

# Capitolo 1

## Livello collegamento e LAN

### 1.1 Il livello collegamento

I dispositivi che supportano un protocollo link-layer sono detti *nodi*. I canali di comunicazione che connettono nodi adiacenti sono detti *collegamenti*. Un nodo incapsula il datagramma ricevuto dal network layer sovrastante in un *link-layer frame* e lo trasmettono sul collegamento.

#### 1.1.1 I servizi forniti dal livello collegamento

##### **Incapsulazione**

Quasi tutti i protocolli link-layer incapsulano i datagrammi ricevuti dal network layer prima di trasmetterli sul collegamento. Il frame è composto da un campo dati, dove viene inserito il datagramma, e degli header.

##### **Accesso al collegamento**

Un protocollo di medium access control (MAC) specifica come il frame deve essere trasmesso sul collegamento.

##### **Trasporto affidabile**

Un protocollo di trasferimento affidabile garantisce che ogni frame raggiunga la sua destinazione senza errori.

##### **Individuazione e correzione degli errori**

Il nodo mittente fornisce un meccanismo per individuare gli errori, che verranno poi corretti dal destinatario.

#### 1.1.2 Implementazione del livello collegamento

Le funzionalità Ethernet sono integrate nella scheda madre o in un chip Ethernet. Il livello collegamento è implementato su un chip detto *network adapter* o *NIC*.

### 1.2 Individuazione e correzione degli errori

#### 1.2.1 Controlli di parità

La forma più semplice di error detection è l'utilizzo di un bit di parità. Gli schemi di parità possono essere pari o dispari. Con uno schema di parità *bidimensionale*, dove i bit sono disposti a matrice, è

possibile identificare il bit corrotto e correggerlo. Questo schema non può correggere due errori in un singolo pacchetto, ma li può individuare.

### 1.2.2 CRC

I codici CRC (*cyclic redundancy check*) sono anche detti codici polinomiali in quanto è possibile considerare la stringa da inviare come un polinomio i quali coefficienti sono i valori 0 e 1 della stringa di bit. I CRC possono individuare  $\text{resto} \leq$  bit errati consecutivi.

## 1.3 Multiple access link

Esistono due tipi di collegamento. Il collegamento *point to point* consiste in un solo mittente e un solo destinatario. Il collegamento *broadcast* può avere più nodi mittenti e destinatari connessi allo stesso canale di broadcast. Per coordinare la trasmissione di pacchetti all'interno di una rete broadcast, si utilizzano *protocolli di accesso multiplo*. Quando due o più nodi trasmettono frame allo stesso momento, i frame *collidono* e vengono persi. Esistono tre tipi di protocolli ad accesso multiplo.

### 1.3.1 Protocolli a partizionamento di canale

- *TDMA*: l'accesso al canale avviene in "round", e ogni nodo ha uno slot di tempo in cui può trasmettere in ognuno di questi round. Il tasso di trasmissione è  $R/N$ , e i canali inutilizzati vengono sprecati.
- *FDMA*: divide il canale da  $R$  bps in multiple frequenze e assegna ciascuna di queste frequenze ai nodi.
- *CDMA*: assegna un codice a ogni nodo, e ogni nodo usa quel codice per codificare i bit da inviare.

### 1.3.2 Protocolli ad accesso casuale

Con questi protocolli, il nodo mittente trasmette alla velocità concessa dal canale. Quando avviene una collisione, i nodi affetti ritrasmettono il pacchetto finché non viene ricevuto, attendendo prima di ritrasmettere il pacchetto. Ogni nodo sceglie indipendentemente l'intervallo di ritrasmissione.

#### Slotted ALOHA

Assumiamo che i frame abbiano tutti la stessa dimensione  $L$ , il tempo sul canale sia diviso in slot di dimensione  $L/R$ , i nodi siano sincronizzati e se due frame collidono in un slot, tutti i nodi rilevano la collisione in quello slot. Sia  $p$  una probabilità tra 0 e 1.

- Quando un nodo ha un frame da inviare, attende fino al prossimo slot e lo trasmette.
- Se non si verifica una collisione, il nodo non ritrasmette.
- Altrimenti, il nodo rileva una collisione e ritrasmette il suo frame negli slot successivi con probabilità  $p$  finché non riesce a ritrasmettere senza collisione

La probabilità introduce casualità, che rende più efficiente il protocollo. Slotted ALOHA permette a ogni nodo di trasmettere a full rate ed è decentralizzato, ma nelle collisioni gli slot vengono persi, possono esserci slot inutilizzati ed è necessario un meccanismo di sincronizzazione. Inoltre, non è molto efficiente: con un gran numero di nodi, solo il 37% degli slot viene effettivamente utilizzato.

## CSMA

I protocolli CSMA e CSMA/CD seguono due regole:

- *carrier sensing*: un nodo ascolta sul suo canale prima di trasmettere; se il canale è occupato, attende
- *collision detection*: se un nodo rileva un altro nodo che sta trasmettendo sul canale, annulla la trasmissione

Nonostante il carrier sensing, le collisioni possono comunque avvenire a causa del ritardo di propagazione. Quando avviene una collisione, tutto il tempo impiegato a inviare un pacchetto viene sprecato. Il CSMA semplice non effettua collision detection.

## CSMA/CD

CSMA/CD effettua collision detection, annullando una trasmissione se nota che il canale è occupato. Prima di ritrasmettere, il nodo attende una quantità di tempo casuale. Algoritmo CSMA/CD di Ethernet:

1. Ethernet riceve il datagramma dal livello rete e lo incapsula in un frame.
2. Se il canale è libero, trasmette, altrimenti attende.
3. Se non vengono rilevate collisioni, la trasmissione è andata a buon fine.
4. Altrimenti, la trasmissione viene annullata e viene inviato un segnale.
5. Ethernet entra in fase di *binary exponential backoff*: dopo la  $m$ -esima collisione, sceglie un numero  $K$  con  $0 \leq 2^{m-1}$ . Attende  $512K$  bit volte e ritorna al punto 2, ripetendo fino al completamento della trasmissione.

### 1.3.3 Protocolli a turni

I protocolli a turni permettono di ottenere buone prestazioni sia con carichi leggeri che con carichi pesanti.

- *Polling protocol*. Un nodo viene scelto come nodo master. Questo interPELLa ognuno dei nodi con metodo round-robin. In questo modo, vengono eliminate le collisioni e non ci sono tempi morti. I principali svantaggi sono l'introduzione di un ritardo di polling, la latenza e il potenziale fallimento del nodo master.
- *Token-passing protocol*. Un frame apposito, detto token, viene passato in ordine tra i nodi. Quando un nodo riceve un token, lo tiene finché ha dei frame da trasmettere. I principali svantaggi sono l'overhead introdotto dal token, la latenza e il fatto che il token rappresenta un potenziale punto di rottura.

## 1.4 Switched Local Area Networks

Gli switch utilizzano indirizzi propri al livello collegamento per inoltrare frame.

### 1.4.1 Indirizzamento nel livello collegamento e ARP

#### Indirizzi MAC

Le interfacce di rete degli host e dei router hanno indirizzi livello collegamento, ma non gli switch. Un indirizzo livello collegamento viene chiamato *indirizzo MAC*. Gli indirizzi MAC sono di solito lunghi 6 bytes (48 bit) e sono espressi in notazione esadecimale. Ogni interfaccia nella LAN ha un unico indirizzo

MAC e un (localmente) unico indirizzo IP. Ogni interfaccia possiede un unico indirizzo MAC perché questi sono controllati dalla IEEE.

Quando un'interfaccia vuole inviare un frame, inserisce l'indirizzo MAC di destinazione nel frame e lo inoltra sulla LAN. Se un mittente vuole inviare un frame a tutte le interfacce presenti sulla LAN, questo inserisce un indirizzo speciale, l'*indirizzo broadcast* nel frame.

## ARP

ARP è il protocollo che si occupa della traduzione tra indirizzi IP e MAC, ma solo per interfacce sulla stessa sottorete.

Ogni host e router possiedono una *tabella ARP*, che contiene mappature tra indirizzi IP e MAC, e un valore di time-to-live che indica la durata di quella voce nella tabella.

Per ottenere l'indirizzo MAC del destinatario, un mittente invia sull'indirizzo MAC di broadcast un *pacchetto ARP*, attendendo la risposta del nodo con l'indirizzo IP corrispondente. Una volta ricevuta la risposta, il mittente aggiorna la sua tabella ARP.

## Inviare datagrammi in un'altra sottorete

Come inviare un datagramma da un host *A* a un host *B*? Supponiamo *A* conosca l'indirizzo IP di *B*, l'indirizzo IP del router e l'indirizzo MAC del router (via ARP). Allora:

- *A* crea un datagramma con destinazione l'indirizzo IP *B* (non può conoscere il suo MAC)
- *A* incapsula il datagramma in un frame indirizzato al router
- il frame è ricevuto dal router e passato a IP
- il router determina la giusta interfaccia sulla quale inoltrare il datagramma
- il router incapsula il datagramma con destinazione indirizzo MAC di *B*

### 1.4.2 Ethernet

La LAN Ethernet originamente utilizzava un bus coassiale per connettere i nodi, e i frame erano trasmessi in broadcast. Successivamente, il bus è stato rimpiazzato con uno switch, che a differenza dei router opera esclusivamente sul livello collegamento.

## Struttura di un frame Ethernet

- *Preambolo*. Serve a sincronizzare le interfacce.
- *Indirizzo di destinazione*. Contiene l'indirizzo MAC di destinazione.
- *Indirizzo di provenienza*. Contiene l'indirizzo MAC di provenienza.
- *Tipo*. Serve all'interfaccia di destinazione per indirizzare il frame al giusto protocollo di livello rete.
- *Campo dati*. Contiene il datagramma IP.
- *CRC*.

Ethernet è connectionless e non affidabile.

### 1.4.3 Switch

Gli switch sono dispositivi operanti nel livello collegamento. Sono trasparenti agli host e ai router nella sottorete. Gli switch, come i router, hanno dei buffer per contenere i frame in eccesso.

#### Forwarding e filtering

Il *filtering* è la funzionalità degli switch che determina se un frame deve essere inoltrato o scartato. Il *forwarding* è la funzionalità che determina le interfacce alle quali il frame va inoltrato. Queste funzioni sono svolte tramite una *tabella di switching*. Questa tabella contiene informazioni su alcuni dispositivi presenti in LAN. Ogni voce contiene un indirizzo MAC, il numero di interfaccia dello switch che porta a quell'indirizzo, e quando quell'indirizzo è stato aggiunto alla tabella.

Supponiamo che un frame con indirizzo di destinazione DD-DD-DD-DD-DD-DD giunga a uno switch sull'interfaccia  $x$ . Lo switch consulta la sua tabella. Si possono verificare tre casi.

- Nessuna voce nella tabella corrisponde all'indirizzo DD-DD-DD-DD-DD-DD. Lo switch inoltra copie del frame a tutte le interfacce eccetto l'interfaccia  $x$ .
- È presente una voce corrispondente nella tabella, che associa l'indirizzo DD-DD-DD-DD-DD-DD con l'interfaccia  $x$ . Non serve inoltrare il frame ad altre interfacce, quindi viene scartato (filtering).
- È presente una voce corrispondente nella tabella, che associa l'indirizzo DD-DD-DD-DD-DD-DD con l'interfaccia  $y \neq x$ . Il frame viene inoltrato sul segmento della LAN corrispondente all'interfaccia  $y$  (forwarding).

#### Self-Learning

La tabella di uno switch viene riempita automaticamente, dinamicamente e autonomamente.

1. La tabella è inizialmente vuota.
2. Per ogni frame in arrivo, lo switch memorizza nella sua tabella l'indirizzo MAC del mittente del frame, l'interfaccia dal quale è arrivato e quando.
3. Lo switch elimina dalla tabella un indirizzo se nessun frame con quell'indirizzo viene ricevuto in un certo lasso di tempo.

#### Proprietà

- *Eliminazione delle collisioni*. In una LAN gestita tramite switch non ci sono collisioni. Gli switch bufferizzano i frame e non trasmettono più di un frame su uno stesso segmento.
- *Collegamenti eterogenei*. Poiché uno switch isola segmenti di LAN l'uno dall'altro, questi possono avere velocità differenti o operare su architetture differenti.
- *Gestione*. Uno switch semplifica la gestione della rete. Se un'interfaccia di un dispositivo si guasta e continua a inviare frame in broadcast, uno switch può rilevare il problema e disconnettersi dall'interfaccia malfunzionante.

### 1.4.4 VLAN

Le reti LAN tradizionali non sono facilmente scalabili o portabili, ma le VLAN sì. Uno switch che supporta VLAN permette di definire LAN virtuali su una singola LAN fisica. Gli host su una VLAN possono comunicare tra loro come se fossero solo loro connessi a quello switch.

Nelle VLAN basate su porte, le porte dello switch sono divise in gruppi. Ogni gruppo costituisce una VLAN, e le porte in ogni VLAN formano un dominio di broadcast. Per connettere due VLAN bisogna utilizzare un router.

Una soluzione più scalabile per connettere due VLAN è detta *VLAN trunking*. Una porta dello switch è designata come porta per connettere due VLAN. Questa porta appartiene a tutte le VLAN, e i frame inviati a ogni VLAN sono inoltrati su quel collegamento a un altro switch. I frame che passano per il trunk sono in uno speciale formato, detto 802.1Q. Questi frame sono identici ai frame Ethernet standard, ma possiedono una *tag VLAN* nell'header che contiene informazioni circa la VLAN alla quale il frame appartiene.

## 1.5 Networking nei data center

### 1.5.1 Architetture dei data center

I data center non sono solamente connessi a Internet, ma a dei loro network interni che connettono gli host tra loro. Gli host nei data center sono chiamati *blades*, impilati in rack. In cima ad ogni rack c'è uno switch, detto *Top of Rack* (TOR), che connette gli host nel rack tra di loro e con gli altri switch nel data center. Ogni host nel rack ha un'interfaccia di rete che si connette al proprio TOR, e ogni TOR ha porte che possono essere connesse ad altri switch.

I data center supportano due tipi di traffico: il traffico tra client esterni e host interni e traffico tra host interni. Per gestire il primo, i data center utilizzano dei *border router*, che connettono il data center con Internet.

#### Load balancing

Le richieste ricevute da un data center sono innanzitutto dirette a un load balancer che si occupa di distribuire le richieste agli host. I grossi data center possiedono molti load balancer, ognuno dedicato a specifiche applicazioni cloud. Un tale load balancer è spesso chiamato "layer-4 switch" in quanto basa le sue decisioni sul numero di porta e sull'indirizzo IP del pacchetto. Al ricevimento di una richiesta, il load balancer la inoltra a uno degli host che gestisce l'applicazione. Il load balancer funziona anche come NAT, in quanto traduce l'IP pubblico della richiesta nell'IP interno e viceversa.

## 1.6 Il processamento di una richiesta

# Capitolo 2

## Livello fisico

### 2.1 Comunicazione dei dati

#### 2.1.1 Segnali a larghezza di banda limitata

L'ampiezza del range di frequenza trasmessa senza essere attenuata è detto larghezza di banda, ed è una proprietà fisica del mezzo di trasmissione.

I segnali che vanno da 0 a una frequenza massima sono detti baseband. Quelli che sono spostati per occupare un range di frequenze più alto sono detti passband.

#### 2.1.2 Data rate massimo per una canale

Equazione di Nyquist per derivare il data rate massimo per un canale senza rumore con banda finita:

$$\text{data rate massimo} = 2B \log_2 V \text{ bit/sec}$$

Se un segnale viene fatto passare attraverso un low-pass filter di banda  $B$ , il segnale filtrato può essere ricostruito con  $2B$  campioni al secondo.  $V$  sono i livelli discreti differenti. In presenza di rumore il segnale degrada rapidamente. Il rumore si misura come il quoziente tra potenza di segnale e potenza del rumore, detto SNR, unità decibel.

Equazione di Shannon:

$$\text{numero massimo di bit/secondo} = B \log_2 \left(1 + \frac{S}{N}\right)$$

### 2.2 Modulazione digitale

Il processo di convertire tra bit e segnali è detto modulazione digitale.

#### 2.2.1 Trasmissione baseband

La forma di modulazione più diretta è quella di utilizzare una tensione positiva per rappresentare 1 e una negativa per lo 0. Questo schema è detto NRZ (Non-return-to-zero). Per decodificare i bit, il destinatario mappa i segnali ai simboli più coerenti.

Con NRZ, il segnale si alterna tra due livelli, quindi è necessaria una banda di almeno  $\frac{B}{2}$  se il bit rate è  $B$  bit al secondo. Utilizzando quattro tensioni diverse, si possono inviare 2 bit alla volta come singolo simbolo.

È necessario un clock accurato per distinguere i bit (es. molti 0 di fila). Una strategia è inviare segnale di clock separato al destinatario, mettendo in XOR il segnale di clock e quello dei dati. Una transizione

da alta e bassa tensione simbolizza uno 0, da bassa a alta un 1: questo schema è detto Manchester. Necessita di banda doppia rispetto a NRZ.

Si può codificare 1 come transizione e 0 come non transizione: NRZI.

4B/5B: ogni 4 bit sono mappati a una sequenza di 5 bit con una tabella di traduzione fissa. Aggiunge 25% di overhead.

Scrambling: XOR tra dati e una sequenza pseudorandom.

### **Segnali bilanciati**

Segnali che hanno tanta tensione positiva che negativa sono detti bilanciati. Non hanno componente DC.

Un modo per costruire un codice bilanciato è utilizzare due tensioni diverse per rappresentare 1, mentre 0 è rappresentato da 0 volt: bipolar encoding.

### **2.2.2 Trasmissione passaband**

Il segnale baseband è aumentato per occupare una banda da  $S$  a  $S + B$  Hz senza cambiare la quantità di dati trasmessa. ASK utilizza due diverse ampiezze per rappresentare 0 e 1. FSK usa due o più toni. PSK: l'onda cambia fase, da 0 a 180 gradi. Se utilizza 4 fasi, è detta QPSK.

### **FDM**

FDM utilizza trasmissione passband per condividere un canale. Divide lo spettro in bande di frequenza separate da un eccesso detto band guard. Ci sono comunque sovrapposizioni tra canali.

In OFDM, la banda del canale è suddivisa in molti subcarrier che inviano dati indipendentemente. I subcarrier sono campionati nella loro frequenza centrale senza interferenza.



# Capitolo 3

## Reti wireless e mobili

### 3.1 Elementi delle reti wireless

Nelle reti wireless si possono identificare i seguenti elementi:

- *Host wireless.*
- *Collegamenti wireless.* Un host si connette a una base station o un altro host wireless tramite un collegamento wireless.
- *Base station.* Gestisce l'invio e la ricezione dei dati da e a un host wireless associato. Gli host associati con una base station operano in *modalità infrastruttura*. Nelle *reti ad hoc*, gli host non hanno un'infrastruttura a cui connettersi.

Classificazione dei network wireless:

- *Single-hop, con infrastruttura.* Queste reti hanno una base station connessa a una rete più grande, e tutte le comunicazioni avvengono in uno solo wireless hop (4G LTE).
- *Single-hop, senza infrastruttura.* Non hanno base station connessa a una rete wireless (Bluetooth).
- *Multi-hop, con infrastruttura.* I nodi comunicano tra di loro prima di connettersi alla base station (wireless mesh networks).
- *Multi-hop, senza infrastruttura.*

### 3.2 Collegamenti wireless e caratteristiche

Problematiche dei collegamenti wireless:

- *Diminuzione della potenza di segnale.*
- *Interferenza da altre sorgenti.*
- *Propagazione multipath.*

Il *signal-to-noise ratio* (SNR) è la misura relativa della potenza del segnale ricevuto e del suo rumore. È misurata in decibel. Maggiore è il SNR, più facile diventa estrarre il segnale dal rumore di sottofondo.

Per un dato sistema di modulazione, maggiore è il SNR, minore sarà il bit error rate (BER). Un mittente può incrementare il SNR incrementando la potenza di trasmissione, ma ciò richiede più energia.

Per un dato SNR, una tecnica di modulazione con un bit transmission rate maggiore avrà un BER maggiore.

## CDMA

In un protocollo CDMA, ogni bit inviato viene codificato moltiplicandolo per un segnale (il codice) che varia molto più velocemente (chipping rate) della sequenza di bit originale. Supponiamo che ogni bit trasmesso richieda uno slot di tempo da un bit. Sia  $d_i$  il valore del bit per lo slot  $i$ -esimo. Ogni slot è diviso in  $M$  mini-slot. Il codice CDMA utilizzato dal mittente consiste in una sequenza di  $M$  valori.

Per il  $m$ -esimo mini-slot del tempo di trasmissione del bit  $d_i$ , l'output del codificatore CDMA,  $Z_{i,m}$ , è pari a:

$$Z_{i,m} = d_i \cdot c_m$$

Il destinatario può recuperare la sequenza di bit originale calcolando:

$$d_i = \frac{1}{M} \sum_{m=1}^M Z_{i,m} \cdot c_m$$

Con più mittenti, il valore ricevuto dal destinatario è la somma dei bit trasmessi dagli  $N$  mittenti in quel mini-slot:

$$Z_{i,m}^* = \sum_{s=1}^N Z_{i,m}^s$$

Se i codici sono scelti in maniera opportuna, ogni destinatario può utilizzare la seconda equazione per recuperare i dati ricevuti.

## 3.3 Reti WLAN 802.11

Lo standard IEEE 802.11 wireless LAN, detto anche WiFi, è lo standard più utilizzato.

### 3.3.1 Architettura

Il blocco fondamentale dell'architettura 802.11 è il *basic service set* (BSS). Un BSS contiene una o più stazioni wireless e una base station centrale, detto *access point* (AP). Ogni wireless station possiede un indirizzo MAC.

### Canali e associazioni

Quando un amministratore installa un AP, gli assegna un *service set identifier* (SSID) e un numero di canale. 802.11 definisce 11 canali parzialmente sovrapposti. Due canali non si sovrappongono solo se sono separati da 4 o più canali.

Per ottenere accesso a Internet, un dispositivo wireless deve associarsi con un AP. Un AP invia periodicamente dei *beacon frame* contenenti il proprio SSID e indirizzo MAC. Il dispositivo wireless scandisce gli 11 canali per individuare i beacon frame.

Il processo di scandire i canali è detto *passive scanning*. Un dispositivo wireless può anche condurre *active scanning* inviando in broadcast un frame che viene ricevuto da tutti gli AP in range.

Una volta scelto l'AP al quale collegarsi, il dispositivo invia un frame di richiesta di associazione all'AP, e questo risponde con un frame di risposta. Una volta associato con un AP, il dispositivo invia un messaggio DHCP nella sottorete tramite l'AP per ottenere un indirizzo IP.

Per associarsi con un AP, il dispositivo potrebbe doversi autenticare. L'autenticazione può avvenire tramite indirizzo MAC o username e password. In entrambi i casi, l'AP comunica con un server d'autenticazione.

### 3.3.2 Il protocollo MAC 802.11

Il RLC frammenta e riasmonta utilizzato da 802.11 è ad accesso casuale ed è chiamato *CSMA/CA*.

Quando una stazione di destinazione in una rete WLAN riceve un frame che intatto (il CRC è corretto), attende per un determinato lasso di tempo, detto *short inter-frame spacing* (SIFS) e poi invia un frame di acknowledgement. Se il mittente non riceve un ACK, ritrasmette il frame usando il protocollo CSMA/CA. Passi per inviare un frame:

1. Se la stazione vede che il canale è vuoto, trasmette un frame dopo un certo lasso di tempo detto *distributed inter-frame space* (DIFS).
2. Altrimenti, la stazione sceglie un valore di backoff casuale e attende.
3. Quando il tempo scade, la stazione invia un frame e attende un ACK.
4. Se l'ACK viene ricevuto, la stazione mittente sa che il frame è arrivato a destinazione. Se ha un altro frame da trasmettere, ritorna al punto 2. Se l'ACK non viene ricevuto, ritorna al passo 2 scegliendo un tempo di backoff più lungo.

A differenza di CSMA/CD, CSMA/CA non invia frame se il DIFS non è terminato, anche se il canale è libero.

#### RTS e CTS

Per evitare il problema dei terminali nascosti, 802.11 permette alla stazione di utilizzare un frame *request to send* (RTS) e un frame *clear to send* (CTS) per riservare un canale. Quando un mittente vuole inviare un frame contenente dati, invia innanzitutto un frame RTS all'AP, indicando il tempo richiesto per trasmettere i dati e un frame di ACK. Quando l'AP riceve un frame RTS, risponde inviando a tutti gli host (broadcast) un frame CTS. Questo frame previene alle altre stazioni di trasmettere.

### 3.3.3 Il frame IEEE 802.11

È simile a un frame Ethernet.

#### Payload e CRC

Il payload consiste in un pacchetto ARP o un datagramma IP. I frame 802.11 includono un CRC a 32 bit.

#### Indirizzi

Il frame 802.11 ha 4 campi di indirizzi, ognuno dei quali può contenere un indirizzo MAC a 6 byte.

- L'indirizzo 1 è l'indirizzo MAC della stazione di destinazione.
- L'indirizzo 2 è l'indirizzo MAC della stazione mittente.
- L'indirizzo 3 è l'indirizzo MAC dell'interfaccia router associata all'AP.
- L'indirizzo 4 è utilizzato solo in modalità ad hoc.

#### Numeri di sequenza, durata e frame control

Il numero di sequenza garantisce reliable data transfer, permettendo al destinatario di distinguere tra un frame appena trasmesso e una ritrasmissione. Il campo durata permette di riservare il canale per un certo periodo di tempo. Il frame control contiene campi che descrivono il tipo di frame.

### 3.3.4 Mobilità nella stessa sottorete IP

Quando un host si muove nella stessa sottorete IP, il suo indirizzo IP rimane invariato. Gli switch sono in grado (grazie al self-learning) di ricordare quale porta può essere utilizzata per raggiungere quell'host.

### 3.3.5 Caratteristiche avanzate di 802.11

#### Rate adaptation

Alcune implementazioni di 802.11 sono in grado di selezionare adattivamente la tecnica di modulazione, variando di conseguenza il SNR. Quando un host si allontana dalla base station, il SNR diminuisce e aumenta il BER: quando il BER diventa troppo elevato, la stazione riduce il tasso di trasmissione per ridurlo.

#### Power management

Un nodo può annunciare all'AP la sua entrata nello stato di sleep. L'AP bufferizza i frame finché il nodo non si sveglia. Ciò permette al nodo di risparmiare energia.

### 3.3.6 Bluetooth

Le reti Bluetooth vengono anche chiamate *wireless personal area networks* (WPAN). Operano nella banda radio 2.4 GHz; i canali sono gestiti con TDM, con frequenza di canale variabile. Le reti Bluetooth non possiedono infrastruttura: i nodi si organizzano in una rete di al più 8 elementi. Uno di questi elementi è detto *master*, gli altri sono *client*. Il master determina il tempo per il cambio di slot e canale, controlla i dispositivi nella rete. Oltre a 8 dispositivi attivi, ci possono essere fino a 255 dispositivi "parked", che si risvegliano secondo uno scheduling imposto dal master.

Quando un nodo master vuole formare una rete Bluetooth, deve innanzitutto determinare quali dispositivi si trovano nel suo range (*neighbor discovery*). Per farlo, il master invia in broadcast una serie di 32 messaggi di inquiry, ognuno un canale differente. I client ascoltano sui canali; una volta ricevuto un messaggio di inquiry, va in backoff (per evitare collisioni con altri client) e risponde al master con un messaggio contenente l'ID del dispositivo.

Quando il master ha scoperto tutti i client, li invita nella sua rete. La seconda fase è detta *Bluetooth paging*. Il master informa i client del pattern di frequency hopping che userà e il clock del mittente. Quando il client riceve le informazioni, risponde con un ACK e il master li interroga usando il pattern scelto per assicurarsi che siano connessi alla rete.

#### Standard ZigBee

È l'unico standard open source. Utilizza una topologia mesh, scalabile, in grado di coprire una vasta area con dispositivi a basso consumo energetico.

ZigBee prevede due tipi di indirizzi, uno a 64 per identificare il dispositivo univocamente e uno a 16 bit assegnato a un dispositivo quando si associa alla rete. Nell'architettura ci sono tre tipi di nodi: il coordinatore PAN, che gestisce la rete, i full function device, che funzionano come router, e i reduced function device che funzionano da endpoint.

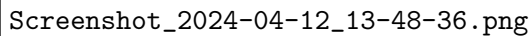
## 3.4 Reti cellulari: 4G e 5G

Il termine cellulare si riferisce al fatto che la regione coperta da una rete cellulare è divisa in una serie di aree geografiche, dette *celle*. Ogni cella contiene una *base station* che trasmette e riceve i segnali dai dispositivi mobili presenti nella cella.

### 3.4.1 Reti cellulari 4G

Elementi di una rete 4G:

- *Dispositivi mobili.* Si connettono alla rete cellulare. Hanno un identificatore unico detto International Mobile Subscriber Identity (IMSI), memorizzato nella SIM.
- *Base station.* Gestisce le risorse radio e i dispositivi mobili nella sua cella, coordinando l'autenticazione dei dispositivi e l'allocazione delle risorse.
- *Home Subscriber Server.* È un database che memorizza informazioni sui dispositivi nell'home network.
- *Serving Gateway (S-GW), Packet Data Network Gateway (P-GW) e altri.* S-GW e P-GW sono due router nel percorso tra il dispositivo mobile e l'Internet. P-GW svolge funzioni simili a un router gateway e fornisce servizi NAT.
- *Mobility Management Entity.* Il MME è un elemento del piano di controllo. Insieme a HSS, fornisce autenticazione dei dispositivi e gestisce il passaggio di cella.

A screenshot of a document page, likely from a PDF, showing a large empty rectangular area. The text 'Screenshot\_2024-04-12\_13-48-36.png' is visible at the bottom left of the page, indicating the file name and timestamp of the capture.

### 3.4.2 Protocolli LTE

LTE suddivide il livello collegamento del dispositivo mobile in tre sottostrati:

- *Packet Data Convergence*. Questo strato si trova sotto IP. Il protocollo PDCP comprime e cifra i datagrammi IP.
- *Radio Link Control*. Il protocollo RLC frammenta e riassembla i datagrammi IP, e garantisce trasporto affidabile grazie al protocollo ARQ.
- *Medium Access Control*. Il livello MAC gestisce lo scheduling delle trasmissioni e svolge controllo degli errori.

I dispositivi sono connessi alla base station da tunnel IP, definiti quando un dispositivo si collega alla rete. Ogni tunnel ha un identificatore (TEID). Quando la base station riceve datagrammi dal dispositivo

mobile, li incapsula utilizzando il GPRS Tunneling Protocol, e li invia in segmenti UDP al Server Gateway all'altro estremo del tunnel.

### 3.4.3 Rete di accesso radio

LTE utilizza una combinazione di FDM e TDM per il canale downstream, detta orthogonal frequency division multiplexing (OFDM). Ad ogni dispositivo mobile viene allocato uno o più time slots da 0.5 ms in uno o più canali. Lo scheduling delle trasmissioni è determinato dagli algoritmi forniti dai fornitori di equipaggiamento LTE.

#### Collegamento alla rete

- *Collegamento a una base station.* Il dispositivo mobile scandisce i canali in tutte le bande di frequenza per trovare un segnale di sincronizzazione inviato in broadcast da una base station. Una volta individuato, il dispositivo rimane sul canale e attende un secondo segnale di sincronizzazione. Il dispositivo ottiene ulteriori informazioni sulla base station. Con queste informazioni, il dispositivo può scegliere la base station migliore alla quale connettersi.
- *Autenticazione.* Il dispositivo rende noto alla rete la sua associazione con un determinato IMSI, autenticandosi con il MME.
- *Configurazione del percorso da dispositivo a PDN.* MME contatta il gateway PDN, il Serving gateway e la base station per stabilire i tunnel.

#### Gestione dell'energia

Un dispositivo mobile può trovarsi in due stati di sleep:

- *Light sleep.* Il dispositivo si risveglia periodicamente (ogni 100 msec) per controllare le trasmissioni downstream.
- *Deep sleep.* Il dispositivo si risveglia periodicamente ogni 5 o 10 secondi.

### 3.4.4 Rete cellulare globale

L'home network di un utente è collegato alle reti degli altri carrier mobili e a Internet tramite router gateway. Le reti mobili sono connesse tra loro dall'Internet pubblico o da un Internet Protocol Packet eXchange (IPX) Network.

## 3.5 Gestione della mobilità

Se un dispositivo si muove dal suo access network, continuando a inviare datagrammi IP, la rete dovrà svolgere *handover*.

### 3.5.1 Routing indiretto

1. I datagrammi sono inviati all'home network, indirizzati all'indirizzo permanente del dispositivo mobile da raggiungere.
2. Il gateway dell'home network intercetta i datagrammi, consulta HSS per determinare il visited network dove il dispositivo mobile risiede, li incapsula in un altro datagramma (lasciando quello originale intatto) e lo inoltra al gateway router del visited network.

3. Il visited network gateway router riceve il datagramma, lo decapsula e lo inoltra al dispositivo mobile.
4. Due opzioni:
  - (a) Il datagramma geenerato dal dispositivo mobile viene spedito all'home gateway router e al corrispondente.
  - (b) Il datagramma viene inviato direttamente al corrispondente dal visited network (*local breakout*).

### 3.5.2 Routing diretto

Il routing indiretto soffre del problema di triangle routing. Il direct routing supera l'inefficienza interrogando l'HSS dell'home network del dispositivo. Il corrispondente può così inviare diagrammi direttamente al gateway router del visited network.

### 3.5.3 Gestione della mobilità nelle reti 4G/5G