

# Ingeria del Software

luca carabini

September 2023

# Contents

<b>1 I protocolli di Internet</b>	<b>6</b>
1.1 Arcitettura . . . . .	6
1.2 Internet Protocol(IP) . . . . .	6
1.2.1 La struttura degli indirizzi IP . . . . .	6
1.3 Formato del pacchetto . . . . .	7
1.3.1 Fragment ofset . . . . .	8
<b>2 Instradamento IP</b>	<b>11</b>
2.1 Come funziona Internet . . . . .	11
2.2 Internet: rete di reti . . . . .	11
2.3 La tecnologia . . . . .	12
2.4 La network IP . . . . .	12
2.5 Rete logica e fisica . . . . .	12
2.6 Interconnettere le isole . . . . .	12
2.6.1 I router . . . . .	13
2.6.2 Cosa fa IP . . . . .	14
2.6.3 Ho un pacchetto da trasmettere, deve andare sulla mia network oppure devo usare un ponte? . . . . .	14
2.7 Semantica dell'indirizzo IP . . . . .	15
2.7.1 Reti IP private(RFC 1918) . . . . .	15
2.7.2 Come si distingue net-ID da host-ID . . . . .	15
2.8 Instradamento diretto e indiretto . . . . .	16
2.8.1 Instradamento diretto . . . . .	16
2.8.2 Instradamento indiretto . . . . .	16
2.8.3 Routing . . . . .	16
2.9 Relazione indirizzi fisici - IP . . . . .	16
2.9.1 Adress Resolution Protocol (ARP) . . . . .	16
2.10 Da mittente a destinatario . . . . .	17
2.11 Tabella di instradamento IP . . . . .	17
2.11.1 Uso della tabella di routing . . . . .	18
2.11.2 Table lookup . . . . .	18
2.11.3 Esempio look up . . . . .	19
2.11.4 Semplificazione delle tablelle . . . . .	20
2.11.5 Perchè ordinare i route . . . . .	21
2.12 Gateway . . . . .	22
2.12.1 Il ruolo del gateway . . . . .	22
2.12.2 Uso del Gateway . . . . .	22

<b>3 La logica degli indirizzi IP</b>	<b>23</b>
3.1 IP e Netmask . . . . .	23
3.2 Classi delle reti . . . . .	23
3.2.1 Classi di Indirizzi . . . . .	24
3.2.2 Intervalli di Indirizzi . . . . .	24
3.3 Le sottoreti . . . . .	24
3.3.1 Subnetting . . . . .	25
3.3.2 CIDR: Classeless InterDomain Routing . . . . .	25
3.3.3 Supernetting . . . . .	26
3.3.4 Esempio . . . . .	26
3.3.5 Supernetting e Subnetting . . . . .	26
3.3.6 Oggi . . . . .	27
<b>4 Protocollo ICMP</b>	<b>28</b>
4.1 Quando viene usato . . . . .	28
4.2 Pacchetto ICMP . . . . .	29
4.3 Tipi di errori . . . . .	29
4.3.1 Destination Unreachable (Type 3) . . . . .	29
4.3.2 Time Exceeded (Type = 11) . . . . .	30
4.3.3 Source Quench (Type = 4) . . . . .	30
4.3.4 Redirect (Type = 5) . . . . .	30
4.4 Informazioni . . . . .	30
4.4.1 Echo (Type=8) / Echo Reply (Type = 0) . . . . .	30
4.4.2 Additional Fields . . . . .	30
4.4.3 Timestamp Request (Type = 13) / Reply(Type = 14) . . . . .	30
4.4.4 Address Mask Request (Type = 17) / Reply (Type = 18) . . . . .	30
4.4.5 Router Solicitation (Type = 10) . . . . .	30
4.4.6 Router Advertisement (Type = 9) . . . . .	30
<b>5 Applicazioni di ICMIP</b>	<b>31</b>
5.1 PING . . . . .	31
5.1.1 funzionamento . . . . .	31
5.1.2 Opzioni . . . . .	31
5.1.3 Output . . . . .	32
5.1.4 Traceroute . . . . .	32
5.1.5 Funzionamento . . . . .	32
5.1.6 Output . . . . .	32
<b>6 Gestione della enumerazione</b>	<b>33</b>
6.1 Dispositivi di rete . . . . .	33
6.1.1 DHCP . . . . .	33
6.1.2 Packet Filter . . . . .	34
6.1.3 Application Layer Gateway (ALG) / Proxi . . . . .	34
6.1.4 Firewall . . . . .	35
6.1.5 Network Address Translator (NAT) . . . . .	35
<b>7 Packet Filter e Firewall</b>	<b>36</b>
7.1 Firewall . . . . .	36
7.1.1 Packet filter . . . . .	36
7.1.2 Stateful Packet Inspection . . . . .	37
7.1.3 Application Layer Gateway (trasparente o proxy esplicito) . . . . .	38
7.2 Protezione Host: firewall . . . . .	39
7.3 Livelli di implementazione . . . . .	40

7.3.1	Packet Filter . . . . .	40
7.3.2	Proxy server0 . . . . .	41
7.4	Configurazione di packet filter e proxy . . . . .	41
<b>8</b>	<b>Network Address Translation</b>	<b>42</b>
8.1	Motivazioni . . . . .	42
8.2	Network (+Port) Address Translator (NAT) . . . . .	43
8.3	Basic Nat . . . . .	43
8.3.1	Conversione di Indirizzo . . . . .	43
8.3.2	Conversione di indirizzo e porta . . . . .	44
8.3.3	Direzione delle connessioni . . . . .	44
8.3.4	Port forwarding . . . . .	45
8.3.5	Analisi di connessioni attraverso NAT . . . . .	46
8.4	NAT e applicazioni di rete . . . . .	47
8.4.1	Le applicazioni non sono trasparenti al NAT . . . . .	47
8.4.2	Il tipo di traffico permesso dipende dal ipo di nat . . . . .	47
<b>9</b>	<b>IPv6</b>	<b>48</b>
9.1	Problematiche dell'indirizzamento IP . . . . .	48
9.2	Soluzione: IPPv6 . . . . .	48
<b>10</b>	<b>Instradamento nelle reti a pacchetto e in Internet</b>	<b>49</b>
10.1	Funzioni dell' IP . . . . .	49
10.2	Il nodo di commutazione a pacchetto . . . . .	50
10.2.1	Store-and-Forward . . . . .	50
10.3	Flooding . . . . .	50
10.3.1	Funzionamento . . . . .	50
10.3.2	Problema . . . . .	50
10.3.3	Soluzione . . . . .	51
10.4	Deflection routing (hot potato) . . . . .	51
10.4.1	Per quali reti è adatto? . . . . .	51
10.4.2	Propblemi . . . . .	51
10.4.3	soluzioni . . . . .	51
10.5	Shortest path routing . . . . .	51
10.5.1	Iplementazione . . . . .	51
10.6	Rappresentazione della rete . . . . .	52
10.7	Il grafo della rete . . . . .	52
10.8	Routing shortest path nel mondo IP . . . . .	52
10.9	Rouing distance vector . . . . .	53
10.9.1	Cosa implementa . . . . .	53
10.9.2	Problemi . . . . .	53
10.9.3	Esempio . . . . .	53
10.9.4	. . . . .	53
10.9.5	Bouncing effect . . . . .	54
10.10	Convergenza lenta . . . . .	54
10.10.1	Count to infinity . . . . .	55
10.10.2	Split horizon . . . . .	55
10.10.3	Triggered update . . . . .	55
10.10.4	Non basta . . . . .	55
10.11	Routing link state . . . . .	56
10.11.1	Scopo . . . . .	56
10.11.2	Raccolta delle informazioni . . . . .	56
10.11.3	Diffusione ed elaborazione delle informazioni . . . . .	56

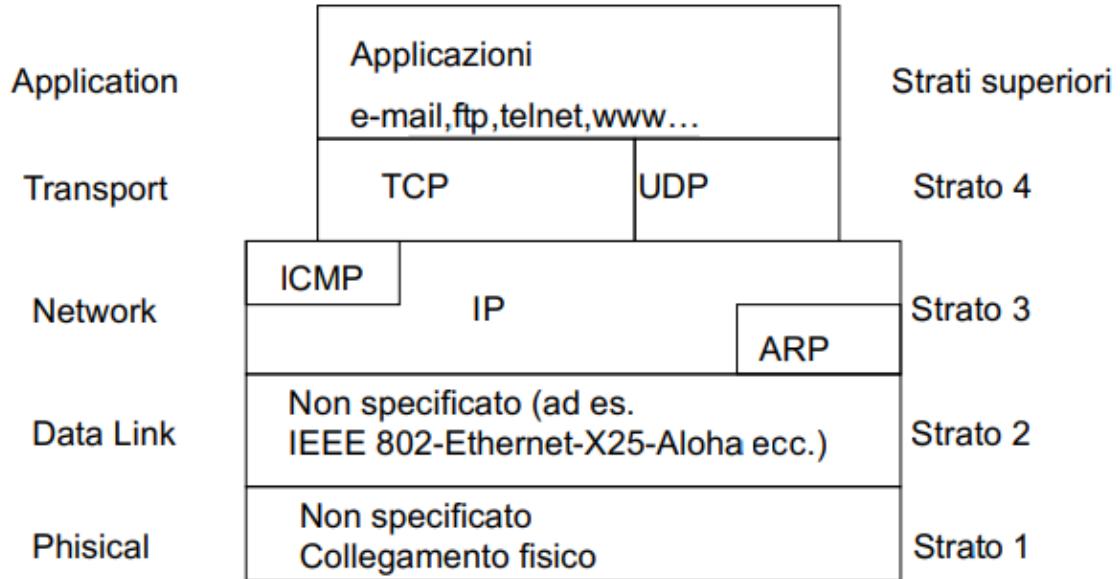
10.11.4 Esempio . . . . .	57
10.12 Il router IP . . . . .	57
10.12.1 Classificazione dei router . . . . .	57
10.12.2 Le funzioni . . . . .	57
10.12.3 Schema funzionale di un router . . . . .	58
10.12.4 Tabella di routing . . . . .	58
10.12.5 Tabelle di forwarding . . . . .	59
10.12.6 Routing vs forwarding table . . . . .	59
10.12.7 Arrivare alla FIB . . . . .	59
<b>11 Instradamento nell'Internet globale</b>	<b>60</b>
11.1 Routing gerarchico . . . . .	60
<b>12 Autonomus Systems and peering</b>	<b>61</b>
12.1 Internet . . . . .	61
12.1.1 rete di reti . . . . .	61
12.1.2 Sistemi Interconnessi . . . . .	62
12.1.3 Grafo semplificate . . . . .	62
12.2 Routing a livello globale . . . . .	63
12.2.1 Routing gerarchico . . . . .	63
12.2.2 Tipi di grafo . . . . .	63
12.3 Protocolli di routing . . . . .	63
12.3.1 RFC 1930 . . . . .	63
12.3.2 Esempio . . . . .	64
12.4 Internet Routing Register . . . . .	64
12.4.1 AS 137 . . . . .	65
12.4.2 AS20965 Regole di Import . . . . .	66
12.4.3 Interconnessione fra AS . . . . .	67
12.5 Internet Service Provider . . . . .	67
12.5.1 Servizi . . . . .	67
12.5.2 ISP dal punto di vista giuridico . . . . .	67
12.5.3 Internet Region . . . . .	68
12.5.4 Classificazione degli ISP . . . . .	68
12.5.5 Peering . . . . .	68
12.5.6 ISP locali e POP . . . . .	69
12.5.7 Esempio di POP . . . . .	69
12.5.8 Indirizzamento . . . . .	69
12.5.9 Interconnessione . . . . .	70
12.5.10 Da Tier 3 a Tier 1 . . . . .	71
12.6 Internet Exchange . . . . .	71
12.7 In Italia . . . . .	71
12.7.1 IXP in Italia . . . . .	72
<b>13 Interior Gateway Protocol (IGP)</b>	<b>73</b>
13.1 Routing Information Protocol (RIP) . . . . .	73
13.1.1 Dove si utilizza . . . . .	73
13.1.2 Tipi di messaggi . . . . .	73
13.1.3 Da chi sono trasportati? . . . . .	73
13.1.4 RESPONSE . . . . .	73
13.1.5 Formato dei pacchetti . . . . .	73
13.1.6 Significato dei campi . . . . .	74
13.1.7 La tabella di routing . . . . .	74
13.1.8 Aggiornamento tabella di routing . . . . .	74

13.1.9 Problematiche . . . . .	75
13.1.10 RIP versione 2 . . . . .	75
13.2 Open Shortest Path First (OSPF) . . . . .	75
13.2.1 Per cosa è stato progettato . . . . .	75
13.2.2 Aree di Routing . . . . .	76
13.2.3 Tipi di route . . . . .	76
13.2.4 Tipi di aree . . . . .	76
13.2.5 Ulteriori caratteristiche . . . . .	76
13.2.6 Rappresentazione di host e router . . . . .	77
13.2.7 Tipologie di rete . . . . .	77
13.2.8 Rappresentazione di reti multi-accesso . . . . .	77
13.2.9 Vicinanza e adiacenza tra router . . . . .	77
13.2.10 Identificazione di router e priorità . . . . .	77
13.2.11 Elezione di DR e BDR . . . . .	78
13.2.12 Link State Database . . . . .	78
13.2.13 I protocolli . . . . .	78
13.2.14 Type . . . . .	78
13.2.15 Hello protocol . . . . .	79
13.2.16 Exchange protocol . . . . .	79
<b>14 Come fa un pacchetto ad arrivare a destinazione</b>	<b>80</b>
<b>15 Esercitazione Router</b>	<b>81</b>

# Chapter 1

## I protocolli di Internet

### 1.1 Arcitettura



### 1.2 Internet Protocol(IP)

È stato progettato per funzionare a **commutazione di pacchetto** in modalità **connectionless**. Si prende carico della trasmissione di datagrammi da sorgente a destinazione, attraverso reti eterogenee. Identifica host e router tramite indirizzi di lunghezza fissa, raggruppandoli in reti IP. Frammenta e riassembra i datagrammi quando necessario. Offre un servizio di tipo best effort, cioè non sono previsti meccanismi per:

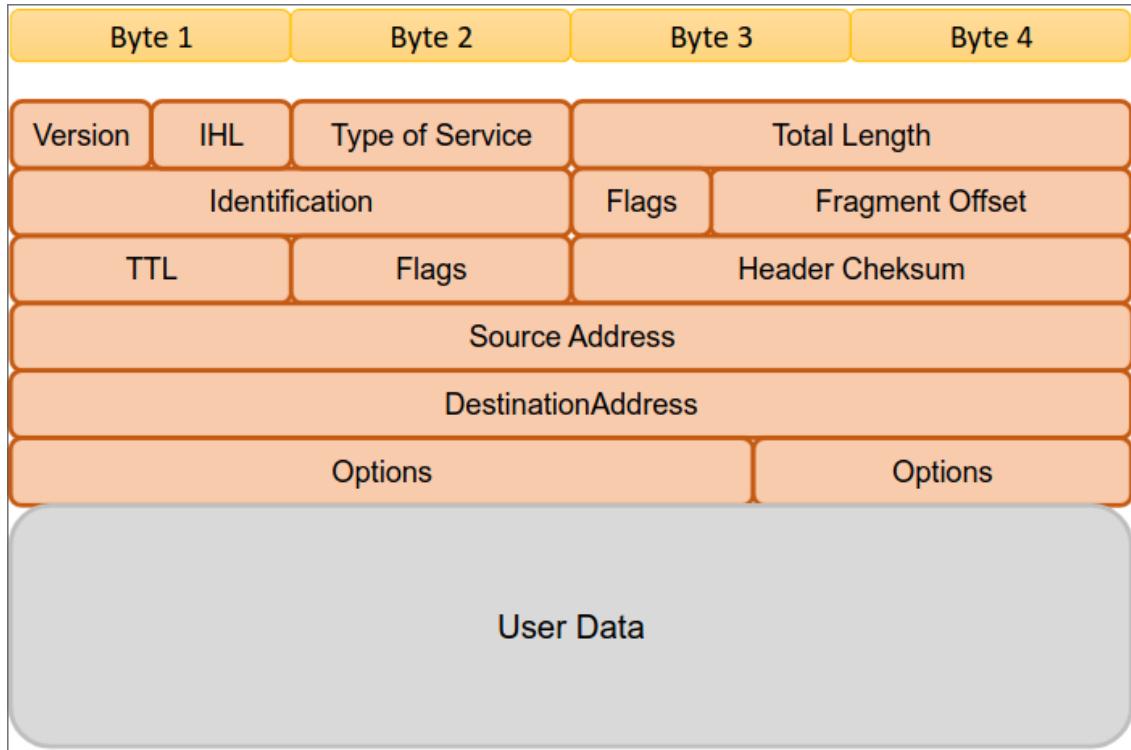
- aumentare l'affidabilità del collegamento end-to-end
- eseguire il controllo di flusso e della sequenza

#### 1.2.1 La struttura degli indirizzi IP

La loro lunghezza è fissa e pari a 32 bit, che convenzionalmente sono scritti come sequenza di 4 numeri decimali che vanno da 0 a 255 separati da un punto.

Il numero teorico massimo di indirizzi è  $2^{32}$  (in realtà si riesce a sfruttare un numero molto inferiore)  
 Sono assegnati dalla IANA (Internet Assigned Numbers Authority)

### 1.3 Formato del pacchetto



- **Version** : indica il formato dell'intestazione
- **IHL** : lunghezza dell'intestazione, espressa in parole di 32 bit
- **Type of service** : indicazione sul tipo di servizio richiesto
- **Total length** : lunghezza totale del datagramma, misurata in bytes, la lunghezza massima è 65535 bytes (non è detto che tutte le implementazioni siano in grado di gestire questa dimensione)
- **Identification** : valore intero che identifica univocamente il datagramma, indic a quale datagramma appartiene un frammento
- **Flag**:
  - **bit 0** : sempre a zero
  - **bit 1** : don't fragment (DF), DF=0 si può fragmentare, DF=1 non si può fragmentare
  - **bit 2** : more fragment (MF), MF=0 ultimo frammento, MF=0 frammento intermedio
- Fragment offset : indica qual è la posizione di questo frammento nel datagramma, come distanza in unità di 64 bit dall'inizio
- Time to live (TTL) : max numero di nodi attraversabili :

- Il nodo sorgente attribuisce un valore maggiore di 0 a TTL (tipicamente TTL=64, al massimo 255)
  - Ogni nodo che attraversa il datagramma pone TTL=TTL-1
  - Il primo nodo che vede TTL=0 distrugge il datagramma
- **Protocol** : indica a quale protocollo di livello superiore appartengono i dati del datagramma
  - **Header checksum** : controllo di errore della sola intestazione, viene ricalcolato da ogni nodo attraverso dal datagramma.
  - **Source and Destination Address** : indirizzi sorgente e destinazione
  - **Padding** : bit privi di significato aggiunti per fare in modo che l'intestazione sia con certezza multipla di 32 bit

### 1.3.1 Fragment offset

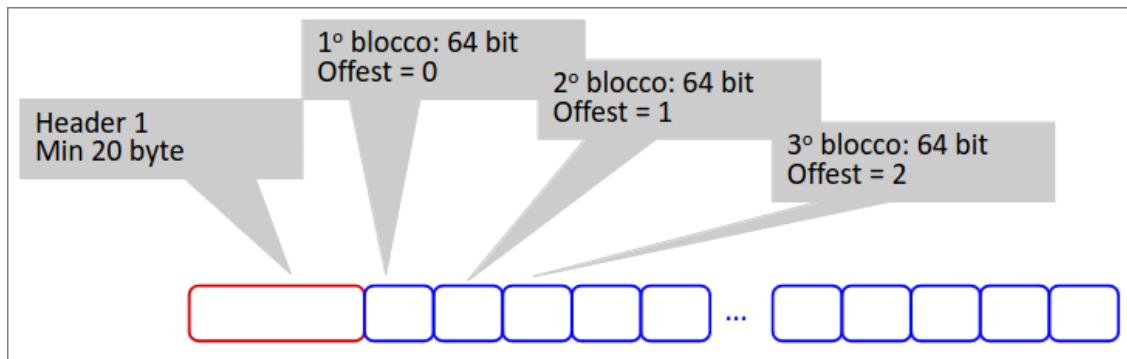
Il datagramma IP viene virtualmente suddiviso in sotto-blocchi di 8 byte(64 bit).

Per l'IP che trasmette, il primo blocco del datagramma è il numero 0, i blocchi successivi sono logicamente numerati sequenzialmente, il numero logico del primo blocco viene scritto ne Fragment offset del datagramma

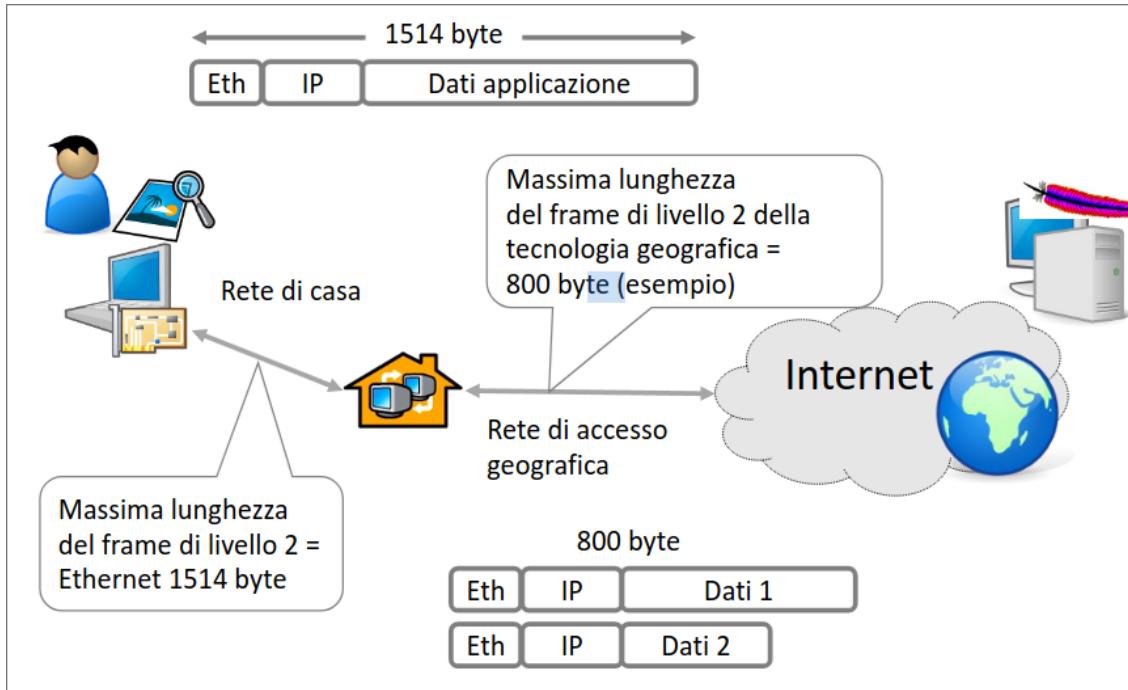
#### Implementazione

Un qualunque apparato di rete dotato di protocollo IP può frammentare un datagramma, tipicamente i nodi intermedi non riabbellano, ma lo fa solamente il terminale ricevente.

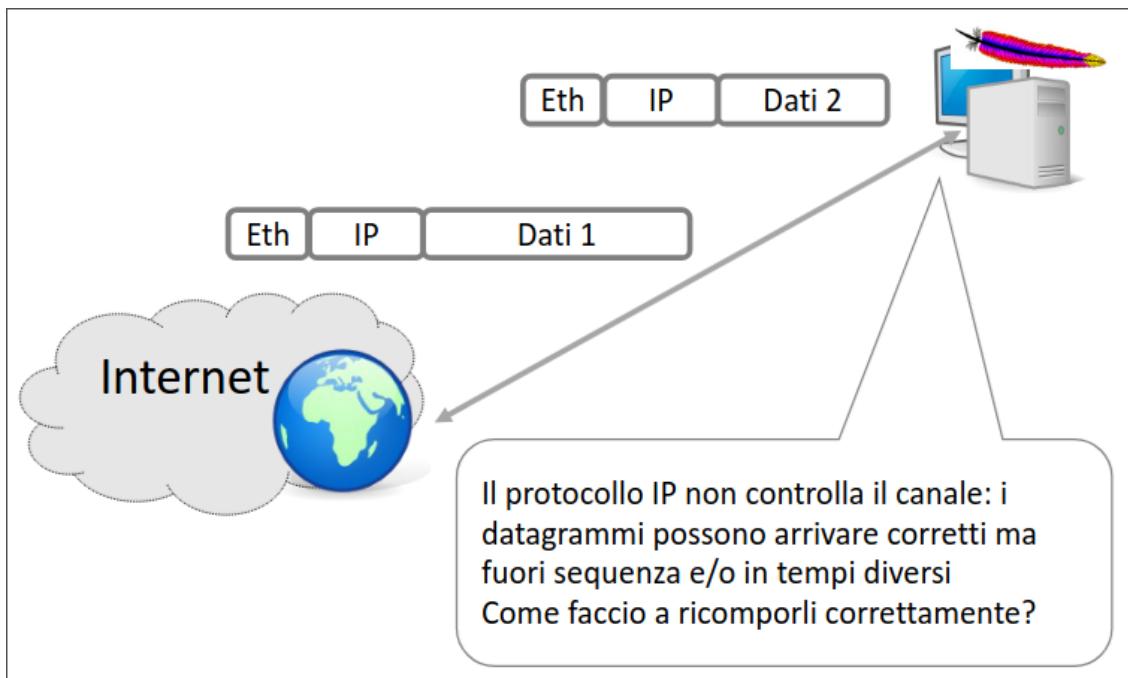
Un datagramma può essere frammentato a più riprese in nodi successivi (Frammentazioni multiple)  
La numerazione tramite "offset" permette di rinumerare facilmente frammenti di un frammento



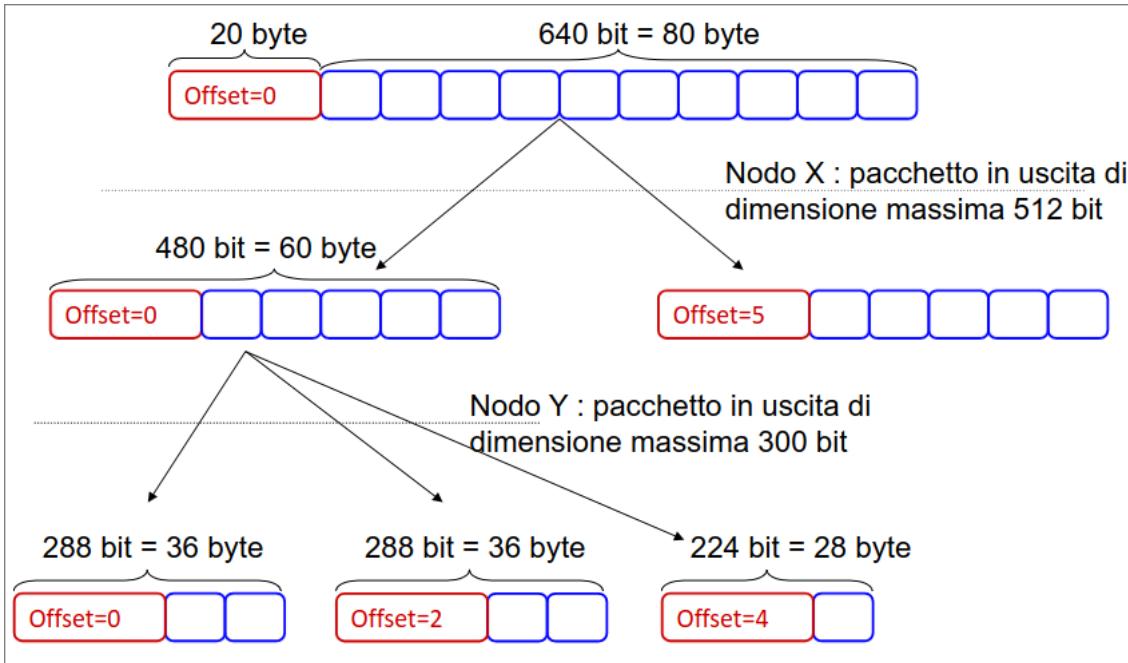
## Perchè la frammentazione



## Riassemblamento



## Calcolo dell'offset



# Chapter 2

## Instradamento IP

La rete internet una rete a commutazione di pacchetto, In generale esistono più modi per raggiungere una destinazione da una certa sorgente

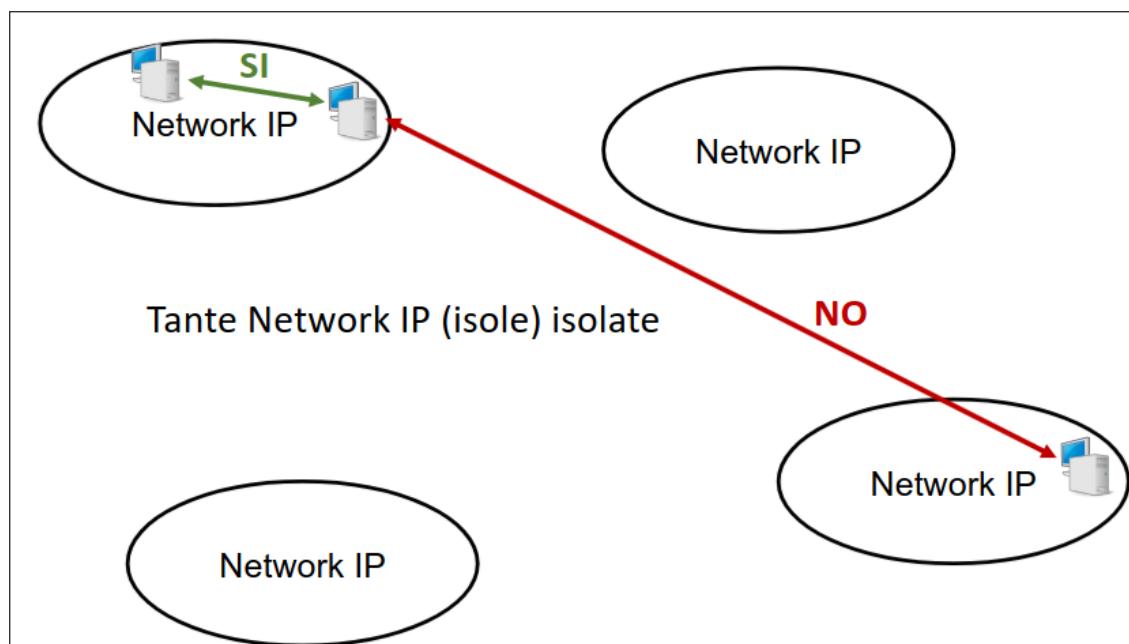
### 2.1 Come funziona Internet

Internet è una grande "rete di reti"

La componente principale è la **network IP**; ogni network IP è una sorta di isola, e contiene calcolatori che fungono da nodi nella rete detti **host**.

Le isole sono connesse da apparati che svolgono la funzione di "ponte", si tratta di calcolatori specializzati detti **router** o **gateway**.

### 2.2 Internet: rete di reti



## 2.3 La tecnologia

Ogni network IP può essere implementata con una **tecnologia specifica**.

Ad esempio:

- Wi-Fi : Network realizzata con tecnologia wireless in area locale.
- ADSL : Network realizzata con tecnologia a media distanza via cavo tramite infrastruttura di uno specifico fornitore di servizio pubblico
- Ethernet : Network realizzata con tecnologia a breve distanza via cavo privata in area locale
- GPRS/EDGE/LTE : Network realizzata con tecnologia radio a media distanza tramite infrastruttura di uno specifico fornitore di servizio pubblico

## 2.4 La network IP

I calcolatori di una network IP sono connessi dalla medesima infrastruttura di rete fisica (livelli 1 e 2) Tutti gli host di una medesima network IP sono in grado di parlare tra loro grazie alla tecnologia con cui essa viene implementata ( senza l'utilizzo di router o gateway)

## 2.5 Rete logica e fisica

**Rete logica** la network IP a cui un Host appartiene logicamente.

**rete fisica** la rete (tipicamente LAN) a cui un Host è effettivamente connesso, normalmente ha capacità di instradamento e può avere indirizzi locali (es. indirizzi MAC)

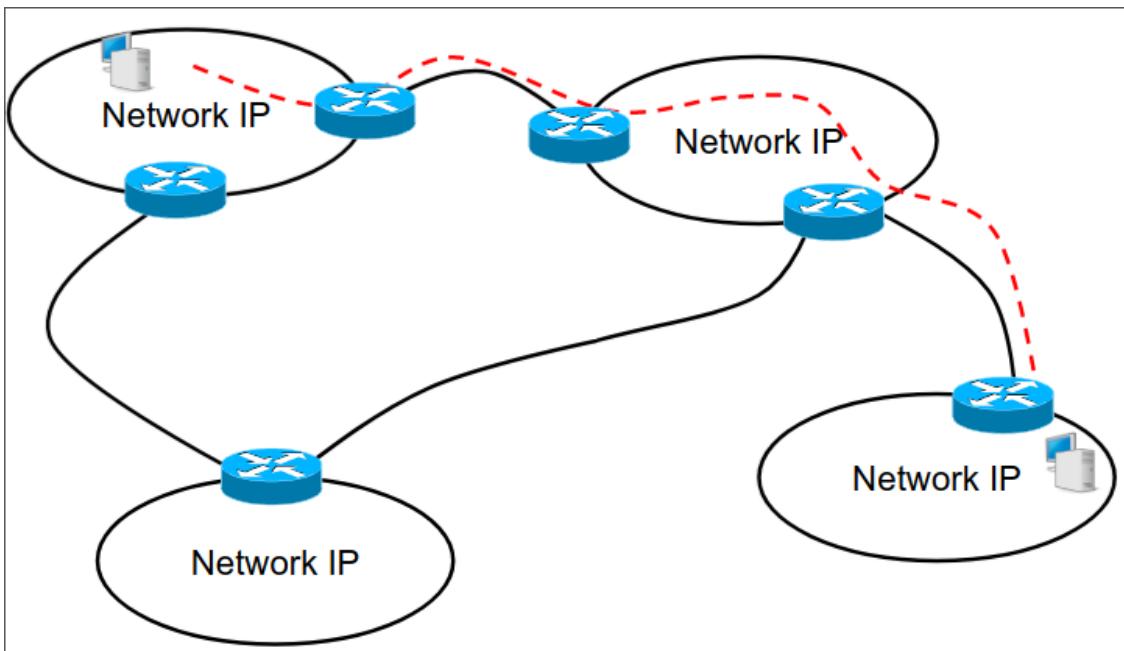
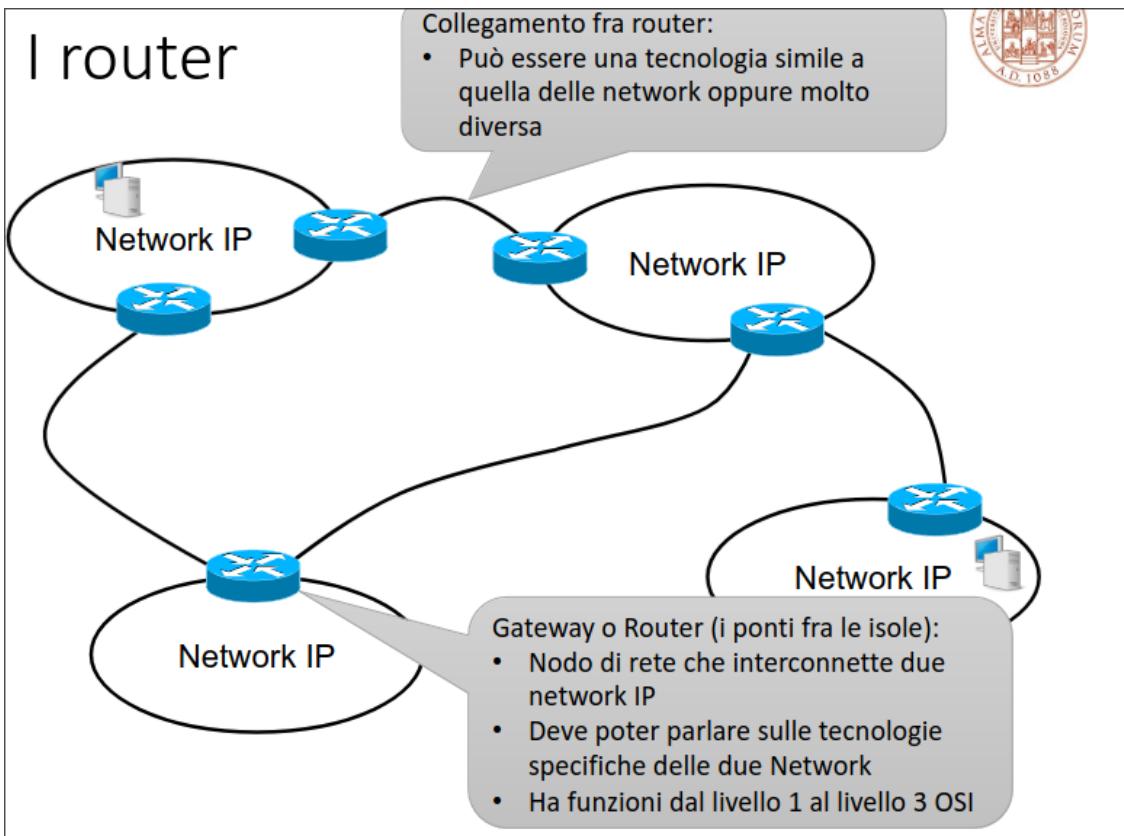
L'architettura a strati nasconde gli indirizzi fisici e consente alle applicazioni di lavorare solo con indirizzi IP.

## 2.6 Interconnettere le isole

Per far parlare tra di loro le isole (network IP) è necessario che:

- Vi siano dei collegamenti fra le isole stesse, spesso realizzati con tecnologie diverse da quelle dell'isola.
- Vi siano degli apparati che permettono di usare questi collegamenti nel modo opportuno
- Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere.

## 2.6.1 I router



## 2.6.2 Cosa fa IP

La tecnologia IP è agnostica rispetto alla tecnologia con cui sono realizzate le network, quindi può lavorare indifferentemente su diverse tecnologie.

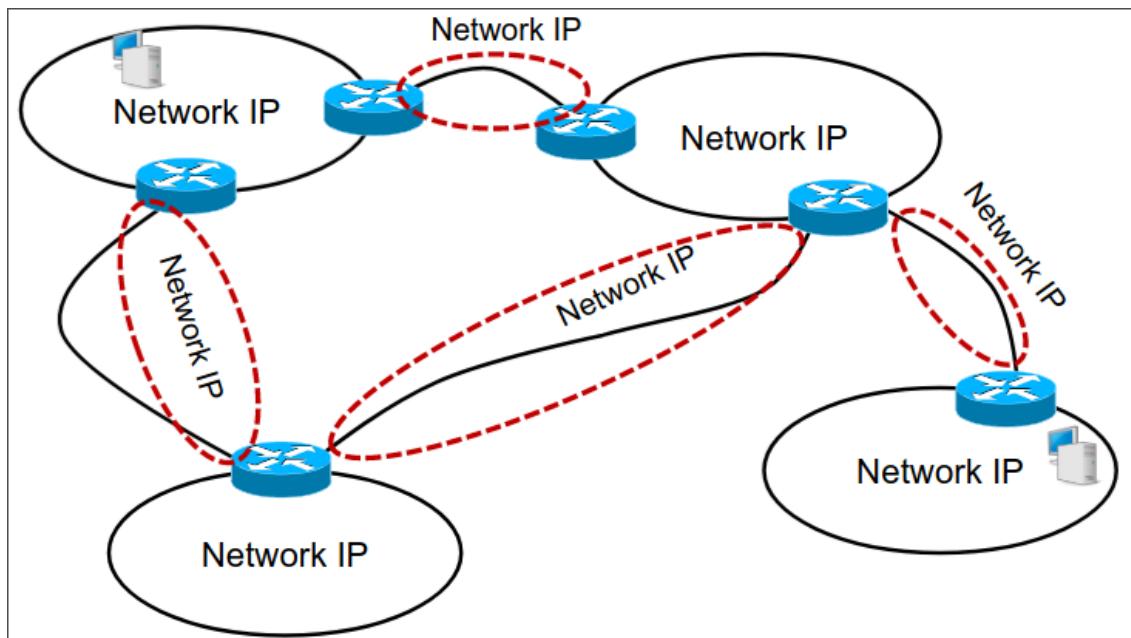
L'obiettivo di IP è quello di rendere possibile il dialogo fra le network a prescindere dalla loro implementazione e localizzazione-

## 2.6.3 Ho un pacchetto da trasmettere, deve andare sulla mia network oppure devo usare un ponte?

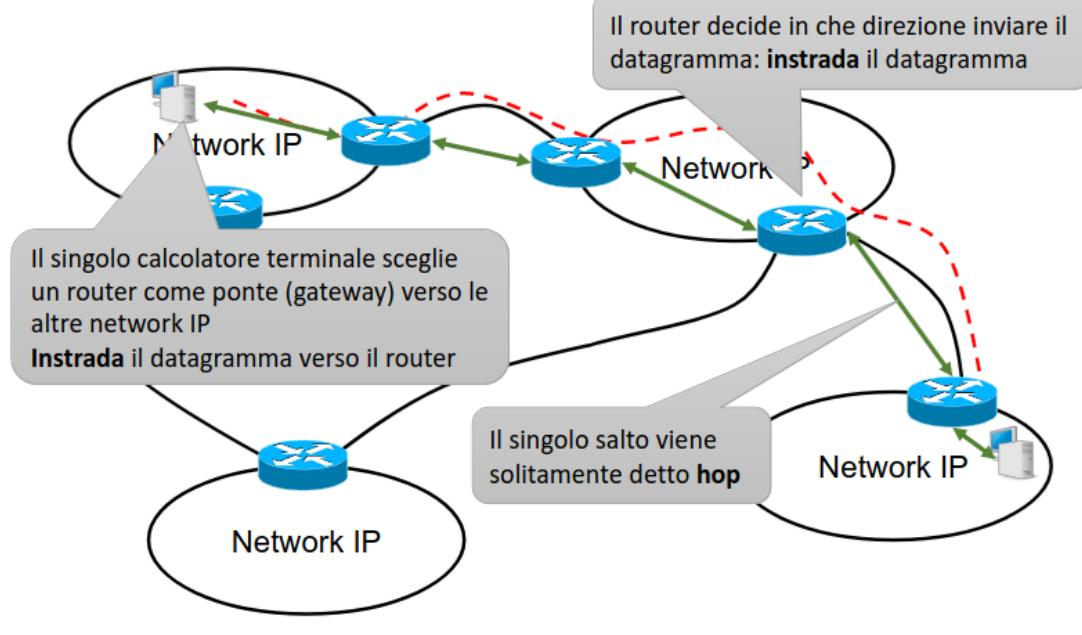
Ogni nodo di Internet ha una base dati di destinazioni possibili, quindi quando deve inviare un datagramma:

- Parte dall'indirizzo IP destinazione
- Legge la base dati
- Decide quale azione intraprendere

La tecnologia della propria network può essere utilizzata, per raggiungere la destinazione finale, o per raggiungere il primo ponte da attraversare



# L'instradamento IP



## 2.7 Semantica dell'indirizzo IP

L'indirizzo IP è logicamente suddiviso in due parti:

- **Network ID (Net ID)** : è il prefisso che identifica la Network IP a cui appartiene l'indirizzo, quindi tutti gli indirizzi di una medesima Network IP hanno lo stesso Net ID, e occupa la parte sinistra dell'indirizzo.
- **Host ID** : Identifica l'Host (l'interfaccia) vero e proprio di una certa Network, occupa la parte destra dell'indirizzo

### 2.7.1 Reti IP private(RFC 1918)

Alcuni gruppi di indirizzi sono riservati a reti IP private, non sono raggiungibili dalla rete pubblica.  
I router di Internet non instradano datagrammi destinati a tali indirizzi.

Possono essere riutilizzati in reti isolate.

- da **10.0.0.0** a **10.255.255.255**
- da **172.16.0.0** a **172.31.255.255**
- da **192.168.0.0** a **192.168.255.255**

### 2.7.2 Come si distingue net-ID da host-ID

Si usa la netmask, al numero IP viene associata una maschera di 32 bit, i bit a 1 nella netmask identificano i bit dell'indirizzo IP che fanno parte del net-ID

## 2.8 Instradamento diretto e indiretto

### 2.8.1 Instradamento diretto

Nel **Direct delivery** l'IP sorgente e l'IP destinazione sono sulla stessa network, e l'host sorgente spedisce il datagramma direttamente al destinatario

### 2.8.2 Instradamento diretto

Nell' **Indirect delivery** l'IP sorgente e L'IP destinatario, non sono sulla stessa network, l'host sorgente invia il datagramma ad un router intermedio

### 2.8.3 Routing

Il routing è la scelta del percorso su cui inviare i dati, i router formano una struttura interconnessa e cooperante, i datagrammi passano dall'uno all'altro finché non raggiungono quello che può consegnarli direttamente al destinatario

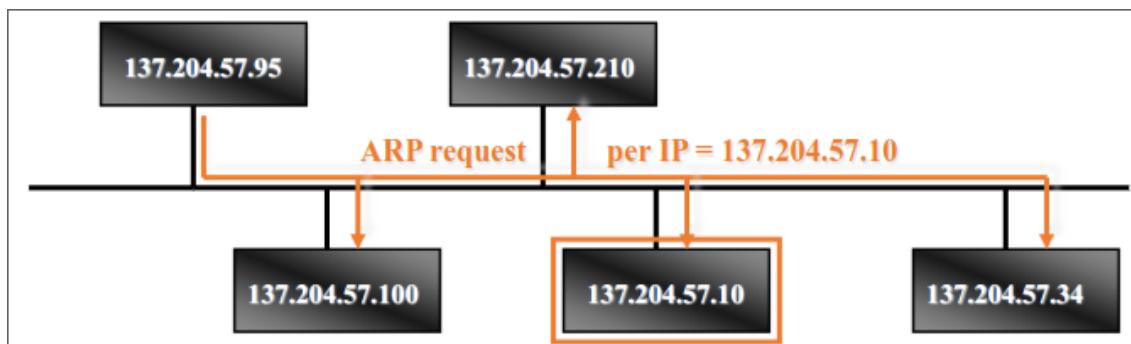
## 2.9 Relazione indirizzi fisici - IP

Il software di basso livello nasconde gli indirizzi fisici e consente di lavorare ai livelli superiori con gli indirizzi IP.

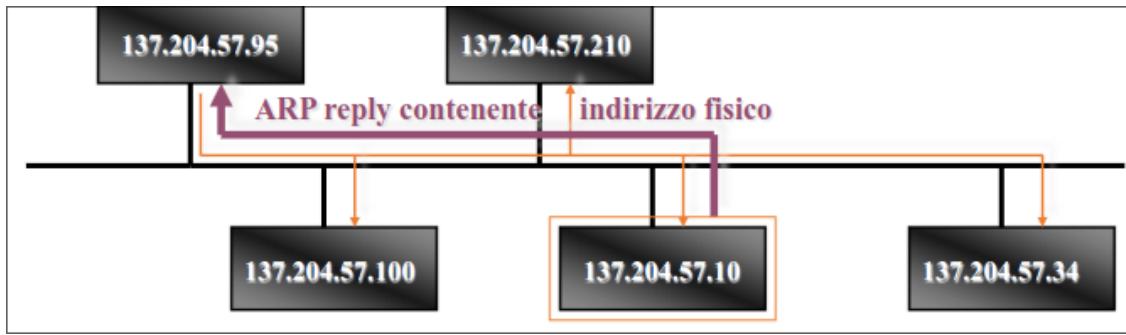
Gli Host comunicano attraverso una rete fisica (es. LAN) quindi devono conoscere reciprocamente gli indirizzi fisici.

L'host A vuole mandare datagrammi a B, che si trova sulla stessa rete fisica e di cui conosce solo l'indirizzo IP.(come ricava l'indirizzo fisico?)

### 2.9.1 Adress Resolution Protocol (ARP)



Il nodo sorgente invia una trama broadcast (**ARP request**) contenente l'indirizzo IP del nodo destinazione. Tutte le stazioni della rete locale leggono la trama broadcast



Il destinatario risponde al mittente, inviando un **ARP reply** che contiene il proprio indirizzo fisico, l'host sorgente ora è in grado di associare l'appropriato indirizzo fisico all'IP destinazione.  
Ogni host mantiene una tabella (**cache ARP** con le corrispondenze fra indirizzi logici e fisici.

## 2.10 Da mittente a destinatario

C'è sempre un aconsegna diretta, può non esserci una consegna indiretta, e possono esserci una o più consegne indirette.

## 2.11 Tabella di instradamento IP

Base dati in forma di tabella:

- **Righe (route)** : Insieme di informazioni relative alla singola informazione di instradamento. I suoi tipici campi sono:
  - Destinazione(D): numero IP valido (può essere indirizzo di Host o di network)
  - Netmask(N) : mascara di rete valida (identifica il net-ID)
  - Gateway(G) : numero IP a cui consegnare il datagramma (indica il tipo di consegna da effettuare)
  - Interfaccia di rete(IF) : interfaccia di rete utilizzata per la consegna del datagramm (seleziona il dispositivo hardware da utilizzare per l'invio del datagramma)
  - Metrica(M) : specifica il "costo" di quel particolare route (Possono esistere più route verso una medesima destinazione).
- **Colonne (campi)** : Informazioni del medesimo tipo relative a diverse opzioni di instradamento.

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	ppp0	1
137.204.64.0	255.255.255.0	137.204.64.254	en0	1
137.204.65.0	255.255.255.0	137.204.65.254	en1	1
137.204.66.0	255.255.255.0	137.204.66.254	en2	1
137.204.67.0	255.255.255.0	137.204.67.254	en3	1
192.168.10.0	255.255.255.252	192.168.10.2	ppp0	1

## 2.11.1 Uso della tabella di routing

Il singolo nodo riceve un datagramma:

- Estraе dall'intestazione IP\_D=indirizzo IP di destinazione
- Seleziona il route per tale IP\_D, confrontandolo con i campi D presenti nella tabella, processo di **table lookup**
- Se il route esiste, esegue l'azione di instradamento suggerita dai campi G e IF, altrimenti genera un messaggio di errore(Tipicamente notificato all'indirizzo sorgente (ICMP-Destination Unreachable

## 2.11.2 Table lookup

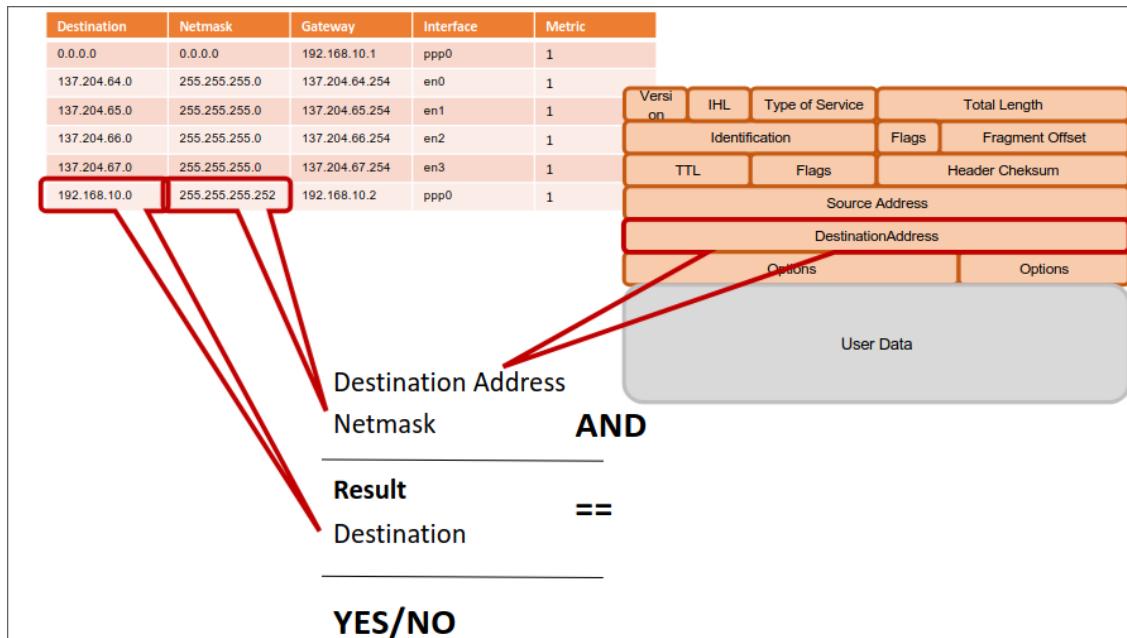
La ricerca nella tabella avviene confrontando:

- indirizzo di destinazione IP\_D del datagramma
- destinazione D di ciascun route
- Utilizzando la netmask (N) del route

La procedura viene detta di "longest prefix match":

- IP\_D AND N = R : l'indirizzo del datagramma e netmask di ciascuna riga
- R=D : se è uguale la route viene selezionata e il processo termina altrimenti si passa al route successivo

L'ordine di lettura, inizia dalla riga che presenta una netmask con un numero maggiore di bit a 1



### 2.11.3 Esempio lock up

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	...
2	192.168.2.0	255.255.255.0	...
3	192.168.2.18	255.255.255.255	...

- Datagramma con IP dest. = 192.168.2.18
  - Confronto prima con riga 3, poi con riga 2 e poi riga 1

192.168.002.018      bitwise AND  
255.255.255.255  
192.168.002.018  $\equiv$  192.168.002.018

- La riga 3 è quella giusta (host specific)

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	...
2	192.168.2.0	255.255.255.0	...
3	192.168.2.18	255.255.255.255	...

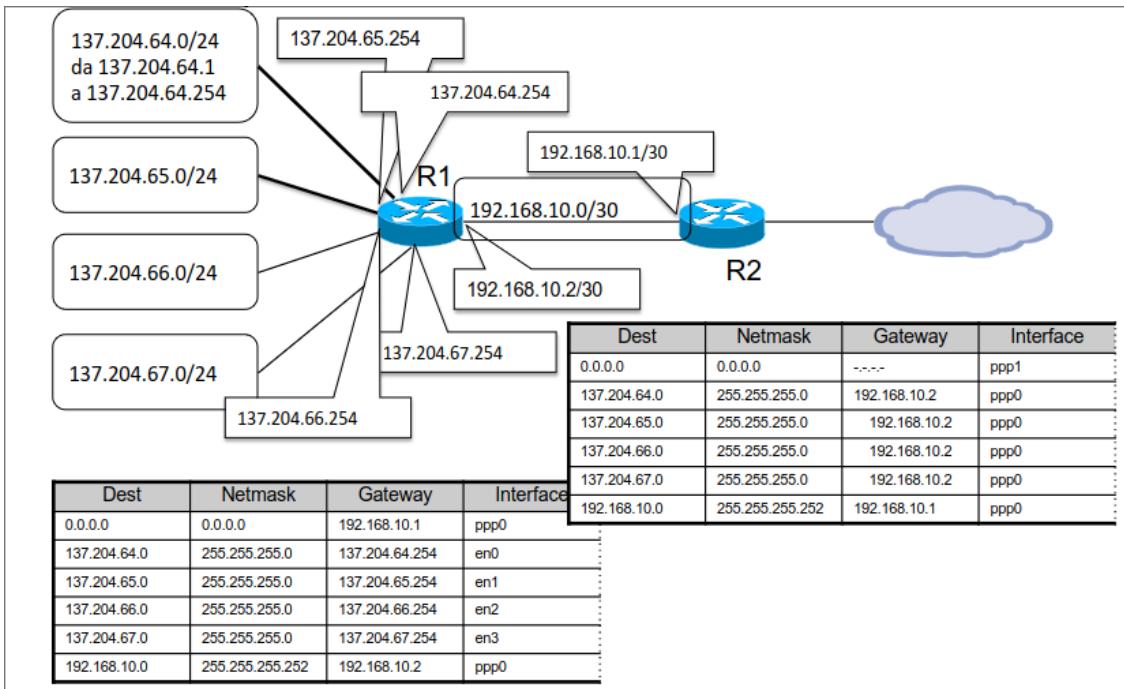
- Datagramma con IP dest. = 192.168.2.22

192.168.002.022  
255.255.255.255

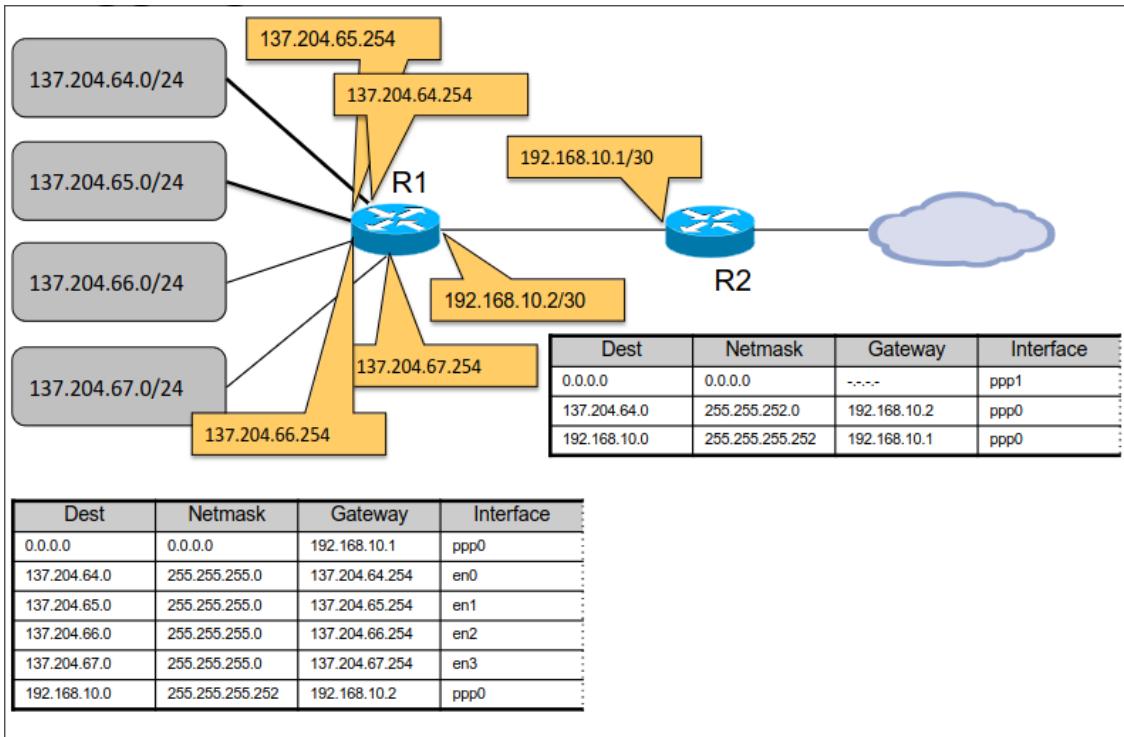
192.168.002.022  
255.255.255.000  
192.168.002.000 == 192.168.002.000

- La riga 2 è quella giusta (network specific)

## 2.11.4 Semplificazione delle tabelle



I route verso le 4 network possono essere aggregate in una sola, R2 vede le 4 reti come 1 sola (il gateway verso quelle destinazioni è R1)

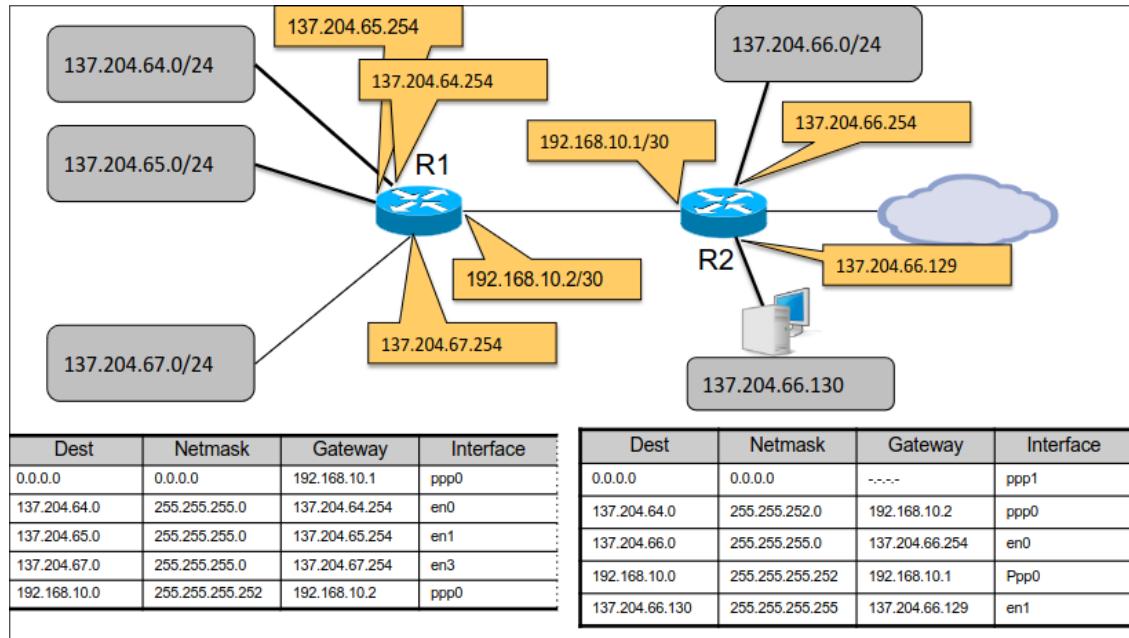
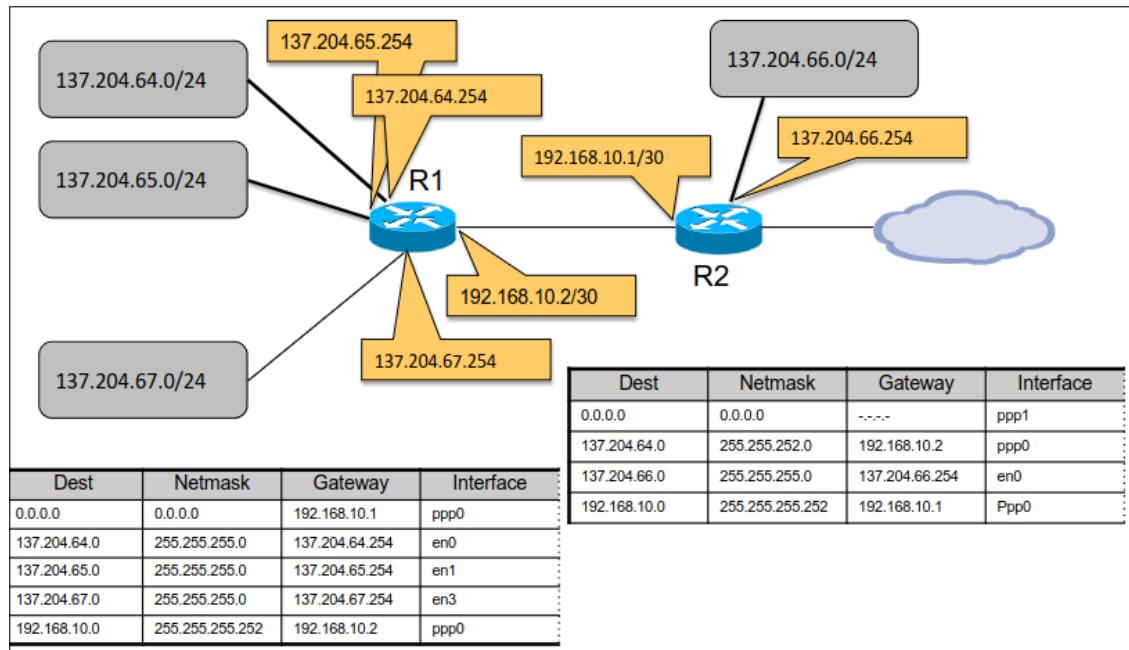


## 2.11.5 Perchè ordinare i route

Dare priorità alle route più specifiche.

L'ordinamento in funzione della Netmask decrescente garantisce di considerare: singoli host, reti piccole, reti grandi.

E' possibile implementare eccezioni a regole generali che possono convivere nella medesima tabella



## 2.12 Gateway

Il Gateway è il responsabile della consegna del datagramma.

### 2.12.1 Il ruolo del gateway

Il table look-up sceglie la D i-esima =  $D_i$

La funzione di instradamento invia il datagramma a  $IF_i$ , con l'obiettivo di consegnarlo al gateway  $G_i$

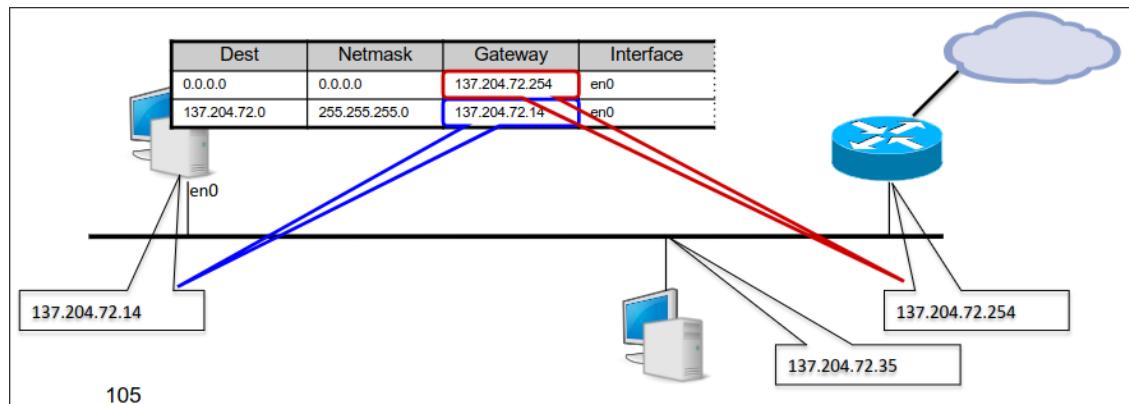
**Perchè non è sufficiente  $IF_i$ ?**

Perchè l'instradamento IP è basato sull'appartenenza alla network, Host della stessa network possono comunicare direttamente, Host di network diverse comunicano attraverso gateway

### 2.12.2 Uso del Gateway

Il campo gateway della tabella di routing serve per specificare il tipo di instradamento.

- **Instradamento diretto** : la sintassi dipende dall'implementazione (In win l'instradamento è locale se gateway=IP locale, in UNIX se = 0.0.0.0)
- **Instradamento indiretto** : Gateway = numero IP del router da contattare



105

# Chapter 3

## La logica degli indirizzi IP

### 3.1 IP e Netmask

Il numero IP ha valore assoluto in rete, un IP pubblico deve essere unico su Internet, i numeri IP sorgente e destinazione caratterizzano il dtagramma in quanto parte della sua intestazione

La netmask:

- relativa al singolo nodo
- non viene trasportata nell'intestazione del dtagramma
- è parte della tabella di routing dei singoli nodi
- Ai medesimi indirizzi possono corrispondere netmask diverse in nodi diversi (route aggregation)

Non è sempre stato così, inizialmente la suddivisione tra net-ID e host-ID era assoluta

### 3.2 Classi delle reti

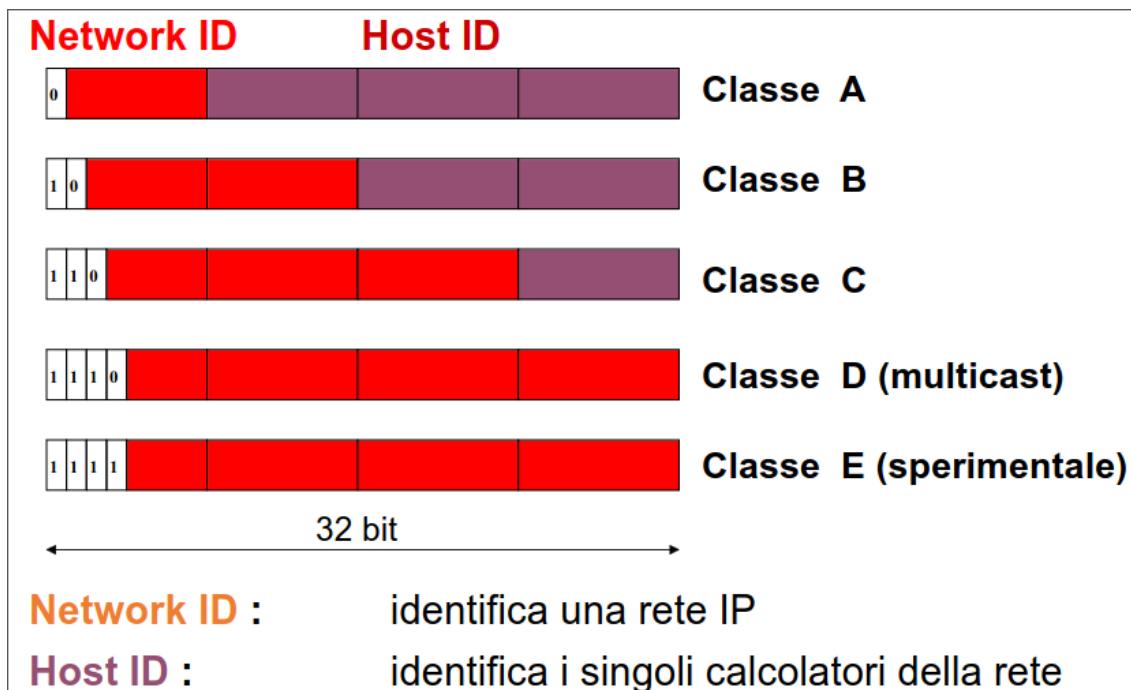
Durante a fase iniziale di Internet furono definite diverse "classi" di network differenziate per dimensione

La parte iniziale del Net-ID differenzia le classi:

- 0 classe A
- 10 classe B
- 110 classe C

La definizione delle classi è standard e quindi nota a tutti, i router riconoscono la classe di una rete dai primi bit dell'inizio (ricavando di conseguenza il Net-ID)

### 3.2.1 Classi di Indirizzi



### 3.2.2 Intervalli di Indirizzi

- Classe A: da **0.0.0.0** a **127.255.255.2255**
- Classe B: da **191.0.0.0** a **191.255.255.2255**
- Classe C: da **192.0.0.0** a **223.255.255.2255**
- Classe D: da **224.0.0.0** a **239.255.255.2255**
- Classe E: da **240.0.0.0** a **255.255.255.2255**

Indirizzi riservati:

- **0.0.0.0** : indica l'host corrente senza specificarne l'indirizzo
- HOST-ID tutto a zero : viene usato per indicare la rete
- **0.x.y.z** : indica un certo Host-ID sulla rete corrente senza specificare il Net-ID
- **255.255.255.255** : è l'indirizzo di broadcast su Internet
- **127.x.y.z** : è il loopback, che redirige i datagrammi agli strati superiori dell'host corrente

## 3.3 Le sottoreti

A un'amministrazione è assegnata una network, la quale può essere suddivisa in sotto-amministrazioni logicamente separate.

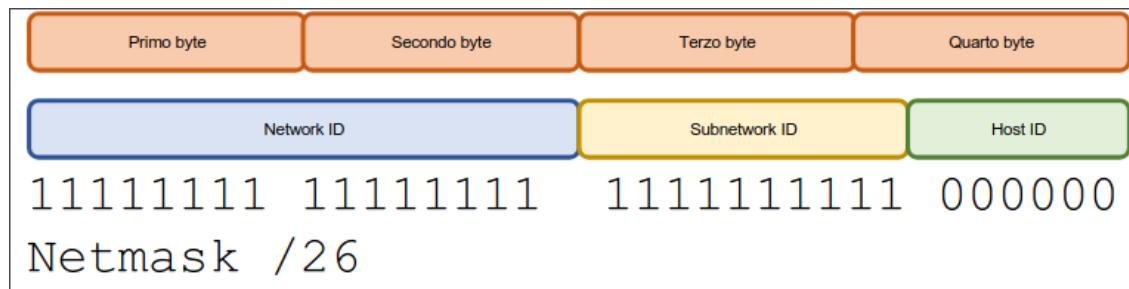
Converrebbe quindi "frammentare" la network in **"sub-network"** da assegnare alle sotto-amministrazioni. Si decide localmente una sotto-partizione Net/Hpst ID indipendentemente dalle classi. Si frammetta l'Host-ID in due parti:

- la prima identifica la sottorete (subnet-ID)
- la seconda identifica i singoli host della sottorete

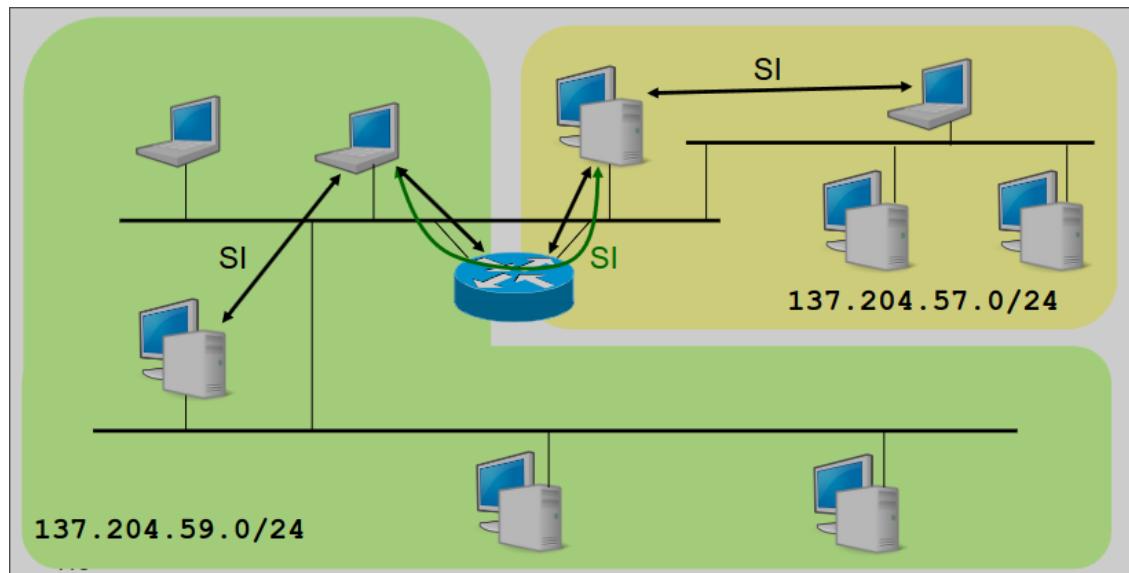
La ripartizione deve essere locale e reversibile, tutta Internet vede comunque una certa network come entità unitaria

### 3.3.1 Subnetting

La suddivisione è locale alla singola intervaccia (deve essere configurabile localmente)  
Si personalizza la netmask.



Subnet diverse essendo Network diverse, hanno bisogno di un gateway per comunicare.



#### Esempio: Università di Bologna

Una network di classe B (137.204.0.0) ha numerose entità distinte nella stessa amministrazione (Facoltà, Dipartimenti ecc..).

Si suddivide la network in sottoreti .

Il primo byte del Host-ID viene utilizzato come indirizzo di sottorete, dalla network di classe B si ricavano 254 network della dimensione di una classe C, **Netmask = 255.255.255.0**

### 3.3.2 CIDR: Classeless InterDomain Routing

Il CIDR rompe la logica delle classi nei router:

- la dimensione del Net-ID può essere qualunque
- Le tabelle di routing devono comprendere anche la netmask
- Generalizzazione delle subnetting/supernetting (reti IP definite da Net-ID/Netmask)

### Obiettivi del CIDR

I suoi obiettivi sono:

- Allocazione di reti IP di dimensioni variabili (utilizzo più efficiente degli indirizzi)
- Accorpamento delle informazioni di routing (où reti contigue rappresentate da un'unica riga nelle tabelle di routing)
- Miglioramento di due situazioni critiche
  - Limitatezza di reti di classe A e B
  - Crescita esplosiva delle dimensioni delle tabelle di routing

### 3.3.3 Supernetting

Consiste nel raggruppare più reti con indirizzi consecutivi, e indicarle nelle tabelle di routing con una sola entry accompagnata dalla opportuna Netmask.

### 3.3.4 Esempio

Un ente ha bisogno di circa 2000 indirizzi IP, una rete di classe B è troppo grande (64k indirizzi, meglio 8 reti di classe C ( $8 * 256 = 2048$  indirizzi) dalla 194.24.0.0 alla 194.24.7.0.

**Supernetting:** si accorpano le 8 reti contigue in un'unica super-rete:

- Identificativo: 194.24.0.1-194.24.7.254
- Supernet mask: 255.255.248.0
- Indirizzi: 194.24.0.1-194.24.7.254
- Broadcast 194.24.7.255

### Accorpamento

Accorpamento di N reti IP ( $N = 2^{32}$ ):

- contigue:
  - 194.24.0.0/24+194.24.1.0/24=194.0.0/23
  - 194.24.0.0/24+194.2.0/24=non contigue
- allineate secondo i multibl di  $2^n$ :
  - 194.24.0.0/24+.1.0/24+.2.0/24+.3.0/24=194.24.0.0/22
  - 194.24.0.0/24+.3.0/24+.4.0/24+.5.0/24=non allineate

### 3.3.5 Supernetting e Subnetting

subnetting e Supernetting sono operazioni duali:

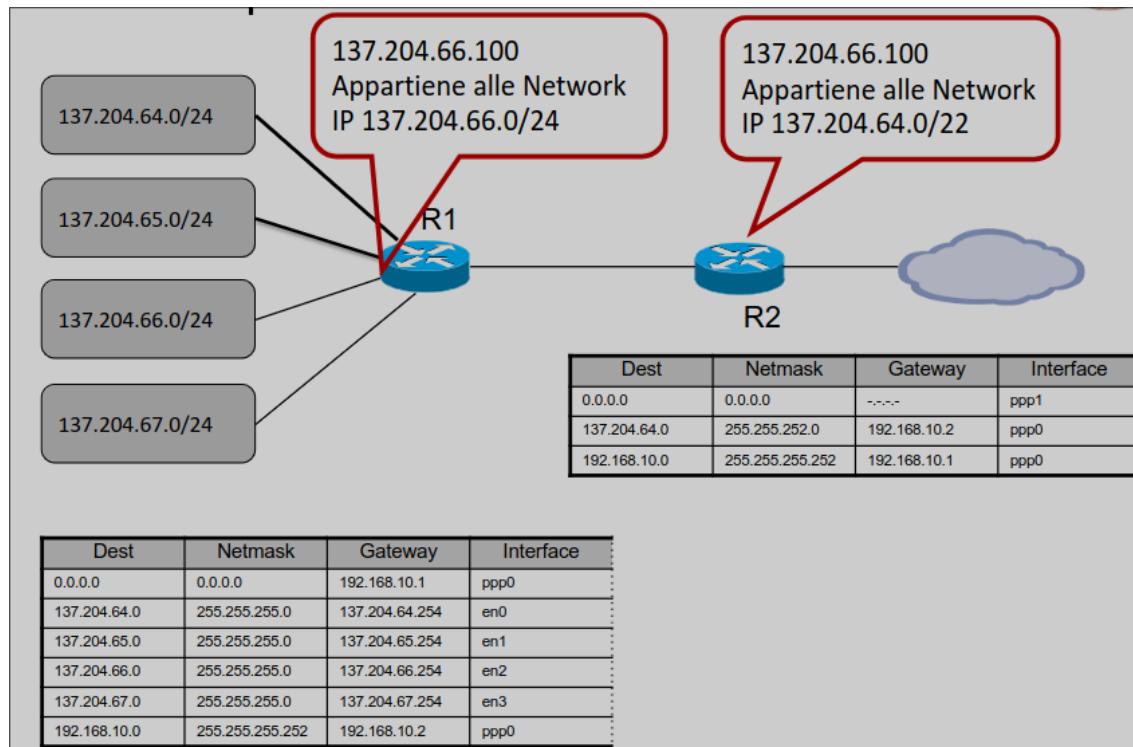
- Subnetting: n bit del Host-ID diventano parte del Net-ID
- Supernetting: n bit del Net-ID diventano parte del Host-ID

### 3.3.6 Oggi

La distinzione fra Net-ID e Host-ID è locale funzione della Netmask

Lo stesso indirizzo può essere intrprerato in modo diverso in punti diversi della rete

Tutte le tabelle di instradamento devono contenere la colonna Netmask



# Chapter 4

## Protocollo ICMP

Il protocollo IP offre un servizio di tipo best effort, quindi non garantisce la corretta consegna dei datagrammi, se necessario si affida a protocolli affidabili di livello superiore.

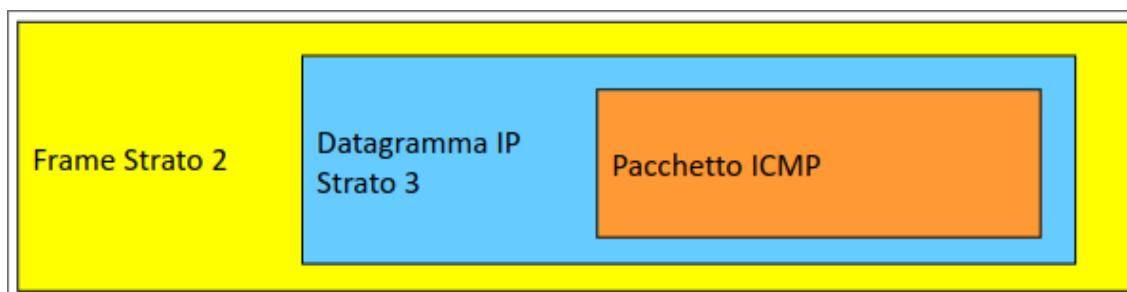
È comunque necessario un protocollo di controllo per :

- gestione di situazioni anomale
- notifica di errori o di irraggiungibilità della destinazione
- scambi di informazioni sulla rete

**ICMP:** Internet Control Message Protocol, segnala solamente errori e malfunzionamenti, ma non esegue alcuna correzione, e non rende affidabile l' IP

### 4.1 Quando viene usato

L'IP usa ICMP per la gestione di situazioni anomale, per cui ICMP offre un servizio ad IP.  
I pacchetti ICMP sono incapsulati in datagrammi IP, per cui ICMP è anche utente IP



## 4.2 Pacchetto ICMP

<b>IP header</b>	20 - 60 byte
<b>Message Type</b>	1 byte
<b>Message Code</b>	1 byte
<b>Checksum</b>	2 byte
<b>Additional Fields (optional)</b>	variabile
<b>Data</b>	variabile

- Type : definisce il tipo di messaggio ICMP
- Code : descrive il tipo di errore nel messaggio ICMP
- Checksum : controlla i bit errati nel messaggio ICMP
- Add. Fields : dipendono dal tipo di messaggio ICMP
- Data : intestazione a arte dei dati del datagramma che ha generato l'errore

## 4.3 Tipi di errori

### 4.3.1 Destination Unreachable (Type 3)

Generato da un Gateway quando la sottorete o l'host non sono raggiungibili.

Oppure è generato da un host quando si presenta un errore sull'indirizzo dell'entità di livello superiore a cui trasferire il datagramma.

#### Codici di errore

I codici di errore di Destination Unreachable possono essere:

- 0 = sorgente non raggiungibile
- 1 = host non raggiungibile
- 2 = protocollo non disponibile
- 3 = porta non raggiungibile
- 4 frammentazione necessaria ma bit don't fragment settato

### **4.3.2 Time Exceeded (Type = 11)**

È generato da un router quando il Time-to-Live di un datagramma si azzerà ed il datagramma viene distrutto (Code = 0).

Ottimamente viene generato da un Host quando un timer si azzerà in attesa dei frammenti per riassemblare un datagramma ricevuto in parte (Code = 1)

### **4.3.3 Source Quench (Type = 4)**

I datagrammi arrivano troppo velocemente rispetto alla capacità di essere processati: l'host sorgente deve ridurre la velocità di trasmissione (obsoleto)

### **4.3.4 Redirect (Type = 5)**

Generato da un router per indicare all'host sorgente un'altra strada più conveniente per raggiungere l'host destinazione

## **4.4 Informazioni**

### **4.4.1 Echo (Type=8) / Echo Reply (Type = 0)**

L'host sorgente invia la richiesta ad un altro host o ad un gateway., la destinazione deve rispondere. Questo metodo è usato per determinare lo stato di una rete e dei suoi host, la loro raggiungibilità e il tempo di transito nella rete

### **4.4.2 Additional Fields**

Identifier : identifica l'insieme degli echo appartenenti allo stesso test.

Sequence Number : identifica ciascun echo nell'insieme

Optional Data : usato per inserire eventuali dati di verifica

### **4.4.3 Timestamp Request (Type = 13) / Reply(Type = 14)**

L'host sorgente invia all'host destinazione un Originale Timestamp che indica l'istante in cui la richiesta è partita

L'host destinazione risponde inviando un:

- Recive Timestamp che indica l'istante che indica in cui la richiesta è stata ricevuta
- Transmit Timestamp che indica l'istante in cui la risposta è stata inviata

Serve per valutare il tempo di transito nella rete, al netto del tempo di processamento =  $T_{Transmit} - T_{Receive}$

### **4.4.4 Address Mask Request (Type = 17) / Reply (Type = 18)**

Inviato dall'host sorgente all'indirizzo di broadcast (255.255.255.255) per ottenere la subnet mask da usare dopo aver ottenuto il proprio indirizzo IP tramite RARP o BOOTP

### **4.4.5 Router Solicitation (Type = 10)**

### **4.4.6 Router Advertisement (Type = 9)**

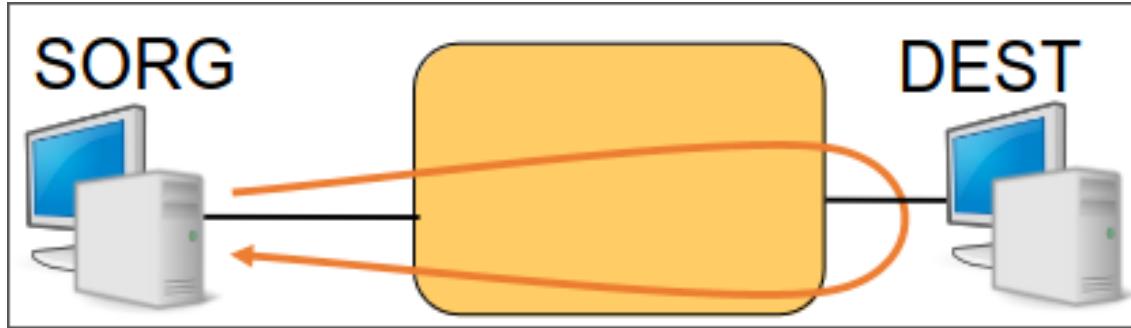
Utilizzato per localizzare i router connessi alla rete

## Chapter 5

# Applicazioni di ICMIP

### 5.1 PING

Il comando ping DEST permette di controllare se l'host DEST è raggiungibile o meno dalla sorgente (SORG



#### 5.1.1 funzionamento

SORG invia a DEST un pacchetto ICMP di tipo "echo", se l'host DEST è raggiungibile da SORG, dest risponde inviando indietro un pacchetto ICMP di tipo "echo reply"

#### 5.1.2 Opzioni

- **-n N** : permette di specificare quanti pacchetti inviare (un pacchetto al secondo)
- **-l M** specifica la dimensione in byte di ciascun pacchetto
- **-t** : esegue il ping finché interrotto con Ctrl-C
- **-a** : traduce l'indirizzo IP in nome DNS
- **-f** : setta il bit dont'fragment a 1
- **-i T** : setta time-to-live = T
- **w T<sub>out</sub>** : specifica un timeout in millisecondi

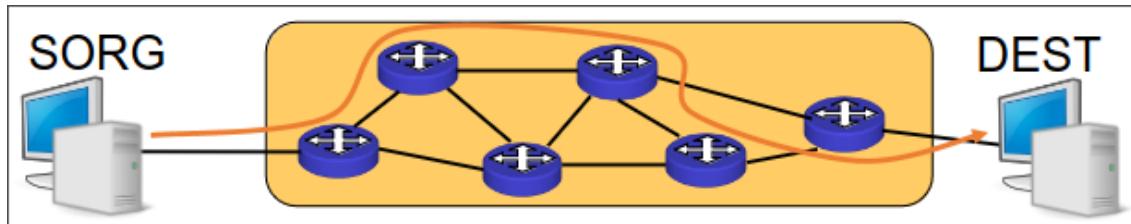
### 5.1.3 Output

L'output mostra:

- la dimensione del pacchetto "echo reply"
- l'indirizzo IP di DEST
- il numero di sequenza della risposta
- il "time-to-live" TTL
- il "round-trip time" (RTT)
- alcuni risultati statistici: N° pacchetti persi, MIN, MAX e media del RTT

### 5.1.4 Traceroute

Il comando **tracert DEST** permette di conoscere il percorso seguito dai pacchetti inviati da SORG e diretti verso DEST



### 5.1.5 Funzionamento

1. SORG invia a DEST una serie di pacchetti ICMP di tipo ECHO con un TIME-TO-LIVE progressivo da 1 a 30 (per default)
2. Ciascun nodo intermedio decremente TTL
3. Il nodo che rileva TTL=0 invia a SORG un pacchetto ICMP di tipo TIME EXCEEDED
4. SORG costruisce una lista dei nodi attraversati fino a DEST

### 5.1.6 Output

L'output mostra il TTL, il nome del DNS e l'indirizzo IP dei nodi intermedi ed il ROUND-TRIP-TIME (RTT)

# Chapter 6

## Gestione della enumerazione

### 6.1 Dispositivi di rete

#### 6.1.1 DHCP

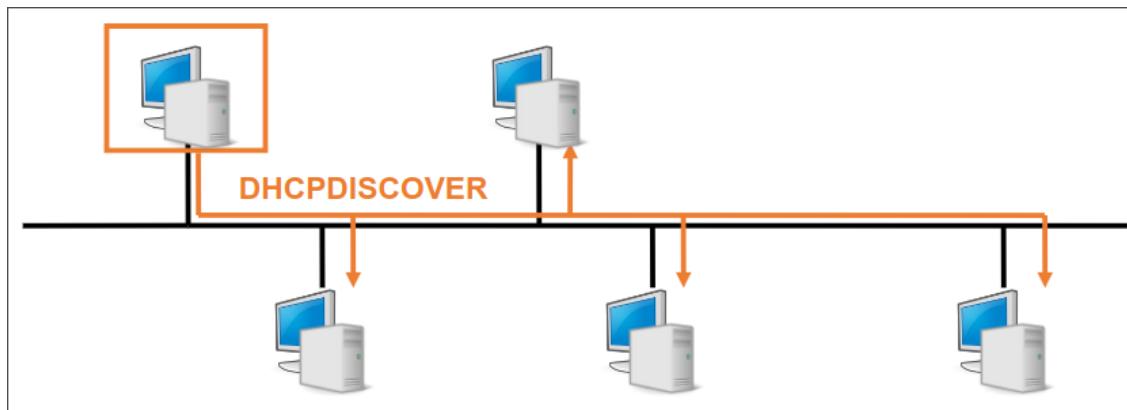
Il DHCP permette ad un Host di ottenere una configurazione IP.  
Consente la configurazione automatica e dinamica di:

- Indirizzo IP
- Netmask
- Host name
- Default gateway
- Server DNS

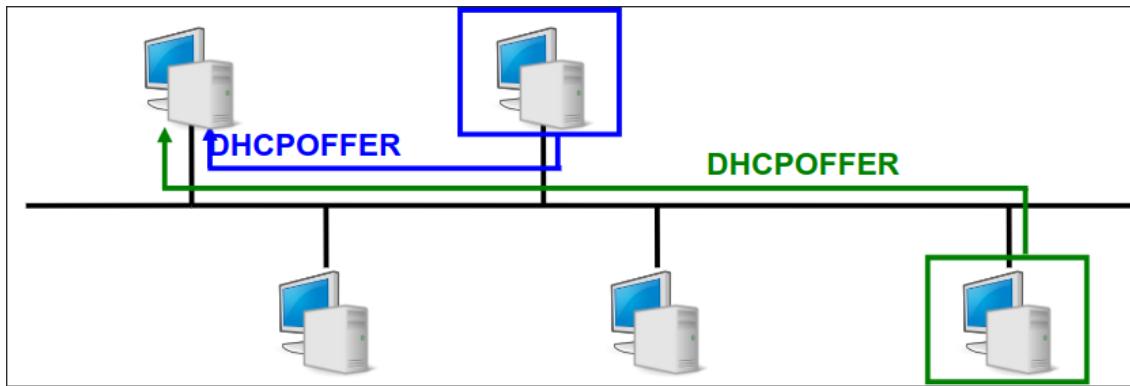
Server su porta 67 UDP

#### Funzionamento

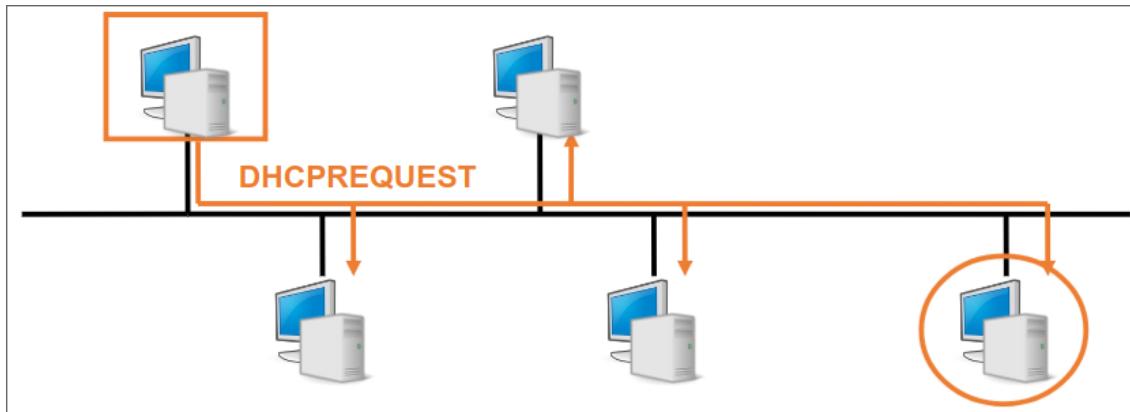
Quando l'host attiva l'interfaccia di rete, invia in modalità broadcast un messaggio **DHCPDISCOVER** in cerca di un server DHCP



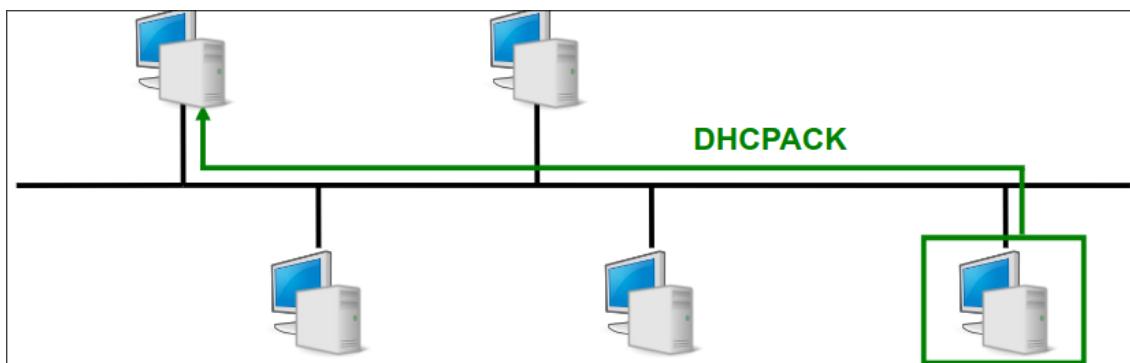
Ciscun server DHCP persente risponde all'host con un messaggio **DHCPOFFER** con cui propone un indirizzo IP



L'host accetta una delle offerte proposte dal server e manda un messaggio **DHCPREQUEST** in cui chiede la configurazione, specificando il server



Il server DHCP risponde con un messaggio **DHCPACK** specificando i parametri di configurazione



### 6.1.2 Packet Filter

Il Packet Filter permette o blocca l'invio di pacchetti da e verso determinati indirizzi, e protegge la rete dal traffico "vagante"

### 6.1.3 Application Layer Gateway (ALG) / Proxi

Il Proxi controlla la comunicazione a livello applicativo

#### **6.1.4 Firewall**

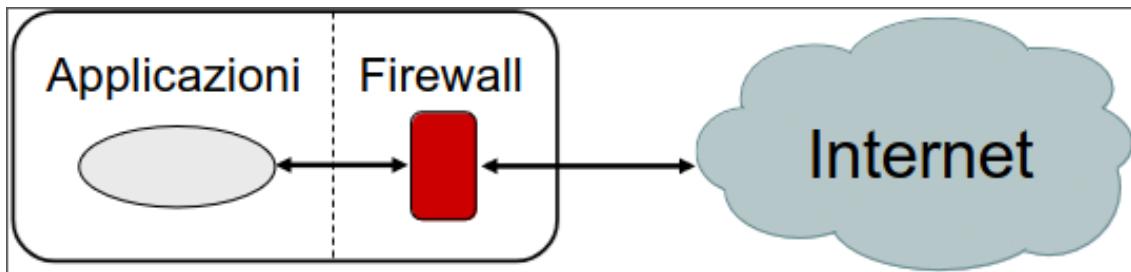
Il Firewall, è la combinazione dei precedenti dispositivi, e serve per proteggere le risorse interne da accessi esterni

#### **6.1.5 Network Address Translator (NAT)**

Il NAT riduce la richiesta dello spazio di indirizzamento Interne, nasconde gli indirizzi IP interni e esegue un packet filtering per il traffico sconosciuto

# Chapter 7

## Packet Filter e Firewall

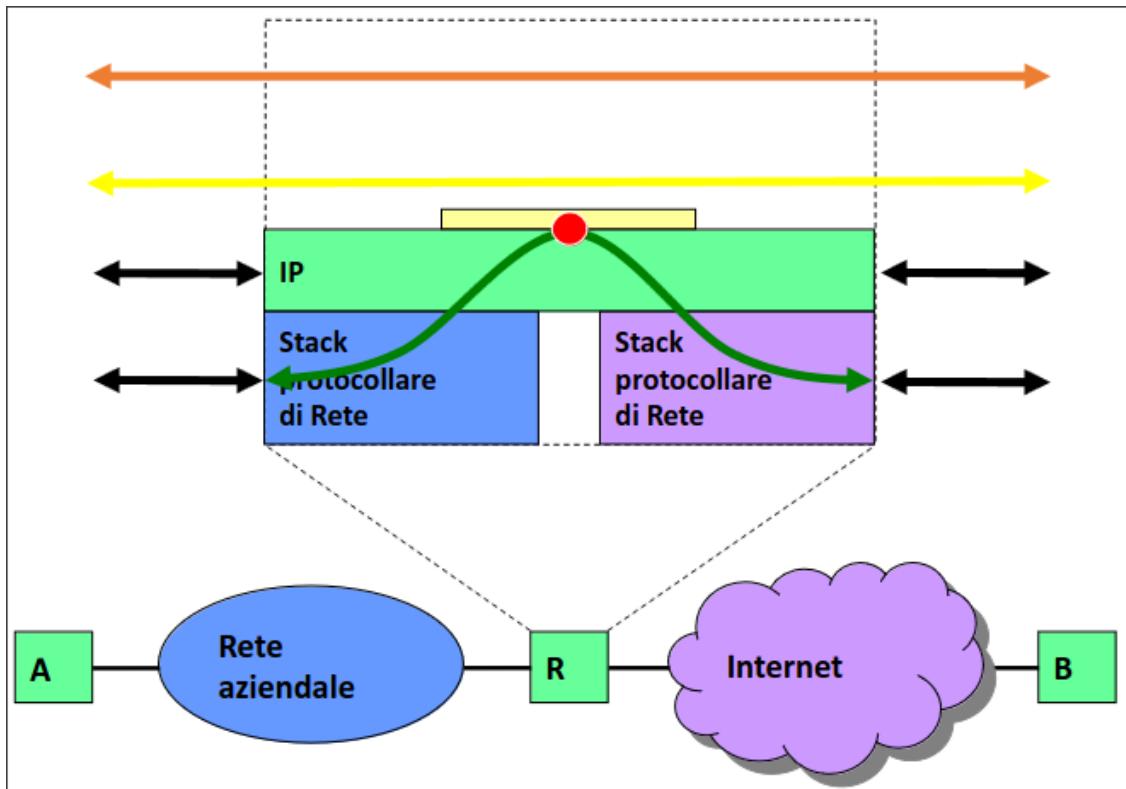


### 7.1 Firewall

#### 7.1.1 Packet filter

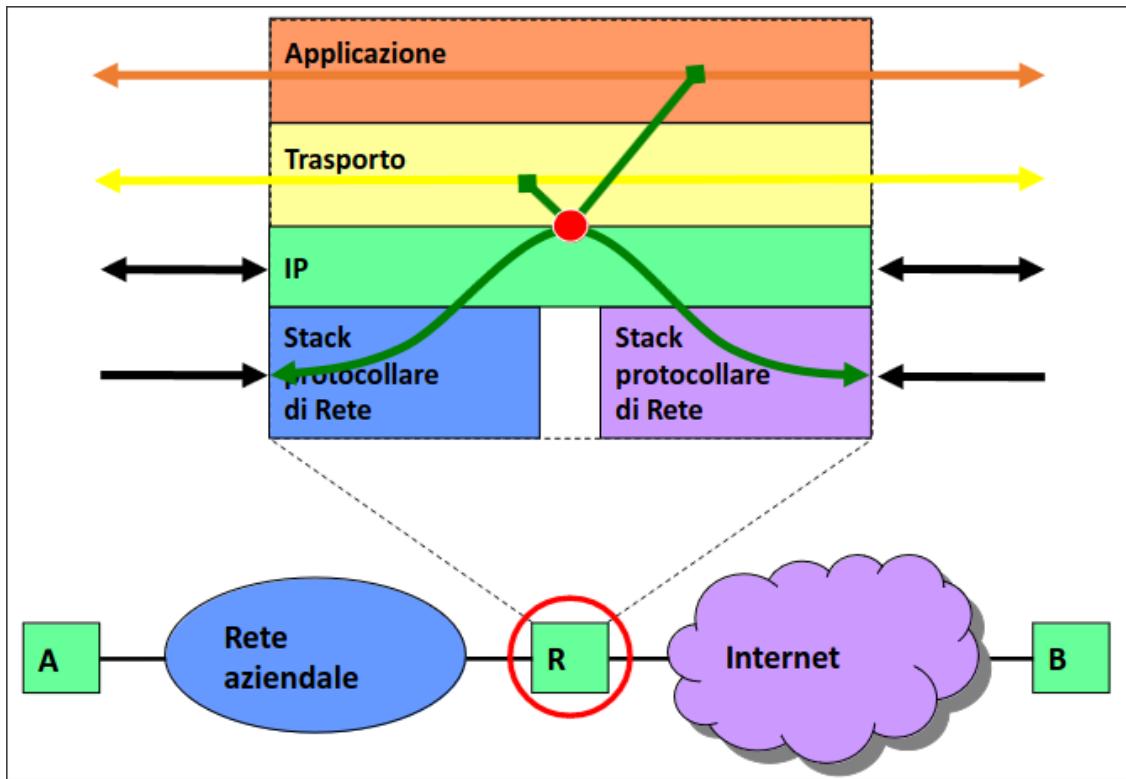
IL packet filter filtra i pacchetti seguendo le politiche stabilite :

- Filtri: generalmente configurati staticamente
- La maggioranza delle configurazioni non permettono pacchetti per porte "non-standar" (Internet Assigned Numbers Authority - IANA)



### 7.1.2 Stateful Packet Inspection

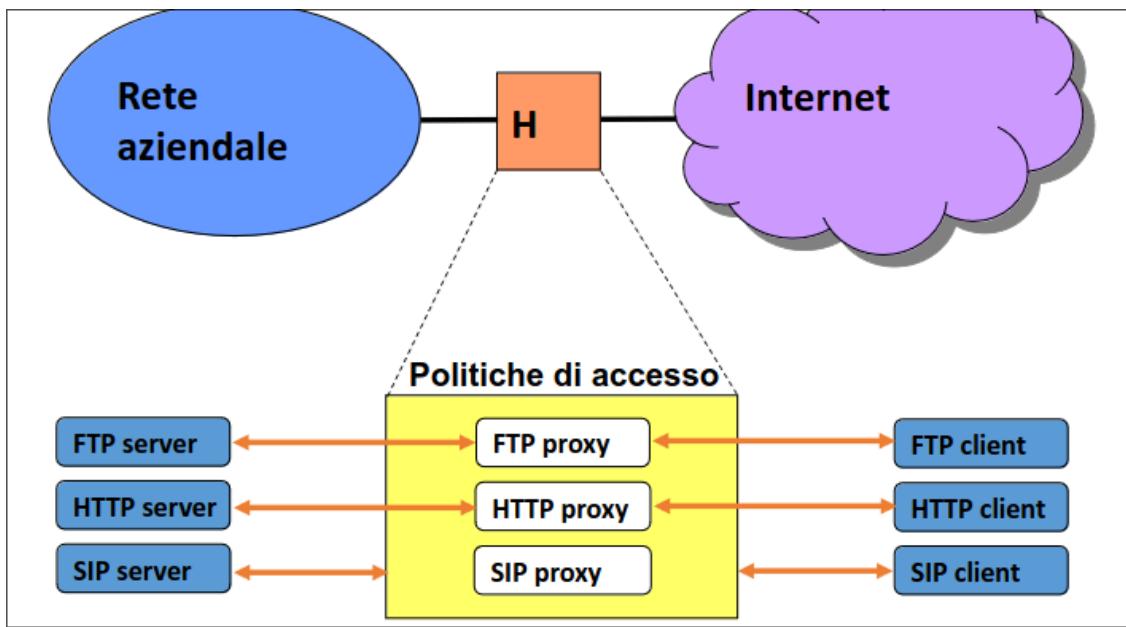
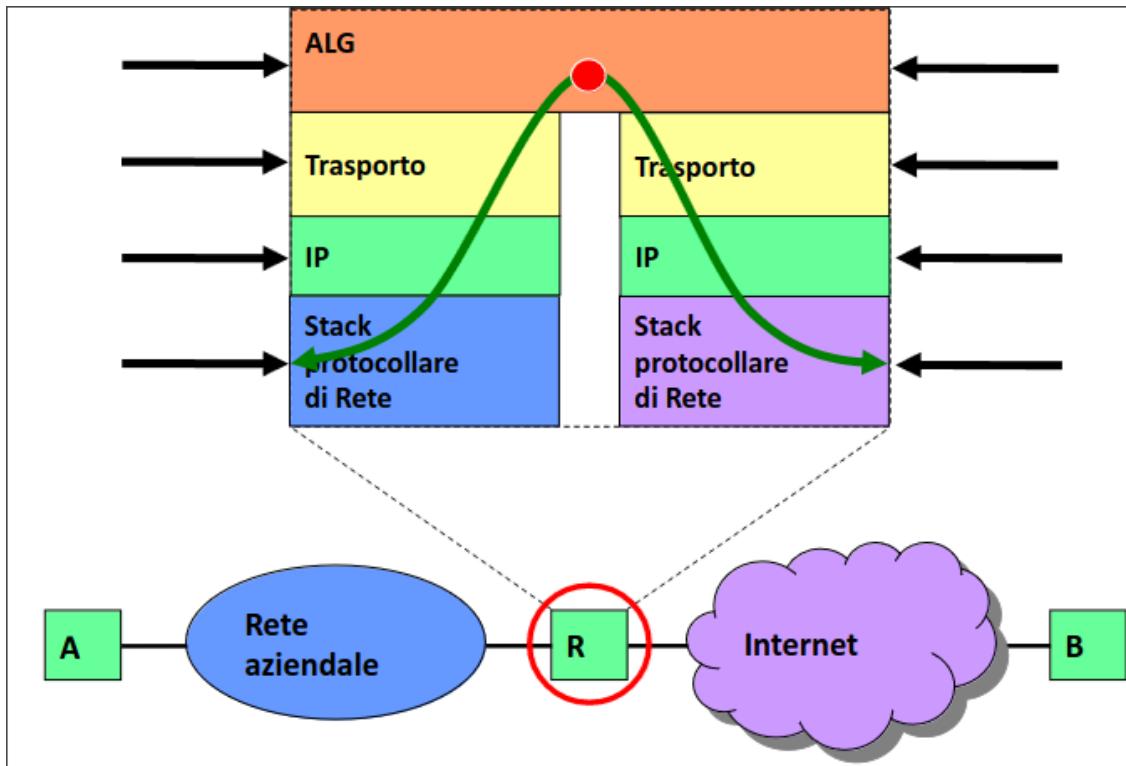
Mantiene il contesto dei pacchetti sia nel trasporto che nello strato applicativo, e adatta dinamicamente le specifiche dei filtri.



### 7.1.3 Application Layer Gateway (trasparente o proxy esplicito)

Monitora le conessioni: analizza il contenuto dei protocolli applicativi, a scapito della sicurezza di comunicazione end-to-end.

Adatta dinamicamente le specifiche dei filtri.

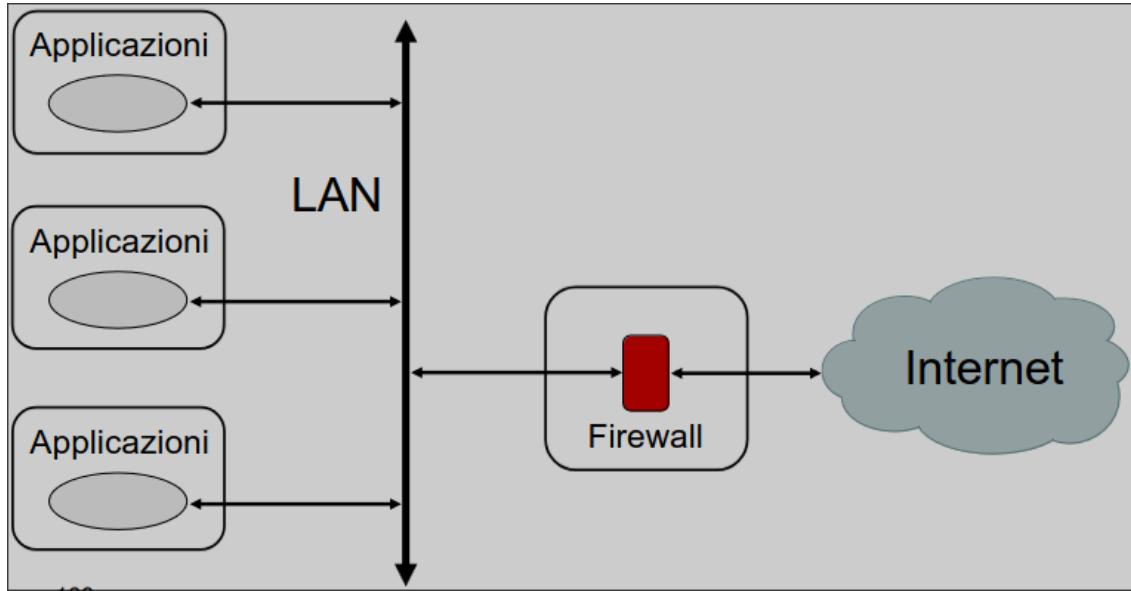


## 7.2 Protezione Host: firewall

Un firewall è un filtro software/hardware che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete.

Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi

esterni. Tipicamente è usato in accessi domestici a larga banda (ADSL, FTTH).  
Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale.



Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall, e solo il traffico autorizzato deve attraversare il firewall.

Ma si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti.

Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host

In fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete:

- **default deny** : tutti servizi non esplicitamente permessi sono negati
- **default permit** : tutti i servizi non esplicitamente negati sono permessi

## 7.3 Livelli di implementazione

Un firewall può essere implementato come:

- packet filter
- proxy server
  - application gateway
  - circuit-level gateway

### 7.3.1 Packet Filter

Si interpone un router fra la rete locale e internet, sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce, il filtro scarta i datagrammi sulla base di :

- indirizzo IP sorgente e destinazione
- tipo di servizio a cui il datagramma è destinato (per TCP/UDP)
- interfacce di provenienza o destinazione

### 7.3.2 Proxy server0

Nella rete protetta l'accesso ad internet è consentito solo ad alcuni host.

Si interpone un server apposito detto proxy server per realizzare la comunicazione per tutti gli host.  
Il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale.

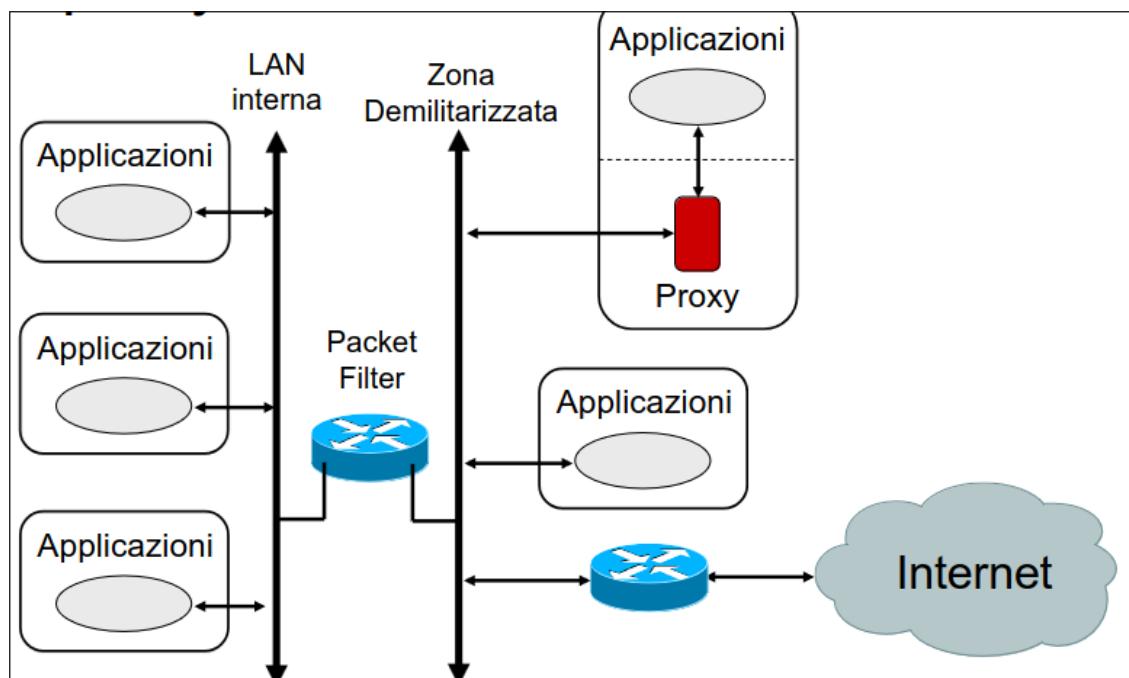
#### Application level

Viene impiegato un proxy server dedicato per ogni servizio che si vuole garantire

#### Circuit level gateway

È un proxy server generico in grado d inoltrare le richieste relative a molti servizi

## 7.4 Configurazione di packet filter e proxy

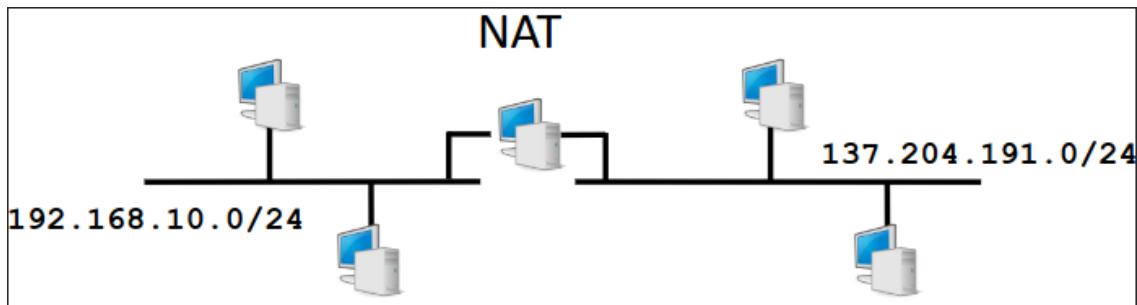


## Chapter 8

# Network Address Translation

Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento).

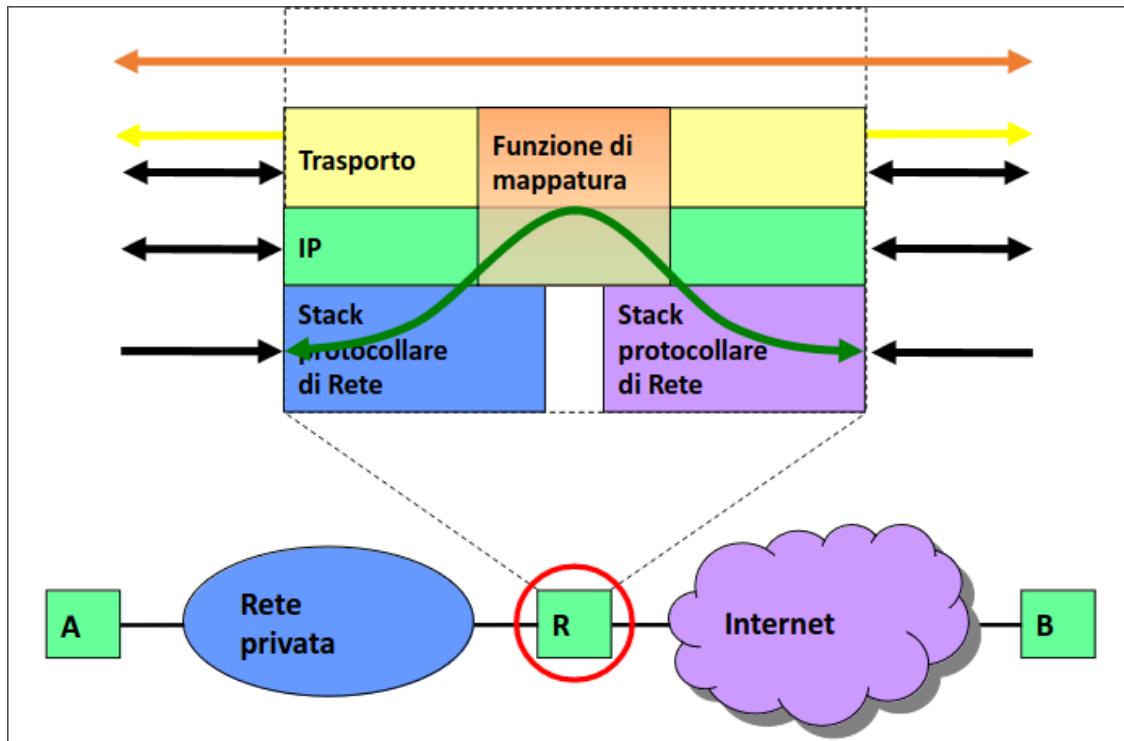
Permette a IP private l'accesso a reti IP pubbliche tramite un apposito gateway, è utile per ripiarmiare indirizzi IP pubblici e il riutilizzo di indirizzi IP privati



### 8.1 Motivazioni

- Efficiente uso dello spazio degli indirizzi
- Condividere uno o pochi indirizzi
- Uso di indirizzi privati nella LAN locale (10.x.x.x., 192.168.x.x, ..)
- Rende gli host interni non accessibili dall'esterno
- Include un packet filter, stateful packet inspection configurati dinamicamente

## 8.2 Network (+Port) Address Translator (NAT)

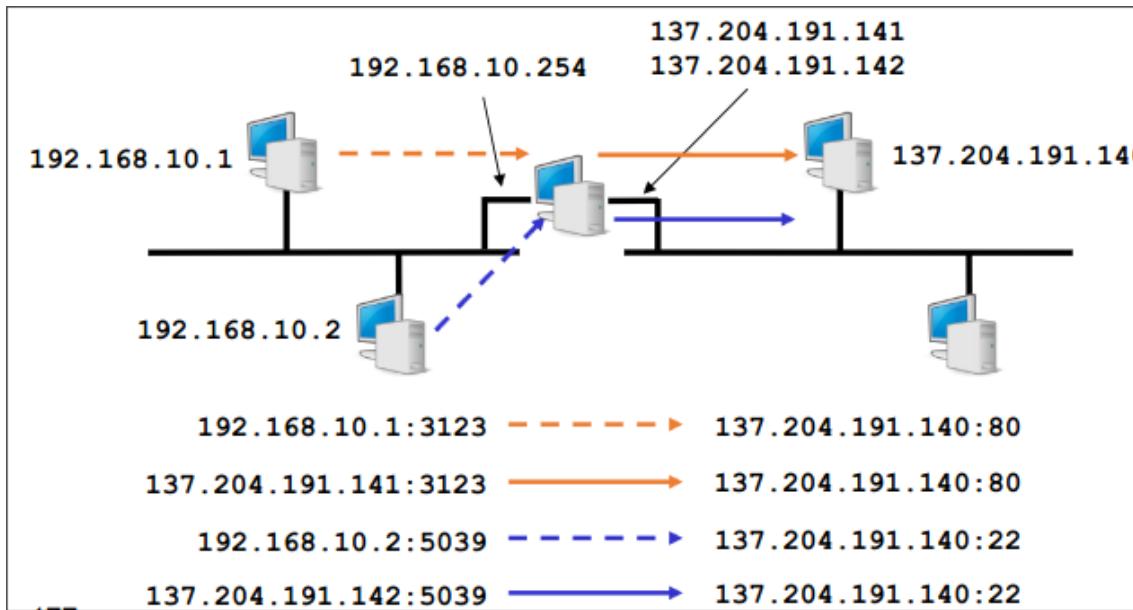


## 8.3 Basic Nat

### 8.3.1 Conversione di Indirizzo

Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica).

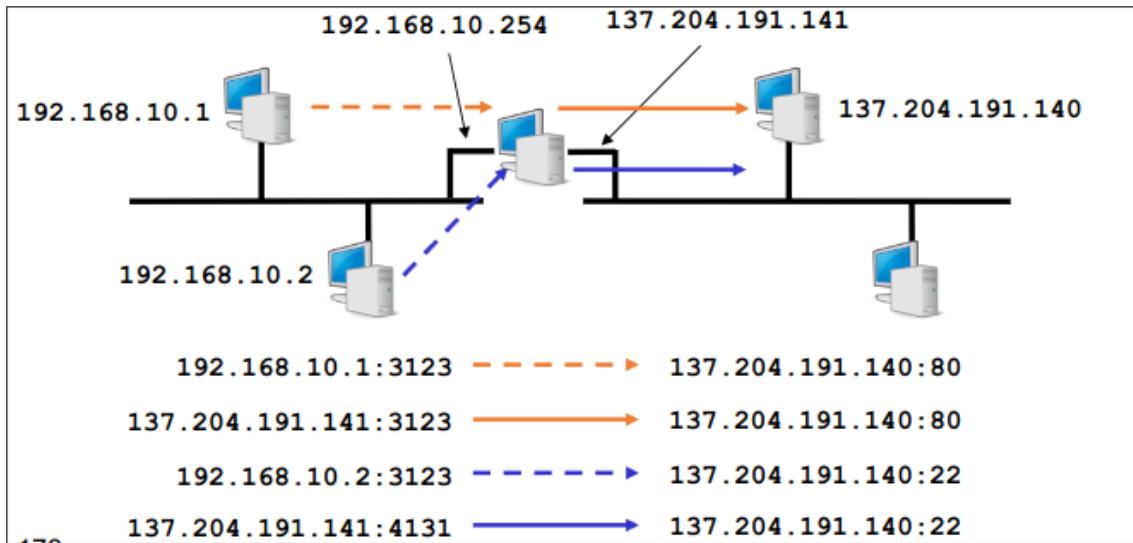
Conversioni contemporaneamente limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



### 8.3.2 Conversione di indirizzo e porta

Il NAT può fornire anche la conversione di indirizzo IP e porte TCP o UDP.

Le conversioni contemporanee sono possibili anche con un unico indirizzo IP pubblico del gateway NAT

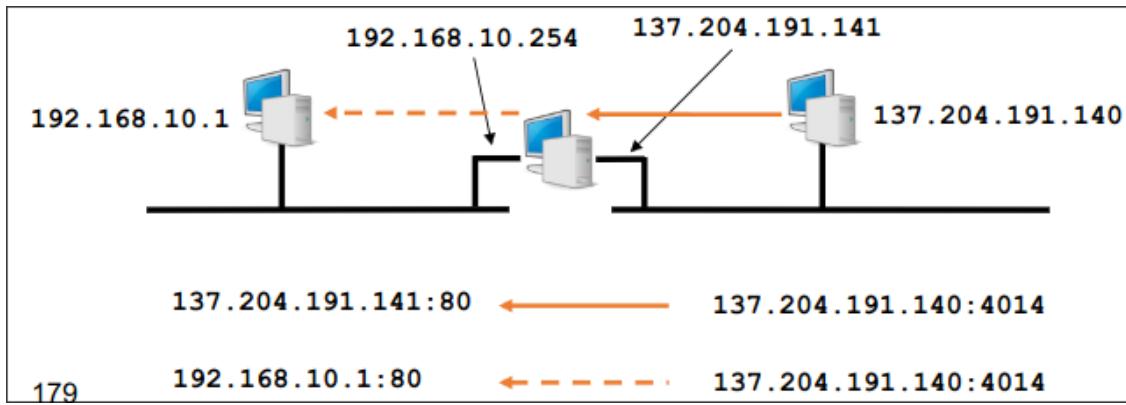


### 8.3.3 Direzione delle connessioni

La direzione delle connessioni sono tipicamente da rete privata verso rete pubblica.

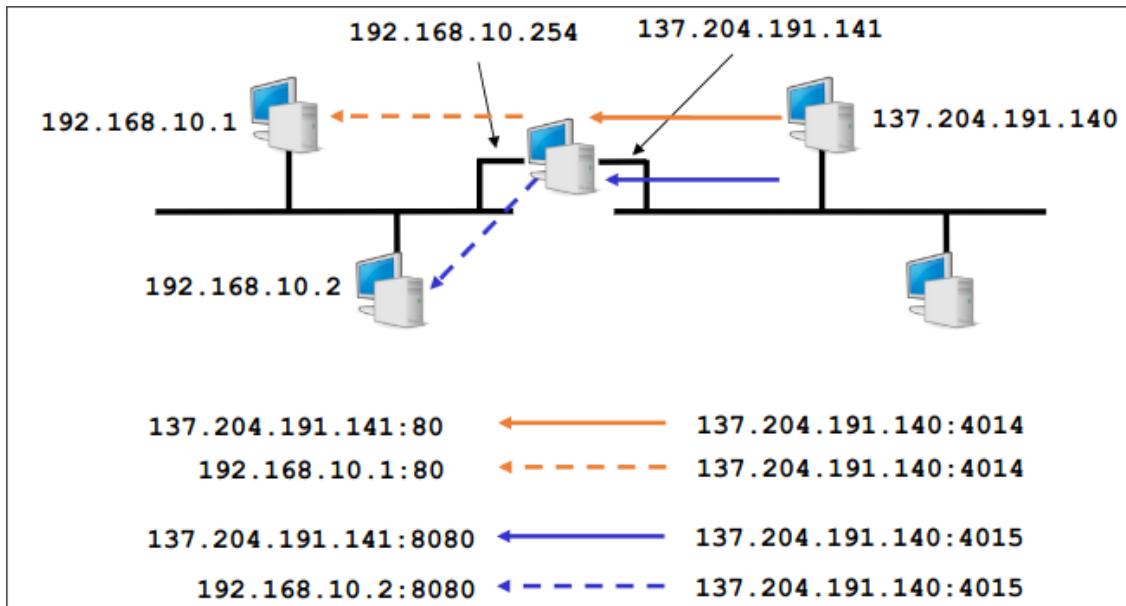
Il NAT si preoccupa di effettuare la conversione inversa quando arrivano le risposte, e registra le corrispondenze in corso in una tabella.

È anche possibile contattare dalla rete pubblica un host sulla rete privata se il tipo di NAT e la relativa configurazione lo permette.

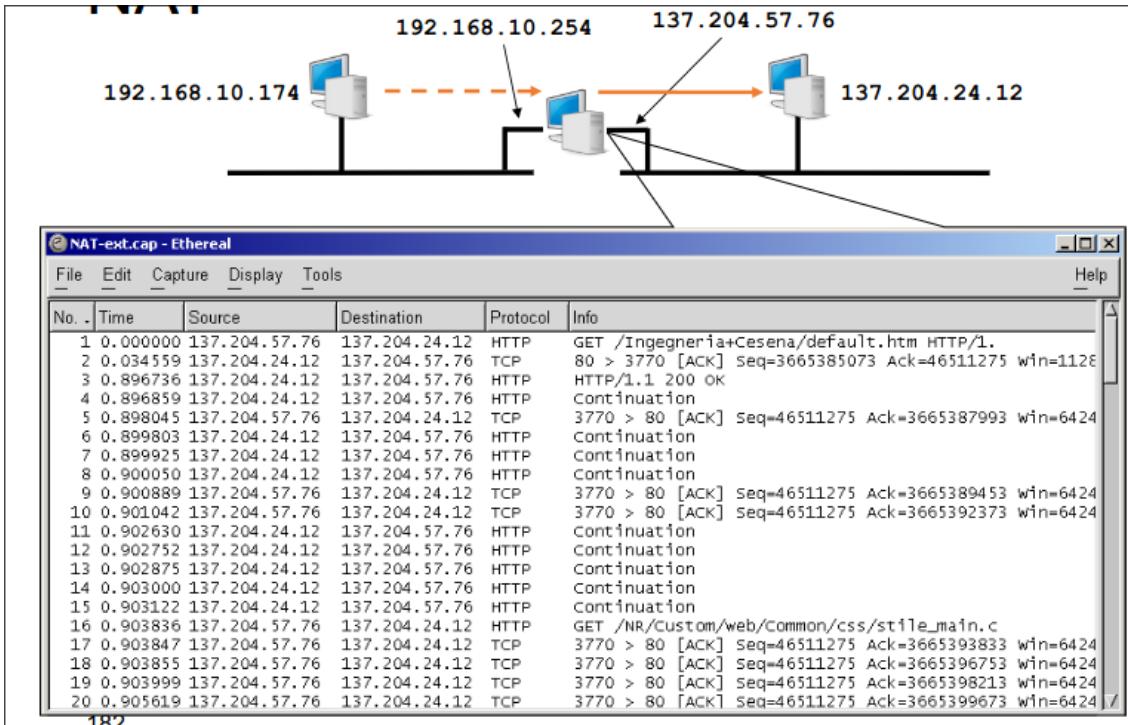
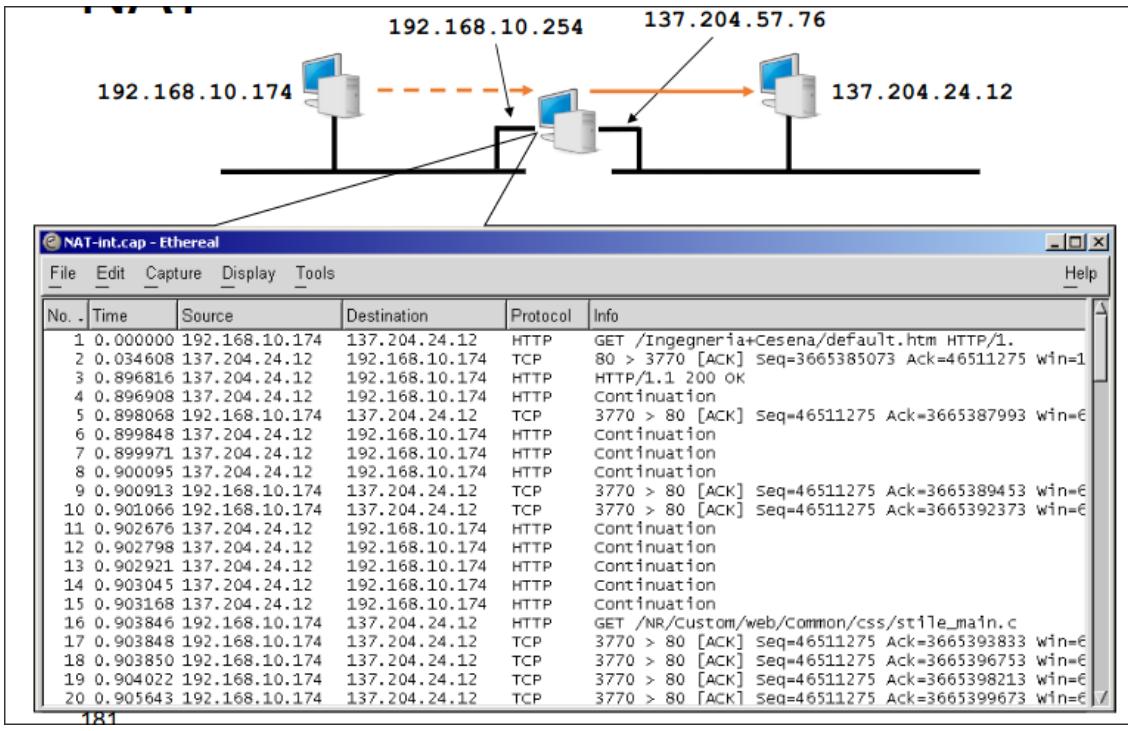


### 8.3.4 Port forwarding

Il NAT permette l'ingresso di pacchetti estinti a porte specifiche effettuando la traduzione opportuna.



### 8.3.5 Analisi di connessioni attraverso NAT



## 8.4 NAT e applicazioni di rete

Il NAT è trasparente per l'applicazione, modifica l'intestazione IP e TCP/UDP ma non il payload. Questo potrebbe essere un problema in alcuni casi specifici:

### 8.4.1 Le applicazioni non sono trasparenti al NAT

Contengono indirizzi IP e payload.

FTP utilizza due connessioni parallele:

- connessione per l'intestazione con il server tramite linea di comando
- connessione per il trasferimento dei dati da e verso il server
- i parametri della seconda sono specificati dai dati della prima

### 8.4.2 Il tipo di traffico permesso dipende dal tipo di nat

- Full Cone NAT
- (Port) Restricted Cone NAT
- Symmetric NAT

# Chapter 9

## IPv6

### 9.1 Problematiche dell'indirizzamento IP

- Mobilità :
  - Indirizzi riferiti alla rete di appartenenza
  - Se un host viene spostato in un'altra rete, il suo indirizzo IP deve cambiare (configurazione automatica con DHCP, mobile IP)
- Sicurezza :
  - Scarsa protezione del datagramma IP (intestazione in chiaro), IPsec applicabile anche a IPv4
- Dimensioni della rete prefissate :
  - subnetting e CIDR
- Data l'enorme diffusione di Interne, il numero di indirizzi possibili è troppo basso (Reti IP private NAT)

### 9.2 Soluzione: IPPv6

Dati i problemi dell'IPv4 si è lavorato su una nuova versione con i seguenti obiettivi:

- Supportare molti miliardi di host
- Semplificare il routing
- Offrire meccanismi di sicurezza
- Offrire qualità di servizio (multimedialità)
- Gestire bene unicast e broadcast
- Consentire la mobilità
- Fare tutto questo consentendo future evoluzioni e garantendo compatibilità con il passato

# Chapter 10

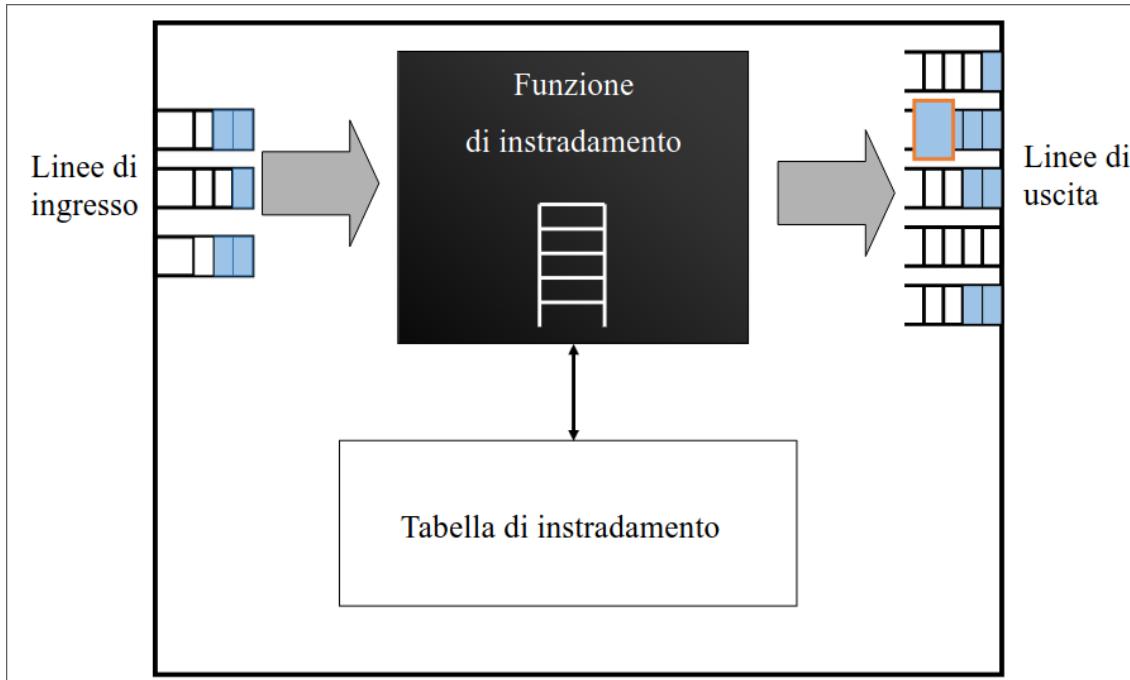
## Instradamento nelle reti a pacchetto e in Internet

### 10.1 Funzioni dell' IP

- Indirizzamento
- Frammentazione
- Instradamento
  - Decidere che percorso un datagramma deve seguire per raggiungere la destinazione alla sorgente
  - Utilizza le PCI dei datagrammi, in particolare l'indirizzo destinazione
  - Determina il comportamento della funzione di commutazione

Il problema dell'instradamento è più generale rispetto allo specifico protocollo di livello 3

## 10.2 Il nodo di commutazione a pacchetto



### 10.2.1 Store-and-Forward

Il pacchetto è verificato e memorizzato, si estraggono le informazioni di instradamento (indirizzo, priorità, casse di servizio).

Si confrontano queste informazioni con la tabella di instradamento, identificando una o più uscite su cui inviare il pacchetto.

Il pacchetto è inserito nella coda relativa all'uscita prescelta, in attesa della effettiva trasmissione. IL pacchetto viene prima memorizzato interamente nel nodo e quindi ritrasmesso nella direzione opportuna.

In generale dovrebbe esistere una base dati per il confronto che è la tabella di instradamento

## 10.3 Flooding

La soluzione più semplice è il flooding.

È molto adatto quando si desidera inviare una certa informazione a tutti i nodi della rete (broadcasting)

### 10.3.1 Funzionamento

Ogni nodo ritrasmette su tutte le porte di uscita ogni pacchetto ricevuto.

Prima o poi un pacchetto viene ricevuto da tutti i nodi della rete e quindi anche da quello a cui è effettivamente destinato.

Il primo pacchetto che arriva a destinazione ha fatto la strada più breve possibile.

L'elaborazione associata è pressoché nulla.

### 10.3.2 Problema

IL problema è la proliferazione di pacchetti, perchè nel singolo nodo ogni pacchetto viene copiato tante volte quante sono le intrfacce, e se è ritrasmesso sull'interfaccia da cui è arrivato il numero di copie cresce

esponenzialmente

### 10.3.3 Soluzione

Le soluzioni potrebbero essere:

- un nodo non può ritrasmettere il pacchetto nella direzione dalla quale è giunto
- ad ogni pacchetto viene associato un identificativo unico (l'indirizzo della sorgente e un numero di sequenza) e ciascun nodo mantiene in memoria una lista con gli identificativi dei pacchetti già trasmessi
  - Il nodo crea una lista dei pacchetti ricevuti e trasmessi
  - Ogni pacchetto già trasmesso, viene ignorato
  - Ogni pacchetto viene ritrasmesso da ogni nodo una sola volta
- Contatore del tempo di vita (TTL) di un pacchetto per evitare che giri all'infinito

## 10.4 Deflection routing (hot potato)

Nel Deflection routing quando un nodo riceve un pacchetto lo ritrasmette sulla linea d'uscita avente il minor numero di pacchetti in attesa di essere trasmessi

### 10.4.1 Per quali reti è adatto?

È adatto a reti in cui, i nodi di commutazione dispongono di spazio di memorizzazione molto limitato, e se si desidera minimizzare il tempo di permanenza dei pacchetti nei nodi

### 10.4.2 Propblemi

I pacchetti possono essere ricevuti fuori sequenza, e alcuni pacchetti potrebbero percorrere all'infinito un certo ciclo interno alla rete, semplicemente perchè le sue linee sono poco utilizzate

### 10.4.3 soluzioni

Si deve prevedere un meccanismo per limitare il tempo di vita dei pacchetti.

Non tiene conto della destinazione finale

## 10.5 Shortest path routing

Si assume che ad ogni collegamento della rete possa essere attribuita una lunghezza.

la **lunghezza** è un numero che serve a caratterizzare il peso di quel collegamento nel determinare la funzione di costo del percorso totale di trasmissione.

L'algoritmo cerca la strada di lunghezza minima fra ogni mittente e ogni destinatario.

Si applicano algoritmi di calcolo dello shortest path (Bellman Ford e Dijkstra).

### 10.5.1 Iplementazione

L'impementazione può essere:

- Centralizzata: un solo nodo esegue i calcoli per tutti
- Distribuita :
  - Ogni nodo esegue i calcoli per se

- Sincrona : tutti i nodi eseguono gli stessi passi dell'algoritmo nello stesso istante
- Asincrona : i nodi eseguono lo stesso passo dell'algoritmo in momenti diversi

## 10.6 Rappresentazione della rete

Ad una generica rete di telecomunicazione si può associare un grafo orientato  
Nel quale,

- i nodi rappresentano i terminali ed i commutatori
- gli archi rappresentano i collegamenti
- L'orientamento degli archi rappresenta la direzione di trasmissione
- il peso degli archi rappresenta il costo dei collegamenti, che può essere espresso in termini di:
  - numero di nodi attraversati (ogni arco ha peso unitario)
  - distanza geografica
  - ritardo introdotto dal collegamento
  - ritardo introdotto dal collegamento
  - inverso della capacità del collegamento
  - costo di un certo instradamento
  - una combinazione dei precedenti

## 10.7 Il grafo della rete

Una rete è un insieme di nodi di commutazione interconnessi da collegamenti.

Per rappresentarla si possono usare i modelli matematici della teoria dei grafi:

- Sia  $V$  un insieme finito di nodi
- Un arco è definito come una coppia di nodi  $(i, j), i, j \in V$
- Sia  $E$  un insieme di archi
- Un grafo  $G$  è definito come la coppia  $(V, E)$  e può essere:
  - Orientato se  $E$  consiste di coppie unitarie, cioè se  $(i, j) \neq (j, i)$
  - non-orientato: se  $E$  consiste in coppie non ordinate, cioè se  $(i, j) = (j, i)$
- Se  $(i, j) \in E$ , il nodo  $j$  è vicino del nodo  $i$

## 10.8 Routing shortest path nel mondo IP

Quando i nodi di rete vengono accesi conoscono solamente la configurazione delle loro interfacce, statica o dinamica con il DHCP.

Con queste informazioni popolano la tabella di instradamento iniziale.

Per implementare il routing shortest path verso una qualunque destinazione devono utilizzare:

- Uno o più protocolli di routing per scambiarsi informazioni ed apprendere la tecnologia della rete
- Uno o più algoritmi per il calcolo degli SP sulla base delle informazioni

## 10.9 Rouing distance vector

È basato su Bellman-Ford, in versione dinamica e distribuita (proposta da Ford-Fulkerson). È un protocollo semplice che richiede poche risorse.

### 10.9.1 Cosa implementa

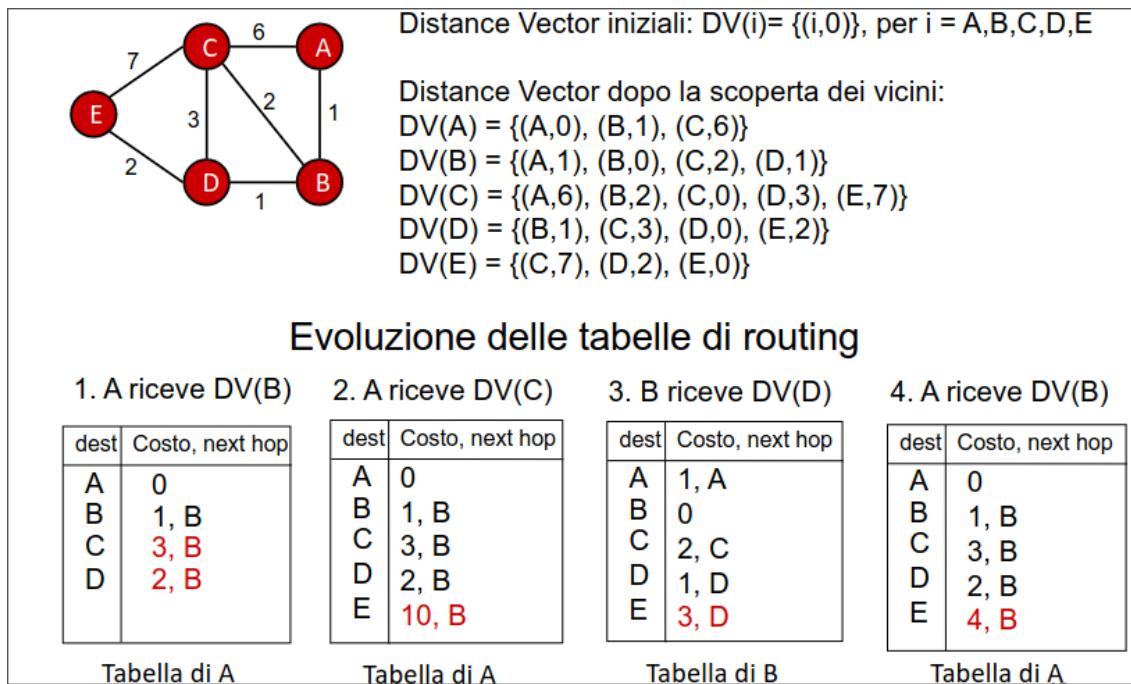
Implementa meccanismi di dialogo per fare si che:

- ogni nodo scopre i suoi vicini e ne calcola la distanza da se stesso
- e che ad ogni passo, ogni nodo invia ai propri vicini un vettore contenente la stima della sua distanza da tutti gli altri nodi della rete (quelli di cui è a conoscenza)

### 10.9.2 Problemi

Ha una convergenza e una partenza (cold start) lenta, inoltre ha problemi di stabilità, in quanto può portare al conteggio infinito

### 10.9.3 Esempio



### 10.9.4

Cold start e tempo di convergenza Allo start-up le tabelle dei singoli nodi contengono solo l'indicazione del nodo stesso a distanza 0 (i distance vector scambiati al primo passo contengono solo queste informazioni).

Da qui in poi lo scambio dei distance vector permette la creazione di tabelle sempre più complete. L'algoritmo converge al più dopo un numero di passi pari al numero di nodi della rete.

Se la rete è molto grande il tempo di convergenza può essere lungo.

Cosa succede se lo stato della rete cambia in un tempo inferiore a quello di convergenza dell'algoritmo?

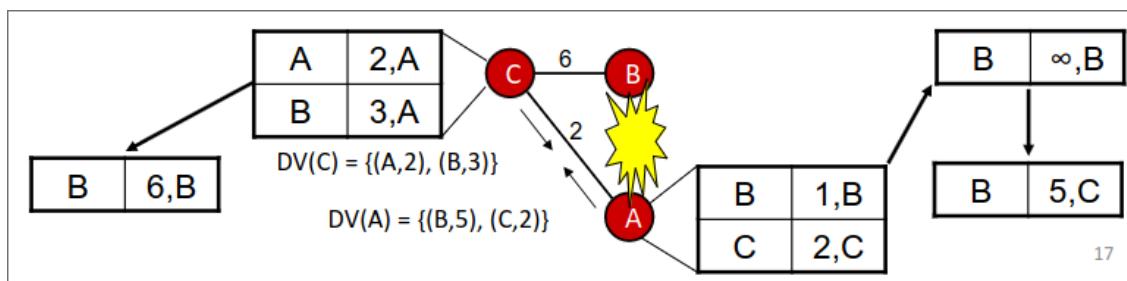
Il risultato diventa imprevedibile e si ritarda la convergenza

### 10.9.5 Bouncing effect

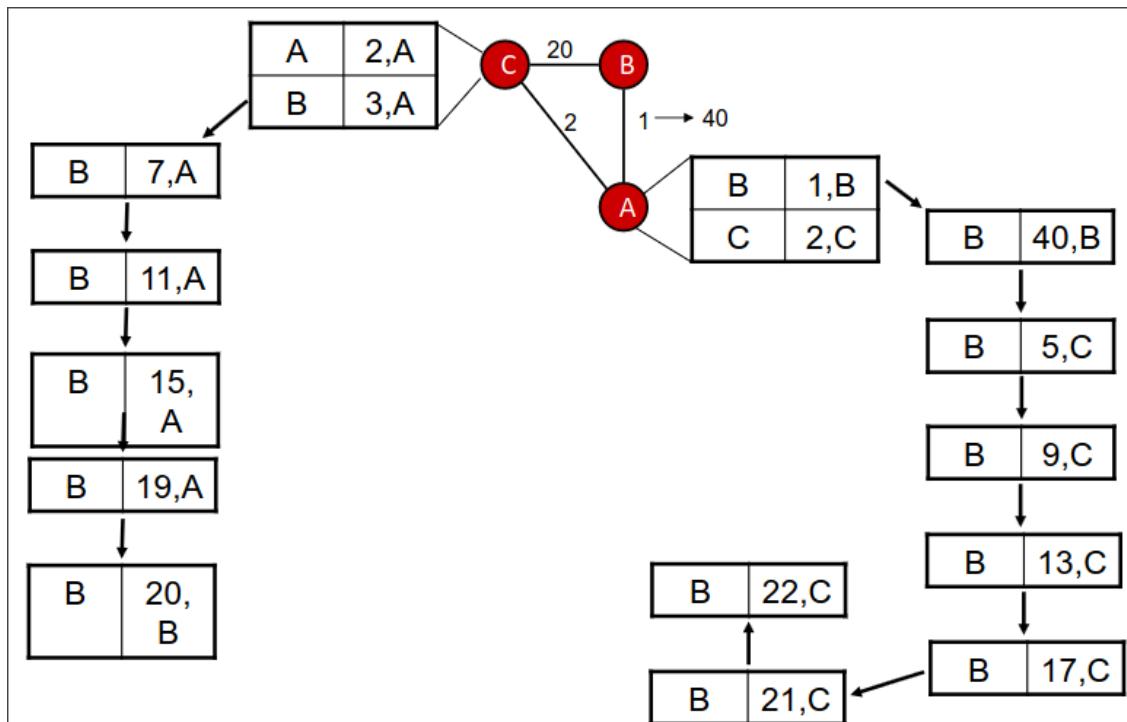
Il link tra due nodi A e B cade, A e B si accorgono che il collegamento non funziona e immediatamente pongono ad infinito la sua lunghezza.

Se altri nodi hanno nel frattempo inviato anche i loro vettori delle distanze, si possono creare delle incongruenze temporane, di durata dipendente dalla complessità della rete, ad esempio A crede di poter raggiungere B tramite un altro nodo C che a sua volta passa attraverso A

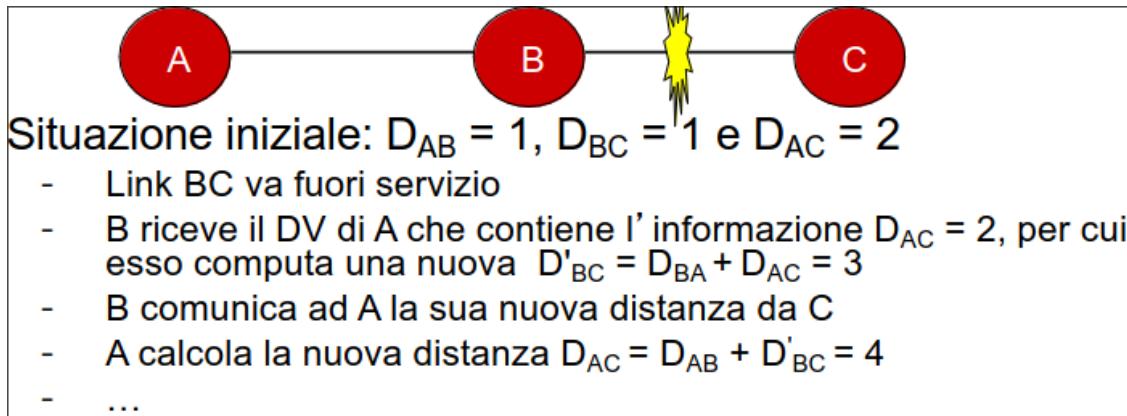
Queste incongruenze possono dare luogo a cicli, per cui due o più nodi si scambiano datagrammi fino a che non si esaurisce il TTL o finché non si converge nuovamente



### 10.10 Convergenza lenta



#### 10.10.1 Count to infinity



La cosa può andare avanti all'infinito, si può interrompere imponendo che quando una distanza assume valore  $D_{i,j} > D_{max}$  allora si suppone che il nodo destinazione  $J$  non sia raggiungibile  
Inoltre si possono introdurre meccanismi migliorativi.

#### 10.10.2 Split horizon

Split horizon è una tecnica molto semplice per risolvere in parte i problemi suddetti:

- Se A instrada i pacchetti verso una destinazione X tramite B, non ha senso per B cercare di raggiungere X tramite A.
- di conseguenza non ha senso che A renda nota a B la sua distanza da X

Un algoritmo modificato di questo tipo richiede che un router invii informazioni diverse ai diversi vicini.  
In pratica A, omette la sua distanza da X nel DV che invia a B (forma semplice) o inserisce tutte le destinazioni nel DV diretto a B, ma pone la distanza da X uguale a infinito

#### 10.10.3 Triggered update

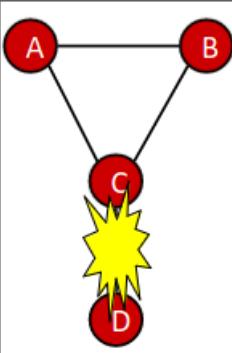
Una ulteriore modifica per migliorare i tempi di convergenza è relativ alla tempistica con cui i DV ai vicini. I protocolli basati su questi algoritmi richiedono di inviare periodicamente le informazioni delle distanze ai vicini.

È possibile che un DV legato ad un cambiamento della tipologia parta in ritardo e venga sopravanzato da informazioni vecchie inviate da altri nodi.

In pratica un nodo deve inviare immediatamente le informazioni a tutti i vicini qualora si verifichi una modifica della propria tabella di instradamento.

#### 10.10.4 Non basta

Questi rimedi non davvero risolutivi, infatti, sono ancora presenti situazioni patologiche in cui i protocolli Distance Vector convergono troppo lentamente o non convergono affatto.



- Inizialmente, A e B raggiungono D tramite C
- Dopo il guasto, C mette a  $\infty$  la sua dist. da D
- Dopo aver ricevuto il DV da C, A crede di poter raggiungere comunque D tramite B
- Idem per B che crede di poter usare A
- Stavolta A e B trasmettono i propri DV a C
- Si crea di nuovo un loop e un problema di convergenza

## 10.11 Routing link state

Utilizzando il **protocollo di routing** ogni nodo si costruisce un'immagine del grafo della rete.  
Noto il grafo della rete ogni nodo calcola le tabelle di routing utilizzando un opportuno algoritmo di routing

### 10.11.1 Scopo

Il protocollo di routing ha come scopo quello di permettere ad ogni nodo di crearsi l'immagine della rete:

- scoperta dei nodi vicini
- raccolta di informazioni dai vicini
- diffusione delle informazioni raccolte a tutti gli altri nodi della rete

### 10.11.2 Raccolta delle informazioni

Ogni router deve comunicare con i propri vicini ed "imparare" i loro indirizzi **Hello Packet**  
Deve poi misurare la distanza dai vicini, **Echo Packet**.

In seguito ogni router costruisce un pacchetto con lo stato delle linee (**Link State Packet o LSP** che contiene:

- La lista dei suoi vicini
- le lunghezze dei collegamenti per raggiungerli

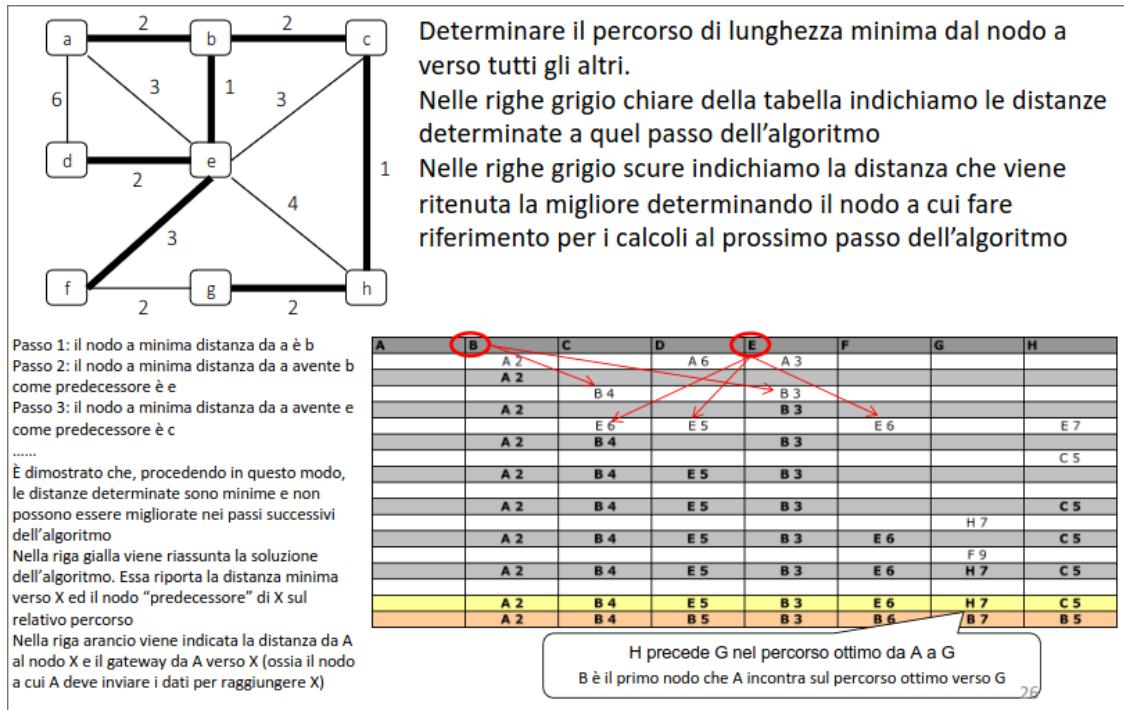
### 10.11.3 Diffusione ed elaborazione delle informazioni

I pacchetti LSP devono essere trasmessi da tutti i router a tutti gli altri router della rete. Per fare ciò si usa il **Flooding**, e nel pacchetto LSP occorre aggiungere :

- l'indirizzo del mittente
- un numero di sequenza
- una indicazione dell'età del pacchetto

Avendo ricevuto LSP da tutti i router, ogni router è in grado di costruirsi un'immagine della rete, tipicamente si usa l'algoritmo di Dijkstra per calcolare i cammini minimi verso ogni altro router

#### 10.11.4 Esempio



## 10.12 Il router IP

Il nodo di commutazione nelle reti IP viene detto **router**, il router è un nodo di commutazione a pacchetto specializzato per l'utilizzo del protocollo IP.

Nonostante siano tutti identificati con il termine router i nodi di commutazione della rete Internet possono essere fra loro molto diversi

### 10.12.1 Classificazione dei router

- SOHO(Small Office and HOme) router: utilizzo domestico o piccoli uffici, l'interfaccia sulla LAN (switch con poche porte Fast Ethernet 100Mbit/s e wifi)
- Router di accesso :
  - usato da ISP per fornire servizi di accesso
  - grande numero di porte di velocità media-bassa (50kbps /10Mbps)
  - è compatibile diversi protocolli e tecnologie di accesso (PPP, SLIP, ADSL, ecc...)
- Enterprise/campus router : sono interconnesse fra LAN per organizzazioni di medie dimensioni, e hanno poche porte ad alta velocità (Fast o Gigabit Ethernet)
- Backbone router : utilizzate per reti di trasporto e connessioni inter-domain, ha un piccolo numero di porte ad elevata velocità ( $\geq 1$  Gbps), ed è equipaggiato con sistemi di garanzia dell'affidabilità (ridondanza, monitoraggio remoto, ecc..)

### 10.12.2 Le funzioni

Le funzioni del router sono principalmente 4 :

## Routing

Il routing comprende :

- Scambio di informazioni con altri router (IGP/EGP)
- L'elaborazione locale (routing algorithm)
- popolazione delle tabelle di routing

## Forwarding IP

Table lookup e Header update

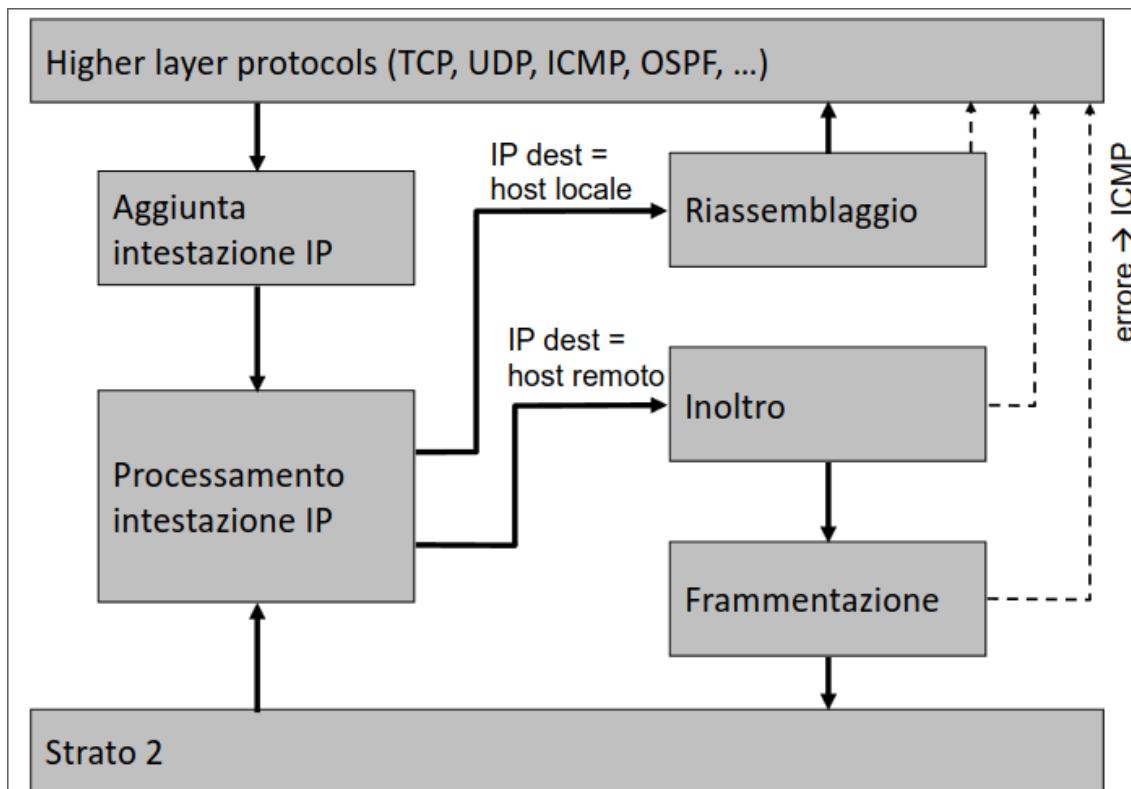
## Switching

Trasferimento dal datagramma da interfaccia di input a interfaccia di output

## Trasmissione

Trasmissione del datagramma sul mezzo fisico (utilizzando l'interfaccia di rete di output)

### 10.12.3 Schema funzionale di un router



### 10.12.4 Tabella di routing

La tabella di routing è il risultato degli algoritmi di routing e algoritmi. Ogni voce include il route prefix, next hop e metric.

Chiamata anche Routing Information Base (RIB)

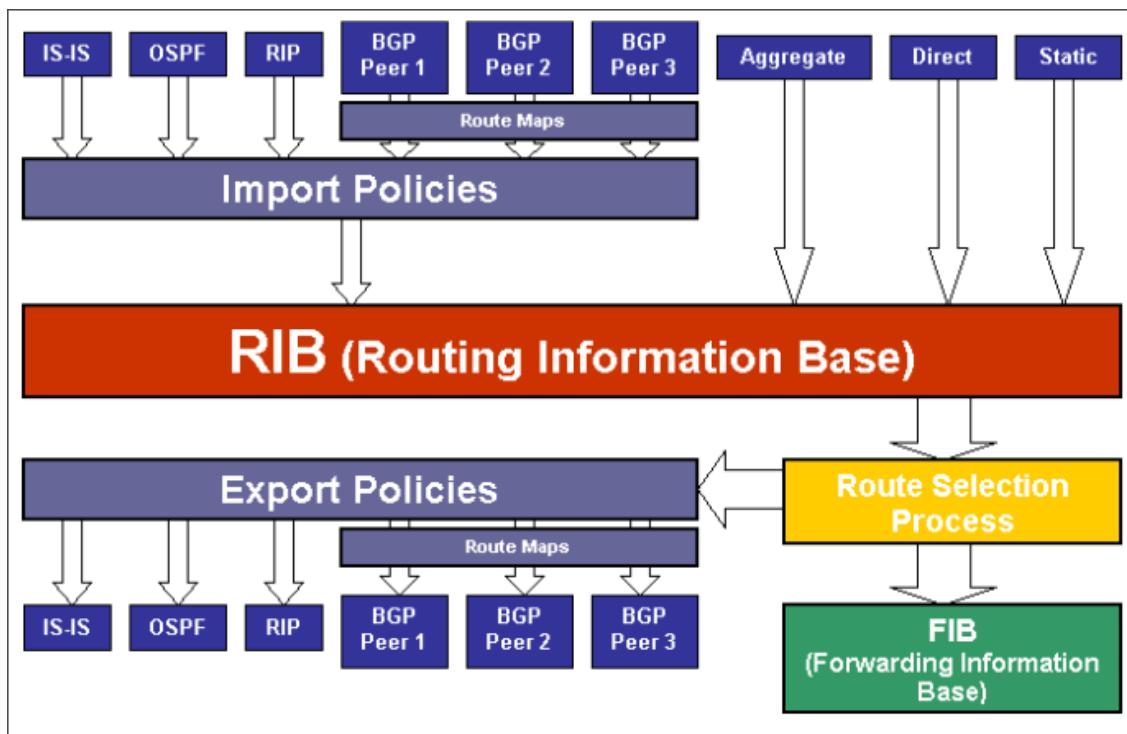
### 10.12.5 Tabelle di forwarding

Sono basate sul contenuto della tabella di routing (completa o parziale), ogni voce include anche l'interfaccia di output.

È ottimizzato per un rapido table lookup.

È anche chiamato Forward Information Base(FIB)

### 10.12.6 Routing vs forwarding table



### 10.12.7 Arrivare alla FIB

La RIB è una base dati che viene compilata con il concorso di numerosi protocolli e con diverse strategie di sintesi delle informazioni note

La FIB si ottiene a partire dalle informazioni della RIB (vengono utilizzati opportuni algoritmi)

Nel complesso queste operazioni determinano la strategia di instradamento utilizzata dai nodi della rete

# Chapter 11

## Instradamento nell'Internet globale

### 11.1 Routing gerarchico

In Internet si usa il routing gerarchico e le aree di routing sono chiamate **Autonomous System**(AS). Un AS può essere ulteriormente suddiviso in porzioni dette **Routing Area**(RA) interconnesse da un **backbone**(dorsale). Ogni network IP è tutta contenuta in un AS o in una RA (tradizionalmente secondo la classe, oggi secondo il CIDR).

Gli AS decidono autonomamente i protocolli e le politiche di routing che intendono adottare al loro interno, i vari enti di gestione si devono accordare su quali protocolli utilizzare per il dialogo tra router che interconnettono AS diversi.

I protocolli di routing all'interno di un AS sono detti **Interior Gateway Protocol** (IGP), mentre i protocolli di routing fra AS sono detti **Exterior Gateway Protocol**

## Chapter 12

# Autonomous Systems and peering

I sottoinsiemi in cui viene suddivisa logicamente la rete internet sono detti **Autonomous Systems**, il quale è un insieme di router gestiti da un'unica amministrazione, che utilizza: un solo protocollo di routing e un'unica logica per definire le metriche. ( Questa definizione era applicabile nella prima fase di sviluppo di Internet ma è diventata troppo limitata con l'evolversi della rete)

### 12.1 Internet

#### 12.1.1 rete di reti

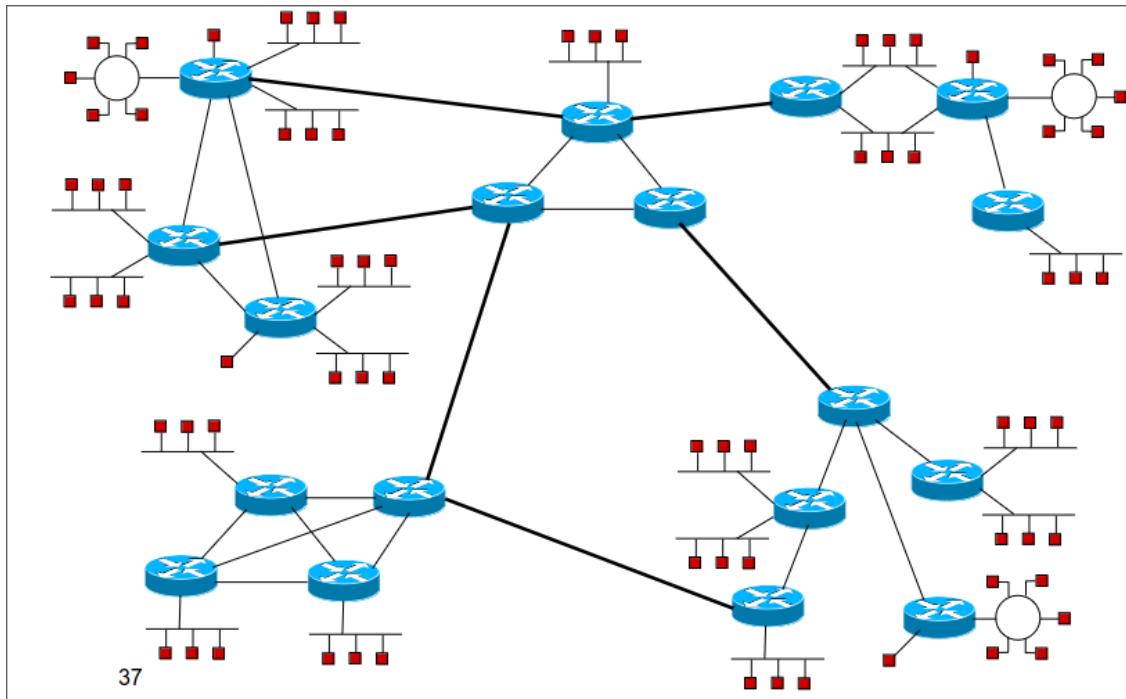


Figure 12.1: Internet = reti di reti

### 12.1.2 Sistemi Interconnessi

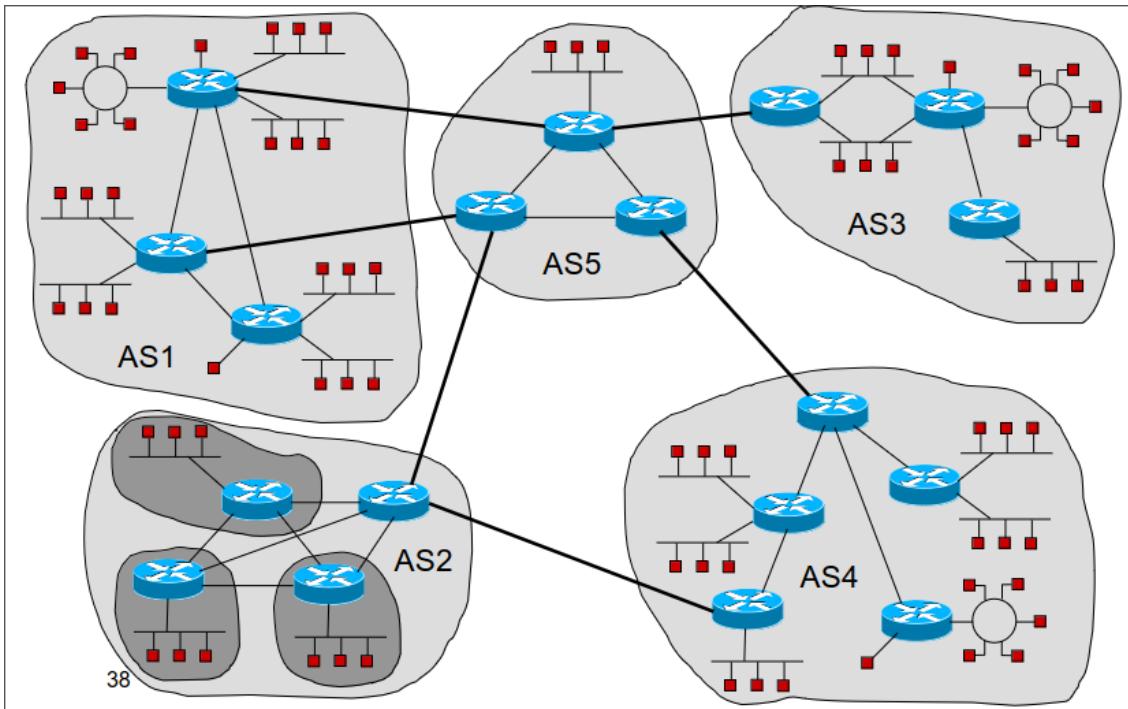
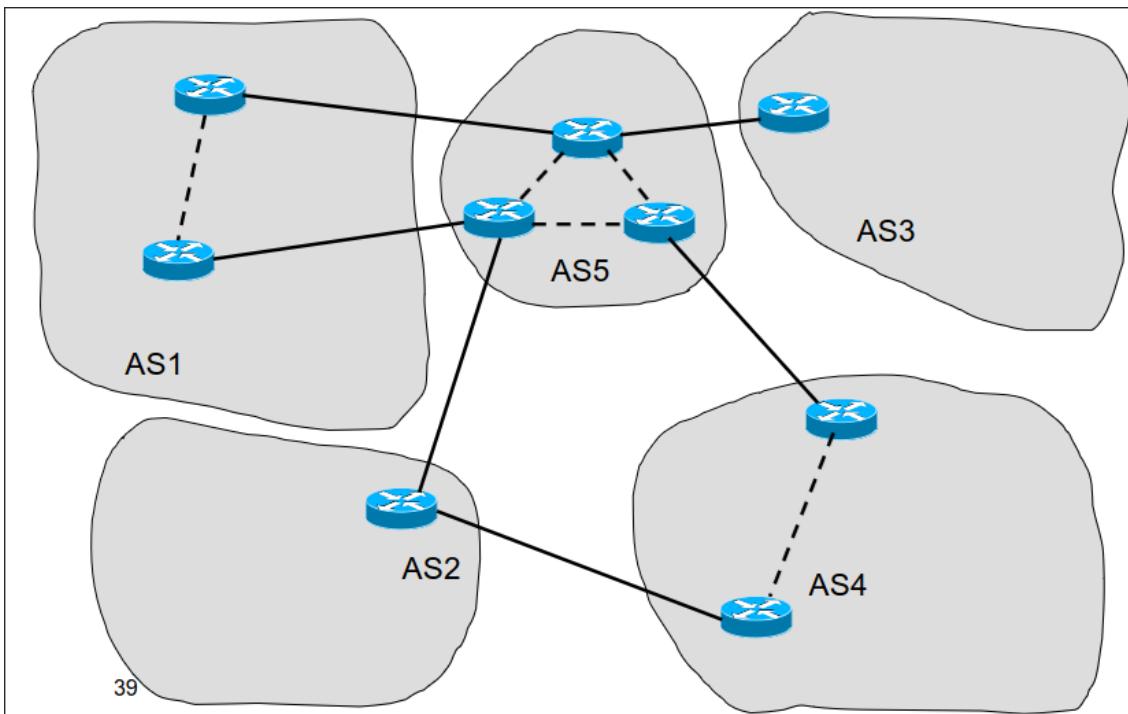


Figure 12.2: Internet = Sistemi Interconnessi

### 12.1.3 Grafo semplificate



## 12.2 Routing a livello globale

### 12.2.1 Routing gerarchico

Il Routing gerarchico consiste nell'identificazione di sottosistemi di rete autonomi per quanto riguarda l'instradamento, e di punti di contatto fra i sottoinsiemi

### 12.2.2 Tipi di grafo

Ci possono essere due tipi di grafo:

- Topologia dei sottoinsiemi della rete: Grafi di dettaglio
- Topologie dei sottoinsiemi interconnessi : Grafo semplificato, dove i sottoinsiemi sono nodi e i collegamenti fra sottoinsiemi sono archi

A ciascun livello non si ha conoscenza dell'altro

## 12.3 Protocolli di routing

Un AS deve implementare il routing al suo interno, lo fa utilizzando uno o più protocolli di routing detti Interior Gateway Protocol (RIP: Routing Information Protocol, OSPF: Open Shortest Path First)  
Deve anche comunicare con altri AS per implementare il routing fra AS, per farlo utilizza un protocollo di routing pensato appositamente detto Exterior Gateway Protocol (EGP: Exterior Gateway Protocol, BGP: Border Gateway Protocol)

### 12.3.1 RFC 1930

L'evoluzione di Internet e l'introduzione del CIDR richiedono una definizione più estensiva dell'AS.  
Un AS oggi è un insieme di prefissi di rete IP (network IP definite secondo la logica CIDR), gestito in modo unitario e con una ben definita politica di routing (Questo significa che chi gestisce l'AS ha definito in modo chiaro al suo interno come raggiungere le network IP)  
Quindi l'AS può avere uno o più enti gestori e utilizzare una o più tecnologie, ma deve avere un'unica logica che garantisca la connettività con il resto del mondo.

### 12.3.2 Esempio

- Università di Bologna -> 137.204.0.0/16
- Politecnico di Torino -> 130.192.0.0/16
- Entrambi
  - sono connessi al GARR, la rete italiana degli enti di ricerca
  - comunicano con il resto del mondo tramite il GARR
- Non c'è bisogno di avere un AS per ogni ateneo e infatti il GARR (e tutte le reti connesse ad esso) costituiscono un unico AS (AS137)

## 12.4 Internet Routing Register

Il database contenente le politiche di routing degli AS è il RAdB

## 12.4.1 AS 137

The screenshot shows the RADb website interface. At the top, there is a logo for 'RADb THE INTERNET ROUTING REGISTRY'. To the right of the logo are search fields labeled 'Query the RADb:' with a placeholder 'AS137', a 'Query' button, and links for 'Advanced Query' and 'Query Help'. Below the header, there are navigation links: 'Register Now', 'Features', 'Support', 'FAQ', 'Contact Us', and 'Log In'. A red button labeled 'Advanced Query' is prominently displayed. The main content area has a blue background with a grid pattern. It contains a 'Query the RADb:' input field with 'AS137', a 'Query' button, and links for 'Advanced Options' and 'Query Help'. The bottom half of the page displays a list of configuration parameters for AS 137:

```
aut-num: AS137
as-name: ASGARR
descr: Connectium GARR
org: OSG-CIRal-RIPE
import: from AS20965 action pref=300; accept ANY
import: from AS1299 action pref=100; accept ANY
mp-import: afi ipv4.multicast from AS20965 action pref=100; accept ANY
mp-import: afi ipv6.unicast from AS20965 action pref=100; accept ANY
mp-import: afi ipv6.multicast from AS20965 action pref=100; accept ANY
export: to AS20965 announce AS-GARRYGEANT
export: to AS1299 announce AS-GARR
mp-export: afi ipv4.multicast to AS20965 announce AS-GARRYGEANT;
mp-export: afi ipv6.unicast to AS20965 announce AS-GARRYGEANT;
mp-export: afi ipv6.multicast to AS20965 announce AS-GARRYGEANT;
admin-cr: DUNY-RIPE
tech-cr: DUNY-RIPE
status: LEGACY
mnt-by: RIPE-NCC-LEGACY-MNT
mnt-by: GAUH-LIR
created: 2002-08-21T13:53:42Z
last-modified: 2018-06-29T06:43:36Z
source: RIPE
remarks: *****
```

D 108

```

aut-num: AS137
as-name: ASGARR
descr: Consortium GARR
org: ORG-GIRal-RIPE
import: from AS20965 action pref=300; accept ANY
import: from AS1299 action pref=100; accept ANY
mp-import: afi ipv4.multicast from AS20965 action pref=100; accept ANY
mp-import: afi ipv6.unicast from AS20965 action pref=100; accept ANY
mp-import: afi ipv6.multicast from AS20965 action pref=100; accept ANY
export: to AS20965 announce AS-GARRTOGEANT
export: to AS1299 announce AS-GARR
mp-export: afi ipv4.multicast to AS20965 announce AS-GARRTOGEANT;
mp-export: afi ipv6.unicast to AS20965 announce AS-GARRTOGEANT;
mp-export: afi ipv6.multicast to AS20965 announce AS-GARRTOGEANT;
admin-c: DUMY-RIPE
tech-c: DUMY-RIPE
status: LEGACY
mnt-by: RIPE-NCC-LEGACY-MNT
mnt-by: GARR-LIR
created: 2002-08-21T13:03:42Z
last-modified: 2018-06-25T06:43:36Z
source: RIPE
remarks: ****
remarks: * THIS OBJECT IS MODIFIED
remarks: * Please note that all data that is generally regarded as personal
remarks: * data has been removed from this object.
remarks: * To view the original object, please query the RIPE Database at:
remarks: * http://www.ripe.net/whois
remarks: ****

```

**Regole di Import:**  
Da quali AS posso ricevere informazioni di routing  
(con scambio di path vector BGP ad esempio)

**Regole di Export:**  
A quali AS comunico informazioni di routing  
(invia path vector BGP ad esempio)

## 12.4.2 AS20965 Regole di Import

```

import: from AS137 accept AS-GARRTOGEANT
import: from AS378 accept AS-MACHBA
import: from AS559 accept AS-SWITCH and AS-CERNEXT
import: from AS680 accept AS-DFNTWINISP
import: from AS766 accept AS-REDIRIS {192.243.16.0/22, 192.171.2.0/24}
import: from AS786 accept AS-JANETEURO
import: from AS1103 accept AS-SURFNET
import: from AS1213 accept AS-HEANET
import: from AS1853 accept AS-ACONET and AS-ACOSERV and AS-ACONET-STH
import: from AS1930 accept AS-RCCN
import: from AS1955 accept AS-HBONE
import: from AS2107 accept AS-ARNES
import: from AS2108 accept AS-CARNet
remarks: AS7500 (DNS root name-server) is behind RENATER
import: from AS2200 accept AS-RENATER AS7500
import: from AS2602 accept AS-RESTENA
import: from AS2603 accept AS-NORDUNET
import: from AS2607 accept AS-SANET2
import: from AS2611 accept AS-BELNET
import: from AS2614 accept AS-ROEDUNET AS9199
import: from AS2847 accept AS-LITNET
import: from AS2852 accept AS2852 {130.129.0.0/16}
import: from AS3208 accept AS3208
import: from AS3221 accept AS3221
import: from AS3268 accept AS3268 AS198336
import: from AS5379 accept AS5379
import: from AS5408 accept AS5408:AS-TO-GEANT
import: from AS5538 accept AS-SigmaNet-Geant
import: from AS6802 accept AS-ISTF
import: from AS6879 accept AS6879
import: from AS8501 accept AS-PLNET
import: from AS8517 accept AS-ULAKNET
import: from AS12046 accept AS-RICERKANET
import: from AS12687 accept AS-URAN-GEANT
import: from AS13092 accept AS13092
import: from AS35385 accept AS35385
import: from AS35656 accept AS35656
import: from AS21274 accept AS-BASNETH
import: from AS40981 accept AS40981
import: from AS57965 accept AS57965 and AS-PALNREN
import: from AS202993 accept AS202993

```

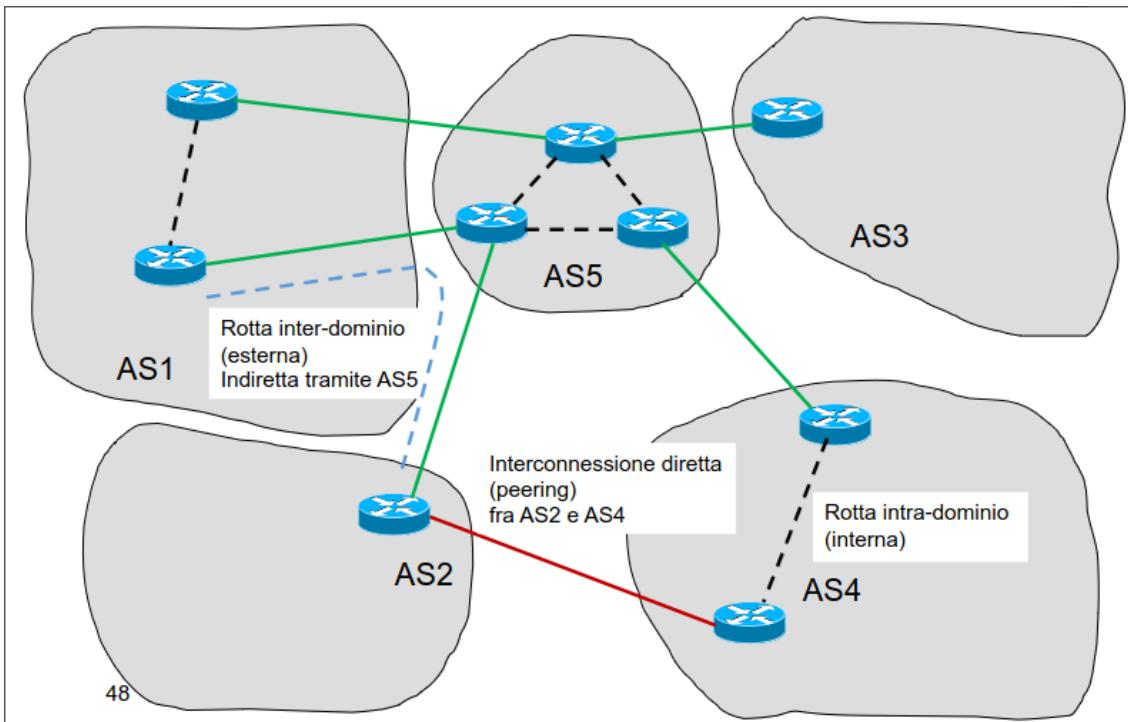
GEANT è la rete degli enti di ricerca  
Europea

Ha interconnessioni con le principali  
reti mondiali

Importa ed esporta informazioni di  
routing verso numerosi AS

1. Le network IP di GARR sono inviate  
a GEANT
2. GEANT le invia alle altre reti di  
trasporto mondiali

### 12.4.3 Interconnessione fra AS



## 12.5 Internet Service Provider

Un Internet Service Provider (ISP) è un'organizzatore che fornisce servizi per l'utilizzo di Internet. Tipicamente un ISP si registra come AS

### 12.5.1 Servizi

Alcuni dei servizi che può offrire sono:

- Connettività
- Web, mail hosting
- Registrazione e noleggio di numeri IP e nomi di dominio

### 12.5.2 ISP dal punto di vista giuridico

L'ISP dal punto di vista giuridico può essere:

- Privato con finalità di lucro
- Privato senza fini di lucro
- In forma cooperativa
- ecc...

### 12.5.3 Internet Region

Gli AS non sono necessariamente vincolate ad aree geografiche o confini nazionali.

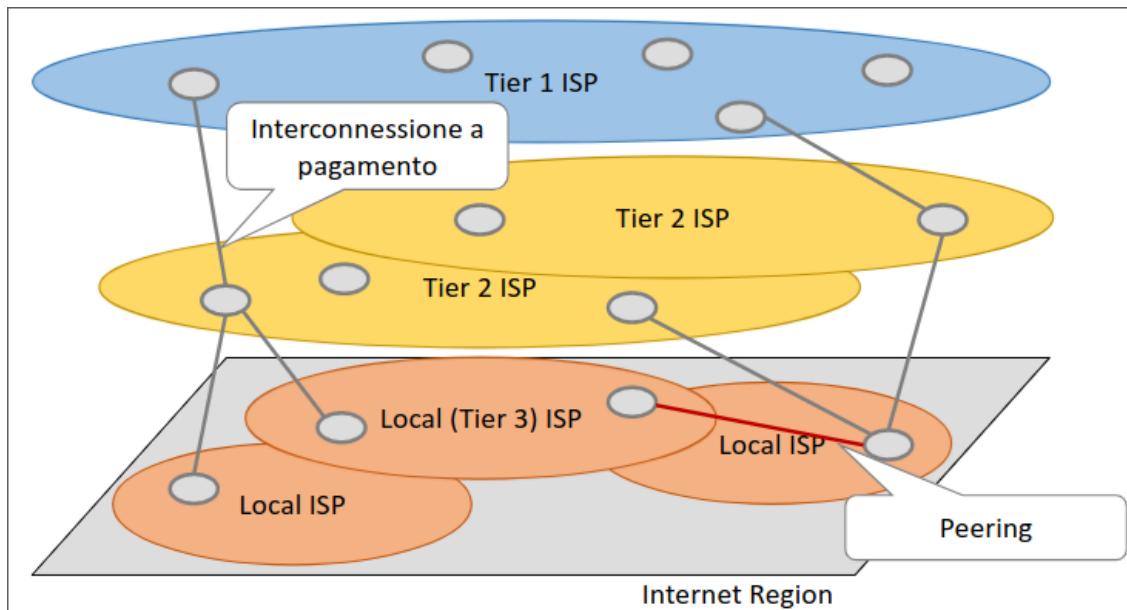
L'internet region è una porzione di Internet contenuta in una specifica area geografica (Tipicamente una nazione o un insieme di nazioni)

#### Relazione tra ISP e Internet region

Un Internet Region è solitamente servita da più ISP e uno stesso ISP può servire più Internet Region

### 12.5.4 Classificazione degli ISP

- **Tier 1 ISP** : È un IS che all'interno di una Internet Region raggiunge tutte le reti senza accedere a servizi a pagamento di altri, in breve un soggetto che possiede un'infrastruttura di rete che copre tutta la nazione (Tipicamente il gestore "incumbent"). A loro volta possono essere:
  - **Nazionali** : quando servono una sola Internet Region
  - **Globali** : quando hanno punti di accesso i paesi e continenti diversi
- Tier 2 : È un ISP che raggiunge l'internet globale acquistando servizi di interconnessione da un Tier 1 ISP, può avere interconnessioni anche con più di un ISP Tier 1 nelle stesse o in diverse Internet Region
- Tier 3 : È un TSP che serve un'area abbastanza delimitata (ISP locali o regionali), per raggiungere l'internet globale acquista servizi di interconnessione da un ISP Tier 2. Può avere interconnessioni dirette (peering) con altri ISP Tier 3 che servono la stessa zona o zone limitrofe



### 12.5.5 Peering

La relazione di peering è l'interconnessione fra due AS stabilita al fine di scambiarsi traffico (con l'operatore di contenuti: Netflix, Amazon, Aruba).

Questa relazione non ha carattere economico, quindi gli AS non devono pagarsi reciprocamente per lo scambio di traffico, e i loro intriti rimangono limitati alla tariffazione dei rispettivi utenti. Tipicamente il peering avviene tra ISP del medesimo Livello

## Pearing Policy

Ci sono due tipi di policy:

- **Ristretta** : devi chiedere di fare l pooling e la richiesta va approvata
- **Aperta** : Approvato di default

## 12.5.6 ISP locali e POP

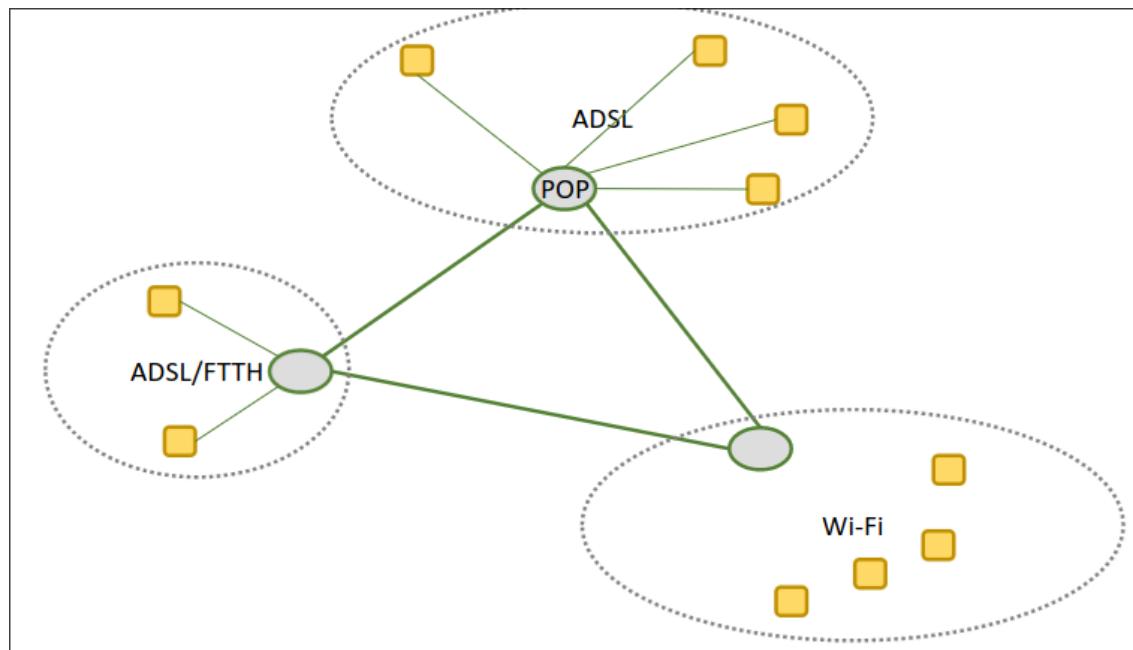
Un ISP locale fornisce il servizio a gruppi di utenti co-localizzati (singola città, area industriale, ecc...) Realizza un'infrastruttura con router e switch in un punto della zona detto **Point of Presence o POP**

**Come collega gli utenti a quella infrastruttura?**

Il collegamento può avvenire in vari modi :

- Riutilizzando il vecchio collegamento telefonico in rame (ADSL)
- Fibra ottica (FTTH)
- Collegamento radio (Wi-Fi e simili)
- Soluzioni miste (rame+fibra ad esempio nel FFTC)

## 12.5.7 Esempio di POP



## 12.5.8 Indirizzamento

Un ISP dispone di un sottoinsieme di numeri IP da utilizzare per i suoi clienti ( se sono consecutivi possono avere lo stesso prefisso quindi lo stesso Net ID, altrimenti deve gestire più Net ID).

In funzione della dimensione (numero di utenti e distanze geografiche) la rete dell'ISP può essere composta da una o più LAN

### 12.5.9 Interconnessione

Come scambiano traffico ISP che coprono la medesima zona geografica?

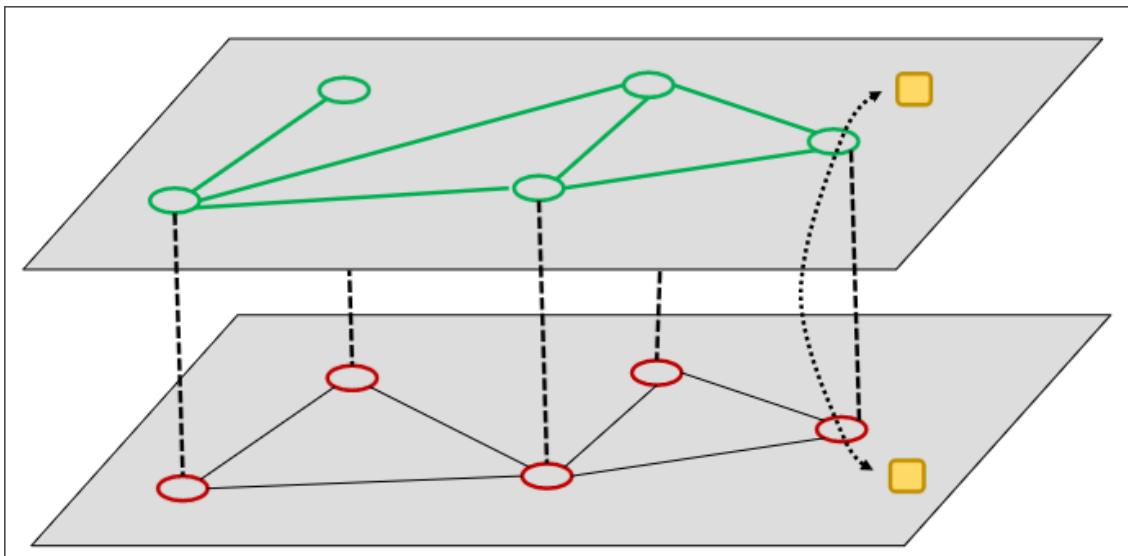
#### Interconnettere fra loro tutti i POP

Ha numerosi collegamenti, e una complessità di gestione del routing (Rotte specifiche per ogni POP in funzione dei numeri a loro connessi) e percorsi di lunghezza minima

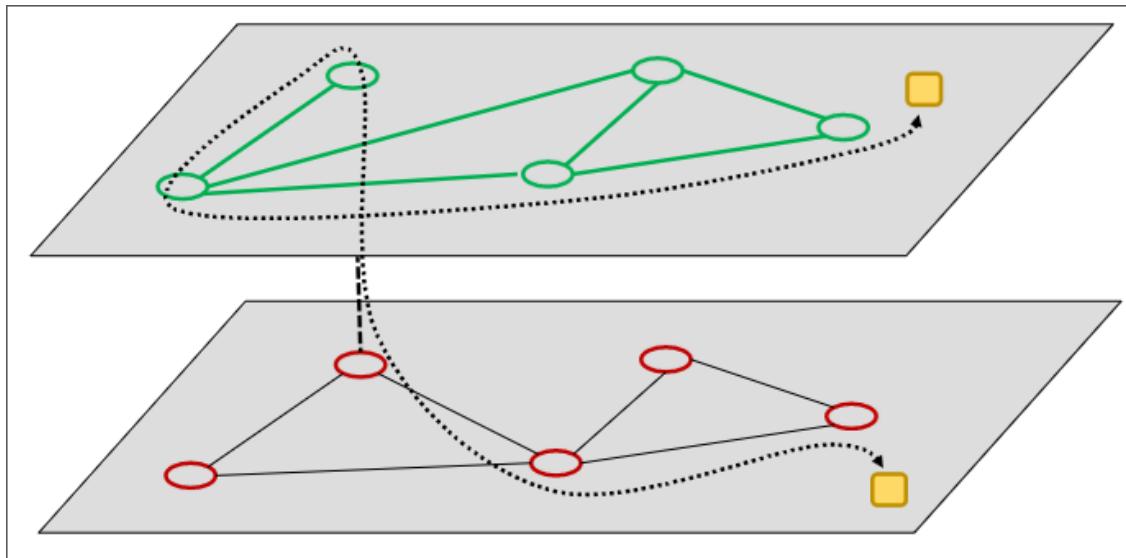
#### Interconnettere uno o pochi POP

Ha un minor numero di collegamenti, il routing è semplificato, ma ha percorsi potenzialmente più lunghi

#### Interconnessione non utilizzata



### Peering diretto tramite due POP



#### 12.5.10 Da Tier 3 a Tier 1

Teoricamente ogni ISP dovrebbe fare peering con ogni altro ISP con cui vuole scambiare traffico, e ogni AS dovrebbe essere connesso con ogni altro AS (gran numero di collegamenti dedicati fra POP)

Alcuni ISP svolgono la funzione di AS di transito per interconnettere con una topologia "a stella" gli ISP (Gli ISP specializzati nel fornire servizi di transito sono anche detti Network Service provider (NSP))  
Talvolta gli NSP coincidono con ISP Tier 1.

## 12.6 Internet Exchange

Per favorire l'interconnessione fra ISP e NSP (ossia fra i loro AS) esistono gli IXP.

Gli Internet Exchange Point (IX o IXP) sono delle infrastrutture attraverso le quali gli ISP possono stabilire relazioni di peering.

L'IXP è costruito per permettere l'interconnessione diretta degli AS senza utilizzare reti di terze parti.  
Inoltre fornisce soluzioni di connettività con specifiche garanzie di qualità (disponibilità elevata, sicurezza fisica, banda garantita ecc.)

## 12.7 In Italia

IL principale ISP Tier 1 è Telecom Italia Sparkle.

```
aut-num: AS6762
as-name: SEABONE-NET
descr: TELECOM ITALIA SPARKLE S.p.A.
remarks: International Internet Backbone
```

Figure 12.3: Da RadB

#### 12.7.1 IXP in Italia

- MIX (Milan Internet eXchange) : a Milano, Palermo, Catania
- NaMeX (Nautilus Mediterranean eXchange point) : a Roma
- TOP-IX (Torino Piemonte Internet Exchange) : a Torino
- Tuscany Internet eXchange : a Firenze
- PCIX : a Piacenza

# Chapter 13

## Interior Gateway Protocol (IGP)

### 13.1 Routing Information Protocol (RIP)

È un protocollo distance vector, di vecchia implementazione, discende dal protocollo di routing realizzato per la rete XNS di Xerox.

Ne esiste una **versione 2** più recente.

#### 13.1.1 Dove si utilizza

Era molto diffuso in passato perché il codice, mentre oggi si utilizza in reti TCP/IP

#### 13.1.2 Tipi di messaggi

Utilizza due tipi di messaggi:

- **REQUEST** : serve per chiedere esplicitamente informazioni ai nodi vicini (Es. all'invio del nodo)
- **RESPONSE** : serve in generale per inviare informazioni di routing (cioè i distance vector)

#### 13.1.3 Da chi sono trasportati?

I messaggi RIP sono trasportati da UDP ed usano la porta 520 sia in trasmissione che in ricezione

#### 13.1.4 RESPONSE

Un **RESPONSE** con nuove informazioni di routing viene inviato:

- periodicamente
- come risposta ad una richiesta esplicita
- quando una informazione di routing cambia

Le informazioni periodiche sono inviate ogni 30 secondi, con uno scarto da 1 a 5 secondi, per evitare "tempeste" di aggiornamenti.

Il response contiene il distance vector de router che lo può inviare a destinazione o a distanza (hop count)

#### 13.1.5 Formato dei pacchetti

La struttura del pacchetto è basata su parole di 32 bit, e può avere lunghezza variabile fino a 512 byte

### 13.1.6 Significato dei campi

I bit del pacchetto sono molto ridondanti rispetto alla quantità di informazioni da inviare (molti campi fissi con i bit tutti a zero). Inizialmente pensati per adattarsi ad altri protocolli.

- **command** : distingue tra REQUEST (1) e RESPONSE (2)
- **version** : versione del RIP
- **address family identifier** : indica il tipo di indirizzo di rete utilizzato, vale 2 per IP
- **address** : identifica la destinazione per la quale viene data la distanza
- **metrica** : è la distanza della destinazione indicata

### 13.1.7 La tabella di routing

Ogni riga nella tabella contiene:

- **L'indirizzo destinazione** : è un indirizzo IP a 32 bit
- **distanza della destinazione(metrica)** :
  - in termini di hop-count, ogni link ha peso = 1;
  - mentre la distanza massima( $\infty$ ) per RIP è pari a 16, al fine di limitare il conteggio all'infinito, adatto per reti relativamente piccole
- **next-hop** : sul percorso verso la destinazione (il router vicino a cui inviare i datagrammi per la destinazione)
- due contatori
  - **Timeout** : se una route non aggiornata dopo T0 secondi, la sua distanza è posta all'infinito (si ipotizza una perdita di connettività)
  - **Garbage Collector timer** : dopo ulteriori GC secondi la route viene eliminata del tutto dalla tabella
  - I valori sono TO=180 e GC = 120 (secondi)

### 13.1.8 Aggiornamento tabella di routing

A riceve un RESPONSE da B, a questo punto :

- Si controlla la correttezza dei dati (indirizzi IP e metriche validi)
- Si considerano solo le voci **i** con distanze  $d_i < \infty$
- Si calcola  $d_i = d_i + 1$

Se esiste già una entry per la destinazione **i**, se  $d_i$  è minore di quella presente in tablela, la entri viene aggiornata con next hop=B e distanza =  $d_i$ , e si fa ripartire il time out.

Se non esiste si crea una nuova entry, con distanza= $d_i$ , next hop =B (mittente del response) e si fa partire il timeout

### 13.1.9 Problematiche

Le problematiche sono:

- Fa uso di split horizon, quindi RESPONSE di interfacce diverse possono essere diverse.
- Fa uso di triggered update, quindi non è necessario indicare nella RESPONSE tutte le entry della tabella ma solamente quelle appena modificate.
- Non supporta il CIDR
- È un protocollo insicuro: chiunque trasmetta datagrami dalla porta UDP 520 viene considerato come un router autorizzato.

#### Esempio di malfunzionamento indotto

Un router non autorizzato trasmette messaggi contenenti l'indicazione di una distanza 0 tra se stesso e tutti gli altri della rete, dopo qualche tempo tutti i percorsi ottimi convergono su questo router

#### La mancanza del CIDR

### 13.1.10 RIP versione 2

I miglioramenti introdotti riguardano soprattutto, il subnetting e CIDR e l'autenticazione.

#### Novità

- compatibilità verso il basso: RIP-1 ignora le entry con i campi riservati diversi da zero.
- Possibilità di indicare sottoreti o indirizzamenti CIDR, tramite il campo **subnet mask**
- Possibilità di autenticare chi invia i messaggi
- Possibilità di indicare il proprio AS e di scambiare informazioni con i protocolli EGP (tramite i campi **route tag** e **route domain**)
- Possibilità di specificare un **next-hop** più appropriato

#### Problematiche

Rimane non adatto ad AS grandi e ha problemi di convergenza.

## 13.2 Open Shortest Path First (OSPF)

È divenuto standard nella versione 2, e oggi è il più diffuso IGP.

È un protocollo di link state, si occupa dell'invio di **Link State Advertisement**(LSA) a tutti gli altri router.

È encapsulato direttamente nell' IP, il valore del campo protocol dell'intestazione IP (89 per OSPF) serve a distinguere questi pacchetti da altri.

### 13.2.1 Per cosa è stato progettato

È stato progettato specificatamente per:

- Semplificare il routing in reti grandi, tramite la suddivisione in aree
- gestire intrinsecamente reti punto-punto e punto-multipli
- separare logicamente gli host dai router

### 13.2.2 Aree di Routing

Un AS può essere suddiviso in porzioni dette **Routing Area** (RA) interconnesse da un **backbone** (Area 0). Ciascuna area risulta separata dalle altre per quanto riguarda lo scambio delle informazioni di routing e si comporta come un'entità indipendente (3° livello gerarchico di routing)

Per interconnettere le aree vi devono essere router connessi a più aree e/o al backbone (almeno un router per area)

#### Classificazione dei router secondo OSPF

- **Internal Router** : router a ciascuna area
- **Area Border Router** : router che scambiano informazioni con altre aree
- **Backbone Router** : router che si interfacciano con il backbone
- **AS Boundary Router** : router che scambiano informazioni con altri AS usando un protocollo EGP

#### Esempio

### 13.2.3 Tipi di route

- **Route intra-area** : aggiornamento delle informazioni di routing pertinenti all'area
- **Router inter-area** : aggiornamento delle informazioni di routing pertinenti ad aree diverse da quella considerata
- **Router esterni** : Aggiornamenti delle informazioni di route provenienti da altri protocolli al di fuori del dominio OSPF, sono inoltrati nel dominio OSPF dal ASBR

### 13.2.4 Tipi di aree

- **Area normale** : accetta tutti i tipi di route;
- **Stub area** : accetta route intra e inter area, Tutti i router della stub area usano un "default route" verso destinazioni al di fuori dell'AS (Comunicato dall'Area Border Router (ABR))  
I requisiti di memoria dei router sono ridotti
- **Totally stub area** : Vengono propagati solamente route intra-area ed il route di default, il default route viene propagato dal ABR, e tutti i router dell'area usano il default route per destinazioni esterne all'area
- **Not so stubby area** : Stub area che importa alcuni route esterni, uno dei router dell'area è connesso a un AS diverso e diventa un ASBR

### 13.2.5 Ulteriori caratteristiche

**Bilanciamento del carico** se il router ha più percorsi di uguale lunghezza verso una certa destinazione, il carico viene ripartito equamente su di essi

L'**Autenticazione** serve per garantire maggiore sicurezza nello scambio delle informazioni di routing è prevista l'autenticazione con password ed uso di crittografia

Il routing **dipende dal grado di servizio**, quindi i router scelgono il percorso sul quale instradare un pacchetto sulla base dell'indirizzo e del campo Type of Service dell'instradamento IP, tenendo conto che percorsi diversi possono offrire diversi gradi di servizio.

### 13.2.6 Rappresentazione di host e router

### 13.2.7 Tipologie di rete

OSPF è progettato per operare correttamente con reti:

- **Punto-punto**
- **Broadcast Multi-Acces**
- **Non-Broadcast Multi-Acces**

In una rete ad accesso multiplo tutti gli N router connessi alla rete sono di fatto connessi con tutti gli altri.

- Il numero di archi bidirezionali da inserire nel grafo è  $N(N - 1)/2 + N$  (sono inclusi gli archi per collegare i router alle network)
- Il numero totale di LSA da trasmettere è  $N(N - 1)$
- conviene adottare una **topologia a stella equivalente**, inserendo un nodo virtuale che rappresenta la rete, solo N archi bidirezionali

### 13.2.8 Rappresentazione di reti multi-accesso

### 13.2.9 Vicinanza e adiacenza tra router

Due router si dicono **Vici** se sono connessi alla medesima rete e possono comunicare direttamente(punto-punto, punto-multiplo)

Mentre si dicono **Adiacenti** se si scambiano informazioni di routing.

In una rete ad accesso multiplo risulta molto più efficiente eleggere un **Designated Router**(DR) fra gli N vicini:

- ogni router della LAN è adiacente solo al DR
- lo scambio di informazioni di routing avviene solo tra router adiacenti (cioè il DR fa da tramite)
- Il DR è l'unico a comunicare la raggiungibilità di router e host della LAN al mondo esterno.
- Per ragioni di affidabilità occorre anche un **Backup Designated Router** (BDR) adiacente a tutti i router locali

### 13.2.10 Identificazione di router e priorità

Ogni router di un AS utilizzante OSPF deve avere un identificativo univoco(**router ID**), il quale :

- di default si prende l'indirizzo IP più alto fra quelli assegnati alle interfacce del router
- si può assegnare manualmente ad ogni router configurando opportunamente l'interfaccia di loop-back
- configurare l'interfaccia di loop-back è un modo più stabile e sicuro di assegnare il router ID perché questa interfaccia non viene mai disabilitata

Ai singoli router di un'area possono essere associate delle priorità, che sono utilizzate nell'elezione del DR, hanno un valore compreso tra 0 e 255 (8 bit).

Di default i router hanno priorità 0(più bassa)

### 13.2.11 Elezione di DR e BDR

Ciascun router nella rete ad accesso multiplo:

- esamina la lista dei suoi vicini.
- elimina dalla lista tutti i router non eleggibili (esempio tutti quelli con priorità nulla)
- fra quelli rimasti seleziona il router avente la priorità maggiore(in caso di parità si sceglie il router ID più alto)
- elegge il router selezionato a DR
- ripete il procedimento per eleggere il BDR(il router DR non è più eleggibile)
- termina la procedura una volta eletti DR e BDR

### 13.2.12 Link State Database

Il grafo della rete sul quale ciascun router calcola lo **shortest path tree** è rappresentato dal **Link State Database** presente in ogni router.

### 13.2.13 I protocolli

L'OSPF invia i messaggi utilizzando direttamente il protocollo IP (campo protocol = 89), il quale si compone in 3 sottoprotocolli : **hollo, exchange, flooding**

Tutti i messaggi hanno una intestazione comune, vengono aggiunte informazioni per il particolare scopo a cui il messaggio è destinato (tipo di pacchetto)

#### Intestazione comune

- **Version** : indica la versione di OSPF
- **Type** : indica il tipo di pacchetto
- **Packet Length** : numero di byte del pacchetto
- **Router ID** : indirizzo IP che identifica il router mittente
- **Area ID** : identifica l'area di appartenenza (il numero 0.0.0.0) è l'area di backbone
- **Checksum** : calcola su tutto il pacchetto OSPF escludendo gli 8 byte del campo authentication (si utilizza l'algoritmo classico di IP)
- **AuType** : indica il tipo di autenticazione:
  - 0 : nessuna autenticazione
  - 1 : autenticazione semplice (password nel campo **authentication**)
  - 2 : autenticazione crittografata (dati nel campo **authentication**)

### 13.2.14 Type

- Type 1 : Hello (Hello protocol, neighbour discovery)
- Type 2 : Database description (exchange protocol)
- Type 3 : Link state request
- Type 4 : Link state update
- Type 5 : Link state acknowledge

### 13.2.15 Hello protocol

Unico tipo di pacchetto: **Hello** (Type=1).

È utilizzato per controllare l'operatività dei link, per scoprire e mantenere relazioni fra vicini e per eleggere DR e BDR I pacchetti HELLO sono inviati sulle interfacce periodicamente secondo quanto specificato dal parametro **HelloInterval** (così si riescono a coprire i propri vicini)

Includono una lista di tutti i nodi vicini (**Neighbor**) dai quali è stato ricevuto un pacchetto HELLO recente (cioè non più vecchio di **RouterDeadInterval**), si riesce così a conoscere se per ciascun vicino è presente un collegamento bidirezionale e se esso è ancora attivo.

I campi **Router Priority**, **Designated Router** e **Backup Designated Router** sono utilizzati per l'elezione di DR e BDR.

**Netwok Mask** indica la maschera relativa all'interfaccia del router (l'indirizzo è nell'header IP)

**Options** indica se si supportano funzionalità opzionali.

### 13.2.16 Exchange protocol

Una volta stabilite le adiacenze, i routeradiacenti devono sincronizzare i rispettivi LInkk State Database.

La procedura di sincronizzazione è asimmetrica:

- Si stabilisce chi è il master e chi lo salve
- Il master invia una serie di pacchetti **Database Desription**(Ty)

## Chapter 14

# Come fa un pacchetto ad arrivare a destinazione

O è un messaggio in broadcast oppure ha l'indirizzo IP destinazione.  
Ma al tempo 0 come fanno ad arrivare a destinazione?

## Chapter 15

# Esercitazione Router

```
#router
#router enable
#router show router-config mostra comandi principali.
#router configure terminal
#router(config) interface nome_interfaccia
#router(config-if)
#router_H1(config-if) no ip address : Toglie il numero IP dalla configurazione delle Vlan
#router(config) no router rip : spegne il router
#router(config) interface vlan1
#router_H1(config-if)
#router_H1(config-if) ip address ip_num : assegna il numero ip num_ip alla vlan1(in questo caso)
#router write : salvare le modifiche
#router(config) router rip
#router(config-router) version 2 : Spiegherà successivamente
#router_R2(config-router) network 192.168.3.0 : network da raggiungere
#router_R2(config-router) network 192.168.0.0 : è raggiungibile da
```