Università di Roma Tor Vergata
Corso di Laurea triennale in Informatica

Sistemi operativi e reti

A.A. 2019-2020

Pietro Frasca

Parte II: Reti di calcolatori

Lezione 18 (42)

Martedì 12-05-2020

IPv6

- Nei primi anni '90, l'**IETF** (Internet Engineering Task Force) propose il 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.
- Prima della versione IPv6, era stata proposta la versione IPv5 basata sul modello OSI. Tuttavia tale versione non è mai stata realizzata.

Formato del datagram IPv6

- Le più importanti modifiche introdotte da IPv6 sono:
  - ***Estensione dell'indirizzamento***. L'IPv6 incrementa le dimensioni dell'indirizzo IP da 32 a **128 bit**. Oltre agli indirizzi unicast e multicast, è stato definito un nuovo tipo di indirizzo, detto **indirizzo anycast** , che permette di inviare 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 contenuto trasmesso.

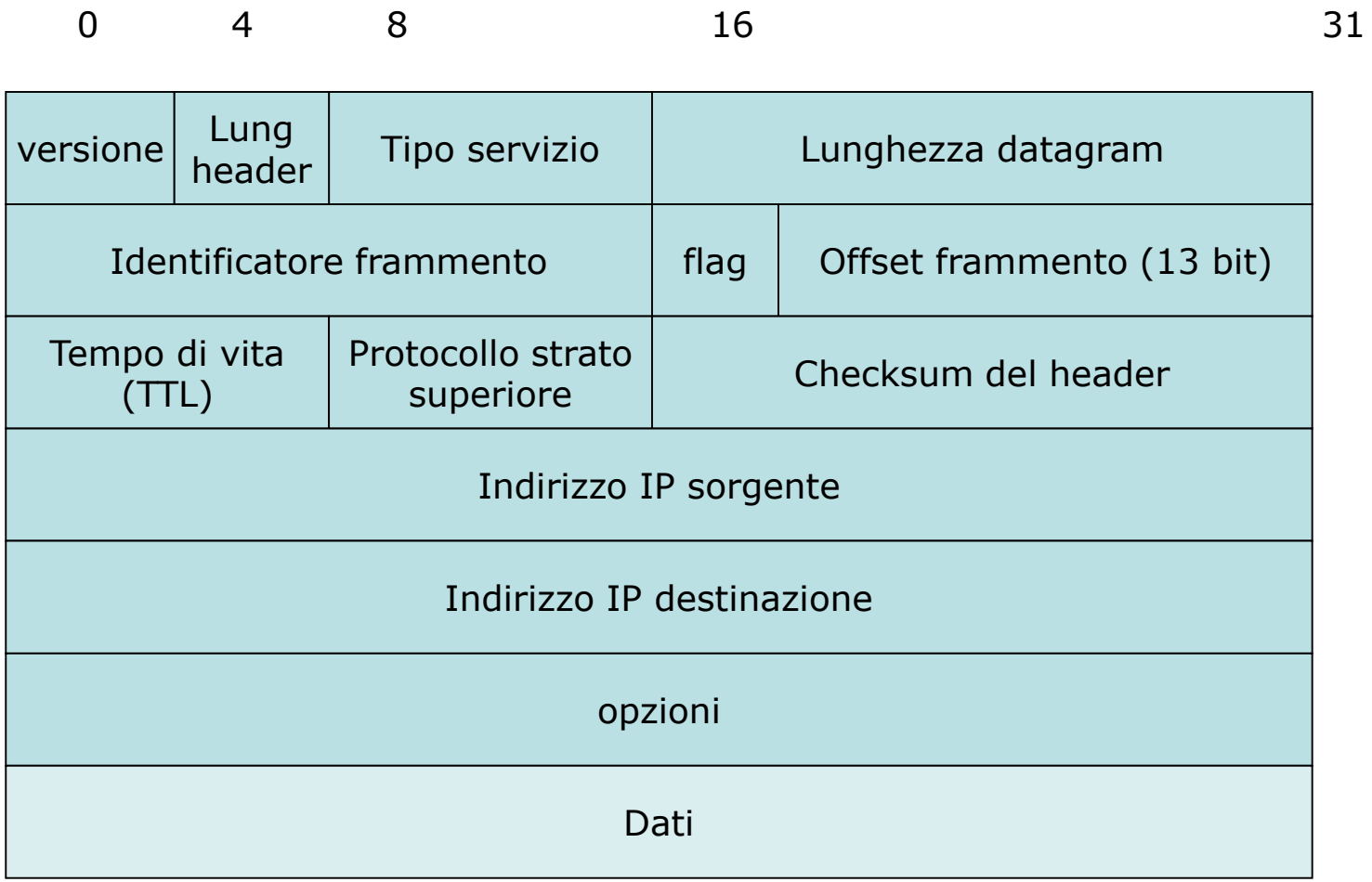
Ad esempio, trasmissioni di streaming audio e video, prodotte da applicazioni soft real-time, potrebbero essere trattate in modo diverso da comunicazioni relative alla posta elettronica e al trasferimento di file.

L'intestazione IPv6 ha anche un campo 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.

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

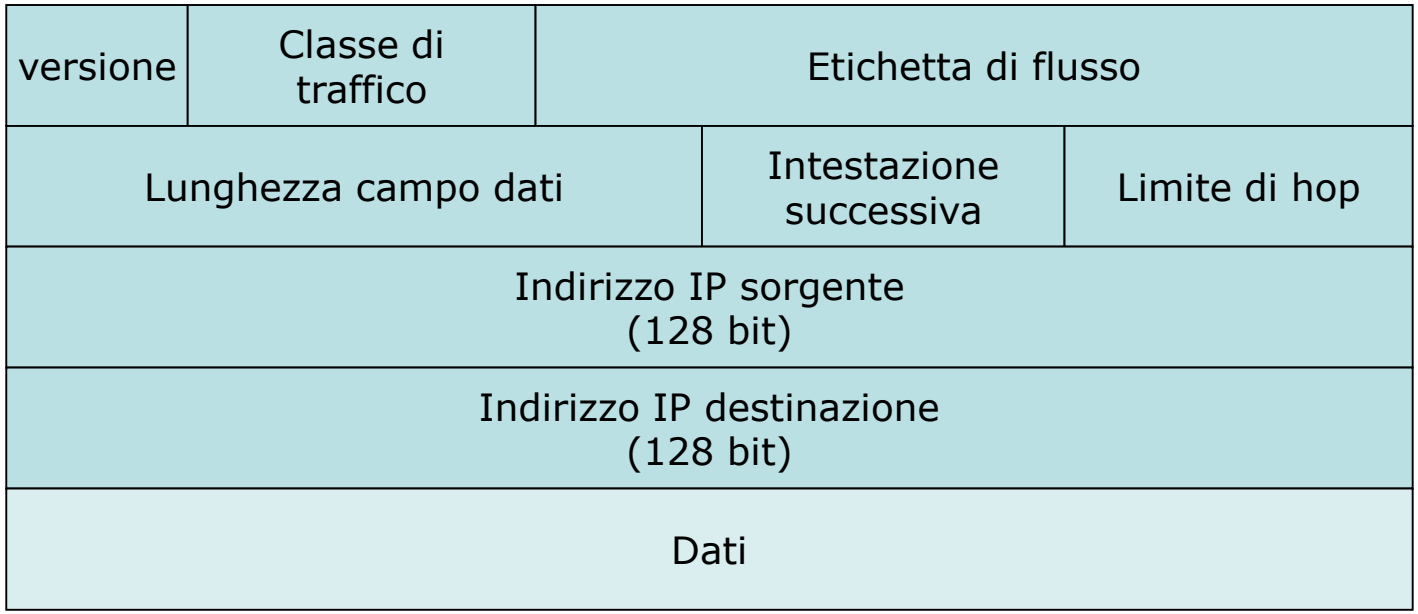
Formato del datagram IPv4

- Il formato del datagram di **IPv4**.



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***. (4 bit) identifica il numero della versione IP.
  - ***Classe di traffico***. (8 bit) è analogo al campo TOS dell'IPv4.
  - ***Etichetta di flusso***. (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***. (16 bit) specifica la lunghezza del campo dati.
  - **Intestazione successiva**. 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***. 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 e viene inviato un messaggio di notifica ICMP al mittente.

- ***Indirizzi di sorgente e destinazione****.* I vari formati degli indirizzi IPv6 a 128 bit sono descritti nella RFC 2373.
- ***Dati****.* contiene il carico utile del datagram IPv6. Quando il datagram raggiunge la sua destinazione, il campo dati 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****.* 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

- Il motivo 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 da persone. Diverse notazioni sono state proposte per rappresentare indirizzi IPv6 quando sono gestiti da persone.
- La notazione esadecimale divide l'indirizzo in otto parti, ciascuna formata 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 primi 60 bit costituiscono il prefisso di rete.

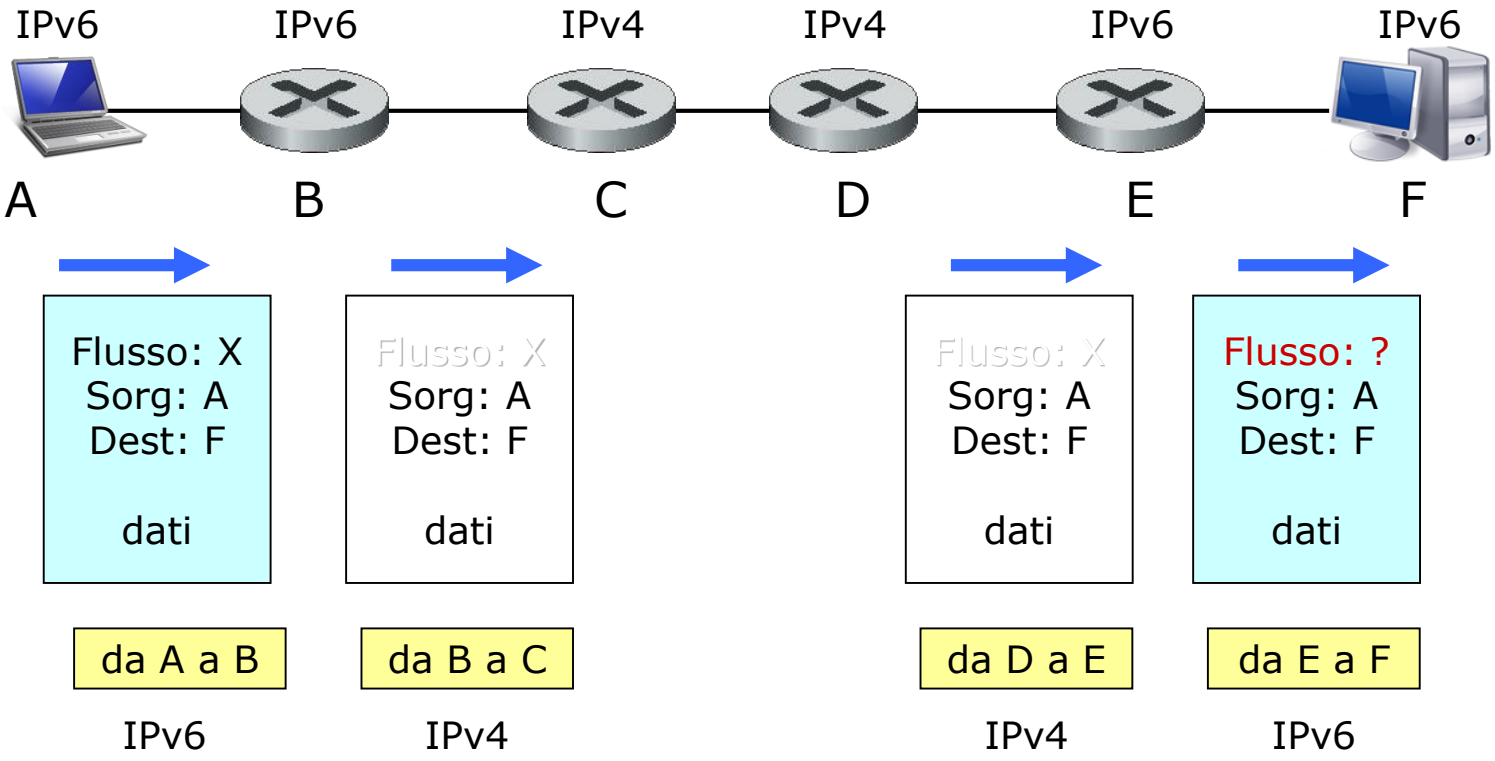
La transizione da IPv4 a IPv6

- 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, con il quale comunicare, sia 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.



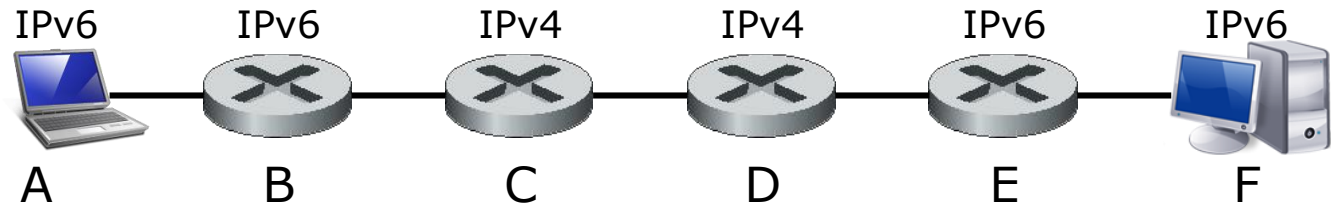
Soluzione dual-stack

- 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**.

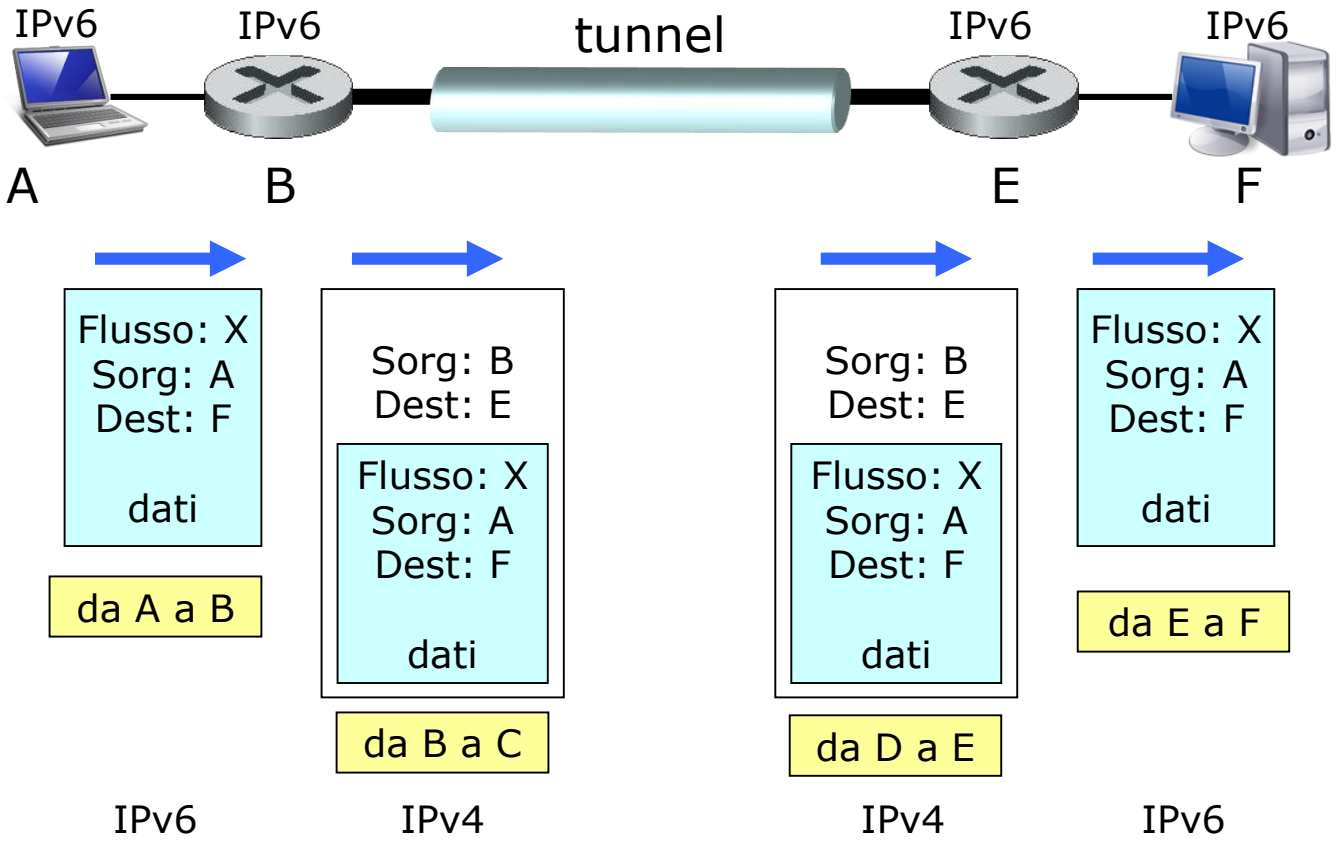
Metodo del tunneling

- 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



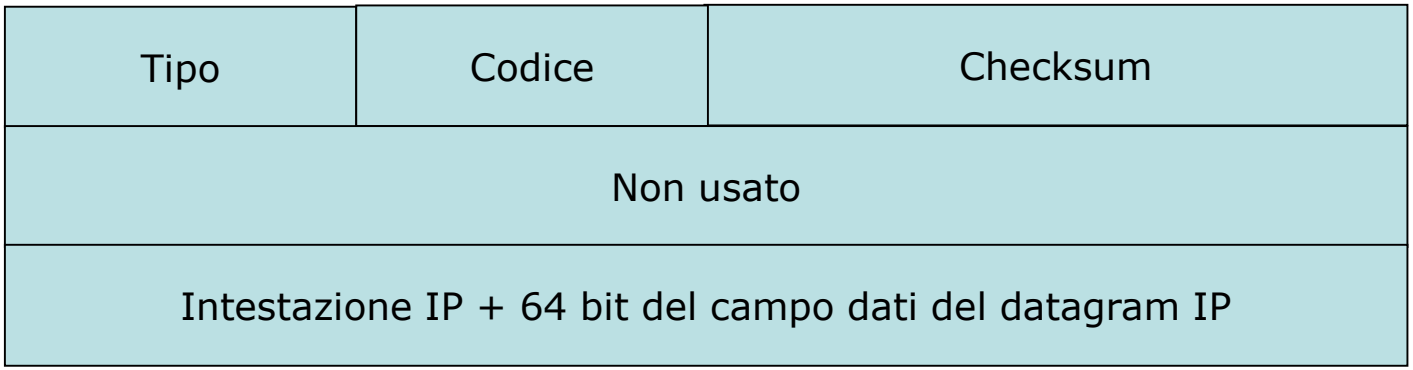
Vista logica



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 irraggiungibilità.
- 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 datagramma IP, come i segmenti TCP o UDP.
- I messaggi ICMP hanno un campo **tipo** e un campo **codice**, e contengono, come campo dati, l'intestazione e i primi otto byte del campo dati del datagramma IP che ha causato l'eccezione, in modo che il mittente possa determinare il pacchetto responsabile dell'errore. Il campo *non usato* è riservato per usi futuri.



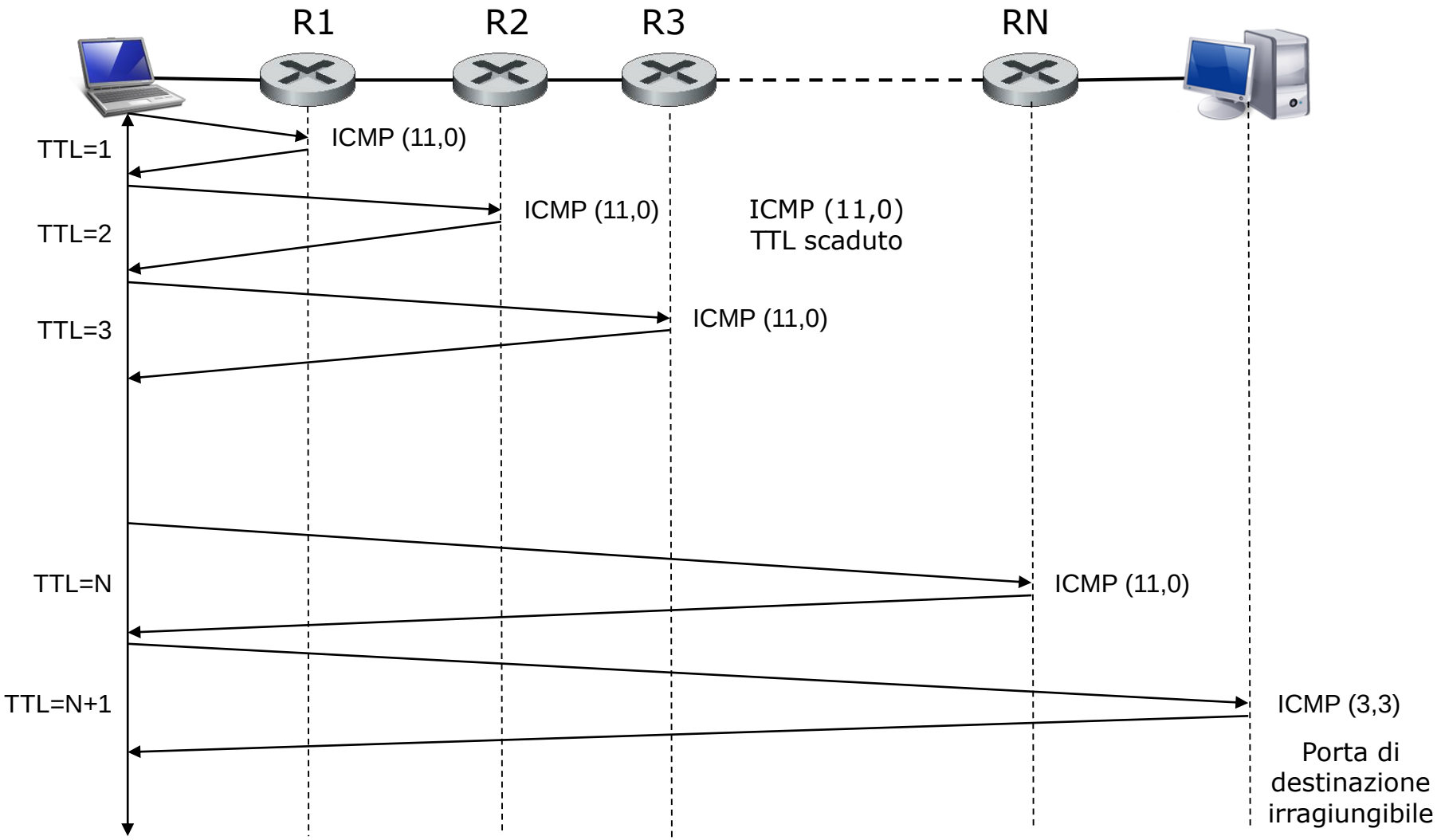
Formato del protocollo ICMP

Nella tabella seguente sono riportati i messaggi ICMP più frequentemente usati.

Type	Code	Description
0	0	echo reply (to ping)
3	0	rete non raggiungibile
3	1	host non raggiungibile
3	2	protocollo non raggiungibile
3	3	porta di destinazione non raggiungibile
3	4	frammentazione necessaria e DF settato
3	6	rete di destinazione sconosciuta
3	7	host di destinazione sconosciuto
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

- I messaggi ICMP sono anche usati per scambiare informazioni. Ad esempio, l'utility **ping** invia un messaggio ICMP **echo request** (**tipo 8, codice 0)** all'host specificato. L'host di destinazione, risponde con il messaggio ICMP **echo reply (tipo 0, codice 0).**
- 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 speciali datagrammi 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 hostname (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.

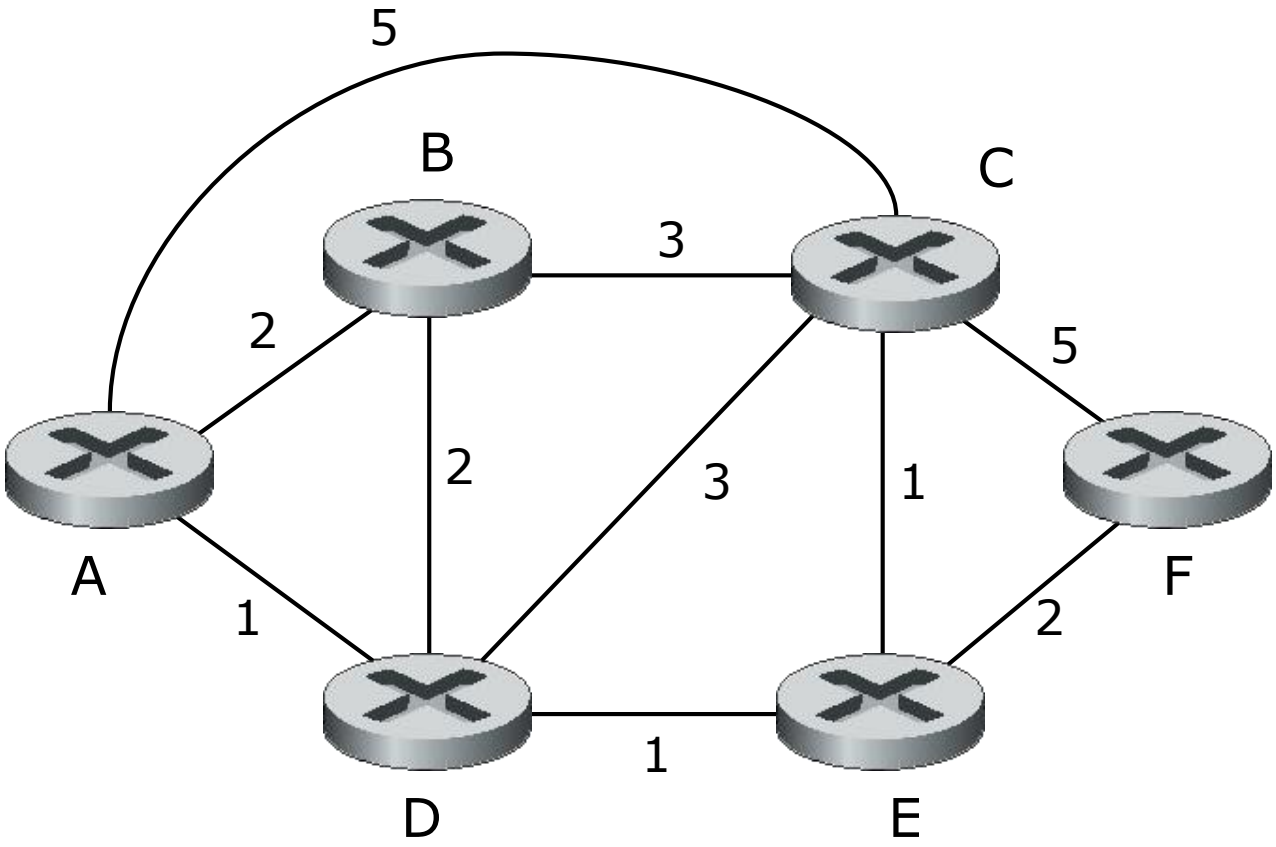

R1
R2
R3
RN
TTL=1
ICMP (11,0)
TTL=2
ICMP (11,0)
ICMP (11,0)
TTL scaduto
TTL=3
ICMP (11,0)
TTL=N
ICMP (11,0)
TTL=N+1
ICMP (3,3)
Porta di destinazione irragiungibile

ICMP per IPv6

- Come descritto in precedenza, 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.

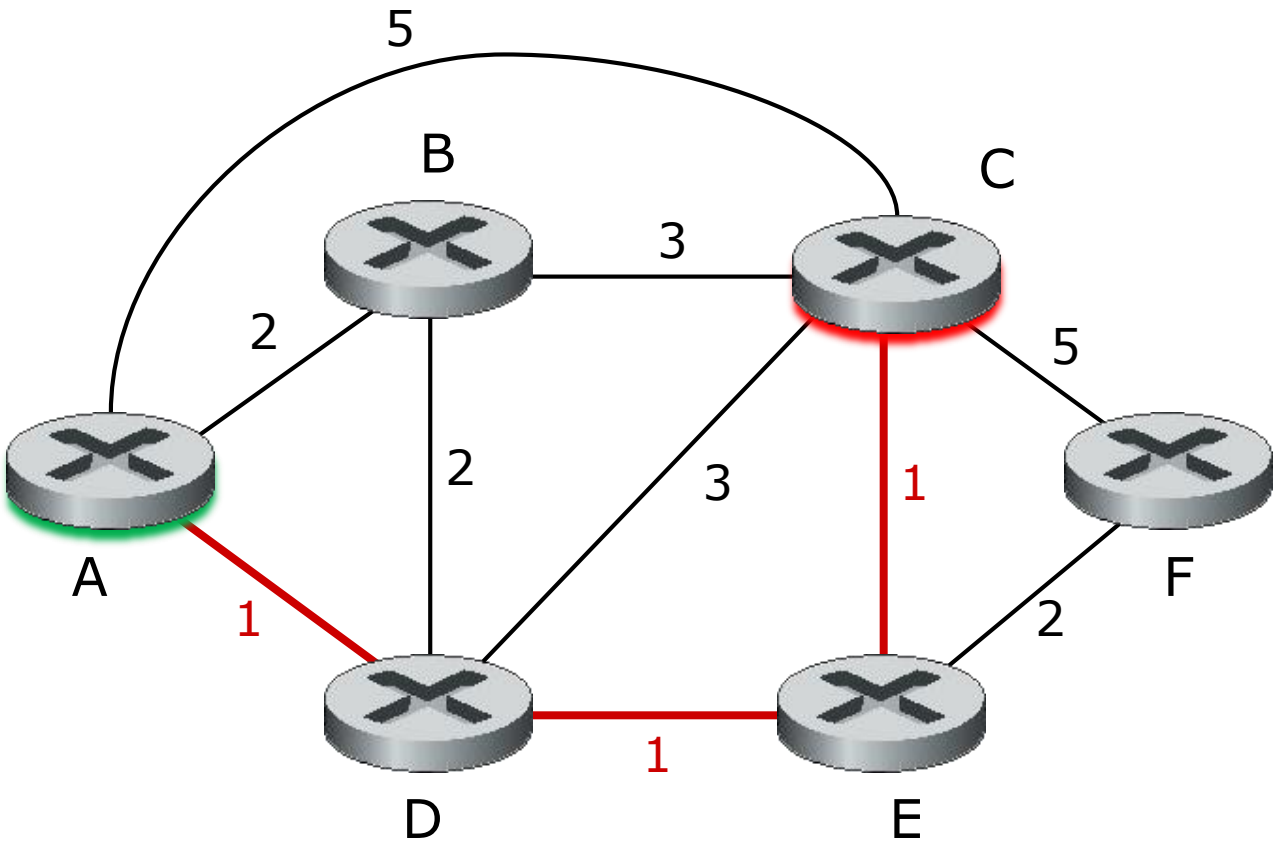
Algoritmi di instradamento

- **I protocolli di instradamento** *(**routing protocol**)* dello strato di rete hanno il compito di **determinare un percorso**, dalla sorgente alla destinazione, che i pacchetti devono seguire che sia a **"minimo costo".**
- Poiché un host è collegato al **router di default**, il problema di instradare un datagram dalla sorgente alla destinazione si riduce ad instradare il datagram dal router sorgente al router destinazione.
- Un modello astratto per lo studio di algoritmi di instradamento è il grafo illustrato in figura. I nodi rappresentano i router e gli archi i collegamenti che connettono tra loro i router.
- Un collegamento può avere anche un peso associato per rappresentare varie grandezze, come ad esempio la distanza tra i nodi, la larghezza di banda, il livello di congestione, o anche un valore che dipende da una funzione delle varie grandezze.



Modello astratto di rete.

- Nella Figura, per esempio, il percorso di minor costo fra il nodo A (sorgente) e il nodo C (destinazione) è ADEC.



Percorso minimo tra A e C.

Classificazione degli algoritmi

Algoritmi globali e decentralizzati

- In genere, gli algoritmi di instradamento sono classificati in **globali** e **decentralizzati.**
- Un **algoritmo di instradamento globale** calcola il percorso di minor costo tra una sorgente e una destinazione usando **informazioni complete e globali della rete**.
- L'algoritmo, prima di essere eseguito, richiede di conoscere le connessioni tra tutti i nodi e tutti i pesi (costi) dei collegamenti prima di eseguire il calcolo del cammino minimo.
- Questi algoritmi, con informazioni di stato globali, sono chiamati algoritmi basati sullo **stato dei collegamenti** *(**link state algorithm**).*
- In un **algoritmo di instradamento decentralizzato** *(decentralized routing algorithm),* il calcolo del percorso di minor costo è eseguito in modo distribuito e iterativo.

- Non è necessario che i nodi abbiano informazioni complete sul costo di tutti i collegamenti della rete. Inizialmente, ogni nodo ha la sola conoscenza del costo dei collegamenti che sono direttamente collegati ad esso.
- Successivamente, scambiando iterativamente informazioni con i nodi a esso vicini, ciascun nodo calcola, a mano a mano, il percorso di minor costo verso una destinazione o un gruppo di destinazioni.
- Una classe di algoritmi di instradamento decentralizzato molto diffusa è **distance vector, DV** (vettore delle distanze).

Algoritmi statici e dinamici

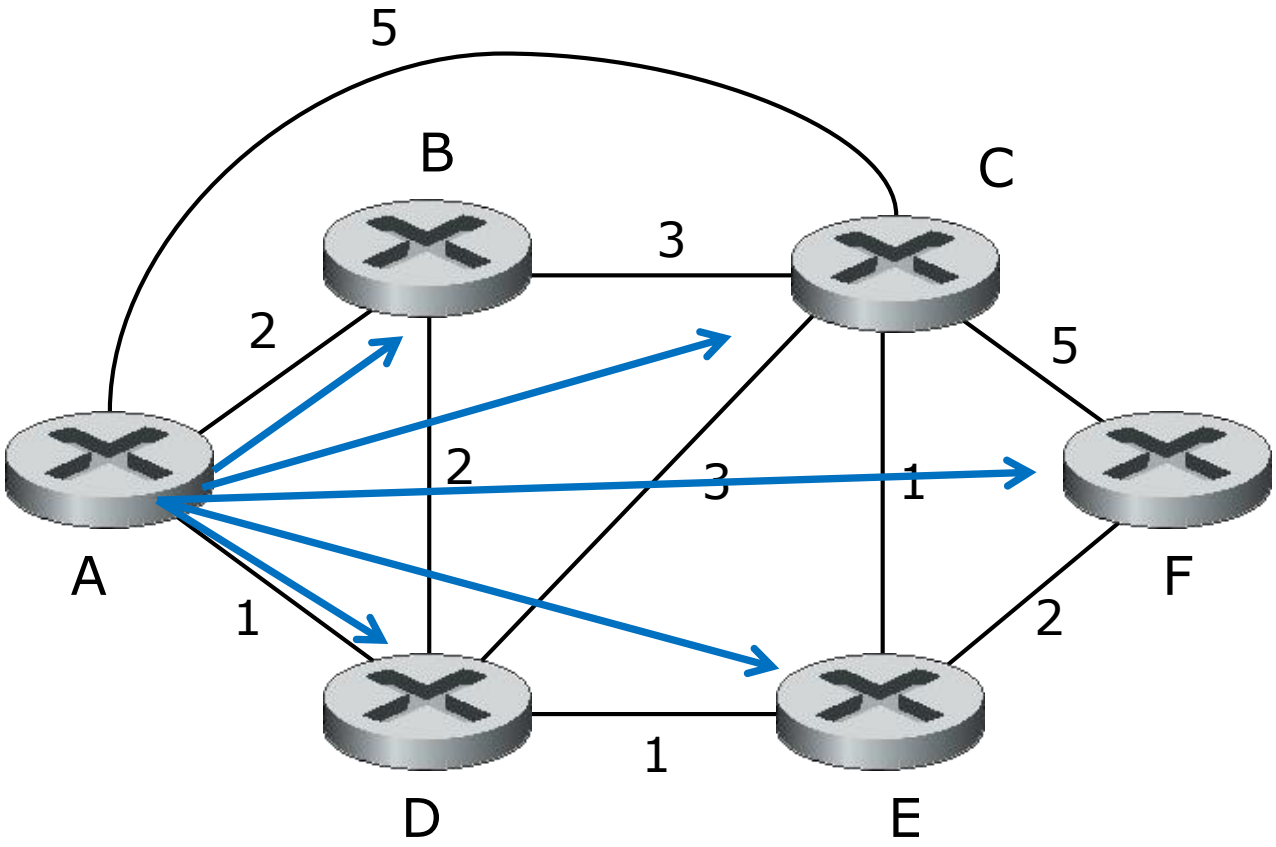
- Un secondo modo per classificare gli algoritmi di instradamento è in base al fatto che siano **statici** o **dinamici**.
- Gli **algoritmi di instradamento statici**, sono usati in reti in cui i percorsi cambiano molto raramente. In questo caso l'amministratore di rete modifica a mano le tabelle di instradamento dei router.
- Gli **algoritmi di instradamento dinamici** modificano i percorsi di instradamento quando varia la topologia della rete o la quantità di congestione del traffico. Gli algoritmi dinamici sono più reattivi alle variazioni nella rete, ma sono anche più suscettibili a problemi come ***routing loop*** (**percorsi ciclici**) e oscillazioni nei percorsi.

Algoritmi sensibili e insensibili al carico

- Un terzo modo di classificare gli algoritmi di instradamento è in relazione al fatto che siano **sensibili al** o **insensibili al carico***.*
- Gli algoritmi sensibili al carico, variano i costi dei collegamenti dinamicamente in base allo stato attuale di congestione dei collegamenti. I primi algoritmi di instradamento di ARPAnet erano sensibili al carico e hanno avuto molti problemi di funzionamento.
- Gli algoritmi di instradamento di Internet di oggi (come **RIP**, **OSPF** e **BGP**) sono **insensibili al carico**, dato che il costo di un link non dipende dal suo livello di congestione.
- Solo due classi di algoritmi di instradamento *sono* usati in Internet:
  - **algoritmo dinamico basato sullo stato globale dei link *(dynamic global link state algorithm)* e**
  - **algoritmo dinamico decentralizzato vettore delle distanze *(dynamic decentralized distance vector algorithm).***

Algoritmo di instradamento basato sullo stato dei link

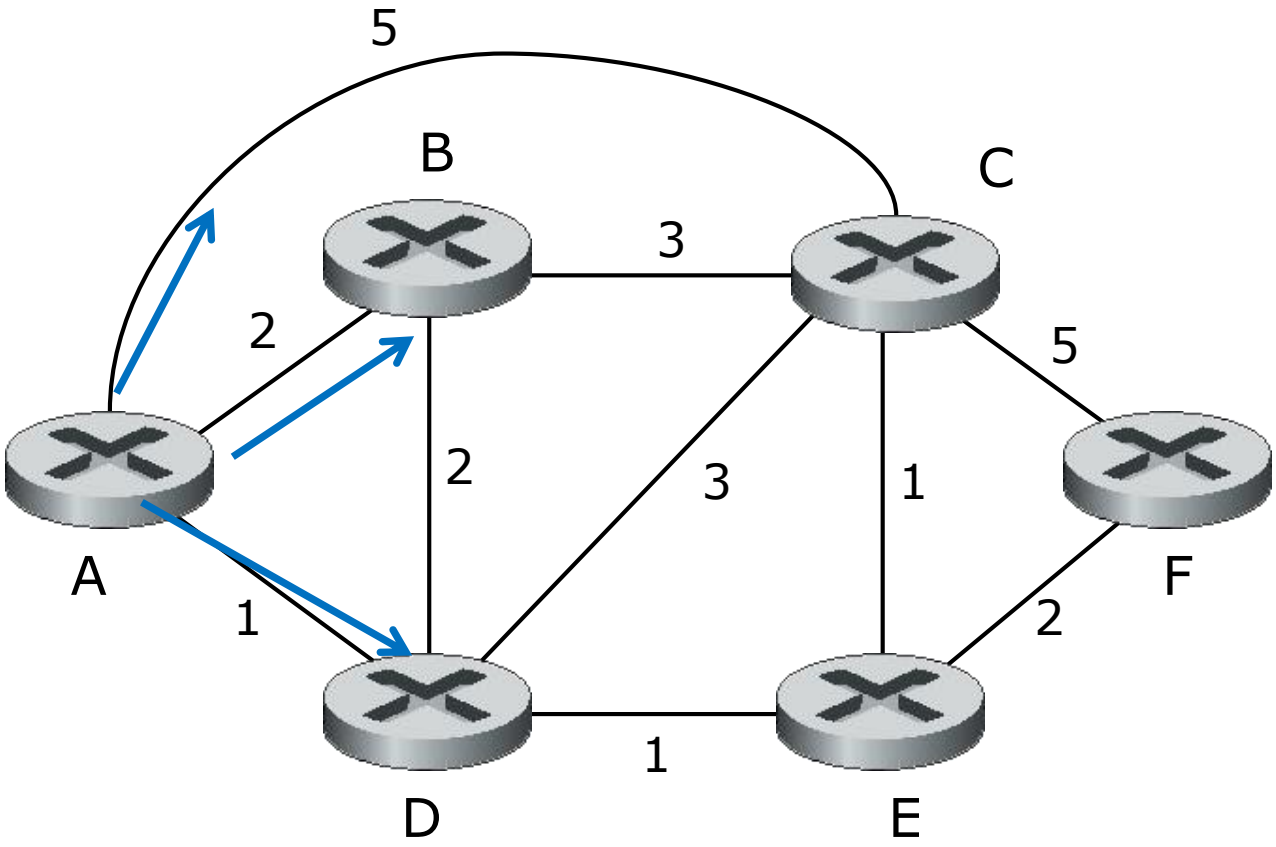
- In un algoritmo basato sullo stato dei collegamenti *(link state algorithm)* la topologia della rete e tutti i costi dei collegamenti sono informazioni note come input dell'algoritmo.
- Per conoscere la topologia completa della rete ciascun router trasmette gli indirizzi IP delle proprie interfacce e i costi dei link a esso collegati a tutti gli altri router della rete. Questa trasmissione dello stato dei link, detta ***link state broadcast***, da parte di ciascun nodo porterà **tutti i nodi a conoscere la completa topologia della rete**. Ciascun nodo può allora eseguire l'algoritmo per calcolare i percorsi di minor costo.
- L'algoritmo dello stato dei link molto usato è l'algoritmo di **Dijkstra**.
- L'algoritmo di Dijkstra calcola il percorso di minor costo da un nodo sorgente a tutti gli altri nodi nella rete.



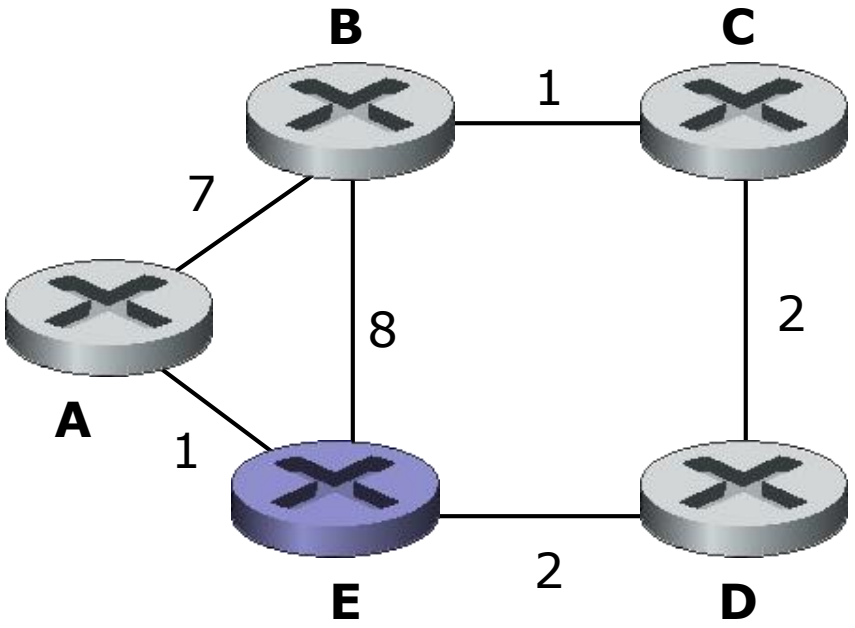
Algoritmo globale.

Algoritmo di instradamento Distance Vector

- Mentre l'algoritmo **LS** è un algoritmo che usa in formazioni globali, l'algoritmo **distance vector** (**DV, vettore delle distanze**) è distribuito, iterativo e asincrono.
- L'algoritmo è distribuito in quanto ciascun nodo riceve informazioni solo dai "vicini" ai quali è direttamente collegato, esegue un calcolo sulle sue tabelle, e quindi distribuisce i risultati ai suoi vicini. E' asincrono perché tutti i nodi scambiano tra loro le informazioni in modo non sincronizzato. L'algoritmo è iterativo perché questo processo continua finché lo scambio di informazione tra i vicini termina.
- La principale struttura dati dell'algoritmo **DV** è la **tabella delle distanze** mantenuta **in ciascun nodo**. La tabella delle distanze ha una riga per ogni destinazione nella rete e una colonna per ciascuno dei vicini direttamente collegati al nodo.



Algoritmo decentralizzato.



vicini

destinazione $D^E()$	A	B	D
A	(1)	14	5
B	7	8	(5)
C	6	9	(4)
D	4	11	(2)

$D^X(Y,Z) = c(X,Z) + \min_w\{D^Z(Y,w)\}$

x: sorgente
Y: destinazione
Z: via (router successivo)

Esempio:
$D^E(A,B) = c(E,B) + \min_w\{D^B(A,w)\}$

Esempio tabella delle distanze per il nodo sorgente E

Confronto fra gli algoritmi di instradamento dello stato del link e distance vector

- Concludiamo il discorso sugli algoritmi basati sullo stato dei link e distance vector con un rapido confronto di alcune loro caratteristiche.
- ***Complessità del messaggio***.
  - L'algoritmo **LS** richiede che ciascun nodo conosca il costo di ciascun link della rete. Questo richiede la spedizione di ***O(N·L)*** messaggi, dove **N** è il numero di nodi nella rete ed **L** è il numero di link. Inoltre, ogni volta che il costo di un link cambia, il nuovo costo del link deve essere comunicato a *tutti* i nodi.
  - L'algoritmo DV richiede per ciascuna iterazione lo scambio dei messaggi fra vicini direttamente collegati. Il tempo richiesto dall'algoritmo per convergere può dipendere da diversi fattori. Quando cambiano i costi dei link, l'algoritmo DV propagherà i risultati della variazione del costo del link interessato *solo* se il nuovo costo del link produrrà una variazione del percorso di minor costo per uno dei nodi collegati a quel link.

- ***Velocità di convergenza***.
  - **LS** è un algoritmo $O(N^2)$ che richiede $O(N \cdot L)$ messaggi.
  - L'algoritmo **DV** può convergere lentamente e può avere percorsi ciclici durante la convergenza.
- ***Robustezza***. Cosa può succedere se un router si guasta?
  - Con LS, un router può trasmettere in broadcast un costo errato per uno dei suoi collegamenti oppure ricevere un pacchetto con qualche errore. Tuttavia, ciascun router LS calcola solo la propria tabella di instradamento. Questo significa che i calcoli dei percorsi in LS sono separati, e questo fornisce un certo grado di robustezza.
  - Con DV, un router può comunicare percorsi di minor costo errati a qualsiasi o tutte le destinazioni. Infatti, ad ogni iterazione, il calcolo della tabella in un nodo è trasmesso ai suoi vicini e quindi, indirettamente, ai vicini dei suoi vicini all'iterazione successiva. Per questo motivo, con DV un calcolo sbagliato di un nodo può essere diffuso attraverso l'intera rete.

- Molti altri algoritmi sono stati proposti, oltre a LS e DV i quali però sono gli unici utilizzati in pratica in Internet.