Appunti Reti2

Brendon Mendicino

October 25, 2022

Contents

1 Introduzione

...

2 Multicast

Gli indirizzi che identificano dei gruppi multicast sono quelli di tipo D, iniziano con 1110 (224.0.0.0 − 239.255.255.255).

Si prendono i 23 bit bassi dell'IP e vengono assegnati ai 23 bit bassi dell'indirizzo MAC multicast, questa operazione si chiama di **join** ad un gruppo multicast. Questo approccio potrebbe portare a dei conflitti, la probalità che una collisione avvenga è molto bassa ma non è zero, i conflitti comportano ricevere il traffico di un altro gruppo multicast anche se non abbiamo fatto un join con quello.

Esempio: viene usato l'indirizzo 224.0.0.0 come un gruppo multicast, gli host che vogliono connettersi a questo gruppo dovranno fare il join, e quindi impostare la loro scheda di rete (solitamente una scheda di rete virtuale, in cui viene aggiunto il MAC multicast) con il MAC multicast, in questo caso gli ultimi 23 bit saranno a 0.

3 IPv6

Gli indirizzi ipv6 sono rappresentati su 128, quindi si hanno 2^{128} combinazioni. Per rappresentarli si divide l'indirizzo in 8 gruppi di 2 byte, separati da un ":". Ci sono delle strategie per rendere più leggibile l'indirizzo:

1. gli zeri in fronte possono essere omessi;
2. gli zeri (":0:") posso essere sostituiti con un "::" solo una volta;

Per rappresentare l'indirizzo di rete si usano 64 bit. Il concetto di aggregazione gerarchico viene mentenuto del prefix length e dalla netmask, dunque il prefix viene usato per il subnetting.

I principi di assegnamento sono:

- **subnetwork**: set of host with the same prefix;
- **link**: physical network;
- **on-link**: comunicazioni tra host con lo stesso prefisso;
- **off-link**: comunicazioni tra host con prefisso diverso;

Indirizzi Multicast Il multicast ha una rappresentazione simile ad IPv4, infatti hanno un range di FF00::/8, che si dividono in tre sottocategorie:

- **well-known multicast**: FF00::/12, questo range di indirizzi è assegnato e quindi venduto, utilizzato per scopi di comunicazione;
- **transient**: FF10::/12, assegnati dinamicamente;
- **solicited-node multicast**: FF02:0:0:0:0:1:FF00::/104, simile al broadcast;

Un indirizzo multicast è formato da:

- I primi 8 bit mi identificano un indirizzo multicast, tutti settati ad 1;
- 4 bit assegnati a dei flag: l'unico utilizzabile è il campo T che specifica se l'indirizzo è permanente (0), ovvero assegnato dalla IANA, oppure non-permanente (1), gli altri campi non hanno un'assegnazione;
- gli ultimi 112 rappresentano il **group id**;

4 bit per stabilire lo **scope** per difinire il range di indirizzi multicast;

Unicast Sono l'equivalte degli indirizzi publici IPv4. Quando un nuovo host si collega alla rete, sa automaticamente il suo indirizzo, infatti è gli indirizzi unicast sono plug and play. Gli indirizzi sono composti da:

- 3 bit: 001;
- n bit: global routing prefix;
- m bit: subnet ID;
- 1280-m-n-3 bit: interface ID;

Il prefisso moderno è stato assegnato formalmente da entità multi-livello:

- 3 bit: 001;
- 13 bit: TLA ID, Top Level Authority (Large ISP);
- 32 bit: NLA ID, Next Level Authority (Organizzazione);
- 16 bit: SLA ID, Subnet Level Authority;
- 64 bit: Interface ID;

Link Local/Site Local Gli indirizzi link/site local sono assegnati automaticamente, iniziano con 1111 1110 1... (febf::/), allora:

- link local: usati per gli indirizzi di rete per comunicare,
- site local: fec0::/10, indirizzi deprecati, utilizzati per assegnare degli indirizzi privati univoci;

Unique Local Address Gli ULA sono univoci, rimanendo comunque privati, e quindi non dovrebbero essre esposti alla rete, usando un range è di fc00::/7. La particolarità è che l'ottavo bit è il **local flag** (L), se questo bit è settato ad 1 l'indirizzo è assegnato localmente, se invece è a 0 potrebbe essere assegnato in futuro. I successivi 40 bit sono asseganti casualmente, per mantenere l'univocità.

IPv4 Embedded Address Sono usati per rappresentare gli indirizzi ipv4 sugli indirizzi ipv6. Sono composti da:

- i primi 80 bit a 0;
- 16 bit a 1;
- gli ultimi 32 bit rappreesntano l'indirizzo ipv4;

Loopback Address L'indirizzo ::1 ha lo stesso scopo dell'indirizzo di loopback 127.0.0.1 di ipv4.

Unspecified Address È un indirizzo unicast non specificato ::0, anche in questo caso il suo comportamento è lo stesso di ipov4.

Indirizzi Anycast Ho degli indirizzi assegnati a dei nodi nelle rete e quando mando un pacche voglio che esso arrivi ad uno di essi (inizialmento pensato per i DNS server). Gli indirizzi anycast non sono utilizzati.

3.1 Protocolli IPv6

In ipv6 alcuni protocolli sono stati integrati o rimossi rispetto ad ipv4, infatti ARP ed IGMP sono stati integrati in ICMP, la maggior parte degli altri protoccolli è stata fatta una modifica per supportare gli indirizzi a 128 ma le modifiche rimangono minime.

3.1.1 IP

L'header in ipv6 contiene molte meno dati, il motivo è che le informazioni sono presenti nel padding, tutto ciò è possibile grazie al campo next header. Si crea così una catena di header. Se non ho bisogno di estensioni allora il campo next header punterà all'header tcp.

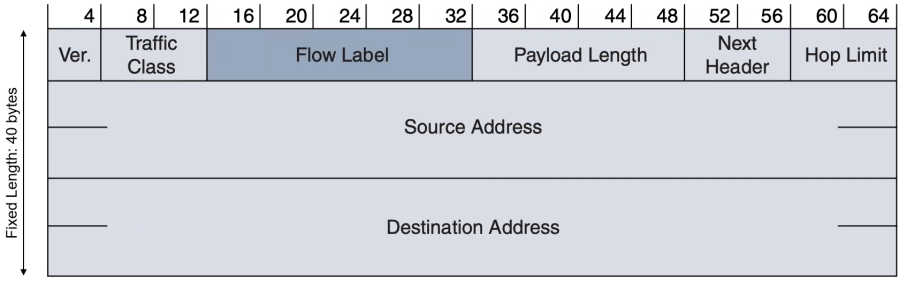

Figure 1: Ipv6 Header

I campi rimasti sono:

- ver: la versione del protocollo;
- traffic class: si definiscono delle classi di pacchetti per determinare delle priorità tra i traffici;
- flow label: etichetta associata al flusso, sarà possibile fare routing grazie a questo campo;
- payload lenght: lunghezza del payload;
- hop limit: time to live del ipv4;
- source address;
- destinatoin address;

Headers extensions Il protocollo utilizza dei codici per specificare quale sarà il campo dell prossima estensione.

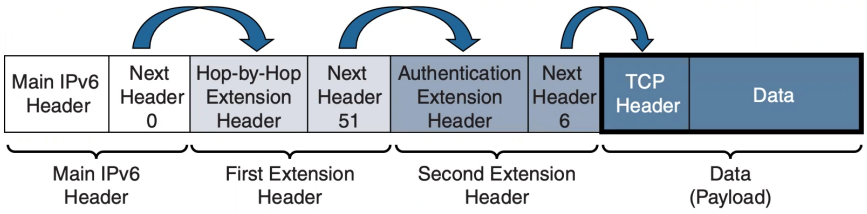

Figure 2: Header Chaining

Gli header hanno tutti lo stesso formato:

- next header;
- length: più o meno dato dell'header;
- extension data: dati dell'header;

3.1.2 Interfaccia con i livelli più bassi

Nel livello si è deciso di differenziare il protocllo ipv4 e ipv6 (approccio dual stack), infatti nel livello 2 esiste un campo che specifica il protocollo a livello superiore. Il **type** per ipv6 è 86DD.

3.1.3 Mapping

I 32 bit bassi dell'indirizzo ipv6 vengono mappati ai 32 bit bassi dell'indirizzo MAC, questo mapping viene specificato quando i primi 2 byte sono settati a 33:33, dunque un indirizzo MAC mappato sarà 33:33:xx:xx:xx:xx. Quanso si manda un pacchetto all'indirizzo di broadcast ff0c::89:aabb:ccdd l'indirizzo MAC corrispondente sarà 33:33:aa:bb:cc:dd.

3.1.4 Neigbhor Discovery

Il protocollo ARP sarà sostituito dalla nuova version del protocollo ICMPv6.

Il meccanismo avviene nel seguente modo: partendo da un indirizzo unicast si prendono i 24 bit bassi dell'indirizzo e si crea un indirizzo multicast solicited-node con i 24 bit bassi corrispondenti a quelli dell'unicast. Questo permette, quando si fa il mapping, di avere gli indirizzi MAC multicast che iniziano con 33:33:ff, grazie a come sono composti gli indirizzi solicited-node.

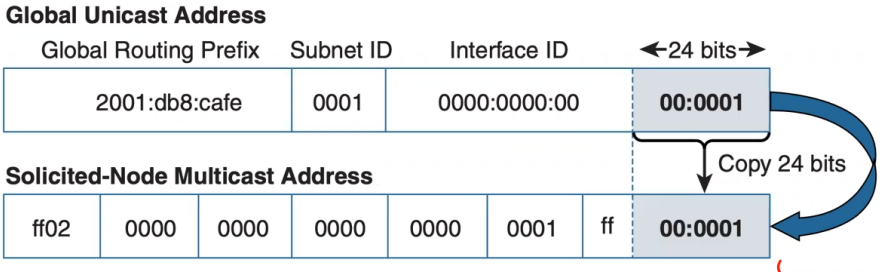

Figure 3: Solicited Node Multicast Address

ARP:

- manda un trama in broadcast;

Multicast:

- manda a tutti;
- manda solo a chi fa parte di un gruppo: il MAC di multicast permette di mandare messaggi solo a chi appartiene a chi potenzialmente fa parte di quel gruppo;

3.2 ICMPv6

Il protocollo mantiene le opzioni di quello usato in ipv4 aggiungnendo delle funzionalità per sostituire ARP e IGMP, ICMP è usato per:

- diagnostica;
- neighbor discovery;
- multicast group;
- issue notification;

3.2.1 Formato del messagio

ICMP è incapsulto nel pacchetto ip.

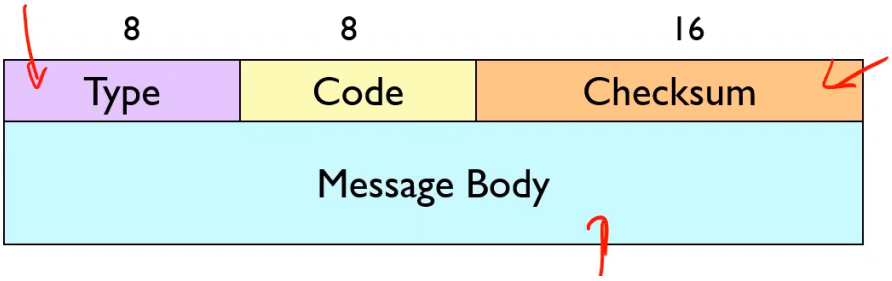

Figure 4: Icmp Format

Messaggi di errore:

- 1: destination unreachable;
- 2: packet too big;
- 3: time exeeded;
- 4: parameter problem;

Echo:

- 128: echo request;
- 129 echo: reply;

Neighbor Solicitation

Neighbor Advertisement Vengono aggiunti 3 flag:

- router: indica se il pacchetto arrivo da un router;
- solicited: specifica se il nodo è stato sollicitato o meno;
- override: specifice se l'host cache deve essere sovrascritta;

L'indirizzo MAC viene messo nel campo options, mente l'ip di sorgente viene messo nel campo target address.

3.2.2 Group Management

Da rivedere...

- query;
- report;
- done;

3.3 Configurazione

Le informazioni necessarie sono:

- address prefix;
- interface id;
- default gateway;
- dns server;
- host name;
- domain name;
- MTU maximux transmission unit;

Per creare queste informazioni:

- stateful config: informazioni date da un DHCP;
- stateless config: generate automaticamente;
- ibrida (stateless DHCP);

3.3.1 Interface ID

Si può configurare manualmente, ottenere dal DHCP oppure generati automaticamente. Nel modo di configurare i 64 bit bassi non si hanno garanzie che siano univoci, esiste un protocollo che permette il controllo e l'univocità.

EUI-48 to EUI-64 Mapping EUI = Extended Unique Id
OUI = Organization Unique Id

Per creare l'interface ID in modo automatico si può sfruttare la tecnica del mapping, si prende il MAC del interfaccia e viene mappato nel seguente modo:

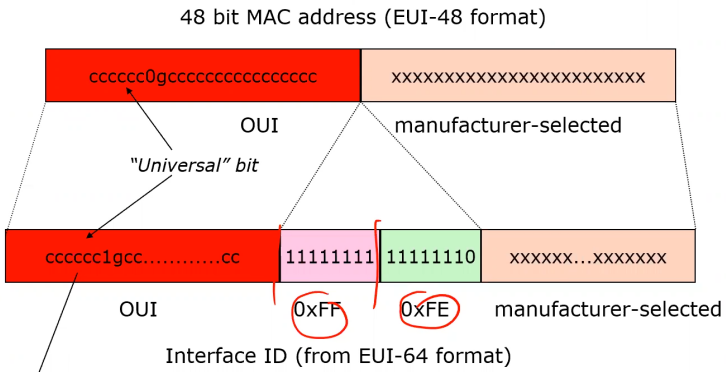

Figure 5: Mac To Id Mapping

Il settimo bit viene settato a 0 se l'ID viene assegnato automaticamente, mentre viene settato a 1 se l'ID è stato assegnato manualmente (quidni l'indirizzo sarà necessariamente univoco), questa è una convenzione ma non la regola.

Privacy Extension Algorithm Per evitare che l'interface Id possa essere calcolato da qualcun'altro ch conosca il MAC del mio dispositivo si usa un approccio per garantire maggior privacy ed aumentare la sicurezza.

Per generare l'interface Id si prendono 64 bit random e 64 bit generati del MAC mapping e poi viene fatto un hash. In fine il settimo bit viene settato a 0 perché non si ha comunque la certezza che l'interface Id sia univoco.

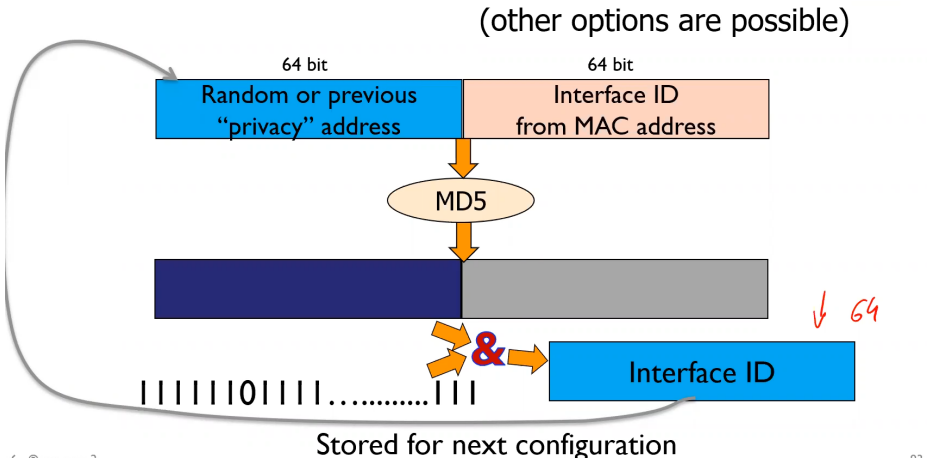

Figure 6: Privacy Extension Alogorithm

3.3.2 Address Prefix

Anche in qeusto caso è possibile configurare la parte alta dell'indirizzo ip in modo manuale oppure in modo automatico.

Per ottenere queste informazioni in modo automatico esistono due messaggi:

- **Router Solicitation**: nelle opzioni solitamente si chiede l'indirizzo

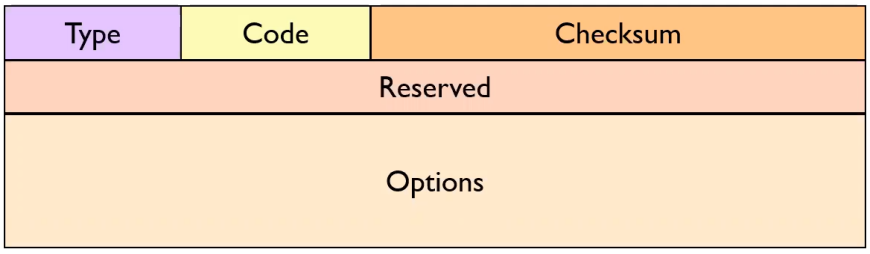

Figure 7: Router Solicitation

- **Router Advertisement**: può essere una risposa ad una solicitaion, M (Managed Address Configuration): se settato ad 1 indica che l'indirizzo è disponibile via DHCP; O (Other Configuration): parametri come il DNS server; Reachable Time: tempo in cui il router è disponibile; Retrans Timer: tempo in cui l'indirizzo è disponibile;

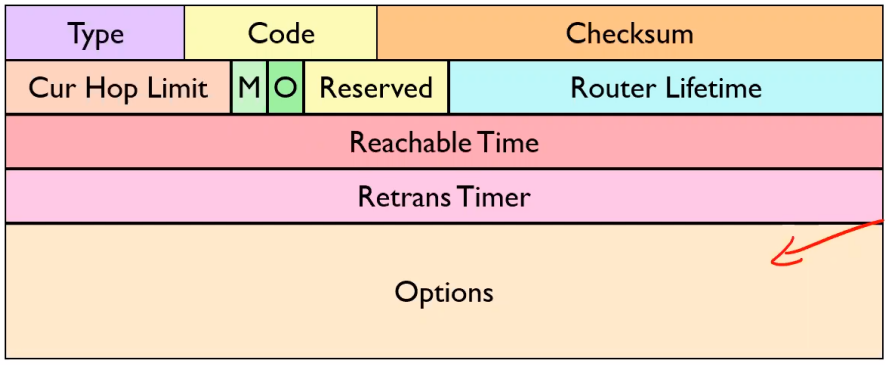

Figure 8: Router Advertisement

Quando un host si collega ad una rete potrà fare una solicitation e ricevere una advertisement oppure i router periodicamente mandano una advertisement.

Le informazioni sul prefisso sono:

- L: ad 1 se il prefisso può essere on-link;
- A: ad 1 se il prefisso può essere usato con una configurazione autonoma;

Un'altra informazione è il **Link Layer Address Option**, si mette il MAC del default gateway.

Un messaggio molto importante è l'**ICMP Redirect**, in una rete ci sono più router, l'host manda i pacchetti al suo default gateway, se per raggiungere un altro host un altro è router è più vicinino allora i pacchetti vengono rediretti in quel router.

3.3.3 Duplicate Address Detection (DAD)

L'host manda un messaggio di DAD. Per verificare che non esistano indirizzi duplicati ...

3.4 Stateless Config

Il link local address viene generato automaticamente, successivamente viene fatta una DAD, l'host si iscrive al Solicited Node Multicast Address, abilita le comunicazioni on-link.

Una volta acquisita la parte bassa si ottiene la parte alta: router solicitation, router advertisement listening, si crea il prefisso dall'adversement, si fa una DAD, ci si iscrive al Soliced Node Mutlicast Address.

Un altra grosso vantaggio è il **Renumbering**, tramite l'advertisement si riassegnano gli indirizzi in modo automatico.

3.5 Stateful Config

La configurazione stateful rimane invariata tranne che per le informazioni date dal flag M. ...

4 Scope

Qunado un dispositivo ha più interfaccie, gli indirizzi generati automaticamente saranno gli stessi, per distinguere le due interfacce l'host tiene conto a quale interfaccia mandare un messaggio. Per distinguere le due interfaccie si mette %x, dove x è l'id dell'interfaccia.

5 IPv6 Transitioning

5.1 IPv4 Traversing

Si fa del **Tunneling**, partendo da un paccheto ipv6 che si interfaccia ad una rete ipv4, si parte da un indirizzo ipv4 e nul suo header viene encapsulato l'indirizzo ipv6. Le soluzioni ci permettono di avere un mapping automatico o manule:

- **IPv4-compatible**: quando devo inviare un messaggio a destinazione gli ultimi 32 bit dell'indirizzo ipv6 sono i bit dell'indirizzo ipv4 (::/96);
- **6over4**: sfrutta il multicast dell'ipv4 e dell'ipv6;
- **ISATAP**: si basa su un prefisso comune (fe80::5efe) e gli ultimi 32 bit come l'indirizzo ipv6,
- ...

6 Wireless and Cellular Networks

6.1 Wireless LAN

Le caratterisiche del link wireless sono:

- un link Wireless ha un degrado maggiore del segnale, rispetta ad una fibra ottica;
- è soggetto a interferenze;
- problema del **fading**, causato dai rimbalzi del segnale su ostacoli;

Esistono vari standard dello IEEE 802.11 wireless LAN, i più moderni arrivano fino a 5GHz, il problema con le alte frequenze è

Tutte le implementazioni utilizzano il protocollo di accesso **CSMA/CA**.

Un **access point** o una **base station** serve una **Basic Service Set (BSS)**, dentro la BSS si trovano sia gli access point che gli host.

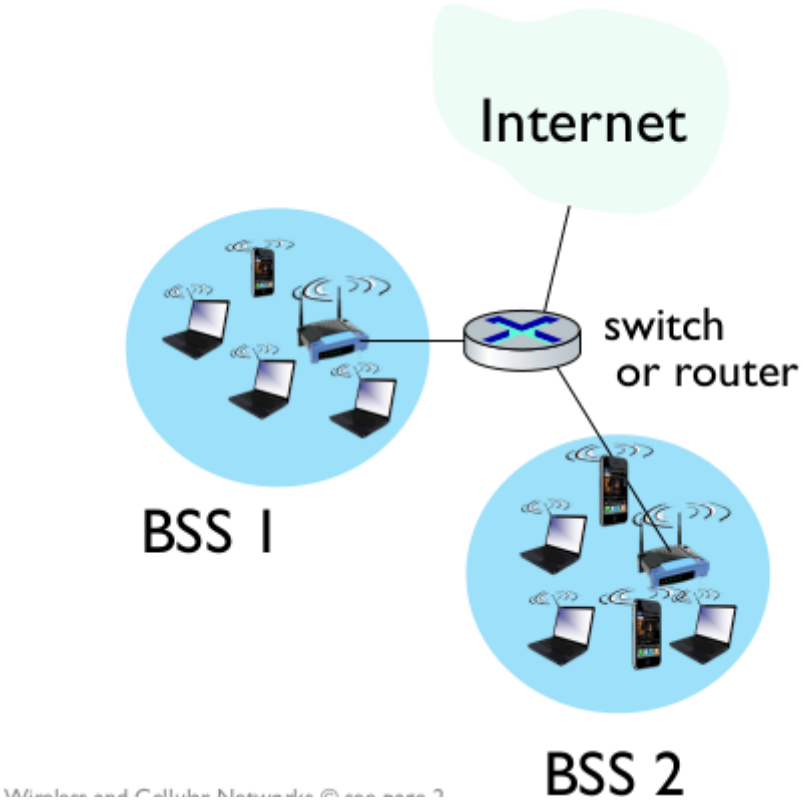

Figure 9: BSS

Un dispositivo fa il **sensing** per cercare un canale operativo, che provengono di vari access point, ascoltando per il **beacon frame** che serve ad agganciarsi ad un access point, ci sono diversi beacon fram ed il dispositivo si collega all'access point con il segnale più forte, il beacon frame contiene:

- il nome dell'AP (SSID);

- l'indirizzo MAC;

Per poter accedere ad una rete wifi, oggigiorno, hanno tutte bisogno di autenticazione, e tipicamente sarà presente un DHCP per ottenere una configurazione IP.

6.2 CSMA/CA

Il protocollo fa il sensing del canale (CSMA = carrier sense multiple access), ed la collision avoidance (CA), il motivo è che in una rete wireless il mezzo di trasmissione è l'aria che è un mezzo condiviso. Il sender:

- si fa il sense del canale, si aspetta un tempo di DIFS e si trasmettono i dati;
- se si fa il sense ed il canale è occupato si aspetta, per applicare la CA parte un randon exponential backoff timer quando sento il canele occupato (in ethernet il timer partiva solo quando avveniva una collisione!);

Per evitare le collisione gli hots mandano un piccolo pacchetto , per sprecare la minor banda possibile, detti RTS (ready to send) usando CSMA, l'AP rispondono in broadcast agli host con un CTS (clear to send) per un degli host che ha mandato l'RTS, dopichè l'host a cui l'AP ha mandato il CTS che inizia a trasmettere una trama e l'AP manda sempre in broadcast un ACK all'host che ha trasmesso la trama.

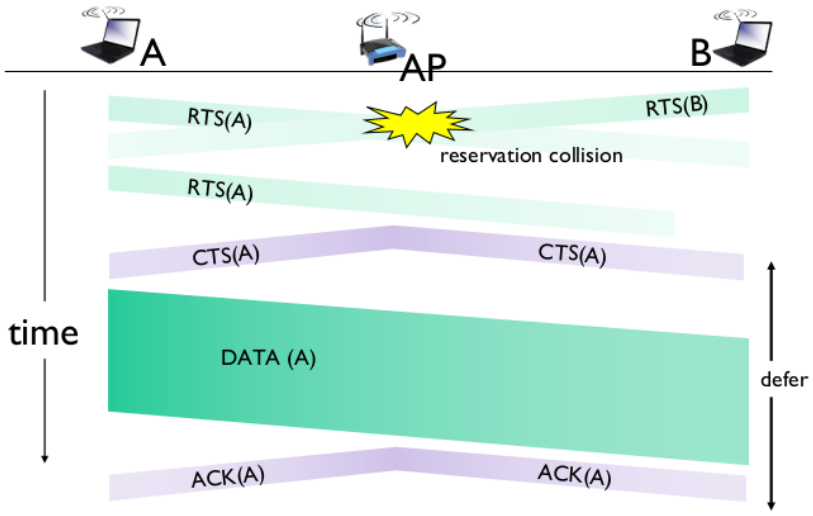

Figure 10: Collision Avoidance

Una trama 802.11 è fatta da:

- frame control: è composto da:
  - protocal version;

  - type: RTS, CTS, ACK, data;
  - power mgt;
  - ...;

- duration: la durata che ci mette la trama per essere trasfertita;
- address 1: indirizzo dell'interfaccia MAC dell'AP, il motivo per cui è presente questo indirizzo è che nelle reti wireless bisogna prima passare dell'AP (violando in qualche modo il principio su cui si basa il livello link nelle reti ethernet, dove se uno swith è presente il pacchetto viene direttamente inoltrato al mac di destinazione, senza passare dal router);
- address 2: indirizzo sorgente;
- address 3: indirizzo dell'interfaccia del router a cui l'AP è collegato;

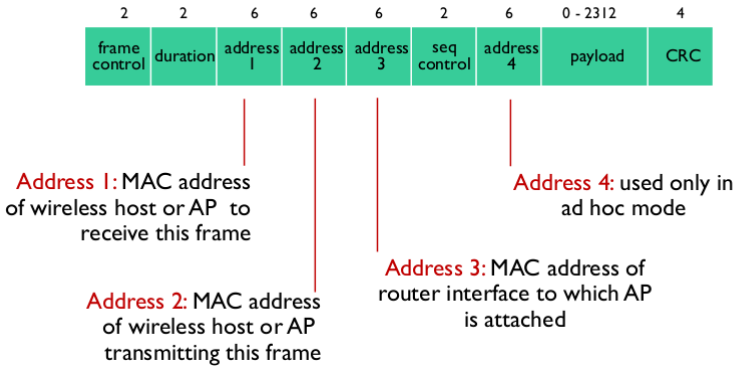

Figure 11: 802.11 Frame

In una rete wireless va gestita anche la mobilità, questo è improbabile in una rete wifi, solitamente il movimento è fatto in una subnet, ovvero in una rete in cui sono presenti più AP collegati allo stesso router di una sottorete.

Un'altra capacità dei dispositivi è il poter entrare in **sleep mode**, un nodo manda all'AP questa richiesta, se l'AP riceve delle trame da mandare al nodo li bufferizza finché il nodo non si svelgia, un nodo si riattiva quando un beacon frame viene mandato, nel beacon frame vengono anche segnalati gli host per cui ci sono dei messagi in coda, allora il nodo capisce che deve svegliarsi e colleziona le trame, oppure continua a dormire.

6.3 Cellular Networks

Una rete cellulare è una rete che cerca di coprire un'area geografica molto vasta attraverso le **celle**, dove il terminale utente si muove anche su lunghe distanze, gestendo il cambiamento du una cella all'altra, detto **handover**.

La forma e le dimsioni di una cella sono determinate da:

- potenza emessa;
- altezza;
- il guadagno dell'antenna: indica quanto un'antenna è buona nella trasmissione;
- morfologia del territorio;
- condizioni di propagazione: se nevica il segnale sarà più attenuato;

Le celle utilizzate in pratica sono:

- Una **macrocella** viene relizzata con un'antenna posizionata molto in alto;

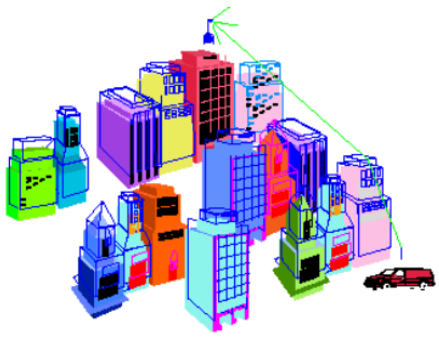

Figure 12: Macrocella

- **Microcella** realizzata con antenne non molto posta in alto,

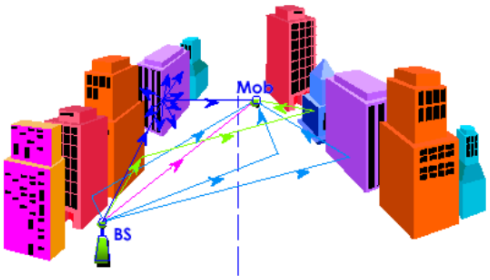

Figure 13: Microcella

Nelle reti cellulari non si usa CSMA/CD, le tecniche di condivisione sono: fdma, tdma, cdma, sdma. Per quasi tutte le reti cellulari si usa FDMA con riutilizzo dell

frequenze, sfruttando la distanza fisica che separe le celle. Vengono creati dei **cluster** di celle in cui vengono usate tutte le frequenze disponibili, al di fuori di questo cluster si possono riutilizzare le frequenze, il numero di celle presenti in un cluster si indica con G=x. Nei cluster le celle che hanno le stesse frequenze si chimano **co-channel**.

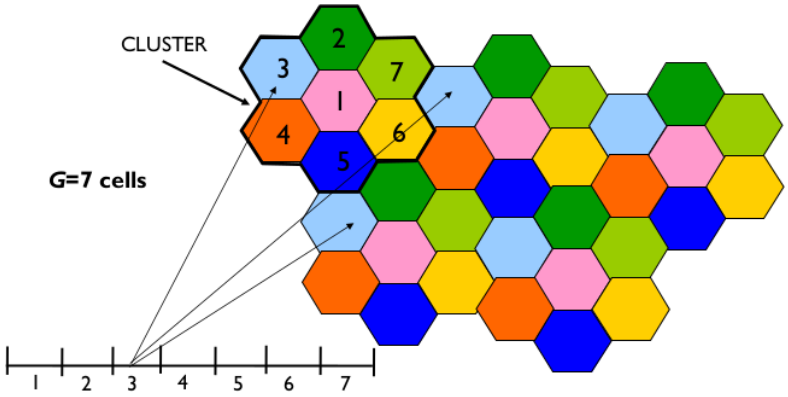

Figure 14: 7 Cell Cluster (G=7)

Per soddisfare più utenti si possono diminuire le dimensioni delle celle, soddisfando meno utenti per area ma incrementando l'ottimizzazoine di utilizzo delle frequenze, se però si inzia a diminuire troppo la dimensione sorgono dei problemi:

- aumento dei costi per creare le maggiori celle;
- diminuendo il numero di celle in un cluster aumento l'interferenza, la distanza tra i co-channel diventa più piccola, creando interferenze maggiori nella stessa frequenza;

Tecniche di freqency reuse:

- **Splitting**: coesistenza di microcelle e macrocelle, esempio: in campagna sarebbe meglio gestita con macrocelle più copertura e meno persone da gestire, in città ha più senso usare delle micro celle, meno copurtura per più utenti da gestire e più ostacoli da evitare;
- **Cell Shaping**: per evitare degli handover mette le micro celle in posti dove le persone so che rimarranno ferme, e per le persone che si muvono avrò delle macrocelle che caoprono un area più ampia;
- **Power Control**: è una tecnica per evitare di sprecare più batteria del necessario, per decidere la potenza da utilizzare; le strategia sono: open loop, closed loop, ...; nell'open loop
- **Sectoring**: si vanno a considerare delle antenne con capacità di trasmissioni non omnidirezionali, diminuendo le interferenze in una certa direzione;

- **Tilting**: non usare un angolo di 90 gradi per le trasmissioni, limitando le interferenze;
- **Creating femtocell**: si creano delle celle al volo quando ne ho bisogno dove ne ho bisogno, esempio: uno stadio non avrebbe senso di essere gestito ogni giorno della settimana, se non quando lo stadio si riempe di gente per un evento;

jArchittura ...

6.4 Basi Procedures

- **Registrazione**: fornire un associazione ad un rete cellulare, la registrazione viene fatta ogni qual volta un utente voglia accedere ad un servizione;
- **Mobilità**: le procedure legate alla mobilità sono:
  - **Roaming**: il roaming è la capacità di un terminale di essere tracciabile in una rete, tenendo i log su ogni cella in cui è stato attaccato. Per effettuare il roaming la rete ricorda in quale location area il terminale si trova, più celle adiacenti formano una lacation area, non è detto che una location area sia fatta da celle di un solo opertatore. Ognuna di queste lacation area ha un ID detto Location Area Id (LAI);
  - **Location updating**: è l'operazione che un utente deve fare ogni qual volta si muove e cambia location area, un treminale si accorge di aver cambiato LA quando visualizza un LAI diverso;
  - **Paging**: come si fa ed essere tracciabili? La rete conosce la LA in cui il terminale si trova, ma non la specifica cella, allora quando arriva un messagio per host x, il sistema manda un **paging message** in broadcast in tutta la LA (simile ad un ARP request), il motivo per cui si manda un messaggio in broadcast in una location area è limitare il numero delle laction updating;
  - **Handover**: procedura molto complessa per continuare a mantenere la connessione passando da una cella all'altra, si classificano in: intra-cella vs inter-cella, (soft vs hard) sono collegato ad entrambe le base station, sono collegato prima ad una e poi ad un altra, (MT vs BS) inizializzata da MT a dalla BS (tipicamente), (Backward vs Forward) procedure gestite dalla cella di arrivo o dalla cella di partenza;