Introduzione al protocollo 802.11 (WiFi)

Questo è il primo di due articoli in cui presenteremo alcuni aspetti tecnici dei protocolli 802.11, anche noti con il nome commerciale di WiFi. L'idea che ci ha spinti a preparare questi articoli è che per poter realizzare delle reti Wireless con un ragionevole livello di sicurezza e funzionalità, è necessario essere a conoscenza delle basi su cui sono costruiti questi protocolli. Pertanto in questo primo articolo ci dedichiamo quasi esclusivamente a descrivere i protocolli utilizzati sia dagli 802.11 che da altri protocolli Wireless nei livelli più bassi della pila OSI. Nella seconda parte ci concentreremo sugli 802.11 e sugli aspetti tanto discussi della loro (in−) sicurezza.

1. WLAN

In realtà i protocolli Wireless sono utilizzati in modi diversi a seconda dell'applicazione: si parla di *Wireless Bridges* quando si collegano ed unificano tramite un ponte radio due LAN tradizionali, di *Wireless Distribution System* quando un ISP collega alla propria dorsale i clienti tramite ponti radio, di *Cable Replacement* quando si sostituiscono i cavi che collegano i computer a tastiere, mouse ecc. con collegamenti ad esempio infrarossi, ed infine di *Wireless LAN* quando si sostituisce il cablaggio locale (Ethernet) con collegamenti radio. Per semplicità nel proseguio considereremo per lo più il caso di WLAN. In pratica nei device sul network, computer, stampanti ecc., si sostituisce ad una scheda Ethernet una scheda Wireless ove al posto di una presa RJ−45 è presente un'antenna. Uno schema funzionale di una scheda Wireless è indicato in Figura 1 [5]:

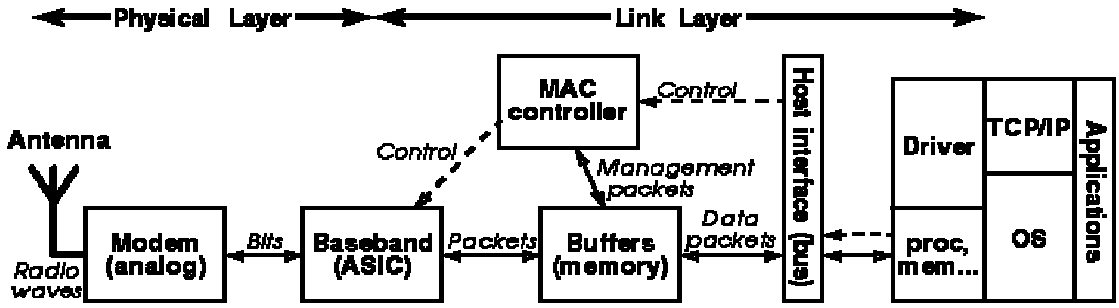

Figura 1. Schema funzionale di scheda Wireless

Il Physical Layer, o radio modem, è quasi interamente analogico (eccetto l'ASIC) ed è di solito schermato per evitare interferenze. Il Link Layer gestisce invece il protocollo MAC.
Nelle prossime sezioni descriveremo alcuni tra i protocolli esistenti, prima per il Physical Layer, poi il Link Layer. Infine metteremo insieme i pezzi per costruire l'802.11b.

2. Physical Layer

Le frequenze utilizzate in Europa sono i 2.4GHz (i 0.9 GHz sono utilizzati dai telefoni cellulari GSM) ed i 5GHz. In particolare l'802.11b prevede l'utilizzo della banda tra i 2.4GHz ed i 2.4835GHz. La massima potenza consentita legalmente è di 100mW. La trasmissione elettromagnetica è fatta seguendo le regole dello *Spread Spectrum* che in linea di principio limita la velocità massima nella banda di 2.4GHz a 2Mbps. L'utilizzo di modulazioni più complesse permette di raggiungere gli 11Mbps. La tecnica dello Spread Spectrum cerca di evitare che il segnale venga inviato su frequenze *cattive* (ovvero con molte interferenze) utilizzando una banda più larga per inviarlo, quindi più spreco di banda per ottenere maggiore affidabilità. All'interno dello Spread Spectrum vi sono due principali tecniche: il *Direct Sequence* ed il *Frequency Hopping*.

Il *Direct Sequence* sovra−modula il segnale (ovvero un bit) con un pattern veloce che si ripete 11 volte (detti 11 *chips*), a 2Mbps questo occupa 22 Mhz di banda (vedi Figura 2 [5]). In questa modalità si usa quindi un canale largo ma fisso, quindi pochi

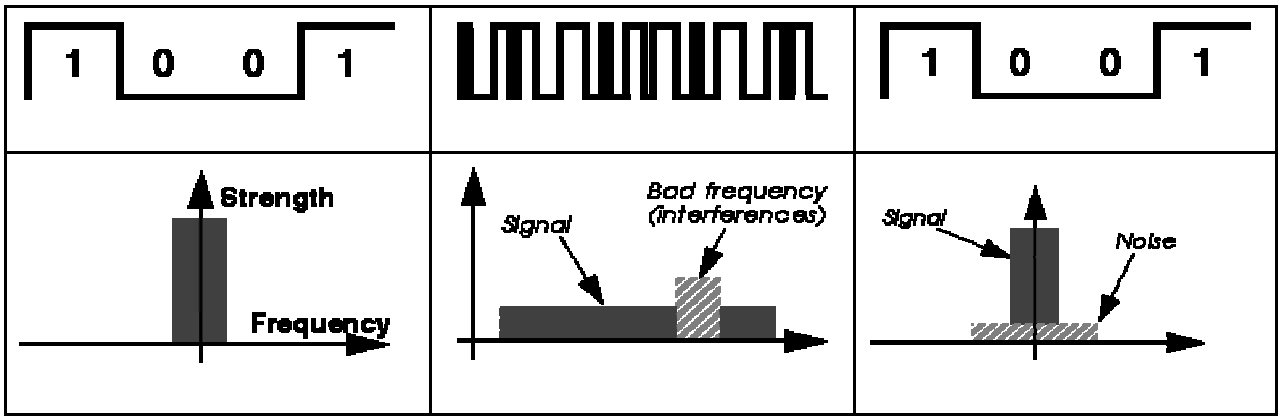

Figura 2. Direct Sequence Spread Spectrum

canali sono disponibili nella banda totale (su 13 canali solo 3 non si sovrappongono nella banda dei 2.4 GHz), d'altra parte il modulatore deve essere molto veloce e perciò complicato a livello hardware.

Il *Frequency Hopping* invece utilizza 79 canali stretti (1MHz) e salta da un canale all'altro ciclicamente con una frequenza dai 20 ai 400ms. In presenza di una interferenza su di una banda stretta questo risulta molto efficiente (vedi Figura 3 [5]), inoltre essendo i canali molto stretti è possibile averne molti nella stessa banda. D'altra parte il MAC deve essere molto complicato per poter inseguire i canali che si spostano continuamente, e vi sono problemi con possibili collisioni fra frequenze adiacenti.

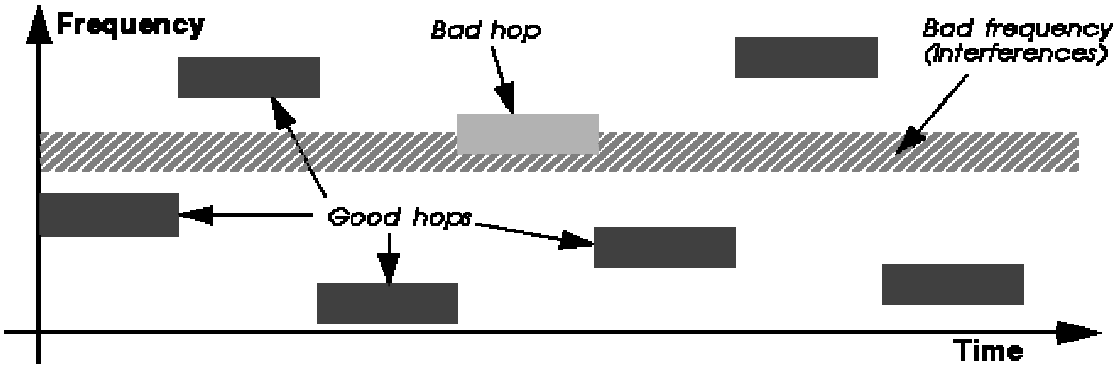

Figura 3. Frequency Hopping Spread Spectrum

Per trasmettere il segnale si modula una frequenza di base. Dati i problemi di attenuazione che descriveremo, modulare l'ampiezza non è conveniente, mentre è possibile modulare la frequenza o la fase dell'onda. La più semplice tecnica di modulazione è la 2FSK (2 Frequency Shift Keying, vedi Figura 4 [5]).

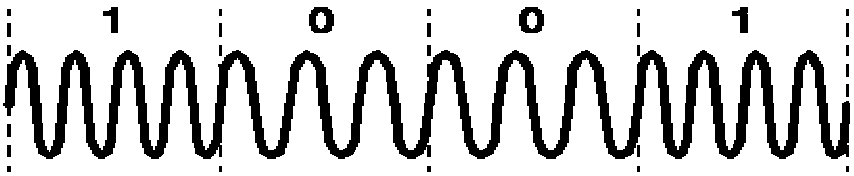

Figura 4. 2 Frequency Shift Keying

E' ovvio che utilizzando modulazioni più complicate è possibile trasmettere più informazioni nello stempo tempo, e quindi aumentare la velocità di trasmissione, a scapito di una maggiore complicazione e precisione richiesta all'apparato. La modulazione CCK (Complementary Code Keying) è utilizzata dall'802.11 e permette di raggiungere i 5.5 e gli 11 Mbps. Infine la nuova modulazione OFDM (Orthogonal Frequency Division Multiplex) utilizza un set di sottofrequenze ortogonali modulate indipendentemente sulle quali trasmette il segnale, passato attraverso una Fast Fourier Transform, in parallelo. Questo richiede una grande precisione sulle frequenze ma permette di eliminare il problema del Delay Spread, discusso più avanti, presente in modo particolare nella banda a 5GHz (802.11a e 802.11g).

I problemi principali della trasmissione via onde radio sono l'attenuazione del segnale dovuta alla distanza ed agli ostacoli fisici, la presenza di interferenze su frequenze ben precise (e non di rumore bianco), quali dovute a fondi a microonde, telefoni cordless, apriporta, telecomandi ecc., e la presenza di cammini multipli per cui il segnale può arrivare allungato nel tempo (Delay Spread), vedi Figura 5 [5]. Per combattere questi problemi si utlizzano doppie antenne od antenne direzionali, la ritrasmissione a livello MAC dei pacchetti non arrivati od arrivati ma corrotti, e

l'utilizzo di un Equalizzatore Digitale o dell'OFDM per eliminare il Delay Spread.

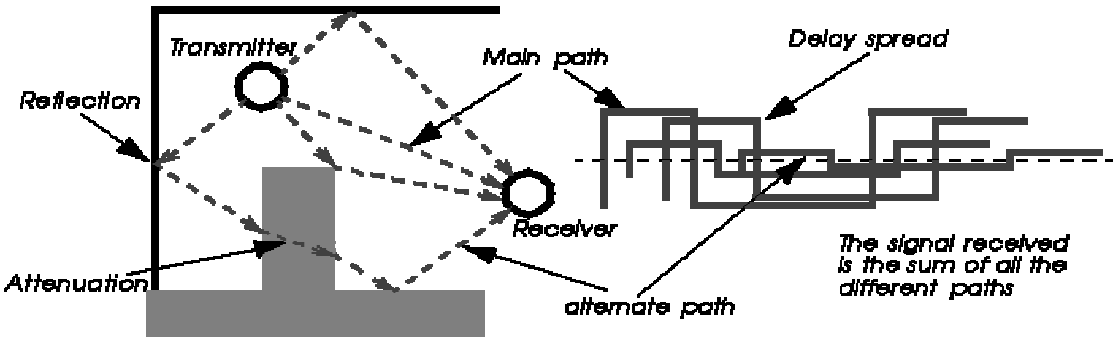

Figura 5. Cammini multipli e Delay Spread

3. Link Layer

Al livello del Link Layer viene gestito il protocollo MAC che controlla l'accesso al mezzo, ovvero quando è possibile trasmettere, quando si riceve ecc. I protocolli principali a questo livello sono il TDMA, il Polling ed il CSMA/CA. Poiché in pratica solo il CSMA/CA è utilizzato nelle WLAN, ci limiteremo a descrivere solo questo protocollo. Il CSMA/CA è derivato dal CSMA/CD che è alla base dell'Ethernet (tra l'altro il protocollo Ethernet stesso proviene da un precedente protocollo Wireless, l'Aloha). La differenza fra CSMA/CA e CSMA/CD è che nel caso dell'Ethernet è possibile effettuare la Collision Detection (CD) poiché sul cavo una stazione ha la possibilità di ascoltare mentre trasmette e quindi di rendersi conto se due stazioni stanno trasmettendo nello stesso momento. Questo non è possibile nel Wireless dove un'antenna può solo trasmettere o ricevere in un dato momemnto (e la transizione tra le due fasi richiede del tempo). Pertanto il protocollo Wireless introduce la Collision Avoidance (CA) che purtroppo di nuovo riduce l'efficienza ed il throughput. L'idea dei protocolli CSMA (Carrier Sense Multiple Access) è che prima di trasmettere bisogna ascoltare la portante per vedere se qualcuno trasmette. Se nessuno trasmette, si invia il proprio pacchetto. Altrimenti si attende il termine della trasmissione dell'altro. A questo punto ogni stazione attende un numero random di slot (uno slot è di 50 microsec in 802.11−FH e 20 microsec in 802.11−DS, la lunghezza dello slot garantisce che ogni stazione riesca a passare dalla fase di ascolto a quella di trasmissione e viceversa), la stazione che ha scelto l'attesa minore incomincia la trasmissione. Questo meccanismo garantisce che in media ogni stazione abbia a propria disposizione la stessa quantità di banda trasmissiva (vedi Figura 6 [5]).
Ovviamente questo meccanismo non previene in maniera assoluta le collisioni. Poiché le stazioni non sono in grado di ricevere mentre stanno trasmettendo, non possono rendersi conto se sta avvenendo una collisione: Pertanto sono stati aggiunti altri meccanismi per prevenire le collisioni e gestire più efficacemente le trasmissioni.

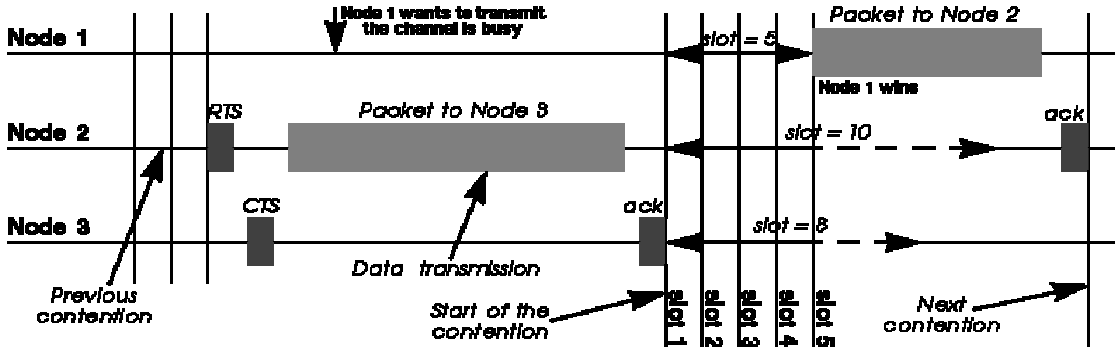

Figura 6. CSMA/CA

In primo luogo vi sono il Positive Acknowledgment ed il MAC Level Retransmission. Appena una stazione ha finito di ricevere un pacchetto, invia un ACK per confermarne la ricezione, prima che incominci per tutte le stazioni il periodo di attesa con un numero random di slot. Se la stazione che ha inviato il pacchetto non riceve l'ACK, vuol dire che c'è stata una interferenza ed il pacchetto è ri−inviato immediatamente. Non ci sono Sliding Windows come in TCP, al contrario il protocollo è più semplice, minimizza i ritardi e garantisce l'arrivo in sequenza dei pacchetti. Questo è necessario perché la probabilità di errori è molto più alta nelle trasmissioni Wireless che in quelle su cavo, e se i pacchetti fuori sequenza o sequenze di pacchetti con omissioni fossero passati direttamente a TCP, le prestazioni sarebbero ulteriormente penalizzate poiché TCP richiederebbe la ritrasmissione di un gran numero di pacchetti. Inoltre in presenza di un mezzo con molti errori è conveniente trasmettere (e ri−trasmettere) pacchetti piccoli, e perciò frammentare i pacchetti grandi. Questo ha due vantaggi: se il pacchetto è piccolo è più facile che arrivi a destinazione intatto, e se non arriva la ritrasmissione è più veloce. Però frammentare i pacchetti richiede ripetere su ognuno gli headers MAC e quindi si riduce il throughput.

Un ulteriore problema è quello dei nodi nascosti (Hidden Nodes). Supponiamo di avere tre stazioni disposte in linea una dopo l'altra in modo tale che la stazione centrale riesca a parlare con la prima e la terza, ma che a causa dell'attenuazione del segnale la prima non riesca a parlare direttamente con la terza. Supponiamo che non ci interessi far parlare direttamente la prima e l'ultima stazione poiché la stazione centrale è il nostro Access Point e le due stazioni laterali devono parlare solo con esso. Il problema è che le due stazioni laterali non sono in grado di sentire se vi è una trasmissione in corso da parte dell'altra stazione laterale, e quindi la probabilità di collisioni aumenta di molto. Per risolvere questo problema, prima di trasmettere un pacchetto la stazione invia un piccolo pacchetto RTS (Request To Send) ed attende che il ricevente risponda con un CTS (Clear To Send) prima di inviare il proprio pacchetto. Bisogna notare che quando il ricevente (nel nostro esempio la stazione centrale) manda un CTS, tutte le stazioni nel suo raggio lo sentono

e quelle che non hanno inviato il RTS capiscono che un'altra stazione sta trasmettendo e quindi tacciono per evitare collisioni (i pacchetti RTS/CTS contengono anche la lunghezza del pacchetto da trasmettere, il che fornisce alle altre stazioni una stima del tempo di attesa). In questo modo teoricamente le collisioni possono avvenire solo per pacchetti RTS, che sono molto piccoli e quindi non molto tempo è perso. D'altra parte l'overhead del meccanismo RTS/CTS è parecchio, e di nuovo diminuisce il throughput totale.

L'802.11b prevede trasmissioni ad una velocità massima di 11Mbps; vista la discussione precedente non è difficile capire che il throughput effettivo a livello IP può essere al più di 6Mbps. Ovviamente questa banda è condivisa da tutte le stazioni presenti in una zona poiché solo una può trasmettere in un certo momento. Quindi se più di due stazioni sono presenti la banda effettiva a disposizione di ognuna di esse nel caso in cui tutte debbano trasmettere può essere di molto inferiore, nel caso peggiore sino a 6/n Mbps con n stazioni. Spesso la banda effettiva disponibile si aggira intorno ai 3Mbps, come per un Ethernet a 10MHz.

4. 802.11b

Nel settembre 1999, il comitato 802 dell' IEEE decise di estendere lo standard allora conosciuto come 802.11 con nuove specifiche riguardo la modulazione e la crittazione del segnale. Questo standard si chiama 802.11b ed è al giorno d'oggi sinonimo di Wireless LAN. Un'altro sinonimo conosciuto per l'802.11b è Wi−Fi (Wireless Fidelity) che è un consorzio di produttori che garantisce l'interoperabilità tra schede di rete ed Access−Point 802.11b di marche diverse.

Nell'802.11b le modifiche sostanziali furono adottate a livello fisico con l'adozione della modulazione DSSS (Direct Sequence Spread Spectrum) la quale, nonostante sia più costosa e più sensibile ai disturbi del FHSS, permette come abbiamo visto una maggiore banda passante. Per tutte le altre specifiche ricalca totalmente l'802.11 dal quale eredita sia il metodo di accesso e di autenticazione all'Access Point, sia la crittazione dei dati tramite il "famigerato" protocollo a chiave fissa, il WEP, che sarà oggetto di analisi insieme alle vulnerabilità ed alle contromisure in un altro articolo.

Come abbiamo già indicato, l'802.11b a livello fisico utilizza la HR/DSSS (High Rate DSSS). A livello Datalink abbiamo il MAC (Media Access Control) che descrive l'insieme delle regole di accesso al media ed il LLC (Logical Link Control) proprio di qualunque protocollo LAN 802. A lato i protocolli 802.3 (l'usuale Ethernet) e per il Wireless anche l'802.5, i quali specificano la contenzione del media ed il metodo per evitare le collisioni dei pacchetti, come già visto. In particolare ad ogni stazione è associato un numero identificativo, il MAC Address, come per il

comune Ethernet. Quindi a livello 2 una rete Wireless appare esattamente come una (vecchia) rete Ethernet cablata con BNC (quindi non con uno switch ma con un bridge).

In una infrastruttura Wireless è possibile realizzare due tipi di topologia che identificano come le stazioni parlano l'una con l'altra. La prima è detta IBSS (Indipendent Basic Service Set) dove ogni stazione può comunicare direttamente con qualunque altra. Questa particolare topologia à detta *Ad Hoc* e viene utilizzata per piccoli gruppi di lavoro. Al crescere delle esigenze e per lo sfruttamento di uno dei cardini delle Wireless LAN, la mobilità, è necessaria l'introduzione di un dispositivo centrale di controllo: l'*Access Point*. L'Access Point è l'equivalente di un Bridge nelle reti Ethernet e svolge la funzione di ridistribuzione dei frame tra le stazioni, e la gestione del roaming. Questa topologia è detta *Infrastructure BSS*. Più BSS possono essere connesse fra loro al fine di coprire aree più vaste. Questa nuova topologia si chiama *ESS* (Extended Service Set).
Stazioni con lo stesso ESS possono comunicare tra loro anche se appartengono a BSS diverse e stanno transitando tra diversi Access Point. L'Access Point in una topologia ESS, permette a chiunque esterno alla rete Wireless, di accedere ad una stazione Wireless utilizzando un singolo MAC, funzione propria di un bridge. Gli Access Point, effettivamente, lavorano come dei bridge e quindi sono in grado di aggiornare le loro tabelle ARP con l'elenco dei MAC address delle stazioni sotto copertura. E' possibile nell'ambito di una rete Wireless che una stazione sia in copertura contemporanea di due AP. Per evitare sovrapposizioni ambigue di indirizzi, gli AP comunicano tra loro aggiornandosi le tabelle di ARP con il protocollo *IAPP* (Inter−Access Point Protocol) il quale realizza a tutti gli effetti un sistema di distribuzione. Gli Access Point possono usare l'IAPP sia tramite il backbone cablato che tramite il segnale radio. Al momento le implementazioni commerciali dell'IAPP sono realizzate con protocolli proprietari e funzionano correttamente in un ambiente con Access Point dello stesso vendor.

Prima di utilizzare un network bisogna... trovarlo. Nel caso di una rete cablata è semplice, basta collegare il cavo, ma nel caso di una rete Wireless le cose si complicano moltissimo. Nell'ambito Wireless il processo di scoperta ed identificazione della rete è detto ***scanning***. I diversi parametri che sono utilizzati in questa procedura possono essere specificati dall'utente ma molti sono di default nei driver delle schede Wireless. I parametri più importanti sono:

- ***Tipo BSS***. Indentifica se la rete è *Ad Hoc* oppure *Infrastructured BSS*
- ***SSID***. Assegna una stringa di bit ad un ESS. Molti produttori identificano il SSID con il nome del network
- ***BSSID***. Identifica se l'SSID è inviato o no in broadcast

- ***Scan Type***. E' attivo se la stazione invia pacchetti per identificare la rete, passivo se rimane in ascolto dei pacchetti *beacon* inviati dall'Access Point o dalle altre stazioni
- ***Channel list***. Invio della lista dei canali disponibili sui quali tentare una connessione oppure rimanere in ascolto per identificare quale sia il canale utilizzato.

Nello scanning passivo la stazione rimane in ascolto dei pacchetti di beacon dell'Access Point. Nei pacchetti di beacon vi sono i parametri necessari ad una stazione al fine di collegarsi al network: tipo di BSS, SSID e canale da utilizzare. Nello scanning attivo, una stazione piuttosto che ascoltare trasmette dei pacchetti, canale per canale, richiedendo l'accesso ad uno specifico ESS. Al termine dello scan, attivo o passivo, la stazione ha l'insieme dei parametri necessari a connettersi alla rete: tipo di BSS, SSID e canale da utilizzare. A questo punto la stazione può passare alla autenticazione. Nell'802.11 i metodi di autenticazione usati sono l'***open system*** e la ***shared key:***

- *Autenticazione Open System*

  Con l'autenticazione open system, l'Access Point accetta la connessione da qualunque stazione senza verificarne l'identità. L'unico parametro identificativo preso in considerazione è il MAC address sul quale è possibile eseguire delle regole di filtraggio.
- *Autenticazione Shared key*

  L'autenticazione shared key utilizza il WEP (Wired Equivalent Privacy) ed implica che ogni stazione abbia il WEP attivo ed utilizzi una shared key. In questa procedura viene introdotto un meccanismo di controllo della shared key tramite l'utilizzo della stessa per criptare un 'challenge text' e la sua decriptazione che può avvenire solo se le due shared key sono uguali.

Una volta che l'autenticazione è stata completata la stazione può *associarsi* ad un Access Point o riassociarsi ad un nuovo Access Point nel caso di roaming. L'associazione è una procedura di registrazione della identità della stazione in modo che il sistema di distribuzione sappia sempre dove la stazione è per indirizzare correttamente i frame. Dopo che l'associazione è stata completata l'Access Point deve registrare la stazione nella rete cablata in modo che i frame destinati alla stazione siano corettamente inviati all'Access Point. Un metodo di registrazione è associare il MAC della stazione alla porta dello switch dove l'Access Point è collegato tramite il protocollo ARP. Dopo che la stazione è autenticata sull'AP viene inviato un pacchetto di *association request*. L'Access Point processa l'association request. Se l'associazione va a buon fine l'Access Point comincia a far transitare i frame da e per la stazione.

Infine la *riassociazione* è il processo di spostamento di una associazione da un vecchio Access Point ad uno nuovo. Se nel raggio di azione di una stazione vi è un altro AP con lo stesso ESS, la

stazione ne monitorizza la qualità del segnale. Quando la stazione decide che questo nuovo Access Point è una scelta migliore, inizia la procedura di riassociazione: invia una richiesta di riassociazione al nuovo AP specificando quale era il suo vecchio AP, il nuovo Access Point comunica con il vecchio, tramite il protocollo IAPP, verificando che la stazione fosse realmente a lui associata. In caso positivo accetta la associazione comunicandola al vecchio Access Point il quale forwarda al nuovo Access Point gli eventuali pacchetti bufferizzati da inviare alla stazione e termina l'associazione della stazione. La procedura è conclusa e la stazione ha cambiato Access Point in modo del tutto trasparente all'utente.

In questa serie di articoli abbiamo presentato i principali protocolli utilizzati sia dagli 802.11 che da altri protocolli Wireless nei livelli più bassi della pila OSI. Riteniamo infatti che una comprensione dei molteplici aspetti della sicurezza di una rete Wireless si basi sulla conoscenza del funzionamento di tutti i suoi componenti, dal livello fisico, in questo caso le onde radio, in su. Armati di queste informazioni, in un futuro articolo ci occuperemo più dettagliatamente dei problemi di sicurezza facendo riferimento in modo particolare all'802.11b.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Fabrizio Croce
Country Manager Italy WatchGuard Technologies
fabrizio.croce@watchguard.com

Riferimenti Bibliografici:

[1] Wireless LAN Association (presso http://www.wlana.org/)
[2] WiFi (presso http//www.wirelessethernet.org/
[3] WECA (presso http://www.weca.org/)
[4] IEEE (presso http://www.ieee.org/)
[5] J. Tourilhes, *Wireless LAN Howto* (presso http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/)
[6] Stefano Quintarelli, *Wireless Fidelity* (presso http://www.clusit.it/)
[7] Jim Zyren e Al Petrick, *802.11 Tutorial* (presso http://www.ieee.org/)
[8] Wireless Communications Association International (presso http://www.wcai.com/)