Capitolo 1

Lo stack di rete

In questo capitolo si vuole presentare la suite di protocolli utilizzata nel progetto di tesi. Verrà descritto brevemente il modello ISO/OSI per poi soffermarsi con particolare attenzione sulla tecnologia Wi-Fi e sui protocolli toccati dal progetto di tesi. ISO/OSI è uno standard che definisce un modello composto su più livelli: ogni *layer* si occupa di uno specifico aspetto delle comunicazioni di rete fornendo delle funzionalità a livello superiore e sfruttando le astrazioni fornite dal livello immediatamente inferiore. In questo modo è possibile ridurre la complessità non banale delle comunicazioni di rete.

1.1 Il modello ISO/OSI

Il modello OSI Open System Interconnection è uno standard per le reti di calcolatori stabilito da ISO International Standard Organization che definisce l'architettura logica di rete come una struttura a strati composta da una pila di protocolli di comunicazione di rete suddivisa in 7 livelli, i quali insieme espletano in maniera logico-gerarchica tutte le funzionalità della rete. Ciascun layer racchiude in sé a livello logico uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layers vanno dal livello fisico (quello del mezzo fisico, ossia del cavo o delle onde radio) fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di alto livello. Come già accennato ciascun livello fornisce servizi e funzionalità al livello superiore utilizzando le astrazioni fornite dal livello inferiore. Ma vediamo brevemente le funzioni di ciascun livello all'interno dello stack ISO/OSI.

Physical Layer Si occupa di trasmettere dati non strutturati attraverso un mezzo fisico e di controllare la rete, gli hardware che la compongono e i dispositivi che permettono la connessione. In questo livello vengono decisi diversi aspetti legati al mezzo fisico come ad esempio le tensioni scelte per rappresentare i valori logici dei bit trasmessi, la durata in microsecondi del segnale che identifica un bit, la modulazione e la codifica utilizzata e l'eventuale trasmissione simultanea in due direzioni (duplex).

Datalink Layer Questo livello si occupa in primis di formare i dati da inviare attraverso il livello fisico, incapsulando il pacchetto proveniente dallo strato superiore in un nuovo pacchetto provvisto di un nuovo header (intestazione) e tail (coda). Questa frammentazione dei dati in specifici pacchetti è detta framing e i singoli pacchetti sono chiamati *frame*. Il livello Datalink effettua inoltre un controllo degli errori e delle perdite di segnale in modo tale da far apparire, al livello superiore, il mezzo fisico come una linea di trasmissione esente da errori di trasmissione.

Network Layer Si occupa di rendere i livelli superiori indipendenti dai meccanismi e dalle tecnologie di trasmissione usate per la connessione e prendersi carico della consegna a destinazione dei pacchetti. È responsabile del *routing* ovvero della scelta ottimale del percorso di rete da utilizzare per garantire la consegna delle informazioni dal mittente al destinatario, scelta svolta dal router attraverso dei particolari algoritmi di routing e tabelle di routing. È responsabile inoltre della conversione dei dati nel passaggio fra una rete ed un'altra con diverse caratteristiche, come il protocollo di rete utilizzato: si deve occupare quindi di tradurre gli indirizzi di rete, valutare la necessità di frammentare i pacchetti dati se la nuova rete ha una diversa Maximum Transmission Unit (MTU) e di valutare la necessità di gestire diversi protocolli attraverso l'impiego di gateway. L'unità dati fondamentale è il pacchetto o *datagram*.

Transport Layer Permettere un trasferimento di dati trasparente e affidabile (implementando anche un controllo degli errori e delle perdite) tra due host. È il primo livello realmente end-to-end, cioè da host sorgente a destinatario. Si occupa di stabilire, mantenere e terminare una connessione, garantendo il corretto e ottimale funzionamento della sottorete di comunicazione nonché del controllo della congestione: evitare che troppi pacchetti dati arrivino allo stesso router contemporaneamente con effetto di perdita di pacchetti stessi. A differenza dei livelli precedenti, che si occupano di connessioni tra nodi contigui di una rete, il Transport Layer si occupa solo

del punto di partenza e di quello finale. Si occupa anche di effettuare la frammentazione dei dati provenienti dal livello superiore in pacchetti, detti "segmenti" e trasmetterli in modo efficiente ed affidabile usando il livello rete ed isolando da questo i livelli superiori. Inoltre, si preoccupa di ottimizzare l'uso delle risorse di rete e di prevenire la congestione.

Session Layer Consente di aggiungere, ai servizi forniti dal livello di trasporto, servizi più avanzati, quali la gestione del dialogo (mono o bidirezionale), la gestione del token (per effettuare mutua esclusione) o la sincronizzazione (inserendo dei checkpoint in modo da ridurre la quantità di dati da ritrasmettere in caso di gravi malfunzionamenti). Si occupa anche di inserire dei punti di controllo nel flusso dati: in caso di errori nell'invio dei pacchetti, la comunicazione riprende dall'ultimo punto di controllo andato a buon fine.

Presentation Layer Si occupa di trasformare i dati forniti dalle applicazioni in un formato standardizzato e offrire servizi di comunicazione comuni, come la crittografia, la compressione del testo e la riformattazione.

Application Layer Il livello Applicazione è quello più vicino al livello utente fornisce quindi un interfaccia tra le applicazioni e lo stack di rete sottostante che si occupa dell'invio di messaggi. I protocolli di livello applicazione si occupano quindi dello scambio di informazioni tra apps in esecuzione sull'host sorgente e quello destinatario della comunicazione.

1.2 ISO/OSI vs TCP/IP

TCP/IP sviluppato inizialmente dal dipartimento della difesa americano e utilizzato nei primi computer UNIX-based attualmente è lo *standard de facto* per tutte le comunicazioni internet.
TCP/IP, come l'OSI model, è strutturato su più livelli alcuni molto simili per caratteristiche e funzionalità a quelli di ISO/OSI: TCP/IP accorpa in un unico layer funzionalità contenute su più livelli del modello OSI.

TCP/IP è l'approccio utilizzato in ogni tipo di comunicazione internet. L'obbiettivo di ISO/OSI invece è quello fornire uno standard da usare come guideline per la definizione di protocolli e applicazioni internet.

I layer nello stack TCP/IP sono quattro e sono così organizzati rispetto al modello OSI come illustrato nella figura 1.1.

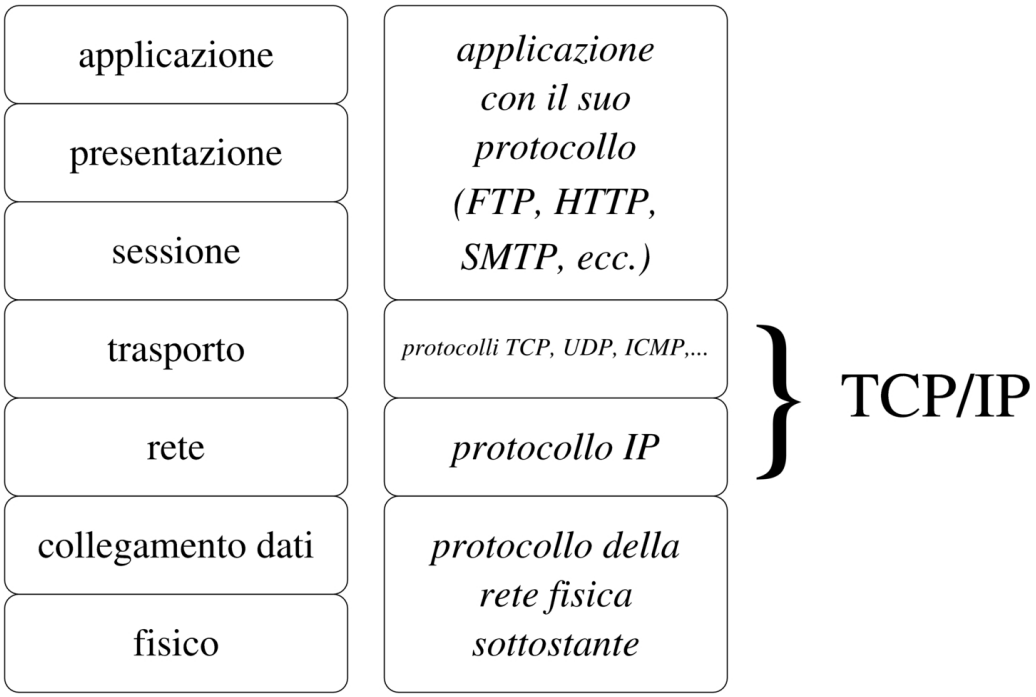

Figura 1.1: Stack di rete ISO/OSI e TCP/IP

1.3 Wi-Fi

Wi-Fi indica una tecnologia che consente a calcolatori collocati su di una stessa WLAN (Wireless Local Area Network) di comunicare senza fili attraverso specifiche frequenze di onde radio. Sempre più dispositivi dispongono di interfacce di rete Wi-Fi dai laptop, gli smartphone fino agli elettrodomestici di ultima generazione che possono essere così interconnessi entro un certo raggio di copertura. La tecnologia Wi-Fi può essere usata per fornire connettività internet ai dispositivi presenti nel raggio di copertura della WLAN se la Local Area Network è connessa a internet.

1.3.1 WLAN architecture and types

L'architettura di una WLAN è caratterizzata da diverse componenti.

Stazioni In una WLAN ciascun dispositivo munito di Wireless Network Interface Controllers (WNICs) e che quindi può comunicare senza fili è detto stazione. Vi sono due categorie di stazioni:

- access points (AP) ovvero dispositivi elettronici che ricevono/trasmettono segnali radio da/verso nodi mobili equipaggiati con schede di rete Wi-Fi
- clients tutti i nodi mobili che possono essere equipaggiati con una wireless network interface come ad esempio laptops, smartphones, workstations

Basic service set Il Basic Service Set (BSS) è un insieme di tutte le stazioni che possono comunicare tra loro. Ciascun BSS ha un proprio identificativo detto BSSID che corrisponde al indirizzo MAC dell'access point che serve i diversi clients per quella BSS.
Vi sono due tipi di BSS:

- Indipendent BSS (IBSS) ovvero una *rete ad-hoc* caratterizzata dall'assenza di un access point. Questo tipo di BSS non può quindi essere interconnesso con altri Basic Service Set
- Infrastructure BSS caratterizzati dalla presenza di un access point, un BSS di questo tipo può essere connesso con altri Basic Service Set

Extended Service Set Un Extended Service Set (ESS) è un insieme di BSS interconnessi tra loro. Gli access points in un ESS sono connessi tra loro da un *Distribution System*. Ciascun EES è caratterizzato da una stringa identificativa lunga al massimo 32 byte detta SSID.

Distribution System Il Distribution System (DS) interconnette tra loro gli access point di diversi EES. Un access point può essere principale, di inoltro o remoto. Un access point principale è collegato tipicamente alla rete cablata. Un access point di inoltro trasmette i dati fra le stazioni remote e principali. Un access point remoto accetta i collegamenti dai client senza fili e li passa a quelli di inoltro o quelli principali.

Esistono due tipologie di rete WLAN che differiscono dalle modalità di comunicazione:

- infrastructure i nodi comunicano tra loro attraverso a una base station che funge da wireless access point

- reti ad-hoc, ovvero una rete dove le stazioni possono comunicare peer-to-peer (P2P) senza alcun access point. Questo viene realizzato tramite IBSS

1.4 IEEE 802.11

IEEE 802.11 è uno standard di trasmissione per reti WLAN operanti su frequenze 2.4, 3.6, 5 e 60 GHz che definisce un interfaccia di comunicazione base per comunicazione Wi-Fi. Le specifiche definite nello standard 802.11 si focalizzano sul livello fisico e MAC del modello ISO/OSI. Il sistema di numerazione 802.11 è dovuto a IEEE che utilizza 802.x per indicare una famiglia di standard per le comunicazione di rete tra cui lo standard *Ethernet* (IEEE 802.3). Per tanto IEEE 802.11 si adegua perfettamente agli altri standard 802.x per reti locali wired e le applicazioni che lo utilizzano non dovrebbero notare nessuna differenza logica, una degradazione delle performance invece è tuttavia possibile. IEEE 802.11b è stato il primo protocollo largamente utilizzato seguito da 802.11a, 802.11g, 802.11n, and 802.11ac. Vi sono altri standard nella famiglia 802.11 (c-f, h, j) che sono per lo più piccole modifiche, estensioni o correzioni alle precedenti specifiche.
Per quanto concerne le performance lo stream data rate può arrivare fino a 780 Mbit/s in 802.11ac grazie anche alla tecnologia MIMO (Multiple-Input and Multiple-Output) che consente di aumentare la capacità del canale trasmissivo usando più trasmittenti e ricevitori sfruttando così il fenomeno del *multipath-propagation* ovvero un segnale radio può raggiungere un ricevitore attraverso diversi percorsi, *path*.

1.4.1 Physical Layer in 802.11

Come già detto IEEE 802.11 utilizza le bande di frequenza 2.4, 3.6, 5 e 60 GHz e a *livello fisico* vengono usate delle tecniche di modulazione *half-duples*: in particolare viene utilizza la Orthogonal Frequency-Division Multiplexing (OFDM) che utilizza un numero elevato di sotto-portanti ortogonali tra di loro, oppure quella chiamata Direct Sequence Spread Spectrum (DSSS), che è una tecnologia di trasmissione a banda larga nella quale ogni bit viene trasmesso come una sequenza ridondante di valori, detti chip, rendendola così più resistente ad eventuali interferenze.

1.4.2 Media Access Control

Media Access Control (MAC) è un *sublayer* del livello *Data Link* del modello OSI. MAC fornisce meccanismi di indirizzamento e di controllo di accesso al canale che consentono a nodi mobili di comunicare attraverso una rete con medium condiviso. L'hardware che implementa MAC è detto *media access controller*. Le funzioni principali del MAC sono quindi quelle di regolamentare l'accesso al mezzo fisico, frammentazione dati in frame e riconoscimento frame stessi e controllo degli errori.

1.4.3 CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance è un protocollo di accesso multiplo in cui i nodi cercano di evitare a priori il verificarsi di collisioni in trasmissione. Questo approccio è l'ideale per tipologie di reti nella quale non risulta possibile (oppure poco affidabile e dispendioso) rilevare un'avvenuta collisione.
Quando un nodo vuole effettuare una trasmissione ascolta il canale *(listen-before-talk)* (LBT): se il canale risulta *idle* il nodo aspetta un certo *DISF time (Distribuited Inter Frame Space)* trascorso il quale, se il canale risulta ancora libero, comincerà a trasmettere. A termine della trasmissione il nodo sorgente aspetterà per certo intervallo *SISF (Short Inter Frame Space)*, più piccolo di DISF, la ricezione di un *ACK*. Se il nodo sorgente non riceve alcun ACK ritrasmetterà il messaggio per un certo numero di volte.
Per tutta la durata della trasmissione e per la durata dello SISF time le altre stazioni, trovando il canale occupato, non avvieranno altre comunicazioni evitando così collisioni. La durata dello SISF inferiore a quello dell'intervallo di DISF assicura che nessuna stazione comincerà una trasmissione prima della ricezione dell'eventuale messaggio di acknowledgment da parte del nodo che ha appena concluso la trasmissione.
Nel caso in cui una stazione volesse trasmettere e rileva il canale occupato attenderà per un certo intervallo di tempo casuale, detto intervallo di *back-off*, prima di riprovare a trasmettere. L'intervallo di back-off è realizzato per mezzo di un timer che decrementa il valore di un contatore, inizializzato con il valore dell'intervallo, solamente nei periodi di inattività del canale, ovvero quando non vi sono trasmissioni, il valore del contatore resterà invece invariato durante i periodi di trasmissione da parte di altre stazioni (*frozen back-off*). Quando il valore del contatore raggiungerà lo zero la stazione effettuerà un nuovo tentativo di trasmissione. Questo meccanismo di accesso al mezzo è detto *Basic Access Mechanism*

1.4.4 Il problema dei nodi nascosti

Il problema dei nodi nascosti in una rete wireless si ha quando un nodo all'interno della rete è visibile da un Access Point ma non da tutte le altre stazioni collegate al medesimo AP. Questo può comportare una serie di problemi per quanto riguarda il controllo dell' accesso al mezzo.

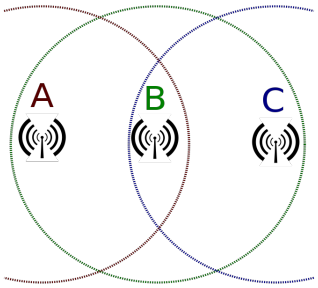

Figura 1.2: Il problema dei nodi nascosti

Come si può vedere dalla figura 1.2 la stazione A e la C sono nel raggio di copertura della stazione B. Per qualche motivo (come può essere la distanza o un ostacolo) A e C non possono comunicare direttamente e quindi non possono nemmeno rilevare (*sensing*) la portante trasmessa dall'altra stazione verso la stazione centrale B. In particolare si possono quindi verificare delle collisioni quando sia A che C, rilevando il canale libero, effettuano in contemporanea una trasmissione verso B.
Per ovviare a questo problema IEEE 802.11 definisce un meccanismo opzionale che introduce due tipi di pacchetti di controllo, in particolare:

- *RTS* (Request To Send), quando un nodo vuole trasmettere, prima di inviare il frame vero e proprio, invia al destinatario un pacchetto di tipo RTS contenente destinatario del messaggio, mittente e durata della trasmissione che seguirà

- *CTS* (Clear To Send), quando un nodo riceve un pacchetto di tipo RTS risponde con un pacchetto di tipo CTS che contiene essenzialmente le stesse informazioni contenute nel frame di tipo RTS; quando il nodo mittente avrà ricevuto il frame CTS potrà cominciare l'inoltro del frame effettivo precedentemente annunciato tramite il rispettivo RTS

I pacchetti RTS e CTS vengono inoltrati a tutte le stazioni comprese quindi anche quelle nascoste al mittente che si metteranno in attesa per tutta la durata della trasmissione come specificato dai frame di controllo.
Questo meccanismo non è del tutto esente da collisioni. Infatti le collisioni

possono ancora avvenire durante lo scambio dei pacchetti di controllo: ad esempio due stazioni mandano contemporaneamente una Request To Send. Nonostante ciò la probabilità di collisione risulta essere più bassa e meno significativa rispetto all'approccio che non fa uso dei pacchetti RTS/CTS in quanto i frame di controllo hanno una dimensione molto ridotta (up to 2347 Bytes).
Se una stazione vuole trasmettere un pacchetto di dimensione inferiore al frame di controllo il messaggio verrà inoltrato immediatamente senza prima generare il corrispettivo RTS.

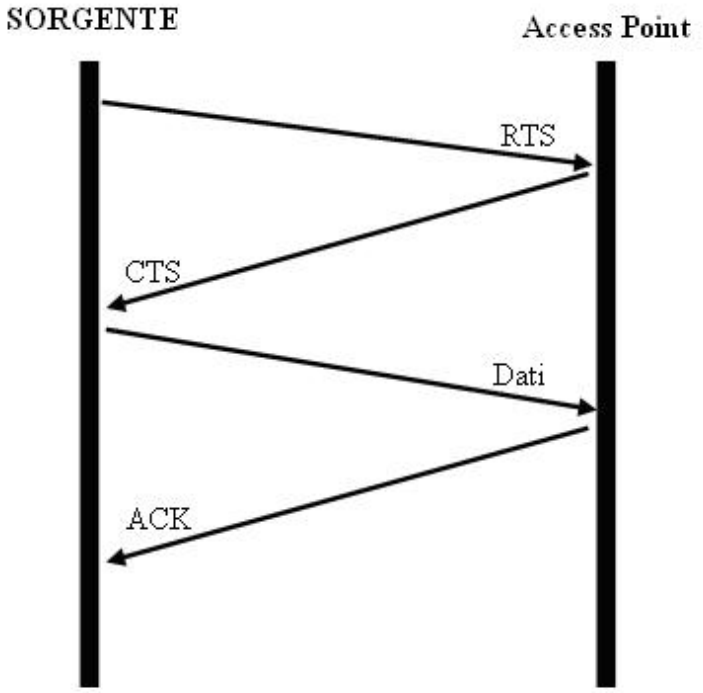

Figura 1.3: *Four-way handshake* via RTS/CTS

1.4.5 IEEE 802.11 frame

IEEE 802.11 definisce tre tipologie di frame:

- DATA, contengono meramente dati
- CTRL, servono per facilitare l'interscambio di data frame tra le stazione; appartengono a questa categoria i frame RTS, CTS e ACK

- MGMT, frame utili al mantenimento della comunicazione; i *beacon frame* (frame inviato periodicamente da un AP per annunciare al sua presenza e il suo SSID) appartengono a questa categoria

Ciascun frame è composto da un *MAC header*, un *payload* e un *frame check sequence (FCS)*.

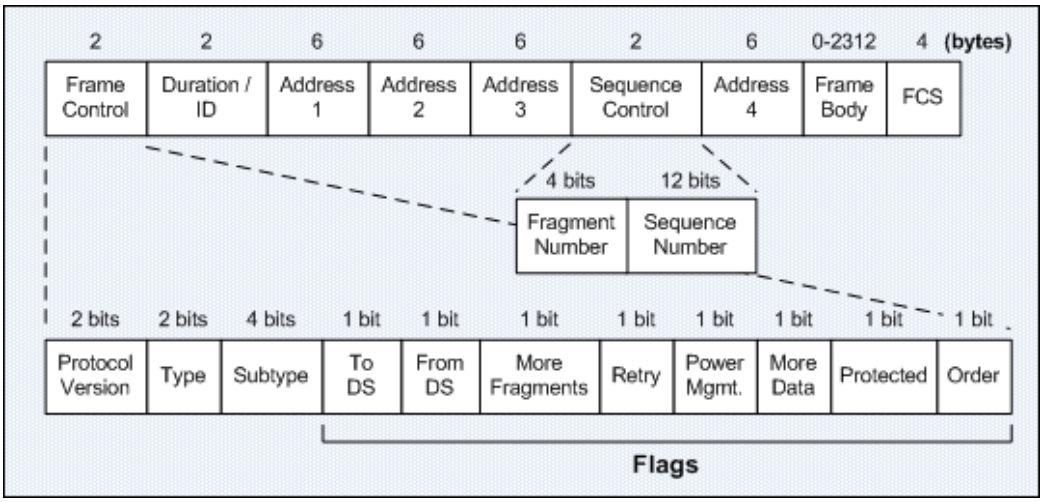

Figura 1.4: IEEE 802.11 frame

MAC header I primi due Byte del MAC header contengono un campo molto interessante, il *frame control*. Il frame control contiene diversi sottocampi:

- Protocol Version, ovvero due bit rappresentanti la versione del protocollo, posto sempre a zero; altri valori sono riservati per un uso futuro
- Type, due bit identificanti appunto il tipo di frame
- Subtype, quattro bit che identificano il sottotipo del frame; ad esempio come beacon è un sottotipo di MGMT
- ToDS & FromDS, ciascun campo occupa un bit e indica se un data frame è diretto o proviene da un distribution system. I frame di tipo CTRL e MGMT hanno entrambi i flag settati a zero
- More Fragments, bit settato quando un pacchetto è viene frammentato in più frame per la trasmissione; tutti i pacchetti con eccezione dell'ultimo inviato avranno questo flag settato

- Retry, indica se un frame è stato oggetto di ritrasmissione; utile per eliminare eventuali frame duplicati.
- Power Management: indica il *power management state* (ovvero se la stazione è in power-save state o meno) del mittente settato dopo la trasmissione. Gli AP non setteranno mai questo bit in quanto sempre attivi per la gestione delle connessioni
- More Data, questo bit indica che c'è almeno un pacchetto disponibile; settato dagli AP per facilitare le stazioni in power-save mode
- Protected, indica se il payload del frame è stato cifrato o meno
- Order, questo bit è settato solamente quando i frame sono inviati in ordine uno dietro l'altro; spesso ciò non avviene per motivi di performance

Gli altri campi contenuti nell'header MAC sono la durata di trasmissione, gli indirizzi MAC (*source*, *destination*, *transmitter* e *receiver*) e il *Sequence Control*.
Il campo Sequence Control è composto da due Byte usato per identificare l'ordine dei frame spediti. I primi 4 bit corrispondono al *fregmentation number* e gli ultimi 12 bit sono il *sequence number*. Il fragmentation number indica il numero di ogni pacchetto precedentemente frammentato, il sequence number, invece, è un valore modulo 4096 assegnato a un frame e rimane costante per ogni ritrasmissione o per ciascun fragment di quel pacchetto.

Payload Il Payload ha dimensione variabile da 0 a 2304 Byte; contiene informazioni provenienti dai livelli di rete superiori.

Frame check sequence (FCS) Spesso detto anche *Cyclic Redundancy Check* (CRC) permette di verificare l'integrità di un frame appena ricevuto: quando un frame sta per essere spedito la stazione sorgente calcola questo valore e lo appende al frame IEEE 802.11. Quando un nodo riceve il frame ricalcola l'FCS sulla base dei dati ricevuti e lo confronta con il valore contenuto nel *trailer* del pacchetto; se i due valori coincidono il frame non ha subito delle modifiche durante la trasmissione.
Il campo FCS occupa gli ultimi quattro Byte del frame IEEE 802.11

1.4.6 Security in IEEE 802.11

Data la sempre più larga diffusione delle reti Wi-Fi e dalla natura del loro segnale (è molto difficile controllare quale dispositivo riceve il segnale radio

) la sicurezza è un aspetto molto importante e assolutamente da non sottovalutare in 802.11. Nel corso degli anni sono stati sviluppati e proposti diversi approcci per rendere le reti WLAN sempre meno sensibili a intercettazioni e attacchi da parte di terzi.

Access Control List Un primo banale approccio è quello dell'*access control list*. L' Access Point mantiene una lista degli indirizzi MAC autorizzati alla comunicazione: l' AP riceve messaggi provenienti solo dai clients presenti nell'access control list. Qualsiasi messaggio proveniente da una stazione non presente nella lista sarà ignorato.
Questo approccio presenta due grandi difetti. Innanzitutto fornisce solamente una politica di controllo degli accessi senza fornire nessun meccanismo di protezione sui dati trasmessi. Inoltre questo approccio può essere facilmente raggirato tramite una tecnica di *MAC spoofing*. In particolare tramite un software di *wireless network analysis* è possibile monitorare il traffico delle rete WLAN vicine e quindi captare informazioni sensibili da eventuali messaggi trasmessi in chiaro: data la mancanza di confidenzialità nei messaggi trasmessi su reti che adottano esclusivamente la politica dell'Access Control List come protezione è possibile quindi risalire ad indirizzi MAC autorizzati alla comunicazione. A questo punto è possibile modificare l'indirizzo MAC dell'interfaccia di rete (possibile sia in ambiente UNIX che Windows) per impersonare un altro client della rete WLAN.

WEP (Wired Equivalent Privacy) WEP (Wired Equivalent Privacy) è stato il primo protocollo di sicurezza definito nello standard IEEE 802.11. L'obbiettivo di WEP è quello di garantire confidenzialità e integrità del traffico trasmesso in maniera wireless. Il nome è dovuto al fatto che WEP è stato pensato per fornire confidenzialità sui dati trasmessi paragonabile a quella delle reti cablate.
WEP sfrutta il cifrario a chiave simmetrica RC4 con chiave a 64 o 128 bit. La chiave WEP utilizzata è la concatenazione di due valori: il primo dinamico detto Initialization Vector (IV) e la seconda parte statica corrispondente alla chiave segreta condivisa. Il vettore di inizializzazione è una sequenza di 24 bit generata casualmente al momento dell'invio del frame da parte dell'interfaccia di rete (per ogni trasmissione verrà generato un IV in quanto RC4 è un *cifrario a flusso*). A seconda della lunghezza della WEP key la chiave segreta condivisa sarà quindi lunga 40 bit nel caso di una WEP key di 64 bit oppure 104 bit nel caso di una chiave a 128 bit.
Al momento dell'invio di un frame la stazione sorgente genera il vettore di inizializzazione e lo concatena alla shared key. Una volta che la WEP key è

stata formata viene data in pasto all'algoritmo di cifratura RC4 per produrre una stringa pseudo-casuale della lunghezza pari ai dati da trasmettere. Una volta generata la stringa pseudo-random quest'ultima viene posta in XOR dalla scheda di rete con i dati da trasmettere: il risultato assieme al vettore di inizializzazione in chiaro sarà appeso a un header IEEE 802.11 e trasmesso verso il destinatario del messaggio.
Quando il nodo destinatario riceve il messaggio cifrato come prima cosa legge l'IV lo concatena alla shared key e calcola la psudo-random string via RC4 (data la stessa WEP key la stringa pseudo-casuale generata sarà sempre uguale). Il risultato ottenuto viene posto in XOR con i dati cifrati contenuti nel frame ottenendo così il testo in chiaro.
A partire dal 2003 questo approccio non è più considerato sicuro a causa dalle numerose falle presenti in WEP e dalla facilità con cui RC4 può essere violato.

WPA (Wi-Fi Protected Access) Una volta scoperte le falle che affliggevano WEP è iniziato lo sviluppo del protocollo IEEE 802.11i, un nuovo standard considerato pienamente sicuro. Nel frattempo viene rilasciato dalla Wi-Fi Alliance WPA (Wi-Fi Protected Access) che soddisfa molte delle linee guide di IEEE 802.11i Il WPA è caratterizzato da tre componenti principali:

- TKIP (Temporal Key Integrity Protocol), è la componente che più va a sostituire la logica di WEP risolvendo la maggior parte delle sue vulnerabilità. Una delle innovazioni più importanti è quella che ogni messaggio trasmesso viene cifrato con una chiave diversa in modo tale da non esporre la chiave principale.
  Molte funzioni di crittografia sono built-in nell'hardware di rete per tanto, non essendo possibile un aggiornamento software, per rendere compatibile a pieno WPA con il precedente hardware IEEE 802.11 il nuovo standard sfrutta alcune delle feature usate anche da WEP: in particolare anche WPA fa utilizzo di RC4. WPA inoltre utilizza un meccanismo di *key hierarchy* ovvero la chiave principale (Pairwise Master Key) viene utilizzata per generare chiavi temporanee come le sessione key, group keys etc etc. In particolare WPA sfrutta RC4 in modo diverso rispetto a WEP ovvero RC4 viene utilizzato per generare una chiave temporanea a partire dalla shared key anzichè per cifrare direttamente il messaggio. La prima chiave a essere generata è la *session key* che sarà poi utilizzata come seme per la generazione delle future *per-packet key.*
  Ciascuna per-packet key, lunga 104 bit, è generata da una funzione hash che calcola un digest a partire dall'indirizzo MAC sorgente, il vet-

tore di inizializzazione (che in WPA è stato esteso da 24 a 48 bit ed è implementato come un contatore, emphsequence counter, per evitare *replay attack*) e la session key. Una volta ottenuta la per-packet key le operazioni di cifratura e decifratura sono identiche a quelle di WEP con la sola differenza che il vettore di inizializzazione è sostituito con i 16 bit meno significativi del IV di WPA e con un dummy Byte inserito in mezzo.
TKIP risulta quindi essere un sistema di cifratura a 128 bit a chiave dinamica molto più sicuro rispetto al sistema adottato da WEP che prevedeva 24 bit dinamici con una chiave di 40 o 104 bit statica.

- MIC (Message Integrity Code)