CORSO DI RETI DI CALCOLATORI Prof. ORAZIO MIRABELLA

Principi di progettazione di reti geografiche di trasporto wireless

1. **Definizione dB, dBm, EIRP,BER**
2. **Leggi propagazione elettromagnetica: Equazioni di Friis e loro applicazioni pratiche :Propagazione in line of sight**
3. **Ellissoide di Fresnel,**
4. **Esempi di propagazione NLOS :Knife edge attenuation**
5. **Calcolo del SOM di una tratta radio a microonde ed equazioni di dimensionamento**
6. **Calcolo della affidabilità del link (Reliability)**
7. **Descrizione degli apparati:AP,Bridge,Repeater,WDS**
8. **Performance dei vari protocolli: CCK, DSS, FHSS, OFDM**
9. **Problematiche di sicurezza su reti radio: WEP, WPA, 802.1x, EAS, EAP, RADIUS**
10. **Laboratorio**
    - Strumenti informatici di dimensionamento tratte radio:Radio Mobile
11. **Bibliografia**

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

1.Definizione dBi, dBd, dBm, EIRP, BER

Prima di passare ad introdurre le equazioni fondamentali che governano la propagazione delle onde elettromagnetiche occorre definire le grandezze fondamentali usate per valutare l'attenuazione , il guadagno e la soglia statica di un ricevitore.

Guadagno di un antenna

Il **dB** è la grandezza logaritmica usata per caratterizzare il guadagno di un'antenna. Normalmente ci si riferisce alla sorgente ISOTROPA , ovvero all'antenna ideale che irradia in tutte le direzioni in maniera uniforme allora si parla di **dBi ,** ma spesso nei data sheet dei costruttori è possibile trovare il guadagno espresso in **dBd** ovvero dB rispetto al dipolo. In tal caso occorre sommare 2,15dB al valore espresso per riportarlo in dBi:

$$dBd = dBi - 2{,}15$$

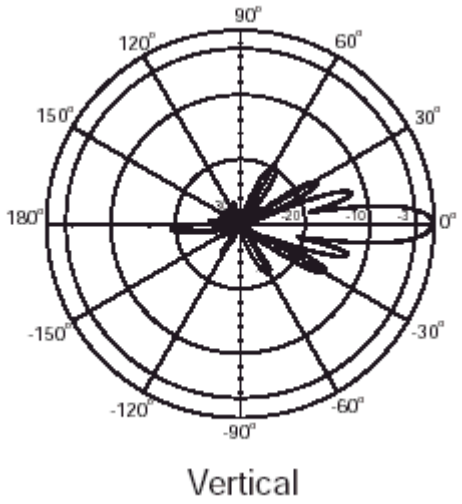
es**:** il vendor A ci dice che nella direzione di massimo guadagno la sua antenna ha un G= 10 dbi mentre il vendor B riporta nel suo dsta sheet G=9dBd. Alla luce di quanto visto:

antenna A G = 10dBi

antenna B G= 9 dBd= (9+2,15) dBi= 11,15 dBi

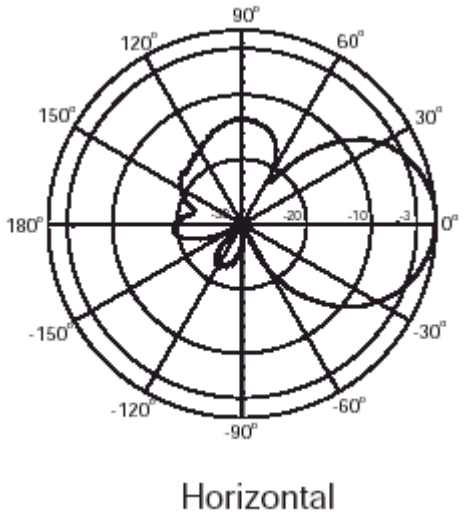
Quindi B è più performante di A.

Quando si parla di guadagno occorre specificare l'angolo **θ** rispetto alla piano normale che contiene l'antenna. Per **θ= 90°** il guadagno è massimo e coincide con il dato di targa dell'antenna stessa. Se **θ varia** anche il guadagno si riduce secondo la legge che caratterizza il diagramma di radiazione dell'antenna in oggetto. Normalmente , da un punto di vista progettuale, si considera il fascio a -3dB cioè a metà potenza sul piano H e V. Tale valore espresso in gradi chiamato Beamwidth (BW) ci permette di calcolare nei sistemi punto-punto e punto-multipunto il degrado di guadagno che si ha allontanandosi dalla normale rispetto al piano dell'antenna. Per maggiore chiarezza analizzamo il diagramma di radiazione sul piano verticale di un'antenna commerciale. Le circonferenze rappresentano valori differenti di guadagno decrescente verso l'interno. Si nota la circonferenza a -3 dB e quella a -10dB. L'intersezione con il diagramma di radiazione dà il BW.



Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

Nella valutazione delle caratteristiche occorre considerare la polarizzazione del vettore Campo Elettrico del segnale irradiato:



- **Lineare Verticale**
- **Lineare Orizzontale**
- **Circolare destra o sinistra RHCP , LHCP**

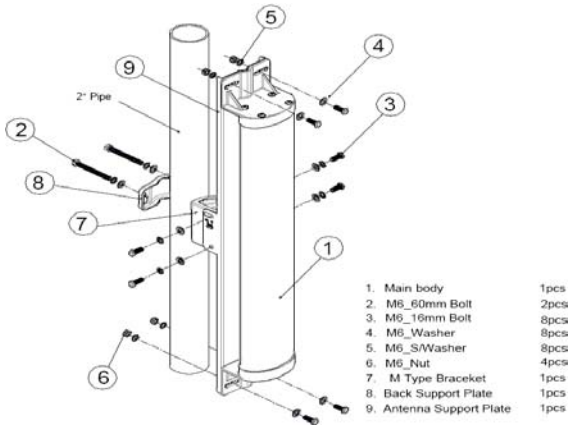
Di solito per le reti di distribuzione a lunga distanza si usa la lineare orizzontale , per le reti di accesso degli utenti la polarizzazione lineare verticale , in caso di percorsi affetti da scattering o multipath la circolare RHCP,LHCP. Occorre porre molta attenzione affinché le antenne di un sistema utilizzino lo stesso tipo di polarizzazione poiché qualora Sorgente e Destinatario usino polarizzazione diversa si avrebbero delle attenuazioni aggiuntive sul segnale di oltre 20 dB non contemplate nelle leggi di propagazione elettromagnetica. Esempi di antenne commerciali sono:

- **Yagi (10<G<18 dbi)** dal nome degli scienziati Uda-Yagi che ne teorizzarono il comportamento. Esse sono costituite da un elemento radiante detto **dipolo,** da un riflettore posto dietro il dipolo ad una opportuna distanza che è strettamente legata alla lunghezza d'onda , e da un certo numero di altri elementi passivi detti **direttori.** L'elemento che meccanicamente sostiene riflettore, dipolo e direttori si chiama **boom .** Sono caratterizzate da una elevata direttività **,** ovvero guadagno nella direzione **θ= 90° ,** superata solo dalle antenne con riflettore parabolico.
- **Antenne a Pannello o settoriali (8<G<13 dBi) ,** sono quelle che normalmente vediamo nelle BTS della telefonia cellulare. Hanno discreti guadagni a fronte di BW di 60°,90°,120° sul piano orizzontale e BW da 5° a 15° sul piano verticale. Sono indicate nella realizzazione di WiPOP (Wireless Point of Presence) e permettono la creazione di una rete di accesso WiFi simile alla rete cellulare. Con 3 AP e tre pannelli a 120° riesco ad illuminare a 360° un WiPOP.
- **Antenne verticali Omnidirezionali (6<G<10 dBi)** hanno un diagramma di radiazione ominidirezionale sul piano orizzontale e di 10-15 gradi sul piano verticale . Sono indicate

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

solo per celle a bassa densità di utenti . A causa del ridotto guadagno le zone di copertura da esse create si limitano a poche centinaia di metri attorno all'AP.

8 dBi Omni Antenna **Pannello da 13dBi 120°**



- **Antenne paraboliche (18< G < 34 dBi)** sono le antenne universalmente utilizzate per i collegamenti punto-punto a lunga distanza i cosiddetti TRUNK. Esse sfruttano la proprietà geometrica della parabola di concentrare tutti i raggi provenienti dall'infinito in un punto detto Fuoco. Facendo ruotare la parabola attorno al proprio centro di ottiene un paraboloide di rotazione. L'elemento radiante (detto FEED) viene posto nel fuoco ed è progettato in modo da illuminare la parabola con una densità di energia decrescente verso il bordo (tapering a -10 dB). Commercialmente sono classificate come Primo Fuoco od Offset. Nel caso di piccoli diametri si preferisce la geometria Offset (es. ricezione DVB sat) per minimizzare gli effetti di blocking generati dal FEED. Di solito hanno BW di pochi gradi (1°-4°) decrescenti al crescere del guadagno e della frequenza di lavoro.

  Dopo questa carrellata sui tipi di antenna normalmente utilizzati nel settore delle telecomunicazioni definiamo altre grandezze utili per parametrizzare un collegamento radio .

  Si definisce dBm (dB rispetto al milliwatt) grandezza data da:

$$\mathbf{dbm = 10\ log_{10}(P_{milliwatt} / 1mw)}$$

es: ho un trasmettitore che eroga 100mw a quanti dBm corrispondono**:**

$$\mathbf{dBm = 10\ log_{10}(100/1) = 10 * 2 = 20dBm}$$

viceversa se conosco che il mio tx eroga 17,5 dBm a quanti milliwatt corrispondono?

$$\mathbf{P_{milliwatt} = 10^{(dBm/10)} = 10^{(17,5/10)} = 56,23\ milliwatt}$$

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

Il vantaggio è che nelle equazioni che governano la propagazione delle onde radio e di bilancio energetico posso sommare algebricamente attenuazioni (-dB) , guadagni (+dB) e potenze (dBm). Un'altra grandezza utilizzata in campo RF è la potenza **E.IR.P.**

La potenza **E.IR.P** (Effective Irradiated Power) è definite come la somma algebrica della potenza del trasmettitore espresso in dBm all'ingresso dell'antenna più il guadagno dell'antenna stessa espressa in dBi.

Esercizio : calcolare la E.IR.P di un sistema costituto da un trasmettitore, un cavo coassiale che collega il trasmettitore all'antenna e da una antenna Yagi con guadagno di 20 dBd. Il trasmettitore eroga 200mw di potenza RF, il cavo per microonde è lungo 20mt. ed attenua il segnale alla frequenza di esercizio di 4dB.

Dalla definizione di EIRP

EIRP = Ptx(dBm) – attenuazione del cavo + Guadagno Antenna

$10\log_{10}(200/1) – 4dB + (20 +2,15)$ dbi $= 23 – 4 + 22,15 = 41,15$ dBm

Se volessi conoscere la potenza irradiata lungo la direzione di massimo guadagno:

$P_{milliwatt} = 10^{(41,15/10)} = 13031$ mw = **13 ,03 Watt**

Ultima grandezza da considerare è il **B.E.R. (bit error rate).** Tale grandezza è legata alla sensibilità dei ricevitori, alla potenza del segnale in ingresso, e alla capacità di decodificare un segnale da parte del ricevitore con un numero di errori minori di una certa quantità prefissata

Si esprime nella forma :

-xx dBm con BER 10^{-6}

esempio : i ricevitori per wlan integrati negli AP hanno una sensibilità di

-77dBm@36Mbit/s con BER 10^{-6} ciò mi dice che se la potenza incidente è maggiore -77dBm avrà la certezza che gli errori di decodifica saranno meno di $1/10^6$

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

2. Leggi propagazione elettromagnetica: Equazioni di Friis e loro applicazioni pratiche:Propagazione in line of sight

Nella progettazione di reti di accesso e distribuzione geografiche si tiene in considerazione come ipotesi progettuale la propagazione del segnale in termini di L.O.S. (line of sight) . Ciò porta delle semplificazioni in termini di progettazione poiché si adottano delle metodologie sedimentate che portano a dei risultati pratici molto vicini ai calcoli teorici.
Il modello matematico universalmente utilizzato, nell'ipotesi di semplice propagazione L.O.S. è quello espresso della legge di **Friis che ci permette di calcolare il path-loss $L_{p(dB)}$:**

(nel caso di distanza in miglia) $L_{p(dB)} = -(36{,}57 + 20\log(F) + 20\log(D))$

(nel caso di distanza in chilometri) $L_{p(dB)} = -(32{,}44 + 20\log(F) + 20\log(D))$

$L_{p(dB)}$= attenuazione in dB della tratta radio, da cui il segno meno nell'espressione di Friis
F = frequenza di lavoro dell'impianto espressa in MHz
D= Distanza tra trasmettitore e ricevitore espresso in Km o miglia (1 mile= 1,609344 Km)

Tale modello risulta approssimato perché non tiene conto di altri fattori variabili e dipendenti dalle condizioni ambientali e dalla frequenza di lavoro che introducono delle attenuazioni aggiuntive. Per tener conto di questi altri fattori che introducono attenuazione sulla tratta radio occorre sommare a $L_{p(dB)}$ altri termini K_i :

Legge di Friis nella formulazione generale:

$$L_{p(dB)} = -(32{,}44 + 20\log(F) + 20\log(D) + K_{Fresnel} + K_{Rain} + K_{Ossigeno} + K_{Vapore\ acqueo} + K_{Ostacoli})$$

Innanzitutto occorre considerare l'attenuazione aggiuntiva introdotta dalla parziale occlusione delle zone di **Fresnel.**

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

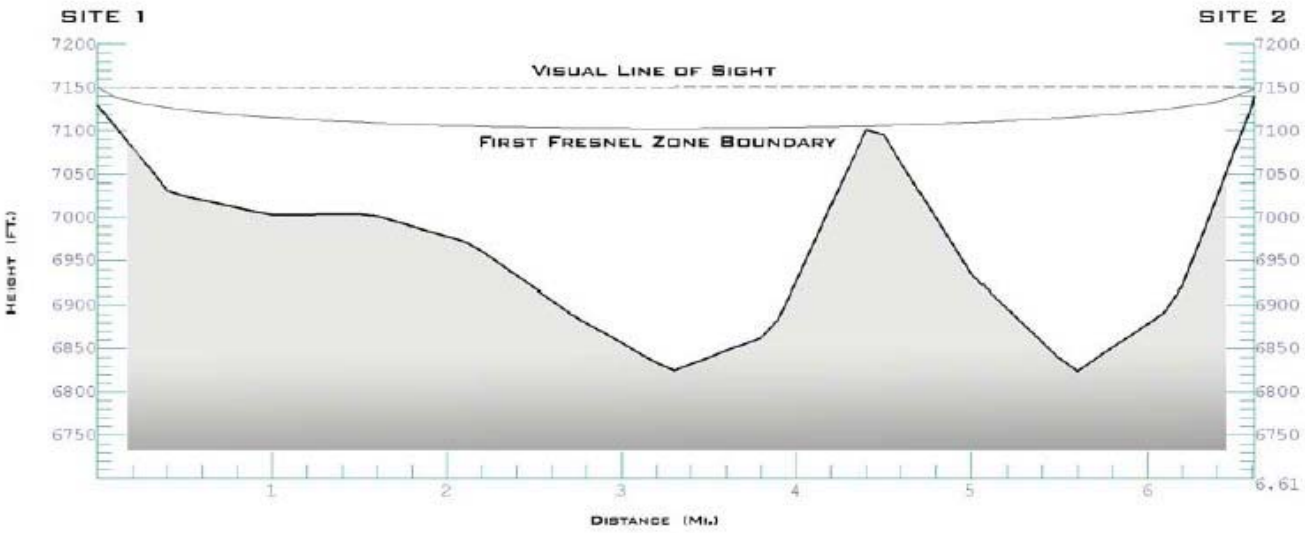
3.Ellissoide di Fresnel ($K_{Fresnel}$)

Si definisce ellissoide di Fresnel il volume di spazio racchiuso dall'elissoide che ha le due antenne trasmittente e ricevente agli estremi del radio link poste nei fuochi. Una rappresentazione in 2D della zona di Fresnel è data dall'immagine seguente:

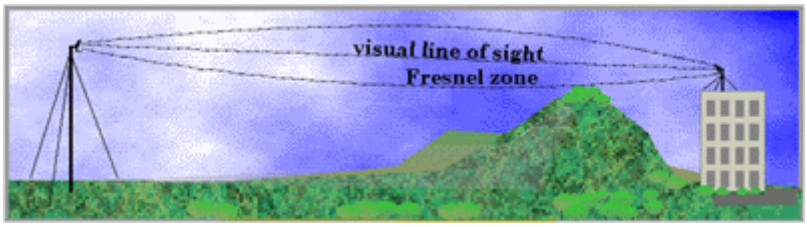
La superficie dell'elissoide è definita dal percorso ACB, che differisce dal percorso AB di **nλ/2** dove **λ** è la lunghezza d'onda (data dal rapporto c/f c=300, f = MHz). Da un punto di vista fisico occorre fare le seguenti considerazioni: luce e onde radio sono onde elettromagnetiche la cui unica differenza è la lunghezza d'onda. Nel caso della luce **λ** è molto piccola pertanto al centro del percorso tra A e B la larghezza dell'elissoide è di pochi mm. Diverso è il discorso alle frequenze di lavoro delle W-LAN le cui **λ** sono di 12,2 cm e 6cm **.** Può accadere infatti che un site-survey di un sito mediante una osservazione visiva tramite un cannocchiale ci indichi la fattibilità del collegamento poiché le due postazioni sono in visibilità ottica , mentre nella realtà i risultati sperimentali e la pratica ci mostrano spesso comportamenti (scarse performance in termini di throughput, segnale evanescente , attenuazioni che differiscono dalla previsione della legge di Friis) diversi da quanto previsto dai calcoli numerici. Ciò è dovuto a fenomeni di diffrazione che impattano pesantemente sulla propagazione delle onde radio nella regione delle microonde (2,4 GHz e 5,4GHz) in presenza di ostacoli lungo il percorso. Le leggi che regolano la propagazione di onde millimetriche sono simili a quelle dell'ottica geometrica , la loro descrizione esatta esula dagli scopi di questo lavoro, ciò che ci interessa da un punto di vista Ingegneristico è la loro conoscenza e quantificazione in termini di attenuazione aggiuntiva e come porvi rimedio a priori durante la fase di dimensionamento e progettazione della tratta radio. Si era detto che i percorsi possibili da A a B differivano dal percorso principale di **nλ/2.** Al crescere di n (n=1,n=2 ecc.) si generano tanti ellissoidi aventi i fuochi in A e B. Ai fini dei calcoli che faremo occorre considerare **solo n=1** cioè solo il primo ellissoide di Fresnel detto anche **F1 (nei sacri testi…).** E' stato dimostrato che se almeno il **60% del volume** generato dal primo ellissoide di Fresnel è libero da ostacoli la

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

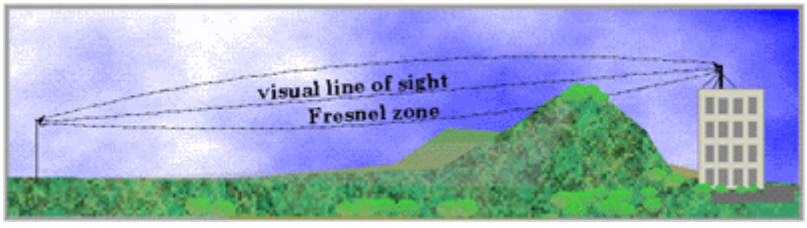
propagazione si può considerare di tipo L.O.S. e il termine $\mathbf{K_{Fresnel}}$ **essere approssimato a zero**. Questo è il caso ideale mostrato nella immagine seguente:



Nei casi reali occorre poter valutare l'impatto sul path loss dovuto ad ostacoli lungo il percorso che penetrano dentro il primo ellissoide dando luogo a fenomeni diffrattivi e quindi attenuazione aggiuntiva rispetto ai valori calcolati con la formula di Friis in forma semplice. Poter prevedere l'entità dell'ostruzione ci permette di calcolare di quanto elevare i supporti delle antenne per riportare in condizioni di **clearance la F1** o qualora i risultati fossero irrealizzabili nella pratica dove riposizionare le antenne stesse al fine di rendere possibile il collegamento.



Le immagini mostrano le due situazioni di clearance e ostruzione della F1



Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

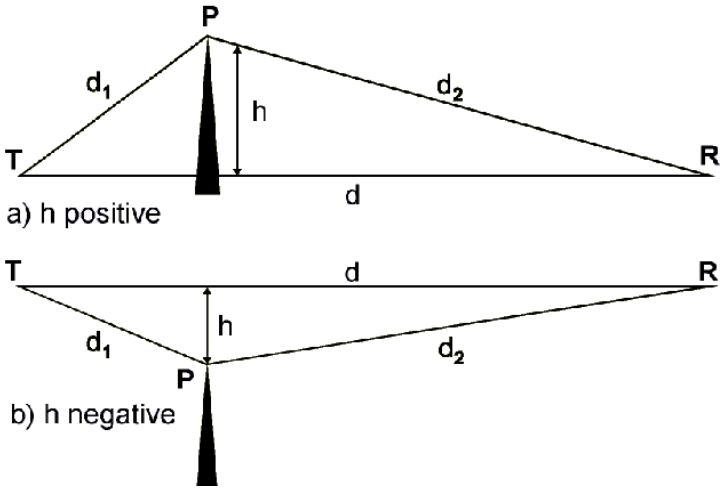
Al fine di poter valutare le perdite aggiuntive dovute all'ostruzione della F1 occorre valutare un parametro adimensionale **v** dato da :

$$v = 2\sqrt{\frac{\Delta d}{\lambda}}$$

La grandezza **Δd** data da:

$$\Delta d = d_1 + d_2 - d$$

Rappresenta la differenza tra il percorso dell'onda, che andando dal trasmettitore T al ricevitore R, compie toccando la punta dell'ostruzione P . Vi sono due casi di ostruzione **h>o** allora siamo in una condizione di **N.L.O.S. ovvero di percorso diretto bloccato** che verrà trattata con altre formule, **h<0** che invece è il nostro caso con ostruzione dell'elissoide di Fresnel.



Il valore di **v** calcolato **si assumerà** , di conseguenza , positivo se h>0 e negativo se h<0 , se h=0 ovvero l'ostruzione sfiora il percorso diretto **v=0 .** Si dimostra che in questo caso $\mathbf{K_{Fresnel}}$**= - 6dB** ovvero l'intensità del segnale è attenuata del 75% infatti **:**

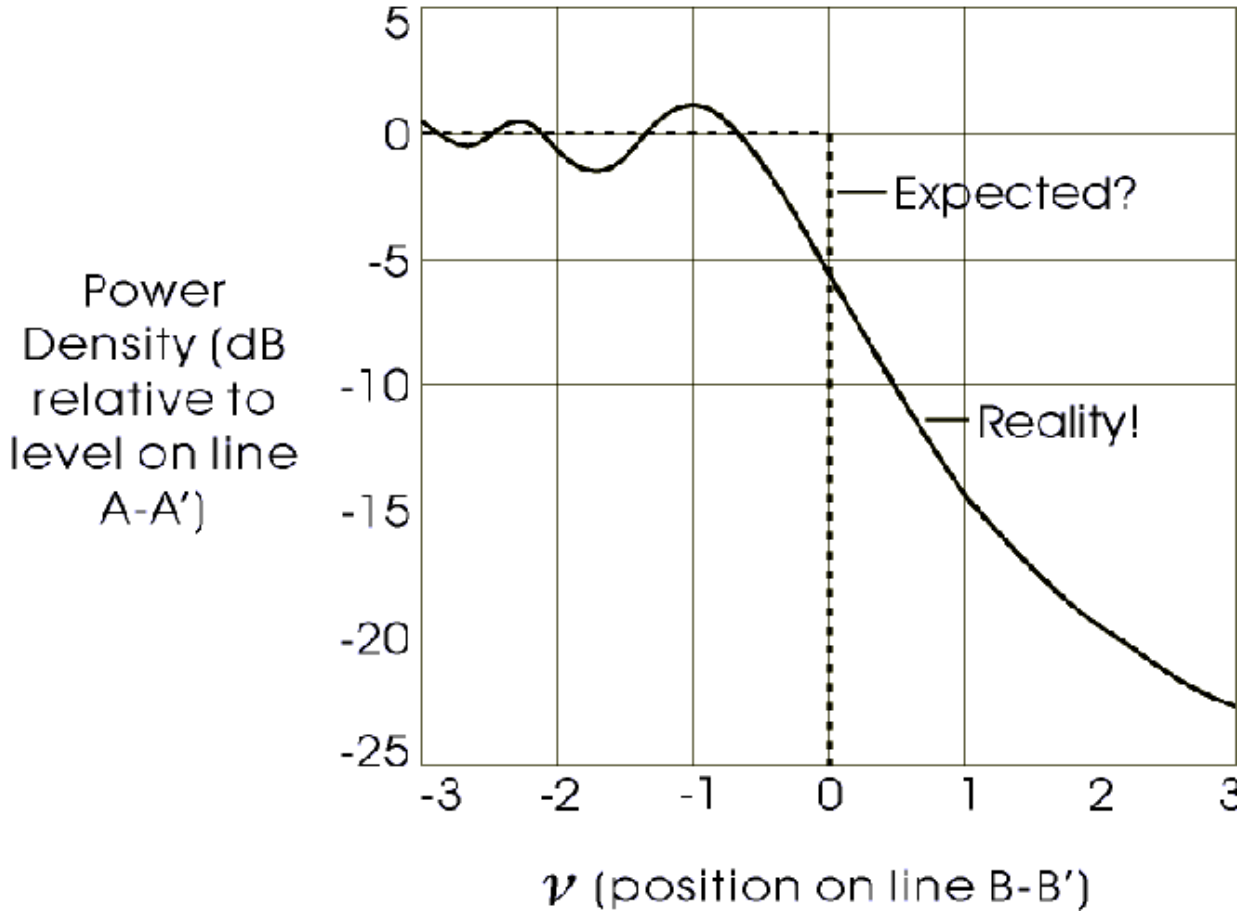
$$-6dB = 10 \log(P_{in}/P_{out})$$

da cui segue :

$$P_{out} = P_{in} * 10^{(-6/10)} = 0{,}2511 * P_{in}$$

con $\mathbf{P_{out}}$ intensità del segnale dopo l'ostacolo e $\mathbf{P_{in}}$ intensità del segnale prima dell'ostacolo. Questo è il caso , che spesso si incontra nella realizzazione di M.A.N. , dei tetti dei palazzi che sfiorano il percorso tra 2 siti e che otticamente rendono possibile il collegamento ma causano attenuazione aggiuntiva nella regione delle microonde. Per determinare il valore di attenuazione in qualunque caso (con h<0) occorre determinare prima il valore di h che ci determina la clearance della F1, che dipende dalla posizione considerata all'interno del percorso da T a R. Se dai calcoli l'ostacolo penetra all'interno dell'ellissoide potremo valutare dal grafico seguente, ricavato dalle soluzioni delle equazioni di Fresnel , il valore di attenuazione aggiuntiva $\mathbf{K_{Fresnel}}$. Ricavato **v** numericamente mediante semplice interpolazione potremo trovare in ordinata il valore di attenuazione aggiuntiva:

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net



Dall'andamento della curva si possono fare le seguenti considerazioni:

Si è detto che ai fini della valutazione dell'attenuazione di Fresnel ci basta valutare la F1 ovvero la prima zona Fresnel. Con n=1(F1) si ha che **nλ/2= λ/2** la differenza di cammino tra T e R vale solo :

$$\Delta d = d_1 + d_2 - d = \lambda/2$$

Per cui sostituendo nella espressione di

$$v = 2\sqrt{\frac{\Delta d}{\lambda}}$$

Si ricava per **v:** **v= - 1,414**

Interpolando nel grafico si ha un valore di attenuazione prossima a **0 dB.**

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

Altri valori notevoli di **ν** sono **ν= -1** ricavato con **Δd= λ/4** per il quale si ha a una intensificazione del segnale pari a **1,2dB** rispetto al valore calcolato con la legge di Friis in LOS, e **ν= -0,85** cui corrisponde una attenuazione di **0 dB. Si dimostra che ν= -0.85 corrisponde a garantire il 60% di clearance della F1 . Se in fase di progetto riesco a garantire il 60% di clearance della prima zona di Fresnel avrò la certezza di non avere attenuazione aggiuntiva dovuta a fenomeni di diffrazione dell'onda elettromagnetica.**

Cio si traduce in un'accurata scelta dei siti ove ospitare le antenne e al calcolo dell'altezza dei supporti d'antenna. Vediamo di legare il parametro **ν** all'effettiva altezza degli ostacoli ricavata in maniera opportuna. Vi sono diverse metodologie progettuali per arrivare a tali risultati, la prima è quella basata su misure altimetriche e di distanza effettuate con normali GPS portatili , la seconda è quella di realizzare delle simulazioni numeriche con opportuni CAD a RF, che permettono di simulare a partire dai dati altimetrici di tipo **SRTM** (Shuttle Radar Topography Mission) l'andamento altimetrico dei luoghi. Alla fine i dati ricavati dall'analisi del territorio e i risultati delle simulazioni numeriche devono essere correlati entro i limiti dell'approssimazione dei dati SRTM. Una considerazione importante da fare è la zona di Fresnel è una sorta di "dirigibile" attorno al percorso in line-of-sight pertanto gli stessi fenomeni si riscontrano anche se vi sono ostacoli che occludono lateralmente la clearance della F1. Vediamo come si procede al calcolo di **h** (ampiezza della zona F1) che ricordiamo varia in funzione della distanza (maggiore è il path e maggiore sarà il valore di h) e che raggiunge il suo valore massimo al centro della tratta radio). Nelle ipotesi h<0 ovvero propagazione LOS e clearance della F1 la distanza **h** dal punto piu' vicino dell'ostacolo al percorso diretto deve essere almeno:

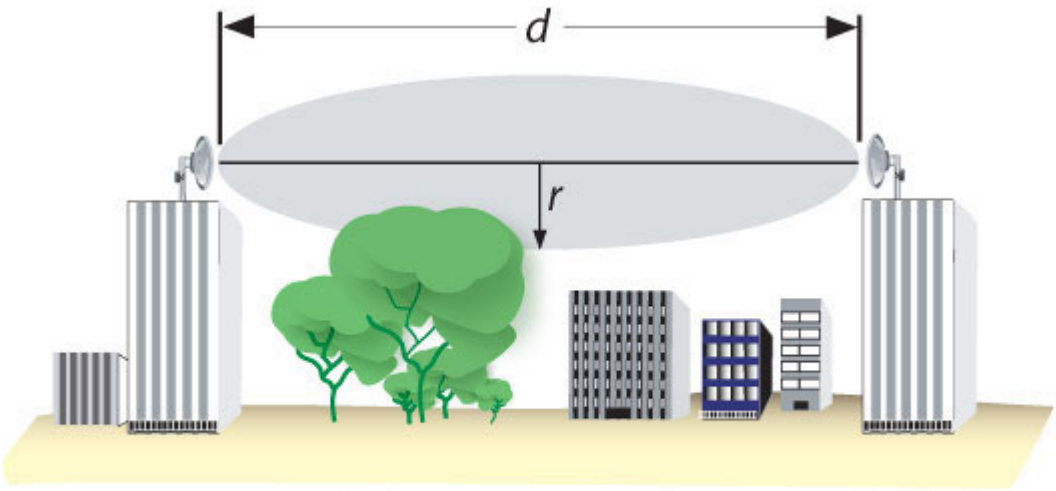
Con d1 e d2 rispettivamente le $h = 2\sqrt{\frac{\lambda\, d_1 d_2}{d_1 + d_2}}$ distanze dalla punta dell'ostacolo del trasmettitore T e del ricevitore R. Tale formula è una approssimazione che diventa imprecisa se si è molto vicini a T o R . Nella pratica ciò non accade mai poiché occorre valutare h lontano da T o R.

Il valore di h può per semplicità essere legato alla frequenza , espressa in **GHz** e se $\mathbf{d_1}$ e $\mathbf{d_2}$ sono espressi in km il valore di **h in metri** è dato da:

$$h = 17.3\sqrt{\frac{d_1 d_2}{f(d_1 + d_2)}}$$

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

Dall'immagine seguente si ha la spiegazione di quanto visto (h=r):



$$r_{(\text{in mts})} = 17.32 \times \sqrt{\frac{d\ (\text{in Km})}{4f\ (\text{in GHz})}} \qquad r_{(\text{in ft})} = 72.05 \times \sqrt{\frac{d\ (\text{in miles})}{4f\ (\text{in GHz})}}$$

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

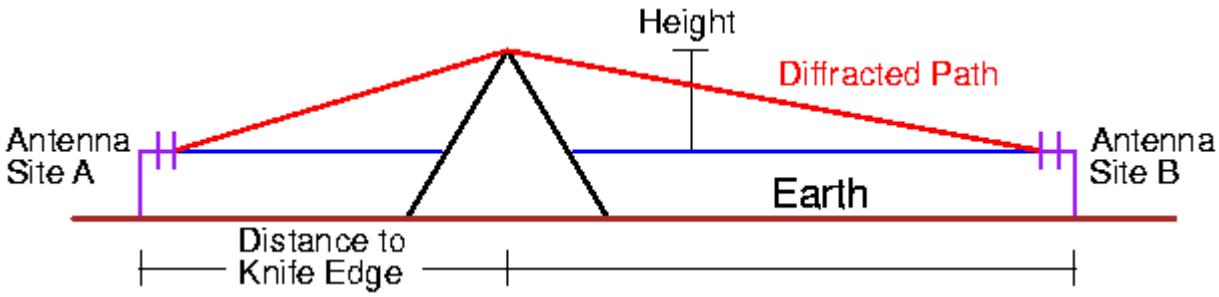
4.Esempi di propagazione NLOS :Knife edge attenuation

Consideriamo il caso in cui h>0 , ovvero ostruzione che occlude il cammino dal trasmettitore al ricevitore. In questo caso si parla di propagazione di tipo **NLOS** (Non Line of Sight)

Nel caso semplice in cui vi sia una ostruzione modellabile come knife-edge (lama di coltello) l'attenuazione di un percorso radio NLOS può essere calcolata semplicemente. Ricordando quanto detto a proposito del paramento di diffrazione **v** si ha

$$v = 2\sqrt{\frac{\Delta d}{\lambda}}$$

Con **v >0** , dalla curva si può ricavare mediante interpolazione l'attenuazione aggiuntiva.



Una buona approssimazione delle perdite in dB la si può avere dalla seguente formula:

$$K_{knife\ edge} = 20 \log_{10}(h * RadQ(f/D) - 38.8$$

Con **h** = altezza dell'ostacolo in metri

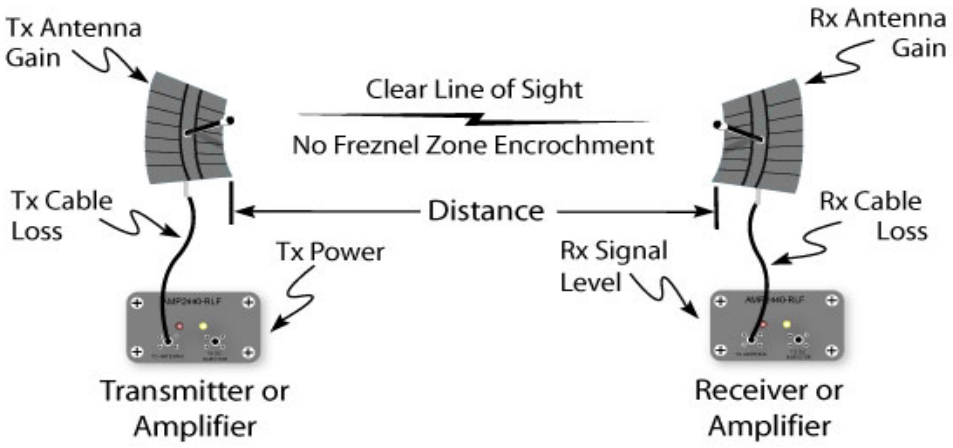
f = frequenza di lavoro in MHz

D = distanza in Km dell'ostruzione dalla sorgente

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

5.Calcolo del SOM di una tratta radio a microonde ed equazioni di dimensionamento

Per calcolare il margine di Fading (SOM) di una tratta radio occorre determinare innanzitutto, per il tramite di una semplice equazione di bilancio energetico , l'energia a RF disponibile all'ingresso del ricevitore :



$$Free\ Space\ Loss = 20Log_{10}(MHz) + 20Log_{10}(Distance\ in\ Miles) + 36.6$$

$$Rx\ Signal\ Level = Tx\ Power - Tx\ Cable\ Loss + Tx\ Antenna\ Gain - FSL + Rx\ Antenna\ Gain - Rx\ Cable\ Loss$$

$$SOM = Rx\ Signal\ Level - Rx\ Sensitivity$$

RSL= PTx+G_{ANTTx}+G_{ANTRx}–Loss_cableTx–Loss_cableRx-LossFilterTx-Loss_FilterRx + $L_{p(dB)}$

Con :

PTx = potenza a RF del tramettitore in dBm 0dBm= 1 milliwatt

G_{ANTTx} = guadagno dell'antenna trasmittente in dBi

G_{ANTRx}= guadagno dell'antenna trasmittente in dBi

Loss_cableTx= perdite del cavo d'interconnessione tra Tx ed antenna

Loss_cableRx= perdite del cavo d'interconnessione tra Rx ed antenna

Loss_FilterTx= perdita del filtro di ricezione

Loss_FilterRx= perdita del filtro di banda di trasmissione

$L_{p(dB)}$= Attenuazione di tratta secondo la legge di Friis semplice o generalizzata

Esercizio:

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

Vogliamo collegare tramite due bridge 802.11a operanti a 5450MHz le due sedi di un cliente , la distanza da coprire è di 20Km . Si suppone di operare in condizioni LOS e che dai data sheet degli apparati ho letto le seguenti caratteristiche:

PTx=17dbm@36Mbit/s

Minimum received signal level @36Mbit/s per BER 10^{-6} = -77dBm

Ipotizziamo di utilizzare due riflettori parabolici del diametro di 90cm con guadagno dichiarato alla frequenza di esercizio di 30dBi.

La lunghezza dei cavi di interconnessione tra apparati ed antenne è rispettivamente di 12mt. e 7mt.

Occorre determinare l'RSL e il SOM del sistema e verificare la fattibilità del collegamento stesso.

Calcoliamo tramite la legge di Friis l'attenuazione di tratta, nelle ipotesi di clearance della F1:

$$L_{p(dB)} = -(32{,}44 + 20\log(F) + 20\log(D))$$

$$L_{p(dB)} = -133{,}2\ dB$$

Dobbiamo stimare il valore di attenuazione introdotta dai cavi coassiali , a tal fine usiamo la tabella della pagina seguente che ci dà i valori di attenuazione di alcuni cavi commerciali. A queste frequenze il cavo che normalmente si utilizza è LDF4-50 da ½" di sezione .Interpolando opportunamente i valori abbiamo

Attenuazione @5,45 GHz = 21,6dB/100mt.

Per cui i cavi utilizzati nel progetto produrranno una attenuazione di :

12/100*21,6=**2,6dB**

7/100*21,6=**1,5dB**

Possiamo supporre che i filtri abbiamo una attenuazione massima di 1 dB in pass-band (valore reale). L'equazione di bilancio sarà:

$$RSL = PTx + G_{ANTTx} + G_{ANTRx} - Loss\_cableTx - Loss\_cableRx - LossFilterTx - Loss\_FilterRx + L_{p(dB)} = 17dBm + 30dbi + 30dbi - 2{,}6dB - 1{,}5dB - 1dB - 1dB - 133{,}2 = -62{,}3dBm$$

Calcolo del SOM:

per definizione il SOM è dato da:

$$S.O.M = -(\textbf{Rxsensitivity}) - RSL - SNR_{minimum} = 77dBm - 62{,}3dBm - 16dB = -1{,}3dB < 0$$

Con $SNR_{minimum}$ = valore di Signal to noise ratio minimo per garantire una trasmissione error free. Tale valore viene dato dal costruttore del bridge ed è un parametro di progetto legato al data-rate.

Il calcolo ci da un SOM<0 pertanto il link non è realizzabile a meno di agire su:

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

- Guadagno delle antenne
- Data rate del link

Poiché la sensibilità e SNR minimo sono legati al data rate , posso con una semplice operazione di configurazione software modificare la configurazione degli apparati radio per rendere il SOM >0 senza dover modificare le antenne:

la seguente tabella:

Data Rate	Soglia RX	SRN minimal
6 Mbit/s	-88dBm	4 dB
9 Mbit/s	-87dBm	5 dB
12 Mbit/s	-86dBm	7 dB
18 Mbit/s	-84dBm	9 dB
24 Mbit/s	-81dBm	12 dB
36 Mbit/s	-77dBm	16 dB
48 Mbit/s	-73dBm	20 dB
54 Mbit/s	-69dBm	21 dB

Se riduciamo la banda a 18 Mbit/s si ha :

S.O.M= -(**Rxsensitivity**)- **RSL**- $\mathbf{SNR_{minimum}}$= 84dBm – 62,3dBm –9dB= **12,7dB>0**

Il link è realizzabile avendo un SOM >0 , chiaramente tanto maggiore è tale valore , tanto più stabile e con outage minimo sarà il collegamento.

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

TABELLA ATTENUAZIONE CAVI COMMERCIALI 50Ω STANDARD

Cable Type	144 MHz	220 MHz	450 MHz	915 MHz	1.2 GHz	2.4 GHz	5.8 GHz
RG-58	6.2 (20.3)	7.4 (24.3)	10.6 (34.8)	16.5 (54.1)	21.1 (69.2)	32.2 (105.6)	51.6 (169.2)
RG-8X	4.7 (15.4)	6.0 (19.7)	8.6 (28.2)	12.8 (42.0)	15.9 (52.8)	23.1 (75.8)	40.9 (134.2)
LMR-240	3.0 (9.8)	3.7 (12.1)	5.3 (17.4)	7.6 (24.9)	9.2 (30.2)	12.9 (42.3)	20.4 (66.9)
RG-213/214	2.8 (9.2)	3.5 (11.5)	5.2 (17.1)	8.0 (26.2)	10.1 (33.1)	15.2 (49.9)	28.6 (93.8)
9913	1.6 (5.2)	1.9 (6.2)	2.8 (9.2)	4.2 (13.8)	5.2 (17.1)	7.7 (25.3)	13.8 (45.3)
LMR-400	1.5 (4.9)	1.8 (5.9)	2.7 (8.9)	3.9 (12.8)	4.8 (15.7)	6.8 (22.3)	10.8 (35.4)
3/8" LDF	1.3 (4.3)	1.6 (5.2)	2.3 (7.5)	3.4 (11.2)	4.2 (13.8)	5.9 (19.4)	8.1 (26.6)
LMR-600	0.96 (3.1)	1.2 (3.9)	1.7 (5.6)	2.5 (8.2)	3.1 (10.2)	4.4 (14.4)	7.3 (23.9)
1/2" LDF	0.85 (2.8)	1.1 (3.6)	1.5 (4.9)	2.2 (7.2)	2.7 (8.9)	3.9 (12.8)	**6.6 (21.6)**
7/8" LDF	0.46 (1.5)	0.56 (2.1)	0.83 (2.7)	1.2 (3.9)	1.5 (4.9)	2.3 (7.5)	3.8 (12.5)
1 1/4" LDF	0.34 (1.1)	0.42 (1.4)	0.62 (2.0)	0.91 (3.0)	1.1 (3.6)	1.7 (5.6)	2.8 (9.2)
1 5/8" LDF	0.28 (0.92)	0.35 (1.1)	0.52 (1.7)	0.77 (2.5)	0.96 (3.1)	1.4 (4.6)	2.5 (8.2)

Table 1 - Attenuation of Various Transmission Lines in Amateur and ISM Bands in dB/ 100 ft (dB/ 100 m)

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

6.Calcolo dell'affidabilità di un link radio

E' la grandezza espressa in percentuale e in minuti di outage (Interruzione) annui che ci permette di valutare l'affidabilità di una tratta radio. Tale grandezza dipende dal S.O.M. (System Operating Margin) detto anche margine di fading (F) e da vari fattori climatici che tengono conto del tipo di terreno e del tipo di clima sul quale si sviluppa il link, oltre che naturalmente dalla distanza e dalla frequenza di lavoro .

La formula utilizzata per determinare questa grandezza la si deve a **Lunkert(1970)** che effettuò delle misure statistiche di affidabilità per elaborare il modello che segue :

$$\textbf{Outage Probability} = A*B*2{,}5*10^{-6}*f(GHz)*(D/1{,}609344)^3*10^{(-F/10)}$$

$$\textbf{\% Reliability} = 100*(1-\textbf{Outage Probability})$$

A= terrain factor , tiene conto dell'umidità del terreno:

- **A=4 nel caso di terreno coperto d'acqua (mare, laghi , fiumi)**
- **A=1 terreno con umidità media**
- **A=0,25= montagna o zona secca**

B=climate factor , tiene conto del clima medio della zona oggetto di interesse:

- **0,5 = clima umido, costiero**
- **0,25 = entroterra**
- **0,125 =montagna o zona secca**

f= freq. del link espressa in GHz

D= distanza tra TX e RX in chilometri

F= margine di fading del collegamento

Il valor massimo di outage mensile in secondi nel caso peggiore sarà dato da:

outage_s_mese= Outage Probability * 2.600.000

con 2.600.000 numero di secondi medio in un mese.

Il valore massimo di outage annuo (worst case) è dato da:

outage_s_mese*3*(t_Fahrenheit)/50

con t_Fahrenheit = (5/9* $t^{celsius}$-32)

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

7.Descrizione degli apparati:AP,Bridge,Repeater,WDS

Gli apparati per W-LAN utilizzanti i protocolli 802.11b/g operano in una porzione di spettro chiamata banda ISM (2,412-2472) suddivisa in 13 canali (ETSI) , 11 canali (FCC) o 14 canali (Japan) sempre spaziati di 5MHz . Il band plan per la banda 2,4 GHz è mostrato nella figura seguente:

Channel ID	FCC/World (GHz)	ETSI (GHz)	France (GHz)	Japan (GHz)
1	2.412	2.412	--	2.412
2	2.417	2.417	--	2.417
3 (default in most countries)	**2.422**	**2.422**	**--**	**2.422**
4	2.427	2.427	--	2.427
5	2.432	2.432	--	2.432
6	2.437	2.437	--	2.437
7	2.442	2.442	--	2.442
8	2.447	2.447	--	2.447
9	2.452	2.452	--	2.452
10	2.457	2.457	2.457	2.457
11 (default in France)	2.462	2.462	**2.462**	2.462
12	--	2.467	2.467	2.467
13	--	2.472	2.472	2.472
14				2.484

Per quanto riguarda il protocollo 802.11a , la sua diffusione in Europa e quindi in Italia è stata fortemente frenata da problemi di co-allocazione di spettro con altri servizi esistenti e con gli apparati **Hyperlan** (standard Europeo di apparati per W-LAN sopraffatto dalla diffusione nel mondo di 802.11a) . L'imissione sul mercato di tali prodotti è stata subordinata all'ottenimento dell'omologazione da parte del Ministero delle Comunicazioni come prodotti Hyperlan "compatibili" secondo lo standard 802.11h. Tale "compatibilità" è stata garantita con l'introduzione del **DFS** (dynamic Frequency selection) e del **TPC** (Transmitter power control) come "features" obbligatorie negli apparati a 5GHz. Come precedentemente detto nel segmento 5-6GHz voi sono altri servizi (Ministero Difesa, Radar avvicinamento aereo ecc.) che devono essere garantiti dai disturbi provenienti dagli apparati W-LAN , il DFS disabilità da parte dell'utente la possibilità di settare la frequenza di lavoro degli apparati che viene gestita in maniera automatica.

La tabella mostra il bandplan dei 5GHz , l'unico segmento destinato ad un uso outdoor è quello che va da 5470MHz a 5725MHz , la banda netta è 5500-5680MHz la differenza costituisce la cosiddetta banda di guardia. La potenza massima E.IR.P. consentita in Italia è:

- 100 mwatt (20dBm) in 2,4GHz
- 1Watt (30dBm) in 5,4 GHz

il segmento **5,150-5,350 GHz** è consentito sono in indoor con antenne interne ed incorporate agli apparati. La legislazione Italiana consente anche l'uso degli **SRD** (Short range Devices) nel segmento **5,725GHz-5,825GHZ** ma con una E.I.R.P. di appena 25mwatt.

Channel ID	FCC	ETSI
56	5.280	–
60	5.300	–
64	5.320	–
100	–	5.500
104	–	5.520
108	–	5.540
112	–	5.560
116	–	5.580
120	–	5.600
124	–	5.620
128	–	5.640
132	–	5.660
136	–	5.680
149	5.745	–
153	5.765	–
157	5.785	–
161	5.805	–
165	5.825	–

Gli apparati per W-LAN (2,4 e 5 GHz) sono classificati nel seguente modo:

- **AP – Access Point**
- **Client Station** (PC laptop o desktop con scheda Wireless, print server ecc)
- **Bridge Pt-Pt** (punto – punto)
- **Bridge Pt-Mpt** (punto multipunto)
- **Repeater Station o WDS**

Gli **AP** e le **client station** formano la classica rete wireless in modalità **infrastructure,** che permette ad utenti dotati di pc desktop o portatili dotati di scheda wireless (802.11b/g/a) o processore con estensioni wireless (Intel Centrino) di accedere , all'interno di un'area ben delimitata, alle risorse aziendali senza una connessione fisica in rame .

L'AP coordina le attività di tutti i client nell'area di copertura, le stazioni client si devono autenticare/deautenticare dall'AP secondo precise policy di sicurezza basate o sul MAC address della scheda o tramite l'uso della suite di sicurezza 802.1x . Solo dopo il processo di autenticazione all'AP essi possono fruire dei servizi di rete .Gli AP effettuano essenzialmente un bridging (OSI 2)

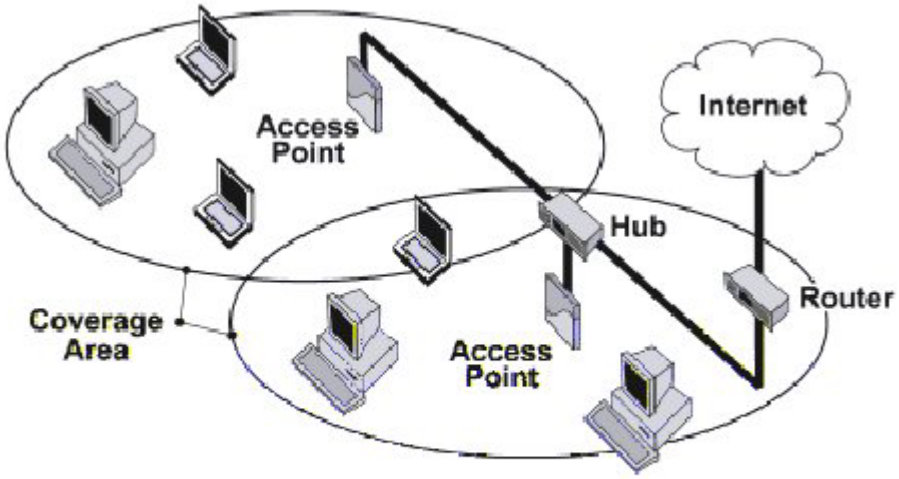


Figure 1-1 Typical wireless network access infrastructure

tra stazioni client e rete LAN cablata effettuando un filtraggio delle comunicazioni (ove richiesto) tra le stazioni client (intra-cell blocking).

Le stazioni client , per poter accedere alla rete wireless devono eseguire la scansione delle WLAN accessibili , scegliere l'SSID (Service Set IDentifier) dell'AP a cui si vogliono connettere e , se dotati delle opportune credenziali, connettersi al'AP.

L'altra modalità di funzionamento è chiamata **AD-HOC (IBSS) ,** si tratta di una connessione peer-to-peer tra pc dotati di scheda wireless che prescinde dalla presenza dell'AP. Le due modalità infrastructure (BSS) e AD-HOC (IBBS) sono mutuamente esclusive tra loro.

I bridge **Bridge Pt-Pt** (punto – punto) **Bridge Pt-Mpt** (punto multipunto) vengono normalmente utilizzati per realizzare trunk di trasporto all'interno di una rete geografica o per collegare tra di loro le LAN di una azienda . Non dimentichiamo che essi lavorano a livello OSI 2 e una corretta segmentazione della rete deve essere fatta tramite 2 Router posti tra i bridge e la LAN del cliente. I router dovranno essere dotati di 2 porte ethernet una WAN che guarda il bridge wireless ed una porta LAN che verrà interconnessa allo switch di piano più vicino.

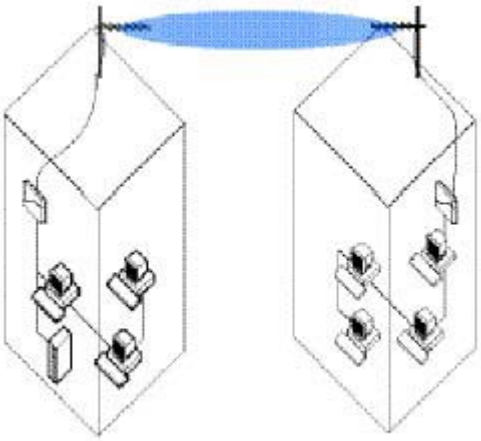


Figure 1. Point-to-Point Link

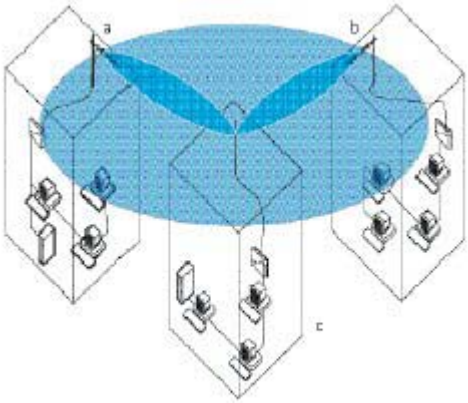


Figure 2. Point-to-Multipoint Network

Al livello IP si provvederà all'assegnazione di classi diverse sia per la parte WAN che per le due LAN. Solo il traffico diretto alla rete IP remota verrà instradato attraverso i router e la rete geografica, con notevoli risparmi di banda che una soluzione a livello OSI 2 non avrebbe permesso.

I **Repeater** sono degli apparati che permettono di estendere l'area di copertura di un AP , essi non sono dotati di connessione alla rete cablata e lavorano solo sulla parte wireless. Eseguono una sorta di store-and-forward dei pacchetti provenienti dalla stazione client verso l'AP e viceversa.

Chiaramente ciò impatta sulle performance generali del sistema. La banda disponibile e il throughput massimo si dimezzano poiché raddoppia l'occupazione del canale per trasmettere la singola frame. Un approccio più performante lo si ottiene con i WDS (Wireless Distribution sistems). In questo caso l'interconnessione con l'AP avviene su un canale dedicato o meglio sui 5GHz.

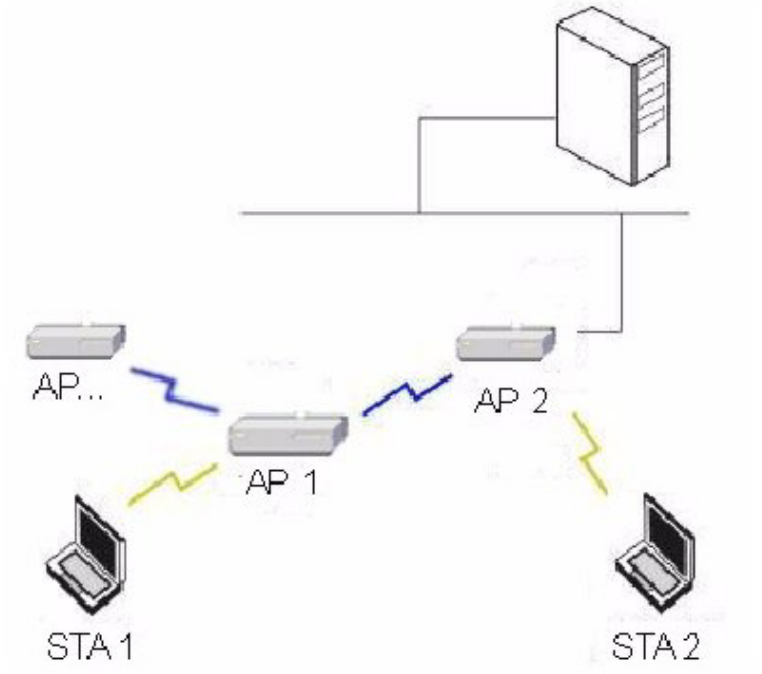


Figure 4-15 WDS Example

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

8.Performance dei vari protocolli :CCK, DSS, FHSS, OFDM

Il throughput di una rete wireless è definito come la velocità (mbit/s) alla quale un utente può trasmettere e ricevere dati tra un client wireless e l'AP. Il throughput è legato alla distanza delle stazioni client dall'AP e nel caso di bridging alla distanza tra i 2 bridge. Tale comportamento è legato all'intensità del segnale che si degrada allontanandosi dall'AP. Se consideriamo la parte radio , maggiore è il data rate maggiore sarà la larghezza di banda richiesta nella catena RF. Ciò comporta un degrado delle performance della parte ricevente in termini di noise-floor e la necessità di maggiore potenza all'ingresso dell'RX. Dai data sheets degli AP commerciali si può notare che per un data rate di 1Mbit/s la soglia statica è di soli **-90 dBm** mentre al massimo data rate di 54Mbit/s (802.11g/a) la soglia statica peggiora fino ad arrivare a **-65dBm** ovvero 25dB di segnale in più. Poiché quando il client si allontana dall'AP l'ampiezza del segnale si degrada secondo quanto stabilito dalla legge di Friis , ne consegue che il data rate massimo a parità di antenna e potenza del trasmettitore dipende dalla distanza e dagli eventuali ostacoli che si frappongono tra AP e client.

Si possono modellare dei cerchi attorno all'AP legati alla distanza, caratterizzati da diversi e decrescenti valori di data rate . Al degradarsi del segnale il data-rate si abbassa fino al valore ottimale per il valore di S.N.R. (Signal to Noise Ratio) derivante dalla distanza in cui si trova la stazione client, ciò avviene in maniera trasparente per l'utente poiché il meccanismo dell'**Auto fall-back** rate provvedere al settaggio del data rate ottimale della scheda client.

I **rendimenti massimi teorici** per i vari protocolli 802.11 sono i seguenti:

	Number of Channels	Modulation	Maximum Link Rate	Maximum TCP Rate	Maximum UDP Rate
802.11b	3	CCK	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g (with 11b)	3	OFDM/CCK	54 Mbps	14.4 Mbps	19.5 Mbps
802.11g (11g-only mode)	3	OFDM/CCK	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a	19	OFDM	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a TURBO	6	OFDM	108 Mbps	42.9 Mbps	54.8 Mbps

Tali valori sensibilmente diversi dai physical-layer data-rate (1,2,5.5,11 Mbit/s 802.11b 6,9,12,18,24,36,48,54 Mbit/s 802.11a) principalmente perché:

- Il canale radio è half-duplex
- L'overhead del pacchetto (preambles,headers ecc) riduce il payload
- Ogni pacchetto deve essere confermato tramite un acknowledge (rendimento TCP<UDP)

- Il trasmettitore aspetta un intervallo di tempo random prima di impegnare il media (CSMA/CA).

L'efficienza espressa in termini rapporto tra Throughput/occupazione di banda è maggiore per i protocolli 802.11g e 802.11a che utilizzano modulazioni OFDM di cui parleremo tra poco.

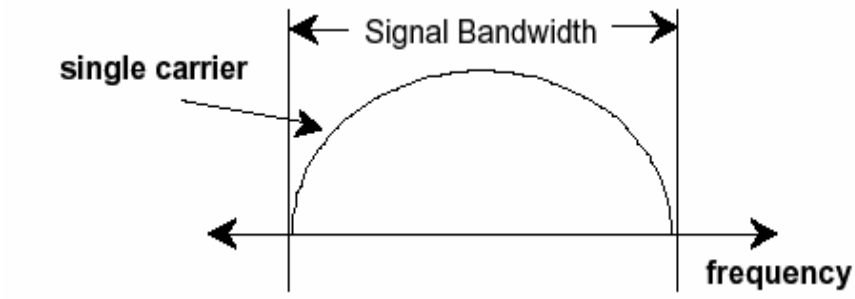
Data Throughput Tables

5GHz		
Mbit/s	Net Mbit/s	Efficiency
6	4.6	77%
9	6.7	75%
12	8.7	73%
18	12.4	69%
24	15.8	66%
36	21.5	60%
48	26.2	55%
54	28.3	52%

2.4GHz		
Mbit/s	Net Mbit/s	Efficiency
1	0.8	82%
2	1.5	76%
5.5	3.4	62%
11	5.2	47%

I protocolli 802.11g e 802.11a , anche se operanti su diverse frequenze e quindi con apparati non interoperanti tra loro, presentano il vantaggio di utilizzare uno schema di modulazione nuovo rispetto all' 802.11b :l'**OFDM** (Orthogonal Frequency Division Multiplexing) . Tale schema di modulazione è stato progettato espressamente per sistemi radio ad elevati data-rates e supporta nativamente la velocità di 54Mbit/s. La novità rispetto allo spread spectrum tradizionale che usa **CCK** (Complementary Code Keying) è che nel caso di **OFDM** il payload è suddiviso su diverse portanti a più basso data-rates :

CCK

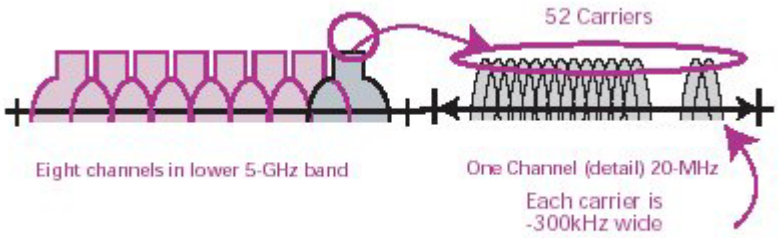


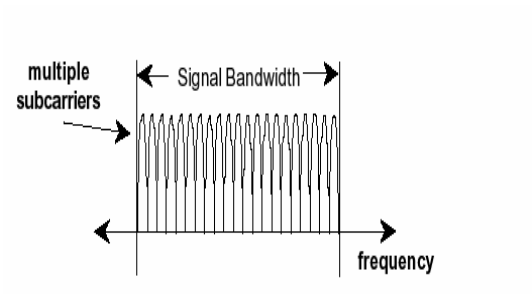
OFDM

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

L'efficienza della modulazione OFDM rispetto alla CCK la si nota nelle condizioni estreme , dove fenomeni di multi-path renderebbero impossibile la realizzazione di un collegamento e in condizioni NLOS come nei collegamenti cittadini.

La modulazione OFDM splitta il payload in 52 portanti larghe 300KHz cadauna:





Altro grosso vantaggio è che nella frame la durata del preambolo è di solo 16µsec contro i 72 µsec del CCK con minore sovraccarico della rete e performance migliori.

Le performance massime raggiungibili in termini di throughput aggregato nel caso di collocazione di più access point/ bridge **per sito** sono legate alla frequenza e al tipo di protocollo. Analizziamo lo spettro dei 2,4GHz:

Si hanno a disposizione circa 83,5MHz di banda su 13 canali spaziati di 5 MHz. Poiché ogni Access Point impegna con i suoi client circa 25MHz di banda, non più di 3 AP possono essere collocati sullo stesso sito in banda 2,4 GHz (802.11b e 802.11g) senza interferire tra loro .Se aumentassi il numero di AP avrei un degrado delle prestrazioni legato al parziale overlapping delle bande occupate. Si definiscono canali non-overlapping i canali **1,6,11 (FCC)** e **1,6,13 (ETSI)**

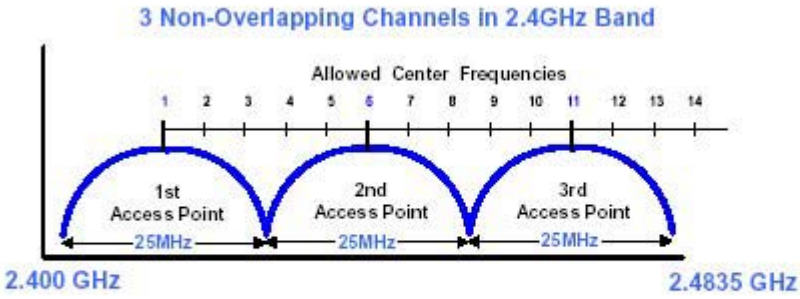


Figure 1-6. Typically, channels 1, 6, and 11 are used as the three non-overlapping channels in the 2.4 GHz band

La banda dei 5GHz utilizzata dagli apparati 802.11a permette la collocazione di molti AP grazie ai suoi 455MHz di spazio allocato per le W-LAN. Inoltre grazie al fatto che i canali sono spaziati di

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

ben 20MHz è possibile avere ben **24 canali non-overlapping** a differenza di ciò che succedeva nei 2,4 GHz con la spaziatura di soli 5 MHz.

5 GHz in the European Community

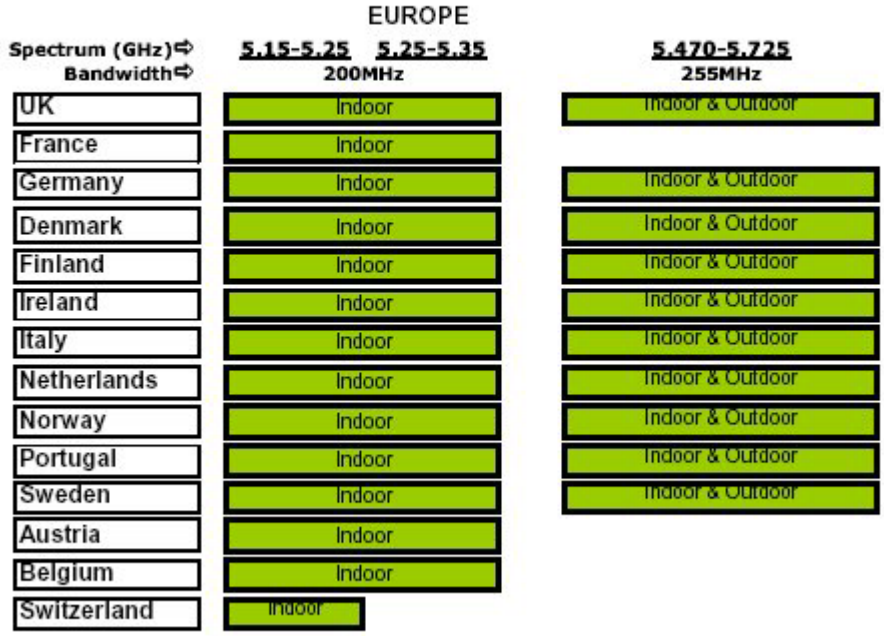


Figure 1-5. European Community

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

9.Problematiche di sicurezza su reti radio: WEP, WPA, 802.1x, EAS, EAP, RADIUS

Le problematiche legate alla sicurezza impattano molto sulla diffusione, sia a livello aziendale e privato dell'uso, massivo delle W-LAN in alternativa al rame. Purtroppo, inizialmente l'uso di apparati wireless all'interno delle aziende non è stato soggetto ad alcun tipo di coordinamento da parte dei responsabili IT dando luogo a notevoli problematiche di sicurezza. Spesso si trovano in azienda ma anche in Università semplici reti di tipo Infrastructure costituite da un AP e pochi client che trasmettono **in chiaro** senza alcuna forma di crittografia dati riservati e spesso critici per la vita aziendale .La cosa che più ci colpisce è la totale ignoranza di chi utilizza tali strumenti della possibilità da parte di malintenzionati di "sniffare" i propri dati semplicemente con un laptop da dentro una macchina posta nelle vicinanze della rete in oggetto. Tale tecnica , purtroppo in fase di diffusione anche in Italia , denominata War-driving costituisce un reato contemplato e punito dal codice penale. E' chiaro a tutti, che non esiste un sistema informativo impenetrabile , ma l'utilizzo di tecniche di crittografia ed autenticazione allo stato dell'arte sicuramente ci mette al riparo dagli attacchi portati alla nostra rete dall'hacker della porta accanto.

Esistono 4 tipologie di attacco alla sicurezza di una rete wireless :

- **Eavesdropping** (to eavesdrop= origliare): l'aggressore con uno "sniffer" e una scheda di rete wireless ascolta il traffico tra una stazione client e l'Access Point per rubare informazioni sensibili
- **Mac Spoofing :** l'aggressore clona il MAC address della schede di rete di utenti autorizzati per ottenere accesso abusivo alla rete. Tale tecnica viola le policy di sicurezza presenti su tutti gli AP basate filtraggio dei MAC address delle stazioni client. (MAC FILTERING)
- **Rogue Access Point :** è un attacco del tipo man-in-the middle, l'aggressore si sostituisce ad un AP legittimo per catturare username e password di utenti autorizzati.
- **Theft of service :** l'aggressore ottiene accesso ad Internet attraverso risorse aziendali o domestiche, per usi illeciti con le conseguenze civili e penali che si possono immaginare.

Analizziamo i vari protocolli di sicurezza sviluppati fino ad oggi partendo da quelli più vulnerabili.

a) WEP (Wired Equivalent Privacy)

Storicamente è il primo protocollo di sicurezza per reti wireless , è stato sviluppato nel 1999 dall' IEEE 802.11 working group con l'intento di fornire livelli di sicurezza simili a quelli delle reti wired. Si è dimostrato subito vulnerabile per l'esigua lunghezza della chiave di crittografia e per errori di implementazione. Inizialmente i vendors storici quali Lucent e Cisco

Medianet Comunicazioni S.R.L. – Corso Italia n° 63 , 95129 CATANIA
www.medianetonline.net e-mail:luigi.crocella@medianetonline.net

implementarono chiavi di 40 bit , successivamente si è passati ad implementazioni a 64, 128 e 256 bit. La lunghezza della chiave influisce solo sulla quantità di traffico da catturare da parte degli aggressori per rompere la chiave WEP. Ormai sono disponibili in rete tool open-source sotto Linux sviluppati ad-hoc e capaci di scoprire la chiave WEP tramite attacchi basati su dizionari o cattura di traffico.

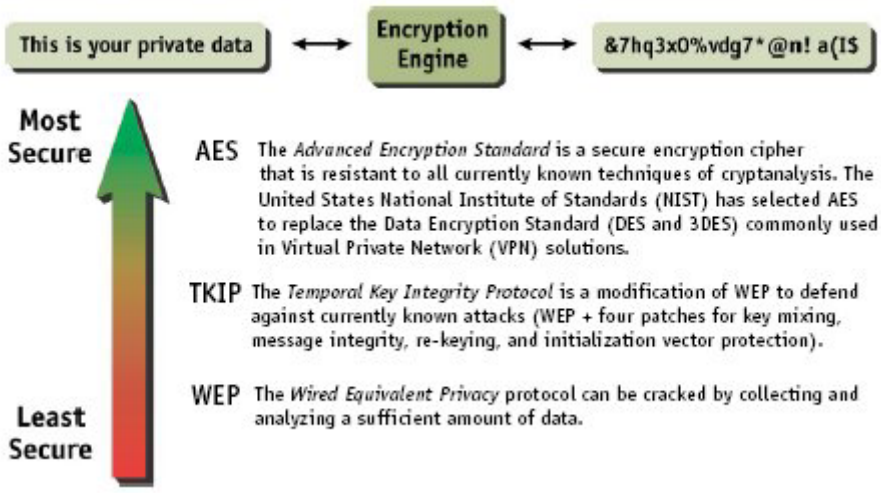
b) 802.11i

Non appena fu chiara la debolezza del WEP fu creata la task force IEEE 802.11i per studiare nuove tecniche di crittografia e sicurezza da utilizzare nelle reti Wireless. I risultati di tali lavori sono stati ratificati come standard e sono costituiti da due parti:

AES-Advanced Encryption Standard : per la crittografia del traffico nelle W-LAN

*IEEE802.*1x Port Based Network Authentication Standard : per l'autenticazione degli utenti delle W-LAN e gestione delle chiavi

La task force 802.1i inoltre propose alcune fix per il protocollo WEP (TKIP) da adottare in quelle schede wireless legacy non upgradabili ad AES.



Attualmente AES rappresenta il metodo più sicuro e resistente alle tecniche di criptoanalisi , alla luce di ciò il NIST (US National Institute of Standard) lo ha scelto al posto del DES (data encryption standard) e 3DES per la sicurezza nelle VPN.

Il protocollo 802.1x (Port Based Network Authentication Standard) usato per l'autenticazione degli utenti wireless **(detti supplicant)** utilizza un Server di Autenticazione posto nella rete wired dietro

gli AP **(autenticator).** Il Server di Autenticazione è di solito un server **RADIUS** (**R**emote **A**uthentication **d**ial-**i**n **U**ser) normalmente usato a livello corporate per autenticare gli utenti dial-in.

Il processo di autenticazione si può così riassumere:quando una stazione client **(supplicant)** tenta di accedere ad una WLAN tramite 802.1x , l'AP abilita il passaggio solo del traffico di autenticazione forzando la stazione in un "authenticate state" dove solo il traffico EAP (Extensible Authentication Protocol) viene passato al server RADIUS. Attraverso l'uso di messaggio EAP , chiavi pubbliche/private di crittografia e di password il RADIUS autentica la stazione client. Il RADIUS fornisce all'AP una chiave iniziale di crittografia che è ricavata dalla stazione client durante la prima fase di autenticazione . Successivamente l'AP genera una seconda chiave da usare nelle comunicazioni con il client , cripta questa seconda chiave con la chiave fornita dal RADIUS e la invia al client. L' AP ad intervalli di tempi presettati invia nuove chiavi al client per preservarne l'integrità nel tempo.

c) WPA (Wi-Fi Protected Access)

La Wi-Fi alliance ha proposto in alternativa a WEP (durante la fase di standardizzazione di 802.11i) WPA (Wi-Fi Protected Access) come soluzione transitoria alle problematiche di sicurezza. Essa si basa sulla versione provvisoria del draft 3.0 di 802.11i del 2002. A partire dal 2003 è stato implementato su tutte le schede dei maggiori vendors. Il target commerciale di questo standard di sicurezza è il mercato SOHO (home users, piccoli uffici) , dove non è mai presente un RADIUS come server di autenticazione . WPA si basa sul meccanismo delle Pre-shared Key (PSK) per migliorare la sicurezza rispetto a WEP. Per utilizzare PSK occorre specificare sia a livello di stazione che di AP una Pass-phrase che verrà utilizzata per autenticare tutte le stazioni che tentano di collegarsi al'AP. L'AP quindi fornisce alla stazione una session-key che è aggiornata ad intervalli di tempo regolari. Ciò implica la presenza di un **802.1x-WPA** supplicant a livello di stazione . Microsoft ha implementato solo su **XP** tale feauture ma non intende farlo per gli altri SO legacy (98,95,NT ecc) .

WPA2

Al fine di rendere WPA conforme agli standard IEEE 802.11i, è stato sviluppato WPA2 , backward compatible con WPA. Il miglioramenti più importante riguarda l'introduzione della stronger encryption mediante l'uso di AES come in 802.11i. Un altro miglioramento sensibile è il supporto per il fast roaming , questa funzionalità è molto importante per applicazioni VoIP che sono molto

sensibili ai ritardi dovuti alla latenza in trasmissione e ricezione. Per risolvere il problema della latenza nella fase di roaming tra un AP ed un altro WPA2 consente una pre-autenticazione agli AP delle celle confinanti oltre a quello con cui si sta comunicando.

11. Bibliografia

Legenda **WP=**white Paper

a) Deployment consideration for 5Ghz WLAN Technology – **Intersil Corparation** WP

b) **Atheros Communications** : Range and Throughput Comparisons of WLAN Products WP

c) **Atheros Communications**: Worldwide Regulatory Progress for Wireless LANs WP

d) **Atheros Communications:** Measuring Throughput and Coverage of Wireless LANs WP

e) **Atheros Communications:** Security White Paper

f) **Harvard University** : Radio Propagation Models study

g) **VHF/UHF/Microwave Radio Propagation** ve3jf@tapr.org

h) **Microwave System Equations** :Softwright Corporation FAQ engineering

i) **NON-LINE OF SIGHT**: Technology & Implementation – Solectek WP

l) **Plotting Line of Sight and Fresnel Zones** : **Softwright** Corporation FAQ engineering

m) **Factors influencing Signal clarity**: **Solectek** WP

n) **Introducing Wimax**: The next Broadband Wireless Revolution - **Alvarion** WP

o) **802.11a**: A very High-Speed Hig-scalable Wlan standard – **Proxim** Corporation WP

p) **Effect of Obstructions on RF Signal Propagation - EMS** Wireless Technical Support

q) **Ultra Wideband** -- the Next-Generation Wireless Connection by Rafael Kolic

r) **WISP** – Wireless Service Provider Tutorial – **Solectek** WP

t) **Radios in Outdoor Environment - Solectek** WP

u) Progetto rete di trasporto Wireless Credito Siciliano SPA