Politecnico di Torino

Tecnologie e Servizi di Rete

Computer Engineering

Marco Lampis

18 dicembre 2022

Indice

0 Informazioni

I seguenti appunti sono stati presi nell'anno accademico 2022-2023 durante il corso di Tecnologie e Servizi di Rete.

Il materiale non è ufficiale e non è revisionato da alcun docente, motivo per cui non mi assumo responsabilità per eventuali errori o imprecisioni.

Per qualsiasi suggerimento o correzione non esitate a contattarmi.

E' possibile riutilizzare il materiale con le seguenti limitazioni:

- Utilizzo non commerciale
- Citazione dell'autore
- Riferimento all'opera originale

E' per tanto possibile:

- Modificar parzialmente o interamente il contenuto

Questi appunti sono disponbili su GitHub al seguente link:

```
1 https://github.com/Guray00/polito_lectures/tree/main/Tecnologie%20e%20
    Servizi%20di%20Rete
```

Figura 1: Repository GitHub

1 IPv4 Summary

In questo capitolo viene fatto un ripasso generico su quanto visto nei corsi precedenti, con particolare riferimento a Reti Informatiche (o equivalenti).

In ogni sottorete tutti i dispositivi che ne fanno parte avranno lo stesso indirizzo ip.

1.1 Indirizzi speciali

- tutti i bit a 1: indirizzo di broadcast, non può essere assegnato
- `127.x.x.x`: indirizzo di loopback, è una classe di indirizzi e servono a identificare l'host stesso e per tale motivo vengono solitamente utilizzate a scopo di debug.

Spesso oggi giorno non è consentito l'invio di messaggi in broadcast per motivi di sicurezza.

1.2 Indirizzamento IP con classi

Le rappresentazioni possono essere classes (a classe) o classness (senza l'utilizzo di classi). In particolare esistono di tre tipologie:

- **A**: prevede i primi 8 bit per l'indirizzo di rete, i rimanenti sono per identificare i dispositivi. Il totale degli indirizzi è 2^7 per la rete e 2^24 per i dispositivi. Si possono avere 128 networks.
- **B**: 2 bit per la classe, 14 bit per la rete e 16 bit per i dispositivi. Si possono avere 16384 networks.
- **C**: 3 bit per la classe, 21 bit per la rete e 8 bit per gli host.
- **D**: 4 bit per la classe, 28 bit per la rete e 4 bit per gli host. Questi indirizzi sono riservati per i multicast.

Basta guardare il primo bit per capire se era una classe A, B, C o D.

Nota:I bit di riconoscimento servono per sapere quali bit individuano la rete e quali gli host.

1.3 Indirizzamento IP senza classi (CIDR)

Il sistema ***C****lassless* ***I****nter****D****omain* ***R****outing* permette di indirizzare la porzione più precisa di indirizzi tra rete e e dispositivi. La porzione di rete è dunque di lunghezza arbitraria. Il formato con cui può essere rappresentato un indirizzo è il seguente: `networkID + prefix length` oppure `netmask`.

Il prefix length, specificato con `/x`, è il numero di bit di network.

La netmask è identificata da una serie di bit posti a 1 che determinano quali bit identificano la rete, attraverso un and bit a bit.

Esempio:

```
200.23.16.0/23                # prefix length
200.23.16.0 255.255.255.254.0 # netmask
```

L'indirizzo viene espresso attraverso gruppi di 8 bit, rappresentanti in modo decimale puntato (4 gruppi in quanto 32 bit totali). Ogni raggruppamento avrà un valore da 0 a 255.

Non tutti i valori sono permessi possibili, il più piccolo è 252. Questo è dovuto al fatto che abbiamo l'indirizzo dell'intera sottorete e l'indirizzo del inter broadcast che non possono essere utilizzati nell'assegnazione.

Un modo per sapere se un indirizzo è scritto in modo corretto è prendere il prefix length `/x` e controllare che ci l'ultimo numero puntato sia multiplo di 2^(32-x).

Esempi:

```
130.192.1.4/30  =>  4%2^(32-30) = 4%4  = 0 si!
130.192.1.16/30 => 16%2^(32-30) = 16%4 = 0 si!
130.192.1.16/29 => 16%2^(32-29) = 16%8 = 0 si!

130.192.1.1/30 => 1%2^(32-30) = 1%4  != 0 no!
130.192.1.1/29 => 1%2^(32-29) = 1%8  != 0 no!
130.192.1.1/28 => 1%2^(32-28) = 1%16 != 0 no!
```

Per il ragionamento di sopra appare evidente che un indirizzo che termina con `.1` non sarà mai un indirizzo corretto, in quanto ritornerà sempre un resto.

1.4 IP routing

Il routing degli host avviene attraverso la routing table, caratterizzata da due colonne che identificano:

- **destinazione** (indirizzi ip)

- **interfaccia** (eth0…)

Quando viene inviato un pacchetto, si cerca un match all'interno della tabella per identificare dove inviare un pacchetto IP. Se è presente più di un match, viene considerato quello con il prefisso più lungo.

nota: i router sono identificati solitamente con un cerchio con dentro una x.

Di seguito è mostrato un esempio di routing:

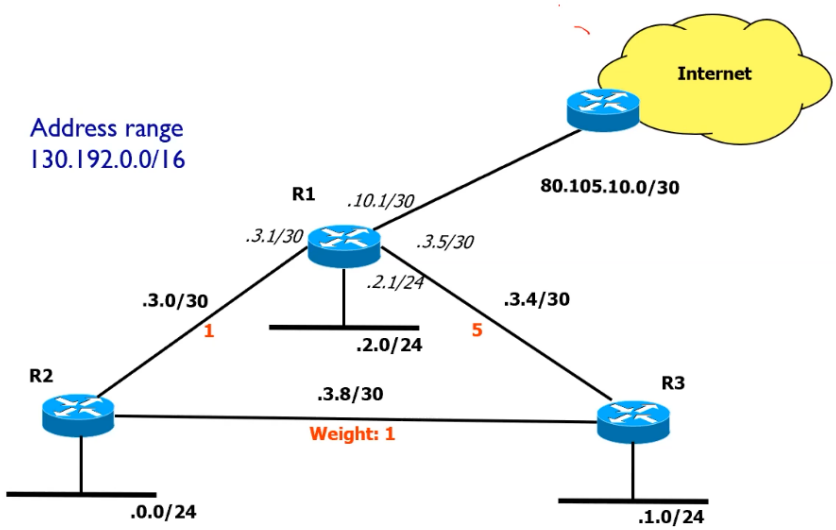


Figura 1.1: routing

Sono presenti in totale 7 sottoreti, di cui 3 reti locali e 4 reti punto punto. Tutta la sottorete ha come indirizzo quello raffigurato in alto a sinistra. Gli indirizzi di ciascuna di queste sono come segue:

Scriviamo la routing table del router identificando le reti direttamente connesse e raggiungibili. Prendiamo come riferimento **R1**:

Destination	Next	Type
130.192.3.0/30	130.192.3.1	direct
130.192.3.4/30	130.192.3.5	direct
130.192.2.0/24	130.192.2.1	direct
80.105.10.0/30	80.105.10.1	direct
80.105.10.0/30	80.105.10.1	direct

Destination	Next	Type
130.192.0.0/24	130.192.3.2	static
130.192.3.8/30	130.192.3.2	static
130.192.1.6/24	130.192.3.2	static

1.5 IP addressing methodology

La metodologia da adoperare è la seguente:

1. Localizzare le reti IP, *in questo caso 3*.
2. Individuare il numero di indirizzi richiesti, *in questo caso nel router in alto a destra è sufficiente `/30` perché ne sono richiesti 4 (2^2), `/26` a sinistra (2^6) e `/25` in basso a destra (2^7)*.
3. Quanti indirizzi posso allocare.
4. Il range di validità degli indirizzi,*in questo caso `/26`, `/25` e `/30` dunque mi basterebbe o tutti e 3, o due `/25` o infine un solo `/24`*
5. netmask / prefix length
6. Address range
7. Host addresses

Nota: in basso a sinistra sono richiesti 43 indirizzi per 40 dispositivi. Ciò è dovuto al fatto che oltre ai 40 richiesti serve l'indirizzo di rete, l'indirizzo di broadcast e l'indirizzo del router.

Per riuscire a trovare le sottoreti, si prosegue in ordine dal maggiore (decimale minore):

```
# tutta la rete
10.0.0.0/24

# subnet2 (/25), 32-25 = 7 => 2^7 = 128 indirizzi
# range: 0-127
10.0.0.0/25
10.0.0.127 <- ultimo

# subnet3 (/26), 32-26 = 6 => 2^6 = 64 indirizzi
# range: 128-191
10.0.0.128/26
10.0.0.191 <- ultimo

#subnet4 (/30), punto punto
10.0.0.192/30
```

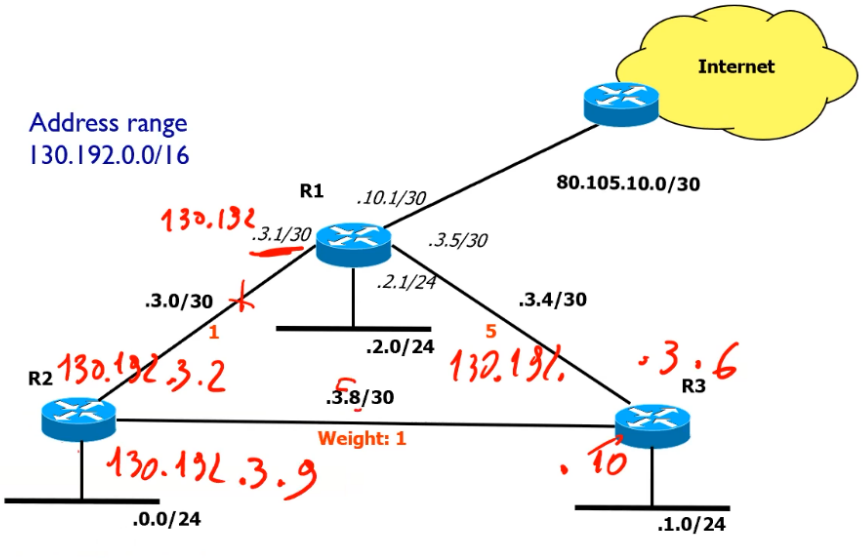


Figura 1.2: routing2

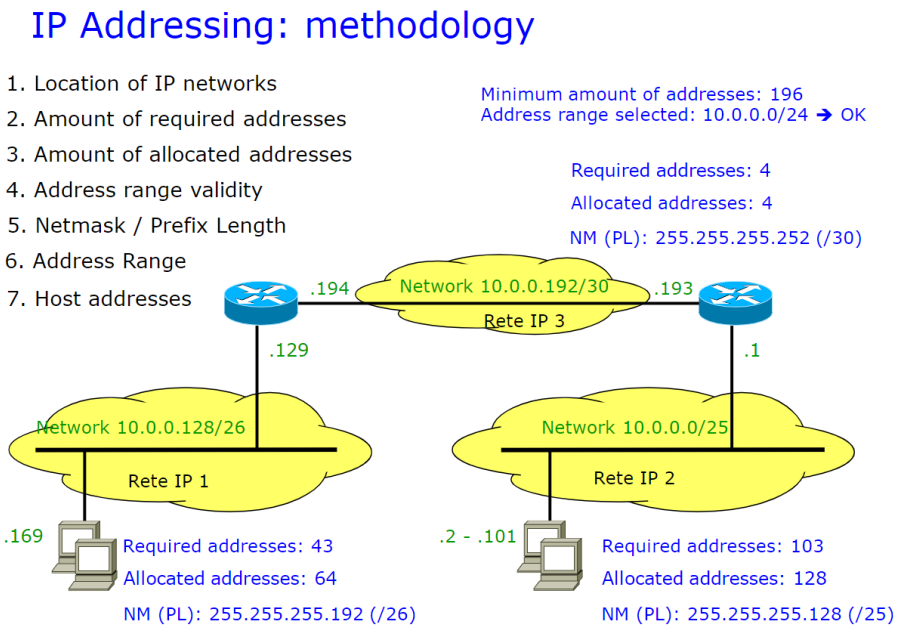


Figura 1.3: Rete di esempio

1.5.1 Esercizio 1

Numero di hosts	NetMask	Prefix Length	Available Addresses
2	`255.255.255.252`	(32-2) -> `/30`	$2^2 - 2 = 2$
27	`255.255.255.224`	(32-5) -> `/27`	$2^5 - 2 = 30$
5	`255.255.255.248`	(32-3) -> `/29`	$2^3 - 2 = 6$
100	`255.255.255.128`	(32-7) -> `/25`	$2^7 - 2 = 126$
10	`255.255.255.240`	(32-4) -> `/28`	$2^4 - 2 = 14$
300	`255.255.254.000`	(32-9) -> `/23`	$2^9 - 2 = 510$
1010	`255.255.252.000`	(32-10) -> `/22`	$2^10 - 2 = 1022$
55	`255.255.255.192`	(32-6) -> `/26`	$2^6 - 2 = 62$
167	`255.255.255.000`	(32-8) -> `/24`	$2^8 - 2 = 254$
1540	`255.255.248.000`	(32-11) -> `/21`	$2^11 - 2 = 2046$

Nota: per calcolare la netmask, si esegue $256 - 2^bit$

1.5.2 Esercizio 2

> Verifica se i seguenti indirizzi sono validi o meno.

IP / Prefix Length pair	Valido?
`192.168.5.0/24`	Si, gli ultimi 8bit sono a 0
`192.168.4.23/23`	No
`192.168.2.36/30`	Si, $36 \bmod 2(32 - 30) = 0$
`192.168.2.36/29`	No, $36 \bmod 2(32 - 29)! = 0$
`192.168.2.32/28`	Si, $32 \bmod 2(32 - 28) = 0$
`192.168.2.32/27`	Si, $32 \bmod 2(32 - 27) = 0$
`192.168.3.0/23`	No, $3 \bmod 2(1)! = 0$
`192.168.2.0/31`	No, `/31` non ha senso

IP / Prefix Length pair	Valido?
`192.168.2.0/23`	Si, $2 \bmod 2^(1)! = 0$
`192.168.16.0/21`	Si, $16 \bmod 2^3 = 0$
`192.168.12.0/21`	No, $12 \bmod 2^3 = 0$

1.5.3 Esercizio 3

> Trova l'errore di configurazione nella rete indicata di seguito e spiega il motivo per cui questa non funziona come dovrebbe.

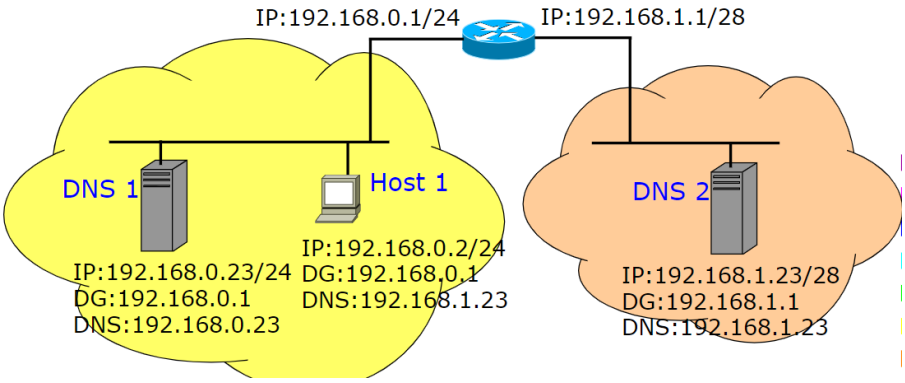


Figura 1.4: Configurazione

1.5.4 Esercizio 4

> Definisci un piano di indirizzamento IP per la rete in figura. Considera entrambi i tipi di indirizzamento: "tradizionale" (senza minimizzare) e una soluzione che minimizzi il numero di indirizzi IP utilizzati. Assumi di utilizzare il range 10.0.0.0/16.

Partiamo evidenziando come il router a sinistra, al fine di servire 350 host, ha in realtà bisogno di 353 indirizzi: 350 host + 1 indirizzo di rete + 1 indirizzo di broadcast + 1 indirizzo del router, dunque `/23`. Stesso ragionamento è applicabile al router di destra, che ha bisogno di 123 indirizzi `/25`.

Troviamo così che `10.0.0.0/23` è la rete A (sinistra). Il suo indirizzo di broadcast sarà `10.0.1.255` in quanto adoperiamo 9 bit (quindi gli ultimi 8 bit a 1 e il primo bit del terzo gruppo a 1).

La sottorete C (destra) sarà identificata da `10.0.2.0/25` in quanto l'indirizzo immediatamente successivo. Il suo indirizzo di broadcast sarà `10.0.2.127`.

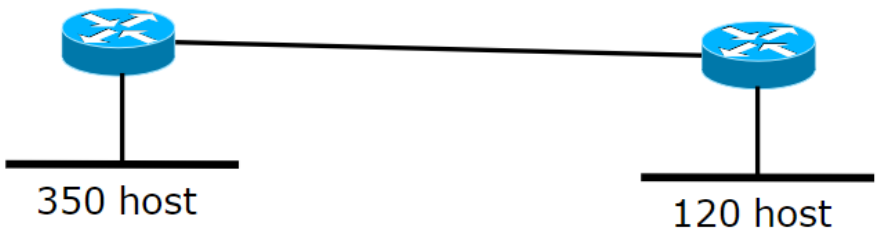


Figura 1.5: Rete

La sottorete B (centrale) sarà identificata da `10.0.2.128/30`, con `/30` proveniente dal fatto che è una sottorete punto punto.

Questa soluzione comporta un grosso spreco, in quanto c'è un `/25` che non viene utilizzato.

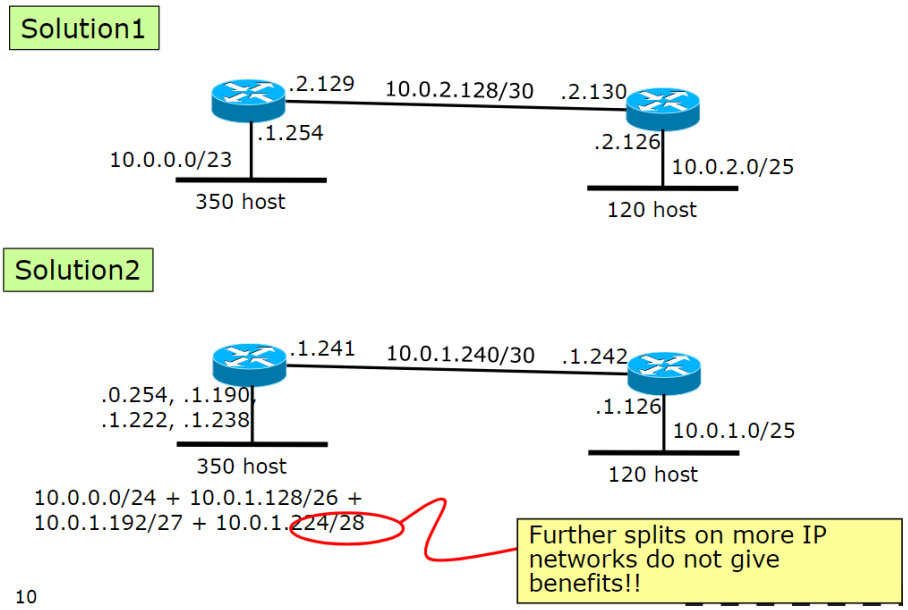


Figura 1.6: Soluzioni

1.5.5 Esercizio 5

> Definisci un albero di routing per tutti i nodi della rete mostrata di seguito.

L'**albero di instradamento** è quello che, a partire da un router della rete, stabilisce i percorsi minimi per raggiungere tutti i nodi. Per calcolare l'albero di instradamento si prende un router come riferimento, ad esempio **A**.

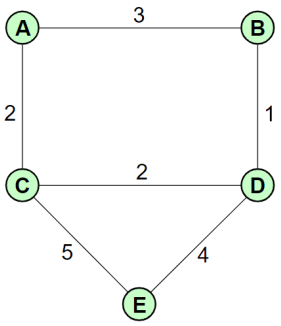


Figura 1.7: Rete esercizio 5

dest	next
B	3 (ramo dx)
C	2 (ramo inf)
D	4 (sia dx che inf)
E	7 (ramo inf)

La stessa procedura dovrà essere poi eseguita per tutti i nodi rimanenti, minimizzando le distanze. A parità di distanza solitamente ci sono motivi differenti per cui si scegli un percorso piuttosto che un altro (es router più nuovi).

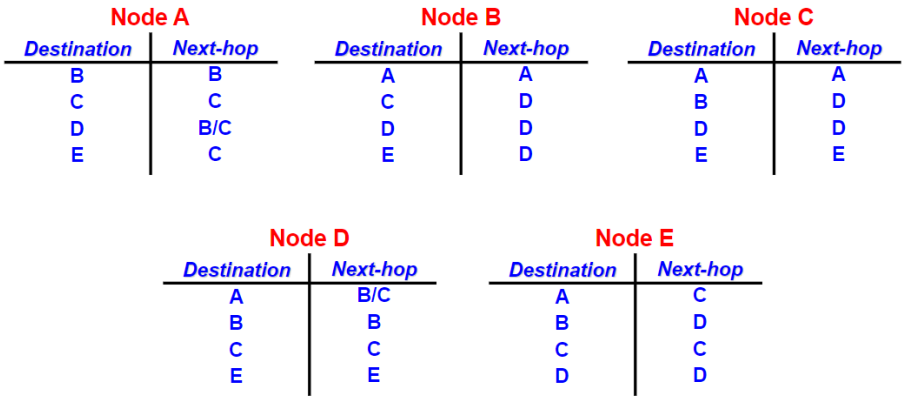


Figura 1.8: Soluzione esercizio 5

1.5.6 Esercizio 6

> Data la rete mostrata di seguito, definire la routing table di R1. La route aggregation deve essere massimizzata. Gli indirizzi ip mostrati in figura sono relativi all'interfaccia del router più vicino.

Cominciamo scrivendo la routing table di **R1**:

dest	next hop	Type
130.192.2.36/30 (A)	130.192.2.37	D

dest	next hop	Type
`130.192.1.126/30` (D)	`130.192.2.38`	S
`130.192.0.0/24` (E)	`130.192.2.38`	S
`130.192.1.128/25` (F)	`130.192.2.38`	S
`130.192.2.32/30` (G)	`130.192.2.38`	S

D ed **F** possono essere accorpati con `130.192.1.0/24`, che a sua volta può essere aggregato con e ottenendo l'indirizzo `130.192.0.0/23` avendo il valore di broadcast pari a `130.192.1.255`, per includere anche **G** è possibile usare `130.192.0.0/22`. Dobbiamo però stare attenti a controllare come questi si rapportano con le entry statiche. In questo caso le include tutte, e non è un problema.

1.5.7 Esercizio 7

> Realizzare un piano di indirizzamento che minimizza il numero di indirizzi necessari.

Troviamo la routing table di **R1**, analizzando ogni nodo a partire dai collegamenti diretti:

- Nella sottorete **A** sono presenti 27 host, per cui sono necessari 27+3 indirizzi e un prefix length di $(32 - 5) = 27$.
- Nella sottorete **B** sono invece necessari 120+3 indirizzi, per cui un prefix length di $(32 - 7) = 25$.
- Le sottorete C e D sono invece una sottoreti punto punto, per cui è necessario un prefix length di 30.
- La sottorete E ha bisogno di 60+3 indirizzi, per cui un prefix length di $(32 - 6) = 26$. Infine la sottorete F ha bisogno di 10+3 indirizzi, per cui un prefix length di $(32 - 4) = 28$.

Troviamo adesso quali sono gli indirizzi delle sottoreti, partendo da quella di dimensione maggiore (B, in quanto `/25`).

- **B**: `130.192.0.0/25`, con indirizzo di broadcast `130.192.0.127` in quanto gli ultimi 7 bit sono a 1.
- **E**: `130.192.0.128/26` con indirizzo di broadcast `130.192.0.191`
- **A**: `130.192.0.192/27`, con indirizzo di broadcast `130.192.0.223`
- **F**: `130.192.0.224/28`, con indirizzo di broadcast `130.192.0.239`
- **C**: `130.192.0.240/30`, con indirizzo di broadcast `130.192.0.243`
- **C**: `130.192.0.244/30`, con indirizzo di broadcast `130.192.0.247`

E' ora possibile calcolare gli indirizzi dei next hop, prendendo come riferimento il router più vicino:

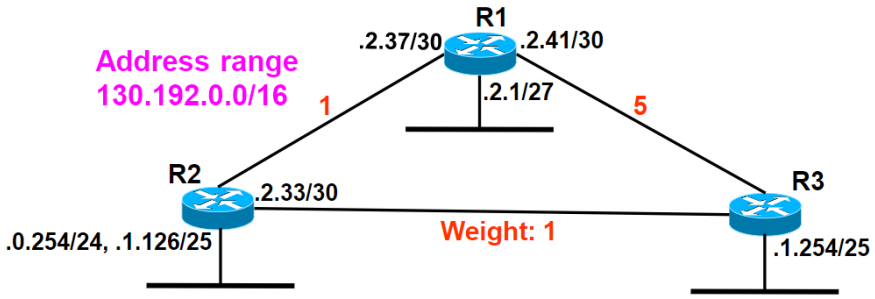


Figura 1.9: Esercizio 6

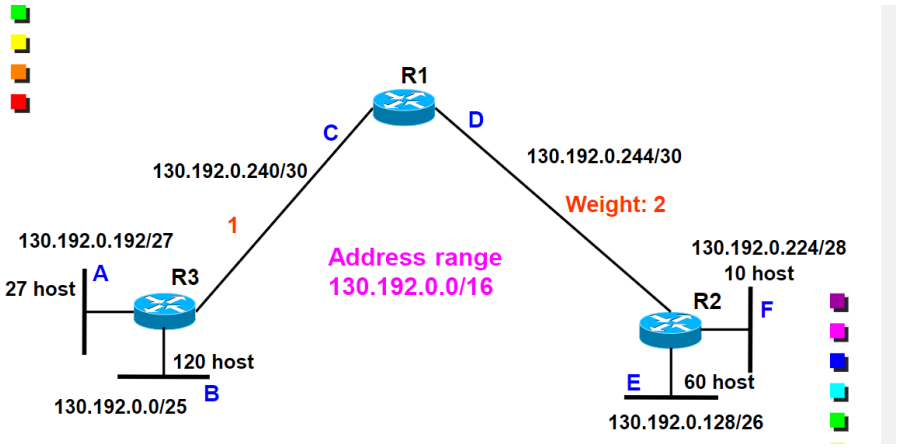


Figura 1.10: Esercizio 7

dest	Gateway	Type
`130.192.0.240/30` (C)	`130.192.0.241`	D
`130.192.0.244/30` (D)	`130.192.0.245`	D
`130.192.0.192/27` (A)	`130.192.0.242`	S
`130.192.0.0/25` (B)	`130.192.0.242`	S
`130.192.0.128/26` (E)	`130.192.0.246`	S
`130.192.0.224/28` (F)	`130.192.0.246`	S

Di queste entry bisogna valutare se è possibile fare qualche aggregazione. E' possibile farlo con **E** ed **F** in quanto: avendo `/26` e `28`, possono essere racchiusi in un `/25` (quindi 2^7) con il medesimo indirizzo di **E** (`130.192.0.128/25` è valido perché 128 % 128 = 0). La soluzione risulta comunque inefficiente perché non abbiamo ottenuto solo una entry.

1.5.8 Esercizio 8

> Realizzare un piano di indirizzamento che minimizza il numero di indirizzi necessari. Utilizzare il risultato della routing table di R1.

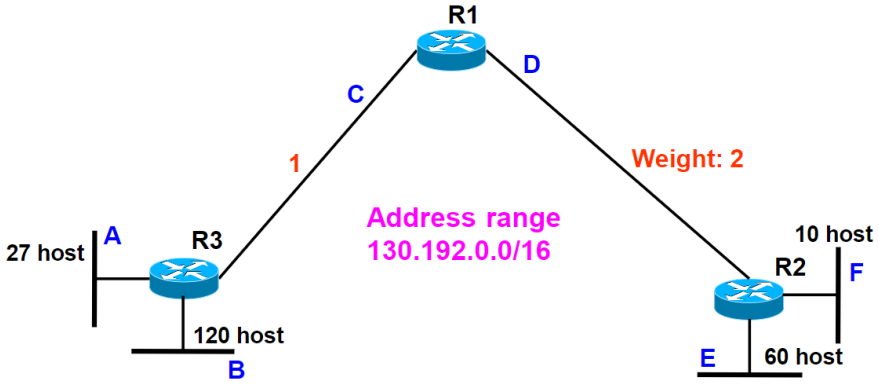


Figura 1.11: Esercizio 9

1.5.9 Esercizio 9

> Assumendo di avere interamente la cache libera, indicare il numero e il tipo di frames catturati da uno sniffer localizzato nella rete cablata dell'host A.

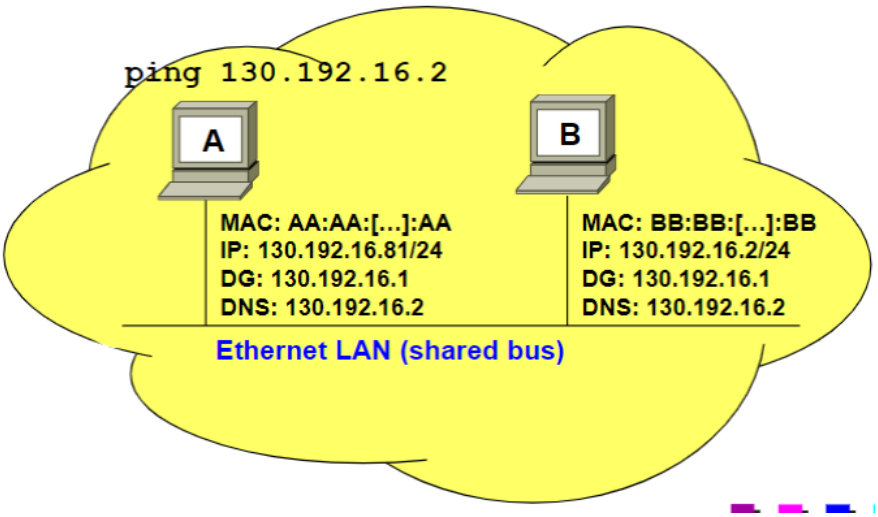


Figura 1.12: Esercizio 10

In una macchina Windows il ping viene eseguito 4 volte.

Bisogna innanzitutto verificare che le due macchine siano effettivamente nella stessa rete, lo si fa vedendo se hanno la stessa sottorete (in questo caso si, entrambi coerenti sulla `130.192.16.0/24`).

Scriviamo ora la tabella:

ID	MACS	MACD	IPS	IPD	DESCRIZIONE
1	MACA	broadcast	-	-	ARP Request
2	MACB	MACA	-	-	ARP Response
3	MACA	MACB	IPA	IPB	ICMP echo request
4	MACB	MACA	IPB	IPA	ICMP echo response

Il passaggio 3 e 4 sono quelli eseguiti 4 volte.

1.5.10 Esercizio 10

> Assuming that all caches are empty, indicate the number and the type of the frames captured by a sniffer located sulla rete dell'host A.

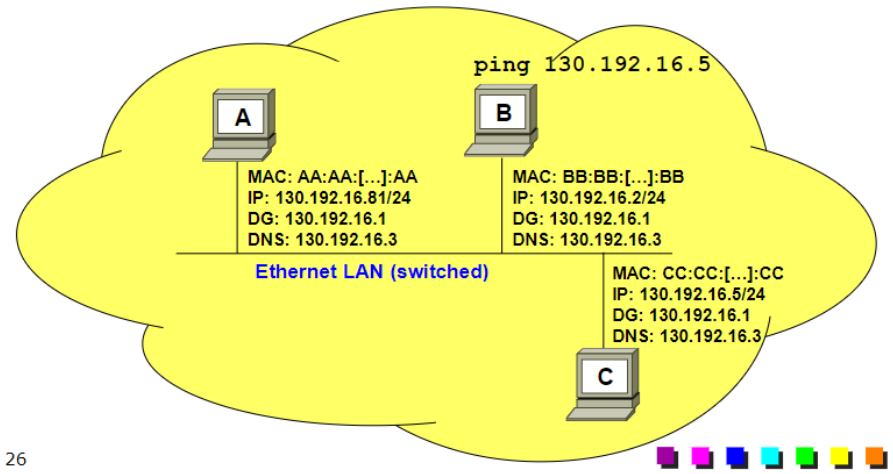


Figura 1.13: Esercizio 10

L'indirizzo IP del DNS è in realtà l'indirizzo di un host in quanto l'indirizzo della sottorete, con prefix length pari a `/23` abbiamo `130.192.16.0/23` (osservando il router). Il relativo indirizzo di broadcast viene calcolato sapendo di avere gli ultimi 9 bit a 1, quindi `130.192.17.255`, quindi l'indirizzo fornito è incluso.

La sottorete di A ha indirizzo della sottorete pari a `130.192.16.0`, è errato il prefix length in quanto viene indicato `/24` invece di `/23`.

A quando comunica per parlare con il DNS, che è all'esterno della sua sottorete, parla con il suo default gateway.

ID	MACS	MACD	IPS	IPD	DESCRIZIONE
1	MACA	broadcast	-	-	ARP Request
2	MACDG	MACA	-	-	ARP Response
3	MACA	MACDG	IPA	IPDNS	DNS request
4	MACDG	broadcast	-	-	ARP request
5	MACDNS	MACDG	-	-	ARP response
6	MACDG	MACDNS	IPA	IPDNS	DNS request
7	MACDNS	broadcast	-	-	ARP request

ID	MACS	MACD	IPS	IPD	DESCRIZIONE
8	MACA	MACDNS	-	-	ARP response
9	MACDNS	MACA	IPDNS	IPA	DNS response
10	MACA	MACDG	IPA	IP google	ICMP echo request
11	MACDG	MACA	IP google	IPA	ICMP echo response

Essendo uno shared bus tutti i pacchetti sono condivisi, solo che che chi non è interessato ai pacchetti che riceve li scarta. *Nota: DG viene utilizzato per indicare default gateway; arp è di livello 2.* Il traffico viene ottenuto prima che entri nel nodo A.

Il passaggio 10 e 11 sono quelli eseguiti 4 volte.

1.6 Multicast

Il multicast è un concetto che sta nel mezzo tra una comunicazione unicast (1 a 1) e broadcast (1 a tutti). Una sorgente A manda i pacchetti ad *alcuni* host. Ci sono dunque dei gruppi a cui degli host possono entrare o uscire. E' vantaggioso in quanto l'alternativa sarebbe mandare pacchetti uno ad uno in modo molto più lento. Nel multicast viene inviato un solo pacchetto, che viene poi instradato correttamente dal router ai destinatari utilizzando meno traffico (nel broadcast è sempre un pacchetto, ma viene poi mandato a tutti appesantendo). In IPv4 viene utilizzato poco perché si ha problemi con l'indirizzamento.

E' ampiamente utilizzato in IPv6 ed è chiave per la comunicazioni tra gruppi (videoconferenze, video broadcast ecc).

A ogni gruppo multicast viene associato un indirizzo IPv4. Questo indirizzo è un indirizzo di classe D, che è un indirizzo di broadcast. Fanno parte del range `224.0.0.0` - `239.255.255.255` che sono riservati, ed è per questo necessario acquistarne uno per utilizzarlo.

Il protocollo prevede che il livello 2 scarti i pacchetti che non sono di interesse, ma comunque è possibile associare un indirizzo di livello 2 al livello 3 in modo che possa essere scartato successivamente. L'indirizzo MAC è formato da 48 bit, rappresentato in forma compatta da gruppi di 8 bit ognuno dei quali rappresentato da 2 cifre esadecimali. La parte alta, solitamente riservata al produttore, ha invece la costante `01-00-5E-0` che identifica la mappatura per un totale di 25 bit (l'ultimo gruppo è solo un bit). La mappatura è fatta non comprendendo tutti i casi ma cercando di ridurre il numero di collisioni.

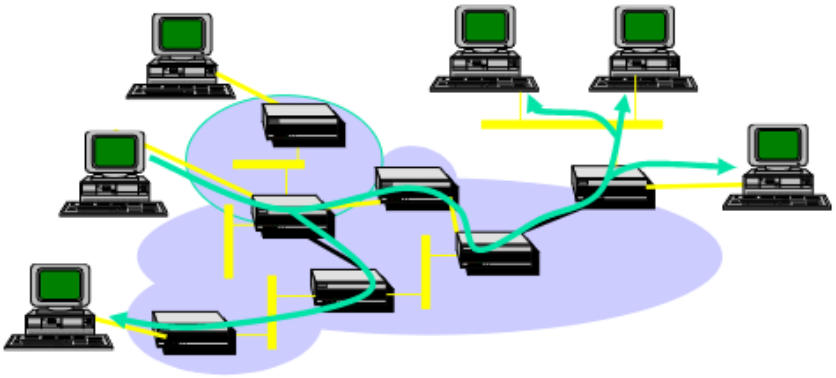


Figura 1.14: Multicast

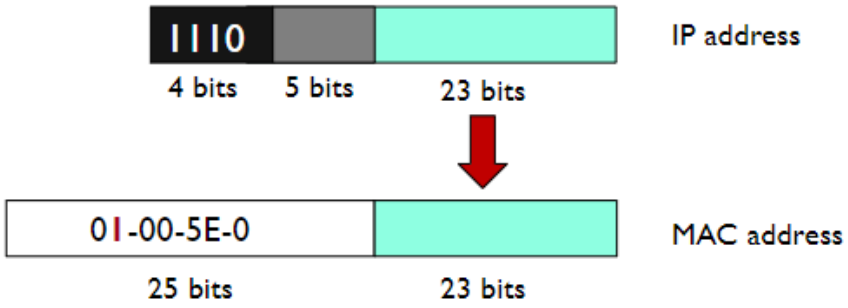


Figura 1.15: Mappatura IP a MAC

2 IPv6

IPv6 nasce per soddisfare le esigenze di un maggior numero di indirizzi, superando i limiti di IPv4. La nuova versione del protocollo risulta sotto molti punti di vista superiore, anche se IPv4 è ancora in uso e non è ancora stato completamente sostituito e nel corso degli anni è stato ampiamente esteso e migliorato.

Altre motivazioni che hanno portato alla nascita di IPv6 sono:

- Più efficiente sulle LAN
- Supporto di Multicast e Anycast
- Sicurezza
- Policy routing
- Plug and Play
- Traffic Differentiation
- Mobility
- Quality of Service support

Per riuscire a definire il protocollo IPv6 ha richiesto molto tempo e siamo attualmente in una fase di migrazione (richiedendo soluzioni temporanea applicate su IPv4).

2.1 Perché IPv4 non basta e soluzioni

Il protocollo IPv4 ha indirizzi di lunghezza 32 bit, con un totale di circa 4 miliardi di indirizzi. Nonostante ciò„ solo parte di questi indirizzi possono essere utilizzati a causa dell'utilizzo di classi, multicast, ecc. Inoltre, molti di questi sono utilizzati in modo gerarchico: il prefisso usato in una rete fisica non può essere usato in una differente. Infine, molti di questi indirizzi IP risultano non utilizzati, causando un grande spreco.

Alcune delle soluzioni utilizzate per risolvere questi problemi sono:

- Introduzione di reti "su misura" mediante l'utilizzo di netmask.
- Indirizzi privati (intranet), ma non abbastanza da risolvere il problema.

- NAT, che però rompe la connessione end to end aumentando il carico dei gateway e la relativa complessità
- ALG (Application Layer Gateway).

2.2 Chi assegna indirizzi IP

Gli indirizzi IP vengono assegnati da parte dell'organizzazione IANA, che assegna a ciascun Regional Internet Registry (RIR) un blocco di $/8$ indirizzi ip:

- AFRINIC: Africa
- APNIC: East Asia, Australia and Oceania
- ARIN: USA, Canada and some Caribbean islands
- LACNIC: South America, Mexico and some Caribbean islands
- RIPE NCC: Europe, Middle East and Central Asia

Successivamente, le RIR dividono i blocchi in blocchetti di dimensione minore da assegnare alle National Internet Registries (NIR) e alle Local Internet Registries (LIR).

2.3 Address pool status e scalabilità

Ogni singolo indirizzo IPv4 può essere in uno dei seguenti stati:

- part of the IANA unallocated address pool,
- part of the unassigned pool held by an RIR,
- assigned to an end user entity but unadvertised by BGP, or
- assigned and advertised in BGP

Ciò comporta dei problemi anche in termini di scalabilità, dovuti:

- dimensione delle routing table (ogni subnet network deve essere advertised)
- Risorse dei router limitate (troppe informazioni da gestire)
- Limitazioni dei protocolli di routing (spesso i router cambiano)
- Perlopiù riguarda i router backbone

Sono state tentate alcune soluzioni, come:

- aggregazione di router
- CIDR (Classless Inter-Domain Routing)
- Limitazione di assegnamento di prefissi IP "non razionali" e indirizzi IP (es vendita di $/8$)

Ma nonostante ciò il problema persiste, in particolare la scalabilità dei protocolli di routing risulta attualmente non risolvibile.

2.4 Indirizzi IPv6

E' stato scelto, attraverso un approccio di tipo scientifico e con un focus sull'efficienza, l'utilizzo di indirizzi di lunghezza pari a **128 bit**, con un totale di 2^128 indirizzi.

La notazione non è più puntata, ma bensì si è deciso di dividere in gruppi di **2 byte** (4 cifre esadecimali) separati dal carattere `:`. E' possibile utilizzare due regole per rendere più compatto l'indirizzo:

- è possibile rimuovere cifre pari a `0`. Esempio: da `1080:0000:0000:0000:0007:200:A00C:3423:A089` a `1080:0:0:0:7:200:A00C:3423:A089`.
- e' possibile omettere un gruppo di soli zeri inserendo `1080::7:200:A00C:3423:A089`, ma è lectio **solo una volta**. Questo perché non saprei quanti zeri inserire ciascuna volta.

2.5 Routing

Il routing IPv6 è stato pensato in modo da non modificare la struttura adoperata in IPv4, a eccezione della lunghezza degli indirizzi.

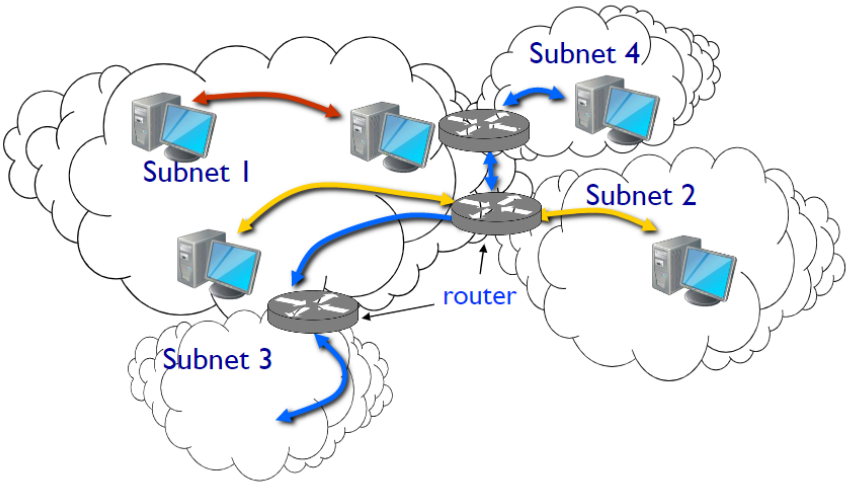


Figura 2.1: Routing

Per dividere la parte del prefisso di rete e la parte dell'interfaccia si è deciso, per il momento, di applicare

una separazione a metà con un prefisso di rete pari ad n=64, ma prevedendo che in futuro potremmo aver bisogno di un prefisso di rete più lungo.

Il concetto di aggregazione rimane il medesimo, è infatti possibile utilizzare il prefix length come già visto, ad esempio: FEDC`:0123:8700::100/40`. Non è necessario l'utilizzo di classi.

> **Nota**: non sarà, per quanto detto precedentemente, superiore a 64.

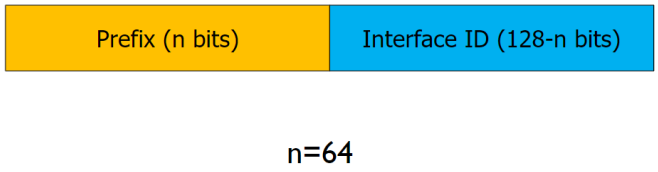


Figura 2.2: Struttura dell'indirizzo

I principi di assegnamento sono i medesimi dell' IPv4, con alcune differenze in termini di terminologia:

- **Link**: physical network
- **Subnetwork**: Link

Dividiamo le comunicazioni in:

- **On-link**: gli host hanno lo *stesso prefisso*, comunicano direttamente tra loro all'interno della stessa sottorete.
- **Off-link**: gli host hanno un *prefisso diverso*, comunicano attraverso un router.

A loro volta è possibile ulteriormente suddividere gli indirizzi di rete:

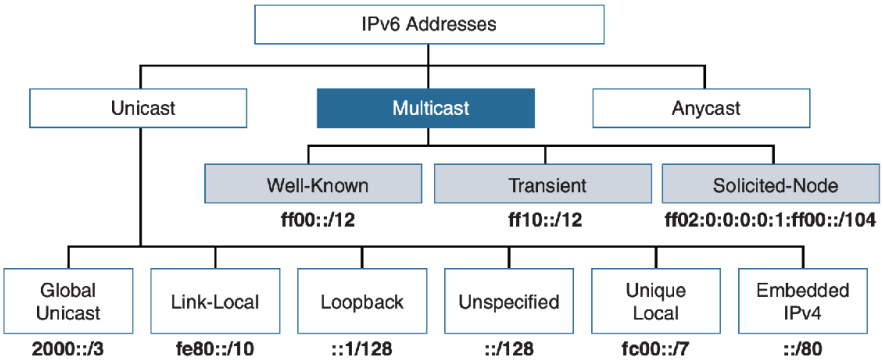


Figura 2.3: Spazio di indirizzamento

2.6 Multicast

L'equivalente dell'indirizzo multicast IPv4 '`224.0.0.0/4` è `FF00::/8`, che si suddivide in questo caso in:

- **Well-know Multicast**: `FF00::/12`, comunicazioni di servizio assegnati a gruppi di dispositivi e sono riservati. Un esempio è l'indirizzo di google.
- **Transient**: `FF10::/12`, indirizzi transitori, assegnati dinamicamente da applicativi multicast (corrispettivo della vecchia modalità multicast in IPv4).
- **Solicited-node Multicast**: `FF02:0:0:0:0:1:FF00::/104`, simile a un indirizzo IP broadcast in ARP.

Una caratteristica importante è notare come in IPv6 scompaia l'utilizzo del broadcast, che in seguito alle evoluzioni ha dimostrato essere un rischio per la sicurezza.

L'indirizzo si scompone in:

- **8 bit** iniziali, identificano che è un indirizzo multicast.
- **4 bit** per il **T flag**, dice se è well known (permanente o non permanente), viene assegnato da IANA.
- **4 bit** per lo scopo, viene lasciato ai dispositivi.
- **112 bit** per il group ID.

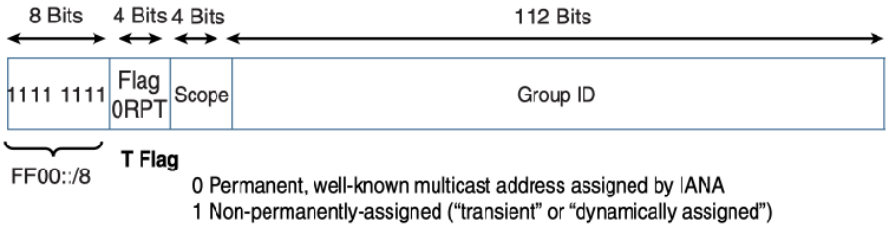


Figura 2.4: Struttura indirizzo multicast

2.7 Unicast

In IPv6 continuano a essere disponibili gli indirizzi unicast, con i seguenti indirizzi:

- `2000::/3` Global Unicast
- `FE80::/10`, Link-Local
- `::1/128`, Loopback (in IPv4 era `0.0.0.0`)
- `::/128`, Unspecified

- `FC00::/7`, Unique Local
- `::80`, Embedded IPv4

2.7.1 Global Unicast Addresses

Sono indirizzi di tipo aggregato, che andiamo a utilizzare in modo equivalente agli indirizzi pubblico IPv4. E' globalmente raggiungibile e indirizzabile ed ha la caratteristica di essere plug and play. Attualmente sono disponibili in un range definito tra `3FFF::` e `2000::`. Questi indirizzi hanno i primi 3 bit posti a `001`.

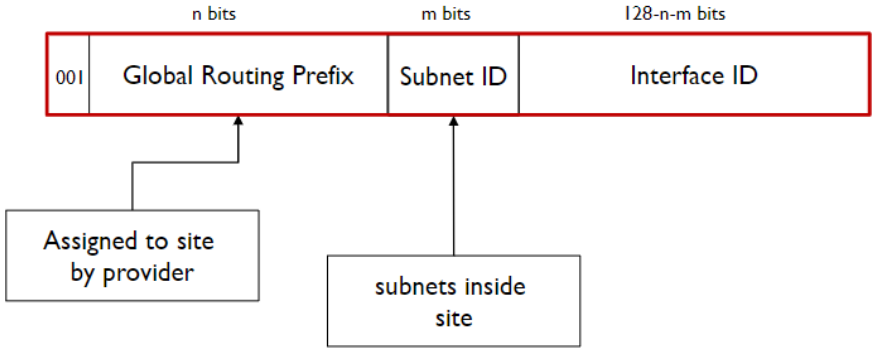


Figura 2.5: Global Unicast Addresses

I prefissi per il Global Routing sono formalmente assegnati da multi-level authorities:

- **3 bit**, tipologia (`001`).
- **13 bit**, TLA ID *(Top Level Authority, grandi ISP)*
- **32 bit**, NLA ID *(Next-level Authority, organizzazioni)*
- **16 bit**, SLA ID
- **64 bit**, Interface ID

2.7.2 Link local/site local Addresses

i link local/site local sono un gruppo di indirizzi che iniziano con `FEBF`, sono assegnati in automatico ai link quando viene acceso un router.

Gli indirizzi Link local vengono assegnati quando più router devono parlare tra di loro oppure devono annunciarsi a un router vicino.

Gli indirizzi site local sono nella rete `FEC0::/10`, sono ormai ritenuti deprecati perché pensati come vecchi indirizzi privati riconfigurabili, possono avere assegnati i router nelle comunicazioni (tipo stella e mesh ecc..). Utilizzano comunicazioni dirette e possono essere assegnati sono a indirizzi di rete.

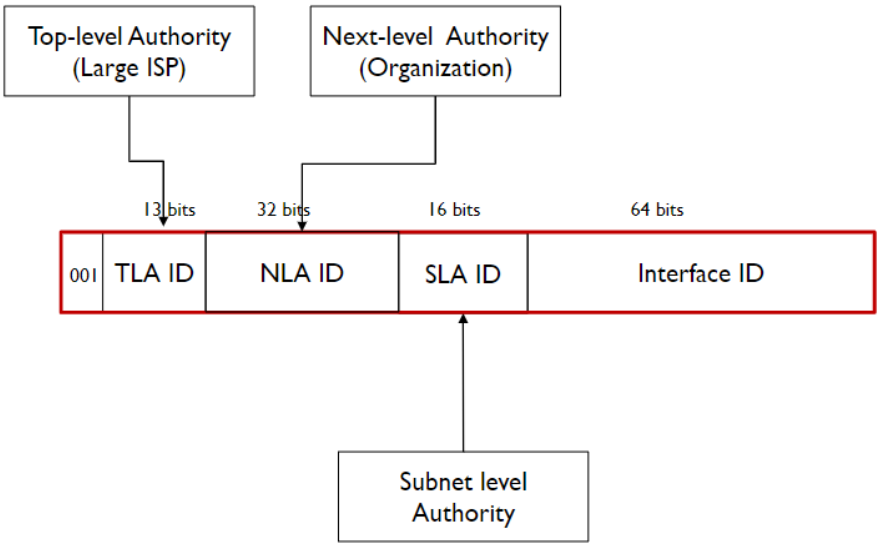


Figura 2.6: Global Routing Prefix

2.7.3 Unique Local Addresses

Gli Unique Local Addresses possono essere utilizzati in modo simile agli indirizzi globali unicast, ma sono per un utilizzo privato e non per l'indirizzamento sull'internet. Sono identificati da `FFC0::/7`, e vengono utilizzati dai dispositivi che non hanno mai necessità di connettersi all'internet e non hanno bisogno di essere raggiungibili dall'esterno. Sono indirizzi privati che possono comunicare su internet grazie ad operazioni di tunneling.

L'ottavo bit è il *Local (L) Flag*, che divide in:

- `FC00::/8`, se L flag è `0`, verrà assegnato in futuro
- `FD00::/8`, se L flag è `1`, l'indirizzo è assegnato localmente

Attualmente gli indirizzi `FD00::/8` sono gli unici indirizzi validi. Sono dunque privati e non utilizzati da altri dispositivi.

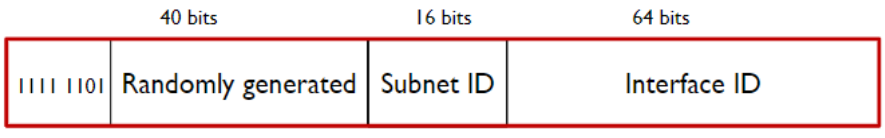


Figura 2.7: Unique Local Addresses

Dopo i primi 8 bit, sono presenti 40 bit generati casualmente in modo da non avere collisioni con altri indirizzi.

2.7.4 IPv4 Embedded Addresses

Gli IPv4 embedded addresses sono utilizzati per rappresentare indirizzi IPv4 all'interno di un indirizzo IPv6. Vengono utilizzati per facilitare la transizione tra i due protocolli. L'indirizzo IPv4 è inserito negli ultimi 32 bit (low order) mentre i primi 80 devono necessariamente essere pari a `0`, a cui seguono 16 bit dal valore di `FFFF` (16 1).

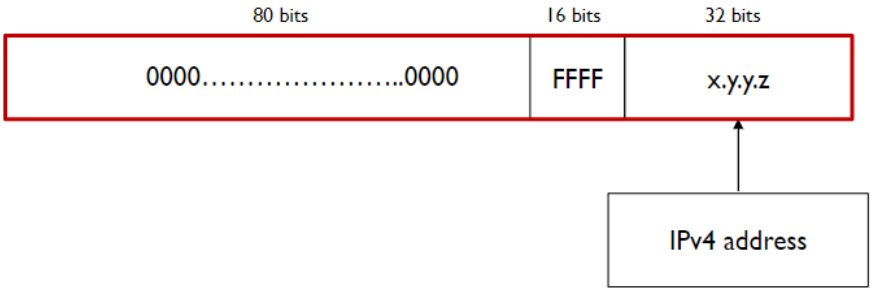


Figura 2.8: Struttura indirizzi IPv4 Embedded

2.8 Anycast Addresses

Gli indirizzi anycast possono essere assegnati a più di una interfaccia (tipicamente su dispositivi differenti), dando dunque la possibilità di avere su dispositivi differenti lo stesso indirizzo anycast. Un pacchetto che viene inviato a un indirizzo anycast viene reindirizzato all'interfaccia più vicina avente quel indirizzo. Questo permette di avere un indirizzo unico per un servizio, ma che può essere raggiunto da più dispositivi. Inizialmente venne realizzato per il DNS, ma è ancora in uno stato sperimentale.

> **Nota**: molto utile, ma non è ancora utilizzato.

2.9 Architettura del protocollo

L'architettura del protocollo IPv6 è molto simile a quella di IPv4, ma presenta alcune differenze:

- **IP**: utilizzato, salvo alcune modifiche
- **ICMP**: viene utilizzato *ICMPv6*
- **ARP**: non più utilizzato, inglobato in *ICMPv6*
- **IGMP**: non più utilizzato, inglobato in *ICMPv6*

Attenzione: non è più possibile utilizzare *ARP* E *IGMP* per risolvere gli indirizzi IPv6.

Sono invece stati aggiornati senza modifiche essenziali:

- DNS (type AAAA record)
- RIP e OSPF
- BGP e IDRP
- TCP e UDP
- Socket interface

2.10 Packet Header Format

L'header è stato modificato in modo sostanziale in seguito all'introduzione del IPv6. Ciò è stato fatto al fine di avere un header il più snello possibile, ottenendo una lunghezza di **40 byte**.

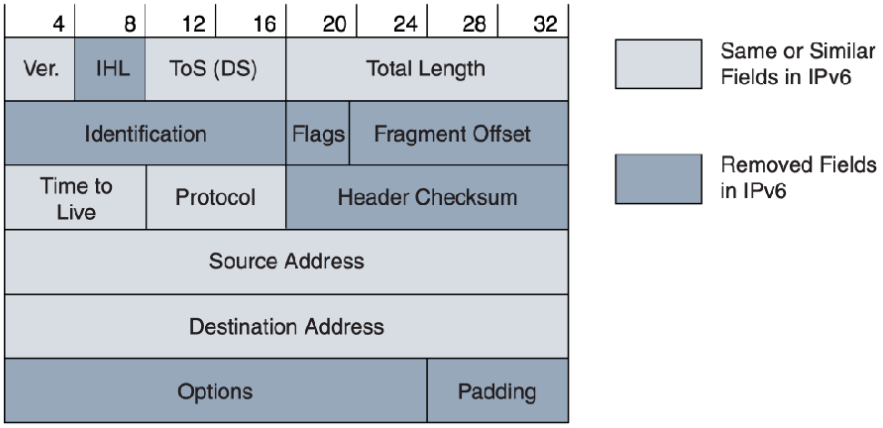


Figura 2.9: Header IPv4

L'header utilizzato in IPv6 è invece il seguente:

Osservando le immagini si può notare come alcune informazioni siano stati rimossi:

- Header Checksum: viene utilizzato per verificare se il dato trasmesso è corrotto, ma non è più necessario in IPv6.
  - Redundant: Layer 2 data link technologies perform own checksum and error control.
  - Upper-layer protocols such as TCP and UDP have their own checksums
- Frammentazione

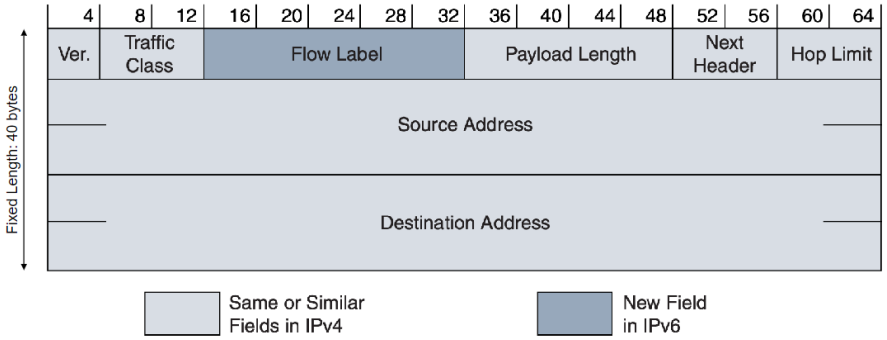


Figura 2.10: Header IPv6

- IPv6 routers do not fragment a packet unless they are the source of the packet
- Packets larger than MTU are dropped and an ICMPv6 Packet Too Big message is returned to source

Nota: Il checksum su UDP diventa opzionale in IPv6.

L'header può essere ulteriormente esteso attraverso il campo next header, che consente di puntare a un altro header contenente ulteriori informazioni creando una catena di header. Funzionano in modo simile al campo "protocol" di IPv4.

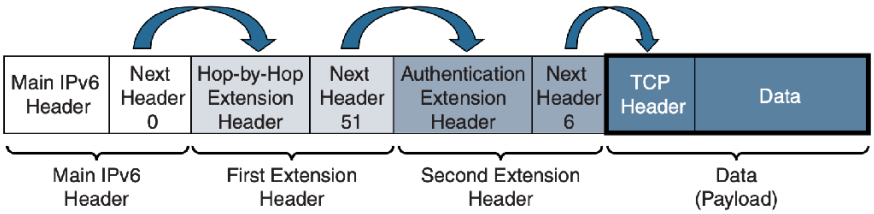


Figura 2.11: Chaining

Inoltre, sono presenti:

- **version**: versione del protocollo
- **traffic class**: permette di indicare la priorità del traffico (quality of service)
- **flow label**: permette di indicare il flusso di dati (nuovo campo), permette di associare un'etichetta a un certo tipo di traffico (label routing). Un esempio è se non mi fido dei miei dipendenti e voglio che tutto il loro traffico passi per un dispositivo di sicurezza che lo analizzi.
- **payload length**: lunghezza del payload
- **hop limit**: numero di router che possono essere attraversati prima che il pacchetto venga scartato. Se il valore è 0, il pacchetto viene scartato. Se il valore è 1, il pacchetto viene inviato al destinatario

senza essere inoltrato. Se il valore è 255, il pacchetto non viene scartato mai.

Nota: Header length non serve più! Viene eseguita la frammentazione attraverso il next header.

Il formato del campo next header è il seguente:

- **next header**: indica il tipo di header successivo
- **length**: lunghezza del header successivo
- **extension header**: header successivo
- **extension data**: dati dell'header successivo

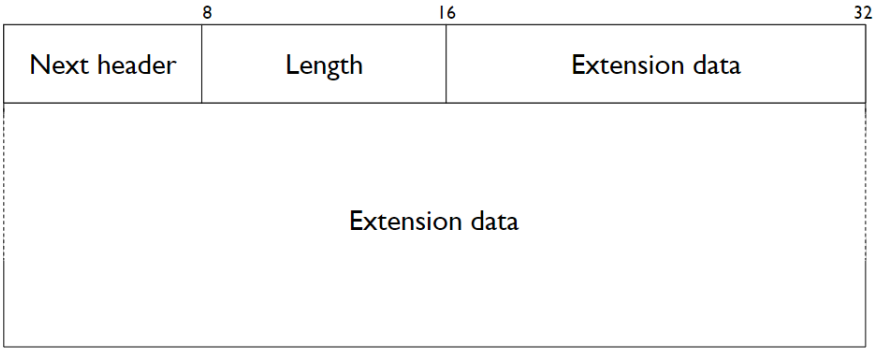


Figura 2.12: Extension Header Format

2.10.1 Hop-by-Hop Extension Header

E' utilizzato per andare a inserire dei campi/vincoli che servono all'hop per capire se il pacchetto deve essere scartato o meno (strumento di analisi). Se è presente, è indicato immediatamente dopo l'header IPv6. Questo header viene utilizzato per inserire dei campi opzionali. Ogni opzione ha un set di:

- **option type**: indica il tipo di opzione
- **option length**: lunghezza dell'opzione
- **option value**: valore dell'opzione

Si ottiene una tripletta **TLV** (type-length-value).

2.10.2 Routing Extension Header

IL routing extension header permette alla sorgente di un pacchetto di specificare il percorso di destinazione, indicando uno o più router intermedi. Viene utilizzato per il supporto alla mobilità in

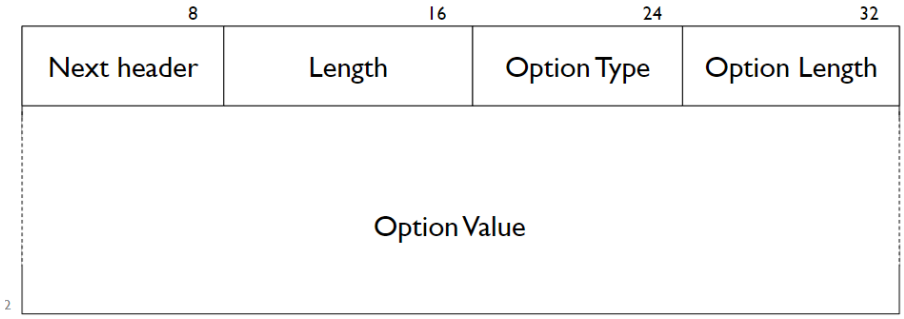


Figura 2.13: Hop-by-Hop Extension Header

IPv6.

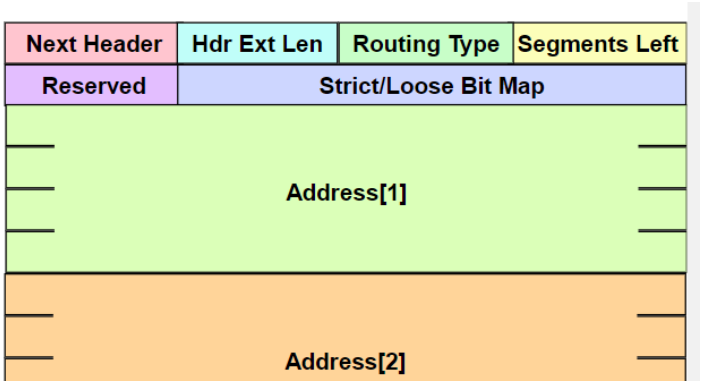


Figura 2.14: Routing Extension Header

2.10.3 Altre estensioni

Sono possibili altri due tipi di estensioni a seconda delle necessità.

2.10.3.1 fragmentation header

Viene utilizzato per la frammentazione dei pacchetti ognuno dei quali ha un proprio header IPv6 e un frammento di extension header. Il ricevente del pacchetto deve riunire i frammenti in un unico pacchetto. A differenza di IPv4, il protocollo IPv6 non frammenta un pacchetto almeno che non sia la sorgente del pacchetto.

2.10.3.2 Authentication and Encapsulation Header

Viene utilizzato per la sicurezza, adoperato da IPsec e fornisce una suite di protocolli per l'invio in sicurezza dei pacchetti in una rete IP. Il Authentication Header (AH) è utilizzato per l'autenticità e la integrità dei pacchetti. Il Encapsulating Security Payload (ESP) è utilizzato per la cifratura, autenticazione e integrità dei pacchetti.

2.11 Interfacciarsi con i livelli più bassi

2.11.1 Incapsulamento

La prima cosa che risulta evidente appena vi si approccia è che lo stack iso/osi prevede un campo in cui viene specificato il contenuto del livello superiore. Questo approccio è detto **dual stack**: creando uno nuovo stack è possibile far funzionare sia i dispositivi in IPv4 chee in IPv6 (lo trattiamo come un nuovo protocollo), senza alterare il funzionamento in IPv4.

I pacchetti IPv6 sono incapsulati nel frame di livello 2, ad esempio per ethernet il tipo è 86DD.

2.11.2 Address mapping

Un indirizzo di un pacchetto IPv6 viene associato a un MAC di destinazione attraverso:

- **IP unicast address**: discovery procedurale (protocol based)
- **IP multicast address**: algorithm mapping

2.11.3 IPv6 Multicast transmission

La trasmissione Multicast si basa sul ethernet multicast, ma a differenza del ethernet broadcast, un ethernet multicast può essere filtrato dalla scheda di rete (NIC).

Gli indirizzi multicast IPv6 vengono mappati su indirizzi MAC, in particolare è riservato l'indirizzo MAC Ethernet 33-33-xx-xx-xx-xx per il trasporto di pacchetti multicast IPv6.

Un esempio può essere il seguente: quando viene inviato un pacchetto all'indirizzo IP multicat FF0C::89:AABB:CCDD, questo viene incapsulato in un MAC frame con indirizzo 33:33:AA:BB:CC:DD.

> **Nota**: abbiamo FF all'inizio dell'indirizzo proprio perchè è multicast.

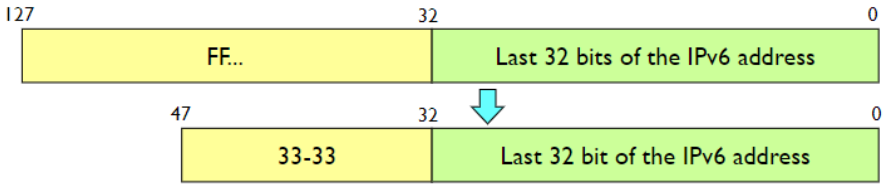


Figura 2.15: Multicast Transmission

2.12 Neighbor Discovery and Address Resolution

ICMPv6 adesso sostituisce completamente il protocollo **ARP**. E' basato su multicast e sfrutta il Solicicited-NOde MUlticast Address. A causa di come il multicast solicited address è realizzato, per lo più solo un nodo viene coinvolto.

2.12.1 Solicited-Node Multicast Address

Gli indirizzi vengono automaticamente creati per ogni indirizzo unicast dell'interfaccia. Tutti gli host si iscrivono e vengono mappati nel seguente modo: `FF:02::1:FF/104 | 24 ip meno significativi` (per lo più un host per gruppo).

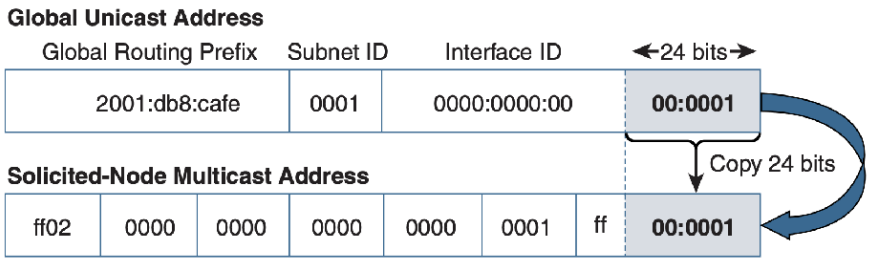


Figura 2.16: Mappatura indirizzo

2.12.2 Risoluzione indirizzo

La risoluzione di un indirizzo avviene attraverso **ICMP Neighbor Solicitation**: Il richiedente invia un frame al Solicited Node Multicast Address dell'indirizzo target IPv6.

:::tip **Come ricordarlo**: Il funzionamento è analogo al seguente: non lo chiedo a tutti, ma soltanto a chi mi potrebbe rispondere. :::

Avviene in seguito la risposta **ICMP Neighbor Advertisement**, attraverso la quale viene inviata la risposta indietro all'indirizzo unicast del richiedente. La mappatura tra IPv6 e MAC address viene

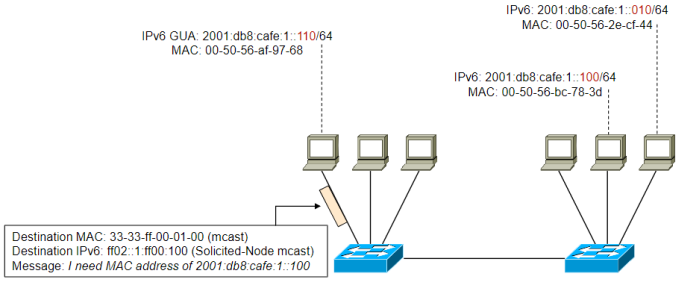


Figura 2.17: Risoluzione dell'indirizzo

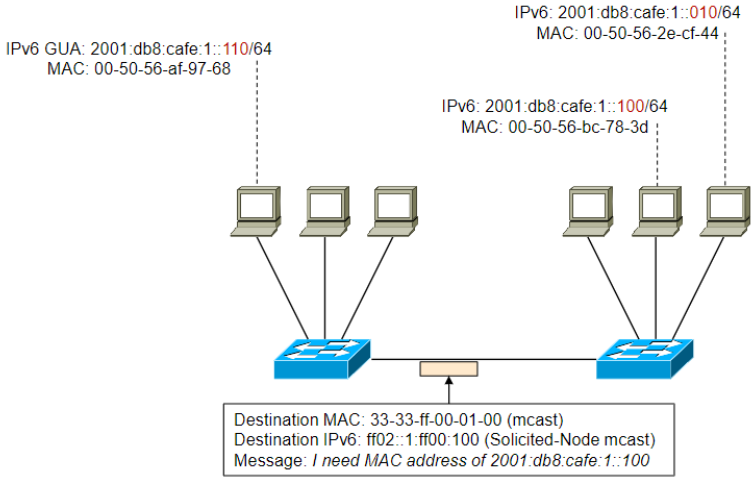


Figura 2.18: Risoluzione dell'indirizzo

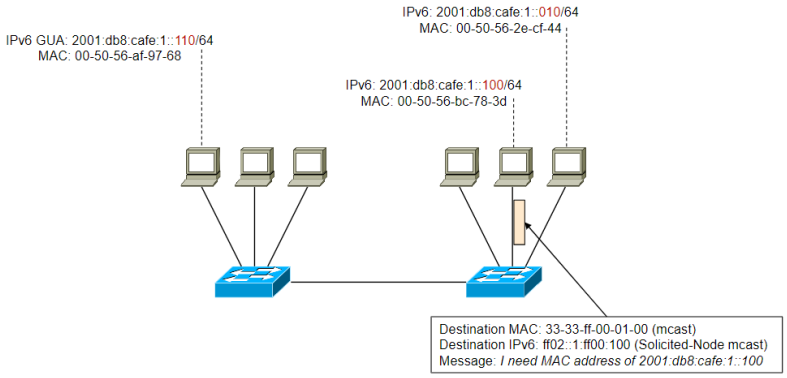


Figura 2.19: Risoluzione dell'indirizzo

memorizzata nella cache dell'host (in modo equivalente alla cache ARP).

Di fatto il numero di MAC aumenta molto, a causa della mancanza degli indirizzi broadcast. Per questo motivo è necessario che il router sia in grado di rispondere alle richieste di risoluzione indirizzo.

2.13 La transizione tra IPv4 e IPv6

La transizione da IPv4 a IPv6 sta venendo in modo **incrementale**, non è stato stabilito un limite entro cui eseguire il passaggio ma bensì sarà stabilito automaticamente quando sarà, nel pratico, il più utilizzato. Questo approccio trasparente e graduale ha consentito che prima di far prendere piede IPv6 nel corso di molto tempo ma in modo **seamless** (ovvero senza cambiamenti). Inoltre, come già accennato, è possibile generare e ricevere pacchetti per entrambi i protocolli senza problemi grazie all'approccio **dual stack**.

Questo risultato viene ottenuto attraverso tre meccanismi:

- Address Mapping
- Tunneling
- Translation mechanisms

Quando è nato IPv6 erano presenti poche reti dual stack, quindi era presente una parte di backbone su ipv4.

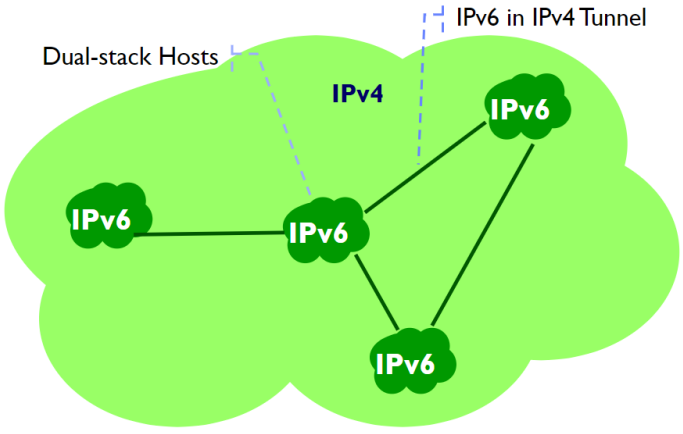


Figura 2.20: Pochi host IPv6

Nel corso del tempo le infrastrutture si sono adeguate al passaggio, aumentando il numero di host con comunicazioni onlink.

L'obbiettivo è quello di riuscire a creare una rete maggioritaria su IPv4 con solo poche connessioni IPv4. In realtà abbiamo già le infrastrutture per eseguire il passaggio completo.

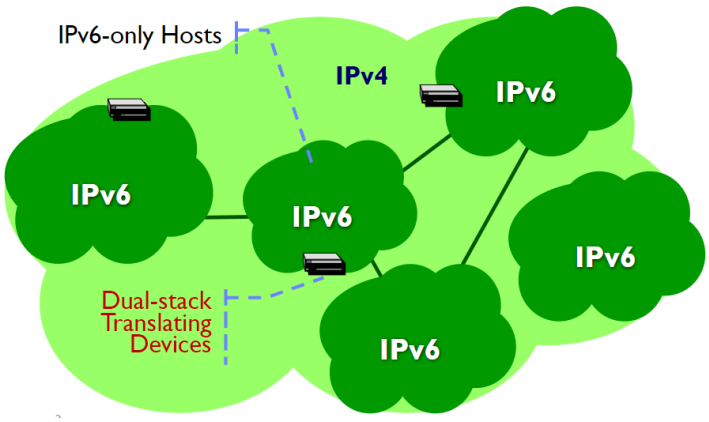


Figura 2.21: Molti host IPv6

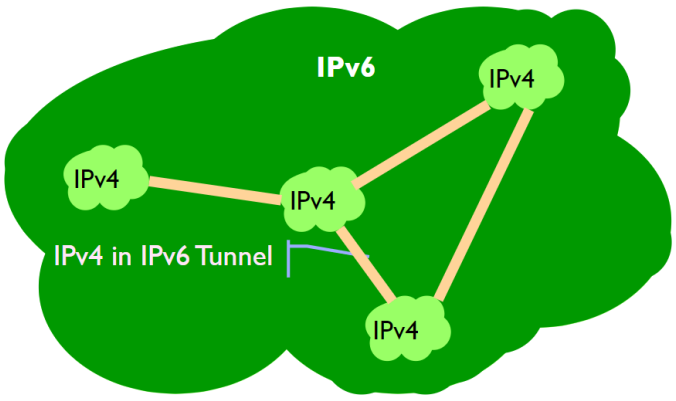


Figura 2.22: Maggioranza IPv6

2.14 ICMPv6

ICMPv6 permette di eseguire operazioni di:

- diagnostica
- neighbor discovery
- Multicast group management
- issue notification

Inoltre, include alcune funzioni che in IPv4 erano delegate ad **ARP** (Address Resolution Protocol) e **IGMP** (Internet Group Membership Protocol).

2.14.1 Formato del messaggio

Il messaggio è incapsulato nei pacchetti IPv6 con `next header = 58`, che mi permette di identificare il nuovo header di tipo **ICPMv6**, che avrà al più **576 byte**.

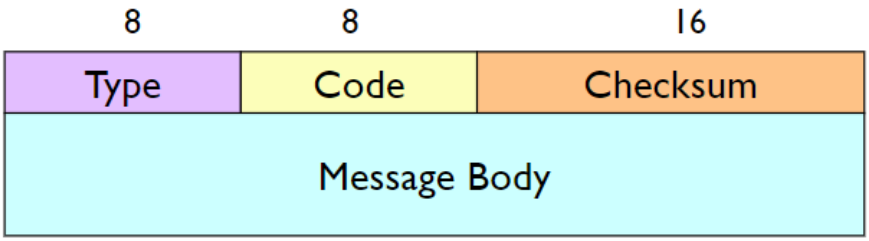


Figura 2.23: Formato del messaggio

Code	Spiegazione	tipo
1	Destination Unreachable	Errore
2	Packet too big	Errore
3	Time exceeded	Errore
4	Parameter Problem	Errore
128	Echo Request	Informativo
129	Echo Reply	Informativo
130	Multicast Listener Query	Informativo
131	Multicast Listener Report	Informativo

Code	Spiegazione	tipo
132	Multicast Listener Done	Informativo
133	Router Solicitation	Informativo
134	Router Advertisement	Informativo
135	Neighbor Solicitation	Informativo
136	Neighbor Advertisement	Informativo
137	Redirect	Informativo

2.14.2 Neighbor Solicitation

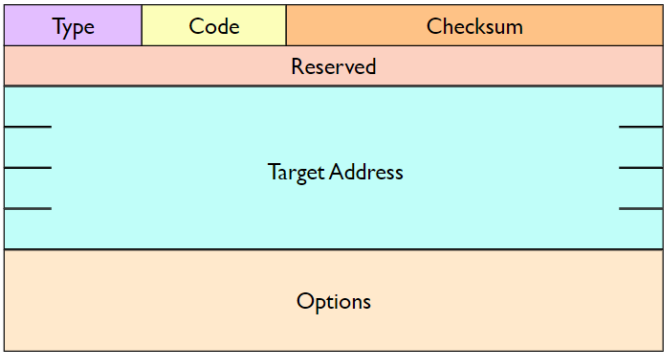


Figura 2.24: Neighbor Solicitation

2.14.3 Neighbor Advertisement

Sono presenti dei flag aggiuntivi:

- R **router flag**, se `true` arriva da un router.
- S **solicited flag**, se arriva da un nodo che ha fatto una richiesta di risoluzione.
- O **override flag**, se la host cache deve essere aggiornata o meno.

Nota: non è presente un campo MAC, in quanto può essere si da per scontato sia presente nelle opzioni. Viene invece specificato l'ip, anche se ridondante, in quanto potrebbe essere sia un nodo che un router.

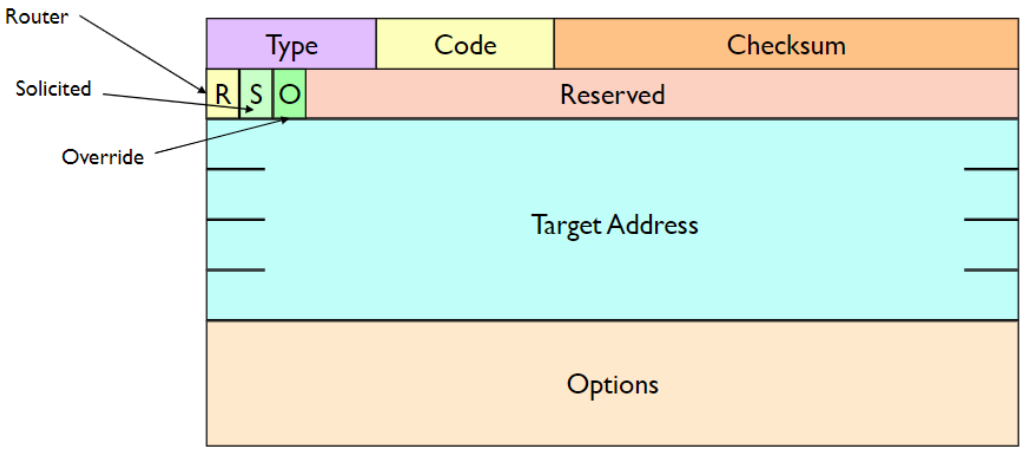


Figura 2.25: Neighbor Advertisment

2.14.4 Host Membership Discovery

La **Multicast Listener Query** è una domanda che il router manda ai suoi host per capire se sono interessati a far parte di un gruppo multicast, ponendosi in attesa di una risposta. La risposta con la quale un host comunica al router che è interessato a ricevere i pacchetti multicast è detto **Multicast Listener Report**.

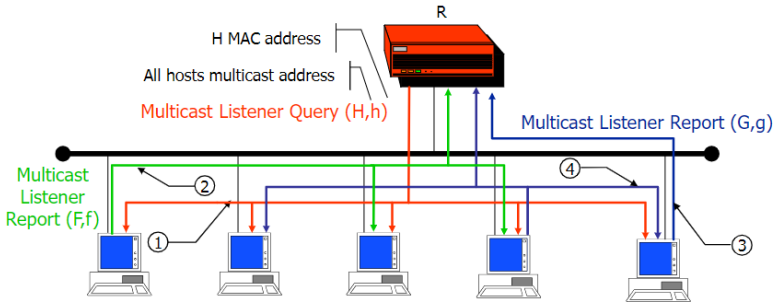


Figura 2.26: Host Membership Discovery

- **Multicast listener query** (`type=130`): il router manda una query per capire se un host è interessato a ricevere i pacchetti multicast.
- **Multicast Listener Report** (`type=131`): il host risponde al router dicendo che è interessato a ricevere i pacchetti multicast.
- **Multicast Listener Done** (`type=132`): il router manda un messaggio di fine per dire che non è più interessato a ricevere i pacchetti multicast.

La done è importante, perchè se un host esce da un gruppo, il router deve essere informato. Potrebbe succedere che il messaggio non venga inviato. In questo caso il router prevede dei timer, se dopo un intervallo di tempo (maximum response delay) l'host non manda un messaggio di interesse verso un gruppo, allora il router non inoltrerà più i pacchetti multicast.

Adesso la gestione del multicast è viene rappresentato solo a livello 3 (quindi compito del router e non più anche dello switch).

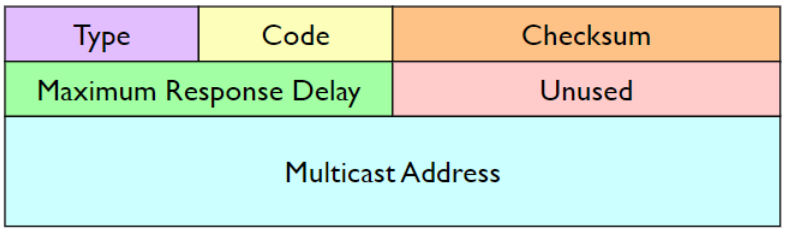


Figura 2.27: Formato richiesta

2.15 Device Configuration in IPv6

Le informazioni necessarie per la configurazione di un dispositivo sono:

- Address prefix
- Interface identifier
- Default gateway
- DNS server
- Hostname
- Domain name
- MTU (Maximum Transmission Unit)
- …

Molte di queste informazioni vengono recuperate automaticamente tramite in quanto lo scopo del IPv6 e di rendere gli host plug and play.

Le configurazioni possono essere:

- Manual configuration
- Stateful configuration: tutte le informazioni recuperate mediante DHCPv6
- Stateless configuration: generate automaticamente, con il prefisso dell'indirizzo ottenuto dal router
- Hybrid (Stateless DHCP): Information other than address obtained through DHCP

L'identificatore dell'interfaccia (64 bit bassi) può essere ottenuto in più modi:

- configurato manualmente
- ottenuto tramite DHCPv6
- generato automaticamente da EUI-64 MAC address

Ci sarà un ulteriore meccanismo che si assicura che l'indirizzo utilizzato sia unico all'interno della rete.

EUI-48 a EIU-64 (Extended Unique Identifier) estende l'indirizzo MAC da 48 bit a 64 bit, aggiungendo i bit `11111110` (8 bit) e `10` (2 bit) in posizione 1 e 2.

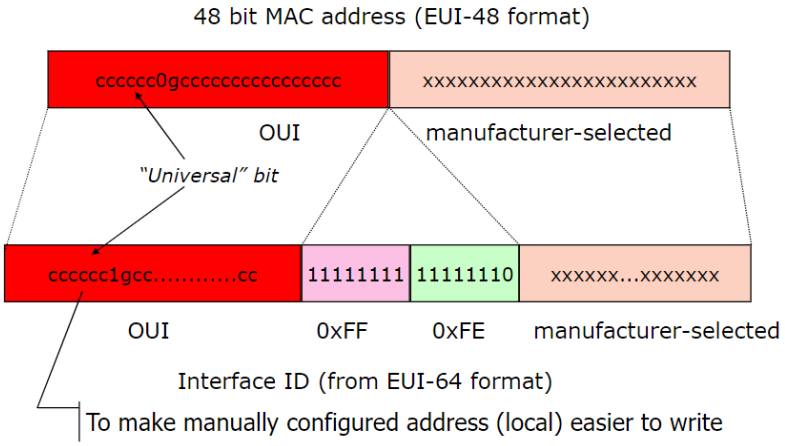


Figura 2.28: EUI-48 to EUI-64 mapping

Per convenzione, il settimo bit deve essere post a uno nel caso in cui l'indirizzo mac sia stato manualmente configurato si dovrebbe mettere il bit a `1`.

Dal punto di vista della tracciabilità, i 64 bit meno significativi di un indirizzo IPv6 di un'interfaccia non cambiano mai quando viene utilizzato un MAC address.

2.15.1 Privacy extension Algorithm

Non viene più utilizzato MD5. Questo algoritmo garantisce la privacy al livello 3, non è possibile da questi 64 bit ricavare un indirizzo.

2.15.2 Indirizzi

Un host pu avere più di un indirizzo IPv6, che possono essere *default* o *privacy aware*. Questi possono essere utilizzati per accettare o iniziare connessioni. Solo una un numero selezionato di indirizzi

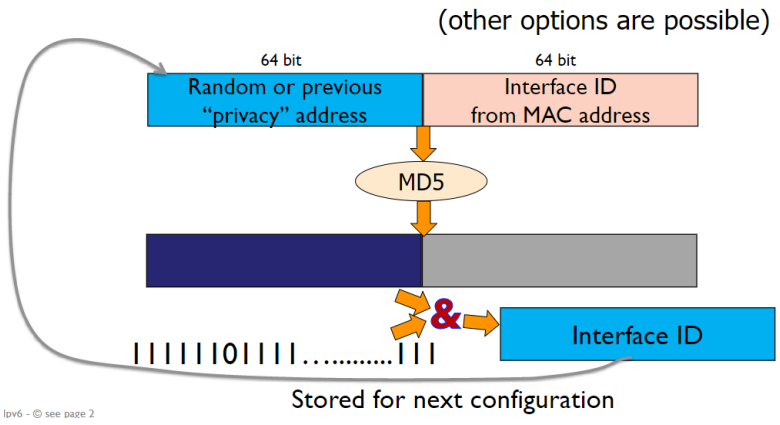


Figura 2.29: Privacy extension Algorithm

potrebbe essere disponibile per un user o una applicazione.

Il prefisso di un indirizzo può essere configurato manualmente, ottenuto tramite DHCPv6, generato automaticamente (link local) oppure ottenuto dal router.

Come faccio a capire quali sono i 64 bit alti che ha comprato il mio amministratore di rete? dal router. In particolare sono di nostro interesse il **router prefix discovery**, **router solicitation** e il **router advertisement**.

Attraverso la Router/Prefix Discovery è presente una sincronia: se l'host non ha chiesto un messsaggio potrebbe essere direttamente il router a mandare l'informazione tempestiva senza che venga richiesta solecitation.

La solicitation viene viene mandata a solamente i router, dunque non `all node` ma bensì `all routers`.

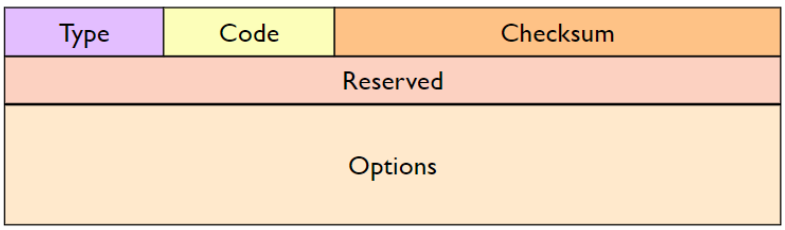


Figura 2.30: Router Solicitation

Nel messaggio di advertisement ci sono dei parametri interessanti:

- `M` flag *(Managed addres Configuration)*: se è settato a 1 significa che l'indirizzo è stato configurato tramite DHCPv6

- `O` flag *(other configuration)*: se è settato a 1 sono presenti altre configurazioni, ad esempio dns server.
- `reachable time`: tempo in millisecondi che il router impiega per raggiungere un host.
- `retrans timer`: ogni quanto ritenere valido questo indirizzo in un intervallo di tempo.
- Option: sono presenti delle opzioni, in formato generico e dunque: type, length (multipli di 8) e value.

tra le opzion c'è il prefix information option che ha sempre

- `lifetime`: tempo di vita dell'indirizzo
- `preferred lifetime`: periodo in cui non dovrei più utilizzarlo
- `L`, se lo utilizzo all'interno di un on-link
- `A`, il prefisso può essere utilizzato per una configurazione automatica
- `prefix`: il prefisso

Un'altre opzione è l'mtu.

Link layer address option: indirizzo MAC del mio default gateway. Se il default gateway invia il messaggio perché lo inserisco? per comodità dello stack iso/osi.

2.15.3 ICMP Redirect

Il concetto di redirect viene utilizzato per informare, all'interno di una stessa sottorete, un host che, per raggiungere un determinato host, è più conveniente utilizzare un altro router. Se la comunicazione è a livello globale questo solitamente non avviene.

2.15.4 Duplicate Address Detection (DAD)

Il DAD è un meccanismo che permette di verificare che un indirizzo sia unico all'interno della rete. Il meccanismo è molto semplice: l'host manda un messaggio ICMPv6 a tutti gli host con destinazione `all nodes` e con il payload che contiene l'indirizzo che si vuole utilizzare. Se l'indirizzo è unico, nessuno lo conosce e quindi non risponde (timeout, ad esempio un minuto). Se l'indirizzo è già utilizzato, un host risponde con un messaggio ICMPv6 di tipo `DAD` con il payload che contiene l'indirizzo che si vuole utilizzare.

2.15.5 Fasi di configurazione di una configurazione Stateless

- generazione di un indirizzo link local
- verifica dell'unicità dell'indirizzo (DAD)

- si mette in ascolto di un messaggio di router advertisement o manda una solicitation per andare a scoprire le informazioni sull'indirizzo privato

Una volta scoperta la parte alta:

- verifico se anche all'interno della mia sotto rete l'indirizzo è univoco (di nuovo).
- iscrizione al corrispondente IPv6 Solicited Node Multicast Address, configurando per la ricezione del multicast MAC corrispondente e inviando un ICP MUlticast Listener Report.

Un altro vantaggio è quello del renumbering, che consente un funzionamento plug and play. Tramite l'advertisement vengono riconfigurati tutti i dispositivi in modo automatico. Rimangono in ascolto per il Router Advertisement e quando arriva un messaggio con un nuovo prefisso, cambiano indirizzo. Gli host possono essere riconfiugurati in qualsiasi momento. Si identificano così indirizzi "preferred" e "deprecated". E' possibile dunque cambiare ISP senza dover cambiare tutti gli indirizzi.

2.16 Scoped Addresses

Un dispositivo può avere più interfaccie con il medesimo indirizzo, per cui essendo generato a partire dal mac potrebbero avere lo stesso indirizzo per cui un determinato pacchetto viene mandato su un interfaccia piuttosto che un'altra in base allo scopo e al programma che lo ha generato(concetto di scopo). UN indirizzo scoped è composto da un indirizzo IPv6 seguito da % e un numero che identifica l'interfaccia.

Ad esempio: `FE80::0237:00FF:FE02:a7FD%19`

> **Attenzione**: il valore dello scopo è specifico per ogni implementazione.

Questo byte di scope non viene poi considerato perchè è interesse solo per il sistema operativo.

2.17 Routing Protocols

Per prima cosa distinguiamo il routing in due tipologie:

- **On the fly routing**: è il forwarding, usa la routing table
- **proactive routing**: la creazione di routing tables

La creazione di tali tabelle possono essere di tipo manuale, dunque static routing, oppure mediante la distribuire delle informazioni all'interno della rete adoperando protocolli di routing.

Le routing table in IPv6 sono basate sul più lungo prefisso che fa match (come in IPv4). Nonostante alcune peculiarità, IPv4 e IPv6 si comportano come due protocolli indipendenti (con routing table separate).

I protocolli di routing possono essere:

- **integrate routing**: viene adoperato un singolo protocollo che informa i destinatari per entrambe le protocol families, dunque sia IPv4 che IPv6. Ha come vantaggio quello di non avere meccanismi di duplicazione, ma è necessaria l'implementazione di un nuovo protocollo dedicato che potrebbe comportare bug con il funzionamento delle operazioni in IPv4. Inoltre, le topologie di rete tra IPv4 ed IPv6 potrebbero essere diverse e quindi il routing potrebbe non essere ottimale.
- **ships in the night**: ogni family address ha il suo protocollo di routing, con la caratteristica che tutti i protocolli sono indipendenti l'uno dall'altro. In questo modo è possibile utilizzare protocolli di routing differenti (scelti in base alla topologia o scenario). Il vantaggio è una più semplice integrazione e trubleshooting, ma comporta un inevitabile meccanismo di duplicazione.

Esempi di routing protocol:

Protocol	Approach
Static	Ships in the night
RIPng	Ships in the night
EIGRP	Ships in the night
OSPFv3	Ships in the night (Integrated routing is possible)
IS-IS	Integrated routing
MP-BGP	Both (configuration-dependent);"Integrated Routing" is the most commonly deployed because of practicality: BGP process identified by AS number, which is the same for both IPv4 and IPv6.

Figura 2.31: Protocolli di routing

2.18 Transizione

La transizione tra IPv4 e IPv6, come già detto, è tutt'ora in corso e molto lenta. In prima battuta, quando la maggior parte delle connessioni erano su IPv4 si andava a utilizzare il tunneling di IPv6, il cui nome deriva dal fatto che IPv6 veniva inserito in un header IPv4 per compatibilità.

Alcuni protocolli che lo implementano:

- **GRE** (Generic Routing Encapsulation)
- IPv6 in IPV4 (protocollo di tipo 41)

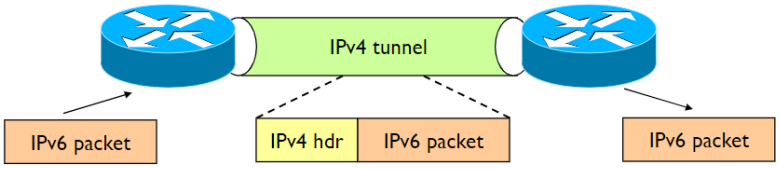


Figura 2.32: Esempio di Tunneling

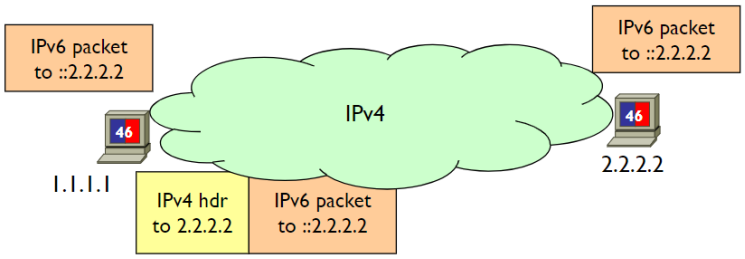
- setup manuale ed automatico

2.19 Host centered solutions

Una soluzione potrebbe essere di realizzare un dual stack host, ovvero un host che supporta sia IPv4 che IPv6. In questo modo, il tunneling non è più necessario.

Per fare ciò, degli indirizzi IPv6 devono essere riservati per la compatibilità con IPv4, in particolare quelli con il prefisso `::96`, in modo da ignorare i bit più significativi e renderlo retrocompatibile.

Le applicazioni mandano pacchetti IPv6 attraverso un indirizzo IPv6, ad esempio `2.2.2.2` e vengono reindirizzati a `::96` attraverso una pseudo-interfaccia (che fa tunneling automaticamente). La pseudo interfaccia dunque incapsula i pacchetti ipv6 in pacchetti ipv4 e li invia.



2.19.1 6over4

- IPv4 network emulates a virtual LAN
- Broadcast multiple access data link
- IP Multicasting used for the purpose
- Neighbor and router discovery enabled
- IPv4 address is used for automatic IPv6 Interface ID generation of link local address

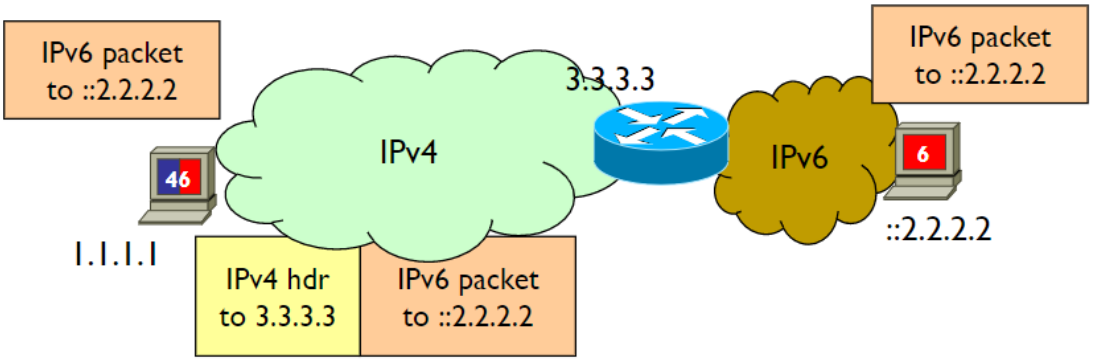


Figura 2.33: Dual stack router

- Not very used because IPv4 multicast support is not widespread

2.19.2 ISATAP: Intra-site Automatic Tunnel Addressing Protocol

Invece di usare il multicast, usiamo una soluzione che utilizzi un prefisso di rete `0000:5EFE`. - IPv4 network as Non-Broadcast Multiple Access (NBMA) data link - No IP multicast support needed - Interface ID derived from IPv4 address - Prefixed by 0000:5efe - E.g., fe80::5efe:0101:0101 for 1.1.1.1

2.19.3 (Lack of) Neighbor Discovery

Mi baso sul protocollo DNS, ma ha come limite che ogni indirizzo deve avere associato un hostname. Quindi la richiesta non parte dall'indirizzo di IPv6, ma dal hostname (potrebbe essere in alcuni casi un problema).

- Not needed for data-link address discovery as IPv4 address is embedded in IPv6 address
- Last 4 bytes
- PRL (Potential Router List) must be provided
- Router discovery not possible
- By configuration
- Automatically acquired from DNS
- Hostname not mandated
- E.g., isatap.polito.it

2.19.4 Automatic Configuration

E' diventato lo standard nel tempo.

- IPv4 address, DNS address and domain name obtained through DHCPv4
- Generation IPv6 link-local address
- Interface ID from IPv4 address
- DNS query to obtain PRL
- If not provided by DHCPv4 (proprietary)
- Periodic Router Discovery to each router
- On-link prefixes for autoconfiguration

2.20 Network center solution

Configuro intere reti IPv6 all'interno di una struttura ancora IPv4, rinunciando però in parte in quanto non è possibile utilizzare tutte le funzionalità di IPv6 e anche il range di indirizzi continua a essere ridotto.

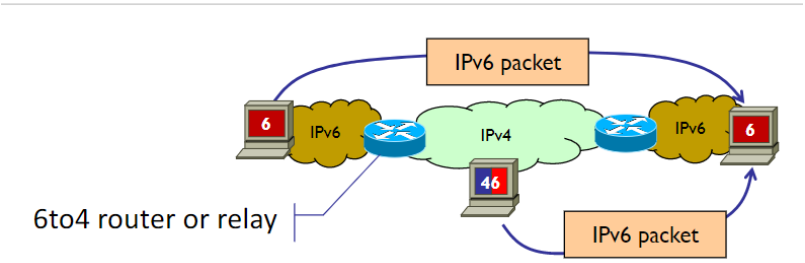


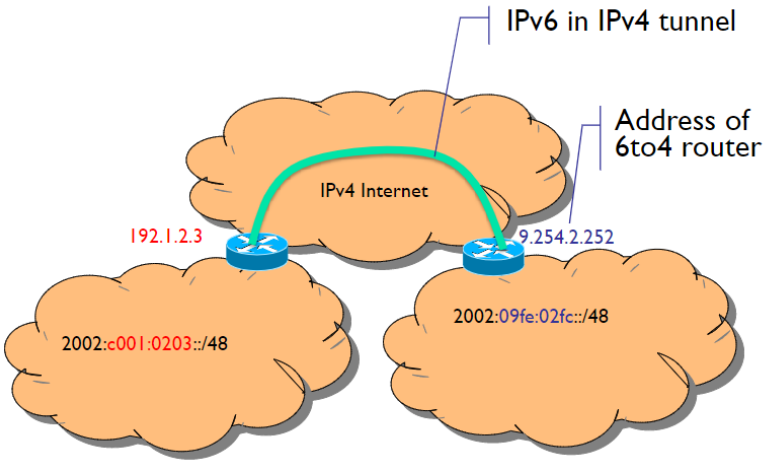
Figura 2.34: Host centered

2.20.1 6to4

Gli indirizzi dei relay sono embedded in un prefisso IPv6. Iniziano con `2002`, sono indirizzi pubblici (inizia con 2).

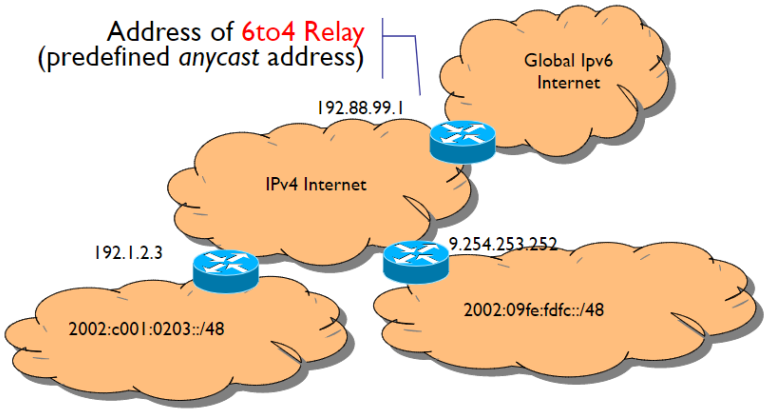
2.20.2 Basic 6to4 Scenario

Not meant for IPv4 host to IPv6 host communication



2.20.3 Mixed 6to4 scenario

6to4 Relay must be default gateway of 6to4 routers



2.20.4 Tunnel broker

- Communication with a tunnel broker server
- Identifies tunnel server and mediates tunnel setup
- IPv6 in IPv4 (a.k.a. proto-41) tunnels
- Tunnel Setup Protocol (TSP) or Tunnel Information Control (TIC) protocol used to setup tunnels

soluzione centralizzata.

2.21 Scalable, Carrier-grade Solutions

Soluzioni per grandi provider. Purtroppo ancora è necessario supporto, in quanto i server ipv4 devono poter comunicare con host ipv6 e host ipv4. Le soluzioni più utilizzate sono:

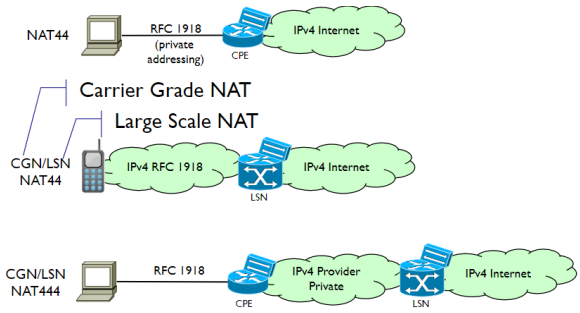
- **Several Options**
- **DS-Lite**
- **A+P (DS-Lite evolution)**
- **MAP-T and MAP-E**
- **NAT64**
- **6PE (MPLS-based)**

Tutte queste soluzioni si basano sul concetto di mapping di indirizzo IP, che è un concetto del NAT. Questo fa un mapping tra ipv4 e ipv4 e non è perciò un concetto nuovo. Quello che viene fatto è associare una porta a un indirizzo privato.

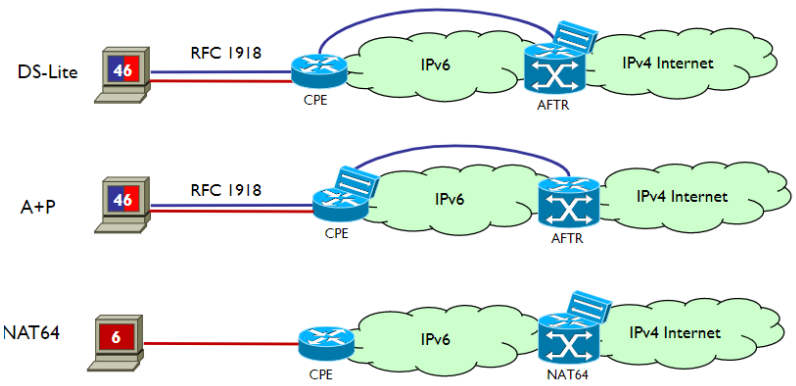
- LSN: large scale NAT, riesce a gestire una quantità di richieste molto grandi

E' possibile avere più livelli di NAT.

Avere più nat in cascata è abbastanza in comune.



Non dobbiamo dimenticare che nelle nostre soluzioni, anche se utilizziamo il nat, prevede comunque l'utilizzo di tunnel.



2.21.1 AFTR: Address Family Transition Router

Abilita host ipv4 di comunicare con altri IPv4 attraverso una rete IPv6. Permette di connettere strutture ipv6 con una struttura nel mezzo ipv4. Ha due tipi di funzionalità:

- sia come nat, gestire richieste di natting
- parte hw che consentono le operazioni di tunneling

2.21.2 DS-Lite

La soluzione dual stack lite abbiamo gli internet service provider usano come parte di backbone (infrastruttura di rete) di tipo IPv6. Possiamo avere così solo parti ipv4 che ipv6 con le altri sottoreti o ipv4 o ipv6. Questa soluzione, rispetto a quelle già viste, sono molto articolate e consentono di coprire tutte le casistiche.

- educes requirement for IPv4 addresses compared to dual-stack approach
  - Dual-stack requies public IPv4 address per host
- Extended NAT enables customer assigned (i.e., overlapping) addressing
  - IPv6 address of CPE in NAT table

i problemi sono:

- il customer non ha controllo sul nat
- problmi con server, ad esempio static mapping e port forwarding non possono essere configurati

2.21.3 A+P (Address plus port)

Il NAT è sotto il controllo dei customer. Il range di TCP/UDP è assegnato a ciascun customer (solo le porte sono utilizzate dal nat in uscita)

Concetto di spostare la complessità sulle foglie.

2.21.4 Mapping Address and Port (MAP)

Approccio di tipo stateless; cerchiamo di sfruttare i vantaggi del dhcp e del dns anche all'interno del sistema. In particolare non vado ad associare dei range di porte ma bensì dei set: un set si differenzia dal fatto che ci sono più porte che non sono necessariamente contigue. Inoltre, il CPE utilizza la stessa rete pubblica IPv4, così non siamo limitati.

- Client IPv4 address and port set mapped to unique IPv6 address
  - Prefix routed to CPE
- IPv4 public server address mapped to unique IPv6 address
  - Prefix routed to Border Relay
- MAP-E: MAP with Encapsulation
  - IPv4 packets are tunneled
- MAP-T: MAP with Translation
  - IPv4 packets are translated into IPv6 packets and then back to IPv4

sostituisco header ipv6 con un header ipv4, bisogna fare attenzione a non perdere informazioni.

a ogni CPE viene assegnato un unico PSID (Port set Identifier) e un public ipv4 address; Il PSID è un numero che identifica un set di porte.

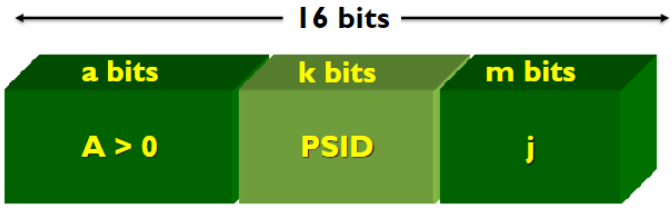


Figura 2.35: Port set

attenzione: non porre i primi a bit a zero perchè sennò diventa una well known port.

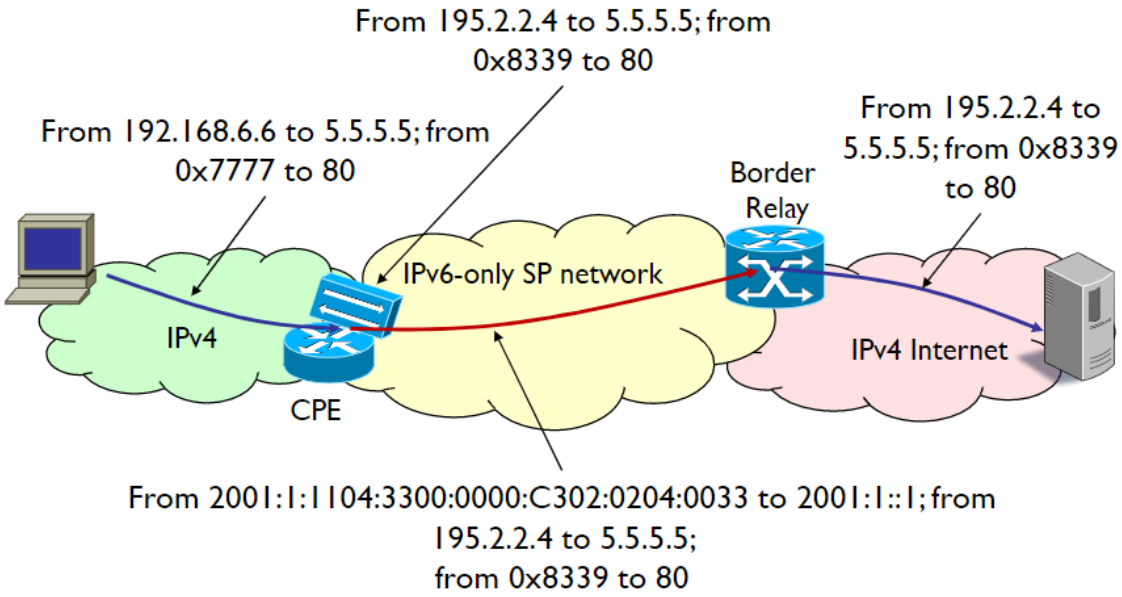
il CPE è associato a un unico valore del PSID. Queste informazioni viene messa nel Embedded address (EA).

- Rule IPv6 prefix
- Rule IPv4 prefix
- EA bits length

Moreover, a PSID offset (value of a) is set for the whole MAP domain.

- BR address must be known to CPEs
- Multiple BRs might have same address
- Anycasting
- MAP-E: BR address terminates tunnel
- MAP-T: prefix associated to BR used for translation of outside IPv4 addreses
- BR prefix is advertised on the backbone
- Might be advertised by multiple BRs

2.22 MAP-E



2.23 MAP-T

Prendo l'indirizzo IPV4 e lo vado a sostituire con un header IPv6.

2.24 Nat64 + DNS64

NAT64 (outbound) - Translates IPv6 address and packet into IPv4 - Picks a free IPv4 address/port from its pool - Builds NAT session entry

Il vantaggio del map risiede nella possibilità di avere più cpe e maggiormente distribuite.Questa è dunque una forma semplificata, che può vedere il suo utilizzo su rete più piccole.

3 Reti Wireless e cellulari

3.1 Introduzione

Le reti wireless sono reti che permettono la comunicazione tra dispositivi senza la necessità di un cavo fisico. Questo tipo di reti è molto comune nei nostri giorni, e sono presenti in molti dispositivi, come ad esempio i cellulari, i tablet, i computer portatili, i router, i dispositivi di rete, e molti altri. Un altro aspetto molto importante è la mobilità (che con il cavo non si poneva).

Una parte importante di ogni rete wireless è in realtà la sua componente wired, oltre al wireless link.

I link wireless comportano però alcuni svantaggi rispetto a un link cablato:

- Un degrado maggiore del segnale.
- Interferenza tra i dispositivi.
- Multipath propagation (fading): effetto dovuto ai rimbalzi sugli ostacoli.

Con SNR si identifica il *Signal to Noise Ratio*, ovvero la relazione tra il segnale ricevuto e il rumore. Questo valore è molto importante per la qualità del segnale.

La modulazione è il processo attraverso cui viene inviato un bit. Vi sono varie tipologie come:

- quam256
- quam16
- bpsk

Un ulteriore problema che ritroviamo all'interno delle reti wireless è inerente al problema del nodo (o terminale) nascosto: dati 3 nodi a, b, c se b comunica con entrambi i rimanenti, questi potrebbero però non essere a conoscenza della reciproca presenza e generare interferenze.

3.2 Wireless LAN

Nel corso degli anni lo standard 802.11 si è evoluto dando origine a vari standard. Tutti quanti utilizzano il protocollo csma/ca.

Un BSS (Basic Service Set) contiene:

- host wireless
- yb access point (base station)
- ad hock mode

Ogni rete wifi lavora su un canale differente, è dunque in grado di gestire fino a 16 frequenze (di cui utilizza solo una) per la trasmissione dei dati. La configurazione può essere automatica o manuale.

Ogni host rimane in attesa di un `beacon frame`: un frame particolare inviato dagli access point per effettuare la connessione. Il dispositivo si connetterà al beacon frame più forte in modo da aumentare la qualità della connessione. Per poter iniziare a dialogare con la rete wifi sarà inoltre necessaria una autenticazione.

Esistono due tipologie di scanning eseguite da un host che si connette a una rete:

- passive scanning: il beacon frame viene inviato dall'access point e ricevuto dall'host
- active scanning: è l'host a richiedere il beacon frame all'access point, in 4 fasi contraddistinte da un `probe request` dal host, un `probe response` dagli APs, un `association request` dall'host verso l'access point scelto e un `association response` dal APs in questione.

3.3 IEEE 802.11: multiple access (CSMA)

L'accesso multiplo su un canale wireless è un problema molto complesso, che prevede l'utilizzo di CSMA per l'eliminazione di collisioni tra due o più nodi che trasmettono contemporaneamente.

Mentre in ethernet viene utilizzato csma/cd (collision detection), in wireless viene utilizzato csma/ca (collision avoidance).

3.3.1 CSMA/CA

Il dispositivo che invia:

1. Se il canale è riconosciuto in idle per DIFS time, allora il dispositivo inizia a trasmettere.
2. Se il canale è riconosciuto occupato, viene avviato un random backoff time che lo pone in attesa prima del nuovo tentativo. Se anche al nuovo tentativo il canale è occupato, il dispositivo ripete il processo aumentatdo il random backoff interval.

Il dispositivo che riceve:

- Se il frame è ricuvato correttamente, viene inviato un ACK frame dopo **SIFS** tempo.

Il collision avoidance mostrato sopra non è però deterministico, per riuscire ad ottenerlo è possibile utilizzare un sistema di “prenotazione” che riserva il canale per i data frame usando dei pacchetti di “prenotazione” (RTS/CTS) caratterizzati da trame piccole. Questi possono ancora collidere, ma sono molto più piccoli e quindi meno dannosi. RTS (ready to send) viene inviato dal dispositivo che vuole trasmettere, CTS (clear to send) viene inviato dal dispositivo che ha ricevuto il RTS verso tutti i dispositivi in ascolto in modo da far partire chi deve trasmettere e porre in attesa i rimanenti.

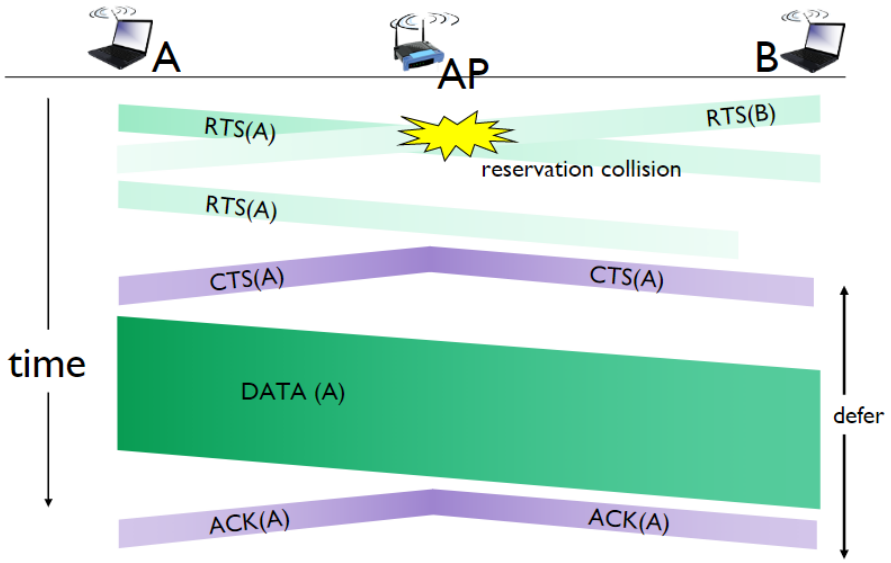


Figura 3.1: Schema temporale RTS-CTS

3.3.2 Frame addressing

Il frame contiene:

- frame control
- duration
- address 1: mac address del host wireless o Access Point che deve ricevere il frame
- address 2: MAC address del host wireless o Access Point che deve trasmettere il frame
- address 3: MAC address dell’interfaccia del router a cui l’access point è connesso
- seq control: necessari per gli ack
- address 4: usato solo in modalità ad hoc
- payload
- crc: controllo di errore

Dentro frame control troviamo ulteriori campi, tra cui ad esempio:

- protocol verison
- tipo (RTS, CTS, ACK, data)
- sottotipo
- bit per il powe management

3.3.3 Mobilità

Solitamente per le reti wirless l'host rimane all'interno della stessa subnet IP, motivo per cui è possibile riutilizzare lo stesso indirizzo.

nswitch: which AP is associated with H1? nself-learning; switch will see frame from H1 and "remember" which switch port can be used to reach H1 H1 BBS 2BBS 1 Wireless and Cellular Networks © see page 2 26

Dal punto di vista energetico, esiste il `node-to-AP` attraverso il quale l'Access Point viene a conoscenza del fatto che non deve inoltrare i frame al nodo, il quale si sveglierà prima del prossimo beacon frame (contains list of mobiles with AP-to-mobile frames waiting to be sent).

3.4 Reti Cellulari

Le reti cellulari sono reti wireless che coprono aree geografiche molto vaste attraverso la definizione di zone adiacenti denominate celle. A differenza di altre reti, gli host si muovono anche attraverso lunghe distanza e diventa importante non far disconnettere l'utente attraverso la gestione della mobilità denominata `handover`.

La copertura cellulare è garantita da reti isotopiche o con antenne direzionali da 120 gradi. L'emissione non è pero omni direzionale a causa della presenza di ostacoli (montagne, edifici), l'altezza, il guadagno dell'antenna, la morfologia del territorio, la potenza dell'antenna e infine le condizioni di propagazione (neve ecc).

Le celle si dividono in macrocelle e microcelle in base alle loro dimensioni. Le prime coprono un'area ragionevolmente estesa.

Abbiamo nuovamente un problema di accesso multiplo condiviso sul canale, risoolti attraverso varie tecniche:

- **FDMA**: scelgo una frequenza in cui trasmettere.
- **TDMA**: scelgo uno slot temporale in cui trasmettere.
- **CDMA**: assegno a ogni stazione un codice ortogonale agli altri, ovvero un gruppo di segnali da cui è possibile recuperare ogni singolo segnale.

- **SDMA**: riutilizzo di frequenze a patto che siano luoghi sufficientemente distanti tra loro.

Andremo quindi a riutilizzare le stesse frequenze in posti diversi in modo da non causare interferenze. Questo viene fatto a ccausa del numero ridotto di risorse, e allo scopo di coprire un'area più ampia e servire un alto numero di utenti.

Un gruppo di celle viene definito cluster, come nell'esempio in figura.

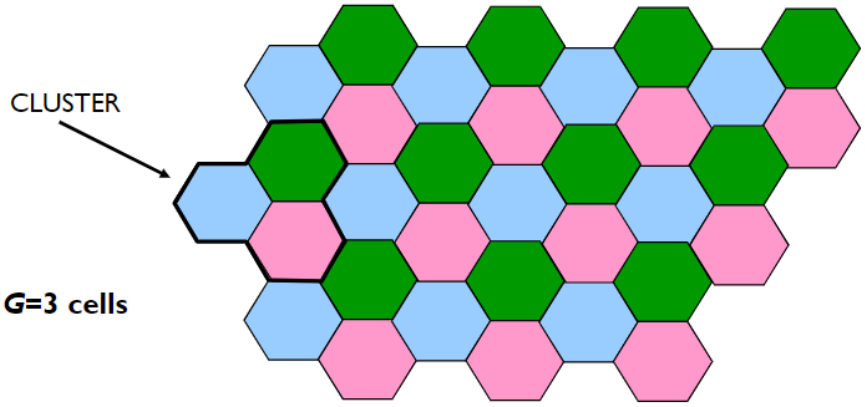


Figura 3.2: 3-Cell Cluster

Le celle verdi, rosa e blu usano un set differente di canali. Le celle dello stesso colore sono chiamate **"co-channel" cells**.

Se io vario la dimensione delle celle *R* cambio la capacità, ovvero il numero di utenti che posso soddisfare. Il numero di celle *G* impatta invece sul costo, in quanto un numero maggiore di celle ha dei costi maggiori. Aumentando il cluster aumento la qualità, aumentando anche G aumento la qualità ma diminuisco la capacità. Non esiste una legge assoluta per definire il valore di R e di G, sono però presenti alcune tecniche per diminuire le interferenze ed aumentare la capacità come:

- **splitting**: non utilizzare celle delle stesse dimensioni, ma basarsi sulle necessità.
- **sectoring**: utilizzare delle antenne non omnidirezionali per ridurre le interferenze e ridurre solo nelle direzioni in cui non è necessario.
- **tilting**: non usare un angolo a 90 gradi per la trasmissione.
- **creating femtocells**: possiamo creare delle celle non fisse in base alle necessità (esempio stadio o concerti).

3.4.1 Splitting

Utilizzare celle di dimensioni scelte in base alle necessità delle zone, e non quindi tutte uguali.

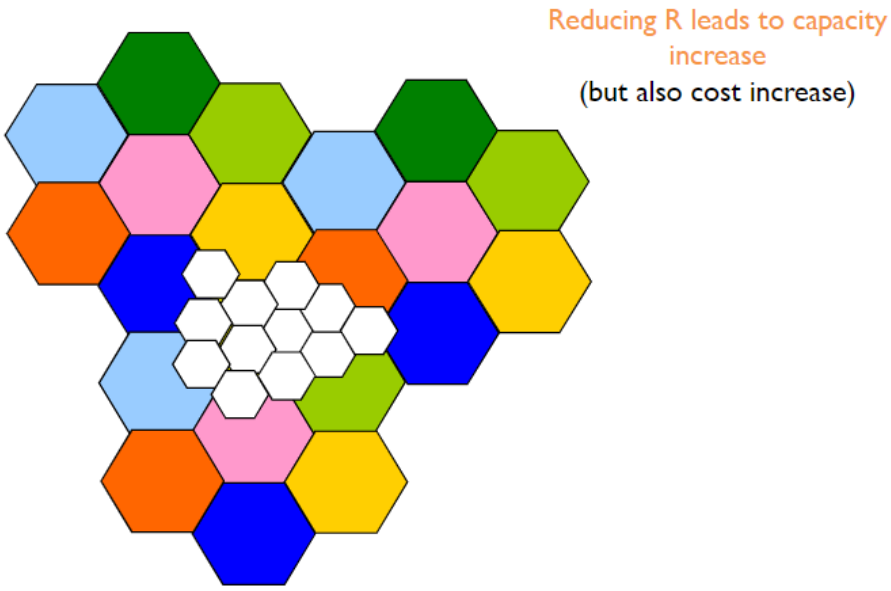


Figura 3.3: Splitting

3.4.2 Cell shaping

Utilizzo di antenne direzionali per avere celle con dimensioni e forme ad-hoc. E' possibile utilizzare una copertura multi livello (umbrella coverage). Le microcelle seguono l'utente dove si muove.

Altri esempi sono possibile tenendo conto di strade oppure ferrovie, dove le celle cercano di seguire la forma della strada.

3.4.3 Power Control

Metodo attraverso cui si gestiscono al meglio le capacità delle batterie a disposizione. Si cerca di ridurre l'utilizzo di potenza in base alle necessità. Per sapere la potenza necessaria da utilizzare si utilizzano strategie di due tipi:

- a catena aperta: sistema senza reazione
- a catena chiusa: sistema con feedback

3.4.3.1 Open loop

Il sistema, non avendo a disposizione un feedback, analizza e misura la qualità del segnale ricevuto per decidere se aumentare o diminuire la potenza in trasmissione. Questo adattamento non è preciso

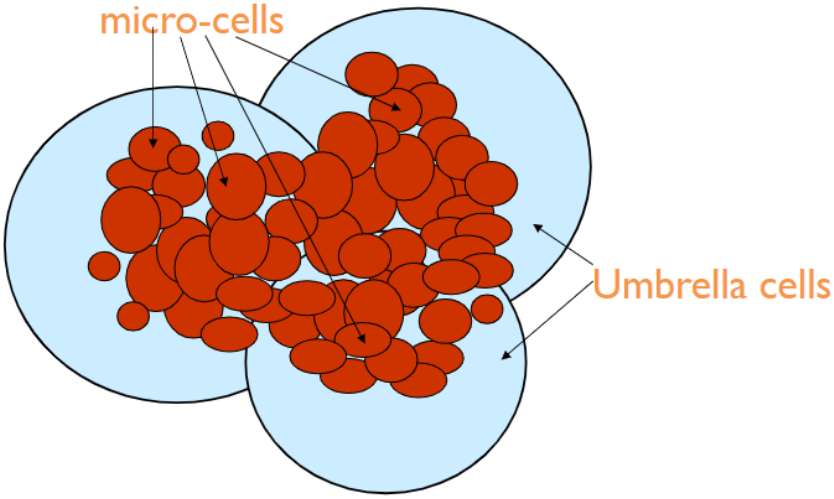


Figura 3.4: Shaping

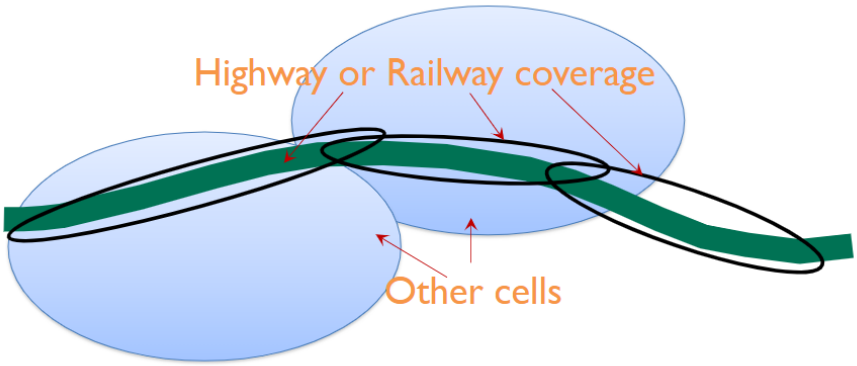


Figura 3.5: Shaping su strade

e non è detto che ciòò che succede su una frequenza sia uguale a un'altra. Not very accurate as uplink and downlink transmissions typically occur on different channels.

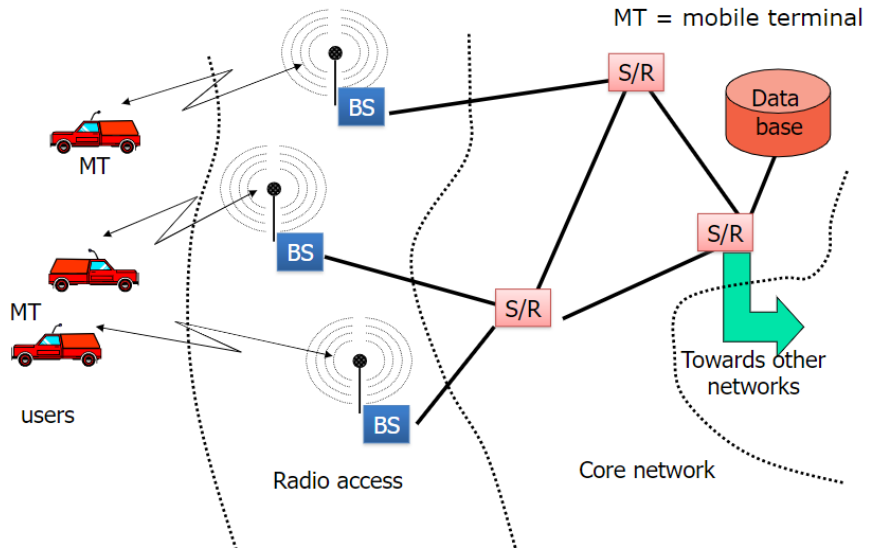
3.4.4 Frequency allocation

L'allocazione dele frequenze possono avvenire nei seguenti modi:

- Fixed Channel Allocation (FCA), Based on the concept of cluster, Frequencies are assigned in a static way, Frequency plan is changed only rarely to improve performance and adapt to slow variations in user traffic
- Dynamic Channel Allocation (DCA)
  - Resources assigned to cells by a central controller when needed
  - Frequency plan changes over time to adapt to the system status
- Hybrid Channel allocation Scheme (HCS)
  - One portion is statically allocated (FCA)
  - One portion is dynamically allocated (DCA)

3.4.5 Architettura di rete

Le reti sono costituite da mobile terminal che si connettono a dei BS (base station) radio che a loro volta si connettono a dei core network attraverso Switch Router (commutatori a pacchetto o circuito). I core network sono costituiti da un set di server che si occupano di gestire le connessioni e le risorse, in modo wired. Il database è molto importante ed è dove vengono memorizzate le informazioni degli utenti.



3.4.6 Registrazione

Permette a un terminale mobile di connettersi alla rete attraverso una registrazione che lo identifica e autentica. La procedura avviene peridiocamente ogni volta che si deve accedere al servizio.

3.4.7 Mobility Management

Per gestire la mobilità sono necessarie più procedure legate alla gestione:

- Roaming
- Location updating
- Paging
- Handover

3.4.7.1 Roaming

Il roaming è la capacità di un terminale di essere tracciabile quando si sposta nella rete. Il sistema deve memorizzare la posizione in un database e localizzare l'utente quando necessario. Per salvere tali informazioni, la rete viene divisa in location areas (LAs), gruppi di celle adiacenti. Ogni LA ha un identificativo univoco.

3.4.7.2 Location updating

La procedura che avviene ogni volta che un utente si sposta verso un'altra location area. Periodicamente l'utente deve comunicare la sua posizione alla rete, in modo da essere tracciato. Questa procedura è necessaria per mantenere aggiornate le informazioni sul database.

3.4.7.3 Paging

Procedure through which the system notifies a mobile terminal about an incoming call/data delivery The system broadcasts a paging message within the LA where the user is

3.4.7.4 Handover

Procedure that enables the transfer of an active connection from one cell to another, while the mobile terminal moves over the network area Complex procedure that poses constraints on the network architecture, protocols and signaling

- Intra vs. Inter Cell: It indicates whether the handover is between frequencies within the same cell or different cells
- Soft vs. Hard It indicates whether during handover both radio channels are active (soft) or only one at the time is active (hard)
- MT vs. BS initiated It indicates whether the first control message to start a handover is sent by the mobile terminal (MT initiated) or by the BS (BS initiated), i.e., which entity performs measurements to understand where and when a handover has to be executed
- Backward vs. Forward It indicates whether handover signaling occurs via the origin BS (backward) or the destination BS (forward)

3.5 Evoluzione della rete cellulare

Nel corso degli ultimi anni la rete cellulare ha subito una serie di evoluzioni che hanno portato ad una maggiore capacità di trasmissione e ad una maggiore efficienza energetica.

La prima generazione GSM era di tipo analogico, con ampio utilizzo di FDMA e traffico esclusivamente voce. La qualità del segnale era bassa e l'efficienza nel riutilizzo della frequenza era basso.

La seconda generazione comporta il passaggio al digitale, con il vantaggi in termini di servizi (sms) crittografia e e voice coding avanzato per ridurre la banda necessaria. La seconda generazione estesa, 2.5G, caratterizzata da GPRS/EDGE in europa e IS-95B in USA, viene introdotto il servizio dati con packet switched, 170kb/s in GPRS e 384kb/s in EDGE. Si passa a tariffe basate sul traffico e non più sul tempo.

La terza generazione, 3G, ha comportato dei miglioramenti in termini di data service (multimedia service), l'introduzione di CDMA e l'avvento di UMTS e CDMA2000. Il rate dati ha raggiunto i 2Mb/s ed possibile l'handover tra reti differenti oltre alla exploit spatial diversity. La generazione 3.5G ha comportato una evoluzione di UMTS soprattutto sul livello fisico, con miglioramenti del trasferimento dati fino a 56Mb/s in download e 22Mb/s in upload.

La quarta generazione, conosciuta come LTE, ha raggiunto un rate di 250Mb/s. Utilizza MIMO (multiple input multiple output) che consentono performance di modulazione più elevate. Per la prima volta abbiamo una rete completamente IP con l'introduzione di VoLTE per consentire il passaggio della voce sulla rete dati.

La quinta generazione, il 5G, ha lo scopo di unificare le tecnologie di accesso wireless rimuovendo la differenza tra rete wireless e cellulare, attraverso mmWave che consentono trasmissioni ad alto throughput. Introduce il NFV (network function virtualization) che permette di virtualizzare le funzioni di rete, come il routing, il firewall, il load balancing, il caching, il DPI (deep packet inspection) e il DDoS (distributed denial of service) protection. Inoltre, anche il SDN (software defined networking) permette di virtualizzare il controllo della rete consentendo di utilizzare un hardware general purpose.

3.5.1 GSM

Rete con full rate di 13 kbit/s e half rate di 6.5Kbit/s. Consente l'invio di SMS e servizi supplementari come call forward, recall, e busy tone.

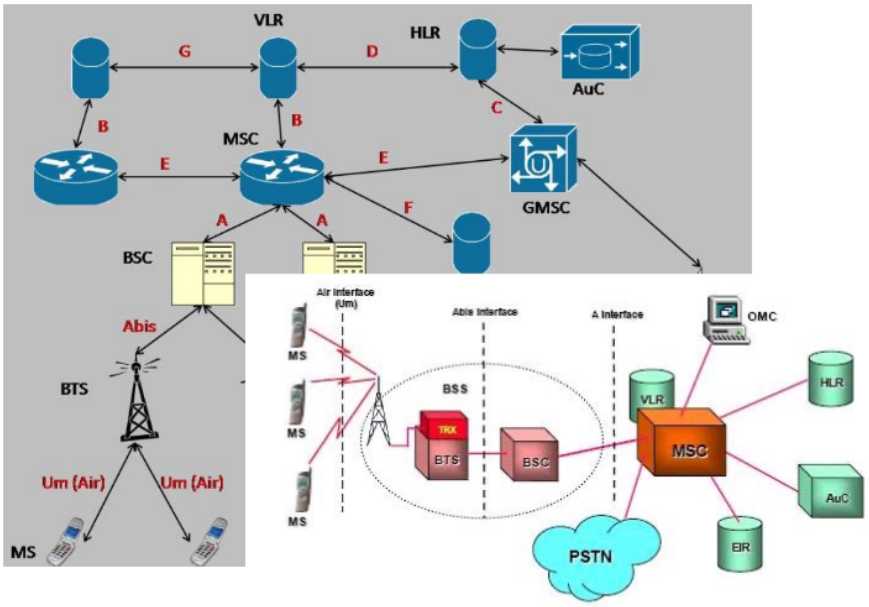


Figura 3.6: Architettura GSM

La Mobile Station (MS), ovvero il dispositivo, sono quelli in grado di connettersi alla rete GSM (come telefoni, antenne dei veicoli). Hanno differenti potenze di trasmissione all'antenaa:

- fino a 2W per i telefoni
- fino a 8W per dispositivi mobili
- fino a 20W per le antenne dei veicoli

La MS p però unicamente hardware, per connetteri alla rete è necessaria una SIM, ovvero una smart card con un processore e una memoria in grado di memorizzare, crittografato, le informazioni dell'utente come il numero di telefono, i servizi accessibili, parametri di sicurezza etc. MSI è l'identificativo univoche della SIM.

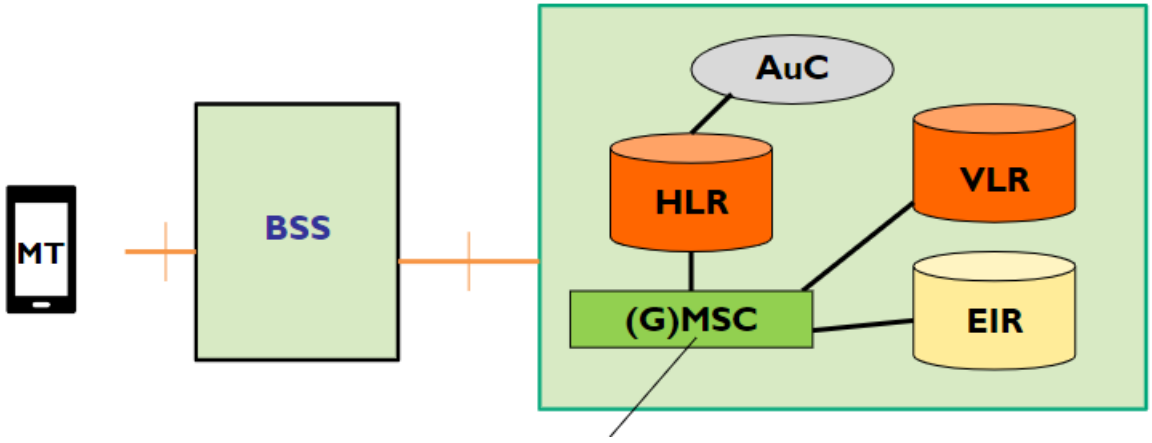
La Base Station Subsystem (BSS) comprende:

- BTS (base transceiver station): interfaccia fisica con il compito di trasmettere e ricevere.
- BSC (base station controller): gestisce il controllo delle risorse sull'interfaccia radio. BSC e BTS comuniciano con un link cablto. Un BSC controlla un alto unmero di BTS (da decine a centinaia). Tipicamente, BSC sono collocate con un MSC, invece di essere allocate vicino ai BTS. Il suo ruolo principale è quello di eseguire il transcodig vocale a 13 kb/s / 64 kb/s, eseguire il paging, radio

resource control (assegnamento dinamico delle frequenze ai BTS), misurazione della qualità del segnale e controllo dell'handover tra BTS controllato dallo stesso BSC.

Il network and switching subsystem (NSS) ha il compito di gestire le chiamate, il service support, mobility support e autenticazione. E' composto da:

- **MSC**: mobile switching center, ha il compito di gestire la mobility support, call routing tra MT, GSMC ovvero l'interfaccia tra GSM e le altre reti
- **HLR**: home location register, si occupa di salvare le informazioni nel database come le informazioni permanenti dell'utente (id, servizi abilitati, parametri di sicurezza) e dati dinamici per la gestione della user mobilità (VLE identifier).
- **VLR**: visitor location register, salva nel dtatabase le informazioni relative a dove si trova il MT attualmente nell'area controllata dal MSC come id, stato on/of, LAI, informazioni di routing e sicurezza.
- AUC: authetication center, autenticazione basata su un protocollo challenge & response con generazione di chiave di crittograzia per comunicazioni over-the-air.
- EIR: equipment identity register, memorizza le informazioni dei dispositivi rubati.



{width=450px}

Le frequenze allocate sono 859, 900 1800, 1900 MHz. Le frequenze sono differenti in base alla ricezione e alla trasmissione e funzionano attraverso FDD (frequency division duplex) system.

I canali GSM sono composti da una frequenza e uno slot, che identificano un canale fisico. Le trasmissioni sono organizzate in burst (da non confondere con pacchetti), blocchi di dati trasmessi su canali fisici. Sono simili ai pacchetti, ma funzionano su switching a circuito. La velocità di trasmissione è di 272 kbit/s. I cnali possono essere acceduti con FDMA o TDM, e le frequenze sono divise in FDM channels, ciascuno largo 200kHz. Ognuno è diviso in TDM frames, che a loro volta sono divisi in 8 slot.

Lo slot time dura 0.577 ms, e ogni time slot porta 1 trasmission burst. Gli slot sono raggruppati in TDM

frames, ciascuno di 8 slot.

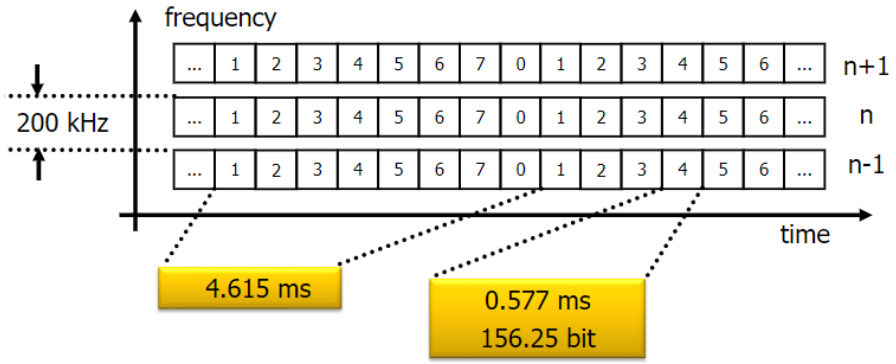


Figura 3.7: Accesso al canale

Il GSM non prevede una trasmissione simultanea (non è dunque full duplex), per limitare costi abbiamo un unico transceiver per cui è possibile o solo trasmettere o solo ricevere. Ogni MT trasmette per un time slot un burst di dati e rimane silezioso per gli altri 7 slot. I frame su UL e DL sono sincronizzati in base ai time slot e shiftati di 3 slot.

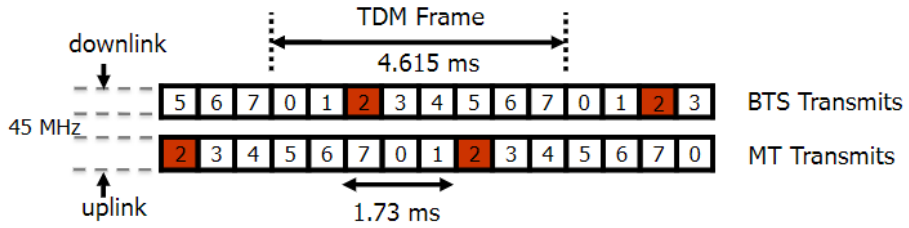


Figura 3.8: GSM frame

I tempi di propagazioni però non sono nulli, per cui possono nascere problemi nella struttura di questi slot. I burst trasmessi da MT potrebbero arrivare al BTS quando lo slot è già finito. Inoltre è possibile ci siano collisioni. La soluzione è utilizzare la timing advance, ovvero la trasmissione del MT comincia prima del reale inizio del timeslot. a inizio e fine birst sono presenti dei “bit di guardia” che permettono di sincronizzare i burst.

La struttura di un burst è caratterizzato dai bit di guardia, il coded data, stealing bit viene utilizzato per comunicare all’utente informazioni importanti.

I canali fisici del GSM soon composti da 8 canali, con timeslots da 0 a 7, mentre i canali logici mantengono le informazioni e specificano “cosa” è trasmesso. Sono mappati nel livello fisico in accordo a determinati criteri. I canali logici si dividono in control channels che trasportano le informazioni di controllo, e traffic channels che trasportano le informazioni.

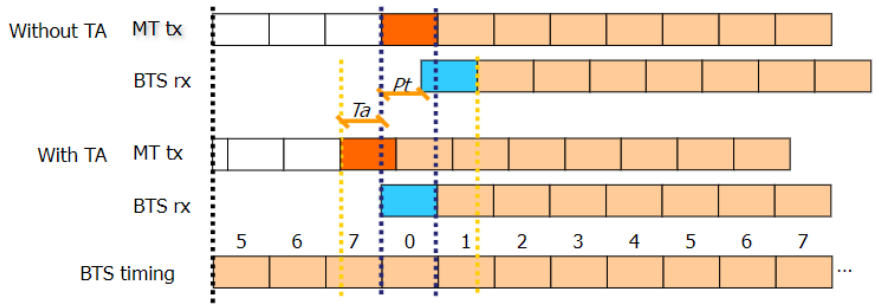


Figura 3.9: Timing advance

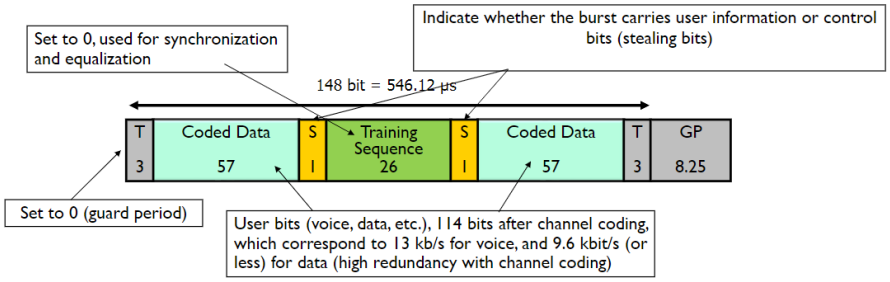


Figura 3.10: Burst structure

3.5.2 4G/LTE

Una delle caratteristiche è l'utilizzo del FDMA che va a soppiantare il CDMA, che era stato pensato per gestire in efficienza il fading e sembrava una tecnologia migliore per il trasferimento dei dati. Il CDMA è però difficile da mantenere in termini tecnologici e i rapporti costi/benevici non era sufficientemente buono, per questo motivo per LTE è stato pensato FDMA, ovvero un FDM dove le frequenze portanti sono più vicine e ortogonali (posso sovrapporre lo spettro) in modo da non generale interferenze.

Abbiamo una diffusione dei MIMO e il livello fisico è statp migliorato per arrivare ad downlink di 300Mb/s e uplink da 50Mb/s.

Le frequenze utilizzate dipende dalla distanza:

- 2600 MHz utilizzata per massimizzare la capacità in aree urbane
- 1800 MHz alta capacita ma limitata interferenza
- 800 MHz alta coperture e alta interferenza, per esempio nelle aree rurali.

Nella terminologia compaiono inoltre i termini:

- user plane: tutte le operazioni legate al trasporto di dato utente in dl o ul (access stratum)
- control plane: tutte le operazioni legate al setup, controllo e mantenimento delle comunicazioni tra utente e la rete (non access stratum)

La radio access network prende il nome di E-UTRAN, mentre il core network, che include tutti i dispositivi responsabili al trasporto da/a internet verso gli utenti, viene deniminato EPC.

Le BS vengono denominate eNodeB.

MME setup di un home tunnel da rete di casa a rete di un operatore, si occupa della mobilità. Attenzione: si riparla di pacchetti a differenza del gsm.

L'approccio utilizzato per EPC di tipo clean state design, di fatto ripensandolo completamente da zero. Utilizzo del packet switching transport per il traffico appartenente a tutte le classi QoS inclusi conversazione, streaming, tempo reale, non in tempo reale e in background.

- Radio resource management for: end-to-end QoS, transport for higher layers, load sharing/balancing, policy management/enforcement across different radio access technologies
- Integration with existing 3GPP 2G and 3G networks

3.5.2.1 Beares

Tutte le comunicazioni sono gestite attraverso dei "tunnel" denominati Bear. Tra il pwg e swg si crea un tunnel, e a sua volta dal svg e la base station si crea un altro tunnel, o ancora tra user agent e eNodeB.

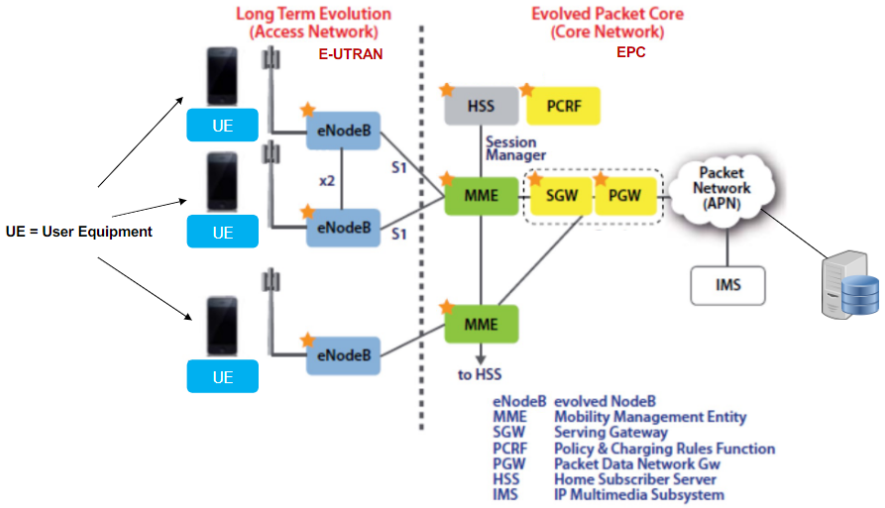


Figura 3.11: LTE architecture

All'interno della rete i tunnel possono essere creati per soddisfare dei requisiti in termini di qualità del servizio. Possono essere creati dei bearer dedicati per dei servizi specifici. E' presente un bearer default che stabilisce una connessione con il PGW quando UE è attivato. the UE can establish other dedicated bearers to other networks, based on quality-of-service (QoS) requirements.

Sono presenti in particolare tre differenti beares:

- The S5 bearer: connects the Serving Gateway (S-GW) to the P-GW. (The tunnel can extend from P-GW to the Internet).
- The S1 bearer: connects the eNodeB with the S-GW. Handover establishes a new S1 bearer for end-to-end connectivity.
- The radio bearer: connects the UE to the eNodeB. This bearer follows the mobile user under the direction of the MME as the radio network performs handovers when the user moves from one cell to another.

3.5.2.2 E-UTRAN

Principalmente sono dei eNodeB con un interfaccia X2 connetere eNodeB. Le funzioni principali sono di management delle risorsse audio come radio bearer control, radio mobility control, schedulinc ed allocazione dinamica delle risorse radio per uplink e downliik. Gestiscono la compressione (senza perdita) degli header, la sicurezza e la connettività verso EPC.

3.5.2.3 Data Plane e Control Plane

control plane è new protocols for mobility management , security, authentication (later)

Nel data plane abbiamo un estensivo uso dei tunnel che a livello datalink e fisico ha causato la creazione di nuovi protocolli per giustire gli accessi, oltre a nuovi standard di compressione per migliorare l'utilizzo del canale.

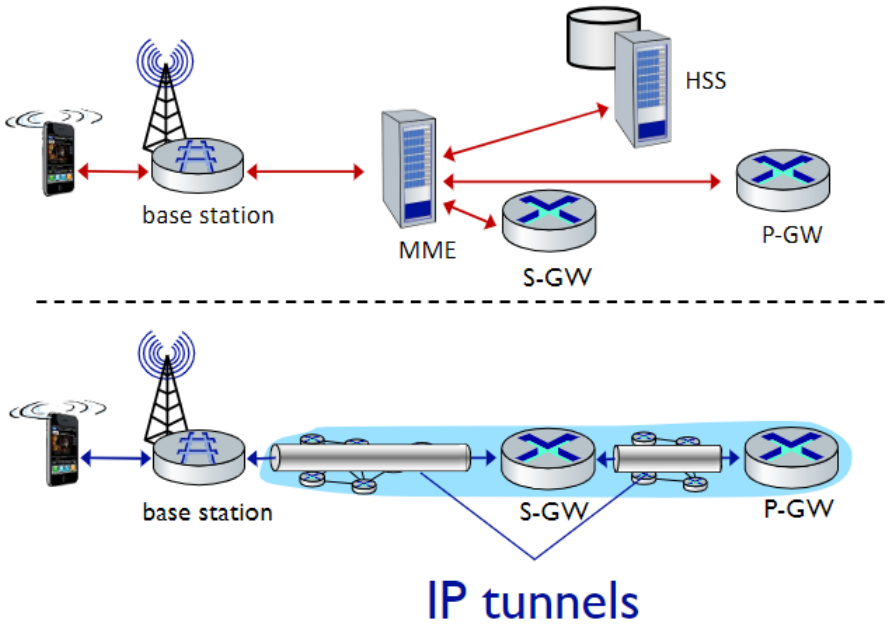


Figura 3.12: Data Plane (basso) e Control Plane (alto)

A livello 3 abbiamo IP, a livello data link abbiamo tre sottolivelli:

- **medium access**: equivalente del sottolivello mac, si occupa dell'accesso al canale
- **radio link**: si occupa della frammentazione e assemblaggio dei dati. Offre un reliable data transfer, ovvero si assicura che la comunicazione avvenga con successo.
- **Packet data convergence**: si occupa della compressione dell'header e dell'encryption.

Il livello fisico è gestito attraverso OFDM (tante frequenze ortogonali che minimizzano l'interferenza tra i canali) e definisce degli slot TDM (non diversamente dalla gestione del canale link wireless su GSM).

- downstream channel: FDM, TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
  - "orthogonal": minimal interference between channels
- upstream: FDM, TDM similar to OFDM

- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
  - scheduling algorithm not standardized – up to operator
  - 100's Mbps per device possible

Qui abbiamo tanto slot piccolini e la rete può assegnare più o meno slot in modo dinamico, in modo da adattarsi a quello che deve essere inviato in modo efficiente.

I bit trasmessi sono inseriti all'interno di un frame che ha una struttura suddivisa in modo predefinito denominata Physical channels. Ciascun channel ha informazioni specifiche relative a user data, tx/rx parameters, eNB identity, network control etc come il format del canale stesso. iascun canale fisico è mappato in una porzione del LTE subframe. I canali fisici sono divisi in downlink e uplink channels, ciascun u/d channel è ulteriormente diviso in data e control.

In uplink è possibile utilizzare gruppi di 3 TTIs per aumentare la performance e ridurrre l'overhead dei livelli superiori..

La tecnologia tunneling utilizzata per le reti cellulari si chiama **GPRS Tunneling Protocol**, ovvero tunnel realizzati su UDP.

Un nodo per associarsi a una base station deve eseguire vari step. Periodicamente la base station invia su tutte le frequenze un broadcast primary synch signal ogni 5ms. Il dispositivo troa il primary sync signal e a quel punto attende il second synch signal alla medesima frequenza. In questo modo si trovano le informazioni dalla base station come la bandwith del canale, la configurazion, cellular carrier info etc. Il dispositivo sceglie il BS a cui associarsi e inizia il processo di autenticazione e set up data plane.

I terminali possono andare in una delle due fasi di sleep, che consente un risparmio del consumo energetico. Le fasi di sleep sono:

- light sleep: ogni 100ms il dispositivo si sveglia per controllare se ci sono messaggi da inviare o ricevere. Se non ci sono messaggi il dispositivo torna a dormire.
- deep sleep: dopo 5 o 10 secondi di innatività, il dispositivo si mette in deep sleep. In questo modo si risparmia molto energia. Si da per scontato che l'utente debba ripartire da zero in quanto anche la cella potrebbe essere cambiata.

3.5.3 5G

L'obbiettivo del 5G è superare la differenza tra rete cellulare e wifi, e raggiungere un alta mobilità e connettere la società. Per riuscire a fornire i nuovi servizi saranno necessari, oltre al miglioramento della rete, di una integrazione di risorse di rete, di computing e storage. Per ottenere ciò è necessario dislocare le varie risorse e di "networks slices", porzioni di risorse riservate a una certa comunicazione

che consentano di emulare ciò che faceva il “circuito” ovvero qualità. Per fare ciò è richiesto l’utilizzo del SDN. Abbiamo bisogno di gestire tutte queste risorse e la relativa creazione in modo flessibile e dinamico, attraverso quello che è un “orchestratore di rete” denominato orchestrator function (o network).

Alcuni utilizzi potrebbero essere:

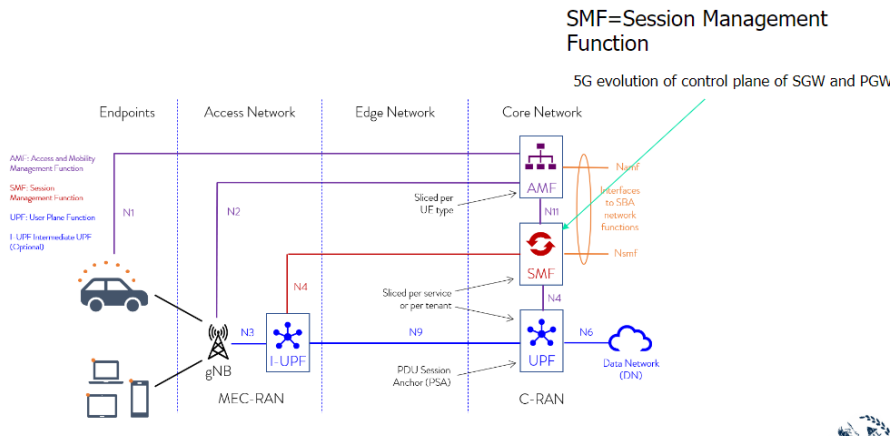
- **eMBB**: enanched mobile broadband, come in una rete 5G sia possibile usare servizi ad alta qualità per utenti mobili
- **mMTC**: massive machine type communication, comunicazione industriale a bassa latenza.
- **URLLC**: Ultra-Reliable Low-Latency Communication, in grado di garantire latenze fino a 1ms in modo da mettere in comunicazione la rete cellulare con, ad esempio, il robot.

Le tecnologie che si usano, e che si useranno, saranno:

- forme d’onda avanzate
- MIMO avanzate (antenne), che superano l’efficienza delle MIMO di LTE
- Millimeter Wave, ovvero uno spettro ad altissime sequenze con chunk fino a 2Ghz
- software define networking, SDN is an approach to networking in which routing control is centralized and decoupled from the physical infrastructure (data plane), which is distributed
- Network Function virtualization, muove i servizi di rete dall’hardware al software, creando una virtual building blocks capace di connettersi semplicemente.
- SDN/NFV Orchestration, ovvero la gestione di tutte queste risorse in modo dinamico e flessibile.

La Radio access Network è basata sui gNodeB, evoluzione dei eNodeB. E sono presenti gli Edge Network (MEC) che ha computing e storage elements per i servizi locali, mentre il Core Network include tutti i dispositivi responsabili per il trasporto dei dati da e verso internet attraverso i dispositivi utenti.

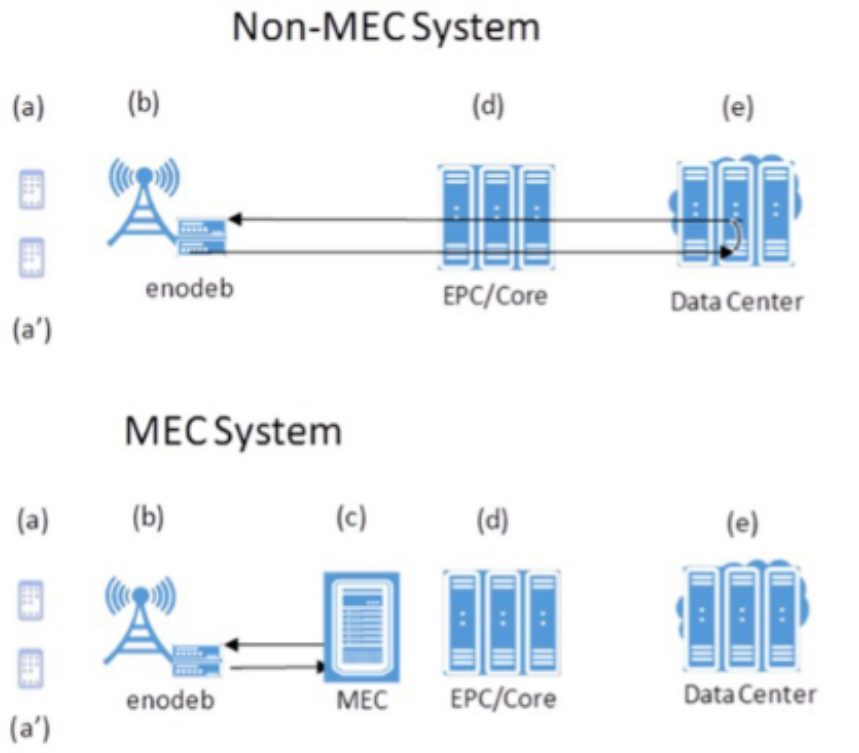
Abbiamo una distinzione netta tra il data plane e il control plane.

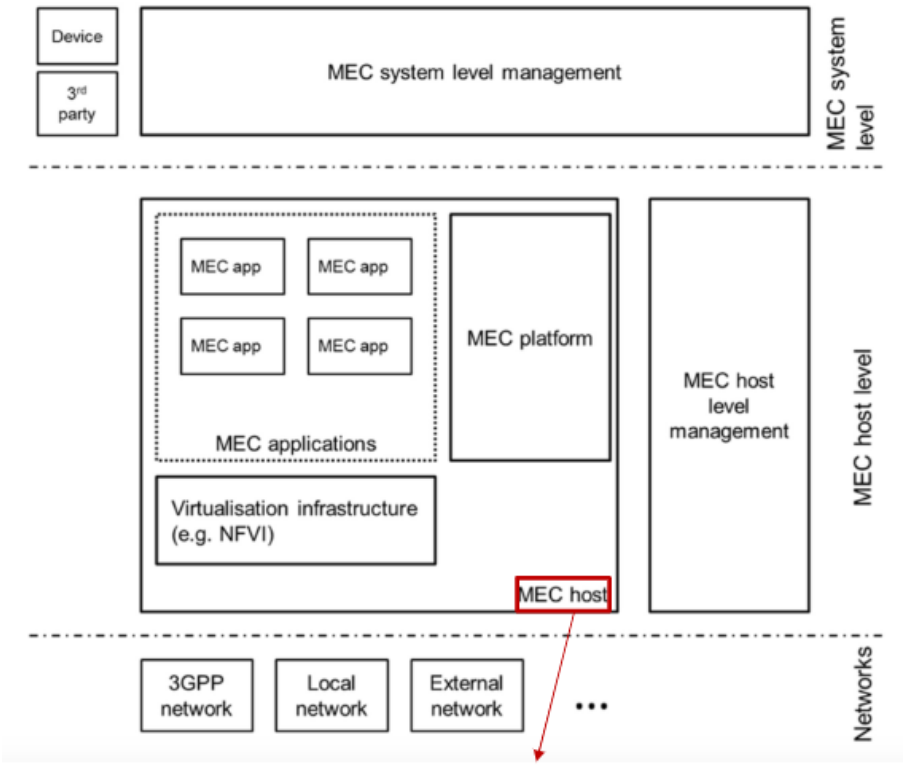


3.5.3.1 Edge Network

L'infrastruttura edge network fornisce servizi IT e cloud computing ai dispositivi mobili, in prossimità dei mobile subscribers. La standardizzazione è cominciata nel 2014 e pubblicata nel 2017. I benefi attesi sono:

- ultra low latency
- alta bandwitch
- accesso real time alla radio network
- contextual information
- location awareness
- flexible and exendable framework for services





MAC host contains the MEC platform and a virtualization infrastructure which provides compute, storage, and network resources for the MEC applications.

3.5.3.2 Radio Access Network

Introduzione di un framework flessibile basato slot, che consenta l'utilizzo di un numero variabile di slot per subframe. La trasmissione può iniziare in un punto qualsiasi dello slot. Supporta lo slot aggregation per trassmissioni con dati molto pesanti. Different subcarrier spacing ("numerology"): shorter slots for higher spacing.

3.6 Mobilità nel 4G/5G

Nelle reti cellulari la mobilità è gestita chiedendo alla rete di riferimento dove l'utente si trovi (stesso approccio di trovare una persona di cui non si conosce la persona, come chiamare a casa per chiedere ai genitori dove sia). E' presente una home network e una visited network dove faccio roaming. Quando accedo alla visiting network la nuova rete mi assegna un indirizzo (spesso privato). Devo dunque dialogare con mms di quella rete in modo che possa indicare al hss che mi trovo attualmente nella sua rete. Quando un utente si sposta devo gestire 4 fasi:

- associazione alla nuova base station
- configurare la control plane informando la rete dove si trova il dispositivo
- configurazione della data plane per la creazione dei tunnel
- mobile handover, se la cella dovesse cambiare (ad esempio durante la chiamata) dovrebbe essere eseguito l'handover

La configurazione della data plane tunnel per i dispositivi avviene:

- S-GW a BS tunnel: quando il dispositivo cambia base station, semplicemnte cambia l'endopoint ip address del tunnel
- S-GW a home P-GW tunnel: implementazione del routing indiretto
- tunneling via GPT (GPRS tunneling protocol): i datagrammi del dispositivo vengono inviati allo streaming server incapuslati utilizzando GTP inside UDP, all'interno del datagramma

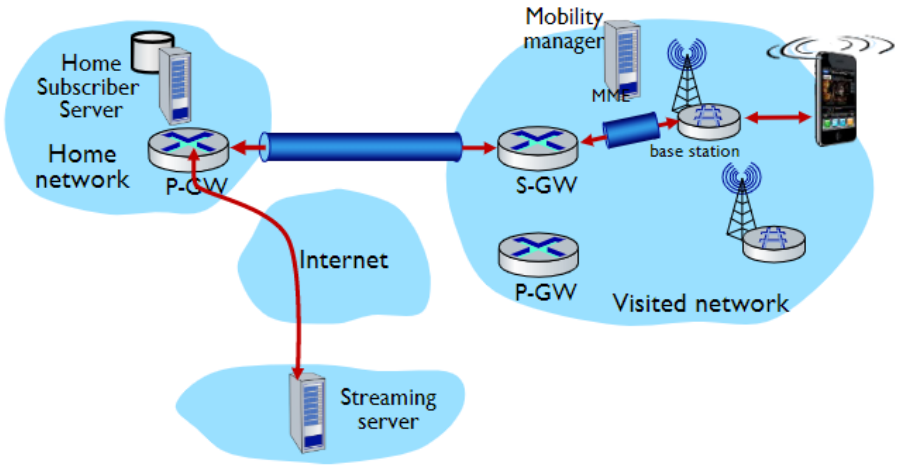


Figura 3.13: Configuring data plane

L'handover attraverso le base station all'interno della stessa rete cellulare avviene in quattro step:

- il source BS seleziona il target BS, invia un Handover Request message al traget BS
- Il target BS prealloca un radio time slots, risponde con HR ACK con le informazioni del dispositivo
- Il source BS informa il dispositivo del nuovo BS (ora il dispositivo può inviare e ricevere attraverso la nuova BS) e l'handover risulta completato agli occhi del dispositivo
- Il source BS smette di inviare i datagrammi al dispositivo, invece li inoltra alla nuova base station (che li inoltrerà al dispositivo attraverso il radio channel)
- Il target Bs informa MME che del nuovo BS per il dispositivo (MME istruisce S-GW di cambiare l'endopooint del tunnel al nuovo BS)
- La base station target inoltra un ack alla base station sorgente informando che l'handover è completato e la bs sorgente può rilasciare le sue risorse.

- I datagrammi del dispositivo possono ora utilizzare il nuovo tunnel dal target BS al S-GW