Il roaming nelle reti mobili per le applicazioni seamless dal punto di vista del livello 2

Candidato
Matteo Raimondi

Relatori
Maurizio Bonuccelli
Antonio Cisternino

Anno Accademico 2006--2007

Indice

Introduzione

Mobility & Wireless

Per mobilità, in senso lato, si intende la qualità di essere capace di movimento o di muoversi prontamente da posto ad un altro. Questo concetto è facilmente estendibile anche ad altri protocolli (ad esempio: Ethernet, Bluetooth, WiMax, GSM, UMTS) ma in questo elaborato l'attenzione sarà rivolta ai dispositivi WLAN (802.11).

La mobilità e la tecnologia wireless non sono sinonime, ma vanno di pari passo, specialmente per i computing devices. Senza tecnologia wireless, le comunicazioni mobili sarebbero difficili, infatti permette di comunicare anche quando il dispositivo è in movimento. Soltanto negli ultimi questa tecnologia ha potuto soddisfare le esigenze del mercato totale e la diminuzione del costo, l'aumento della velocità e l'affidabilità di trasmissione hanno favorito l'integrazione della tecnologia wireless in un numero sempre più crescente di computing devices.

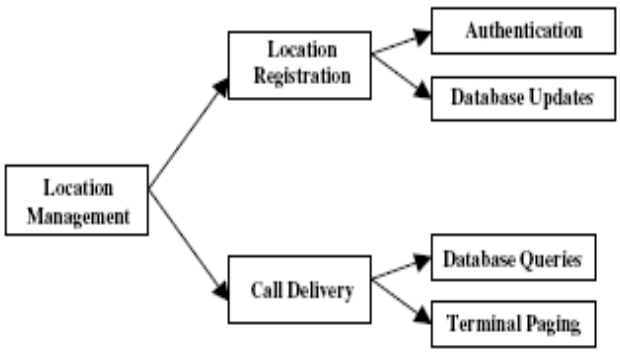
La gestione della mobilità permette alle reti di comunicazione di effettuare quanto segue:

- Scenario statico: localizzare un dispositivo mobile (STA) per trasportare data packets;
- Scenario Dinamico: mantenere le connessione con la STA che si muove verso una nuova area

Ci sono due diversi tipi di gestioni:

- Amministrazione della posizione: Come individuare una STA, rintracciare il relativo movimento e aggiornare le informazioni di posizione;
- Amministrazione del Handoff: focalizzato principalmente sul controllo del cambiamento da parte della STA di access point (AP) durante la trasmissione dati.

Le operazioni dei due componenti sono visualizzate nel seguente schema:



La mobilità interessa l'intero stack del protocollo, dal livello fisco, livello data link, ed i livelli di rete fino ai livelli applicazione e di trasporto. Un esempio include il riutilizzo delle risorse radio effettuato al livello fisico, la crittografia e la compressione dati del livello data link, il controllo di congestione al livello di trasporto ed il service discovery al livello applicazione.

Inquadrando la mobilità come cambio di punto di accesso alla rete da parte della STA, questa può essere supportata del livello di rete effettuando il cambiando di percorso dei pacchetti destinati al dispositivo mobile facendoli arrivare al nuovo punto di accesso. Gestire la mobilità al livello di rete può permettere agli strati superiori del protocollo di lavorare indipendentemente dalla natura del mezzo fisico e rendono la mobilità trasparente a applicazioni e protocolli di più alto livello quale il TCP (es: Mobile-IP).

Dietro le funzioni di base che permettono la gestione della mobilità, ci sono molti altri requisiti di prestazione e di scalabilità che dovrebbero essere presi in considerazione con molta attenzione quando si progetta o seleziona uno schema per la gestione della mobilità, tra cui i seguenti:

1. *Fast Handoff veloce*: Le operazioni di handoff dovrebbero essere effettuate abbastanza rapidamente per essere sicuri che la STA possa ricevere i pacchetti IP all'interno della nuova area in cui si è posizionata. Queste azioni devono essere eseguite in un intervallo di tempo ragionevole così da ridurre, quanto possibile, il packet delay.
2. *Seamless Handoff*: L'algoritmo di handoff dovrebbe minimizzare la perdita dei pacchetti, cercando di azzerarla o comunque portarla a valori vicino allo zero.
3. *Signaling traffic overhead*: Il carico dei dati di controllo, dovrebbe essere abbassato riportando il valore entro un range accettabile.
4. *Efficienza del routing*: I percorsi di routing tra i nodi di comunicazione alla STA dovrebbero essere ottimizzati per escludere trasferimenti o percorsi ridondanti.
5. *QoS*: Lo schema di gestione della mobilità dovrebbe sostenere l'istituzione di nuova prenotazione di QoS in modo da per trasportare una traffico di varia natura, minimizzando dell'effetto disgregativo durante questa istituzione.
6. *Fast Security*: Lo schema di mobilità dovrebbe sostenere i differenti livelli di requisiti di sicurezza quali crittografia di dati ed autenticazione dell'utente. Questo deve essere fatto limitando però il traffico ed il periodo necessario per l'esecuzione delle fasi di attuazione del meccanismo di sicurezza adottato(ad esempio, scambio chiavi).
7. *Richiesta di supporti speciali*: Un nuovo meccanismo di mobilità deve richiedere minimi cambiamenti sui componenti di rete(ad esempio: dispositivi mobili, router, mezzi di comunicazione, reti ed altri nodi di comunicazione). Questo per rendere il sistema il più possibile compatibile e meno invasivo con l'attuale implementazione della rete.

Ci sono molte tecniche distinte ma complementari, specialmente la gestione della mobilità, utili per

realizzare i relativi requisiti di scalabilità e di prestazioni elencati sopra, tra cui le seguenti:

- *Buffering e forwarding*: Inserire i pacchetti nella cache del vecchio AP durante la procedura di handoff della STA e successivamente inoltrarli al nuovo AP dopo l'esecuzione del handoff.
- *Rilevazione e previsione del movimento*: Rilevare e predire il movimento del dispositivo mobile tra differenti AP, in modo che in futuro la rete visitata sia in grado di prepararsi in anticipo ed i pacchetti possono essere trasportati durante la fase di handoff.
- *Controllo del Handoff*: Adottare meccanismi differenti per il controllo di handoff, (per esempio, controllo al livello due e/o livello tre, o handoff duro/morbido).
- *Gestione della mobilità basata sul tipo di dominio*: Dividere la mobilità in micro-mobility e macro-mobilità a seconda che il movimento effettuato dal dispositivo mobile sia intra-domain o inter-domain.

Negli ultimi anni l'interesse per la mobilità si è concentrato specialmente verso il processo di handoff legato alla tecnologia wireless, anche grazie ai seguenti fattori:

- *Integrazione con le reti LAN:* l'aumento della potenza di calcolo dispositivi mobili e la disponibilità di nuovi protocolli di comunicazione (es: UMTS), ha portato alla migrazione in questi strumenti, di servizi gestionali e di comunicazione basati sulla connessione alla rete internet (es: email, exchange). La diffusione della tecnologia wireless nei dispositivi mobili ha introdotto un principio precedentemente inattuabile: l'integrazione con le reti presenti nelle abitazioni e nelle aziende. Questa possibilità è stata spinta anche dalla possibilità di risparmio economico, introdotto dall'utilizzo di questa tecnologia, che ha permesso l'abbattimento delle spese derivanti degli abbonamenti ad internet disponibili per i dispositivi mobili.
- *Utilizzo del VoIP:* che grazie all'abbattimento dei costi che riesce a portare ed alle innumerevoli funzionalità che aggiunge rispetto alle chiamate tradizionali, l'introduzione della tecnologia wireless nei dispositivi mobili è esplosa con la diffusione di questo protocollo di comunicazione.

In questo contesto la tesi si pone l'obiettivo di analizzare le soluzioni più rappresentative presenti in letteratura allo scopo di dare una visione dettagliata dello stato della ricerca in questo ambito. Il problema sarà analizzato dal punto di vista del livello 2 della rete, per focalizzare l'attenzione sui meccanismi nativi dei protocolli di comunicazione (in particolare IEEE 802.11) in relazione alla necessità di supportare servizi di tipo seamless.

In particolare verrà evidenziato come l'elevata complessità della problematica del handoff renda difficile effettuare una gestione efficace di questo fenomeno, lavorando con soluzioni al livello 2 della rete. Saranno presentati anche i nuovi protocolli, attualmente in fase di definizione, progettati per sopperire le lacune presenti negli standard attualmente utilizzati (IEEE 802.11), inserendo al loro

interno appositi meccanismi di supporto al roaming.

L'analisi di questo fenomeno sarà svolta concentrando l'attenzione sul problema del handoff legato alla tecnologia Wireless IEEE 802.11b/g, di cui saranno evidenziati gli aspetti e limiti strutturali del mezzo trasmissivo in relazione anche all'uso di protocolli di sicurezza utilizzati nelle comunicazioni tra computing devices.

Durante il percorso realizzato saranno anche analizzate le singole fasi che caratterizzano il processo di handoff, nel tentativo di approfondire questo meccanismo per poi presentare soluzioni ed implementazioni presenti in letteratura.

Molti termini descrivono la mobilità, ma nei prossimi capitoli useremo *mobilità* e *roaming* per descrivere l'atto di muoversi fra access point (AP).

Cap.1 IEEE 802.11 Standard

Lo scopo di questo capitolo è quello di fornire una descrizione dello standard IEEE 802.11*[1]*, per presentarne i concetti base, il principio di funzionamento e le operazioni che caratterizzano il processo di roaming. La descrizione fornita di tutti gli argomenti e meccanismi compresi nello standard 802.11 non può essere esaustiva in quanto fuori dal nostro focus. Sarà comunque data una descrizione degli elementi fondamentali, in modo da comprendere le considerazioni che verranno sviluppate nei successivi capitoli.

1.1 Componenti dell'architettura dello standard IEEE 802.11

L'architettura IEEE 802.11 consiste di tutta una serie di componenti che interagiscono e provvedono a rendere invisibile la mobilità ai livelli superiori. L'elemento cardine dell'architettura è il *Basic Service Set (BSS)*.

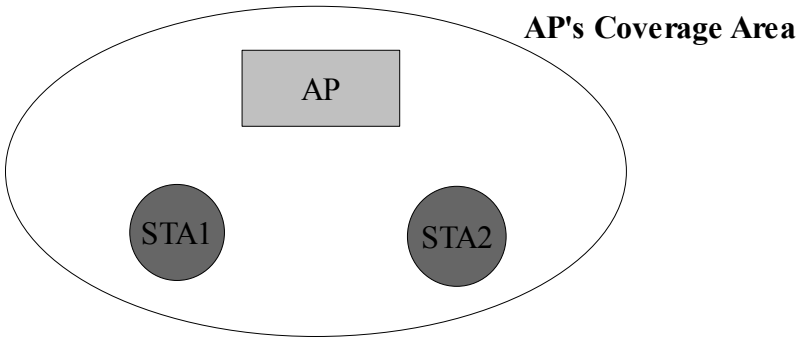


Figura 1: esempio di BSS

Una rete BSS *(figura 1)* è un gruppo di stazioni 802.11, fisse o mobili, collocate geograficamente all'interno di una cella, che possono stabilire connessioni dirette, o con l'ausilio di strutture intermedie. Nel caso di connessione diretta tra STA in cui non è presente l'access point, si parla di reti Ad-Hoc *(Indipendent Basic Service Set - IBSS)*, struttura che non sarà presa in esame.

La struttura base è composta dai seguenti elementi:

- **Station (STA):** Le stazioni sono computing devices con interfaccia wireless. Questa definizione non si limita solo ai dispositivi mobili ma anche quelli "fissi" come ad esempio i desktop;
- **Access Point (AP):** Un qualsiasi dispositivo, con le stesse funzionalità di una stazione, che permette all'utente mobile associati di collegarsi al *distribution services* tramite segnali radio. L'access point, può essere collegato fisicamente ad una rete cablata oppure via radio ad un altro AP, che comunicano tra di loro attraverso una particolare stazione conosciuta come AP.

  Le stazioni comunicano seguendo il seguente schema *(figura 2)*:

1. Station mittente *(STA1)*: invia il frame all'access point;
2. Access Point *(AP)*: instrada i frame ricevuti verso il destinatario *(STA2)*;
3. Passaggio inverso per la risposta;

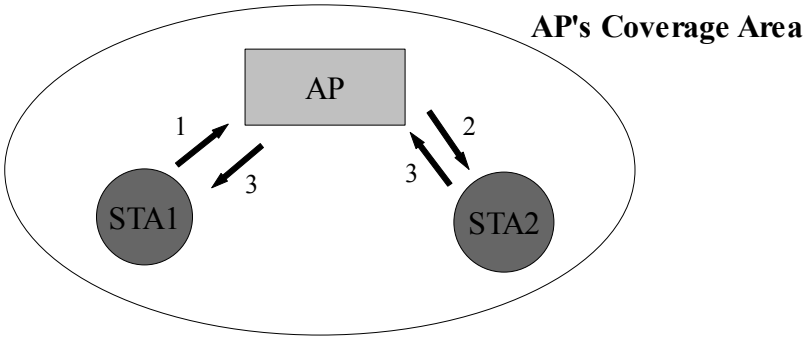


Figura 2: BSS: esempio di comunicazione tra STA1 e STA2

Extended Service Set (ESS)

Le BSS possono coprire piccole aree come uffici e case, ma non aree più ampie. Per aumentare la copertura wireless è necessario interconnettere più BSS in una *Extended Service Set (ESS)*. La ESS è creata collegando BSS tra di loro attraverso un backbone network (*figura 3*). Tutti gli access point nella ESS, in genere, sono forniti di stesso *Service Set Identifier (SSID)*, il quale rappresenta il nome della rete visualizzato dagli utenti quando effettuano la connessione.

Lo standard IEEE 802.11 non specifica nessuna particolare tecnologia per il backbone, richiede solo che fornisca una serie di servizi specifici.

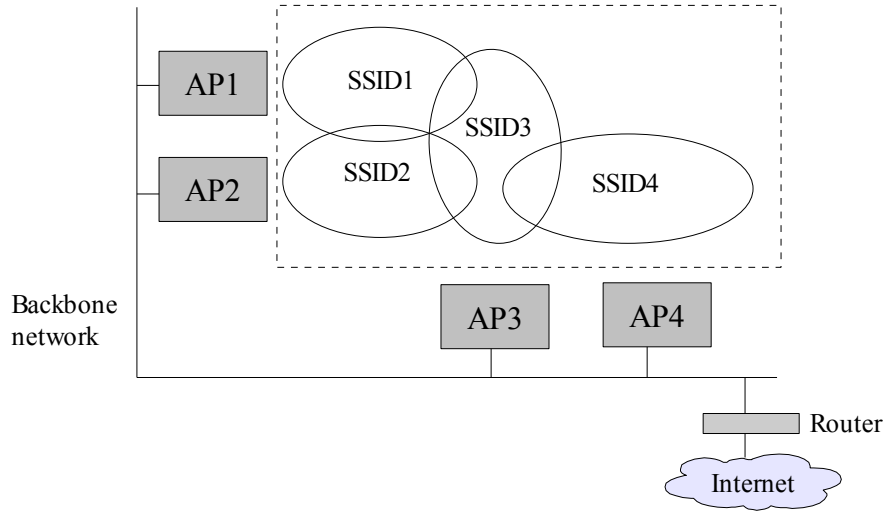


Figura.3: Esempio di Extended Service Set

Le reti ESS sono l'astrazione di più alto livello supportata dalle reti IEEE 802.11. Gli access point all'interno di una ESS cooperano per permettere che il *"mondo esterno"* possa comunicare con la stazione usando il MAC address della stazione, qualunque sia la posizione all'interno della ESS.

Nella *figura 3*, il router usa il MAC della stazione come destinazione a cui inviare i frames, ma il compito di fornire i pacchetti alla stazione mobile è affidato al AP a cui è associato in quanto è a conoscenza della posizione della stazione mobile.

Distribution System (DS)

Per la maggior parte delle reti, la distanza che può essere coperta attraverso una rete ad hoc è insufficiente e conseguentemente si rende necessaria l'introduzione di un nuovo componente che permetta sia l'ampliamento geografico della rete sia la comunicazione su una scala più vasta.

Le BSS possono esistere indipendentemente l'una dall'altra oppure venire a far parte di una più estesa forma di reti in accordo alla quale le varie BSS sono collegate attraverso un nuovo componente chiamato *Distribution System (DS)*.

Il DS è una architettura di cui nello standard IEEE 802.11 non viene specificata la natura e conseguentemente può essere di vario genere come ad esempio ethernet, wireless, token ring o FDDI. Questo componente è una sorta di backbone network responsabile della comunicazione inter BSS. La comunicazione fra le varie BSS e il DS è resa possibile dagli access point (AP). Il traffico dati si muove all'interno delle BSS e attraverso gli AP può raggiungere sia un qualunque host fisso, sia una qualunque STA appartenente ad un'altra BSS.

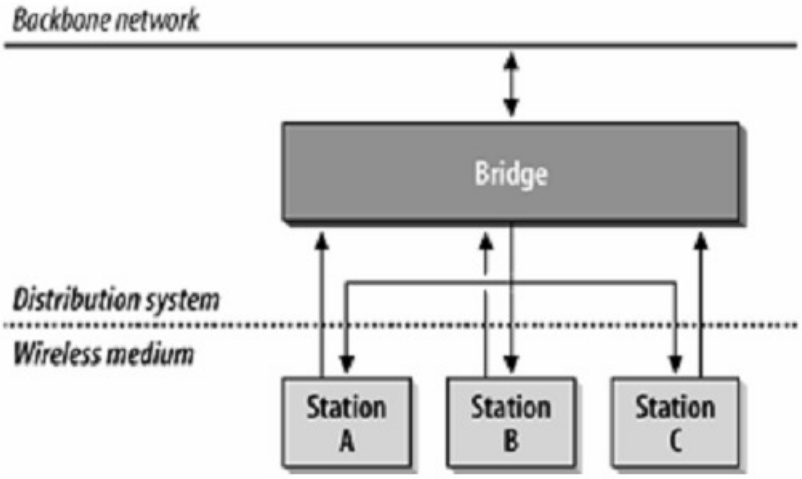


Figura 4: Relazione tra AP, distribution system, backbone network

Nella maggior parte dei prodotti commerciali il sistema di distribuzione, implementato come combinazione del *bridging engine* e del *distribution system medium*, è la backbone network usata per trasmettere frame tra gli AP . Spesso il sistema di distribuzione viene identificato direttamente con il termine backbone network. Una scelta molto diffusa è l'utilizzo della tecnologia Ethernet come backbone network.

1.2 MAC sublayer

L'architettura del MAC sublayer prevede la coesistenza di due metodi di accesso al mezzo, il *DCF (Distributed Coordination Function)* ed il *PCF (Point Coordination Function)*. Prendiamo in considerazione solo il DCF, in quanto il PCF viene utilizzato su reti infrastrutturate, che non sono argomento di questo lavoro.

Il DCF, che viene utilizzato in IEEE 802.11, è il CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*. Si tratta di un algoritmo distribuito per l'accesso al mezzo che deve essere implementato su tutte le STAs. Il CSMA prevede il *sensing* del mezzo per un tempo ben determinato *(DIFS)*, a seguito del quale, se non sono state rilevate altre stazioni mobili in trasmissione, viene fatto partire l'algoritmo di trasmissione.

Se il *sensing* del mezzo fallisce, allora la trasmissione viene schedulata nel futuro attraverso un algoritmo detto *backoff alghoritm*. L'utilizzo della funzionalità *collision avoidance* attraverso la negoziazione dei *frames RTS/CTS* permette di ridurre in alcuni casi le collisioni e di risolvere il problema del *terminale nascosto* rappresentato in *figura 5*.

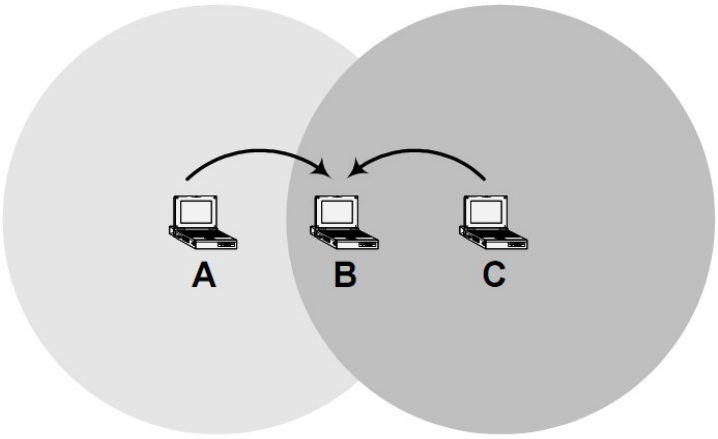


Figura 5: Problema del nodo nascosto

Distributed Coordination Function (DCF)

Il metodo di accesso al mezzo più semplice, reso disponibile dal protocollo, è un particolare tipo di *DCF* che permette di accedere al mezzo attraverso il CSMA/CA e rimandare l'accesso nel caso il mezzo sia occupato attraverso un algoritmo di backoff. Tutto il traffico dati è sottoposto al cosiddetto *positive acknowledgement*, in questo modo un frame DATA non riscontrato da un ACK frame viene ritrasmesso.

Il protocollo CSMA/CA è stato sviluppato con il preciso fine di diminuire la probabilità di collisione nel momento in cui essa è più alta. Non appena il mezzo diventa libero, dopo una trasmissione, si ha il momento in cui la probabilità di collisione è più alta. Questo fenomeno è dovuto alla presenza di più STA che ascoltano il mezzo in attesa che si liberi per poter iniziare a trasmettere. Per poter gestire questa situazione si ricorre all'algoritmo di backoff, che cerca di risolvere la contesa del mezzo. Il *sensing* del mezzo viene portato a termine attraverso due meccanismi: il primo messo a disposizione dal livello fisico, mentre il secondo di tipo virtuale. Il meccanismo di *virtual carrier sense* è implementato distribuendo informazioni circa l'uso futuro del mezzo.

Questo meccanismo viene portato a termine in due modi, il primo attraverso la negoziazione dei *frames RTS/CTS*, mentre il secondo, attraverso la lettura del campo *Duration* contenuto in qualunque Data frames in transito. Lo scambio dei frames RTS/CTS prima del traffico dati è un metodo di informazione circa l'utilizzo futuro del mezzo. Entrambi i frames contengono un campo *Duration* che permette a tutte le stazioni che lo osservano di fare una stima del tempo necessario per trasmettere il futuro DATA frames e ACK. Tutte le STA, che siano in grado di ricevere il solo RTS o il solo CTS o entrambi vengono a conoscenza in questo modo del tempo necessario alla futura trasmissione. In questo modo, anche le STA non in prossimità del trasmettitore vengono a conoscenza dell'allocazione futura del mezzo, attraverso l'analisi del frame CTS trasmesso dal ricevitore.

Va ricordato che il meccanismo RTS/CTS non può essere implementato in trasmissioni broadcast e multicast, in quanto esistono destinazioni multiple del frame RTS e potenzialmente esisterebbero più trasmettitori del frame CTS con destinazione la stessa STA. Il meccanismo RTS/CTS, inoltre, non è necessario per ogni Data frames in transito. In particolare, a causa del overhead che esso introduce, è sconsigliato per Data frames di dimensioni ridotte.

Il meccanismo di Carrier-sense

Le funzioni fisiche e virtuali di sensing del mezzo trasmissivo vengono utilizzate per valutarne lo stato. Il mezzo è considerato occupato quando una delle due funzioni lo rileva come tale, altrimenti è considerato inattivo.

Il meccanismo fisico di sensing del mezzo è messo a disposizione dal livello fisico sottostante *(PHY layer)*. I dettagli di questo meccanismo dipendono dall'implementazione del livello PHY.

Il meccanismo virtuale è implementato a livello MAC ed è incentrato sull'esistenza del NAV *(Network Allocation Vector)*. Il NAV mantiene una stima del futuro traffico sul mezzo in base al valore letto nel campo Duration appartenente ai frames RTS e CTS che vengono scambiati prima di ogni Data frames.

Il *meccanismo di carrier-sense* combina lo stato del NAV e lo stato della STA con il sensing del mezzo vero e proprio per determinare lo stato del mezzo.

MAC-Level acknowledgements

La corretta ricezione (anche dal punto di vista del FCS) di un qualunque frame necessita di essere riscontrata da parte della STA ricevente attraverso un frame di riscontro che in genere è costituito dal ACK frame. Questa tecnica è conosciuta come *positive acknowledgement*.

La mancata ricezione di un ACK indica alla STA trasmittente che è avvenuto un errore. I seguenti scenari possono essersi verificati:

1. Mancata consegna del DATA frame al ricevitore;
2. Mancata consegna del ACK frame al trasmettitore;
3. Corruzione del DATA frame ;
4. Corruzione del ACK frame.

Interframe space (IFS)

L'intervallo di tempo che separa i frames è definito come IFS (Inter Frame Space). L'utilizzo della

tecnica DCF implica la conoscenza di tre intervalli di tempo :

1. ***SIFS (Short Interframe Space):*** L'intervallo di tempo pari al SIFS viene utilizzato per i frames di ACK e CTS. Il SIFS viene considerato come l'intervallo di tempo che va dalla trasmissione dell'ultimo simbolo appartenente al frame precedente, fino alla ricezione del primo simbolo, appartenente al preambolo del frame seguente;
2. ***DIFS (DCF Interframe Space):*** L'intervallo di DIFS viene utilizzato dalle STAs che operano in accordo al DCF per trasmettere frames sia di tipo DATA sia di tipo management. Una STA che utilizza DCF è autorizzata a trasmettere solo dopo avere rilevato il mezzo libero per un tempo pari al DIFS e sia spirato il tempo di backoff;
3. ***EIFS (Extended Interframe Space):*** L'intervallo EIFS viene utilizzato nell'ambito di DCF quando il livello PHY di una STA comunica al livello MAC che si è rilevato un errore da parte del controllo FCS. La ricezione di un frame con il corretto FCS durante il tempo di EIFS, permette alla STA di riallinearsi allo stato attuale del mezzo con conseguente terminazione dell'intervallo di EIFS e proseguimento con il normale metodo di accesso al mezzo ovvero DIFS e se necessario backoff.

La figura 6 mostra l'utilizzo dei vari intervalli temporali.

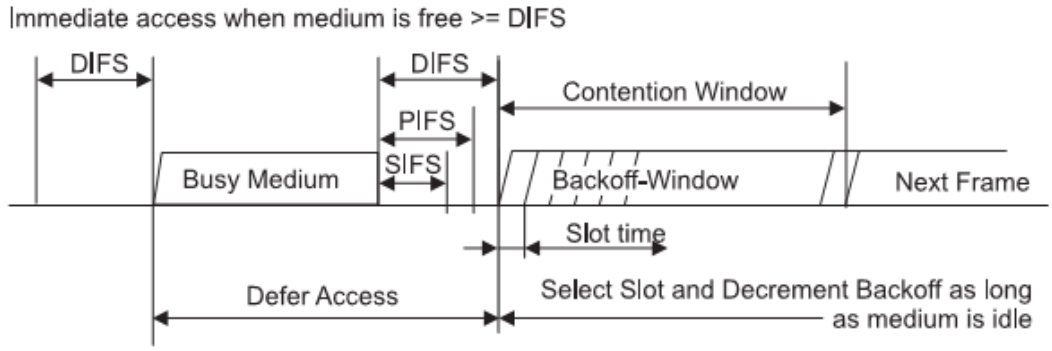


Figura 6: intervalli temporali DCF

Random backoff time

Una STA che desidera trasferire un frame di tipo DATA o management invoca il meccanismo di carrier sense per determinare lo stato del mezzo. Se il mezzo risulta occupato, la STA continua il controllo del mezzo ininterrottamente fino al momento in cui il mezzo non risulta libero per un periodo di tempo pari al DIFS. Se l'ultimo frame è stato ricevuto corrotto, allora il periodo di tempo necessario a considerare il mezzo libero risulta pari a l'EIFS. Quando il mezzo viene considerato idle (ovvero dopo un tempo DIFS o EIFS in cui non si sono rilevate trasmissioni), la STA genera un tempo pseudocasuale di backoff che posticipa ulteriormente il tempo di trasmissione.

$$BackoffTime = Random() * aSlotTime \qquad [eq.1]$$

dove :

- *Random()* : intero pseudocasuale estratto da una distribuzione uniforme su un intervallo pari a [0,CW], dove CW (Contention Window) è un intero il cui valore è compreso nell'intervallo $aCWmin \leq CW \leq aCWmax$;
- *aSlotTime* : Dipendente dal livello PHY implementato. Il parametro CW o Contention Window assume inizialmente il valore pari a aCWmin. La CW assume il valore successivo in una serie ben definita tutte le volte che è necessaria una ritrasmissione di un frame, fino ad assumere il valore massimo; pari a aCWmax. Una volta raggiunto il valore precedente, la CW rimane tale fino a che un nuovo evento non la reimposta al valore aCWmin. Questo funzionamento garantisce la stabilit`a del protocollo in condizioni di canale molto sfavorevoli.

  La figura 7 mostra l'andamento della CW a seguito di ritrasmissioni continuate.

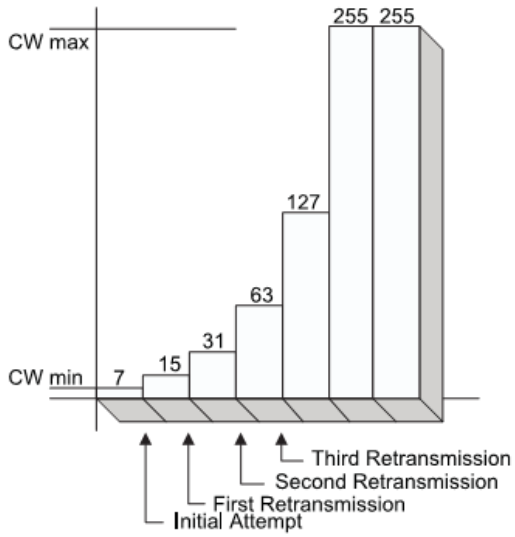


Figura 7: andamento della CW in finzione di ritrasmissioni

La sequenza di valori assunti dalla CW è pari alla potenza di 2 meno 1 partendo da aCWmin fino ad aCWmax.

1.2.1 DCF access procedure

Basic access

Il metodo base di accesso è quello descritto nelle sezioni precedenti e lo si può vedere rappresentato nella segente figura:

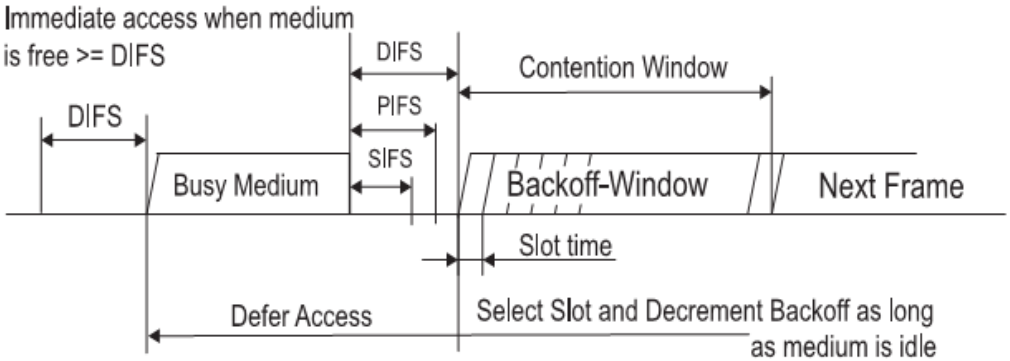


Figura 8: metodo base di accesso

La procedura di base per l'accesso al mezzo prevede la trasmissione di un frame non appena il mezzo venga osservato inattivo per un tempo pari al DIFS o al EIFS. Se il mezzo è valutato occupato viene invocato l'algoritmo di backoff. In genere la procedura è diversa per diminuire ulteriormente la contesa del mezzo come viene spiegato nelle sezioni successive.

Backoff procedure

La procedura di backoff viene invocata da una stazione mobile dopo che il mezzo è stato rilevato occupato oppure si è verificato un errore nel trasferimento del frame a causa del mancato riscontro (ACK frame).

La figura 8 mostra la procedura di backoff in presenza di cinque STA.

Per iniziare una procedura di backoff, la STA setta un timer *(backoff timer)* al valore calcolabile

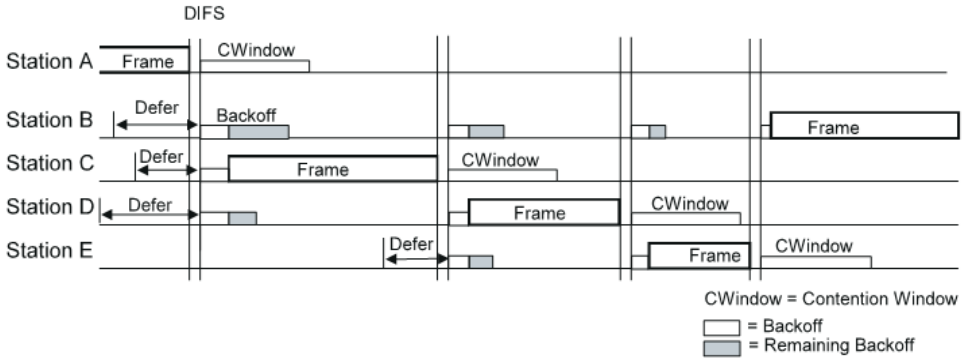


Figura 9: backoff procedure

attraverso *l'equazione (eq.1)* pari alla *backoff window.* La backoff window deve iniziare a trascorrere dopo un tempo di DIFS o un EIFS durante i quali il mezzo deve essere rilevato inattivo.

Durante la backoff window una STA osserva il mezzo per determinare se vi è attività in esso. La backoff window viene decrementata di uno slot per ogni backoff slot in cui il mezzo viene rilevato inattivo.

Se durante la backoff window, ad un dato istante, il mezzo viene rilevato occupato, la procedura di backoff viene sospesa. Il mezzo dovrà essere rilevato inattivo per un tempo pari al DIFS o al EIFS prima che la procedura di backoff abbia di nuovo inizio.

La procedura di backoff deve essere invocata alla fine di ogni trasmissione anche se non vi sono ulteriori trasmissioni in coda. Nell'ipotesi in cui la trasmissione sia andata a buon fine con la ricezione di un frame di ACK allora la procedura inizia al termine della ricezione dell'ACK. Se la trasmissione non è andata a buon fine e l'ACK non viene ricevuto, la procedura di backoff ha inizio allo spirare del timer che il trasmettitore ha associato al frame di ACK. Questo scenario garantisce che ogni frame venga separato da almeno una backoff window.

Le stazioni si sincronizzano ascoltando il mezzo per un tempo pari al DIFS, invocano la procedura di backoff, che determinerà la prossima STA a trasmettere. La STA che trasmetterà sarà quella che ha schedulato un tempo minore delle altre e iniziando a trasmettere annullerà le procedure di backoff delle altre STA che si disporranno in ascolto sul mezzo.

Procedure di recupero Il recupero da errore è responsabilità della STA che ha trasmesso il frame. Il recupero da errore viene effettuato attraverso la ritrasmissione del frame di cui non è avvenuto il riscontro (ACK frame). Le ritrasmissioni dello stesso frame avvengono fino a che il frame non viene riscontrato oppure fino al raggiungimento del numero massimo delle ritrasmissioni.

Il numero di ritrasmissioni associate ad un frame viene salvato in due variabili in funzione della politica di accesso al mezzo (CSMA o CSMA/CA). Viene incrementato il short retry count se il frame da trasmettere ha dimensione inferiore al dot11 RTSThreshold, mentre viene incrementato il long retry count se la dimensione del frame è tale da attivare la negoziazione dei frame RTS/CTS. In entrambi i casi il frame viene ritrasmesso per un numero di volte comunque inferiore al numero massimo di ritrasmissioni possibili e successivamente viene scartato.

Per la gestione del NAV*(Network Allocation Vector),* le stazioni mobili che ricevono un frame valido possono aggiornare il loro valore di NAV con l'informazione prelevata dal campo Duration del frame, nell'ipotesi in cui il nuovo NAV sia maggiore del vecchio oppure il frame non sia indirizzato proprio alla stazione ricevente.

La figura 10 mostra la gestione del NAV da parte di stazioni mobili che ascoltano il canale utilizzato durante una trasmissione.

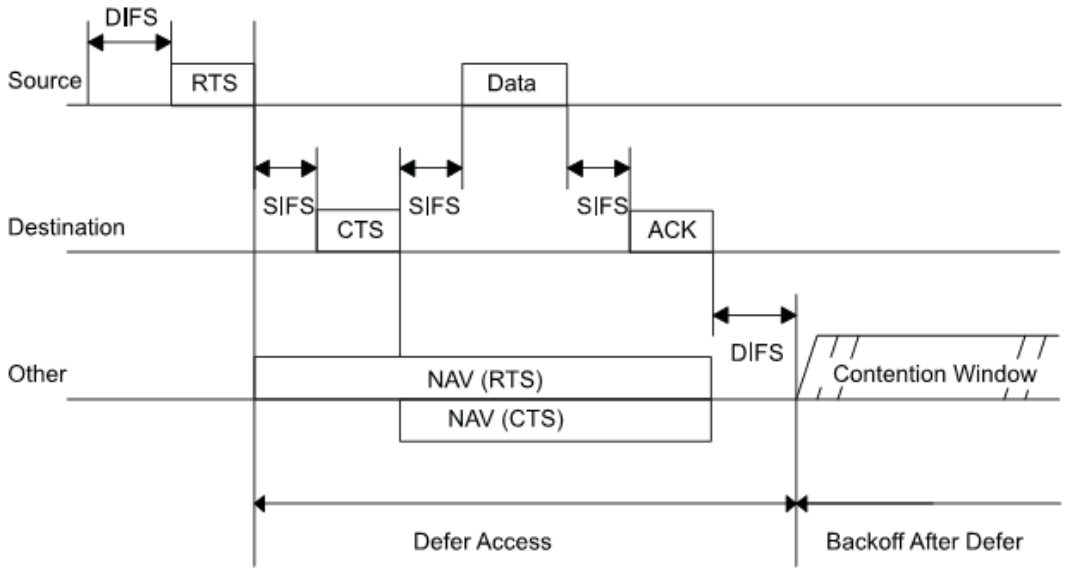


Figura 10: RTS/CTS/data/ACK and NAV setting

La figura mostra l'aggiornamento del NAV per le stazioni mobili che possono ricevere il solo RTS oppure per le STA che possono ricevere il solo CTS. Una STA che riceve un frame RTS a lei indirizzato deve rispondere con un frame CTS dopo un periodo di SIFS solo e soltanto se il suo NAV indica un mezzo libero. Se il NAV sulla STA ricevente indica la presenza di un mezzo occupato allora la STA non trasmette il CTS. Il campo RA del CTS viene copiato dal campo TA del frame RTS, mentre il campo DURATION del CTS viene calcolato dal DURATION del RTS sottraendo un SIFS e il tempo necessario a trasmettere il CTS.

La STA che trasmette il frame RTS schedula un timer CTS Timeout interval per l'attesa del CTS. La STA conclude che la trasmissione del frame RTS è fallita se il CTS Timeout interval spira prima della ricezione del frame CTS. Qualunque altro frame ricevuto durante tale intervallo fa fallire la procedura di RTS e invocare il backoff.

Procedura di ACK

Una STA genera un frame di ACK tutte le volte che riceve un frame unicast, a lei indirizzato, che necessita di riscontro. La trasmissione del frame di ACK inizia dopo un tempo di SIFS successivo alla ricezione del frame da riscontrare indipendentemente dallo stato del mezzo.

La STA trasmittente attende un tempo pari all'ACK Timeout prima di concludere che la trasmissione è fallita. Se il timer spira prima dell'arrivo del frame di ACK allora la STA invoca la procedura di backoff. L'arrivo di un qualunque altro frame all'interno del tempo di attesa fa fallire la trasmissione e invoca la procedura di backoff.

1.3 Logical service interfaces

Lo standard IEEE 802.11 non fa riferimento ai dettagli implementativi del DS in quanto si prescinde dalla tecnologia di implementazione, si fa invece riferimento ai servizi che deve offrire.

Ogni servizio è supportato da uno o più tipi di frame che devono essere fatti transitare per portare a

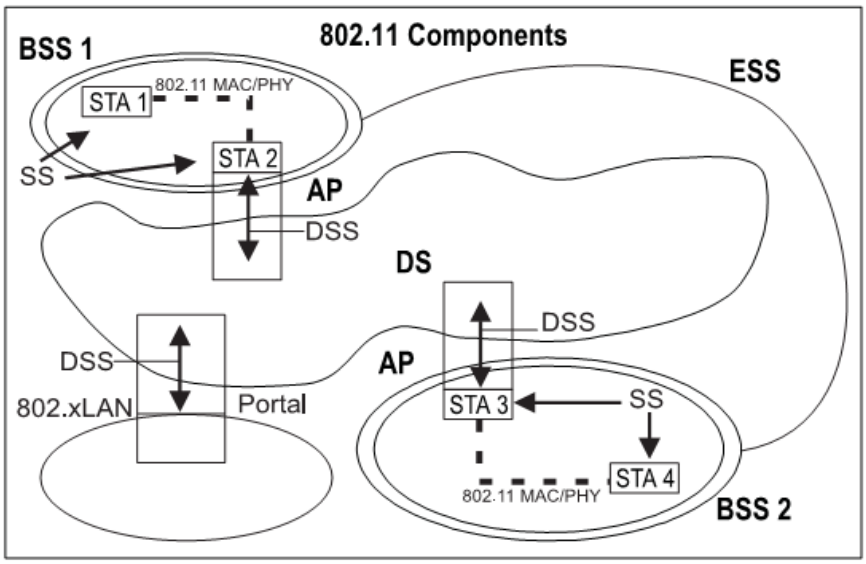


Figura 11: IEEE 802.11 architettura completa

buon fine l'adempimento del stesso. Esistono due categorie di servizi, *station services* e *distribution system services*, entrambe usate dal livello MAC, implementate la prima sulle STA mentre la seconda sui DS. La *figura 11* riassume l'architettura IEEE 802.11 considerando i vari servizi offerti dalle varie componenti.

Lo standard*[1]* definisce anche il concetto di *Portal (figura 11)*. Un Portal è un dispositivo che permette l'interconnessione tra una rete LAN 802.11 e un'altra rete 802. Anche se lo standard non lo richiede espressamente, la maggior parte delle installazioni riuniscono l'access point e il Portal in un'unica entità fisica.

SS : Station Services (SS)

Sono i servizi presenti su ciascuna STA, sia essa un dispositivo mobile o un AP:

1. Authentication;

2. Deauthentication;

3. Privacy;

4. MSDU Delivery.

DSS : Distribution System Services

Sono i servizi offerti dai soli AP per consentire l'accesso al DS:

1. Association;

2. Disassociation;

3. Distribution;

4. Integration;

5. Reassociation.

1.4 Frame Format

Analizziamo ora gli elementi base che compongono tutte le operazioni che caratterizzano lo standard IEEE 802.11, i frames.

Ogni frame è caratterizzato da tre componenti:

1. *MAC Header:* Intestazione del frame.
2. *Frame Body:* il corpo del frame che trasporta i dati veri e propri.
3. *FCS:* Frame Check Sequence ovvero un CRC cyclic redundancy code a 32 bit

Lo standard IEEE 802.11 prevede tre tipi fondamentali di frames:

- *Data Frames:* che sono usati per la trasmissione dei dati;
- *Control Frames:* che sono usati per il controllo dell'accesso al mezzo (esempio RTS, CTS e ACK);
- *Menagement Frames:* ovvero frames che vengono trasmessi allo stesso modo dei Data Frames per lo scambio di informazioni di controllo ma non sono passati ai livelli superiori dello stack protocollare (esempio i Beacon Frames).

Ciascun tipo di frame è poi suddiviso in differenti sottotipi, in base alla specifica funzione. I frames sono composti dei seguenti elementi:

Figura 12: Struttura del frame

Campo Frame Control

Il campo Frame Control, di cui possiamo vedere la struttura nella *figura 13*

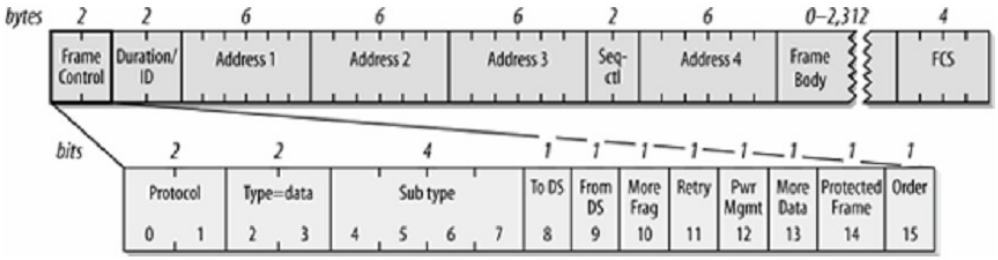


Figura 13: Struttura del campo di controllo del Frame

contiene le seguenti informazioni:

- *Protocol Version*: Questo campo consiste di 2 bits che sono invarianti sia per dimensione sia per posizionamento nelle successive versioni dello standard 802.11e saranno utilizzati per riconoscere le future versioni quando queste saranno disponibili. Nella versione attualmente disponibile dello standard questo valore è fissato a 0;
- *Type e Subtype*: Questi 6 bits definiscono il tipo e il sottotipo del frame nel modo descritto nella *tabella* 1 tratta da *[2]*.

Subtype value	Subtype name
Management frames (type=00)[a]	
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action (for spectrum management with 802.11h, also for QoS)
Control frames (type=01)[b]	
1000	Block Acknowledgment Request (QoS)
1001	Block Acknowledgment (QoS)
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack
Data frames (type=10)	
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll

0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted)
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	CF-Ack+CF-Poll (no data transmitted)
1000	QoS Data[c]
1001	QoS Data + CF-Ack[c]
1010	QoS Data + CF-Poll[c]
1011	QoS Data + CF-Ack + CF-Poll[c]
1100	QoS Null (no data transmitted)[c]
1101	QoS CF-Ack (no data transmitted)[c]
1110	QoS CF-Poll (no data transmitted)[c]
1111	QoS CF-Ack+CF-Poll (no data transmitted)[c]
(Frame type 11 is reserved)	
[a] *Management subtypes 0110-0111 and 1110-1111 are reserved and not currently used.*	
[b] *Control subtypes 0000-0111 are reserved and not currently used.*	
[c] *Proposed by the 802.11e task group, but not yet standardized. Note that these frames all have a leading one, which has caused some to refer to the first bit as the QoS bit.*	

Tabella 1: Type e Subtype Frame Control

- *ToDS e FromDS*: Il bit *ToDS* è posto al valore 1 quando il frame è indirizzato al AP allo scopo di essere trasferito ad una stazione collegata al Distribution System, compresi i casi in cui la stazione di destinazione è nella stessa BSS e AP funziona da semplice ripetitore per il frame. In tutti gli altri frame questo bit è posto al valore zero. Il bit *FromDS*, invece, è posto al valore uno quando il frame è ricevuto dal Distribution System;
- *More Fragments*: Questo bit è posto al valore uno quando più frammenti appartenenti allo stesso frame seguono il frammento corrente;
- *Retry*: Questo bit indica che il frammento corrente è la ritrasmissione di un frammento precedentemente trasmesso. Questo è utilizzato per riconoscere le trasmissioni duplicate dei

frame che si possono verificare quando un pacchetto di Acknowledgment va perso;

- *Power Management*: Questo bit serve per cambiare lo stato da Power Save ad Active e viceversa;
- *More Data*: Questo bit è utilizzato per il Power Management ma viene sfruttato anche dall'access point per indicare che ci sono molti frame memorizzati e indirizzati a questa stazione. La stazione può decidere di utilizzare questa informazione per continuare il Polling o anche per commutare il modo di funzionamento in Active;
- *Protection Frame bit:* Se il frame è protetto da un protocollo di sicurezza a livello 2 della pila iso/osi, il bit è settato a uno (precedentemente chiamato WEP bit);
- *Order*: Questo bit indica che il frame è stato inviato con Stricly-Order service class. Questa classe di funzionamento è definita per utenti che non possono accettare cambi di ordinamento tra frame Unicast e frames Multicast (l'ordinamento dei frame Unicast a uno specifico indirizzo è sempre mantenuto).

Duration/ID

Questo campo ha due significati diversi in base al tipo di frame:

- In messaggi di Power Save Poll questo campo rappresenta l'identificativo della stazione;
- In tutti gli altri frame questo campo rappresenta il valore di durata utilizzato per il calcolo del NAV.

I campi Indirizzo

Un frame può contenere al più 4 indirizzi come definito dai campi ToDS e FromDS definiti nel campo Control:

- *Address-1*: è sempre l'indirizzo del destinatario. Se ToDS è a uno questo è l'indirizzo del AP, mentre se è a 0 questo rappresenta l'indirizzo del destinatario finale;
- *Address-2*: è sempre l'indirizzo di colui che effettua la trasmissione. Se FronDS è a uno questo è l'indirizzo dell'AP mentre se è a 0 è l'indirizzo della stazione;
- *Address-3*: in molti casi è l'indirizzo mancante. Se un frame ha il campo FromDS al valore uno Address-3 rappresenta l'indirizzo della vera sorgente del frame. Se ToDS invece a uno il valore in questo campo identifica l'indirizzo di destinazione;
- *Address-4*: è usato in casi particolari dove è presente un Distribution System completamente wireless e il frame è stato trasmesso da un AP ad un altro. In questo caso sia ToDS sia FromDS sono a uno così sia l'indirizzo di destinazione sia l'indirizzo della vera sorgente del frame sono mancanti.

La seguente tabella 2 riassume l'utilizzo dei vari indirizzi in funzione del valore di ToDS e FromDS.

Function	ToDS	FromDS	Address1	Address2	Address3	Address4
IBSS	0	0	DA	SA	BSSID	N/A
To AP (infra)	0	1	DA	BSSID	SA	N/A
From AP (infra.)	1	0	BSSID	SA	DA	N/A
WDS (bridge)	1	1	RA	TA	SA	SA

Tabella 2: Possibili valori dei campi Address

Sequence Control

Questo campo è utilizzato per rappresentare l'ordine di differenti frammenti che appartengono ad uno stesso frame e di controllare la duplicazione dei pacchetti. E' in realtà costituito da due sottocampi, Fragment Number e Sequence Number, che definiscono il frame e il numero del frammento nel frame.

CRC

Il CRC è un campo di 32 bit contenete un Cyclic Redundancy Check (CRC) a 32 bit.

1.5 Management Operations

In questa sezione saranno presentate le principali *management operations* che caratterizzano lo standard IEEE 802.11. Dopo un descrizione accurata del loro funzionamento saranno effettuate considerazioni, attraverso una macchina a stati, sulle relazioni tra i servizi.

1.5.1 Management Architecture

Concettualmente, l'architettura di gestione dello standard IEEE 802.11 è costituita di tre componenti: the MAC Layer Management Entity (MLME), un Physical-Layer Management Entity (PLME) e un System Management Entity (SME). La relazione tra le differenti entità di management e le relative parti dello standard IEEE 802.11*[1]* sono visualizzate nella seguente figura:

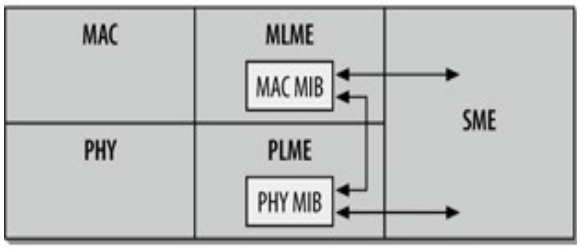


Figura 14: Relazione tra le differenti entità di management e le relative parti del 802.11

Lo standard IEEE 802.11 non specifica formalmente il SME ma definisce il suo ruolo: mezzo tramite il quale gli utenti ed i device drivers interagiscono con l'interfaccia della rete 802.11 la quale fornisce informazioni circa il suo stato. Sia il MAC che il PHY layer hanno accesso al Management Information Base (MIB). Il MIB ha oggetti che possono essere interrogati per ottenere le informazioni sullo stato, così come gli oggetti che possono effettuare determinate azioni.

Ci sono tre interfacce definite fra i componenti dell'amministrazione. L'entità dell'amministrazione della stazione può alterare sia il MAC che PHY MIB attraverso le interfacce di servizio di PLME e di MLME. Ulteriormente, i cambiamenti al MAC possono richiedere corrispondenti cambiamenti nel PHY, così che un'interfaccia supplementare fra il MLME e il PLME permette che il MAC faccia i cambiamenti al PHY.

1.5.2 Management Frames

Il frame delle Management Operation è composto dai seguenti campi:

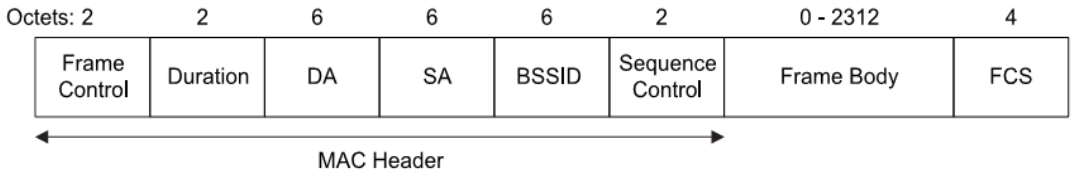


Figura 15: Campi management frame

Un dispositivo mobile (STA) usa il contenuto del campo Address1 per migliorare l'address matching per ricevere le decisioni. Nel caso in cui in campo Address1 contiene un gruppo di indirizzi ed il frame type è diverso dal Beacon, il campo BSSID è utilizzato per essere sicuri che il messaggi di broadcast o multicast siano originati nella stessa BSS.

Il campo address per i management frames non varia a seconda del sul sottotipo.

Il valore BSSID è determinato come segue:

- Se la stazione è in un AP ed è associata con un AP, il BSSID è l'indirizzo attualmente in uso dalla STA all'interno della zona di copertura dell'AP;
- Se la stazione è membro di una rete IBSS, il BSSID coincide con quello della rete IBSS;
- Nel caso di un Probe Request frame, il valore del BSSID o è uno specifico, o è uno di broadcast.

1.5.3 Management Operations: Tipologie

Lo standard 802.11 prevede le seguenti management operations:

a. Sincronizzazione

Come altre tecnologie di rete senza fili, 802.11 dipende molto dalla distribuzione delle informazioni di

sincronizzazione a tutti i nodi. È particolarmente importante nelle reti che usano latenza di trasmissione di frequency-hopping perché tutte le stazioni devono cambiare i canali delle frequenze in modo coordinato. Oltre che la sincronizzazione locale della stazione, ogni stazione in una BSS effettua una copia della funzione di sincronizzazione (TSF), che è un temporizzatore locale sincronizzato con il TSF di ogni altra stazione nell'area di servizio di base. I Beacom Frames sono usati per annunciare periodicamente il valore del TSF alle altre stazioni (STA) presenti nella BSS, e sono caratterizzati dai seguenti valori del *frame body*:

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

Tabella 3: Tipologie di frame body

In una rete infrastruttura, la AP sarà il timing master e dovrà gestire il TSF in modo performante. In caso di reti con AP multipli, ogni AP inizializza il proprio TSF timer indipendentemente dagli altri, in modo da minimizzare il costo della sincronizzazione. La AP trasmetterà periodicamente i *Beacon Frames* che contengono una copia del relativo TSF timer per sincronizzare le STA in una BSS. Una STA in ricezione accetterà sempre le informazioni di sincronizzazione trasmessi dal AP che gestisce la BSS. Se il TSF timer della stazione mobile è differente dal timestamp contenuto del *Beacon Frame* ricevuto, la STA in ricezione regolerà il relativo timer locale al valore ricevuto. I *Beacon Frames* saranno generati per essere trasmessi dalla AP ogni unità di tempo dal nome *BeaconPeriod*.

Le stazioni mobili useranno le informazioni dall'elemento dell'insieme di parametro dei CF di tutti i beacon frames per aggiornare il loro NAV come specificato precedentemente. Le STA in una rete BSS infrastruttura useranno anche altre informazioni contenute nei beacon frames ricevuti, se il campo di BSSID è attualmente uguale al MAC address in uso dalla STA contenuta nella BSS della AP a cui è collegato.

Invece, le stazioni mobili in un IBSS useranno altre informazioni contenute nel beacon frame ricevuti per cui il sottocampo di IBSS è settato a uno ed il contenuto del campo SSID è uguale al SSID del IBSS.

b. Scanning

Un dispositivo mobile può funzionare due modalità: *Scanning Passivo* e *Scannig Attivo* secondo il valore corrente del parametro di ScanMode. I *Beacon Frames* permettono ad una stazione di scoprire tutti le informazioni utili riguardanti la BSS cominciare le comunicazioni. Analizziamo ora le due diverse tipologie di scanning:

- **Scanning Passivo**

  Questo tipo di scanning è adottato per diminuire il consumo di energia del dispositivo. Infatti la STA non farà altro che controllare tutti i canali del dispositivo wireless in attesa di ricezione di un Beacon Frame.

  Una STA per controllare se fa parte di una determinata ESS, usando lo *scanning passivo*, ricercherà i beacon frames che contengono SSID di quel ESS, restituendo tutte le strutture corrispondenti nelle quali sarà a che contenuta l'informazione sulla provenienza del Beacon Frame da un'infrastruttura BSS o IBSS.

  Ad esempio in una situazione tipica, come quella presentata nella seguente figura, la stazione

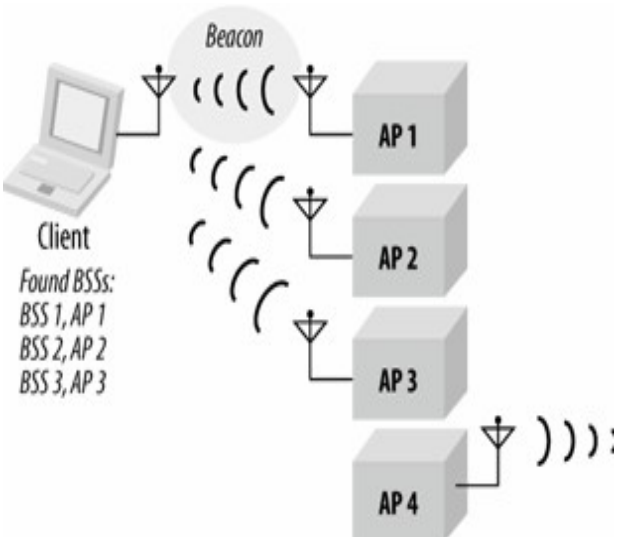


Figura 16: Esempio di risposta beacon frame

  mobile usa lo *scanning passivo* per trovare BSS nella relativa zona e riceve solo *Beacon Frame* dai primi tre AP, di cui ne segnala la presenza (il quarto AP, non lo segnala in quanto non riceve frame provenienti da lui).

- **Scanning Attivo**

  La procedura di *scanning attivo*, la STA trasmetterà un *Probe Request frame* in ogni canale del mezzo trasmissivo, per sollecitare la risposta di una determinata rete (presente SSID della rete richiesta), di cui segue il contenuto del *frame body:*

Order	Information
1	SSID
2	Supported rates

Tabella 4: probe request frame body

Una scansione attiva tenta di trovare la rete. Le stazioni che usando lo scanning attivo eseguono la seguente procedura per ogni canale:

1. Passare da un canale ad un altro canale ed aspettare un'indicazione di ricezione di frame o che il *ProbeDelay* scada. Se un frame è ricevuto significa che quel canale è in uso e può essere sondato. Il *ProbeDelay* impedisce un canale vuoto blocchi l'intera procedura; la stazione non aspetterà all'infinito di ricevere frames.
2. Accedere al mezzo seguendo la procedura di base di accesso di DCF e trasmettere un *Probe Request* frame in broadcast.
3. Aspettare per un tempo pari al valore di MinChannelTime*[Par.3.1]*:
   - Se il mezzo non fosse mai occupato, non c'è rete. Spostarsi sul canale successivo;
   - Se il mezzo fosse occupato durante l'intervallo di MinChannelTime, attendere fino al tempo massimo, MaxChannelTime e ricevere *Probe Response frame.*

Una stazione in ogni BSS è responsabile della risposta alle richieste. Nelle reti infrastrutturate, gli AP trasmettono Beacon Frame ed inoltre sono responsabili della risposta alle stazioni mobili che cercano la rete a cui collegarsi. I *Probe Response frames* sono unicast e sono quindi conforme al requisito di riconoscimento positivo del MAC, questo affinché in caso di risposte multiple siamo trasmesse come conseguenza di uno specifico *Probe Request frame*.

Lo scopo della procedura di scanning è trovare ogni area BSS a cui la stazione mobile può accedere, per questo i *Probe Request* frame sono inviati in broadcast.

Nella seguente figura è rappresentata la fase di scanning attivo ed il relativo diagramma temporale delle operazioni presentate precedentemente:

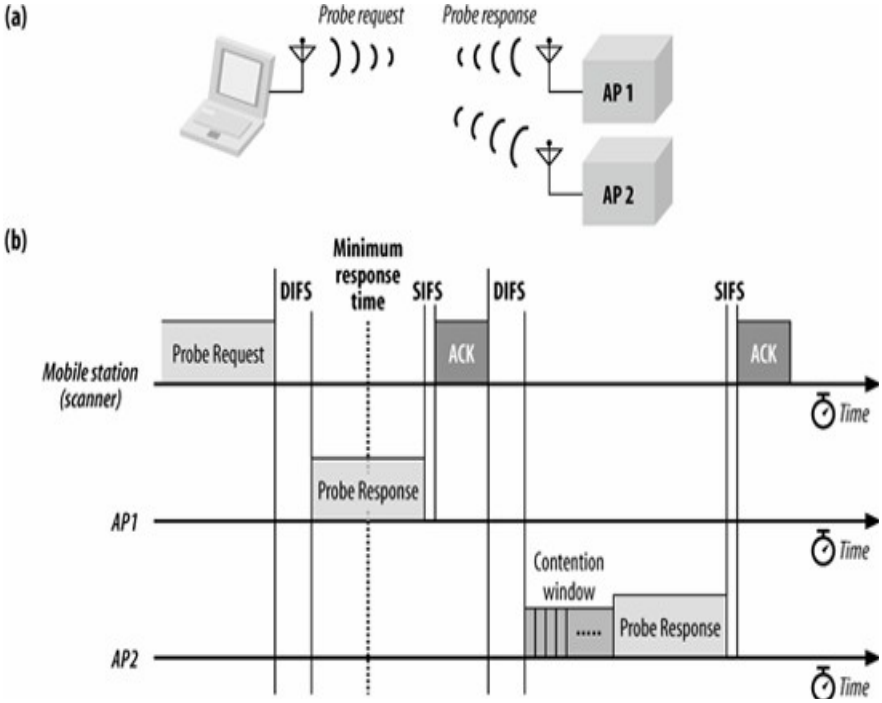


Figura 17: Scanning attivo ed il relativo diagramma temporale

Le informazioni trasportare da un *Probe Response frame*, come risultato della fase di scanning sono indicate nella seguente tabella:

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Probe Response frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Probe Response frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Probe Response frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Probe Response frames generated by STAs in an IBSS.

Tabella 5: Probe Response frame, risultato della fase di scanning

c. Joining

Dopo la ricezione dei valori, una stazione può scegliere di unirsi ad una BSS. La fase di Joining è un precursore all'associazione. Non permette l'accesso di rete: infatti, prima che questo possa accadere,

sono richieste sia l'autenticazione che l'associazione. Scegliere a quale BSS unirsi è una decisione che può coinvolgere l'intervento dell'utente. Le BSS che fanno parte dei lo stesso ESS è permesso prendere la decisione in tutto il senso che scelgono.

Generalmente i parametri usati per effettuare la decisione sono:

- potenza del segnale;
- livello di energia.

Il processo di Joining non è percepibile all'esterno in quanto è un'operazione interna al nodo.

d. Autenticazione

IEEE 802.11 definisce due sottotipi di servizio di autenticazione: *Open System e Shared Key* . Il sottotipo vine indicato nel corpo dei frame al momento della richiesta di autenticazione. Tutti i management frame utilizzati per l'autenticazione devono essere messaggi in unicast poiché l'autenticazione è realizzata fra due stazioni.

Le stazioni mobili sono chiamate ad indicare la tipologia tecnica di autenticazione usata nei messaggi di richiesta di annessione ad una rete, mentre gli AP non sono costretti ad autenticarsi a loro volta agli STA. Lo standard IEEE 802.11, prevede quindi una posizione di privilegio per gli AP, probabilmente in quanto fanno parte di una rete infrastruttura.

I frame di tipo Deautentication sono di segnalazione e possono quindi essere trasmessi ad gruppo di indirizzi, di cui è riportato il frame body:

Order	Information
1	Reason code

Tabella 6: Deauthentication, frame body

L'autenticazione a cui si farà riferimento è quella usata fra le stazioni mobili (STA) e l'access point in una infrastruttura BSS. L'autenticazione può essere usata fra due STA in un IBSS.

Il frame body dei management frame utilizzati per la fase di autenticazione sono i seguenti:

Order	Information	Notes
1	Authentication algorithm number	
2	Authentication transaction sequence number	
3	Status code	The status code information is reserved and set to 0 in certain Authentication frames as defined in Table 14.
4	Challenge text	The challenge text information is only present in certain Authentication frames as defined in Table 14.

Tabella 7: Authentication, frame body

Autenticazione di tipo "Open System"

L'autenticazione di tipo *Open System* è il metodo di default indicato nello standard IEEE 802.11. Questo metodo è più corretto definirlo un sistema di *"non autenticazione"*. Infatti, l'identità del client che si vuole aggregare alla rete non viene controllata in nessun modo. Qualsiasi STA che chiede l'autenticazione con questa procedura può essere autenticato se AP è regolato all'autenticazione di tipo *Open System*.

Nello standard IEEE 802.11*[1]*, l'identità della stazione mobile è il relativo MAC address. Come le reti Ethernet, gli indirizzi del MAC devono essere unici all'interno della rete. L'access point usa l'indirizzo del mittente dei frame come suo elemento identificativo. Nessun altro campo all'interno della struttura è usato per tale scopo.

L'autenticazione del sistema aperto coinvolge una sequenza in due fasi di transazione, come evidenziato nella figura 19 tratta da *[2]*:

- Il primo passo della sequenza è la richiesta di autenticazione.
- Il secondo passo nella sequenza è il risultato di autenticazione. Se il risultato è positivo la stazione mobile e l'access point saranno autenticate reciprocamente.

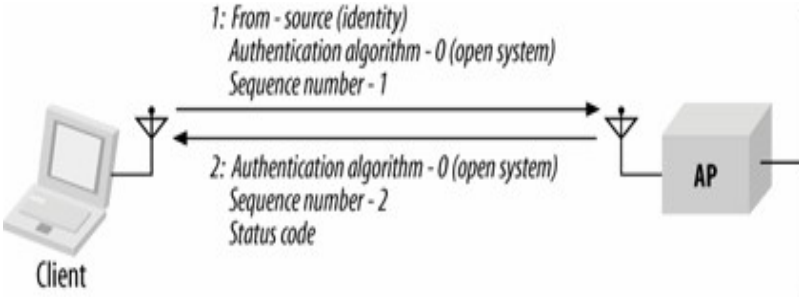


Figura 18: Open System, sequenza messaggi

Analizziamo nel dettaglio le fasi che compongono questo metodo di autenticazione mettendone in risalto i frame adoperati nelle comunicazioni partendo dal primo, di cui è indicato qui di seguito il contenuto:

- Message type: Management;
- Message subtype: Authentication;
- Information items:
  - Authentication Algorithm Identification = "Open System", value "0";
  - Station Identity Assertion (in SA field of header);
  - Authentication transaction sequence number = 1;

- Authentication algorithm dependent information (none);

- Direction of message: From STA to AP.

Come si nota l'identificativo del metodo di autenticazione è regolato a zero per indicare che il metodo in uso è di tipo Open System. Per indicare la sequenza dei messaggi è inserito il numero progressivo di transazione a cui viene assegnato il valore uno per indicare che il primo frame nella sequenza.

L'access point che riceve la richiesta, la elabora e restituisce la relativa risposta di cui indichiamo qui di seguito il contenuto del messaggio:

- Message type: Management;
- Message subtype: Authentication;
- Information items:
  - Authentication Algorithm Identification = “Open System”:
  - Authentication transaction sequence number = 2;
  - Authentication algorithm dependent information (none);
- Direction of message: From AP to STA.

A differenza del primo frame il numero progressivo della sequenza dei frame viene impostato con valore *due* e viene inserito un *codice status* indica il risultato della richiesta di autenticazione.

Autenticazione di tipo “Shared Key”

Il metodo di autenticazione *Shared Key* prevede l'uso di un sistema a chiavi per proteggere i contenuti delle comunicazioni. La fase di handshake non prevede scambio di chiavi, che si assume siamo già conosciute dalla stazione mobile e dal AP coinvolto. Nella seguente è rappresentato la tipica fase di comunicazione per la validare l'autenticazione attraverso algoritmi di sicurezza WEP. Il WEP*[Par. 2.3.2]* è l'algoritmo di sicurezza previsto di base dallo standard IEEE 802.11 di cui successivi miglioramenti, noti i problemi di sicurezza di cui soffre, sono stati apportati nello standard IEEE 802.11i (802.1X, WPA, WPA2) *[Par.2.3.3]*

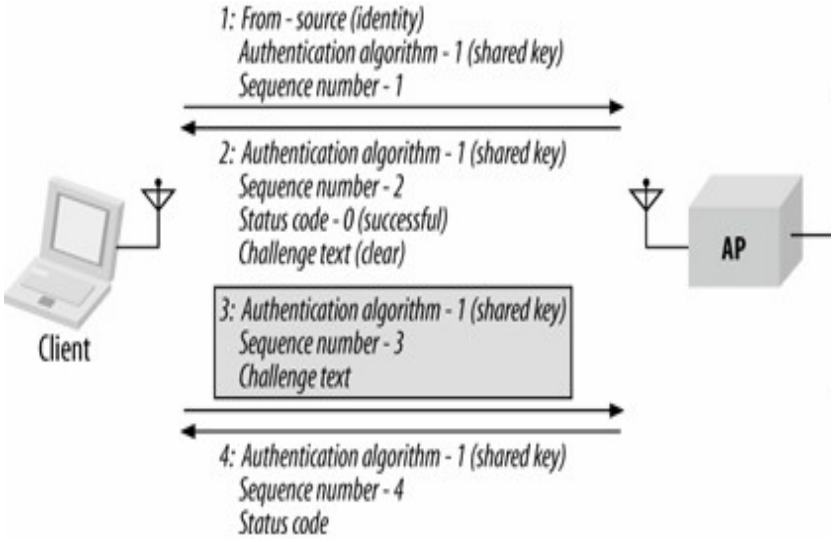


Figura 19: Shared Key System, sequenza messaggi

A conclusione della sezione riassumiamo le sequenze di messaggi nel caso di utilizzo di servizi di autenticazione *Open System e Shared Key*:

Authentication algorithm	Authentication transaction sequence no.	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

Tabella 8: Open System e Shared Key, riassunto sequenze di messaggi

Questi aspetti saranno approfonditi nel secondo capitolo.

e. Associazione

Una volta che la fase di autenticazione è completata, le stazioni possono associarsi con un AP (o riassociarsi ad un nuovo AP) per guadagnare l'accesso completo alla rete. L'associazione è una management operation che permette al sistema di distribuzione di rintracciare la posizione di ogni stazione mobile, in modo che i frame destinati ad una stazione mobile possono essere spediti al relativo AP.

Dopo che la fase di associazione è completata, un AP deve registrare la stazione mobile sulla rete in

modo che i frame per la STA siano trasportati al AP. L'associazione si limita alle reti infrastrutturate ed è logicamente equivalente al collegamento in una wired lan.

Una volta che la procedura è completata, una stazione wireless può usare il sistema di distribuzione per comunicare con il *mondo esterno* alla rete e viceversa, riceverne le risposte. Lo standard IEEE 802.11 proibisce a esplicitamente che una stazione mobile possa associarsi con più di un AP.

Procedure di Associazione

Sono riassunte qui di seguito le procedure di associazione:

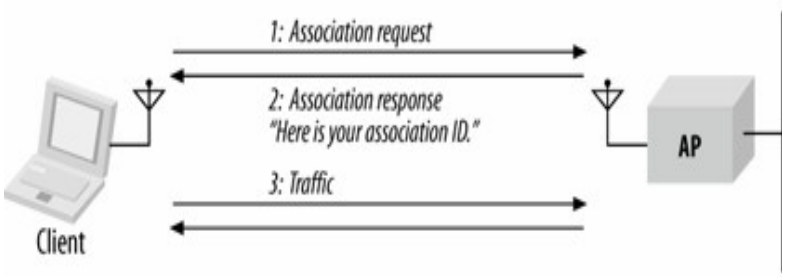


Figura 20: Association procedure, sequenza messaggi

a. STA Association Procedures

Inviata una richiesta dalla stazione monile (STA), deve essere associata con un AP attraverso la seguente procedura:

1. La STA trasmette una *association request*, caratterizzato dal seguente frame body:

Order	Information
1	Capability information
2	Listen interval
3	SSID
4	Supported rates

Tabella 9: Association request, frame boby

   all'access point (AP) con il quale si è precedentemente autenticata;

2. Se un *Association Response* frame:

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

Tabella 10: Association response, frame body

è ricevuto con stato *"successful"*, la STA è associata con AP, e conferma la fine della fase di associazione;

3. Se l'*Association Response* frame ricevuto ha il campo *status code* diverso da *"successful"* o il tempo scade l'*AssociateFailureTimeout*, la stazione mobile non è associata con l'access point e viene comunicato il fallimento della fase di associazione.

b. AP Association Procedures

Un Access Point per supportare l'associazione delle stazioni mobili opera nel seguente modo:

1. Quando un *Association Request* frame è ricevuto da una STA autenticata, l'access point deve trasmettere un *Association Response;*

   Se il campo *status code* ha valore "successful", l'*Association ID* assegnato alla stazione mobile deve essere incluso nella risposta. Altrimenti l'access point trasmetterà un *Deauthentication* frame alla STA;

2. Quando l'access point riceve la conferma di ricezione dell'*Association Response* frame mandato alla stazione mobile, con il campo s*tatus code* di valore "successful", essa viene considerata effettivamente associata al AP;

3. L'access point deve informare il Distribution System (DS) dell'avvenuta associazione.

f. Riassocazione

Le situazioni in cui si possono verificare le procedure di riassociazione sono le seguenti:

- **Caso 1:** Uscita temporanea dalla zona di copertura del AP a cui la STA era precedentemente autenticata e ritorno in essa;

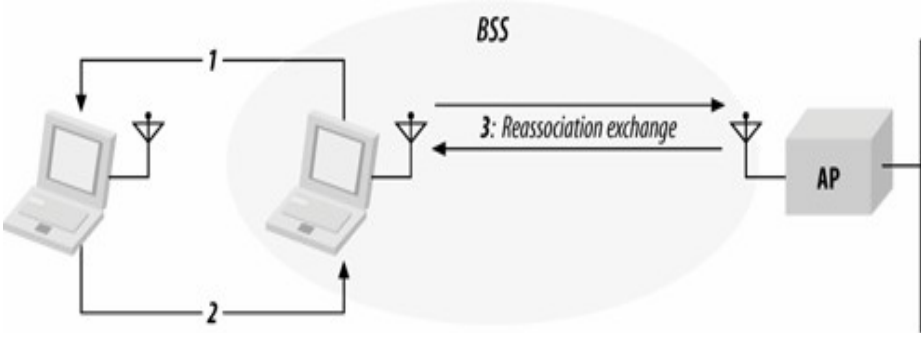


Figura 21: reassociation procedure, sequenza messaggi

- **Caso 2:** Passaggio di una STA dalla zona di copertura dell'access point (*Old AP)*, a cui era associato, a quella di un nuovo access point (*New AP*).

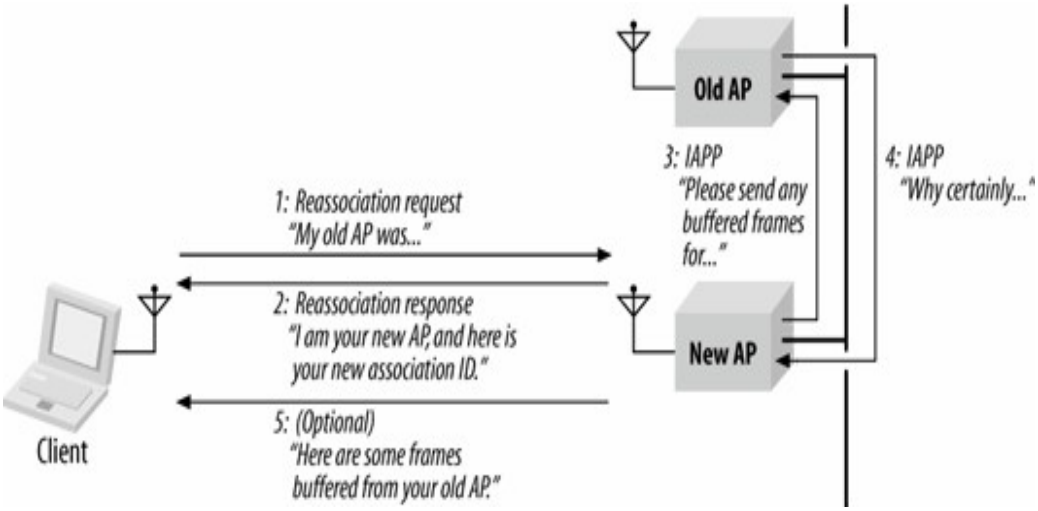


Figura 22: reassociation procedure, sequenza messaggi

Caso 1 - STA

La sequenza di operazioni che caratterizza le procedure di riassociazione in cui è coinvolta la stazione mobile è la seguente:

1. La stazione mobile trasmette un *Reassociation Request* frame all'access point con il seguente frame body:

Order	Information
1	Capability information
2	Listen interval
3	Current AP address
4	SSID
5	Supported rates

Tabella 11: Reassociation Request, frame body

2. Se il *Reassociation Response* frame:

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

Tabella 12: Reassociation Response, frame body

ricevuto ha il campo *status code* uguale a "successful," la stazione mobile è associata con l'access point e viene generata una notifica per indicare che l'operazione si è conclusa correttamente. Invece, se il *Reassociation Response* frame ricevuto non ha come *status code* il valore "successful" o trascorre il *ReassociateFailureTimeout*, la stazione mobile non è associata all'access point.

Caso 1- AP

Un access point opera nel seguente modo:

1. Quando è ricevuto un *Reassociation Request* frame da una STA autenticata, l'access point deve trasmettere un *Reassociation Response* frame. Se lo stato ha valore "successful", alla stazione mobile viene assegnato un *Association ID* e sarà incluso nella risposta. In caso contrario l'access point deve trasmettere un Deauthentication frame alla STA;
2. Quando una stazione mobile notifica la ricezione del *Reassociation Response* con il campo *status code* di tipo "successful", viene considerata associata all'access point;
3. L'access point deve informare il distribution system (DS) dell'avventa riassociazione.

Caso 2

Quando una stazione si muove dalla zona di coperture di un altro AP, usa il processo di riassociazione per informare la rete 802.11 della nuova posizione. La stazione controlla la qualità del segnale che riceve dal punto di accesso a cui è connesso, così come la qualità del segnale da altri punti di accesso nello stesso ESS. Quando la stazione mobile valuta utile il passaggio ad un altro punto di accesso, inizia la procedura di riassociazione. I fattori che determinano l'inizio della riassociazione possono essere i dipendenti dai singoli vendor. Un elemento fondamentale in queste valutazioni è la potenza del segnale ricevuto dagli AP, in cui le trasmissioni costanti di frame Beacon forniscono un buon punto di partenza per controllare la potenza del segnale proveniente da un punto di accesso.

Analizziamo le fasi di questa procedura:

- La stazione del mobile invia una richiesta di riassociazione al nuovo AP. Le richieste di riassociazione hanno un frame simile alle richieste di associazione. L'unica differenza è che i frame di richiesta di riassociazione contengono un campo con l'indirizzo di vecchio punto di accesso. Il nuovo AP deve comunicare con il vecchio AP per determinare se esiste la STA è associata. Anche se è stato definito dalla IEEE un protocollo standard *IAPP(Inter-Access Point Protocol)* per favorire queste comunicazioni, molte implementazioni rimangono proprietarie. Il nuovo AP risponderà con un Deauthentication frame e conclude la procedura, se non può verificare che il vecchio AP ha precedentemente autenticato la stazione mobile (STA);
- L'access point invia la richiesta di riassociazione. L'elaborazione delle richieste di riassociazione è simile a quelle di associazione, infatti gli stessi fattori possono essere usati nel decidere se permettere la riassociazione:
  - Se la richiesta di riassociazione è assegnata, il punto di accesso risponde con un codice status di 0 (successful) ed il AID;
  - Le richieste di riassociazione fallite includono nel frame appena un codice status e la procedura di chiusura.
- Il nuovo AP si mette in contatto con il vecchio AP per finire la procedura di riassociazione. Questa comunicazione fa parte dello IAPP;
- Il vecchio AP trasmette tutti i frame presenti nel buffer per la stazione mobile al nuovo AP. Lo Standard IEEE 802.11 non specifica la comunicazione fra AP. Alla conclusione del trasferimento dei frame presenti nel buffer:
  - Tutti i frame del vecchio AP sono trasferiti al nuovo AP in modo che possono essere trasportati alla stazione mobile;
  - Il vecchio AP termina la relativa associazione con la stazione mobile. Lo standard IEEE 802.11 impone che le stazioni mobili possono associarsi soltanto con un AP alla volta.
- Quando il nuovo AP riceve un frame destinato alla stazione mobile, è inviato attraverso il bridge Ethernet-Wireless o è bufferizzato nel caso un cui la stazione mobile è in modalità power saving.

1.5.4 Management Operations: Relazione fra i servizi

Ogni STA mantiene due variabili di stato :

1. Authentication state;
2. Association state.

In funzione del valore delle due variabili di stato, ogni STA può trovarsi in tre stati diversi :

Stato 1 : authentication=false, association=false;

Stato 2 : authentication=true, association=false;

Stato 3 : authentication=true, association=true;

Ciascun stato identifica una classe di frame che può essere negoziata. La *figura 28* mostra il diagramma di stato di una generica STA.

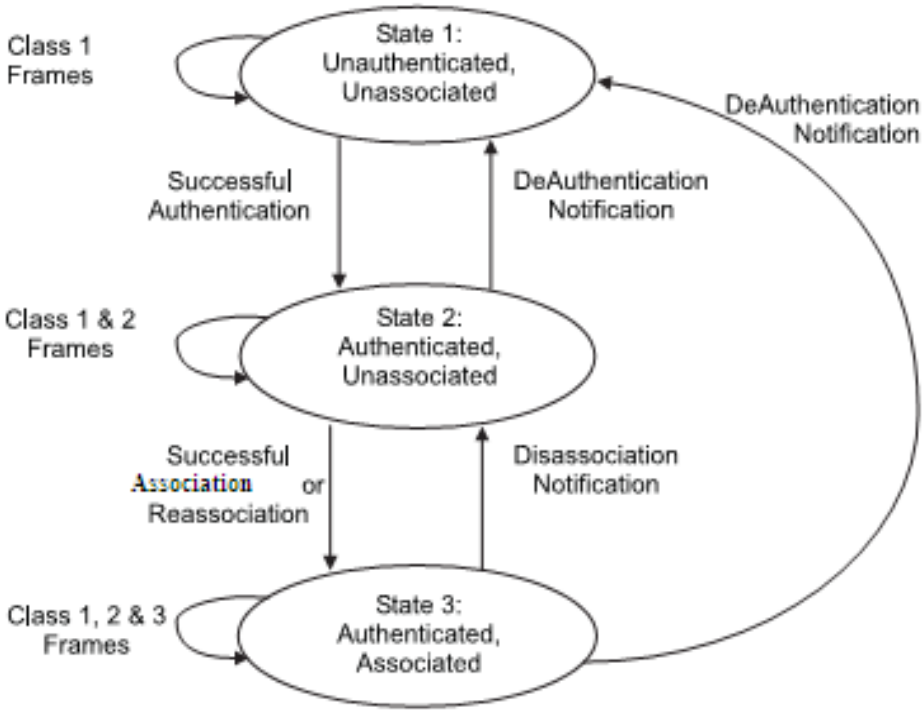


Figura 23: Diagramma di stato di una generica STA

Le classi dei frame sono definite come segue :

Class 1 frames	Class 2 frames	Class 3 frames
a) Control frames	**a) Management frame**	**a) Control frames**
- RTS - CTS - ACK - CF-END+ACK - CF-END	- Association request/response - Reasssociation request/response - Disassociation	- PS-Poll
b) Management frames	**b) Managemet frames**	**b) Managemet frames**
- Probe request/response - Beacon - Authentication - Deauthentication - ATIM	none	- Deauthentication
c) Data frames	**c) Data frames**	**c) Data frames**
- Data con i bits ToDS e FromDS false.	none	- Data con i bits ToDS e FromDS true.

Tabella 13: Le classi del diagramma di stato

Considerazioni sulla macchina a stati

La macchina a stati presente nella figura 23, esemplifica le relazioni che intercorrono tra i servizi dello standard IEEE 802.11. Nel meccanismo di annessione di una stazione mobile ad una rete il sevizio che ricopre un ruolo fondamentale è l'Autenticazione. Senza avere superato con successo la fase di autenticazione (stato 2), non è possibile accedere alle operazioni di Associazione/Riassociazione (stato 3).

Qualsiasi operazione che causa la perdita di Autenticazione forza la STA a ripetere tutte le operazioni per l'annessione ad una rete, provocando quindi anche la Deassociation della stazione mobile dal relativo access point. Questo meccanismo ha una forte influenza sui tempi di riconnessione alla rete. Infatti senza standard appositamente progettati come IAPP e 802.11r, approfonditi rispettivamente nel capitolo 2.4 e 3.2, lo standard IEEE 802.11 non risulta performante nel supporto alle operazioni di roaming. Attualmente senza la possibilità di passaggio di contesto delle informazioni tra gli AP legate all'autenticazione, eventuali operazioni di passaggio tra AP facenti parte di una rete ESS, alla stazione mobile è richiesto di ripetere le operazioni di Autenticazione e di Associazione con il conseguente aumento del ritardo.

Cap.2 Roaming di Livello2

Ci sono due tipologie di Roaming:

- Seamless
- Nomadic

Seamless roaming, ha come maggiore analogia la telefonata fatta su rete GSM. Questo tipo di rete prevede un alto numero di base station dislocate nel territorio per garantire massima copertura del segnale. Quando una persona telefona mentre viaggia in macchina su un'autostrada, attraversa molte aree di copertura della rete cellulare, e ciò nonostante la comunicazione resta attiva e non termina. Infatti, questo tipo di rete prevede un sistema di roaming che consente al cellulare di passare di area in area mantenendo attiva la comunicazione (vocale o dati) senza risentirne dei passaggi di associazione alle relative base station.

Questo tipo di roaming viene definito seamless in quanto le applicazioni di rete richiedono che la connessione alla rete resti sempre attiva durante le fasi di roaming.

Nomadic roaming, è differente da quello semaless. Un contesto che ne descrive a pieno le caratteristiche è quello in cui abbiamo notebook connessi alla rete wireless dell'ufficio. In questo ambientazione un utente finché si ritrova a lavorare all'interno della zona coperta dall'AP a cui è associato può connettersi tranquillamente alla rete per effettuare le sue operazioni. Nel momento in cui smette di lavorare e si trasferisce all'interno di un'altra stanza di competenza di un nuovo AP, viene effettuato il processo di roaming. Questa operazione non causa ripercussioni se l'utente adopera servizi di rete che non richiedono il mantenimento della connessione attiva.

Un esempio tipico è l'invio di email, in cui l'operazione può essere effettuata nel luogo di partenza e di destinazione, senza avere l'esigenza che la comunicazione sia attiva durante lo spostamento del notebook da una stanza all'altra.

Prendiamo in considerazione i fattori possono influire sul processo di roaming:

a. Natura dello standard IEEE 802.11

Lo standard IEEE 802.11 è nato tipicamente per servizi che richiedono un roaming di tipo nomadic. Infatti come previsto nelle specifiche, in presenza di un nuovo access point la stazione mobile effettua tutte le operazioni di annessione alla rete. Questo comporta un serie di ritardi che non consentono il mantenimento della connessione attiva e quindi l'interruzione delle applicazioni in esecuzione che adoperavano la rete.

b. Tipo di applicazione di rete

Il tipo di comunicazione che usa l'applicazione ha grande rilevanza nel processo di roaming. Le applicazioni connection-oriented, come quelle che sono basare sul TCP, risultano essere più tolleranti

alla perdita di pacchetti durante il roaming perché utilizzano un protocollo orientato alla connessione. Il TCP richiede acknoledgment positivi, come le comunicazioni 802.11 MAC. Questo requisito permette a tutti i dati persi durante il processo di roaming di essere ritrasmessi attraverso il protocollo TCP. Alcune applicazioni contano sul User Datagram Protocol (UDP) come il protocollo di trasporto. Questo protocollo è caratterizzato da un basso overhead in quanto connectionless. Applicazioni quali il Voice over IP (VoIP) ed il video streaming adoperano UDP. La possibilità di ritrasmissione che il TCP offre finisce con il far aumentare la perdita del pacchetto per le applicazioni di VoIP, in cui la ritrasmissione dei pacchetti si riduce ad un disturbo della comunicazione.

c. Elementi di valutazione

Con il termine *Roaming Duration* indichiamo il tempo necessario affinché la fase di roaming sia completata. Il roaming è sostanzialmente il processo di associazione descritto nel capitolo precedente, e dipende dalla durata delle seguenti operazioni:

- The probing process.
- The 802.11 authentication process.
- The 802.11 association process.
- The 802.1X authentication process.

Applicazioni, come il VoIP, sono estremamente sensibili ai ritardi e non possono tollerare tempi di roaming troppo ampi.

Tipi di domini del Roaming

Nella tecnologia Ethernet, viene indicato con *broadcast domain* una rete che connette dispositivi a reti che sono capaci di mandare e ricevere frames in broadcast tra di loro. Questo dominio prende il nome di *Layer 2* network. Il concetto di *broadcast domain* è applicabile anche allo standard 802.11.

Nel 802.11, access point (AP) che appartengono allo stesso broadcast domain, configurati con lo stesso SSID, si dicono appartenenti allo stesso roaming domain. Una tipica struttura di rete a cui ci si riferisce in questo caso è la ESS, cioè un insieme di reti BSS unite da un DS (Distribuition System), generalmente una rete wired.

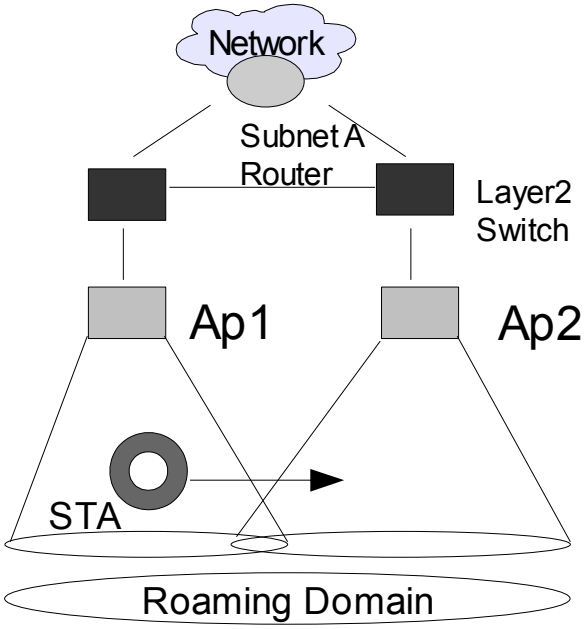
Ci sono due tipologie di roaming, quello a *Livello 2* della rete, nativamente supportato dallo standard IEEE 802.11 e quello a *Livello 3* della rete che richiede metodi e supporti dei livelli superiori per mantenere l'indirizzo IP costante anche dopo lo spostamento.

Queste tipologie sono direttamente legate alla tipo di roaming domain:

- intra roaming domain
- between roaming domain

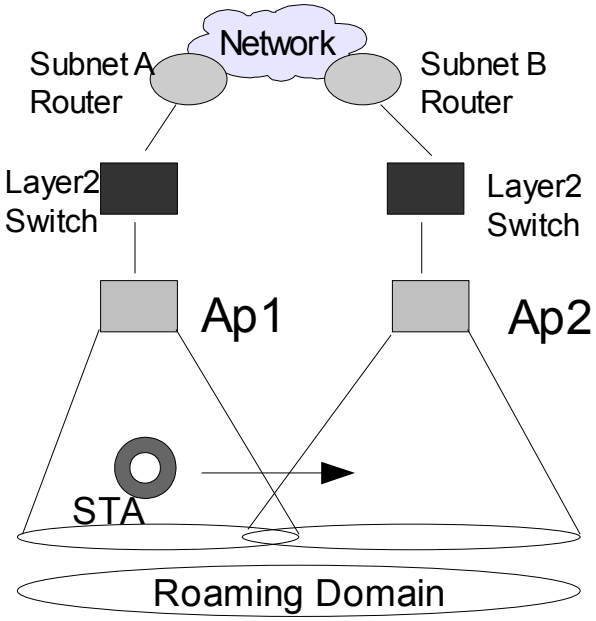
a. Roaming all'interno dello stesso dominio

Durante il passaggio di una STA tra zone di copertura di due AP, ad esempio da AP1 a AP2, i servizi attivi nel dispositivo mobile mantengono la propria connessione sino a quando l'indirizzo di rete a livello 3 viene mantenuto invariato.



b. Roaming tra domini diversi

Il passaggio dei una STA tra due sottoreti, A e B, comporta il cambiamento a livello 3 dell'indirizzo di rete per far si che la connessione sia mantenuta nella sottorete B. Questo comporta l'interruzione delle applicazioni e dei servizi attivi. In questo caso per il mantenimento delle connessioni attive durante e successivamente dei servizi attivi della STA, parleremo di *"Mobile IP"*.



2.1 Layer 2 Roaming: Caratteristiche

Il roaming al livello 2 dello standard IEEE 802.11 è definibile come:

"mobilità fornita dalla possibilità di effettuare handover tra access links(AP) in un'area ristretta e tra componenti della stessa tecnologia".

Il meccanismo per determinare il momento in cui effettuare roaming non è definito nelle specifiche delle standard IEEE 802.11, e viene implementato dagli stessi produttori. Questo pone l'accento sul problema di compatibilità a cui si rischia di andare incontro. Negli ultimi anni diverse industrie che producono prodotti 802.11, stanno collaborando per garantire un'interoperabilità di base. Le modalità in cui è scritto questo algoritmo può essere per le singole aziende un elemento caratterizzante importante rispetto ai prodotti delle altre pretendenti, facendolo diventare un vero valore aggiunto.

Analizzando un po' le operazioni che caratterizzano la fase di roaming, sicuramente questo algoritmo terrà conto di problemi come *signal strength, retry counters, missed beacons* e altri concetti del livello MAC. Ad esempio il *binary exponential backoff algorithm* previsto dallo standard IEEE 802.11 per regolare l'accesso al dispositivo fisico, incrementa il *frame-retry counter* se la STA non è in grado di trasmettere dopo un certo numero di tentativi. Questa situazione fornisce informazioni utili al client per capire che si sta allontanando dalla zona di copertura del AP. L'algoritmo dei roaming userà i *frame-retry counter* tra i fattori di decisione per iniziare le fasi di roaming. Allo stesso tempo molto importante è al capacità dell'algoritmo di bilanciare tra *fast roam time* e *client stability* per evitare falsi positivi.

2.1.2 Processo di roaming nel protocollo 802.11

Analizziamo la procedura di roaming nei suoi dettagli. Nella figura 24 viene rappresentata la procedura di handoff relativa allo standard IEEE 802.11.

Questa operazione può essere suddivisa in due fasi: ***discovery e reauthetication***.

1. ***Discosvery***: Attributi importantissimi della mobilità sono, il *signal strength e signal-to-noise* del segnale tra il dispositivo mobile e l'access point a cui è collegato. Infatti il segnale può degradare causando la perdita della connettività e l'inizio della fase di handoff. Il client ha la necessità di trovare tra i potenziali AP (presenti all'interno del suo raggio d'azione) quello a cui associarsi.

   Questa operazione viene svolta, come precedentemente presentato *[Cap1.5.3],* al livello MAC attraverso la funzione di ***scan***: *passivo o attivo.*

   - **attivo**: il dispositivo mobile invia richieste attivamente in broadcast su ogni canale in ricerca di un AP. In questa modalità il dispositivo mobile resterà su ogni singolo canale *10ms-20ms* in in attesa di un probe response.

- **passivo**: il dispositivo mobile attende di ricevere i beacon frame inviati dagli access point, che tipicamente ne manda 10 ogni secondo. Questo metodo dipende dai segnale inviati dai singoli AP, introducendo così un potenziale rischio di non percepire un AP se i beacons frame non sono ricevuti durante la fase di scanning.

Per velocizzare questa fase è possibile inviare meno informazioni all'interno dei beacon frame, dipendentemente dalle configurazioni degli AP.

2. ***Reauthentication:*** La stazione cerca di riautenticarsi su un AP, scelto seguendo la usa lista di priorità. La tipicamente questa fase è composta di due sottoparti: *autenticazione* e *riassocazione al nuovo AP*. Questo processo consiste generalmente nel trasferimento delle credenziali ed altre informazioni dal vecchio AP al nuovo AP. Per rendere più performante questa operazione è stato realizzato uno specifico protocollo, IEEE 802.11f IAPP *[3]*, che ottimizza la comunicazione tra access point, di cui tratteremo successivamente*[Cap.2.3]*.

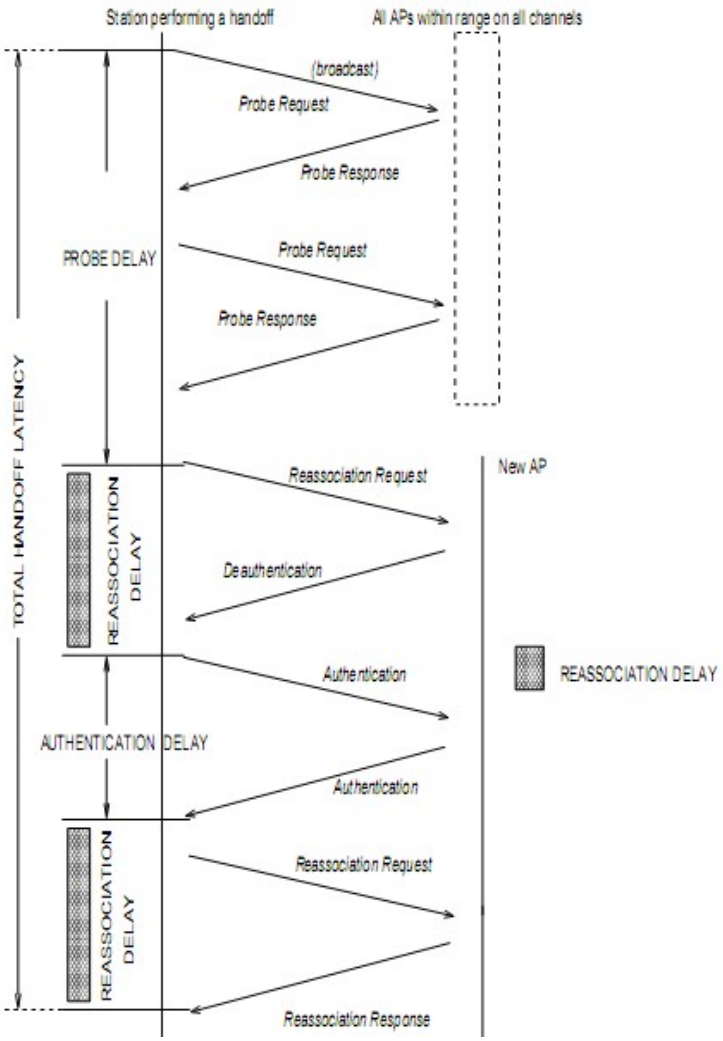


Figura 24: IEEE 802.11 handoff

Come evidenziato in figura 24, in risposta al primo frame del tentativo di riassocazione, siccome non è stata trasferita nessuna informazione al nuovo AP riguardante l'autenticazione del dispositivo mobile (STA), l'access point risponde con un frame di deautenticazione. Questo tipo di risposta rispetta il diagramma di stato di una generica STA*[Par.1.6.3]*. In questa situazione emerge il ruolo fondamentale della validità dell'autenticazione al fine di compiere la fase di roaming.

Infatti per completare la fase di roaming vengono ripercorse tutte le fasi indicate dal diagramma di stato presentato nello standard IEEE 802.11 (autenticazione ed associazione).

Considerazioni sulla fase di Roaming IEEE 802.11

La fase di roaming non si presenta composta solo dai singoli frames evidenziati nella figura 24, infatti questa operazione è influenzata anche da fattori esterni.

Come presentato nell'articolo*[4]*, lo schema precedente ha una valenza teorica. Infatti dalle sperimentazioni che hanno effettuato è emerso come la STA può scambiare dati nel periodo che va dalla fase di search fino a quella di execution. Successivamente un diagramma riassuntivo.

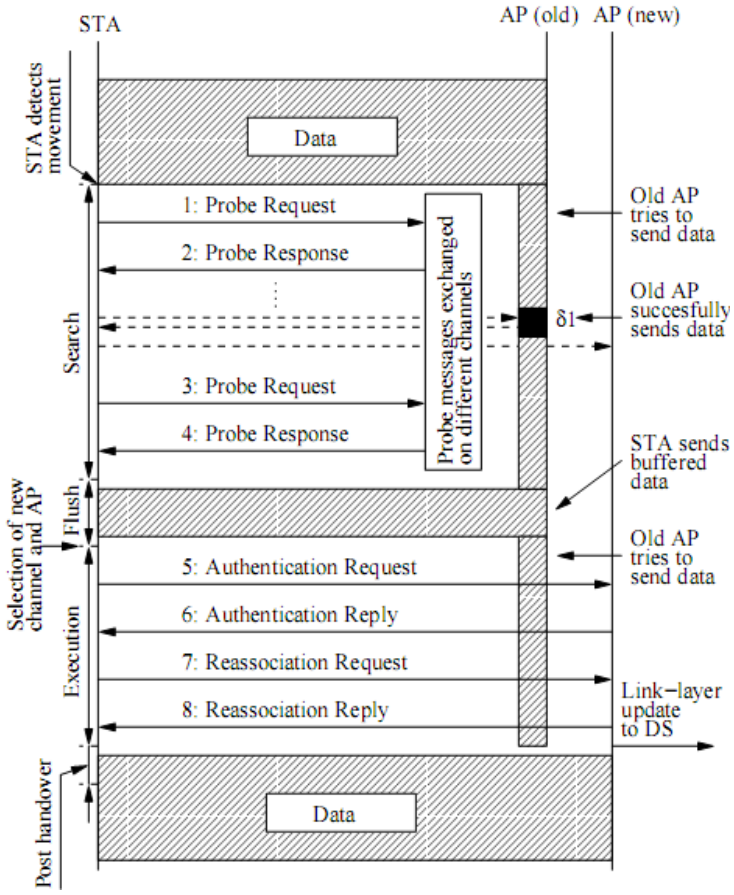


Figura 25: Schema sperimentale di handoff

Se un dispositivo mobile (STA) continua a trasmettere dati, questi pacchetti in upstream possono essere bufferizzati dalla STA durante le fasi *search* ed *execution* indicate in figura 25. Questi dati

possono essere inviati durante la fase di *search* e devono essere flushed al vecchio AP tra la fase di *search* ed *execution* o al nuovo AP dopo la fase di *execution*.

Se consideriamo il caso opposto dove il vecchio AP riceve i dati (downstream) per la STA, il AP può dei bufferizzare questi pacchetti su richiesta della STA (la STA potrebbe chiede di entrare in power safe mode). Dopo la fase di ricerca la STA potrebbe informare l'access point che torna in modalità attiva, così da permettere al AP di fare un flush dei dati bufferizzati dalla STA prima che esso entri nella fase di esecuzione. A meno che la STA entri in power save mode, AP proverà a trasmettere le strutture di dati alla STA mentre arrivano. Da osservare è che questi pacchetti non saranno per forza persi, infatti durante la fase di ricerca c'è una probabilità che alcuni di questi pacchetti downstream possono realmente arrivare.

2.1.3 Preautenticazione

La fase di preautenticazione è usata per accelerare il trasferimento di associazione tra il vecchio AP ed il nuovo AP. L'autenticazione può causare spesso un aumento di ritardo fra il tempo che impiega una STA per decidere verso quale AP muoversi ed il tempo in cui i frames inviati dal dispositivo mobile raggiungono il nuovo AP. La preautenticazione tenta di ridurre il tempo predisponendo tutte le informazioni necessarie per il passaggio di autenticazione prima dell'inizio della fase di associazione.

Low-level 802.11 Preauthentication: Le stazioni si devono autenticare con un AP prima di associarsi con esso. Lo standard IEEE 802.11 non spiega nei dettagli il funzionamento di questo processo ma definisce solo delle linee generali. I dispositivi mobili si possono autenticare con più AP durante il processo di scanning in modo che al momento dell'associazione, risultino già autenticati. Grazie alla preautenticazione, le stazioni possono riassociarsi immediatamente al AP più vicino, piuttosto che dover aspettare lo scambio di messaggi per l'autenticazione.

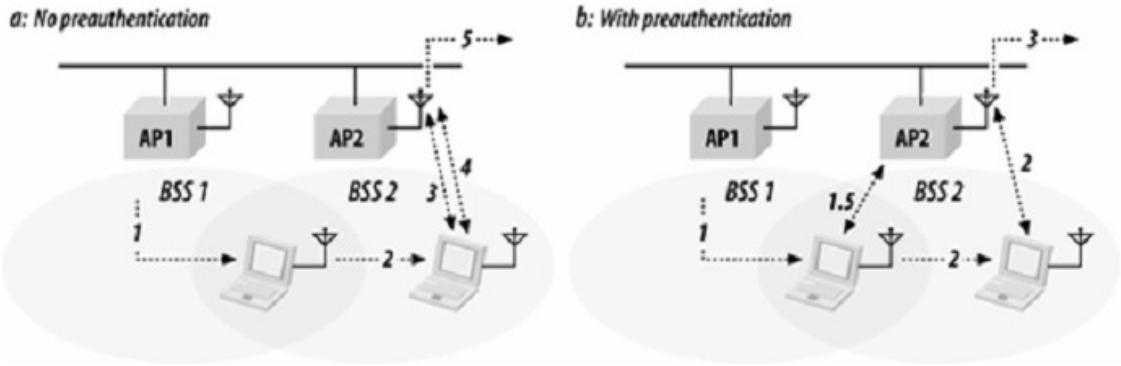


Figure 26: 802.11 - No-Preauthentication e Pre-Authentication

Nella figura 26 sono posti in confronto un sistema che non utilizza la preautenticazione (figura.26-a)

ed uno che adopera la fase di preautenticazione (figura .26-b). La rete ESS rappresentata è composta da due punti di accesso, AP1 e AP2, e per semplicità è indicata una sola STA. Nell'esempio riportato la stazione mobile è associata con AP1.

I dettagli delle fasi che compongono questi processi sono indicati nella tabella seguente.

Step	**Azioni senza preautenticazione [Figure X(a)]**	**Azioni con preautenticazione [Figure X(b)]**
0	La stazione è associata con AP1	La stazione è associata con AP1
1	La stazione si sposta verso destra nella fase di sovrapposizione tra le BSS1 e BSS2	La stazione si sposta verso destra nella fase di sovrapposizione tra le BSS1 e BSS2 ed avverte la presenza di AP2
1.5	nessuna	La stazione si preautentica con AP2
2	Forte segnale dell'AP2, la stazione decide di associarsi con AP2	Forte segnale dell'AP2, la stazione decide di associarsi con AP2
3	La stazione si autentica con AP2	La stazione può iniziare ad usare la rete
4	La stazione si riassociata con AP2	nessuna
5	La stazione può iniziare ad usare la rete	nessuna

Tabella 14: Confronto roaming con preautenticazione abilitata e disabilitata

2.2 Layer 2 Roaming: Autenticazione

Come emerso nei paragrafi precedenti il processo di autenticazione può avere un'importante rilevanza nella fase di roaming. La scelta dell'algoritmo con cui criptare le comunicazioni, comporta una variazione del numero di pacchetti scambiati tra l'access point ed il dispositivo mobile. Queste variazioni possono condizionare in qualche modo la fase di roaming influendo sui ritardi, provocando una diminuzione delle prestazioni con conseguente perdita delle connessioni attive. Nei paragrafi successivi saranno date le nozioni di base sui sistemi di autenticazione e nel capitolo successivo sarà valutato l'effetto degli algoritmi di crittografia sulla fase di roaming*[Par.3.1]*.

2.2.1 Background

Inizialmente il Wired Encryption Protocol (WEP)*[1]* è stato proposto come alternativa alla connessione in modalità Open, per cifrare il flusso di dati e per fornire una prima autenticazione. Dopo poco tempo viene scoperta l'insicurezza totale di questo protocollo.

Successivamente sono state proposte diverse soluzioni per cercare di aumentare la sicurezza delle comunicazioni:

- *Temporary Key Integration Protocol (TKIP):* basato su WEP per effettuare un re-keying veloce nel tentativo che migliori la sicurezza. Spesso ci si riferisce a questo metodo con il nome WPA.
- Il protocollo 802.1x*[5]*: sviluppato per ovviare alla debole autenticazione offerta del sistema aperto e dell'autenticazione di WEP.

Lo standard IEEE 802.11i*[6]*, conosciuto anche come WPA2**,** è stato ratificato il 24 Giugno 2004 e rappresenta un superset (estensione) del precedente standard WEP. Prima dello standard IEEE 802.11i la Wi-Fi Allinace aveva introdotto il Wi-Fi Protected Access (WPA), un sottoinsieme delle specifiche 802.11i.

Il WPA è nato con lo scopo di tamponare l'emergenza sicurezza dovuta al WEP e rappresenta solamente uno standard transitorio mentre l'802.11i veniva terminato e perfezionato. La Wi-Fi Alliance 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.

La diffusione di questo standard è stata legata strettamente a quella dell'hardware compatibile. Al momento dell'uscita dello standard non tutto l'hardware presente sul mercato ne supportava le caratteristiche implementative. Questo fattore a portato un forte ritardo nell'utilizzo di questa soluzione.

Lo standard IEEE 802.11i utilizza come algoritmo crittografico Advanced Encryption Standard (AES) a differenza del WEP e del WPA che utilizzano l'RC4.

L'architettura dello standard IEEE 802.11i utilizza i seguenti componenti:

- IEEE 802.1X per autentificare. Può essere utilizzato EAP (Extensible, authentication Protocol) o un server di autentificazione RSN per tenere traccia delle associazioni
- Protocollo CCMP *(Cipher Block Chaining Message Authentication)* per garantire la confidenzialità, l'integrità e la certezza del mittente.

Un elemento importante del processo di autenticazione è il processo *four-way handshake*.

2.2.2 Wired Encryption Protocol (WEP)

La specifica IEEE 802.11 MAC*[1]* descrive un protocollo di crittografia denominato WEP. Il WEP fornisce supporto a due aspetti critici dello standard IEEE 802.11, *autenticazione e riservatezza,* usando un meccanismo a chiave comune con una cifra simmetrica denominata RC4. La chiave che il dispositivo mobile sta usando per l'autenticazione e la crittografia del flusso di dati deve essere la stessa chiave usata dal AP.

Anche se lo standard IEEE 802.11 fissa la lunghezza della chiave a 40bit, la maggior parte dei fornitori hanno effettuato una chiave di 104 bit al fine di aumentare la sicurezza.

WEP Data Processing

La riservatezza e l'integrità sono gestite simultaneamente, come illustrato nella figura 27.

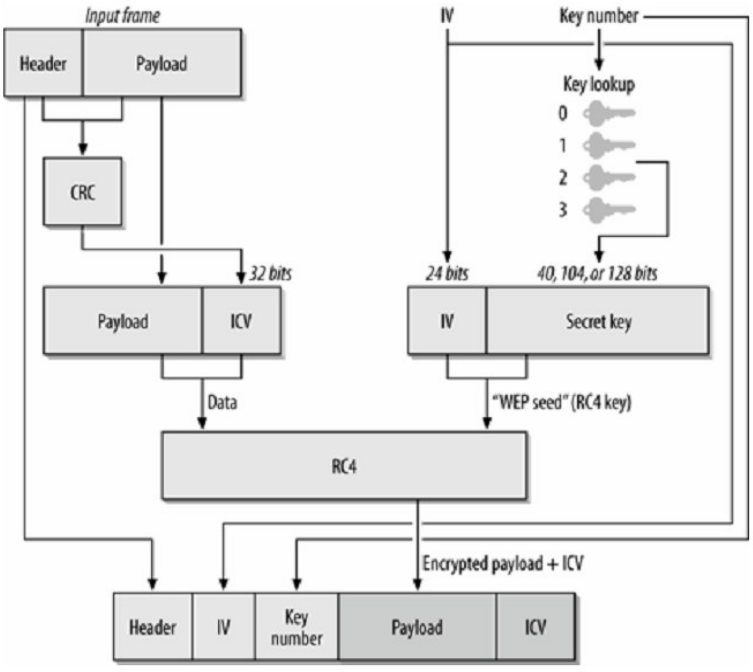


Figura 27: Operazioni WEP

Prima della fase di encryption, viene effettuata una procedura di controllo di integrità sul frame, la quale genererà un hash denominato: Integrity Check Value (ICV). ICV protegge il contenuto dall'alterazione accertandosi che il frame non sia cambiato durante il transito. Il frame e ICV vengono

entrambi cifrati, in modo ICV non sia esposto attacchi.

Come input, WEP richiede tre elementi:

- *Il payload che deve essere protetto*: il quale viene dai livelli dello stack protocollare superiori.
- *Secret key*: che viene usata nella fase di encryption del frame. A seconda dell'implementazione, le chiavi possono essere specificate come stringhe di bit, o key number. Il protocollo WEP permette che quattro chiavi siano immagazzinate simultaneamente.
- *Initalization vector (IV)*: usato con la chiave segreta nella trasmissione del frame.

Dopo l'elaborazione, il protocollo WEP produce un frame cifrato, contenente anche le informazioni utili per permettere al destinatario di decriptare il frame, pronto per la trasmissione su una rete non sicura.

WEP Procedure

Il driver software ed l'interfaccia hardware sono responsabili dell'elaborazione dei dati e della spedizione del pacchetto cifrato, usando la seguente sequenza di operazioni:

- Il frame del protocollo 802.11 è composto da un header e un payload. Il protocollo WEP protegge soltanto il payload del MAC 802.11 e lascia gli header delle 802.11 inalterati, così come tutti gli header degli livelli più bassi.
- Un Integrity Check Value (ICV) è calcolato sul payload del frame 802.11 MAC (dal primo bit del SNAP header fino all'ultimo bit dei dati contenuti nel corpo del frame). Il valore del FCS (Frame Check Sequence) del protocollo 802.11 non è stato ancora calcolato, in modo tale che non sia incluso nel calcolo anche ICV. L'ICV usato dal WEP è il codice Cyclic Redundancy Check (CRC).
- La chiave di crittografia del frame, o *WEP seed*, è la combinazione di due parti: la *secret key* ed l'*initalization vector (IV)*. L'initalization vector è usato per produrre stream di dati cifrati differenti per ogni struttura trasmessa. Infatti per ridurre le occorrenze della crittografia realizzata con le stesse key stream, il mittente combina IV alla secret key.

  Lo standard IEEE 802.11 non dispone vincoli sulla procedura usata per scegliere gli IV. Alcuni prodotti assegnano IV sequenziali, mentre altri usano un algoritmo di pseudorandom hashing.

  La scelta degli IV ha alcune implicazioni di sicurezza perché una cattiva selezione degli IV può compromettere le chiavi.
- La chiave di crittografia del frame è usata come chiave dell'algoritmo RC4 per cifrare il payload del 802.11 MAC. Il processo di crittografia spesso è realizzato da appositi circuiti dedicati RC4 presenti sulla scheda hardware.

- Una volta cifrato il payload, la stazione mittente realizza il frame che sarà effettivamente trasmesso. Fra 802.11 MAC header ed il payload cifrato, è inserito il WEP header . Oltre al IV, il WEP header include un key number. Una volta che il header finale è aggiunto, il valore del 802.11 FCS può essere calcolato sull'intera struttura del MAC dall'inizio dell'intestazione alla fine del ICV (cifrato).

La fase di decrittazione effettuerà le stesse operazioni ma nell'ordine inverso. Come con qualunque altra trasmissione wireless, il valore FCS è convalidato per accertarsi che la struttura ricevuta non sia stata corrotta durante il transito. Per decriptare la parte protetta del frame, il ricevente prenderà la relativa chiave segreta, la combina con IV e genera la key stream. Una volta decriptati i dati, può convalidare ICV. Una volta che ICV è convalidato con successo, i dati del pacchetto possono essere passati al protocollo dei livelli superiori secondo il contenuto dello SNAP header.

2.2.3 Lo standard IEEE 802.11i

Lo standard IEEE 802.11i*[6]* introduce cambiamenti fondamentali come la separazione tra l'autenticazione dell'utente dalla segretezza e l'integrità del messaggio, fornendo una architettura di sicurezza robusta e scalabile adatta sia per le reti domestiche sia per grossi sistemi aziendali. La nuova architettura per le reti wireless è nominata Robust Security Network (RSN) e utilizza l'autenticazione 802.1X, una distribuzione della chiave robusta e nuovi meccanismi di segretezza e integrità dei dati.

Anche se l'architettura RSN è molto complessa, essa fornisce delle soluzioni sicure e scalabili per le comunicazioni wireless. Un RSN normalmente accetta solo dispositivi RSN, ma lo standard IEEE 802.11i definisce anche un'architettura Transitional Security Network (TSN) in cui possono partecipare sia RSN sia i sistemi WEP, consentendo anche agli utenti di aggiornare i loro strumenti. Se le procedure di autenticazione o di associazione tra le stazioni utilizzano *handshake a 4 vie*, l'associazione è detta RSNA *(Robust Security Network Association)*.

Una RSNA definisce un certo numero di caratteristiche di sicurezza oltre la Wired Equivalent Privacy (WEP) e l'autenticazione dello IEEE 802.11.

Queste caratteristiche di sicurezza includono quanto segue:

- Meccanismi aumentati di autenticazione per STA;
- Algoritmi di Key management;
- Cryptographic key establishment;
- Un meccanismo potenziato di incapsulamento dati, denominato CTR con protocollo CCMP e, facoltativamente, Temporal Key Integrity Protocol (TKIP).

Un RSNA conta su componenti esterni all'architettura dello IEEE 802.11, e per stabilire una comunicazione sono necessarie quattro fasi (riassunte in figura.28):

1. Accordo sulla politica di sicurezza;
2. Autenticazione 802.1X;
3. Derivazione e distribuzione di chiave;
4. Segretezza e integrità dei dati RSNA.

Analizziamo ora le fasi che compongono il processo di autenticazione 802.11i, riassunte nella seguente immagine:

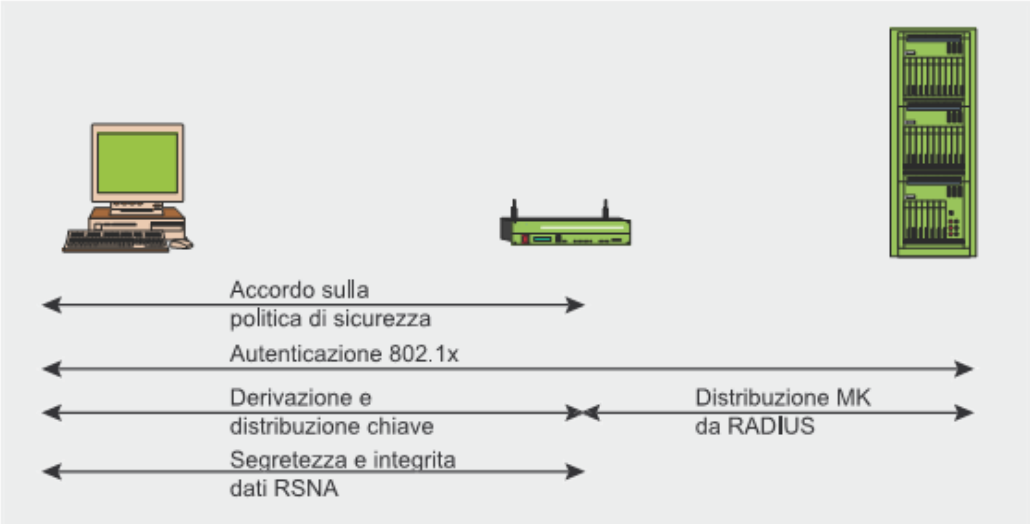


Figura 28: 802.11i - Riassunto Fasi

Fase 1: Accordo sulla politica di sicurezza

La prima fase richiede alle parti coinvolte nella comunicazione di stabilire un accordo sulla politica di sicurezza da adottare (figura 29). Le politiche di sicurezza supportate dal AP sono pubblicizzate su *Beacon* o in un messaggio *Probe Respond.* A questo messaggio seguirà un'autenticazione aperta standard.

La risposta del dispositivo mobile (STA) viene inclusa nell'*Association Request frame* al quale segue l'*Association Response frame* inviato dal AP come conferma. Le informazioni sulla politica di sicurezza è inviata nel campo RSN IE (*Information Element*) e contiene i seguenti dettagli:

- metodi di autenticazione supportati (802.1X, Chiave segrete pre-condivisa (PSK)),
- protocolli di sicurezza per traffico unicast (CCMP, TKIP ecc.) – la pairwise cipher suite,
- protocolli di sicurezza per il traffico multicast (CCMP, TKIP etc.) – il group cipher suite,
- supporto per la preautenticazione, permettendo agli utenti di preautenticarsi prima di passare ad un nuovo punto di accesso della stessa rete per un passaggio senza interruzioni.

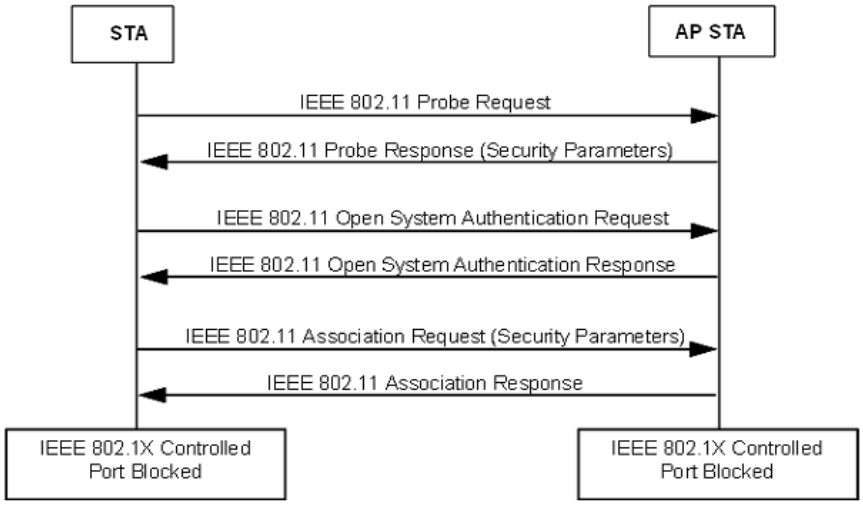


Figura 29: 802.11i - Prima fase

Fase 2: Autenticazione 802.1X

La seconda fase è l'autenticazione 802.1X basata sul EAP ed il metodo di autenticazione concordato in precedenza: EAP/TLS con certificati client e server (che richiedono una infrastruttura per chiave pubblica), EAP/TTLS o PEAP per l'autenticazione ibrida (con certificato richiesti solo per i server) ecc.

L'autenticazione 802.1X viene iniziata quando AP richiede i dati di identità del dispositivo mobile il quale risponde con un messaggio contenente il metodo di autenticazione scelto. Tra il client e il server di autenticazione sono scambiati i messaggi necessari per generare una chiave maestra comune (MK). Alla fine della procedura, un messaggio *Radius Accept* è inviato dal server di autenticazione al AP contenete la MK e il messaggio *EAP Success* per il client.

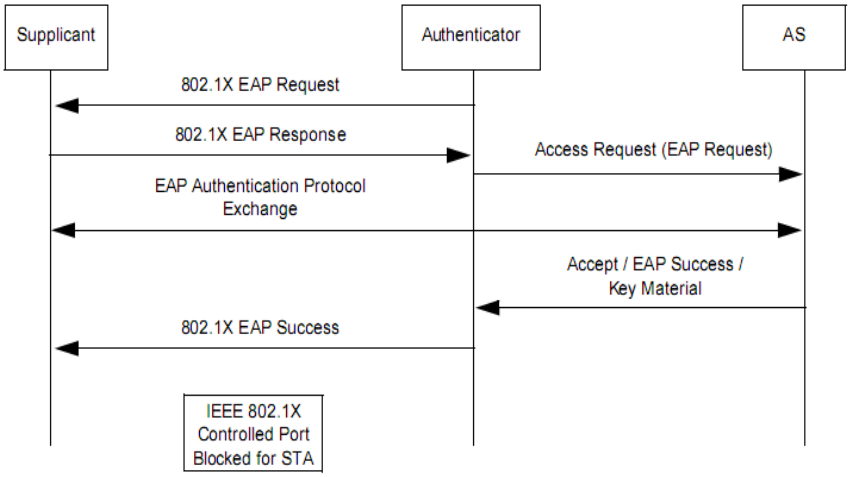


Figura 30: 802.11i - Seconda fase

Fase 3: Distribuzione e gerarchia di chiave

La sicurezza nelle connessioni dipende molto dalle chiavi segrete. Nel RSN, ogni chiave ha una vita limitata e la sicurezza generale è garantita da un'insieme di diverse chiavi, organizzate in una gerarchia. Quando viene stabilito un contesto di sicurezza dopo una autenticazione andata a buon fine, le chiavi temporanee (di sessione) vengono create e aggiornate regolarmente fino a quando il contesto di sicurezza non viene chiuso. La generazione e lo scambio delle chiavi sono affidati alla terza fase del processo 802.11i.

Si hanno due handshake durante le derivazione delle chiavi:

- ***Handshake a quattro vie*** per la derivazione della PTK (*Pairwise Transient Key*) e della GTK (*Group Transient Key*),
- ***Group Key Handshake*** per il rinnovo della GTK.

La derivazione della PMK (*Pairwise Master Key*) dipende dal metodo di autenticazione usato:

- se viene usata una PSK (*Pre-Shared Key*), PMK = PSK. La PSK viene generata dalla passphrase (da 8 a 63 caratteri) o una stringa di 256 bit e fornisce una soluzione per le reti domestiche e di piccole imprese che non hanno un server di autenticazione,
- se viene usato un server di autenticazione, la PMK è derivata dall'autenticazione 802.1X MK(Master Key).

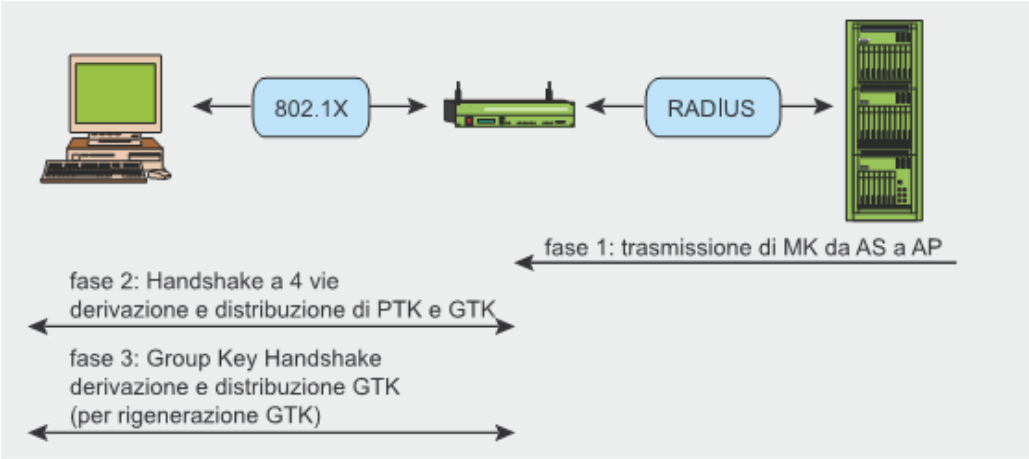


Figura 31: 802.11i - Terza fase: Derivazione e Distribuzione chiavi

La PMK stessa non è mai usata per il controllo di cifratura o integrità. Invece, è usata per generare una chiave di cifratura temporanea – per il traffico unicast si tratta di una PTK (*Pairwise Transient Key*). La lunghezza della PTK dipende dal protocollo di cifratura: 512 bit per TKIP e 384 bit per CCMP.

La PTK consiste di diverse chiavi temporanee:

- KCK (*Key Confirmation Key* – 128 bit): Chiave per i messaggi di autenticazione (MIC)

durante la *Handshake a 4 vie* e la *Group Key Handshake*,

- KEK (*Key Encryption Key* – 128 bit): Chiave per garantire la segretezza durante la *Handshake a 4 vie* e la *Group Key Handshake*,
- TK (*Temporary Key* – 128 bit): Chiave per la cifratura dei dati (usata per TKIP o CMMP),
- TMK (*Temporary MIC Key* – 2x64 bit): Chiave per l'autenticazione.

E' usata una chiave appositamente generata per ogni lato delle comunicazione.

Tramite lo *Handshake a 4 vie*, iniziato dall'access point, è possibile:

- confermare la conoscenza del dispositivo mobile della PMK,
- derivare una nuova PTK,
- installare chiavi di cifratura e di integrità,
- cifrare il trasporto della GTK,
- confermare la selezione di cifratori.

I quattro messaggi EAPOL-Key sono scambiati tra il dispositivo mobile e l'access point durante la fase di *Handshake a 4 vie*. Questo processo viene illustrato nella seguente figura:

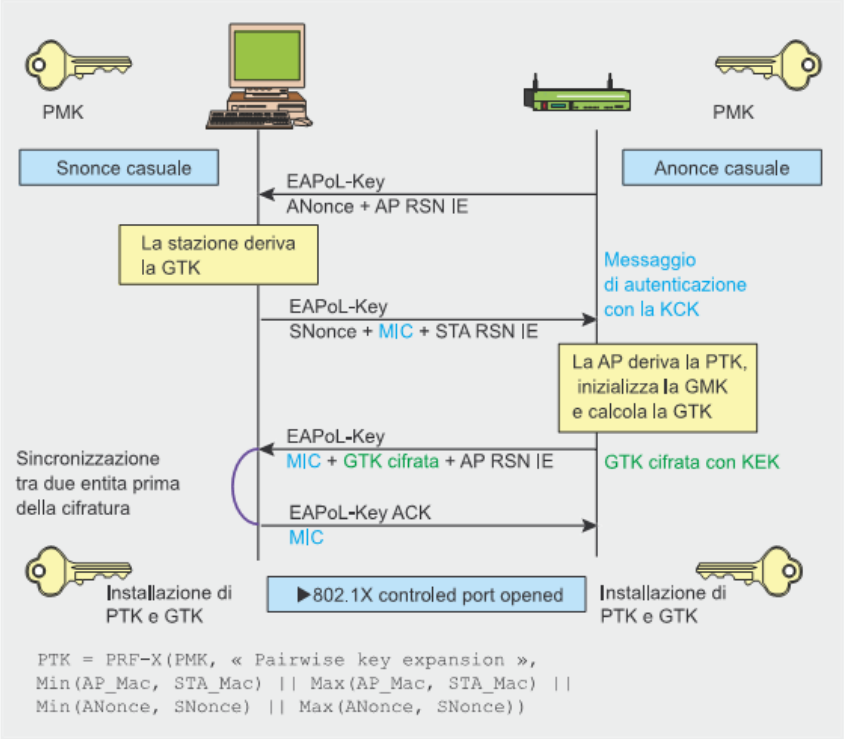


Figura 32: 802.11i - Terza fase Handshake a 4 vie

La PTK viene derivata dalla: PMK, una stringa fissa, l'indirizzo MAC del AP, l'indirizzo MAC del client e due numeri casuali (*ANonce* e *SNonce*, generati rispettivamente dall'autenticatore e dal

supplicant).

Di seguito le fasi:

- L'access point inizializza il primo messaggio selezionando il numero casuale *ANonce* e lo invia al supplicant, senza cifrare il messaggio o proteggendolo in alternativa.
- Il supplicant genera il proprio numero causale *SNonce* e adesso può calcolare una PTK e le chiavi di derivazione temporanee, quindi invia *SNonce* e la chiave MIC calcolata dal secondo messaggio usando la chiave KCK.
- Quando l'autenticatore riceve il secondo messaggio, può estrarre *SNonce* (perché il messaggio non è cifrato) e calcolare la PTK e le chiavi di derivazione temporanee. Adesso può verificare il valore della MIC nel secondo messaggio e essere sicuro che il supplicant conosca la PMK e che ha calcolato correttamente la PTK e le chiavi di derivazione temporanee.
- Il terzo messaggio inviato dall'autenticatore al supplicant contiene la GTK (cifrata con la chiave KEK), derivata da una GMK casuale e *GNonce*, insieme ad una MIC calcolata dal terzo messaggio usando la chiave KCK. Quando il supplicant riceve questo messaggio, la MIC viene controllata per essere sicuri che l'autenticatore conosca la PMK e ha calcolato correttamente la PTK e le chiavi di derivazione temporanee.
- L'ultimo messaggio riconosce il completamento dell'intera fase di handshake e indica che il supplicant installerà la chiave e iniziare la cifratura. Dopo la ricezione, l'autenticatore appena verificato il valore MIC installa le proprie chiavi.

A questo punto il dispositivo mobile e l'access point hanno ottenuto, calcolato e installato le chiavi di cifratura e adesso sono in grado di comunicare su un canale sicuro per traffico unicast e multicast.

Il traffico multicast è protetto da un'altra chiave, la GTK (*Group Transient Key*) generata da una chiave principale detta GMK (*Group Master Key*) composta dei seguenti elementi: una stringa fissa, l'indirizzo MAC del punto di accesso e un numero casuale *GNonce*. La lunghezza GTK dipende dal protocollo di cifratura da 256 bit per la TKIP e 128 bit per la CCMP.

La GTK si divide in diverse chiavi temporanee :

- GEK (*Group Encryption Key*): Chiave per la cifratura dei dati (usata da CCMP per l'autenticazione e la cifratura e dalla TKIP),
- GIK (*Group Integrity Key*): Chiave per l'autenticazione dei dati (usata solo da Michael con TKIP).

Durante il *Group Key Handshake v*engono scambiati due messaggi *EAPOL-Key* tra la STA e AP. Questo handshake fa uso di chiavi temporanee generate durante la fase di *handshake a 4 vie* (KCK e KEK).

La *Group Key Handshake* è richiesta solo per dissociare un host e per rigenerare la GTK su richiesta di un client. L'autenticatore inizializza il primo messaggio scegliendo il numero causale *GNonce* e calcolando una nuova GTK. Poi invia al supplicant la GTK cifrata (usando KEK), il numero di sequenza GTK e la MIC calcolata da questo messaggio usando KCK. Quando il supplicant riceve il messaggio, la MIC viene verificata e la GTK può essere decifrata.

Il secondo messaggio riconosce il completamento della *Group Key Handshake* inviando un numero di sequenza GTK e la MIC calcolata su questo secondo messaggio. Dopo la ricezione, l'autenticatore installa la nuova GTK (dopo aver verificato il valore MIC).

Esiste anche una fase *STAkey Handshake* la quale supporta la creazione da parte del punto di accesso di chiavi segrete di tipo *transient* chiamate *STAkey* per le connessioni ad-hoc. Di questa fase non saranno illustrati i particolari di funzionamento.

Fase 4: Segretezza e integrità dei dati RSNA

Tutte le chiavi generate in precedenza sono usate nei protocolli che supportano la segretezza e l'integrità dei dati RSNA:

- TKIP (*Temporal Key Hash*),
- CCMP (*Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol*),
- WRAP (*Wireless Robust Authenticated Protocol*): attualmente non usato.

Prima di analizzare in dettaglio questi protocolli dobbiamo capire un concetto importante: la differenza che passa tra un MSDU (*MAC Service Data Unit*) e un MPDU (*MAC Protocol Data Unit*). Entrambi si riferiscono ad un singolo pacchetto di dati, ma il MSDU rappresenta anche i dati prima della frammentazione, mentre i MPDU sono unità di dati multipli dopo la frammentazione. La differenza è importante nella cifratura TKIP e CCMP, dal momento che in TKIP la MIC viene calcolata dal MSDU, mentre nel CCMP viene calcolata dal MPDU.

TKIP

Proprio come WEP, la TKIP si basa sull'algoritmo di cifratura RC4, ma esiste per una sola ragione: per permettere ai sistemi WEP di essere aggiornati e implementare protocolli più sicuri. La TKIP è richiesta per la certificazione WPA ed è anche inserita nel RSN 802.11i come opzione facoltativa. La TKIP aggiunge anche misure correttive per tutte le vulnerabilità WEP descritte prima:

- integrità del messaggio: una nuova MIC (*Message Integrity Protocol*) chiamata Michael che può essere implementata nei software che girano su microprocessori lenti,
- IV: una nuova selezione di regole per i valori IV, re-utilizzando il vettore IV come contatore replay (TSC, o *TKIP Sequence Counter*) e aumentando le dimensioni del vettore IV per evitare il riutilizzo,

- funzione *Per Packet Key Mixing*: per generare chiavi di cifratura apparentemente non legate,
- gestione chiave: nuovo meccanismo per la distribuzione e la modifica delle chiavi.

Il modello TKIP Key-Mixing si divide in due fasi:

- *La Fase 1 riguardante i dati statici:* la chiave di sessione segreta TEK, l'indirizzo trasmettitore MAC TA (per prevenire le collisioni tra vettori IV) e i 32 bit più alti del vettore IV.
- *La Fase 2:* dipende dall'output della Fase 1 e comprende i 16 bit più bassi del vettore IV, modificando tutti i bit del campo *Per Packet Key* per ogni nuovo IV. Il valore IV inizia sempre con il valore zero ed è aumentato di uno per ogni pacchetto inviato, con il rifiuto di qualsiasi messaggio il cui TSC non è più grande dell'ultimo messaggio. L'output della *Fase 2* e parte del IV esteso (più un byte di prova) sono l'input per la RC4, generando un keystream con un operatore XOR con un MPDU in formato testo, la MIC calcolata dalla MPDU e il vecchio ICV di WEP .

Il calcolo MIC utilizza l'algoritmo Michael di Niels Ferguson, creato per la TKIP ed ha un livello di sicurezza di 20bit (l'algoritmo non usa la moltiplicazione per ragioni di prestazione, poiché deve essere supportato da hardware wireless di vecchia generazione e deve essere aggiornato per il WPA).

A causa di questi limiti, sono necessarie contromisure per evitare alterazioni della MIC. Sono tollerati al massimo due guasti del MIC, superato questo limite viene applicato un blackout di *60s* e le nuove chiavi (GTK e PTK) devono essere stabilite in un secondo momento.

Micheal calcola un valore di controllo di 8 ottetti chiamato MIC e lo aggiunge al MSDU prima della trasmissione. La MIC viene calcolato basandosi sui seguenti elementi: indirizzo di origine (SA), indirizzo di destinazione (DA), MSDU in testo chiaro e la TMK appropriata (a seconda dei casi, viene usata una chiave diversa per la trasmissione e la ricezione).

CCMP

Il CCMP si basa sulla suite dei cifrario a blocco AES (*Advanced Encryption Standard*) in modalità CCM con le chiavi e i blocchi di 128 bit. AES è per CCMP quello che RC4 è per TKIP, ma al contrario di TKIP che era stato creato per accogliere l'hardware WEP esistente, CCMP non è un ibrido bensì un nuovo protocollo. Il CCMP utilizza una modalità combinato ad un messaggio di autenticazione detto *Cipher Block Chaining* (CBC-MAC) per produrre una MIC.

Esso aggiunge altre funzionalità interessanti, come l'uso di una singola chiave per la cifratura e l'autenticazione (con diversi vettori di inizializzazione) o che si occupavano dati non cifrati dall'autenticazione. Il protocollo CCMP aggiunge 16 byte alla MPDU: 8 byte per l'intestazione CCMP e 8 byte per la MIC. L'intestazione CCMP è un campo non cifrato incluso tra l'intestazione MAC e i dati cifrati, inclusi il PN di 48 bit (*Packet Number* = IV esteso) e il *Group Key KeyID*. La PN viene aumentata di uno per ogni MPDU successivo.

Il calcolo MIC utilizza l'algoritmo CBC-MAC che cripta il blocco nonce (calcolato dai campi *Priority*, MPDU indirizzo di origine e il PN aumentato) e i blocchi XOR successivi per ottenere una MIC finale di 64 bit (la MIC finale è un blocco di 128 bit, dal momento che i 64 bit più bassi sono rifiutati). La MIC viene poi aggiunta ai dati in testo semplice per la cifratura AES in modalità contatore. Il contatore è costruito da un *nonce* simile a quello della MIC, ma con in più un campo contatore inizializzato a uno che viene incrementato per ogni blocco.

2.2.4 Standard IEEE 802.11i: Preautenticazione e Key Caching

IEEE 802.1x è uno standard IEEE basato sul controllo delle porte di accesso alla rete LAN, MAN. Questo standard provvede si autenticare e autorizzare i dispositivi collegati a switch e access point stabilendo un collegamento punto a punto e prevenendo collegamenti non autorizzati alla rete locale. Viene utilizzato dalle reti locali wireless per gestire le connessioni agli AP e si basa sul protocollo EAP, Extensible Authentication Protocol *(RFC-2284)*.

Normalmente, l'autenticazione è fatta da una terza parte, come un server RADIUS(Remote Access Dial-In User Service) . Questo fornisce l'autenticazione del client o l'autenticazione forte mutua.

Questo standard è composto dai seguenti elementi:

- *Supplicant:* il client che richiede di essere autenticato.
- *Authenticator:* il dispositivo che esegue l'inoltro della richiesta di accesso.
- *Authentication Server (o backend authentication server):* il dispositivo che effettua il controllo sulle credenziali di accesso del supplicant ed autorizza l'accesso.

Lo standard 802.1x non definisce un metodo preciso ma uno schema architetturale nel quale possono essere usate varie metodologie, per questo una delle sue caratteristiche fondamentali è la versatilità. Fin dalla sua ratifica, 802.1x è divenuto il framework di autenticazione delle wireless LAN. La sua rapida diffusione è stata dovuta, in larga parte, alla possibilità di utilizzo di standard precedentemente accettati, principalmente EAP (Extensible Authentication Protocol). Il controllo degli accessi alla rete basato sulle porte fa uso delle caratteristiche di accesso fisico alle infrastrutture LAN basate sugli standard IEEE 802, allo scopo di fornire autenticazione e autorizzazione tramite dispositivi connessi a una porta della LAN che abbia caratteristiche di connessione punto-punto, e prevenzione dell'accesso a tale porta nel caso in cui autenticazione ed autorizzazione falliscono. Una porta, in questo contesto, è un singolo punto di accesso all'infrastruttura della LAN. La specifica 802.1x definisce il passaggio dell'autenticazione tra il client wireless(supplicant), un access point wireless(autenticatore) e un server di autenticazione di tipo RADIUS(Remote Authentication Dial-In User Service). Il client wireless viene autenticato dal server RADIUS, e l'access point gioca un ruolo di intermediario.

Segue una breve descrizione delle fasi di autenticazione 802.1X:

1. Quando un nuovo nodo wireless (STA) richiede l'accesso alle risorse di una LAN, l'access point (AP) ne richiede l'identità. Nessun altro tipo di traffico è consentito oltre a EAP, prima che il nodo sia autenticato (la "porta" è chiusa). Il nodo wireless che richiede l'autenticazione è spesso denominato *supplicant*, tuttavia sarebbe più corretto dire che esso contiene un supplicant. Il supplicant ha il compito di fornire risposte all'autenticatore che ne verificherà le credenziali. L'autenticatore non è l'access point, ma può essere un programma che gira sul AP o può essere un componente esterno. Viene utilizzato il mascheramento dell'identità, la quale non viene inviata finché non è instaurato un tunnel TLS criptato.
2. Dopo l'invio dell'identità, comincia il processo di autenticazione. Il protocollo utilizzato tra il supplicant e l'autenticatore è EAP, o, più correttamente, EAP incapsulato su LAN (EAPOL). L'autenticatore re-incapsula i messaggi EAP in formato RADIUS, e li passa al server di autenticazione. Durante l'autenticazione, l'autenticatore ritarda i pacchetti tra il supplicant e il server di autenticazione. Quando il processo di autenticazione si conclude, il server di autenticazione invia un messaggio di successo (o di fallimento, se l'autenticazione fallisce) e l'autenticatore di conseguenza apre la "porta" al supplicant.
3. Se l'autenticazione andata a buon fine, viene garantito al supplicant l'accesso alle altre risorse della LAN e/o ad Internet.

Standard IEEE 802.1X: Preautenticazione

Il sistema di autenticazione basato su certificati, è caratterizzato da un alto numero di round-trips di comunicazione dieci volte superiore al quello normalmente richiesto. Dalla letteratura emerge che se usato un backend authentication server questo ritardo alla prima autenticazione è stimabile sui *100ms*. Anche se è possibile ridurre le comunicazioni per l'autenticazione attraverso "fast reconnect", se il backend authentication server è situato lontano dall'Authenticator la latenza di comunicazione può restare rilevante.

Quando una rete è autenticata attraverso 802.1X, la maggior parte del tempo è utilizzato per ottenere l'abilitazione ad inviare pacchetti di autenticazione 802.1X, specialmente se si adopera il metodo EAP che è caratterizzato dallo scambio di un alto numero frame. Il processo di preautenticazione mostrato nella figura X, consente ad una stazione mobile (STA) di stabilire una comunicazione sicura con il nuovo AP prima che ci si associ. Essenzialmente la preautenticazione disaccoppia le procedure d'associazione e di sicurezza consentendo di essere eseguite indipendentemente l'una dall'altra. Il processo di autenticazione non prevede l'utilizzo del protocollo WPA per criptare la comunicazione tra i componenti.

IEEE 802.1X: Macchina a Stati della Preautenticazione

La *macchina a stati* del processo di preautenticazione 802.1X presenta alcune sostanziali differenze rispetto quella presentata nello standard IEEE 802.11 *[par.1.5]*.

All'interno di una RSN, i frame dello standard IEEE 802.11 di autenticazione non sono usati. Piuttosto, l'autenticazione è compiuta tramite la trasmissione e la ricezione delle strutture dello IEEE 802.1X. Per esempio, con la preautenticazione IEEE 802.1X, l'authenticator PAE controlla il movimento dallo Stato1 (unauthenticated, unassociated) allo Stato2 (autenticated, unassociated), basato sul risultato dell'istituzione delle chiave e dell'autenticazione.

Evidenziamo i frame caratteristici della preautenticazione 802.1X con riferimento alla *macchina a stati* descritta nello standard IEEE 802.1X:

Classe1

Management frames

- *Deauthentication*

  All'interno di una RSN, i messaggi di deautenticazione sono autenticati usando il materiale chiave derivato durante l'autenticazione dello IEEE 802.1X. Mentre per default una stazione RSN-enabled dovrebbe scartare i messaggi di deautenticazione che sono non sono autenticati o che falliscono l'autenticazione. Una stazione appartenente ad una RSN, se appositamente configurata, può processare messaggi di deautenticazione non autenticati. Poiché questo espone la stazione ad attacchi DOS basati sullo spoofing di messaggi di deautenticazione, questa possibilità dove essere concessa con cautela.

Classe2

Management frames

- Association request/response

  All'interno di una RSN, i messaggi di richiesta e di risposta di associazione devono essere autenticati ed l'integrità deve essere protetta usando le chiavi ottenute durante l'autenticazione 802.1X. Quando un sistema RSN è abilitato, le stazioni devono scartare la richiesta di associazione o i messaggi di risposta non autenticati, o che falliscono l'autenticazione

- Reassociation request/response

  All'interno di una RSN, i messaggi di riassociazione di richiesta e di risposta devono essere autenticati e l'integrità deve essere protetta usando le chiavi ottenute durante l'autenticazione 802.1X. Quando un sistema RSN è abilitato, le stazioni devono scartare la richiesta di riassociazione o i messaggi di risposta non autenticati, o che falliscono.

Classe3

Data frames

- Data subtypes: Sono abilitati all'utilizzo i Data frames . Entrambi i campi “To DS” or “From DS” del FC(Frame Control) sono posti a *true* per utilizzare il DSS(Distribution System Service). I data frame del IEEE 802.1X con entrambi i campi “To DS” or “From DS” del FC posti a *true* sono classificati come frame di Classe 3. Questi frame devono avere il campo WEP di FC posto a *true*.

IEEE 802.1X: Fasi Operazione Preautenticazione

Analizziamo le fasi che caratterizzano la procedura di preautenticazione:

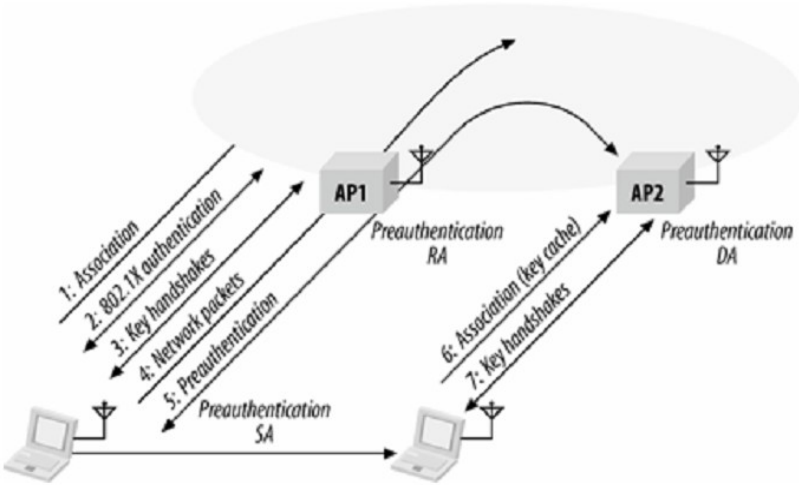


Figura 33: Fasi preautenticazione IEEE 802.1X

1. **Association:** La stazione mobile si associa al primo AP che trova nella rete. La scelta del AP dipende dai criteri presenti all'interno del suo firmware*(vendor dependent)*.
2. **802.1X authentication:** Una volta associata, la STA può effettuare un'autenticazione 802.1X. Questo punto utilizzerà i frame EAPOL, i quali sono convertiti in pacchetti RADIUS dal AP e la sessione è autenticata.
3. **Key handshake:** Le chiavi dinamiche per i radio link sono ottenute da entrambi i lati: le *pairwise keys* attraverso *four-way handshake* e le *group keys* attraverso il *group key handshake.*
4. **Network packets:** Con le chiavi configurate, la stazione è abilitata a trasmettere e ricevere i pacchetti di protocollo di rete. Il software della stazione controlla il comportamento del roaming e può usarlo a proprio vantaggio. Mentre la stazione si muove verso AP2 può effettuare la preautenticazione per accelerare il processo di spostamento su AP2. L'uso della

preautenticazione riduce l'interruzione fra la trasmissione dei pacchetti nella rete, evitando così un passaggio brusco tra AP.

5. **Preauthentication:** La preautenticazione comincia con un messaggio EAPOL-Start trasmesso dalla stazione al nuovo AP. Una stazione può essere associata soltanto con un singolo AP, ed i frame di preautenticazione sono incanalati attraverso il vecchio AP.

   La fase si preautenticazione è uno scambio completo 802.1X:

   a. L'indirizzo del mittente dei frame è la stazione, l'indirizzo del ricevente è il BSSID relativo al AP corrente (in questo caso, l'indirizzo MAC dell'interfaccia wireless di AP1) e l'indirizzo di destinazione è il BSSID del nuovo AP (in questo caso, interfaccia wireless di AP2).

   b. Una volta ricevuti da AP1, i frame sono trasmessi tramite il sistema di distribuzione (DS) verso AP2. L'access point ha soltanto un MAC address. Se i due AP non sono collegati direttamente allo stesso dominio Ethernet, devono avere un metodo alternativo di muovere i frame di preautenticazione avanti e indietro fra i dispositivi.

   c. Durante questo intero passo, la stazione resta associata ad AP1 e può trasmettere e ricevere i pacchetti della rete attraverso il relativo collegamento cifrato esistente.

   d. Il risultato del preautenticazione è la creazione di un contesto di sicurezza con AP2. La stazione e AP2 hanno ottenuto la pairwise master key, che può essere ulteriormente utilizzata per generare le chiavi per la stazione e AP2. Sia la stazione che AP salvano la pairwise master key in una key cache.

6. **Association (key cache):** L'associazione è spostata verso AP2. Come componente dell'associazione iniziale, la stazione include una copia della sua *key cache* per comunicare ad AP2 che già sia stata autenticata.

7. **Key handshake:** AP2 riceve la richiesta di autenticazione e cerca la chiave all'interno della key cache. Appena trovata una entry corrispondente, inizia immediatamente il *fourway pairwise key handshake*. Effettuando le operazioni necessarie per determinare la chiave, la stazione non può trasmettere e ricevere i pacchetti soltanto per un breve intervallo di tempo.

La preautenticazione IEEE 802.11 spalma il tempo richiesto da una autenticazione di tipo IEEE 802.1X EAP tramite un'esecuzione in parallelo della trasmissione e della ricezione di frame su una connessione autenticata. La prima associazione sarà lenta perché è richiesto di eseguire tutte le fasi richieste dal processo EAP.

Grazie alla preautenticazione le associazioni successive potranno essere caratterizzate da una ridurre drammaticamente i tempi di handoff.

Preautenticazione 802.1X: Considerazioni

Il tempo disponibile per la preautenticazione dipende dal grado della sovrapposizione delle zone di copertura degli AP come pure la velocità della STA. Un esempio di roaming di una stazione mobile (STA) è indicato in Figura 34. Nell'esempio, la STA si muove a velocità *v* e sta passando dall'associazione con il AP-A ad un'associazione con il AP-B. Altri parametri presenti nella figura sono: la sovrapposizione delle zone di copertura degli AP (di dimensione *c*), il diametro di delle singole aree di copertura è *D* ed il tempo di reassociation roundtrip è RTT.

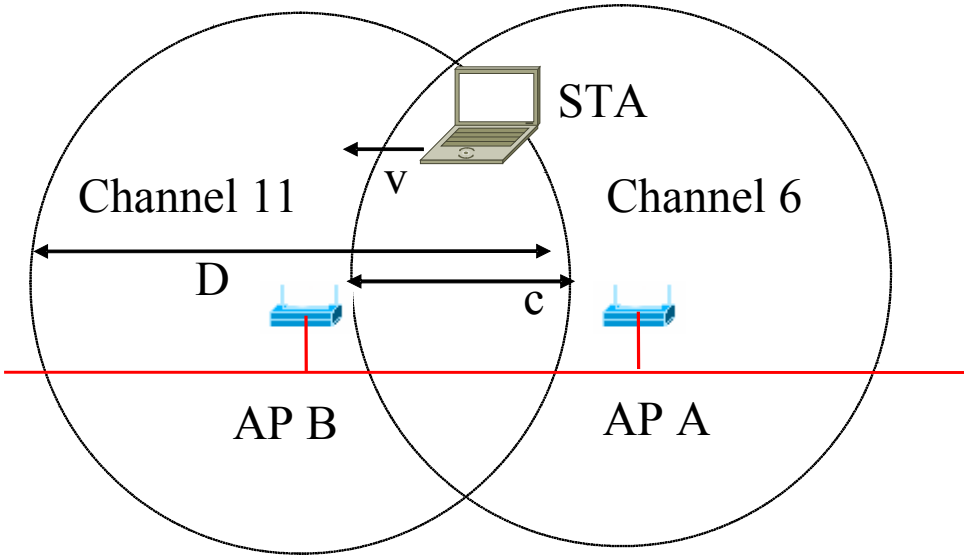


Figura 34: A roaming station

Dato i parametri descritti nella figura 34, se la STA tenta di preautenticarsi all'access point AP-B mentre è associato all'access point AP-A, le operazioni di preautenticazione devono essere completate entro il lasso di tempo ΔT uguale o minore di c/v per evitare la perdita della connettività.

Generalmente, dove il *"fast reconnection"* è sopportato, è richiesta una zona di sovrapposizione delle aree di copertura dei due AP coinvolti di dimensione ridotta rispetto la media, per consentire alla preautenticazione di terminare in tempo. Questo a condizione che la STA si muova ad una velocità paragonabile a quella di un essere umano a piedi o in bicicletta.

Per concludere, incontriamo un limite superiore per velocità, oltre cui le reti IEEE 802.11 non possono funzionare correttamente, anche senza l'uso di autenticazione. La riassociazione deve essere completata in un intervallo di tempo (RTT) minore di che D/v; altrimenti, la STA lascerà la zona di copertura prima che la riassociazione possa essere completata.

2.3 Layer2 Roaming: Inter Access Point Protocol (IAPP)

Lo standard IEEE 802.11f*[3]*, anche noto come IAPP o Inter Access Point Protocol (IAPP). Questo standard definisce il processo di handover che abilita gli utenti a muoversi in maniera trasparente tra access point diversi, consentendo quindi la realizzazione di installazioni "multi-vendor" laddove però tutti i produttori siano conformi allo standard.

Un ESS è un insieme di BSS, dove gli AP comunicano tra di loro attraverso il Distribution System (DS), agevolando lo spostamento delle STA tra BSS. L'idea è quella di definire una raccomandazione "pratica" per l'implementazione di un Inter-Access Point Protocol(IAPP) su un Distribution System(DS) su wireless LAN (WLAN).

2.3.1 Descrizione del sistema

La struttura prevede la presenza dell'entità APME (AP Management Entity). Nello standard con la sigla APME ci si riferisce ad una funzione esterna allo IAPP, comunque probabilmente ancora una funzione del dispositivo di AP. Tipicamente, questa entità dell'amministrazione è il programma operativo principale del AP, che implementa le caratteristiche riservate e le procedure del fornitore di AP ed incorpora l'entità dell'amministrazione della stazione (PMI) di 802.11. La Figura 35 descrive un'architettura tipica di un AP in cui lo IAPP funziona.

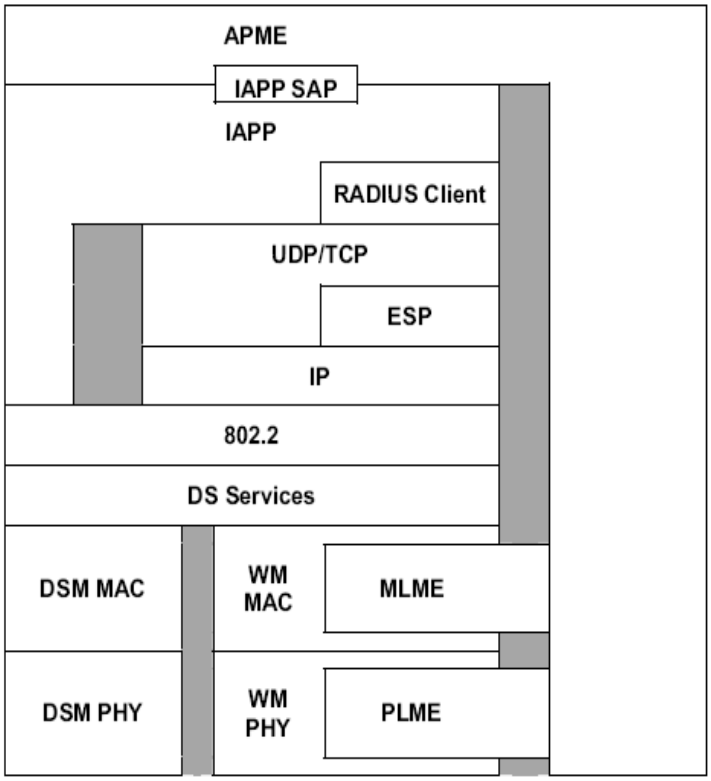


Figura 35: Architettura di un AP con supporto IAPP

Le zone grigie indicano le parti dove c'è un'assenza di collegamento fra i blocchi. I servizi di IAPP sono raggiunti dal APME tramite lo IAPP SAP. Le primitive di servizio di IAPP definite nello standard consente alla APME di interagire con lo IAPP affinché effettui una certa funzione o comunichi con un altro AP nel DS o con un RADIS server. Altre primitive di servizio indicano all'entità APME che alcune funzioni sono state effettuate da altri AP presenti nel DS e che può avere un effetto sulle informazioni locali al AP da lui gestito.

Le invocazioni delle primitive di servizio di qualche IAPP contano sul protocollo del RADIUS per effettuare determinate funzioni che sono richieste per il funzionamento corretto e sicuro del protocollo IAPP. In particolare, l'entità di IAPP deve poter trovare ed utilizzare un RADIUS server reperire l'indirizzo IP dell'altro AP all'interno della ESS fornendogli il valore BSSID del AP che si deve contattare(se è presente una possibilità locale per realizzare questo tipo di traduzione) e per ottenere le informazioni di sicurezza per proteggere il contenuto di determinati pacchetti di IAPP.

Riporto qui di seguito alcune caratteristiche del protocollo IAPP:

- IAPP è un protocollo di livello applicazione, appoggiato tipicamente su un multicast IP (chiuso nella distribution network), per supportare applicativi di gestione dell'ESS, ed attualmente lo standard prevede come gestione solamente l'handover.
- Lo standard 802.11f non è un protocollo di routing
- L'IAPP non tratta direttamente della consegna dei data frames 802.11 alle STA.

Il protocollo funziona presupponendo che le STA siano configurate in maniera tale da mantenere un indirizzo/indirizzi di rete validi quando si associano o riassociano non è compito di IAPP gestire gli indirizzi È in grado di costruire dinamicamente delle tabelle di AP fisicamente vicini.

L'inizializzazione del primo AP stabilisce la formazione di una ESS. I successivi AP interconnessi da un DS comune e che utilizzano lo stesso SSID, estendono la ESS creata dal primo IAPP può usare un server RADIUS per definire gli AP membri di una ESS.

Il protocollo IAPP supporta le seguenti funzioni:

- DS Services, come definito nello standard ISO/IEC 8802-11:1999.
- Corrispondenza degli indirizzi degli AP (il loro BSSID) e gli indirizzi del livello network del DS (Indirizzi IP).
- Formazione di un DS.
- Mantenimento di un DS.
- Rafforzamento delle restrizioni dello standard ISO/IEC 8802-11:1999, secondo cui una STA può effettuare solo una associazione attiva alla volta.

- Trasferimento delle informazioni di contesto di una STA tra AP.

Il servizio di distribuzione di dati del DS funzionerà come voluto quando la STA mantiene un indirizzo di rete validi per il loro punto di collegamento alla rete, quando effettua operazioni di associazione o di riassociazione. La STA si deve accertare che il suo indirizzo di rete sia configurato in modo tale che le funzioni di routing della rete siano in grado di trasportare i pacchetti all'interno della rete(BBS) a cui è collegato. In caso negativo, la STA deve ottenere tali indirizzo, prima che tutto il traffico di rete possa essere trasportato all'interno della rete.

Una STA può ottenere un indirizzo IP locale in più modi:

- rinnovare a Dynamic Host Configuration Protocol (DHCP) lease per il suo indirizzo IP
- usare Mobile IP per ottenere un indirizzo IP locale.

Il protocollo relega alla STA l'uso della struttura di richiesta di riassociazione 802.11 quando si sposta da una AP ad un altro, per fornire i servizi più completi al AP usando IAPP. Quando una STA usa la richiesta di associazione dello standard 802.11, piuttosto che la richiesta di riassociazione, lo IAPP non può informare l'access point a cui era precedentemente collegato della nuova associazione. Ciò può provocare il mantenimento da parte del vecchio AP (indicato nel campo “Current AP” del frame di richiesta di riassociazione) del contesto per la STA che si è spostata verso una nuovo AP per un tempo maggiore di quanto strettamente necessario. Ciò può causare uno spreco di risorse eccessivo a parte del vecchio AP, così come limitare le capacità del protocollo IAPP di aiutare il rispetto del requisito di singola associazione attiva tra una STA ed un AP.
Una situazione che può causare problemi significativi in una WLAN è il funzionamento di un AP anche quando ha perso il collegamento al DS. Quando un AP continua ad accettare le associazioni senza un collegamento al DS, diventa un “buco nero” nella WLAN, dove la STA associata non può comunicare nessuna entità esterna al BSS del AP. Quando un AP perde il collegamento al DS, dovrebbe cessare di trasmettere i Beacon frame, dissociare tutte le stazioni collegate e cessare di rispondere alle richieste di tipo probe, all'autenticazione ed agli altri frame di richiesta di associazione.

Caratteristiche della ESS

Il protocollo IAPP è stato definito per fornire un meccanismo di handoff sicuro tra due AP di una STA, all'interno della stessa ESS. Il protocollo IAPP può utilizzare un registro RADIUS centrale per definire gli AP che compongono la rete ESS.

Descriviamo ora tre livelli di supporto per le reti ESS con l'utlizzo del protocollo IAPP:

- Livello 1: nessuna supporto di gestione o sicurezza;
- Livello 2: supporto per il mapping diniamico tra BSSID ed indirizzi IP ;
- Livello 3*:* supporto per crittografare delle comunicazioni ed autenticazione dei messaggi

IAPP.

Il supporto di *livello uno* può essere ottenuto configurando ogni AP della ESS con il mappatura del BSSID con gli indirizzi IP per tutti gli altri AP all'interno della ESS. Questa operazione è accettabile solo per ESS di piccole dimensioni. Molte ESS necessitano il *livello di supporto due o tre*, i quali si basano sul protocollo RADIUS. L'inclusione di questo protocollo richiede che il RADIUS server ed il client RADIUS AP sia configurato con la chiave condivisa e con tutti gli indirizzi IP. Questa operazione deve essere fatta prima che il primo AP inizi qualsiasi operazione. Ogni AP che agisce con RADIUS client deve avere una propria chiave segreta condivisa con il RADIUS Server, differente da ogni altro AP, per contenere il danno che potrebbe succedere da una situazione in cui è presente una unica chiave condivisa e questa viene compromessa.

Dal punto di vista del protocollo IAPP, il set di entry BSSID definisce i membri di una ESS:

a) BSSID,

b) RADIUS BSSID Secret (160 bits max length),

c) IP address or DNS name,

d) Cifratura supportata dal AP per la protezione delle comunicazioni tra IAPP.

2.3.2 Definizione dei servizi

L'entità IAPP fornisce i servizi ad un AP in cui risiede con lo IAPP SAP. SAP permette che l'entità di amministrazione del AP (APME) possa invocare i servizi di IAPP e ricevere indicazioni delle invocazioni di servizio provenienti da altri AP appartenente alla stessa ESS. Questa clausola definisce i servizi che sono disponibili a SAP.

Ci sono quattro tipi di primitive di servizio:

- richieste
- conferme
- indicazioni
- risposte

Riportiamo i principali servizi del protocollo IAPP:

- **IAPP-INITIATE.request:** Causa l'inizializzazione dell'entità IAPP da parte del AP, incluso le sue strutture dati, funzioni e protocollo.

Questa funzione è composta dei seguenti campi:

```
IAPP-INITIATE.request {
                        TCP Port,
                        UDP Port,
                        IP Address,
                        BSSID Secret
                        }
```

Il valore del campo BSSID Secret è usato per fornire integrità, autenticazione e confidenzialità del blocco di sicurezza tra RADIUS server e AP.

Quando questa primitiva viene ricevuta da un APME, l'azione intrapresa dalla entità IAPP dipende dal livello di servizio implementato:

- *livello 1:* non c'è uso di RADIUS
- *livelli 2 e 3:* l'entità IAPP invia un RADIUS Initiate-Request e riceve un RADIUS Initiate-Accept or Initiate-Reject. Se è ricevuto un Initiate-Accept l'entità IAPP inizializza le sue strutture dati, funzioni e protocolli, perdendo tutte le precedenti informazioni. La porta per il protocollo IAPP viene aperta in questa fase dall'entità IAPP. Altrimenti se viene ricevuto un Initiate-Reject il protocollo IAPP non parte.

- **IAPP-ADD.request:** Questa primitiva viene usata quando una STA si associa con un AP tramite un frame di richiesta di associazione del protocollo IEEE 802.11. La funzione IAPP-ADD.request ha un duplice scopo:
  - *Primo:* provocare l'aggiornamento delle tabelle di forwarding dei dispositivi di livello 2 (internetworking device, bridge, switch) prima la STA che si sta associando effettui una qualunque trasmissione, la quale potrebbe verificarsi in un periodo di tempo arbitrario dopo l'associazione.
  - *Secondo:* notificare agli AP all'interno del dominio di multicast la nuova associazione della STA, per permettere altri AP di cancellare le informazioni di contesto lasciate dagli STA che non si sono riassociati correttamente nel passaggio da un AP ad un altro.

Il pacchetto è composto dai seguenti campi:

```
IAPP-ADD.request {
                    MAC Address,
                    Sequence Number,
                    Timeout
                    }
```

La ricezione di questa primitiva può causare le seguenti azioni:

a) L' entità IAPP invia un frame di aggiornamento di livello due al Distribution System, indirizzate in modo tale da causare l'aggiornamento delle tabelle di forwarding dei dispositivi del livello due della rete in modo che tutto il traffico futuro da loro ricevuto sia diretto sulla porta su cui è stato ricevuto il frame di aggiornamento.

b) L'entità IAPP notifica agli AP presenti nel dominio locale di multicast del DS, dell'avvenuta associazione tra un AP e la STA inviando un pacchetto IAPP ADD-notify in IAPP IP multicast address (224.0.1.178, see RFC 1112:1989).

c) La funzione IAPP-ADD indica anche che tutte le cache entry riferite ad uno STA deve essere cancellata in quanto è avvenuta una nuova associazione.

- **IAPP-ADD.indication**

The IAPP-ADD.indication è utilizzato per indicare alla APME che l'associazione è stata stabilita tra uno STA e altro AP nel DS.

Il pacchetto è composto dai seguenti campi:

```
IAPP-ADD.indication {
                    MAC Address,
                    Sequence Number
                    }
```

- **IAPP-MOVE.request**

Questo primitiva è inviata dall'entità APME quando riceve un messaggio di tipo MLME-REASSOCIATE.indication dal MLME indicando che un dispositivo mobile si è riassociato al AP.

Il pacchetto è composto dai seguenti campi:

```
IAPP-MOVE.request {
                    MAC Address,
                    Sequence Number,
                    Old AP,
                    Context Block,
                    Timeout
                    }
```

Questa funzione tenterà di inviare un pacchetto IAPP-MOVE.notify al vecchio AP con il quale STA è stato associato precedentemente per notificagli la sua riassociazione con un nuovo AP.

Caso di utilizzo del proactive caching

Se l'entità APME utilizza il caching, deve prima controllare in contesto della STA nella IAPP

cache usando il MAC Address del dispositivo mobile. Se lo trova(cache hit), la primitiva IAPP-MOVE.request non deve essere inviata fino a quando non viene ricevuto un Reassociation Response frame del protocollo 802.11. Se il contesto del dispositivo mobile non è trovato nella cache(cache miss) l'entità APME deve inviare un IAPP-MOVE.request come previsto dallo standard. Comunque, il MAC Adress del vecchio AP, ottenuto attraverso il Reassociation Response frame del protocollo 802.11 è aggiunto al neighbor graph dell'entità APME.

- **IAPP-MOVE.response**

  Usata per mandare i contesti "rilevanti" residenti in un AP inviando questa primitiva ad un altro AP quando una STA si è riassociata con esso. Il contesto è definito *"rilevante"* per una STA come quegli elementi di informazione che altri standard 802.11 richiedono per spostati quando una STA si riassocia.

  Il pacchetto è composto dai seguenti campi:

```
IAPP-MOVE.response {
                    MAC Address,
                    Sequence Number,
                    AP Address,
                    Context Block,
                    Status
                    }
```

  Quando viene ricevuta questa primitiva, AP inoltra tutti i contesti *"relevanti"* relativi al dispositivo mobile che si è riassociato e lo stato del peer IAPP entity del AP con il quale STA è associato, inviando un pacchetto IAPP-MOVE.response. Tutti i contesti per la STA identificati dal parametro MAC Address possono essere scartato tramite la distribuzione di questa risposta.

- **IAPP-CACHE-NOTIFY.request**

  E' utilizzato dal APME quando il caching è abilitato e riceve un MLME-REASSOCIATE.indication o un MLME-ASSOCIATE.indication inviato dall'entità MLME, indicando che il dispositivo mobile si è riassociato o associato al AP .Il pacchetto è composto dai seguenti campi:

```
IAPP-CACHE-NOTIFY.request {
                    MAC Address,
                    Sequence Number,
                    Current AP,
                    Context Block,
                    ContextTimeout,
                    RequestTimeout,
                    }
```

Questa primitiva fa in modo l'entità IAPP invii un pacchetto IAPP CACHE-notify ad ogni AP appartenente al neighbor graph, che contiene gli AP vicini a quello in esame, richiedendo di includere il contesto nella cache. A questo pacchetto seguirà l'invio di una primitiva IAPP-CACHE-NOTIFY.indication.

La semantica di questa primitiva è la seguente:

```
IAPP-CACHE-NOTIFY.request {
                    MAC Address,
                    Sequence Number,
                    Current AP,
                    Context Block,
                    ContextTimeout,
                    RequestTimeout,
                    }
```

- **IAPP-CACHE-NOTIFY.confirm**

Questa primitiva di servizio, è usata per confermare che le azioni iniziate con il messaggio di IAPP-CACHE-NOTIFY.request sono terminate ed informa il APME dello stato di questa azione. Questo servizio viene anche generato dalla scadenza del tempo di timeout il cui valore specificato nel messaggio IAPP-CACHE-NOTIFY.request con il campo RequestTimeout.

La semantica di questa primitiva è la seguente:

```
IAPP-CACHE-NOTIFY.confirm {
                    MAC Address,
                    Sequence Number,
                    Status
                    }
```

Quando la primitiva viene ricevuta da un APME con lo stato avente valore:

- SUCCESSFUL, questo indica che tutti gli AP vicini rispondono con lo stato impostato a SUCCESSFUL nel CACHE-response packet, quindi il contesto della stazione presente nella cache è aggiornato e di conseguenza lo è anche il neighbor graph.
- STALE_CACHE, indica che APME deve cancellare la entry nella cache che si riferisce alla stazione indicata dal parametro MAC Address.
- TIMEOUT, indica che IAPP entity non può ricevere risposte dagli AP vicini prima che scada il tempo indicato dal parametro RequestTimeout presente nella primitiva IAPP-CACHE-NOTIFY.request.

- **IAPP-CACHE-NOTIFY.indication**

  E' usato per indicare che il pacchetto CACHE-notify è stato ricevuto dal AP da uno di quelli presenti nelle sue vicinanze. Il pacchetto IAPP-CACHE-NOTIFY.indication Contiene le informazioni di contesto della STA che deve essere aggiornato o aggiunto alle informazioni presenti nella cache degli AP vicini.

  La semantica di questa primitiva è la seguente:

```
IAPP-CACHE-NOTIFY.indication {
                    MAC Address,
                    Sequence Number,
                    Current AP,
                    Context Block,
                    Context Timeout
                    }
```

2.3.3 Analisi delle operazioni ed overview delle caratteristiche del protocollo

Il protocollo IAPP supporta tre sequenze di scambi di messaggi:

- invocando **IAPP-ADD.request [Association Phase]**: dopo che APME riceve una primitiva MLME-ASSOCIATE.indication.
- invocando **IAPP-MOVE.request [Reassociation Phase]**: dopo che APME riceve una primitiva MLME-REASSOCIATE.indication.
- invocando **IAPP-CACHE.request [Caching context for Fast Roaming]**: per far aggiungere il contesto nella cache degli AP componenti il neighbort graph, al fine di facilitare il fast roaming.

Descriveremo qui di seguito le principali caratteristiche di queste fasi.

a) **Fase di Associazione**

   Questo insieme di azioni compongono la fase di associazione della STA al AP scelto in base ai criteri presentati in precedenza *[Par.2.1.1]*. Analizziamo ora le fasi ed i sevizi coinvolti.

   Quando l'entità IAPP riceve una richiesta IAPP-ADD deve inviare un pacchetto IAPP-ADD.notify ed un Update frame a livello due della rete.

   Il pacchetto IAPP-ADD.notify è composto dei seguenti campi:

   - destinatario identificato da un indirizzo IP (IAPP IP multicast address)
   - indirizzo IP del mittente
   - MAC Address del AP

- message body composto a sua volta da: MAC Address della STA, Sequence Number per la richiesta di Associazione inviata dalla STA

Quando arriva questo messaggio, l'entità APME deve controllare la propria tabella delle associazioni e rimuovere l'entry nella tabella nel caso sia già presente ed è più vecchia di quella indicata nel pacchetto ADD-notify. Da notare è che questa operazione non è stata creata per modificare la learning table, ma per rimuovere la presenza di associazioni vecchie non più valide presenti nella tabella della APME. Infatti la learning table è aggiornata tramite il frame di Update del livello 2 della rete di cui riporto di seguito la struttura:

MAC DA	MAC SA	Length	DSAP	SSAP	Control	XID Information Field
Octets: 6	6	2	1	1	1	3

Tabella 15: Struttura del Update Frame

dove viene indicato con:

- MAC DA: broadcast MAC Address
- MAC SA: MAC Address della STA che si è appena associata o riassociata
- DSAP e SSAP: i campi SAP, destinazione e sorgente, sono posti entrambi a NULL
- Control e XID: le informazioni sono definite nello standard IEEE 802.2

b) Fase di Riassociazione

Qui di seguito presenteremo l'insieme di azioni compongono la fase di riassociazione della STA ad un AP, ed analizzeremo i sevizi coinvolti.

Quando una entità IAPP riceve un pacchetto IAPP-MOVE.response, deve rispondere con un pacchetto IAPP-MOVE.notify al vecchio AP a cui corrisponderà come risposta un pacchetto MOVE-response. Questo pacchetto trasporta il blocco del contesto per l'associazione della STA dal vecchio AP al nuovo AP.

Il pacchetto IAPP-MOVE.notify e MOVE-Response sono trasmessi in tramite una sessione TCP stabilita tra gli AP. L'indirizzo IP del vecchio AP è ottenuto mediante la mappatura del codice BSSID contenuto nel messaggio di riassociazione con il suo indirizzo IP.

Questa corrispondenza è effettuata tramite l'utilizzo di sessioni RADIUS (è sufficiente qualsiasi standard RADIUS server che supporta il servizio di Call Check) o sono informazioni configurate localmente al AP.

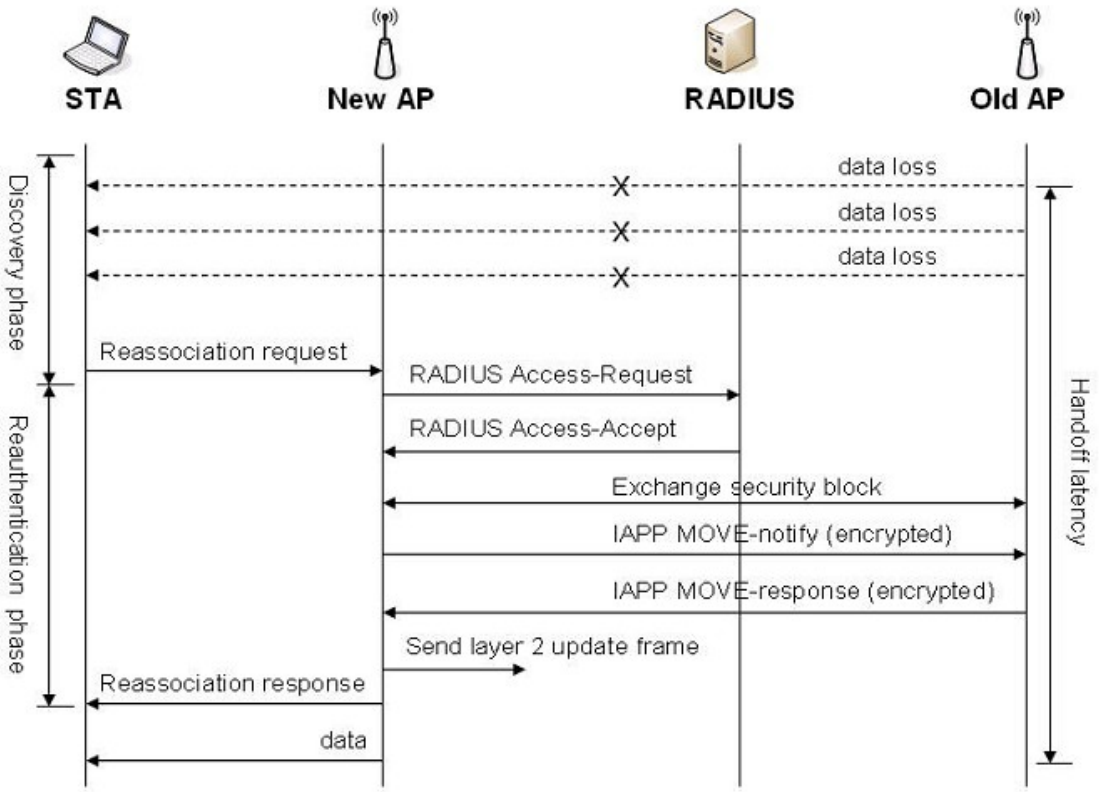


Figura 36: Scambio di messaggi sessione di Riassociazione IAPP

Per criptare il pacchetto IAPP-MOVE.response, nella risposta RADIUS diretta al nuovo AP dovrà includere oltre all'indirizzo IP del vecchio AP, i campi di risposta con i Security Blocks relativi al nuovo ed al vecchio AP.

Il Security Block contiene informazioni per la connessione sicura tra AP generate dinamicamente dal RADIUS server al momento della sua costruzione, ed è criptato usando i valori di BSSID user password del AP, contenuti nel RADIS registry.

Il nuovo AP invia il Security Block destinato al vecchio AP appena lo riceve del RADIUS Server, attraverso il pacchetto Send-Security-Block. Questo è il primo messaggio del protocollo IAPP nelle comunicazione tra access point eseguita utilizzando il protocollo TCP. Il vecchio AP risponde con un pacchetto Ack-Security-Block.

A questo punto entrambi gli AP hanno le informazioni per criptate i pacchetti che verranno scambiati durante le comunicazioni tra AP.

c) Metodo di Caching dei contesti, Fast Roaming

Il protocollo IAPP consente l'utilizzo di un metodo di caching dei contesti per consentire una velocizzazione della fase di Roaming. Analizziamo le fasi ed i sevizi coinvolti.

Quando un entità IAPP riceve un IAPP-CACHE-NOTIFY.request dal suo APME, deve inviare in contesto ricevuto a tutti gli AP appartenenti al neighboring graph, attraverso pacchetti

CACHE-notify. Quando ogni AP appartente al neighboring graph ricevono questo pacchetto, le loro APME generano in risposta un IAPP-CACHE-NOTIFY.indication, che porterà la APME del mittente ad aggiornare il contesto della STA presente nella cache aggiungendo o aggiornando l'entry corrispondente.

Efettuato questo aggiornamento ogni APME invierà alla propria IAPP entity un IAPP-CACHE-NOTIFY.response a cui seguirà l'invio del pacchetto CACHE.response al AP originale.

A sua volta l'entità IAPP del AP origiale invierà un messaggio IAPP-CACHE-NOTIFY.confirm al suo APME.

Nel caso in cui il pacchetto CACHE.response non è ricevuto da ogni AP appartenente al neighboring grafh, prima che il tempo di timeout scada (IAPP-CACHENOTIFY.request{RequestTimeout}), l'entità IAPP deve cancellare gli AP di cui non riceve risposta dal neighboring graph.

Da notare è che solo quando tutti gli AP appartenenti al neighboring graph non riescono a rispondere entro il tempo di timeout, l'entità IAPP dell'access point original invierà un IAPPCACHE-NOTIFY.confirm{Status=TIMEOUT} alla sua APME.

Nel caso in cui tutti i pacchetti CACHE.response sono ricevuti con stato STALE_CACHE, l'entità APME cancellerà l'entry corrispondente al contesto della stazione(STA) dalla cache locale.

2.3.4 Proactive caching

Proactive caching è un metodo che supporta il *fast roaming* attraverso il *caching del contesto* relativo dispositivo all'interno degli AP verso il quale si sposta. L'access point successivo a cui la STA si assocerà è identificato dinamicamente, senza bisogno di preconfigurazioni, tramite l'apprendimento delle identità degli AP presenti nelle vicinanze.

Il neighbor graph relativo ad un AP è un inseme di AP presenti nelle vicinanze nelle sue vicinanze. L'apprendimento automatico degli AP vicini attraverso le informazioni presenti nei frame di REASSOCIATION-REQUEST e di IAPP-MOVE.Request, permette di evitare l'overhead introdotto dalla gestione manuale della lista. L'access point può prevenire l'inserimento di un finto AP vicino selezionando solo quelli per cui il RADIUS Server ritorna un messaggio RADIUS Access-Accept.

L'implementazione esatta del grafo dipende dal produttore, ma è facilmente prevedibile l'utilizzo della cache con politica LRU(Least Recently Used) in presenza di fallimento di identificazione di una STA in procinto di spostarsi ma senza utilizzare il operazioni del protocollo IEEE 802.11 (ad esempio un portatile spento che si sposta). In questo caso la STA fallisce l'operazione di disassociazione e si

riassocierà ad un altro AP , il quale potrebbe non essere un vicino valido. Questo tipo di eventi possono succedere meno frequentemente quando gli handoff sono effettuati verso vicini validi e la cache LRU viene ripulita delle entry non valide del grafo. Per migliorare l'occupazione delle risorse richieste da questo metodo occorre fissare la grandezza del grafo. Un aspetto delicato di questo sistema è la consistenza della cache. La sua consistenza dipende dal contesto della STA e l'implementazione dell'entità APME deve garantire che le primitive IAPP-CACHE-NOTIFY.request siano emesse quando il contesto della STA, presente sul AP, subisce variazioni.

Riassunto dell'algoritmo

L'algoritmo di Proactive Caching può essere riassunto attraverso uno pseudo-linguaggio nel seguente modo:

Quando STA *c* si associa/riassocia ad AP

- se *context(c)* in cache:
  - inviare al client Reassociation Response
  - Inviare al vecchio AP Move-Notify
- se *context(c)* non in cache:
  - effettuare le normali operazioni IAPP
- Inviare il security context a tutti i *Vicini(i)*

Riporto qui di seguito lo schema riassuntivo dei messaggi IAPP:

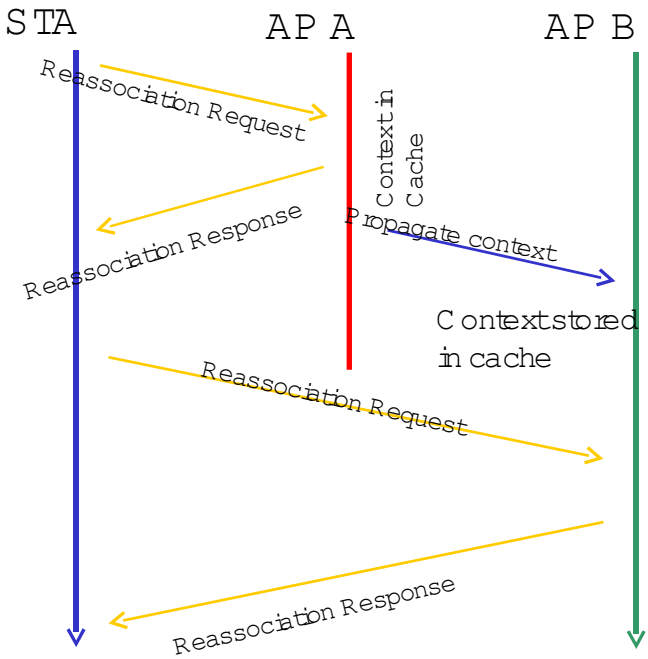


Figura 37: Messaggi IAPP con Procative Caching

Cap.3 Layer2 Roaming: Studio delle Prestazioni

3.1 Prestazioni della fase di Handoff

Originariamente il tecnologia WLAN era nata come soluzione al problema dell'eliminazione dei cavi di rete per LAN indoor, per questo il problema del handoff non è mai stato percepito come critico. Invece la diffusione e di vantaggi introdotti da servizi pubblici di Wi-Fi ed applicazioni multimediali (es.VoIP) hanno accentuato il problema del supporto alla fase di handoff tra access point, aspetto fino a qualche anno fa non pensabile[6], [7].

A causa dell'insufficiente supporto dello Standard IEEE 802.11, avviene una significativa interruzione della connessione alla rete durante la fase di handoff. La tabella in figura 38, mostra le misure di handoff delay, che fanno emergere come questi ritardi rendano impossibile il supporto ad applicazioni multimediali in reti IEEE 802.11.

AP / MH	Cisco			Soekris			Lucent		
	P	A	R	P	A	R	P	A	R
Lucent	37.2	3.08	5.07	196.9	1.77	1.77	81.2	0	1.73
Cisco	399.8	3.56	4.13	349.9	4.48	1.79	347.3	1.485	1.09
ZoomAir	195.6	2.403	8.84	191.3	2.37	1.77	347.5	0	3.085

Figura 38: Handoff delays in different vendors (unità: msec, P: Probe Delay, A: Authentication Delay, R: Reassociation Delay)

Di conseguenza, supportare fast handoff in reti di tipo IEEE 802.11 è diventato un problema fondamentale per fornire servizi mobili di tipo seamless*[Cap.2]*.

Attualmente, molti gruppi di lavoro del IEEE hanno tentato di migliorare e rendere più completo il protocollo IEEE 802.11, cioè, 11g per 2.4 gigahertz OFDM *[9]*, 11e per qualità di servizio (QoS)*[10]*, 11i per sicurezza*[6]*, 11f per il Inter-AP il Protocollo*[3]* e così *via[11]*. Per quanto riguarda il supporto di handoff, i gruppi di lavoro 11i e 11f hanno proposto parecchi schemi per supportare la sicurezza dei messaggio scambiati e per sostenere le comunicazioni fra il AP .

In questi anni molti studi sono stati intrapresi per migliorare le prestazioni di handoff nelle reti IEEE 802.11. Gli attuali schemi di fast handoff sono stati valutati tramite le simulazioni o misurazioni pratiche attraverso prove specifiche.

In questo paragrafo si vuole fornire un aggiornamento sullo stato dell'arte del progresso negli schemi di fast handoff per IEEE 802.11 reti e di valutare completamente i loro vantaggi e svantaggi.

Soluzioni senza modifiche allo standard

Analizziamo ora i principali fattori che influiscono sulle prestazione dell'operazione di handoff evidenziando solo soluzioni attinenti allo standard IEEE 802.11, che non ne prevedono modifiche o alterazioni.

La figura 39 illustra riassume il flusso di messaggi durante la fase di handoff. Il processo di handoff parte con l'invio del messaggio probe request e termina con il messaggio di reassociation response originato dal AP.

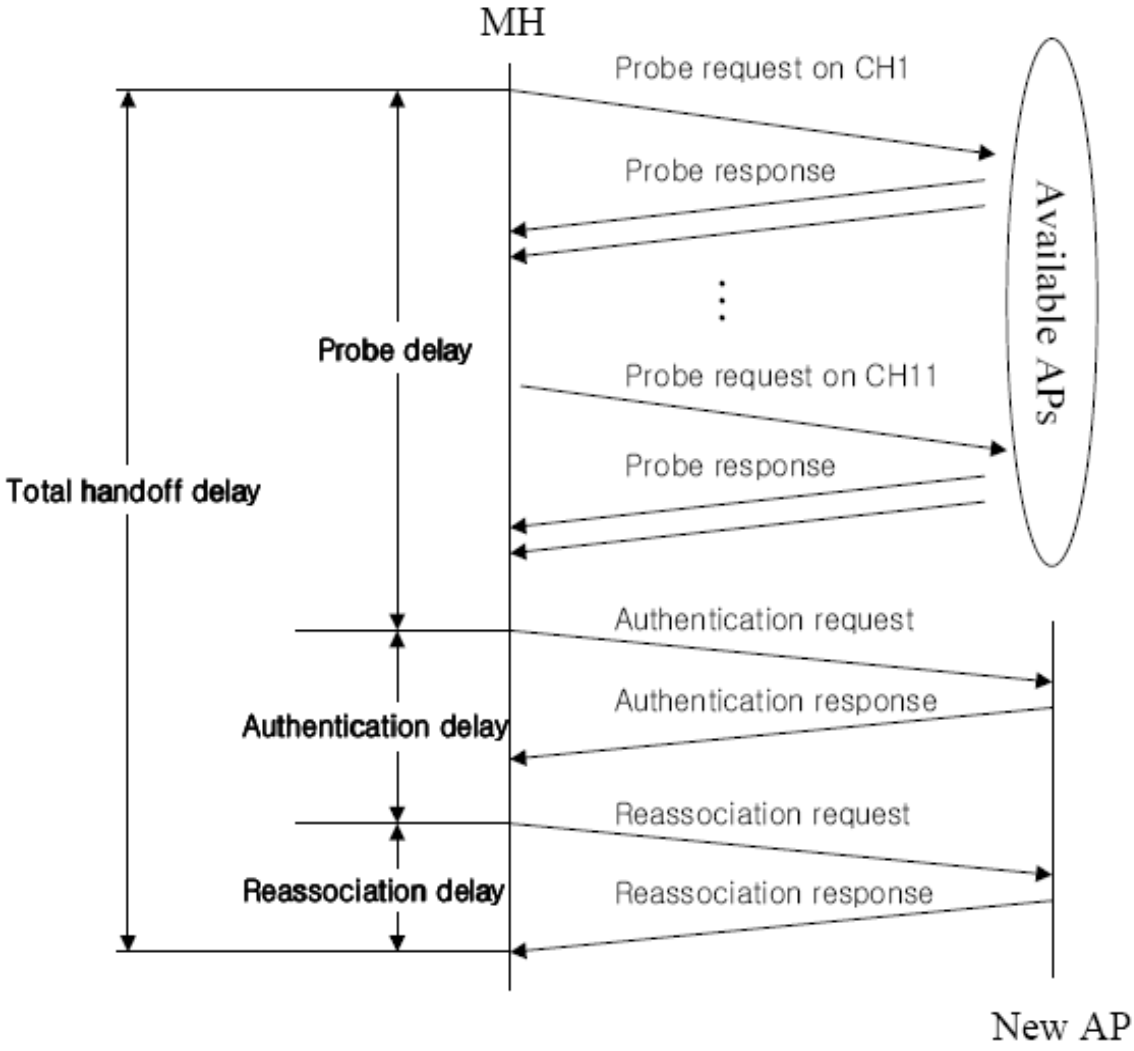


Figura 39: Hadoff: Flusso di messaggi

In questo schema sono anche indicate le tre tipologie di ritardo che caratterizzano handoff delay: *probe delay*, *authentication delay*, and *reassociation delay.*

A. Probe Delay

Il *probe delay* è dipendente dal tipo di scan mode usato(passivo o attivo):

- *Passivo:* Il ritardo medio nello *scanning* passivo può essere rappresentato come funzione dell'intervallo di beacon ed il numero di canali disponibili. Analizzando in dettaglio, se il beacon interval è *100 msec*, il ritardo medio *probe delays* dello standard IEEE 802.11b con 11 canali e lo standard IEEE 802.11a con 32 canali raggiunge i *1100 msec* and *3200 msec*, respettivamente. Da notare che il ritardo dovuto al passaggio tra un canale all'altro è trascurabile, approssimabile a *40-150 usec [12]*.
- Attivo: Il *probe delay* nel caso dell'utilizzo della modalità di *scanning attivo,* di cui riportiamo qui di seguito lo schema:

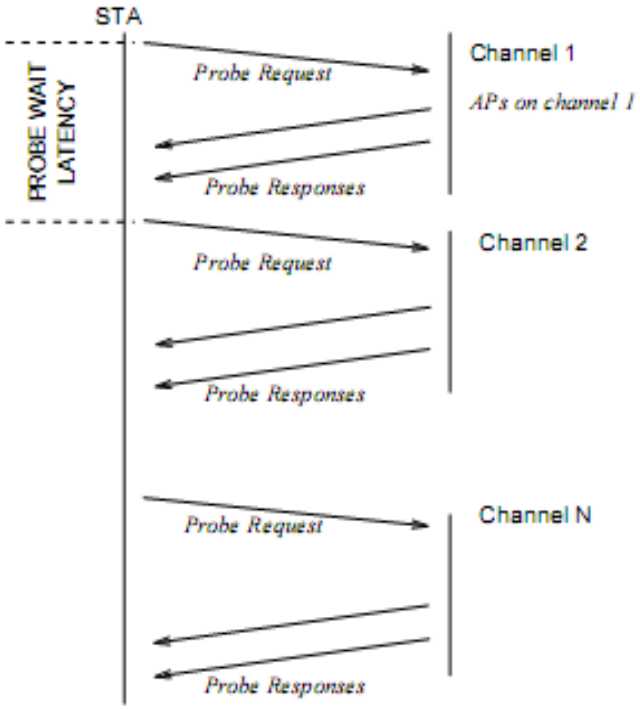


Figura 40: Schema di active scan

può essere determinato dei due valori *MinChannelTime* and *MaxChannelTime* values, i quali sono tipicamente device-dependent. L'attuale procedura di scanning richiede per una STA di effettuare lo scan di tutti i canali disponibili (11 channels for IEEE 802.11b and 32 channels for IEEE 802.11a).

Il probe delay, *TA*, nel caso in cui venga utilizzato lo *scanning attivo* può essere rappresentato come segue:

$$N \times MinChannelTime \leq T_A \leq N \times MaxChannelTime,$$

con *N*, numero di canali disponibili.

Il metodo più intuitivo per ridurre questo ritardo è ridurre il numero di canali da sondare, ad esempio focalizzando l'attenzione solo alcuni di essi. Un'altra soluzione è ridefinire i valori di *MinChannelTime* e *MaxChannelTime* in modo da ridurre i tempi di attesa.

B. Authentication Delay

In generale ci sono due modalità di autenticazione:

- *Open system authentication*: nella quale l'access point accetta qualsiasi dispositivo mobile senza effettuare alcuna operazione di autenticazione. Opzionalmente, può essere implementato il MAC address filtering ma questo non fa parte dello standard IEEE 802.11.

  Il delay introdotto dall'utilizzo di sistemi senza autenticazione è trascurabile e si avvicina a *1ms.*

- *Shared-key authentication*: si basa sul protocollo Wired Equivalent Privacy (WEP), il quale richiede che gli access point ed i dispositivi mobili implementino questo protocollo. La shared-key authentication richiede lo scambio di quattro messaggi*[Par.2.4]* riassunti qui di seguito:

  1) La STA manda una richiesta di autenticazione al AP inviando un messaggio Challenge-Request.
  2) AP invia un numero causale alla STA tramite un messaggio Challenge-Response.
  3) La STA firma questo numero causale usando il protocollo WEP, il quale è un pre-shared key, ed invia un messaggio di tipo Response di riposta al AP.
  4) Il AP verifica che il numero casuale sia stato validato con la chiave corretta.

     Se la chiave viene verificata poositivamente dal AP, autentica la STA e gli invia un un messaggio di tipo Approval.

L'authentication delay è proporzionale al numero di messaggi scambiati tra AP e STA. Di conseguenza risulta che l'autenticazione shared-key è caratterizzata da un alto tempo di delay rispetto all'autenticazione di tipo open-system.

L'utilizzo in reti IEEE 802.11 degli schemi di autenticazioni descritti nello standard IEEE 802.11i (es: IEEE 802.1x e EAP-TLS *[Par.2.2.3]*), richiede uno scambio alto di messaggi.

Nello studio*[13]* in cui viene analizzato l'impatto della dei meccanismi di sicurezza del protocollo

IEEE 802.11i applicato in una tipica struttura di rete aziendale. In queste sperimentazioni sono state usate le stazioni mobili riassunte nella seguente tabella:

Client Name	STA_1	STA_2	STA_3
Device Type	AMD Turion64, 1.8 GHz	PIII, Intel, 850 MHz	PocketPC, Intel, 400 MHz
OS	Windows XP	Ubuntu 6.06, Kernel 2.6.15	Windows Mobile 2003
WLAN Adapter	Internal, Ralink,11a/b/g	External, Proxim ORiNOCO 11a/b/g	External, SDIO, Go WiFi E300, b/g
WPA2 Software	wpa_supplicant v0.4.9, NDIS v5.1	wpa_supplicant v0.4.8, MadWiFi	Odyssey Client v4.05

Tabella 16: STA utilizzati nell'articolo[13]

e due modelli di AP: Prxim AP-4000(costo circa 300USD) ed il Linksys WRT54g(costo circa 60USD).

L'aspetto che rende particolarmente interessante questo articolo è l'utilizzo di palmari (PDA) nei test dei dispositivi mobili (STA3), contribuendo così ad approfondire lo stato dell'arte degli apparecchi mobili di ultima generazione in relazione al processo di roaming.

Le situazioni analizzate sono le seguenti:

L'accesso in un rete RSN . Come emerge dalla figura 41, la fase di scanning conferma il suo ruolo di maggiore fattore del handoff delay, eseguita dal dispositivo mobile STA3 in circa *6s.* Questa fase come già detto in precedenza è vendor dependent.

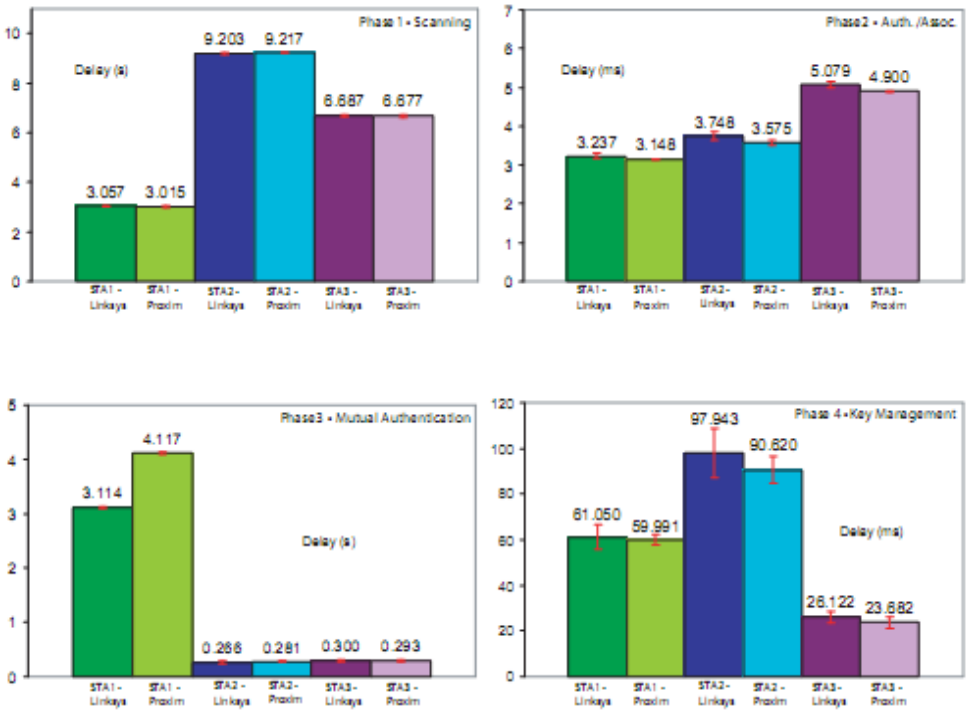


Figura 41: Accesso alla rete RSN: Latenza delle fasi

La fase di Autenticazione e di Associazione vengono svolta in media in *300ms*. Da osservare che il supplicant STA1 non risponde alla Identity Request fatta dagli AP. Questo lo porta a non rispettare pienamente lo standard 802.11i, con il conseguente rallentamento dell'esecuzione di queste fasi(ritardo di circa *4s*).

Handover in reti RSN. La fase di handoff viene effettuata con il supporto della Preautenticazione e del PMKSA Caching. Nella figura 42 la fase di scanning ha un impatto quasi nullo in quanto viene svolta in anticipo, appena le stazioni sono collegate nella rete. La STA3, ovvero il PDA, al momento richiede di rieffettuare la fase scanning ed essendo già connesso alla rete l'esecuzione di questa operazione scende da un tempo di circa *6s* a *1s*.

La *Mutual Authentication Phase* mostra come i dispositivi STA1 e STA2 acquistino vantaggio dall'utilizzo della Preautenticazione e del PMKSA Caching, mentre la STA3 come nel precedente scenario preso in analisi, continua ad eseguire questa fase in circa *300ms*. Emerge di invece che la fase di Key Management è obbligatoria per ogni connessione e che non è differente in modo significativo dai valori rilevati nel precedente scenario.

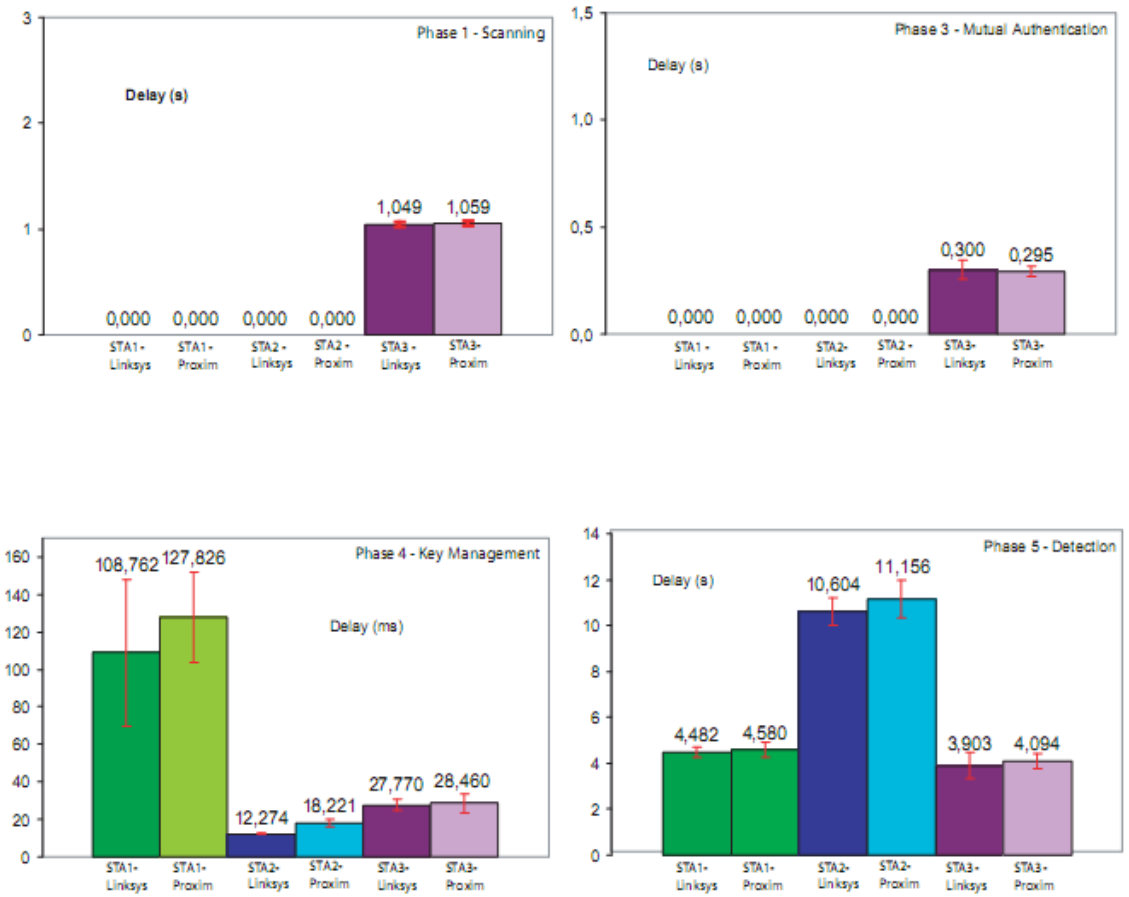


Figure 42: Latenza delle fasi handover in rete RSNSA

I risultati mostrano che in attesa delle nuove caratteristiche che saranno introdotte dal protocollo

802.11r, l'attuale processo di riconnessione alla rete richiede *172ms* per la STA *1,27ms* per la STA2 e circa *1.422s* nel caso di STA3. L'utilizzo della Preautenticazione e del PMKSA Caching permette di migliorare le prestazioni della STA1 e STA2 riducendo rispettivamente i delay a *110ms* e *19ms*.

Concludendo con l'utilizzo sempre crescente di WLAN per servizi pubblici il problema di ridurre l'authentication delay diventerà una delle maggiori sfide del settore.

C. Reassociation Delay

Il processo di riassociazione dovuto allo spostamento di una STA da un AP ad un altro all'interno di una Extended Service Set (ESS).

Il processo di riassociazione è molto simile a quello di associazione, infatti, una volta completata con successo l'autenticazione la STA invia una richiesta di riassociazione al AP il quale risponderà con un messaggio per comunicare il risultato dell'operazione(reassociation response frame) completando così il processo di handoff.

Nella backbone network, gli AP possono interagire tra loro per scambiarsi i frame relativi alla riassociazione. Nuove implementazioni potranno includere l'utilizzo inter-AP protocol (IAPP) *[Par.2.3.2]* che potrebbero aumentare il reassociation delay a causa dell'aumento dei messaggi scambiati. Questo aspetto sarà approfondito successivamente.

Fast Handoff: stato dell'arte

In questa sezione saranno presentati un certo numero schemi ideati per ridurre il handoff delay in IEEE 802.11 reti. Saranno suddivisi in due categorie: riduzione del probe delay e ridurre del ritardo nella fase di autenticazione/riassociazione. Si noti che le procedure di riassociazione e di autenticazione hanno funzionamenti simili e quindi consideriamo queste due procedure come una unica.

a. Reducing Probe Delay

A tele proposito gli studi*[14]* hanno analizzato in modo più approfondito *MinChannelTime* e *MaxChannelTime* evidenziandone le caratteristiche. Le prove di questo studio sono state effettuate su una rete IEEE 802.11b con il tempo di handover, uplink e downlink, bilanciati ad uno stesso valore e senza l'utilizzo di criteri di autenticazione.

MinChannelTime: Trascurando il tempo di propagazione ed il tempo di generazione del probe response il massimo tempo di risposta è rappresentabile come:

$$MinChannelTime \geq DIFS + (aCWmin \times aSlotTime)$$

Dove: *DIFS* Distributed InterFrame Space, *aCWmin* massimo numero di slot nella

aSlotTime lunghezza dello slot.

Qui di seguito sono indicati i valori relativi allo standard IEEE 802.11b

	IEEE 802.11b
aSlotTime	20 µs
aCWmin	31 slots
DIFS	50 µs

Il valore di MinChannnelTime ottimale emerso da questi studi di circa *1msec*.

MaxChannelTime: Dalle simulazioni è emerso che il tempo di trasmissione del probe response frame dipende dal numero di stazioni e dal carico di lavoro. Il valore di *MaxChannelTime* risulta non essere limitato finché può crescere il numero delle stazioni presenti all'interno della rete. Come risulta dalle sperimentazioni:

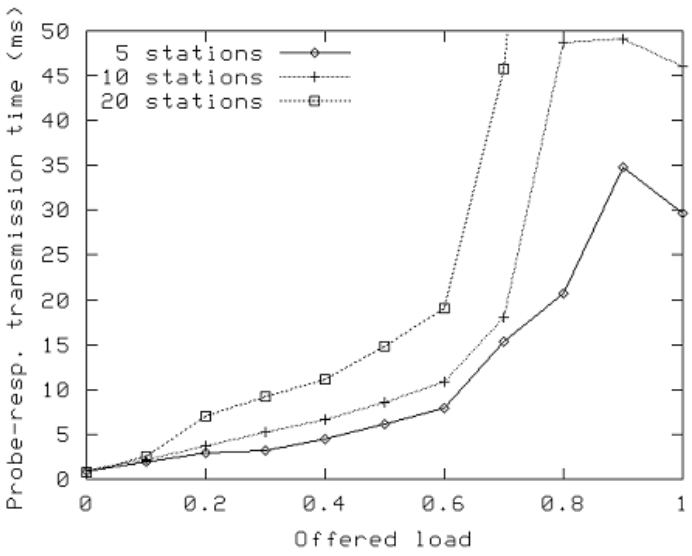


Figura 43: Tempo di trasmissione del Probe response (ms)

fino a dieci stazioni per cella si ottiene un buon valore di *throughput,* e mette in luce come valore ragionevole per MaxChannelTime *10ms.* E' importante mantenere questo valore piccolo per prevenire tempi lunghi tempi di ricerca in una rete con un alto numero di AP.

Un altro aspetto interessante di questo studio è l'attenzione che viene posta anche alla *detection phase* non limitando quindi l'analisi al solo caso di ricerca volontaria degli AP disponibili. *Detection phase*: Quando la fase di handoff inizia, la detection phase consiste nel messaggio di deassociazione mandato dal AP al dispositivo mobile *[fastest detection phase]*. La fase di handover presa normalmente in considerazione è quella iniziata dalla stazione mobile nel momento in cui rilevata una scarsa qualità qualità del segnale e conseguentemente una cattiva connettività. La maggiore difficoltà e capire la ragione del fallimento tra collisioni, segnale radio debole ed una serie di

trasmissioni senza successo. Le schede di rete presentano un diverso *detection time* dipendente dal numero di frame falliti permessi e dal numero di probe frame inviati. Dalle rilevazioni effettuate tre collisioni consecutive sono un evento molto raro anche in saturazione, di conseguenza se un frame e le sue ritrasmissioni consecutive falliscono, la STA può scartare le collisioni come causa di fallimento e passare alla *search phase*. Inoltre in particolari condizioni viene evidenziato come sia possibile ridurre il *beacon interval* dal valore tipico di *100ms* fino a *60ms* senza aumentare in modo sensibile la *bandwidth* utilizzata.

Il lavoro *[15]* ha presentato un metodo nuovo euristico usando un grafico del vicini (NG) ed il grafico di non-overlap (NOG). Questo schema (come nel citato *NG-pruning scheme)* focalizza l'attenzione sulla riduzione sia del numero totale di scanalature da sondare che del tempo di attesa su ogni scanalatura. Hanno suggerito due algoritmi: le procedure di NG-pruning e di NG. Il funzionamento di questi metodi si basa sull'accertare se una scanalatura deve essere sondata o no (dalla procedura di NG) e quando la STA deve attendere un po' di probe response message su uno specifico canale prima della scadenza di MaxChannelTime (algoritmo NG-pruning).

La NG astrae le relazioni di handoff tra AP adiacenti. Usando questo schema possono essere imparati l'insieme dei canali su cui gli AP vicini attualmente stanno funzionando e l'insieme degli AP vicini su ogni canale possono essere imparati. Sulla base di queste informazioni, una STA può determinare se un canale debba essere sondata oppure no. Il NOG astrae il rapporto di non-overlapping fra il AP. Due AP sono considerati come non sovrapponibili se e soltanto se la STA non può comunicare simultaneamente con entrambi con qualità accettabile di collegamento. Per esempio, se la distanza fra *APi* e *APj* è grande, una STA può associarsi con soltanto uno di loro. In questo caso, *APi* e *APj* sono non sovrapponibili. Di conseguenza, se la STA ha ricevuto un frame di tipo probe response dall'*APi*, implica che la STA non possa ricevere un frame di tipo probe response da APj per il principio di non sovrapponibilità. Per mezzo del NOG, la STA può eliminare gli AP che sono non sovrapponibili con il gruppo corrente di AP che già ha risposto.

La figura 44 illustra il funzionamento dello schema NG-pruning.

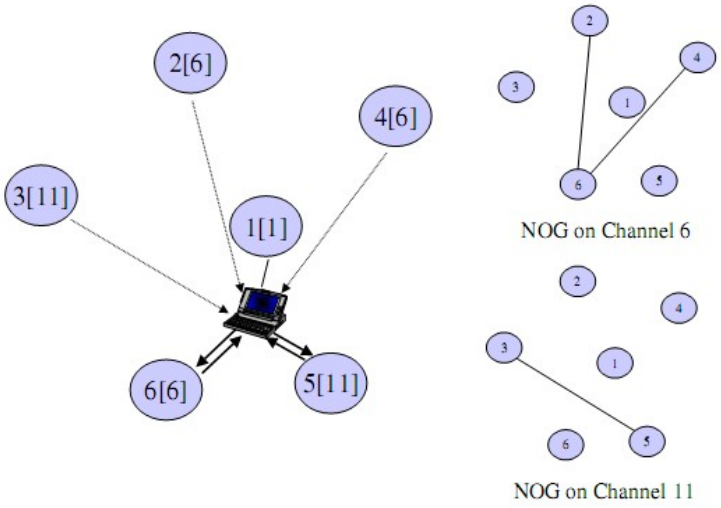


Figura 44: Schema di NG-pruning

I numeri presenti nei nodi rappresentano le informazioni sul vicino che possono essere acquisite tramite la costruzione dello schema NG. In questo esempio, soltanto tre le scanalature (cioè, 1, 6 e 11) sono utilizzate ed il AP corrente (AP1) ha cinque AP vicini (AP2-AP6). Usando queste informazioni, acquisite grazie allo schema NG, la STA sa che il numero di canali che deve sondare è appena due (cioè, scanalature 6 e 11). I diversi NOG sono costruiti su ogni canale, cioè, un NOG sul canale 6 e l'altro sul canale 11.

In primo luogo, supponiamo che la STA sondi il canale n.6. Quando riceve un messaggio di risposta della sonda da AP6, la STA decide che è inutile aspettare i messaggi di risposta supplementari della sonda sul canale 6. Questo perché AP6 è non sovrapponibile con AP2 e AP4 anche se utilizza il canale 6. Dopo il sondaggio del canale 6, la STA trasmette un messaggio di probe response sulla scanalatura 11. Allora, la STA riceve un messaggio di risposta della sonda da AP5 e smette di sondare su questo canale perché usando AP3 il canale 11 è non sovrapponibile con AP5.

In *[16]*, viene proposto un algoritmo di *selective scanning* con un meccanismo di caching (chimato *channel mask scheme*). Nel *channel mask scheme*, soltanto un sottoinsieme bene-selezionato di tutti i canali disponibili è sondato. La selezione dei canali è realizzata per mezzo di una channel mask che è sviluppata quando il driver è caricato dalla STA. Visto in dettaglio, viene prima effettuato un full-scan e la channel mask è costruita dalle informazioni ottenute. In IEEE 802.11b, soltanto tre canali non si sovrappongono fra tutti gli 11. Quindi, in una rete wireless configurata, conviene che tutti o la maggior parte degli AP utilizzino i canali 1, 6 e 11. Di conseguenza, la channel mask è costituita dalla combinazione dei tre canali più frequenti (cioè, 1, 6 e 11) ed i canali sondati dal primo full-scan.

Usando questa channel mask, una STA può ridurre la tempo che spende inutilmente sondando scanalature inesistenti fra gli AP vicini. Per ridurre ulteriormente handoff delay, è stato introdotto il meccanismo di caching. L'idea di base di caching che quella di registrare per ogni STA la relativa storia di handoff. Quando una STA si associa con un AP, questo è inserito nella cache mantenuta dalla STA. Quando si sta verificando un handoff, la STA effettua dei controlli preliminari nella cache per cercare una entry che corrisponde al MAC address relativo al AP. Se è trovata, la STA può associarsi con la AP senza effettuare le procedure di probe. Le figure X,X illustrano il funzionamento del *channel mask scheme*.

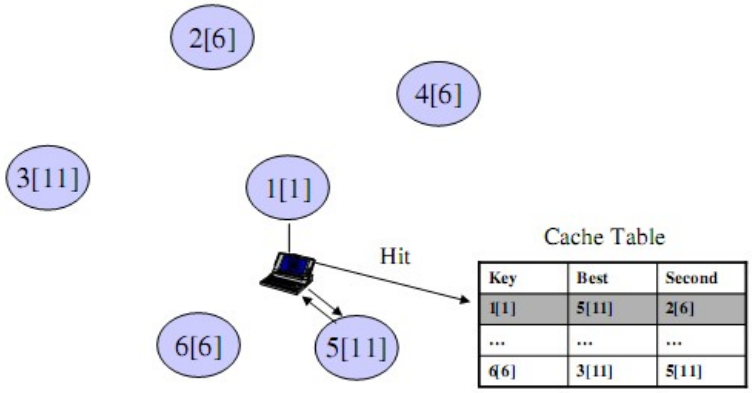


Figura 45: Channel mask scheme - cache hit

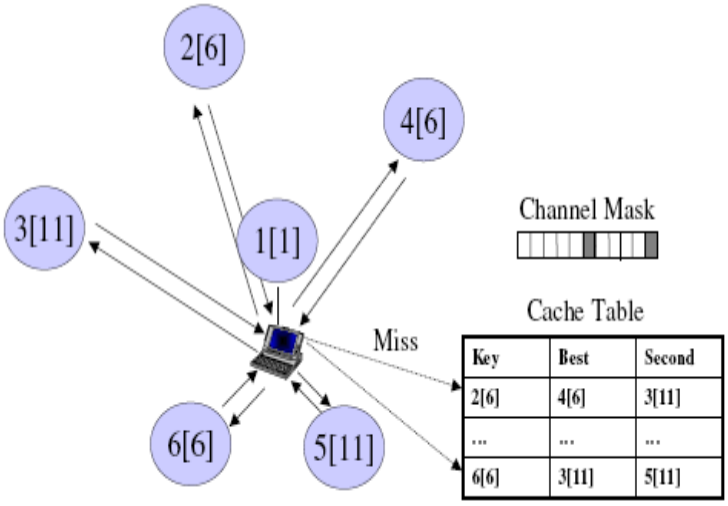


Figura 46: Channel mask scheme - cache miss

Ogni STA ha una propria channel mask, la quale è costruito durante la fase di setup della rete. Allo stesso tempo, ogni STA ha propria tabella di cache che è costruita dinamicamente ed aggiornata dagli

eventi di handoff. Questo significa che, quando una STA si associa con un AP, l'identificatore del AP (cioè, MAC address) è inserito nella cache come chiave. In più, due AP con le migliori recived signal strengths (RSS) sono salvati nella cache. Quando si verifica un handoff, la STA effettua i controlli preliminari che la entry(MAC Address del AP) relativa al AP sia presente nella cache. Se è presente, la STA prova a associarsi con il primo AP che ha il più alto RSS. Se l'associazione riesce, il processo di handoff è rifinito e quindi la handoff latency può essere ridotta in modo significativo. Altrimenti, viene provata l'associazione al secondo AP. Soltanto quando i tentativi di associazione con il primo ed il secondo AP falliscono, la STA effettua il selective scanning probing usando la channel mask.

Nello studio [17], viene proposto un nuovo handoff scheme, chiamato *SyncScan*, per ridurre il probe delay. Diversamente dalle procedure attuali di probing definite in IEEE 802.11, SyncScan permette che una STA controlli continuamente la prossimità di un AP vicino. Cioè la STA commuta regolarmente ad ogni canale e registra la forza del segnale dei canali. Facendo così, la STA può tenere traccia delle informazioni di tutti gli AP vicini. Inoltre, con il controllo continuo la qualità di segnale di più AP, permette di effettuare una decisione migliore di handoff e può anche essere ridotto il ritardo della fase di l'autenticazione/riassociazione. Per minimizzare la perdita di pacchetti durante il controllo periodico, è utilizzato il power saving mode (PSM) specificato nello IEEE 802.11. Poiché SyncScan è basato sul regolare controllo degli AP, il time synchronization è un aspetto critico. Per sincronizzarsi con gli AP, può essere utilizzato il Network Time Protocol (NTP). Daltronde, se più AP utilizzano lo tesso canale e generano beacon frame nello stesso tempo, può essere impiegato una sistema di randomizzazione. La seguente figura mostra lo schema cronometrante in SyncScan:

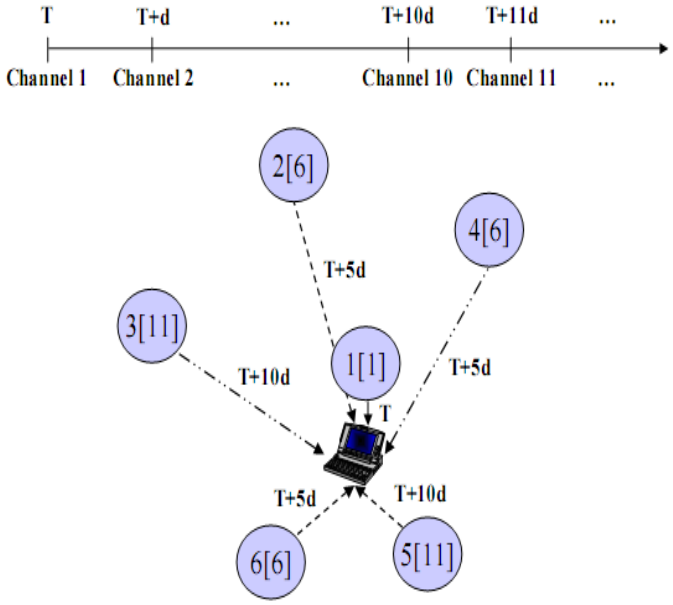


Figura 47: SyncScan: Operazioni

in cui la d è un parametro di variazione che determina il beacon bradcasting timing. Per esempio, degli AP che operano sul canale-1 ed inviano beacon frame in broadcast al tempo T, mentre altri AP operano sul canale-2 e faranno lo stesso al tempo T+d , altri AP operano sul canale-3 e faranno lo stesso al tempo T+2d e così via. Questo permette che siamo acquisite continuamente informazioni sugli AP vicini. Di conseguenza, SyncScan permette ad una STA di determinare quando un handoff dovrebbe essere effettuato, riducendo così il valore di handoff delay.

b. Reducing Authentication/Reassociation Delay

Anche se il probe delay influisce sul ritardo totale di handoff, il ritardo dovuto all'autenticazione/riassociazione dovrebbe anche essere ridotto per realizzare i servizi mobili seamless. Attualmente, nei servizi pubblici di WLAN, lo schema di autenticazione basato sull'assistente centralizzato di autenticazione ampiamente è adottato nell'interesse di servizio sicuro e della contabilità efficiente. In un tal ambiente, il ritardo dovuto alla fase di autenticazione/riassociazione può essere superiore a quelli osservati nel caso dove la procedura aperta di autenticazione è impiegata *[18]*. I metodi veloci differenti di autenticazione in IEEE che 802.11 reti sono presentati ed analizzati dentro *[19]* in termini di architettura di rete e dei modelli di fiducia. Qui di seguito verranno descritti alcuni schemi che focalizzano la loro attenzione sul modello di comunicazione.

Nell'articolo *[20]*, viene proposto uno schema preventivo di handoff per la riduzione del ritardo introdotto dalla fase di autenticazione/riassociazione (FHR). In questo schema, le informazioni di autenticazione della STA sono distribuite in modo proattivo a più AP secondo alla categoria del modello e dei servizi di mobilità della STA. Per predire il modello di mobilità della STA, deve essere introdotto il concetto di frequent handoff region(FHR). Il FHR è un insieme di AP che hanno alte possibilità di visita da una STA nell'immediato futuro. Lo schema FHR è costruito sulla base della frequenza di handoff e della priorità della STA al sistema centralizzato. Il FHR può essere facilmente implementato basandosi sul modello dello standard IEEE 802.1x [21]. Dopo molti studi di misura il numero del AP connesso con un MH durante il relativo tempo di servizio è limitato tipicamente a 2 o a 3. Di conseguenza, nello schema di FHR, le informazioni di autenticazione della STA sono trasportate ad un sottoinsieme di AP adiacente situato ad una distanza massima di due hop dal AP corrente.

La seguenti figure mostra il funzionamento dello schema di FHR.

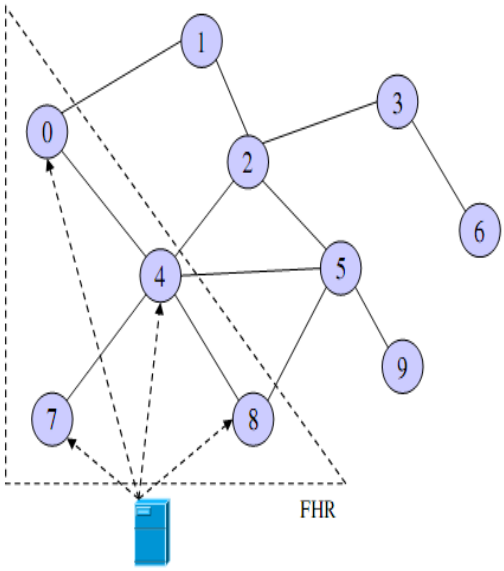


Figura 48: Login al AP4

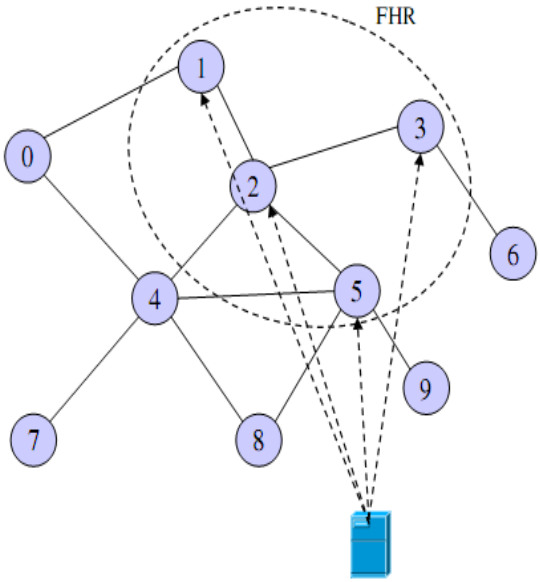


Figura 49: Handoff da AP4 a AP2

In questo esempio, una STA si associa con AP4 e forma un FHR che consiste di AP0, di AP4, di AP7 e di AP8. Di conseguenza, autenticazione le informazioni sono distribuite in anticipo a quattro AP (cioè, AP0, AP4, AP7 e AP8). Se la STA si muove verso uno degli AP selezionati, non c'è nessuna procedura di autenticazione all'assistente di autenticazione necessaria. Tuttavia, se la STA si muove verso un altro AP (per esempio, AP2 nella figura 49), che non è stato coinvolto nell'autenticazione preventiva, la nuova autenticazione e le procedure di riassociazione devono essere effettuate. In più, dopo effettuando la fase di handoff passando al AP2, un nuovo FHR deve essere costituito e sarà composto nel seguente modo AP1, AP2, AP3 e AP5.

Nello studio*[22]*, invece di usare il sistema centralizzato, è stato proposto uno schema proattivo basato su una struttura distribuita di caching. Questo schema è denominato schema *proactive neighbor caching* (PNC). Lo schema PNC usa un neighbor graph, che cattura dinamicamente la topologia di una rete wireless allo scopo di pre-posizionare il contesto della STA. Questo schema si accerta che il contesto della STA sia sempre spedito one-hop avanti per ridurre il ritardo della fase di handoff. Qui, il contesto include le informazioni per quanto riguarda la sessione della STA, la qualità di servizio (QoS) e la sicurezza *[23]*. Il neighbor graph è costruito usando le informazioni scambiate durante la fase di handoff della STA, le quali sono mantenute da ogni AP in un modo distribuito. Il contesto della STA viene immagazzinato nella cache e può essere sostituito, nel caso di mancanza di capacità nella cache, con una politica *last recently used* (LRU).

Il funzionamento dello schema di PNC è illustrato nelle figure seguenti (in cui la STA viene indicata con il nome MH):

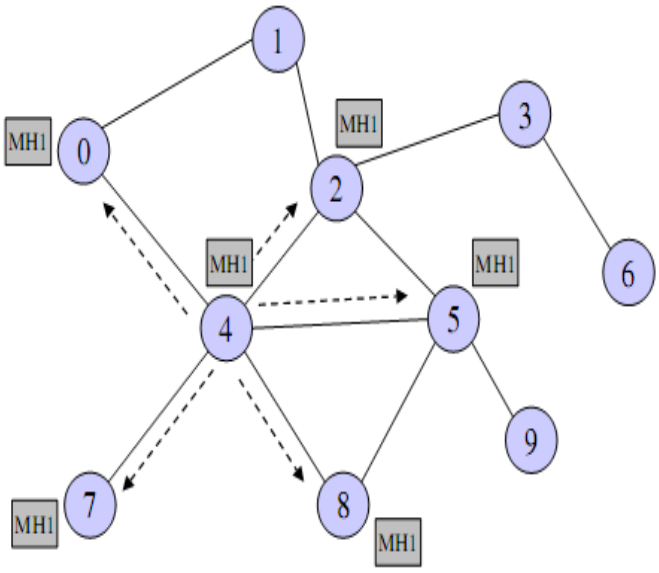


Figura 50: PNC: Login con AP4

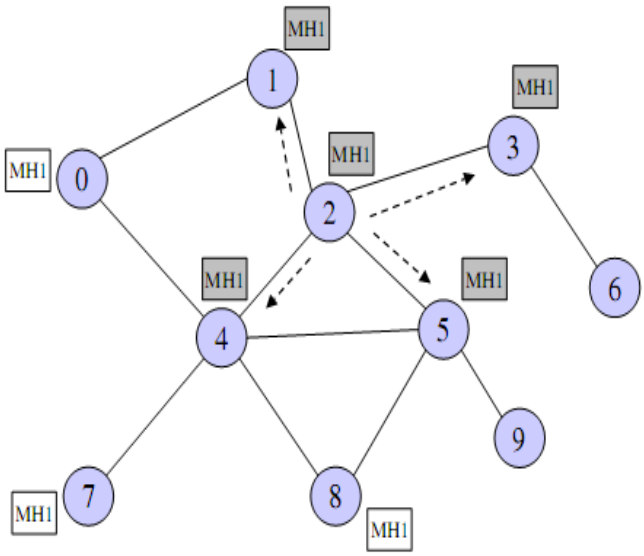


Figura 51: PNC: Handoff da AP4 a AP2

Quando un STA si associa con AP4, questo AP propaga il contesto del STA a tutto gli AP vicini (cioè, AP0, AP2, AP5, AP7 e AP8). Quando la STA si muove verso AP2, nessuna ulteriore procedura di autenticazione è effettuato perché AP2 già ha ricevuto il contesto del MH. Allo stesso tempo, i contesti della STA sono rimossi dagli AP non più vicini, cioè più distanti di un hop (AP0, AP7 e AP8). Nello schema di PNC, il contesto della STA è propagato a tutto gli AP vicini ogni volta che viene effettuata

una nuova associazione. Questo provoca una grande generazione di messaggi per la diffusione delle informazioni in particolarmente quando in presenza di molte STA all'interno di una rete IEEE 802.11. Per ridurre le spese generali di segnalazione causate dalla diffusione del contesto il trasferimento, nello studio *[24]* viene proposto uno schema denominato *selective neighbor caching* (SNC). Lo schema di SNC migliora lo schema di PNC aggiungendo un nuovo concetto: il *peso del vicino*. Il peso del vicino rappresenta la probabilità di handoff per ogni AP vicino. Sulla base di questo nuovo parametro, il contesto della STA è propagato soltanto agli AP vicini il cui peso sia maggiore o uguale di un soglia predefinita. Lo schema di SNC può fornire le prestazioni simili di handoff se il valore di soglia è selezionato con attenzione. In più, se la cache degli AP è limitata, lo schema di SNC è preferibile rispetto allo schema di PNC.

L'ultimo elaborato analizzato è *[25]*. In questo studio viene presentata uno schema NG alternativo a quelli precedentemente analizzati basato sul protocollo IAPP. Come evidenziato dallo schema:

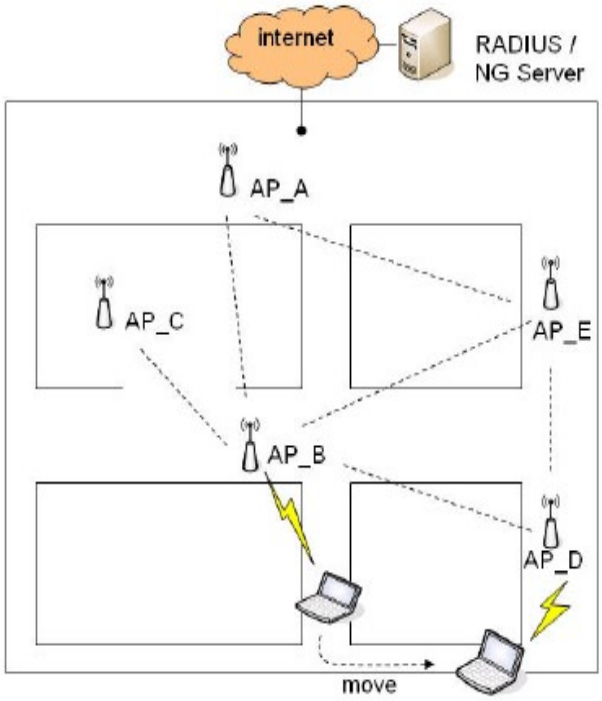


Figura 52: Architettura NG-IAPP

lo schema NG-IAPP è basato su una struttura centralizzata e prevede l'installazione su ogni STA di un NG-CLIENT responsabile dello scambio dei messaggi con il NG-SERVER.

Le linee rappresentano le relazioni di vicinanza tra gli AP. Il NG-SEVER mantiene un tabella, come la seguente NG-TABLE, per tenere traccia delle informazioni riguardanti gli AP presenti nella rete:

Current AP	Neighbor	Ch.	Loading	IP	BSSID
AP_A	AP_B	6	2	192.168…	00:60:B3 …
	AP_E	6	6	192.168…	00:60:B3 …
	AP_D	11	7	192.168…	00:60:B3 …
	…	…	…	…	…
AP_B	AP_A	1	3	192.168…	00:60:B3 …
	AP_C	11	1	192.168…	00:60:B3 …
	AP_D	11	7	192.168…	00:60:B3 …
	…	…	…	192.168…	…
…	…	…	…	…	…

Tabella 17: NG-TABLE mantenuta dal NG-SERVER

dove *Ch* è il canale utilizzato, *Loanding* il numero di STA gestite dal AP.

Le informazioni mantenute per ogni entry della tabella sono indicizzate in base all'attuali AP della STA e possono essere inserite manualmente o essere aggiornate in base alla storia della fase di roaming del dispositivo mobile. Il meccanismo si basa sulla *pre-registrazione* per ridurre il ritardo introdotto dalla fase di handoff e sull'introduzione del *forwarding-and-buffering frame* per fare fronte alla perdita dei frame che può avvenire durante le operazioni di migrazione.

Il NG-CLIENT si connette al server appena entra nella rete per apprendere gli AP vicini segnalati nella entry della tabella. Periodicamente il client controlla il RSSI(Received Signal Strength Indication) del suo attuale AP. Se è basso entra in *power save mode* in modo che il suo attuale AP possa bafferizzare i frame diretti alla STA mentre questa effettua un *selective scanning* coinvolgendo tutti gli AP vicini. Finita questa fase esce dal *power save mode* la STA manderà un IAPP Pre-Registration-indication packet al AP con migliore RSSI (AP candidato) il quale attraverso uno scambio di messaggio con il NG-SEVER controllerà la validità della richiesta.

Se è valida il NG-SEVER darà la conferma al AP candidato inviandogli anche il security block per comunicare con l'attuale AP collegato alla STA. AP candidato richiederà il contesto della STA. Nel momento in cui il valore di RSSI dell'attuale AP sarà troppo basso la STA migrerà al AP candidato con il quale si riassocerà direttamente. Successivamente il NG_CLIENT si connetterà al server al quale richiederà le informazioni contenute nella di tabella relative al nuovo AP. Nella seguente figura sono riassunte rispettivamente le fasi presentate di questo schema:

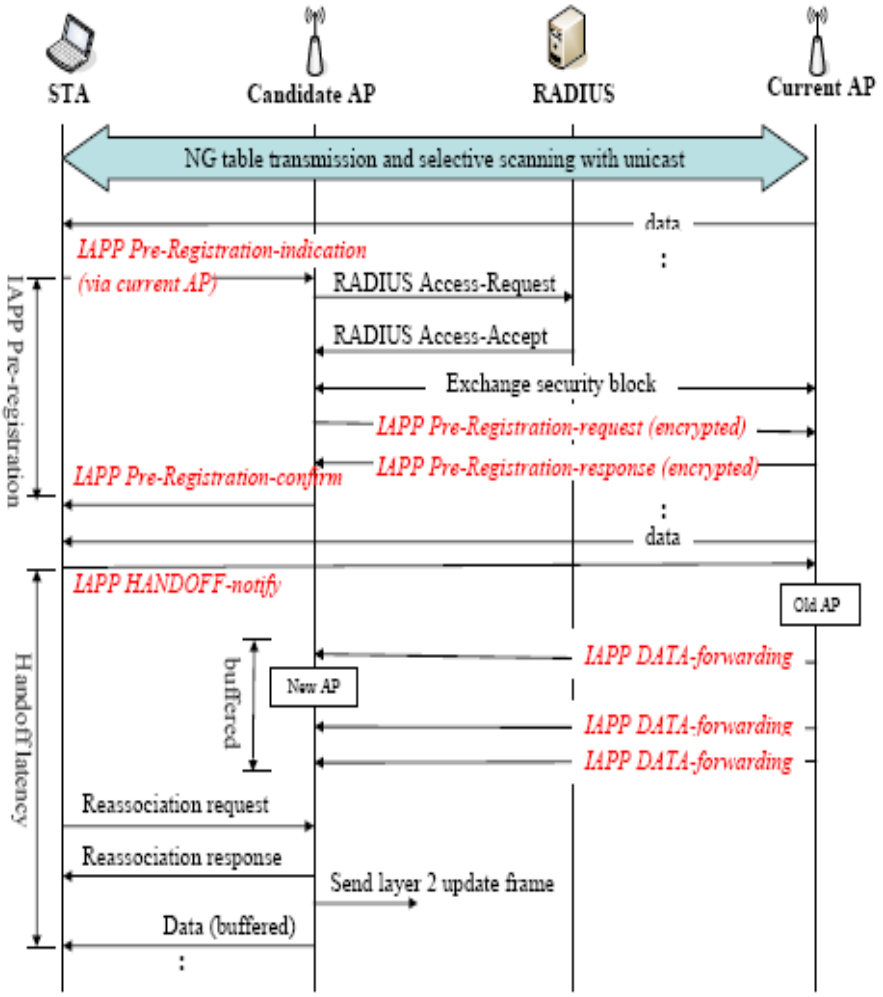


Figura 53: Schema NG-IAPP

3.2 Considerazioni sulle soluzioni presentate

La tabella X mostra che il confronto degli schemi per la riduzione della sonda fa ritardare in termini di compatibilità, necessità dei cambiamenti (lato AP o lato STA), della complessità di esecuzione e di signiling overhead.

Tecniche / **Aspetti Considerati**	**Tuning**	**NG-pruning**	**Channel Mask**	**SyncScan**
Compatibilità	Si	Parziale	Si	Parziale
Cambiamenti necessari	STA	STA/AP	STA	STA/AP
Complessità di implementazione	Bassa	Alta	Media	Alta
Singling overhead	Bassa	Alta	Bassa	Media

Tabella 18 Tecniche per riduzione Probe Delay: Confronti

Lo schema Tuning richiede soltanto la modifica della STA e non è ha problemi di incompatibilità. Anche se questo schema può essere implementato facilmente con un valore di singling overhead basso, la selezionare i valori di tuning appropriati dipende molto dal tipo di rete in cui si opera.

Per sostenere lo schema NG-pruning, sia il AP che la STA dovrebbero essere modificati anche se una parte di questo schema fa parte dello standard IEEE. Lo svantaggio principale dello schema NG-pruning è l'alta complessità e valore di singling overhead alto a causa della la mantenimento del NOG e di NG. Quindi, per rendere questo schema più fattibile le spese generali di esecuzione e ed il singling overhead dovrebbero essere diminuiti.

Lo schema di channel mask è meno complesso dello schema NG-pruning e può funzionare nell'attuale standard IEEE 802.11. Tuttavia, il caching e le procedure di selezione sono euristiche e procedure quindi richiede che siano sfruttate algoritmi più raffinati.

Il SyncScan richiede modifiche leggere al AP per evitare la perdita del pacchetto dovuto alla sincronizzazione periodica con gli AP. Questo schema è alla base della modalità di scansione passiva, in modo da abbassare il segniling l'overead. Anche se SyncScan può migliorare le prestazioni di handoff, esso può provocare latenza nella ricezione del pacchetto dovuto al sondaggio degli AP vicini. Di conseguenza, sono richieste più indagini sulla selezione e sui parametri di prestazioni in ambienti realistici.

La tabella 19 confronta gli schemi per la riduzione dei ritardi dovuti alla fase di autenticazione/riassociazione seguendo i parametri utilizzati in precedenza per il probe delay:

Tecniche / Aspetti Considerati	FHR	PNC	SNC	NG-IAPP
Compatibilità	Si	Parziale	Si	Si
Cambiamenti necessari	STA	STA/AP	STA	STA
Complessità di implementazione	Bassa	Alta	Media	Media
Singling overhead	Bassa	Alta	Bassa	Media

Tabella 19: Tecniche per riduzione Authentication/Reassociation Delay - Confronti

Lo schema di FHR richiede soltanto la modifica del AP. Tuttavia, è basato sul sistema centralizzato, che rischia di essere un collo di bottiglia. Questo problema si ripercuote anche nello schema NG-IAPP in cui tutte le comunicazioni per il trasporto delle informazioni utili per effettuare il roaming sono richieste all'unico NG-SERVER presente nell'architettura. Questo schema presenta comunque dei delay compatibili con il limite massimo necessario per avere buone comunicazioni di VoIP *(50ms)[36]*. Per superare i limiti introdotti dall'utilizzo del protocollo IAPP, la soluzione presentata tenta di eliminare il delay dovuto al protocollo applicando la tecnica della pre-registazione e di ridurre il valore di delay introdotto dalla fase di probing in reti IAPP *(tipicamente da 40ms a 300 ms*) al tempo di scanning *(3ms per AP)*. Lo schema si presenta comunque abbastanza invasivo al livello implementativo, infatti richiede l'installazione di appositi client e server per il funzionamento.

Lo schema di PNC è incluso nello standard IEEE (cioè, IEEE 802.11f), in modo che nessun si presenti nessun problema di compatibilità. In più, poiché le operazioni sono completamente distribuite, non c'è un singolo collo di bottiglia. Tuttavia, le informazioni del vicino sono sviluppate in un modo incrementale e quindi le prestazioni iniziali non sono molto buone. Inoltre, l'alto signiling traffic può essere indotto anche dalle STA ferme. Introducendo la tabella del peso al AP, lo schema di SNC può ridurre il fattore Singling overhead dello schema di PNC ed inoltre può essere implementato basandosi sullo schema di PNC senza cambiamenti significativi nello standard. Tuttavia, una struttura dati supplementare dovrebbe essere costruita e mantenuta e lo schema di SNC abbassa il ritardo dell'autenticazione/riassociazione soltanto in modo probabilistico.

3.2 Layer2 Roaming: Sviluppi Futuri (802.11r)

Rispetto alla prima generazione di reti WLAN, il roaming è diventato più complesso e richiede prestazioni alte del processore e questo è un problema importante da risolvere per applicazioni realtime. Il protocollo 802.11r è stato pensato per ridurre il tempo necessario per i processi di transizione all'interno di una rete BSS. Lo scopo di nuova iniziativa è di accertarsi che la maggior parte dei processi di autenticazione siano realizzati prima che la stazione incominci la fase di roaming. La draft corrente raccomanda di effettuare il metodo scelto per generare la PMK (IEEE 802.1X) una volta che la stazione si unisce alla rete. La PMK è distribuita al tutti gli AP che sono autenticati nella sottorete. Quindi, nel momento in cui una stazione si sposta tra gli AP si presuppone che la PMK sia già presente all'interno di essi. Questo fornisce un grande contributo a ridurre l'esigenza di ripetizioni e così anche l'overhead derivante dalla fase di autenticazione che si verifica quando la STA effettua il processo di roaming. Specialmente viene ridotta la latenza supplementare generata dalla connessione con il server di autenticazione.

3.2.1 Caratteristiche della Sicurezza per il protocollo 802.11r

Per permettere ad una stazione di realizzare i funzionamenti di sicurezza quale la chiave la derivazione prima del roaming, il draft del protocollo 802.11r specifica una nuovo sistema di gestione delle chiavi, che include una nuova gerarchia delle chiavi e corrispondenti algoritmi per l'ottenimento delle chiavi di derivazione. Il key management framework del protocollo 802.11r, consiste di due livelli di *key holder*, organizzati in *Security Domains*, alcuni dei quali aggregate per formare un *Security Mobility Domain*.

In questo framework, un *key holder* è un'entità logica della rete che è autorizzato per memorizzare il materiale necessario per la creazione delle chiavi. Ci sono due livelli di key holder*[26]*:

- Livello 0, o *R0 Key Holders* (R0KH) immagazzinano le chiavi di alto livello, chiamate PMK-R0.
- Livello 1, o *R1 Key Holders* (R1KH) che immagazzina chiavi del secondo-livello, chiamate PMK-R1.

Nella gerarchia delle chiavi, sotto la R1KH c'è l'access point che immagazzina il più basso livello di chiave (il PTK). I Key Holders sono entità logiche e quindi possono essere situate all'interno del AP o possono essere un dispositivo fisico dedicato. Per esempio, un controller che gestisce AP multipli può funzionare da R0KH, con gli AP che funzionano da R1KH. Alternativamente, ogni AP può funzionare da R0 e R1 Key Holders.

Generalmente, le entità ad ogni livello della gerarchia delle chiavi ottengono le loro chiavi dall'entità associate di livello superiore della gerarchia e derivano le chiavi per il livello che lo segue attraverso i

seguenti elementi: dalla chiave che possiede, l'indirizzo della STA, l'identità o l'indirizzo di rete dell'entità che immagazzinerà la chiave e possibilmente altre informazioni.

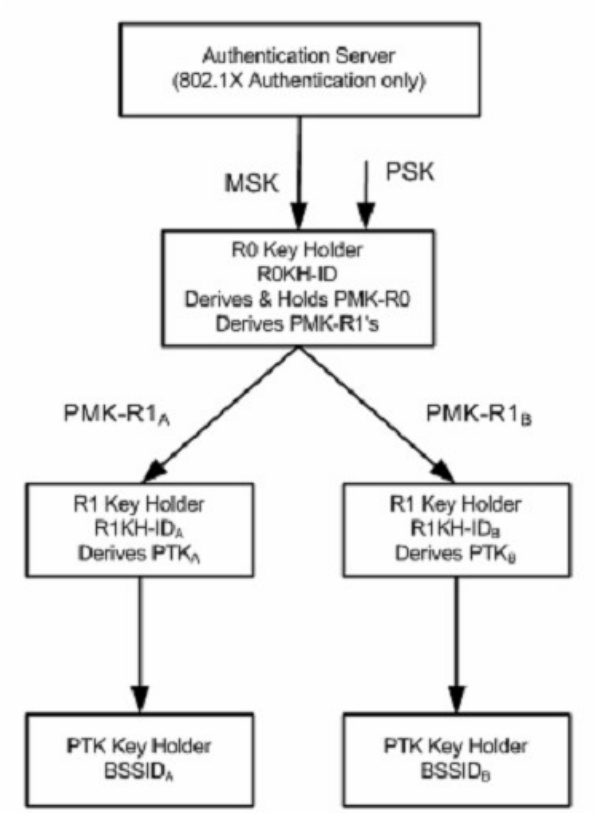


Figura 54: 802.11r - Gerarchia della chiavi

Nel sistema di amministrazione delle chiavi del 802.11r, un Security Domain consiste: di un singolo R0HK, di tutte le relative chiavi R1HK e gli AP a loro associati. Il *Security Mobility Domain* (SMD) è un insieme dei domini di sicurezza dentro i quali ogni R1 Key Holders può ottenere PMK-R1 da ogni R0KH presente. Cioè un R0 Key Holders all'interno di un SMD può derivare una PMK-R1 per tutti i R1 Key Holders all'interno del SMD, anche se non all'interno dello stesso Security Domain. Un SMD definisce il limite in cui una stazione può effettuare le transizioni veloci come definite dal protocollo 802.11r senza avere bisogno di realizzare le autenticazioni supplementari dello standard IEEE 802.1X.

La prima volta che una STA si associa con un AP all'interno di un SMD, le chiavi sono derivate usando il R0-KHID e il R1-KHID del R0KH e R1KH che corrispondenti all'access point. Le chiavi PMK-R1 sono derivate usando il R0-KHID del primo AP contattato e il R1-KHID del AP a cui la STA è attualmente transitato. Così quando un AP ammette un cliente che usa la transizione veloce, il suo R1KH ha già ottenuto la PMK-R1 dal R0KH in Dominio di sicurezza che contiene il primo access point contattato dalla stazione.

Dopo che una stazione effettua il contatto iniziale per un'associazione, il *R0 Key Holders* può derivare e distribuire il PMK-R1 all'altra R1KH all'interno del SMD. Se un client passa ad un altro AP in un

SMD, il R1KH associato al AP dovrebbe avere PMK-R1 e nessun'altra autenticazione dello IEEE 802.1X è richiesta. Il protocollo 802.11r non specifica i metodi esatti da usare per distribuire le chiavi fra i key holders e gli AP. Viene assunto che esistono dei collegamenti sicuri fra i key holders e che questi sono usati per trasmettere le informazioni chiave.

3.2.2 Funzionalità QoS disponibili in 802.11r

Il protocollo 802.11r permette a una STA di richiedere risorse per il Quality of Services(QoS) durante la riassociazione, evitando così uno scambio di messaggi per riservare le risorse necessarie prima che il trasferimento dei dati possa riprendere. In molti casi questo risparmio di tempo può essere sufficiente per contribuire al mantenimento della voice quality durante le passaggio di una STA tra AP. Comunque ci possono essere delle situazioni in cui la ripartizione delle risorse durante la riassociazione può comportare dei rischi. Per esempio, se un AP deve consultare un server dedicato al QoS per assegnare le risorse ed il collegamento con questo server è lento, il tempo di riassociazione può essere più lungo di quanto voluto. In questi casi la STA può trarre beneficio dal richiedere le risorse di QoS prima di effettuare la riassociazione. La specifica 802.11r permette anche di effettuare delle prenotazioni delle risorse quando un AP è molto cariato di lavoro e la capacità ammissione di stazioni mobili è ridotta. In questi casi effettuare la prenotazione mentre la stazione è associata al AP corrente può contribuire a evitare di avere fallimenti dei tentativi di riassociazione.

3.2.3 Funzionamento del protocollo

La STA deve stabilire il contatto iniziale con un AP all'interno di una rete abilitata al supporto del protocollo 802.11r ed informa il AP che vuole usare la transizione veloce (FT) durante la fase di roaming all'interno della SMD secondo le indicazioni.

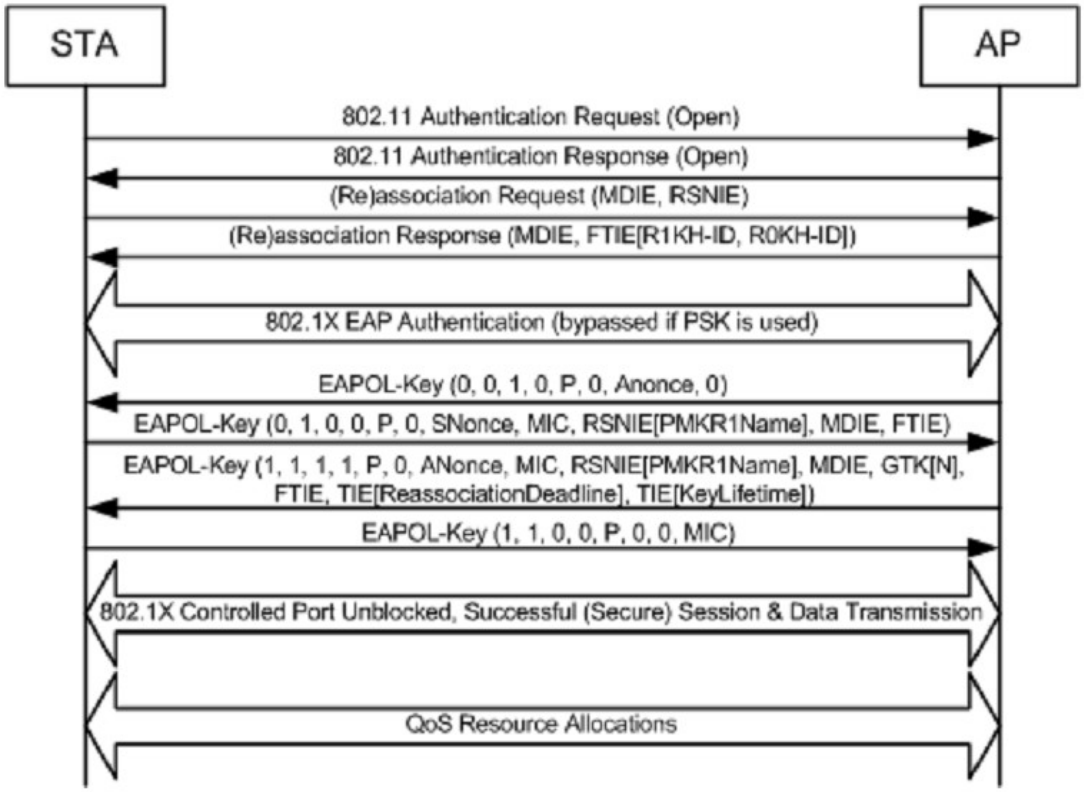


Figura 55: 802.11r: Riassunto fasi protocollo

La stazione determina se un AP è abilitato al FT esaminando i beacon e/o probe response frame analizzando gli elementi che forniscono informazioni sulla FT (IEs). Quando la stazione ha selezionato un AP con cui associarsi, effettua l'autenticazione di tipo *open* dello standard IEEE 802.11 e successivamente la richiesta di (re)associazione contenente il valore IE definito dal protocollo 802.11r che indica i meccanismi che la stazione desidera usare FT. Avvenuta l'associazione, l'autenticazione 802.1X continua (a meno che PSK sia in uso) con la derivazione della MSK. Una volta che questo processo viene completato con successo, il R0KH del AP può ricevere PMK-R0 con cui deriva PMK-R1 per tutti gli R1KH del dominio SDM. Questo permette che tutti gli R1KH nello SMD immagazzinino il PMK-R1 relativo alla STA e divenendo così disponibile nel caso che la STA si sposti verso un altro AP che possiede un R1KH. Dopo che l'entità R1KH dell'access point riceve PMK-R1 per questa primo contatto della fase di associazione, questa procede con un 4-way handshake per derivare il PTK. Il risultato del completamento di questa procedura è la connessione dati fra la stazione mobile ed AP. A questo punto può iniziare se necessario la QoS negoziation. Se la STA

decide di spostarsi verso un altro AP sempre appartenente allo SMD, dopo che una prima associazione riuscita del contatto, essa possa usare i meccanismi di transizione veloce per eseguire la transizione. Il meccanismo base di transizione permette che la stazione installi il PTK prima della riassociazione ed stanziare in modo sicuro risorse di QoS al momento della riassociazione.

Il meccanismo base compie la transizione in due fasi:

- prima fase: stabilisce le informazioni necessarie affinché il PTK siano derivate sulla stazione sul AP .
- seconda fase: esegue la riassociazione insieme alla ripartizione delle risorse e convalida recentemente derivato PTK.

La prima fase può essere effettuato con o senza il sistema di distribuzione (DS) il AP corrente. Se effettuato senza DS(over the air), la stazione ed il AP eseguono uno scambio di autenticazione 802.11, usando un nuovo algoritmo di autenticazione che specifica l'uso della transizione veloce come nella specifica *[26]*. La stazione dovrà andare off-channel per un minimo periodo di tempo in modo da realizzare lo scambio. Se l'autenticazione è effettuata usando un DS, sono usati gli Action Frame usati e quindi non è necessario l'off-channel time. La seconda fase del meccanismo base di transizione è la fase di riassociazione. La stazione include nella richiesta di riassociazione tutte le richieste di allocazione delle risorse necessarie, più un Message Integrity Chack(MIC) per autenticare la richiesta. Il MI

C è calcolato usando il PTK derivata nella prima fase. La risposta del AP alla richiesta di Riassociazione della STA contiene la chiave temporale del gruppo (GTK) e tutte le chiave collegata e un MIC per convalidare la risposta. Una volta che la seconda fase è stata completa con successo, viene stabilita una connessione sicura di dati tra STA ed il AP con QoS (se necessario).

L'access point compatibile con il protocollo 802.11r può opzionalmente supportare il meccanismo di prenotazione per le transizioni veloci, come già presentato precedentemente. La transizione veloce con prenotazione è compiuta in tre fasi.

La prima fase è la stessa del prima fase del meccanismo base . La prima fase può essere eseguita “over the air” usando i frame di autenticazione dello standard 802.11 o tramite DS (attraverso AP corrente) usando gli Action frames. La seconda fase tiene conto della prenotazione delle risorse e può essere eseguita “over the air” usando i frame di autenticazione dello standard 802.11 o attraverso il DS usando gli Action frames. Nella seconda fase del processo, la STA trasmette la sua richiesta di risorse al AP destinatario ed inoltre include un MIC calcolato con il PTK derivato nella fase 1 del processo. Il messaggio di risposta del AP indica i particolari delle risorse riservate ed inoltre contiene la MIC per convalidare il messaggio. La terza fase è la riassociazione che è essenzialmente la stessa vista precedentemente nel meccanismo basse. In questo caso, la STA specifica le risorse negoziate nella fase 2, possibilmente compreso le nuove risorse richieste. Durante il processo di transizione FT, la STA può

autenticare e, se desidera, riservare risorse ad uno o più AP e può scegliere un AP tra dalla lista prima scadenze della riassociazione.

Studio delle Prestazioni

Nell'articolo*[27]* sono stati effettuati degli studi di prestazione senza il supporto del QoS resource reservation.

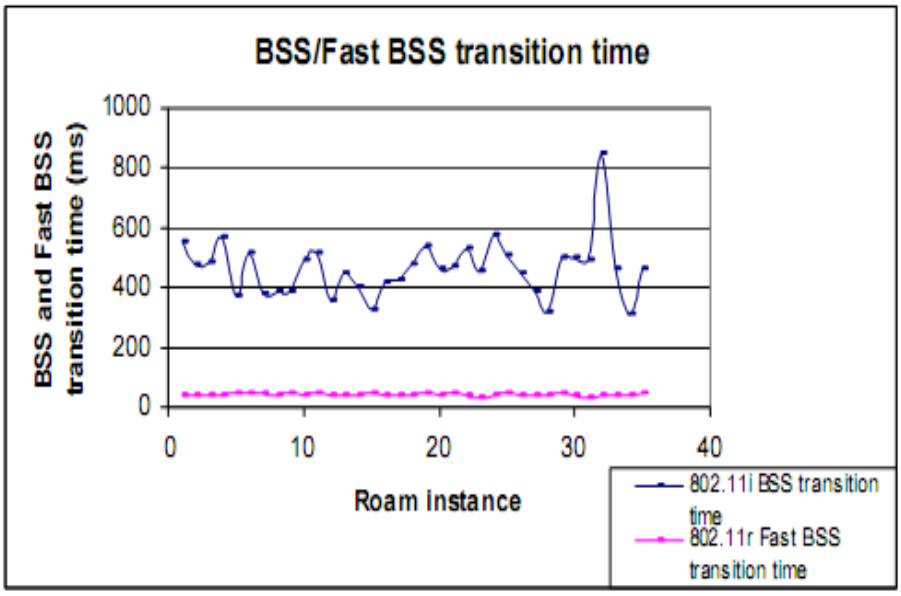


Figura 56: Tempi di transizione del BSS e Fast BSS

Il prototipo dello IEEE 802.11r è risultato caratterizzato da un tempo di transizione significativamente basso confrontato ai casi basati su IEEE 802.11i.

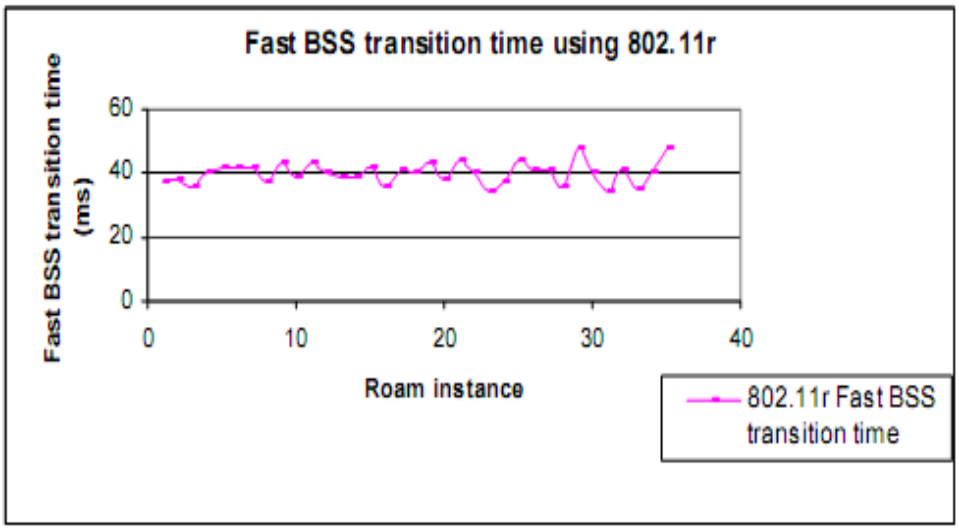


Figura 57: Tempi di transizione del Fast BSS usando 802.11r

La tabella 20 mostra i particolari vaganti medi di perdita del pacchetto e di tempo che usando l'autenticazione della linea di base 802.11i e la transizione veloce di BSS. Questa è stata realizzata utilizzando diverse sessioni 2-way di stream VoIP utilizzato con il codec G.711u (un intervallo di 20ms) fra la STA ed il punto finale della connessione. La transizione di BSS viene effettuata durante un particolare momento della prova.

Authentication method	Average Roaming time (ms)	Average Packet loss %	Maximum consecutive lost datagrams (Average)
Baseline – Full 802.1X EAP authentication	525	1.8	53
Fast Transition using 802.11r	42	0.2	6

Tabella 20: Effetto del roaming sulla perdita dei pacchetti

Il protocollo 802.11r presenta una bassa perdita dei pacchetti e quindi garantisce una migliore Quality of Voice.

Conclusioni

La tecnologia wireless per poter rafforzare il suo ruolo nelle applicazioni mobili e di chiamata VoIP-mobile, deve poter fornire una mobilità sicura. Per realizzare questo scopo, le stazioni mobili hanno bisogno di sistemi di autenticazione e crittografia robusta, roaming veloce e QoS (qualità di servizio).

La valutazione della adeguatezza della soluzione adottata è in relazione alla riduzione dei ritardi introdotti dalla fase di roaming e dipende dalla tipologia di applicazione seamless*[36]*. Ad esempio siamo in presenza di tolleranze di ritardi differenti tra applicazioni di Multimedia streaming o VoIP.

Durante questo studio è emersa tutta la complessità della problematica del roaming, sia dal punto di vista architetturale del mezzo di comunicazione che da quello gestionale, come indicato nella seguente tabella*[36]*:

Layer	**Item**	**Time (ms)**
L2	802.11 scan (passive)	0 ms (cached), 1 second (wait for Beacon)
L2	802.11 scan (active)	40 to 300 ms
L2	802.11 assoc/reassoc (no IAPP)	2
L2	802.11 assoc/reassoc (w/ IAPP)	40
L2	802.1X authentication (full)	1000
L2	802.1X authentication (fast resume)	250
L2	Fast handoff (4-way handshake only)	60
L3	DHCPv4	1000
L3	Initial RS/RA	5
L3	Wait for subsequent RA	1500
L3	DAD (full)	1000
L3	Optimistic DAD	0
L3	MN-HA BU	1 RTT (IKE w/HA SA), 4 RTT (IKE w/CoA SA)
L3	MN-CN BU	1-1.5 RTT (CAM) to 2.5 RTT (RR)
L4	TCP parameter adjustment (status quo)	5000 (802.11/CDMA) - 20000 (802.11/GPRS)
Best case	All fixes	150 ms
Average case	6to4, RR, Active scan	1300 ms
Worst case	No TCP changes, full EAP auth, IAPP, DHCPv4	25000 ms

Table 21: Latency budget

In questo complesso panorama sono stati analizzati gli aspetti del roaming legati la livello 2 della pila ISO/OSI (L2). Durante questo percorso il mezzo trasmissivo wireless, ha mostrato le sue debolezze

nei meccanismi di roaming. Queste derivano dalla progettazione dello standard IEEE 802.11 in cui l'aspetto della migrazione tra AP, non è stato preso in considerazione nell'ottica del mantenimento dei servizi seamless(es:VoIP).

Le analisi effettuate si sono concentrate specialmente su due fattori per la riduzione dei ritardi introdotti dalla fase di roaming: le fasi che caratterizzano il processo di handoff e l'influenza dei protocolli di sicurezza.

Gli studi trattati in questo elaborato*[Cap.3]* hanno indirettamente dimostrato come, i vantaggi introdotti dall'applicazione di particolati soluzioni al problema del roaming a livello 2 della rete, siano limitati. Infatti, le soluzioni presentate, possono solo attenuare i ritardi introdotti dalla fase di handoff, ma non riescono a risolvere pienamente il problema.

Ad esempio, nelle reti aziendali di tipo VoWLAN(Voip su WLAN) si tende ad usare meccanismi di autenticazione avanzata e tecniche dinamiche di crittografia basata su chiave, resi possibili dallo protocollo IEEE 802.11i e le possibilità di QoS definite dal protocollo IEEE 802.11e. Purtroppo, le migliorie previste dall'utilizzo di questi protocolli, nell'ottica di ottenere un romaing veloce, sono del tutto insufficienti. L'autenticazione completa usando il protocollo IEEE 802.11i, per esempio, può generare ritardi di diverse centinaia millisecondi durante il roaming fino a raggiungere *1.5 secondi* nel caso di un dispositivo PDA*[Cap.3]*.

Preso atto degli attuali limiti che si incontrano nel gestire la fase di handoff al livello 2 della rete, le forze di stanno concentrando sulla ricerca di soluzioni software a livello 3 (es: sistemi di Mobile-IP).

Dalle analisi effettuate, si può concludere che soluzioni efficaci al livello 2 della rete si diffonderanno con la standardizzazione ed applicazione del protocollo IEEE 802.11r *[Cap3,Par3]* appositamente progettato per definire una modalità di roaming veloce standard, in modo ad esempio che gli utenti non debbano autenticarsi a ogni nuovo access point che incontrano.

La nuova transizione veloce di BSS definita da 802.11r elimina gran parte del handshacking presente nella rete. Questa fornisce una soluzione senza alcun compromesso per la comunicazione VoWlan sicura, permettendo transizioni fast-roaming con tempi di circa *50ms* conservando il contesto di sicurezza del dispositivo e quello di QoS.

In tutto questo contesto, per il futuro si prevede che l'aspetto di ottimizzazione della fase di autenticazione diventerà sempre più critico, in quanto il meccanismo di sicurezza sembra destinato ad affermarsi come il principale collo di bottiglia del meccanismo di handoff.

Riferimenti

[1] IEEE 802.11. IEEE Standard for Local and Metropolitan Area Networks- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard, Luglio 1999.

[2] "802.11 Wireless Networks The Definitive Guide (2005)", 2Ed Bbl Lotb-Oreilly.

[3] IEEE 802.11f, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," *IEEE Standard*, Luglio 2003.

[4] Jon-Olov Vatn, "An experimental study of IEEE 802.11b handover performance and its effects on voice traffic", TRITA-IMIT TSLAB, Luglio 2003.

[5] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1x-2001, June 2001.

[6] IEEE 802.11i, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements," *IEEE Standard*, Luglio 2004.

[7] A. Balachandran, G. Woelker, P. Bahl, and P. Rangan, "Characterizing User Behaviour and Network Performance in a Public Wireless LAN," in *Proc. ACM SIGMETRIC 2002*, Giugno 2002.

[8] D. Schwab and R. Bunt, "Characterising the Use of a Campus Wireless Network," in *Proc. IEEE INFOCOM 2004*, March 2004.

[9] IEEE 802.11g, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band," *IEEE Standard*, Giugno 2003.

[10] IEEE 802.11e, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Quality of Service Enhancements," *IEEE Standard*, Novembre 2005.

[11] S. Choi, "Overview of Emerging IEEE 802.11 Protocols for MAC and Above," *SK Telecom Telecommunications Review*, vol. 13, Novembre 2003.

[12] P. Bahl, R. Chandra, and J. Dunagan, "SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks," in *Proc. ACM Mobicom 2004*, Ottobre 2004.

[13] Ivan Martinovic, Frank A. Zdarsky, Adam Bachorek, and Jens B. Schmitt,"Measurement and Analysis of Handover Latencies in IEEE 802.11i Secured Networks".

[14] A. Mishra, M. Shin, W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *ACM SIGCOMM Computer Communications Review*, vol. 33, n. 2, Aprile 2003.

[15] M. Shin, A. Mishra, and W. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs," in *Proc. ACM MobiSys 2004*, Giugno 2004.

[16] S. Shin, A. Forte, A. Rawat, and H. Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs," in *Proc. ACM MobiWac 2004*, October 2004.

[17] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks," in *Proc. IEEE Infocom 2005*, March 2005.

[18] K. Chi, J. Jiang, and L. Yen, "Cost-Effective Caching for Mobility Support in IEEE 802.1X Frameworks," *IEEE Transaction on Mobile Computing*, to appear.

[19] M. Bargh, R. Hulseboch, E. Eertink, A. Prasa, H. Wang, and P. Schoo, “Fast Authentication Mothods for Handovers between IEEE 802.11 Wireless LANs,” in *Proc. ACM WMASH 2004*, October 2004.

[20] S. Pack and Y. Choi, “Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems,” *IEEE Proceedings Communications*, vol. 151, n. 5, Ottobre 2004.

[21] IEEE 802.1x, “IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control,” *IEEE Standard*, Giugno 2001.

[22] A. Mishra, M. Shin, and W. Arbaugh, “Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network,” in *Proc. IEEE INFOCOM 2004*, Marzo 2004.

[23] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, “Context Transfer Protocol (CXTP),” *IETF RFC 4067*, Luglio 2005.

[24] S. Pack, H. Jung, T. Kwon, and Y. Choi, “SNC: A Selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks,” in *ACM Mobile Computing and Communications Review*, vol. 9, no. 4, Ottobre 2005.

[25] Ping-Jung Huang, Yu-Chee Tseng,“A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks”, 2006.

[26] IEEE Std 802.11r /D01.0, Draft “Amendment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer Specifi cations:Amendment 8: Fast BSS Transition”, 2005.

[27] Sangeetha Bangolae, Carol Bell, Emily Qi,“Performance Study of Fast BSS Transition using IEEE 802.11r”.

[28] International Telecommunications Union. ITU-T Recommendation G.114 (1998): "Delay”.

[29] B. Goode, “Voice Over Internet Protocol (VOIP)”. *Proceedings of the IEEE*, VOL. 90, n. 9, Settembre. 2002.

[30] Anonymous, “Voice Over IP Via Virtual Private Networks: An Overview”. *White Paper, AVAYA Communication*, Febbraio, 2001.

[31] Barbieri, R., Bruschi, D. and Rostu, R, “Voice over IPSec: Analysis and Solutions”. *18° Annual Computer Security Apllications Conference (ACSAC’02) Las Vegas*, Luglio 2002.

[32] R. Sinden, “Comparison of Voice over IP with circuit switching techniques”. *Department of electronics and Computer Science, Southampton University, UK*, Gennaio. 2002.

[33] C-N. Chuah, “Providing End-to-End QoS for IP based Latency sensitive Applications.”. *Technical Report, Dept. of Electrical Engineering and Computer Science, University of California at Berkeley*, 2000.

[34] K. Percy and M. Hommer, “Tips from the trenches on VOIP”. *Network World Fusion*, Gennaio 2003.

[35] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, “Security Considerations for Voice Over IP Systems Recommendations of the National Institute of Standards and Technology”, *of NIST Special Publication 800-58*.

[36] Bernard Adoba Microsoft, “Fast Handoff Issues”, doc.:IEEE 802.11-03/155r0, 22 Luglio 2007 .