este să furnizeze remedieri intermediare la vulnerabilitățile WEP. Echipamentul din rețeaua existentă 802.11 poate fi upgradat la WPA prin intermediul software-ului sau upgrade-uri de firmware. Caracteristicile cheie ale WPA sunt după cum urmează:

2.2.1. Temporal Key Integrity Protocol (TKIP)

TKIP este conceput pentru a aborda deficiențele WEP în criptarea datelor. Ca în secțiunile anterioare, implementarea WEP foloseste un cod secret comun static, împreună cu un vector de inițializare (de 24 de biți) pentru a genera keystream-ul de criptare folosind algoritmul RC4. TKIP continuă să utilizeze algoritmul RC4 pentru criptarea pachetelor de date. Cu toate acestea, spre deosebire de WEP care folosește o cheie statică comună secretă, TKIP utilizează o cheie temporală care este schimbată la fiecare 10000 de pachete. Un vector de inițializare mai lung, de 48 de biți este, de asemenea, adoptat pentru a preveni refolosirea vectorilor de inițializare peste durata de viață a unei chei temporale. Aceste măsuri fac ca spargerea cheii TKIP de către potențialii atacatori folosind tehnici de spargere a WEP să fie mult mai dificilă. Un alt aspect defectuos al WEP este reutilizarea unei chei binecunoscute de către toate staţiile din WLAN. TKIP rezolvă acest dezavantaj prin generarea cheii de bază care este combinată cu cheia din fiecare pachet. O nouă cheie este generată de fiecare dată când o staţie stabileşte o legătură cu un punct de acces. Cheia de bază este obţinută prin amestecarea unei valori secrete de sesiune cu nişte numere aleatoare generate de punctul de acces şi de staţie, precum şi a adreselor MAC ale staţiei şi AP.

2.2.2 Michael Message Integrity Check (MIC)

MIC destinat să ofere protecția datelor în tranzit împotriva modificărilor neautorizate sau a violării lor. Algoritmul Michael foloseste un rezumat de mesaj (digest) criptografic al mesajului original ca o sumă de control. Aceasta protejează integritatea pachetelor de date la rețele wireless, deoarece orice încercare de a modifica pachetele va fi detectată.

Cu toate acestea, un aspect important în proiectarea WPA a fost să fie în măsură să funcționeze pe dispozitivele 802.11 existente cu capacitate scăzută a CPU. Din cauza constrângerilor (de puterea procesorului), nu este realizabilă proiectarea Michael MIC care să aibă același nivel de securitate ca și alte sume de control pentru verificarea integrității, cum ar fi MD5. Având în vedere această slăbiciune, TKIP pune în aplicare măsuri suplimentare pentru a lucra cu Michael MIC. Mai exact, atunci când un punct de acces detectează două pachete care

nu au reușit să treacă de algoritmul Michael pe o anumită cheie temporală, acesta va arunca asocierea, va genera noi chei și va aștepta un minut înainte de a crea o nouă asociere cu gazda. Un dezavantaj la măsurile TKIP este că atacatorii pot lansa un atac de tip „denial of service" prin inundarea punctelor de acces cu mesaje care au corupt sumele de control. Acest lucru poate duce în repetate rânduri la time-out la punctele de acces (de până la un minut de fiecare dată), și interzice astfel utilizatorilor legitimi de accesul la rețea.

Cu toate acestea, acest risc de un posibil atac "denial of service" ar trebui să fie pus în balanță cu alternativele WEP (care sunt depășite) sau care nu au deloc mecanism de securitate. În cazurile din urmă, un atacator poate avea acces nerestricționat la rețea și poate provoca daune în timp ce rămâne nedetectat. În cazul WPA, instrumente de monitorizare a rețelei pot fi programate pentru a urmări time-out-uri frecvente la punctele de acces, fapt care ar putea indica un atac activ. Acest lucru poate duce la detectare și executare a planurilor de urgență pentru a opri un atac.

2.3 IEEE 802.11I

Standardul IEEE 802.11i a fost dezvoltat de către IEEE ca un înlocuitor pentru protocolul WEP. Protocolul a fost ratificat de către IEEE, iar primele produse de sprijin 802.11i au aparut pe piață în prima parte a anului 2005. IEEE 802.11i este proiectat pentru a fi compatibil cu protocolul WPA. 802.11i suportă criptare TKIP și Michael Message Integrity Check folosite în WPA, precum și protocolul 802.1x pentru autentificare. Cu toate acestea, trebuie remarcat faptul că TKIP este construit în jurul implementarii defectuoase a algoritmului de criptare RC4 WEP, și prin urmare este considerat a fi o soluție interimară pentru criptarea de securitate. Pentru a contracara punctele slabe ale criptarii bazate pe RC4, 802.11i introduce două protocoale de criptare suplimentare bazate pe algoritmul aprobat FIPS - Advanced Encryption Standard (AES). Cifrurile AES operează pe blocuri de128 de biţi, folosind chei de dimensiuni 128, 192 şi respectiv 256 biţi. Pentru cifrul AES-128 se folosesc 10 runde de criptare, pentru AES-192 se folosesc 12 runde, iar pentru AES-256 se folosesc 14 runde. Toate lungimile acestor chei asigură o protecţie suficientă a informaţiei, până la nivelul SECRET cu 128 biţi, iar pentru nivelul TOP SECRET cu cheile 192 şi 256. În prelucrarea textului original, fiecare rundă este împărţită în patru etape, una de permutare şi trei de subtituire, astfel:

a) Substituirea octeţilor(Byte Substitution) din blocul de intrare(S-box) presupune că fiecare element este supus unei transformări neliniare folosind un tabel de căutare cu proprietăţi matematice speciale.

b) Permutarea rândurilor(ShiftRows) permite lucrul la nivel de octet.

c) Substituirea coloanelor (MixColumns) este o operaţie matricială care combină blocuri de câte 4 octeţi.

d) Adunarea cheii(Key Addition)este o operaţie XOR între blocul curent şi cheie.

Se folosesc chei secundare pentru fiecare rundă, generate din cheia AES inițială. Operaţiile din cadrul etapelor de prelucrare AES folosesc calcule peste câmpuri Galois. Un câmp finit conţine 256 de elemente, notaţia folosită fiind GF(2^8). A fost ales acest camp pentru că fiecare element poate fi reprezentat pe un octet. Pentru etapele de Subtituirea octeţilor şi a coloanelor, AES consideră fiecare octet din blocul de date ca fiind un element din câmpul

GF(2^8) şi realizează operaţii aritmetice în acest câmp finit. Dacă ordinul unui câmp finit nu este prim, atunci trebuie utilizat un câmp extins pentru a reprezenta adunarea şi înmulţirea modulo 2^8. În AES, fiecare element A din GF(2^8) este reprezentat astfel:

$$A\ x = a_7\ x^7 + \ \ldots + \ a_1 x + a_0\ , \qquad a_i\ \in GF\ 2 = 0{,}1$$

Algoritmul modifică la fiecare pas acest tablou de numere denumit *state*, și îl furnizează apoi ca ieșire. Funcționarea sa este descrisă de următorul pseudocod:

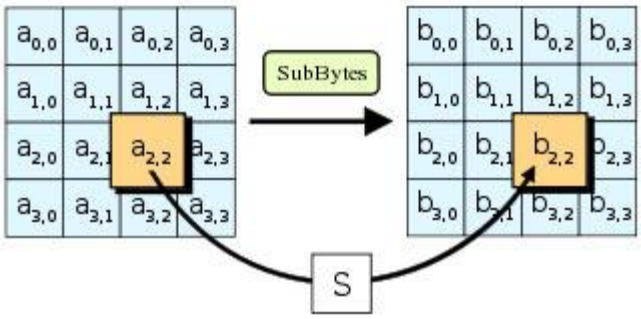
```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[0, Nb-1])
     for round = 1 step 1 to Nr–1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
     end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
  out = state
end
```

Nb = numărul de coloane al stării, în varianta standardizată acesta fiind intotdeauna 4. Se observă din descrierea algoritmului că o anumită secvență este realizată iterativ, de un numar de *Nr* ori. Acest *Nr* depinde de lungimea cheii și este 10, 12 sau 14, pentru chei pe 128, 192, respectiv 256 biți.

SubBytes este un cifru cu substituție, fără punct fix ce rulează independent pe fiecare octet din *state*. Transformarea este neliniară și face astfel întreg cifrul să fie neliniar, ceea ce îi conferă un nivel sporit de securitate. Se calculează fiecare octet conform :

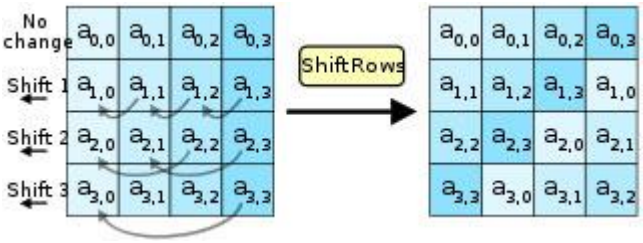
$$b_i' = b_i \oplus b_{(i+4) mod 8} \oplus b_{(i+5) mod 8} \oplus b_{(i+6) mod 8} \oplus b_{(i+7) mod 8} \oplus c_i$$

bi = bitul poziției *i* din cadrul octetului
ci = bitul pozitiei *i* din octetul ce reprezintă valoarea hexazecimală *63*, sau, pe biti, *01100011*

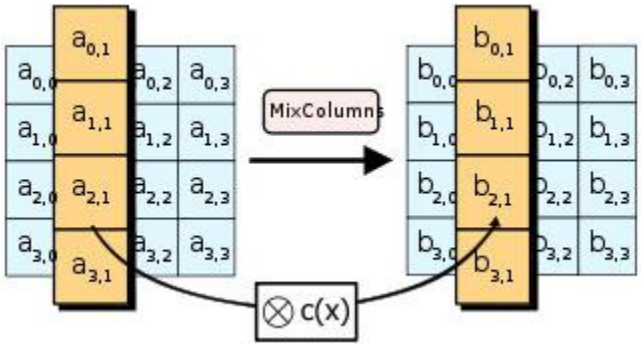


SubBytes este denumit în acest fel pentu că realizează p subtituție octet cu octet. Acest pas constă în găsire unui octet pentru cel dat în matricea de stare de intrare într-un lookup table de 16x16. Intrările în lookup table sunt create folosind noțiuni de inverse multiplicative și „bit scrambling" pentru a strica corelațiile la nivel de bit din fiecare octet.

ShiftRows operează la nivel de rând al matricii de stare *state* și constă în simpla deplasare ciclică a octeților de pe randuri, astfel: primul rând rămâne la fel; al doilea rand se deplasează la stanga cu o poziție; al treilea rând se deplaseaza la stanga cu două pozitii; al patrulea se deplasează la stanga cu trei poziții. Rezultatul acestui pas este că fiecare coloana din tabloul *state* se compune din octeți de pe fiecare coloană a stării inițiale. Acesta este un aspect important, din cauză ca tabloul *state* este populat inițial pe coloane, iar pașii ulteriori, inclusiv AddRoundKey în care este folosita cheia de criptare, operațiile se efectuează pe coloane.



Pentru MixColumns, fiecare coloană a tabloului de stare este considerată un polinom de gradul 4 peste corpul Galois $\mathbf{F}2^8$. Fiecare coloană, tratata ca polinom, este inmulțită, modulo $x^4 + 1$ cu polinomul $a(x) = 3x^3 + x^2 + x + 2$. Operația se poate scrie ca înmulțire de matrice.

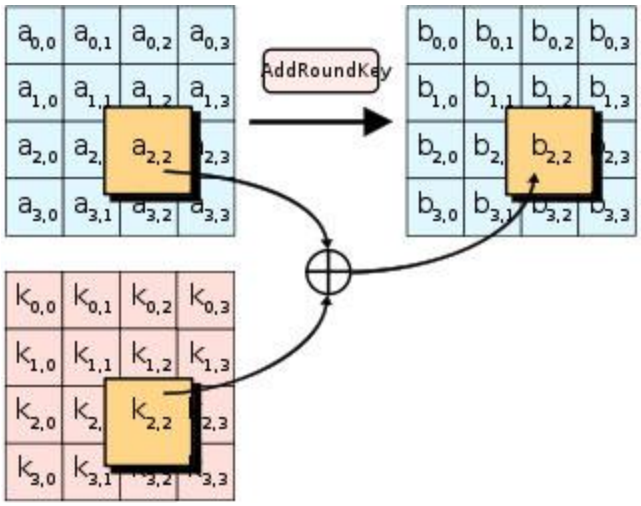


$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

unde s_i' sunt elementele de pe un vector coloană rezultate după inmulțire, iar s_i sunt elementele de pe același vector înaintea înmulțirii.

AddRoundKey constă într-o operație de „sau” exclusiv pe biți între stare și cheia de rundă (o cheie care este unică pentru fiecare iterație, cheie calculată pe baza cheii secrete). Operația de combinare cu cheia secretă este una simpla și rapidă, dar algoritmul ramâne complex, din cauza complexității calculului cheilor de rundă (*Key Schedule*), precum și a celorlalti pași ai algoritmului.
Cheia de rundă este calculată dupa algoritmul urmator:

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
        word temp
        i = 0
        while (i < Nk)
                w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
                i = i+1
        end while
        i = Nk
        while (i < Nb * (Nr+1)]
                temp = w[i-1]
                if (i mod Nk = 0)
                        temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
                else if (Nk > 6 and i mod Nk = 4)
                        temp = SubWord(temp)
                end if
          w[i] = w[i-Nk] xor temp
          i = i + 1
        end while
end
```



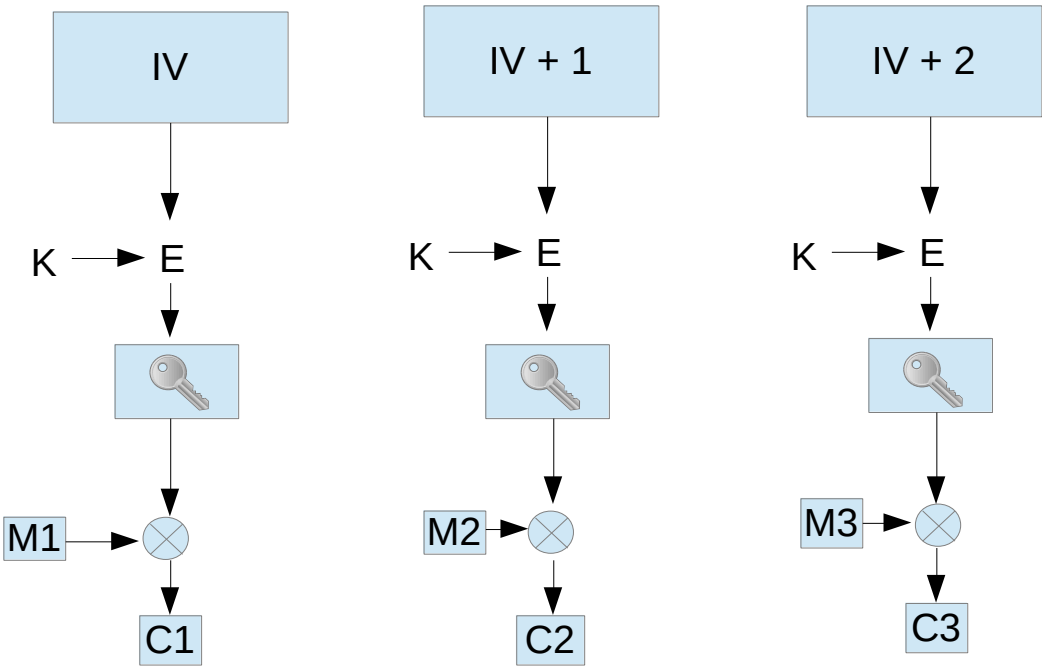
Acest algoritm lucrează pe cheie, de lungime *Nk* cuvinte de 4 octeti (4, 6 sau 8, conform standardului), populând un tabel de Nb(Nr+1) cuvinte, Nb fiind numărul de cuvinte al blocului (în versiunea standardizată, 4), iar Nr numărul de runde (iterații), dependent de lungimea cheii. Algoritmul de planificare a cheilor folosește transformarea *SubWord*, care este o substitutie a octeților identică cu cea din pasul *SubBytes*. *RotWord* este o rotație ciclica la stânga cu un octet a octeților dintr-un cuvânt. Cu *Rcon[i]* se notează în algoritm un cuvânt format din octeții [2^{i-1},{00}, {00}, {00}]. Operația de ridicare la putere este aici cea valabilă în corpul Galois F2^8. Tabloul *w* conține la final cuvintele de pe coloanele cheilor de rundă, în ordinea în care urmează sa fie aplicate.

Algoritmul și imaginile au fost preluate de pe http://www.securitatea-informatiilor.ro/solutii-de-securitate-it.

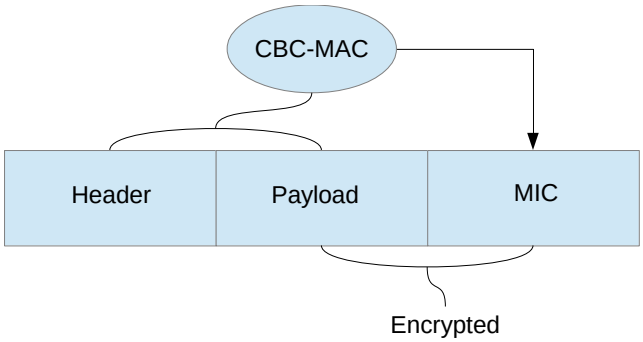
2.3.1 Counter Mode with CBC-MAC Protocol (CCMP)

CCMP este tehnica de criptare în standardul 802.11i. Se folosește algoritmul AES folosind modul de funcționare CCM. CCM utilizeaza modul Counter (CTR) pentru criptarea datelor și Cipher Block Chaining Message Authentication Code (CBC-MAC) pentru a se asigura autenticitatea și integritatea mesajului. CCMP utilizează modul CTR în AES pentru a cripta datele de transmisie. Mecanismul de bază pentru criptarea AES, modul CTR este prezentată în figura de mai jos.

AES Counter (CTR) Mode – procesul de criptare



O cheie temporală (K) de 128 de biți, împreună cu un IV de 48 de biți sunt utilizate pentru a genera un „one-time pad”(cheie acoperitoare - folosirea unei chei o singură dată), folosind algoritmul AES (E) . IV este incrementat după ce se generează fiecare one-time pad. O operație logică OR este apoi efectuată între mesajul plaintext și one-time pad-ul corespunzător. Avantajul folosirii modului CTR este că oferă securitatea criptării echivalentă cu alte moduri de AES, dar este mai puțin de calcul. În modul CTR , one–time pad-urile pot fi pre-calculate pentru o anumită cheie temporală , iar criptarea este o simplă operație logică SAU. Deoarece înlănțuirea (chaining) nu este implementată în mod CTR , pachetele de mesaje pot fi decriptate independent de pachetele de mesaje anterioare. Cu toate acestea, procesul de criptare va fi slăbit dacă este utilizată aceeași cheie și IV pentru a cripta mesaje diferite (aceasta este problema cu care se confruntă WEP). Pentru a rezolva acest lucru, cheia temporală trebuie să fie actualizată periodic prin protocolul 802.1x, și un IV mai mare, pe 48 de biți este folosit pentru a preveni coliziunile IV pe durata de viață a fiecărei chei temporale.



Message Integrity Check folosind CBC-MAC Computation

Pentru a asigura integritatea datelor, o verificare a integrității mesajului (MIC) este executată pentru fiecare mesaj folosind CBC-MAC. Acest lucru este ilustrat în figură. MIC este calculat pentru payload și header, MIC rezultat fiind concatenat. Criptarea este apoi aplicată peste payload și MIC, în timp ce headerul este transmis în clar. Deoarece headerul este inclus în calculul MIC, orice modificare neautorizată sau corupere din header vor fi, de asemenea detectate. Acest lucru previne „spoofing-ul" pachetelor de date în rețea.

2.3.2 WRAP

WRAP a fost inițial propunerea AES pentru criptare în 802.11i. Acest protocol se bazează pe AES în modul OCB (Output Feedback). WRAP a fost înlocuit cu CCMP din cauza problemelor legate de drepturile de proprietate intelectuală, dar a fost păstrat în proiectul 802.11i pentru că unele companii au implementat deja modulele WRAP în hardware-ul lor. Un rezumat al caracteristicile cheie ale WEP, WPA și 802.11i sunt prezentate în tabel.

Caracteristici	WEP	WPA	802.11i
Algoritm de criptare	RC4	RC4	CCMP (folosind AES CCM)
Mărimea cheii	40 sau 104 biți	2 chei folosite -cheie de 128 de biți pentru criptare -cheie de 64 de biți pentru autenticitate și verificarea integrității	128 de biți
Vectorul de inițializare(IV)	24 biți	48 biți	48 biți
Verificarea integrității	CRC de 32 biți	Michael MIC	CBC-MAC
Autentificare și managementul cheilor	Nu are	Bazat pe EAP folosind 802.1x	Bazat pe EAP folosind 802.1x

2.3.3 WPA2

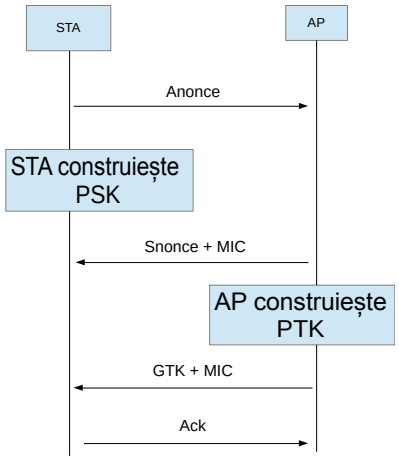
Lansat în 2004, WPA2 este chiar mai sigur decât WPA. Este punerea integrală în aplicare a standardului 802.11i pentru securizarea rețelelor wireless, în timp ce WPA a fost un subset al standardului și destinat doar ca o soluție stop-gap până WPA2 a fost finalizat. WPA2 foloseste AES (Advanced Encryption Standard), care oferă capabilități de criptare de calitate, care sunt mai puternice decât TKIP (Temporal Key Integrity Protocol) utilizat de WPA.

IEEE 802.11i îmbunătățește IEEE 802.11-1999 prin furnizarea de o rețea de securitate robustă (RSN), cu două protocoale noi, 4-Way Handshake și Goup Key Handshake. Acestea

utilizează servicii de autentificare și acces la portul de control descris în IEEE 802.1X pentru a stabili și de a schimba cheile criptografice adecvate. RSN este o rețea de securitate care permite doar crearea de asociații robuste de rețea de securitate (RSNAs)(Robust Security Network Associations), care este un tip de asociere utilizat de către o pereche de statii (STAS), folosită într-o procedură de stabilire de autentificare sau de asociere dintre ele care include 4-Way Handshake. Acesta prevede, de asemenea, două protocoale RSNA a confidențialității și integrității, TKIP și CCMP, cu punerea în aplicare a CCMP fiind obligatorie.

Procesul de autentificare are două considerente: punctul de acces (AP) trebuie să se autentifice la stația client (STA), și cheile de criptare a traficului trebuie să fie derivate. Schimbul EAP sau WPA2-PSK a oferit cheia secretă PMK (Pariwise Master Key). Această cheie este, cu toate acestea, proiectată să dureze întreaga sesiune și trebuie să fie expusă cât mai puțin posibil. Prin urmare, “four-way handshake” este utilizat pentru a stabili o altă cheie numită PTK (Pariwise Transient Key). PTK este generată prin concatenarea următoarele atribute: PMK, AP nonce (ANonce), STA nonce (SNonce), adresa MAC AP, și adresa MAC STA. Rezultatul este apoi trecut prin funcția hash criptografică PBKDF2-SHA1.

Handshake-ul produce, de asemenea, GTK (Grupul Temporal Key), folosită pentru a decripta multicast și traficul de broadcast. Mesajele reale schimbate în timpul handshake-ului sunt descrise în figură și explicate mai jos:



AP trimite o valoare nonce la STA (ANonce) . Clientul are acum toate atributele pentru a construi PTK . STA trimite propria valoare nonce (SNonce) pentru AP , împreună cu un MIC , inclusiv de autentificare , care este de fapt un mesaj de autentificare și de Cod de Integritate : (MAIC). AP transmite GTK și un număr de secvență împreună cu un alt MIC. Acest număr secvență va fi utilizat în următorul cadru de multicast sau broadcast, astfel încât receptorul STA poate realiza detectarea de raspuns. STA trimite o confirmare de AP. Toate mesajele de mai sus sunt trimise ca și cadre de cheie EAPOL. De îndată ce se obține PTK este împărțit în cinci chei distincte : PTK (Pairwise Transient Key - 64 bytes)Cheile TX / RX Autentificator Michael MIC prevăzute în handshake sunt folosite doar în cazul în care rețeaua folosește TKIP pentru criptarea datelor .

2.4 Comparații și recomandări

Comparând performanțele WPA, 802.11i și protocoalele WEP, observăm că 802.11i cel mai sigur. 802.11i adoptă de criptare AES, care este aprobat de către Institutul Național de Standarde și Tehnologie (NIST), pentru utilizarea în aplicații guvernamentale. Mai important, AES este aprobat de către Agenția Națională de Securitate pentru a fi utilizat în protecția informațiilor clasificate până la nivelul SECRET, cu condiția că sunt folosite chei de criptare de cel puțin 128 de biți. Mai mult decât atât, protecția integrității CBC-MAC nu este susceptibilă la atacuri denial-of-service, comparativ cu punerea în aplicare Michael în WPA.

Rijndael, ca și toți ceilalți algoritmi ajunși în etapa finală de selecție pentru standardul AES, a fost revizuit de NSA și, ca și ceilalti finaliști, este considerat suficient de sigur pentru a fi folosit la criptarea informațiilor guvernamentale americane neclasificate. In iunie 2003, guvernul SUA a decis ca AES să poată fi folosit pentru informații clasificate. Până la nivelul *SECRET*, se pot folosi toate cele trei lungimi de cheie standardizate, 128, 192 și 256 biti. Informațiile *TOP SECRET*(cel mai înalt nivel de clasificare) pot fi criptate doar cu chei pe 256 biți.

Atacul cel mai realizabil împotriva AES este îndreptat împotriva variantelor Rijndael cu număr redus de iterații. AES are 10 iterații la o cheie de 128 de biți, 12 la cheie de 192 de biți și 14 la cheie de 256 de biți. La nivelul anului 2008, cele mai cunoscute atacuri erau accesibile la 7, 8, respectiv 9 iterații pentru cele trei lungimi ale cheii.

Există unele probleme care trebuie luate în considerare atunci când se decide să adopte standardul 802.11i în arhitectura enterprise. 802.11i necesită co-procesoare hardware suplimentare pentru a sprijini criptarea AES, iar aceste co- procesoare nu sunt disponibile în NIC-uri 802.11 sau în punctele de acces. Prin urmare, upgrade-uri hardware sunt necesare pentru a face upgrade rețelelelor la standardul 802.11i. În același timp , se recomandă ca actualele 802.11 rețele să fie modernizate pentru standard ul de co- procesoare hardware WPA/WPA2, în scopul de a sprijini criptarea AES.

3. ENTERPRISE ARCHITECTURE DESIGN

In sectiunea anterioara a fost studiata securitatea in standardul IEEE 802.11. In acest capitol, se vor prezenta alte mecanisme de securitate și implementari care pot fi construite pe baza 802.11, pentru a oferi o arhitectura multi-strat de aparare puternica. Obiectivul unei arhitecturi de aparare multi-strat este de a oferi aparare în profunzime, astfel că eșecul unui anumit mecanism de apărare nu va compromite ale intreaga retea. Acesta va oferi, de asemenea, flexibilitate și scalabilitate in proiectare, prin care straturile pot fi adaugate sau eliminate pentru a se potrivi nevoilor specifice ale unui special rețea.

3.1 RETELE PRIVATE VIRTUALE

Rețelele private virtuale (VPN) sunt de obicei utilizate de către întreprinderi pentru a permite utilizatorilor sa acceseze resursele rețelei în siguranță prin infrastructură unei rețele publice. În general, VPN-urile folosesc tehnici de criptare și încapsulare pentru a crea un tunel virtual care suportă comunicații securizate de date pe o rețea nesigură . Cu toate acestea, mecanismele de criptare si incapsulare variaza de la furnizor la furnizor.

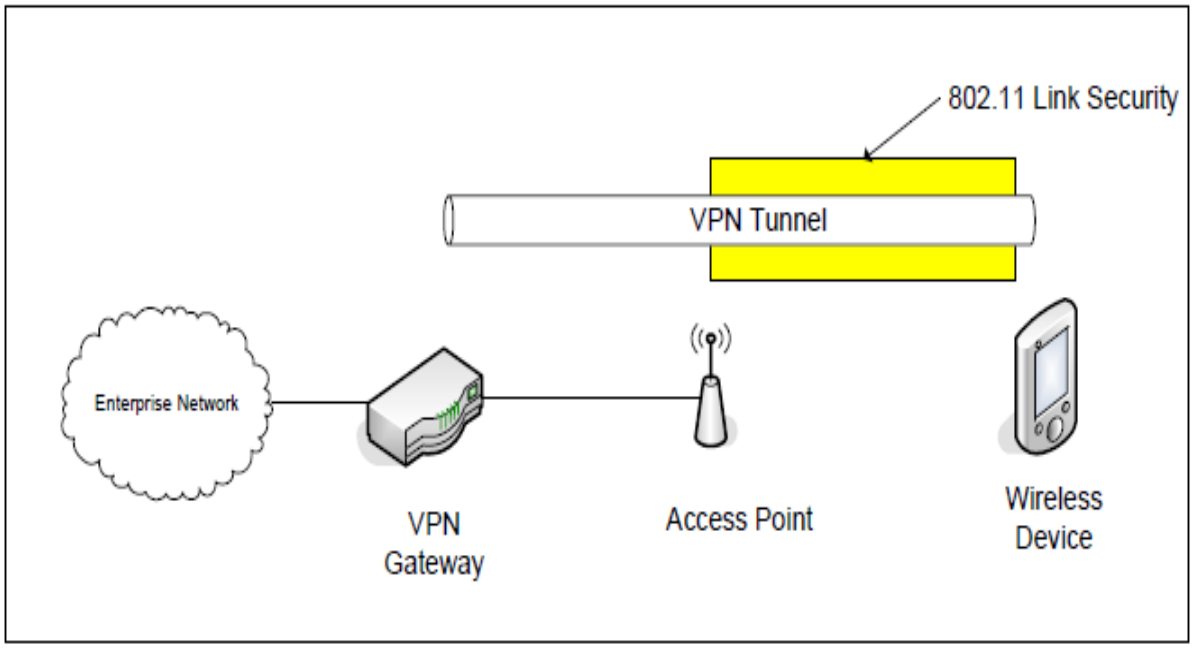
Tunneling reprezintă transmiterea datelor în cadrul unei rețele publice astfel încât aceasta să nu "înțeleagă" faptul că transmiterea (transportul de informații) e parte a unei rețele private. Este realizat prin încapsularea datelor apartenente rețelei private și crearea unui protocol care să nu permită accesul nimănui la acestea. Tunneling permite folosirea rețelelor publice (Internet), văzute astfel ca "rețele private" sau aproape private.

Rețelele VPN oferă mai multe avantaje: prețuri redus pentru implementare / funcționare / administrare / întreținere, securitate informațională sporită (aproape ca la rețelele private propriu-zise, tradiționale), scalabilitate, acces simplificat și, în sfârșit, compatibilitate cu rețelele publice de mare viteză.

Cele mai folosite protocoale pentru comunicatiile VPN sunt Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), si Internet Protocol Security (IPSec). Multe implementări VPN existente se bazează pe securitatea IPSec protocol. IPSec oferă criptare de date, folosind algoritmul de criptare 3-DES. Există, de asemenea implementări VPN care adoptă AES și alti algoritmi de criptare.

Figura ilustrează integrarea VPN pentru rețeaua wireless. Un gateway VPN este desfășurat la marginea rețelei de întreprindere, și toti clienții se vor conecta prin intermediul gateway VPN pentru a accesa resursele de rețelei. Un tunel VPN este creat de la poarta de acces VPN, prin punctul de acces wireless și se termină la client. Pachetele de date transmise pe această rută vor fi protejate prin tunelul VPN. Punerea în aplicare a securității link 802.11i va adăuga o protecție suplimentară de-a lungul tunelului între punctul de acces și dispozitivul fără

fir. Prin urmare, orice atacator care încearcă să se infiltreze prin rețeaua wireless trebuie să rupă 2 straturi puternice de apărare: protecția 802.11i și tunelul VPN. Tehnologia VPN poate fi folosită și pentru securizarea retelelor WLAN folosind tipul de criptare end-to-end. Punctele de acces sunt configurate pentru acces deschis fara criptare WEP, dar reteaua WLAN este izolata de LAN prin serverulVPN. Autentificarea si criptarea are loc la nivelul serverului VPN, care au rol de firewall pentru retea. Spre deosebire de cheia WEP si de adresa MAC, solutia VPN este scalabila la un numar foarte mare de utilizatori.



VPN este de preferat pentru retele mari, deoarece administratorii nu trebuie să mențină adresele MAC pentru fiecare ounct de acces. Momentul în care numărul de stații mobile devine greu de gestionat variază în funcție de capacitatea organizației de a administra rețeaua, la alegerea metodelor de securitate (SSID, WEP, și adresa MAC filtrare), precum și pe toleranța pentru risc. Dacă filtrarea adreselor MAC este utilizată pe o rețea obisnuita, limita superioară fixa este stabilit de numărul maxim de adrese MAC care pot fi programate în fiecare punct de access utilizat într-o instalație. Această limită superioară variază, dar problema practică de a utiliza manual și de a menține adrese MAC valide pentru fiecare punct de acces dintr-o rețea limitează utilizarea filtrarea adresei MAC la rețele mai mici.

Un VPN bine proiectat poate oferi beneficii considerabile pentru o organizație. Acesta poate:

- Extinde conectivitatea geografică.
- Îmbunătăți securitatea liniilor necriptate.
- Reduce costurile operaționale, în comparație cu o rețea tradițională de tip WAN.
- Reduce timpul de tranzit și costurile de transport al datelor pentru utilizatorii aflați la distanță.

- Simplifica topologia rețelei în anumite cazuri.
- Oferi oportunitățile unei rețele globale.
- Oferi compatibilitate cu rețelele de mare viteză de tip broadband.
- Oferi un *return on investment* (ROI) mai rapid decât liniile tradiționale WAN, fie proprietare sau închiriate.
- Prezenta o scalabilitate sporită, când este folosit în cadrul unei infrastructuri cu cheie publică.

Având în vedere faptul că VPN-urile sunt extinderi ale rețelei centrale (de bază), există unele implicații de securitate care trebuiesc luate în considerare cu multă atenție:

- Securitatea pe partea clientului trebuie să fie întărită. Acest procedeu poartă numele de Central Client Administration sau Security Policy Enforcement. Adeseori companiile cer angajaților care doresc să folosească VPN-ul în afara serviciului să își instaleze în prealabil un firewall oficial. Unele organizații care gestionează date importante, precum sunt cele din domeniul sănătății, au grijă ca angajații să dispună de două conexiuni WAN separate: una pentru gestionarea datelor sensibile, și a doua pentru alte interese.
- Accesul la rețeaua țintă poate fi limitat.
- Politicile de jurnalizare trebuie evaluate din nou și în cele mai multe cazuri revizuite.

O singură scurgere de informații nedorită poate duce la compromiterea securității unei rețele. În cazul în care un individ sau o companie are obligații legale privind protejarea datelor confidențiale, pot rezulta probleme legale chiar cu răspundere penală. Servesc ca exemple reglementările HIPAA adoptate în SUA în domeniul sănătății, precum și reglementările pe plan general ale UE.

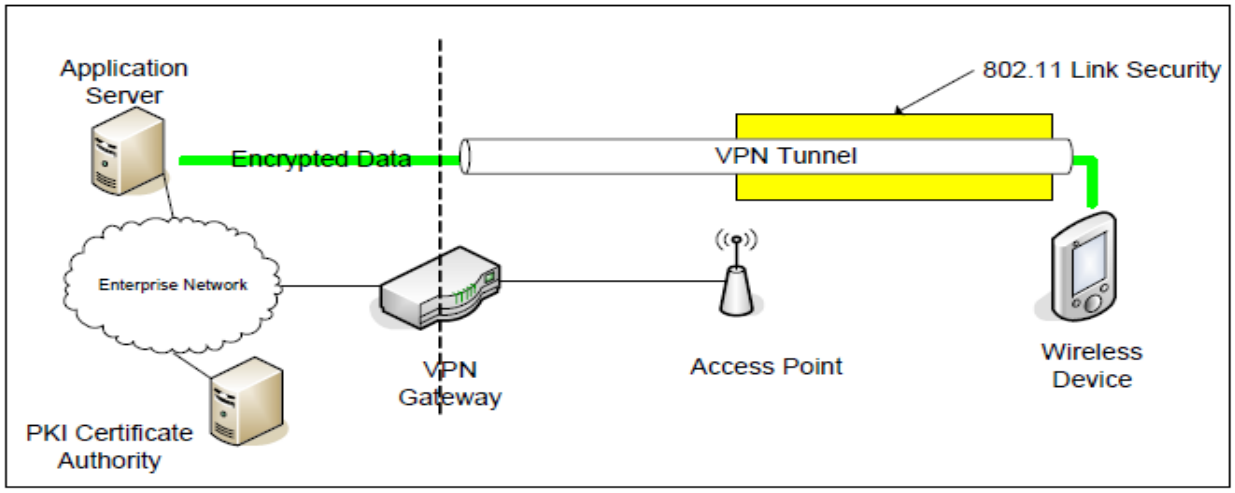
3.2 CRIPTAREA APLICATIILOR

În aplicațiile care necesită nivele mai ridicate de protecție, utilizarea algoritmilor de criptare ar trebui să fie luata în considerare pentru a proteja confidențialitatea și integritatea datelor care călătoresc de la expeditor la destinatar. În timp ce VPN și securitate 802.11 link aplică și criptarea datelor, ele nu oferă o protecție end-to-end. Datele sunt criptate de VPN și 802.11i-l atunci când călătoresc între poarta de acces VPN și terminalul client. Cu toate acestea, datele care călătoresc între rețeaua de întreprindere și poarta de acces VPN sunt transmise fara nici un fel de protectie.

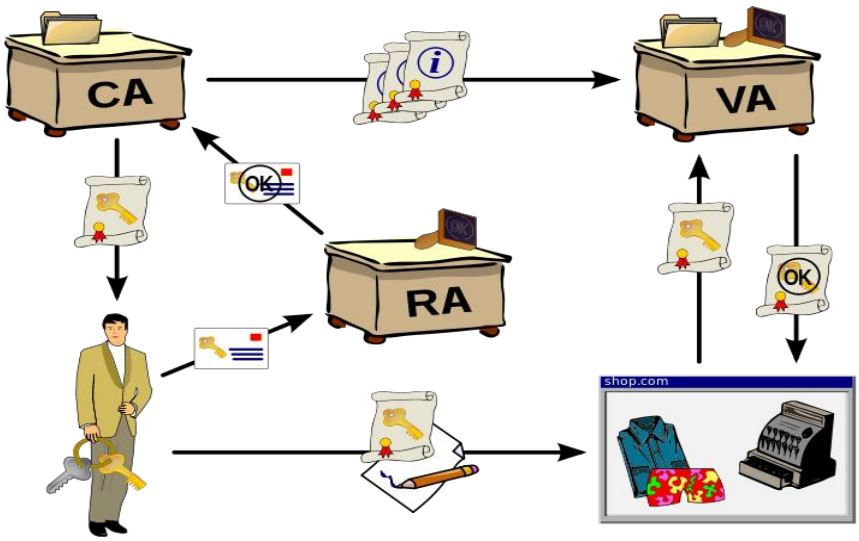
Pentru a asigura o protecție end-to-end, aplicatiile pot cripta pachetele de date înainte de a fi trimise în rețea.La primire, datele criptate vor trebui să fie decriptat cu succes, înainte ca acestea sa poata fi prelucrate. In timp ce procesele de criptare și decriptare sunt relativ simple, complexitate a sistemelor de criptare este în producția, distribuția și managementul cheilor utilizate în procesul de criptare. În prezent, Public Key Infrastructure (PKI) este frecvent utilizat în aplicațiile internet enterprise pentru criptarea datelor și de gestionare a cheilor. PKI oferă criptare puternică, precum și autentificare la fel de puternica prin semnarea digitală. Totuși,

dezavantajul PKI consta in complexitate, și necesitatea de a instala de certificate si alte infrastructuri PKI în rețea.

Figura prezintă integrarea unui sistem de criptare bazat pe PKI în arhitectura wireless. O autoritate de certificare PKI este instalata în cadrul rețelei enterprise pentru a sprijini generarea de certificate PKI pentru utilizatorii din rețea. Folosind această infrastructură, serverul de aplicație și dispozitivele wireless pot cripta datele și să comunice în siguranță end-to-end.



În criptografie, un PKI este un aranjament care se leaga chei publice cu identitatea utilizatorilor folosind o autoritate de certificare (CA). Identitatea trebuie să fie unica în cadrul fiecărui domeniu de CA. Autoritatea de validare (VA) terță parte poate furniza aceste informații în numele CA. Legarea este stabilita prin înregistrare, care, în funcție de nivelul de siguranta al legăturii, poate fi efectuata de către software-ul de la un CA sau sub supraveghere umană. Rolul PKI care asigură această legătură este numit autoritatea de înregistrare (RA), care se asigură că cheia publică este legata de utilizatorul la care este alocata.



Criptografia bazată pe chei publice trebuie însoţită de un set de politici de definire a regulilor sub care sistemele de criptografie pot opera şi de un set de proceduri care specifică modalităţile de generare, distribuţie şi utilizare a cheilor. Exista o infrastructura care stabileşte cadrul funcţional, bazat pe standarde, pentru o mare varietate de componente, aplicaţii, politici şi practici al căror scop este atingerea celor patru funcţionalităţi principale ale unei tranzacţii comerciale:

- Confidenţialitatea – menţinerea caracterului privat al informaţiei (secretizarea informaţiei)
- Integritatea – dovada că respectiva informaţie nu a fost modificată (asigurarea împotriva manipulării frauduloase a informaţiei)
- Autentificarea – dovada identităţii celui ce transmite mesajul (verificarea identităţii unui individ sau a unei aplicaţii)
- Non-repudierea – siguranţa că cel ce generează mesajul nu poate să-l denigreze mai târziu (asigurarea paternităţii mesajului)

Un **Certificat Digital** este un document ce conţine patru componente mari:

- o cheie publică
- informaţia ce leagă cheia publică de deţinătorul ei
- informaţia de validitate a certificatului
- semnatura digitală

Componente PKI

- *Autoritatea Certificatoare (CA):* responsabilă cu generarea şi revocarea certificatelor
- *Autoritatea Registratoare (RA):* responsabilă cu verificarea construcţiei generate de cheile publice şi identitatea deţinătorilor.
- *Deţinătorii de Certificate (subiecţii):* Oameni, maşini sau agenţi software care deţin certificate şi le pot utiliza la semnarea documentelor.
- *Clienţii:* ei validează semnătura digitală şi certificarea de la un CA.
- *Depozitele:* stochează şi fac accesibile certificatele şi Listele de Revocare a Certificatelor (CRLs -Certificate Revocation Lists)
- *Politicile de securitate:* definesc procesele şi principiile de utilizare a criptografiei.

Dintre **funcţiile realizate cu ajutorul PKI** putem menţiona:

Înregistrarea: este un proces în care cel ce doreşte să obţină un certificat de la CA îşi prezintă atributele sale. Acestea sunt verificate iar apoi se eliberează certificatul.

Certificarea: este procesul în care CA eliberează certificatul ce conţine cheia publică subiectului apoi îl depune într-un depozit public.

Generarea Cheilor: în multe cazuri subiectul generează o pereche de chei în mediul său, înainte de a transmite cheia publică la CA pentru certificare. Dacă CA răspunde pentru generarea cheilor, acestea sunt oferite subiectului ca un fişier criptat sau token fizic asemeni unui smartcard.

Recuperarea Cheilor: în unele implementări PKI necesită ca toate cheile schimbate şi/sau criptate să fie depuse într-un depozit securizat. Ele sunt recuperabile dacă subiectul pierde cheia, acest lucru revenind lui CA sau sistemului de recuperare.

Actualizarea Cheilor: toate cheile perechi şi certificatele lor asociate trebuie actualizate la un interval regulat. În acest sens există două situaţii care necesită acest lucru:

- Data care este specificată în certificat ca dată de expirare este depăşită şi se actualizează.
- Cheia privată a uneia din entităţi din PKI este compromisă. În acest caz PKI trebuie să anunţe că vechiul certificat nu mai este valid şi urmează să-l înlocuiască. Una din căi este de pre-generare şi stocare securizată a perechilor de chei pentru astfel de situaţii, acţiune ce duce la informarea fiecărui utilizator de acest lucru. Altă cale este metoda "out-of-band" unde cu ajutorul telefonului, faxului, scrisorii se transmite acea cheie.

Certificarea încrucişată: permite utilizatorilor dintr-un domeniu administrativ să utilizeze certificate generate de un CA operaţional în alt domeniu. Procesul implică un CA (CA_1) ce oferă o certificare pentru alt CA(CA_2). Acest certificat conţine cheia publică CA asociată cu cea privată pe care CA_1 o utilizează, lucru ce permite subiecţilor certificaţi prin CA_2 să accepte certificatele generate de CA_1 sau orice CA subordonat.

Revocarea: apare în momentul expirării perioadei de validitate care poate apărea când: subiectul îşi schimbă numele, angajatul părăseşte compania, cheia privată este compromisă. În cadrul standardului X.509, pentru a revoca un certificat se utilizează Lista Revocărilor Certificatelor (CRL – Certificate Revocation List). Această listă identifică certificate şi sunt semnate de CA.

Există diferite tipuri de sisteme într-un PKI:

- Sisteme cheie private și publice: sisteme private folosesc criptografie simetrică și sisteme publice folosesc criptografia asimetrică. În prezent, sistemele de chei publice sunt cele mai comune.
- Simetrice de criptare Systems: aceeași cheie este utilizat atât pentru procesele de criptare și decriptare.
- Sisteme de criptare asimetrice: O altă cheie este utilizată pentru fiecare proces. O cheie este cheia publică și alte cheia este cheia privata. Dacă ceva este criptat cu cheia publică, atunci decriptare se poate face numai cu cheia privată. Alternativ, în cazul în care ceva este criptat cu cheia privată, apoi decriptare trebuie să se facă numai cu cheia publică.

Există două categorii de criptare: criptarea simetrică și cea asimetrică. Principala deosebire dintre cele două metode este aceea că un sistem de criptare simetric folosește aceeași cheie pentru operațiile de criptare și decriptare, pe când criptarea asimetrică folosește chei diferite.

Modelul cifrului simetric este alcătuit din următoarele componente :

- Textul original, simplu, este mesajul inteligibil care conține datele transmise, fiind aplicat la intrarea algoritmului.

- Algoritmul de criptare, care aplică diverse operații de substituție și de transformare a textului original.
- Cheia secretă este a doua sursă de intrare a algoritmului, fiind independent de text și de algoritm. Cheia va fi folosită în operațiile de criptare și va conduce la un rezultat distinct.
- Textul criptat este mesajul rezultat în urma criptării, depinzând de textul original și de cheia secretă utilizată.

Algoritmul de decriptare este varianta inversă a algoritmului de criptare, având ca date de intrare textul criptat și aceeași cheie secretă.

Avantajele PKI

Iată câteva din avantajele imediate pe care le aduce o implementare a unei infrastructuri PKI la nivel organizaţional:

• Securizarea mesageriei electronice

Cea mai mare parte a interacţiunilor derulate prin Internet se realizează prin intermediul mesageriei electronice. Această activitate presupune însă acceptarea unui grad ridicat de risc, prin expunerea unor informaţii confidenţiale şi prin posibilitatea substituirii autorului unui mesaj sau chiar alterarea voită a conţinutului mesajului.

• Sistem de administrare a documentelor şi semnătură digitală

O parte importantă a aplicaţiilor software se referă la procesarea şi arhivarea documentelor în format electronic. Deşi aceste sisteme contribuie la diminuarea dificultăţilor în prelucrarea şi arhivarea unui volum mare de documente, ele nu rezolvă complet trecerea de la documente în format tradiţional la documente electronice. Ceea ce lipseşte este posibilitatea de a semna aceste documente electronice şi de a asigura în acest fel non-repudierea acestora.

• Securizarea aplicaţiilor Intranet şi Extranet

Din ce în ce mai multe companii şi organizatii tind să-şi transfere procesele de interacţiune către aplicaţii care rulează în mediul Internet. Indiferent dacă acestea se referă la relaţia cu proprii angajaţi şi procesele interne ale organizaţiei (aplicaţii Intranet), sau sprijină interacţiunea cu partenerii şi clienţii (aplicaţii Extranet), aceste aplicaţii îşi demonstrează din plin eficienţa prin reducerea masivă a costurilor şi îmbunătăţirea eficienţei. Pe măsură însă ce aceste informaţii sunt transferate către sistemele şi aplicaţiile Intranet/Extranet, riscul de securitate informaţională creşte semnificativ, în primul rând datorită faptului că Internetul reprezintă prin natura sa un mediu public.

• Criptarea datelor şi a documentelor

Securitatea datelor nu se referă numai la momentul în care acestea sunt utilizate într-un proces informaţional, ci şi la stocarea lor. Păstrarea confidenţialităţii şi integrităţii acestora îmbracă numeroase aspecte, care se referă atât la autentificarea accesului cât şi la criptarea lor astfel încât să nu poată fi utilizate în cazul unui acces neautorizat.

• Autentificare la nivelul sistemului de operare şi al aplicaţiilor

Autentificarea prin nume şi parolă este soluţia cea mai vulnerabilă şi în plus, obligă utilizatorul la memorarea unei astfel de combinaţii pentru fiecare aplicaţie folosită. Folosirea

certificatului digital stocat pe smartcard contribuie nu numai la creşterea gradului de siguranţă dar şi la o utilizare mai facilă, prin folosirea unui mijloc unic de autentificare pentru toate aplicaţiile folosite.

X.509 este un stardad proiectat de ITU pentru certificare. Acesta este folosit pe scare larga in internet si a aparut in anul 1998, acum fiind la cea de a treia versiune. X.509 a fost foarte mult influenţat de lumea OSI, împrumutând unele din cele mai proaste trăsături (ex. politica de nume şi codificarea). În mod surprinzător, IETF a fost de acord cu X.509, chiar dacă în alte domenii, de la adresele maşinilor la protocoalele de transport şi formatul poştei electronice, IETF ignoră OSI şi încearcă să facă lucrurile corect. Versiunea IETF pentru X.509 este descrisă în RFC 3280.

/c=US/O=MoneyBanc/OU=Loan/CN=Bob/ - exemplu X.500

În principal, X.509 este o modalitate de a descrie certificate. Câmpurile principale dintr-un certificat sunt listate in figura. Certificatele sunt codificate folosind OSI ASN.1 (eng.: Abstract Syntax Notation 1, rom.: Notaţia sintactică abstractă 1), care poate fi văzută ca o structură C, cu excepţia unei notaţii foarte specifice şi detaliate.

Câmp	Semnificație
Versiune	Ce versiune de X.509 este utilizată
Număr Serial	Acest număr împreună numele CA-ului identifică în mod unic certificatul
Algoritm de semnare	Algoritmul folosit la semnarea certificatului
Emitent	Numele X.500 al CA-ului
Perioada de validitate	Momentele de început și sfârșit ale perioadei de validitate
Numele subiectului	Entitatea care este certificată
Cheia publică	Cheia publică a subiectului și ID-ul algoritmului folosit
ID emitent	Un identificator opțional identificând în mod unic emitentul certificatului
ID subiect	Un identificator opțional identificând în mod unic subiectul certificatului
Extinderi	Au fost definite mai multe extinderi
Semnătura	Semnătura certificatului (semnat cu cheia privată a CA-ului)

Certificate SSL / TLS şi VPN-uri

Certificatele SSL/TLS se folosesc exact în acelaşi mod ca şi VPN-urile – este definită sau creată o autoritate de certificare şi toate certificatele valabile eliberate de către această autoritate sunt acceptate pentru VPN. Fiecare client trebuie să aibă un certificat valabil, eliberat de acest CA şi astfel îi este permis să stabilească o conexiune la VPN. O listă de revocare a certificatelor (CRL) poate fi folosită pentru a revoca certificatele care aparţin clienţilor cărora nu le mai este permis să se conecteze la VPN. Acest lucru poate fi realizat fără configurarea pe nici un client, pur şi simplu, prin crearea pe server a unei liste corespunzătoare de revocare. Acest lucru este foarte util atunci când un laptop este furat sau accesat neautorizat.

O organizaţie ce foloseşte o cheie prestabilită trebuie să introducă această cheie pe fiecare sistem cu care se conecteaza la serverul VPN. Cheia trebuie să fie schimbată pe toate sistemele în cazul în care un sistem sau o cheie sunt pierdute. Dar, dacă se folosesc certificate cu liste de revocare, tot ce trebuie făcut este să se treacă certificatul de pe sistemul furat sau

compromis pe CRL-ul serverului. Atunci când acest client încearcă să se conecteze la server, accesul va fi interzis.

Conexiunile sunt refuzate în cazul în care:
• Nu este prezentat nici un certificat,
• Este prezentat un certificat de la un CA greşit,
• Este prezentat un certificat revocat.
Aceste certificate pot fi utilizate în scopuri multiple. HTTPS şi OpenVPN sunt doar două aplicaţii cu o varietate bogată de posibilităţi. Alte sisteme VPN (cum ar fi IPsec), servere de web, servere de mail, şi aproape fiecare altă aplicaţie server poate utiliza aceste certificate pentru a autentifica clientii. Dacă această tehnologie este înţeleasă şi aplicată în mod corect, atunci s-a atins un grad foarte ridicat de securitate.

3.3 Concluzii

Pe lângă siguranța oferita de tunelul VPN și mecanismele 802.11i, calitatea unei rețele de întreprindere poate fi sporită prin folosirea tuturor tehnologiilor curente:

Monitorizare

Un instrument de monitorizare a rețelei ar trebui să fie utilizat în arhitectura pentru a monitoriza și a analiza traficul care curge prin rețea. Implementarea unui sistem de monitorizare este esențială pentru detectarea în timp util a atacurilor. Există cateva companii care oferă monitorizare și instrumente de detectare a intruziunilor pentru rețele wireless, cum ar fi AirDefense Network Chemistry and Red-M.

Multi-Factor Authentication

Acest model de autentificare intareste sistemul prin adaugarea unor atribute personale in profesul de autentificare, cum ar fi parole, dar si elemente fizice de tipul cardurilor sau cheilor si elemnte biometrice.

Chiar daca retelele wireless inca au de recuperat in privinta sigurantei, comparativ cu retelele wired, evolutia tehnologiei catre mobilitate a fortat companiile din domeniu sa creeze noi standarde si tehnologii pentru a sporii securitatea retelelor. Rețele fără fir oferă beneficiile mobilității pentru intreprinderi, dar pot deveni o problema de securitate în cazul în care nu a asigurat în mod corespunzăto. O buna punere în aplicare a sistemelor de securitate adecvata poate proteja rețeaua wireless suficient pentru a fi utilizate în întreprindere

Un criteriu important în dezvoltarea unei tehnici de securitate este asigurarea compatibilităţii cu echipamentele deja existente pe piaţă, pentru a asigura o continuitate în

menţinerea confidenţialităţii datelor. Chiar dacă un algoritm este performant, dar necesită putere de calcul suplimentară faţă de cea oferită de echipamentele deja pe piaţă, un factor decisiv în adoptarea sa îl constituie costul de înlocuire 16 al unei întregi infrastructuri. De multe ori, companiile preferă să utilizeze tehnologii mai slabe, decât să schimbe întreaga reţea de echipamente.

4.Bibliografie

Capitolul 1

[1]. Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone, “Establishing Wireless Robust Security Networks” - http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
[2]. http://ro.wikipedia.org/wiki/Re%C8%9Bea_f%C4%83r%C4%83_fir
[3]. http://andrei.clubcisco.ro/cursuri/3rl/razvan/RL_curs05.pdf
[4]. http://oana15.wordpress.com/2010/04/12/avantajele-retelelor-wireless/
[5]. Primer for Wi-Fi by Cisco.pdf
[6]. RETELE MOBILE SI TEHNOLOGII WIRELESS.doc
[7]. http://www.comm.pub.ro/_curs/cmt/cursuri/CMT%2009%20wlan.pdf

Capitolul 2

[1].[Borisov 2002] Nikita Borisov, Ian Goldberg, David Wagner,“ Intercepting Mobile Communications: The Insecurity of 802.11-Draft”. http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf]
[2]. [Bersani 2004] Bersani, “EAP Shared Key Methods: A Tentative Synthesis of Those Proposed So Far” http://ietfreport.isoc.org/idref/draft-bersani-eap-synthesis-sharedkeymethods/
[3]. [Edney & Arbaugh 2004] Jon Edney and William A. Arbaugh. “Real 802.11 Security, WiFi Protected Access and 802.11i”. Addison Wesley 2004
[4] .“Securing WLANs using 802.11i”, Ken Masica, Lawrence Livermore National Laboratory, February 2007
[5]. "Wireless Network Security Threats " , http://www.techfaq.com/wireless-connectionsecurity.html
[6]. “Cryptography and Network Security Principles and Practices, Fourth Edition”, William Stallings, Prentice Hall, November 200
[7]. http://www.securitatea-informatiilor.ro/solutii-de-securitate-it

Capitolul 3

[1]. WIRELESS NETWORK SECURITY: DESIGN CONSIDERATIONS FOR AN ENTERPRISE NETWORK, Oh Khoon Wee, 2004
[2]. THE SECURITY ASPECTS OF WIRELESS LOCALAREA NETWORK (WLAN), Thoetsak Jaiaree, 2003
[3]. http://en.wikipedia.org/wiki/Vpn
[4]. http://en.wikipedia.org/wiki/Public-key_cryptography
[5]. http://www.technopedia.com