UNIVERSITÁ DEGLI STUDI DI PADOVA

FACOLTÀ DI INGEGNERIA
CORSO DI LAUREA TRIENNALE IN INGEGNERIA
DELLE TELECOMUNICAZIONI

RETE WIRELESS :
CONTROLLO ACCESSI, PROBLEMI E SOLUZIONI

Relatore: Prof. Zanella Andrea

Tesina di Laurea di: Mazzucconi Domenico Manuel

ANNO ACCADEMICO 2009-2010

INDICE

Ai miei Nonni
che mi hanno amato sempre

Ai miei Genitori e
A mia Sorella
che mi hanno sostenuto sempre

al mio Amore
che mi è vicino sempre

Capitolo 1

INTRODUZIONE

Negli ultimi anni il mercato dell'informatica è stato caratterizzato da un rapido sviluppo delle reti wireless. Il termine wireless indica i sistemi di comunicazione tra dispositivi elettronici, che non fanno uso di cavi. I sistemi tradizionali basati su connessioni cablate sono detti infatti wired. Generalmente i wireless utilizzano onde radio a bassa potenza, tuttavia la definizione si estende anche per i dispositivi, meno diffusi, che sfruttano la radiazione infrarossa o il laser.

Molti utenti e aziende hanno introdotto questa tecnologia nei loro sistemi informatici alla ricerca di una maggiore flessibilità e mobilità, ma nello stesso tempo si sono incominciati ad analizzare i problemi legati alla sicurezza. I segnali radio ,essendo diffusi nell'etere, possono essere infatti intercettati senza difficoltà, di conseguenza è necessario prendere contromisure di tipo crittografico per garantirne la riservatezza.

È evidente che in questa situazione le necessarie misure di sicurezza hanno caratteristiche differenti da quelle normalmente adottate per le reti cablate.

La prima misura di sicurezza è la modulazione dell'onda elettromagnetica, che grazie ad opportune tecniche rende più complessa l'intercettazione del segnale.

La modalità di modulazione da sola non garantisce la sicurezza della rete, infatti in mancanza di un controllo dell'accesso è possibile per un utente non autorizzato o, peggio, malintenzionato, accedere alla rete semplicemente passando, con un PC e una scheda wireless, vicino all'edificio nel quale è installata la rete. I sistemi per controllare l'accesso alle reti wireless si basano su diverse metodologie che operano a livelli diversi del modello ISO-OSI.

Queste forme di controllo dell'accesso alla rete sono, attualmente, molto diffuse e forniscono un livello di autenticazione di base, il livello di sicurezza offerto da questi servizi non è sufficiente per poter considerare sicure le reti wireless, nonostante l'uso di algoritmi di cripting dei dati. Per questi motivi, il mercato sta spingendo verso forme di autenticazione più complesse e più sicure, basate su database che, oltre al semplice riconoscimento dell'utente, forniscono anche servizi aggiuntivi. Lo standard 802.1x, si muove in questa direzione, sfruttando una autenticazione attraverso server Radius.(Remote Authentication Dial-In User Service è un protocollo AAA authentication, authorization, accounting)

In questa tesina,inoltre, si è scelto di analizzare i sistemi che permettono di gestire l'accesso e l'autenticazione in una rete wireless appartenenti alla categoria dei software che viene chiamata Captive portal che si basa sulla ridirezione del traffico non autorizzato verso una pagina di autenticazione.

L’idea che sta dietro al concetto di Captive portal è semplice: invece che basare la sicurezza della rete sui servizi offerti dallo standard 802.11b che si sono dimostrati molto deboli e quindi concentrare il servizio di autenticazione nell’access point, si inserisce un gateway immediatamente dietro all’access point che si occupi di tale compito. In questo modo il servizio di autenticazione non viene implementato nell’access point evitando problemi di compatibilità simili a quelli tra l’802.1x e gli access point attuali.
Questi sistemi gestiscono l’autenticazione degli utenti a livello Network dello stack ISO-OSI fornendo un livello di sicurezza superiore a quello fornito dallo standard 802.11b.
Il punto di forza di questi sistemi è sicuramente la facilità d’uso: non richiede l’istallazione di alcun software nel lato client, a differenza di altre tecnologie come le VPN, e autentica i vari utenti attraverso pagine web, quindi con una interfaccia user-friendly, ed inoltre permettendo di aggiungere altri servizi come il controllo di routing. Gestiscono quindi l’autenticazione degli utenti a livello Network dello stack ISO-OSI fornendo un livello di sicurezza superiore a quello fornito dallo standard 802.11b.
Nella presene tesina vengono introdotte le caratteristiche delle reti wireless (Capitolo 2), i principali metodi di controllo dell’accesso come 802.1x e WPA (Capitolo 3) ed infine vengono analizzate le caratteristiche e l’accesso e l’autenticazione in una rete wireless appartenenti alla categoria dei software che viene chiamata Captive portal(Capitolo 4)

Capitolo 2

LE RETI WIRELESS

La storia del Wireless Networking si estende indietro nel tempo molto più di quanto si possa immaginare, più di sessanta anni fa durante il secondo conflitto mondiale , quando l'esercito degli Stati Uniti utilizzò per primo i segnali radio per la trasmissione dati sviluppando una tecnologia di radiotrasmissione dei dati che era basata su tecniche di criptazione , e tramite la SST (Spread Spectrum Tecnology : tecnica di dispersione spettro) riuscì ad evitare l'intercettazione o il disturbo delle comunicazione al nemico.

Nel 1971 un gruppo si ricercatori ispirandosi a quanto elaborato nel periodo bellico, creò la prima rete di comunicazione radio a pacchetto, AlohNet questo era il nome della rete, fu essenzialmente la prima rete wireless local area network conosciuta poi in seguito con il suo acronimo WLAN. La prima WLAN era costituita da sette computers che comunicavano bi-direzionalmente in una topologia a stella , cioè con un computer centrale denominato hub attraverso il quale circolavano tutte le trasmissione. Con questa topologia è stato possibile, in caso di interruzione del collegamento tra un pc e hub, che fosse solo il pc interessato a non poter trasmettere più, lasciando tutti gli altri in funzione. Naturalmente la tecnica di trasmissione era differente da quella dei moderni AP(Acces Point) ed anche la frequenza di trasmissione, che si basava sui 900 MHz, era differente rispetto alla banda di frequenza di trasmissione usata oggi con il Wi-Fi (Wireless Fidelity) dei 2,4GHz.

Una rete WLAN è composta essenzialmente da due tipi di dispositivi, da AP(Acces Point) e WT (Wireless Terminal), dove gli AP sono i punti di accesso alla rete e svolgono la funzione di ponte tra la rete wireless e la rete fissa , ad essi infatti, si collegano uno o più wireless client che possono avere accesso alla rete cablata e comunicare tra loro. I WT possono essere dispositivi diversi quali pc, notebook, palmari, cellulari, che una volta collegati alla WLAN possono comunicare con tutti gli host sia di rete wireless che rete cablata.

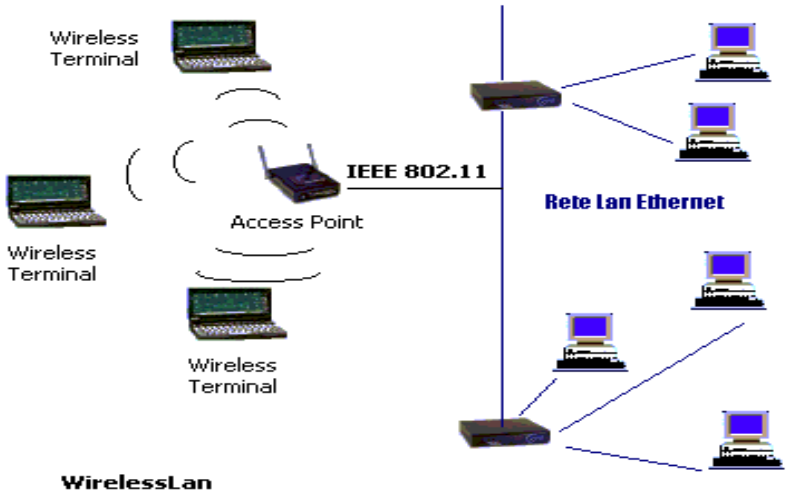


Figura 2-1: rete wireless con AP e WT

All'inizio degli anni novanta , fu approvato lo standard IEEE (Istitute of Elettrical and Electronics Engineers) dove il comitato IEEE 802 si occupa delle reti e il gruppo 802.11 detta le specifiche per l'implementazione di una rete WLAN. Questo standard, impiegava all'inizio i raggi infrarossi e in seguito la tecnologia su onde radio nella banda 2,4 GHz che supportava un transfer rate o bit rate di 1 o 2 Mbps. Fu proprio il confronto tra i bit rate di una rete ethernet e quello di una WLAN a rallentare la diffusione della nuova tecnologia . Successive modifiche ottimizzarono e aumentarono la velocità e fu denominato, ad opera della W.E.C.A. (Wireless Ethernet Compatibility Alliance) organizzazione con l'obiettivo di promuovere la tecnologia Wi-Fi con high rate per le reti wireless, il nuovo standard 802.11 b conosciuto come appunto Wi-Fi dotato di un bit rate pari a 11 Mbps e successivamente con l'adozione di altri standards si è arrivati alla velocità di 100Mbps. Per la prima volta, le wireless LAN potevano essere utilizzate dalla maggior parte degli ambienti operativi e delle applicazioni per l'ufficio. I vari fornitori iniziarono a supportare in breve tempo lo standard 802.11b con una conseguente e sostanziale diminuzione dei costi, un aumento della domanda ed un maggiore supporto da parte loro. Inoltre, lo standard 802.11b assicurava agli utenti l'interoperabilità dei dispositivi. Con la rapida adozione dello standard 802.11b, gli utenti hanno potuto scegliere tra un'ampia gamma di dispositivi wireless ad alte prestazioni, interoperabili e di basso costo. Tuttavia, ancora più importante è stata la possibilità, per molte aziende, di aumentare il proprio valore con l'aggiunta della tecnologia wireless alla propria LAN aziendale, che ha permesso a laptop ed notebook elaborazioni in ogni luogo e in qualsiasi momento. Una possibilità che le reti wireless hanno offerto agli utenti è la massima flessibilità, produttività ed efficienza e hanno dato una forte spinta alla collaborazione ed alla cooperazione tra colleghi, partner commerciali e clienti. Le reti wireless presentano una serie di vantaggi sostanziali rispetto alle reti classiche, ai quali però si contrappongono non poche limitazioni, a causa di un discreto numero di problematiche,

dovute principalmente alla natura stessa di reti nelle quali la connettività è basata sull'uso di un mezzo inaffidabile come l'etere. Analizziamo in dettaglio, qui di seguito, i vantaggi e problemi, portati da questa nuova tecnologia.

2.1 Vantaggi

La mancanza di collegamenti fisici tra i vari terminali assicura alle reti wireless delle caratteristiche uniche che hanno portato alla rapida diffusione di questa tecnologia.
Una rete wireless non richiede infatti la posa dei cavi, e può essere realizzarla in un tempo molto breve, è quindi di **facile installazione** . E' possibile realizzare queste reti per fornire la connessione tra computer senza sostenere spese e tempi associati all'istallazione del mezzo fisico.
Al contrario le reti wired consentono lo scambio di informazioni tra i vari utenti grazie alla presenza dei cavi. Per realizzare una Lan, sono necessarie settimane di lavoro per sistemare i cavi (doppini o le fibre ottiche). L'istallazione di fibre ottiche tra edifici all'interno della stessa area geografica può essere realizzata solo dopo aver ottenuto i permessi per poter effettuare gli scavi necessari per collocare le fibre e tutto ciò prolunga il tempo necessario all'istallazione della rete.
Non va sottovalutato che i costi relativi alla posa dei cavi sono forse la parte più onerosa nella realizzazione di una LAN, l'adozione del wireless porta dunque ad una sensibile riduzione dei costi in questo senso, con gli ovvi benefici che ne conseguono.
Le WLAN sono intrinsecamente scalabili**,** è possibile infatti crearne dapprima una con pochi terminali e poco alla volta, a seconda dei bisogni che via via si creano, è possibile acquistare nuovi dispositivi e connetterli, con minima fatica e senza bisogno di complicate (e costose) opere di connessione, configurazione e posa dei cavi. La filosofia stessa delle WLAN è decisamente improntata sul plug and play, la semplicità d'uso e la dinamicità nella configurazione.
La **scalabilità** è un fattore molto importante anche dal punto di vista economico, la WLAN può crescere di dimensioni e potenza col crescere delle necessità degli utenti. Si consideri, per esempio, una WLAN caratterizzata inizialmente da un basso throughput, che potrà essere utilizzata in futuro per soddisfare la necessità di una banda più ampia. In questo caso, una possibile configurazione potrebbe essere caratterizzata dalla collocazione di diversi access point, uno per ogni gruppo di utenti, per aumentare il throughput aggregato.

Questa configurazione aumenta notevolmente la performance delle WLAN e rende possibile una buona gestione delle prestazioni in presenza di un aumento del numero di utenti.
Un ulteriore vantaggio, che è uno degli aspetti cardine delle WLAN e che può farne una scelta strategica in molti ambiti, è la **mobilità** infatti tutti i WT possono connettersi alla rete senza richiedere un collegamento fisico e l'utente può scegliere se stare alla propria scrivania o spostarsi liberamente in un'altra stanza, in ambienti esterni o interni, il tutto rimanendo connesso alla rete.
Grazie alla funzionalità di Roaming tra diversi Access Point, l'utente può comunicare con continuità anche spostandosi all'interno di un'area più vasta di quella coperta da un singolo Access Point.
Al contrario, la rete wired richiede il collegamento fisico tra la workstation e le risorse di rete e un utente deve interrompere il suo collegamento alla rete e realizzarne un altro quando vuole spostarsi da un ambiente ad una altro, non senza problemi.

2.2 Svantaggi

Le grandi potenzialità delle reti wireless, legate principalmente al tipo di mezzo trasmissivo che si è deciso di utilizzare, l'etere, hanno proprio in questo anche il loro punto debole.
Uno dei più grandi problemi che si incontrano nell'adozione delle tecnologie Wireless per le reti locali è l'intrinseca **inaffidabilità** del mezzo trasmissivo.
E' ovvio che l'adozione o meno di una WLAN è fortemente condizionato dall'ambiente di utilizzo, non sono certo indicate aree con alto rumore elettromagnetico, e comunque, qualunque sia l'ambiente scelto, non è pensabile che la trasmissione via etere sia immune da interferenze che hanno un impatto critico sulla trasmissione dati.
Le WLAN ovviamente sono soggette a disturbi e l'etere, con il passare del tempo, è divenuto molto trafficato. Le interferenze che una WLAN può subire sono molteplici, le microonde per esempio, lavorano proprio nella banda di 2.4 GHz, che è proprio una di quelle utilizzate per trasportare i dati provenienti da una wireless LAN.
Queste difficoltà si riflettono sia nel livello MAC , ove è necessario adottare opportune tecniche di rilevamento dell'errore, che nel livello fisico, per il quale sono state sviluppate diverse metodologie di trasmissione (FHHS, DSSS, HR-DSSS, OFDM), alcune adottate in 802.11a ed altre in 802.11b, che si differenziano nello sfruttamento che hanno dello spettro del segnale,"spalmando" nel tempo lo spettro del disturbo, che tipicamente ha una banda molto stretta, per ridurne così i problemi che verrebbero a generarsi.

L’utilizzo di onde elettromagnetiche per la trasmissione in ambienti chiusi, come uffici, presenta anche il problema della **propagazione** del segnale su più percorsi, tipicamente causata da **riflessioni** su muri, oggetti metalliche etc..

Le soluzioni adottate dai costruttori sfruttano sia l’utilizzo di tecniche di equalizzazione e processamento del segnale, sia l’adozione di particolari antenne.

In particolare il ricevitore può utilizzare anche più d’una antenna per ricevere, in pratica se ne usano spesso due.

Legato principalmente agli aspetti inerenti la trasmissione e gli errori il range di utilizzo può raggiungere al massimo i centocinquanta metri circa. Non si può trasmettere a distanze più elevate anche perché si vogliono mantenere basse le potenze in gioco.

Da notare che la velocità con cui si trasmette è inversamente proporzionale alla distanza, dunque per trasmissioni ad alta velocità (802.11a raggiunge i 54Mb/s) non si potranno superare alcune decine di metri, per esempio 802.11a alla massima velocità comunica fino a 30m.

L’adozione delle WLAN in Italia è piuttosto recente , anche a causa di una legge che limitava la libertà d'utilizzo di queste periferiche se non altro perché era prevista una tassa. Va detto che recentemente questa tassa è stata abolita e l'uso di periferiche che trasmettano su onde radio è libero purché siano omologate dal Ministero delle Comunicazioni o che abbiano il marchio CE. Prima dell'entrata in vigore della nuova normativa, gli apparecchi wireless erano infatti assimilati alle apparecchiature radio-amatoriali e professionali. Con questo provvedimento l'Italia si è allineata alle direttive europee e alla normativa già in vigore negli altri Paesi dell'UE.

Uno degli aspetti più delicati inerenti le reti Wireless è la **sicurezza.** La trasmissione dati su questo tipo di reti infatti avviene tramite segnali elettromagnetici che sono potenzialmente ascoltabili da chiunque si trovi nel range di utilizzo (ovviamente purché possieda l’apparecchiatura adatta).

E’ facile immaginare che il diffondere informazioni magari confidenziali attraverso una antenna sia assolutamente da evitare, a meno che non si prendano precauzioni di qualche natura. Sono infatti molteplici i rischi che corre una WLAN, dall’ascolto delle trasmissioni allo scopo di ottenere dati, all’intrusione nella rete fino al sabotaggio vero e proprio che si può compiere semplicemente facendo sì che sia sempre presente un segnale di fondo.

E’ da tenere in considerazione come la presenza di una parte wireless su di una rete mista (con parti cablate e parti wireless) possa essere potenzialmente fonte di inaffidabilità per tutta la rete nel suo complesso. I meccanismi di autenticazione/privacy si basano sull’algoritmo WEP (Wired Equivalent Privacy).

Nonostante questi meccanismi le reti wireless rimangono, comunque, facilmente attaccabili e al momento non si è raggiunto un livello di sicurezza adeguato.
Le reti WLAN inoltre non fornendo **connessioni** affidabili, sono un problema per i protocolli di livello superiore, come TCP o UDP.
Quando si ha a che fare con reti wireless, il protocollo TCP tende a perdere le connessioni, soprattutto se la copertura di rete è marginale.

2.3 Famiglia di protocolli

Il primo standard di riferimento per le reti wireless, l'IEEE 802.11 nacque nel 1997. Lo standard includeva requisiti dettagliati per il livelli fisico e per la parte inferiore del livello data-link, ovvero il MAC (Medium Access Control), seguendo le specifiche dello standard IEEE 802.

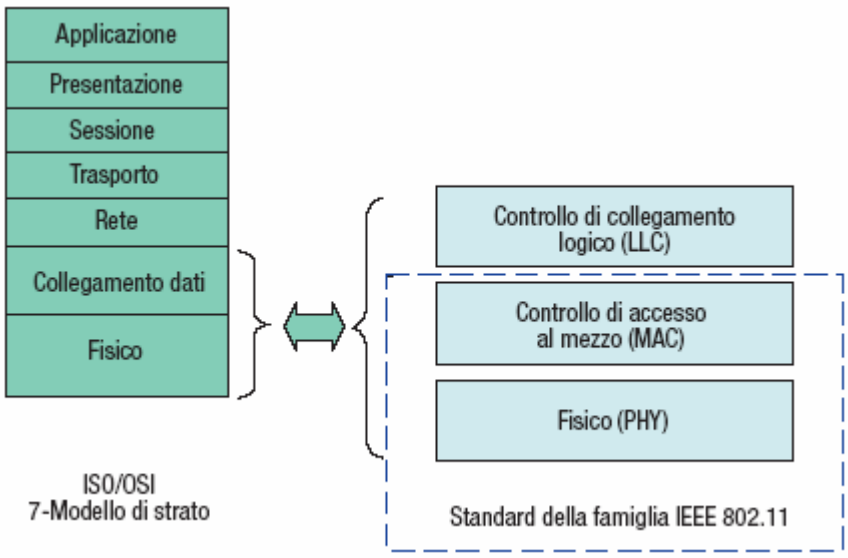


Figura 2-2: Il modello iso-osi e il protocollo 802.11

Tale standard consentiva un data rate di 1 o 2 Mbps usando la tecnologia basata su onde radio nella banda 2.4 GHz o su raggi infrarossi. La limitata velocità ne determinò uno scarso successo e diffusione.
Per migliorare il throughput l'IEEE ha creato, all'inizio, 2 gruppi di lavoro (a e b) per esplorare nuove implementazioni, ad esse successivamente si è aggiunto un nuovo gruppo (g). Essi avevano il compito di creare nuovi standard che si accostarono al 802.11 base.

IEEE 802.11a

Lo standard 802.11a offre una velocità di trasmissione massima dei dati di 54 Mbps ed otto canali di frequenza non sovrapponibili, operando a 5 GHz con 150 MHz di larghezza di banda. Usa la tecnica di modulazione OFDM (Orthogonal Frequency Division Multiplex) di tipo multi-portante, che utilizza un numero elevato di sottoportanti ortogonali tra di loro.
Il vantaggio primario dell'OFDM rispetto agli schemi a singola portante è l'abilità di comunicare anche in condizione pessime del canale, ad esempio nei casi in cui si presenta un'attenuazione ad alta frequenza, come nei doppini di rame, oppure interferenze a banda stretta. Queste caratteristiche consentono di aumentare la capacità di rete, migliorare la scalabilità e di creare implementazioni microcellulari senza interferenze dalle celle adiacenti. Con l'utilizzo della porzione di banda radio libera da 5 GHz, lo standard 802.11a è anche immune da interferenze provenienti da dispositivi che operano sulla banda da 2,4 GHz, come i forni a microonde, i cordless e Bluetooth (un protocollo wireless point-to-point, a bassa velocità e portata).

IEEE 802.11b (Wi-Fi)

Lo standard 802.11b è il protocollo di trasmissione wireless più diffuso, definisce lo strato fisico e lo strato di accesso al mezzo fisico (etere) delle WLAN. Utilizza il range di frequenze 2,4 GHz consentendo bit-rate fino a 11 Mbit/s (teorici). Lo strato fisico utilizza il sistema di codifica denominato DSSS (Direct Sequence Spread Spectrum) un sistema simile alla codifica CDMA (Code Division Multiple Access) dove però il codice utilizzato è condiviso da tutti i dispositivi wireless in rete (host e access point). Per tale motivo il DSSS non può essere considerato un sistema di accesso multiplo al canale, bensì rappresenta un meccanismo per "spalmare" l'energia del segnale trasmesso su uno spettro di frequenze più ampio in modo da facilitare al ricevitore la ricostruzione del segnale trasmesso. Le comunicazoni wireless sono, per loro natura, sensibili all'attenuazione del segnale (esponenziale all'aumentare della distanza) ed a ostacoli interposti tra trasmettitore e ricevitore , pertanto la probabilità di collisioni è sicuramente un fattore rilevante. Per ovviare a ciò lo strato di accesso al mezzo trasmissivo utilizza il protocollo CSMA-CA (Carrier Sense Multiple Access-Collision Avoidance) un sistema che consente lo scambio affidabile di frame a livello di data-link. Lo standard 802.11a, tuttavia, non è compatibile con gli attuali dispositivi wireless conformi all'802.11b. Le organizzazioni con dispositivi 802.11b che desiderano avere ulteriori canali e la velocità offerta dalla tecnologia 802.11a devono installare un'infrastruttura wireless completamente nuova con

access point 802.11a e adattatori client. È importante notare che i dispositivi a 2,4 e 5 GHz possono operare nello stesso ambiente fisico senza interferenze. Ulteriore caratteristica prevista dal protocollo prevede che al degradare del link tra access point e dispositivo remoto (o tra due card in reti ad-hoc) la velocità di trasferimento venga ridotta (gli step sono: 11Mbps, 5,5Mbps e 2Mbps). Da posizioni particolarmente "infelici" pur continuando ad essere connessi, le prestazioni subiranno un notevole degrado.

IEEE 802.11g

Lo standard 802.11g esiste da circa metà del 2003 ed offre anch'esso una velocità massima di trasmissione dei dati di 54 Mbps ma, rispetto all'802.11a, ha un ulteriore ed interessante vantaggio: la compatibilità verso le apparecchiature 802.11b. Ciò significa che le schede client 802.11b possono funzionare con gli access point 802.11g e le schede 802.11g con gli access point 802.11b. La migrazione all'802.11g sarà quindi conveniente per gli utenti con infrastrutture wireless 802.11b, poiché gli standard 802.11g ed 802.11b utilizzano entrambi la stessa banda libera a 2,4 GHz. I prodotti 802.11b non possono essere "potenziati a livello software" in 802.11g poiché, per garantire una velocità di trasferimento dei dati maggiore, le radio 802.11g utilizzano chip diversi dall'802.11b. Tuttavia, come per Ethernet e Fast Ethernet, i prodotti 802.11g possono operare insieme ai prodotti 802.11b sulla stessa rete.

IEEE 802.11i (WAP2)

IEEE 802.11i esiste da circa metà del 2004, è uno standard sviluppato dalla IEEE specificamente per fornire uno strato di sicurezza maggiore alle comunicazioni . L'802.11i rappresenta una estensione dello standard WEP. Prima dello standard 802.11i la Wi-Fi Alliance aveva introdotto il Wi-Fi Protected Access (WPA) un sottoinsieme delle specifiche 802.11i, ed era stato introdotto per tamponare l'emergenza sicurezza dovuta al WEP. La Wi-Fi Alliance inoltre ha deciso di chiamare le specifiche 802.11i con il nome di WPA2 per rendere semplice all'utente comune l'individuazione delle schede basate sul nuovo standard. L'802.11i utilizza come algoritmo crittografico l'Advanced Encryption Standard (AES) a differenza del WEP e del WPA che utilizzano l'RC4.

IEEE 802.11n

Oggi i prodotti elettronici consumer 802.11 precedenti allo standard "n" operano tranquillamente nella banda di frequenza dei 2.4 GHz. Lo standard 802.11n prevede una velocità dati massima teorica di 540 Mbit al secondo (200 Mbit/s typ) e il range arriva a 50 mt.

Per raggiungere throughput così elevati il segnale 802.11n deve occupare una banda molto più larga . L'approccio utilizzato per raggiungere questo livello di velocità dati prevede l'impiego di più antenne, sia lato trasmissione sia lato ricezione. Tutto il sistema è descritto dal termine "multiple-input-multiple-output" (MIMO) e come suggerisce il nome, un sistema MIMO contempla l'invio nell'etere di più segnali che vengono catturati da più antenne.
Il sistema implica un maggior impatto a causa delle interferenze indotte sugli apparati elettronici consumer circostanti. Tale impatto deriva da due grosse problematiche di progetto. La prima è la banda più larga utilizzata, la quale causa degli effetti collaterali che riducono il rapporto tra segnale e rumore (Signal to Noise Ratio - SNR). La seconda - denominata co-locazione - è legata al fatto che una banda più larga implica la disponibilità di un numero ridotto di canali "puliti" per gli altri dispositivi attivi nello stesso spettro di frequenza dei 2.4 GHz. Il protocollo individua e trasferisce la trasmissione dei dati sui canali puliti quando rileva dei segnali di interferenza Wi-Fi. La robustezza del protocollo deriva dalla metodologia utilizzata per la codifica e la decodifica dei dati. Un modo per codificare i dati è di utilizzare la tecnica DSSS *(Dynamic Sequence Spread Spectrum)*. Con questo metodo, ciascun bit di dati presente in un byte viene codificato con più bit utilizzando un codice Pseudo Noise (PN code). Il numero di canali disponibili e i codici PN danno vita a una mole tale di permutazioni che è possibile fare lavorare centinaia di radio all'interno del medesimo spazio di lavoro.

Standard	**Multiplazione**	**Frequenza**	**Velocità di trasferimento (Mbit/s)**
802.11 legacy	FHSS, DSSS, Infrarossi	2,4 GHz, IR	1, 2
802.11a	OFDM	5,2, 5,4, 5,8 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11
802.11g	OFDM	2,4 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11n	DSSS, HR-DSSS, OFDM	2,4 GHz	1, 2, 5,5, 11; 6, 9, 12, 18, 24, 36, 48, 54, 125

Tabella 2-1: Riassunto delle caratteristiche degli standard 802.11

2.4 Topologie di Wlan

L'architettura della rete *wireless* 802.11 è costituita da diversi componenti interagenti che supportano la mobilità delle stazioni in maniera trasparente ai livelli superiori dello stack protocollare.

Una wireless local area network, **WLan**, è un sistema di comunicazione flessibile e implementabile nella sua estensione, o alternativo, ad una rete fissa.

Una rete wireless può essere un'estensione di una normale rete cablata, supportando tramite un access point, la connessione a dispositivi mobili e a dispositivi fissi.

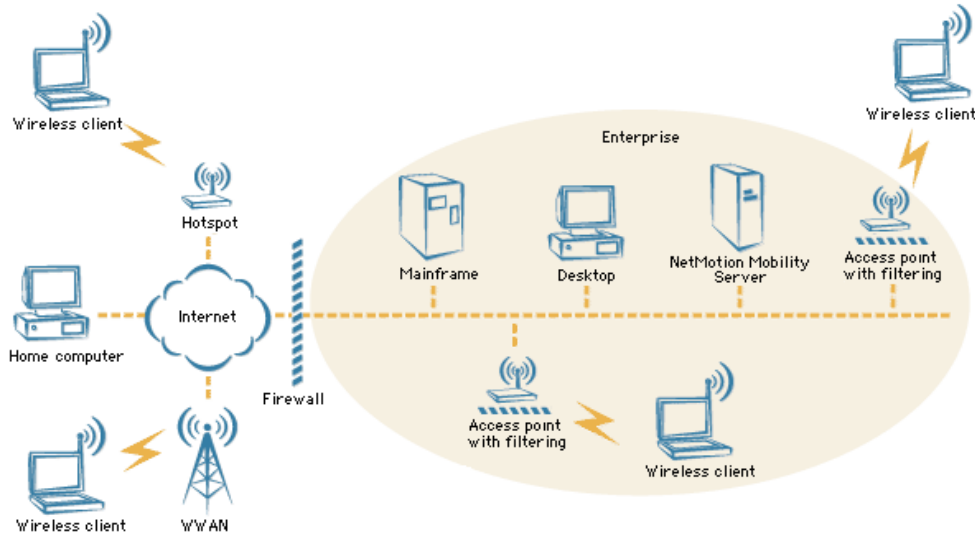


Figura 2-3: Collegamento tra una rete Wlan e una Ethernet

Il blocco fondamentale della WLAN è il ***Basic Service Set*** (**BSS**), definito come un gruppo di stazioni, fisse o mobili, collocate geograficamente all'interno di una cella, che possono stabilire connessioni dirette o con l'ausilio di strutture intermedie.

Nel primo caso, nel quale le stazioni comunicano direttamente l'una con l'altra, si parla di ***Independent*** **BSS** (**IBSS**): la rete *Ad Hoc* ne è un esempio (fig. 2.4) in cui gli utenti possono stabilire una connessione di trasferimento dati o di accesso ai dati in modalità *peer to peer* . In tale configurazione più unità WT possono comunicare tra loro direttamente realizzando una piccola rete paritetica, generalmente impiegata quando si necessita di una piccola rete per breve tempo, riunioni, convegni, stand, dimostrazioni.

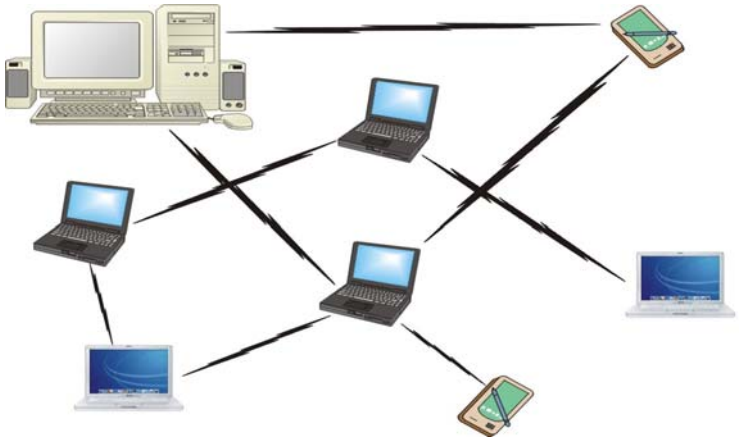


Figura 2.4 Schema di una rete IBSS Ad Hoc

Nel secondo caso, ovvero in una rete con infrastruttura, il BSS comprende, oltre alle stazioni, anche un ***access point*** (AP) che permette di connettere le stazioni all'interno della medesima cella. Volendo garantire una connettività il più possibile distribuita tra ambienti di una stessa sede, si sfrutta una tipologia Client Server. Questo modo di operare consente a più dispositivi di rete di appoggiarsi ad un Access Point che agisca da ponte tra loro e la rete wired. Nel caso in cui sia presente un solo access point si parla di BSS (basic service set). Gli access point provvedono alla coordinazione, sincronizzazione, spedendo pacchetti in modalità broadcast, e alla funzione di bridge verso reti wired, mentre i terminali wireless sono dei dispostivi che usufruiscono dei servizi di rete. L'AP (Access Point) assegna una priorità ad ogni client, in modo da rendere più efficiente la trasmissione dei pacchetti. Gli AP possono essere implementati sia in hardware che in software appoggiandosi per esempio ad un pc, o notebook dotato sia dell'interfaccia wireless sia di una scheda ethernet. I WT possono essere qualsiasi tipo di dispositivo come per esempio notebook, palmari, cellulari, o apparecchiature che interfacciano lo standard IEEE 802.11, o sistemi basati su tecnologia Bluetooth.

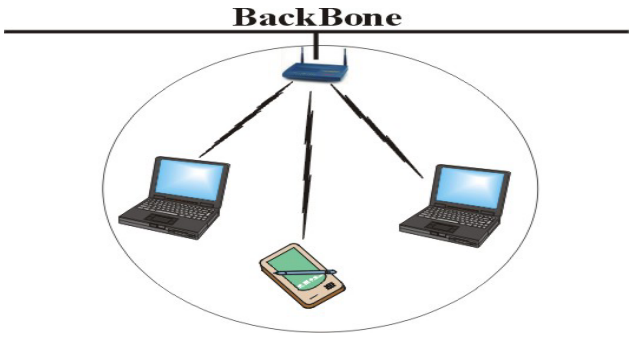


Figura 2.5 Schema di una Infrastructure Network BSS

Normalmente, una Infrastructure Network è formata da diverse celle e l'architettura di interconnessione tra i diversi BSS è il **Distribuition System (DS),** una sorta di backbone network responsabile del trasporto a livello MAC di un MAC Service Data Unit (MSDU). Il DS è indipendente dall'architettura della rete 802.11 e pertanto può essere indifferentemente una rete Wired Ethernet, Token Ring, o un'altra rete Wireless. L'intera WLAN, comprendente le varie celle, i loro rispettivi Access Points ed il Distribuition System, è vista come un'unica rete 802 che va sotto il nome di **Extended Service Set (ESS)** .

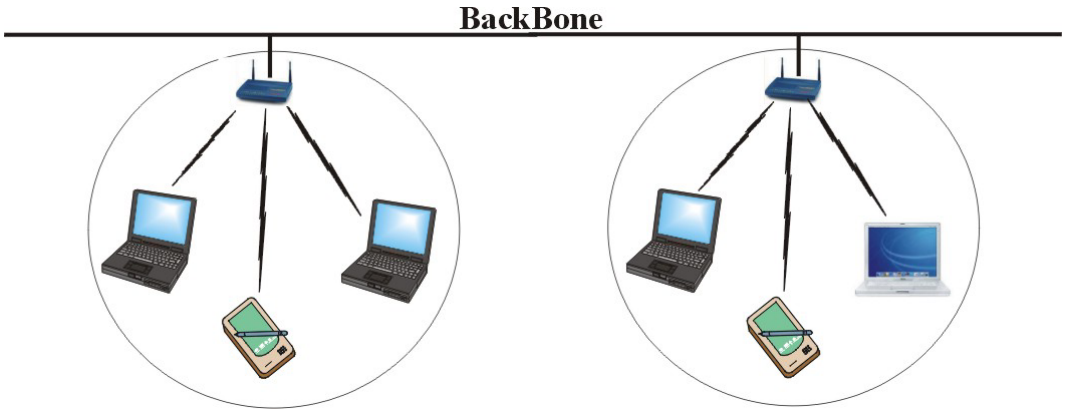


Figura 2.6 Schema di una Infrastructure Network ESS

2.5 MAC

La più grande differenza tra le reti ethernet e le reti wireless è il modo di controllare l'accesso al media condiviso MAC (Media access control). A differenza di una rete ethernet nelle wlan non è possibile durante la trasmissione rilevare le collisioni poiché si trasmette e si ascolta sullo stesso canale e i vari dispositivi hanno una potenza limitata tale che i vari messaggi non arrivano a tutte le stazioni, perciò una stazione non può identificare tutte le collisioni. Per risolvere il problema dell'impossibilità della rilevazione delle collisioni le Wlan utilizzano il CSMA/CA (carrier sense multiple access collision advoidance). Per poter effettuare una trasmissione diretta ad un altro nodo, il nodo sorgente deve spedire un pacchetto RTS (Request to send) al destinatario e se il nodo destinatario riceve il pacchetto, replica con un piccolo frame CTS (Clear to send), se non ci sono state collisioni significa che l'etere è libero e le stazioni che si trovano nelle circostanze sanno che sta per avvenire una trasmissione.
A questo punto il nodo sorgente spedisce i dati e quando è finita la trasmissione il destinatario manda un acknowledgement, in modo tale che le varie stazioni sappiano che la trasmissione è terminata . L'unico tipo di collisioni che può avvenire in questo protocollo è tra i pacchetti RTS e CTS, ma in questo caso si passa ad una ritrasmissione dei pacchetti dopo un tempo pari ad una variabile casuale uniformemente distribuita tra 0 e T. Inoltre nei vari pacchetti esiste un campo "durata" che permette alle varie stazioni di prevedere la durata delle trasmissioni al fine di ridurre le collisioni.

Figura 2-7: Schema di una trasmissione con il CSMA/CA

2.6 Tipi e struttura dei pacchetti

Le Wlan trasmettono tutte le informazioni sotto forma di pacchetti, usano 3 tipologie di frame, pacchetti di dati, di gestione della rete e di controllo. Il protocollo 802.11 è molto più complesso del rispettivo protocollo della rete Ethernet e questo si riflette nell'header dei vari frame. La struttura base di un frame 802.11 è la seguente:

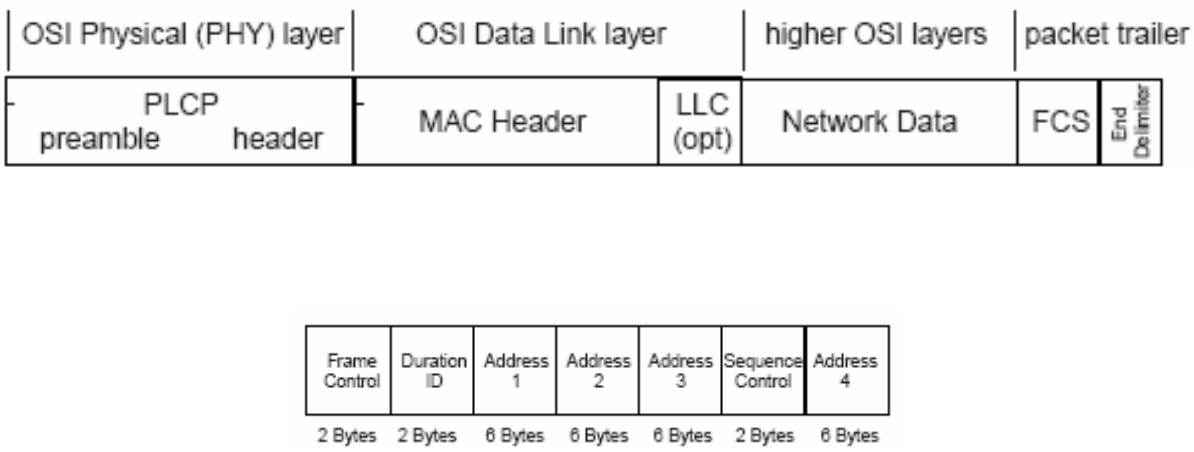


Figura 2-8: Formato di un frame 802.11 e del MAC header

Questa complessità si nota in particolar modo nel PLCP e MAC header dove sono presenti dei campi che riflettono la topologia della rete.

I pacchetti dei dati hanno l'unica funzione di trasmettere "la vera informazione" lungo la rete, mentre i pacchetti di controllo dirigono e controllano la comunicazione, e i frame RTS,CTS e ACK. I pacchetti di gestione della rete, invece, si occupano dell'autenticazione, associazione all'access point e della sincronizzazione.

Authentication / Privacy	
Il primo passo che un dispositivo wireless deve compiere per agganciarsi ad un AP è l'autenticazione. Questa può avvenire in un sistema aperto o a condivisione di chiavi. Essa avviene per scambio di pacchetti di gestione di rete	
authentication ID	E' il nome con il quale il dispositivo si autentica e si unisce alla rete
WEP enabled	Se setttato true il payload (ma non l'header) viene criptato con la chiave wep.
Network membership / Topology	
Il secondo passo per ildispositivo wireless è associarsi all'access point. Se il roaming è attivo una unità può dissociarsi e riassociarsi. Questa funzione avviene per scambio di pacchetti di gestione rete.	
association	Mostra l'associazione corrente dellasorgente del pacchetto
IBSSID or ESSID	L'ID del gruppo o del suo access point.
probe	Gestisce il roaming tra più celle.
Network conditions / Transmission	
Il protocollo 802.11 supporta update al fine di migliorare il throughput.	
channel	Canale usato per la trasmissione.
data rate	Data rate usato per la trasmissione (può dipendere da fattori ambientali).
fragmentation	Il protocollo 802.11 impone una frammentazione completamente indipendente da quella usata da tcp-ip. Al fine di minimizzare l'interferenza del rumore e quindi anche il numero di ritrasmissioni.
synchronization	Esistono diversi tipi di sincronizzazioni molto importanti per il protocollo 802.11 che vengono effettuate in questo campo
power save	Questo campo ha la funzione di gestire la limitazione della potenza erogata nella trasmissione (utile nei portatili).

Transmission control	
La funzione di questi campi è quella di gestire e controllare la trasmissione	
RTS, CTS, ACK	Request to send, clear to send, acknownowledmend gestiscono i 4 scambi di strette di mani.
version	Versione del protocollo usato.
type and sub-type	Tipo di pacchetto (dati, gestione, controllo)
duration	Tempo di durata della trasmssione
length	Lunghezza del pacchetto
retransmission	Segnala se il pacchetto è già stato trasmesso
sequence	Informazioni sulla sequenza dei frammenti
order	Ordine dei pacchetti
Routing	
Campi che gestiscono il routing dei pacchetti	
addresses	Ci sono 4 indirizzi in un pacchetto dati nel protocollo 802.11. Oltre ai soliti indirizzi del mittente e del destinatario sono presenti anche gli indirizzi dell'access point di entrata e di uscita per supportare il roaming fra più celle.
to/from DS	In Ess, un pacchetto può essere spedito, usando un access point, ad un device passando per un altro access point, passando per una rete wired. Questo campo descrive il routing e come interpretare gli indirizzi.
more data	Un access point può memorizzare dati per un dispositivo e farseli restituire successivamente. Questo campo gestisce questo processo

Tabella 2-2: Campi del frame 802.11

Nella tabella sovrastante sono spiegati brevemente i vari campi del frame 802.11 ordinati per funzionalità.

2.7 Suddivisione della banda e gli standard internazionali

La tabella 2.3 illustra le differenti frequenze ed ampiezze di banda previste dalla normativa americana in ambito di radiocomunicazioni. Le bande libere da licenza, e quindi utilizzabili da più utenti contemporaneamente, partono dalle frequenze inserite nella parte sinistra della tabella , e hanno ampiezza di banda differente come segnalato nella parte destra.

Frequenza iniziale	Larghezza di banda
902 MHz	26 MHz
2.4 GHz	83.5 MHz
5.725 GHz	125 MHz

Tabella 2.3 bande disponibili negli USA

Con l'avvento sul mercato dei prodotti funzionanti secondo lo standard 802.11 b, i produttori ed i certificatori di dispositivi wireless si sono spostati sulla frequenza 2.4GHz nella cosiddetta ISM che è una banda liberalizzata ed utilizzata in campo industriale, scientifico e medico. La possibilità di mantenere tale banda di frequenza libera da assegnazioni di licenza in tutto il mondo è data dal fatto che gli apparecchi che trasmettono in questa banda utilizzano la tecnica della SSS, segnali a dispersioni di spettro, le tecniche **SSS**(di spread spectrum signals) occupano una maggior banda di trasmissione radio ma consentono una miglior ricezione dei segnali deboli, garantiscono l'integrità del segnale, e una maggior sicurezza, distribuendo il segnale attraverso l'intero spettro di frequenze. Il segnale non rimane stabile su una singola frequenza , ed è proprio questo motivo che , consentendo a più utenti di operare simultaneamente , consente di mantenere libera la banda ISM, senza prevedere delle assegnazioni di frequenze come avviene ad esempio nella trasmissione mediante UMTS. L'uso dell' SSS è quindi particolarmente importante poiché permette che molti altri utenti occupino la fascia per tutto il tempo assegnato su frequenze separate , compatibilmente con la larghezza di banda disponibile, tre sono i possibili tipi di utilizzo della comunicazione e dispersione:

- DSSS (Direct Sequens Spread Sprectum)
- FHSS (Frequency Hopping Spread Sprectum)
- OFDM (Orthogonal Frequency Division Multiplexing)

Gli apparati wireless con tecnologia IEEE 802.11 b per trasmettere ed evitare le sovrapposizioni di segnali inviati in uno stesso momento, utilizzano i primi due tipi di comunicazione di spettro, il DSSS e il FHSS, mentre il più recente 802.11g utilizza come del resto lo standard 802.11 a la tecnica OFDM .

Nel modello FHSS, le frequenze su cui i dati vengono trasmessi cambiano molto rapidamente , fino a 1600 volte in un secondo, quasi azzerando le possibilità di un contemporaneo utilizzo della stessa frequenza. Nel modello DSSS, invece un campione di bande viene suddiviso in canali separati, e la trasmissione non è mai protratta per lunghi tempi su nessuna delle frequenze dei canali, questo fa si che l'utilizzo di diversi canali nella stessa area , renda possibile il sovrapporsi di reti diverse , senza interferenze tra di esse.

Region	Allocated Spectrum
US	2.4000-2.4835 GHz
Europe	2.4000-2.4835 GHz
Japan	2.471-2.497 GHz
France	2.4465-2.4835 GHz
Spain	2.445-2.475 GHz

Tabella 2-4 : Bande di Frequenza internazionali

La tabella 2.4 illustra come all'interno della stessa banda ISM, gravitante ai 2.4 GHz vi siano differenze a livello internazionale , dovute alle diverse previsioni da parte dei governi riguardo alla ampiezza si spettro utilizzabile. Nel mondo i sistemi SSS sono regolati da apposite normative, emanate dagli organi competenti per territorio per la Comunità Europea e il Giappone valgono le norme E.T.S 300-328 e correlate , emanate dall'organo europeo E.T.S.I. (European, Telecomunication Standardization Institute).

Il sistema **FHSS** permette all'informazione di essere trasmessa su un range di frequenze molto piccolo chiamato canale. Il segnale ad una data frequenza viene fatto "saltare" da una canale all'altro, distribuendosi su una banda di frequenze molto ampia. Il vantaggio di tale sistema, quando il rapporto fra la larghezza di banda originale del segnale e la larghezza di banda del segnale di diffusione è molto grande, è di offrire una grande immunità all'interferenza.

La tecnologia consente a più utenti di condividere lo stesso insieme di frequenze cambiando automaticamente la frequenza di trasmissione fino a 1600 volte al secondo, al fine di una maggiore stabilità di connessione e di una riduzione delle interferenze tra canali di trasmissione.

Il sistema **FHSS** risulta molto sicuro contro interferenza e l'intercettazione in quanto risulta statisticamente impossibile poter ostruire tutte le frequenze che possono essere usate . Il sistema **DSSS** permette di eseguire una trasmissione a "frequenza diretta" a banda larga, ogni bit viene trasmesso come una sequenza ridondante di bit, detta chip. Tale metodo è indicato per

la trasmissione e ricezione di segnali deboli. Consente l'interoperabilità con le reti wireless attuali a 11 Mbps con le precedenti a 1-2 Mbps.

L'interfaccia **DSSS** utilizza un sistema con dispersione in banda base utilizzando un chipping code (codice di dispersione) modulando il dato prima di trasmetterlo, ogni bit trasmesso viene disperso su una sequenza a 11 bit (sequenza Barker). Il segnale trasmesso consumerà una maggior larghezza di banda consentendo la ricezione di segnali deboli. La modulazione **DSSS** assicura una resistenza all'interferenza piuttosto scarsa. Questo limita l'uso della **DSSS** nelle applicazioni reali delle Wlan.

Capitolo 3

LA SICUREZZA NELLE RETI WIRELESS IL FENOMENO DEL WARDRIVING E DEL WARCHALKING

In un'epoca come quella attuale , in cui il bisogno di connettività è cresciuto a tal punto da diventare abitudine, quasi moda, gli individui sono alla continua ricerca di un punto d'accesso, di una porta aperta sulle mille risorse, sulle informazioni che internet può offrire. Questo bisogno collide però con la necessità di sicurezza, garanzia stessa di sopravvivenza per la rete. Se il diritto di accesso gode di notevole considerazione nella pianificazione della legislazione futura ad opera delle commissioni di esperti in ambito di comunicazioni, l'individuazione delle responsabilità di eventuali reati telematici è tuttora posta in primo piano dalla legislazione vigente, la quale impone oneri per i soggetti titolari del trattamento di dati personali altrui nonché per le aziende fornitrici di connettività internet , sia via cavo che via etere. Utilizzando un metodo molto simile a quello del monitoraggio di un'applicazione wireless, è possibile accedere facilmente ad una rete wireless privata dall'esterno, soprattutto se non sono state attivate misure di sicurezza preventive agli amministratori di sistema. Infatti molte società distribuiscono ed installano reti wireless , utilizzando configurazioni delle stazioni base predefinite e non protette , rendendo cosi possibile la connessione ai server delle applicazioni ed ai servizi di rete da parte di qualunque utente . Di fatto , studi condotti da società impegnate per la sicurezza informatica , dicono che quasi la metà degli AP presenti nelle nostre città non implementa alcun livello di protezione , e molti sono i punti d'accesso che presentano ancora configurazioni di default , ben conosciute e facilmente aggirabili da esperti del settore. In ambienti di lavoro poi , un ennesimo pericolo è costituito dai cosiddetti AP *rogue*,cioè un AP che sebbene sia presente sulla rete non è stato installato o autorizzato dagli amministratori. La semplificazione delle operazioni di connessione offerta dai dispositivi wireless spinge talvolta i dipendenti di aziende ed uffici a provvedere personalmente all'implementazione di questi apparecchi, in mancanza di soluzioni unitarie della dirigenza. I dipendenti solitamente però, non tengono conto delle implicazioni di sicurezza di una tale scelta e non attivano le opzioni di protezione e cifratura. Un AP rogue rappresenta un rischio di notevole entità per il sistema , poiché attraverso di esso, un malintenzionato può accedere facilmente alla rete privata o aziendale , senza che i responsabili della sicurezza ne vengano a conoscenza. Per ostacolare gli accessi non autorizzati, sarebbe inoltre opportuno prevedere un'autenticazione reciproca tra i

dispositivi client e gli AP della rete, in modo che solo le richieste di connessione da parte di utenti autorizzati vengano prese in considerazione dal sistema. La proliferazione di punti d'accesso wireless nelle città, l'estrema facilità di connessione di questi dispositivi, l'abitudine alla connettività degli utenti hanno fatto nascere un particolare fenomeno di costume , denominato *wardriving*. Il wardriving consiste nell'intercettare reti wireless, in automobile o a piedi con un computer portatile, solitamente interfacciato con un ricevitore GPS per individuare l'esatta locazione della rete trovata ed eventualmente pubblicarne le coordinate su un sito web. E' necessario utilizzare un software specifico, quasi sempre disponibile gratuitamente e per diverse piattaforme, in aggiunta spesso i wardrivers segnalano l'esistenza di nodi aperti con dei segni sui muri, sui marciapiedi o comunque nelle vicinanze del punto d'accesso, fenomeno del *warchalting*. Sono presenti diverse varianti per segnalare nodi aperti , nodi chiusi, la presenza di protocollo di cifratura WEP, oltre all'indicazione del nome della rete e dell'ampiezza della banda offerta. Inoltre tramite il collegamento wireless un hacker potrebbe attaccare la rete wired allacciata all'access point, bypassando le protezioni offerte dai firewall. È evidente che in questa situazione le necessarie misure di sicurezza hanno caratteristiche differenti da quelle normalmente adottate per le reti cablate. Le misure di sicurezza ovviamente non mancano, dai firewall alla crittografia dei dati, ma gli standard applicati oggi alle reti wireless non forniscono una robustezza tale da poter essere considerati sicuri.

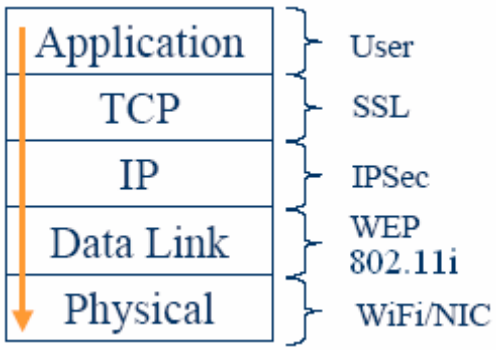


Figura 3-1: i vari livelli di sicurezza dello stack ISO-OSI

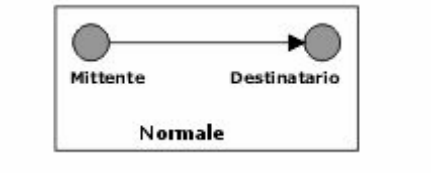
Queste diverse soluzioni lavorano a livelli differenti del modello ISO-OSI, come illustarto dalla figura soprastante, e quindi non sono mutuamente esclusive, ma possono essere usate contemporaneamente per fornire un livello di sicurezza maggiore. Oggi non esistono ancora sistemi che garantiscano per le reti wi-fi un livello di sicurezza equivalente a quello delle reti wired. I 3 servizi base di sicurezza definiti da IEEE per le Wlan 802.11b e compatibili sono:

• **Autenticazione:** verifica dell'identità, controllo dell'accesso alle risorse solo per i client autorizzati.

• **Confidenzialità dei dati:** garantire la privacy della comunicazione criptando i pacchetti (WEP).

• **Integrità dei dati:** evita che le informazioni possano essere modificate durante la trasmissione.

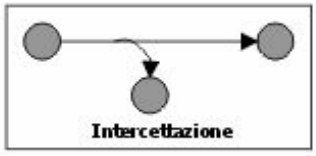
Secondo IEEE, con l'arrivo del WEP si sarebbero raggiunti tali servizi, offrendo un livello di sicurezza pari a quello delle reti wired. Per comprendere il livello di sicurezza assicurato, analizziamo i principali tipi di attacchi che un hacker può effettuare contro una rete wi-fi. Rappresentiamo il normale flusso di pacchetti lungo la rete con il seguente schema:



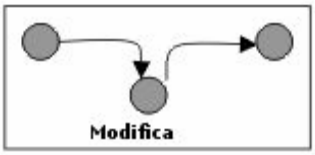
Identifichiamo le seguenti tipologie di attacco:

- **Interruzione:** ovvero il blocco del flusso delle informazioni dal mittente al destinatario.

- **Intercettazione:** si definisce con questo termine la possibilità che entità non autorizzate riescano ad intercettare ed ascoltare in maniera fraudolenta i segnali radio scambiati tra una stazione wireless ed un AP



- **Modifica:** è l'equivalente di intercettare una lettera, aprirla, modificarla, richiuderla e rispedirla senza che ne mittente ne destinatario si accorgano di nulla.



- **Contraffazione:** ossia inviare falsi messaggi creati ex-novo con le credenziali di un utente considerato fidato dal sistema.

L'interruzione della comunicazione tra un client e l'access point viene generata con una sorgente di onde elettromagnetiche che interferisce con la sorgente.
Nelle reti wireless l'intercettazione viene effettuata utilizzando una scheda wi-fi che ascolta la rete in modo promiscuo. Lo sniffing può essere effettuato anche da luoghi pubblici passando inosservati, sfruttando l'impossibilità di confinare il campo elettromagnetico, prodotto dall'access point, all'interno di un edificio.
La modifica di un messaggio è un'operazione più complessa delle altre. Un hacker deve prima di tutto isolare un client (interruzione), poi deve simulare un access point per ricevere i messaggi e rinviarli all'access point originale.
La contraffazione di un messaggio, invece, dipende dal sistema di autenticazione utilizzato. Il metodo più semplice per riconoscere il client è utilizzare il MAC address della scheda di rete dell'utente. In questo caso la contraffazione risulta semplice, in quanto sulla rete esistono software che ascoltando la rete rilevano gli indirizzi MAC dei vari client e li impostano sulla propria scheda di rete.
Abbiamo quindi visto, che le reti wireless non garantiscono un sufficiente livello di sicurezza. Vediamo ora quali sono i livelli di protezione adottabili e riconosciuti nelle specifiche dell'802.11b e facilmente applicabili in tutte le WLAN che supportano tale standard.
Per l'autenticazione lo standard 802.11b prevede due modalità:

- **OSA** (Open Systems Authentication) che non prevede alcuna autenticazione consentendo a qualsiasi dispositivo mobile l'accesso.
- **SKA** (Shared Key Authentication) che prevede l'uso di una chiave pre-condivisa nell'autenticazione; una volta autenticati, i dati scambiati tra l'access point (AP) e il terminale mobile (WT) vengono cifrati mediante WEP. In una connessione AP e WT occorre che i due dispositivi abbiano condiviso la chiave prima di connettersi. Per cui tutti i WT debbono essere configurati manualmente all'interno della Wlan.

Nella pratica si usa, per comodità, una sola chiave per tutti i WT, ciò comporta che un AP nella modalità SKA può verificare l'appartenenza di un WT ad un specifico gruppo ma non la sua

specifica identità. L'autenticazione è unidirezionale dall'AP verso l'WT e non viceversa, ciò può consentire l'intrusione di un AP mascherato. La modalità SKA funziona nel seguente modo: l'access point manda un pacchetto di sfida al nuovo client che lo cripta con la chiave corretta e lo rispedisce al mittente. L'access point controlla la correttezza e se la risposta è giusta il nuovo utente viene associato alla rete.

3.1 Riservatezza dei dati e la crittografia

Le tecniche utilizzate per prevenire il monitoraggio del traffico e l'intercettazione delle comunicazioni in ambito wireless si basano sull'utilizzo della crittografia. In ambito informatico , la crittografia è utilizzata per modificare i bit di ogni pacchetto di dati, al fine di impedire la decodifica dei dati, siano essi i numeri di carta di credito, le password delle caselle postali o semplicemente i messaggi istantanei.

Prima della crittografia i dati appaiono sotto forma di testo semplice, facile da decodificare mediante strumenti di intercettazione. L'utilizzo di tecniche crittografiche converte il testo semplice in testo cifrato, incomprensibile ad eventuali monitoraggi, per la cui decodifica è necessario utilizzare la chiave appropriata.

Il *Service Set Identifier* (SSID) è l'identificatore configurabile che permette ai client di comunicare con l'access point appropriato. E' una stringa di caratteri unica, costituita da una sequenza di venti caratteri alfanumerica definita e configurata dall'amministratore della rete.

Con una configurazione corretta, solo i client con il SSID corretto possono comunicare con lui cioè, SSID lavora come una password condivisa tra access point e client e viceversa, e viene, anche usato per segmentare la rete wireless in molteplici reti servite da uno o più access point.

SSID, comunque, può essere facilmente sniffato in quanto viene trasmesso come testo in chiaro anche quando il WEP è abilitato. Infatti viene inserito nell'header dei pacchetti che non vengono usualmente criptati.

3.2 Access Control List

Un sistema di autenticazione aggiuntivo, che prevede una procedura manuale ad opera degli amministratori di rete, è quello che si basa sul filtraggio dei MAC Address dei dispositivi wireless. Quando si utilizza tale metodo, l'access point esamina l'origine dell'indirizzo MAC di ogni frame in entrata, rifiutando i frame provenienti da un indirizzo MAC che non corrisponda ad un elenco specifico programmato ed inserito manualmente in precedenza dall'amministratore. Di conseguenza, il filtraggio dei MAC Address fornisce una forma

piuttosto rudimentale di autenticazione. Purtroppo, anche questo metodo di autenticazione presenta alcuni punti deboli. Ad esempio, la crittografia WEP non codifica il campo dell'indirizzo MAC del frame. In questo modo, un hacker è in grado di monitorare il traffico di una rete ed individuare indirizzi MAC validi ed abilitati. In seguito egli potrà utilizzare alcuni software, liberamente disponibili in rete, per camuffare l' indirizzo MAC della propria scheda wireless con uno accreditato, in modo da garantirsi l'accesso al sistema vittima quando l'utente a cui sono state sottratte le credenziali non è presente sulla rete. Il filtraggio MAC può inoltre risultare difficile da gestire in presenza di numerosi utenti. Un amministratore deve immettere in una tabella l'indirizzo fisico della scheda di ciascun utente, nonché effettuare delle modifiche nel caso vi siano defezioni o ingresso di nuovi utenti. Per tale motivo, questo metodo può risultare adatto ad applicazioni domestiche o relative a piccoli uffici, ma la natura pratica di un simile approccio non è generalmente indicata per gli amministratori di reti wireless di grandi dimensioni, quali quelle aziendali ed universitarie. La figura 3.2 illustra la pagina di configurazione di un access point in cui devono essere inseriti gli indirizzi MAC degli utenti che si vuole autenticare ed ai quali si vuole permettere il collegamento alla rete.

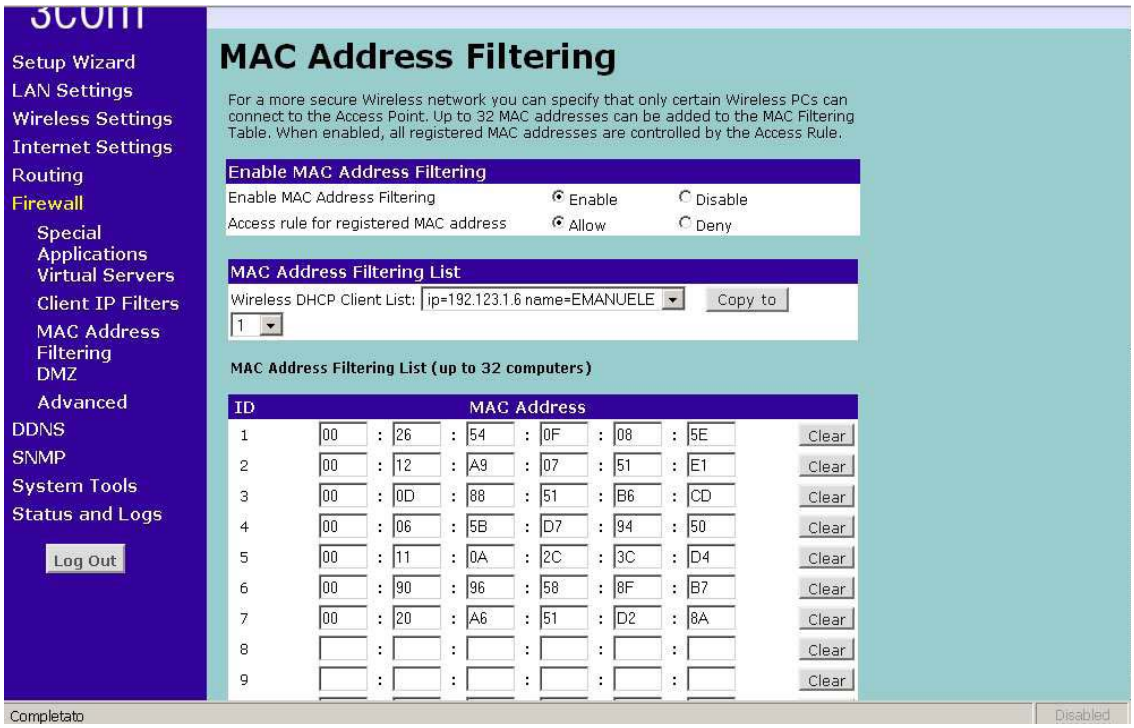


Figura 3-2: pagina di configurazione dei MAC address accreditati di un AP.

3.3 WEP

WEP è lo standard di crittografia, nonché di autenticazione, implementato da tutti i dispositivi 802.11. Come si può evincere dal nome stesso scelto per questo metodo di cifratura - "*Wired Equivalent Privacy*" - l'obiettivo dei suoi creatori era quello di rendere le reti wireless sicure almeno quanto le normali reti cablate.Il protocollo WEP utilizza un algoritmo di cifratura a chiave simmetrica statica condivisa (RC4, 64 o 128bit) . La chiave è formata da un vettore di inizializzazione (IV) di 24 bit e da una chiave vera e propria di 40 o 104 bit. Il vettore di inizializzazione ha il compito di inizializzare il stream chyper e viene trasmesso in chiaro.

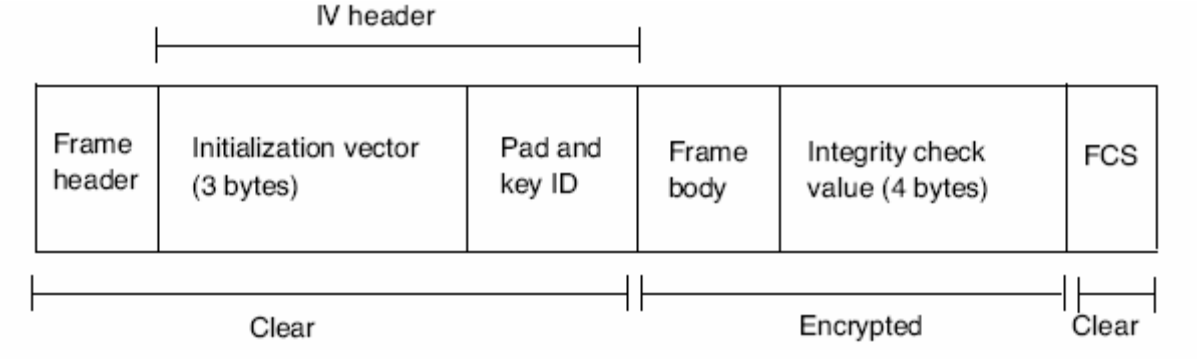


Figura 3-3: WEP frame

Per assicurare l'integrità dei dati nel frame vengono aggiunti i campi ICV e FCS che si basano sul controllo a ridondanza ciclica. Il campo FCS serve per prevenire le alterazioni del frame dovute al mezzo di trasporto. Questo non basta a garantire l'integrità dei dati in quanto un hacker può modificare il frame e ricalcolare il campo FCS. Quindi è stato aggiunto l'integrity check value(ICV) che venendo trasmesso criptato non può essere ricalcolato. Essendo l'IV di soli 24 bit, esistono solo 2^{24} combinazioni e queste si ripetono dopo 17 milioni di pacchetti, rendendo il protocollo più vulnerabile. La scelta della chiave pre-condivisa rappresenta un elemento di vulnerabilità in quanto la chiave deve essere scambiata via radio fra WT e AP. Poiché lo standard 802.11 non supporta la funzionalità di scambio dinamico delle chiavi, queste rimangono in uso per tempi anche molto lunghi (mesi o addirittura anni) senza essere modificate dal gestore di sistema. In questo modo si può compromettere la segretezza della chiave con appositi software che analizzano il traffico nell'etere. Proprio per questo motivo, un'importante precauzione consiste nel modificare frequentemente le password. Tale operazione potrebbe risultare tuttavia complessa se eseguita su reti di grandi dimensioni. Inoltre il tempo per crackare la chiave cresce solo linearmente con la sua lunghezza. Anche la più recente versione a 128 bit dell'algoritmo WEP, infatti, non è esente da limiti, dall'analisi statistica del traffico, non è particolarmente difficile introdursi in un'infrastruttura wireless.

Un altro elemento di vulnerabilità della sicurezza discende dall'unidirezionalità della tecnica di autenticazione dello standard IEEE 802.11b: il punto d'accesso, infatti, può autenticare il terminale ma quest'ultimo, in nessun modo, può autenticare il primo. Pertanto, un nodo di rete intruso può spacciarsi per AP senza che il terminale possa verificarne l'autenticità. Si noti che questa eventualità non è remota, in quanto la semplicità della connessione in rete degli AP è considerato proprio uno dei punti di forza del Wi-Fi.

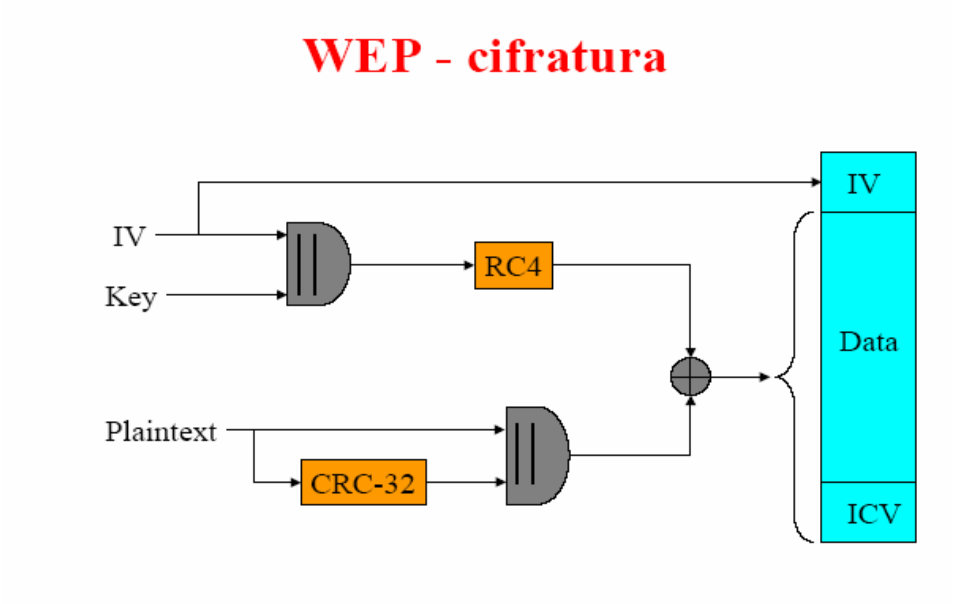


Figura 3-4: Algoritmo di cifratura del WEP

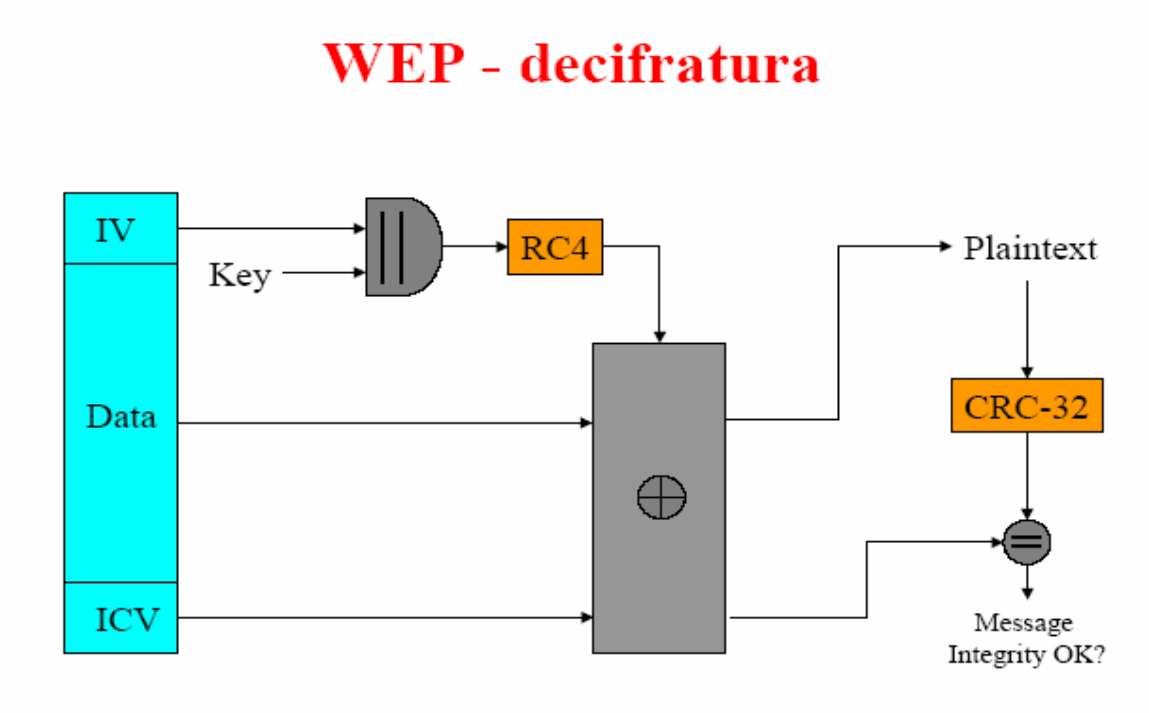


Figura 3-5: Algoritmo di decifratura del WEP

L’algoritmo WEP si compone dei seguenti passi:

1. Si applica l’algoritmo di integrità al Frame per generare un ICV (Integrity Check Value) di 32 bit inviati insieme ai dati e controllati dal ricevitore per proteggere le informazioni trasmesse da eventuali modifiche non autorizzate.
2. Si genera la Key Sequence da un generatore pseudo-casuale che riceve come input la chiave segreta. La Key Sequence ha la stessa lunghezza del Frame + ICV.
3. Si effettua l’OR Esclusivo (X-OR) tra i bit Frame + ICV e la Key Sequence e si genera il testo crittografato
4. Il ricevitore decifra il testo utilizzando la sua chiave e genera la stessa Key sequenze utilizzata per criptare il frame.
5. La stazione calcola l’Integrity Check e lo confronta con la sequenza ricevuta decriptata.
   Se non c’è corrispondenza allora la MSDU non viene inviata all’unità LLC e si invia una“Failure Indication” al Mac Management.

3.4 IL WPA (Wi-Fi Protected Access).

Il WPA ha lo scopo di fornire una migliore crittografia dei dati rispetto al WEP e offre anche un meccanismo per l’autenticazione dell’utente, funzione quest’ultima assente nel WEP. Per migliorare le tecniche di criptazione, WPA utilizza il TKIP. Inoltre esso supporta due differenti configurazioni, Personal e Enterprise. Il metodo Personal o PSK è maggiormente appropriato per reti private che non hanno autonome infrastrutture di autenticazione. Il metodo Enterprise è stato ideato invece per soddisfare le esigenze di tutti quei soggetti quali gli operatori della Pubblica Amministrazione, della Sanità e le aziende del settore terziario, i quali, trovandosi a detenere e manipolare dati personali e sensibili, devono affrontare l' obbligo, non solo legislativo, di implementare misure di sicurezza più imponenti e robuste a difesa dei propri sistemi informatici e telematici e della privacy dei titolari dei dati in essi contenuti. E’ stato inoltre rilasciato una ulteriore versione del protocollo WPA, denominata WPA2, la quale assicura un livello di protezione dei dati e un accesso alla rete ristretto agli utenti autorizzati ancora più evoluto rispetto alla versione precedente.

La differenza sostanziale con WPA è che il WPA2 fornisce un più forte meccanismo di criptaggio attraverso l’AES (Advanced Encryption Standard) piuttosto che il TKIP. AES è un *block cipher*, nel senso che la crittografia viene fatta su blocchi di dati invece che bit a bit (come in RC4).

IEEE 802.11i è un standard che è stato sviluppato da IEEE per sostituire i protocolli attuali per le reti wireless al fine di migliorare la sicurezza. In particolare 802.11i vuole risolvere le debolezze mostrate dal WEP nell'autenticare i client e nel criptare i dati. Lo standard 802.11i è formato dai seguenti componenti:

- 802.1x framework (autenticazione basata su porte)
- TKIP (Temporal key Integry protocol)
- AES (Advance Encryption standard)
- Gestione e gerarchia delle chiavi
- Cypher e Negoziazione dell'autenticazione

Per risolvere gli attuali problemi di sicurezza delle reti 802.11b lo standard (WPA) è basato parzialmente su 802.11i e compatibile dal punto di vista hardware con i dispositivi in commercio (richiede un upgrade software).
Il WPA è formato da tutti i componenti di 802.11i ad eccezione di AES.

Autenticazione 802.1x

Lo standard 802.1x specifica una forma di autenticazione generica e estendibile basata sull'utilizzo di porte applicabile sia alle reti wireless che alle reti wired. Il protocollo WPA sfrutta tutti i suoi componenti. Lo standard 802.1x è supportato dalla maggior parte dei sistemi operativi e access point in commercio.
Esso specifica diversi tipi di autenticazione:

- Login e password
- Certificati
- Smart cart

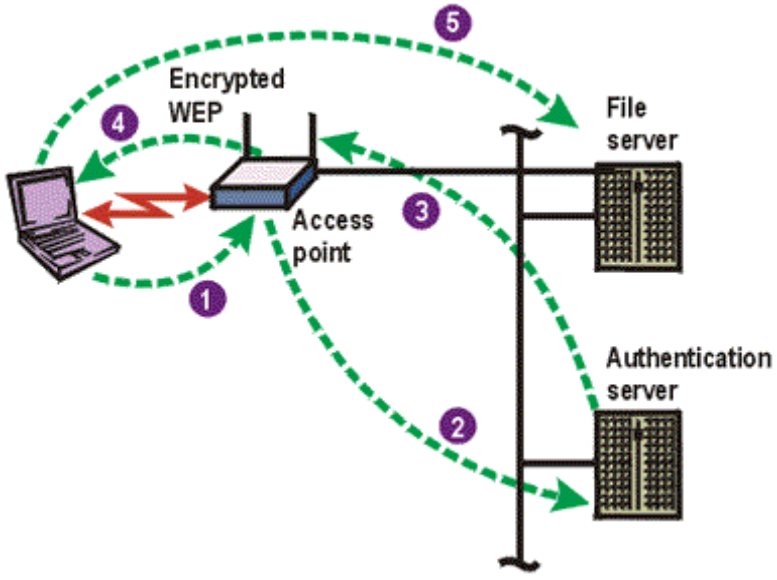


Figura 3-6: Schema di funzionamento di una Wlan 802.1x

802.1x non richiede un particolare protocollo di autenticazione. Infatti, 802.1x usa EAP (Extensible Authentication Protocol). EAP è un protocollo di incapsulazione che permette di usare diversi protocolli di autenticazione. Esistono quattro protocolli di autenticazione principali:

- MD5: protocollo unidirezionale basato su password
- LEAP: protocollo proprietario di Cisco basato su username
- EAP-TLS: protocollo bidirezionale basato su certificati
- EAP-TTLS: sono protocolli di alto livello che non richiedono certificati

Caratteristiche	MD5	Cisco LEAP	EAP-TLS	EAP TTLS
Lunghezza chiave	-	128	128	128
Mutua autenticazione	Si	Si	Si	Si
Rotazione chiavi	Si	Si	Si	Si
Livello di sicurezza	Debole	Intermedia	Robusta	Robusta
Supporto nei client	Supporto nativo in windows XP	Supporto solo nelle schede Cisco	Supporto nativo in windows XP e 2000	Supporto nativo in windows XP e 2000

Tabella 3-1: Riassunto protocolli di autenticazione

L'approccio 802.1x offre i seguenti vantaggi:

- Basato su standard.
- Autenticazione flessibile: l'amministratore può scegliere il metodo di autenticazione.
- Gestito centralmente.
- Scalabile, se si vuole allargare la rete basta aggiungere gli access point e i server di autenticazione.
- Le chiavi dei client sono generate dinamicamente e propagate.
- Il roaming tra più access point è più trasparente in quanto l'autenticazione è gestita centralmente.

Nelle reti aziendali, il processo di autenticazione sarà gestito da un server specifico (Radius server) che sarà in grado di gestire gli utenti meglio dell'attuale WEP e in maniera molto più semplice.

Figura 3-7: Struttura di una wlan con server Radius

Il server ha il compito di gestire e controllare gli accessi alla rete. Questo include la gestione delle credenziali degli utenti, l'autorizzazione delle richieste di accesso alla rete degli utenti e la generazione delle sessioni.
Per le reti domestiche, con minori esigenze in termini di sicurezza, è prevista una modalità a chiave precondivisa, il che ha il vantaggio di non richiede l'uso di un server, anche se il livello di sicurezza è certamente inferiore. Questo approccio offre la facilità di istallazione del WEP insieme ad un metodo di cripting più robusto (TKIP). Il WPA a chiave precondivisa differisce sostanzialmente dal WEP, infatti sotto WPA la chiave precondivisa è usata solo all'inizio dello scambio delle chiavi dinamiche TKIP e non partecipa direttamente al cripting dei dati.

3.5 TKIP

E' un protocollo che permette un metodo di distribuzione delle chiavi dinamico. Esso aumenta significativamente la sicurezza della rete, diminuendo il tempo a disposizione di eventuali aggressori per vincere l'algoritmo prima dell' immissione di una nuova chiave. Fornisce inoltre importanti miglioramenti per quanto riguarda la crittografia dei dati: genera periodicamente e automaticamente una nuova chiave per ogni dispositivo connesso alla rete e quindi per ciascun utente, TKIP si occupa della generazione dinamica delle chiavi e del loro scambio in modo sicuro. TKIP continua usare l'algoritmo di cripting RC4 usato dal WEP ma lavora principalmente sui punti deboli del WEP, risolvendo anche il grave problema del riutilizzo delle key. Il processo inizia con un a chiave temporanea di 28 bit condivisa unicamente fra client e access point. Il TKIP combina questa chiave temporanea con il MAC address della macchina client ed aggiunge un vettore di inizializzazione di 16 ottetti, producendo in questo modo la chiave che verrà usata per crittografare i dati. Questa procedura assicura che ogni stazione usi un differente key stream per crittografare i dati.

3.6 VPN

VPN è una soluzione che è stata sviluppata per permettere ai lavoratori remoti un accesso sicuro alla rete attraverso internet. La VPN provvede a creare un percorso sicuro e dedicato (tunnel) attraverso una rete insicura (in questo caso internet). Esistono diversi protocolli di tunneling (PPTP, L2TP) che vengono usati insieme a delle soluzioni che permettono l'autenticazione centralizzata (Radius server).
Il tipo di connessione che si stabilisce quando si costituisce una VPN si basa sulla tecnica del tunnelling, il processo di incapsulamento di un pacchetto di una rete dentro un altro che

consente, tra le altre numerose funzioni, di nascondere l'indirizzo IP del vero mittente e ricevente. Il pacchetto che viaggia attraverso la rete insicura è cifrato e solamente gli indirizzi pubblici della VPN (Gateway o Client) sono notificati durante il trasporto.

Le principali componenti delle reti private virtuali sono due: il gateway di rete, un elemento che dispone di varie interfacce verso le diverse componenti della rete e di diversi protocolli di cifratura e decifratura del traffico che lo attraversa.

L'altro importante elemento che compone una VPN è il client installato su un computer in grado a sua volta di cifrare e decifrare selettivamente il traffico che trasmette e riceve dalla rete geografica protetta dal gateway della VPN.

Il traffico di una VPN viene indirizzato verso un server remoto attraverso un normale indirizzo IP ma, passando attraverso il dispositivo della VPN, viene cifrato e inserito in una procedura di tunnelling che lo instrada automaticamente verso la rete remota a cui è destinato. Quando il gateway di questa rete riceve il pacchetto di dati cifrati, verifica l'identità del mittente e l'integrità del pacchetto, quindi lo decifra e lo distribuisce al destinatario senza modificarlo. Tra i protocolli utilizzati per cifrare il traffico delle VPN, quello più diffuso è IPSec. IPSec (Internet Protocol Security) non è in realtà un singolo protocollo, ma l'insieme di elementi che costituiscono un'architettura di sicurezza a livello IP. Trovandosi a livello di rete, IPSec è una soluzione molto generale (può proteggere tutto il traffico IP) ed è trasparente rispetto alle applicazioni. La stessa tecnologia VPN può essere utilizzata per garantire un accesso sicuro nelle reti wireless. L'access point viene configurato in modalità OSA (open) con chiave WEP disabilitata, ma l'accesso wireless è isolato dalla rete interna da un server VPN. L'autenticazione e il cripting dei dati vengono eseguiti dal server VPN che funziona come firewall/gateway per la rete interna. La soluzione basata su VPN garantisce una elevata sicurezza e scalabilità.

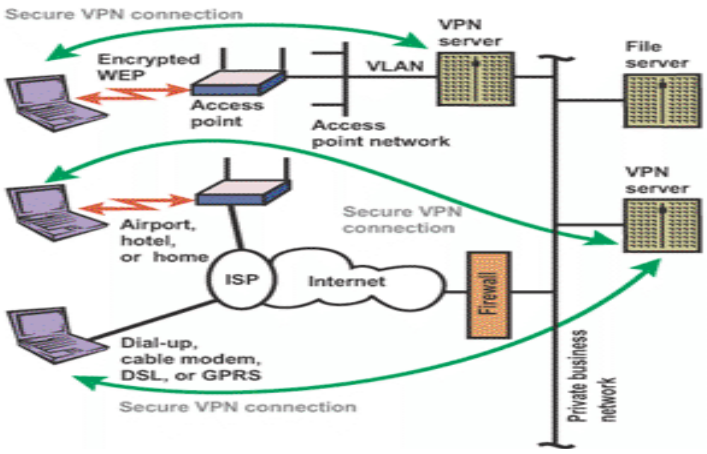


Figura 3-8: Struttura di VPN

La VPN garantisce numerosi vantaggi rispetto le soluzioni concorrenti, è scalabile ad un grande numero di client, ha un basso livello di amministrazione negli access point e nei client. I server VPN possono essere gestiti centralmente e il traffico verso la rete interna è bloccato fino all'autenticazione , il WEP e MAC address list non sono necessari e l'interfaccia che permette l'accesso remoto è uguale in ogni posto.

Capitolo 4

CAPTIVE PORTAL

Dopo aver descritto i servizi, nell'ambito della sicurezza, offerti dallo standard 802.11 e le principali soluzioni disponibili sul mercato, analizziamo un particolare sistema che permette di gestire l'accesso e l'autenticazione in una rete wireless,la categoria di software che viene chiamata Captive portal (oppure catch and release portal). Il Captive portal sta diventando un modo molto diffuso per provvedere alla autorizzazione degli utenti e alla gestione del traffico a livello Network del modello ISO-OSI per le reti wireless. I captive portal permettono, attraverso l'uso di un semplice browser, l'autenticazione sicura degli utenti usando protocolli opportuni per criptare le comunicazioni come SSL e IPSEC.

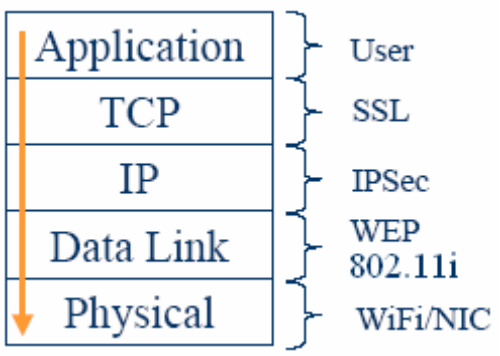


Figura 4-1: i vari livelli di sicurezza dello stack ISO-OSI

L'idea che sta dietro al concetto di Captive portal è semplice: invece che basare la sicurezza della rete sui servizi offerti dallo standard 802.11 che si sono dimostrati molto deboli e quindi controllare chi si associa all'access point, si configura la rete in modalità aperta. Immediatamente dietro all'access point installiamo un router che ha la funzione di gestire il flusso dei dati verso la rete wired, lasciando passare solo gli utenti autorizzati e gestendo la banda disponibile.

Il funzionamento di un Captive portal viene denominato "catch and release". Quando un client non autenticato richiede una pagina web, il Captive portal intercetta la richiesta (catch) e propone all'utente una pagina web di autenticazione. Se il client inserisce l'username e la password corretta, viene autenticato e portato alla pagina web iniziale (release). Analizziamo, ora, se i Captive portal soddisfano tutti questi requisiti.

4.1 Vantaggi e Svantaggi

Sicuramente il punto di forza di questi sistemi è la facilità di uso. Essi non richiedono l'istallazione di alcun software nel lato client, autenticano i vari utenti attraverso pagine web, quindi con una interfaccia user-friendly.
L'architettura stessa è estremamente scalabile, in quanto per autenticare i vari utenti utilizzano un database centrale che, anche nel caso di uso di più gateway non viene duplicato. La separazione tra la rete wireless e le credenziali degli utenti fornisce una maggiore osservabilità al sistema e permette di utilizzare le stesse per altri servizi, diversi dall'accesso alla rete wireless.
I Captive portal permettono una facile installazione a differenza di soluzioni alternative come le VPN. Forniscono servizi differenziati come il controllo della banda dei vari utenti.
Il punto debole di questi sistemi è che criptano solo l'autenticazione e non il resto della comunicazione, permettendo l'ascolto delle comunicazioni dei vari utenti.

4.2 Funzionamento del software

La maggior parte dei software sono composti da due componenti principali che possono risiedere su macchine diverse e comunicano tra di loro attraverso socket: gateway e authservice.
Il gateway si trova su una macchina immediatamente dietro l'access point e si occupa di gestire le connessioni degli utenti e settare la banda delle stesse. Questo viene fatto aggiungendo e eliminando delle regole di firewall opportune in modo dinamico.
L'authservice, invece, si occupa dell'autenticazione degli utenti appoggiandosi ad un database (MySql, Ldap, Radius, Samba, Pam e password file). Il suo unico compito è quello di dare al gateway una risposta affermativa o negativa sulle credenziali dell'utente.
Esistono diverse implementazioni di una rete wireless ESS basata su questi software, alcune sono riassunte nelle due figure sottostanti.
Nella prima il traffico proveniente da tutti gli access point attraversa un unico gateway. Nella seconda implementazione, invece, esiste un unico authservice centrale ma un gateway per ogni access point. La prima implementazione viene utilizzata nelle reti di piccole dimensioni dove il transito del traffico in un unico punto non limita le prestazioni della rete. Se si considerano reti di dimensione più elevata, questo può diventare un collo di bottiglia che limita sensibilmente le prestazioni. In questo caso viene utilizzata la seconda implementazione in cui si usa un

gateway per ogni access point. Questa è una soluzione sicuramente più scalabile, però ha dei difetti. Innanzitutto richiede più router (uno per ogni gateway) con conseguente aumento dei costi, in più il roaming tra due access point non è trasparente: l'utente deve rifare l'autenticazione.

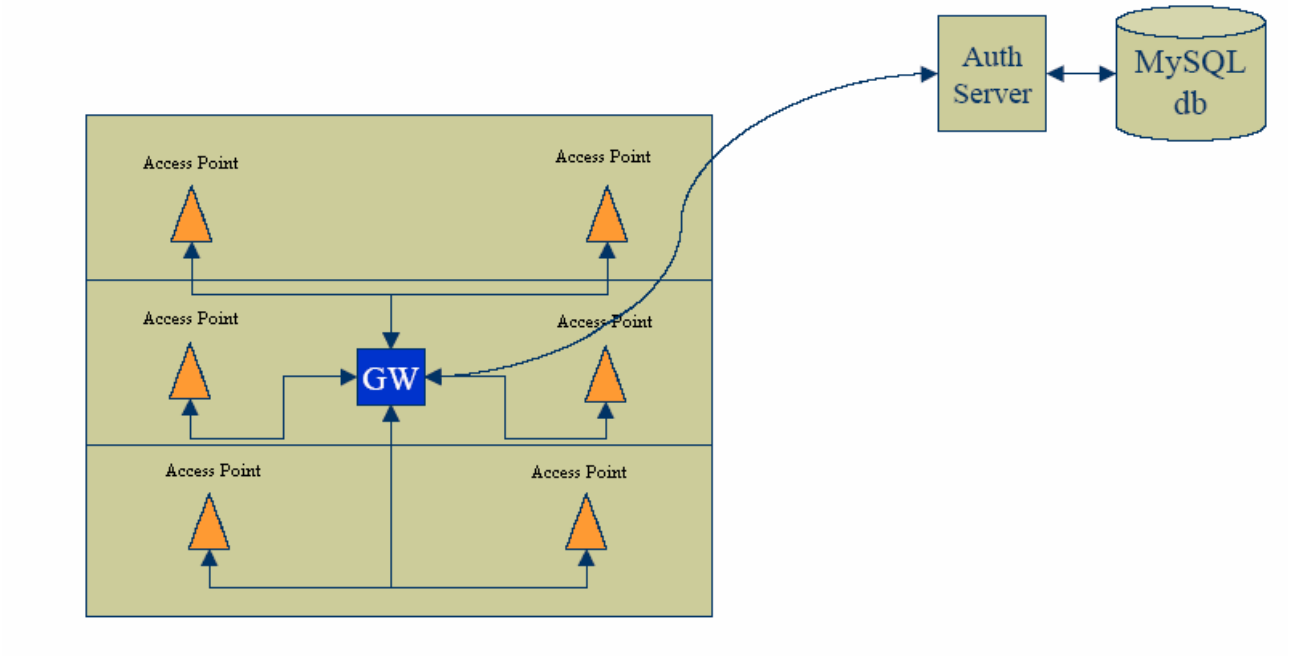


Figura 4-2: Implementazione di un sistema con un gateway

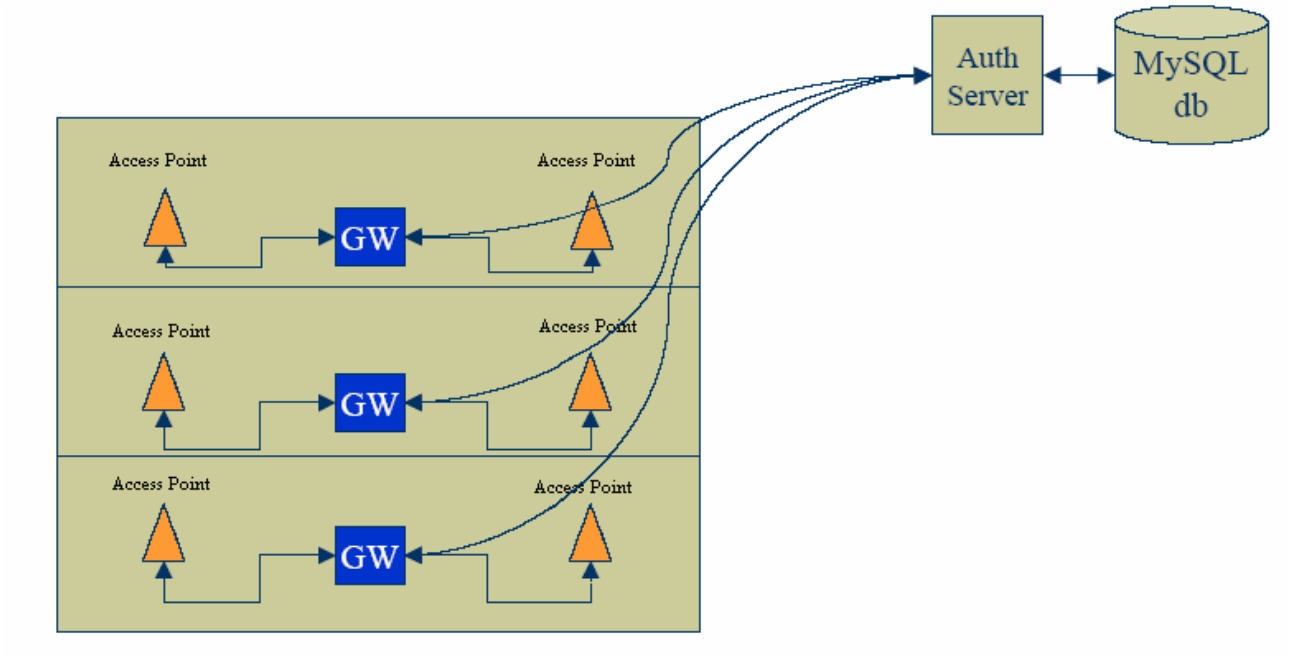


Figura 4-3: Implementazione di un sistema con più gateway

Prendiamo in considerazione una rete wireless BSS, collegata tramite un access point ad una rete wired che ha accesso ad internet. Installiamo, quindi un gateway immediatamente a valle dell'access point e l'authservice dietro di esso. Ogni utente non autenticato può arrivare fino al gateway ma non oltrepassarlo.

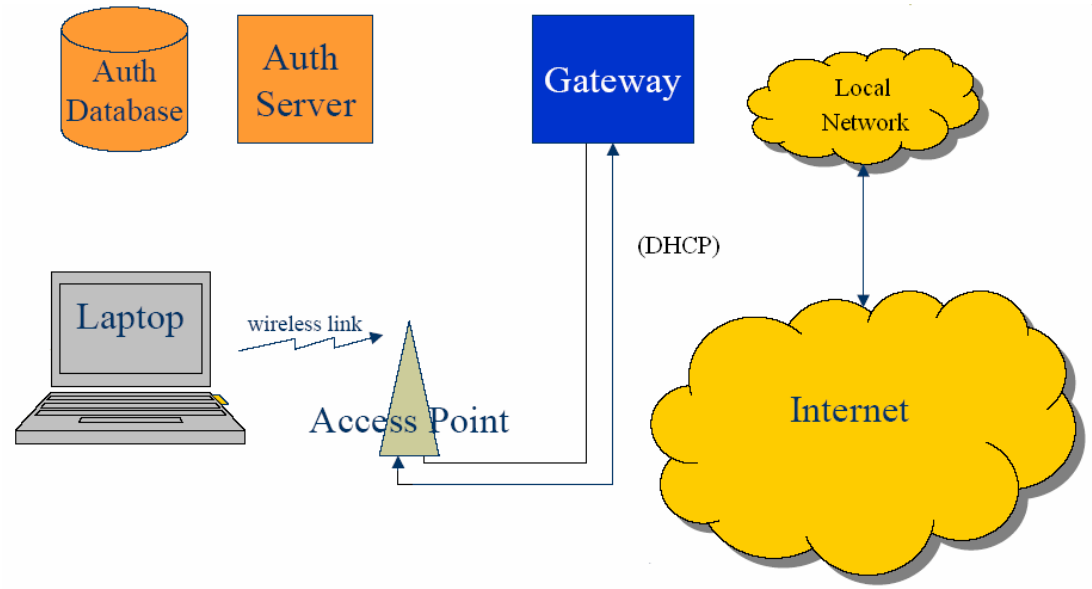


Figura 4-4: Il client si collega alla rete e ottiene un indirizzo IP tramite il DHCP

Un client per autenticarsi deve prima di tutto connettersi con l'access point e ottenere un indirizzo IP valido. Se vogliamo assegnare gli indirizzi IP in modo dinamico dobbiamo installare il DHCP server (Dynamic Host Configuration Protocol), protocollo di configurazione dinamica degli indirizzi che permette ai dispositivi di rete di ricevere la configurazione IP necessaria per poter operare su una rete basata su Internet Protocol nella stessa macchina del gateway o nell'access point. Nella figura 4-4 sono evidenziati i passi necessari per il collegamento alla rete:

1. l' utente si collega all'access point
2. l'utente fa una richiesta di indirizzo IP, tramite il DHCP client
3. La richiesta arriva al DHCP server che gli assegna un indirizzo IP valido e glielo comunica.

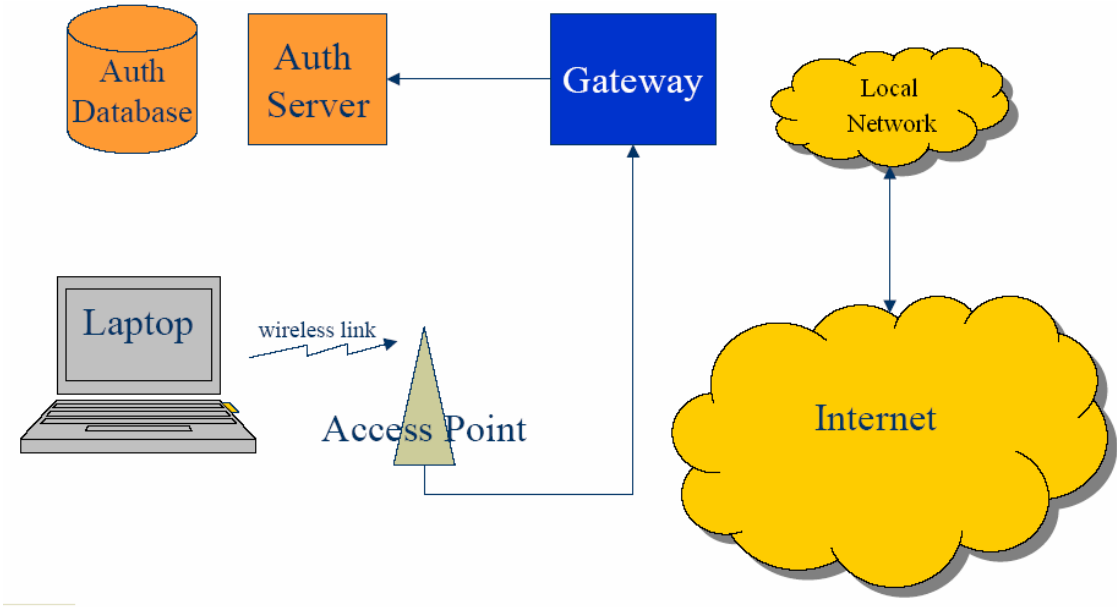


Figura 4-5: Il client richiede una pagina web e viene ridiretto alla pagina di autenticazione

Il client, dopo essersi collegato all'access point tenta di collegarsi ad un computer dietro il gateway (es. richiede una pagina web). Il gateway intercetta la richiesta e la ridirige verso una pagina di autenticazione gestita dall'authservice, dopo avergli appeso un token casuale e altre informazioni sul URL della pagina voluta.

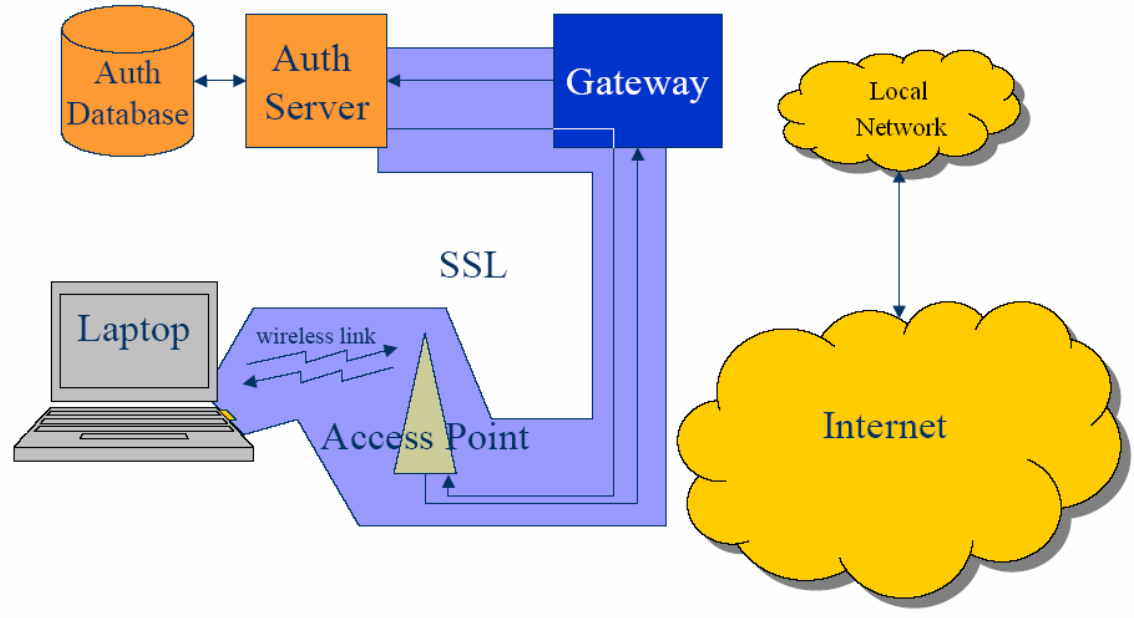


Figura 4-6: L'authservice crea una connessione criptata SSL per l'autenticazione

L'authservice crea una connessione SSL, quindi a livello TCP del modello ISO-OSI, per cifrare la comunicazione. Per creare questa connessione SSL vengono usati appositi certificati e su questo si basa tutta la sicurezza dell'autenticazione. In questo collegamento viaggiano l'username e la password dell'utente che non possono essere oggetto di spoofing perché criptati.

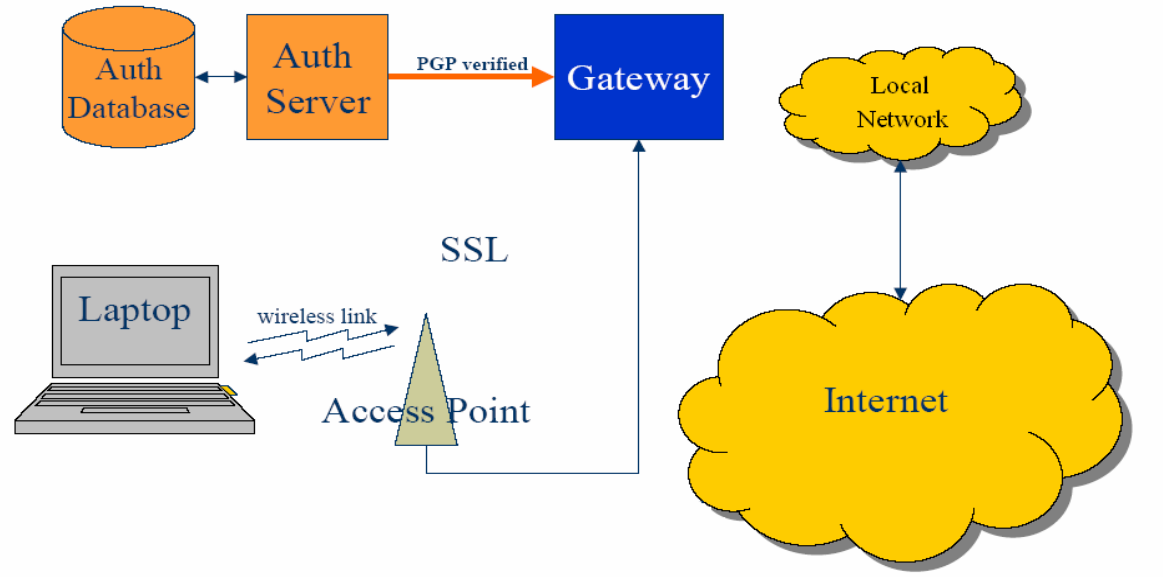


Figura 4-7: L'authservice comunica l'autenticazione al gateway con un messaggio PGP

L'authservice controlla se i dati immessi sono corretti, interrogando un database. In caso affermativo, crea un messaggio criptato PGP e lo manda al gateway. Il gateway che possiede la chiave pubblica PGP dell'authservice controlla l'autenticità del messaggio e autentica l'utente. La presenza di un token casuale nella comunicazione elimina la possibilità di un attacco , la firma digitale PGP impedisce la presenza di authservice fasulli.

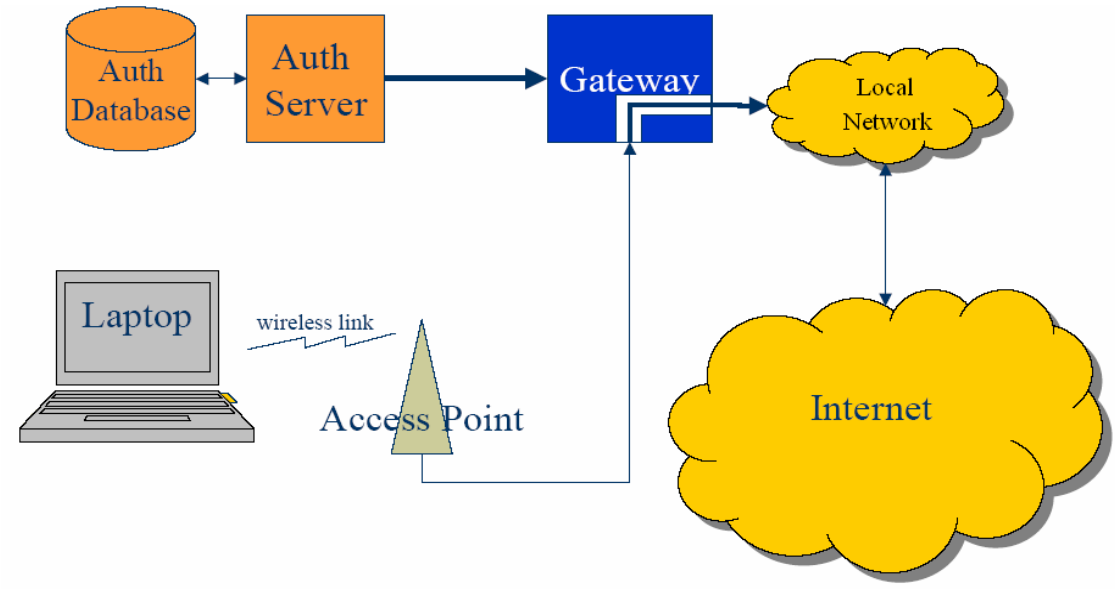


Figura 4-8: Il client viene autenticato e ridirezionato alla pagina richiesta

A questo punto il gateway modifica le regole di firewall per permette ulteriori accessi all'utente e ridirige l'utente verso la pagina che aveva inizialmente richiesto.
Solo a questo punto l'utente può interagire con la rete locale in questo modo si minimizzano i rischi legati alla sicurezza. Queste regole vengono poi cancellate quando l'utente clicca sul pulsante di logout di una apposita finestra, apertasi dopo il login.
Il gateway riconosce l'utente attraverso l'IP e l'indirizzo MAC, quindi attua un livello di sicurezza a livello Network e Data-Link. Queste due informazioni sono facilmente carpibili ascoltando la rete in modalità promiscua. Quindi un hacker potrebbe isolare un utente (interruzione) e connettersi al posto suo. Per evitare questa possibilità, i progettisti solitamente impostano un limite di tempo alla connessioni degli utenti (impostabile in fase di configurazione), dopo di che il client deve riautenticarsi. Questa riautenticazione avviene in modo nascosto all'utente, attraverso un Javascript all'interno della finestra di logout.
Il codice html della pagina di login, ogni $timeout secondi una form, contenente username e password, viene mandato al gateway in forma criptata per mantenere viva la connessione.
Quindi un hacker che causi una interruzione ai danni di un utente ha al massimo $timeout secondi di connessione libera, in quanto non conosce l'username e la password per ripristinare la connessione. Questo metodo evita di tenere aperta una connessione quando non è necessario supportando anche cadute accidentali del collegamento.
Come si è detto la variabile $timeout è configurabile dall'utente e assume un minimo di 60 secondi. Non esiste un valore ottimale assoluto di questa variabile ma dipende dal numero di utenti che si collegano alla rete. Il valore scelto deve essere un compromesso tra overhead di informazioni e il livello di sicurezza che si vuole assicurare.

4.3 Gateway

Il gateway è la parte del sistema che gestisce l'accesso alla rete, opera al livello di rete e superiori del modello ISO/OSI, permettendo l'accesso ai soli utenti autorizzati. Il suo scopo principale è quello di veicolare i pacchetti di rete all'esterno della rete locale. Il compito svolto dal gateway si può, quindi, riassumere nei seguenti punti:

- Permette l'accesso alla rete ai soli utenti autorizzati
- Imposta le limitazioni di banda ai vari utenti
- Imposta il NAT (network address translation una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router)

Per svolgere il suo compito, il gateway imposta in modo dinamico opportune regole di filtraggio dei pacchetti IP. Le regole di firewall permettono di gestire i pacchetti IP in arrivo e in uscita da un router. Sui vari pacchetti si possono eseguire diverse azioni che vengono scelte analizzando l'header dei vari frame, in particolar modo i campi: protocollo, mittente, destinatario e mark. I vari pacchetti, prima di essere spediti, devono transitare in opportune catene dove vengono sottoposti alle varie regole.

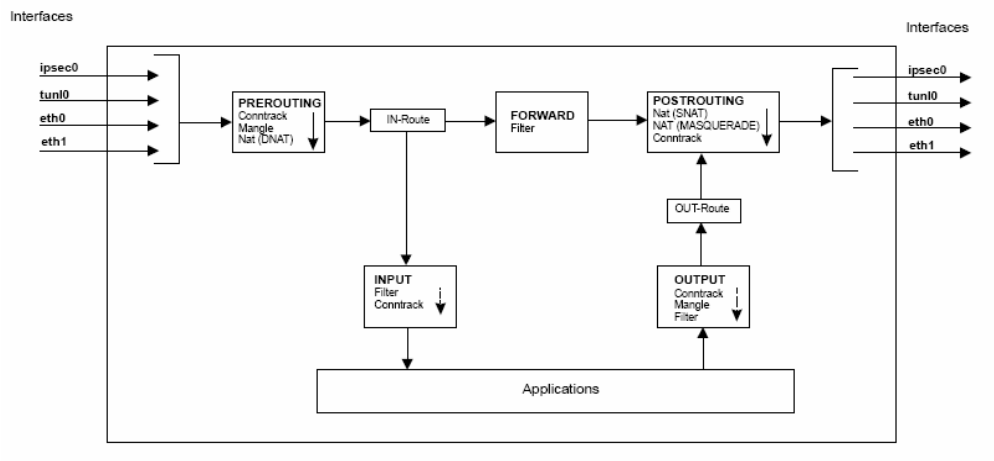


Figura 4-9: Struttura della catena di filtraggio dei pacchetti in un sistema linux

4.4 L'Authservice

L'authservice si occupa dell'autenticazione degli utenti. Questa autenticazione si appoggia al protocollo sicuro HTTPS e, quindi, richiede l'installazione sulla stessa macchina del web server.

I progettisti solitamente consigliano di non installare sulla stessa macchina del gateway in quanto a questa possono accedervi anche gli utenti non autenticati e quindi potenzialmente pericolosi infatti, l'authservice è stato costruito per accedere ad un database locale e non remoto, di conseguenza la presenza delle credenziali degli utenti su una macchina accessibile a tutti è sicuramente da evitare.

I Captive portal permettono un autenticazione sicura, user-friendly e semplice degli utenti wireless. Nonostante questi vantaggi soffrono di alcune limitazioni :

- Limitazione della banda, rigida e poco flessibile.
- Accesso ai soli database locali.
- Gestione credenziali degli utenti poco user-friendly.
- Uso di database proprietari.

Il software non permette di imporre alcuna limitazione di routing ai client cioè non è possibile impedire ad un utente di comunicare con una determinata rete.

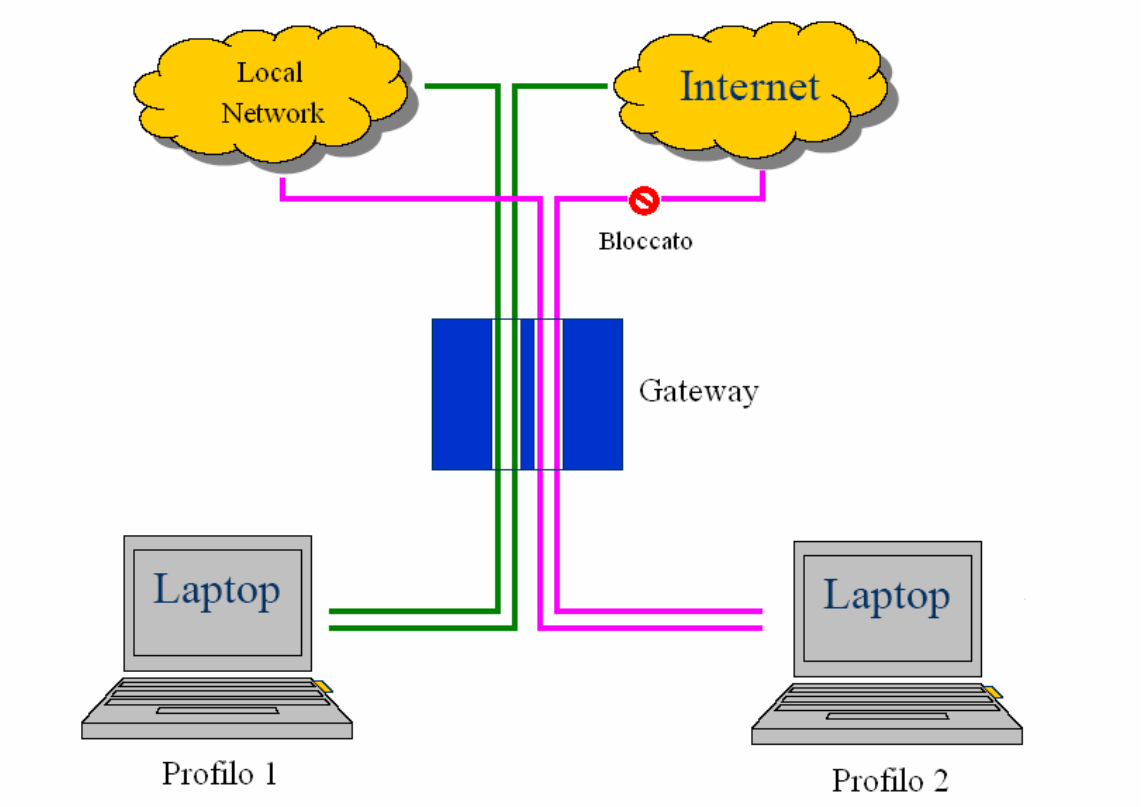


Figura 4-10: Esempio di limitazione di routing

In questo caso il gateway dovrebbe riconoscere i pacchetti dei vari profili e bloccare le connessioni verso reti non autorizzate, come illustrato in figura.

Per imporre queste limitazioni si definiscono diversi profili di routing e si associa ogni utente con uno solo di essi. Questi profili non sono altro che regole di filtraggio dei pacchetti che vengono inserite all'avvio del gateway. I pacchetti IP degli utenti vengono marcati in modo differente a seconda del gruppo a cui appartiene il client, infine il gateway accetta o elimina un pacchetto osservando il campo destinazione del frame.

Per inserire le suddette regole, bisogna conoscere il nome del profilo a cui appartiene l'utente e questa informazione è nota all'authservice ma non al gateway a cui è legato .

Ogni utente ha il suo file, in questo modo si evitano i problemi di accesso simultaneo ad esso, e una volta conosciuto il nome del profilo dell'utente, vengono marcarti i vari pacchetti in modo opportuno e quindi inserite o rimosse le regole correttamente.

Oltre ai profili di routing inseriti dall'amministratore di sistema, esiste un profilo di default che permette di accedere solo alla rete immediatamente dietro al gateway, questo consente di

spostare o replicare il gateway su un'altra rete senza cambiare il profilo base. Questo profilo viene aggiornato ad ogni avvio del gateway .

La gestione degli utenti e dei profili nel software avviene per linea di comando e quindi è poco user-friendly, inoltre con l'aggiunta dei nuovi servizi per limitare il routing e la banda, è cresciuta la mole di informazione da memorizzare nei database e anche la complessità della configurazione dei profili e degli utenti. Infatti per aggiungere o rimuovere un profilo bisogna modificare alcuni script e shell. Fare tutto questo manualmente è molto scomodo, complesso e potenzialmente pericoloso in caso di errore. Per ovviare a questo inconveniente è possibile creare un'interfaccia web, che permette di gestire gli utenti e i profili in modo semplice e intuitivo.

L'aggiunta di nuovi servizi al software si riflette in un miglioramento della qualità del prodotto ma, anche in un aumento delle informazioni da memorizzare nel database. In alcune versioni il software permette di interfacciarsi con due database: uno locale e uno remoto, dove nel database locale sono memorizzate le informazioni usate dalla versione base del software e quelle aggiuntive relative ai nuovi servizi, mentre nel database remoto sono memorizzati gli username e le password degli utenti.

In questo modo i vari utenti possono accedere ai diversi servizi con lo stesso username e password, senza duplicare dati sensibili come le credenziali degli utenti e senza complessi problemi di allineamento dei database. Infatti, quando un utente effettua un login, l'authservice si collega al database centrale, verifica se le credenziali sono corrette e in caso affermativo autentica l'utente.

Capitolo 5

CONCLUSIONI

Le leggi vigenti in materia di tutela della privacy e trattamento dei dati personali impongono l'adozione di forti misure di sicurezza per proteggere le informazioni trasmesse e archiviate.
Con l' entrata in vigore del "Codice in materia di protezione dei dati personali" (Decreto Legislativo n. 196 del 30 giugno 2003) è stata riordinata una materia che dopo la legge n.675/96, a causa dei numerosi testi normativi succedutisi nel tempo, risultava essere di difficile interpretazione. Rilevante interesse per coloro che trattano sistemi informatici basati su reti di telecomunicazioni – ad esempio quelli basati sulla tecnologia wireless oggetto di questo studio – appare il titolo V del Codice che disciplina la sicurezza dei dati e dei sistemi. In particolare, in relazione alle misure di sicurezza, il Codice stabilisce che i dati personali oggetto di trattamento debbono essere custoditi e controllati "*anche in relazione alle conoscenze acquisite in base al progresso tecnico nonché alla natura dei dati ed alle specifiche caratteristiche del trattamento al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta."*
Questo significa prevedere, anche in presenza di tecnologie innovative quali il wireless, data la loro potenziale più facile accessibilità da parte di terzi "estranei" al sistema di rete, misure adeguate alla protezione dei dati in esse custoditi. Tali misure di sicurezza sono a cura di quel soggetto che il Testo Unico sulla Privacy definisce Titolare del Trattamento dei Dati (o del *Responsabile* se designato, oppure dell'*Incaricato* al trattamento).
Questo significa che all'interno di un'azienda pubblica o privata che sia, dove il trattamento di dati personali (non necessariamente sensibili) è per ovvii motivi ampiamente diffuso (basti pensare ai dati riguardanti i dipendenti, i clienti, i fornitori, gli utenti di una rete pubblica quale quella di un ateneo) il titolare che non riesce a garantire l'adeguamento dell'infrastruttura informatica agli standard minimi previsti viene a trovarsi di fatto in una situazione di illecito.
In caso di trattamento di dati sensibili con strumenti elettronici, la legge prevede un complesso di misure di sicurezza tecniche, informatiche, organizzative, logistiche e procedurali, che nell'insieme configurano il livello di protezione necessario. L'art. 34 infatti prevede che "*il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate misure minime di sicurezza, nei modi previsti dal disciplinare tecnico* ".

Appare quindi evidente come anche nell'implementazione di una tecnologia quale il wireless, i soggetti addetti alla progettazione e all'amministrazione della rete debbano ricercare le soluzioni più adatte alla sicurezza dei dati trattati. Le scelte tecnologiche verranno effettuate tenuto conto dell'importanza e della sensibilità delle informazioni custodite nei sistemi informatici, con un occhio di riguardo alle prescrizioni normative dettate dai molteplici testi nascenti a difesa della privacy dei titolari di suddetti dati. Continuando con la disamina del D.Lgs. 196/2003, all' interno del disciplinare tecnico vengono precisate le misure da adottare nella conservazione e nell'utilizzo dei dati personali ed in particolare di quelli sensibili. Nel caso i dati vengano trattati con l'ausilio di strumenti informatici, dal punto di vista tecnico, la legge impone quindi l'adozione di un sistema di autenticazione in grado di assegnare diversi diritti a diverse utenti, la protezione del sistema da intrusioni e virus, l'utilizzo di strumenti di backup dei dati e, in caso di trattamento di dati personali riguardanti, l'adozione di tecniche di crittografia per la conservazione e la trasmissione dei dati o la loro archiviazione disgiunta (dati sensibili in un database, persone fisiche a cui si riferiscono in un altro) al fine di rendere gli stessi incomprensibili da chi non ha il diritto di utilizzarli. La scelta di soluzioni di sicurezza più robuste della semplice crittografia a chiave WEP, l'implementazione di un solido sistema di autenticazione ed autorizzazione mediante l'utilizzo di un server RADIUS dedicato, la creazione di una Virtual Private Network sulla quale far transitare i dati al sicuro da "orecchie" indiscrete, saranno l'arma vincente per la progettazione di una rete wireless a norma.

BIBLIOGRAFIA

[1] Nathan Zorn, Authentication Gateway Howto:
http://www.itlab.musc.edu/~nathan/authentication_gateway/
[2] Maxim, Pollino, La sicurezza delle reti wireless, Apogeo, 2003
[3] Ribeiro, Silva, Severiano, A roming Wifi Autentication using VPNs with client certificates, 2003: http://wifi.tagus.ist.utl.pt/description.pdf
[4] Opengate-an autentication system for public and mobile terminals :
http://www.cc.saga-u.ac.jp/opengate/index-e.html
[5] Agatino, Grillo, Virtual Private Network: www.agatinogrillo.it/pdf/vpn.pdf
[6] IEEE: http://standards.ieee.org/getieee802/802.11.html
[7] Sameer, Implementing secure services over a wireless network
http://verma.sfsu.edu/users/wireless/nocatauth_report.pdf
[8] WiFi Alliance: http://www.wi-fi.org
[9] Brewer, Autentication gateway:
http://bcrc.bio.umass.edu/presentations/wireless_gateways.pdf.
[10] Pauletto, Wireless fidelity, Apogeo, 2003