Università di Roma Tor Vergata
Corso di Laurea triennale in Informatica

# Sistemi operativi e reti

A.A. 2016-17

Pietro Frasca

## Parte II: Reti di calcolatori

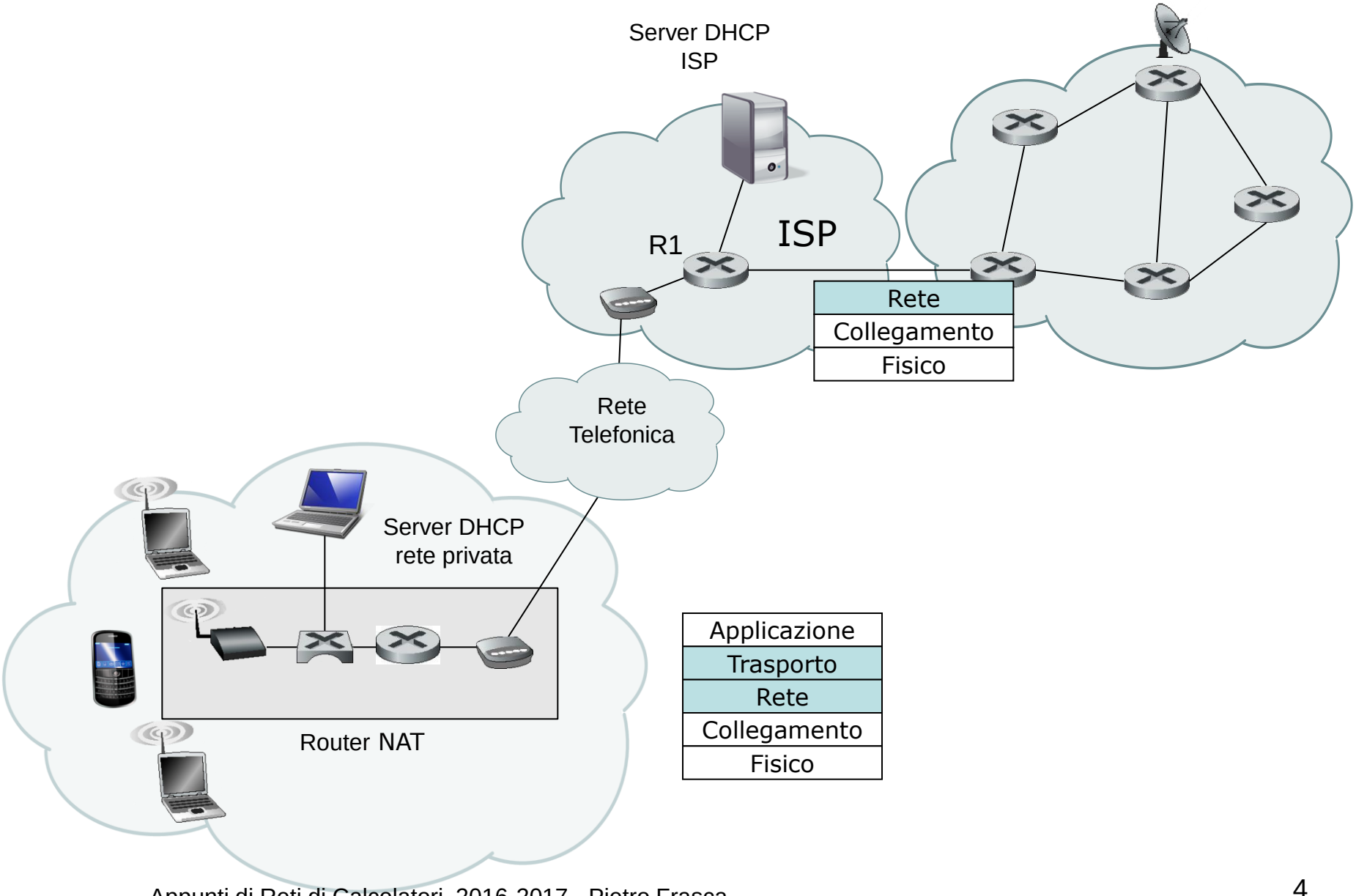
## Lezione 17 (41)

Martedì 9-05-2017

# Traduzione degli indirizzi di rete

- Il crescente aumento del numero di reti ad accesso residenziale ha causato il quasi esaurimento degli indirizzi IP gestiti dagli ISP.
- Una soluzione all'insufficienza di numeri IP, che si è diffusa in questi anni è la tecnologia **NAT (*network address tra**slation,* traduzione degli indirizzi di rete *),*** [RFC 2663 e 3022] implementata in dispositivi, spesso chiamati router NAT.
- Un router NAT è un dispositivo usato per connettere una piccola rete privata con la rete di un ISP.
- I numeri IP privati, utilizzati in queste reti appartengono ai blocchi 10.0.0.0/8 o 172.16.0.0/12 oppure 192.168.0.0/16.
- I router NAT non funzionano come i router ordinari, ma sono visti dalla rete Internet come un **dispositivo** con un ***unico*** **indirizzo IP.**

- Il router NAT ottiene l'indirizzo IP pubblico dal server DHCP dell'ISP. Inoltre, sul router NAT è implementato il lato server DHCP per assegnare gli indirizzi privati agli host della rete privata.
- La figura mostra il funzionamento di un router NAT.
- In questo esempio, le interfacce della rete privata hanno indirizzi IP appartenenti al blocco 192.168.1.0/24.
- Nell'esempio seguente, tutti i pacchetti inviati dal router NAT verso Internet hanno l'indirizzo IP origine 151.27.85.10, e tutti i pacchetti in ingresso al router hanno lo stesso indirizzo come destinazione.
- In pratica, il router NAT nasconde la rete privata al mondo esterno; gli indirizzi IP privati non sono visti al di fuori della rete privata.

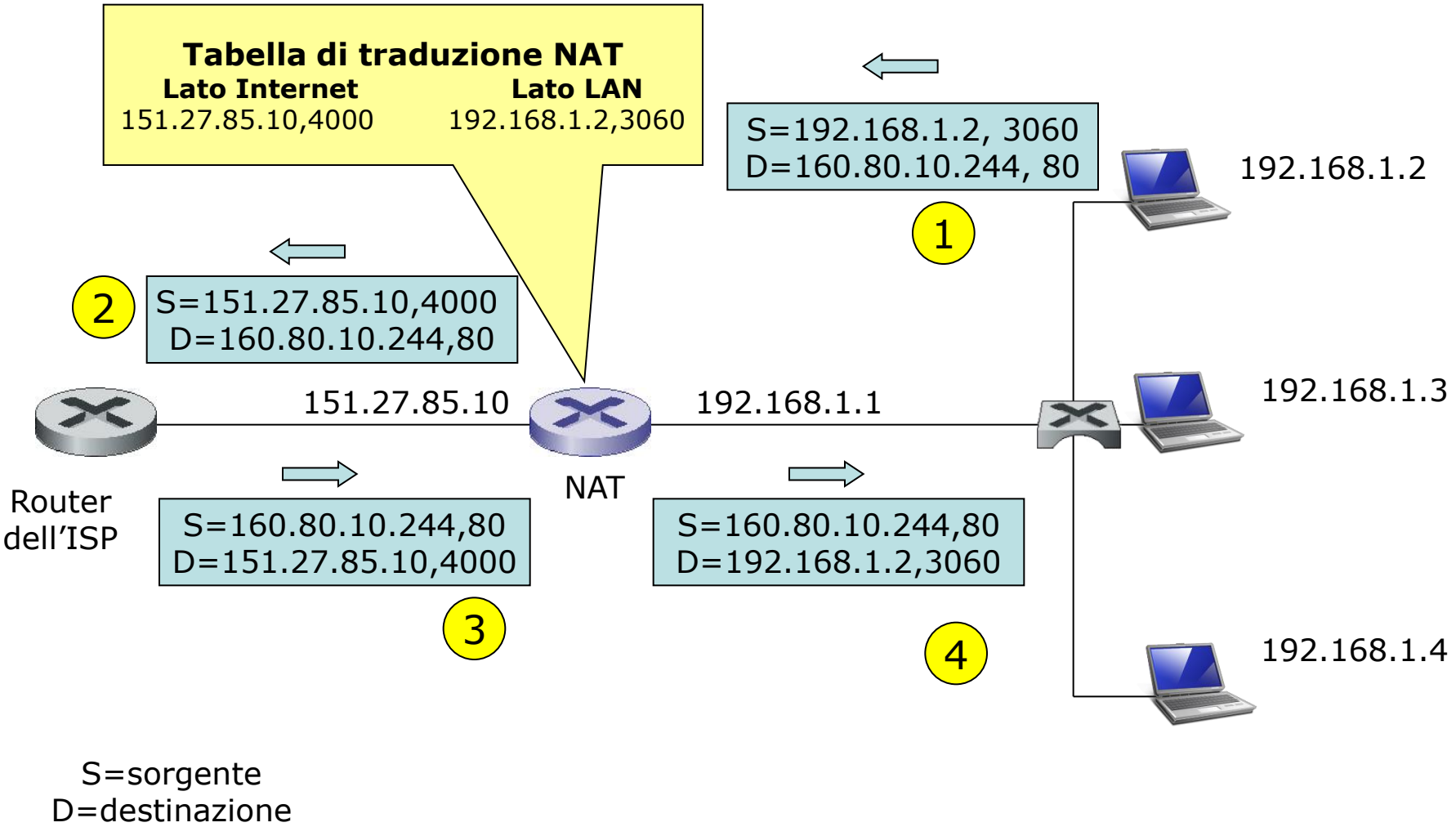

Server DHCP
ISP
R1
ISP
Rete
Collegamento
Fisico
Rete
Telefonica
Server DHCP
rete privata
Router NAT
Applicazione
Trasporto
Rete
Collegamento
Fisico

- Dato che tutti i pacchetti in arrivo al router NAT dalla rete Internet hanno lo stesso indirizzo IP di destinazione descriviamo in che modo il router riesce a inviare i datagram ai diversi host della rete privata.
- La soluzione consiste nell'utilizzare una tabella di traduzione nel router NAT e utilizzare nelle righe di tale tabella i numeri di porta e gli indirizzi IP.

| IP Internet | Porta Internet | IP LAN | Porta LAN |
|---|---|---|---|
| 151.27.85.10 | 4000 | 192.168.1.2 | 3060 |
| 151.27.85.10 | 4001 | 192.168.1.3 | 2050 |
| 151.27.85.10 | 5000 | 192.168.1.3 | 6700 |

- Facciamo riferimento alla figura seguente e supponiamo che l'host 192.168.1.2 si connetta a un server web (porta 80) con indirizzo IP 160.80.10.244. Il TCP nell'host 192.168.1.2 assegna automaticamente il numero di porta sorgente, ad esempio 3060. Quando il router NAT riceve il datagram, estrae dall'intestazione IP il numero IP dell'host mittente e dall'intestazione TCP il numero di porta mittente.

- Esempio di traduzione degli indirizzi di rete




S=sorgente
D=destinazione

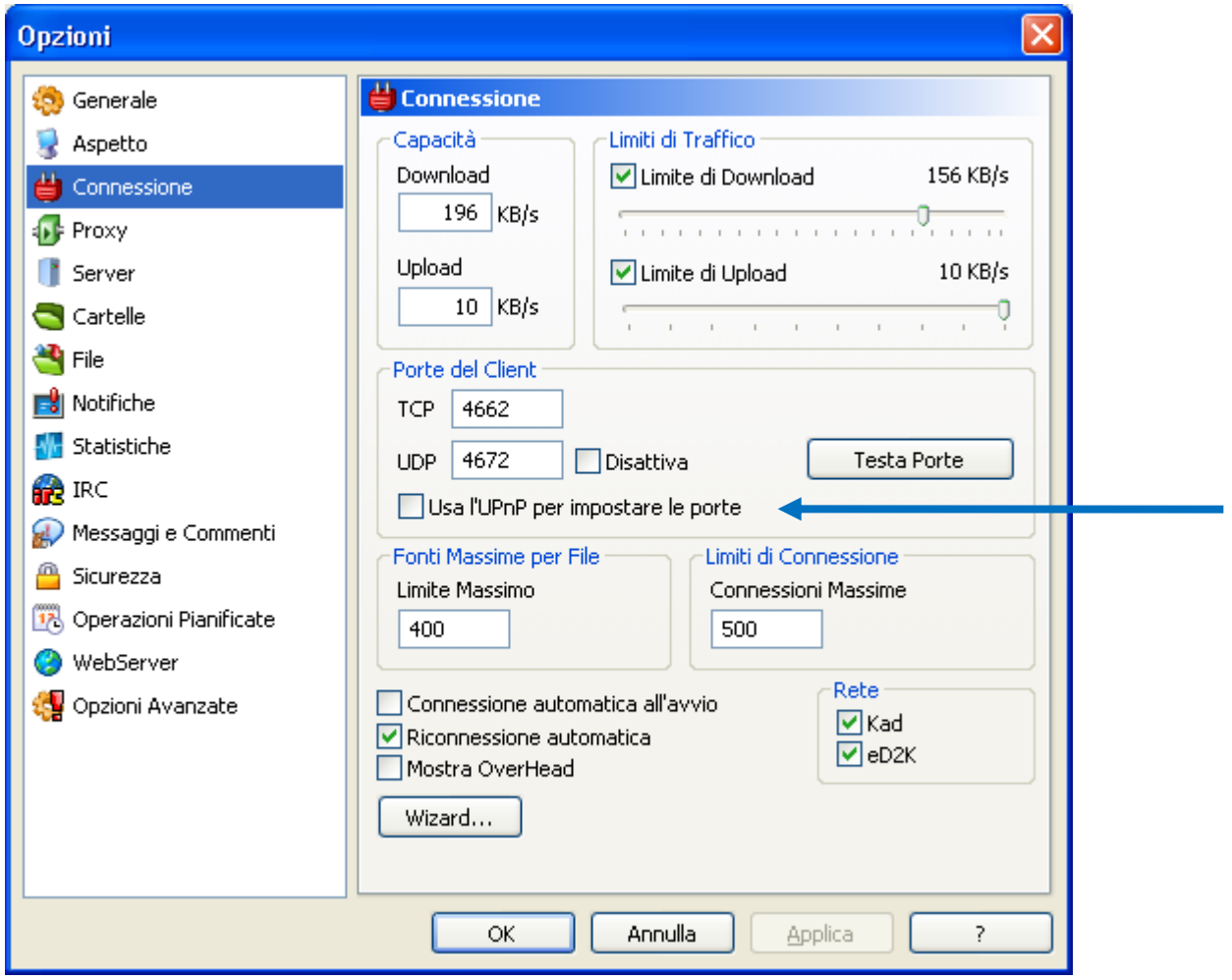
- Scandisce la tabella per verificare se esiste già una riga con questi valori; se non esiste, inserisce una nuova riga avente il valore del campo *IP internet* l'indirizzo IP del dispositivo NAT (151.27.85.10); genera per il datagram un nuovo numero di porta origine, ad esempio 4000, che non sia già presente nelle righe della tabella; negli altri due campi inserisce il numero IP privato dell'host (192.168.1.2) e il numero di porta locale (3060) usato dal processo nell'host.
- Prima di rinviare il datagram verso Internet, sostituisce l'indirizzo IP origine (192.168.1.2) con il proprio indirizzo IP sul lato Internet 151.27.85.10 e sostituisce il numero di porta origine 3060 con il nuovo numero 4000. Il resto del datagram resta invariato.
- Il server web risponde con un datagram con l'indirizzo IP del router NAT come destinazione e il cui numero di porta destinazione è 4000. Quando questo datagram arriva al router NAT, quest'ultimo scandisce la tabella di traduzione NAT usando il numero di porta destinazione per ottenere l'appropriato l'indirizzo IP (192.168.1.2) e il numero di porta destinazione (3060) del browser nella rete privata. Il router, quindi, riscrive l'indirizzo di destinazione del datagram e il suo numero di porta di destinazione, e inoltra il datagram nella rete LAN.

- Notiamo che, essendo il campo numero di porta di 16 bit, il NAT può supportare fino a  65.536 **connessioni** simultanee con un solo indirizzo IP sul lato Internet relativo al router.
- Nonostante la grande diffusione che ha avuto in quest'ultimi anni, la tecnologia NAT ha avuto molte critiche dai membri della comunità IET, che sostengono invece la diffusione del IPv6 per risolvere la mancanza di indirizzi IPv4, anziché ricorrere a una soluzione «tampone».

# UPnP (Universal Plug and Play)

- UPnP è un protocollo che consente ad un host di individuare e configurare un router NAT.
- UPnP consente ad un'applicazione in esecuzione su un host della rete privata di inserire nella tabella del router NAT una corrispondenza tra i propri ***(numero IP privato, numero di porta privato)*** e **(numero IP pubblico, numero di porta pubblico).** In tal modo gli host esterni possono instaurare connessioni TCP o UDP verso l'host della rete privata**.** Inoltre, UPnP consente alle applicazioni di conoscere **(numero IP pubblico, numero di porta pubblico).**
- Ad esempio, supponiamo che sull'host con indirizzo privato 192.168.1.2 sia in esecuzione un'applicazione P2P (come ad esempio Emule o bitTorrent), che utilizza la porta **4662** TCP come porta di ascolto, per le richieste. Supponiamo che l'indirizzo IP pubblico del NAT sia 151.27.85.10. L'applicazione P2P, mediante UPnP chiede al router NAT di aggiungere una riga nella tabella che fa corrispondere (192.168.1.2, 4662) a (151.27.85.10,5001) dove il numero di porta pubblica 5001 viene scelta in modo che non sia già in uso nel router.

- In tal modo, un pari esterno può connettersi con il pari della NAT usando l'indirizzo 151.27.85.10 e la porta 5001.



# IPv6

- Nei primi anni '90, l'**IETF** (Internet Engineering Task Force) iniziò lo studio per la realizzazione del protocollo successore dell'IPv4.
- Il motivo principale per la realizzazione di una nuova versione di IP era che lo spazio di indirizzi IP a 32 bit stava per esaurirsi.
- Fu sviluppato un nuovo protocollo IP, l'IPv6.
- L'IPv6 fu sviluppato in base all'esperienza di utilizzo dell'IPv4, che fu modificato e migliorato in vari aspetti.
- La versione IPv5 era una proposta basata sul modello OSI ma non si è mai realizzata.

# Formato del datagram IPv6

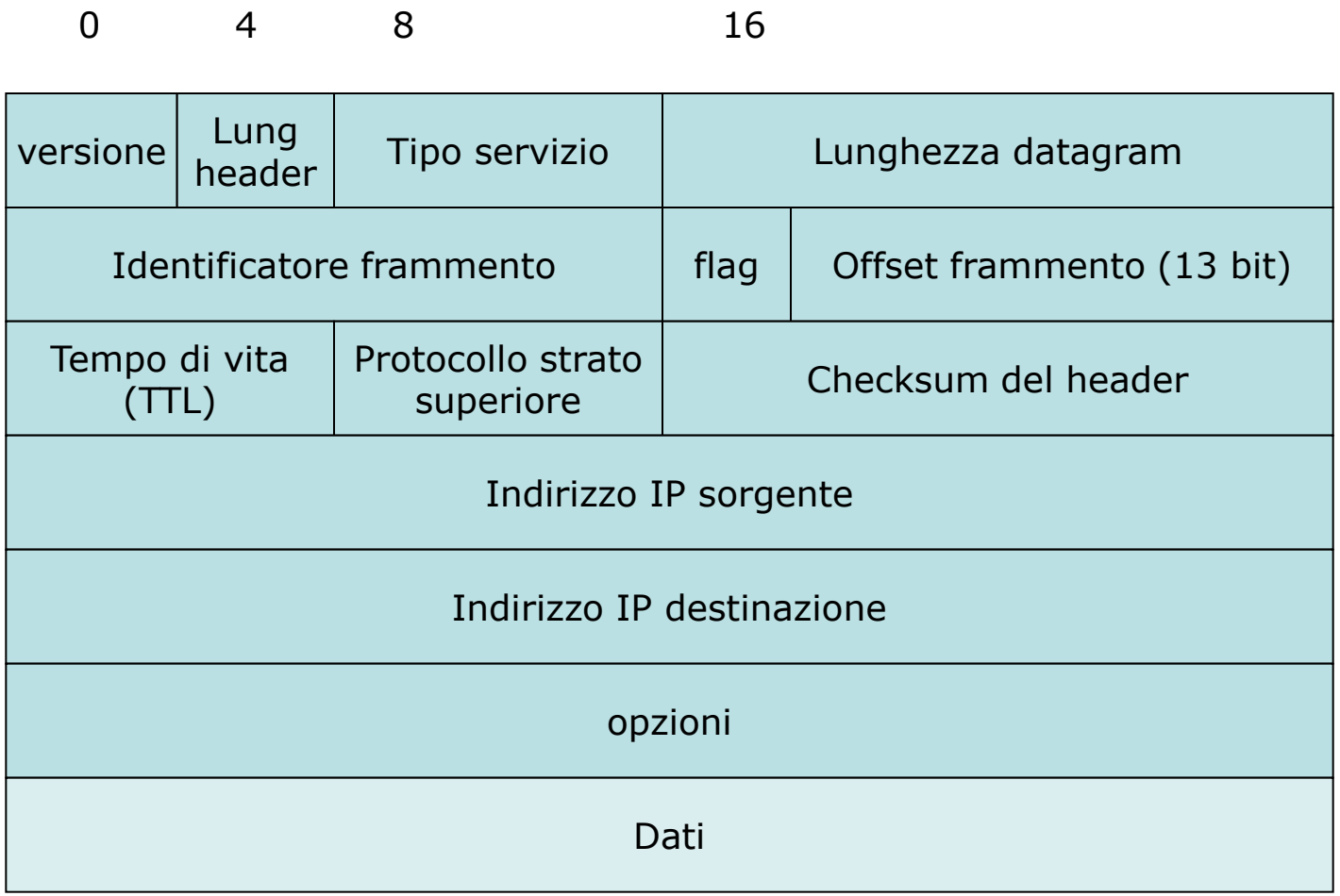
- Le più importanti modifiche introdotte da IPv6 sono:
  - ***Ampliamento dell'indirizzamento***. L'IPv6 incrementa le dimensioni dell'indirizzo IP da 32 a **128 bit**. Oltre agli indirizzi unicast e multicast, è stato introdotto un nuovo tipo di indirizzo, detto **indirizzo anycast** , che permette di inviare un datagram a un host appartenente ad un gruppo. Questa classe di indirizzi può essere usata, per esempio, per inviare una richiesta HTTP al più vicino dei server web duplicati che contengono un documento richiesto.
  - ***Intestazione di lunghezza fissa (40 byte)***. Alcuni campi dell'IPv4 sono stati eliminati portando ad una intestazione con lunghezza fissa di 40 byte che permette una più veloce elaborazione del datagram IP. Il vecchio campo opzioni, se usato, viene incluso nel campo dati.
  - ***Etichettatura e priorità di flusso***. L'IPv6 consente di differenziare la qualità di servizio in base al tipo di traffico. Ad esempio, trasmissioni di streaming audio e video (applicazioni soft real-time) potrebbero essere trattate in modo diverso da comunicazioni relative alla posta elettronica e al trasferimento di file.

L’intestazione IPv6 ha anche un campo (di otto bit) per la **classe di traffico**. Questo campo, come il campo TOS nell'IPv4, può essere usato per **dare la priorità a certi pacchetti** all'interno di un flusso, o può essere usato per dare la priorità ai datagram di certe applicazioni (per esempio, pacchetti ICMP) rispetto ai datagram di altre (per esempio, le news di rete).

- Vediamo ora brevemente tutti i campi di IPv6 e riprendiamo, per il confronto, l’intestazione IPv4.

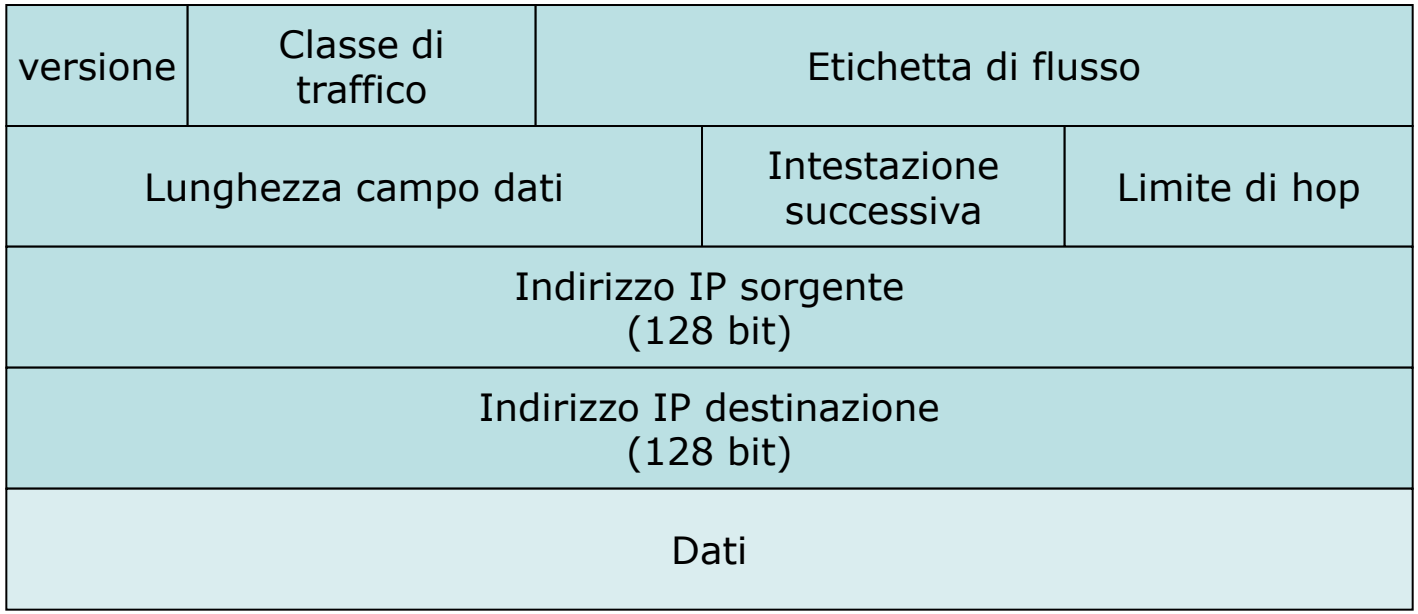
# Formato del datagram IPv4

- Il formato del datagram di **IPv4** (versione più usata di IP).



# Formato del datagram IPv6

- Il formato del datagram di **IPv6** (attuale versione di IP) è mostrato nella figura seguente.



- In IPv6 sono definiti i seguenti campi:
  - ***Versione*** *(version).* (4 bit) identifica il numero della versione IP.
  - ***Classe di traffico*** *(traffic class).* (8 bit) è analogo al campo TOS dell'IPv4.
  - ***Etichetta di flusso*** *(flow label).* (20 bit) è usato per identificare un "flusso" di datagram. Questo campo insieme al precedente, classe del traffico, dovrebbe consentire di implementare servizi per un trattamento speciale dei datagram, al fine di migliorare la gestione del traffico multimediale (audio e video) in tempo reale.
  - ***Lunghezza campo dati*** *(payload length).* (16 bit) specifica la lunghezza del campo dati.
  - **Intestazione successiva** *(next header).* Identifica il protocollo a cui il campo dati del datagram dovrà essere consegnato (per esempio, a TCP o UDP). Il campo usa gli stessi valori del **campo protocollo** nell'intestazione di **IPv4 (ad esempio 6 per il TCP e 17 per l'UDP)**.
  - ***Limite di hop*** *(hop limit).* E' analogo al **campo TTL** di IPv4. Il valore di questo campo è diminuito di uno in ogni router che rinvia il datagram. Se il suo valore raggiunge zero il datagram viene scartato.

- ***Indirizzi di sorgente e destinazione*** *(source and destination address).* I vari formati degli indirizzi IPv6 a 128 bit sono descritti nella RFC 2373.
- ***Dati*** *(data).* contiene il carico utile del datagram IPv6. Quando il datagram raggiunge la sua destinazione, il carico utile viene rimosso dal datagram IP e passato al protocollo specificato nel campo **intestazione successiva**.

- Confrontando il formato del datagram di IPv6 con quello di IPv4, possiamo notare che vari campi del datagram IPv4 in IPv6 non sono più presenti:
  - ***Frammentazione/riassemblaggio*** *(fragmentation/reassembly).* L'IPv6 non permette la frammentazione e il riassemblaggio. Se un router riceve un datagram troppo grande per essere trasmesso su un link in uscita, il router scarta il datagram e invia al mittente un messaggio **ICMP di errore "pacchetto troppo grande"**. Il mittente allora può rispedire un datagram IP di inferiore dimensione. Le operazioni di frammentazione e riassemblaggio sono state eliminate per aumentare la velocità di instradamento IP nella rete.

- ***Checksum***. E’stata eliminata la funzione del calcolo del checksum dato che i protocolli dello strato di trasporto, come ad esempio TCP e UDP eseguono il calcolo delle checksum. Inoltre protocolli di collegamento, come ad esempio Ethernet, eseguono controlli CRC ancora più potenti. Pertanto questa funzionalità nello strato di rete è stata ritenuta ridondante dai progettisti dell’IPv6. L’obiettivo principale è stato **l'elaborazione veloce dei pacchetti IP** dato che la checksum deve essere ricalcolata in ogni router per via della presenza del campo *limite di hop* (TTL nell’IPv4) il cui valore cambia in ogni router.
- ***Opzioni***. Il campo opzioni è stato eliminato dall’intestazione. Tuttavia, le opzioni possono essere inserite nel campo dati del datagram IPv6 specificando un opportuno codice nel campo "**intestazione successiva**". In tal modo le opzioni sono trasportate in modo analogo al TCP o all’UDP.

# Indirizzamento IPv6

- La ragione principale per la migrazione da IPv4 a IPv6 è dovuta alla piccola dimensione dello spazio di indirizzamento in IPv4.
- Un computer memorizza l'indirizzo in binario, ma è chiaro che 128 bit non possono facilmente essere trattati dapersone. Diverse notazioni sono state proposte per rappresentare indirizzi IPv6 quando sono gestiti da persone.
- La notazione esadecimale divide l'indirizzo in otto parti, ciascuna composta di quattro cifre esadecimali separata da due punti. Ad esempio:

  FF56:AB23:1234:0008:0058:DE32:AABB:0067

- Un indirizzo IPv6 anche in forma esadecimale, è molto lungo. Per questo, nel caso in cui siano presenti degli zeri è possibile rappresentarlo con forme abbreviate. Ad esempio il blocco :0008: dell'esempio precedente si può esprimere solo con :8:, il blocco :0067: con 67.

- Anche l'IPv6 ha un indirizzamento gerarchico e pertanto si usa la notazione CIDR. Ad esempio, la notazione

  FF56:AB23:1234:8:58:DE32:AABB:67/60

  indica che i primo 60 bit costituiscono il prefisso di rete.

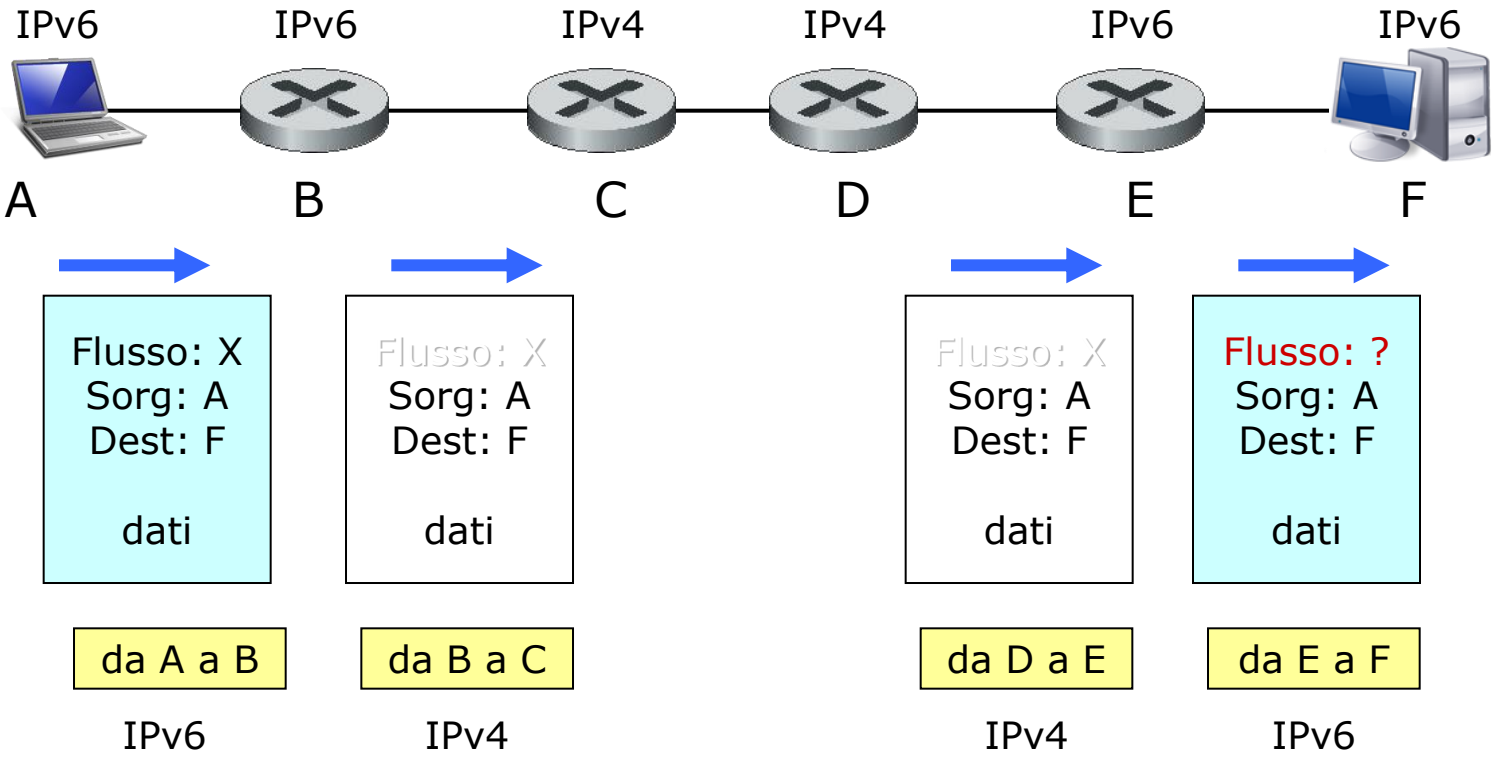
# La transizione da IPv4 a IPv6

- L'IPv6 è "compatibile all'indietro", cioè può inviare, instradare e ricevere i datagram IPv4 mentre l'IPv4, ampiamente diffuso, non è in grado di gestire i datagram IPv6.
- La RFC 2893 descrive due metodi, che possono essere usati per ottenere un graduale aggiornamento degli indirizzi degli host e dei router da IPv4 a IPv6.

**Metodo dual-stack**

- Il metodo più semplice è il **dual-stack**, in cui i nodi hanno sia l'IPv6 che l'IPv4.
- Un nodo **IPv6/IPv4**, è in grado di inviare e ricevere entrambi i datagram IPv4 e IPv6 e deve avere indirizzi sia IPv6 sia IPv4. Deve inoltre essere in grado di determinare se un altro nodo è IPv6 o solo IPv4.

- Questo problema può essere risolto usando il DNS, che può ritornare un indirizzo IPv6 se il nodo destinatario è identificato come IPv6, o altrimenti ritornare un indirizzo IPv4. Ovviamente, se il nodo che invia la richiesta DNS è solo IPv4, il DNS ritornerà solo un indirizzo IPv4.
- Il metodo dual-stack, prevede che, se o il mittente o il destinatario è solo IPv4, deve essere usato un datagram IPv4.
- E' anche possibile che due nodi IPv6 possano finire per scambiarsi datagram IPv4. Questo caso è mostrato nella figura seguente.



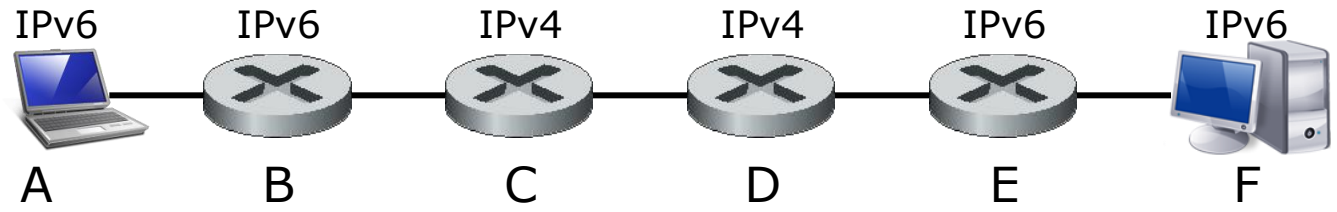

Soluzione dual-stack

- Supponiamo che l'host **A** voglia inviare un datagram all'host **F** e che entrambi gli host siano IPv6. I nodi A e B possono scambiarsi pacchetti IPv6. Il nodo B deve creare un datagram IPv4 da inviare al nodo C. Certamente, il campo dati del pacchetto IPv6 può essere copiato nel campo dati del datagram IPv4 e può essere effettuata la corretta conversione dell'indirizzo. Ma, ci saranno campi specifici di IPv6 nel datagram IPv6 (per esempio, il campo identificatore del flusso) che non hanno il corrispondente in IPv4. L'informazione in questi campi sarà persa. **Quindi, anche se E ed F possono scambiarsi datagram IPv6**, **il datagram IPv4 in arrivo al nodo E da D non contiene tutti i campi che erano presenti nel datagram originale IPv6 spedito da A**.

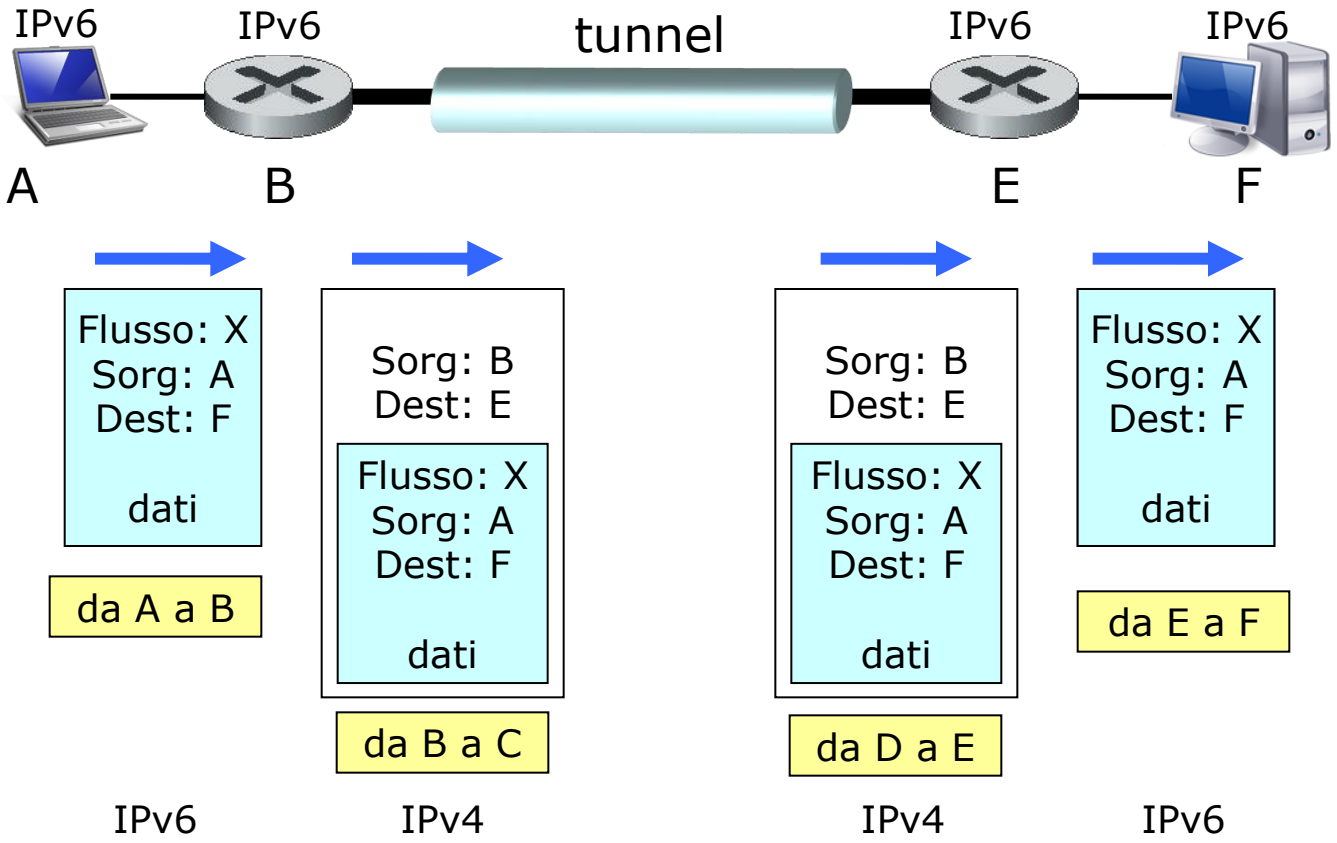
## Metodo del tunneling

- Un'alternativa al metodo dual-stack, è il **tunneling**.
- Con il termine "**tunnel**" si intende una sequenza di router IPv4 presenti in un percorso.
- Con il tunneling, il nodo IPv6 del lato mittente (per esempio, B) **inserisce l'intero datagram IPv6 nel campo dati di un datagram IPv4**.
- Questo datagram IPv4 è quindi indirizzato al nodo IPv6 del lato ricevente (per esempio E) e inviato al primo nodo del tunnel (per esempio, C).
- I router IPv4 presenti nel percorso che costituisce il tunnel rilanciano questo datagram IPv4 fra loro.
- Il nodo IPv6 dal lato ricevente del tunnel alla fine riceve il datagram IPv4, determina che il datagram IPv4 contiene un datagram IPv6, estrae il datagram IPv6 e lo rilancia esattamente come se lo avesse ricevuto da un vicino IPv6 cui fosse direttamente collegato.

## Vista fisica




## Vista logica



# ICMP: protocollo dei messaggi di controllo di Internet

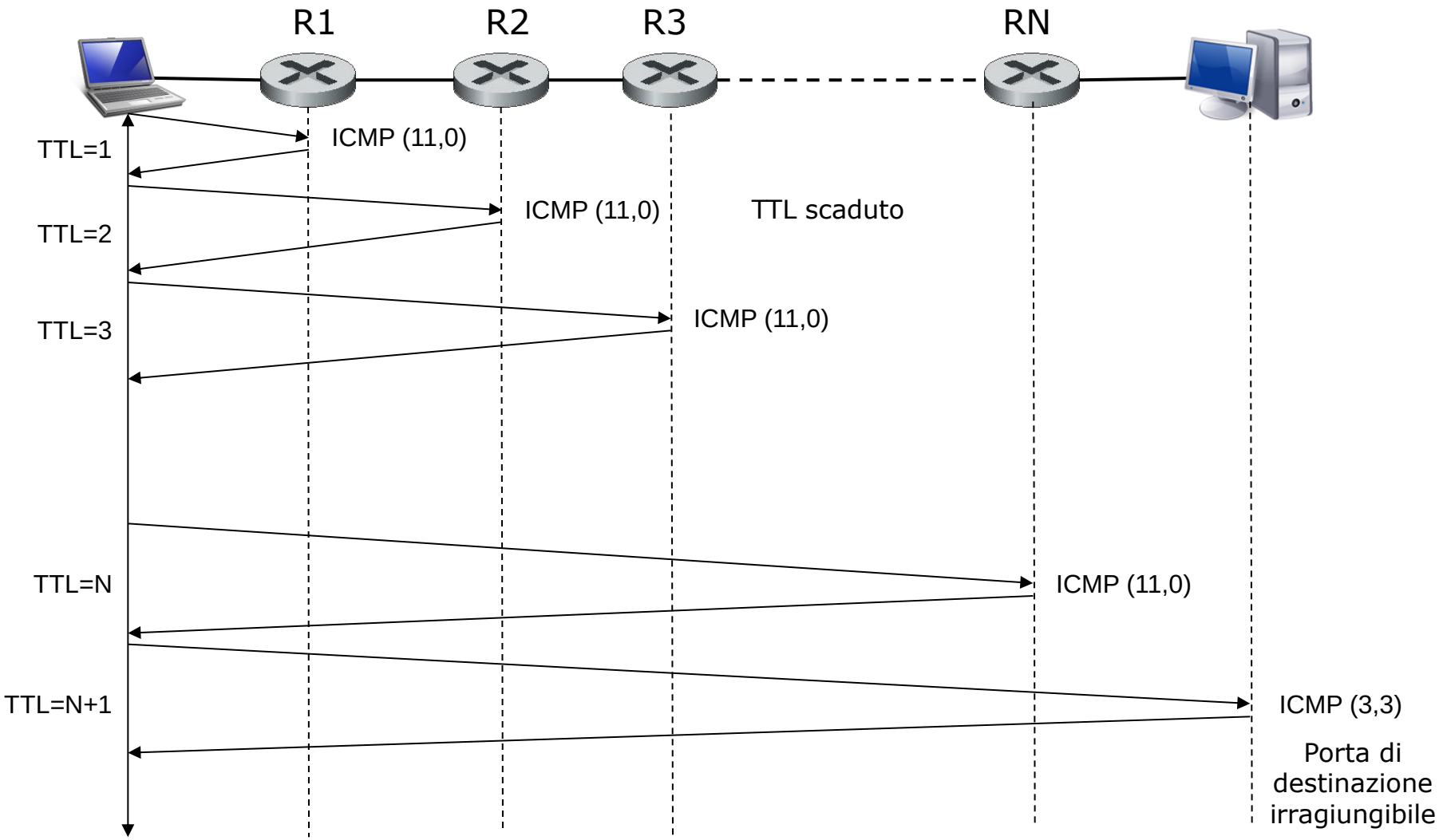
- L'**ICMP**, (***Internet Control Message Protocol***), è usato da host e router per scambiarsi le informazioni dello strato di rete.
- L'ICMP è usato principalmente per il **report degli errori**.
- Ad esempio, quando un client cerca di connettersi ad un server mediante telnet, FTP o HTTP e per qualche problema non è possibile la connessione, il router che non ha potuto rinviare il pacchetto verso la destinazione invia il messaggio ICMP tipo 3 "**Rete di destinazione non raggiungibile**" all'host mittente per segnalare ad esso il problema di irrangiungibilità.
- Quando l'host mittente riceve il messaggio ICMP passa il codice di errore al TCP che, a sua volta, ritorna il codice di errore all'applicazione.

- I messaggi ICMP sono inseriti nel campo dati del datagram IP, come i segmenti TCP o UDP.
- I messaggi ICMP hanno un campo **tipo** e un campo **codice**, e contengono l'intestazione e i primi otto byte del datagram IP che ha causato l'eccezione, in modo che il mittente possa determinare il pacchetto responsabile dell'errore.
- I messaggi ICMP sono anche usati per scambiare informazioni. Ad esempio, il programma **ping** invia un messaggio ICMP **echo request** (**tipo 8, codice 0)** all'host specificato. L'host di destinazione, restituisce una risposta ICMP **echo reply (tipo 0, codice 0).**
- Alcuni messaggi ICMP sono mostrati nella figura.

| Type | Code | Description |
|---|---|---|
| 0 | 0 | echo reply (to ping) |
| 3 | 0 | destination network unreachable |
| 3 | 1 | destination host unreachable |
| 3 | 2 | destination protocol unreachable |
| 3 | 3 | destination port unreachable |
| 3 | 6 | destination network unknown |
| 3 | 7 | destination host unknown |
| 4 | 0 | source quench (congestion control) |
| 8 | 0 | echo request |
| 9 | 0 | router advertisement |
| 10 | 0 | router discovery |
| 11 | 0 | TTL expired |
| 12 | 0 | IP header bad |

**Tipi di messaggio ICMP**

- Anche **traceroute**, che visualizza la lista di router presenti nel percorso tra un host mittente e un host destinatario, utilizza l'ICMP. Per determinare la lista di router, traceroute invia una serie di datagram IP alla destinazione, ciascuno dei quali contiene un segmento UDP con un numero di porta improbabile.
- Il TTL del primo datagram viene posto uguale a 1, il secondo a 2, e così via. Inoltre, per ogni datagram che invia, traceroute memorizza il valore del timer. Quando lo i-esimo datagram raggiunge lo i-esimo router questo rileva che il TTL è scaduto e, in base al funzionamento di IP, il router scarta il datagram e invia un messaggio di notifica ICMP **TTL expired** (**tipo 11, codice 0**) al mittente. Questo **messaggio contiene l'indirizzo IP del router e il suo il nome (se assegnato)**. Quando il messaggio ICMP arriva al mittente, traceroute calcola il tempo di andata e ritorno in base al timer e visualizza il nome e l'indirizzo dello i-esimo router.
- Infine, quando lo i-ennesimo datagram arriva al destinatario, questo verificando che il numero di porta è errato risponderà al mittente con un messaggio ICMP **porta irraggiungibile (tipo=3, codice=3)**. Il mittente quindi non invierà più datagram.


R1
R2
R3
RN
TTL=1
ICMP (11,0)
TTL=2
ICMP (11,0)
TTL scaduto
TTL=3
ICMP (11,0)
TTL=N
ICMP (11,0)
TTL=N+1
ICMP (3,3)
Porta di destinazione irragiungibile

# ICMP per IPv6

- Come abbiamo detto, il protocollo ICMP è usato da host e router per notificare condizioni di errore e brevi informazioni.
- Per l'IPv6 è stata definita una nuova versione di ICMP che oltre agli esistenti tipi e codici, ha anche aggiunto nuovi tipi e codici richiesti dalle nuove funzionalità di IPv6. Tra queste è presente il tipo
  - "**pacchetto troppo grande**" *(**packet too big**),* e
  - "**opzioni di IPv6 non riconosciute**" *(unrecognized IPv6 options).*
- Inoltre, **ICMPv6 svolge la funzionalità dell'IGMP (Internet Group Management Protocol)**, che vedremo in seguito quando parleremo della comunicazione multicast.