



Politecnico
di Torino

Tecnologie e Servizi di Rete

Computer Engineering

Marco Lampis

28 dicembre 2022

Indice

0 Informazioni	1
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	4
1.5 IP addressing methodology	6
1.5.1 Esercizio 1	8
1.5.2 Esercizio 2	8
1.5.3 Esercizio 3	9
1.5.4 Esercizio 4	9
1.5.5 Esercizio 5	10
1.5.6 Esercizio 6	11
1.5.7 Esercizio 7	12
1.5.8 Esercizio 8	14
1.5.9 Esercizio 9	14
1.5.10 Esercizio 10	15
1.6 Multicast	17
2 IPv6	19
2.1 Perché IPv4 non basta e soluzioni	19
2.2 Chi assegna indirizzi IP	20
2.3 Address pool status e scalabilità	20
2.4 Indirizzi IPv6	21
2.5 Routing	21
2.6 Multicast	23
2.7 Unicast	23
2.7.1 Global Unicast Addresses	24
2.7.2 Link local/site local Addresses	24
2.7.3 Unique Local Addresses	25

2.7.4	IPv4 Embedded Addresses	26
2.8	Anycast Addresses	26
2.9	Architettura del protocollo	26
2.10	Packet Header Format	27
2.10.1	Hop-by-Hop Extension Header	29
2.10.2	Routing Extension Header	29
2.10.3	Altre estensioni	30
2.11	Interfacciarsi con i livelli più bassi	31
2.11.1	Incapsulamento	31
2.11.2	Address mapping	31
2.11.3	IPv6 Multicast transmission	31
2.12	Neighbor Discovery and Address Resolution	32
2.12.1	Solicited-Node Multicast Address	32
2.12.2	Risoluzione indirizzo	32
2.13	La transizione tra IPv4 e IPv6	34
2.14	ICMPv6	36
2.14.1	Formato del messaggio	36
2.14.2	Neighbor Solicitation	37
2.14.3	Neighbor Advertisement	37
2.14.4	Host Membership Discovery	38
2.15	Device Configuration in IPv6	39
2.15.1	Privacy extension Algorithm	40
2.15.2	Indirizzi	40
2.15.3	ICMP Redirect	42
2.15.4	Duplicate Address Detection (DAD)	42
2.15.5	Fasi di configurazione di una configurazione Stateless	42
2.16	Scoped Addresses	43
2.17	Routing Protocols	43
2.18	Transizione	44
2.19	Host centered solutions	45
2.19.1	6over4	45
2.19.2	ISATAP: Intra-site Automatic Tunnel Addressing Protocol	46
2.19.3	(Lack of) Neighbor Discovery	46
2.19.4	Automatic Configuration	46
2.20	Network center solution	47
2.20.1	6to4	47
2.20.2	Basic 6to4 Scenario	47
2.20.3	Mixed 6to4 scenario	48

2.20.4 Tunnel broker	48
2.21 Scalable, Carrier-grade Solutions	49
2.21.1 AFTR: Address Family Transition Router	50
2.21.2 DS-Lite	50
2.21.3 A+P (Address plus port)	50
2.21.4 Mapping Address and Port (MAP)	50
2.22 MAP-E	52
2.23 MAP-T	52
2.24 Nat64 + DNS64	52
3 Reti Wireless e cellulari	53
3.1 Introduzione	53
3.2 Wireless LAN	53
3.3 IEEE 802.11: multiple access (CSMA)	54
3.3.1 CSMA/CA	54
3.3.2 Frame addressing	55
3.3.3 Mobilità	56
3.4 Reti Cellulari	56
3.4.1 Splitting	57
3.4.2 Cell shaping	58
3.4.3 Power Control	58
3.4.4 Frequency allocation	60
3.4.5 Architettura di rete	60
3.4.6 Registrazione	61
3.4.7 Mobility Management	61
3.5 Evoluzione della rete cellulare	62
3.5.1 GSM	63
3.5.2 4G/LTE	67
3.5.3 5G	70
3.6 Mobilità nel 4G/5G	73
4 Principi del modern Lan Design	77
4.1 Ripetitori	77
4.2 Bridge	77
4.3 Modern LANs	78
4.4 Multiple LANs	79

5 VPN	83
5.1 Deployment Models	84
5.1.1 Site to Site VPN	86
5.1.2 End to End VPN	86
5.1.3 Remote VPN	86
5.1.4 Overlay Model	86
5.1.5 Peer Model	87
5.1.6 Customer Provisioned VPN	87
5.1.7 Provider Provisioned VPN	87
5.1.8 Access VPN Customer Provisioned	88
5.1.9 Tunneling	89
5.1.10 Topologie	89
5.1.11 Layers	90
5.2 GEneric Routing Encapsulation (GRE)	92
5.3 Layer 2 frame within an IP packet	93
5.3.1 L2TP	93
5.3.2 Point to Point Tunneling Protocol (PPTP)	95
5.4 IPsec	96
5.5 SSL VPN	97
5.5.1 Application translation	98
5.5.2 Application proxy	99
5.5.3 Port forwarding	99
5.6 VPN Gateway Positioning & anomalies	100
5.6.1 Anomalies	100
5.6.2 Monitorability anomaly	101
5.6.3 Skewed Channel anomaly	101
6 Routing	103
6.1 Introduzione	103
6.1.1 Proactive routing	103
6.1.2 On the fly routing	103
6.2 Proactive routing algorithms	104
6.2.1 Non adaptive algorithms	104
6.2.2 Adaptive algorithms	104
6.3 Distance vector (Bellman-Ford)	105
6.4 Path vector	108
6.5 Link State Routing Algorithm	109
6.5.1 Algoritmo di Dijkstra	109

6.6	Internet Routing Architecture	110
6.6.1	Autonomous System	110
6.7	Protocolli di routing	111
6.7.1	IGP	112
6.7.2	EGP	114

0 Informazioni

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

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

Per qualsiasi suggerimento o correzione non esitate a contattarmi.

E' possibile riutilizzare il materiale con le seguenti limitazioni:

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

E' per tanto possibile:

- Modificare parzialmente o interamente il contenuto

Questi appunti sono disponibili su GitHub al seguente link:

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



Scansiona!

Figura 1: Repository GitHub

1 IPv4 Summary

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

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

1.1 Indirizzi speciali

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

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

1.2 Indirizzamento IP con classi

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

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

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

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

1.3 Indirizzamento IP senza classi (CIDR)

Il sistema ***Classless InterDomain Routing*** permette di indirizzare la porzione più precisa di indirizzi tra rete e dispositivi. La porzione di rete è dunque di lunghezza arbitraria. Il formato con cui può essere rappresentato un indirizzo è il seguente: **networkID + prefix length** oppure **netmask**.

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

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

Esempio:

```
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 da 0 a 255.

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

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

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.

1.4 IP routing

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

- **destinazione** (indirizzi ip)

- **interfaccia** (eth0...)

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

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

Di seguito è mostrato un esempio di routing:

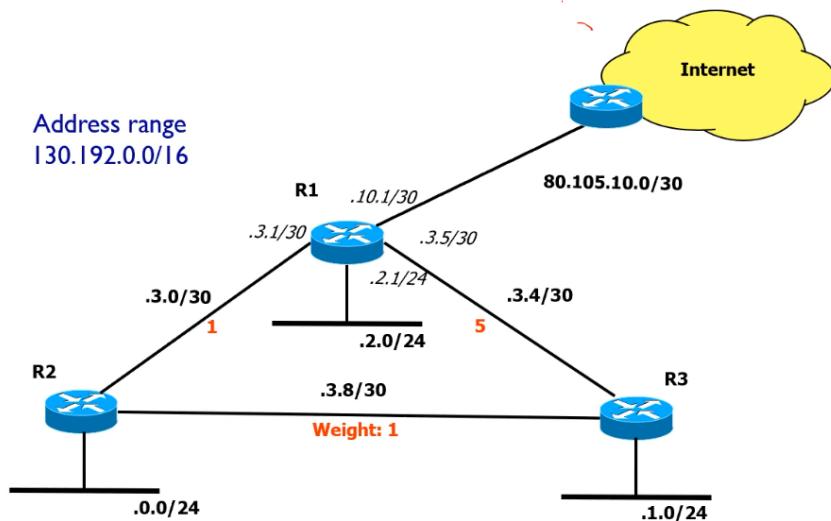


Figura 1.1: routing

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

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

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

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

1.5 IP addressing methodology

La metodologia da adoperare è la seguente:

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

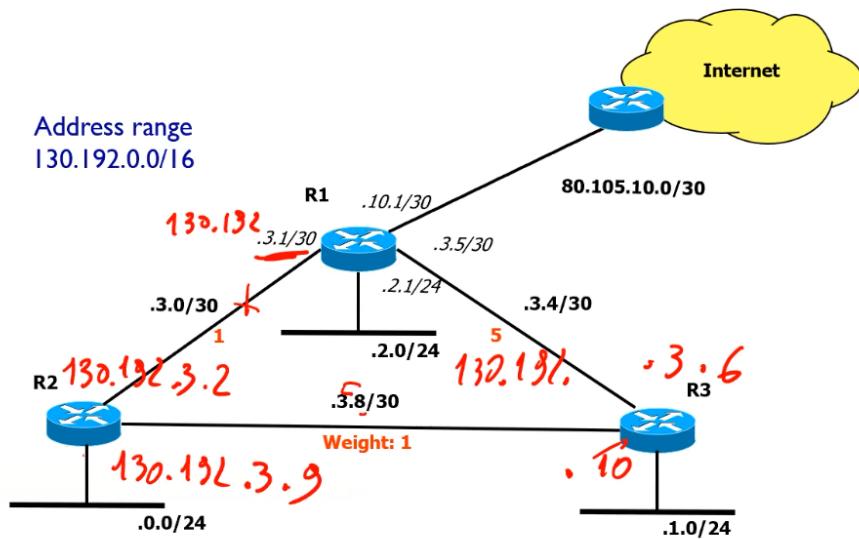
Nota: in basso a sinistra sono richiesti 43 indirizzi per 40 dispositivi. Ciò è dovuto al fatto che oltre ai 40 richiesti serve l'indirizzo di rete, l'indirizzo di broadcast e l'indirizzo del router.

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

```

1 # tutta la rete
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
7 10.0.0.127 <- ultimo
8
9 # subnet3 (/26), 32-26 = 6 => 2^6 = 64 indirizzi
10 # range: 128-191
11 10.0.0.128/26
12 10.0.0.191 <- ultimo
13
14 #subnet4 (/30), punto punto
15 10.0.0.192/30

```

**Figura 1.2:** routing2

IP Addressing: methodology

1. Location of IP networks
 2. Amount of required addresses
 3. Amount of allocated addresses
 4. Address range validity
 5. Netmask / Prefix Length
 6. Address Range
 7. Host addresses
- | | |
|---|--|
| <p>Minimum amount of addresses: 196
Address range selected: 10.0.0.0/24 → OK</p> <p>Required addresses: 4
Allocated addresses: 4
NM (PL): 255.255.255.252 (/30)</p> | <p>Network 10.0.0.192/30
Rete IP 3</p> <p>Network 10.0.0.128/26
Rete IP 1</p> <p>Network 10.0.0.0/25
Rete IP 2</p> |
|---|--|
- .194 .193 .1
.129 .1 .1
.169 .101 .1
- Required addresses: 43
Allocated addresses: 64
NM (PL): 255.255.255.192 (/26)
- Required addresses: 103
Allocated addresses: 128
NM (PL): 255.255.255.128 (/25)

Figura 1.3: Rete di esempio

1.5.1 Esercizio 1

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

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

1.5.2 Esercizio 2

Verifica se i seguenti indirizzi sono validi o meno.

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

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

1.5.3 Esercizio 3

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

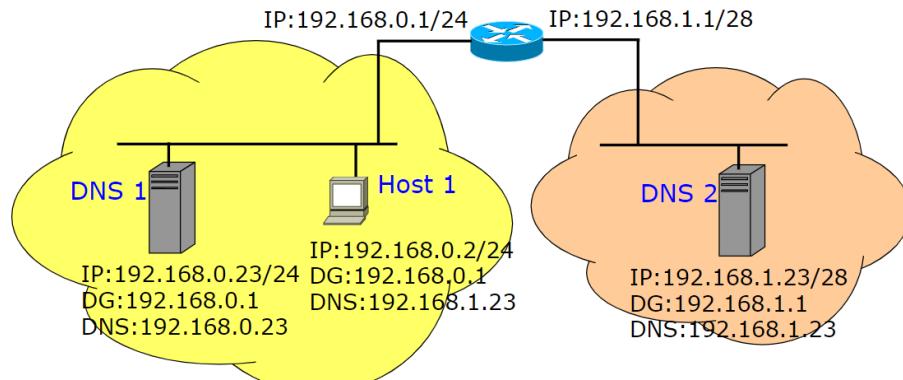


Figura 1.4: Configurazione

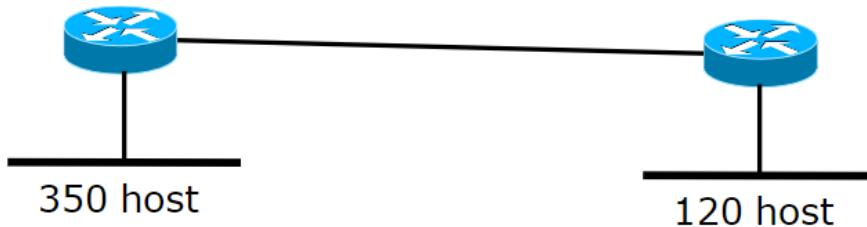
1.5.4 Esercizio 4

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

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

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

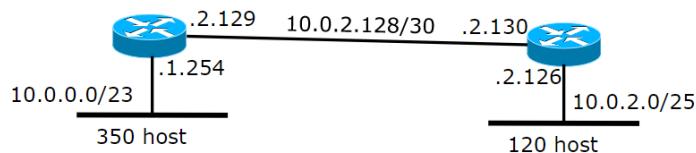
La sottorete C (destra) sarà identificata da 10.0.2.0/25 in quanto l’indirizzo immediatamente successivo. Il suo indirizzo di broadcast sarà 10.0.2.127.

**Figura 1.5:** Rete

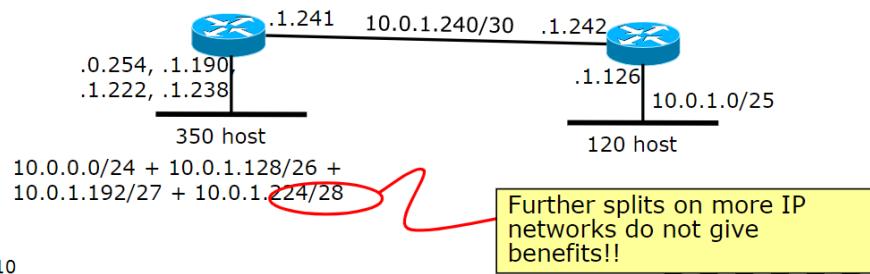
La sottorete B (centrale) sarà identificata da $10.0.2.128/30$, con /30 proveniente dal fatto che è una sottorete punto punto.

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

Solution1



Solution2



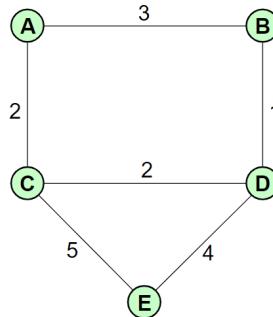
10

Figura 1.6: Soluzioni

1.5.5 Esercizio 5

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

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

**Figura 1.7:** Rete esercizio 5

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

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

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 1.8: Soluzione esercizio 5

1.5.6 Esercizio 6

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

Marco Lampis

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

11

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

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

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

1.5.7 Esercizio 7

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

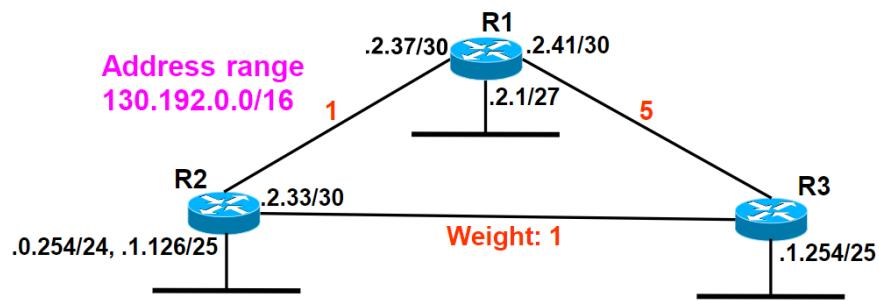
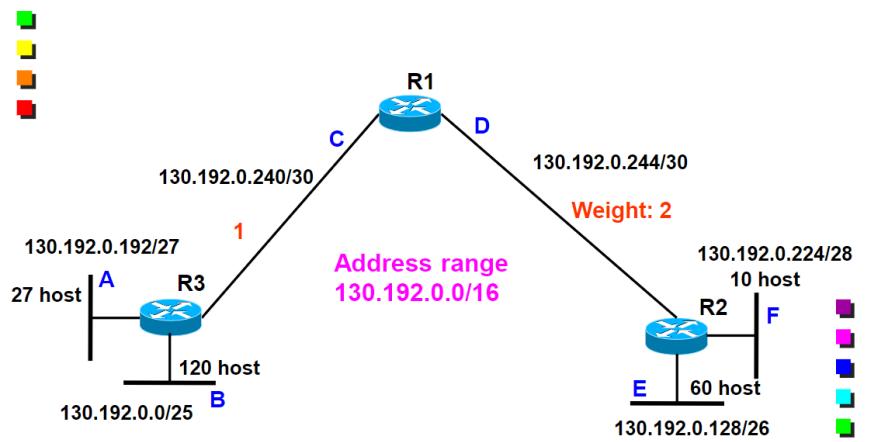
Troviamo la routing table di **R1**, analizzando ogni nodo a partire dai collegamenti diretti:

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

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

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

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

**Figura 1.9:** Esercizio 6**Figura 1.10:** Esercizio 7

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

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

1.5.8 Esercizio 8

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

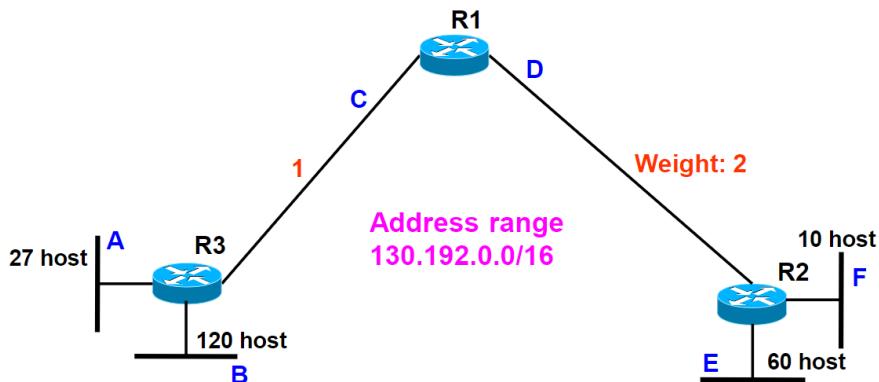


Figura 1.11: Esercizio 9

1.5.9 Esercizio 9

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

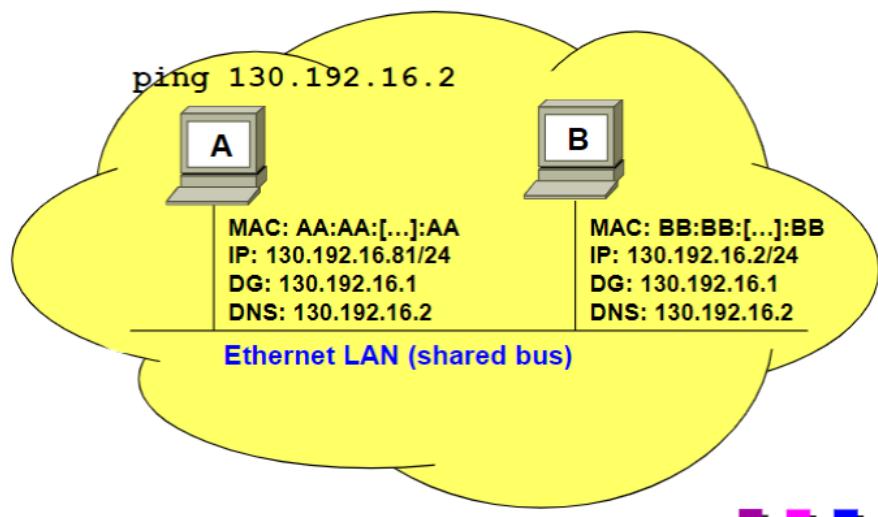


Figura 1.12: Esercizio 10

In una macchina Windows il ping viene eseguito 4 volte.

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

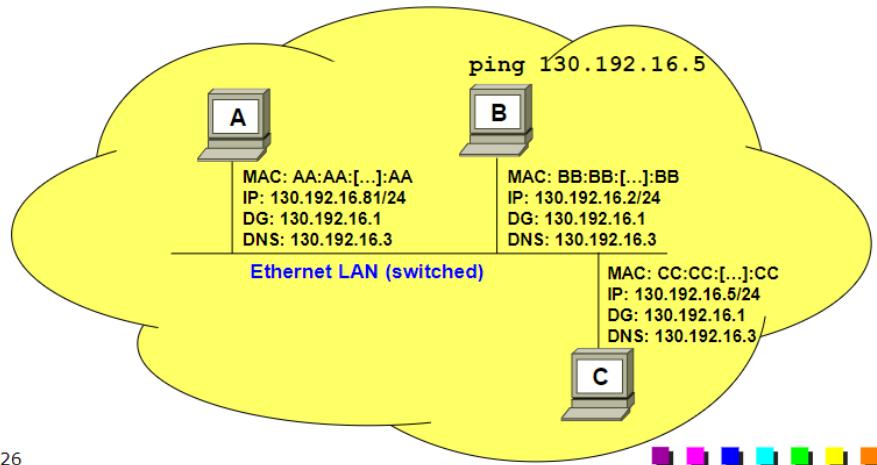
Scriviamo ora la tabella:

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.

1.5.10 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 1.13: Esercizio 10

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

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

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

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

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

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

Il passaggio 10 e 11 sono quelli eseguiti 4 volte.

1.6 Multicast

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

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

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

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

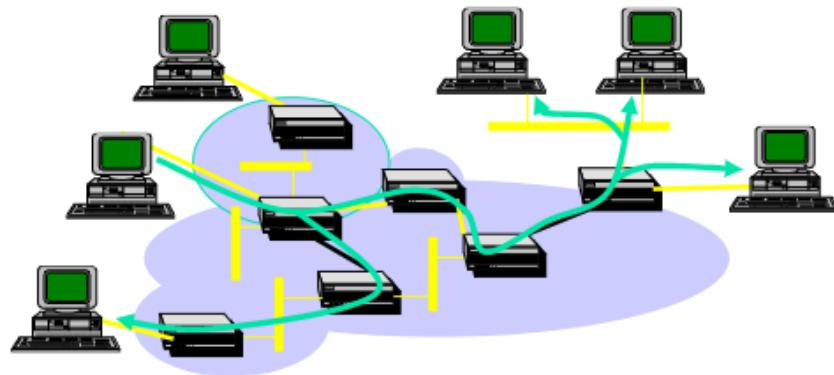


Figura 1.14: Multicast

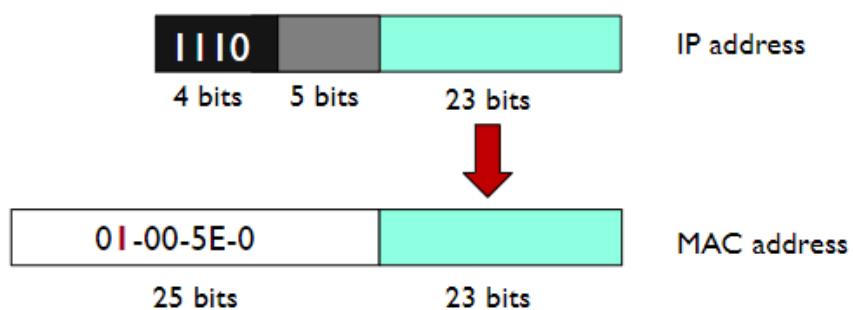


Figura 1.15: Mappatura IP a MAC

2 IPv6

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

Altre motivazioni che hanno portato alla nascita di IPv6 sono:

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

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

2.1 Perché IPv4 non basta e soluzioni

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

Alcune delle soluzioni utilizzate per risolvere questi problemi sono:

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

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

2.2 Chi assegna indirizzi IP

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

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

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

2.3 Address pool status e scalabilità

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

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

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

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

Sono state tentate alcune soluzioni, come:

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

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

2.4 Indirizzi IPv6

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

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

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

2.5 Routing

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

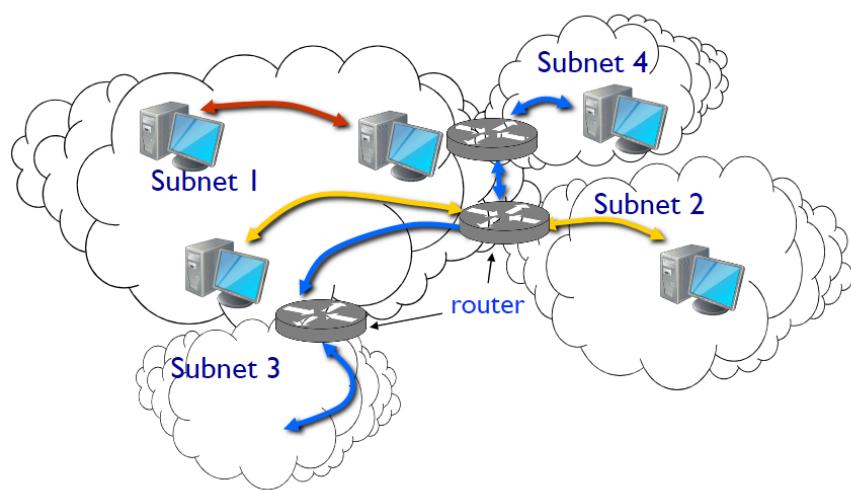


Figura 2.1: Routing

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

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

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

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



$n=64$

Figura 2.2: Struttura dell'indirizzo

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

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

Dividiamo le comunicazioni in:

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

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

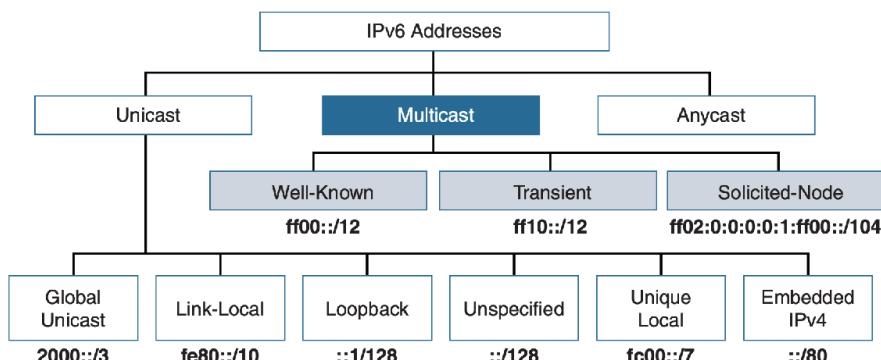


Figura 2.3: Spazio di indirizzamento

2.6 Multicast

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

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

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

L'indirizzo si scomponete in:

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

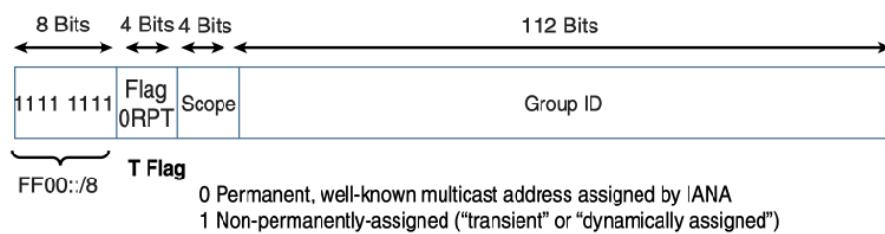


Figura 2.4: Struttura indirizzo multicast

2.7 Unicast

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

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

- $\text{FC00}::/7$, Unique Local
- $::80$, Embedded IPv4

2.7.1 Global Unicast Addresses

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

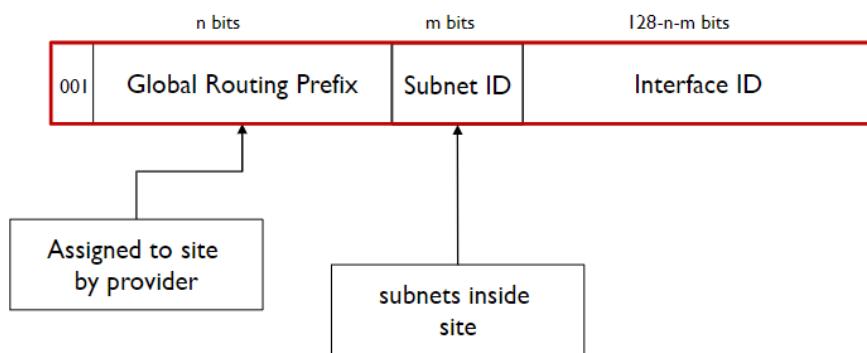


Figura 2.5: Global Unicast Addresses

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

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

2.7.2 Link local/site local Addresses

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

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

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

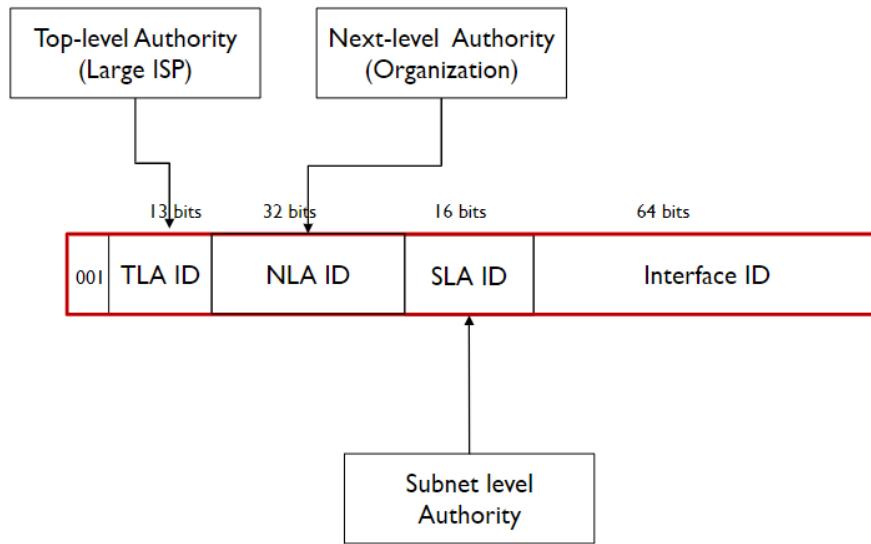


Figura 2.6: Global Routing Prefix

2.7.3 Unique Local Addresses

Gli Unique Local Addresses possono essere utilizzati in modo simile agli indirizzi globali unicast, ma sono per un utilizzo privato e non per l'indirizzamento sull'internet. Sono identificati da **FFC00 :: /7**, e vengono utilizzati dai dispositivi che non hanno mai necessità di connettersi all'internet e non hanno bisogno di essere raggiungibili dall'esterno. Sono indirizzi privati che possono comunicare su internet grazie ad operazioni di tunneling.

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

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

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

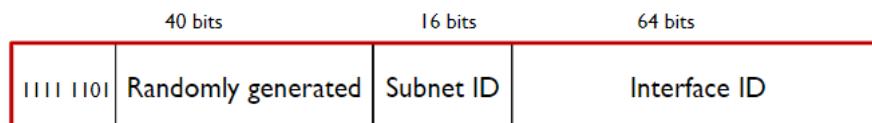


Figura 2.7: Unique Local Addresses

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

2.7.4 IPv4 Embedded Addresses

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

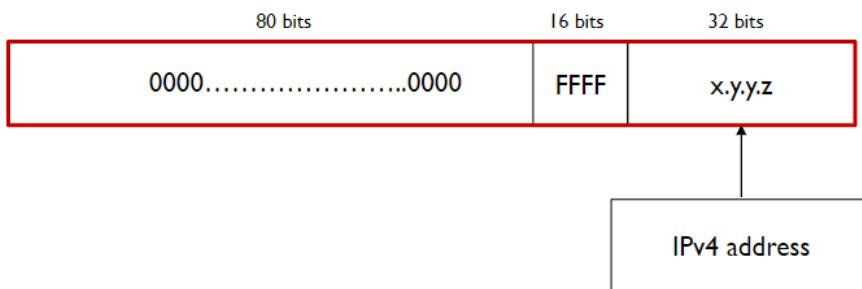


Figura 2.8: Struttura indirizzi IPv4 Embedded

2.8 Anycast Addresses

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

Nota: molto utile, ma non è ancora utilizzato.

2.9 Architettura del protocollo

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

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

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

Sono invece stati aggiornati senza modifiche essenziali:

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

2.10 Packet Header Format

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

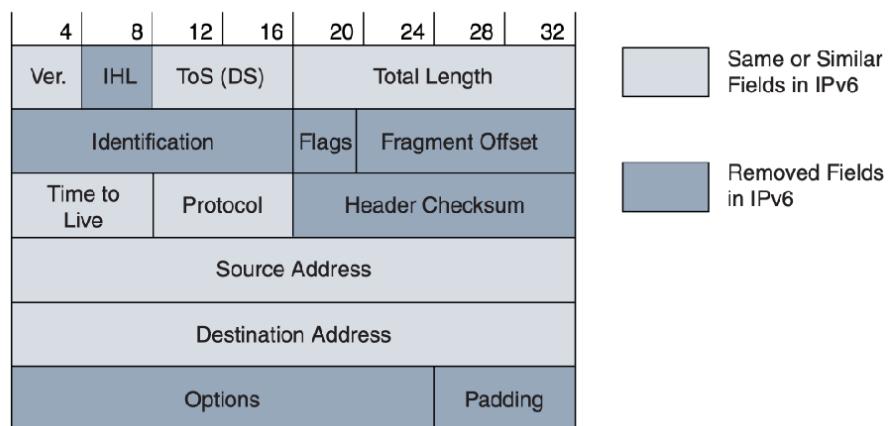
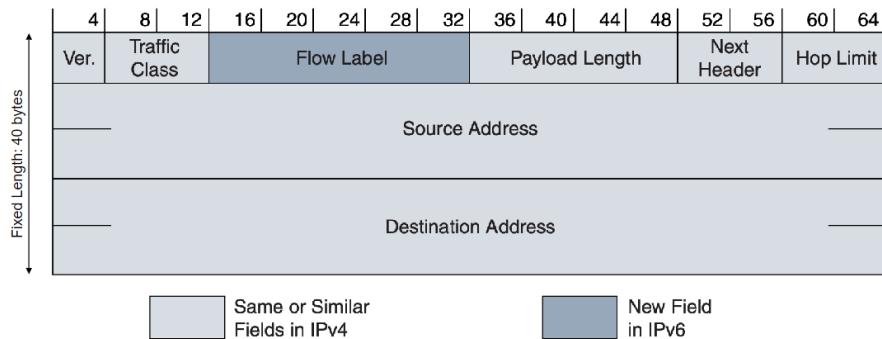


Figura 2.9: Header IPv4

L'header utilizzato in IPv6 è invece il seguente:

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

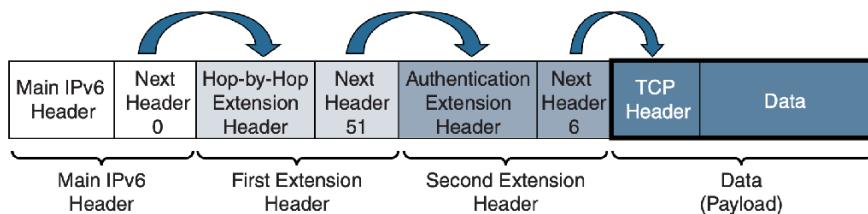
- Header Checksum: viene utilizzato per verificare se il dato trasmesso è corrotto, ma non è più necessario in IPv6.
 - Redundant: Layer 2 data link technologies perform own checksum and error control.
 - Upper-layer protocols such as TCP and UDP have their own checksums
- Frammentazione

**Figura 2.10:** Header IPv6

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

Nota: Il checksum su UDP diventa opzionale in IPv6.

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

**Figura 2.11:** Chaining

Inoltre, sono presenti:

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

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

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

Il formato del campo next header è il seguente:

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

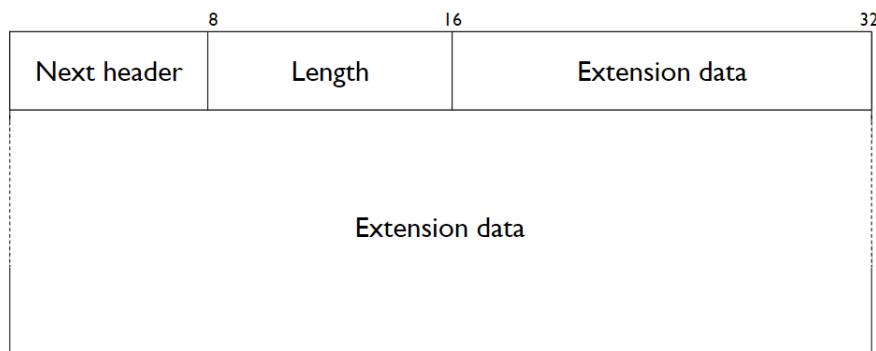


Figura 2.12: Extension Header Format

2.10.1 Hop-by-Hop Extension Header

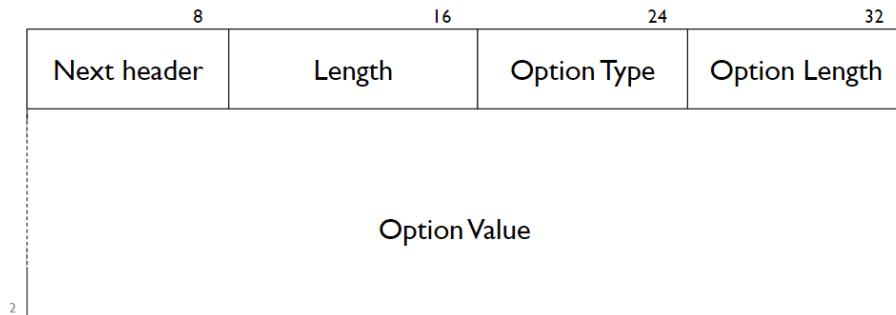
E' utilizzato per andare a inserire dei campi/vincoli che servono all'hop per capire se il pacchetto deve essere scartato o meno (strumento di analisi). Se è presente, è indicato immediatamente dopo l'header IPv6. Questo header viene utilizzato per inserire dei campi opzionali. Ogni opzione ha un set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

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

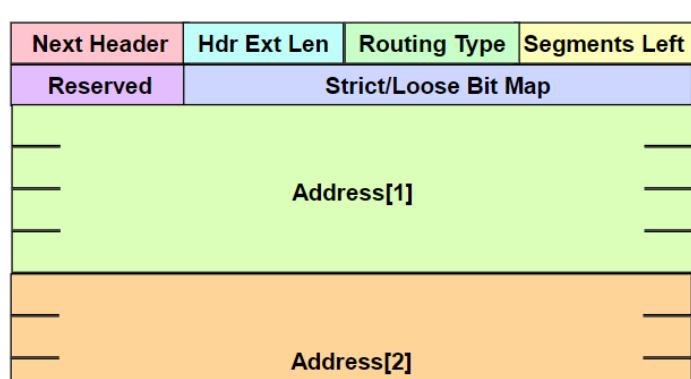
Si ottiene una tripletta **TLV** (type-length-value).

2.10.2 Routing Extension Header

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

**Figura 2.13:** Hop-by-Hop Extension Header

IPv6.

**Figura 2.14:** Routing Extension Header

2.10.3 Altre estensioni

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

2.10.3.1 fragmentation header

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

2.10.3.2 Authentication and Encapsulation Header

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

2.11 Interfacciarsi con i livelli più bassi

2.11.1 Incapsulamento

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

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

2.11.2 Address mapping

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

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

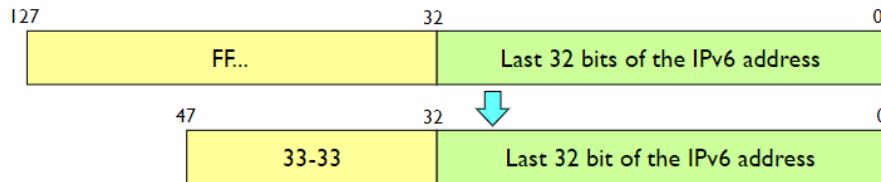
2.11.3 IPv6 Multicast transmission

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

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

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

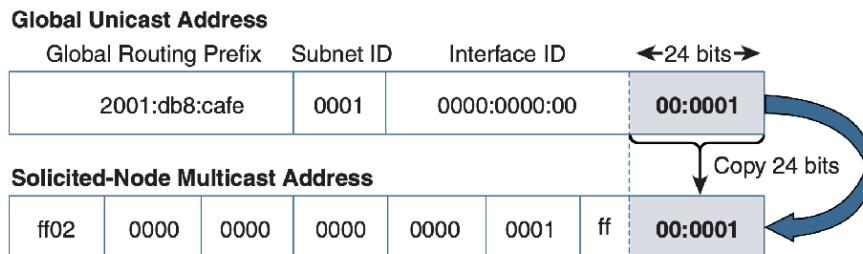
**Figura 2.15:** Multicast Transmission

2.12 Neighbor Discovery and Address Resolution

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

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

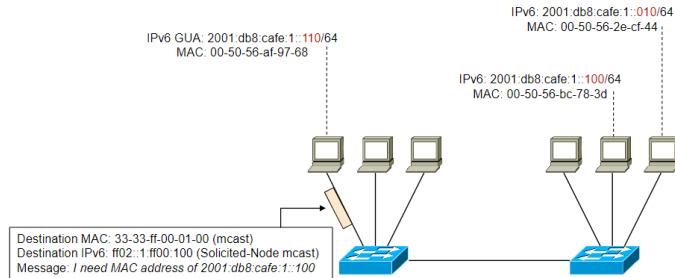
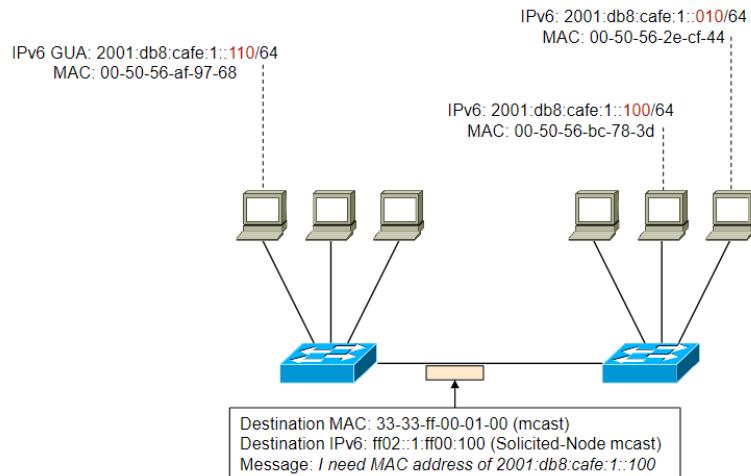
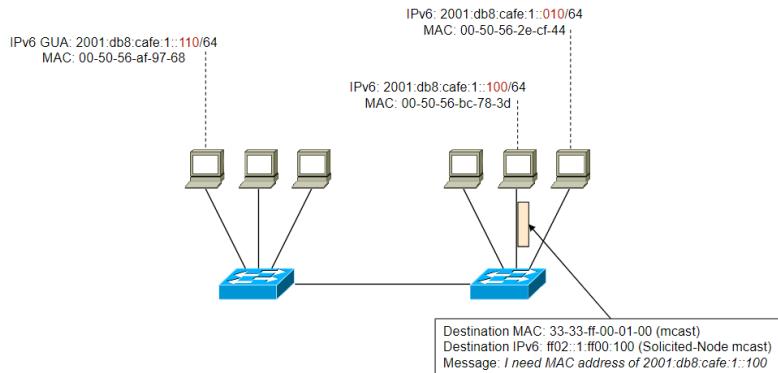
**Figura 2.16:** Mappatura indirizzo

2.12.2 Risoluzione indirizzo

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

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

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

**Figura 2.17:** Risoluzione dell'indirizzo**Figura 2.18:** Risoluzione dell'indirizzo**Figura 2.19:** Risoluzione dell'indirizzo

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

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

2.13 La transizione tra IPv4 e IPv6

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

Questo risultato viene ottenuto attraverso tre meccanismi:

- Address Mapping
- Tunneling
- Translation mechanisms

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

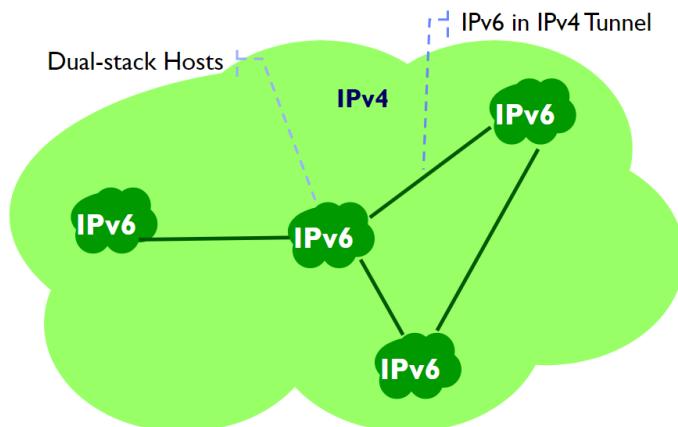


Figura 2.20: Pochi host IPv6

Nel corso del tempo le infrastrutture si sono adattate 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.

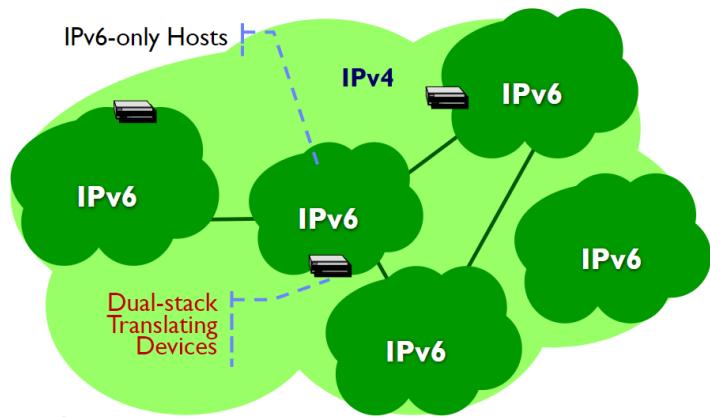


Figura 2.21: Molti host IPv6

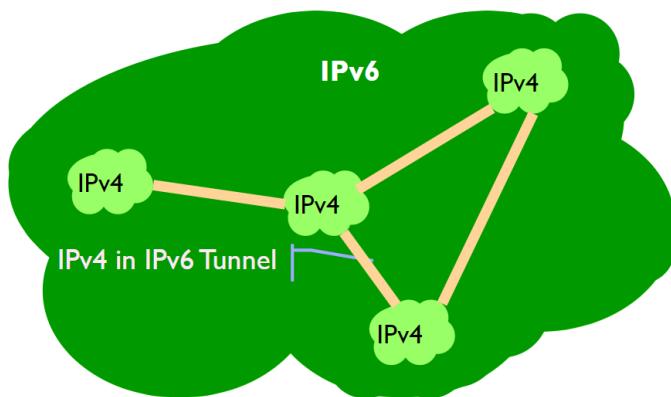


Figura 2.22: Maggioranza IPv6

2.14 ICMPv6

ICMPv6 permette di eseguire operazioni di:

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

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

2.14.1 Formato del messaggio

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

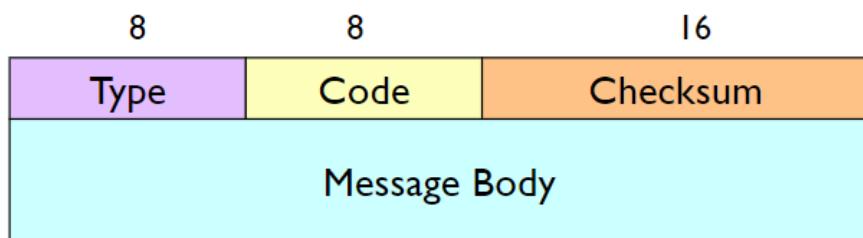


Figura 2.23: Formato del messaggio

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

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

2.14.2 Neighbor Solicitation

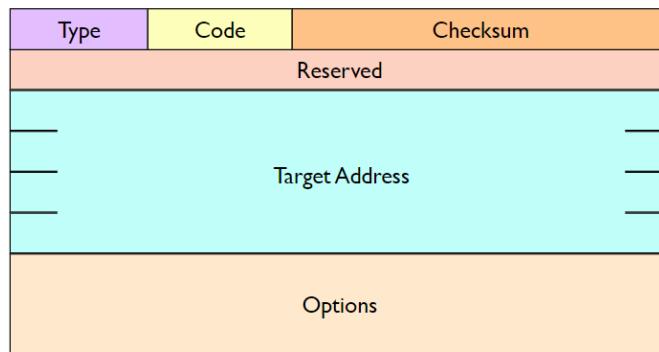


Figura 2.24: Neighbor Solicitation

2.14.3 Neighbor Advertisement

Sono presenti dei flag aggiuntivi:

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

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

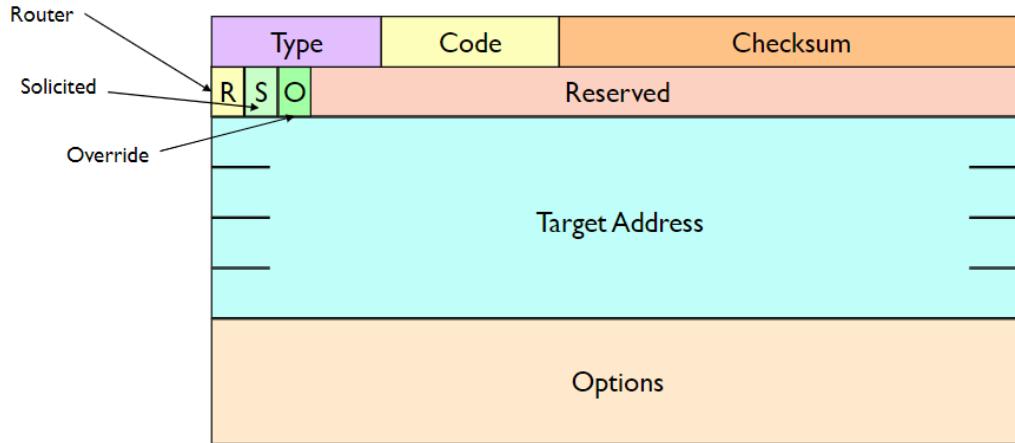


Figura 2.25: Neighbor Advertisement

2.14.4 Host Membership Discovery

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

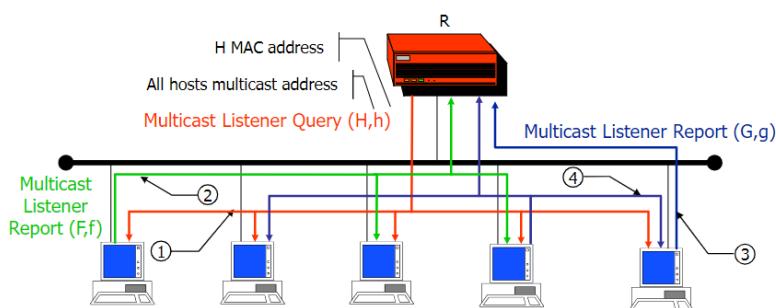


Figura 2.26: Host Membership Discovery

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

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

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

Type	Code	Checksum
Maximum Response Delay		Unused
Multicast Address		

Figura 2.27: Formato richiesta

2.15 Device Configuration in IPv6

Le informazioni necessarie per la configurazione di un dispositivo sono:

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

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

Le configurazioni possono essere:

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

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

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

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

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

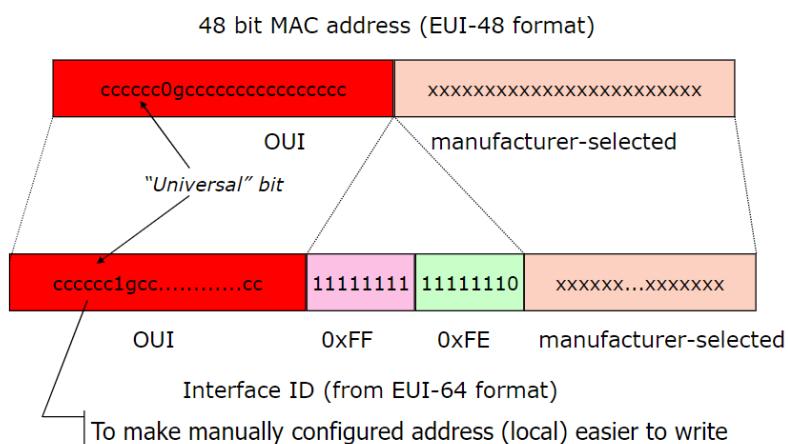


Figura 2.28: EUI-48 to EUI-64 mapping

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

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

2.15.1 Privacy extension Algorithm

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

2.15.2 Indirizzi

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

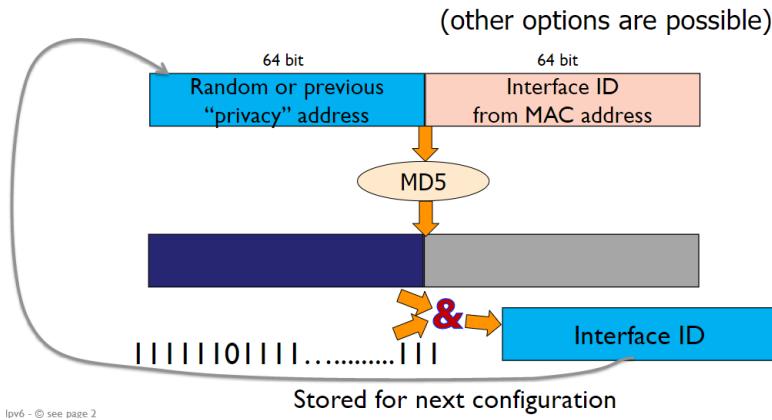


Figura 2.29: Privacy extension Algorithm

potrebbe essere disponibile per un user o una applicazione.

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

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

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

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



Figura 2.30: Router Solicitation

Nel messaggio di advertisement ci sono dei parametri interessanti:

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

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

tra le 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 lo utilizzo all'interno di un on-link
- **A**, il prefisso può essere utilizzato per una configurazione automatica
- **prefix**: il prefisso

Un'altra opzione è l'mtu.

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

2.15.3 ICMP Redirect

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

2.15.4 Duplicate Address Detection (DAD)

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

2.15.5 Fasi di configurazione di una configurazione Stateless

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

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

Una volta scoperta la parte alta:

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

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

2.16 Scoped Addresses

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

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

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

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

2.17 Routing Protocols

Per prima cosa distinguiamo il routing in due tipologie:

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

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

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

I protocolli di routing possono essere:

- **integrate routing:** viene adoperato un singolo protocollo che informa i destinatari per entrambe le protocol families, dunque sia IPv4 che IPv6. Ha come vantaggio quello di non avere meccanismi di duplicazione, ma è necessaria l'implementazione di un nuovo protocollo dedicato che potrebbe comportare bug con il funzionamento delle operazioni in IPv4. Inoltre, le topologie di rete tra IPv4 ed IPv6 potrebbero essere diverse e quindi il routing potrebbe non essere ottimale.
- **ships in the night:** ogni family address ha il suo protocollo di routing, con la caratteristica che tutti i protocolli sono indipendenti l'uno dall'altro. In questo modo è possibile utilizzare protocolli di routing differenti (scelti in base alla topologia o scenario). Il vantaggio è una più semplice integrazione e 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 2.31: Protocolli di routing

2.18 Transizione

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

Alcuni protocolli che lo implementano:

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

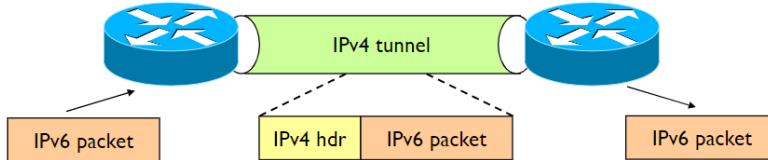


Figura 2.32: Esempio di Tunnelling

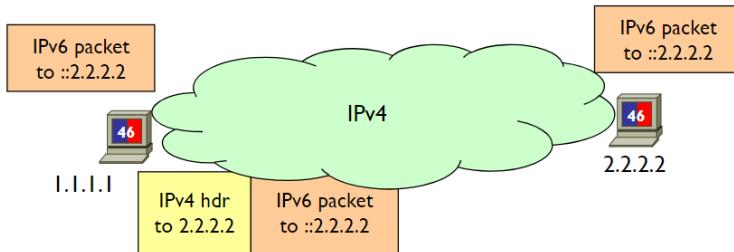
- setup manuale ed automatico

2.19 Host centered solutions

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

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

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



2.19.1 6over4

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

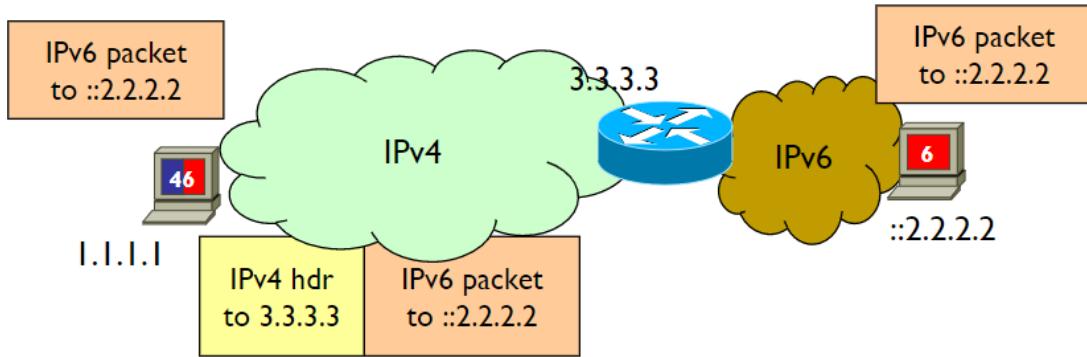


Figura 2.33: Dual stack router

- Not very used because IPv4 multicast support is not widespread

2.19.2 ISATAP: Intra-site Automatic Tunnel Addressing Protocol

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

2.19.3 (Lack of) Neighbor Discovery

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

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

2.19.4 Automatic Configuration

E' diventato lo standard nel tempo.

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

2.20 Network center solution

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

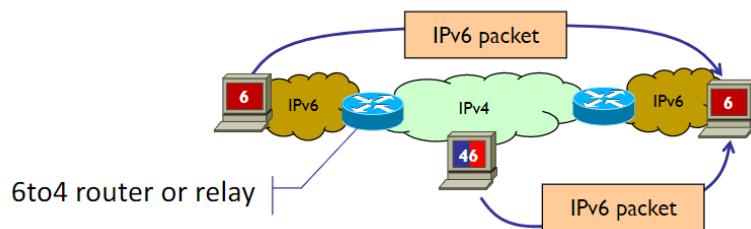


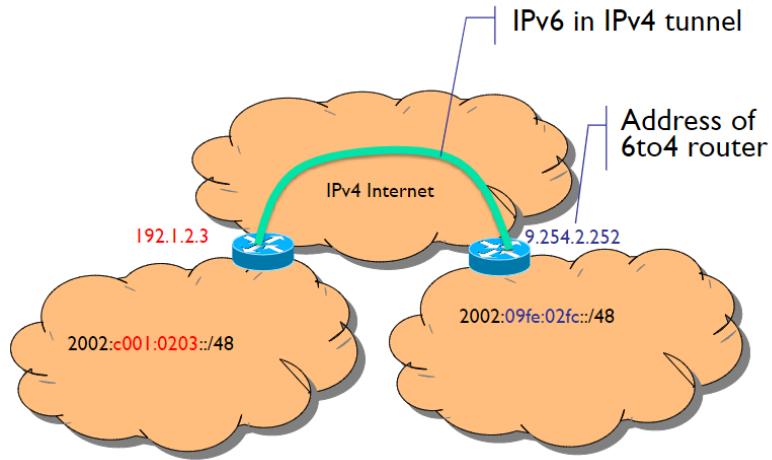
Figura 2.34: Host centered

2.20.1 6to4

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

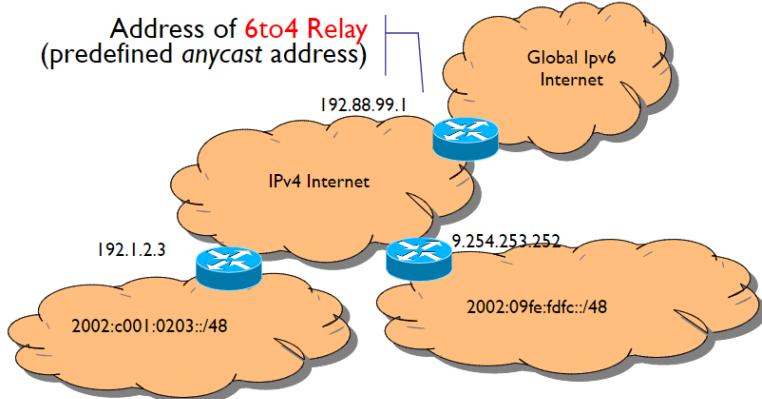
2.20.2 Basic 6to4 Scenario

Not meant for IPv4 host to IPv6 host communication



2.20.3 Mixed 6to4 scenario

6to4 Relay must be default gateway of 6to4 routers



2.20.4 Tunnel broker

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

soluzione centralizzata.

2.21 Scalable, Carrier-grade Solutions

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

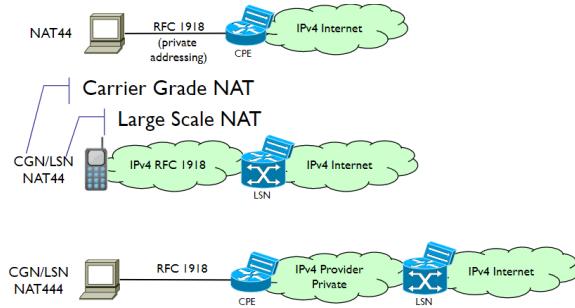
- **Several Options**
- **DS-Lite**
- **A+P (DS-Lite evolution)**
- **MAP-T and MAP-E**
- **NAT64**
- **6PE (MPLS-based)**

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

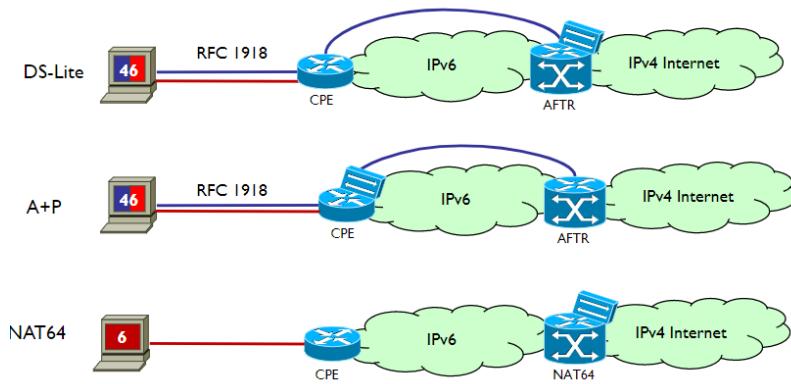
- LSN: large scale NAT, riesce a gestire una quantità di richieste molto grande

E' possibile avere più livelli di NAT.

Avere più nat in cascata è abbastanza in comune.



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



2.21.1 AFTR: Address Family Transition Router

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

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

2.21.2 DS-Lite

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

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

i problemi sono:

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

2.21.3 A+P (Address plus port)

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

Concetto di spostare la complessità sulle foglie.

2.21.4 Mapping Address and Port (MAP)

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

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

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

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

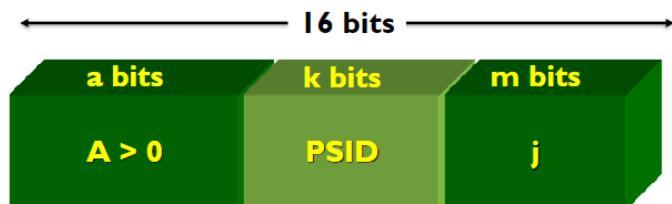


Figura 2.35: Port set

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

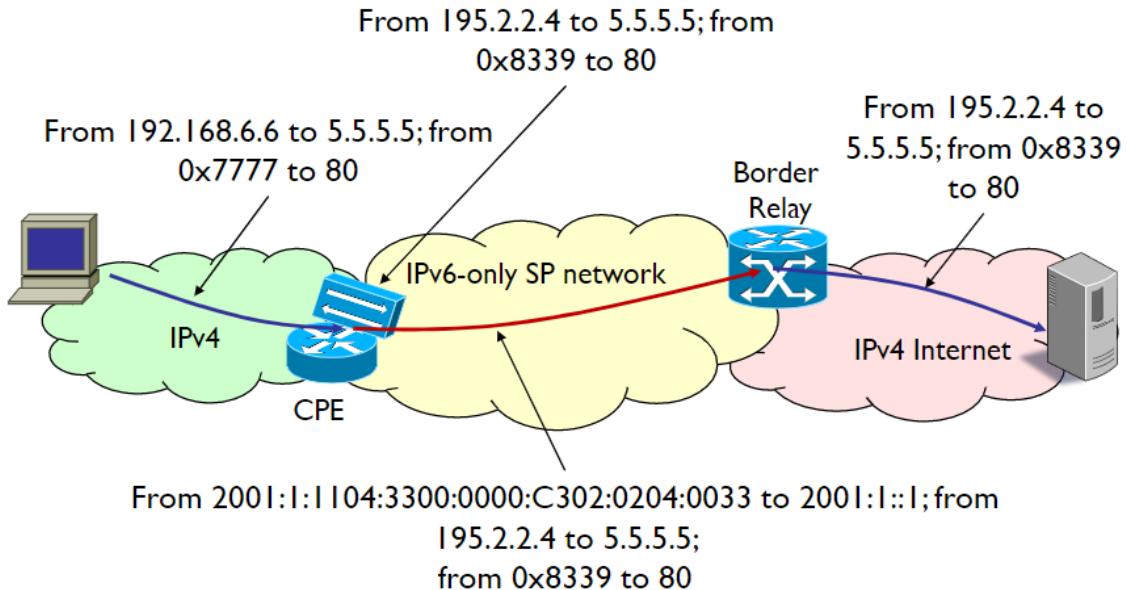
il CPE è associato a un unico valore del PSID. Queste informazioni viene messa nel Embedded address (EA).

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

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

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

2.22 MAP-E



2.23 MAP-T

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

2.24 Nat64 + DNS64

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

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

3 Reti Wireless e cellulari

3.1 Introduzione

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

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

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

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

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

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

- quam256
- quam16
- bpsk

Un ulteriore problema che ritroviamo all'interno delle reti wireless è 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.

3.2 Wireless LAN

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

Un BSS (Basic Service Set) contiene:

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

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

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

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

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

3.3 IEEE 802.11: multiple access (CSMA)

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

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

3.3.1 CSMA/CA

Il dispositivo che invia:

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

Il dispositivo che riceve:

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

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

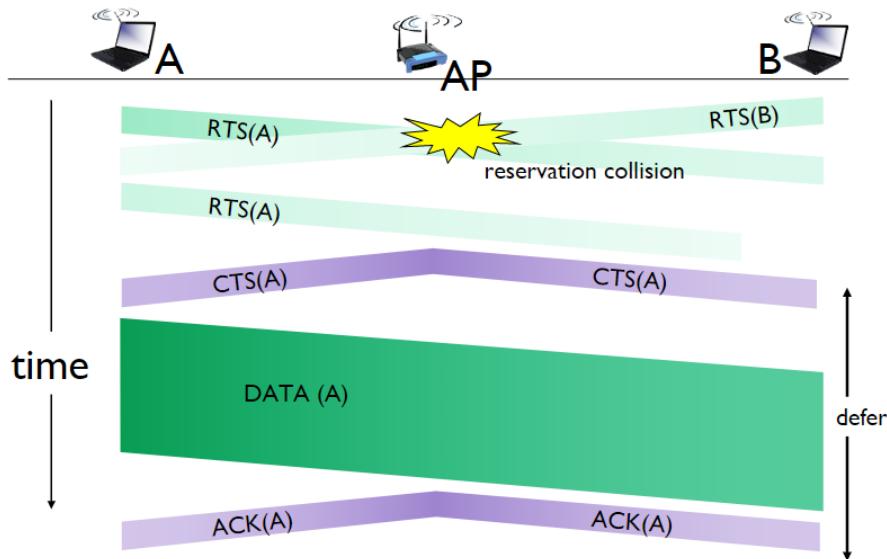


Figura 3.1: Schema temporale RTS-CTS

3.3.2 Frame addressing

Il frame contiene:

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

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

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

3.3.3 Mobilità

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

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

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

3.4 Reti Cellulari

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

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

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

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

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

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

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

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

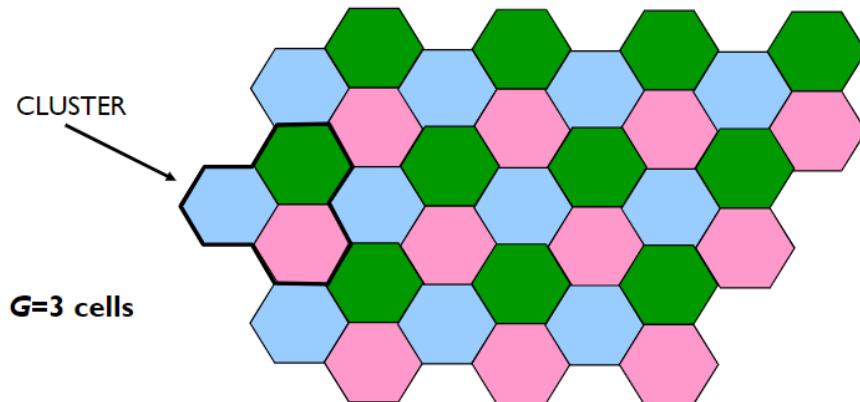


Figura 3.2: 3-Cell Cluster

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

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

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

3.4.1 Splitting

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

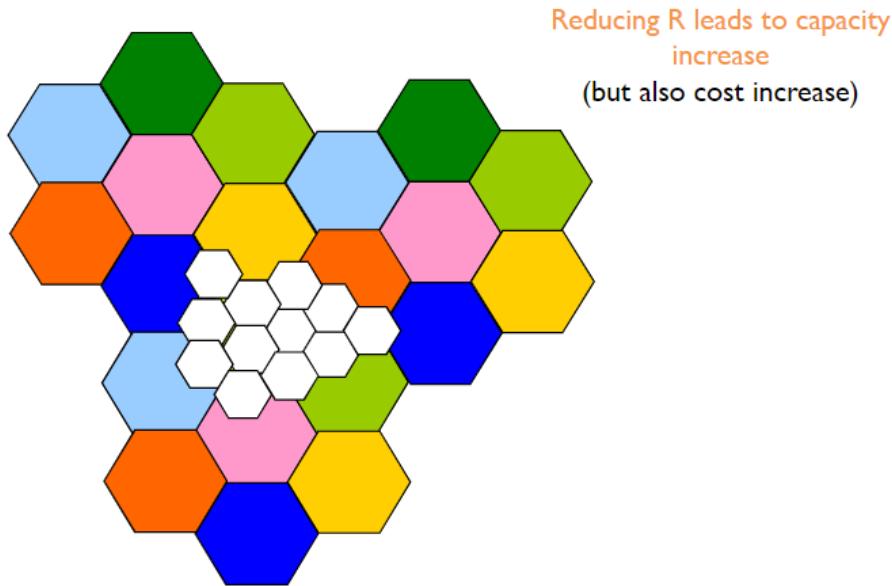


Figura 3.3: Splitting

3.4.2 Cell shaping

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

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

3.4.3 Power Control

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

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

3.4.3.1 Open loop

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

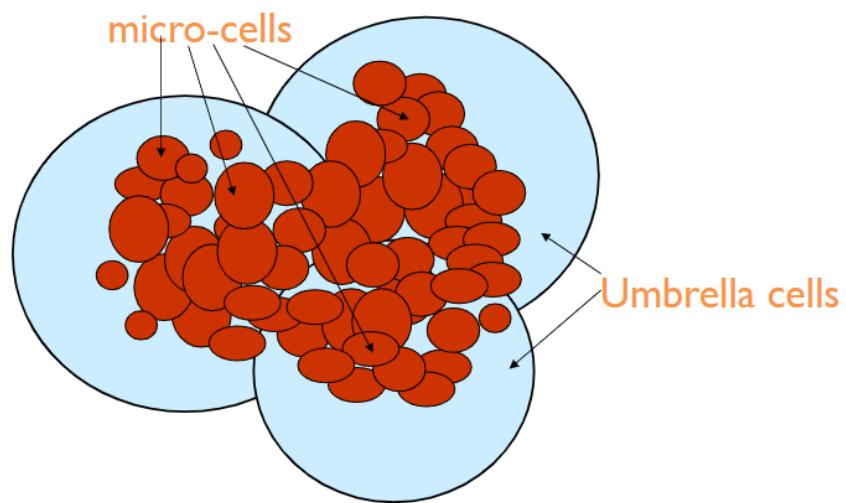


Figura 3.4: Shaping

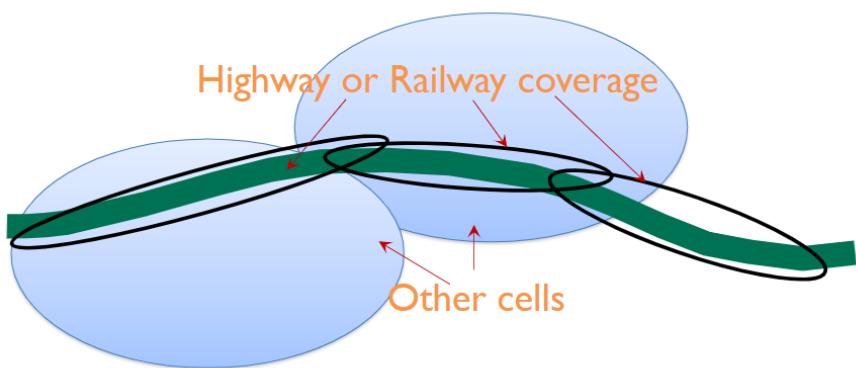


Figura 3.5: Shaping su strade

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

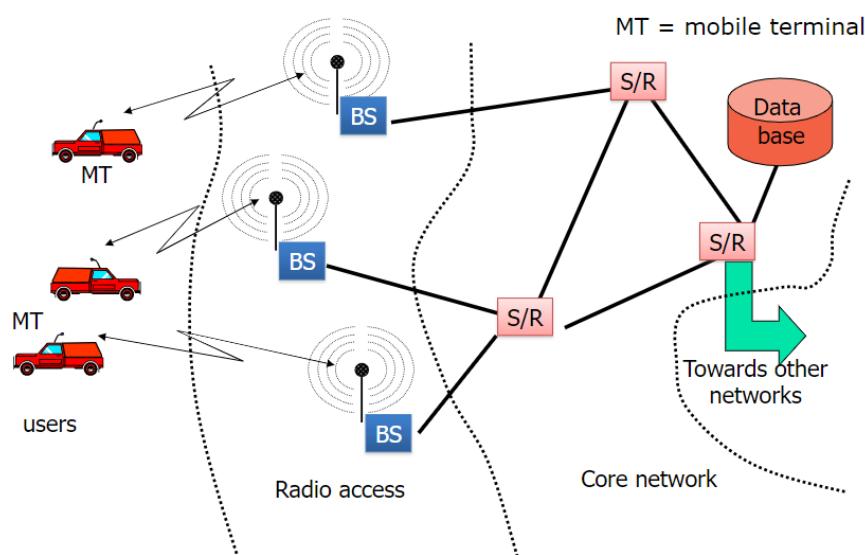
3.4.4 Frequency allocation

L'allocazione delle frequenze possono avvenire nei seguenti modi:

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

3.4.5 Architettura di rete

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



3.4.6 Registrazione

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

3.4.7 Mobility Management

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

- Roaming
- Location updating
- Paging
- Handover

3.4.7.1 Roaming

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

3.4.7.2 Location updating

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

3.4.7.3 Paging

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

3.4.7.4 Handover

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

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

3.5 Evoluzione della rete cellulare

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

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

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

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

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

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

3.5.1 GSM

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

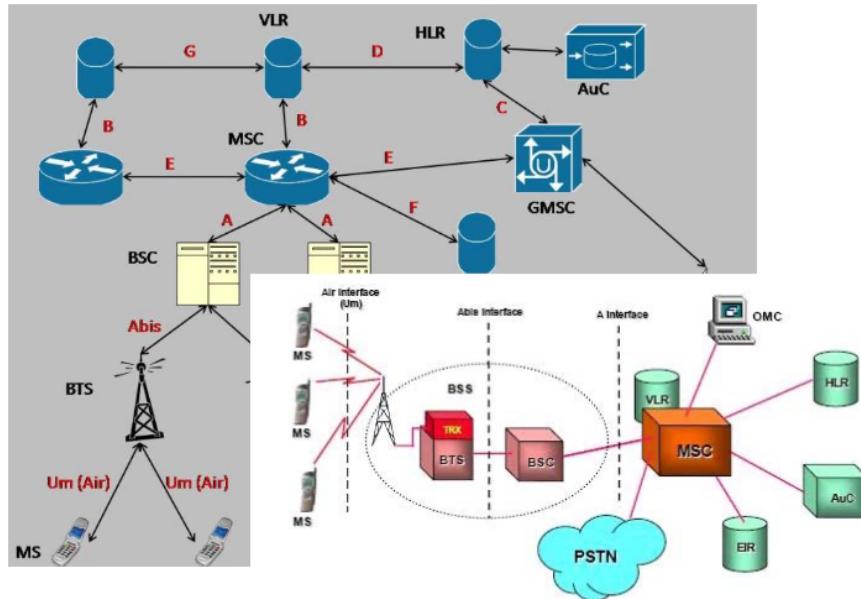


Figura 3.6: Architettura GSM

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

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

La MS 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, crittografato, le informazioni dell'utente come il numero di telefono, i servizi accessibili, parametri di sicurezza etc. MSI è l'identificativo univoco della SIM.

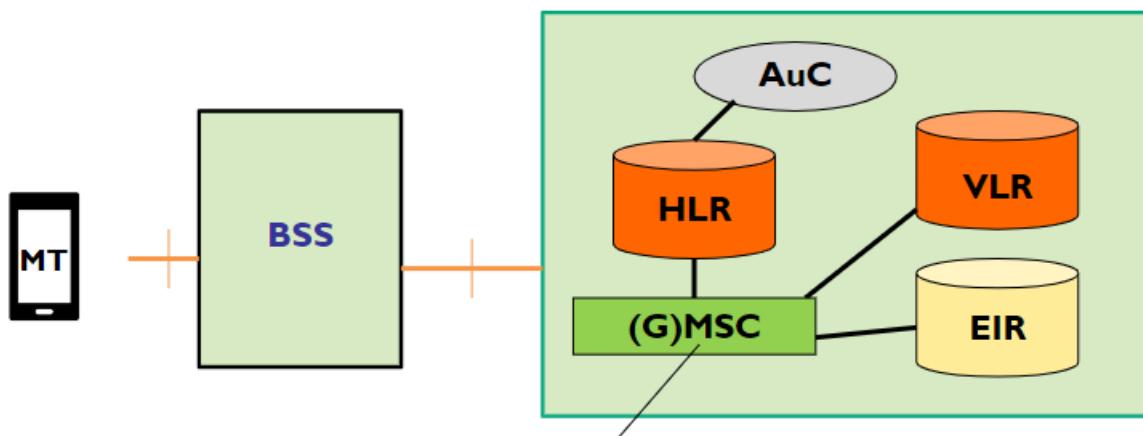
La Base Station Subsystem (BSS) comprende:

- **BTS (base transceiver station)**: interfaccia fisica con il compito di trasmettere e ricevere.
- **BSC (base station controller)**: gestisce il controllo delle risorse sull'interfaccia radio. BSC e BTS comunicano con un link 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. Il suo ruolo principale è quello di eseguire il transcoding vocale a 13 kb/s / 64 kb/s, eseguire il paging, radio

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

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

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



{width=450px}

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

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

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

frames, ciascuno di 8 slot.

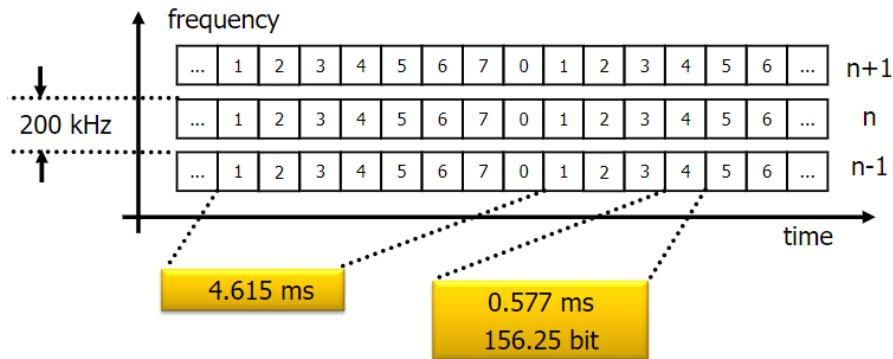


Figura 3.7: Accesso al canale

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

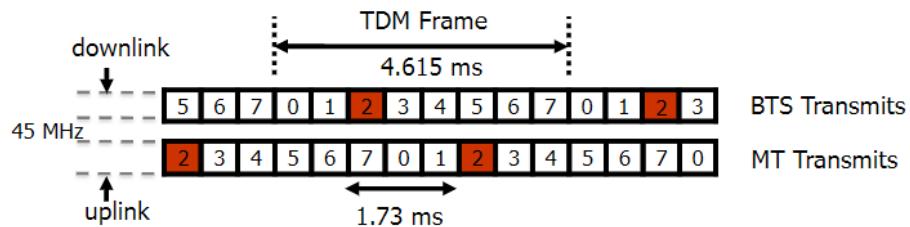
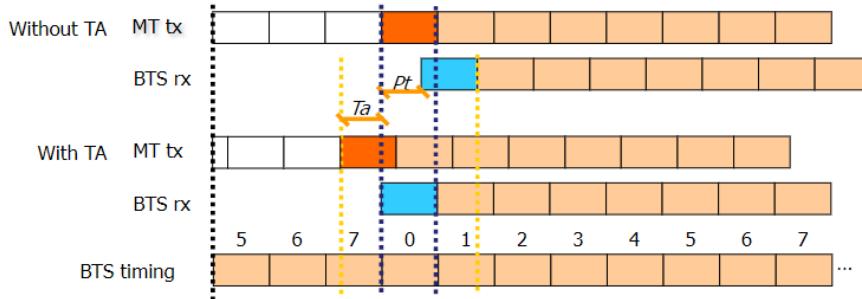
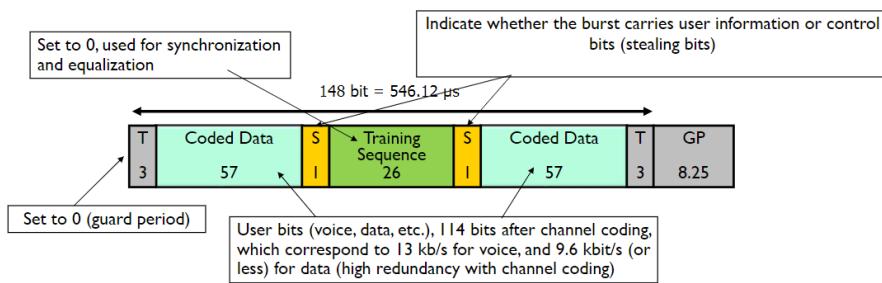


Figura 3.8: GSM frame

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

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

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

**Figura 3.9:** Timing advance**Figura 3.10:** Burst structure

3.5.2 4G/LTE

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

Le frequenze utilizzate dipendono dalla 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.

Nella terminologia compaiono inoltre i termini:

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

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

Le BS vengono denominate eNodeB.

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

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

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

3.5.2.1 Bearers

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

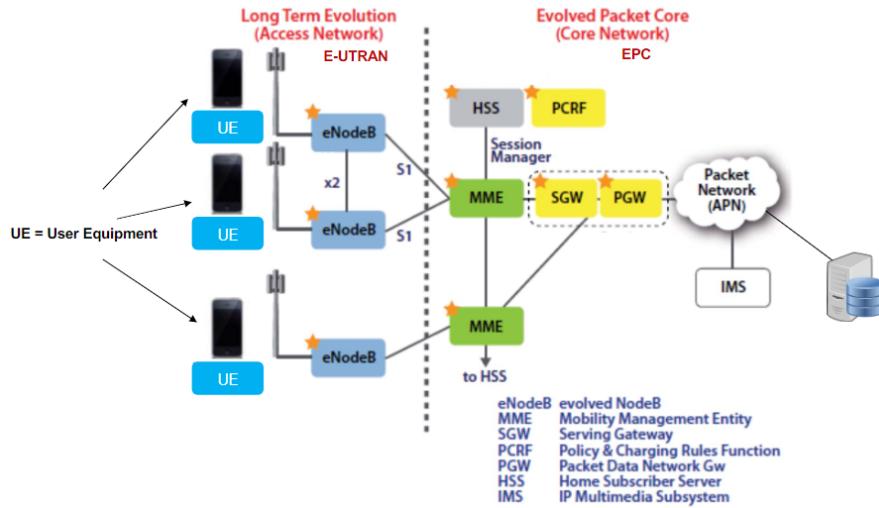


Figura 3.11: LTE architecture

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

Sono presenti in particolare tre differenti bearers:

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

3.5.2.2 E-UTRAN

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

3.5.2.3 Data Plane e Control Plane

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

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

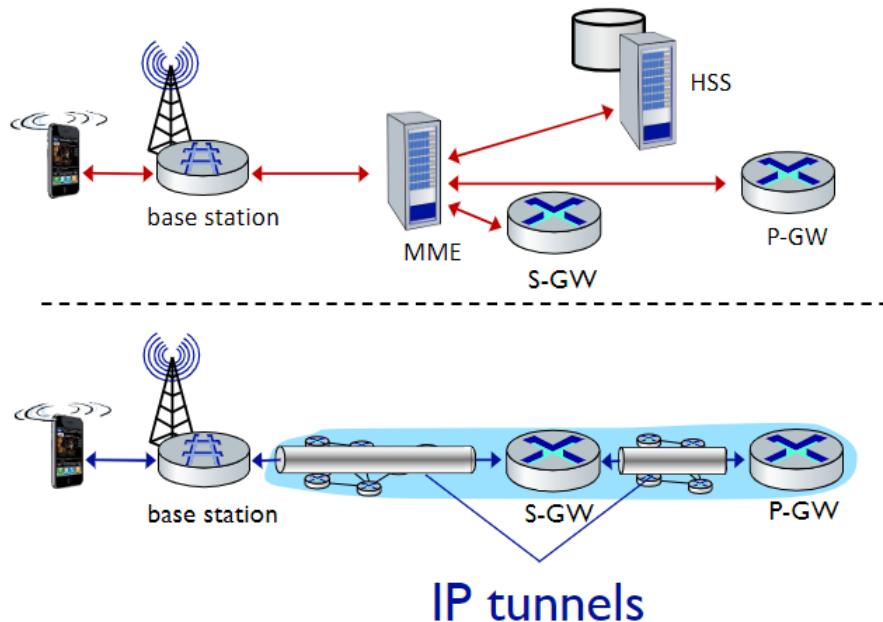


Figura 3.12: Data Plane (basso) e Control Plane (alto)

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

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

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

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

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

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

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

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

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

Un nodo per associarsi a una base station deve eseguire vari step. Periodicamente la base station invia su tutte le frequenze un broadcast primary 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 innatività, il dispositivo si mette in deep sleep. In questo modo si risparmia molto energia. Si da per scontato che l'utente debba ripartire da zero in quanto anche la cella potrebbe essere cambiata.

3.5.3 5G

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

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

Alcuni utilizzi potrebbero essere:

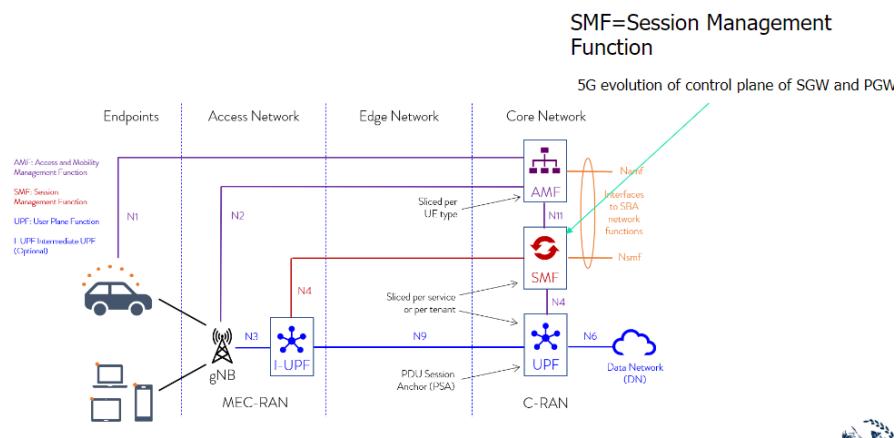
- **eMBB:** enhanced mobile broadband, come in una rete 5G sia possibile usare servizi ad alta qualità per utenti mobili
- **mMTC:** massive machine type communication, comunicazione industriale a bassa latenza.
- **URLLC:** Ultra-Reliable Low-Latency Communication, in grado di garantire latenze fino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

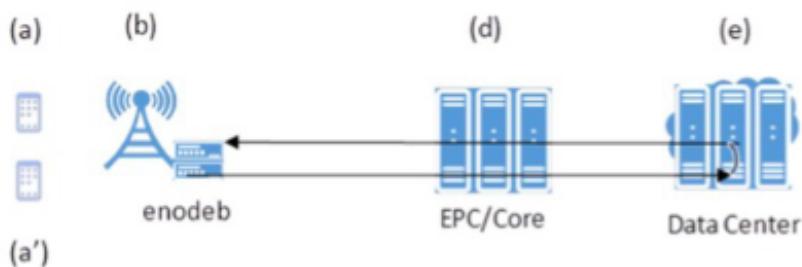


3.5.3.1 Edge Network

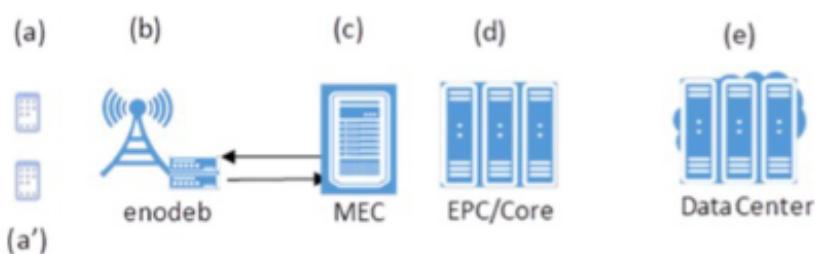
L'infrastruttura edge network fornisce servizi IT e cloud computing ai dispositivi mobili, in prossimità dei mobile subscribers. La standardizzazione è cominciata nel 2014 e pubblicata nel 2017. I benefici attesi sono:

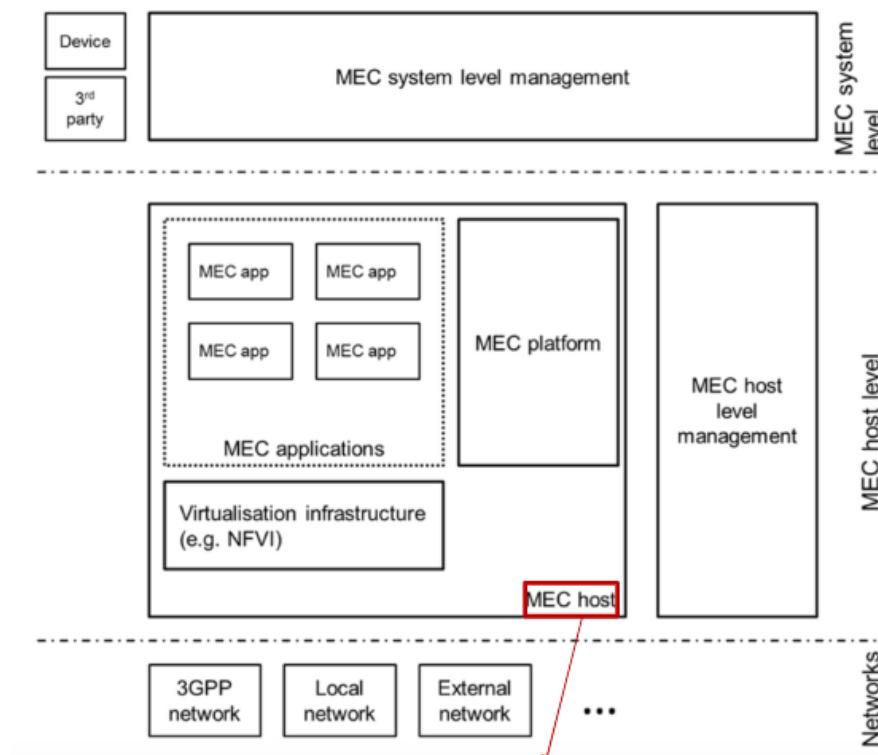
- ultra low latency
- alta bandwitch
- accesso real time alla radio network
- contextual information
- location awareness
- flexible and exendable framework for services

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.

3.5.3.2 Radio Access Network

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

3.6 Mobilità nel 4G/5G

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

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

La configurazione della data plane tunnel per i dispositivi avviene:

- **S-GW a BS tunnel**: quando il dispositivo cambia base station, 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

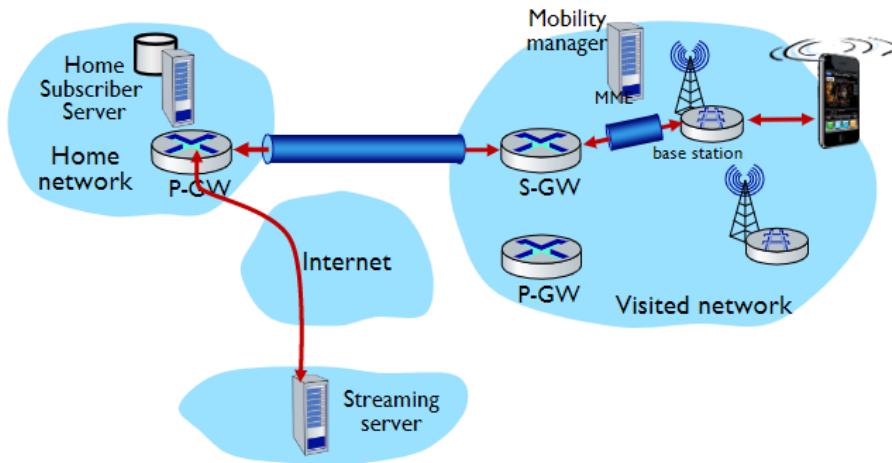


Figura 3.13: Configuring data plane

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 appaiono negli anni 60, con la presenza di alcuni mainframes e la necessità di connettersi da remoto (ad esempio 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 i costi erano abbastanza bassi da non necessitare più dei mainframe (ancora usati ma per motivi differenti).

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

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

In breve, i dispositivi lan si differenziano in:

- ripetitori: hub, stesso collision domain
- bridge: switch, collision domain separato ma stesso dominio di broadcast
- router, L3 switch, separate broadcast domains

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, ovvero una struttura a stella. Tutti i dispositivi connessi a un hub appartengono allo stesso dominio di collisione.

4.2 Bridge

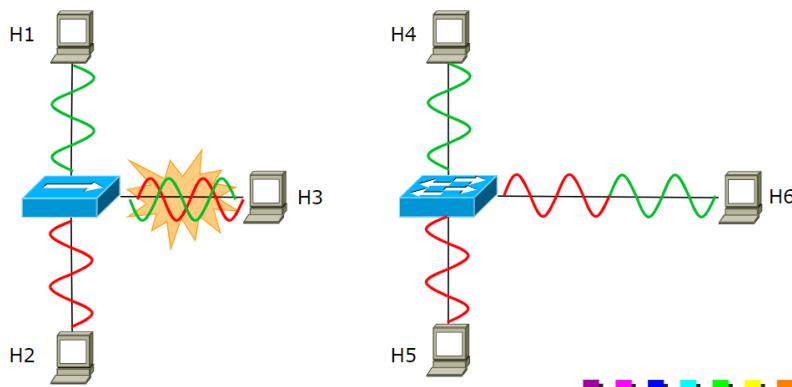
Il bridge è un dispositivo di *livello 2* e pertanto è in grado di comprendere una trama ethernet. Sono implementati completamente in software e composti da due porte (per questioni economiche).

Interconnettono al livello di data link (da ethernet a wifi) e hanno differenti mac (medium access mechanism, framing).

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

Non necessariamente interconnette link layer uguali (anche se oggi 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 con un unico broadcast domain (quindi il broadcast continua a funzionare correttamente).

Nota: Lo switch è un bridge a più porte



Bisogna però fare attenzione al fatto che sui singoli spezzoni di rete possono però esserci ancora collisioni, che vengono risolti 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.

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 ci riferiamo a switch facciamo in realtà riferimento a switch ethernet. Non è più necessario CSMA/CD (non definito per portata sopra 1GE).

Le wireless lan funzionano in modo completamente diverso e troviamo ancora gli hub.

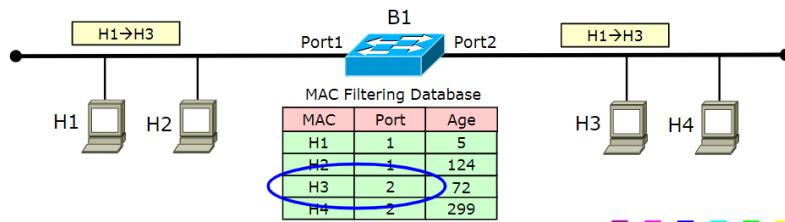
I bridge e gli switch in ethernet prendono il nome di **transparent bridge** (anche altri non trasparenti sono stati proposti ma non più utilizzati). Il nome significa che deve essere plug & play e non dovrebbe

richiedere una configurazione manuale. Inoltre, per l'utente non deve cambiare nulla e deve funzionale ugualmente (se non meglio) rispetto agli hub. I sistemi finali devono funzionare con o senza bridges.

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

Gli switch hanno indirizzi MAC ma definizione (ogni prodotto è marchiato), ed è necessario per consentire di indirizzare il traffico e gestione dei management frames.

Un filtering database è una tabella contenente la posizione di ciascun mac address trovato nella rete, corredata 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.



La tabella ha componenti statiche che automatiche.

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.

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 mi muovo non è che smetto di trasmettere il traffico! Per cui al prossimo pacchetto le informazioni verranno aggiornate.

C'è ancora un problema però se utilizzo una topologia a maglia, in particolare se mando un pacchetto broadcast: 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

4.4 Multiple LANs

Per ragioni di sicurezza o semplice preferenza, è possibile dividere una rete in più parti generando più 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 che consentono di simulare che porte specifiche di uno switch faccia parte di un dominio di broadcast

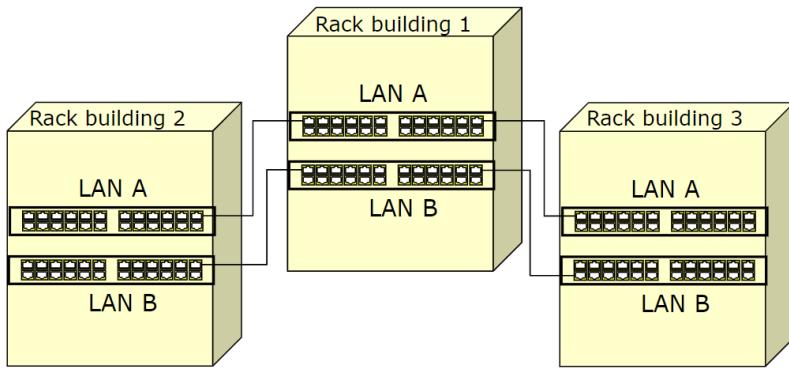
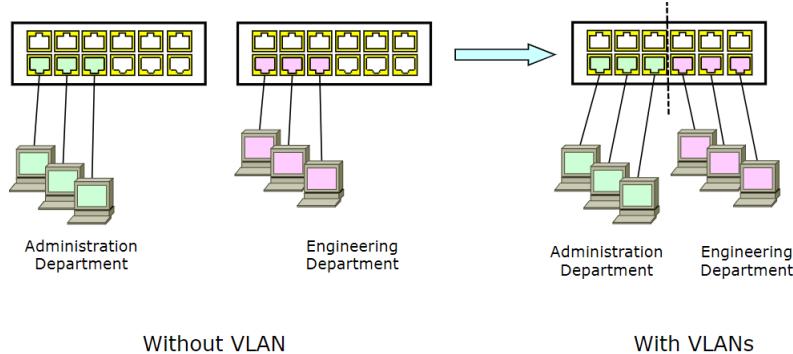


Figura 4.1: Esempio di edifici per lan multipla

differenti, utilizzando una unica infrastruttura di rete. Per far parlare le virtual lan è necessario un router che ha tutte le sottoreti connesse consentendo la comunicazione come sempre, anche se la rete di origine è in realtà la medesima.



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

Come associo un frame a una vlan? Il modo più semplice è marcare il frame quando arriva. Fino a quando la trama non è alterata, questa sarà evidenziata solo all'interno dello switch, ma non è noto a un altro switch. Per superare questo problema è stato introdotto il tagging, un campo nella trama ethernet e fornisce 4 byte aggiuntivi al frame per il vlanID che consente di identificare.

Le configurazioni possono essere in modalità:

- **access:** invia e riceve trame non taggate, quelle che riceve le tagga localmente (??) e le invia
- **trunk:** invia e riceve trame taggate

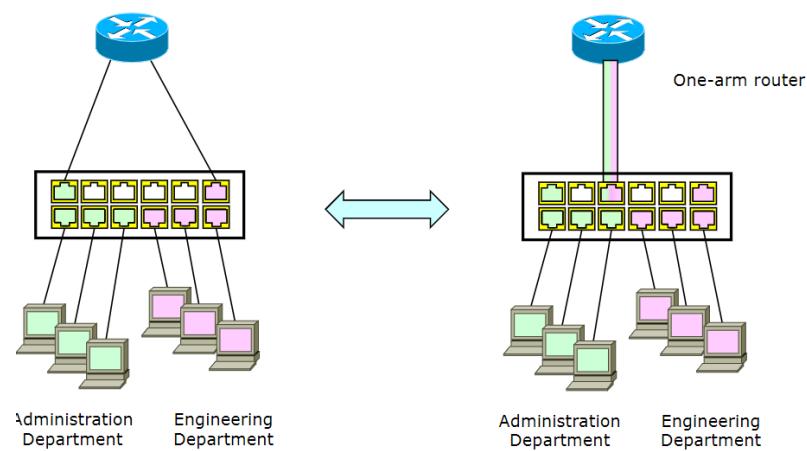


Figura 4.2: One Arm

5 VPN

Una VPN, Virtual Private Network, è un insieme di tecnologie che consente di realizzare una connettività tra due sottoreti distinte in modo che possano comunicare come se fossero una unica rete privata.

Quando ci connettiamo su internet non attraversiamo necessariamente un unico ISP, e questo rende lo scenario molto variegato.

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

Gli elementi chiave sono:

- **tunnel**: incapsulazione sicura di traffico in transito sulla rete condivisa (non presente in alcune soluzioni)
- **vpn gateway**: apre e termina i tunnel, dovranno supportare il protocollo specifico 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)
- **end o 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**: interconnettere uffici remoti della stessa azienda (due sedi di aziende diverse)
- **Extranet VPN**: interconnettere aziende diverse

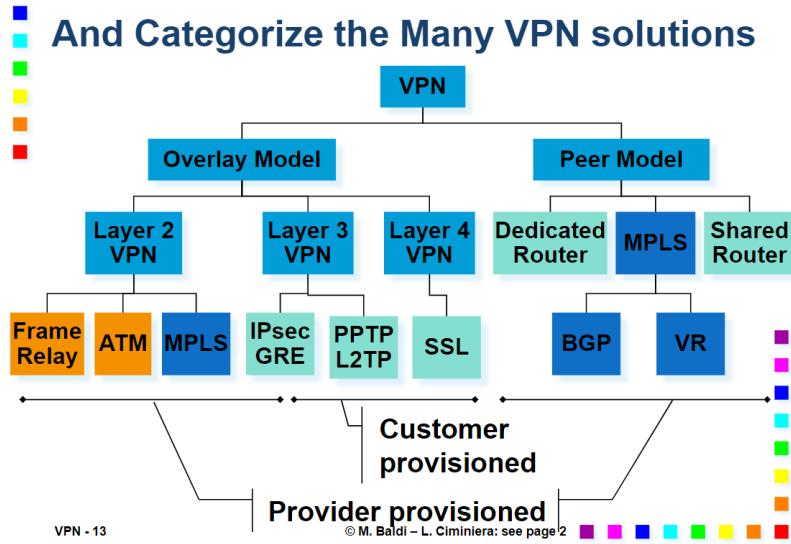


Figura 5.1: Gerarchia dei protocolli

A livello di extranet abbiamo interesse a ridurre l'accesso alle risorse di rete fra le reti connesse mediante firewall, Ottenere l'overlapping Address Spaces mediante network address translation e controllare il traffico in modo che il traffico dei partner non possa compromettere la rete aziendale.

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 totale da e verso internet. L'accesso è centralizzato e controllato da firewall. Il pro 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 pro sono dei costi ridotti.

5.1 Deployment Models

Le features che la VPN mette a disposizione sono:

- Separate Data
- Increase protection
- prevent tempering
- identify source

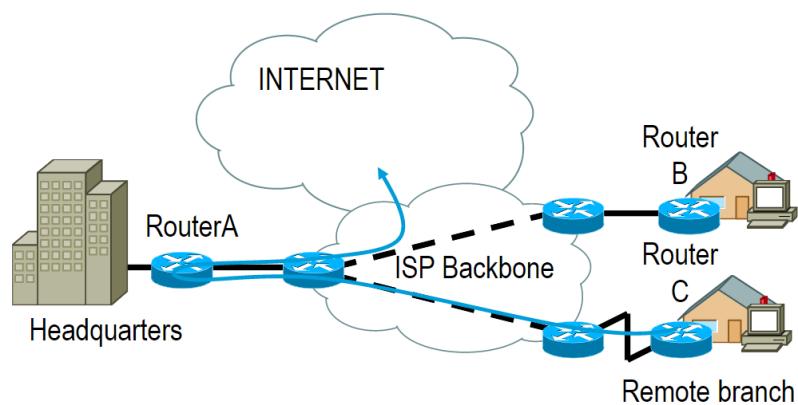


Figura 5.2: Accesso centralizzato

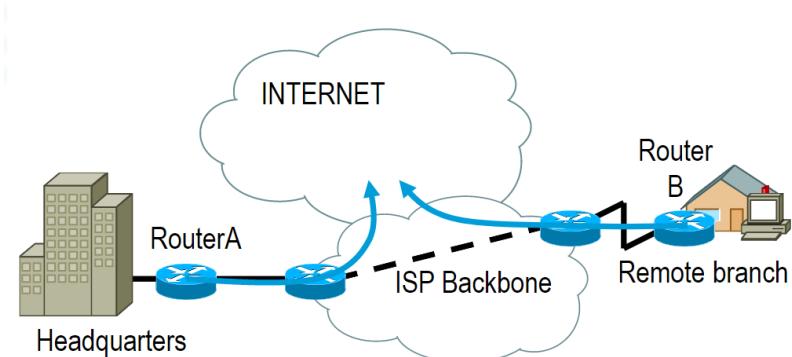


Figura 5.3: Accesso distribuito

5.1.1 Site to Site VPN

I tunnel site to site significa che la garanzia delle 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 sta all'interno della rete l'attacco può avvenire ugualmente.

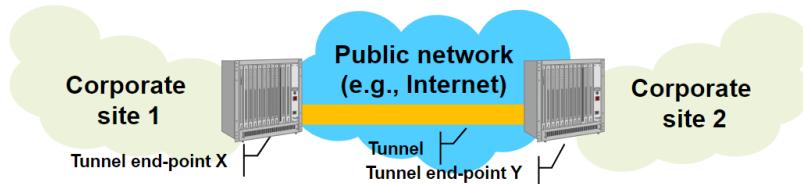


Figura 5.4: S2S tunneling

5.1.2 End to End VPN

Maggiore sicurezza, si crea un tunnel diretto tra i due host. Fin dall'inizio della comunicazione il traffico mantiene le stesse politiche di rete. In termini di complessità è molto più onerosa sia in termini di costo che di gestione.

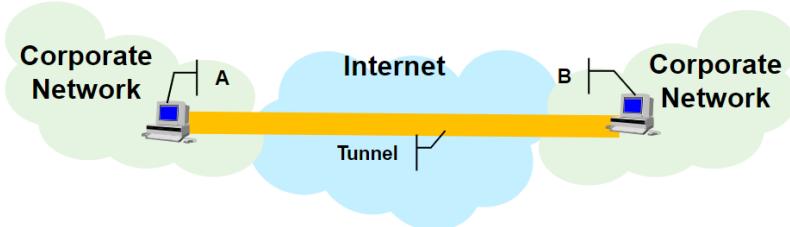


Figura 5.5: E2E tunneling

5.1.3 Remote VPN

Connette un endpoint con un vpn gateway. E' possibile aggregare un'intera sottorete, ma ogni dispositivo deve essere abbastanza robusto per connettersi.

5.1.4 Overlay Model

Nel modello overlay la rete pubblica non partecipa alla realizzazione della vpn, non sa quale siano le destinazioni e la connessione avviene attraverso vpn gateways. Ciascuno deve essere in contatto con

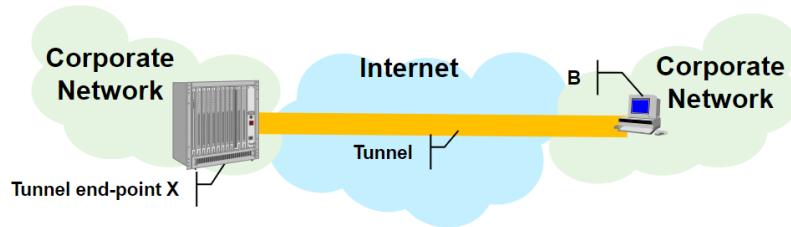


Figura 5.6: Remote tunneling

tutti gli altri generando molti tunnel mesh e 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 e del tutto trasparente (anche se il pacchetto potrebbe metterci un po' di più).

5.1.5 Peer Model

Ciascun VPN gateway interagisce con i router pubblici, scambiando informazioni di routing e il service provider fornisce le informazioni di routing. Il traffico che subisce routing sulla rete pubblica si muove all'interno della stessa rete VPN.

In questo approccio miglioriamo il routing, ma chi realizza la vpn è fortemente coinvolto alla comunicazione di rete (e 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

Il cliente implementa la soluzione VPN e possiede, configura e gestisce i dispositivi connessi adoperando del customer equipment. 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 attivarlo, se non è attivo può operare ugualmente senza VPN.

5.1.7 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 comporta come se si trovasse all'interno di una rete privata, i terminatori dei tunnel sono dei Provider Equipment. E' meno costosa ma devo fidarmi del provider.

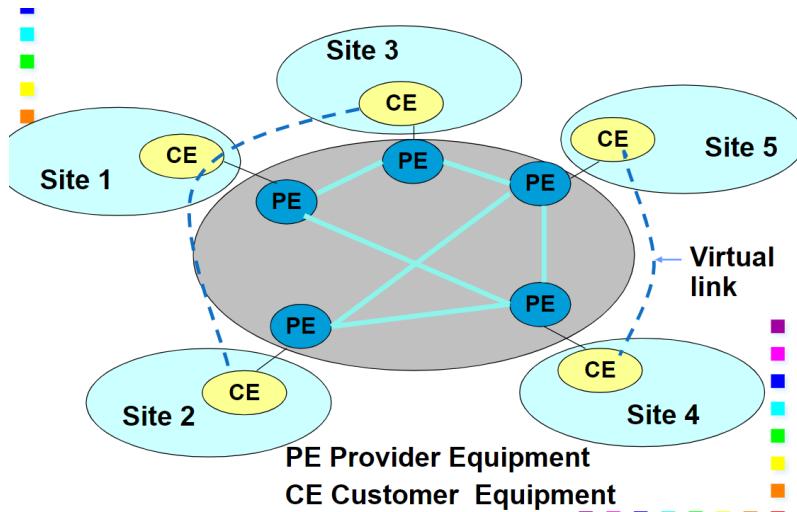


Figura 5.7: Customer Provisioned VPN

Il remote host deve essere sempre nella VPN, obbligo all'utente di installarsi determinati dispositivi. Si ha solamente un indirizzo, sono sempre all'interno della VPN e richiede l'accesso a uno specifico Internet Service Provider.

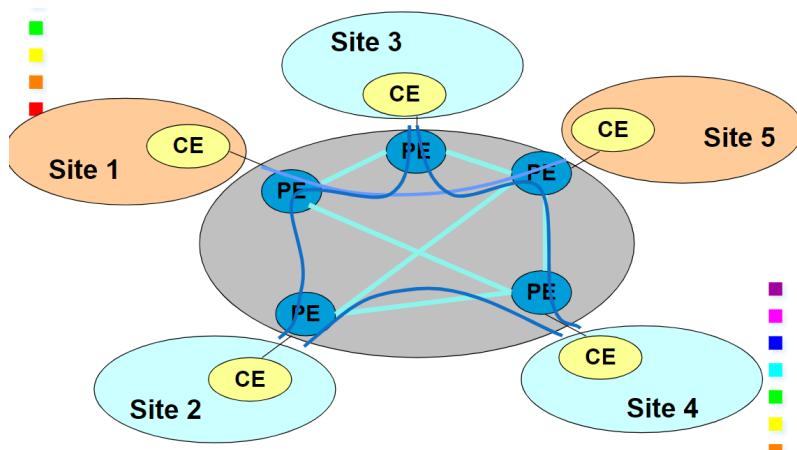
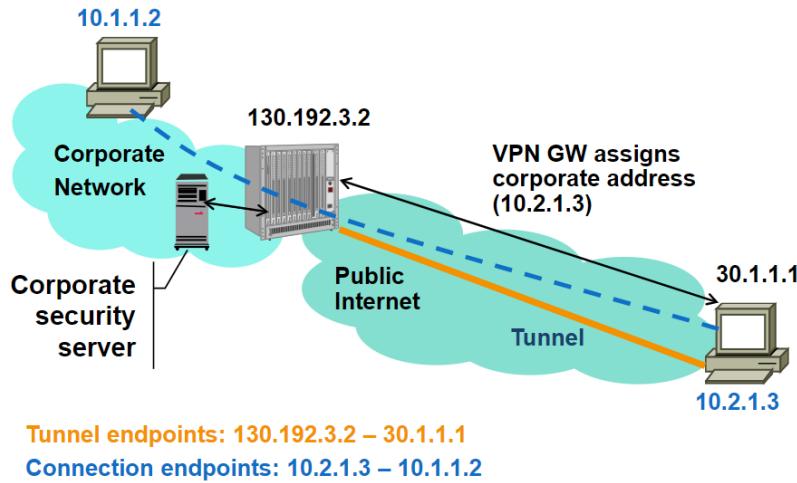


Figura 5.8: Provider Provisioned VPN

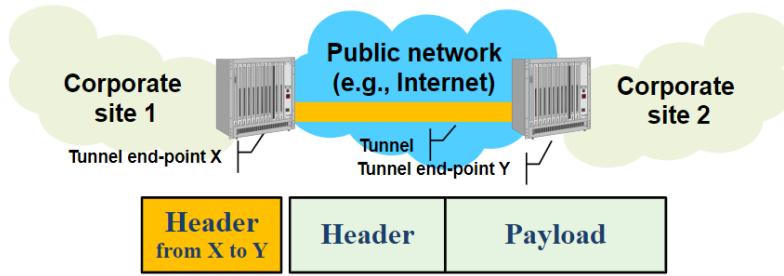
5.1.8 Access VPN Customer Provisioned

Bisogna considerare anche aspetti inerenti al piano di indirizzamento. Sui terminatori della vpn è necessario avere anche un indirizzo pubblico, costringendo ad avere due indirizzi. Tipicamente le remote access sono più semplici a livello di customer provisioner.

**Figura 5.9:** 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 5.10:** Tunneling

5.1.10 Topologie

Le (virtual) VPN si differenziano in due tipologie:

- 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-optima e sono richiesti pochi tunnel, con però il rischio che l'hub possa diventare un bottleneck.
- Mesh: Utilizza un gran numero di tunnel, più difficile da gestire ma migliora il routing.

5.1.11 Layers

5.1.11.1 Layer N

Packet transport (tunneling) provided da Layer N protocol e/o layer N service

5.1.11.2 Layer 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 uns 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 (con ICMP e ARP) per far viaggiare i dati nella VPN.

5.1.11.3 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). I CE sono sia ip routers che IP hosts. I pacchetti (o frame) sono trasportati attraverso la rete IP come pacchetti IP, le modalità sono due:

- 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)

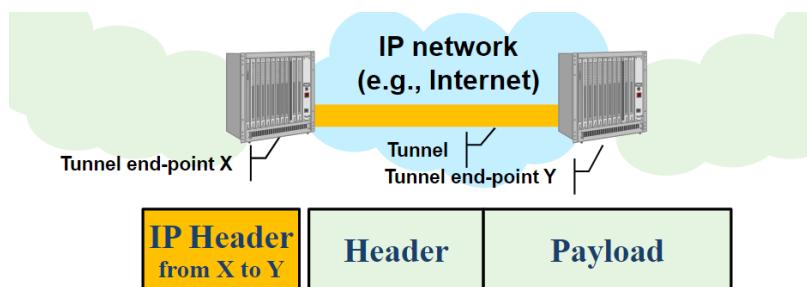


Figura 5.11: Layer 3

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

5.1.11.4 Layer 4

Le soluzioni VPN di livello 4 provvedono solo alla sicurezza, soffrono di adottare soluzioni non standard.

5.1.11.5 Site to Site (s2s)

La VPN è costruita utilizzando connessioni TCP e anche i tunnel utilizzando connessioni TCP, la sicurezza è garantita attraverso SSL/TSL. È possibile avere header di livello 3 o di livello 4.

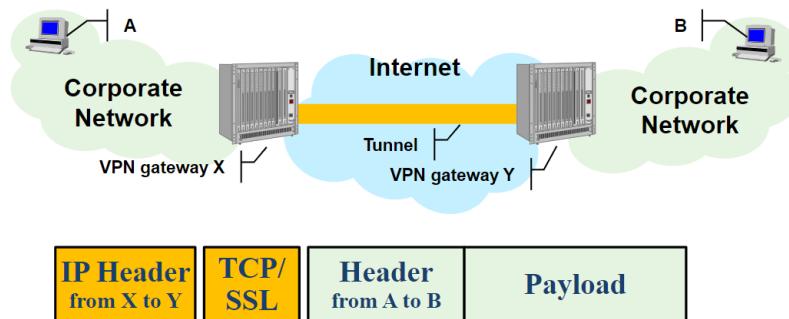


Figura 5.12: s2s

5.1.11.6 End to End (e2e)

Il tunnel è terminato da un end system.

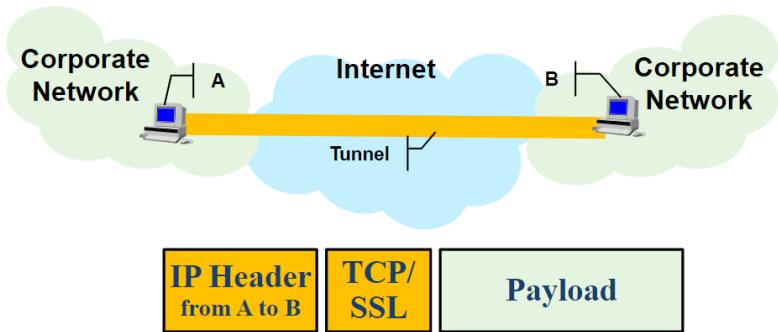


Figura 5.13: e2e

5.2 GEneric Routing Encapsulation (GRE)

E' un protocollo di livello 3 che si basa sul concetto di incapsulamento, il formato utilizzato è il seguente:

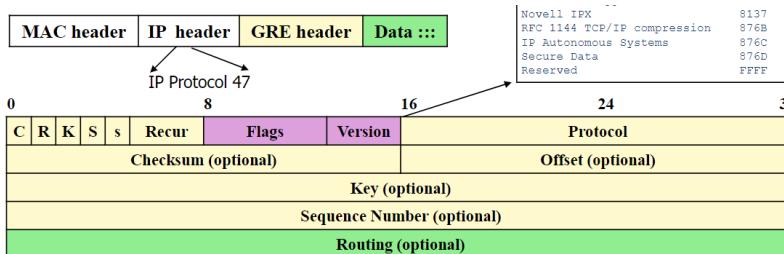
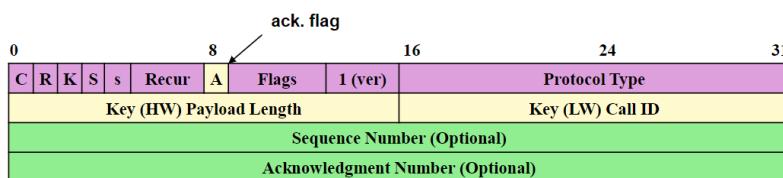


Figura 5.14: Formato del pacchetto

Possiamo notare alcuni campi dell'header:

- **C, R, K, S:** flag che indicano la presenza o l'assenza di alcuni campi opzionali
- **s:** se vado a fare il source routing
- **recur:** Massimo numero di volte che il pacchetto può essere incapsulato (deve essere 0)
- **protocol:** id del protocollo per il payload (nessuno mi vieta di metterci ulteriori protocolli)
- **routing:** Sequenza del'indirizzo del router IP per ASs per source routing

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



Alcune funzionalità avanzate:

- key (16 bit alti), payload length: numero di bytes escludendo l'header GRE
- key (16 bit bassi), Call ID: 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 (comulative ACK)

altri meccanismi presenti in GRE:

- **flow control:** sliding window mechanism

- **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

5.3 Layer 2 frame within an IP packet

Nota: Questi protocolli di livello 2 non sono domande che poi compaiono all'esame. Cosa differente nel caso GRE e IPsec.

Per le Access VPN sono disponibili due protocolli:

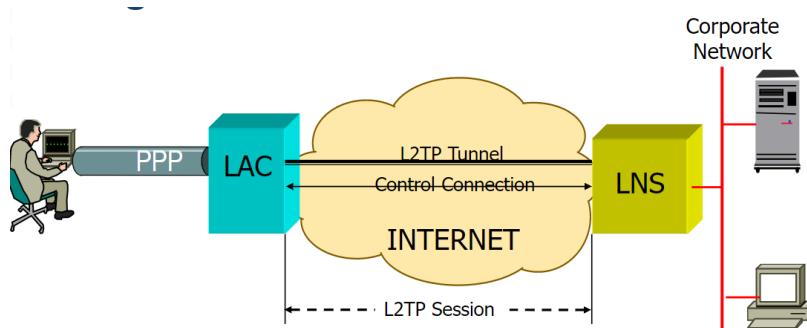
- L2TP (Layer 2 Tunneling Protocol): inizialmente sono provider provisioner e non molto implementato sui terminali. E' indipendente dal protocollo di livello 2 sul host e la sicurezza è garantita da IPsec.
- PPTP (Point to Point Tunneling Protocol): customer provisioner, originariamente proposto da Microsoft,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

5.3.1 L2TP

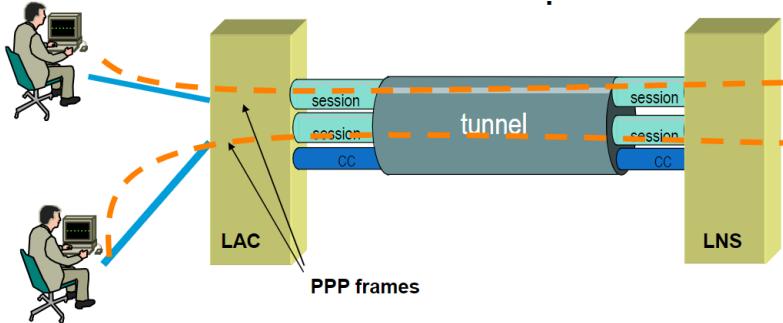
Le due componenti principali sono:

- 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



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



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 connectin 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:

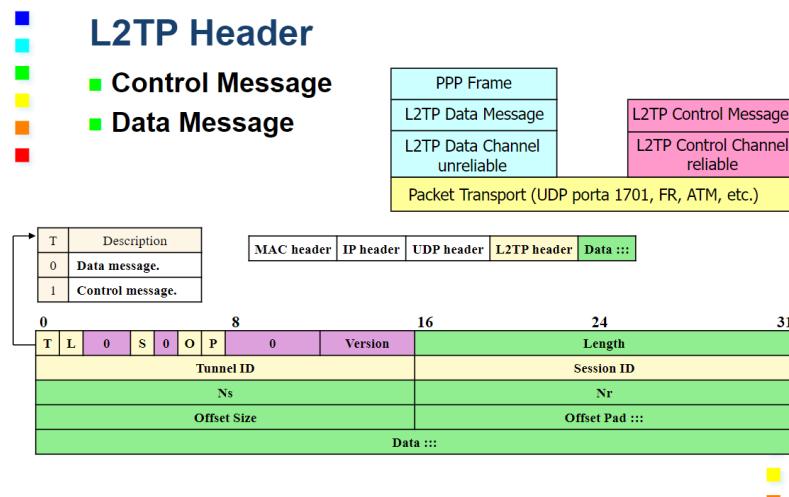


Figura 5.15: L2TP

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).

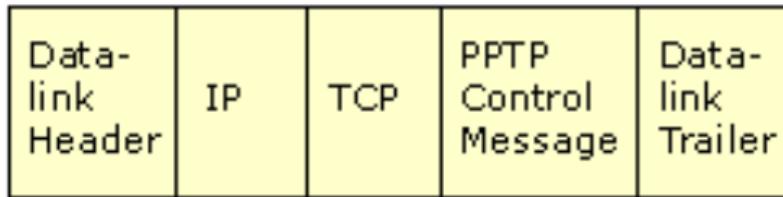
5.3.2 Point to Point Tunneling Protocol (PPTP)

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 uno per il data tunneling.

Data-link Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	Data-link Trailer
------------------	-----------	------------	------------	---	-------------------



5.4 IPsec

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

Si basa sull'utilizzo di due 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, che sta per 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 come sempre (non NAT).

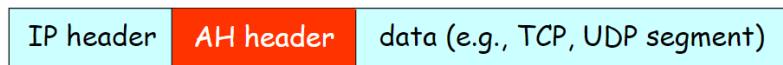


Figura 5.16: AH header

La differenza tra l'integrità di AH e di ESP risiede sul tipo:

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

ESP garantisce la confidenzialità dei dati, data e esp trailer sono crittografati e il next header è presente nel esp trailer. Fornisce l'autenticazione dell'host e l'integrità dei dati, con una autenticazione simile a quella di AH. Il protocol field è 50.

Le security association (SA) negozia prima di cominciare lo scambio di pacchetti IPsec. Hanno canali a logica unidirezionale e utilizzano dei Security Parameter Index (SPI) nel header/trailer IPsec che identificano le SA. Viene specificato quali proprietà di sicurezza necessito.

Viene utilizzato il protocollo Internet Key Exchange (IKE) per stabilire e mantenere le SA in ipsec. Una IKE SA è stabilita per la comunicazione sicura dello scambio dei messaggi IKE. Una o più "figli" SA sono

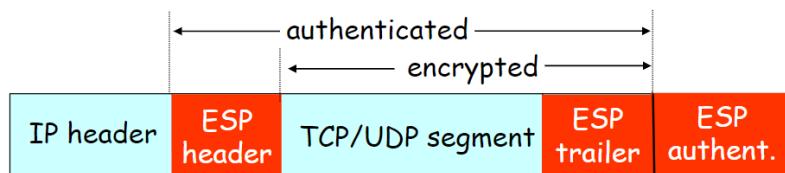


Figura 5.17: ESP header

stabiliti per la comunicazione sicura dei dati. Tutti le SA figlie utilizzano la negoziazione di chiavi tramite IKE SA (potrebbero tutti partire da uno shared secret), con la possibilità di utilizzare certificati.

5.5 SSL VPN

Utilizzano SSL per assicurare il meccanismo di sicurezza. 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 le cose cambiano rispetto al modello classico.

Il modello di trasporto è sempre TCP o UDP.

Uno dei principali grossi problemi è che non sono soluzioni standard, per cui essendo utilizzati protocolli proprietari diventa più complicato.

Perchè non si dovrebbe utilizzare VPN? Perchè può essere troppo costoso per essere utilizzato in modo sicuro: troppe opzioni. Inoltre perchè opera a livello kernel, per cui installazioni sbagliate possono avere problemi catastrofici.

Utilizzare SSLVPN hanno come vantaggio:

- Minore complessità (installazione, configurazione, gestione)
- Non interferisce con il kernel
- Molto più utilizzate
- Maggiore sicurezza (SSL)
- Non ci sono problemi di attraversamento del nat o di mascheramento

Il grosso svantaggio è però che i pacchetti vengono droppati a un livello più alto, rendendolo critico all'attacco DOS.

Le soluzioni più diffuse sono:

- **ip over tcp:**
- **tcp over tcp:**
- large transmitter buffers in gateways

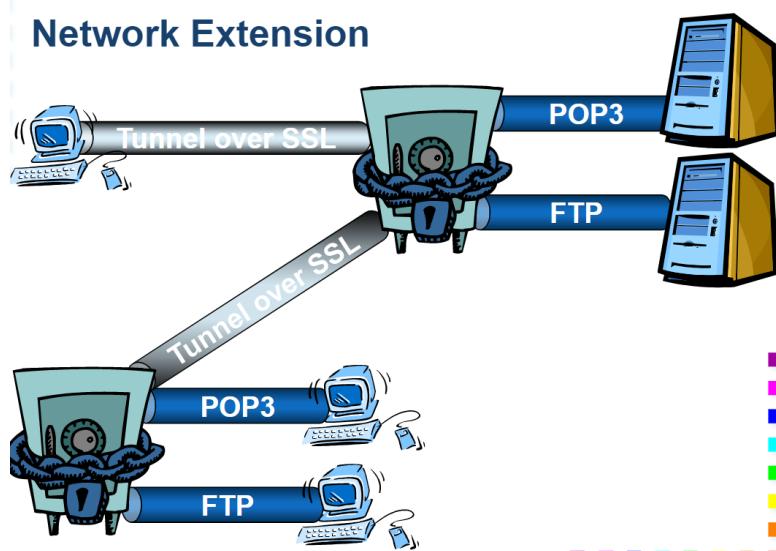
Le principali problematiche sono:

- **interoperabilità:** client e server devono installare lo stesso software.
- **features specifiche del produttore**
- ogni implementazione potrebbero avere dei 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 ssl vpn connettono utenti a servizi o client application a server application.

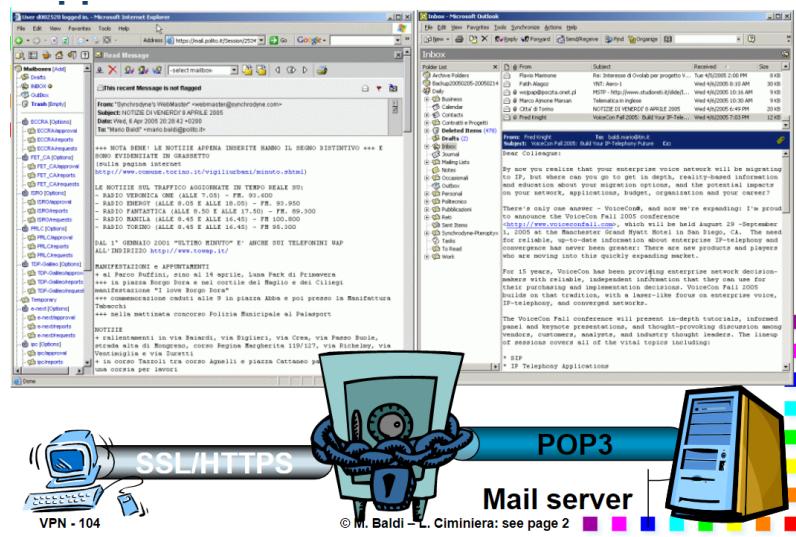
Riassumendo: utilizzano tunneling TCP o UDP, forniscono NAT traversal, packet filter traversal, router traversal e utilizzano client universali (web browser)

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



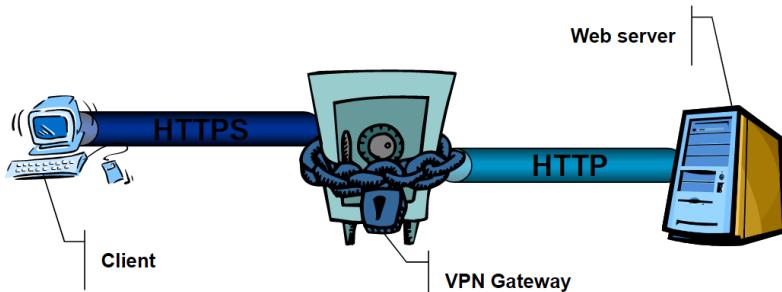
5.5.1 Application translation

Protocolli nativi tra il VPN server e l'application server. Il gateway spezza in comunicazione sicura e non sicura.

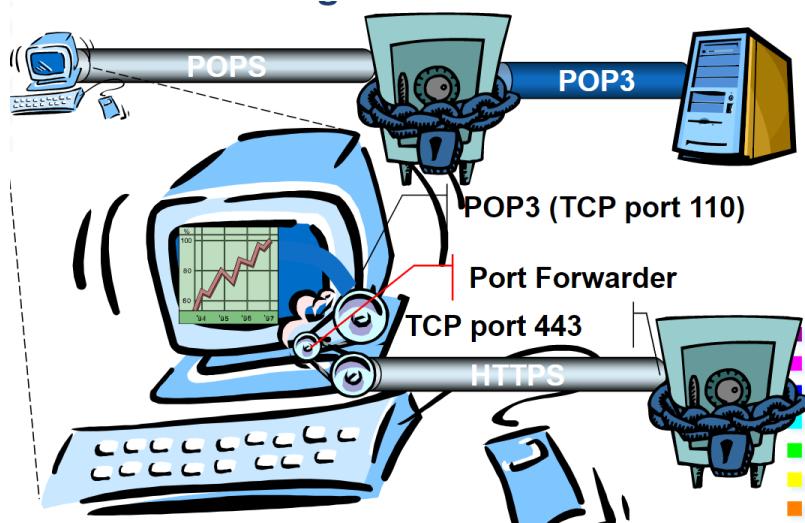


5.5.2 Application proxy

VPN gateway download web pages attraverso http e le invia tramite https



5.5.3 Port forwarding



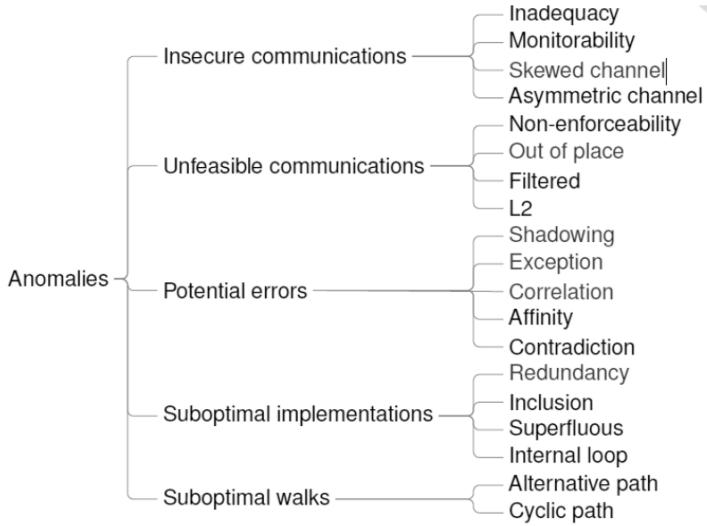
5.6 VPN Gateway Positioning & anomalies

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

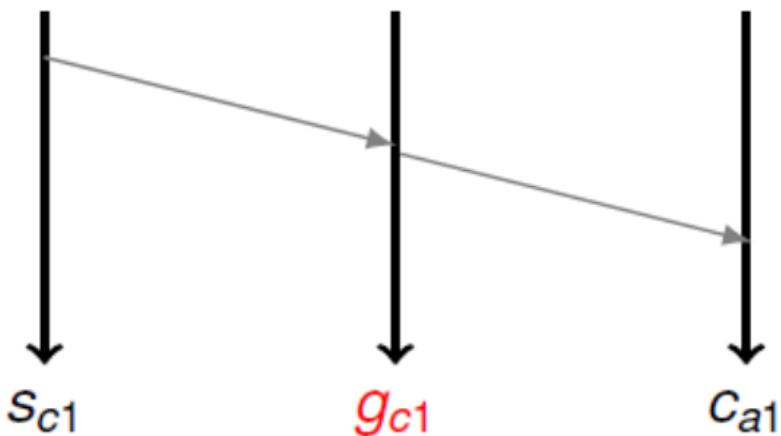
5.6.1 Anomalies

Diversi tipi di problemi:



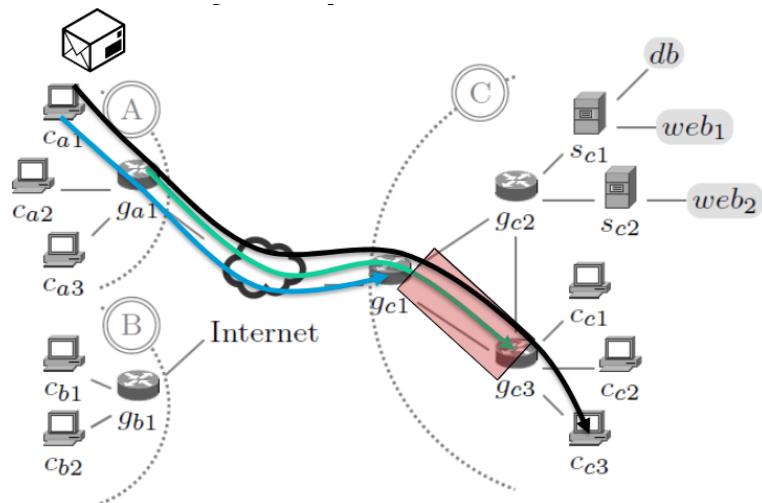
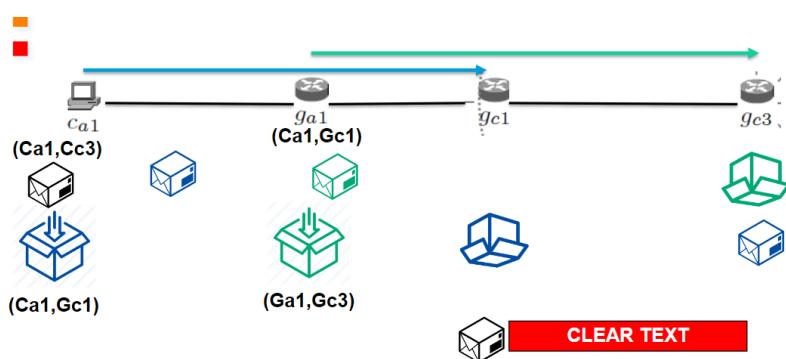
5.6.2 Monitorability anomaly

Si ha un monitorability anomaly quando un nodo del canale “congiunto” può vedere lo scambio dei dati.



5.6.3 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 5.18:** Parte1**Figura 5.19:** Parte2

6 Routing

6.1 Introduzione

Con routing si fa riferimento al percorso che i pacchetti devono compiere nella rete, mentre il forwarding è il processo di inviare pacchetti nella rete e include 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, e in base a qualche metrica definisce quale percorso è migliore rispetto a un altro. Determina quali siano le destinazioni raggiungibili.

Nota: è solitamente chiamato semplicemente *routing*.

6.1.2 On the fly routing

Comunemente definito forwarding, si occupa di gestire i pacchetti mediante informazioni locali come routing/forwarding table. E' il risultato del proactive routing o signaling e viene chiamato anche route.

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

- routing by network address: in base alla destinazione
- label swapping
- source routing

Si ha una operazione di switching, ovvero trasferire verso una porta di output, e di trasmissione.

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, configurato manualmente e di tipo statico, e il flooding and derives (selective), anche questo è un tipo di approccio statico e non cambia in base alla rete.

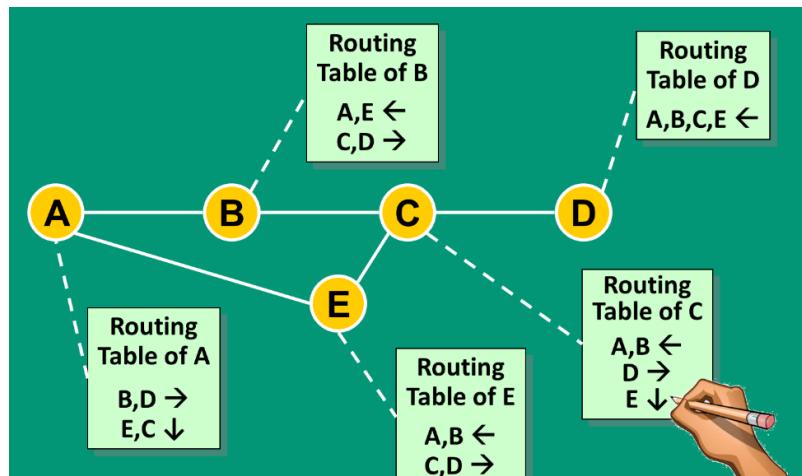


Figura 6.1: Fixed Directory Routing

Il vantaggio è che l'amministratore ha pieno controllo della rete, ma si è più soggetti ad eventuale errore e 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

Quando parliamo di **centralized routing**, si fa riferimento ad un unico nodo che si occupa di gestire la rete denominato Routing Control Center (RCC). Ha bisogno di sapere le informazioni di tutti i nodi

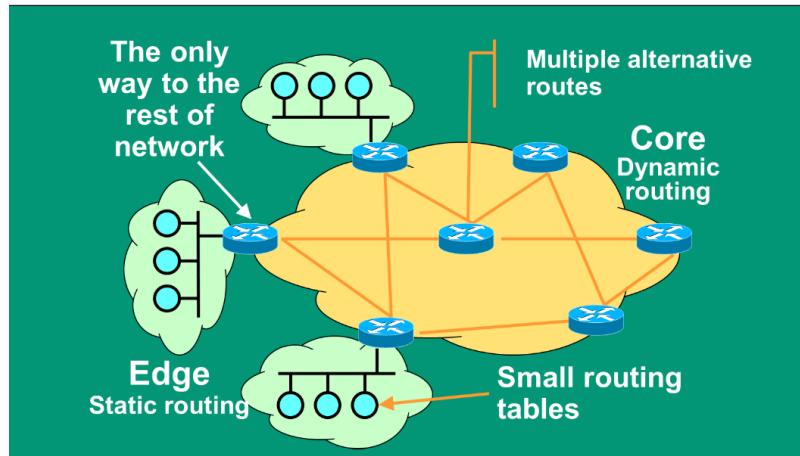


Figura 6.2: Static vs Dynamic

per prendere le strategie di routing migliori e ottimizzare le performance. Inoltre, effettua il calcolo e distribuzione delle 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.

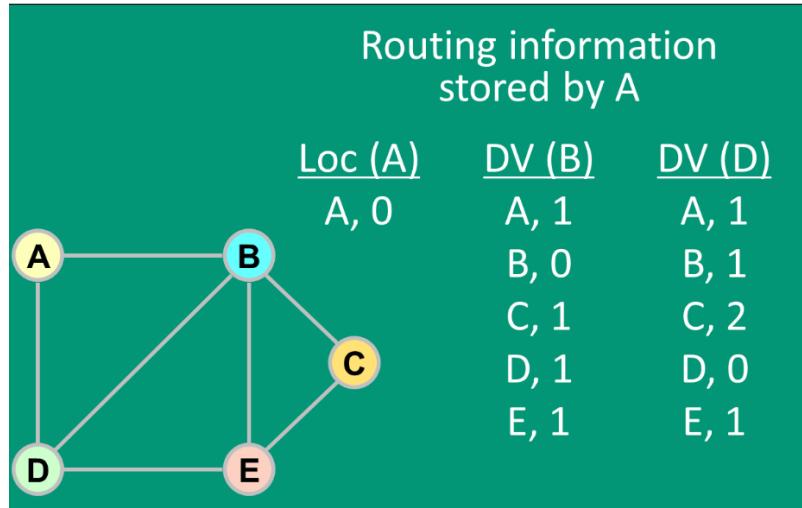
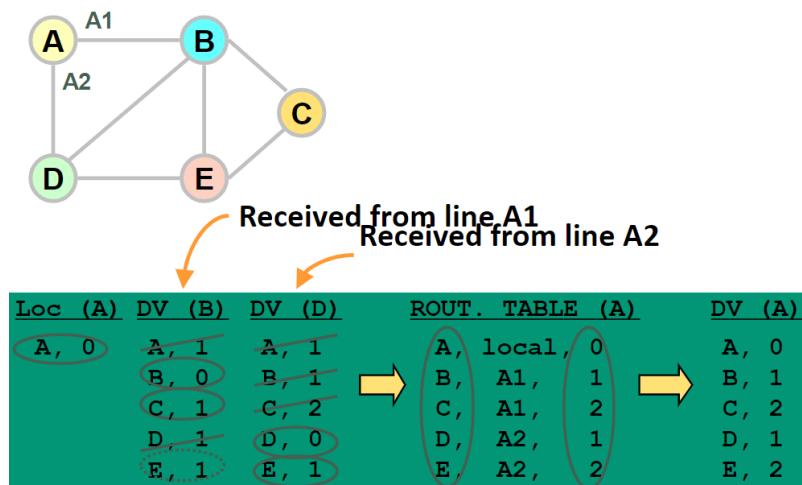
Nell'approccio **distributed routing** i router collaborano nello scambiare le informazioni sulla connettività. Ciascun router decide indipendentemente, ma in modo coerente. Combina i vantaggi e svantaggi rispetto ai due approcci precedenti.

6.3 Distance vector (Bellman-Ford)

Ogni nodo invia e riceve le informazioni ai nodi vicini. E' un algoritmo distribuito e le informazioni che si scambiano è la distanza rispetto agli altri router (raggiungibili o meno). A disposizione hanno la lista 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.

DV (Distance Vector) rappresenta la distanza tra un nodo e un altro. Ad esempio:

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

**Figura 6.3:** Scenario d'esempio (1)**Figura 6.4:** Scenario d'esempio (2)

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.

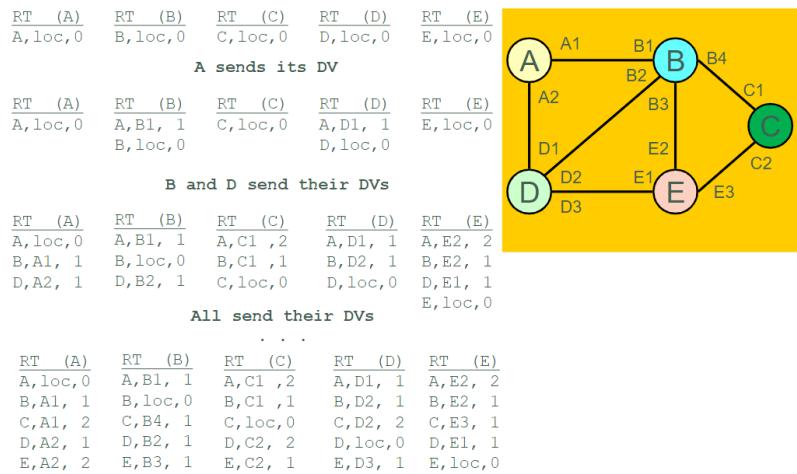


Figura 6.5: Cold Start

I problemi che si possono riscontrare sono:

- black hole: un nodo non risponde ai messaggi di routing, quindi non si ha più informazioni sulla rete.
- count to infinity: scenario di loop,
- 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.

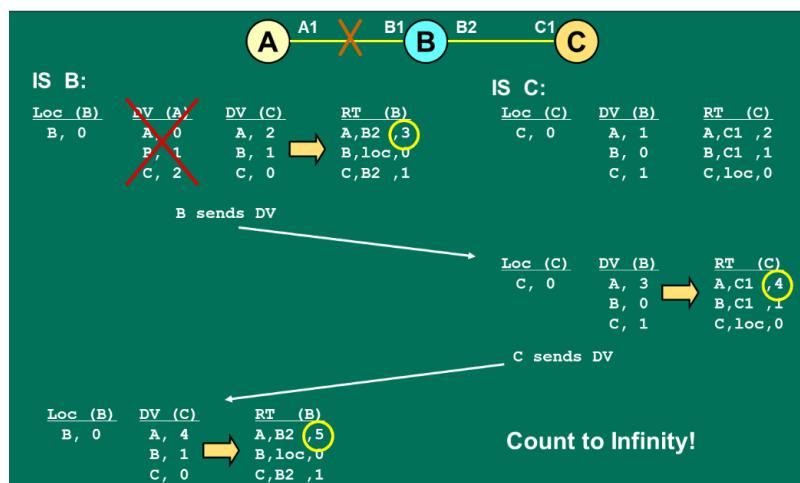


Figura 6.6: Esempio count to infinity

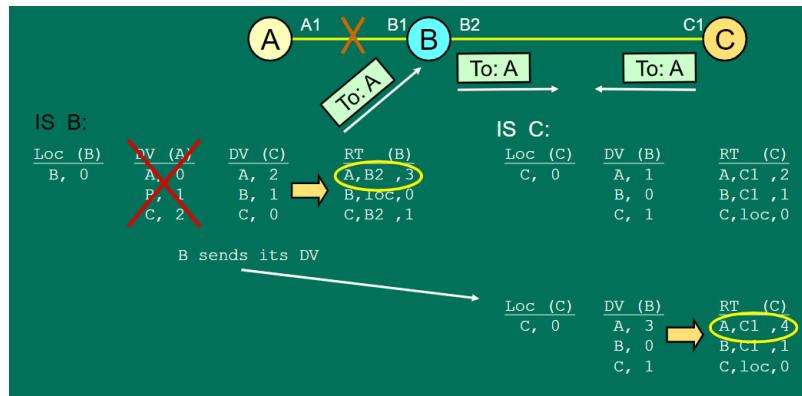


Figura 6.7: Esempio bouncing effect

Alcune soluzioni a questi problemi sono:

- **split horizon:** se C raggiunge A attraverso 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)
- **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).
- **route poisoning:** invia una informazione volutamente scorretta 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) 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.

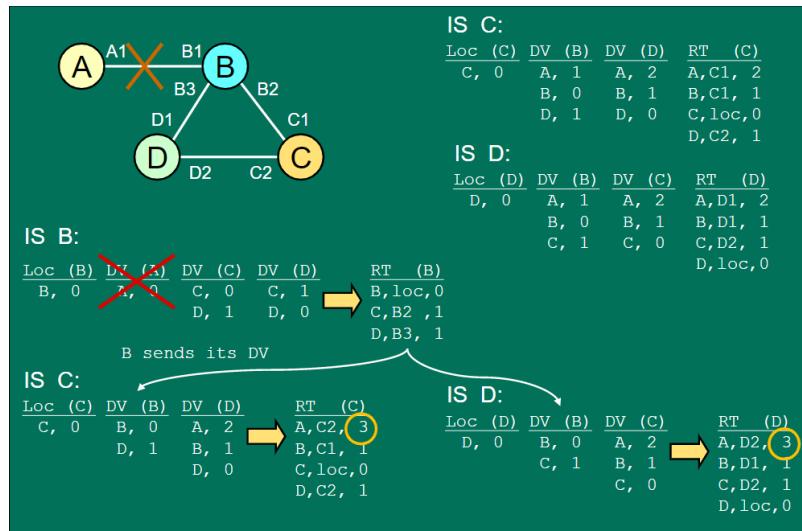
Più varianti sono possibili contemporaneamente, in base al protocollo che viene utilizzato.

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

La complessità del 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

Elimina i loop inviando, oltre le informazioni della distanza, ma anche i nodi attraversati per raggiungere una determinata destinazione. In questo modo si evitano i loop all'interno dei transitori, ma non è molto utilizzato in quanto è un compromesso con gli svantaggi di entrambi.

**Figura 6.8:** Split Horizon su mesh

6.5 Link State Routing Algorithm

Vengono inoltrate le informazioni relative a tutte la rete, relativa allo stato di ogni nodo. Permette di creare su ogni nodo una mappa locale, inviando le informazioni attraverso un *selective flooding*.

La convergenza è rapida, inoltre 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 configuraizioni complesse.

Il link state viene generato quando ci sono cambiamenti topologici. Nei protocolli attuali i link state sono generati periodicamente in modo da generare un aumento di affidabilità.

6.5.1 Algoritmo di Dijkstra

L'algoritmo di Dijkstra è un algoritmo 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.

6.6 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 vado a determinare le rotte per lo scambio di informazioni attraverso una rete, basandosi su un algoritmo di routing di partenza.

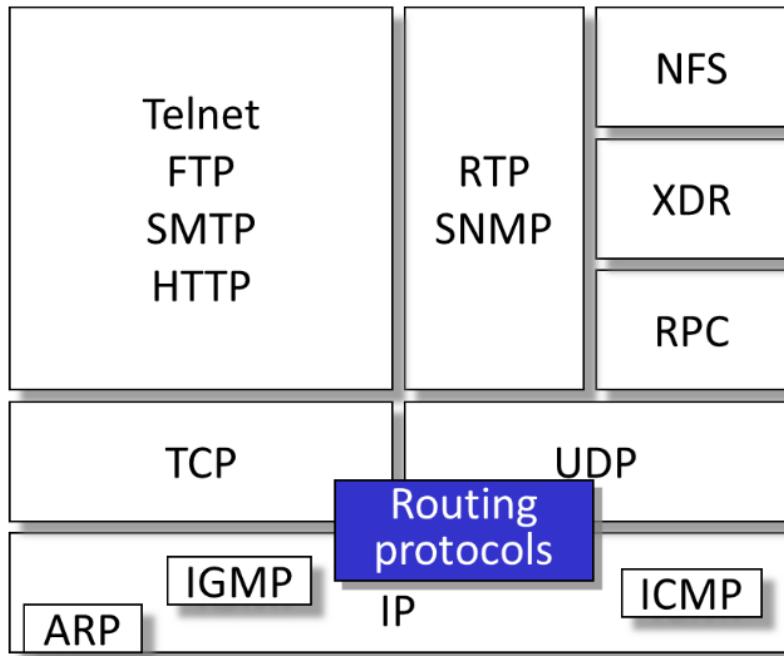


Figura 6.9: Protocol Architecture

Per i routing protocol è necessario definire delle metriche e il loro 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 attraverso un altro. Questo processo è possibile attraverso una conversione delle metriche, utilizzo di filtri di advertisement e information source priority mediante una configurazione dell'amministratore.

6.6.1 Autonomous System

Un autonomous system 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 amministra-

tivo esiste è possibile indicare delle scelte di routing interno autonomo e negoziare scelte di routing esterno. E' inoltre scalabile, in quanto nessuna delle informazioni è propagata "ovunque".

E' identificato da **due byte** numerici assegnati dalla IANA (Internet Assigned Numbers Authority). Il range di numeri privati va da 64512 a 65534.

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.

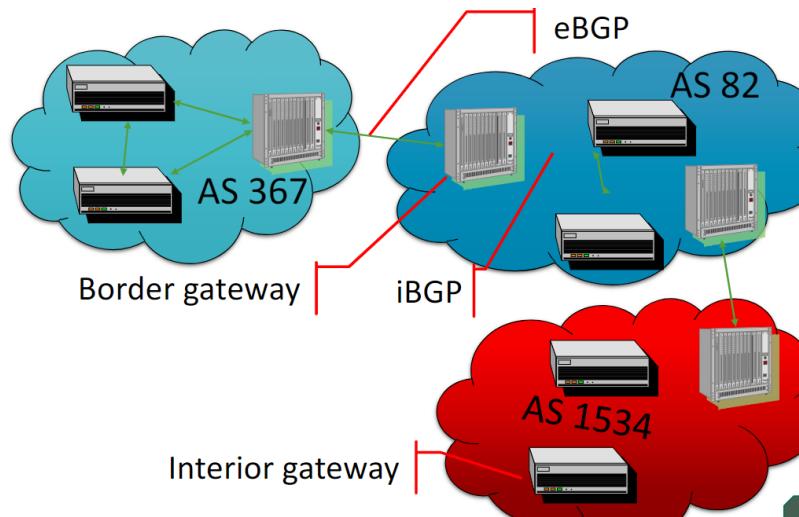


Figura 6.10: iBGP e eBGP

E' il singolo AS che decide dove far passare i propri dati.

Il concetto di percorso più breve non è più applicabile nel caso dell'exterior routing, ma bensì il percorso *migliore*. Le scelte vengono fatte in base a delle policies e riflette gli accordi che avvengono 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) e si esegue 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}

6.7 Protocolli di routing

I protocolli di routing distinguono in iBGP e eBGP.

Le feature del IGP sono:

- informazioni distribuite nella topologia
- le route sono scelte in base alle informazioni della topologia
- trova la migliore route

Le feature del EGP:

- Distribute Autonomous System information
- Distribute administrative costs
- Decide based on policies

6.7.1 IGP

Gli algoritmi di tipo Interior Gateway Protocol li distinguiamo in **distance vector**, che comprende **RIP** (Routing Information Protocol) e **IGRP** (Interior Gateway Routing Protocol), e **link state**, che comprende OSPF e Integrated IS-IS.

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

6.7.1.1 RIP

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

6.7.1.2 IGRP

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

6.7.1.3 OSPF

OSPF fa parte degli algoritmi di link state e 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 forwardato attraverso un edge router. Il routing è limitato in termini di efficacia, ma è maximum scale. I path sono sub-ottimali, si ha però perdita di connettività in caso di errori.

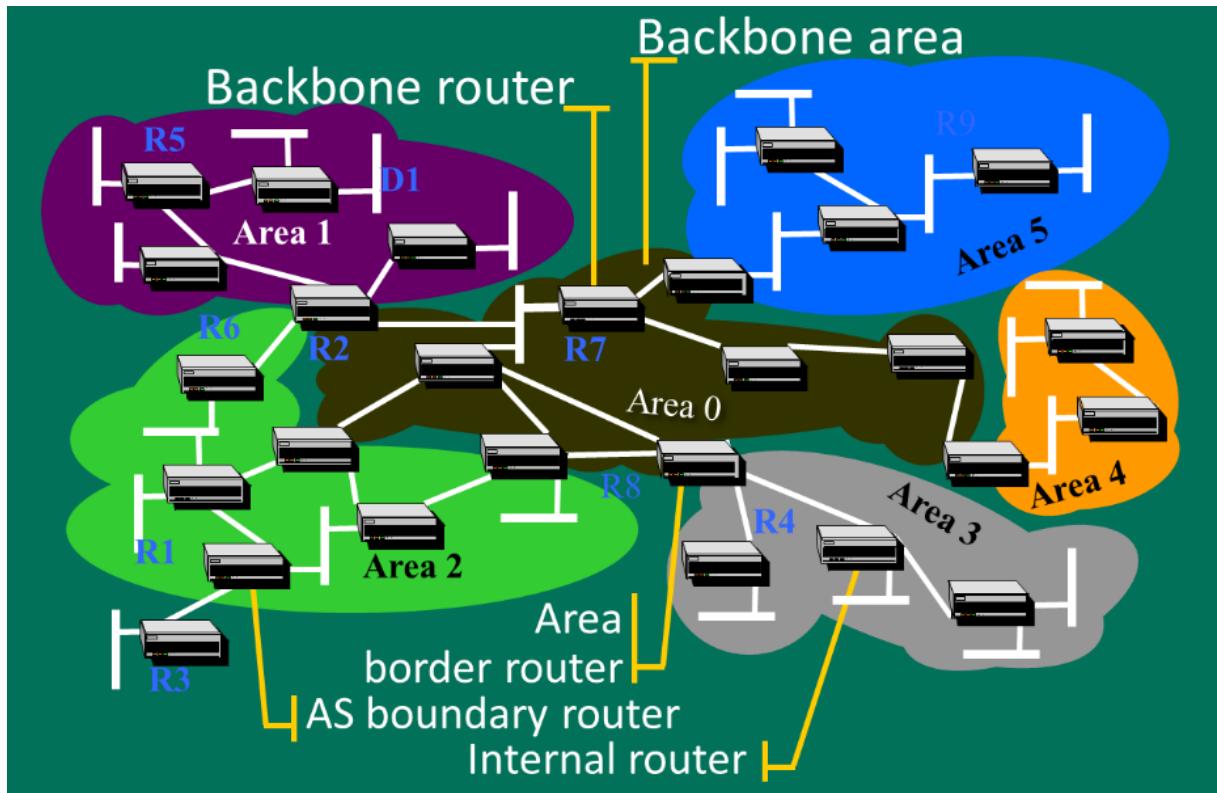
Nel loosely hierarchical routing si ha una scalabilità minore in quanto i router devono mantenere e scambiare più informazioni, ma non è richiede strictly hierarchical addressing. Tutti gli host nel *dominio B* non hanno bisogno di un identificatore comune, bensì si utilizzano dei prefissi. E' possibile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

6.7.1.3.1 Architettura 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 e dunque link. La complessità di Dijkstra è lineare nel numero di link.

6.7.1.4 IS-IS

Variante del protocollo OSPF, è un'estensione del protocollo OSI. Utilizza routing di tipo gerarchico con diversi livelli. È ancora utilizzato, ma non è più diffuso nelle nuove strutture. Ha avuto utilizzo in grandi reti e ISP.



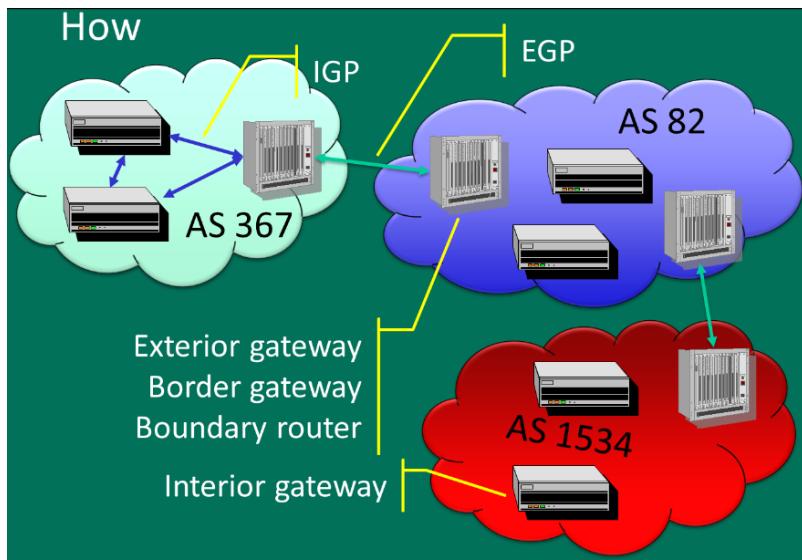
6.7.2 EGP

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 ne completamente distance vector ne link state.

6.7.2.1 BGP

Attualmente alla versione 4. Utilizza Path vector dove la destinazione è la sequenza degli Autonomous System attraversati. Ha molti attributi ed è possibile configurare la route computation policy.

Il vector exchange avviene su tcp (per maggiore affidabilità), solo a seguito di un cambiamento. Vado a creare delle sessioni tra vicini per lo scambio di informazioni attraverso una explicit configuration of neighbors, senza necessità per la connettività diretta.



6.7.2.2 Inter Domain Routing Protocol (IDRP)

IDRP utilizza TCP/IP e rappresenta un'evoluzione di BGP per OSI. È supposto per essere la scelta per IPv6, ma non è molto utilizzato.

