

# Reti di Elaboratori

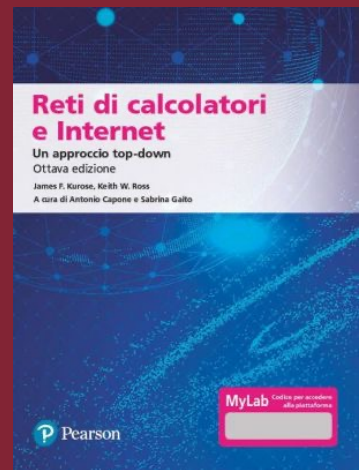
Livello di Rete: Il protocollo Internet



SAPIENZA  
UNIVERSITÀ DI ROMA

Alessandro Checco

[alessandro.checco@uniroma1.it](mailto:alessandro.checco@uniroma1.it)



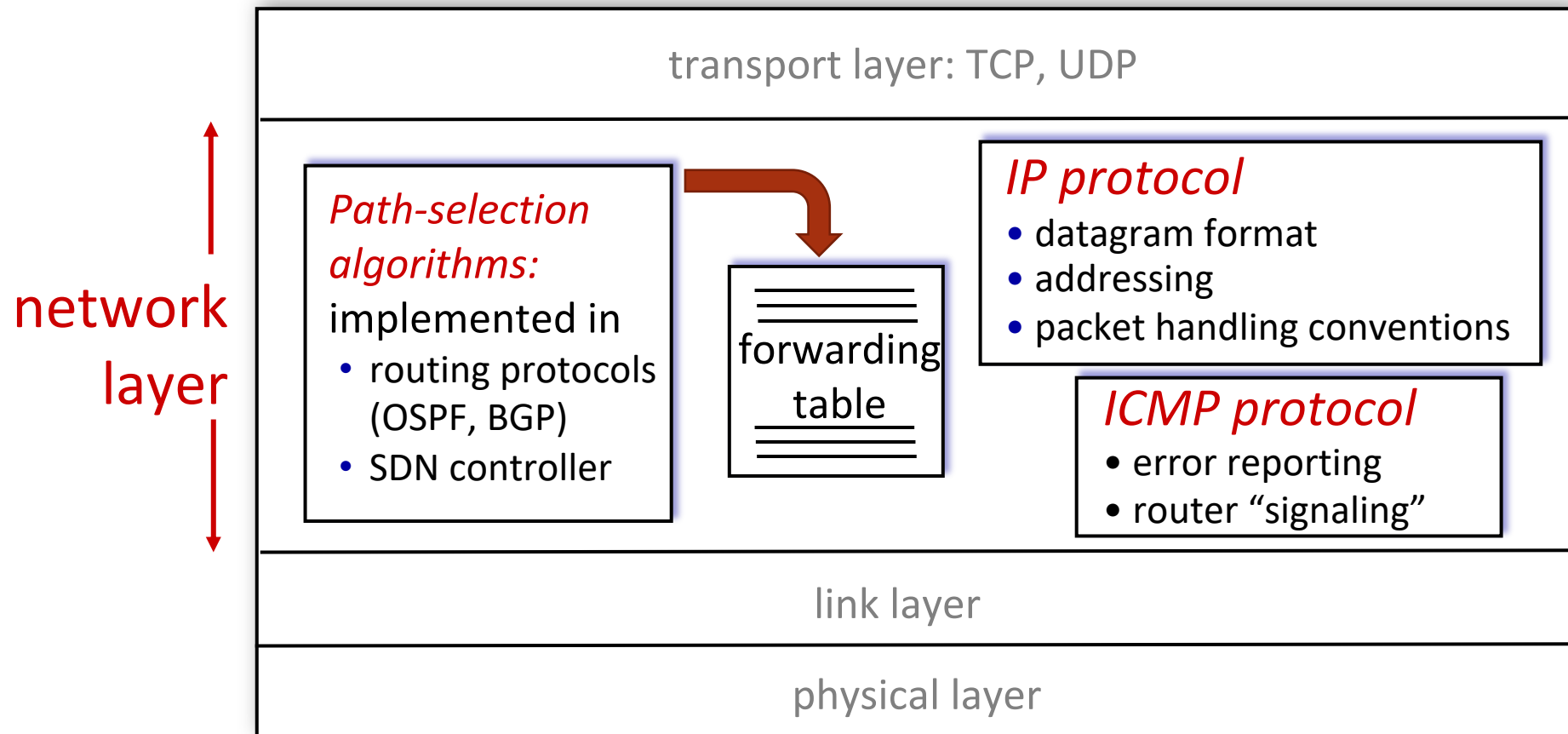
Capitolo 4

# Livello di rete: sommario

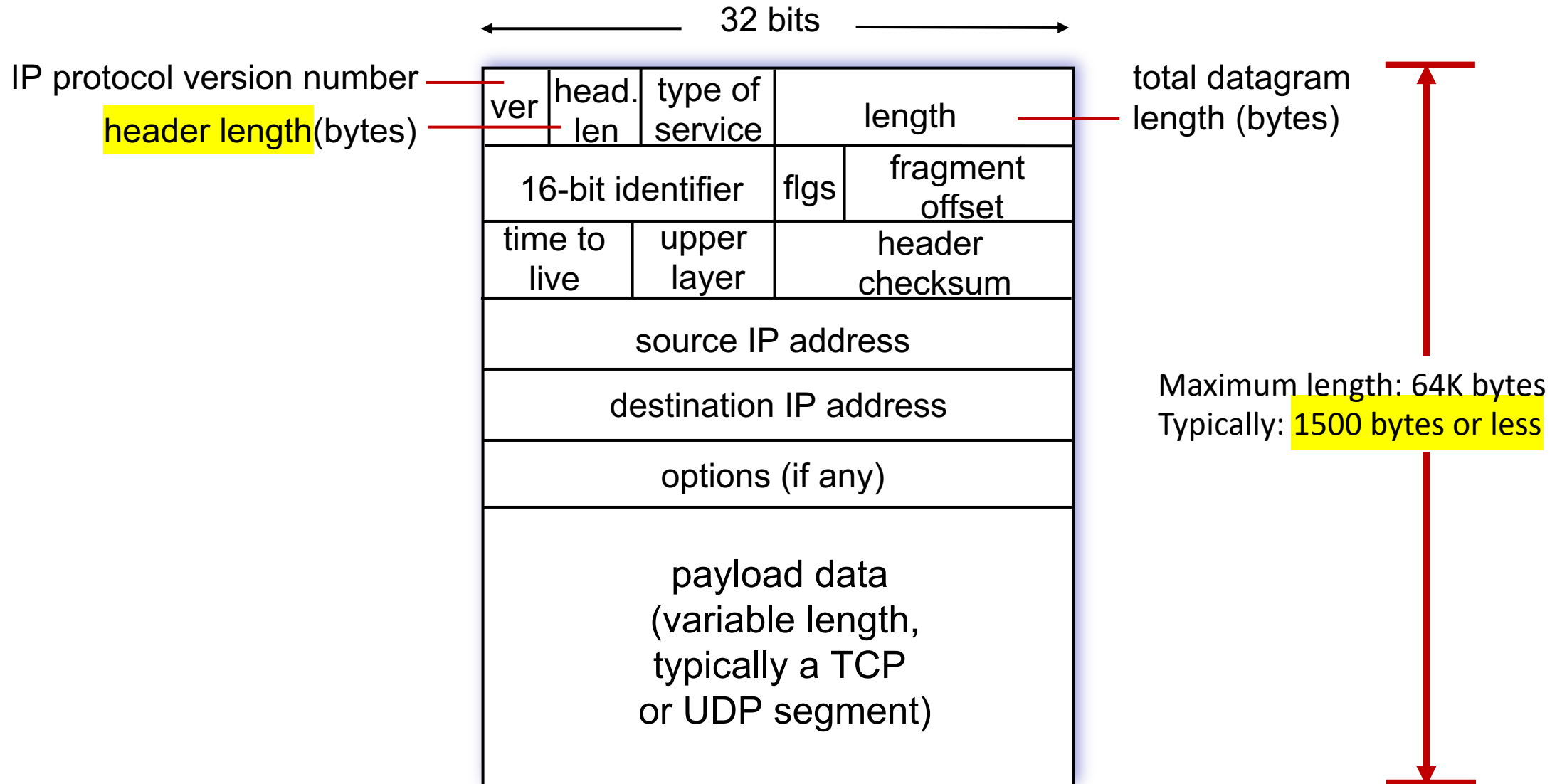
- Livello di rete: panoramica
  - piano dati
  - piano di controllo
- Dentro i router
  - porte di ingresso, commutazione, porte di uscita
  - gestione del buffer, scheduling
- IP: il protocollo Internet
  - formato datagramma
  - indirizzamento
  - NAT: traduzione di indirizzi di rete
  - IPv6
- Forwarding generalizzato, SDN
  - Match+action
  - OpenFlow: incontro+azione in azione
- Middleboxes

# Network Layer: Internet

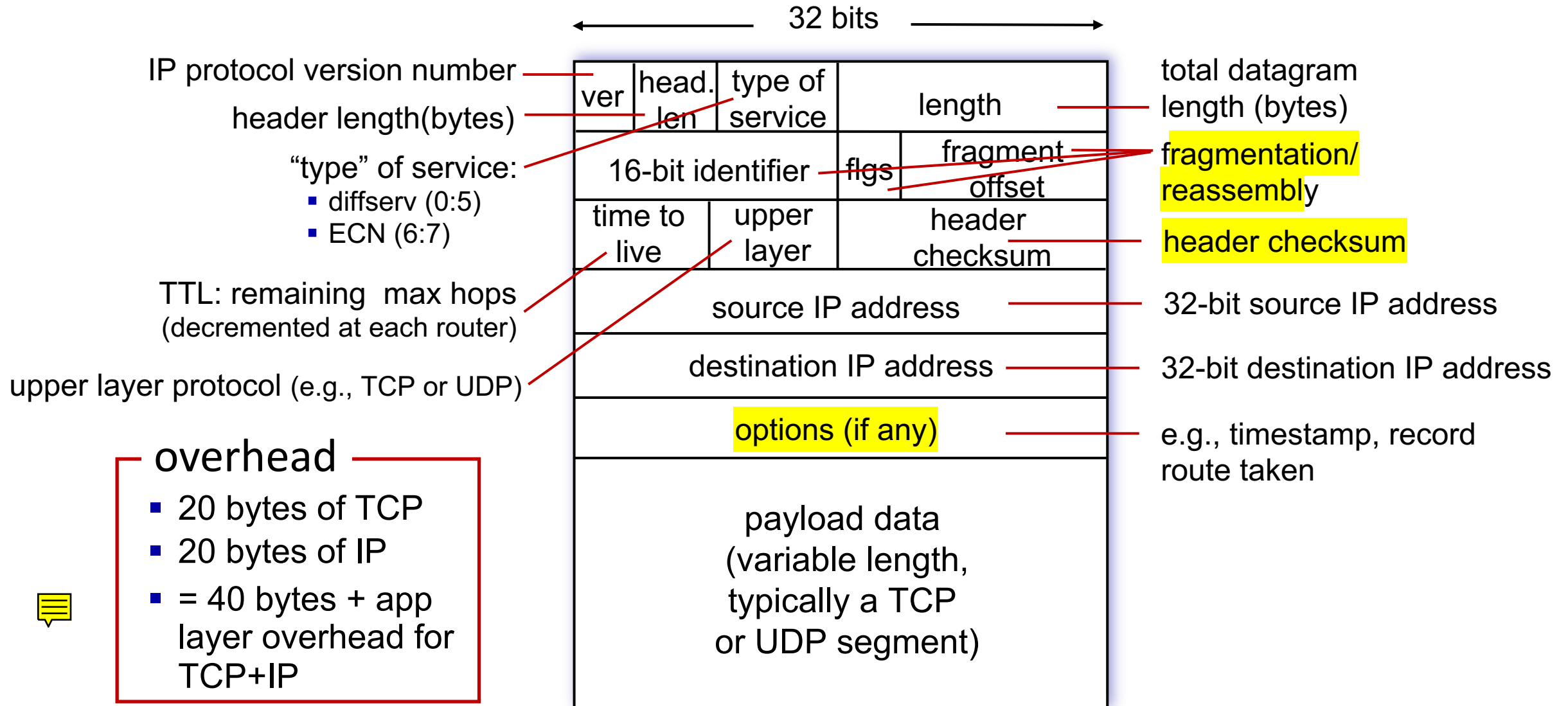
funzioni del livello di rete di router e host:



# formato del datagramma IP

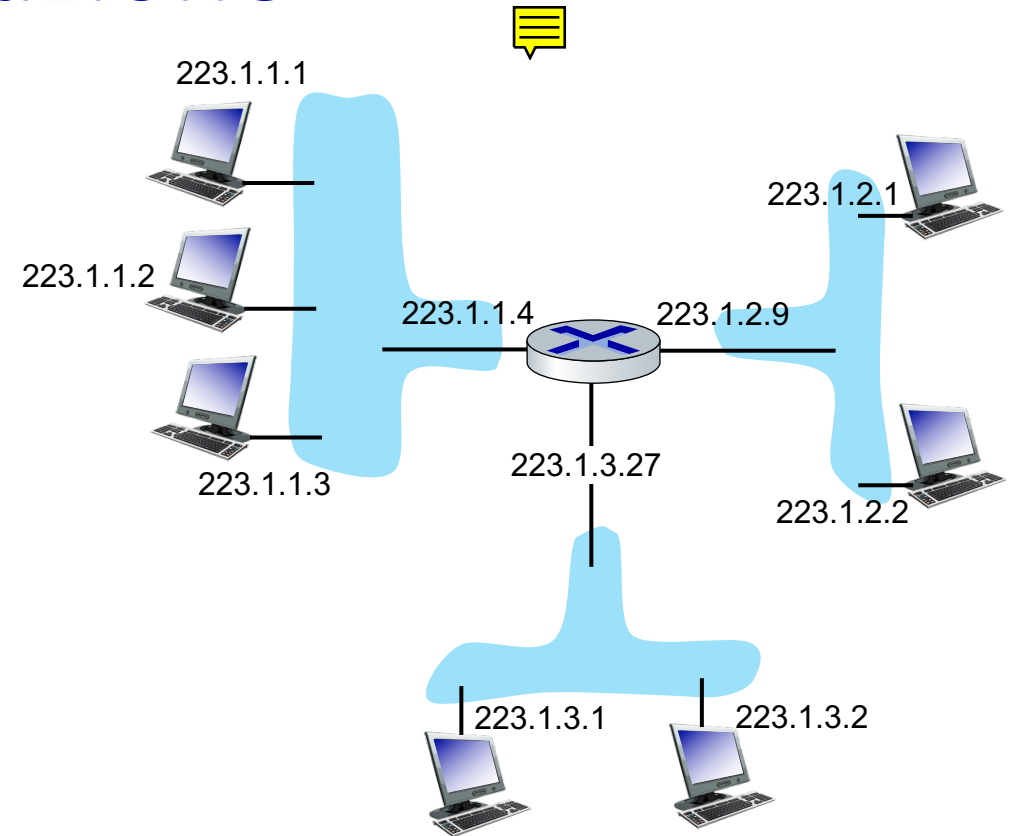


# formato del datagramma IP



# Indirizzamento IP: introduzione

- **Indirizzo IP:** Identificatore a 32 bit associato a ciascuna *interfaccia dell'host o router*
- **interfaccia:** connessione tra host/router e collegamento fisico
  - router in genere hanno più interfacce
  - l'host in genere ha una o due interfacce (ad es. Ethernet cablata, wireless 802.11)



notazione IP decimale puntata:

223.1.1.1 = 11011111 00000001 00000001 00000001

223      1      1      1

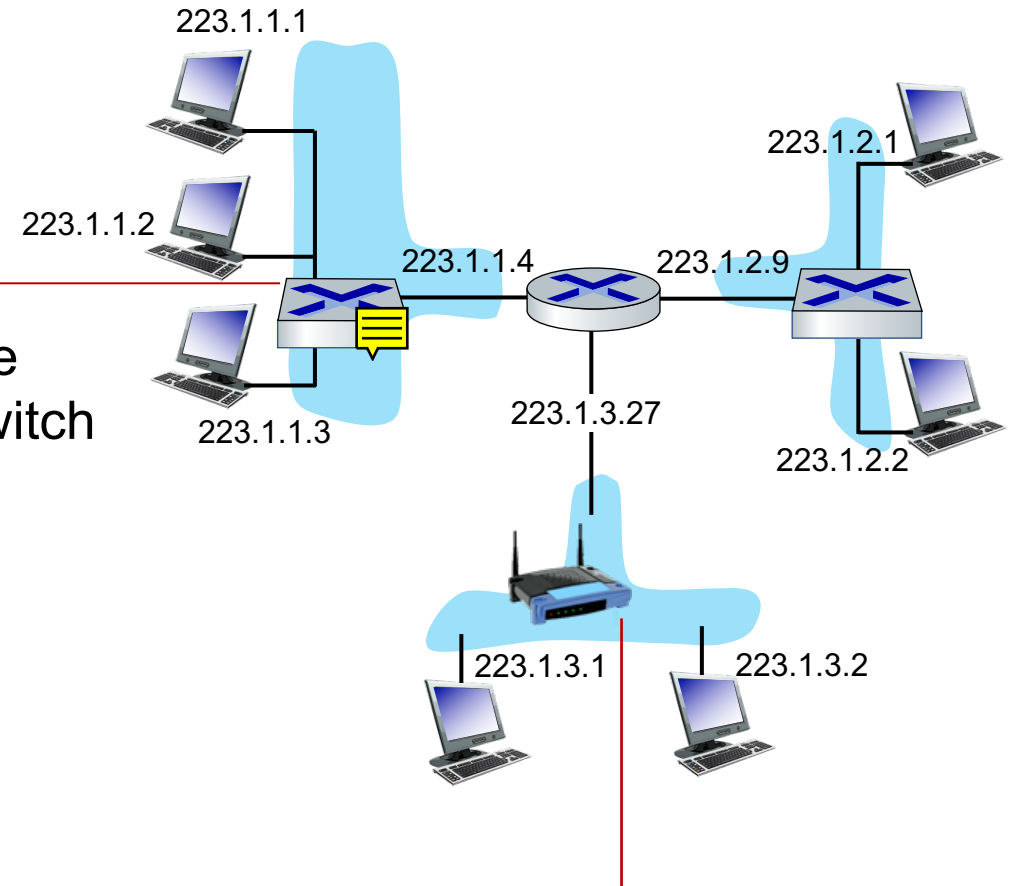
# Indirizzamento IP: introduzione

**D:** Come si connettono le interfacce?

**R:** livello di collegamento e fisico

*Per ora:* non dobbiamo preoccuparci di come un'interfaccia è connessa a un'altra

**R:** interfacce Ethernet cablate connesse da switch Ethernet



**R:** Interfacce WiFi connesse da base station WiFi

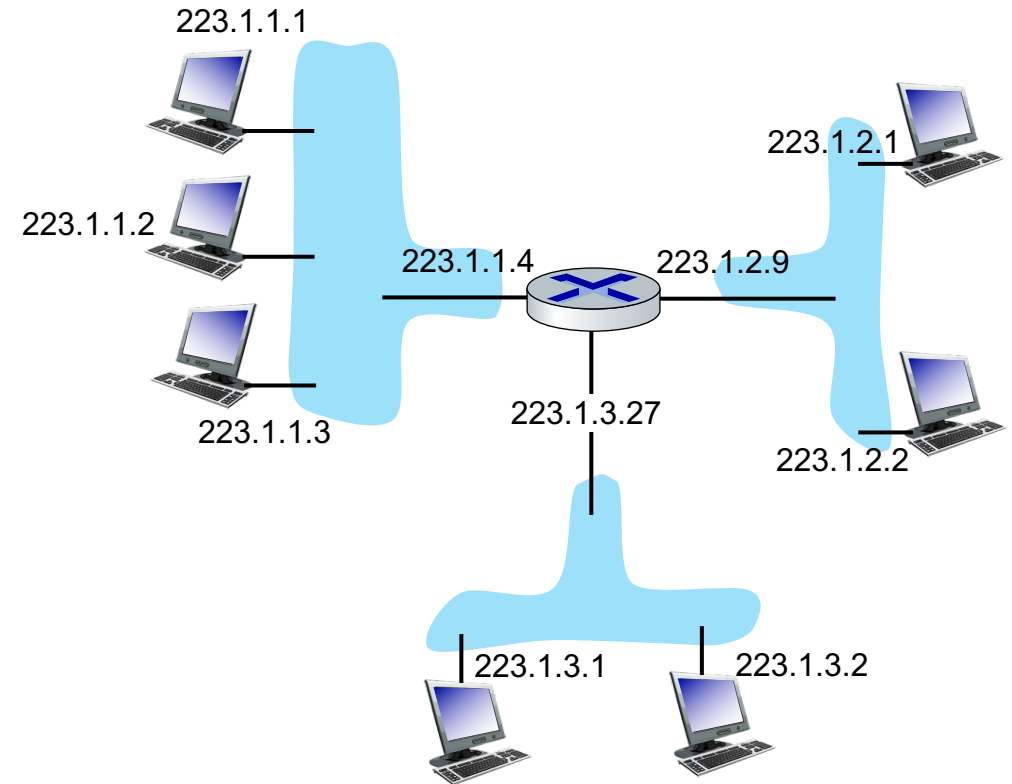
# Sottoreti

## ■ *Cos'è una sottorete?*

- interfacce di dispositivi che possono raggiungersi fisicamente l'un l'altro **senza passare attraverso un router (layer di rete) intermedio**

## ■ Gli indirizzi IP hanno:

- **parte sottorete:** i dispositivi nella stessa sottorete hanno bit più significativi in comune
- **parte host:** bit meno significativi rimanenti



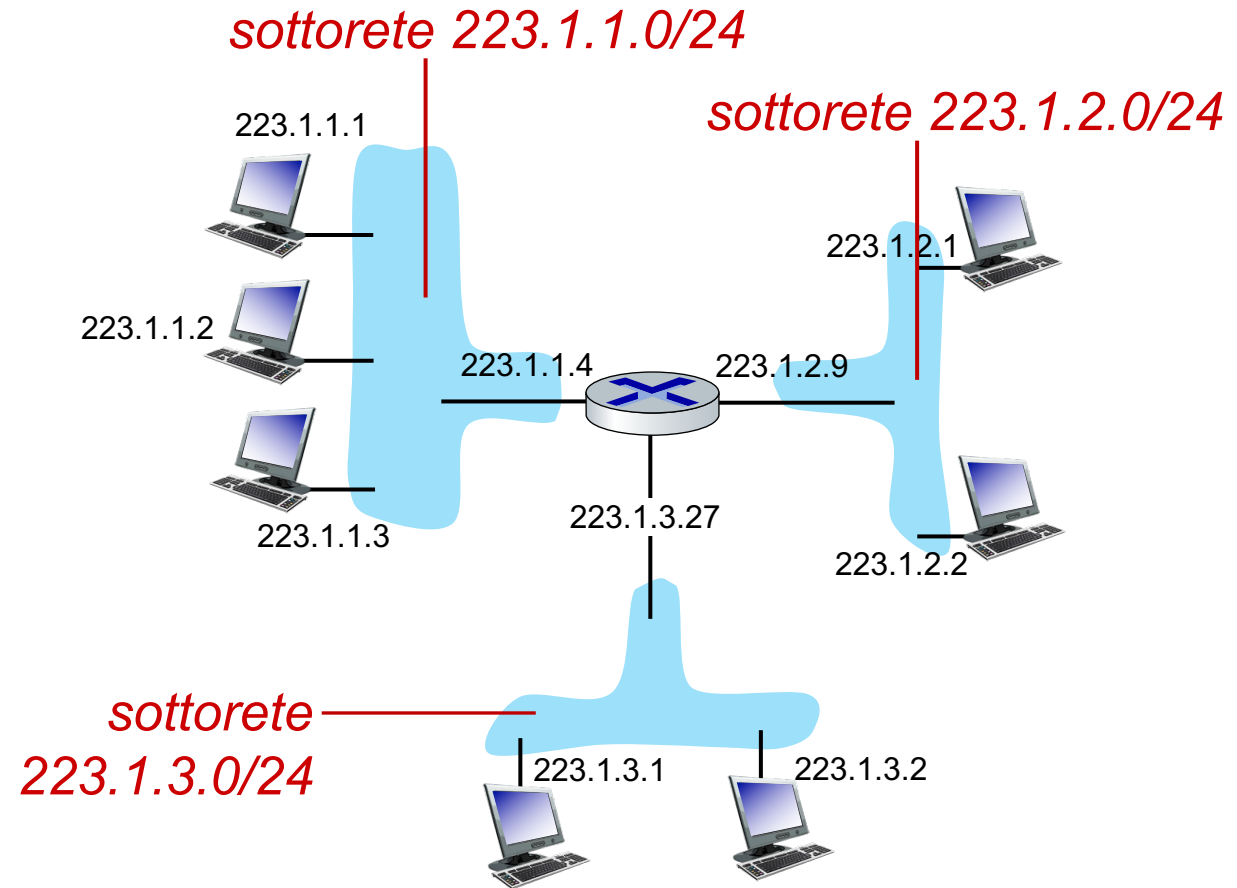
rete composta da 3 sottoreti



# Sottoreti

## *Ricetta per definire le sottoreti:*

- stacca ogni interfaccia dal suo host o router, creando “isole” di reti isolate
- ogni rete isolata è chiamata *sottorete*

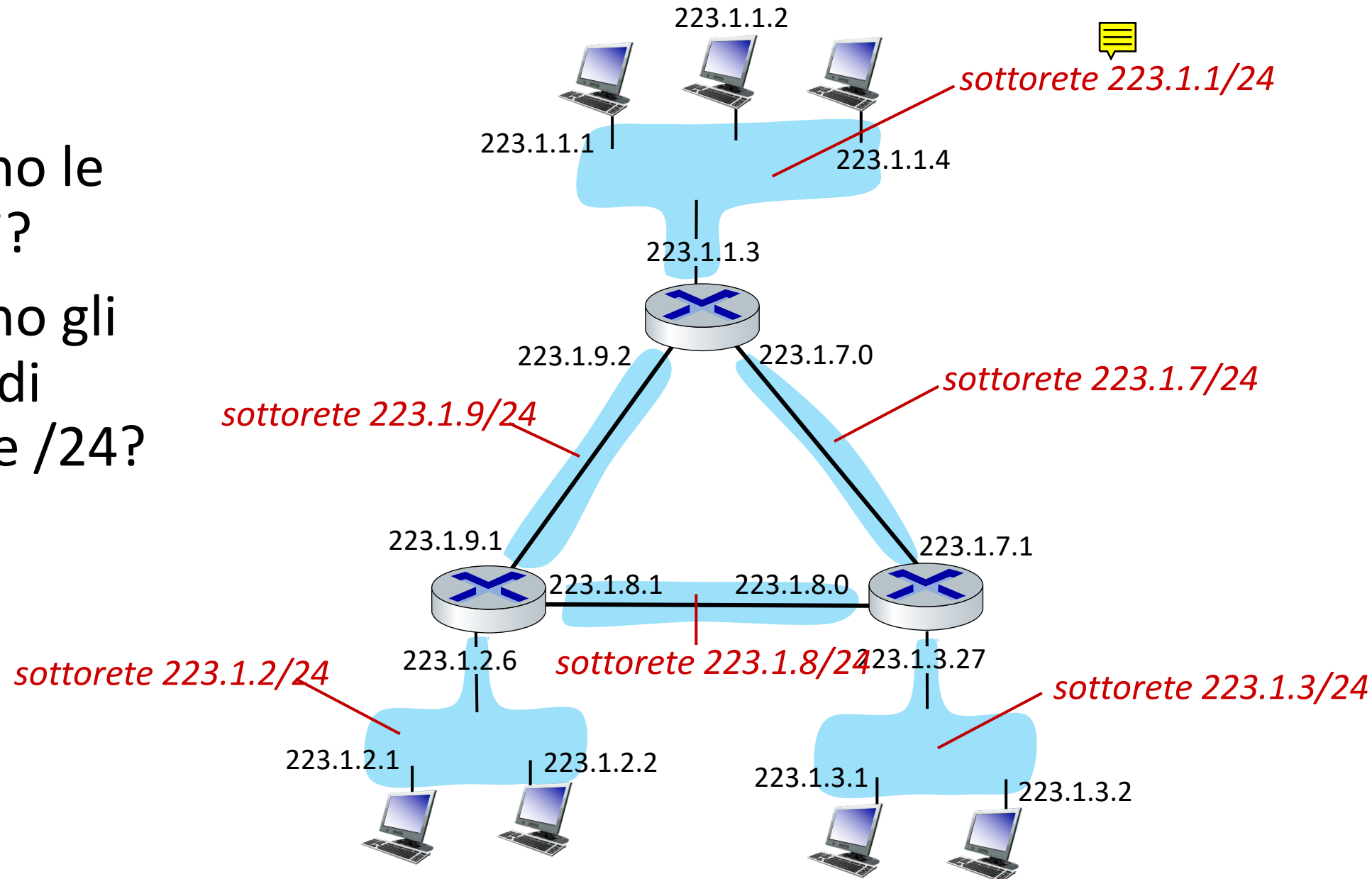


subnet mask: /24

(24 MSB bit: parte della sottorete dell'indirizzo IP)

# Sottoreti

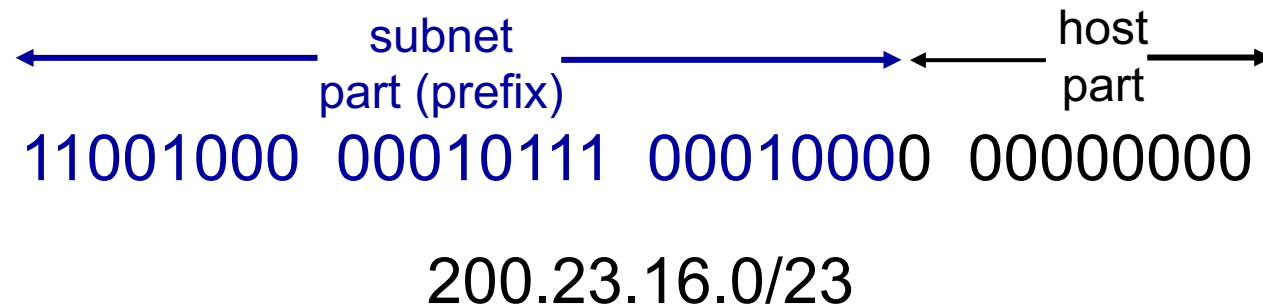
- dove sono le sottoreti?
- quali sono gli indirizzi di sottorete /24?



# Indirizzamento IP: CIDR

**CIDR: Classless Inter Domain Routing** (pronunciato “cider”)

- porzione di sottorete dell'indirizzo di lunghezza arbitraria
- formato dell'indirizzo (ciderized): **a.b.c.d/x** , dove x è il numero di bit nella porzione subnet dell'indirizzo



# Indirizzi IP: come ottenerne uno?

In realtà sono **due** domande:

1. D: In che modo un *host* ottiene l'indirizzo IP all'interno della sua rete (parte **host** dell'indirizzo)?
2. D: In che modo una *rete* ottiene l'indirizzo IP per se stessa (parte subnet dell'indirizzo)

In che modo *l'host* ottiene l'indirizzo IP?

- **hardcoded da sysadmin** nel file di configurazione (ad esempio, /etc/rc.config in UNIX)
- **DHCP: Dynamic Host Configuration Protocol** : ottiene dinamicamente l'indirizzo da un server
  - "plug-and-play" o zeroconf

# DHCP: Dynamic Host Configuration Protocol

**obiettivo:** l'host ottiene *dinamicamente* l'indirizzo IP dal server di rete quando si unisce alla rete

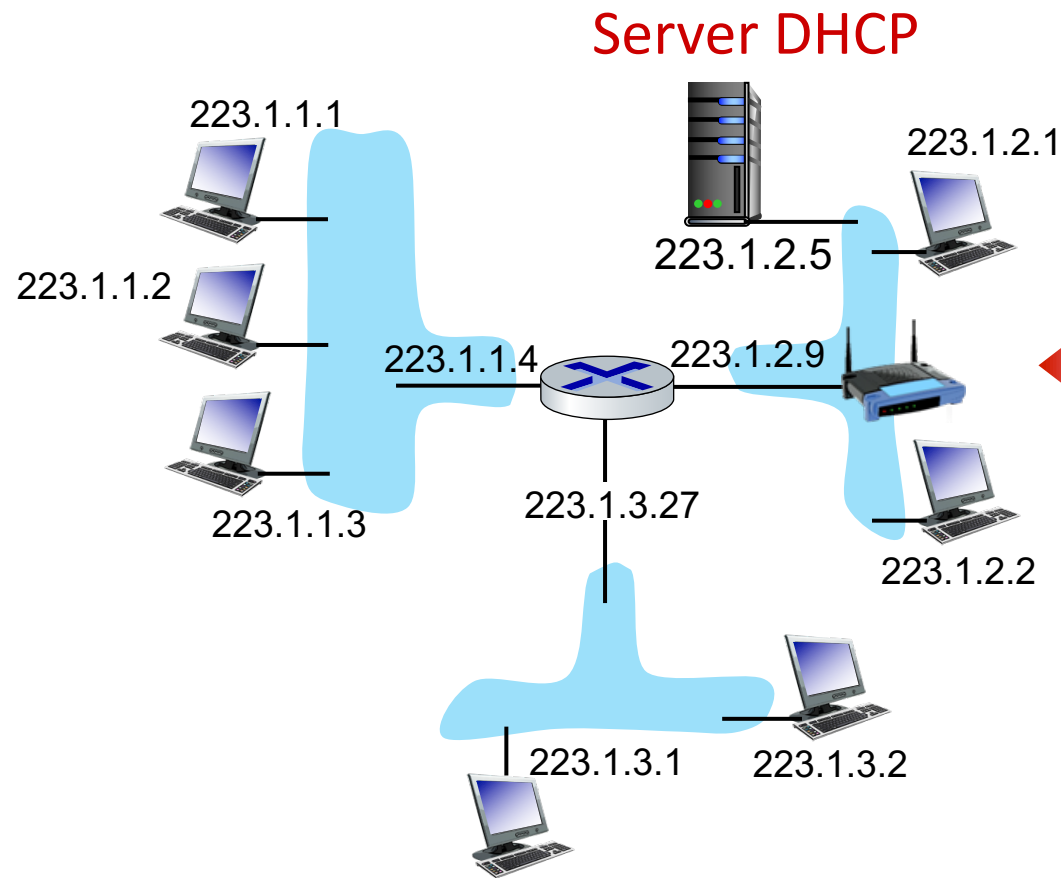
- può rinnovare il suo lease (presa in prestito) con l'indirizzo in uso
- consente il riutilizzo degli indirizzi (mantieni l'indirizzo solo mentre sei connesso/acceso)
- supporto per gli utenti mobili che entrano/escono dalla rete

## Panoramica DHCP:

- l'host trasmette **DHCP discover** msg [opzionale]
- Il server DHCP risponde con un messaggio di **DHCP offer** [opzionale]
- l'host richiede l'indirizzo IP: msg **DHCP request**
- Il server DHCP invia l'indirizzo: **DHCP ack** msg



# Scenario client-server DHCP

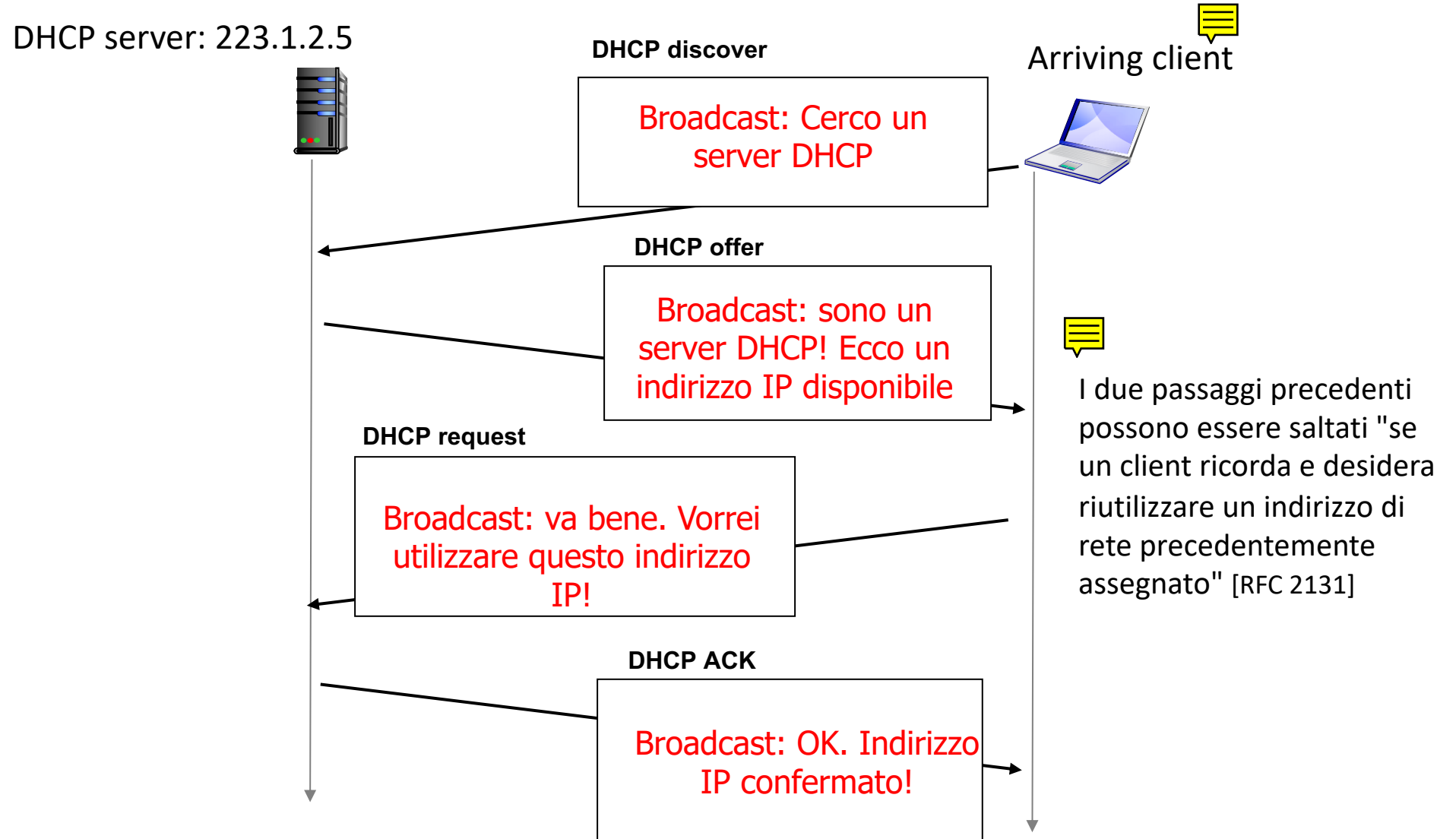


In genere, il server DHCP sarà collocato nel router, al servizio di tutte le sottoreti a cui è collegato il router



**client DHCP** in arrivo  
necessita di un  
indirizzo in questa rete

# Scenario client-server DHCP



# DHCP: Non bastano gli indirizzi IP

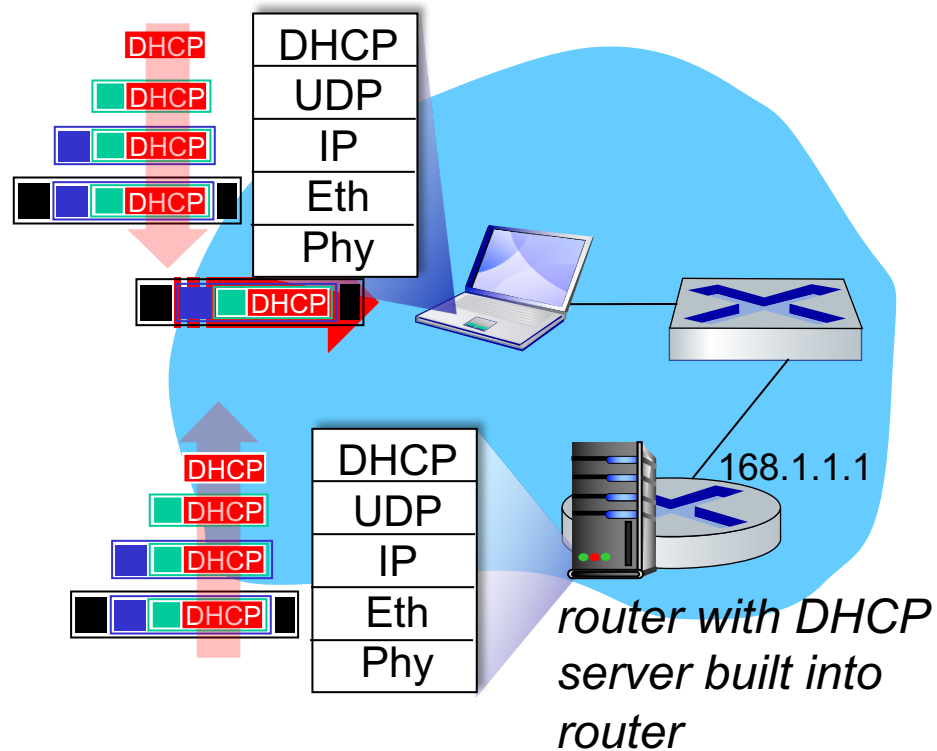
DHCP può restituire più di un semplice indirizzo IP assegnato sulla sottorete:

- indirizzo del router first-hop per il client (gateway)
- nome e indirizzo IP del server DNS
- maschera di rete/subnet mask (che indica la parte dell'indirizzo relativa alla sottorete)



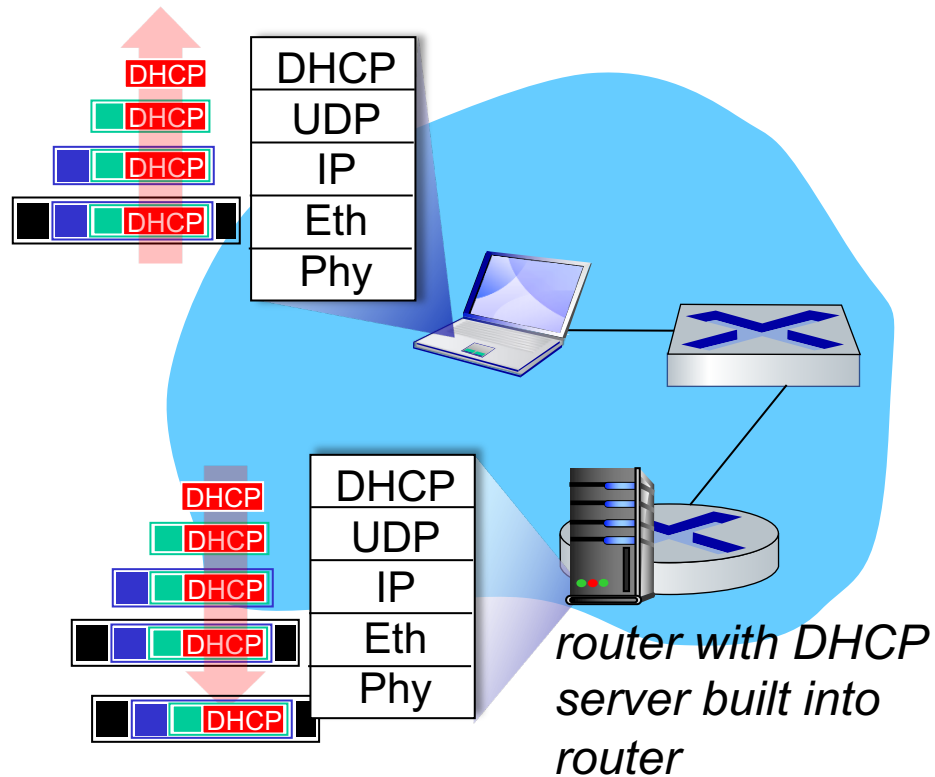


# DHCP: esempio



- il laptop utilizzerà DHCP per ottenere l'indirizzo IP, l'indirizzo del router first-hop, l'indirizzo del server DNS.
- Messaggio DHCP REQUEST incapsulato in UDP, incapsulato in IP, incapsulato in Ethernet
- Trasmissione frame Ethernet (dest: FFFFFFFF) su LAN, ricevuta dal router sul quale gira il server DHCP
- Demux Ethernet -> IP -> UDP -> DHCP

# DHCP: esempio



- il server DHCP prepara l'ACK DHCP contenente l'indirizzo IP del client , l'indirizzo IP del router first-hop per il client, il nome e l'indirizzo IP del server DNS
- La risposta DHCP del server incapsulata viene inoltrata al client, e poi demultiplata fino a DHCP lato client
- il client ora conosce il suo indirizzo IP, il nome e l'indirizzo IP del server DNS, l'indirizzo IP del suo router first-hop

# Indirizzi IP: come ottenerne uno?

*D:* in che modo la *rete* ottiene la parte della sottorete dell'indirizzo IP?

*R: l'ISP alloca una porzione del suo* spazio degli indirizzi

Blocco ISP 11001000 00010111 0001 0000 00000000 200.23.16.0/20

L'ISP può quindi allocare il suo spazio di indirizzi in 8 blocchi:

Organizzazione 0 11001000 00010111 0001000 0 00000000 200.23.16.0/23

Organizzazione 1 11001000 00010111 0001001 0 00000000 200.23.18.0/23

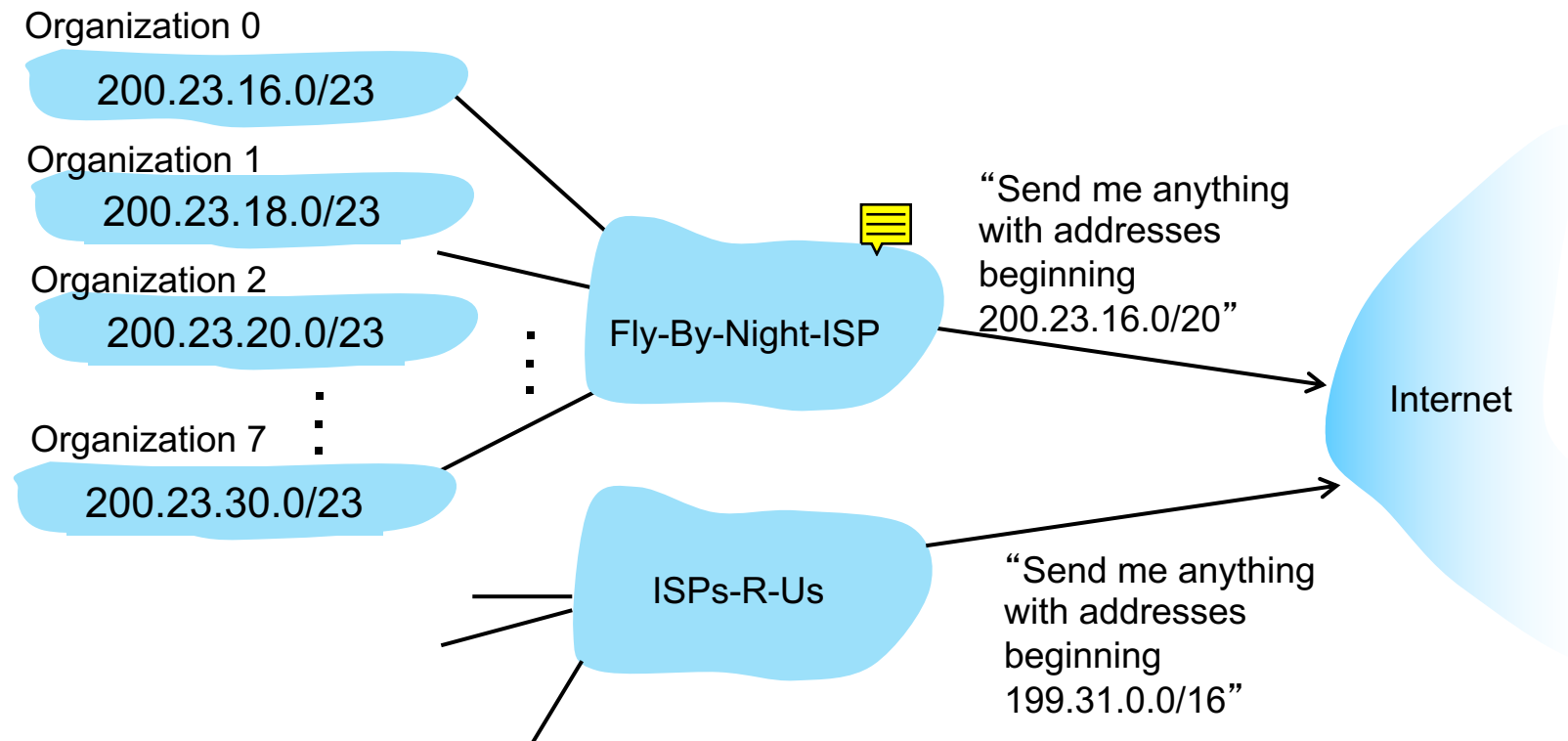
Organizzazione 2 11001000 00010111 0001010 0 00000000 200.23.20.0/23

... ..

Organizzazione 7 11001000 00010111 0001111 0 00000000 200.23.30.0/23

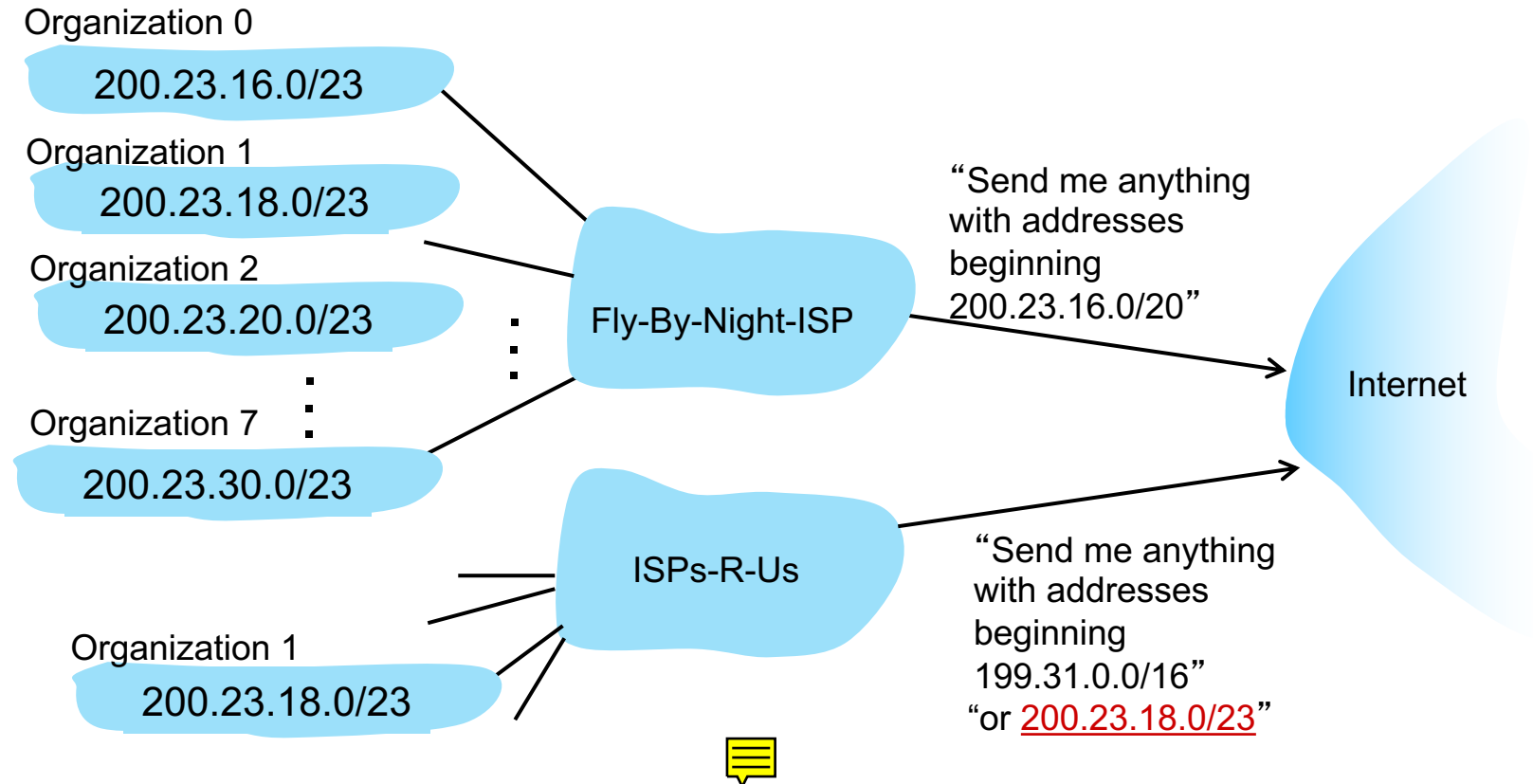
# Indirizzamento gerarchico: route aggregation

l'indirizzamento gerarchico consente la pubblicazione (advertise) efficiente delle informazioni di instradamento:



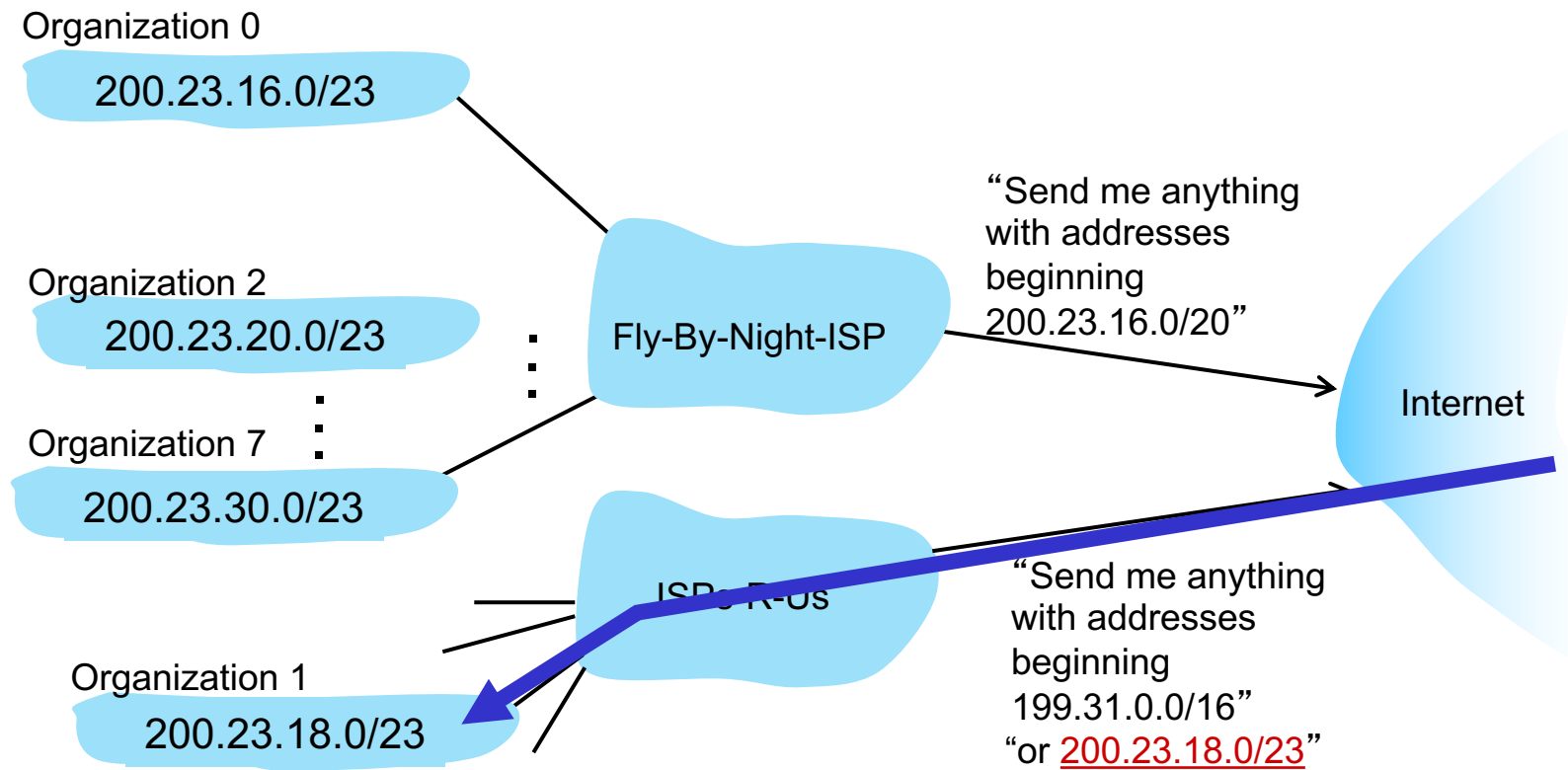
# Indirizzamento gerarchico: percorsi più specifici

- L'organizzazione 1 passa da Fly-By-Night-ISP a ISPs-R-Us
- ISPs-R-Us ora pubblica (advertise) un percorso più specifico per l'organizzazione 1



# Indirizzamento gerarchico: percorsi più specifici

- L'organizzazione 1 passa da Fly-By-Night-ISP a ISPs-R-Us
- ISPs-R-Us ora pubblica (advertise) un percorso più specifico per l'organizzazione 1



# Indirizzamento IP: blocco per ISP

**D:** come fa un ISP a ottenere un blocco di indirizzi?

**R:** ICANN: Internet Corporation for Assigned Names and Numbers  
<http://www.icann.org/>

- alloca gli indirizzi IP, attraverso 5 registri regionali (RR) (che possono quindi allocare ai registri locali)
- gestisce la zona radice DNS, inclusa la delega della gestione dei singoli TLD (.com, .edu, ...).

**D:** ci sono abbastanza indirizzi IP a 32 bit?

- L'ICANN ha assegnato l'ultima parte degli indirizzi IPv4 agli RR nel 2011
- NAT (successivo) aiuta l'esaurimento dello spazio degli indirizzi IPv4
- IPv6 ha uno spazio degli indirizzi a 128 bit


"Chi diavolo sapeva di quanto spazio di indirizzi avremmo avuto bisogno?" Vint Cerf (riflettendo sulla decisione di rendere l'indirizzo IPv4 lungo 32 bit)

# Perchè la maschera?

- Maschera dell'indirizzo: numero composto da 32 bit in cui i primi  $n$  bit a sinistra sono impostati a 1 e il resto  $(32-n)$  a 0
- Può essere usata da un programma per calcolare in modo efficiente le informazioni di un blocco, usando solo tre operatori sui bit
- Il numero degli indirizzi del blocco è  $N = \text{NOT}(\text{maschera}) + 1$
- Il primo indirizzo del blocco = (qualsiasi indirizzo del blocco) AND (maschera)
- L'ultimo indirizzo del blocco = (qualsiasi indirizzo del blocco) OR (NOT (maschera))
- **match**: (indirizzo di destinazione) AND (maschera) =? subnet



# Indirizzi IP speciali

0 0	This host
0 0      ...      0 0      Host	A host on this network
1 1	Broadcast on the local network
Network      1 1 1 1      ...      1 1 1 1	Broadcast on a distant network 
127      (Anything)	Loopback

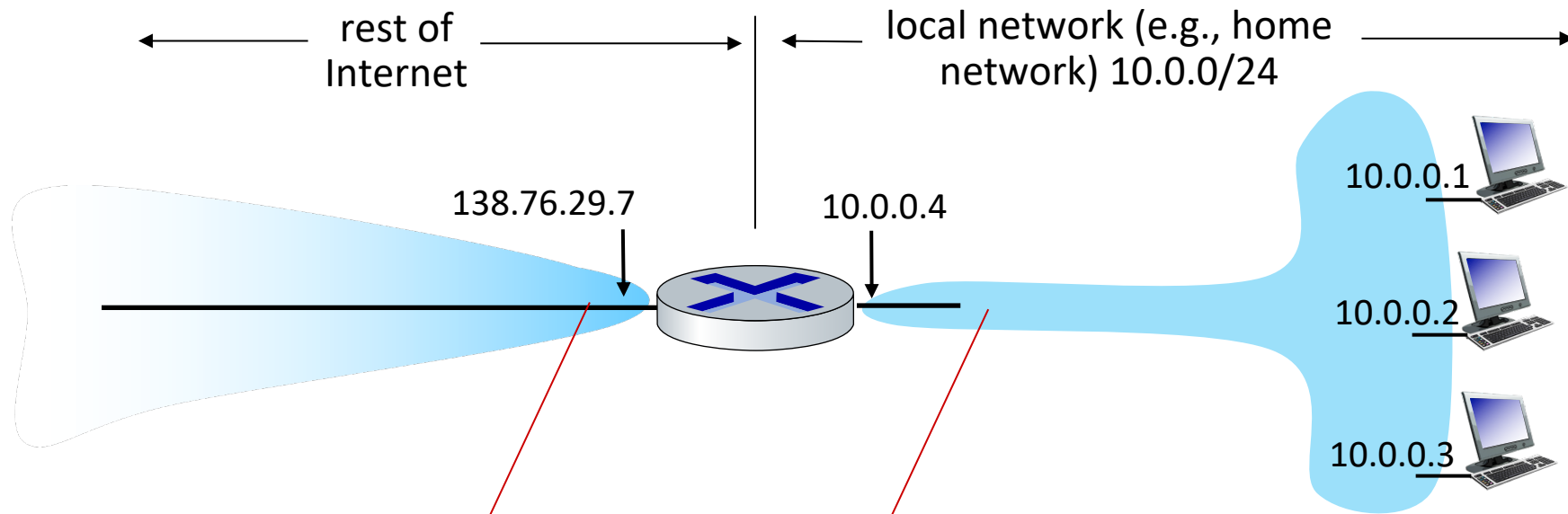
- L'indirizzo **0.0.0.0** è utilizzato dagli host al momento del boot (IP non ancora assegnato)
  - configurare un server in ascolto su 0.0.0.0/24 significa accettare tutti i pacchetti
- Gli indirizzi IP che hanno lo **0** come **numero di rete** si riferiscono alla sottorete corrente
- L'indirizzo composto da tutti 1 permette la trasmissione **broadcast** sulla rete locale (in genere una LAN)
- Gli indirizzi con numero di rete opportuno e tutti **1** nel campo **host** permettono l'invio di pacchetti broadcast a LAN distanti
- Gli indirizzi nella forma **127.xx.yy.zz** sono riservati al **loopback** (questi pacchetti non vengono immessi nel cavo ma elaborati localmente e trattati come pacchetti in arrivo)

# Livello di rete: sommario

- Livello di rete: panoramica
  - piano dati
  - piano di controllo
- Dentro i router
  - porte di ingresso, commutazione, porte di uscita
  - gestione del buffer, scheduling
- IP: il protocollo Internet
  - formato datagramma
  - indirizzamento
  - NAT: traduzione di indirizzi di rete
  - IPv6
- Forwarding generalizzato, SDN
  - Match+action
  - OpenFlow: incontro+azione in azione
- Middleboxes

# NAT: network address translation

**NAT:** tutti i dispositivi nella subnet condividono **un solo indirizzo IPv4** per quanto concerne il mondo esterno



*Tutto i* datagrammi *che escono* dalla rete locale hanno lo *stesso* indirizzo IP NAT di origine: 138.76.29.7, ma *diversi* numeri di porta di origine

i datagrammi con sorgente o destinazione in questa rete hanno indirizzo 10.0.0/24 per sorgente e destinazione (come prima)

# NAT: network address translation

- tutti i dispositivi nella rete locale hanno indirizzi a 32 bit in uno spazio di indirizzi IP "privato" ( prefissi 10/8, 172.16/12, 192.168/16) che possono essere utilizzati solo nella rete locale
- vantaggi per questa rete locale:
  - **un** solo indirizzo IP dal provider ISP per *tutti i* dispositivi
  - può cambiare gli indirizzi dell'host nella rete locale senza avvisare il mondo esterno
  - può cambiare ISP senza cambiare gli indirizzi dei dispositivi nella rete locale
  - sicurezza: dispositivi all'interno della rete locale non direttamente indirizzabili/visibili dall'esterno

# NAT: network address translation

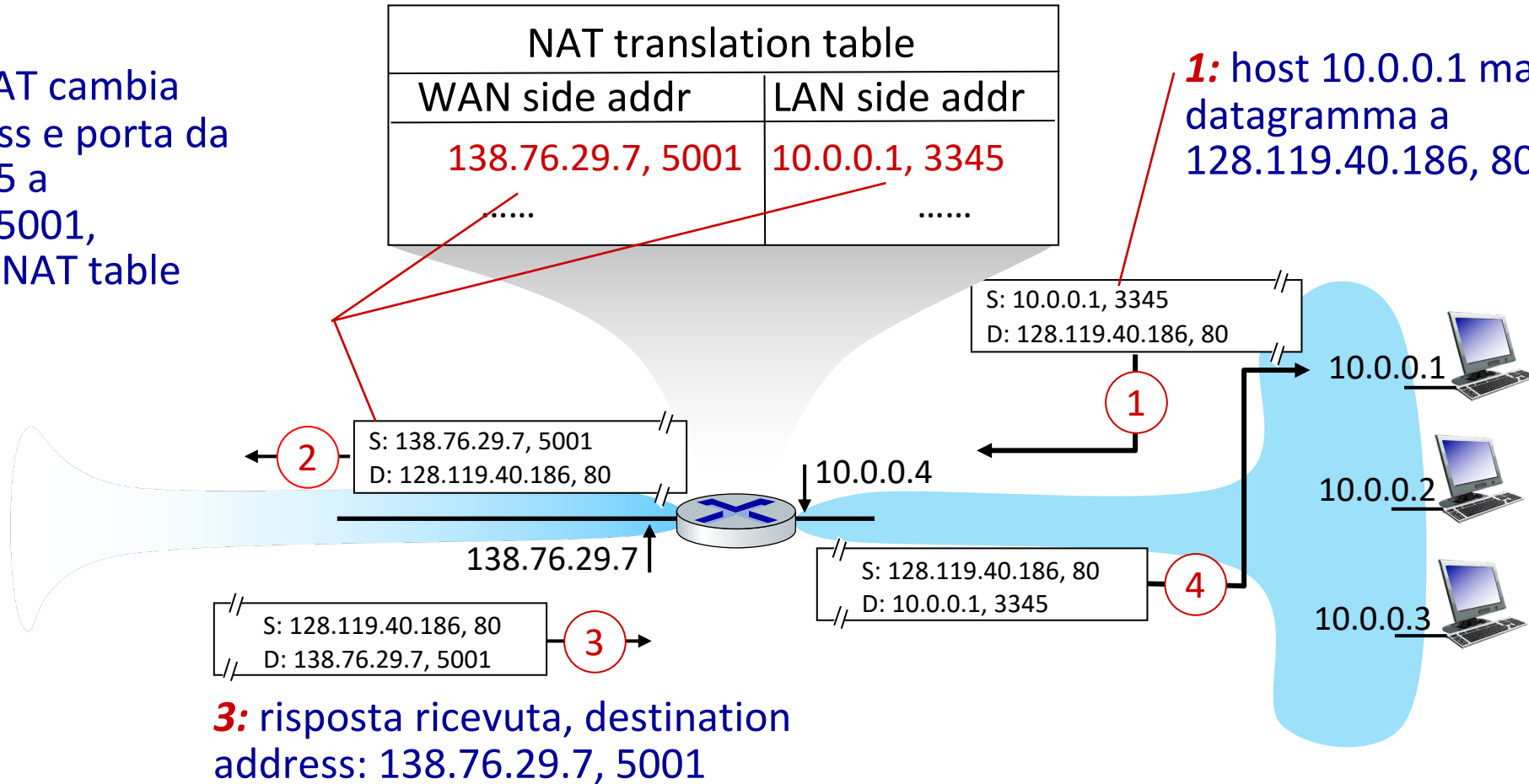
**implementazione:** il router NAT deve (in modo trasparente):

- **datagrammi in uscita:** sostituire <indirizzo IP di origine, numero di porta> di ogni datagramma in uscita con <indirizzo IP NAT, nuovo numero di porta>
  - i client/server remoti risponderanno utilizzando <indirizzo IP NAT, nuovo numero di porta> come indirizzo di destinazione
- **ricordare (nella tabella di traduzione NAT)** ogni coppia di conversione da <indirizzo IP di origine, numero di porta> a <indirizzo IP NAT, nuovo numero di porta>.
- **datagrammi in arrivo:** sostituire <indirizzo IP NAT, nuovo numero di porta> nei campi di destinazione di ogni datagramma in arrivo con il corrispondente <indirizzo IP di origine, numero di porta> memorizzato nella tabella NAT

# NAT: network address translation

**2:** Il router NAT cambia source address e porta da 10.0.0.1, 3345 a 138.76.29.7, 5001, e aggiorna la NAT table

**1:** host 10.0.0.1 manda il datagramma a 128.119.40.186, 80



# NAT: network address translation

- NAT è stato controverso:
  - i router "dovrebbero" processare solo pacchetto fino al livello di rete
  - la "carenza" di indirizzi dovrebbe essere risolta da IPv6
  - viola l'argomento end-to-end (manipolazione del numero di porta da parte del dispositivo a livello di rete)
  - NAT traversal: cosa succede se il client desidera connettersi a un server dietro NAT?
- ma NAT è qui per restare:
  - ampiamente utilizzato in reti domestiche e istituzionali, reti cellulari 4G/5G

# IPv6: motivazione

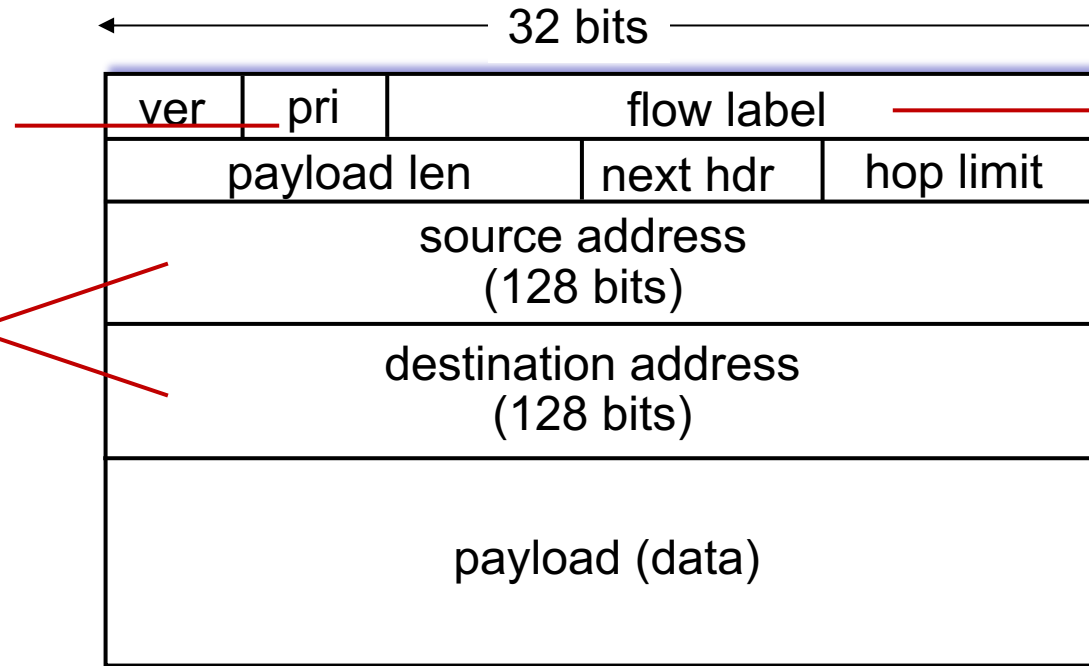
- **motivazione iniziale:** lo spazio degli indirizzi IPv4 a 32 bit sarebbe stato completamente allocato
- motivazione aggiuntiva:
  - velocità di elaborazione/inoltro: intestazione a lunghezza fissa di 40 byte, rimozione frammentazione e checksum
  - consentire un diverso trattamento dei "flussi" a livello di rete, concetto connessione tra endpoint nel pacchetto IP (flow label)
  - anycast: consegna a un qualsiasi host facente parte di un gruppo



# Formato datagramma IPv6

**priority:** livello di priorità del datagramma

**128-bit**  
IPv6 addresses



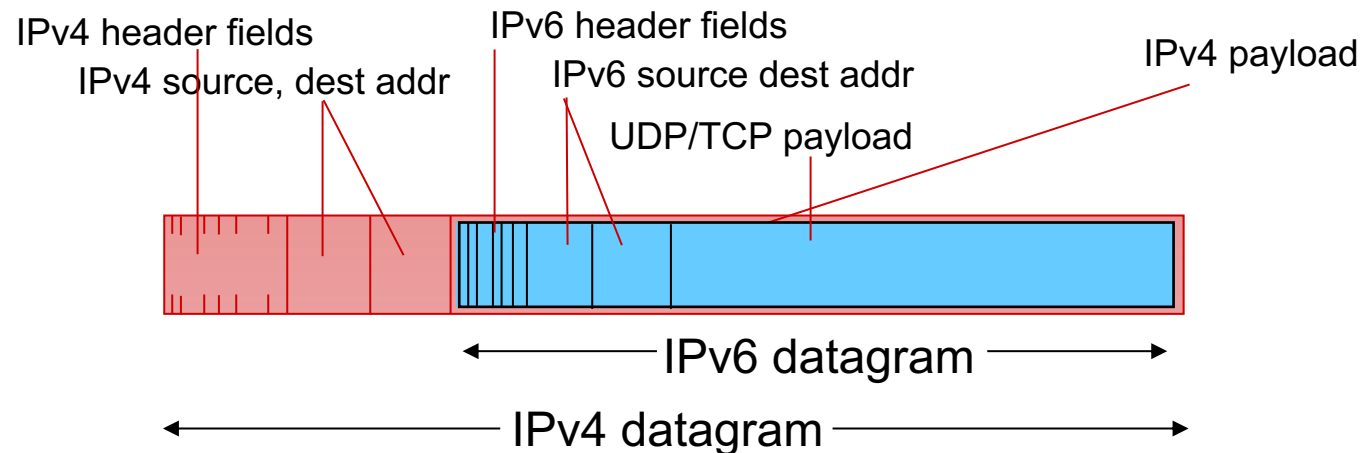
**flow label:** identifica datagrammi nello stesso flusso (concetto di flusso non definito)

Cosa manca (rispetto a IPv4):

- nessun checksum (per velocizzare l'elaborazione sui router)
- nessuna frammentazione/rimontaggio
- nessuna opzione (disponibile usando protocolli di livello superiore)

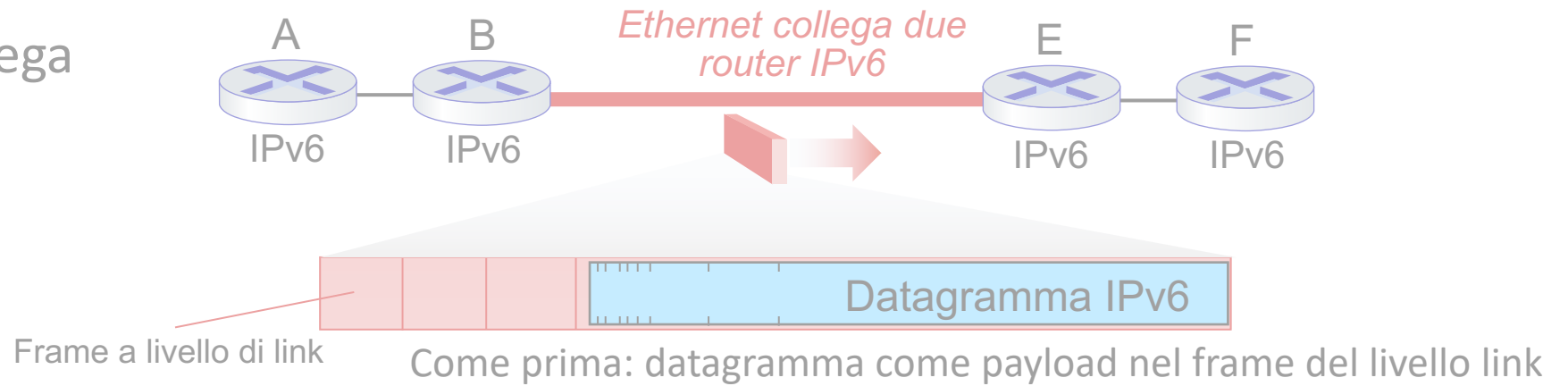
# Transizione da IPv4 a IPv6

- non tutti i router possono essere aggiornati contemporaneamente
  - non è stato deciso un "giorno di cambio" entro cui fare la transizione
  - come funzionerà la rete con router misti IPv4 e IPv6?
- **tunneling**: datagramma IPv6 trasportato come *payload* nel datagramma IPv4 tra router IPv4 ("pacchetto all'interno di un pacchetto")
  - tunneling ampiamente utilizzato in altri contesti (4G/5G)

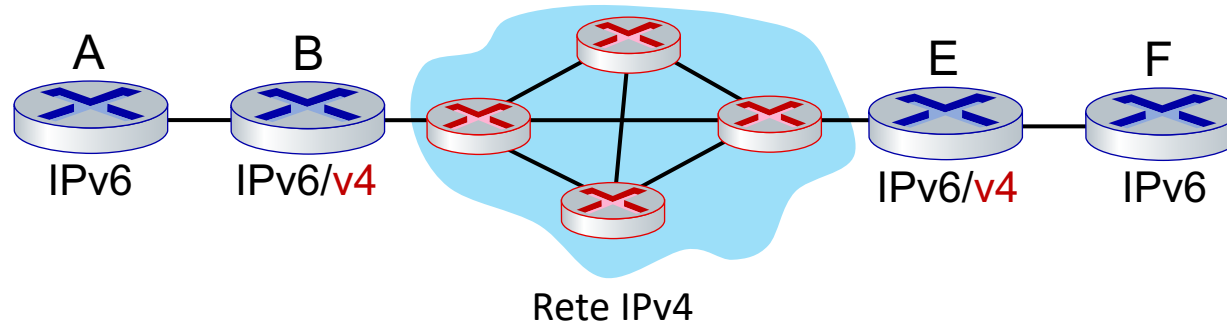


# Tunneling e incapsulamento

Ethernet che collega  
due router IPv6:

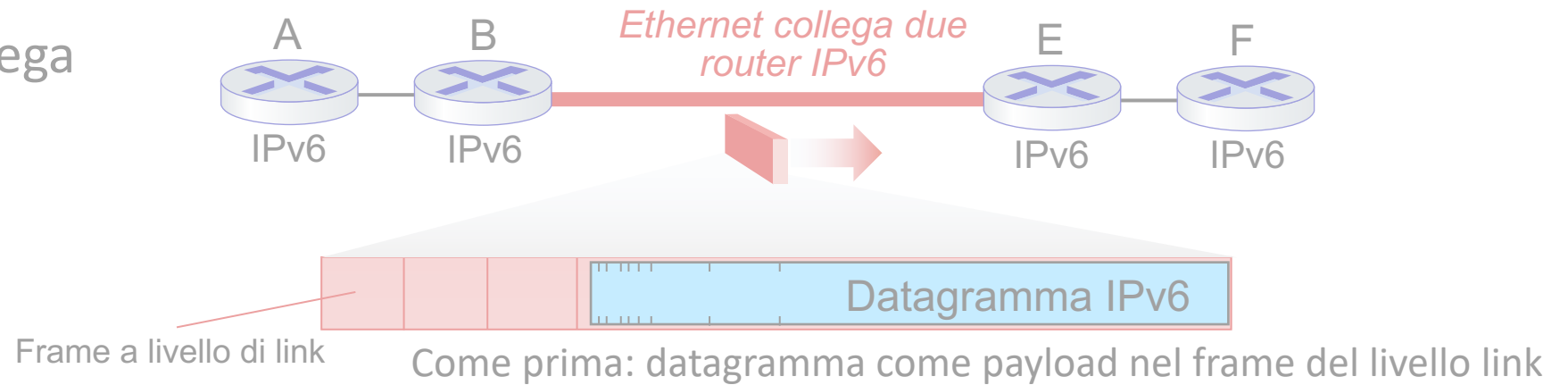


Rete IPv4 che  
collega due router  
IPv6

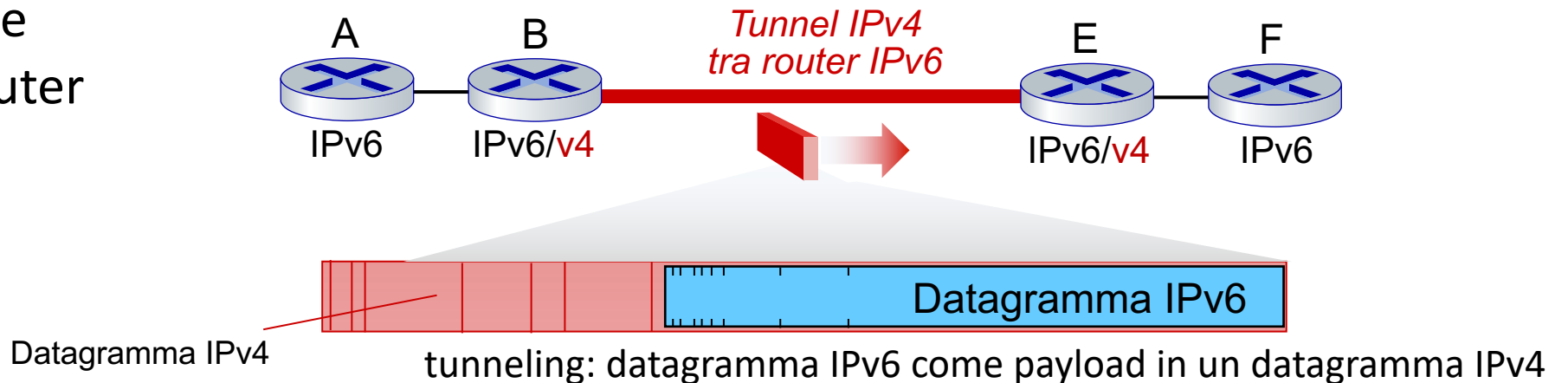


# Tunneling e incapsulamento

Ethernet che collega  
due router IPv6:



Tunnel IPv4 che  
collega due router  
IPv6

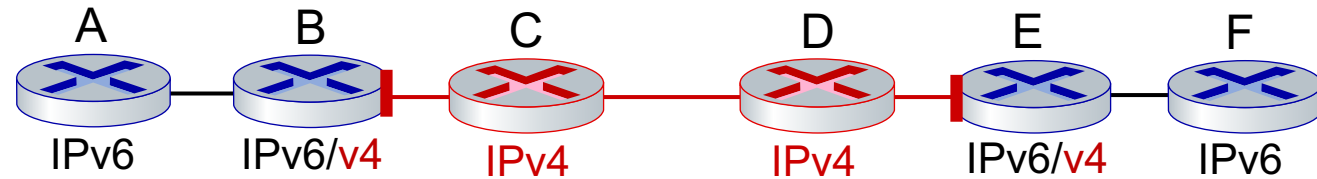


# Tunneling

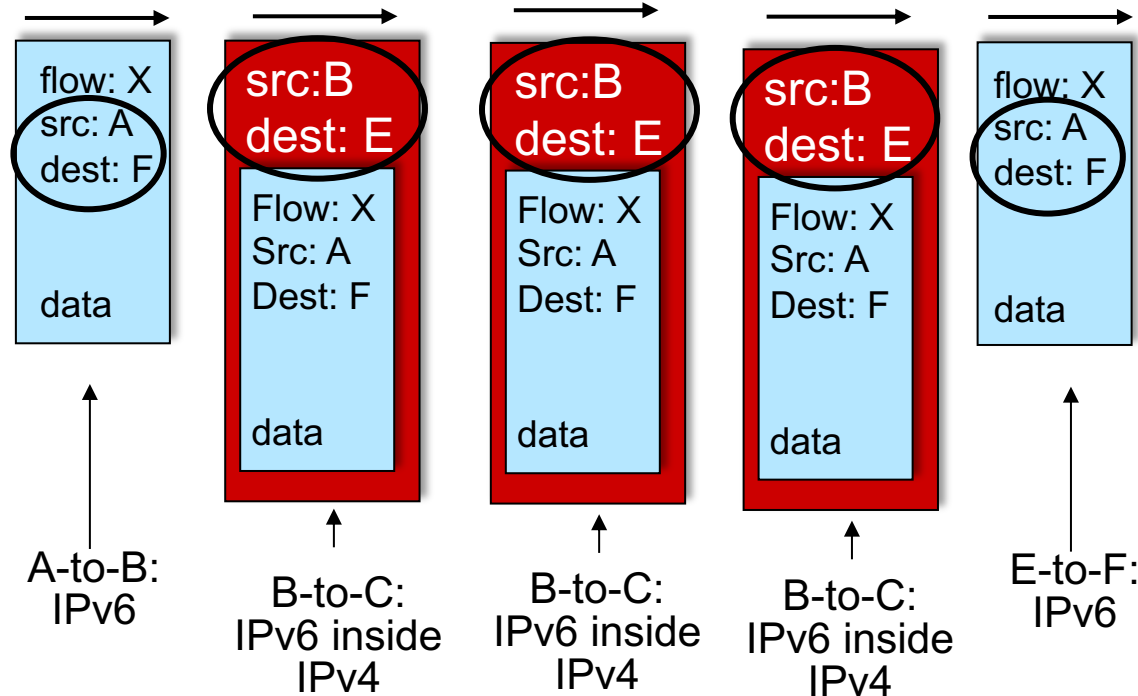
logical view:



physical view:



Nota gli indirizzi  
di sorgente e  
destinazione!

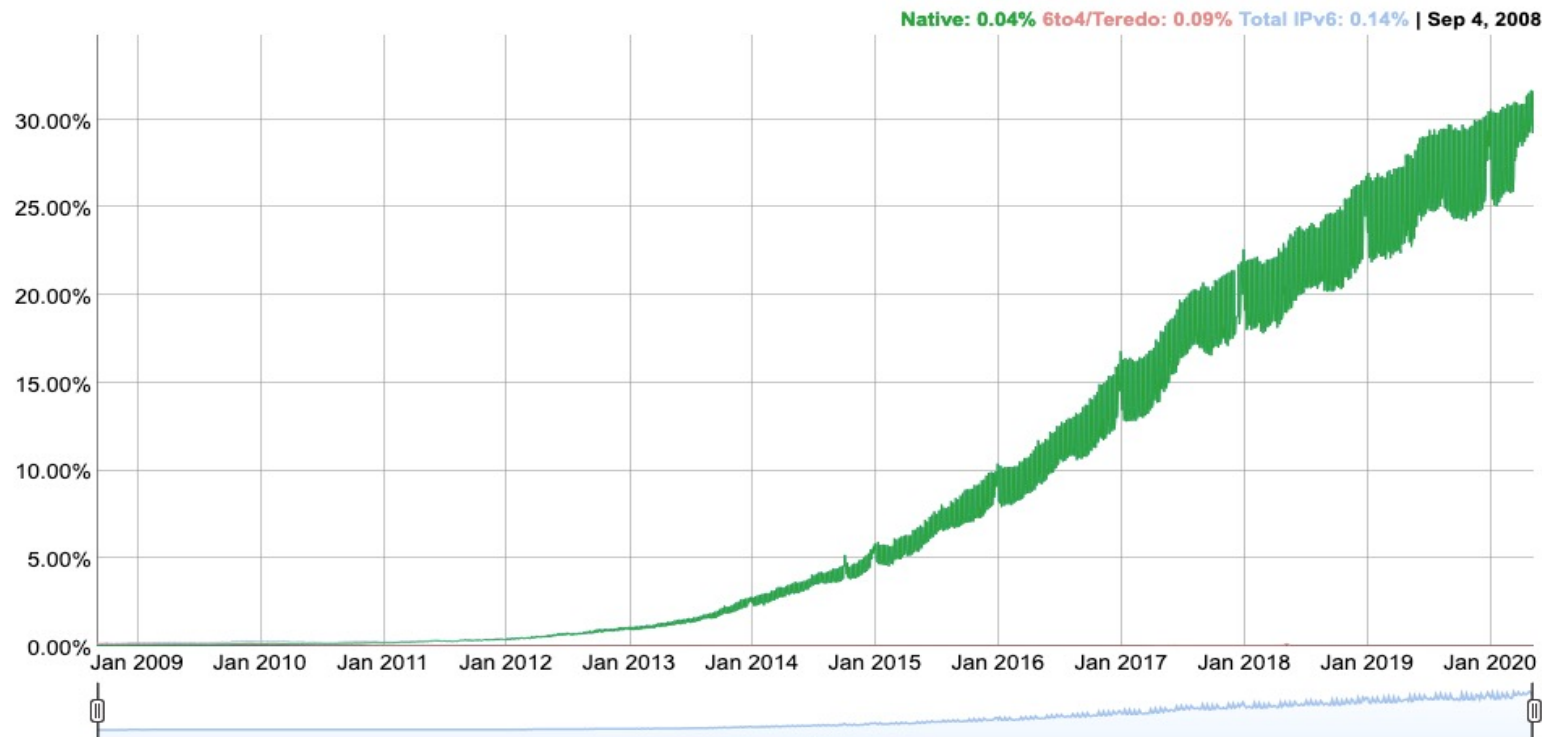


# IPv6: adozione

- Google<sup>1</sup> : ~ 30% dei clienti accede ai servizi tramite IPv6
- NIST: 1/3 di tutti i domini del governo degli Stati Uniti sono compatibili con IPv6

## IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



<sup>1</sup><https://www.google.com/intl/en/ipv6/statistics.html>

# IPv6: adozione

- Google<sup>1</sup> : ~30% dei clienti accede ai suoi servizi tramite IPv6
- NIST: 1/3 di tutti i domini del governo degli Stati Uniti sono compatibili con IPv6
- Tempo lungo (lungo!) per la distribuzione e l'uso
  - 25 anni e oltre!
  - Molto diverso rispetto ai cambiamenti a livello di applicazione negli ultimi 25 anni: WWW, social media, streaming media, giochi, telepresenza, ...
  - *Perché?*
    - *NAT ha reso l'adozione meno urgente*
    - *cambiamenti a livello di rete più costosi*
    - *cambiare fondamenta di una casa con gli abitanti ancora dentro*

<sup>1</sup><https://www.google.com/intl/en/ipv6/statistics.html>