



Politecnico
di Torino

Tecnologie e Servizi di Rete

Computer Engineering

Marco Lampis

23 gennaio 2023

Indice

0 Informazioni	1
0.1 Contributi	2
1 IPv4 Summary	3
1.1 Indirizzi speciali	3
1.2 Indirizzamento IP con classi	3
1.3 Indirizzamento IP senza classi (CIDR)	4
1.4 IP routing	5
1.5 IP addressing methodology	6
1.5.1 Esercizi	8
1.6 Multicast	18
2 IPv6	21
2.1 Perché IPv4 non basta e soluzioni	21
2.2 Chi assegna gli indirizzi IP	22
2.3 Address pool status e scalabilità	22
2.4 Notazione	23
2.5 Routing	24
2.6 Multicast	25
2.7 Unicast	26
2.7.1 Link local/site local Addresses	27
2.7.2 Unique Local Addresses	27
2.7.3 IPv4 Embedded Addresses	28
2.7.4 Loopback Addresses	28
2.7.5 Unspecified Addresses	29
2.8 Anycast Addresses	29
2.9 Architettura del protocollo	29
2.10 Packet Header Format	30
2.10.1 Hop-by-Hop Extension Header	32
2.10.2 Routing Extension Header	32
2.10.3 Altre estensioni	33

2.11	Interfacciarsi con i livelli più bassi	34
2.11.1	Incapsulamento	34
2.11.2	Address mapping	34
2.11.3	IPv6 Multicast transmission	34
2.12	Neighbor Discovery and Address Resolution	35
2.12.1	Solicited-Node Multicast Address	35
2.12.2	Risoluzione di un indirizzo	35
2.13	La transizione tra IPv4 e IPv6	37
2.14	ICMPv6	37
2.14.1	Formato del messaggio	39
2.14.2	Multicast Group Management	42
2.14.3	Host Membership Discovery	42
2.15	Device Configuration in IPv6	43
2.15.1	Privacy extension Algorithm	44
2.15.2	Indirizzi	44
2.15.3	ICMP Redirect	46
2.15.4	Duplicate Address Detection (DAD)	46
2.15.5	Fasi di configurazione di una configurazione Stateless	48
2.16	Scoped Addresses	48
2.17	Routing Protocols	49
2.18	La transizione da IPv4 a IPv6	50
2.18.1	Host centered solutions	50
2.18.2	Network center solution	52
2.19	Scalable, Carrier-grade Solutions	54
2.19.1	AFTR: Address Family Transition Router	56
2.19.2	DS-Lite	56
2.19.3	A+P (Address plus port)	57
2.19.4	Mapping Address and Port (MAP)	57
2.19.5	Port Set	58
2.19.6	Mapping Rules	58
2.19.7	Border Relay	58
2.20	NAT64 + DNS64	59
3	Reti Wireless e cellulari	63
3.1	Introduzione	63
3.2	Wireless LAN	65
3.2.1	CSMA/CA	66

3.3	Reti Cellulari	68
3.3.1	Cluster	69
3.3.2	Power Control	72
3.3.3	Allocazione della frequenza	72
3.3.4	Architettura di rete	73
3.4	Evoluzione della rete cellulare	75
3.4.1	GSM - Seconda generazione	76
3.4.2	4G/LTE - quarta generazione	80
3.4.3	5G	86
3.5	Mobilità nel 4G/5G	89
4	Principi del modern Lan Design	93
4.1	Ripetitori	93
4.2	Bridge	95
4.3	Modern LANs	97
4.3.1	Transparent bridges	97
4.3.2	Filtering database	98
4.4	Multiple LANs	99
5	VPN	105
5.1	Modalità di deployment	108
5.1.1	Site to Site VPN Tunneling (s2s)	108
5.1.2	End to End VPN Tunneling (e2e)	109
5.1.3	Remote VPN Tunneling	109
5.1.4	Overlay Model	109
5.1.5	Peer Model	110
5.1.6	Customer Provisioned VPN	110
5.1.7	Provider Provisioned VPN	110
5.1.8	Access VPN Customer Provisioned	111
5.1.9	Tunneling	112
5.2	Topologie	112
5.3	Layers	112
5.3.1	Layer 2	112
5.3.2	Layer 3	113
5.3.3	Layer 4	113
5.4	Generic Routing Encapsulation (GRE)	114
5.4.1	Enhanced GRE (version 1)	115

5.5	Protocolli di livello 2	115
5.5.1	L2TP	116
5.5.2	Point to Point Tunneling Protocol (PPTP)	118
5.6	IPsec	119
5.7	SSL VPN	121
5.7.1	Protocolli con SSL	122
5.7.2	Application Translation	123
5.7.3	Application Proxying	123
5.7.4	Port Forwarding	124
5.8	VPN Gateway Positioning & anomalies	124
5.9	Posizione	124
5.10	Anomalie	125
5.10.1	Monitorability Anomaly	125
5.10.2	Skewed Channel anomaly	126
6	Routing	129
6.1	Introduzione	129
6.1.1	Proactive routing	129
6.1.2	On the fly routing	129
6.2	Proactive routing algorithms	130
6.2.1	Non adaptive algorithms	130
6.2.2	Adaptive algorithms	130
6.3	Distance vector (Bellman-Ford)	131
6.4	Path Vector	135
6.5	Link State Routing Algorithm	135
6.6	Algoritmo di Dijkstra	136
6.7	Internet Routing Architecture	136
6.7.1	Autonomous System	138
6.8	Protocolli di routing	139
6.8.1	Algoritmi IGP	139
6.8.2	Algoritmi EGP	141
7	MPLS	143
7.1	Architettura di rete	144
7.2	Storia di MPLS	146
7.3	Header MPLS	147
7.4	LSP setup	147
7.4.1	Label Binding	147

7.4.2	Label Mapping	148
7.4.3	Label Distribution	148
7.4.4	Static label binding (and mapping)	148
7.4.5	Dynamic label binding	148
7.4.6	Label Distribution Protocol	148
7.5	Protocolli di routing	149
7.6	Routing modes	149
7.6.1	Hop by hop routing	149
7.6.2	Explicit routing	150
7.6.3	Constraint based routing	150
7.6.4	Label Distribution Protocol (1)	150
7.7	Traffic Engineering	150
7.8	CoS e QoS	152
7.8.1	Class of Service (CoS)	152
7.8.2	Quality of Service (QoS)	152
7.9	Fast fault recovery	152
7.10	Scalabilità	153
7.11	Penultimate Hop Popping (PHP)	153

0 Informazioni

La seguente dispensa è stata realizzata 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 o a eseguire una pull request su GitHub.

E' possibile riutilizzare il materiale con le seguenti limitazioni:

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

E' per tanto possibile:

- Modificare parzialmente o interamente il contenuto

Questi appunti sono disponibili su GitHub al seguente link:

1 https://github.com/Guray00/polito_lectures



Figura 1: Repository GitHub

La seguente dispensa è rilasciata sotto la Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License.



0.1 Contributi

La condivisione è alla base del successo di qualsiasi progetto, citando:

“Open source is about collaborating; not competing. ~ Kelsey Hightower”

La seguente dispensa ha avuto il prezioso contributo di:

- Marco Lampis

1 IPv4 Summary

In questo capitolo viene fatto un ripasso generico su quanto visto nei corsi precedenti relativo al **IPv4**, 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

In IPv4, oltre ai “classici” indirizzi, sono presenti alcuni 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.

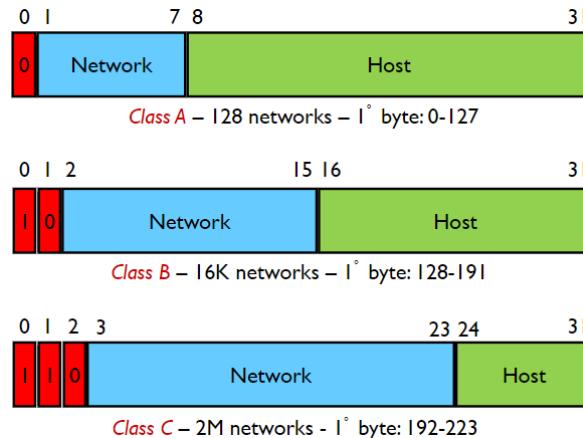
Ricorda: Spesso al giorno d’oggi non è consentito l’invio di messaggi in broadcast per motivi di sicurezza.

1.2 Indirizzamento IP con classi

Le rappresentazioni possono essere **classes** (a classe) o **classness** (senza l’utilizzo di classi). In particolare la suddivisione in classi sulle seguenti 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.

**Figura 1.1:** Classi

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 **Classless InterDomain Routing** permette di indirizzare la porzione più precisa di indirizzi tra rete e dispositivi, rendendo la porzione di rete 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:

```
1 200.23.16.0/23          # prefix length
2 200.23.16.0 255.255.255.254.0 # 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 compreso tra 0 e 255.

Non tutti i valori sono permessi, 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 l'ultimo numero puntato sia multiplo di $2^{(32-x)}$.

Esempi:

```

1 130.192.1.4/30 => 4%2^(32-30) = 4%4 = 0, si!
2 130.192.1.16/30 => 16%2^(32-30) = 16%4 = 0, si!
3 130.192.1.16/29 => 16%2^(32-29) = 16%8 = 0, si!
4
5 130.192.1.1/30 => 1%2^(32-30) = 1%4 != 0, no!
6 130.192.1.1/29 => 1%2^(32-29) = 1%8 != 0, no!
7 130.192.1.1/28 => 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.

Ricorda: prefix length e netmask sono due modi equivalenti per rappresentare un indirizzo.

1.4 IP routing

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

- **destinazione:** indirizzi ip
- **interfaccia:** eth0, wlan etc...

Quando viene inviato un pacchetto, si cerca un match all'interno della tabella per identificare dove l'indirizzo IP di destinazione. 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:

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

Destination	Next	Type
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
0.0.0.0/0	80.105.10.2	static
130.192.0.0/24	130.192.3.2	static
130.192.1.0/24	130.192.3.2	static
130.192.3.8/30	130.192.3.2	static

1.5 IP addressing methodology

Preso come esempio la rete che segue, 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. Calcolare quanti indirizzi è possibile allocare.
4. Verificare 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. Calcolare la netmask / prefix length.
6. Calcolare address range
7. Calcolare gli indirizzi degli host

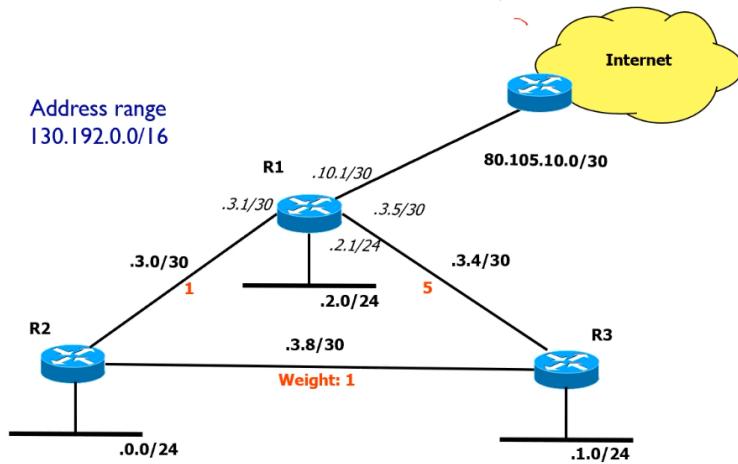
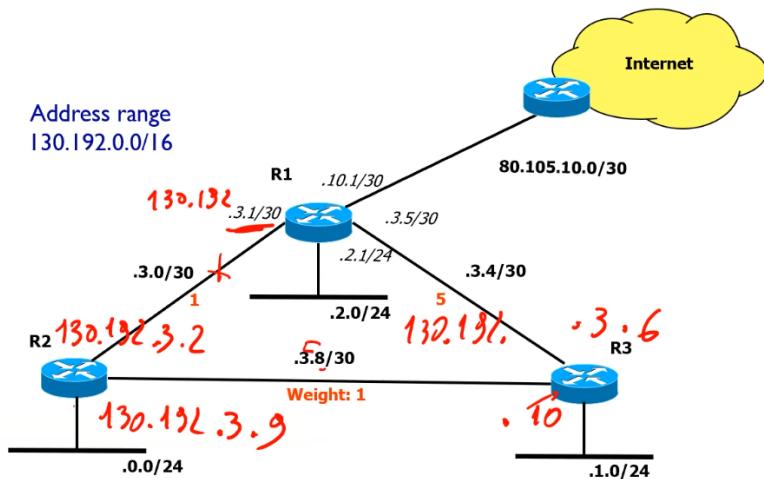
Nota: in basso a sinistra sono richiesti 43 indirizzi per 40 dispositivi. Ciò è dovuto al fatto che oltre ai 40 richiesti serve l'indirizzo di rete, l'indirizzo di broadcast e l'indirizzo del router.

Per riuscire a trovare le sottoreti, si prosegue in ordine dal più grande (*ovvero il valore minore*):

```

1 # tutta la rete (/24)
2 10.0.0.0/24
3
4 # subnet2 (/25), 32-25 = 7 => 2^7 = 128 indirizzi
5 # range: 0-127
6 10.0.0.0/25 <- primo
7 10.0.0.127 <- ultimo
8

```

**Figura 1.2:** routing**Figura 1.3:** routing2

IP Addressing: methodology

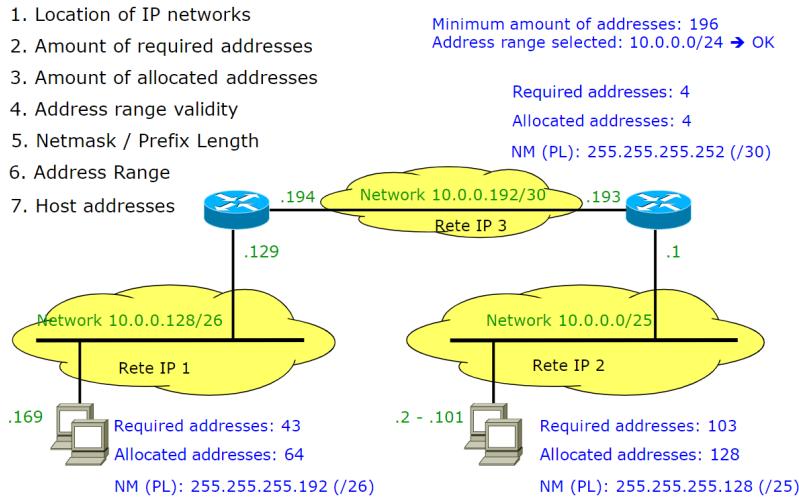


Figura 1.4: Rete di esempio

```

9 # subnet3 (/26), 32-26 = 6 => 2^6 = 64 indirizzi
10 # range: 128-191
11 10.0.0.128/26 <- primo
12 10.0.0.191      <- ultimo
13
14 #subnet4 (/30), punto punto
15 10.0.0.192/30

```

Suggerimento: quando calcoli i bit per la maschera, vedi quanti zeri rimangono e fai $256 - 2^{n_zeri}$.

Ricorda: Quando lasci lo spazio per gli indirizzi è sempre necessario riservarne 2 per l'indirizzo di rete e l'indirizzo di broadcast. Per questo motivo nelle connessioni punto punto (/30) devi comunque riservare 4.

1.5.1 Esercizi

1.5.1.1 Esercizio 1

Assuming a classless addressing plan, define the netmask and the prefix length that have to be assigned to possible networks in order to contain the given number of hosts

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 $256 - 2^{\text{bit}}$

1.5.1.2 Esercizio 2

Verifica se i seguenti indirizzi sono validi o meno.

IP / Prefix Length pair	Valido?
192.168.5.0/24	Si, $0 \bmod 2^{(32-24)} = 0$
192.168.2.36/30	Si, $36 \bmod 2^{(32-30)} = 0$
192.168.2.36/29	No, $36 \bmod 2^{(32-29)} \neq 0$
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, $3 \bmod 2^{(1)} \neq 0$
192.168.2.0/31	No, /31 non ha senso
192.168.2.0/23	Si, $2 \bmod 2^{(1)} \neq 0$
192.168.16.0/21	Si, $16 \bmod 2^3 = 0$

IP / Prefix Length pair Valido?

192.168.12.0/21 No, $12 \bmod 2^3 \neq 0$

Consiglio: quando devi verificare la validità con prefix length che supera 8, significa che il controllo è da fare sul gruppo precedente (e così via), quindi puoi fare $2^{(32-x)-8}$. Stesso ragionamento quando si supera 16, 24, ecc...

1.5.1.3 Esercizio 3

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

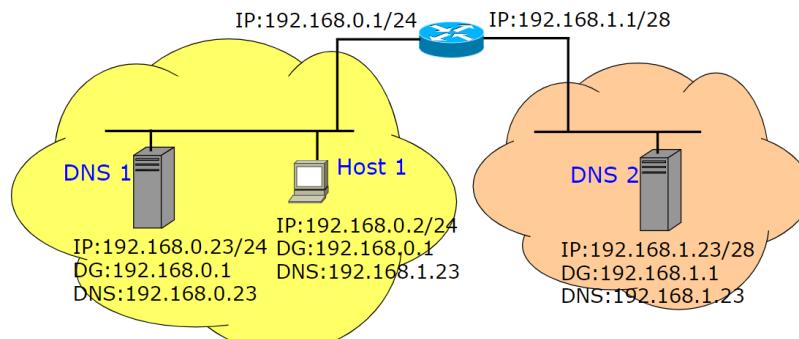


Figura 1.5: Configurazione errata

Il problema è relativo al fatto che il router non si trova nella medesima rete della rete arancione, in quanto essendo una /28 il range di indirizzi vanno da 192.168.1.0 a 192.168.1.15. In realtà quelli utilizzabili però sono da .1 a .14 in quanto i due rimanenti sono riservati per broadcast (.15) e rete (.0).

Le soluzioni sono due:

- utilizzare un /27 invece del /28 in modo da arrivare fino a .31, rendendo .23 corretto
- cambiare l'indirizzo del dns, ad esempio con 192.168.1.10

1.5.1.4 Esercizio 4

Definire un piano di indirizzamento IP per la rete in figura. Considerare entrambi i tipi di indirizzamento: “tradizionale” (senza minimizzare) e una soluzione che minimizzi il numero di indirizzi IP utilizzati. si assuma di utilizzare il range 10.0.0.0/16.

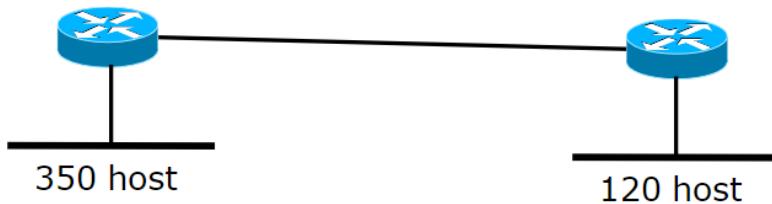


Figura 1.6: Rete

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 dunque /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.

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

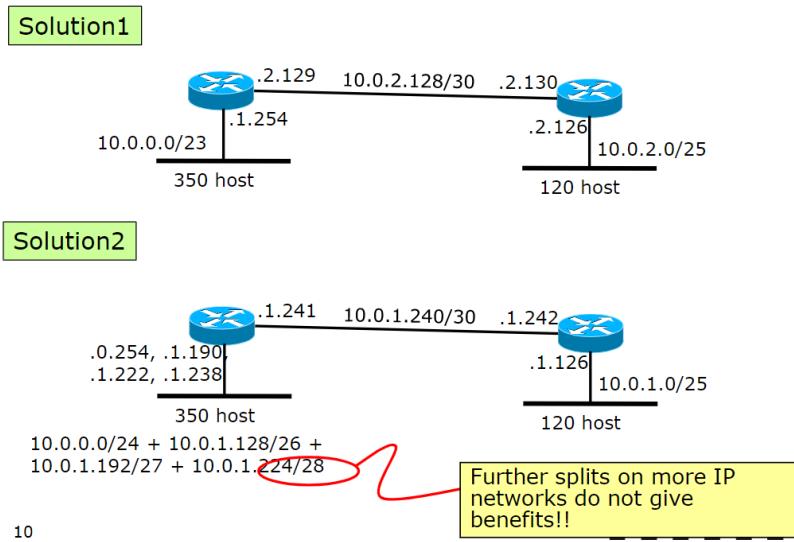
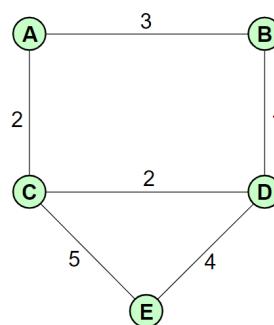
Questa soluzione comporta un grosso spreco, in quanto c’è un /25 che non viene utilizzato.

La seconda soluzione prevede l’utilizzo di più sottoreti per non sprecare indirizzi, in particolare un /24, /26, /27, /28 per un totale di $256 + 64 + 32 + 16 = 368$ indirizzi.

1.5.1.5 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 calcolarlo si prende un router come riferimento, ad esempio **A**, ei si calcolano tutte le distanze dagli altri nodi.

**Figura 1.7:** Soluzioni**Figura 1.8:** 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 (*ad esempio router più nuovi*).

Node A		Node B		Node C	
Destination	Next-hop	Destination	Next-hop	Destination	Next-hop
B	B	A	A	A	A
C	C	C	D	B	D
D	B/C	D	D	D	D
E	C	E	D	E	E

Node D		Node E	
Destination	Next-hop	Destination	Next-hop
A	B/C	A	C
B	B	B	D
C	C	C	C
E	E	D	D

Figura 1.9: Soluzione esercizio 5

1.5.1.6 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.

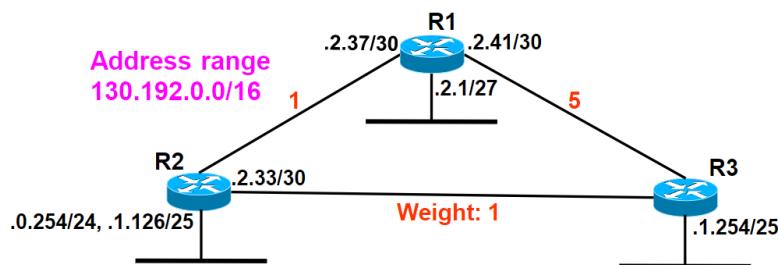


Figura 1.10: Esercizio 6

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

dest	next hop	Type
130.192.2.36/30 (A)	130.192.2.37	D
130.192.2.0/30 (B)	130.192.2.1	D
130.192.2.40/30 (C)	130.192.2.41	D
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.

Nota: l'indirizzo 130.192.2.38 è l'indirizzo del router R2, 130.192.2.36 è l'indirizzo della sottorete (scelto prendendo il più alto multiplo di $2^{(32-30)}$ minore di 36), mentre 130.192.2.37 è l'indirizzo dell'interfaccia di R1 per comunicare con R2.

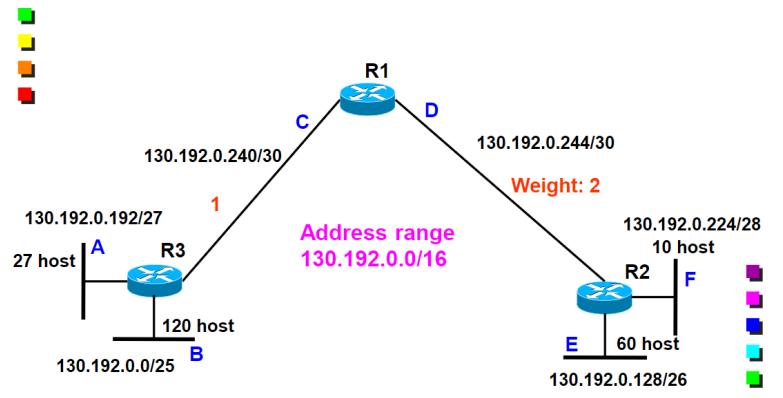
1.5.1.7 Esercizio 7

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).

**Figura 1.11:** Esercizio 7

- **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:

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.

Ricorda: Il piano di indirizzamento si fa sempre partendo dalla sottorete più grande, ovvero l'intero minore.

1.5.1.8 Esercizio 8

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

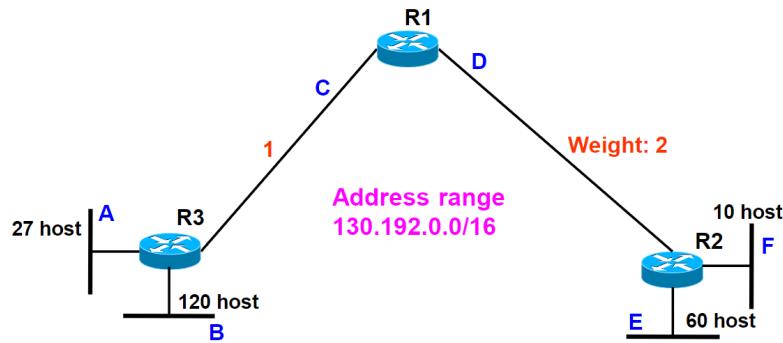


Figura 1.12: Esercizio 9

1.5.1.9 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.

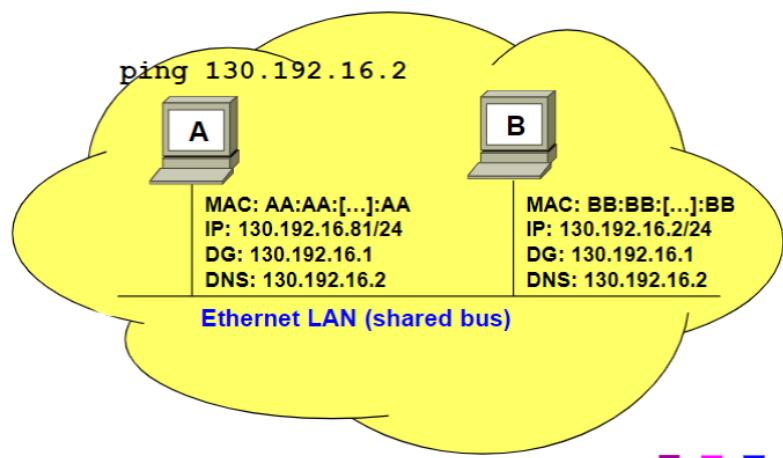


Figura 1.13: Esercizio 10

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 sì, entrambi coerenti sulla 130.192.16.0/24).

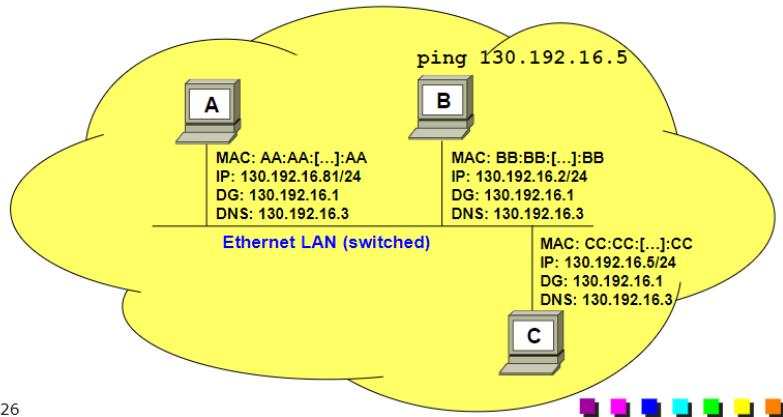
Scriviamo ora la tabella:

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.

1.5.1.10 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.



26

Figura 1.14: 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
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 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).

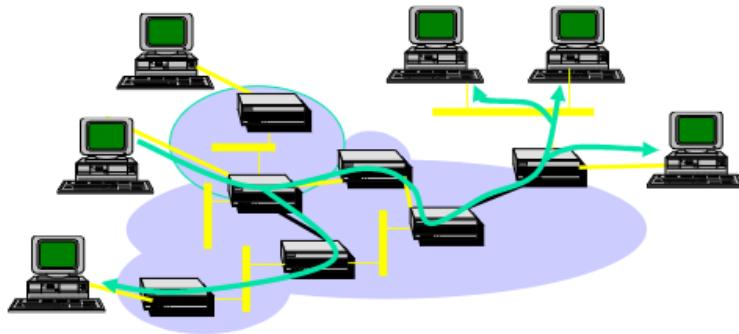


Figura 1.15: Multicast

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 esadecimale. 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.

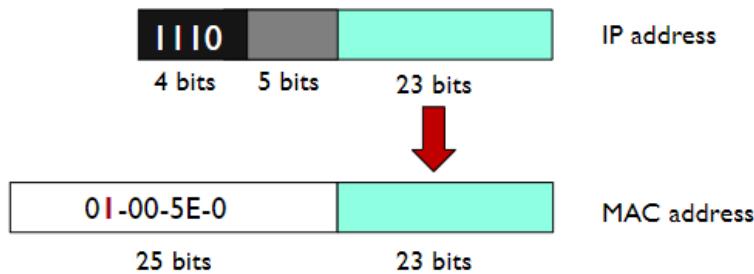


Figura 1.16: Mappatura IP a MAC

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. Nonostante l'introduzione del protocollo, IPv4 è ancora largamente utilizzato e non è stato completamente sostituito, al contrario, 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
- Supporto alla Quality of Service

Riuscire a definire il protocollo IPv6 ha richiesto molto tempo, attualmente è in una fase di migrazione (utilizzando soluzioni temporanee applicate su IPv4).

2.1 Perché IPv4 non basta e soluzioni

Il protocollo IPv4 ha indirizzi di lunghezza pari a **32 bit**, con un totale di circa **4 miliardi** di indirizzi. Nonostante ciò, solo parte di questi indirizzi possono essere effettivamente 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 tali problemi sono:

- Introduzione di reti “su misura” mediante l'utilizzo di netmask.
- Utilizzo di indirizzi privati (intranet), ma non è abbastanza da risolvere il problema.

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

2.2 Chi assegna gli indirizzi IP

Gli indirizzi IP vengono assegnati da parte dell'organizzazione **IANA**, che fornisce 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 più piccoli 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:

- far parte del pool di indirizzi **non allocati da IANA**
- far parte del pool di indirizzi **non allocati da RIR**
- assegnato a un end user entity ma non advertised dal BGP
- assegnato e advertised dal BGP (*Border Gateway Protocol*)

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 e con loro anche i protocolli
- 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.

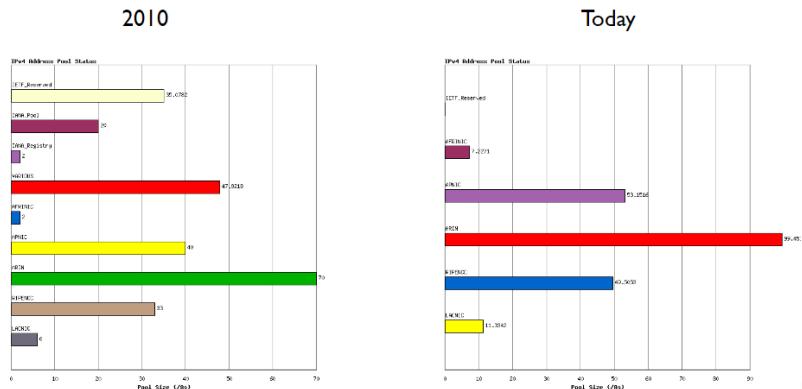


Figura 2.1: Status degli address pool

2.4 Notazione

E' stato scelto, attraverso un approccio 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 utilizzata non è più puntata, ma utilizza gruppi di **2 byte** (4 cifre esadecimali) separati dal carattere **:**.

Tale notazione può essere resa più compatta nei seguenti modi:

- è possibile rimuovere i gruppi pari a 0000 comprimendoli in 0 (o gruppi aventi degli zeri all'inizio). Esempio: da 1080:0000:0000:0007:0200:**A00C**:3423:**A089** a 1080:0:0:0:7:200:**A00C**:3423:**A089**.
- è possibile omettere un gruppo di soli zeri inserendo **::** (1080::7:200:**A00C**:3423:**A089**), ma **solo una volta**. Questo perché in caso contrario non sarebbe possibile sapere il numero di zeri omessi.

Se mettessimo **FEDC::0876:45FA:0562::3DAF:BB01** avremmo raffigurati 12 dei 18 byte, ma non saremmo in grado di dedurre in che modo sono distribuiti i 6 byte mancanti tra i due **::**.

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.

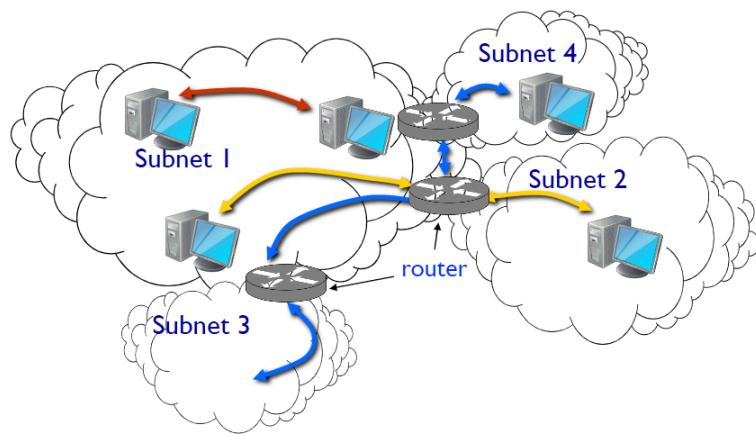


Figura 2.2: Routing

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 è previsto 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 più necessario l'utilizzo di classi.

Nota: il prefix length non sarà, per quanto detto precedentemente, superiore a 64.



n=64

Figura 2.3: Struttura dell'indirizzo

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

- **Link:** physical network.
- **Subnetwork:** Link, set di host con lo stesso prefisso.

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:

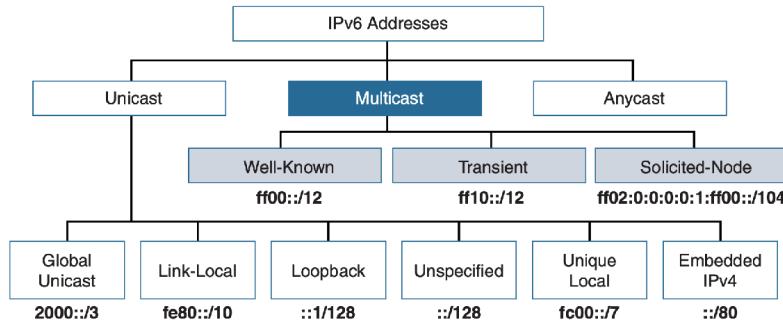


Figura 2.4: Spazio di indirizzamento

2.6 Multicast

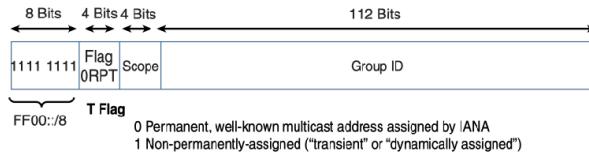
L'equivalente dell'indirizzo multicast IPv4 224.0.0.0/4 è FF00::/8, che si suddivide in:

- **Well-known Multicast:** FF00::/12, utilizzato per comunicazioni di servizio e vengono assegnati a gruppi di dispositivi, sono riservati. Un esempio è l'indirizzo di google (8.8.8.8).
- **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 la **scomparsa in IPv6 l'utilizzo del broadcast**, che in seguito alle evoluzioni ha dimostrato essere un rischio per la sicurezza.

L'indirizzo si scomponete in:

- **8 bit** iniziali, identificano che è un indirizzo multicast (tutti i bit sono posti a 1).
- **4 bit** per il **T flag**, dice se è well known (permanente o non permanente), viene assegnato da IANA.
- **4 bit** per lo scope, consente ai dispositivi di definire il range dei pacchetti multicast.
- **112 bit** per il group ID.

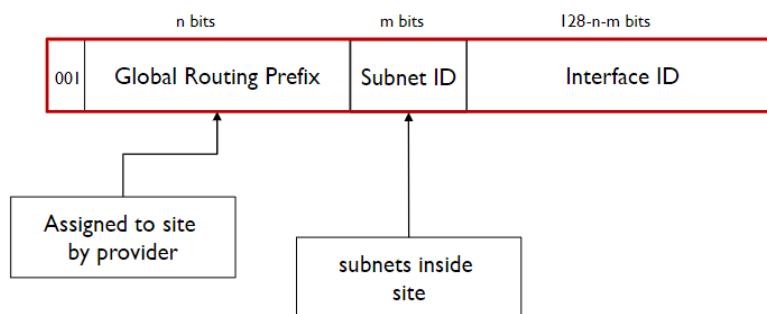
**Figura 2.5:** Struttura indirizzo multicast

2.7 Unicast

Gli indirizzi **unicast**, anche denominati *aggregatable global unicast addresses*, continuano a essere disponibili in IPv6, si suddividono in:

- 2000::/3, Global Unicast
- FE80::/10, Link-Local
- ::1/128, Loopback (in IPv4 era 127.0.0.1)
- ::/128, Unspecified
- FC00::/7, Unique Local
- ::80, Embedded IPv4

Sono indirizzi di tipo aggregato, utilizzati in modo equivalente agli indirizzi pubblici in IPv4. Hanno la caratteristica di essere raggiungibili e indirizzabili globalmente, oltre a essere plug and play. Attualmente sono disponibili in un range definito tra 3FFF:: e 2000::. Questi indirizzi hanno i primi 3 bit (più significativi) posti a 001.

**Figura 2.6:** 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

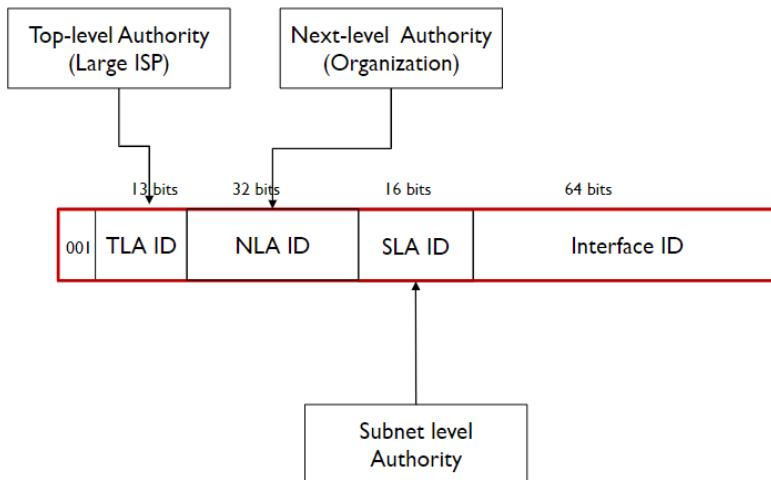


Figura 2.7: Global Routing Prefix

2.7.1 Link local/site local Addresses

I **link local/site local** sono un gruppo di indirizzi compresi tra **FE80** ed **FEBF** e vengono assegnati in automatico ai link quando viene acceso un router.

Gli indirizzi **Link local**, identificati nella rete **FE80 :: /64**, vengono assegnati quando più router devono parlare tra di loro oppure devono annunciarsi a un router vicino, oltre a consentire una configurazione automatica o quando un router non è presente.

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

2.7.2 Unique Local Addresses

Gli **Unique Local Addresses** (ULA) 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 **FFC00 :: /7** e vengono utilizzati dai dispositivi che non hanno mai necessità di connettersi all'internet o 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, potrebbe essere assegnato in futuro
- **FD00 :: /8**, se L flag è 1, l'indirizzo è assegnato localmente

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



Figura 2.8: Unique Local Addresses

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

2.7.3 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** (sedici bit posti a 1).

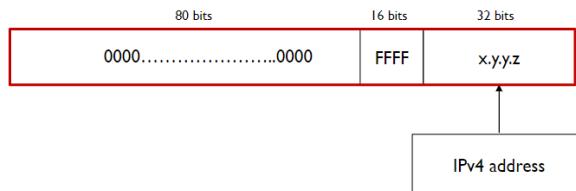


Figura 2.9: Struttura indirizzi IPv4 Embedded

2.7.4 Loopback Addresses

L'indirizzo di loopback viene utilizzato per finalità di test e consiste nel inviare un pacchetto IPv6 a se stesso. E' identificato da **::1** (equivalente di **127.0.0.1** di IPv4) ed è subordinato alle medesime regole di IPv4:

- Non può essere assegnato a un'interfaccia fisica.
- Pacchetti con un indirizzo di loopback non dovrebbero mai essere trasmessi oltre il dispositivo.
- I router non devono mai fare il forwarding di un pacchetto contenente un indirizzo di loopback.
- Il dispositivo deve fare il drop di pacchetti ricevuti da un'interfaccia se il destinatario è un indirizzo di loopback.

2.7.5 Unspecified Addresses

Un indirizzo unicast non specificato è tale da contenere solo 0. Tale indirizzo viene utilizzato come sorgente per indicare l'assenza di un indirizzo. Non può essere assegnato a un'interfaccia e viene utilizzato per il duplicate address detection in *ICMPv6*.

2.8 Anycast Addresses

Gli indirizzi anycast possono essere assegnati a più di un'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*

Sono invece stati aggiornati senza modifiche essenziali:

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

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

2.10 Packet Header Format

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

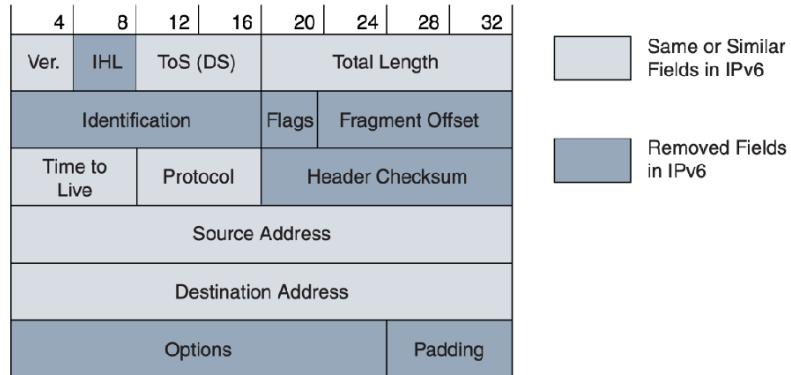


Figura 2.10: Header IPv4

L'header utilizzato in IPv6 è invece il seguente:

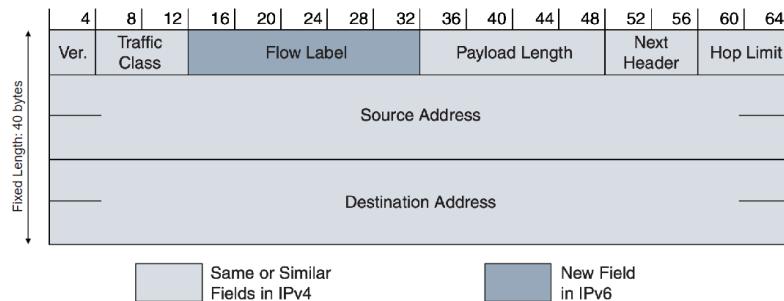


Figura 2.11: Header IPv6

Osservando le immagini si può notare come alcune informazioni siano state rimosse:

- **Header Checksum:** viene utilizzato per verificare se il dato trasmesso è corrotto, non è più necessario in IPv6.
 - **Ridondante:** le tecnologie di data link al livello due hanno i propri meccanismi di checksum.
 - I protocolli di livello superiore come UDP e TCP hanno i propri meccanismi di checksum.
- Frammentazione
 - I router IPv6 non frammentano i pacchetti a meno che non siano loro la sorgente dello stesso.

- I pacchetti più grandi di MTU vengono droppati e viene restituito alla sorgente un messaggio di errore [ICMPv6 Packet Too big](#).

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.

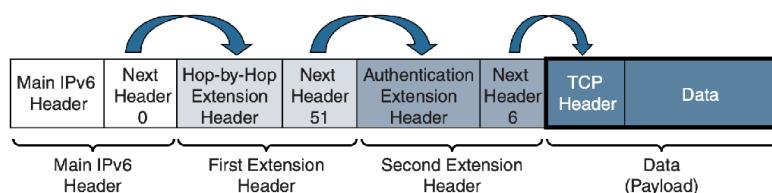


Figura 2.12: Chaining

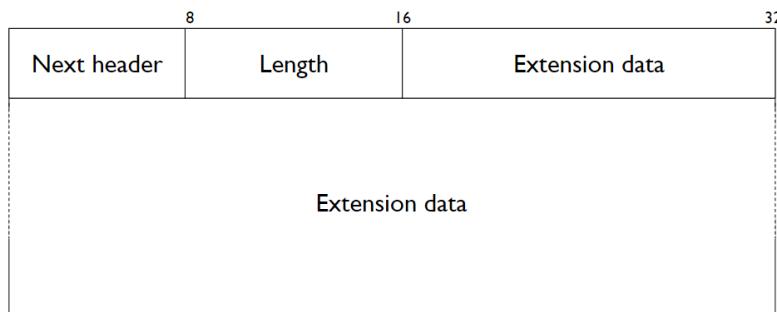
Inoltre, sono presenti:

- **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). Ad esempio: 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.

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.

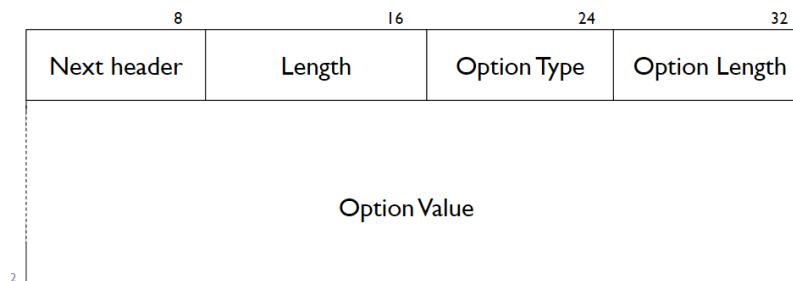
Nota: Header length non serve più! Viene eseguita la frammentazione attraverso il next header.

**Figura 2.13:** Extension Header Format

2.10.1 Hop-by-Hop Extension Header

L'**Hop-by-Hop Extension Header** è 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.

**Figura 2.14:** Hop-by-Hop Extension Header

Nota: 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 IPv6.

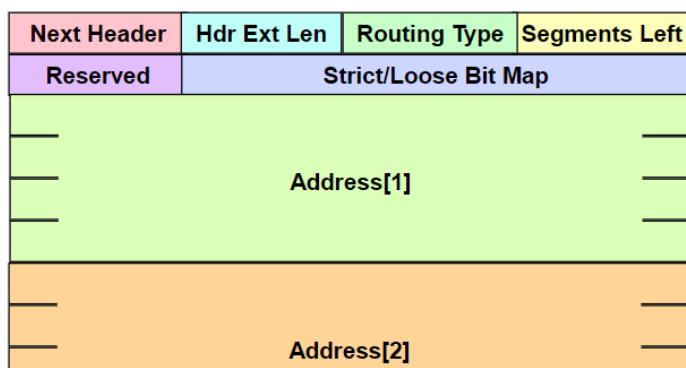


Figura 2.15: Routing Extension Header

2.10.3 Altre estensioni

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

- Fragment Extension Header: utilizzato quando la sorgente necessita di dividere il pacchetto in frammenti, ciascuno dei quali ha un proprio main IPv6 header e un fragment extension header. Il contenitore del pacchetto riunisce i frammenti.
- Authentication and Encapsulating Security Payload Extension Headers: utilizzato da IPsec (una suite di protocolli per la sicurezza).
 - the Authentication Header (AH): utilizzato per garantire autenticità e integrità di un pacchetto.
 - the Encapsulating Security Payload (ESP): assicura autenticità, integrità e cifratura di un pacchetto.

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 si approccia IPv6 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 che in IPv6 (lo trattiamo come un nuovo protocollo), senza alterare il funzionamento nel protocollo precedente.

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**, e a differenza del ethernet broadcast 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.

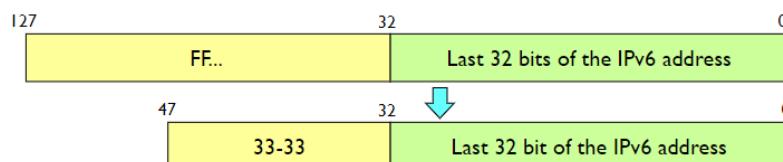


Figura 2.16: Multicast Transmission

Un esempio può essere il seguente: quando viene inviato un pacchetto all'indirizzo IP multicast FFOC ::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.

2.12 Neighbor Discovery and Address Resolution

ICMPv6 adesso sostituisce completamente il protocollo **ARP**. E' basato su multicast e sfrutta il **Solicited-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

Mediante il *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).

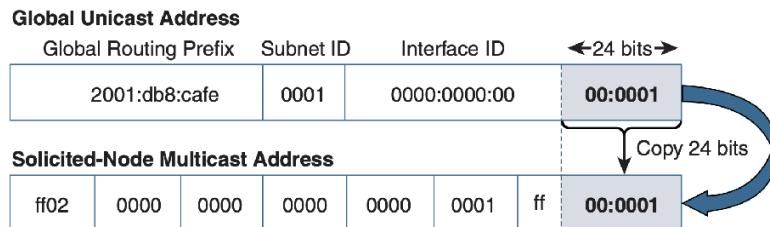


Figura 2.17: Mappatura indirizzo

2.12.2 Risoluzione di un indirizzo

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

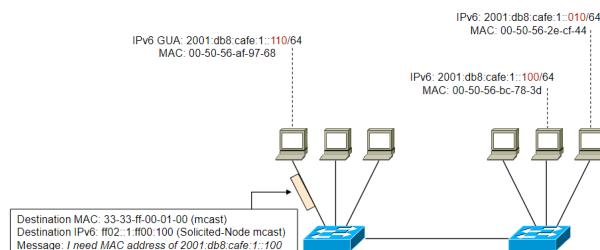
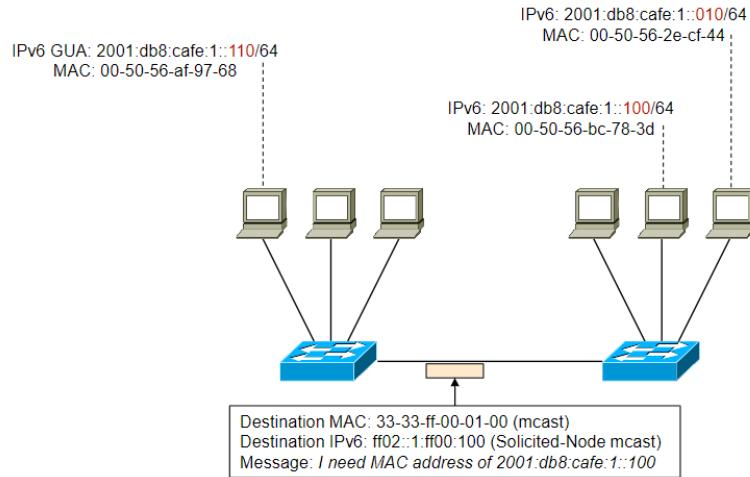
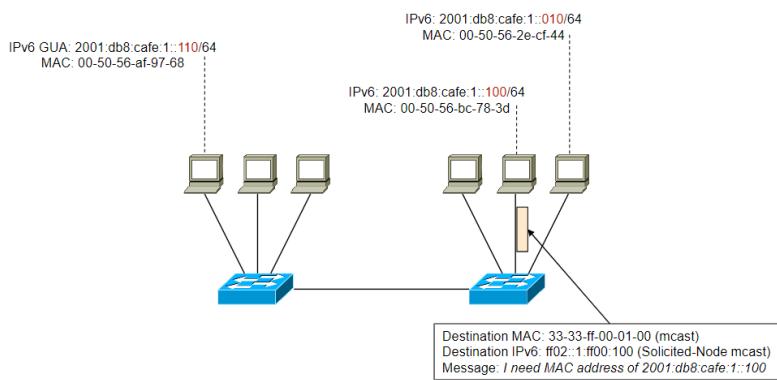


Figura 2.18: Risoluzione dell'indirizzo

**Figura 2.19:** Risoluzione dell'indirizzo**Figura 2.20:** Risoluzione dell'indirizzo

Per 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 indietro all'all'indirizzo unicast del richiedente la risposta. La mappatura tra IPv6 e MAC address viene 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.

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

L'obiettivo 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.

2.14 ICMPv6

Il protocollo **ICMPv6** permette di eseguire operazioni di:

- diagnostica
- neighbor discovery

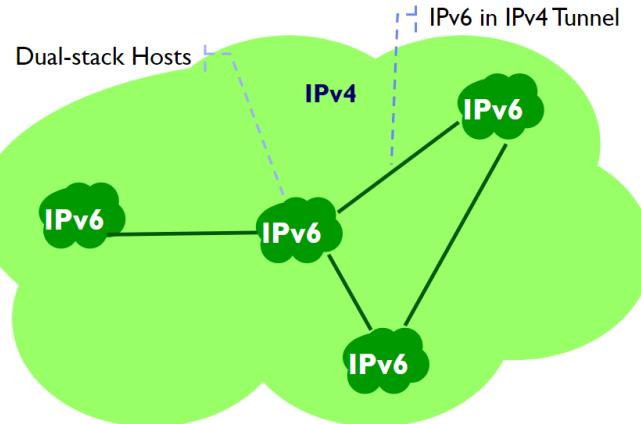


Figura 2.21: Pochi host IPv6

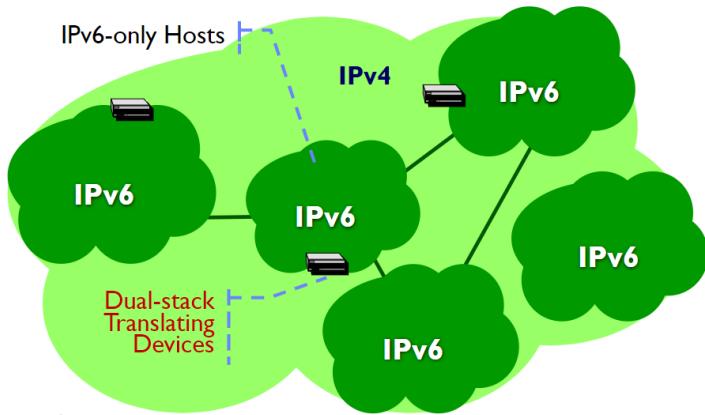


Figura 2.22: Aumento di host IPv6

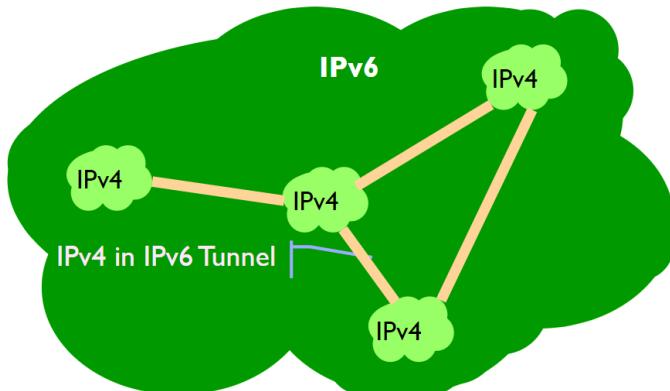


Figura 2.23: Maggioranza IPv6

- 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 permette di identificare il nuovo header di tipo **ICPMv6**, che avrà al più **576 byte**.

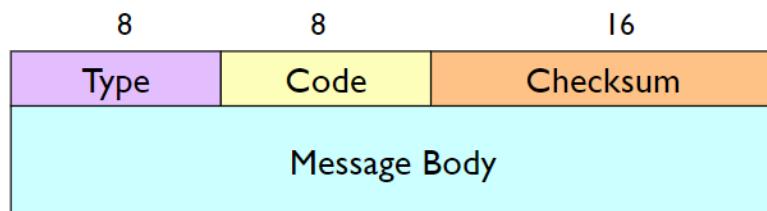


Figura 2.24: Formato del messaggio

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
132	Multicast Listener Done	Informativo
133	Router Solicitation	Informativo
134	Router Advertisement	Informativo
135	Neighbor Solicitation	Informativo
136	Neighbor Advertisement	Informativo

Code	Spiegazione	tipo
137	Redirect	Informativo

2.14.1.1 Messaggi di errore

Analizzando più nel dettaglio i messaggi di errore:

- **Destination unreachable** (*tipo 1*): solitamente generato dal router o firewall, nel campo “code” viene fornita la motivazione (nessuna route, scope errato, indirizzo/porta non raggiungibile).
- **Packet too big** (*tipo 2*): IPv6 non fa più la frammentazione dei pacchetti.
- **Time exceeded** (*tipo 3*): avviene quando il router riceve un pacchetto con **Hop Limit = 0**.
- **Parameter Problem** (*tipo 4*): generato quando un dispositivo trova un problema con un campo del header IPv6 main o con un extension header. Un esempio è un valore non valido del campo Next Header.

2.14.1.2 Messaggi informativi

2.14.1.2.1 Echo La richiesta di echo ha tipo 128 mentre la echo reply ha 129; viene utilizzato, ad esempio, da [ping](#).

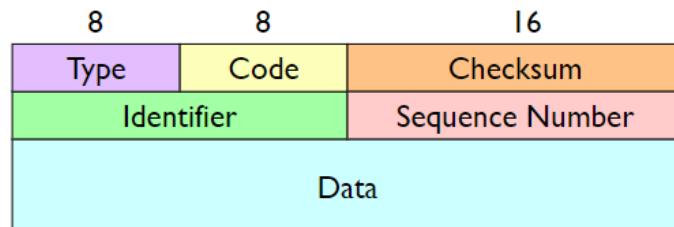


Figura 2.25: Echo request

2.14.1.2.2 Neighbor Solicitation

2.14.1.2.3 Neighbor Advertisement E’ importante evidenziare la presenza di 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.

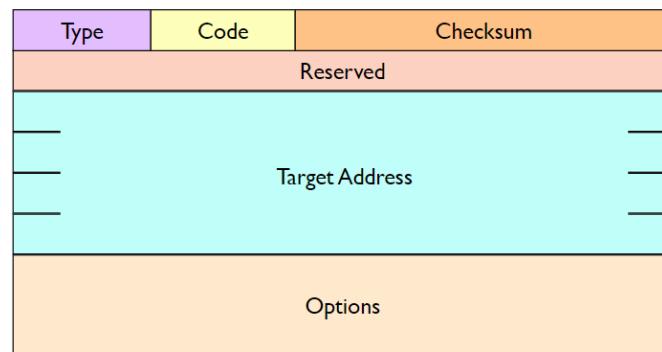


Figura 2.26: Neighbor Solicitation

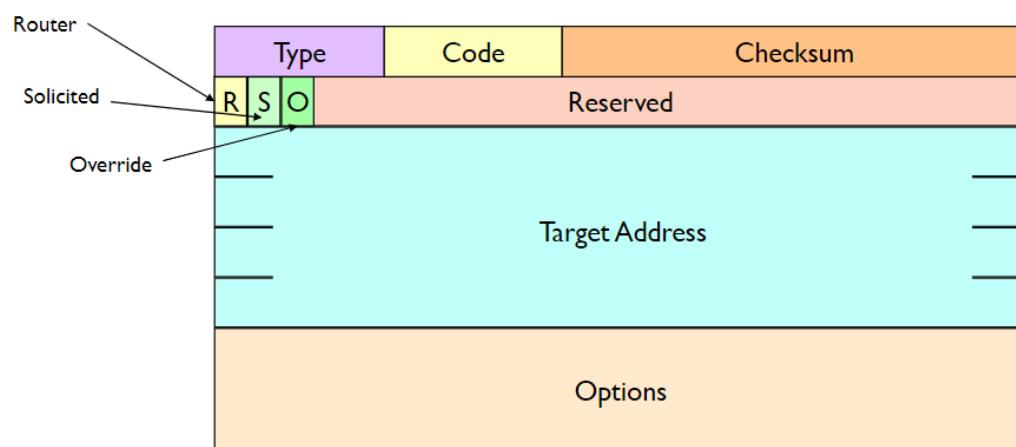


Figura 2.27: Neighbor Advertisement

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.

2.14.2 Multicast Group Management

Quando si ha un collegamento che fa affidamento al data link layer multicasting services, è necessario eseguire il mapping di un indirizzo multicast IPv6 su un indirizzo MAC. Questo deve essere eseguito tra i link e i pacchetti inviati dai router in modo che ICMPv6 sappia i mibri on-link (ovvero gli host interessati a ricevere i pacchetti).

Inoltre consente ai protocolli di multicast routing di sapere quando sono presenti membri off-link.

2.14.3 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 tale interesse è detto **Multicast Listener Report**.

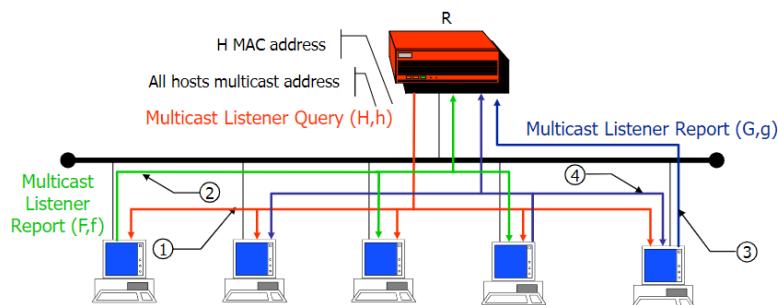


Figura 2.28: Host Membership Discovery

- **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.

Il messaggio di **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).

Type	Code	Checksum
Maximum Response Delay		Unused
Multicast Address		

Figura 2.29: Formato richiesta

2.15 Device Configuration in IPv6

Le informazioni necessarie per eseguire 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 in modo da rendere gli host plug and play.

Le configurazioni possono essere:

- **Manual configuration:** configurazione manuale.
- **Stateful configuration:** tutte le informazioni recuperate mediante DHCPv6.
- **Stateless configuration:** generate automaticamente, con il prefisso dell'indirizzo ottenuto dal router.
- **Hybrid** (Stateless DHCP): ulteriori informazioni oltre l'indirizzo recuperate mediante DHCPv6.

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

- configurazione manuale
- ottenuto tramite DHCPv6
- generato automaticamente da EUI-64 MAC address (privacy aware)

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

EUI-48 yo 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.

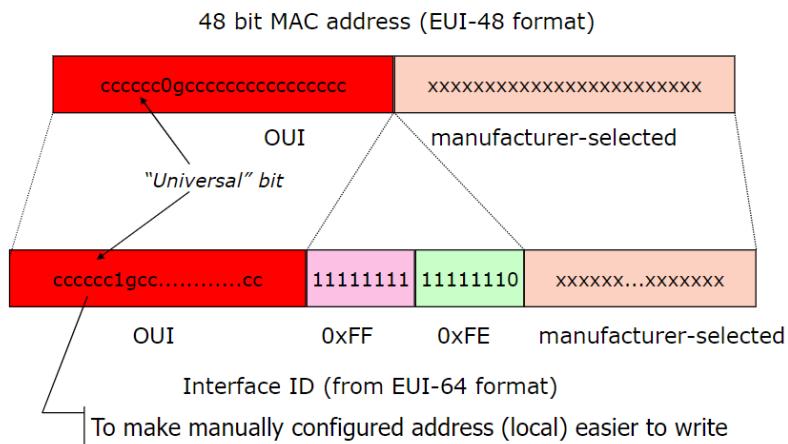


Figura 2.30: EUI-48 to EUI-64 mapping

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

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

Ormai da qualche anno, non viene più utilizzato MD5. Il **Privacy extension Algorithm** garantisce la privacy al livello 3 (network layer), in quanto non è possibile dai 64 bit ricavare l'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 potrebbe essere disponibile per un user o una applicazione.

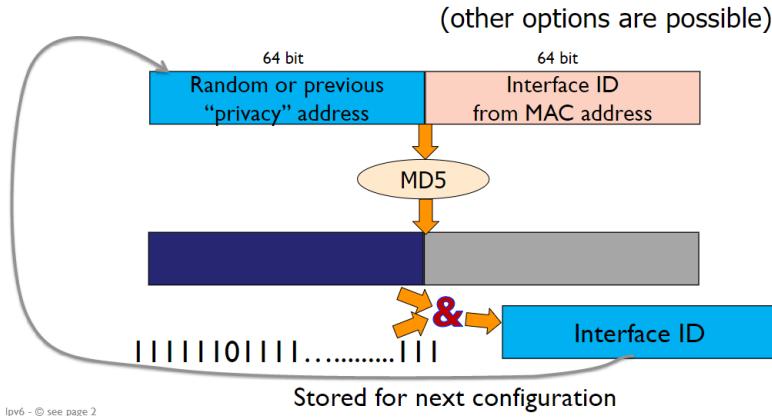


Figura 2.31: Privacy extension Algorithm

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**.

2.15.2.1 Router Prefix Discovery

Attraverso la **Router/Prefix Discovery** è possibile introdurre una “sincronia”: se l’host non ha chiesto un messaggio potrebbe essere direttamente il router a mandare l’informazione tempestivamente senza che venga richiesta un *solicitation*.

2.15.2.2 Router Solicitation

Una router solicitation viene mandata solamente ai router, dunque non `all node` ma bensì `all routers (FF01::2)`.

Type	Code	Checksum
Reserved		
Options		

Figura 2.32: Router Solicitation

2.15.2.3 Router Advertisement

Nel messaggio di advertisement sono rilevanti alcuni parametri:

- **M flag (Managed address 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**: intervallo di tempo per cui ritenerne l'indirizzo valido.
- **Option**: sono presenti delle opzioni, in formato generico ovvero type, length (multipli di 8) e value.

tra le opzioni 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 è utilizzato all'interno di un on-link.
- **A**: il prefisso può essere utilizzato per una configurazione automatica.
- **prefix**: il prefisso.

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 **redirect** viene utilizzato per informare, all'interno di una stessa sottorete, un host **A** che per raggiungere un determinato host **B** 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 **Duplicate Address Detection** (DAD) è un meccanismo che permette di verificare che un indirizzo sia unico all'interno della rete.

Il funzionamento è molto semplice: l'host manda un messaggio ICMPv6 a tutti gli host con destinazione **all nodes** e con il payload contenente 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.

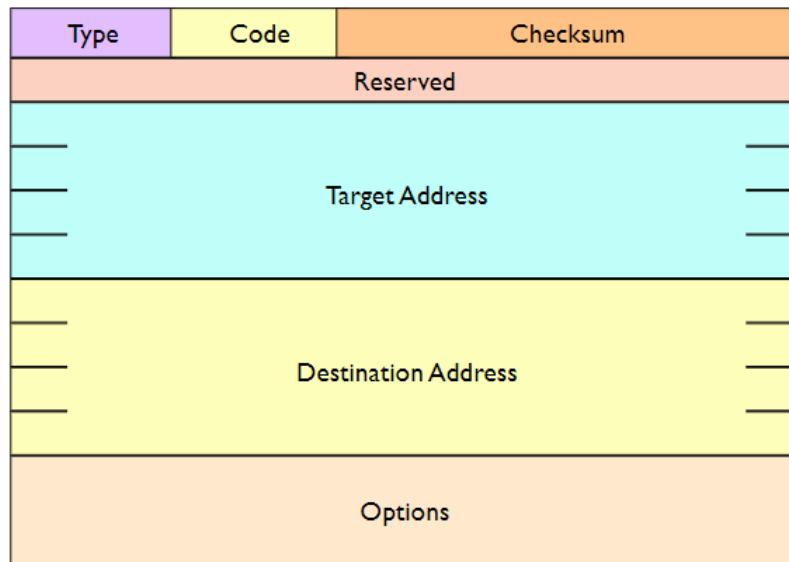


Figura 2.33: Message Format

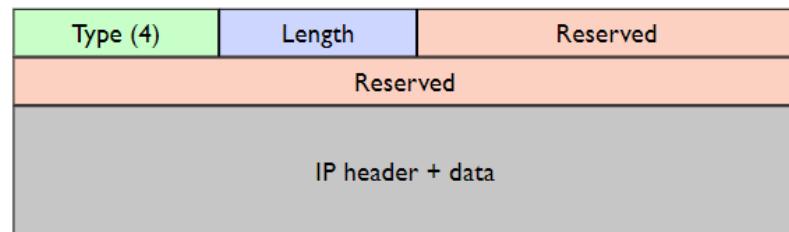


Figura 2.34: header Option

2.15.5 Fasi di configurazione di una configurazione Stateless

La configurazione stateless di un nuovo dispositivo avviene nei seguenti passaggi:

- generazione di un indirizzo link local.
- verifica dell'unicità dell'indirizzo (DAD).
- il dispositivo si pone in ascolto di un messaggio di *router advertisement* o manda una *solicitation* per scoprire le informazioni sull'indirizzo privato.

Una volta scoperta la parte alta:

- si verifica se anche all'interno della sotto rete che l'indirizzo sia unico (di nuovo).
- iscrizione al corrispondente IPv6 Solicited Node Multicast Address, configurando la ricezione del multicast MAC corrispondente e inviando un ICP Multicast Listener Report.
- La comunicazione on-link è abilitata.

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. Questi rimangono in ascolto per il Router Advertisement e quando arriva un messaggio con un nuovo prefisso, cambiano indirizzo. Gli host possono essere riconfigurati in qualsiasi momento. Si identificano così indirizzi "preferred" e "deprecated". In questo modo è possibile cambiare ISP senza dover cambiare tutti gli indirizzi.

2.16 Scoped Addresses

Un dispositivo può avere più interfacce con il medesimo 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.

Attenzione: Questo byte di scope non viene più utilizzato perchè è di 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 le routing tables.
- **Proactive routing:** processo di creazione di routing tables.

La creazione di tali tabelle può essere di tipo manuale, dunque static routing, oppure mediante la distribuzione 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 troubleshooting, 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 2.35: Protocolli di routing

2.18 La transizione da IPv4 a IPv6

La transizione da 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.

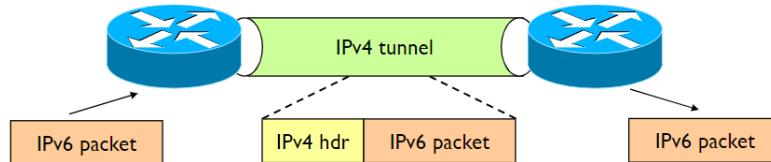


Figura 2.36: Esempio di Tunneling

L'approccio iniziale è stato quello di tipo dual stack descritto precedentemente, con lo scopo di supportare le funzionalità di entrambi i protocolli, ma con la limitazione di non ridurre l'utilizzo di IPv4 e di dare la responsabilità alle applicazioni di utilizzare IPv6 o IPv4.

Alcuni protocolli che implementano soluzioni di tipo tunneling sono:

- **GRE** (Generic Routing Encapsulation)
- **IPv6 in IPV4** (protocollo di tipo 41)
- setup manuale ed automatico

2.18.1 Host centered solutions

Una soluzione potrebbe essere di utilizzare un approccio di tipo 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.

2.18.1.1 6over4

Il protocollo 6over4 utilizza una rete IPv4 per emulare una virtual LAN. Utilizza il broadcast multiple access data link e l'IP multicasting.

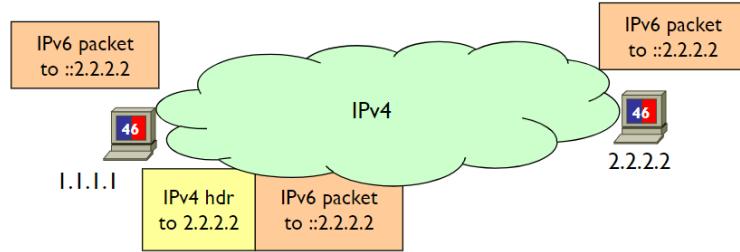


Figura 2.37: End-to-End-Tunneling

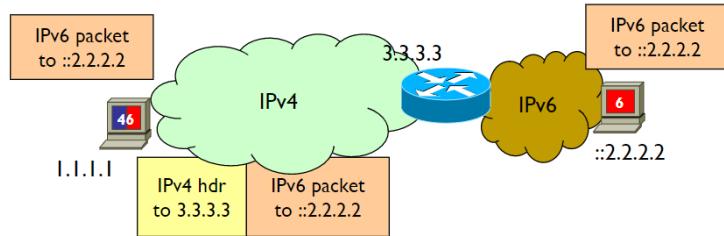


Figura 2.38: Dual stack router

Il neighbor e router discovery è abilitato in modo da consentire l'individuazione di nodi vicini e router.

L'indirizzo IPv4 è utilizzato per la generazione automatica di un interface ID IPv6 dell'indirizzo link local.

Nota: Non è molto utilizzato a causa della poca diffusione del supporto IPv4 multicast.

2.18.1.2 ISATAP: Intra-site Automatic Tunnel Addressing Protocol

Invece di usare il multicast, utilizza una soluzione con un prefisso di rete **0000:5EFE**. La rete IPv4 viene utilizzata come una Non-Broadcast Multiple Access (NBMA) data link, in questo modo non è necessario il supporto per IP multicast.

L'interface ID viene derivata dall'indirizzo IPv4.

2.18.1.3 (Lack of) Neighbor Discovery

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

Non è necessario eseguire data-link address discovery in quanto l'indirizzo IPv4 è incluso nell'indirizzo IPv6, in particolare negli ultimi 4 byte.

Si rende necessario fornire una PRL (Potential Router List) in quanto la router discovery non è possibile. Può essere configurata manualmente oppure acquisita dal DNS.

2.18.1.4 Configurazione automatica

La configurazione automatica è diventata lo standard nel tempo. Vengono utilizzati indirizzi IPv4, indirizzi DNS e il nome del dominio viene ottenuto tramite DHCPv4.

L'indirizzo IPv6 link local viene generato automaticamente, l'interface ID dall'indirizzo IPv4.

Per ottenere il PRL si utilizza una query DNS, se non fornita da DHCPv4.

Periodicamente viene eseguita una router discovery verso tutti i router su link prefixed per l'autoconfigurazione.

2.18.2 Network center solution

Si configurano intere reti IPv6 all'interno di una struttura ancora IPv4, dovendo però rinunciare a parte delle funzionalità IPv6, inoltre il range di indirizzi continua a essere ridotto.

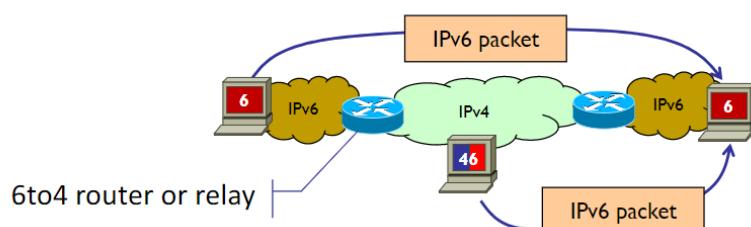


Figura 2.39: Host centered

2.18.2.1 6to4

Attraverso il protocollo **6to4** Gli indirizzi dei relay sono embedded in un prefisso IPv6. Iniziano con 2002 e sono indirizzi pubblici (iniziano con 2).

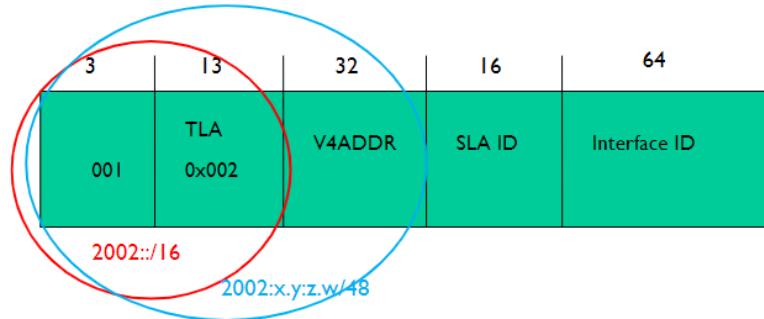


Figura 2.40: Schema indirizzo

Tale protocollo non è pensato per le comunicazioni da host IPv4 a host IPv6.

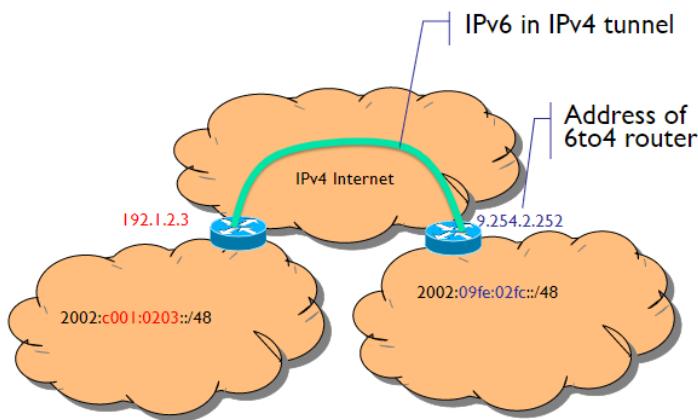


Figura 2.41: Scenario base

Un relay 6to4 deve essere necessariamente il default gateway per i router 6to4.

2.18.2.2 Tunnel broker

In questa modalità le comunicazioni avvengono attraverso un tunnel broker server che si occupa di individuare i tunnel server e fa da mediatore tra le configurazioni dei tunnel.

Vengono utilizzati tunnel IPv6 in IPv4 (a.k.a. proto-41).

Per eseguire la configurazione dei tunnel viene utilizzato il Tunnel Setup Protocol (TSP) o il Tunnel Information Control (TIC).

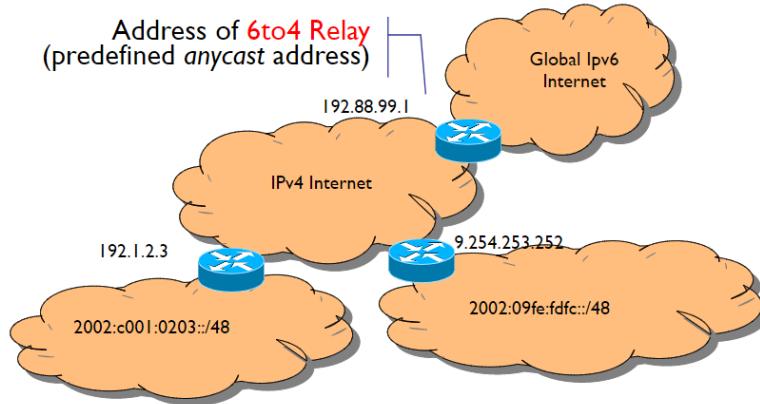


Figura 2.42: Scenario misto

Questo tipo di soluzione è centralizzata.

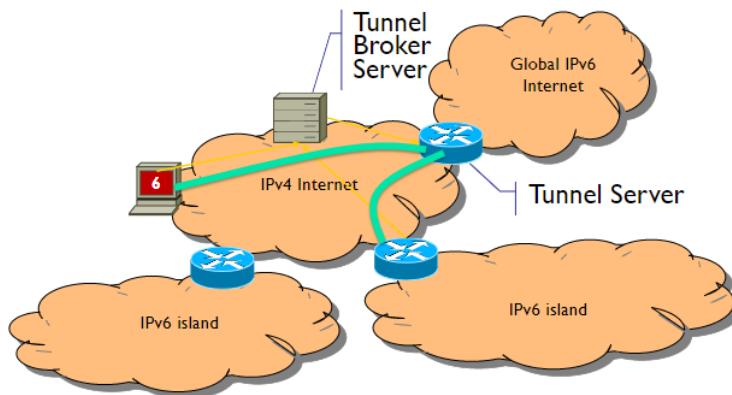


Figura 2.43: Architettura tunnel broker

2.19 Scalable, Carrier-grade Solutions

Devono essere presi in considerazione anche soluzioni per grandi provider. Purtroppo ancora è necessario supporto per i server e i client IPv4 in modo che possano comunicare con host IPv6 e host ipv4. Le soluzioni più utilizzate sono:

- **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, ovvero il NAT, eseguendo un mapping tra ipv4 e ipv4. Quello che viene fatto è associare una porta a un indirizzo privato.

Prende il nome di **LSN** il **Large Scale NAT**, utile in quanto riesce a gestire una quantità di richieste molto elevate.

E' possibile avere più livelli di NAT ponendoli in cascata, pratica piuttosto comune.

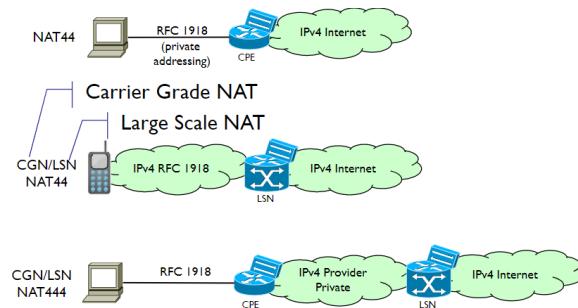


Figura 2.44: Nat è ampiamente utilizzato

E' necessario tenere a mente che nelle soluzioni proposte, anche se è previsto l'utilizzo del NAT, è comunque presente l'utilizzo di tunnel.

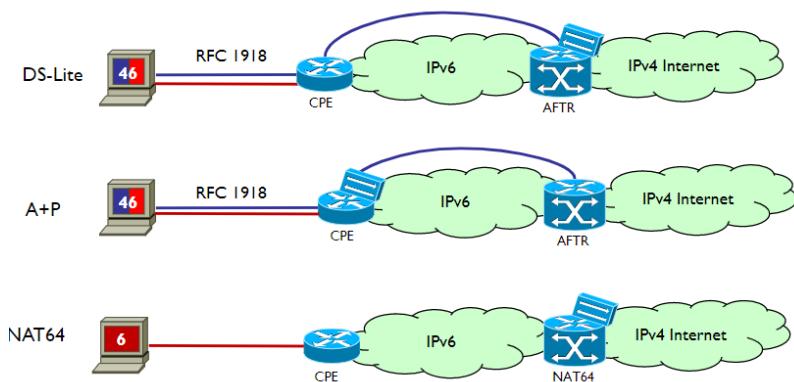


Figura 2.45: Stessa architettura con IPv6

Attenzione: da notare dove le funzionalità di NAT sono presenti.

2.19.1 AFTR: Address Family Transition Router

L'utilizzo del **Address Family Transition Router** (AFTR) Abilita gli host ipv4 a comunicare con altri host IPv4 attraverso una rete (un esempio p la connessione residenziale fornita dagli attuali provider). Ha dunque come conseguenza il poter connettere strutture IPv6 con una struttura nel mezzo ipv4. Ha due tipi di funzionalità:

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

Nota: Viene utilizzato da DS-Lite e A+P.

2.19.2 DS-Lite

La soluzione **Dual-Stack Lite** è caratterizzata da internet service provider che utilizzano una backbone (infrastruttura di rete) IPv6. Questo consente di avere solo parti ipv4 o ipv6 con altre sottoreti ipv4 o ipv6. Questa soluzione, rispetto a quelle già viste, sono molto articolate e consentono di coprire tutte le casistiche.

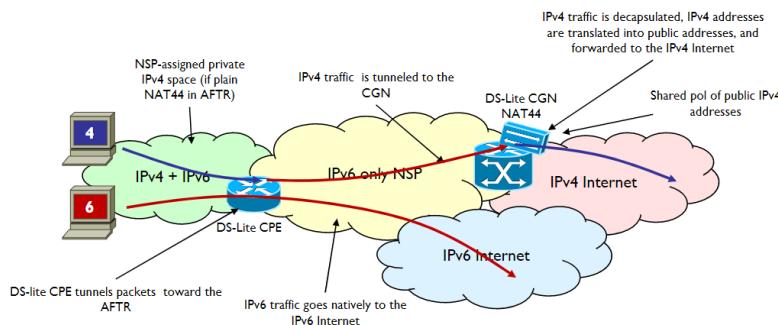


Figura 2.46: DS-Lite

Permette di ridurre il numero di indirizzi IPV4 richiesti rispetto a un approccio dual stack (che aveva bisogno di un indirizzo pubblico per ogni host).

Il NAT esteso consente l'indirizzamento assegnato dal cliente (ovvero sovrapposto).

Le limitazioni sono però le seguenti:

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

2.19.3 A+P (Address plus port)

Il vantaggio di **A+P** è che il NAT è sotto il controllo dei customer. Una ulteriore caratteristica è che il range di TCP/UDP è assegnato a ciascun customer (solo le porte sono utilizzate dal nat in uscita).

Le features sono:

- nessun problema con la sovrapposizione degli indirizzi privati nello spazio di indirizzi dei customer.
- Le porte possono essere assegnate automaticamente al CPE utilizzando il Port Control Protocol (PCP), mentre il CPE può negoziare più porte in qualsiasi momento.
- AFTR è solo un tunnel terminator IPv4 in IPv6 (NAT44 non è più necessario in AFTR).

Nota: Il concetto alla base è di spostare la complessità sulle foglie.

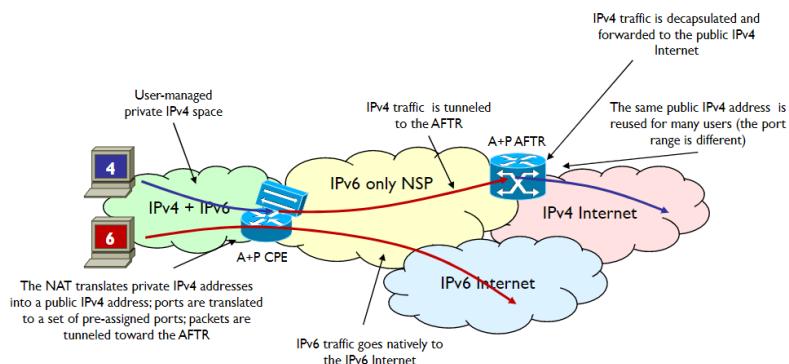


Figura 2.47: A+P

2.19.4 Mapping Address and Port (MAP)

Il **Mapping Address and Port** (MAP) utilizza un approccio di tipo **stateless**. Questo sfrutta i vantaggi del DHCP e del DNS anche all'interno del sistema, non associando 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 da non avere limitazioni.

L'indirizzo e la porta del client IPv4 sono mappati in un unico indirizzo IPv6 (prefix routed dal CPE).

L'indirizzo del server pubblico IPv4 è anche questo mappato in un unico indirizzo IPv6 (prefix routed dal Border Relay).

Esistono due tipi di MAP:

- **MAP-E:** MAP with Encapsulation, ovvero i pacchetti IPv4 vengono tunnelizzati.

- **MAP-T:** MAP with Translation, i pacchetti IPv4 sono tradotti in pacchetti IPv6 e poi nuovamente in IPv4.

Quando però avviene la sostituzione di un header IPv6 con un header IPv4 è necessario fare attenzione a non perdere informazioni.

2.19.5 Port Set

A ogni CPE viene assegnato un unico **PSID** (Port set Identifier) che identifica un set di porte e un indirizzo pubblico IPv4.

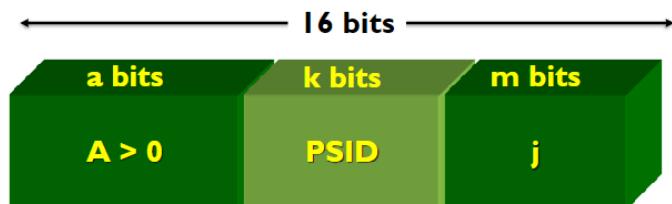


Figura 2.48: Port set

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

L'embedded Address (EA) contiene i bit di PSID e parzialmente l'indirizzo IPv4 (che identifica univocamente il CPE).

2.19.6 Mapping Rules

Le regole per il mapping sono:

- regola IPv6 prefix
- regola IPv4 prefix
- EA bits length

Inoltre, un offset PSID (valore di a) viene settato per l'intero dominio di mappatura.

2.19.7 Border Relay

L'indirizzo del border relay deve essere conosciuto da tutti i CPE, anche se più BR possono avere lo stesso indirizzo (anycasting).

Mentre nel MAP-E il BR termina il tunnel, nel MAP-T il BR è responsabile della traduzione degli indirizzi IPv4 verso l'esterno (sostituisco l'header IPv4 con un header IPv6). Il BR prefix viene advertised sul backbone (e potrebbe essere advertised da più BR).

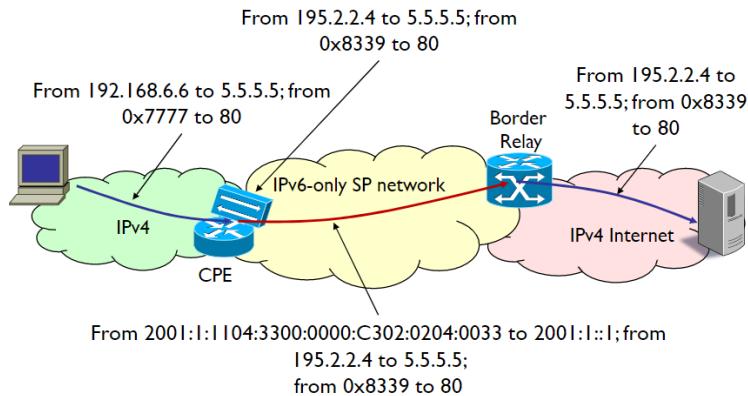


Figura 2.49: Vita di un pacchetto con MAP-E

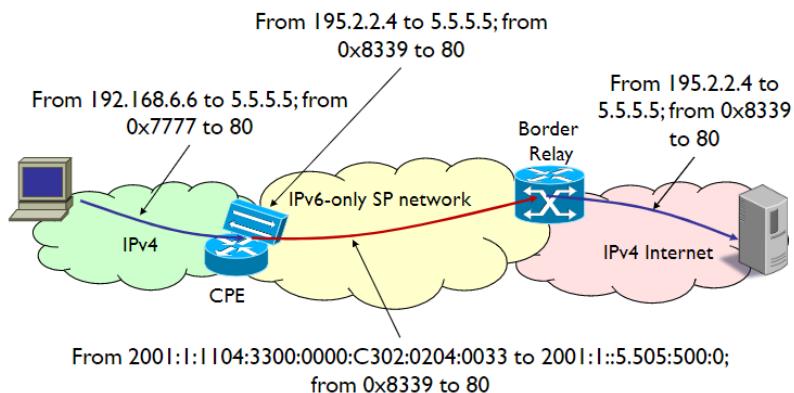


Figura 2.50: Vita di un pacchetto con MAP-T

2.20 NAT64 + DNS64

Il NAT64 è un meccanismo di transizione a IPv6 che facilita la comunicazione tra IPv4 ed IPv6 utilizzando il *Network Address Translation* (NAT), che traduce gli indirizzi e i pacchetti IPv6 in IPv4, prendendo un indirizzo/porta Ipv5 liberi dal pool e realizzando un NAT session entry.

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

Un prefisso IPv5 è dedicato per mappare indirizzi IPv4, comprensivi di well-known che di network specific. Il DNS64 mappa un A record in AAAA utilizzando un prefix NAT64, entrambi vengono poi forniti al client. Il router NAT64 fa il advertise del prefix in una rete IPv5 per attirare il traffico verso gli host IPv4.

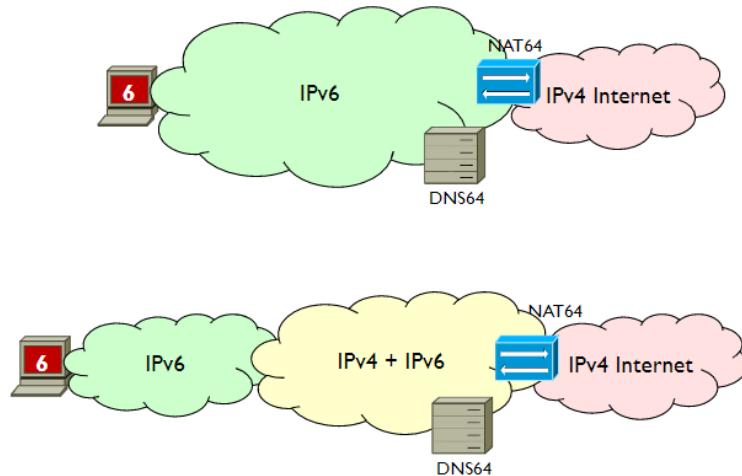


Figura 2.51: Deployment scenarios

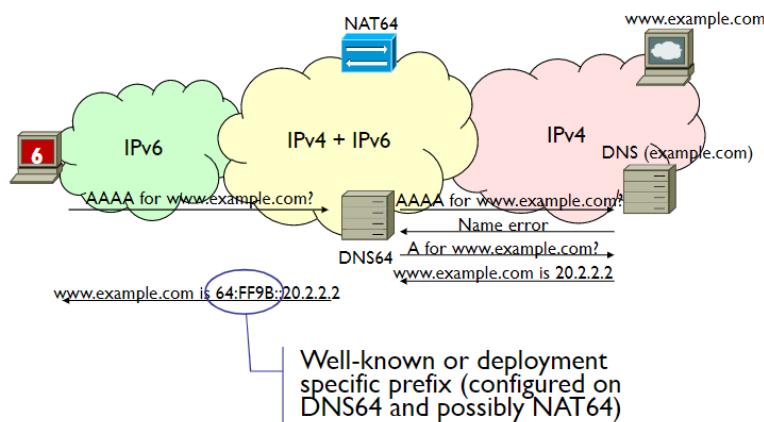


Figura 2.52: Name resolution

Le limitazioni dovute al NAT64 + DNS64 sono:

- Coinvolgimento del DNS (hostname)
- No DNSSEC

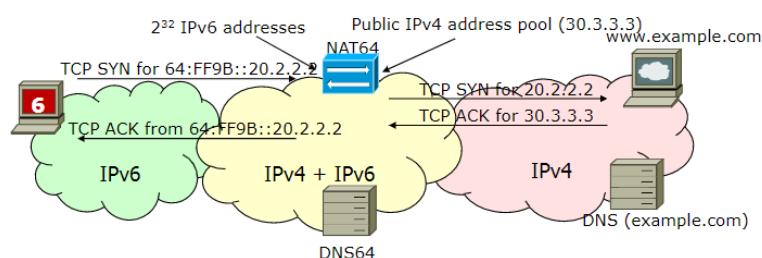


Figura 2.53: Packet forwarding

3 Reti Wireless e cellulari

3.1 Introduzione

Le reti **wireless** permettono la comunicazione tra dispositivi senza la necessità di un cavo fisico. Queste sono molto comuni oggigiorno, 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 aspetto molto importante che ne deriva è la **mobilità**, anche se una parte rilevante di ogni rete wireless è in realtà la sua componente wired (oltre al wireless link).

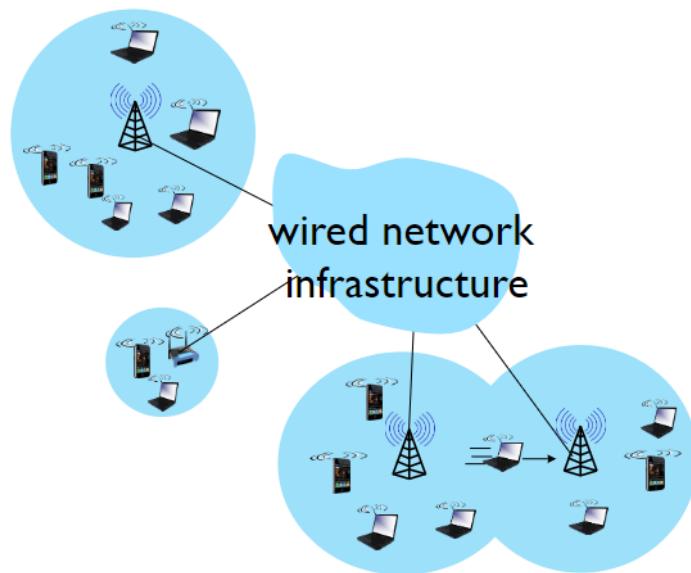


Figura 3.1: Elementi di una rete wireless

Nonostante i grandi vantaggi, il link wireless comportano alcuni svantaggi rispetto a un link cablato:

- **Degrado** maggiore del segnale.
- **Interferenza** tra i dispositivi.
- **Multipath propagation** (fading): effetto dovuto ai rimbalzi del segnale sugli ostacoli.
- le **comunicazioni** tra punti diventa più **complicata**.

Un'altra importante caratteristica è il **Signal to Noise Ratio** (SNR), che esprime la relazione tra il segnale ricevuto e il rumore. Tale valore è molto importante per la qualità del segnale, più è alto più è semplice estrarre il segnale dal rumore. Dato un physical layer, aumentarne l'alimentazione ne comporta un aumento di SNR e una riduzione del *Bit Error Ratio* (BER), mentre dato un SNR è necessario scegliere un livello fisico che rispetta i requisiti di BER in modo da ottenere il massimo throughput. Il valore di SNR può cambiare a causa della mobilità, adattandosi dinamicamente al livello fisico.

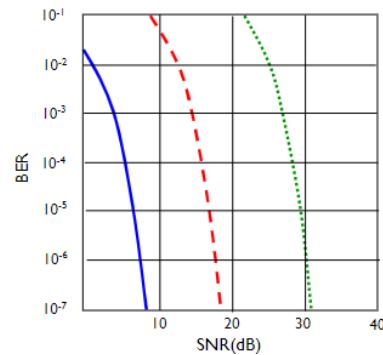


Figura 3.2: SNR e BER

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 inherente 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.

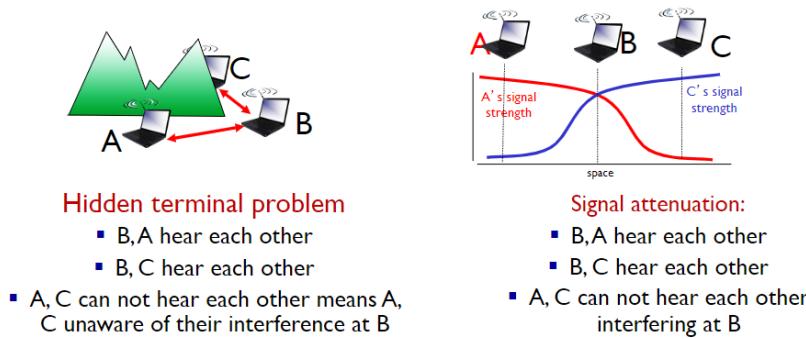


Figura 3.3: Problema del nodo nascosto

3.2 Wireless LAN

Nel corso degli anni lo standard 802.11 si è evoluto dando origine a vari standard, i quali utilizzano il protocollo *Carrier Sense Multiple Access, CSMA/CA*.

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gbps	70m	5 Ghz
802.11ax (WiFi 6)	2021	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

Figura 3.4: Protocolli Wireless 802.11x

Un **BSS** (*Basic Service Set*) contiene:

- hosts wireless
- AP, access point (base station)
- ad hoc mode: solamente host

Ogni rete wifi lavora su un canale differente ed è in grado di gestire fino a 16 frequenze (di cui utilizza solo una alla volta) per la trasmissione dei dati, con la possibilità che ci sia interferenza se il canale viene scelto male. La configurazione può essere automatica o manuale.

Ogni host che vuole connettersi esegue prima una scansione delle reti e rimane poi in attesa di un **beacon frame**: un frame speciale inviato dagli access point per effettuare la connessione. Il dispositivo si conterà 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 dal access point e ricevuto dal host.
- **Active scanning**: l'host richiede il beacon frame all'access point, in 4 fasi che si dividono in:
 - **probe request** dal host.
 - **probe response** dagli APs.
 - **association request** dal host verso l'access point scelto.
 - **association response** dal APs in questione.

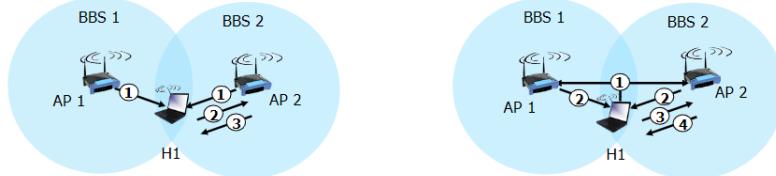


Figura 3.5: A sinistra passive scanning e a destra active scanning

3.2.1 CSMA/CA

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

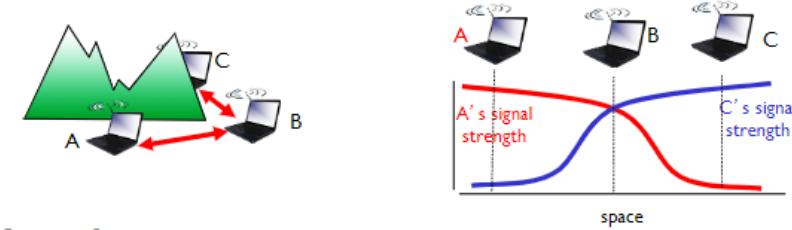


Figura 3.6: Accessi multipli

Mentre in ethernet viene utilizzato CSMA/CD (collision detection), in wireless viene utilizzato **CSMA/CA** (collision avoidance) con lo scopo di eseguire *sense before transmitting*, in modo di evitare le collisioni con la trasmissione già in corso di altri nodi.

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 aumentando il random backoff interval.

Il funzionamento è il seguente:

- Il dispositivo che invia:
 1. Se il canale è in idle per **DIFS** tempo, allora il dispositivo inizia a trasmettere (no CD).
 2. Se il canale è 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 aumentando il random backoff interval.

- Il dispositivo che riceve:

1. Se il frame è ricevuto correttamente, viene inviato un ACK frame dopo **SIFS** tempo (necessario per evitare il problema del terminale nascosto).

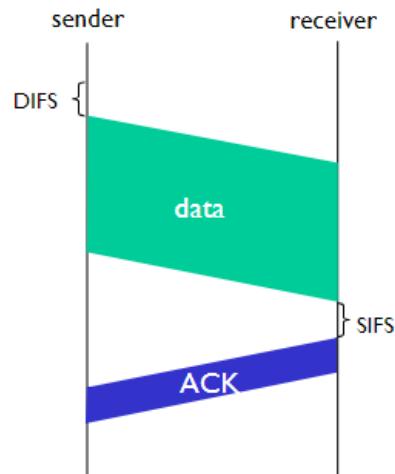


Figura 3.7: Schema di funzionamento

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. Il pacchetto **RTS** (ready to send) viene inviato dal dispositivo che vuole trasmettere, mentre **CTS** (clear to send) viene inviato dal dispositivo che ha ricevuto il pacchetto RTS verso tutti i dispositivi in ascolto in modo da far partire la trasmissione da chi deve trasmettere e porre in attesa i rimanenti.

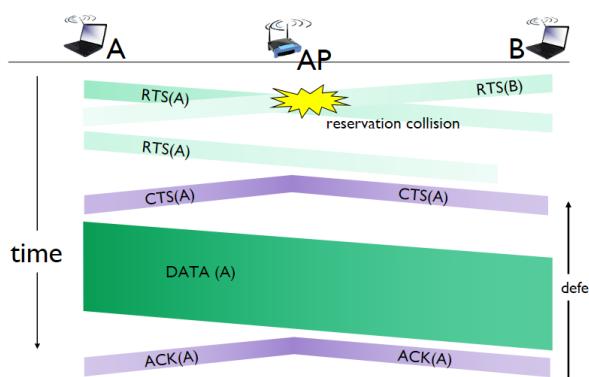


Figura 3.8: Schema temporale RTS-CTS

3.2.1.1 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 version
- tipo (RTS, CTS, ACK, data)
- sottotipo
- bit per il power management

3.2.1.2 Mobilità nella stessa sottorete

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

Spesso gli switch sono self learning, ovvero quando vedono un frame transitare per H1 *ricordano* a quale switch port è stato inviato e la memorizzano.

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 (ha al suo interno la lista dei dispositivi con gli AP-to-mobile frames in attesa di essere inviati).

3.3 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 mediante reti isotopiche e antenne direzionali da 120 gradi. La forma non è esattamente esagonale e l'emissione non è omni direzionale a causa della presenza di ostacoli (montagne, edifici), altezza, il guadagno dell'antenna, la morfologia del territorio, la potenza dell'antenna e infine le condizioni di propagazione (atmosferici ecc...).

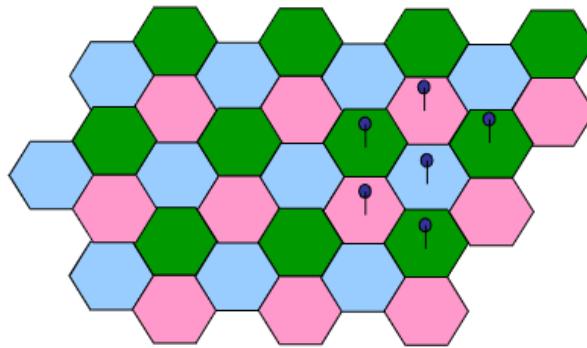


Figura 3.9: Copertura cellulare

Le celle si dividono in **macrocelle** e **microcelle** in base alle loro dimensioni e di conseguenza della copertura.

Come nelle reti wireless, è nuovamente presente il problema di accesso multiplo condiviso sul canale, che viene risolto attraverso varie tecniche:

- **FDMA**: viene scelto una frequenza in cui trasmettere.
- **TDMA**: viene scelto uno slot temporale in cui trasmettere.
- **CDMA**: viene assegnato a ogni stazione un codice *ortogonale* agli altri, ovvero un gruppo di segnali da cui è possibile recuperare ogni singolo segnale.
- **SDMA**: ogni frequenza viene riutilizzata, a condizione che i luoghi siano fisicamente molto distanti tra loro.

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

Definizione: Si definisce **handover** la gestione della mobilità di un dispositivo su una rete cellulare e il conseguente funzionamento di sgancio e riaggancio tra le celle.

3.3.1 Cluster

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

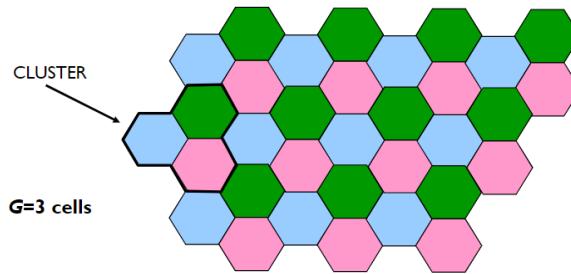


Figura 3.10: 3-Cell Cluster

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

Con la variazione della dimensione delle celle R cambia la capacità, ovvero il numero di utenti che questa è in grado di soddisfare. Il numero di celle G impatta invece sul costo, in quanto un numero maggiore di celle ha dei costi maggiori. Aumentando il cluster aumenta la qualità, aumentando anche G aumenta la qualità ma diminuisce la capacità.

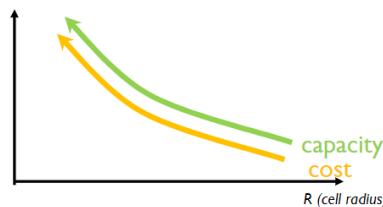


Figura 3.11: Fissando **G** e variando **R** (cell size)

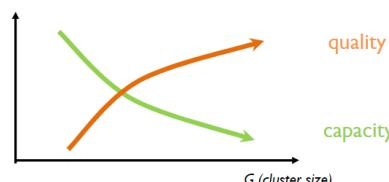


Figura 3.12: Fissando **R** e variando **G** (cluster size)

Non esiste una legge assoluta per definire i due parametri, ma è possibile sfruttare alcune tecniche per diminuire le interferenze ed aumentare la capacità:

- **splitting**: non utilizzare celle delle stesse dimensioni, ma basarsi sulle necessità specifiche.
- **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).

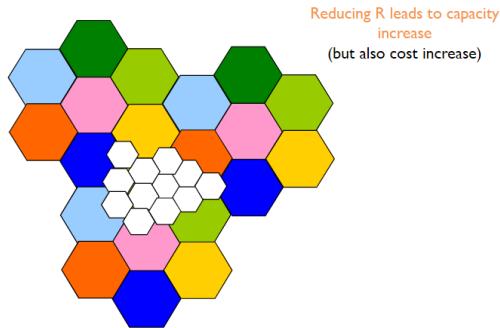


Figura 3.13: Splitting

Inoltre è possibile utilizzare antenne direzionali per avere celle con dimensioni e forme ad-hoc, oppure adoperare una copertura multi livello (umbrella coverage) o infine utilizzare microcelle che seguano l'utente dove si muove.

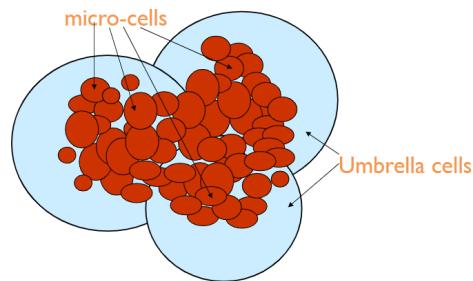


Figura 3.14: Shaping

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

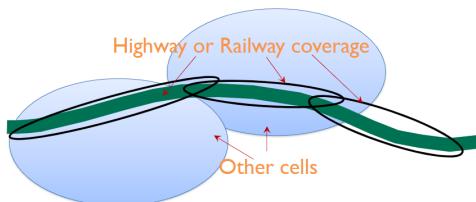


Figura 3.15: Shaping su strade

3.3.2 Power Control

Il **Power Control** mira al gestire al meglio le capacità delle batterie a disposizione: l'obbiettivo è di ridurre l'utilizzo di potenza in base alle necessità. Per capire la potenza necessaria si utilizzano strategie di due tipi:

- **a catena aperta** (*open loop*): sistema senza reazione
- **a catena chiusa** (*closed loop*): sistema con reazione (*feedback*)

In particolare in uplink (da terminale a ripetitore) si utilizzano le seguenti strategie:

- closed loop power control
- open loop power control
- outer loop power control

Mentre in downlink (da ripetitore a terminale) si utilizzano:

- Downlink power control

3.3.2.1 Open loop

Nel **open loop** il sistema, non avendo a disposizione un feedback, analizza e misura la qualità del segnale ricevuto per valutare se aumentare o diminuire la potenza di trasmissione. Questo adattamento non è preciso e non è detto che ciò che succede su una frequenza sia uguale a un'altra. Non è molto accurato in quanto solitamente uplink e downlink trasmettono su canali differenti.

Soltanamente si divide in due fasi:

- l'utente misura la qualità del segnale che riceve dalla base station.
- l'utente utilizza poi un algoritmo per impostare la potenza di trasmissione in modo che la SINR (*Signal-to-interference-plus-noise ratio*) sia sopra una certa soglia.

In questa modalità il terminale “*si regola autonomamente*” sulla potenza di trasmissione.

3.3.3 Allocazione della frequenza

L'allocazione delle frequenze possono avvenire nei seguenti modi:

- **Fixed Channel Allocation** (FCA): Basato sul concetto di cluster, le frequenze sono assegnate staticamente e vengono modificate raramente per aumentare performance e adattare piccole variazioni sull'utilizzo del traffico dell'utente.

- **Dynamic Channel Allocation** (DCA): Le risorse sono assegnate da un controller centrale, quando necessarie. Il frequency plan varia nel tempo in modo da adattarsi allo stato del sistema.
- **Hybrid Channel allocation Scheme** (HCS): Una porzione è allocata staticamente (FCA) mentre una dinamicamente (DCA)

3.3.4 Architettura di rete

Le reti sono costituite da mobile terminal che si connettono a delle 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 modalità cablata (*wired*). Il database è molto importante in quanto è dove vengono memorizzate le informazioni degli utenti.

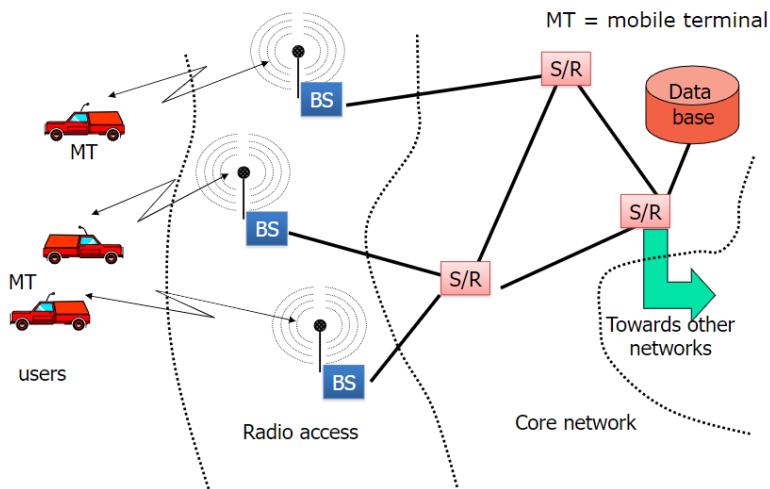


Figura 3.16: Architettura di rete

Il processo di **registrazione** permette a un terminale mobile di connettersi alla rete attraverso una registrazione che lo identifica e autentica. La procedura avviene periodicamente ogni volta che si deve accedere al servizio, oppure quando il terminale si accende e deve associarsi alla rete.

Un'altra procedura è quella del **Mobility Management**, utilizzata per gestire la mobilità e che a sua volta utilizza le seguenti procedure:

- Roaming
- Location updating
- Paging
- Handover

3.3.4.1 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 salvare tali informazioni, la rete viene divisa in location areas (LAs), gruppi di celle adiacenti. Ogni LA ha un identificativo univoco.

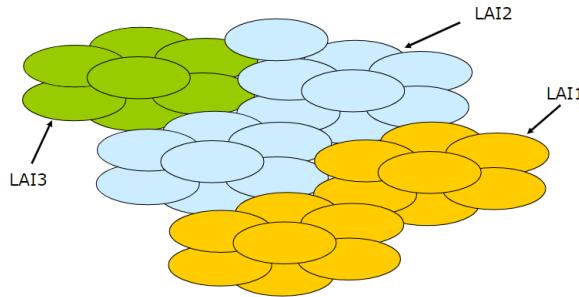


Figura 3.17: Roaming

3.3.4.2 Location updating

Il location updating è 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.

3.3.4.3 Paging

Il **Paging** è la procedura attraverso la quale il sistema notifica un terminale mobile di una chiamata o data delivery.

Il sistema manda la richiesta in broadcast a tutti i terminali della location area, e il terminale che riceve la richiesta risponde con un messaggio di conferma.

3.3.4.4 Handover

La procedura di **Handover** abilita il trasferimento di una connessione attiva da una cella verso un'altra, mentre il terminale mobile si sposta nella rete. Questa procedura è molto complessa e richiede una rete ben architettata, con protocolli e segnali adeguati.

Si classifica nei seguenti tipi:

- **Intra vs. Inter Cell:** Indica se l'handover avviene tra frequenze all'interno della stessa cella o di celle diverse.
- **Soft vs. Hard:** Indica se durante l'handover sono attivi entrambi i canali radio (soft) o solo uno alla volta è attivo (hard).
- **MT vs. BS initiated:** Indica se il primo messaggio di controllo per l'avvio di un handover è inviato dal terminale mobile (MT initiated) o dalla BS (BS initiated), ovvero quale entità esegue le misure per capire dove e quando deve essere eseguito un handover.
- **Backward vs. Forward:** Indica se la segnalazione di handover avviene tramite la BS di origine (backward) o la BS di destinazione (forwarding).

3.4 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 trasportava traffico esclusivamente voce. La qualità del segnale era bassa e l'efficienza nel riutilizzo della frequenza era scarsa.

La seconda generazione ha comportato il passaggio al digitale, con il vantaggio in termini di servizi (sms), crittografia 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, vede l'introduzione del servizio dati con packet switched, 170kb/s in GPRS e 384kb/s in EDGE. Si ha il passaggio 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.

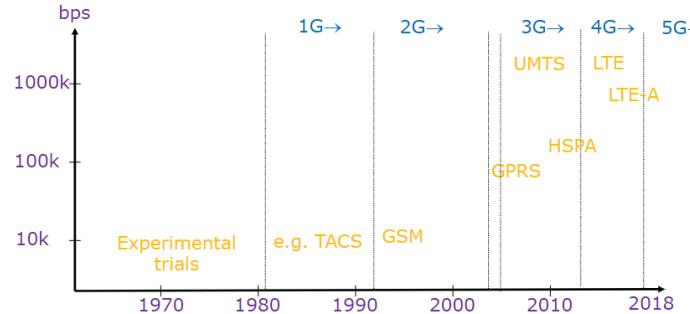


Figura 3.18: Evoluzione della rete cellulare

3.4.1 GSM - Seconda generazione

Il GSM è una 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.

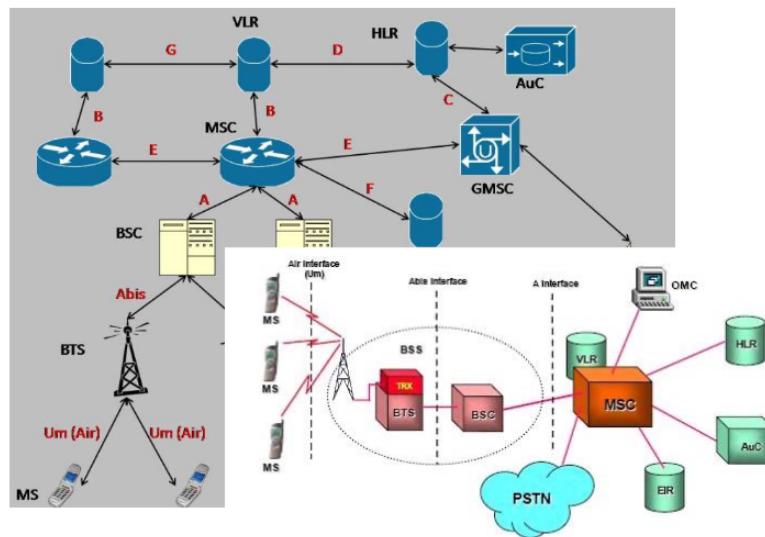


Figura 3.19: Architettura GSM

I **Mobile Station** (MS), ovvero i dispositivi, sono quelli in grado di connettersi alla rete GSM (come telefoni, antenne dei veicoli) ed hanno differenti potenze di trasmissione all'antenna:

- fino a 2W per i telefoni
- fino a 8W per dispositivi mobili

- fino a 20W per le antenne dei veicoli

La MS è però unicamente hardware, per connettersi alla rete è necessaria una SIM, ovvero una smart card con un processore e una memoria in grado di memorizzare, crittografare, le informazioni dell'utente come il numero di telefono, i servizi accessibili, parametri di sicurezza ecc. L'identificativo univoco della SIM si chiama **MSI**.



Figura 3.20: Mobile Terminal

3.4.1.1 Base Station Subsystem

La **Base Station Subsystem** (BSS) comprende:

- **Base Transceiver Station** (BTS): interfaccia fisica con il compito di trasmettere e ricevere. Rappresenta il punto d'accesso per i dispositivi e a differenza di altri sorgenti di segnale (ad esempio radio e TV) trasmette segnale solo verso gli utenti attivi. Arriva fino a 32 canali FDM per BTS.
- **Base station controller** (BSC): gestisce il controllo delle risorse sull'interfaccia radio.

I BSC e i BTS comunicano mediante un collegamento cablato. Un BSC controlla un alto numero di BTS (*da decine a centinaia*). Tipicamente, BSC sono collocate con un MSC, invece di essere allocate vicino ai BTS.

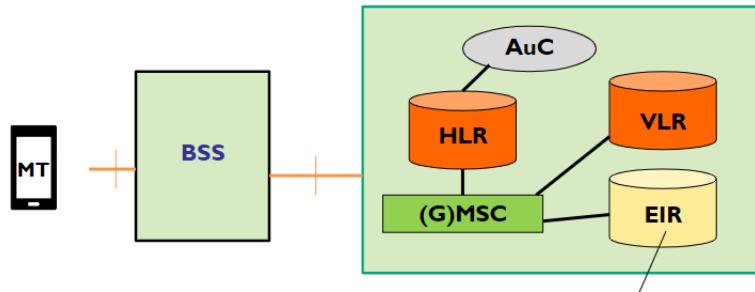
Le funzionalità principali dei BSC comprendono:

- Eseguire il transcoding vocale a 13 kb/s / 64 kb/s
- Eseguire il paging
- signal quality measurement
- Gestione dell'handover tra BTS controllati dallo stesso BSC

3.4.1.2 Network and Switching Subsystem

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

E' composto da:

**Figura 3.21:** NSS

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

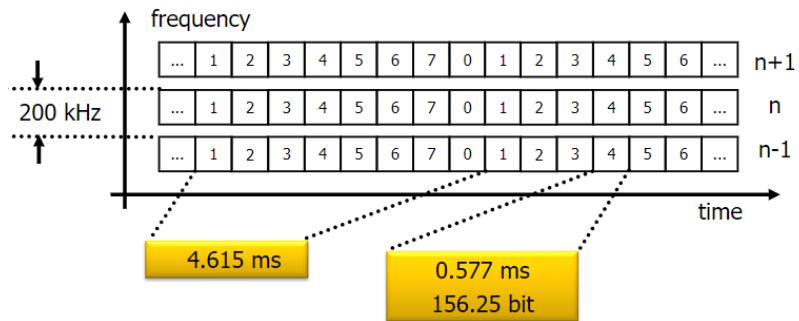
3.4.1.3 Canali fisici

Le frequenze utilizzate per il GSM sono: 859, 900 1800, 1900 MHz e variano in base allo scopo (ricezione o trasmissione) e funzionano attraverso il sistema **FDD** (frequency division duplex).

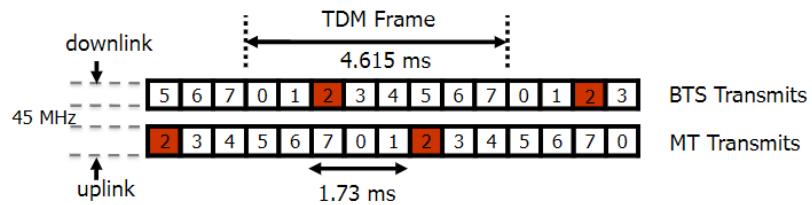
I canali GSM sono composti da una frequenza e uno slot, che identificano un canale fisico. Le trasmissioni sono organizzate in **burst** (da non confondere con pacchetti), ovvero blocchi di dati trasmessi su canali fisici. Sono simili ai pacchetti, ma funzionano su switching a circuito. La velocità di trasmissione è di 272 kbit/s. I canali possono essere acceduti con FDMA o TDMA mentre le frequenze sono divise in **FDM channels** (ciascuno largo 200kHz), che a loro volta sono divisi in **TDM frames** composti da 8 slot (ciascuno dalla durata di 0.577ms per un totale di 4.615ms).

Nota: Data una frequenza è uno time slot è possibile identificare un canale fisico.

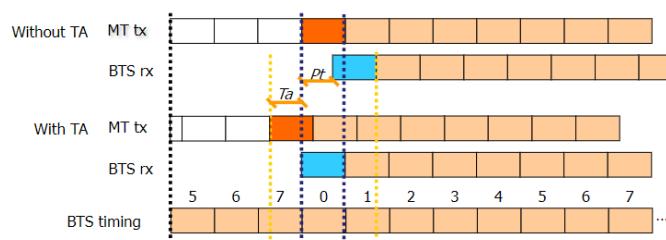
Il GSM non prevede una trasmissione simultanea (non è full duplex), per limitare i costi è presente un unico transceiver che consente la sola ricezione o trasmissione. Ogni MT trasmette per un time slot

**Figura 3.22:** Accesso al canale

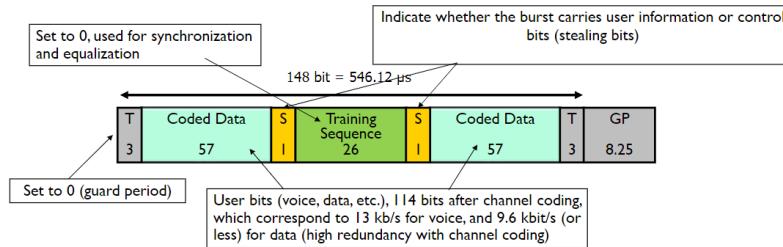
un burst di dati e rimane silenzioso per i rimanenti 7 slot. I frame su UL e DL sono sincronizzati in base ai time slot e shiftati di 3 slot.

**Figura 3.23:** GSM frame

I tempi di propagazioni però non sono nulli, per cui possono nascere problemi nella struttura degli slot in quanto i burst trasmessi dai MT potrebbero arrivare al BTS quando lo slot è già finito, causando anche la possibilità di collisioni. La soluzione utilizzata è la **timing advance**: la trasmissione del MT comincia prima del reale inizio del timeslot. a inizio e fine burst sono presenti dei “bit di guardia” che permettono di sincronizzare i burst.

**Figura 3.24:** Timing advance

Analizzando più nel dettaglio la struttura di un burst, notiamo come questo è caratterizzato dai bit di guardia, il coded data e infine lo stealing bit, il quale viene utilizzato per comunicare all’utente informazioni importanti.

**Figura 3.25:** Burst structure

I canali fisici del GSM sono composti da 8 canali, con timeslot 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**, i quali trasportano le informazioni di controllo (relative all’utente o alla rete), e traffic channels che trasportano le informazioni dell’utente.

3.4.2 4G/LTE - quarta generazione

Una delle caratteristiche di **LTE** è l’utilizzo del **FDMA** al posto del **CDMA**, che era stato pensato per gestire in efficienza il *fading* e sembrava essere una tecnologia migliore per il trasferimento dei dati. Il CDMA è però difficile da mantenere in termini tecnologici e i rapporti costi/benefici, inoltre nonostante tutto si è rivelato non essere sufficientemente buono. FDMA è un *FDM* con frequenze portanti più vicine e ortogonali (è possibile sovrapporre lo spettro) in modo da non generare interferenze.

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

	Release 8 LTE	
	Downlink	Uplink
Peak data rate	300 Mbps (4x4 MIMO) 150 Mbps (2x2 MIMO)	75 Mbps (1x2 SIMO)
Bandwidth	Up to 20 MHz	Up to 20 MHz
Peak Spectrum efficiency	≈ 16.3 bit/s/Hz	≈ 4.3 bit/s/Hz (1x2 SIMO)
Average Spectrum efficiency [bit/s/Hz/cell]	1.69 (2x2 MIMO) 1.87 (4x2 MIMO) 2.67 (4x4 MIMO)	0.74 (1x2 SIMO)
Latency	Data plane : 10 ms (round trip delay) Control plane : 100 ms (idle to active state)	

Figura 3.26: Statistiche del LTE

In LTE WCDMA wè stato sostituito con OFDMA (DL) e SC-FDM (UL).

Le frequenze utilizzate sono differenti al variare della distanza:

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

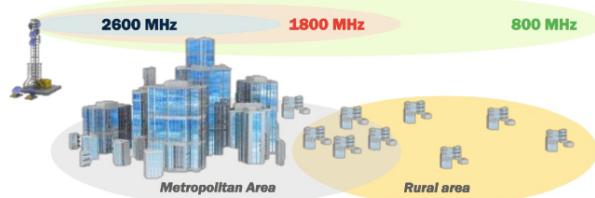


Figura 3.27: Utilizzo delle frequenze

Nella terminologia compaiono inoltre i seguenti termini:

- **user plane:** tutte le operazioni legate al trasporto dei dati degli utenti 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** (RAN), la quale include tutti i dispositivi che interagiscono con i dispositivi utente, 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 denominato **EPC**.

Nota: Le BS vengono denominate **eNodeB**.

3.4.2.1 Architettura di LTE

A differenza del GSM che utilizzava burst, in LTE avviene l'utilizzo di veri e propri pacchetti. La connessione alla rete avviene attraverso un **MME setup**, ovvero la configurazione di un home tunnel dalla rete di casa a quella dell'operatore.

Come mostrato nella figura di seguito, la rete si divide in **Long Term Evolution** (Access Network), ovvero E-UTRAN, ed **Evolved Packet Core** (core network) con l'acronimo di **EPC**, che rappresenta il cuore della rete e comprende tutti i nodi che forniscono funzioni di gestione della mobilità, autenticazione, session management, QoS e bearers configuration.

3.4.2.1.1 EPC L'approccio utilizzato per **EPC** è di tipo clean state design, ovvero ripensato completamente da zero rispetto al passato.

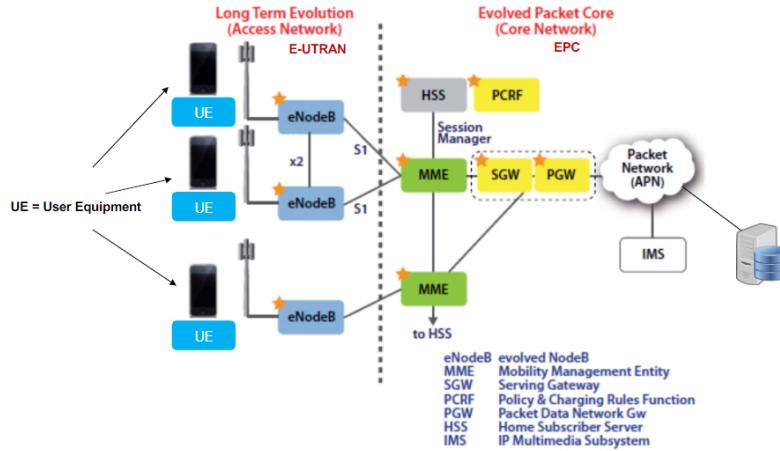


Figura 3.28: LTE architecture

Adopera il **packet switching transport** per il traffico appartenente a tutte le classi QoS comprendente di conversazione, streaming, dirette, non in tempo reale e in background.

Viene utilizzato il **Radio resource management** per: end-to-end QoS, trasporto verso i livelli più alti, load sharing/balancing, policy management/enforcement tra differenti accessi a tecnologie radio.

Sono presenti integrazioni con le reti già esistenti 3GPP, 2G e 3G.

Le funzioni principali di EPC sono:

- **Network access control:** include network selection, authentication, authorization, admission control, policy e charge enforcement e infine lawful interception.
- **Routing e trasferimento** di pacchetti.
- **Sicurezza:** include cifratura, integrity protection e network interface physical link protection.
- **Gestione della mobilità** per tenere traccia della posizione corrente all'interno del User Equipment (UE).
- **Radio resource management** per assegnare, riassegnare e rilasciare le risorse radio prese dalle singole o multiple celle.
- **Gestione della rete** per operazioni di manutenzione.
- Funzionalità di **networking IP** per le connessioni di eNodeB, condivisione di E-UTRAN, supporto in condizioni di emergenza e altre.

Le principali componenti sono:

- **Mobility Management Entity (MME):** si trova all'interno del Control Plane, supporta equipment context, identity, authentication e authorization. Perlopiù esegue procedure di tipo *Non Access Stratum* che si dividono prevalentemente in due gruppi funzioni relative al bearer management e Funzioni relative alla connessione e alla gestione della mobilità.

- **Serving Gateway (SGW)**: si trova all'interno del User Plane, riceve e invia i pacchetti tra gli eNodeB e la core network. Esegue il packet routing e forwarding tra gli EPC, oltre al lawful intercept. E' uno dei punti chiave per la *intra LTE-mobility*.
- **Packet Data Network Gateway (PGW)**: si trova all'interno del User Plane, connette l'EPC con le reti esterne/internet ed esegue operazioni di assegnamento UE IP, user packet filtering e servizi di NAT. E' uno dei punti chiave per l'accesso di reti *non 3GPP*.
- **Home Subscriber Server (HSS)**: database di informazioni relative all'utente e agli iscritti. Viene utilizzato, insieme al MME, per l'autorizzazione. Funziona in modo simile al HLR dell'architettura GSM.

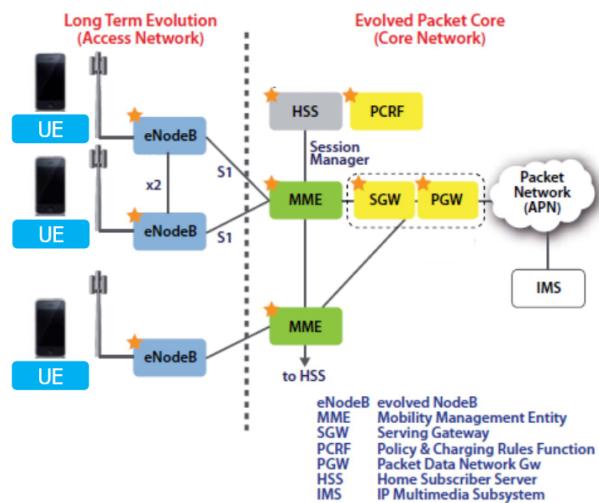


Figura 3.29: Componenti di EPC

3.4.2.1.2 Bearers Tutte le comunicazioni sono gestite attraverso dei “tunnel” denominati **bearers**, situati tra il PGW e SGW che a loro volta sono connessi a un ulteriore tunnel che parte dal SGW e arriva alla base station, e ancora tra user agent ed eNodeB. All'interno della rete i tunnel possono essere creati per soddisfare dei requisiti in termini di qualità del servizio, creando bearer dedicati a servizi specifici. E' presente un bearer default che stabilisce una connessione con il PGW quando un UE è attivato.

Esistono tre differenti tipologie di bearer:

- **S5 bearer**, connette SGW con PGW _(può estendersi da P-GW al Internet).
- **S1 bearer**, connette eNodeB con SGW. Il meccanismo di handover stabilisce un nuovo S1 bearer per le connessioni end-to-end.
- **Radio bearer**, connette UE e eNodeB. Questa tipologia segue l'utente in movimento in direzione del MME in quanto la radio esegue degli handover quando l'utente si muova da una cella

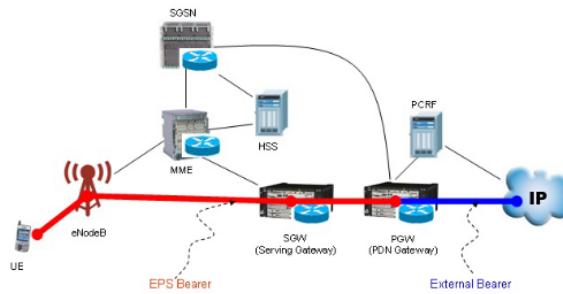


Figura 3.30: Bearers

all'altra.

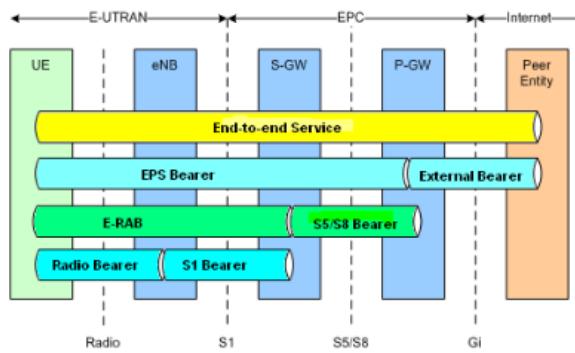


Figura 3.31: Tipologie di Bearers

3.4.2.2 E-UTRAN

La E-UTRAN consiste principalmente di eNodeB con un interfaccia X2 per connettere gli eNodeB (due tipologie: X2 control e X2 user).

Le funzioni principali sono:

- **Gestione delle risorse radio** come radio bearer control, radio mobility control, scheduling ed allocazione dinamica delle risorse radio per uplink e downlink.
- **Compressione** (senza perdita) **degli header**.
- Sicurezza.
- **connettività** verso EPC.

3.4.2.3 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.

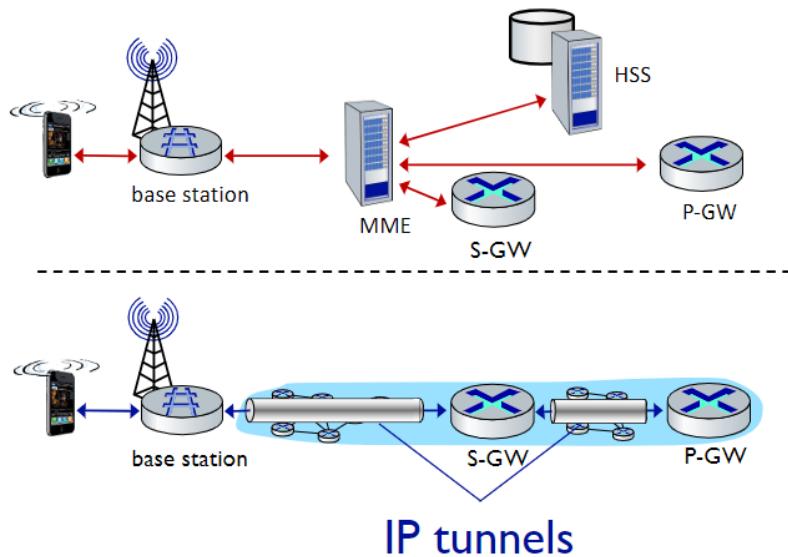


Figura 3.32: Data Plane (basso) e Control Plane (alto)

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 ortogonalni 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 sync signal ogni 5ms. Il dispositivo trova il primary sync signal e a quel punto attende il second sync 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 innattività, 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.

3.4.3 5G

L'obiettivo 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:

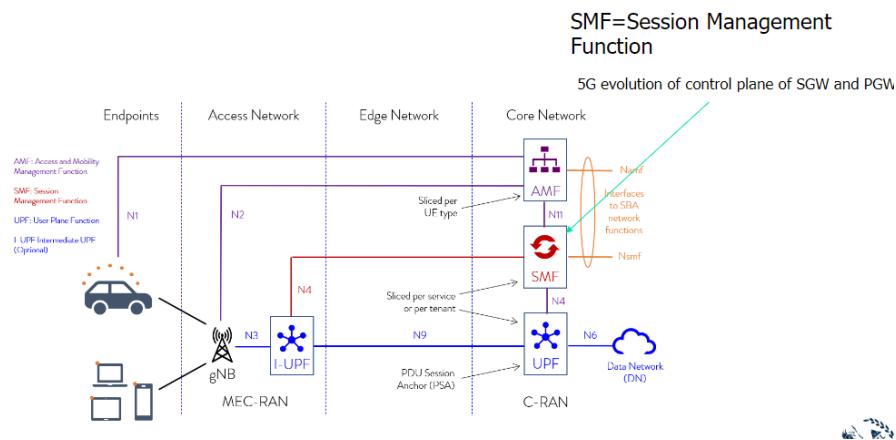
- **eMBB**: enhanced mobile broadband, come in una rete 5G sia possibile usare servizi ad alta qualità per utenti mobili
- **mMTC**: massive machine type communication, comunicazione industriale a bassa latenza.
- **URLLC**: Ultra-Reliable Low-Latency Communication, in grado di garantire latenze fino 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.



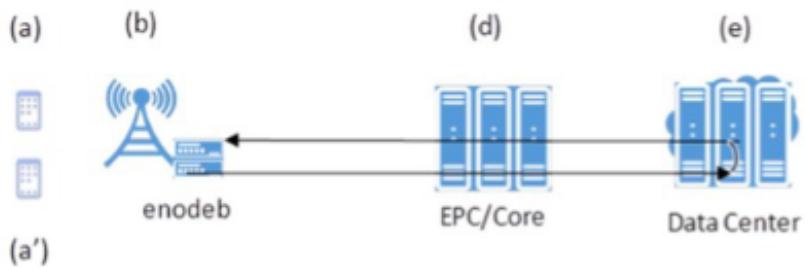
3.4.3.1 Edge Network

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 benefici

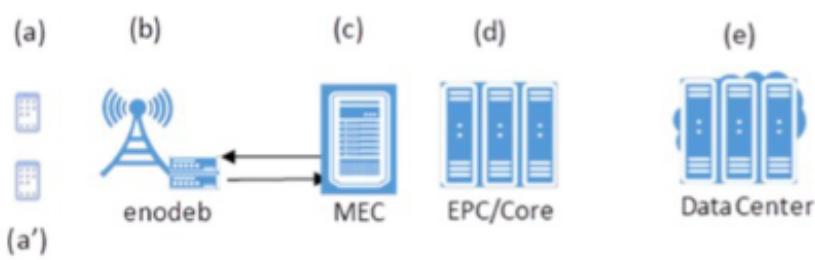
attesi sono:

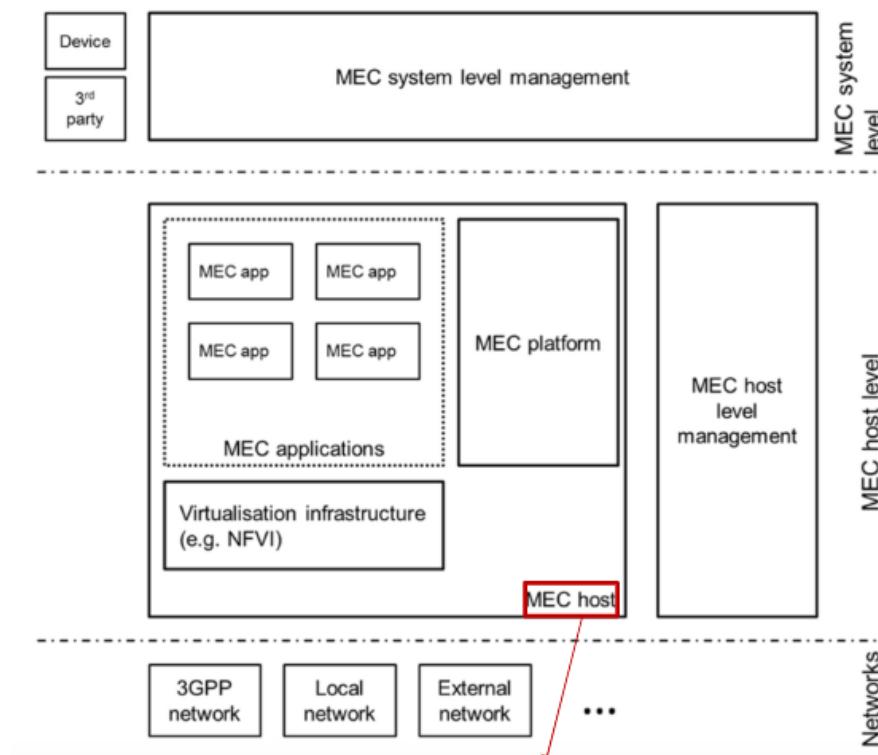
- ultra low latency
- alta bandwitch
- accesso real time alla radio network
- contextual information
- location awareness
- flexible and exendable framework for services

Non-MEC System



MEC System





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

3.4.3.2 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 trasmissioni con dati molto pesanti. Different subcarrier spacing (“numerology”): shorter slots for higher spacing.

3.5 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, semplicemente cambia l'endpoint 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 incapsulati utilizzando GTP inside UDP, all'interno del datagramma

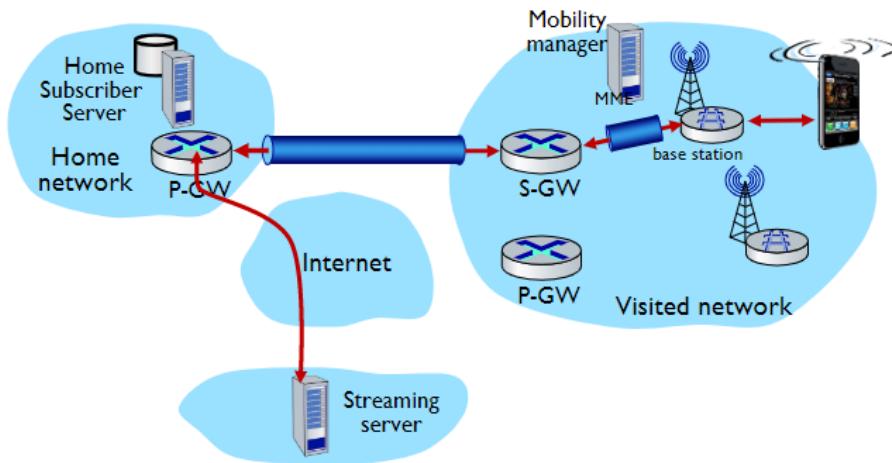


Figura 3.33: Configuring data plane

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

1. il source BS seleziona il target BS, invia un Handover Request message al target BS
2. Il target BS prealloca un radio time slots, risponde con HR ACK con le informazioni del dispositivo
3. 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
4. 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)
5. Il target Bs informa MME che del nuovo BS per il dispositivo (MME istruisce S-GW di cambiare l'endopoint del tunnel al nuovo BS)

6. 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.
7. I datagrammi del dispositivo possono ora utilizzare il nuovo tunnel dal target BS al S-GW

4 Principi del modern Lan Design

Le **Wide Area Network** (WAN) appaiono negli anni 60, caratterizzate dalla presenza di alcuni mainframes e la necessità di connettersi da remoto (per ridurre tra più autorità i costi). Soltanto alla fine degli anni 70 compaiono le **Local Area Networks** in seguito alla comparsa dei primi minicomputer e grazie alla riduzione costi che hanno reso meno utile l'utilizzo di mainframes (*ancora usati per motivi differenti come la ricerca*).

Inizialmente WAN e LAN si sono evolute indipendentemente in quanto erano utilizzati differenti protocolli allo scopo di sopperire a necessità diverse. Soltanto in seguito si è pensato di collegare le LAN con WAN, da cui è risultato come unico vincitore, come protocollo, IP.

Sul livello fisico ha vinto lo standard **IEEE 802**, in particolare **802.3** ovvero **ethernet** e **802.11** ovvero **WIFI**. Dal punto di vista cablato invece: EIA/TIA 568, ISO/IEC 11801.

In breve, i dispositivi lan si differenziano in:

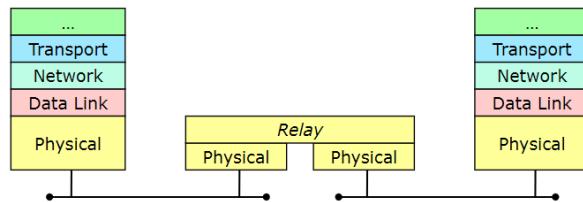
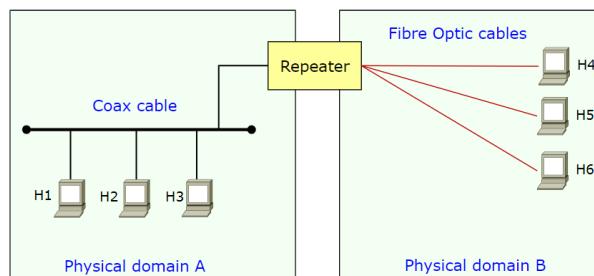
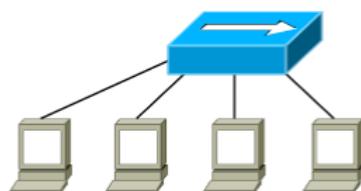
- **ripetitori** (*livello 1*): hub, stesso collision domain ma separato physical domains.
- **bridge** (*livello 2*): switch, collision domain separato ma stesso broadcast domain.
- **router** (*livello 3*): L3 switch, broadcast domains separato, non specifico per le LAN (*e non trattato in questa dispensa*).

4.1 Ripetitori

I **ripetitori**, dispositivi di *livello 1*, consentono di interconnettere il livello fisico ricevendo e propagando una sequenza di bit. E' utilizzato per interconnettere le reti aventi lo stesso MAC (Medium Access Control) address e ripristinare la degradazione del segnale (su lunghi cavi) consentendo la raggiunta di maggiori distanze.

Con l'avvento del cavo in rame compaiono gli HUB che utilizzano una struttura a stella. Tutti i dispositivi connessi a un hub appartengono allo stesso dominio di collisione.

I ripetitore con più di due porte prendono il nome di **hub**, sono necessari per il twisted pairs e il fiber cabling.

**Figura 4.1:** Struttura dei ripetitori**Figura 4.2:** Esempio di utilizzo di un ripetitore**Figura 4.3:** Hub

4.2 Bridge

Il **bridge** è un dispositivo di *livello 2* e pertanto è in grado di comprendere una trama ethernet. Sono implementati completamente in software e composti da due porte (per questioni economiche). Interconnettono al livello di data link (da ethernet a wifi) e hanno differenti MAC (*medium access mechanism, framing*).

Nota: Lo switch è un bridge a più porte.

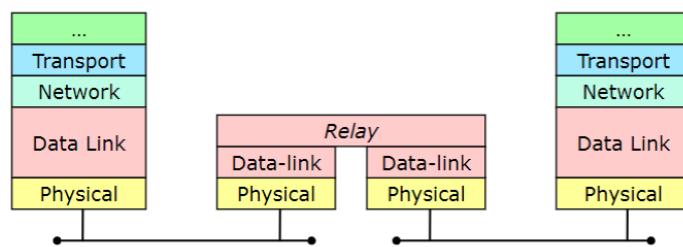


Figura 4.4: Bridge

Adotta una modalità store and forward, ovvero è in grado di ricevere tutta la trama, “ragionarci” e poi inoltrarla verso la porta corretta che ha individuato grazie al mac e la tabella di inoltro.

Non necessariamente interconnette link layer uguali (anche se per lo più è così), ma è pensato per supportarne anche di tipi differenti. Inoltre riesce a gestire le collisioni ed evitarle, ottenendo una **divisione del collision domain** ma mantenendo un **unico broadcast domain** (quindi il broadcast continua a funzionare correttamente).

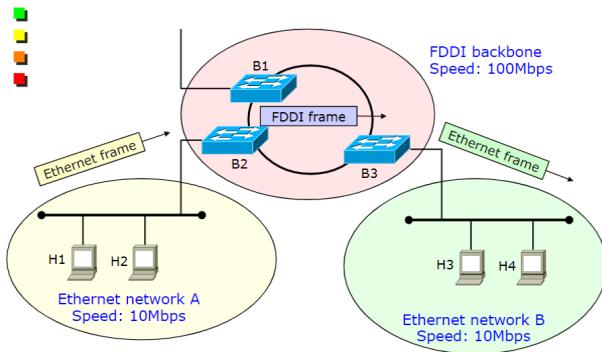
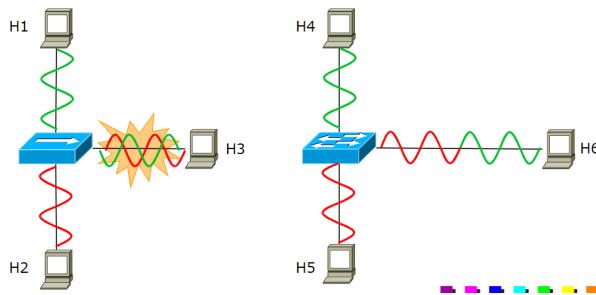
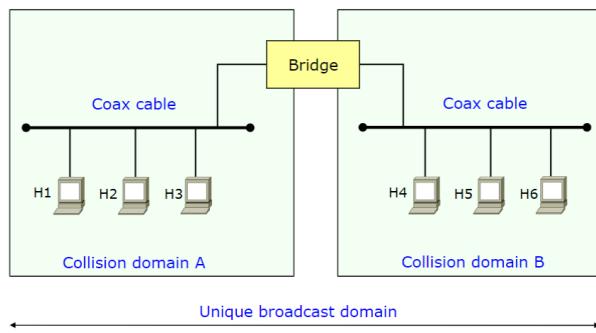
Viene utilizzato per estendere le reti LAN (specialmente per FastEthernet), ma vi sono problemi di collisione.

Il funzionamento consiste nel ricevere e ritrasmettere (dopo) un frame, il quale viene salvato, modificato e rinvia.

Il meccanismo **store and forward** permette un invio più intelligente dei dati nelle interfacce di output, riuscendo a disaccoppiare le collisioni sul dominio di broadcast (dunque il collision domain non è più un problema).

Bisogna però fare attenzione al fatto che sui singoli spezzoni di rete possono ancora esserci collisioni, che vengono risolte attraverso la modalità full duplex (funzionante tra host e switch, switch e switch e host e host).

CSMA/CD non è più necessario in quanto con la modalità full duplex non sono più presenti collisioni.

**Figura 4.5:** Esempio di bridge con interconnessioni**Figura 4.6:** Bridge e collisioni**Figura 4.7:** Broadcast collision domain

4.3 Modern LANs

Le moderne reti LAN sono basate su full-duplex, switch e ethernet. Oggi le porte ethernet possono raggiungere i gigabit e anche se quando ci riferiamo a switch facciamo in realtà riferimento a switch ethernet. Non è più necessario utilizzare CSMA/CD (non definito per portate sopra 1GE).

Attenzione: Le wireless LAN funzionano in modo completamente diverso (utilizzo di CSMA/CA) e troviamo ancora gli hub.

4.3.1 Transparent bridges

I bridge e gli switch in ethernet prendono il nome di **transparent bridge** (anche altri non trasparenti sono stati proposti ma non più utilizzati). Il nome significa che deve essere plug & play e non dovrebbe richiedere una configurazione manuale. Inoltre, per l'utente non deve cambiare nulla e deve funzionare ugualmente (se non meglio) rispetto agli hub. I dispositivi finali devono funzionare allo stesso modo con o senza bridges.

Le performance potrebbero essere differenti rispetto alla rete originale, ma le funzionalità devono essere le medesime. In particolare non devono essere presenti cambiamenti sui frame inviati dagli end systems (stesso frame, stesso MAC address, ecc), potrebbero esserci variazioni nel come questi vengono ricevuti ma non a livello di formato.

Nota: per l'utente gli switch non hanno indirizzi MAC, ma non è così.

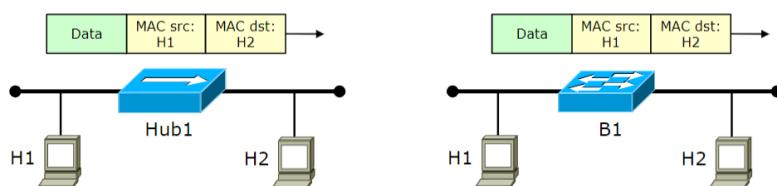


Figura 4.8: Transparent bridges e host finali

Ciascuna porta di un bridge ha un MAC level e per tale motivo ha un indirizzo MAC, che non deve mai essere utilizzato per eseguire il forwarding dei data frames, bensì per consentire di indirizzare il traffico attraverso i management frames.

Il forwarding del traffico è intelligente: è possibile fare forwarding attraverso una sorta di “routing table” che prende il nome di **filtering database** contenente le destinazioni in base agli indirizzi MAC. Questa deve essere disponibile localmente e nel caso di unicast viene memorizzata solo la porta per

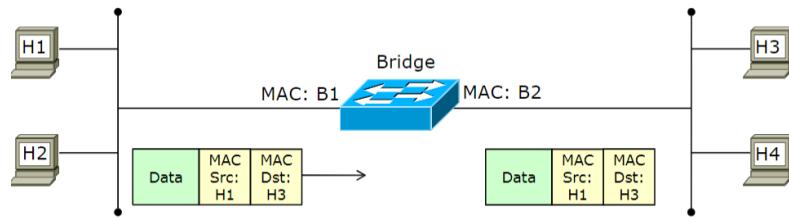


Figura 4.9: Transparent bridges e port addresses

raggiungere la destinazione (destination MAC-based forwarding) mentre nel multicast e broadcast si utilizza il flooding (tutte le porte eccetto quella da cui il frame è stato ricevuto, anche non contemporaneamente). Per far ciò è necessaria una forwarding table locale (filtering database), stazioni auto-learning (backward learning) e loop detection (spanning tree algorithm).

4.3.2 Filtering database

Un **filtering database** è una tabella contenente la posizione di ciascun MAC address trovato nella rete, corredato da informazioni come la destination port ed ageing time (default 300s). Lo scopo della tabella è quello di filtrare “fuori” il traffico non voluto da un link.

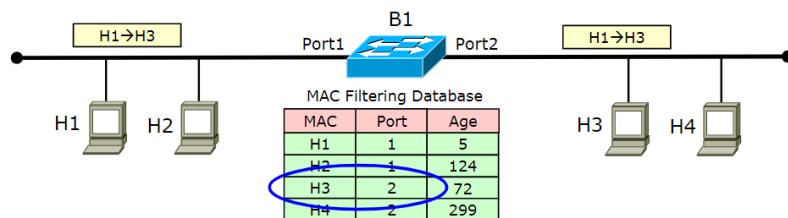


Figura 4.10: Filtering database

La tabella ha entry di due tipi:

- **statiche**: non aggiornate dal processo di learning, solitamente minori di 1000.
- **dinamiche**: popolate e aggiornate dal backward learning process. Il massimo numero di entry è pari a $\$2 / 64000 \$$. Vengono poi eliminate quando le stazioni non esistono più o dopo un lasso di tempo (*default 300 secondi*).

La filter table può essere popolata manualmente (poco comodo) oppure mediante appositi algoritmi con quello che si definisce backward learning, ovvero quando lo switch riceve una trama riceve anche il mac sorgente e capisce che attraverso quella porta può raggiungere quel dispositivo.

Un esempio reale è il seguente:

```

1 Cisco-switch-1> show cam dynamic
2
3 * = Static Entry. + = Permanent Entry.
4 # = System Entry X = Port Security Entry
5
6 Dest MAC Address      Ports Age
7 -----
8 00-00-86-1a-a6-44    1/1   1
9 00-00-c9-10-b3-0f    1/1   0
10 00-00-f8-31-1c-3b   1/2   4
11 00-00-f8-31-f7-a0   1/1   2
12 00-01-e7-00-e3-80   2/2   0
13 00-02-a5-84-a7-a6   2/1   1
14 00-02-b3-1e-b4-aa   2/1   5
15 00-02-b3-1e-da-da   2/5   1
16 00-02-b3-1e-dc-fd   2/4   2

```

Quando uno switch non sa dove si trova un nodo (aging terminato), viene operato il flooding ma non è molto efficiente. In realtà è un falso problema perché i nodi informano di loro semplicemente col traffico, per cui tutti i nodi riceveranno il pacchetto e immediatamente tutti gli switch riescono ad aggiornare i propri database. Quando l'utente si muove non smette di trasmettere il traffico! Per tale motivo al prossimo pacchetto le informazioni verranno aggiornate.

C'è ancora un problema però se si utilizza una topologia a maglia, in particolare se mando un pacchetto broadcast, si verifica il **broadcast storm**: il pacchetto viene mandato a tutti e reinoltrato generando un loop che non termina se non spegnendo gli switch. Per risolvere, si usa lo spanning tree protocol che realizza un albero logico su una tipologia magliata fisica.

4.4 Multiple LANs

Per ragioni di sicurezza o semplice preferenza, è possibile dividere una rete in più parti generando reti distinte. Ciò comporta il dover gestire ciascun edificio con una propria rete che poi, attraverso dei cavi, connettono gli switch dei vari edifici.

Questo è però indubbiamente molto costoso, per questo motivo sono state realizzate le **Virtual LANs** (VLAN) che consentono di simulare che un set di porte specifiche di uno switch facciano parte di un dominio di broadcast differente, utilizzando un'unica infrastruttura di rete. Per far parlare le VLANs è necessario un router con tutte le sottoreti connesse, permettendo la comunicazione in modo tradizionale anche se la rete di origine è in realtà la medesima.

Attenzione: il traffico di livello 2 non può attraversare le VLANs.

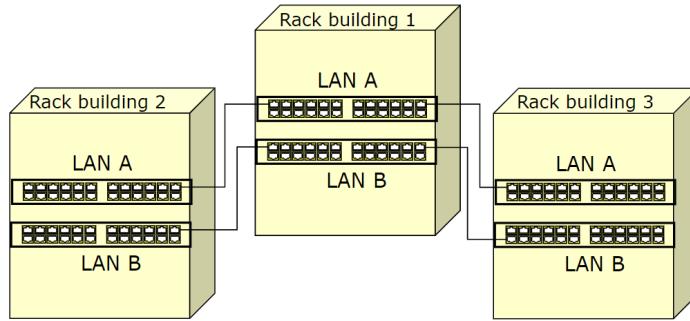


Figura 4.11: Esempio di edifici per lan multipla

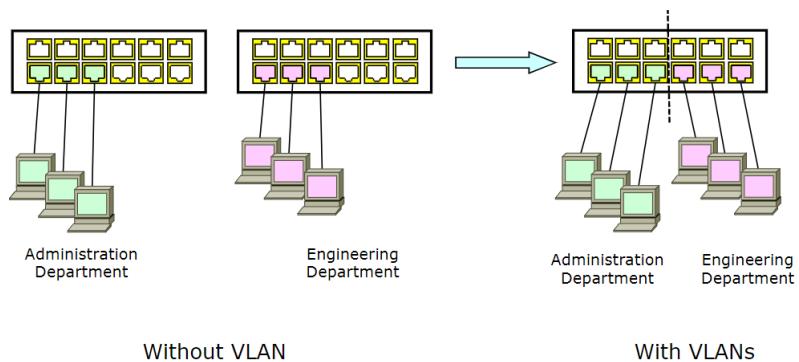


Figura 4.12: Reti fisiche differenti

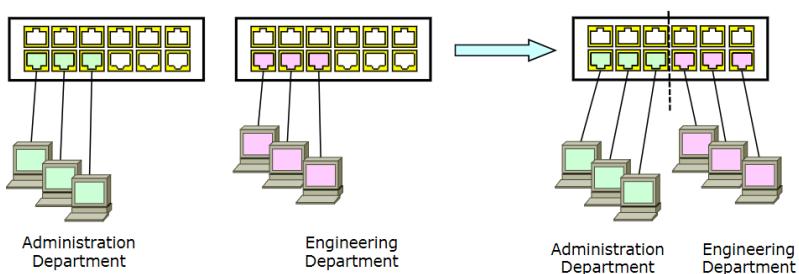


Figura 4.13: VLANs

Un altro modo è connettere il router a un'unica interfaccia che lavora per entrambe le sottoreti, ottenendo il **one arm router**.

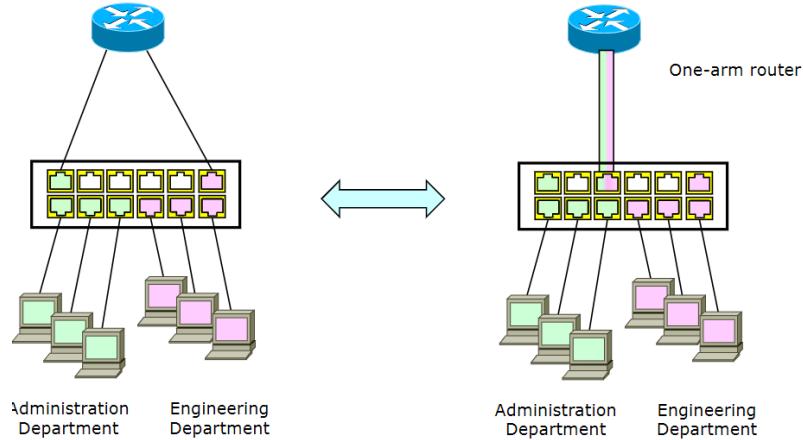


Figura 4.14: One Arm

Per connettere più VLAN è necessario un router (device del livello 3) per eseguire il lookup, l'header di livello 2 viene buttato in favore di uno nuovo creato con un differente MAC address.

Il broadcast non può attraversare VLAN differenti, in quanto non è possibile utilizzare ARP per individuare i MAC address di un'altra VLAN. Gli host di Virtual LANs differenti devono fare riferimento a reti IP differenti.

Il modo più semplice per associare un frame a una VLAN è marcarlo all'arrivo in base alla porta attraversata. Se però non si altera la trama, l'informazione sarà evidenziata solo all'interno dello switch che ha attraversato ma non agli altri switch. Per superare questo problema è stato introdotto il **tagging**, ovvero si utilizza un campo della trama ethernet con 4 byte aggiuntivi al frame per il vlanID, consentendoci di identificarlo anche negli switch rimanenti.

Per apportare le modifiche citate sopra è necessario apportare delle piccole modifiche ai mac già esistenti, in particolare un nuovo framing (per il tagging) indipendente dal MAC e la lunghezza massima dei frame deve essere estesa di 4 byte.

Le porte si dividono in:

- **access:** invia e riceve trame non taggate (default su host, switches, servers, routers ecc), vengono solitamente utilizzate per connettere end-stations alla rete. La tipologia di frame non deve essere cambiata dal host (che non sa dell'esistenza della VLAN).
- **trunk:** invia e riceve trame taggate, deve essere configurato esplicitamente. Spesso viene utilizzato nelle connessioni switch-to-switch e per connettere server/router.

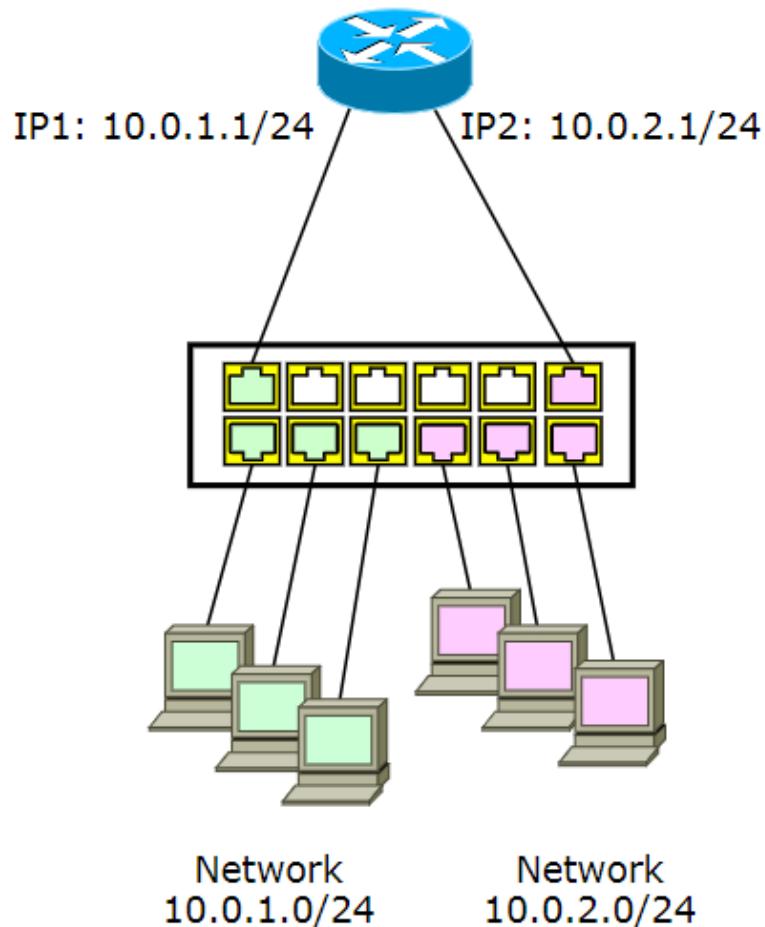


Figura 4.15: VLAN e indirizzi IP

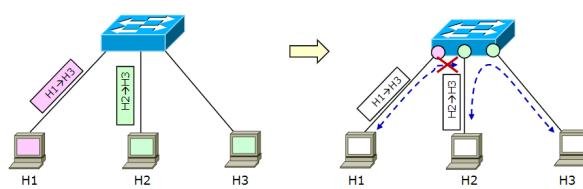
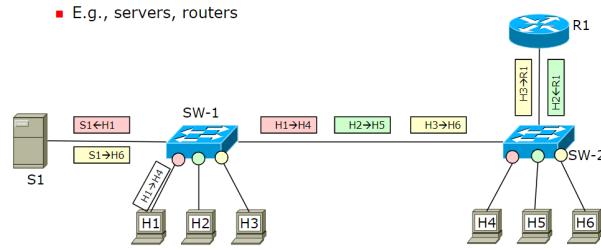
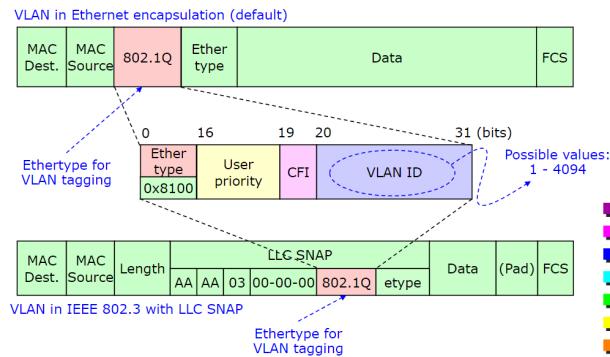
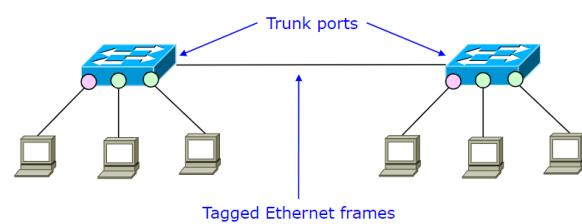


Figura 4.16: VLAN su singolo switch

**Figura 4.17:** VLAN su più switch**Figura 4.18:** Tag encoding**Figura 4.19:** Access Ports**Figura 4.20:** Trunk ports

5 VPN

Una **Virtual Private Network** (VPN) è un insieme di tecnologie che consente di realizzare una connettività tra due sottoreti distinte in modo che possano comunicare come se fossero un'unica rete privata. Quando un utente si connette su internet non attraversa necessariamente un unico ISP, e questo rende lo scenario molto variegato.

L'obiettivo è far sì che due sottoreti (anche in organizzazioni diverse) riescano a comunicare mantenendo le stesse politiche (di sicurezza, quality of service, affidabilità).

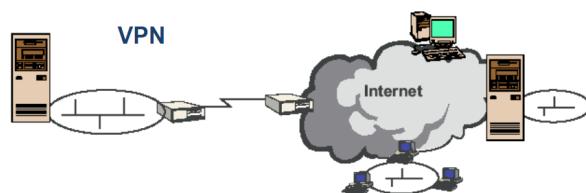


Figura 5.1: Esempio di VPN

Gli elementi chiave sono:

- **Tunnel:** Consente di incapsulare in modo sicuro il traffico in transito sulla rete condivisa (non presente in alcune soluzioni).
- **VPN gateway:** Apre e termina i tunnel, dovranno supportare uno tra i vari protocolli specifici per fare tunneling.

Il motivo per cui utilizziamo le VPN è dunque quello di non dover utilizzare cavi per la realizzazione di reti private.

Alcune funzionalità chiave garantite dalle VPN sono:

- deployment model
- provisioning model
- protocol layer

Definiremo anche alcune soluzioni:

- **site to site:** vpn a livello di sottorete (gateway).

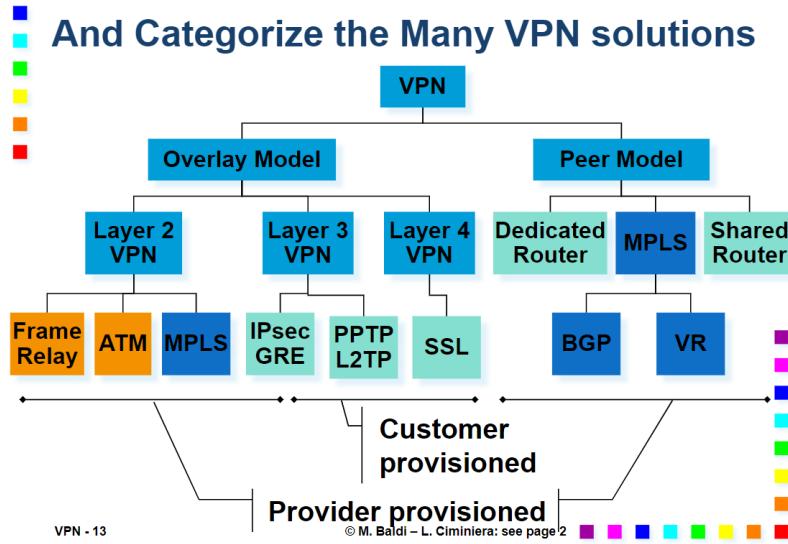


Figura 5.2: Gerarchia dei protocolli

- **end to end:** sottorete a livello di host (terminali).
- **Access VPN / Remote VPN / Dial In:** canale sicuro tra un terminale verso un'intera sottorete (es smart working per collegarsi alla rete aziendale).

Dal punto di vista del deployment:

- **Intranet VPN:** interconnette uffici remoti della stessa azienda.
- **Extranet VPN:** interconnette aziende diverse.

A livello di extranet è di interesse ridurre l'accesso alle risorse di rete mediante **firewall**, ottenere **Overlapping Address Spaces** mediante *Network Address Translation* e **controllare il traffico** in modo che quello dei partner non possa compromettere il funzionamento della rete aziendale.

Nota: Quello che contraddistingue i due tipi di rete sono perlopiù motivi di sicurezza.

L'accesso a internet può essere:

- **Centralizzato:** gli utenti remoti utilizzano una rete IP pubblica per connettersi, disponibile solo negli headquarters e trasmette il traffico nella sua interezza da e verso internet. L'accesso è centralizzato e controllato da firewall. Il vantaggio di tale modalità è un maggior controllo.
- **Distribuito:** gli utenti remoti si connettono attraverso la propria rete IP e la VPN è utilizzata solo per il traffico aziendale. Il vantaggio lo si ha nei costi che risultano essere ridotti.

Riassumendo, le features che una VPN mette a disposizione sono:

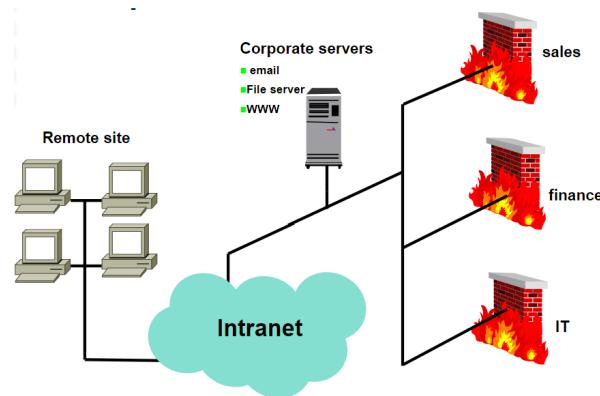


Figura 5.3: Esempio di intranet

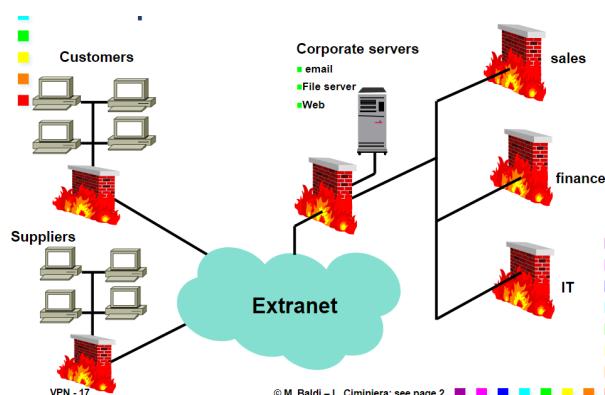


Figura 5.4: Esempio di extranet

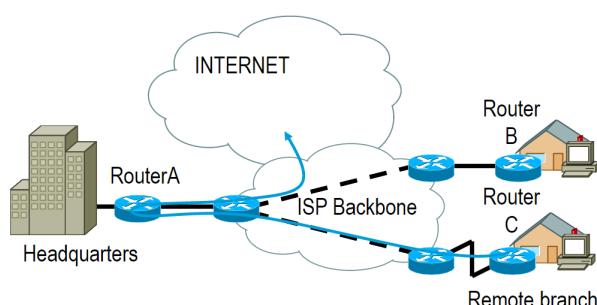


Figura 5.5: Accesso centralizzato

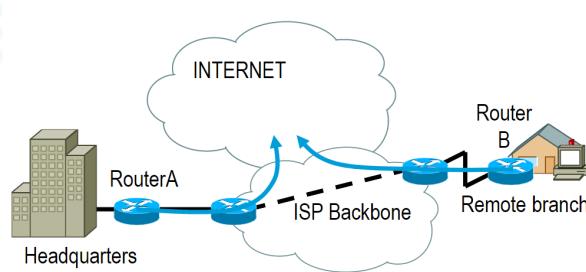


Figura 5.6: Accesso distribuito

- Separazione dei dati (tramite tunneling).
- Aumento della sicurezza (tramite cifratura).
- Prevent tempering (integrità).
- Identificazione delle sorgenti (tramite autenticazione).

Dal punto di vista della sicurezza gli obiettivi sono:

- **End point authentication**, verificando che un dispositivo sia chi dice di essere.
- **Integrità dei dati**, assicurando che non vengano cambiati.
- **Confidenzialità dei dati**, assicurando che non possano essere letti da altri al di fuori del destinatario.

5.1 Modalità di deployment

5.1.1 Site to Site VPN Tunneling (s2s)

I tunnel **site to site** forniscono la garanzia che le politiche di rete avvengono a livello di infrastrutture pubblica. All'interno delle due reti aziendali la comunicazione è ritenuta sicura di default, ma se l'attaccante è interno alla rete questa risulta comunque vulnerabile.

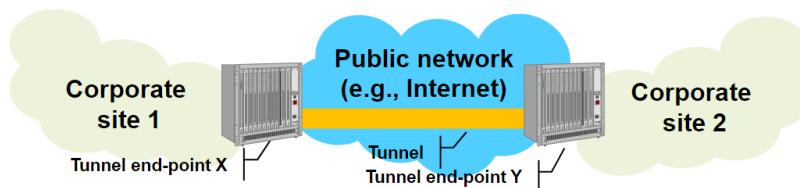


Figura 5.7: S2S tunneling

5.1.2 End to End VPN Tunneling (e2e)

I tunnel **End to End** forniscono maggiore sicurezza in quanto il tunnel è realizzato direttamente tra i due host. Fin dall'inizio della comunicazione il traffico mantiene le stesse politiche di rete, in quanto la complessità è molto più oneroso sia in termini di costo che di gestione.

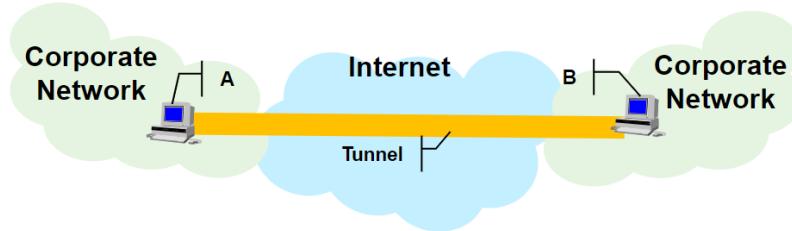


Figura 5.8: E2E tunneling

5.1.3 Remote VPN Tunneling

Il **Remote VPN Tunneling** connette un endpoint con un vpn gateway. È possibile aggregare un'intera sottorete, ma ogni dispositivo deve essere sufficientemente robusto per connettersi.

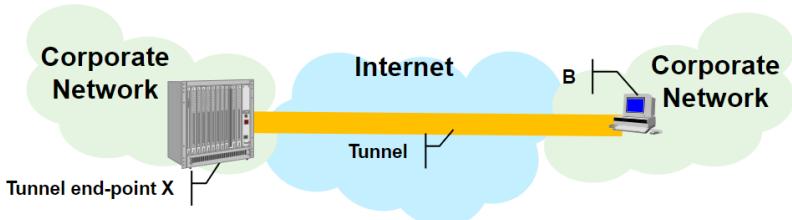


Figura 5.9: Remote tunneling

5.1.4 Overlay Model

Nel **Overlay Model** la rete pubblica non partecipa alla realizzazione della vpn, non sa quale siano le destinazioni e la connessione avviene attraverso VPN gateways. Ciascuno di questi deve essere in contatto con tutti gli altri generando molti tunnel mesh. Il routing è ottenuto attraverso i gateway.

La creazione dei tunnel va a influenzare anche gli aspetti di routing: perdiamo il vantaggio del routing ma costa meno ed è del tutto trasparente (anche se il pacchetto potrebbe metterci un po' di più).

5.1.5 Peer Model

Nel **Peer Model** ciascun VPN gateway interagisce con i router pubblici, scambiando informazioni di routing che si aggiungono a quelle fornite dal service provider. Il traffico che subisce rilouting sulla rete pubblica si muove all'interno della stessa rete VPN.

In questo approccio il routing è migliorato, ma chi realizza la VPN è fortemente coinvolto alla comunicazione di rete (non più trasparente). Inoltre, i tunnel sono tra i router compromettendo in parte la sicurezza (a livello di router posso sniffare il traffico).

5.1.6 Customer Provisioned VPN

Nel **Customer Provisioned VPN** il cliente implementa la soluzione VPN e possiede, configura e gestisce i dispositivi connessi adoperando del *Customer Equipment* (CE). Il Network Provider non è a conoscenza del fatto che il traffico generato dal cliente sia VPN. Tutte le features sono implementate sui device e i CE sono i terminatori dei tunnel.

L'host deve necessariamente avere 2 indirizzi, il remote host deve terminare il tunnel e deve averlo attivo, in caso contrario può operare ugualmente ma senza VPN.

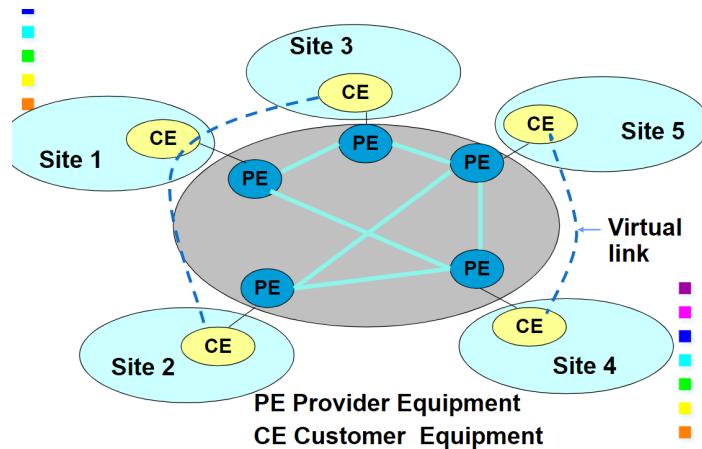


Figura 5.10: Customer Provisioned VPN

5.1.7 Provider Provisioned VPN

Nel **Provider Provisioned VPN** il provider implementa la soluzione VPN (quindi sotto il controllo dell'azienda), e la VPN stessa è mantenuta dal provider che si occupa di gestire i dispositivi. Il customer equipment si potrebbe comportare come se si trovasse all'interno di una rete privata, i terminatori dei tunnel sono dei Provider Equipment. E' meno costosa ma richiede la "fiducia" del provider.

Il remote host deve essere sempre nella VPN, obbligando l'utente ad installare determinati dispositivi. In questo modo si ha un solo indirizzo in quanto si è sempre all'interno della VPN, necessitando di un accesso a uno specifico *Internet Service Provider*. In quest modalità l'accesso è centralizzato.

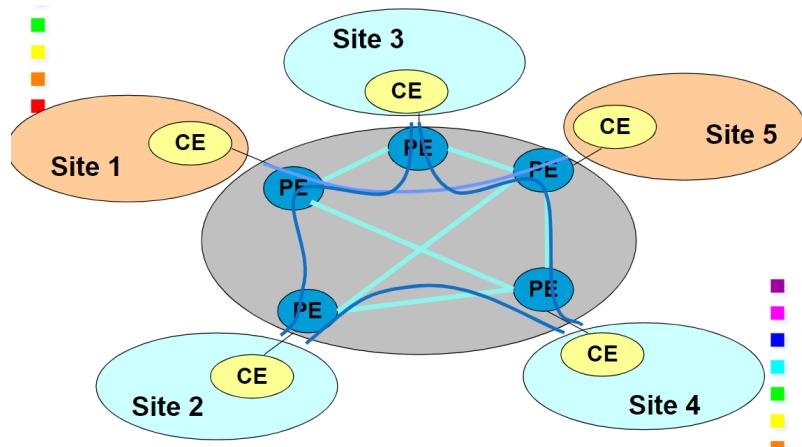


Figura 5.11: Provider Provisioned VPN

5.1.8 Access VPN Customer Provisioned

E' necessario considerare anche gli aspetti inerenti al piano di indirizzamento. Sui terminatori della VPN è necessario avere un indirizzo pubblico, costringendo ad avere due indirizzi. Tipicamente le remote access sono più semplici a livello di Customer Provisioner.

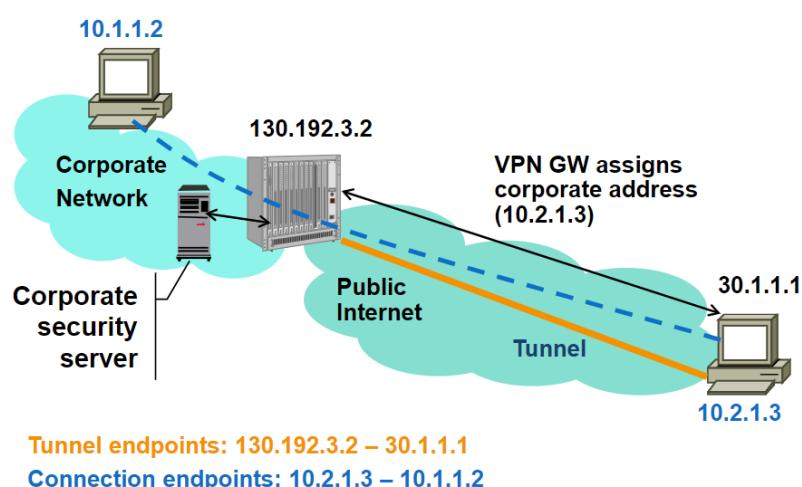


Figura 5.12: Access Customer Provisioned

5.1.9 Tunneling

Un pacchetto (o frame) viene inviato attraverso una rete pubblica tra due siti privati mediante nodi pubblici.

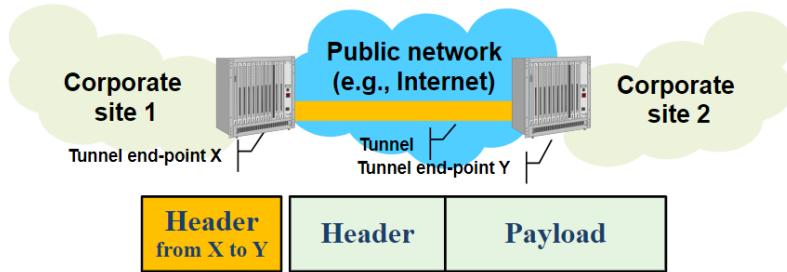


Figura 5.13: Tunneling

5.2 Topologie

Le VPN si differenziano in due topologie (virtuali):

- **Hub and spoke:** Ciascun branch comunica direttamente con l'headquarter e raggruppa il data flow di molte aziende (centralizzate in mainframe o data center). Il routing è sub-ottimo e sono richiesti pochi tunnel, con però il rischio che l'hub possa diventare un bottleneck rallentando le prestazioni.
- **Mesh:** Utilizza un gran numero di tunnel, più difficile da gestire ma migliora il routing.

5.3 Layers

Un qualsiasi servizio di trasporto di pacchetti mediante tunneling funziona o come *Layer N Service* oppure mediante un *Layer N Protocol*.

5.3.1 Layer 2

Il livello 2 si suddivide in:

- **Virtual Private LAN service:** emula le funzionalità di Lan e può essere utilizzato per connettere alcuni segmenti LAN (funziona come una lan singola attraverso la rete pubblica). La soluzione emula anche i learning bridges, con routing basato sul MAC address.

- **Virtual Private Wire Service:** emula una leased line, può trasportare qualsiasi protocollo.
- **IP-only Lan-like Service:** i CE sono IP routers o IP hosts (non ethernet switches), viene utilizzato solo IP (insieme a ICMP e ARP) per far viaggiare i dati nella VPN.

5.3.2 Layer 3

Le soluzioni di livello 3 sono standard: i pacchetti sono inviati attraverso la rete pubblica con routing basato su indirizzi di livello 3, che possono essere **peer** (vpn/corporate/indirizzi cliente) oppure **overlay** (backbone addresses), mentre i CE possono essere sia ip routers che IP hosts.

I pacchetti (o frame) sono trasportati attraverso la rete IP come pacchetti IP nelle seguenti modalità:

- un **pacchetto IP in un pacchetto IP** (IP in IP), come GRE o IPsec.
- Un **frame layer 2 in un pacchetto IP** (IP in frame), come L2TP, PPTP (basato su GRE).

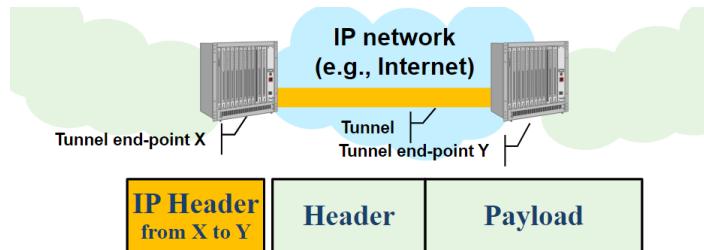


Figura 5.14: Layer 3

In particolare nel tunneling basato su **IP in IP**, dati due nodi A e B, dotati di indirizzo aziendale (non necessariamente pubblico), il tunneling abilita la comunicazione ma non assicura la sicurezza.

5.3.3 Layer 4

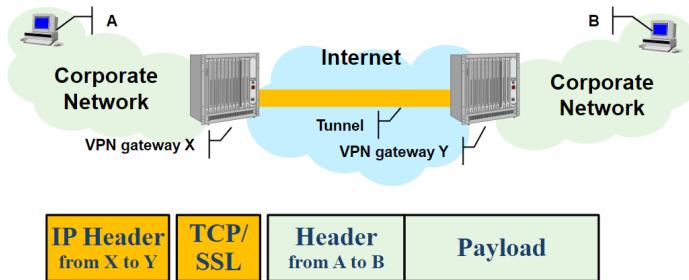
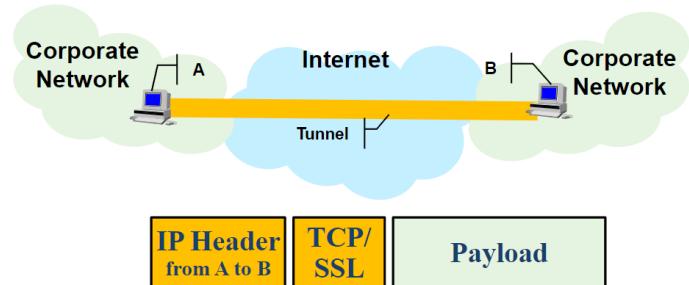
Le soluzioni VPN di livello 4 provvedono solo alla sicurezza. Hanno come grande svantaggio l'utilizzo di soluzioni non standard.

5.3.3.1 Site to Site (s2s)

Nel **Site to Site** la VPN è costruita utilizzando connessioni TCP, sfruttato anche dai tunnel, mentre la sicurezza è garantita attraverso SSL/TSL. E' possibile avere header di livello 3 o di livello 4.

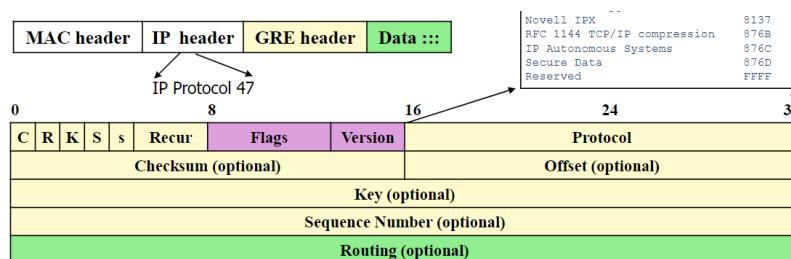
5.3.3.2 End to End (e2e)

Nelle connessioni **End to End** il tunnel è terminato da un end system.

**Figura 5.15:** s2s**Figura 5.16:** e2e

5.4 Generic Routing Encapsulation (GRE)

Il **Generic Routing Encapsulation** è un protocollo di livello 3 che si basa sul concetto di incapsulamento, il formato utilizzato è il seguente:

**Figura 5.17:** Formato del pacchetto

Possiamo notare alcuni campi dell'header:

- **C, R, K, S:** sono dei flag che indicano la presenza o l'assenza di alcuni campi opzionali.
- **s:** *strict source routing flag*, se il destinatario non è raggiunto quando la source route list termina, il pacchetto viene eliminato.
- **Recur:** massimo numero di volte che il pacchetto può essere incapsulato (deve essere 0).

- **protocol:** id del protocollo per il payload (*non è vietato metterci ulteriori protocolli*).
- **routing:** Sequenza di indirizzi dei router IP per ASs o per *source routing*.

5.4.1 Enhanced GRE (version 1)

Esiste una **versione estesa** di **GRE** denominata **version 1** che utilizza *PPTP* e aggiunge un *acknowledgment number* in modo da avere la garanzia di invio dei pacchetti al end-point remoto.

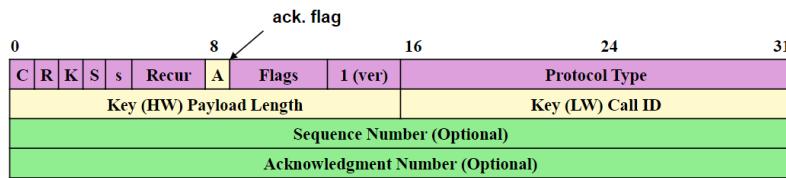


Figura 5.18: Formato di Enhanced GRE

Alcune funzionalità avanzate:

- **Payload Length** (key, 16 bit alti): numero di bytes a esclusione dell'header GRE.
- **Call ID** (key, 16 bit bassi): session ID per il pacchetto.
- **Sequence number:** per ordinare i pacchetti ricevuti, error detection e correction.
- **Acknowledgment number:** massimo numero di pacchetti GRE ricevuti in sequenza in questa sessione (ACK cumulativo).

altri meccanismi implementati in GRE comprendono:

- **Flow control:** gestione del flusso attraverso il meccanismo di *sliding window*.
- **Out of order packets:** Scartato, perché *PPP* consente pacchetti persi, ma non può gestire pacchetti fuori ordine.
- **Timeout values:** ricalcolato ogni volta che un pacchetto ack viene ricevuto.
- **Congestion control:** timeout non causa la ritrasmissione, è utilizzato solo per muovere la sliding window. I pacchetti verranno persi (*il loro valore dovrebbe essere aumentato rapidamente*).

5.5 Protocolli di livello 2

Nota: Questi protocolli di livello 2 non sono domande da esame. Cosa differente nel caso GRE e IPsec.

Per le **Access VPN** sono disponibili due protocolli:

- **L2TP** (Layer 2 Tunneling Protocol): inizialmente sono provider provisioner e non molto implementato sui terminali. E' indipendente dal protocollo di livello 2 sul host e la sicurezza è garantita da IPsec.
- **PPTP** (Point to Point Tunneling Protocol): customer provisioner, originariamente proposto da Microsoft, Apple... Ha una bassa encryption e autenticazione e utilizza un key management proprietario.

5.5.1 L2TP

Le due componenti principali sono:

- **L2TP Access Concentrator (LAC)**: accesso alla rete, NAS (Network access server).
- **L2TP Network Server (LNS)**: corporate VPN gateway

Customer provisioned deployment mode by including LAC functionality in host

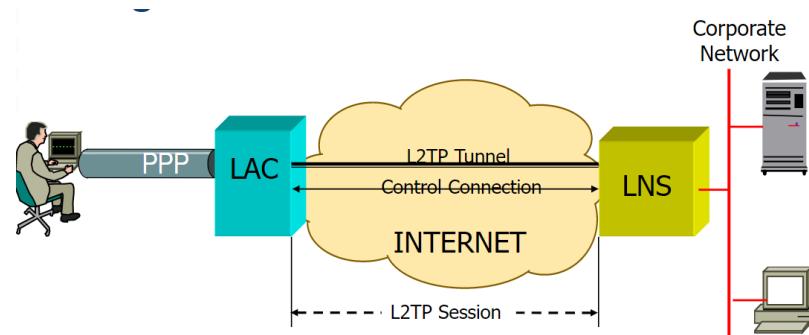


Figura 5.19: L2TP

Più connessioni potrebbero esistere nello stesso tunnel e più tunnel potrebbero essere stabiliti per lo stesso LAC e LNS o multipli LNS.

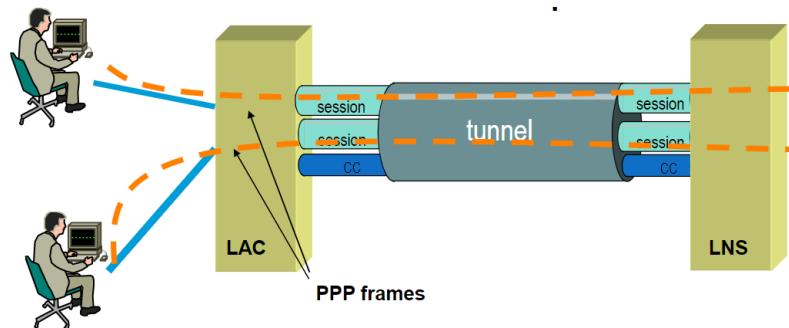


Figura 5.20: L2TP

Le operazioni l2TP compiute sono:

1. Stabilire una control connection per un tunnel tra lac e lns
2. stabilire una o più sessioni triggered da una call request

La control connection deve essere stabilita prima che la connection request sia generata, e una sessione deve essere stabilita prima di inviare nel tunnel i frame PPP.

Quando il tunnel viene stabilito, il peer può essere autenticato. Per fare ciò si condivide uno shared secret tra LAC ed LNS. L2TP utilizza un CHAP-like mechanism: ovvero si utilizza un challenge-response protocol per autenticare il peer. Il challenge viene generato dal peer che lo invia al peer remoto, il quale risponde con la risposta. Il peer remoto può verificare la risposta e quindi autenticare il peer. Il tunnel endpoint scambia infine il local ID attribuito al tunnel.

L'header del protocollo utilizza un meccanismo particolare:

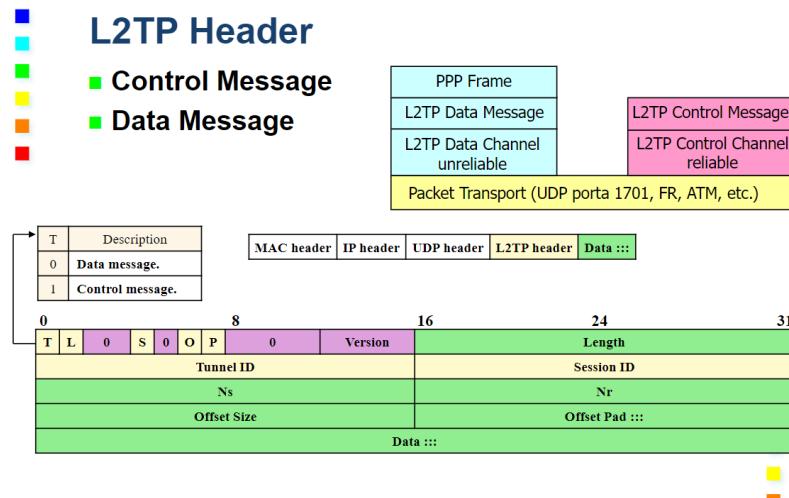


Figura 5.21: L2TP

i campi presenti sono:

- L, S, O
- P
- Ver
- Tunnel ID
- Session ID
- Ns
- Nr
- Offset

Le connessioni dati utilizzano un sequence number per individuare i pacchetti ricevuti fuori ordine. Non è presente la ritrasmissione di un flusso di dati e non vi è nessun ack per i data streams in

quanto altri protocolli di livello 2 possono preoccuparsi di 2. I control packets invece utilizzano ack e ritrasmissione mediante selective repeat, la windows tra Tx e Rx è settata a 32k.

Dal punto di vista della sicurezza, l'autenticazione avviene solo in fase di creazione del tunnel. Un utente potrebbe fare snoop del traffico, e iniettare pacchetti nella sessione. Il tunnel e session ID dovrebbero essere selezionati in un modo non prevedibile (non sequenzialmente).

Crittografia, autenticazione e integrità devono essere assicurati da un meccanismo di trasporto (es IPsec).

5.5.2 Point to Point Tunneling Protocol (PPTP)

Alcuni features:

- Adopted by IETF (RFC 2637)
- Tunneling of PPP frames over packetswitched networks
- Microsoft Encryption: MPPE
- Microsoft Authentication: MS CHAP
- PPTP Network Server (PNS)
- Corporate (VPN) gateway
- PPTP Access Concentrator (PAC)
- For provider provisioned deployment mode

Sono presenti due pacchetti, uno per la parte di controllo e una per il data tunneling.

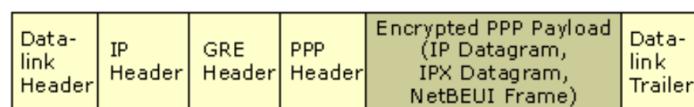


Figura 5.22: PPTP Data

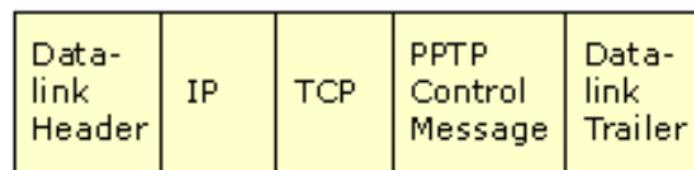


Figura 5.23: PPTP Control

5.6 IPsec

Nota: Questo è un argomento molto importante, spesso chiesto all'esame. È importante sapere cosa garantisce, a cosa serve ESP ed AH, le 3 proprietà ecc mentre è meno importante sapere dettagliatamente Transport mode, tunnel mode, come funziona.

Il protocollo **IPsec** si basa sull'utilizzo di due ulteriori protocolli: **AH** e **ESP**. **AH** è un protocollo che garantisce l'integrità dell'header originale e del payload, mentre **ESP** garantisce integrità ed autenticazione.

AH, acronimo di *authentication header*, garantisce l'integrità dei dati, l'autenticazione del sorgente ma non la confidenzialità. L'header è inserito tra l'header IP e il payload, con protocol field pari a **51**. I router processano datagrammi (non NAT).

Alcuni campi di AH sono i seguenti:

- **SPI:** Security Parameter Index, contiene il Session ID e viene utilizzato per verificare la signature mediante crypto algorithm e un riferimento alla chiave.
- **Authentication data:** contiene la signature generata dal router di destinazione.
- **Next header:** contiene il protocollo nel payload (es TCP, UDP, ICMP, etc).



Figura 5.24: AH header

ESP, acronimo di *_Encapsulation Security Payload*, garantisce la confidenzialità dei dati, i quali sono criptati insieme al next header nel ESP trailer. Inoltre, consente l'autenticazione dell'host e l'integrità dei dati, mediante una autenticazione simile a quella di AH. Il protocol field è **50**.

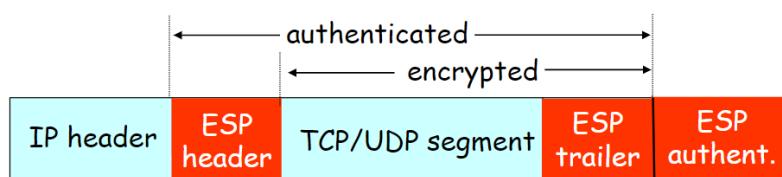


Figura 5.25: ESP header

La differenza tra l'integrità garantita da AH ed ESP risiede nel tipo:

- AH: garantisce l'integrità dell'header originario, del payload originario e del nuovo header.
- ESP: garantisce solo l'integrità dell'header originario e del payload originario, **non** riuscendo per il nuovo header.

Un tunnel IPsec è perciò capace di garantire **incapsulazione, autenticazione e cifratura** tra due VPN gateways.

Dal punto di vista del trasporto, l'header IP non è completamente protetto ma solo autenticato se si utilizza AH.

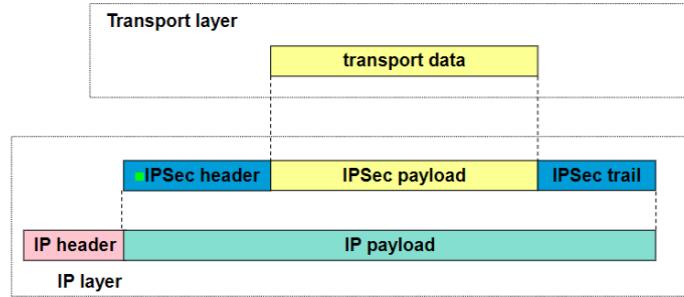


Figura 5.26: Header non completamente protetto

Le cose cambiano se la trasmissione avviene tramite tunnel, in questo caso l'header IP è completamente protetto sia nel header che nel payload.

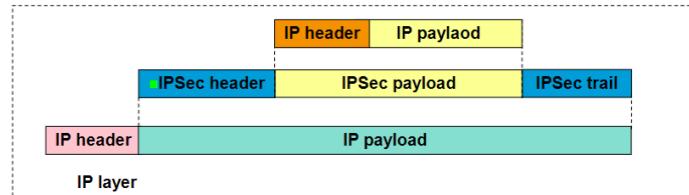


Figura 5.27: Tunnel Mode

Le **Security Association** (SA) sono canali logici unidirezionali. Questi negoziano alcune informazioni prima di cominciare lo scambio di pacchetti IPsec. Sono identificate mediante dei Security Parameter Index (SPI) nel header/trailer IPsec (in base alle proprietà di sicurezza richieste).

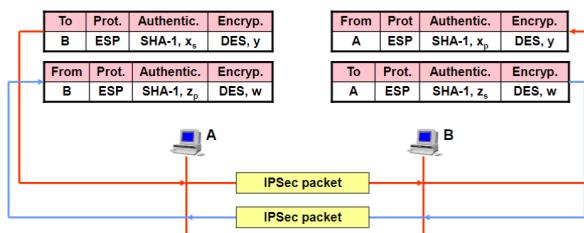


Figura 5.28: Security Association

Il protocollo **Internet Key Exchange** (IKE) viene utilizzato per stabilire e mantenere le SA in ipsec, al fine di ottenere una comunicazione sicura per lo scambio dei messaggi IKE. Al fine di far avvenire una

comunicazione sicura dei dati, vengono utilizzati uno o più SA “figli”. Tutte le SA figlie utilizzano la negoziazione di chiavi tramite IKE SA (potrebbero tutti partire da uno shared secret), con la possibilità di utilizzare certificati. In particolare si parla di **Internet Security Association Key Management Protocol** (ISAKMP), utilizzato per la negoziazione di parametri IKE e dello shared secret, oltre a chiavi pubbliche, certificati e dati firmati ed autenticati (e verifica della Certificate Revocation List, CRL).

5.7 SSL VPN

Il protocollo SSL è il meccanismo centrale su cui si basa l'accesso sicuro. Sono:

- site to site VPN
- remote access VPN
- Secure service access (sarebbe e2e)

Spesso si perde il termine “VPN” o viene aggiunto “pseudo VPN”, in quanto il meccanismo cambia rispetto al modello classico. Il modello di trasporto è sempre TCP o UDP.

Uno dei principali problemi risiede nel fatto che vengono adoperate soluzioni non standard, per cui essendo utilizzati protocolli proprietari diventa più complicato.

Il motivo per non utilizzare IPSec VPN risiede nei costi troppo elevati e/o nelle troppe opzioni che necessitano una configurazione per garantire sicurezza. Un ulteriore motivo potrebbe essere il fatto che opera a livello kernel, per cui installazioni sbagliate possono avere conseguenze catastrofiche (oltre a installazioni difficili e rischiose).

Utilizzare SSLVPN ha come vantaggio:

- **Minore complessità** (installazione, configurazione, gestione)
- **Non interferisce con il kernel**
- **Molto più utilizzato**
- **Maggiore e più robusta sicurezza** (SSL)
- Non ci sono problemi di attraversamento del nat o di mascheramento (non è presente l'autenticazione del header IP e non è presente la cifratura delle porte come con ESP)

Il grosso svantaggio è però che i pacchetti vengono droppati a un livello più alto, rendendolo vulnerabile ad attacchi DDOS.

Alcune insidie sulle prestazioni:

- **IP su TCP:** Nessuna consegna di pacchetti dopo uno smarrito, inoltre la perdita comporta la strozzatura del tunnel (Controllo della congestione TCP). -**TCP su TCP:** imprevedibile, ampi buffer di trasmissione nei gateway.

Le principali problematiche sono:

- **interoperabilità**: client e server devono installare lo stesso software.
- **features specifiche** del produttore.
- Ogni implementazione potrebbe avere **bug** (perchè soluzioni proprietarie).
- **Disponibilità** del client sulle specifiche piattaforme.

Per questo motivo le chiamiamo “pseudo VPN”. Le VPN ipsec connettono reti, host a reti, o host a host. Invece, le SSLVPN connettono utenti a servizi o client application a server application.

Riassumendo: Le SSLVPN utilizzano tunneling TCP o UDP, forniscono NAT traversal, packet filter traversal, router traversal e utilizzano client universali (web browser).

Alcune soluzioni utilizzano schemi di protezione simili a protezioni vpn di livello 3.

Nelle soluzioni Pseudo VPN rientrano:

- Protocolli con SSL
- Application translation
- Port Forwarding
- Web proxying
- Application proxying

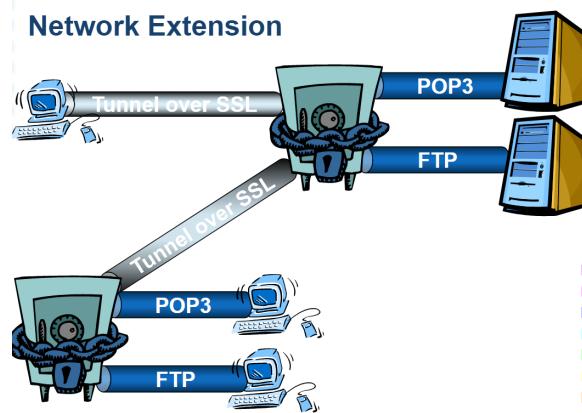


Figura 5.29: Network Extension

5.7.1 Protocolli con SSL

I protocolli che utilizzano SSL sono definiti **secure application protocol**, richiedono i supporto del client e del server e hanno un funzionamento del tipo Protocol-over-SSL (POP-over-SSL, IMAP-over-SSL, SMTP-over-SSL).

Nota: la filosofia che vi è dietro è di utilizzare in modo “standard” e meno protetto il protocollo nativo, che verrà richiamato dall'esterno attraverso un'interfaccia sicura SSL.



Figura 5.30: Protocolli con SSL

5.7.2 Application Translation

La **Application Translation** sfrutta protocolli nativi tra il VPN server e l'application server (FTP, SMTP, POP), sfruttando un'applicazione come user interface (ad esempio web page). Il gateway spezza in comunicazione sicura e non sicura. Inoltre, è presente HTTPS tra VPN Server e Client. Non è una soluzione adatta per tutte le applicazioni.

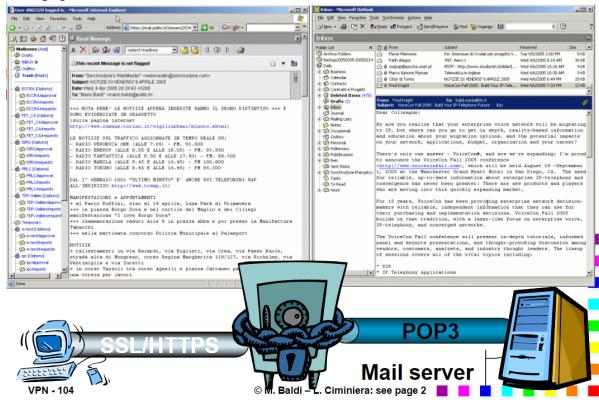
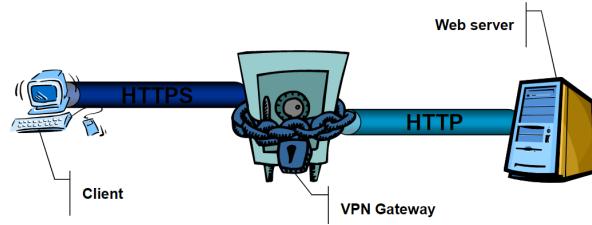
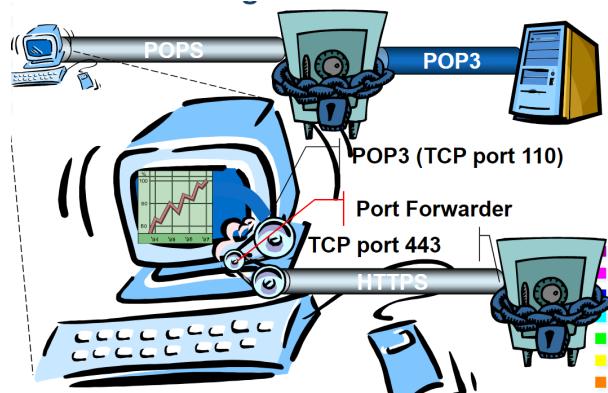


Figura 5.31: App translation

5.7.3 Application Proxying

L'**Application proxying** utilizza VPN gateway per scaricare le webpage attraverso http e le invia tramite https. Consente la compatibilità con server vecchi. I client puntano a un SSL-VPN gateway.

**Figura 5.32:** Application Proxying**Figura 5.33:** Port Forwarding

5.7.4 Port Forwarding

5.8 VPN Gateway Positioning & anomalies

Sono inoltre importanti gli aspetti inerenti ai firewall. Questo può essere messo:

- dentro: nessuna ispezione del traffico VPN, il gateway è protetto dal firewall
- in parallelo: potenziale accesso senza controllo
- fuori: VPN gateway protetto dal access router, policy consistente
- integrato: massima flessibilità

5.9 Posizione

La posizione del VPN comporta delle problematiche differenti a seconda di dove viene posizionato (in riferimento al firewall):

- **Internamente:** nessuna ispezione del traffico VPN oppure il VPN gateway protetto da firewall.
- **Parallelamente:** potenziale accesso non controllato.

- **Esteramente:** il vpn gateway potrebbe essere protetto da un access router, Consistent policy.
- **Integrato:** Massima flessibilità.

Soltanente vengono posti degli Intrusion Detection System (IDS) all'esterno del firewall senza controllo del traffico VPN e dopo il VPN gateway.

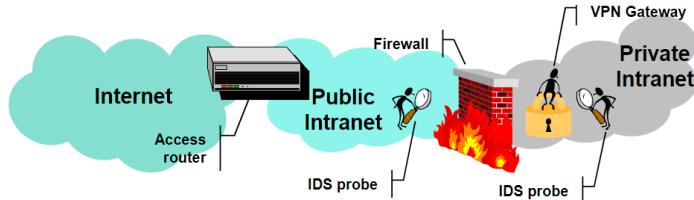


Figura 5.34: IDS

5.10 Anomalie

Le anomalie che si possono verificare nell'utilizzo delle VPN sono varie e dipendono dal contesto:

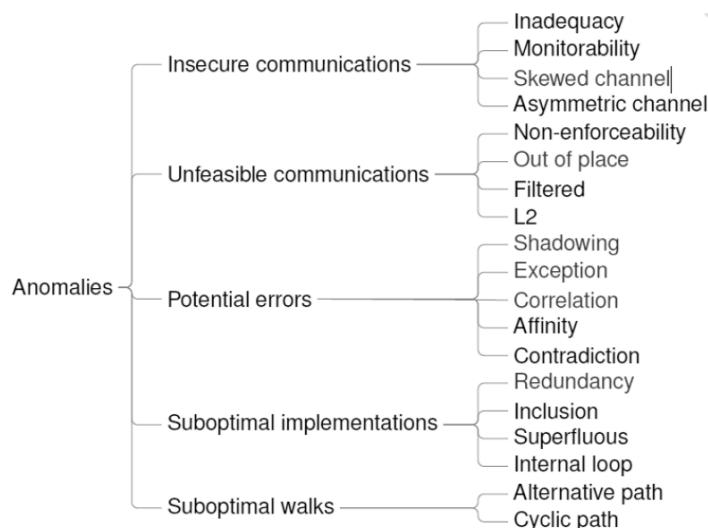


Figura 5.35: Anomalie

5.10.1 Monitorability Anomaly

Si ha un **Monitorability Anomaly** quando un nodo del canale “congiunto” può vedere lo scambio dei dati.

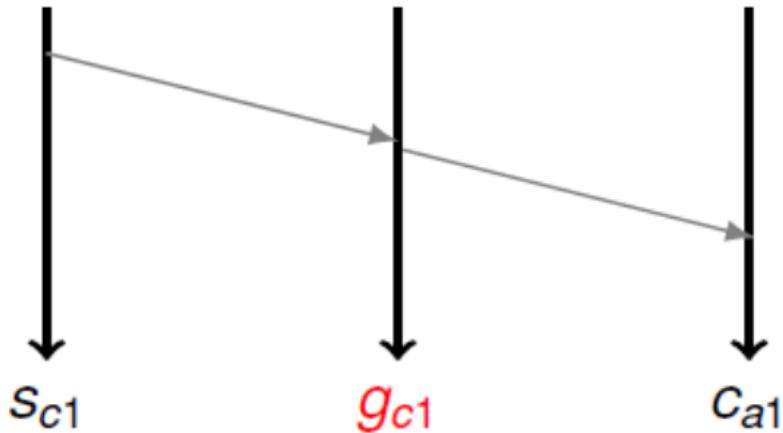


Figura 5.36: Monitorability Anomaly

5.10.2 Skewed Channel anomaly

Si ha uno **Skewed Channel Anomaly** quando si ha una sovrapposizione errata dei tunnel che rimuove la confidenzialità nella comunicazione. Dunque anche avendo più livelli di sicurezza, se configurato male si può avere un problema di confidenzialità e non avere nessuna sicurezza.

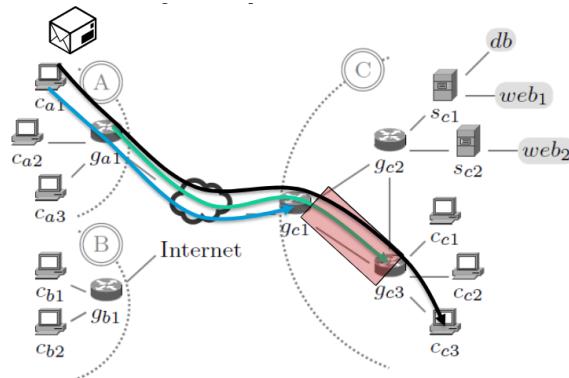


Figura 5.37: Skewed Channel

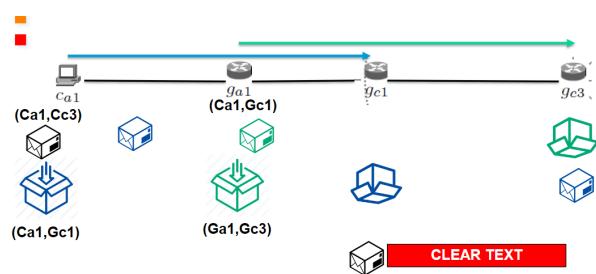


Figura 5.38: Skewed Channel

6 Routing

6.1 Introduzione

Con il termine **routing** si fa riferimento al percorso che i pacchetti devono compiere nella rete, mentre **forwarding** il processo di inviare pacchetti nella rete, includendo decisioni di routing.

Distinguiamo il concetto di:

- **routing** (proactive)
- **forwarding** (on the fly routing)

6.1.1 Proactive routing

Il **proactive routing** è indipendente dal traffico attuale, definisce quale percorso è migliore rispetto a un altro (in base a una metrica scelta). Determina inoltre quali siano le destinazioni raggiungibili.

Nota: è solitamente chiamato semplicemente *routing*.

6.1.2 On the fly routing

Comunemente definito **forwarding**, il **On the fly routing** si occupa di gestire i pacchetti mediante informazioni locali come routing/forwarding table. E' il risultato del proactive routing o signaling.

La scelta dipende dal tipo di indirizzamento che si vuole stabilire:

- **routing by network address**: routing in base alla destinazione
- **label swapping** (es. MPLS)
- **source routing**

Si ha una operazione di switching, ovvero trasferire verso una porta di output, oltre che di trasmissione. Ogni protocollo può adoperare una o più di queste strategie.

Nota: è solitamente chiamato semplicemente *route*.

6.2 Proactive routing algorithms

Gli algoritmi di routing proactive si dividono in:

- **non-adaptive algorithms**: statici
- **adaptive algorithms**: dinamici

6.2.1 Non adaptive algorithms

I **non adaptive algorithms*** si dividono a loro volta in **Fixed Directory routing**, il quale compie static routing ed è configurato manualmente, e il **flooding and derivates** (selective), anche questo con approccio statico che non cambia in base alla rete.

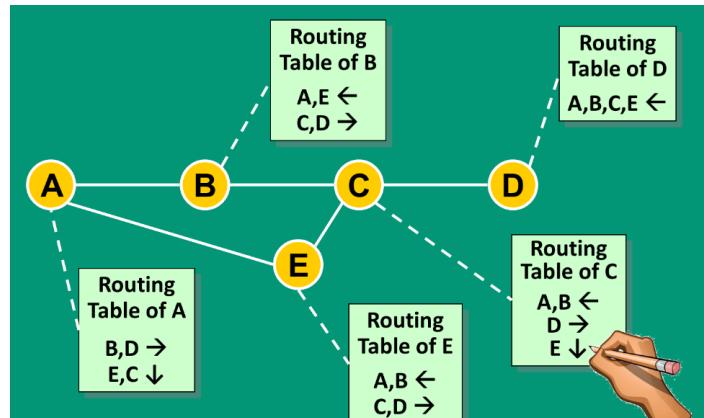


Figura 6.1: Fixed Directory Routing

Il vantaggio principale è il pieno controllo della rete da parte dell'amministratore, ma al costo di essere più soggetti ad eventuali errori e di un architettura che non si adatta al cambio di topologia.

6.2.2 Adaptive algorithms

Gli algoritmi dinamici si dividono in:

- **centralized routing**
- **isolated routing**
- **distributed routing**, distance vector e link state

In riferimento al **centralized routing**, un unico nodo si occupa di gestire la rete denominata **Routing Control Center** (RCC). Ha bisogno di sapere le informazioni di tutti i nodi per prendere le strategie di routing migliori e ottimizzare le performance. Inoltre, effettua il calcolo e la distribuzione delle

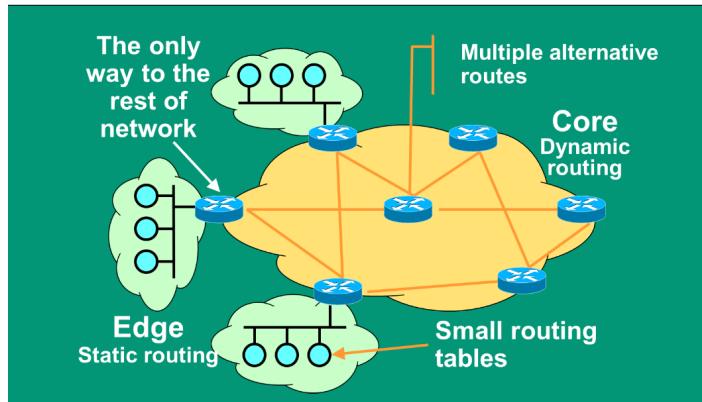


Figura 6.2: Statico vs Dinamico

routing table. Il vantaggio è che semplifica il troubleshooting anche se è presente un carico di rete significativo in prossimità del RCC. Lo svantaggio è però il rischio che RCC diventi un bottleneck o un single point of failure, per tale motivo non è adatto per reti dinamiche di grandi dimensioni.

Nella **isolated routing** ogni nodo si comporta in modo indipendente senza alcun scambio di informazione. Non si ha dunque garanzia che il pacchetto venga effettivamente trasmesso. Uno scenario plausibile è in una rete lineare.

Nell'approccio **distributed routing** i router collaborano nello scambiare le informazioni sulla connettività. Ciascun router decide indipendentemente, ma in modo coerente. Combina i vantaggi e svantaggi rispetto ai due approcci precedenti.

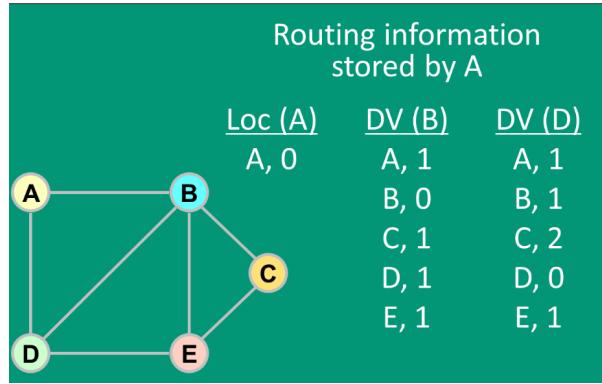
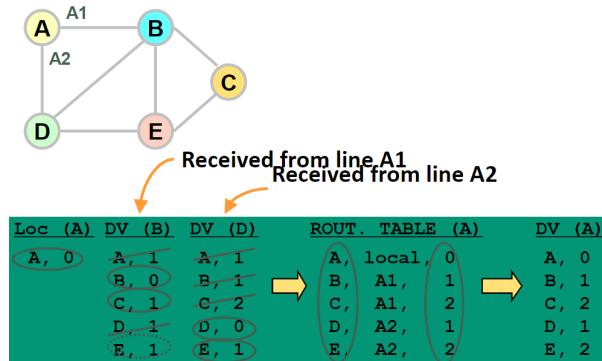
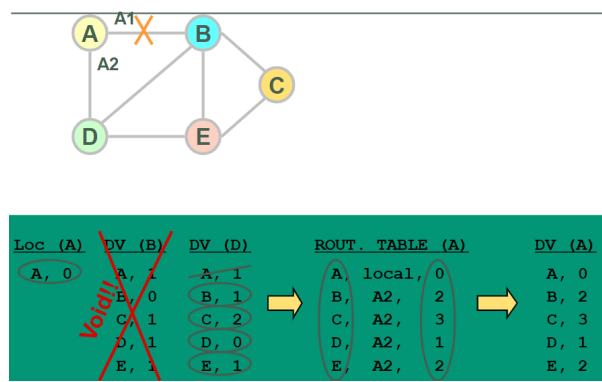
6.3 Distance vector (Bellman-Ford)

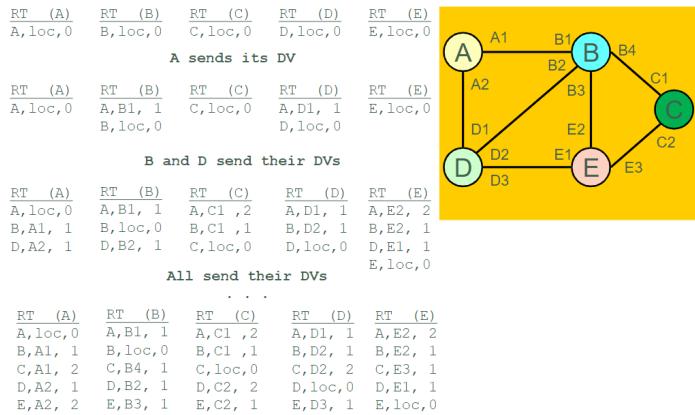
Nel algoritmo **Distance Vector** (DV), facente parte dei *distributed routing (adaptive algorithms)*, ogni nodo invia e riceve informazioni inerenti alla distanza con gli altri router ai nodi vicini. E' un algoritmo distribuito in cui ogni nodo ha la lista completa dei destinatari (tutti). Sono inoltre necessari i transitori (router che non sono destinatari ma che sono necessari per raggiungere la destinazione). Visto che ogni nodo comunica con i vicini, è importante tenere conto della distanza dal announcing routing.

L'algoritmo cerca ogni volta la distanza minore per raggiungere un determinato nodo, tenendo conto dei percorsi alternativi in caso di guasto.

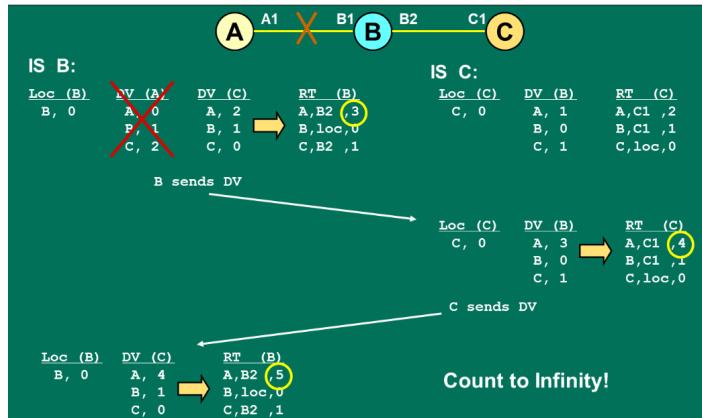
All'inizio ogni router ha solo le informazioni in locale, deve dunque mandare le proprie informazioni ai vicini in modo che si possa propagare nella rete la possibilità di poter raggiungere il nuovo nodo, ad esempio a. Il routing avviene a livello 3.

I problemi che si possono riscontrare sono:

**Figura 6.3:** Scenario d'esempio (1)**Figura 6.4:** Scenario d'esempio (2)**Figura 6.5:** Scenario d'esempio (3) con cambio di topologia

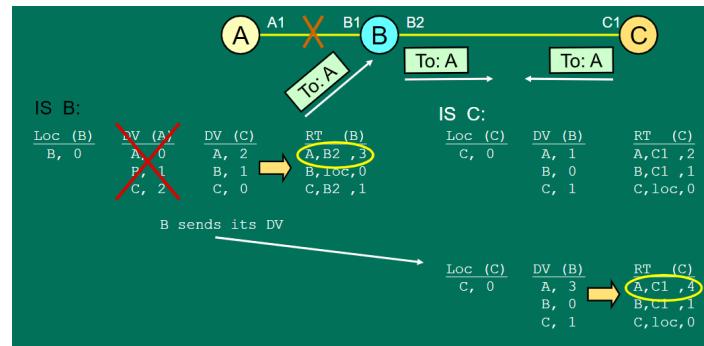
**Figura 6.6:** Cold Start

- **Black hole:** un nodo non risponde ai messaggi di routing, quindi non si ha più informazioni sulla rete.
- **Count to infinity:** scenario di loop, le informazioni sono propagate all'infinito.
- **Balancing effect:** se un nodo è più vicino ad un altro, ma il percorso è più lungo, allora il nodo più vicino non sarà scelto.

**Figura 6.7:** Esempio count to infinity

Alcune soluzioni a tali problematiche sono:

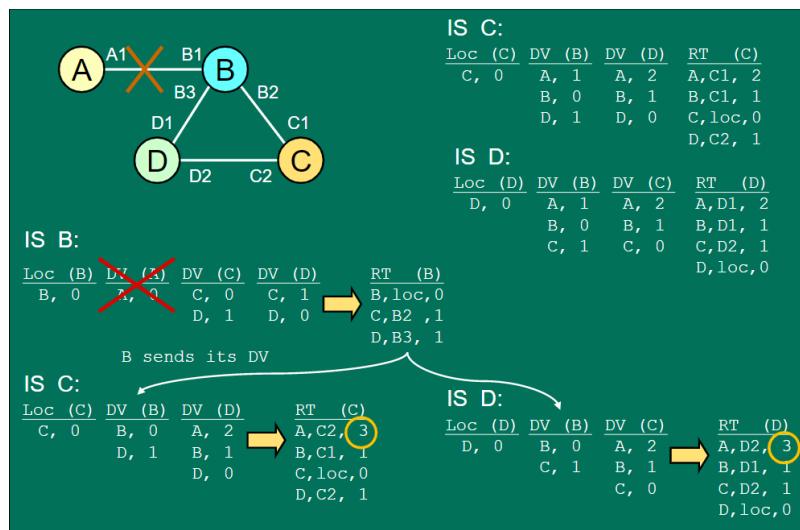
- **Split horizon:** se C raggiunge A mediante B, è inutile per B provare a raggiungere A tramite C. Previene cicli tra due nodi, velocizza la convergenza e consente di “personalizzare” le DV per i vicini. Non risolve tutti i problemi quando abbiamo delle maglie chiuse (*mesh*). Nelle attuali implementazioni la route deve “scadere” dopo un po’ di tempo.
- **Path hold down:** se un link L fallisce, le destinazioni raggiungibili da L vengono considerate non raggiungibili per un certo periodo di tempo (*in quarantena*). Ha un tempo di copertura elevato

**Figura 6.8:** Esempio bouncing effect

e i router che hanno notato l'errore potrebbero non partecipare a un loop fino a quando non è scaduto un *Hold Down timer*.

- **Route poisoning:** invia una informazione volutamente scorretta (invece di ometterla) al fine di scoprire prima cosa succede nella rete, alla ricerca di guasti. Quando il link fallisce il costo è incrementato, fino a quanto non si raggiunge il costo massimo (denominato infinito) e si ricerca un altro percorso. Il tempo di convergenza è più rapido e può sostituire o essere complementare al *path hold down* e *split horizon*.

Più varianti sono possibili contemporaneamente, in base al protocollo che viene utilizzato.

**Figura 6.9:** Split Horizon su mesh

I vantaggi complessivi sono dunque la semplicità di implementazione è la semplicità di deploy per i protocolli, senza necessitare particolare configurazione.

I *routing loops* si verificano quando le *routes* hanno un incremento di costo, per questo motivo non

vengono utilizzate (sono identificate da due advertisements successivi). E' possibile che succeda con il path hold down, potrebbero essere bloccate route con un incremento legittimo dei costi.

Un esempio di utilizzo può essere *Split Horizon with Poisonous Reverse*, che risulta essere più aggressivo e consente di non aspettare per la *expiration* di una *route*.

Il caso più estremo ci consente di fare in modo che i router non siano a conoscenza della topologia della quale fanno parte.

Il vantaggio di tali soluzioni è la semplicità di implementazione, protocolli facili per il *deploy* con poche configurazioni.

La complessità nel caso peggiore relativo al tempo di convergenza va da $O(n^2)$ a $O(n^3)$, risulta inoltre limitata dai router più lenti e il set space dei router. Anche il numero di link presenti risulta essere un fattore limitante in termini di prestazioni.

6.4 Path Vector

L'algoritmo **Path Vector** elimina i loop inviando, in aggiunta alle informazioni sulla distanza, i nodi attraversati per raggiungere una determinata destinazione. In questo modo si evitano i loop all'interno dei transitori, ma nonostante ciò è molto utilizzato in quanto è un compromesso con gli svantaggi di entrambi.

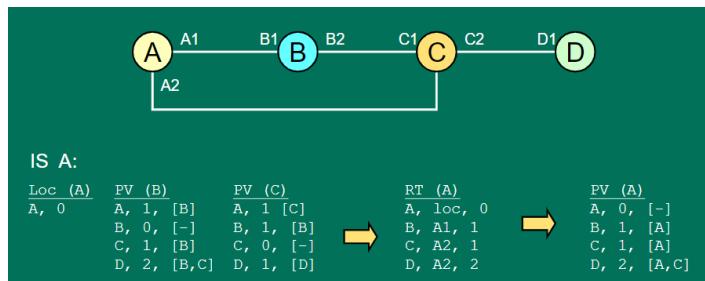


Figura 6.10: Esempio di Path Vector

6.5 Link State Routing Algorithm

Nel **Link State Routing Algorithm** vengono inoltrate le informazioni relative a tutta la rete, contenente lo stato di ogni nodo. In questo modo ogni nodo è in grado di realizzare una mappa locale, inviando le informazioni attraverso un *selective flooding*.

In questo modo la convergenza è rapida e i *link state* sono piccoli. Il traffico di rete e lo storage sono limitati, in quanto il *neighbor greeting* è veloce ed efficiente. Raramente genera loop ed è semplice da comprendere e “riparare”, ma è più complesso da implementare, cosa che comporta protocolli con configurazioni complesse.

I *link state* vengono generati quando avvengono cambiamenti topologici. Nei protocolli attuali i link state sono generati periodicamente in modo da aumentare l'affidabilità.

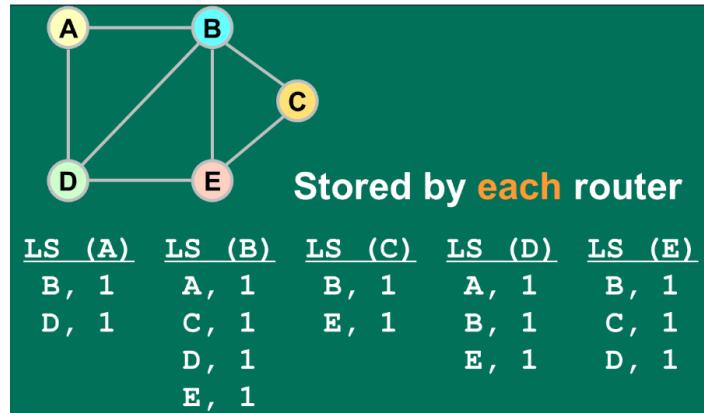


Figura 6.11: Link state database

6.6 Algoritmo di Dijkstra

L'**algoritmo di Dijkstra** viene utilizzato per calcolare l'albero di copertura minima di un grafo. Ha una bassa complessità pari ad $O(L \log n)$, con L numero di link ed n numero di nodi. Utilizza un meccanismo di **shortest path first**, dove il prossimo nodo è il più vicino alla sorgente e il next hop è inserito all'interno della routing table.

I vantaggi sono una rapida convergenza (i LS sono analizzati rapidamente e non c'è processazione intermedia) oltre a un limitato storage e routing del traffico (Link State piccoli e rapido *neighbor greeting*). Inoltre, raramente genera loop ed è semplice fare troubleshoot (tutti i nodi hanno un database identico).

6.7 Internet Routing Architecture

I protocolli di routing viaggiano tra il livello IP e il livello TCP. Un protocollo di routing è il modo con cui si determina le rotte per lo scambio di informazioni attraverso una rete, basandosi su un algoritmo di routing di partenza.

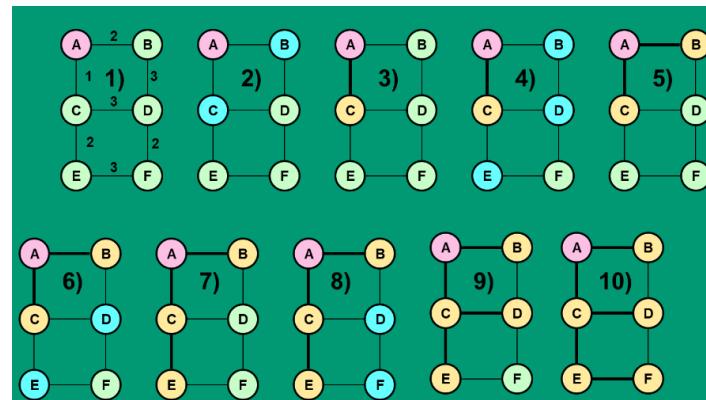


Figura 6.12: Esempio con Dijkstra

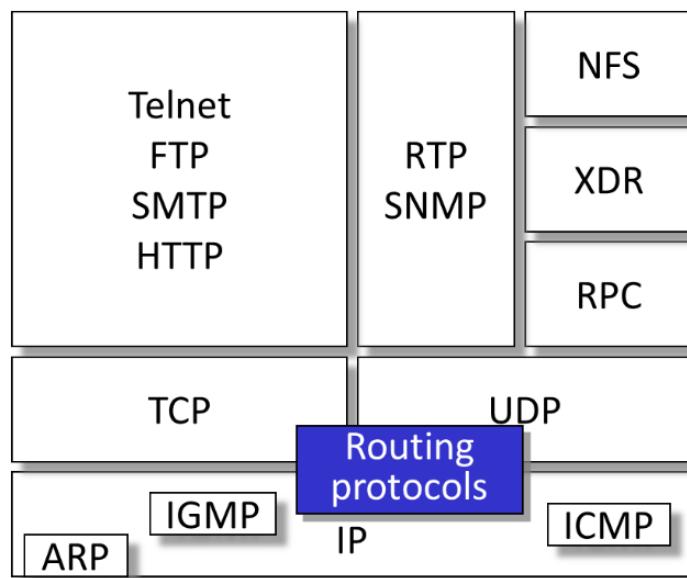


Figura 6.13: Protocol Architecture

Per i routing protocol è necessario definire delle metriche, il meccanismo di encoding per il pacchetto, i parametri configurabili e lo specifico timing.

Il **dominio di routing** è un insieme di router che utilizzano lo stesso protocollo di routing, che sono connessi a una porzione della rete. Un router potrebbe far parte di più routing domains (utilizzando più protocolli di routing) e può **ridistribuire** le informazioni imparate con un protocollo mediante uno differente. Questo processo è possibile attraverso una conversione delle metriche, utilizzo di filtri di advertisement e *information source priority* tramite una configurazione dell'amministratore.

6.7.1 Autonomous System

Un **Autonomous System** (AS) è un set di sottoreti raggruppate in base alla topologia o un criterio organizzativo (ad esempio una subnet di un grande ISP). L'indirizzamento e l'instradamento sono strettamente coordinati e l'interfaccia AS è controllata (data, informazioni di routing). Dal punto di vista amministrativo è possibile indicare delle scelte di routing interno autonome e negoziare scelte di routing esterno. È scalabile, in quanto nessuna delle informazioni è propagata “ovunque” ma è il singolo AS a decidere dove far passare i propri dati.

E' identificato da **due byte** numerici assegnati dalla IANA (*Internet Assigned Numbers Authority*). Il range di numeri privati va da 64512 a 65534, lo scambio di informazioni di routing è controllato.

Distinguiamo i protocolli di tipo **iBGP** (*intra Border Gateway Protocol*) e **eBGP** (*inter Border Gateway Protocol*). Il primo è utilizzato per comunicare tra i router di un AS, mentre il secondo è utilizzato per comunicare tra AS diversi.

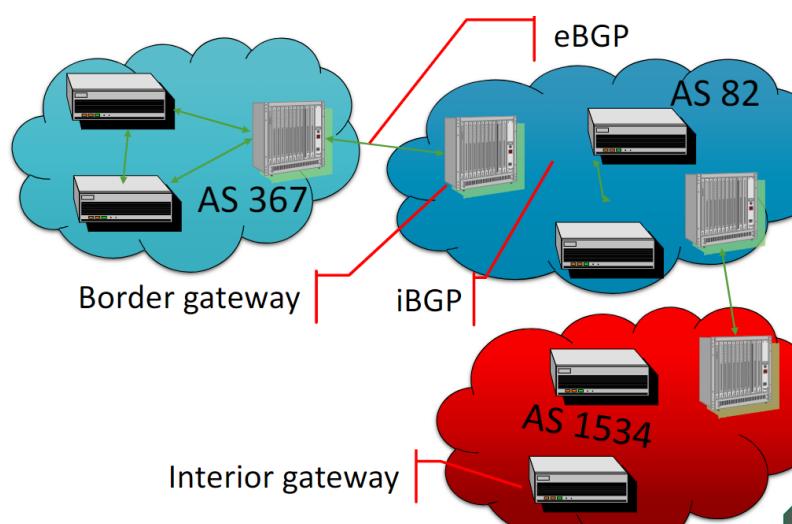


Figura 6.14: iBGP e eBGP

Il concetto di percorso più breve non è più applicabile nel caso dell'*exterior routing*, ma bensì si parla

di percorso *migliore* (che non necessariamente è relativo alla lunghezza). Le scelte vengono fatte in base a delle *policies* e riflette gli accordi tra gli AS.

Le destinazioni possono essere aggregate (195.1.2.0/24 e 195.1.3.0/24 in 192.1.2.0/23) secondo un routing *gerarchico*.

Neutral Access Point (NAP) è un punto di accesso neutrale, che permette di collegare più AS tra loro, mentre un Internet eXchange Point (IXP) è un punto di scambio di traffico tra più AS. Sono realizzabili mediante BGP.

!Implementazione con BGP](./images/06_nap_ixp.png){width=400px}

6.8 Protocolli di routing

I protocolli di routing si distinguono in **IGP** (Interior Gateway Protocol) e **EGP** (Exterior Gateway Protocol).

Le *feature* di **IGP** sono:

- Informazioni distribuite nella topologia
- Le route sono scelte in base alle informazioni della topologia

Le *feature* di **EGP**:

- informazioni degli Autonomous System distribuite
- Costi amministrativi distribuiti
- Decisioni prese in base alle *policies* (trova la route “preferita”, non necessariamente la migliore)

6.8.1 Algoritmi IGP

Gli algoritmi di tipo *Interior Gateway Protocol* si distinguono in:

- **Distance Vector**: comprende **RIP** (Routing Information Protocol) e **IGRP** (Interior Gateway Routing Protocol).
- **Link State**: comprende **OSPF** e Integrated **IS-IS**.

Tali algoritmi consentono di utilizzare differenti metriche rispetto all'hop count, come: delay, bandwidth, reliability, load, maximum packet length. Inoltre, consentono il **multipath routing**, ovvero la possibilità di utilizzare più percorsi per raggiungere una destinazione.

6.8.1.1 RIP (Distance Vector)

Rip è stato il primo protocollo di routing proposto, di tipo distance vector, nel 1988. Veniva supportato da macchine Unix e Linux. Come metrica utilizza *Hop Count*, con un tempo di convergenza di 3 minuti e un massimo di distanza di 15 hop.

6.8.1.2 IGRP (Distance Vector)

E' un sistema proprietario di Cisco, ch supera alcuni dei problemi di RIP, diventandone l'unica alternativa nel primo periodo.

6.8.1.3 OSPF (Link State)

OSPF fa parte degli algoritmi di *link state*, utilizza un routing di tipo gerarchico. Il routing domain è diviso in aree, in ciascuna delle quali avviene una aggregazione delle informazioni. I router sanno tutti i dettagli delle zone/domain/area, ma non sanno nulla o hanno informazioni limitate relative all'esterno. Può essere iterato.

Nello *strictly hierarchical routing* non si hanno informazioni sull'esterno. Quando il destinatario del pacchetto non è nella stessa area, viene eseguito il forwarding mediante un edge router. Il routing è limitato in termini di efficacia, ma è altamente scalabile. I path sono *sub-ottimali*, ma si ha perdita di connettività in caso di errori.

Nel *loosely hierarchical routing* si ha minore scalabilità in quanto i router devono mantenere e scambiare più informazioni, ma non è richiede *strictly hierarchical addressing*. Tutti gli host nel *dominio B* non hanno bisogno di un identificatore comune, bensì vengono utilizzati dei prefissi. E' possibile implementarlo in IPv4.

Ogni area avrà una visione completa della propria topologia interna, ma verso l'esterno soltanto i collegamenti per parlare con le altre aree, avendone una visione aggregata conoscendone i router di *frontiera*.

Per N router si hanno N^2 adiacenze (dunque link). La complessità di Dijkstra è lineare nel numero di link.

6.8.1.4 IS-IS (Link State)

L'algoritmo **IS-IS** è una variante del protocollo **OSPF**, oltre a essere una estensione del protocollo *OSI*. Utilizza routing di tipo gerarchico con diversi livelli. Viene ancora utilizzato, ma non è più diffuso nelle nuove strutture (soppiantato da OSPF). Ha avuto utilizzo in grandi reti e *ISP*.

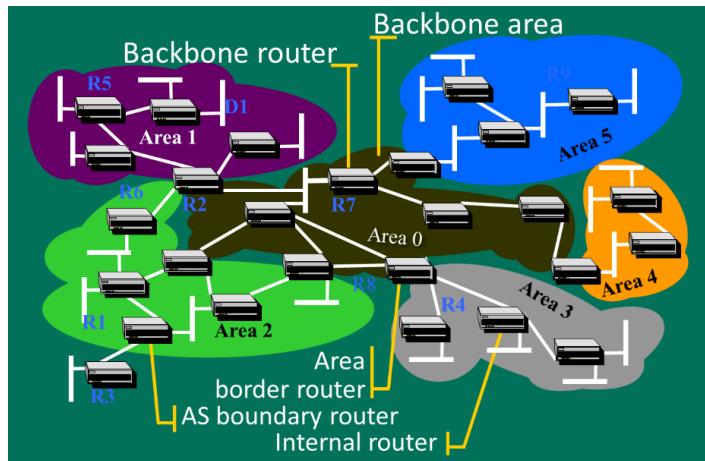


Figura 6.15: OSPF

6.8.2 Algoritmi EGP

Gli algoritmi di tipo *Exterior Gateway Protocol* sono **BGP** (Border Gateway Protocol) e **IDRP** (Inter Domain Routing Protocol). Anche il routing statico è una opzione possibile. Questi non sono né completamente distance vector né link state.

6.8.2.1 BGP

BGP è attualmente alla versione 4. Utilizza Path vector dove le destinazioni sono una sequenza di Autonomous System attraversati. È ricco di attributi ed è possibile configurare la route computation policy.

Il *vector exchange* avviene su TCP (per maggiore affidabilità) solo a seguito di un cambiamento. Vengono create delle sessioni tra *vicini* per lo scambio di informazioni mediante una configurazione specifica, senza la necessità per la connettività diretta.

6.8.2.2 Inter Domain Routing Protocol (IDRP)

L'algoritmo **IDRP** utilizza TCP/IP e rappresenta un'evoluzione di BGP per OSI. Doveva essere “la” soluzione per IPv6, ma nel concreto non è molto utilizzato.

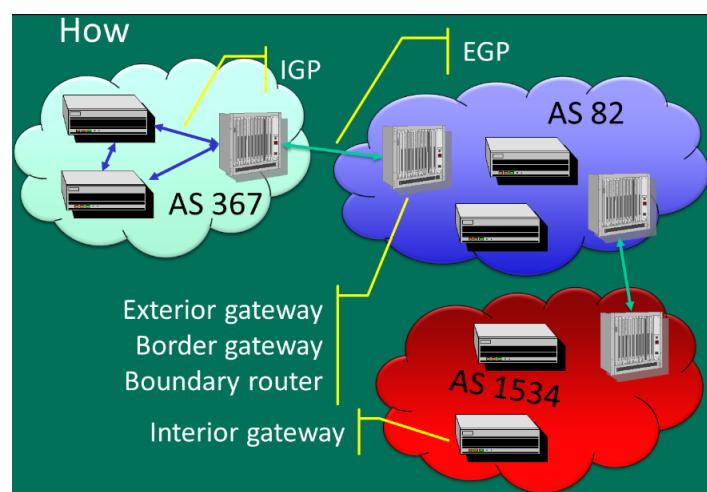


Figura 6.16: BGP

7 MPLS

MPLS è una tecnologia importante in quanto permette la realizzazione di un nuovo tipo di rete pubblica basata su IP, dove con rete pubblica si intende una rete con traffico di diversi utenti e aziende su cui è possibile vendere dei servizi.

Una struttura utilizzata molto in passato era a “cipolla”, con vari strati di livelli protocollari che comunicano tra di loro per implementare varie funzionalità. Ciò comportava però una conoscenza orizzontale da parte dei tecnici su più tecnologie che dovevano comunicare tra di loro.

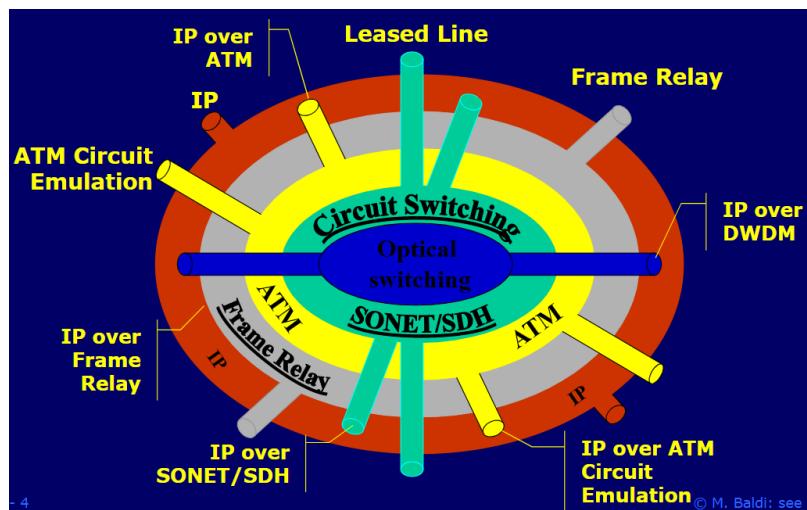


Figura 7.1: Struttura a cipolla

MPLS consente di eliminare questa struttura utilizzando un solo livello protocollare, abbattendo i costi degli operatori.

L'inoltro dei pacchetti avviene attraverso l'aggiunta di una **etichetta**, in base alla quale il routing effettua il forwarding invece di guardare l'indirizzo IP di destinazione. Il motivo di questo approccio risiede nella maggiore rapidità: se utilizzassimo l'indirizzo di destinazione bisognerebbe eseguire il max prefix routing cercando il prefisso più lungo nel quale l'indirizzo IP di destinazione è contenuto (tabelle molto grandi). Oggi è ancora molto utilizzata per il *traffic engineering*, ovvero distribuire il traffico della rete.

Quello che fa MPLS è dunque far diventare IP *connection oriented*. Lo svantaggio di tale approccio è la

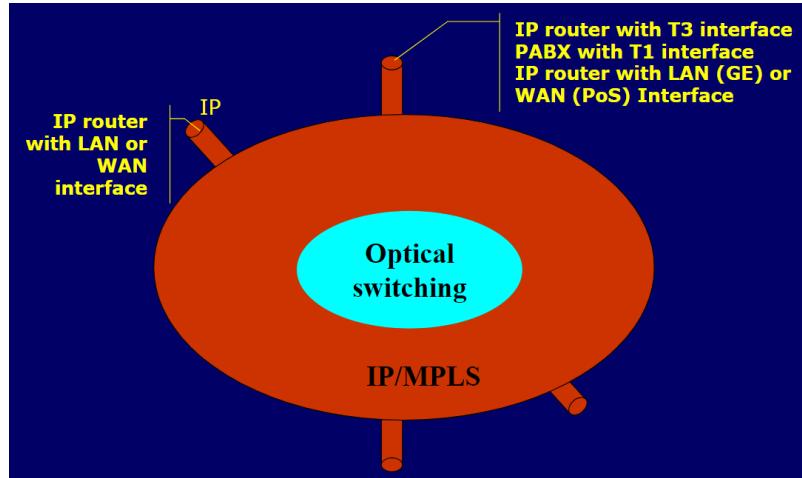


Figura 7.2: La promessa di MPLS



Figura 7.3: Etichetta

necessità di creare una connessione per la comunicazione per poi eliminarla, ma aver implementato IP in modo connection-less ha però generato dei problemi più grandi.

7.1 Architettura di rete

MPLS non utilizza gli *end system* e può essere utilizzato in una porzione di una rete, denominata **MPLS Cloud** (non ha correlazione con il cloud computing).

Osservando l'immagine si può vedere:

- **LSR:** Label Switching Router.
- **Label Edge Router:** router che non ha altri router MPLS collegati.
- **LSP:** label switch path, è un percorso di comunicazione attraverso cui viaggiano i pacchetti.

L'etichetta viene cambiata a ogni nodo, in modo da mantenere una etichetta più corta e poterla riutilizzare senza dover mettere d'accordo i nodi. Questa tecnica prende il nome di **label switching** e consente di ottenere scalabilità.

Gli elementi chiave di MPLS sono:

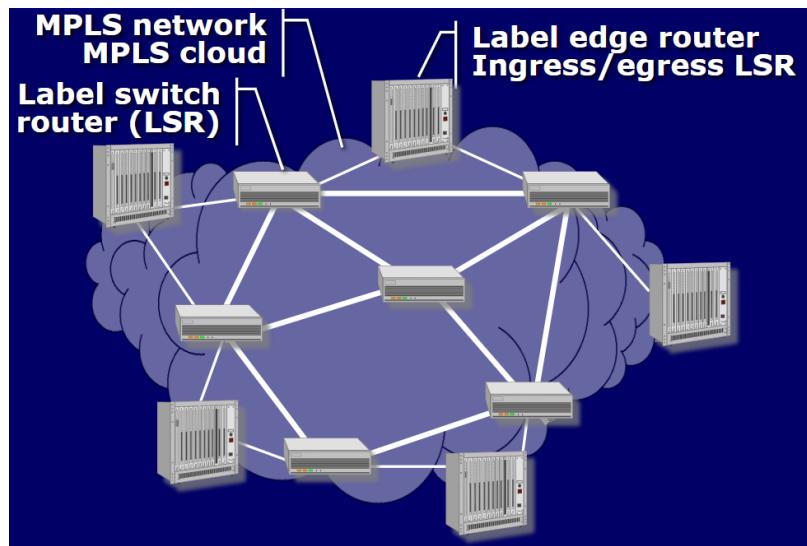


Figura 7.4: Architettura di rete

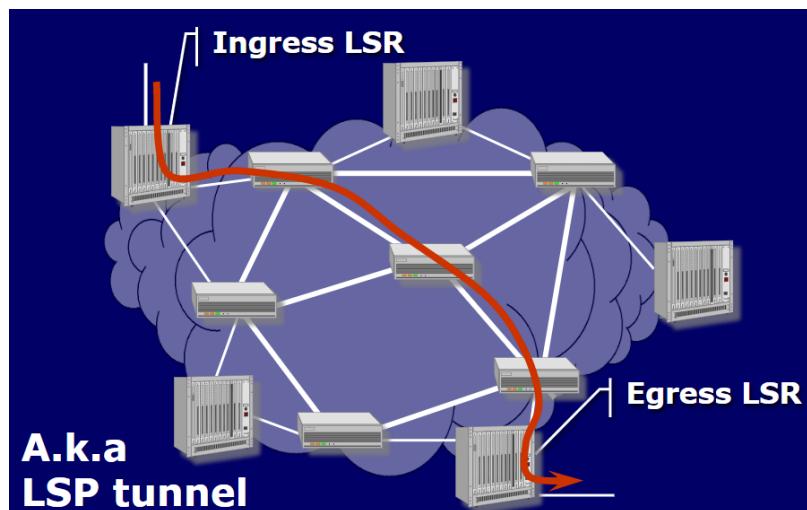


Figura 7.5: LSP tunnel

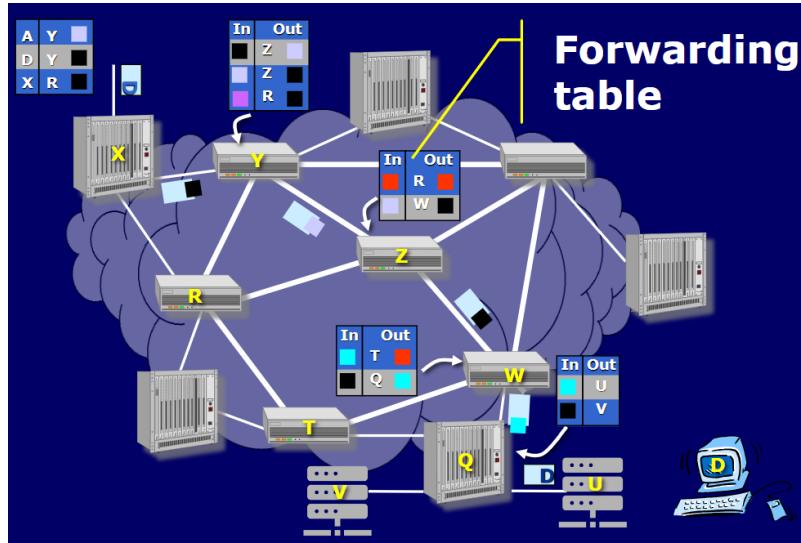


Figura 7.6: Label Switching

- l'header MPLS, che contiene l'etichetta
- protocolli per la distribuzione delle etichette
- protocolli di routing migliorati e modificati

Riassumendo: Il vantaggio è quello di utilizzare un solo protocollo per la gestione delle comunicazioni tra i nodi e anche verso l'esterno.

7.2 Storia di MPLS

A differenza di IPv6, **MPLS** è stato utilizzato da subito in produzione riuscendo a risolvere problemi di attori molto differenti.

Inizialmente venne implementato il *tag switching* da parte di Cisco nei propri sistemi per sostituire il *longest path matching*.

Fino a qualche anno fa si ipotizzava che lo standard di trasmissione **ATM** (*Asynchronous Transfer Mode*) avrebbe soppiantato internet in quanto molto superiore, ma ha come problematica il costo troppo elevato per la struttura (nessun problema di risoluzione indirizzi, signaling semplificato e un solo piano di controllo). Una prima soluzione fu quello di utilizzare ATM con IP, riutilizzando l'hardware del ATM switching. Venne successivamente introdotto MP λ S (*lambda!*) che significava Multi-Protocol Lambda Switching).

7.3 Header MPLS

L'header MPLS è di livello 2 ed è composta da più moduli uniti, che formano uno shim header, formati da:

- label: 20 bit
- exp: experimental bits, 3 bit
- s: bottom of stack, 1 bit, che viene messo a 1 al fondo dello stack, quando viene trovato a zero significa che sarà presente un altro modulo.
- TTL: time to live, 8 bit

Nel caso di ATM e frame relay alcune informazione sono già presenti, per cui si riutilizzano alcuni campi invece di raggiungere un nuovo modulo:

- VIC/VPI in ATM
- DLCI in frame relay

In questi casi non si guarderà il modulo MPLS ma i suddetti campi dei moduli già presenti. In questo modo il costruttore di apparati ATM non deve cambiare l'hardware ma bensì solamente il software, migliorando anche lo standard.

7.4 LSP setup

Una **FEC**, *Forwarding Equivalence Class*, è un insieme di pacchetti che hanno lo stesso destinatario. Un LSP è un percorso di comunicazione che viene utilizzato per trasportare un FEC.

Quando viene creato un LSP, sono necessarie tre operazioni da parte dei LSR:

- label binding: associazione dell'etichetta
- label mapping: creazione della riga nella tabella di forwarding, tra ingresso e uscita
- label distribution: l'etichetta scelta deve essere comunicata ai nodi vicini (o a un nodo vicino)

7.4.1 Label Binding

Un LSR determina l'etichetta che deve essere utilizzata per i pacchetti di una determinata FEC. Quello che avviene è definito Downstream binding, ovvero un LSR (??)

Il label binding può essere **unsolicited** oppure **on-demand**.

7.4.2 Label Mapping

Il label mapping esegue l'associazione tra una etichetta di ingresso, scelta dal LSR considerato, e una etichetta di uscita, scelta dal downstream LSR, per riuscire a raggiungere il next hop in base al routing.

7.4.3 Label Distribution

Quando un router ha fatto un binding di una etichetta, deve comunicare tale etichetta ai nodi vicini, in modo che questi possano fare il mapping (meno al nodo di upstream). Questa operazione è detta label distribution e serve a notificare l'etichetta scelta per un dato FEC, in seguito al label binding.

7.4.4 Static label binding (and mapping)

Il label binding statico avviene attraverso una gestione, ed è equivalente al PVC in ATM. Non è scalabile e non è interoperabile con tra managing systems. Inoltre, è impossibile avere LSPs tra reti differenti.

7.4.5 Dynamic label binding

Il label binding avviene in modo dinamico, in due modi possibili:

- **data/traffic driven:** triggered dai data packets
- **control driven:** ovvero innescato dai messaggi di controllo che può essere di segnalazione o di routing.

7.4.5.1 Control Driven

Sono possibili due modalità:

- topology based: il router scopre che esiste una destinazione, in base alla topologia della rete, dei percorsi e delle destinazioni dunque gli lsr creano degli lsp per le destinazioni.
- explicit creation of LSPs: avviene una segnalazione esplicita, inizializzata dagli label edge routers. Avviene on demand.

7.4.6 Label Distribution Protocol

La distribuzione delle etichette avviene attraverso dei protocolli, in particolare ne esistono 3 e non sono compatibili:

- **BGP**: utilizzo di un protocollo di routing, solo topology based (quando segnalo le destinazioni mando anche le etichette).
- **LDP**: label distribution protocol, realizzato appositamente. E' un'evoluzione del Tag Labelling di Cisco. Poco utilizzato perché si aveva paura di avvantaggiare Cisco, attualmente è deprecato.
- **RSVP**: Resource Reservation Protocol, utilizzato per l'allocazione di servizi integrati all'interno delle reti.

7.5 Protocolli di routing

Servono per determinare il percorso che farà LSP, impattando sulla fase di label mapping e determinare il packet routing.

I protocolli di routing sono in realtà quelli già esistenti:

- OSPF
- IS-IS
- BGP-4

Li utilizziamo per portare informazioni riguardo alle scelte di routing, come:

- capacità dei link
- utilizzo dei link
- dipendenze tra i link (utilizzato per il fault recovery)

7.6 Routing modes

Le modalità di routing sono 2:

- hop by hop routing
- explicit routing

7.6.1 Hop by hop routing

Ciascun LSR decide il prossimo LSR del percorso LSP. Il principio è lo stesso del IP routing tradizionale.

La procedura avviene nei seguenti step:

- viene presa una label per l'upstream link (label binding)

- la label viene mappata all'indirizzo della interfaccia del prossimo LSR del next hop
- Label announced dal next LSR

7.6.2 Explicit routing

Un singolo switch sceglie il percorso per l'intera LSP. Il percorso potrebbe non essere ottimale, ma almeno evitiamo il rischio di fare percorsi circolari, realizza dunque esplicitamente il percorso LSR. Non è dunque specificato solo il FEC ma anche l'intero percorso (il nodo deve avere le informazioni su tutta la rete).

7.6.3 Constraint based routing

La distribuzione delle operazioni tra nodi è impossibile, non c'è un unico criterio per scegliere il percorso e possono esserci vincoli che vanno in conflitto. Inoltre potrebbe essere difficoltoso mantenere i vincoli e le informazioni sincronizzate, in quanto variano più velocemente delle informazioni relative alla topologia.

7.6.4 Label Distribution Protocol (1)

I protocolli per la distribuzione delle etichette dovrebbero essere modificati per supportare informazioni su quale è il percorso, si parla allora di:

- **CR-LDP**: Constraint based routing label distribution protocol
- **RSVP-TE**: Resource Reservation Protocol Traffic Engineering

Questi devono essere utilizzati con OSPF-TE e IS-IS-TE.

Alcune nuove possibilità date da questo nuovo strumento sono:

- **traffic engineering**
- garantire la **qualità del servizio**
- per-class traffic engineering (sinergia con DiffServ)
- fault recovery rapido, in meno di 50 ms (50ms è importante perché la risposta sopra tale soglia è identificata come evento catastrofico)

7.7 Traffic Engineering

I pacchetti, quando spediti mediante ip, vengono inviati verso le destinazioni realizzando quello che è un fenomeno a imbuto e aggregazione causando una riduzione delle prestazioni.

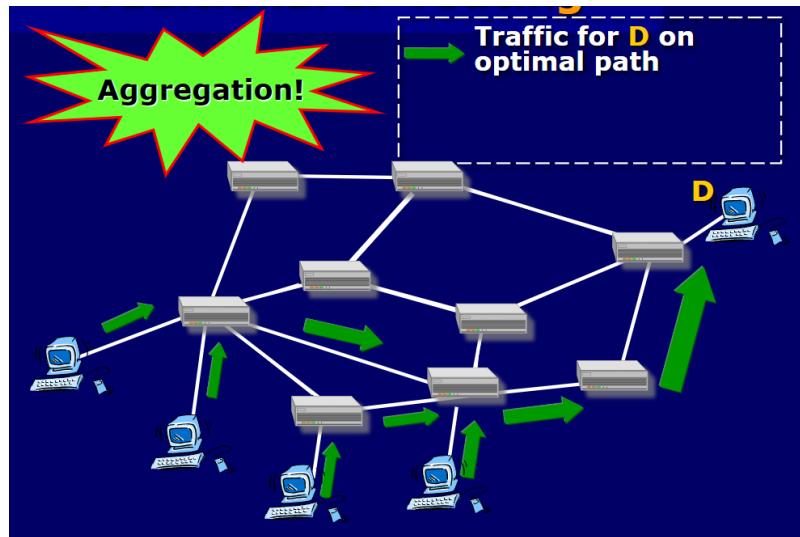


Figura 7.7: Aggregazione delle informazioni

L'unica soluzione sarebbe quella di comprare nuovi router che potrebbero divenire inutile se era un problema temporaneo.

Mediante la traffic engineering possiamo distribuire il classico **non in base alla destinazione**, ma in modo omogeneo evitando la congestione.

Se si scegliesse di inviare pacchetti in modo tradizionale in accordo al carico di ogni link, ogni volta che il router ricalcola i percorsi e i nexthop sono cambiati viene aggiornata la tabella in accordo con i nuovi percorsi di rete. Questo causa un inversione di tendenza tra i carichi che iniziano a cambiare molto velocemente causando **instabilità**.

In MPLS non c'è un aggiornamento costante tra piano di controllo e piano dati, a differenza di IP, consentendo il traffic engineering. Senza MPLS l'alternativa era ATM con due control plans (i router sono ATM-unaware), comportando però una ridotta scalabilità e un alto numero di adiacenze.

MPLS è IP-aware, solo un control plan operativo su una topologia fisica, rendendo il tutto più scalabile e semplice.

MPLS vede alcune estensioni come:

- MPLambdaS, ovvero MPLS control plans su rete ottica
- GMPLS, ovvero Generalized MPLS, estensione di MPLS per supportare più tipi di rete (pacchetti, circuito, optics, etc)

7.8 CoS e QoS

Le risorse e le modalità di servizio potrebbero essere associate a un FEC nel momento di setup di un LSP. Explicit support è richiesto nel data plan e control plan di LSR (??)

7.8.1 Class of Service (CoS)

La CoS è un insieme di parametri che descrivono il servizio richiesto. Consente una priorità relativa tra FEC differenti ed è in grado di fornire un garanzia assoluta.

Supporta il modello DiffServ con un comportamento per-hop, EF (expedite forwarding) e AF (assured forwarding), oltre al per class traffic engineering (ds-aware traffic engineering).

7.8.2 Quality of Service (QoS)

La QoS garantisce specificatamente:

- bandwidth
- Delay
- burst size

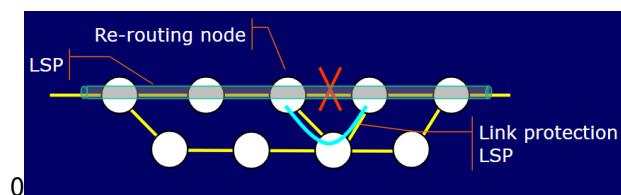
I vantaggi di QoS in MPLS sono vari, tra cui la possibilità di avere una rete unificata in grado di supportare tutti i tipi di servizi (marketing message).

Il supporto per QoS e i servizi real time su IP non è ancora pronto.

Molte reti multi servizio utilizzano ora un paradigma “ships in the night”, dove i protocolli ATM sono per servizi tipi di ATM ed MPLS control plan è utilizzato per i servizi IP.

7.9 Fast fault recovery

E' garantito il fast fault recovery mediante link re-routing e edge-to-edge re-routing.



<

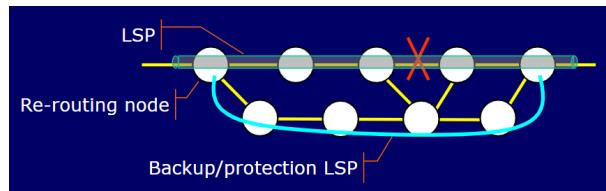


Figura 7.8: Edge to edge re-routing

7.10 Scalabilità

Le label MPLS introducono gerarchie su più livelli, a seconda di quanto richieste per la scalabilità. Le tabelle di routing dei router di transito non devono essere necessariamente complete, in quanto LSP è gestito tra gli edge routers.

In questo modo è più semplice e veloce gestire il match delle label piuttosto che il longest prefix matching.

7.11 Penultimate Hop Popping (PHP)

Il penultimo nodo esegue il pop della label dal LSP, in modo da non doverlo fare il nodo di destinazione. Il LER indirizza il pacchetto in base all'indirizzo IP (o la prossima label nello stack).

La distribuzione di label 3 indica un implicito PHP, in quanto l'edge router vede che il next hop è all'esterno.

Per qualsiasi router sull'ultimo hop avviene lo swap sull'etichetta 0.

