Livello di Rete: Indirizzamento IPv4, DHCP, NAT, ICMP

Gaia Maselli
maselli@di.uniroma1.it

Livello di rete

Introduzione

Reti a circuito virtuale e a datagramma

Che cosa si trova all'interno di un router?

Protocollo Internet (IP)

- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6

Algoritmi di instradamento

- Stato del collegamento
- Vettore distanza
- Instradamento gerarchico

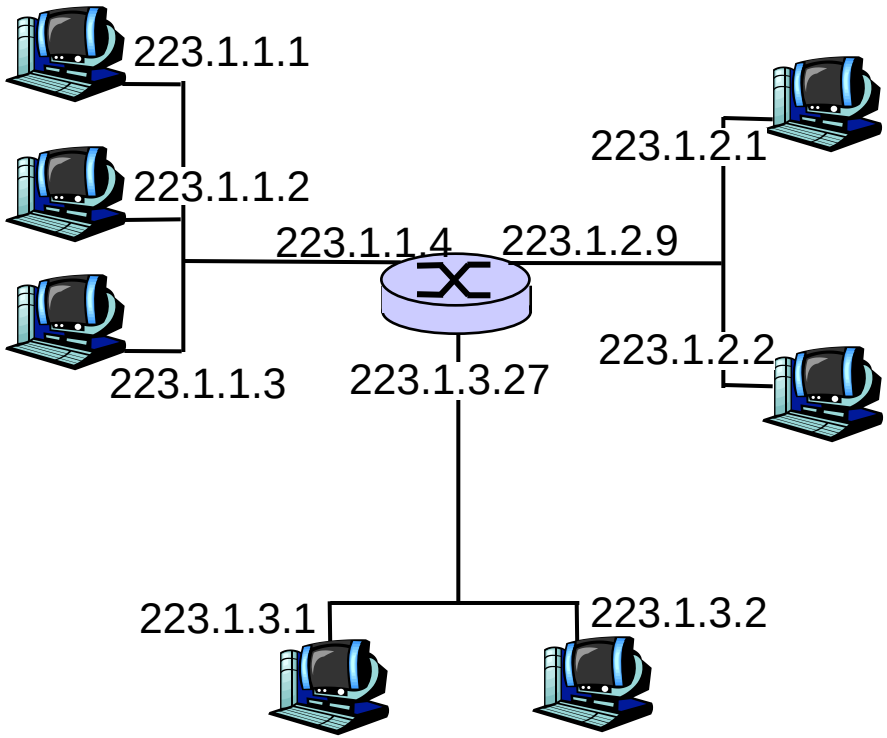
Instradamento in Internet

- RIP
- OSPF
- BGP

Instradamento broadcast e multicast

Indirizzamento IPv4

- Indirizzo IP:
  - 32 bit (4 byte) in notazione decimale puntata (ciascun byte dell'indirizzo viene indicato in forma decimale)
- Ogni **interfaccia** di host e router di Internet ha un indirizzo IP globalmente univoco a 32 bit.
- *Interfaccia:* è il confine tra host e collegamento fisico.
  - I router devono necessariamente essere connessi ad almeno due collegamenti.
  - Un host, in genere, ha un'interfaccia
  - A ciascuna interfaccia è associato un indirizzo IP

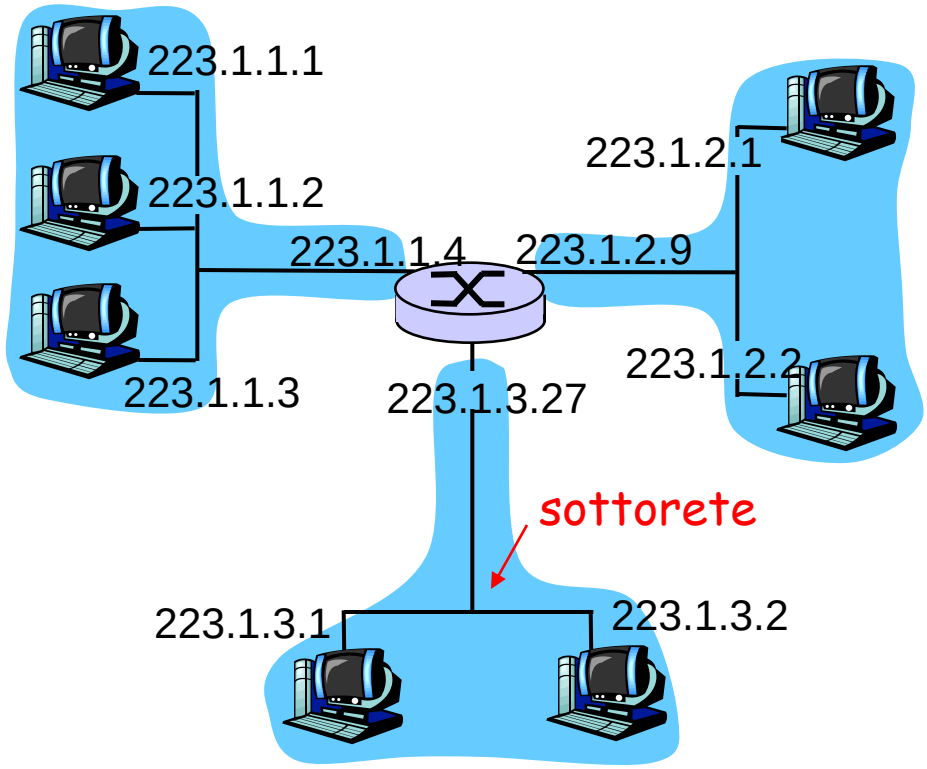


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Sottoreti

- *Indirizzo IP*
  - Parte di sottorete (bit di alto ordine)
  - Parte dell'host (bit di basso ordine)
- *Cos'è una sottorete?*
  - Nella letteratura Internet le sottoreti sono anche chiamate reti IP.

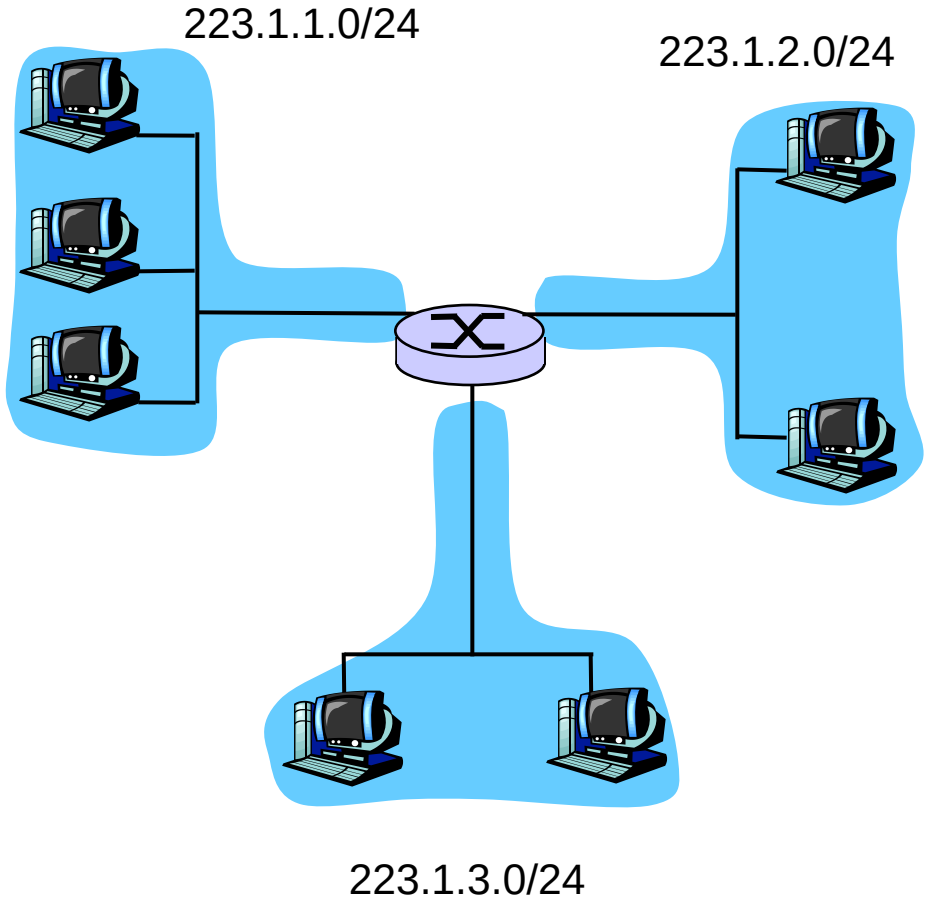


rete composta da 3 sottoreti

Sottorete

Definizione

- È detta *sottorete* una rete isolata i cui punti terminali sono collegati all'interfaccia di un host o di un router.



Indica che i 24 bit più a sinistra dell'indirizzo definiscono l'indirizzo della sottorete.
Ogni host connesso alla sottorete 223.1.1.0/24 deve avere un indirizzo della forma 223.1.1.xxx

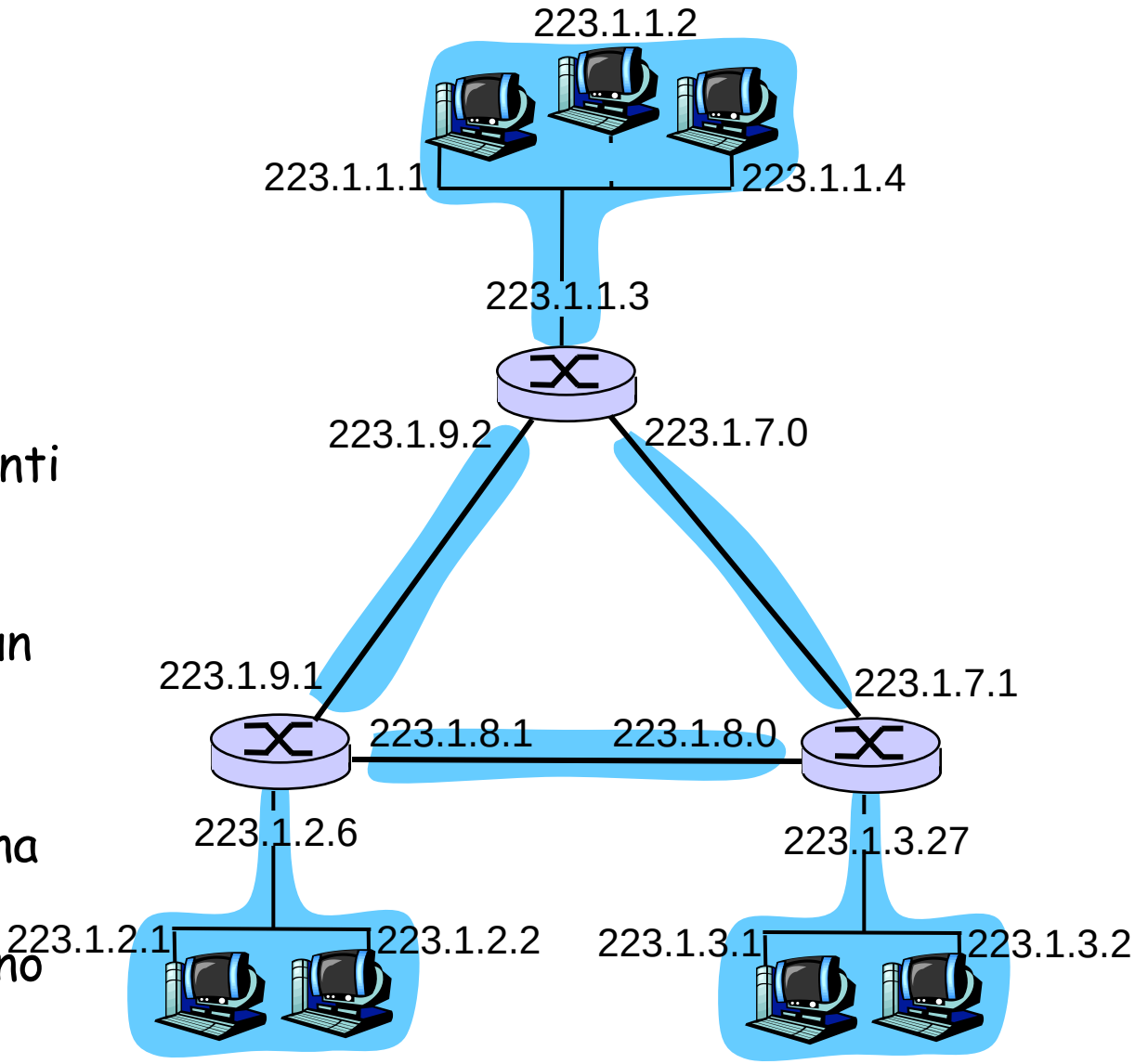
→ Maschera di sottorete o subnet mask: /24

Sottoreti

Quante sono?

La definizione IP di sottorete non è ristretta a segmenti Ethernet che collegano più host all'interfaccia di un router

E' detta sottorete una rete isolata I cui punti terminali sono collegati all'interfaccia di un host o di un router



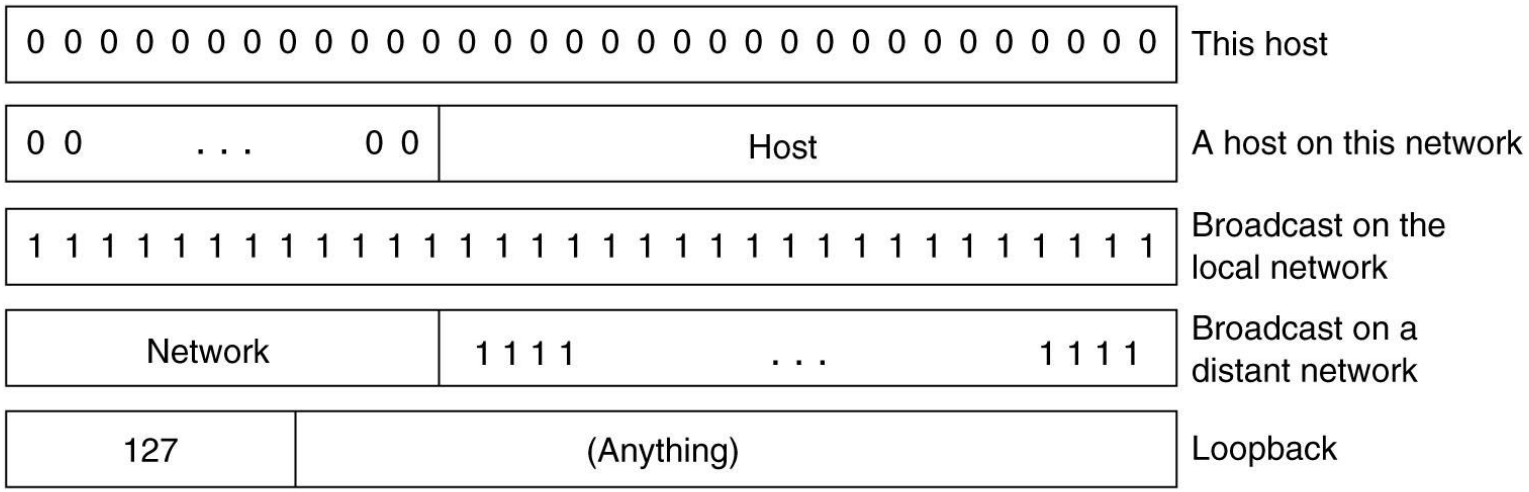
Assegnazione indirizzi Internet CIDR

CIDR: Classless InterDomain Routing (RFC 1519)

- È la strategia di assegnazione degli indirizzi.
- Struttura dell'indirizzo: l'indirizzo IP viene diviso in due parti e mantiene la forma decimale puntata a.b.c.d/x, dove x indica il numero di bit nella prima parte dell'indirizzo ().

200.23.16.0/23

Indirizzi IP speciali



- L'indirizzo **0.0.0.0** è utilizzato dagli host al momento del boot
- Gli indirizzi IP che hanno lo **0** come **numero di rete** si riferiscono alla rete 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)

Come ottenere un blocco di indirizzi

D: Cosa deve fare un amministratore di rete per ottenere un blocco di indirizzi IP da usare in una sottorete?

R: deve contattare il proprio ISP e ottenere un blocco di indirizzi contigui con un prefisso comune

Otterrà indirizzi della forma a.b.c.d/x

Dove x bit indicano la sottorete

e (32-x) bit indicano i singoli dispositivi dell'organizzazione

N.B. i 32-x bit possono presentare un'aggiuntiva struttura di sottorete

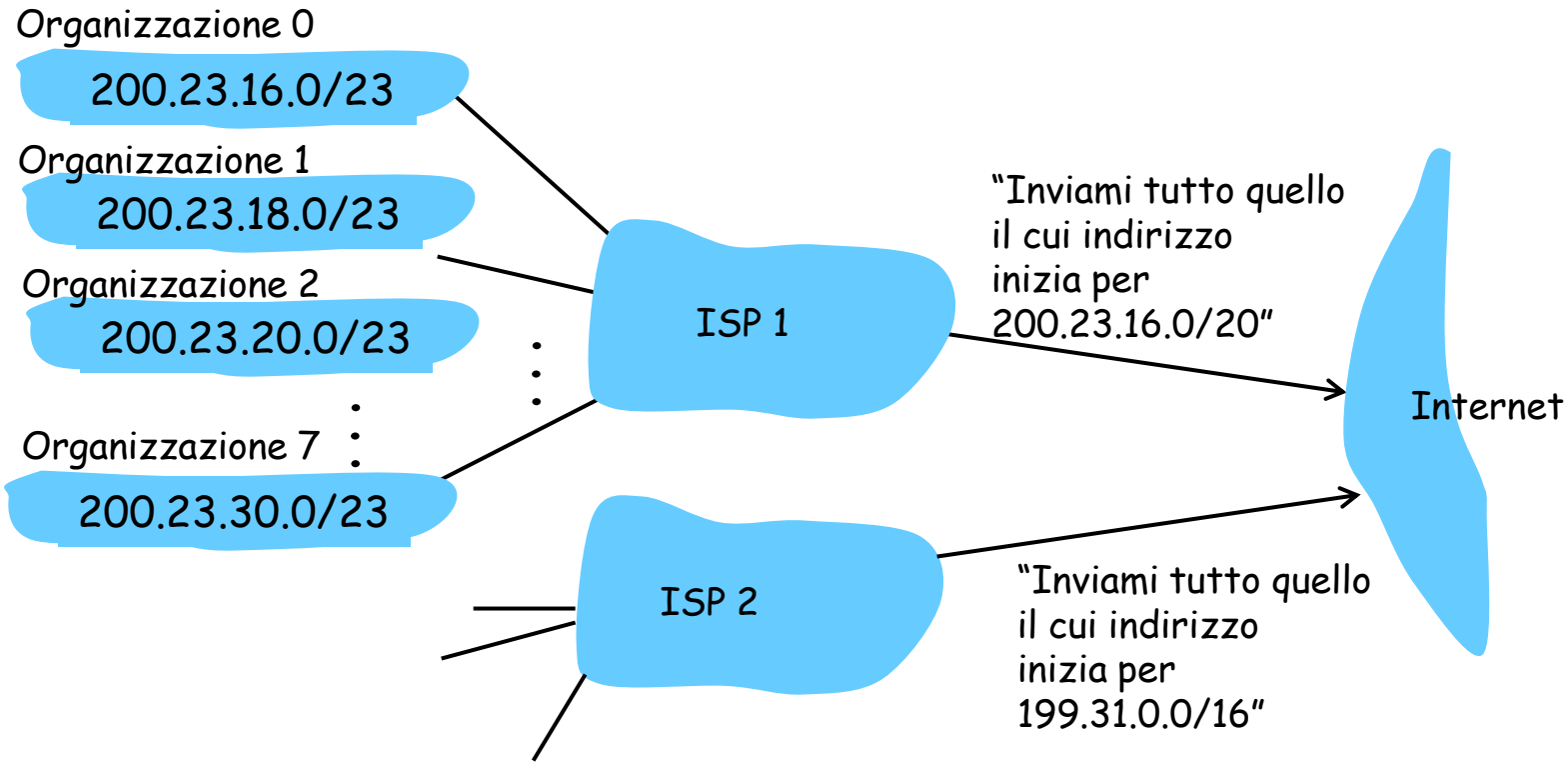
Esempio

- Un ISP connette 8 organizzazioni a Internet.
- L'ISP divide in 8 blocchi uguali gli indirizzi contigui nel blocco a sua disposizione.
- Ogni blocco avrà un prefisso di sottorete di 23 bit invece che di 20 (***aggregazione di indirizzi***) come per l'ISP
- La suddivisone in 8 blocchi non deve essere visibile all'esterno

Blocco dell'ISP	11001000 00010111 00010000	00000000	200.23.16.0/20
Organizzazione 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Organizzazione 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Organizzazione 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	.....	....	....
Organizzazione 7	11001000 00010111 00011110	00000000	200.23.30.0/23

Indirizzamento gerarchico

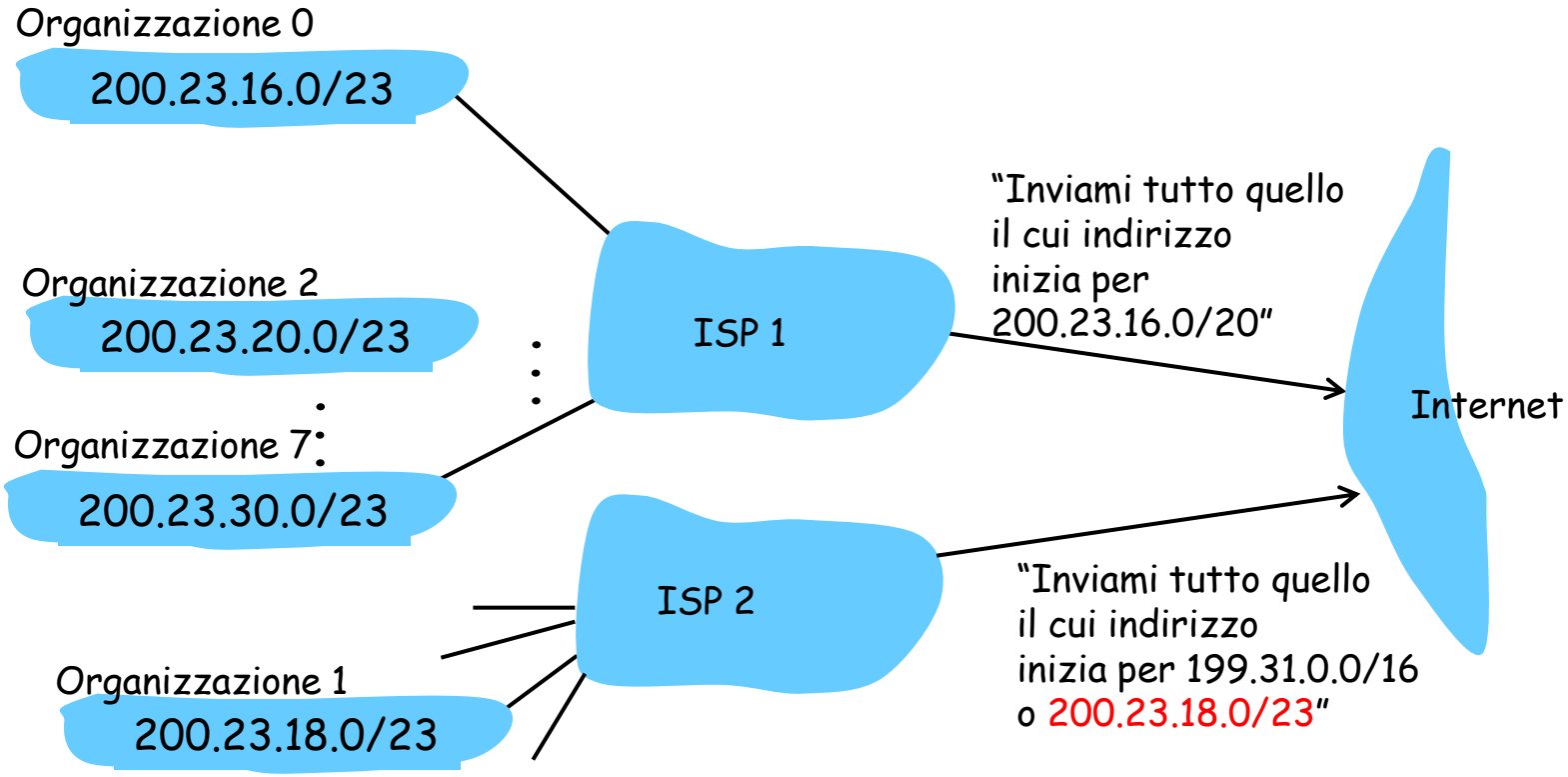
Indirizzamento gerarchico e aggregazione di indirizzi:



Cosa succederebbe se ISP1 acquisisse il provider ISP2 e facesse connettere L'Organizzazione 1 a Internet tramite ISP2?

Indirizzamento gerarchico più specifico

ISP2 presenta un percorso più specifico verso Organizzazione 1



Indirizzi IP alla fonte

D: Ma come fa un ISP, a sua volta, a ottenere un blocco di indirizzi?

R: ICANN: Internet Corporation for Assigned Names and Numbers

- Ha la responsabilità di allocare i blocchi di indirizzi.
- Gestisce i server radice DNS.
- Assegna e risolve dispute sui nomi di dominio.

Come ottenere un indirizzo IP

D: Cosa bisogna fare per assegnare un indirizzo IP a un host?

- Indirizzo assegnato o indirizzo temporaneo?
- Configurazione manuale:
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol:
  - permette a un host di ottenere un indirizzo IP in modo automatico
    - "plug-and-play"
    - Largamente usato dove gli host si aggiungono e si rimuovono dalla rete con estrema frequenza (indirizzo temporaneo)
    - Può essere configurato in modo che un dato host riceva un indirizzo IP persistente (ogni volta che entra in rete gli viene assegnato lo stesso indirizzo)

DHCP: Dynamic Host Configuration Protocol

Obiettivo: consentire all'host di ottenere *dinamicamente* il suo indirizzo IP dal server di rete

- È possibile rinnovare la proprietà dell'indirizzo in uso
- È possibile il riuso degli indirizzi (quantità di indirizzi inferiore al numero totale di utenti)
- Supporta anche gli utenti mobili che si vogliono unire alla rete
- Utilizzato nelle reti residenziali di accesso a Internet e nelle LAN wireless, dove gli host si aggiungono e si rimuovono dalla rete con estrema frequenza

DHCP: Dynamic Host Configuration Protocol

RFC 2131

Protocollo client-server

Client: host appena connesso che desidera ottenere informazioni sulla configurazione della rete, non solo un indirizzo IP

Server:

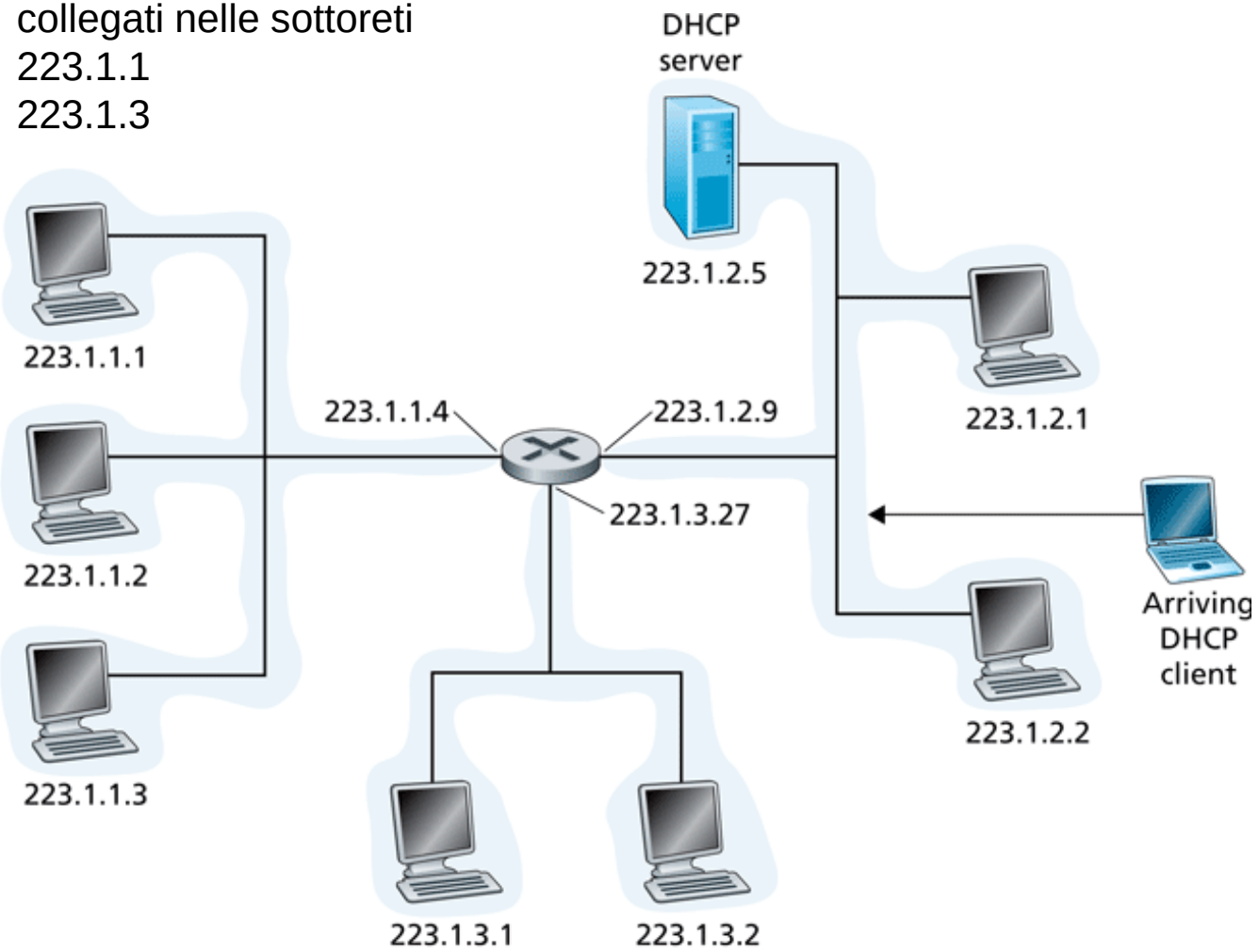
- ogni sottorete in genere dispone di un server DHCP
- Altrimenti router fa da agente di appoggio DHCP, conosce un server DHCP per quella rete

Panoramica di DHCP:

- L'host invia un messaggio broadcasts "DHCP discover"
- Il server DHCP risponde con "DHCP offer"
- L'host richiede l'indirizzo IP: "DHCP request"
- Il server DHCP invia l'indirizzo: "DHCP ack"

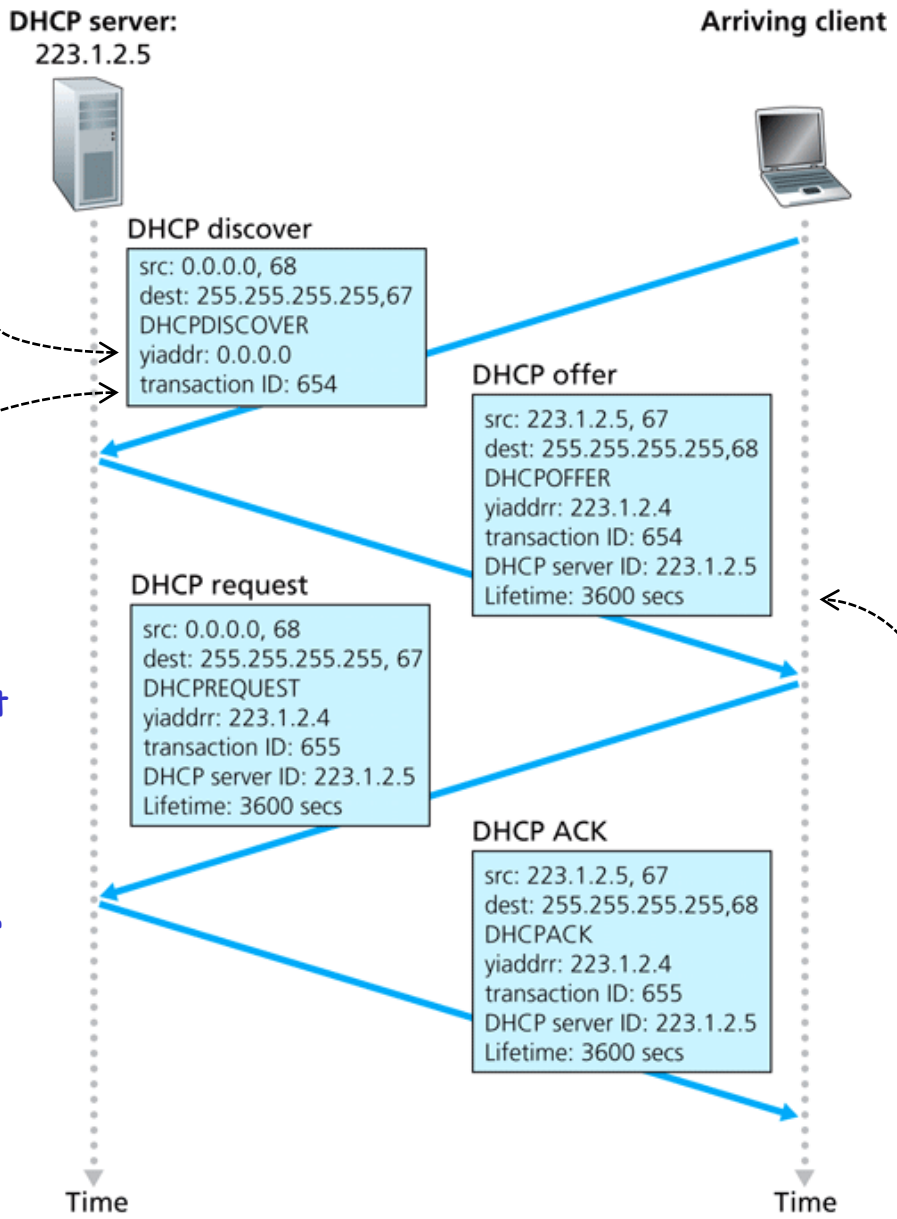
Scenario client-server DHCP

Il router opera da agente di appoggio per i client collegati nelle sottoreti
223.1.1
223.1.3



Il client DHCP in arrivo su questa rete ha bisogno di un indirizzo

Scenario client-server DHCP



yiaddr (your internet address) indica l'indirizzo assegnato al client appena connesso

Transaction Identifier: Campo di 32 bit che contiene un identificativo generato dal client che permette di associare richieste dei client e risposte dei server

lifetime Durata di tempo di validità dell'indirizzo IP

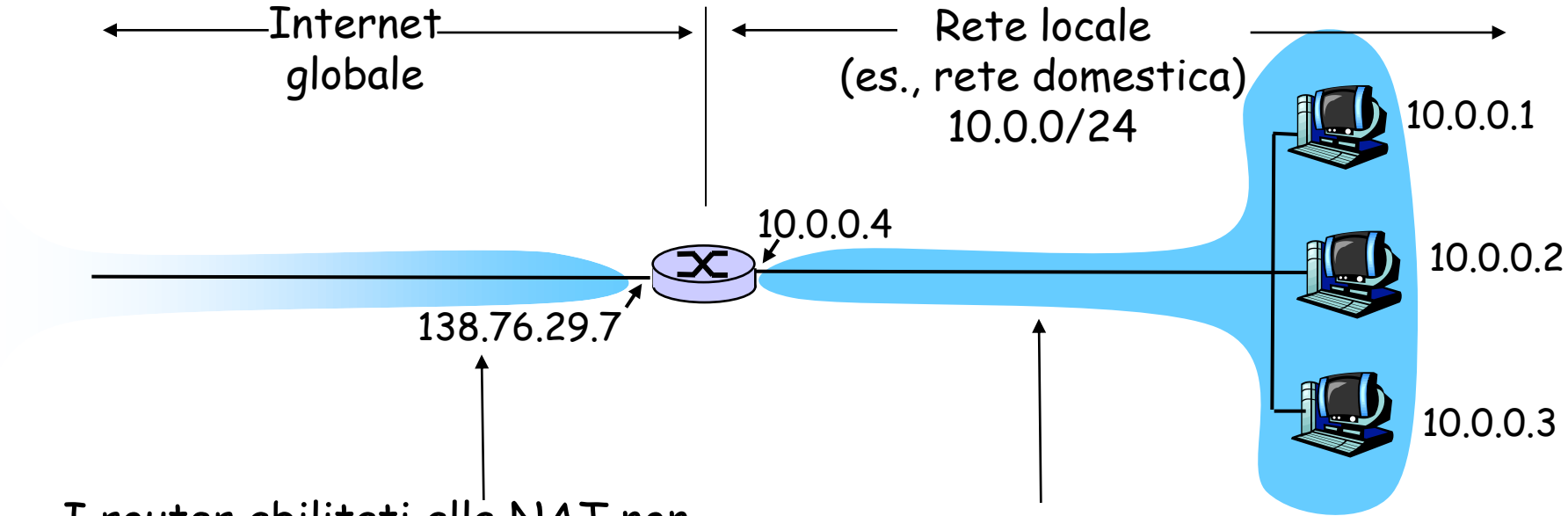
DHCP

- Quando il client riceve l'ACK DHCP, l'interazione è completata e il client può utilizzare il proprio indirizzo IP fornito da DHCP per la durata della concessione (lifetime)
- Per utilizzare il proprio indirizzo IP oltre la durata della concessione, DHCP fornisce un meccanismo per rinnovare la concessione di un IP
  - Il protocollo prevede meccanismi per il rinnovo della concessione o la richiesta di una nuova

Traduzione degli indirizzi di rete

- Proliferazione di sottoreti small office, home office (SOHO)
  - ogni volta che si vuole installare una rete locale per connettere più macchine, l'ISP deve allocare un intervallo di indirizzi per coprire la sottorete
  - Spesso impossibile per mancanza di indirizzi aggiuntivi nella sottorete
- Soluzione: si adotta la traduzione degli indirizzi di rete (NAT, network address translation)
  - *NAT* is a technique that allows an organization to set up a network using private addresses, while still being able to communicate on the public Internet.
  - A NAT-capable router translates private to public addresses and vice-versa as needed. This allows a small number of public IP addresses to be shared amongst a large number of devices.

Traduzione degli indirizzi di rete (NAT)



I router abilitati alla NAT non appaiono al mondo esterno come router ma come un *unico* dispositivo con un *unico* indirizzo IP. Indirizzo IP origine: 138.76.29.7, e tutto il traffico verso Internet deve riportare lo stesso indirizzo.

Spazio di indirizzi riservato alle reti private, molte delle quali usano un identico spazio, 10.0.0/24 per scambiare pacchetti tra i loro dispositivi

Traduzione degli indirizzi di rete (NAT)

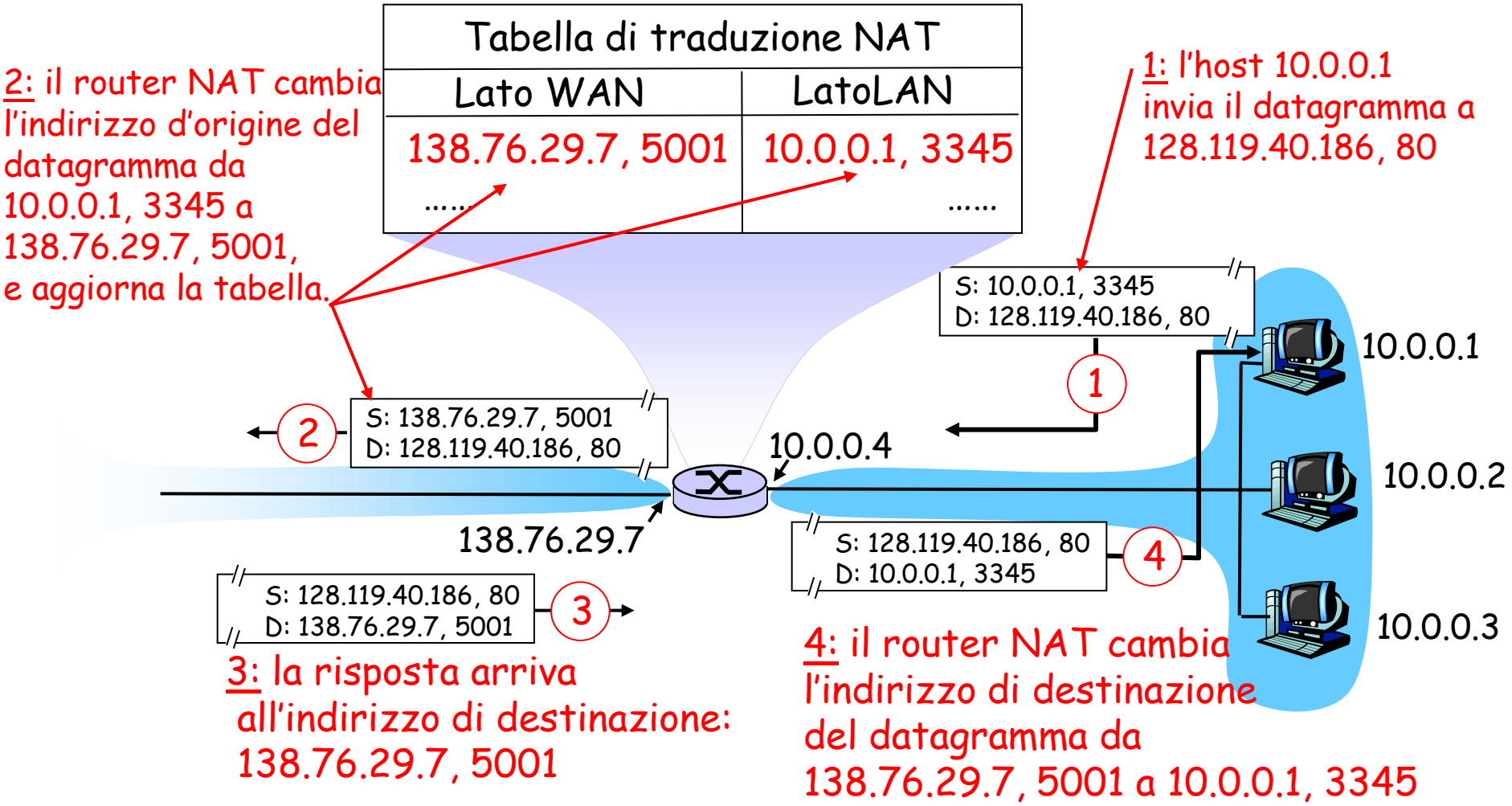
- Il router abilitato alla NAT nasconde i dettagli della rete domestica al mondo esterno
  - Non è necessario allocare un intervallo di indirizzi da un ISP: un unico indirizzo IP è sufficiente per tutte le macchine di una rete locale.
  - È possibile cambiare gli indirizzi delle macchine di una rete privata senza doverlo comunicare all'Internet globale.
  - È possibile cambiare ISP senza modificare gli indirizzi delle macchine della rete privata
  - Dispositivi interni alla rete non esplicitamente indirizzabili e visibili dal mondo esterno (un plus per la sicurezza)

Traduzione degli indirizzi di rete (NAT)

Implementazione:

- Quando un router NAT riceve il datagramma, genera per esso un nuovo numero di porta d'origine (es. 5001), sostituisce l'indirizzo IP origine con il proprio indirizzo IP sul lato WAN (es. 138.76.29.7) e sostituisce il numero di porta origine iniziale (es. 3348) con il nuovo numero (5001)

Traduzione degli indirizzi di rete (NAT)

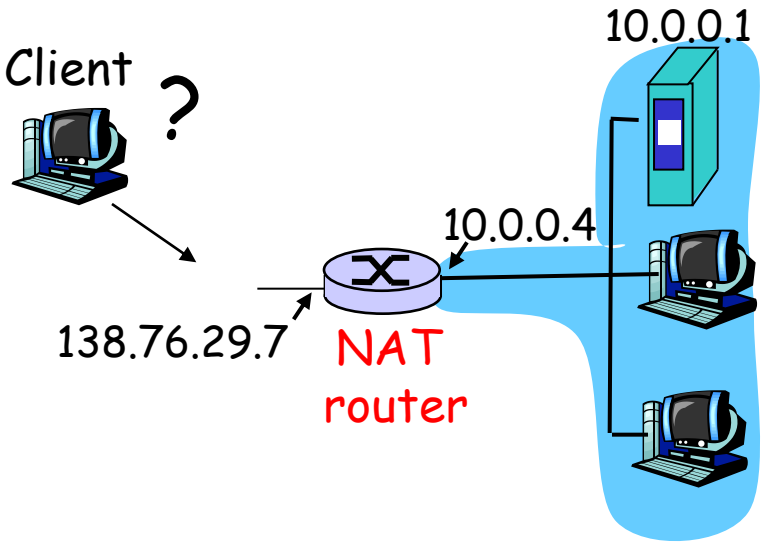


Traduzione degli indirizzi di rete (NAT)

- Il campo numero di porta è lungo 16 bit:
  - Il protocollo NAT può supportare più di 60.000 connessioni simultanee con un solo indirizzo IP sul lato WAN.
- NAT è contestato perché:
  - i router dovrebbero elaborare i pacchetti solo fino al livello 3.
  - Il numero di porta viene usato per identificare host e non processi
  - Viola il cosiddetto *argomento punto-punto*
    - *Gli host dovrebbero comunicare tra di loro direttamente, senza intromissione di nodi né modifica di indirizzi IP e numeri di porta*
    - Per risolvere la scarsità di indirizzi IP si dovrebbe usare IPv6.
  - Interferenza con le applicazioni P2P in cui ogni peer dovrebbe essere in grado di avviare una connessione TCP con qualsiasi altro peer, a meno che il NAT non sia specificamente configurato per quella specifica applicazione P2P.

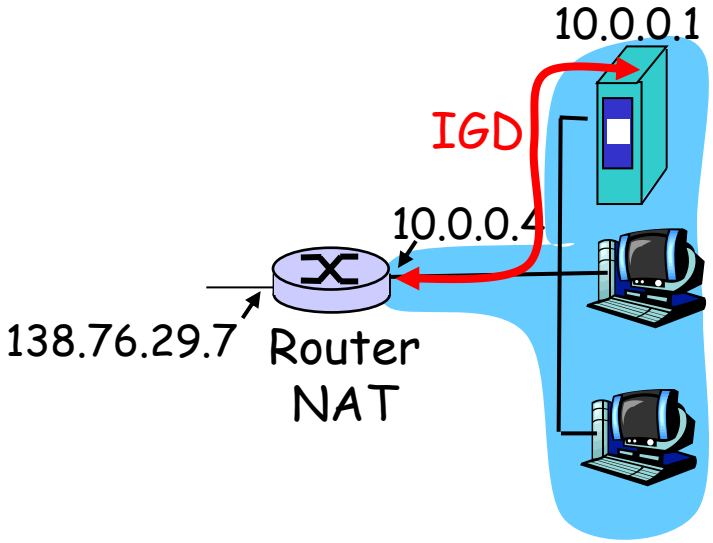
Un altro problema di NAT

- Un client vuole collegarsi al server con indirizzo 10.0.0.1
  - L'indirizzo del server 10.0.0.1 è locale per quella LAN (il client non può usarlo come indirizzo destinazione)
  - Vi è un solo indirizzo NAT esternamente visibile: 138.76.29.7
- Soluzione 1: configurare staticamente NAT per inoltrare le richieste di collegamento entranti a quella data porta del server
  - (123.76.29.7, porta 2500) sempre inoltrato a 10.0.0.1 porta 2500



Un altro problema di NAT

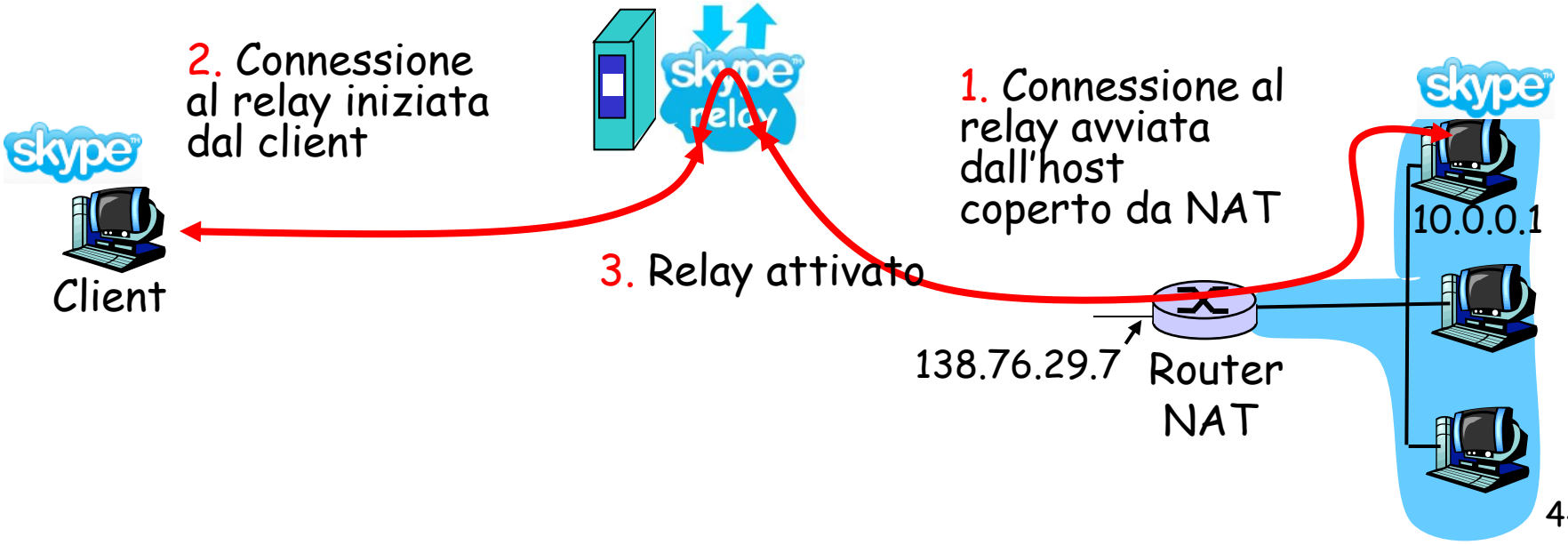
- Soluzione 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Consente agli host coperti da NAT di:
  - Conoscere gli indirizzi IP pubblici (138.76.29.7)
  - Richiedere una corrispondenza NAT per un qualsiasi numero di porta (a scelta)



- Esempio:
  - BitTorrent su 10.0.0.1 e porta 3345 vuole accettare connessioni dall'esterno
  - BitTorrent chiede al NAT di creare un'apertura che faccia corrispondere (10.0.0.1, 3345) a (138.76.29.7,5001), dove 5001 è scelto dall'applicazione
  - BitTorrent può annunciare il proprio tracker su (138.76.29.7,5001)
  - NAT opera da traduttore

Un altro problema di NAT

- Soluzione 3: relay (usato in Skype)
  - Il client NAT stabilisce una connessione con relay
  - Il client esterno si collega al relay
  - Il relay fa da ponte tra le due connessioni



Livello di rete

Introduzione

Reti a circuito virtuale e a datagramma

Che cosa si trova all'interno di un router?

Protocollo Internet (IP)

- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6

Algoritmi di instradamento

- Stato del collegamento
- Vettore distanza
- Instradamento gerarchico

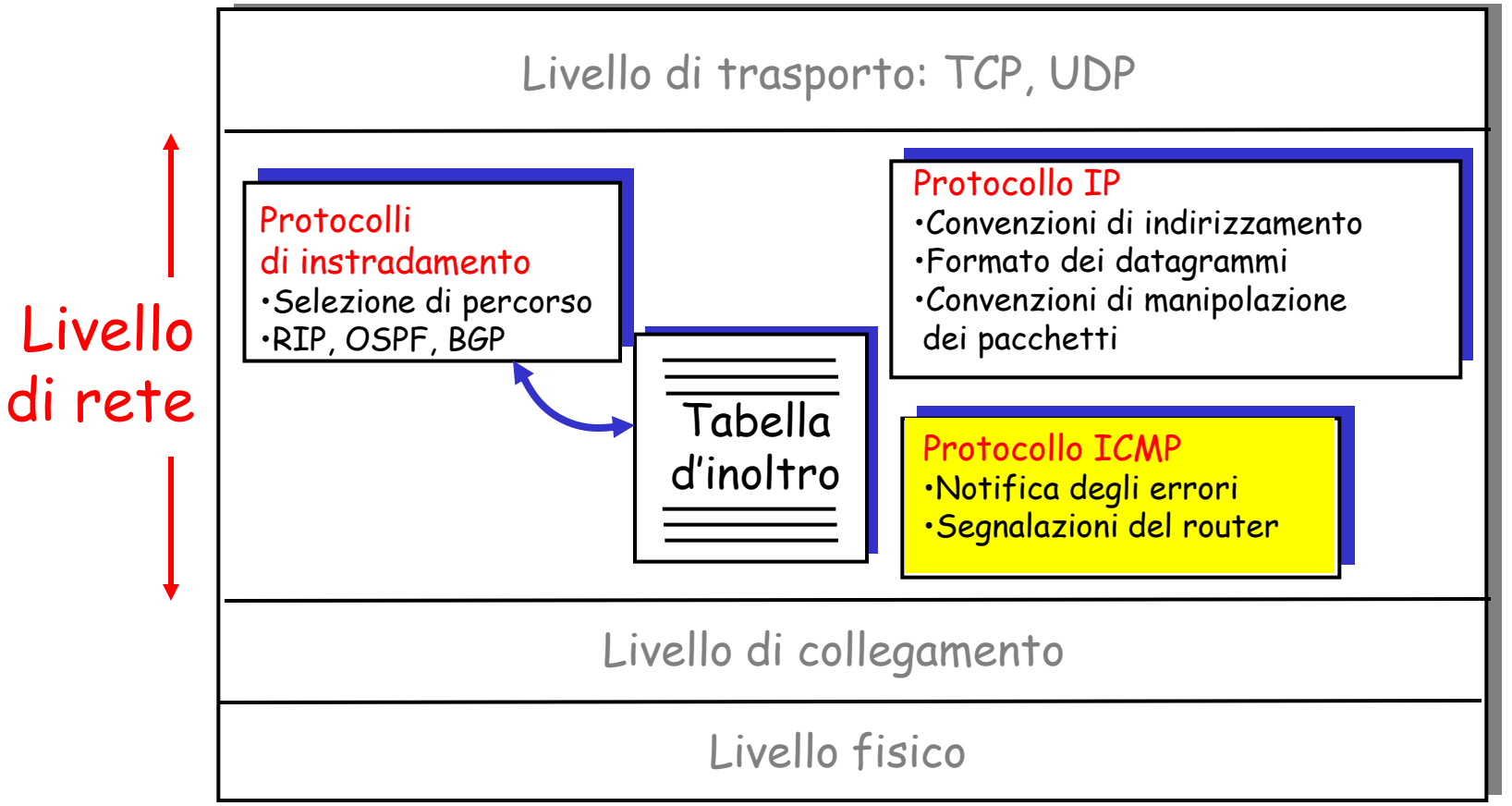
Instradamento in Internet

- RIP
- OSPF
- BGP

Instradamento broadcast e multicast

Livello di rete

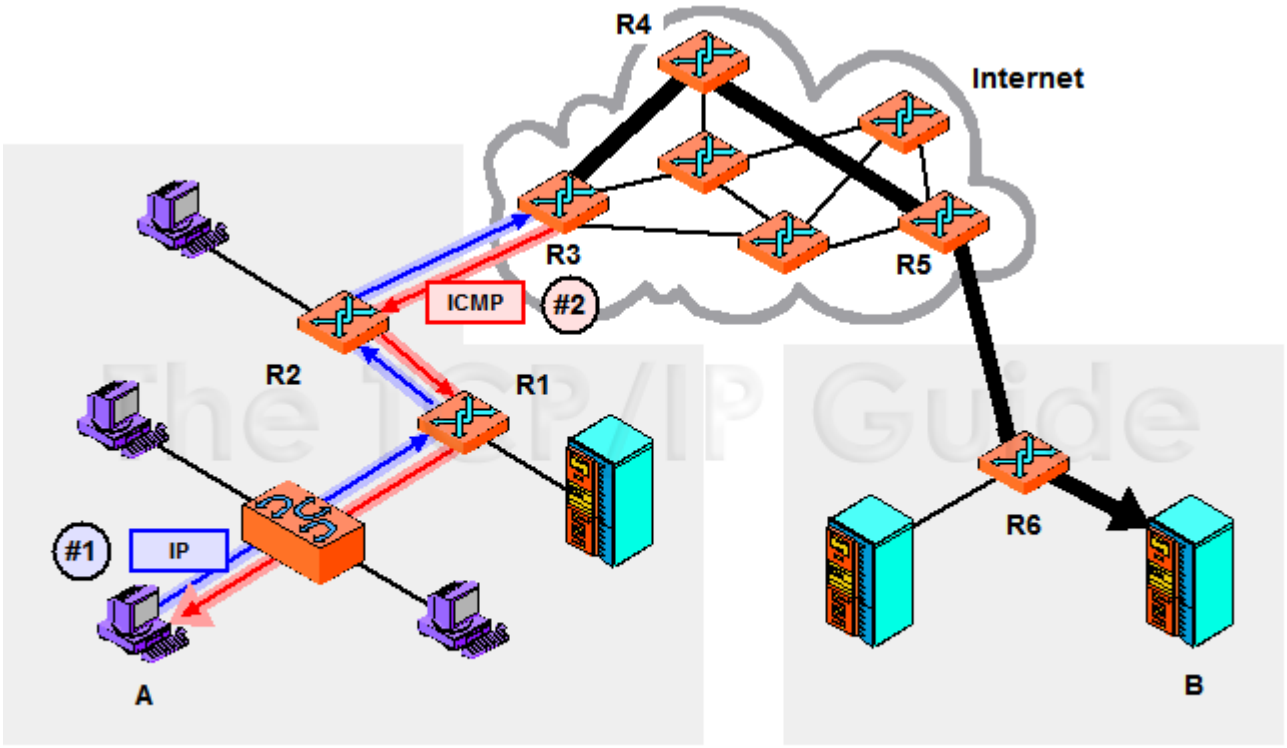
Uno sguardo al livello di rete Internet:



Il campo dati dei datagrammi IP può contenere un messaggio ICMP

Internet Control Message Protocol (ICMP)

- Viene usato da host e router per scambiarsi informazioni a livello di rete.



A typical use of ICMP is to provide a feedback mechanism when an IP message is sent. In this example, device *A* is trying to send an IP datagram to device *B*. However, when it gets to router *R3* a problem of some sort is detected that causes the datagram to be dropped. *R3* sends an ICMP message back to *A* to tell it that something happened, hopefully with enough information to let A correct the problem, if possible. *R3* can only send the ICMP message back to *A*, not to *R2* or *R1*.

Internet Control Message Protocol (ICMP)

- Viene usato da host e router per scambiarsi informazioni a livello di rete.
  - report degli errori: host, rete, porta, protocollo irraggiungibili.
  - echo request/reply (usando il programma ping).
- Livello di rete "sopra" IP:
  - ICMP è considerato parte di IP anche se usa IP per inviare i suoi messaggi
- Messaggi ICMP: hanno un campo **tipo** e un campo **codice**, e contengono l'intestazione e i primi 8 byte del datagramma IP che ha provocato la generazione del messaggio.

Tipo	Codice	Descrizione
0	0	Risposta eco (a ping)
3	0	rete destin. irraggiungibile
3	1	host destin. irraggiungibile
3	2	protocollo dest. irraggiungibile
3	3	porta destin. irraggiungibile
3	6	rete destin. sconosciuta
3	7	host destin. sconosciuto
4	0	riduzione (controllo di congestione)
8	0	richiesta eco
9	0	annuncio del router
10	0	scoperta del router
11	0	TTL scaduto
12	0	errata intestazione IP

Traceroute e ICMP

- Il programma invia una serie di datagrammi IP alla destinazione ciascuno contenente un segmento UDP con un numero di porta improbabile.
  - Il primo pari a TTL =1
  - Il secondo pari a TTL=2, ecc.
  - Numero di porta improbabile
  - L'origine avvia un timer per ogni datagramma
- Quando l'*n*-esimo datagramma arriva all'*n*-esimo router:
  - Il router scarta il datagramma.
  - Invia all'origine un messaggio di allerta ICMP (tipo 11, codice 0).
  - Il messaggio include il nome del router e l'indirizzo IP.
- Quando il messaggio ICMP arriva, l'origine può calcolare RTT
- Traceroute lo fa per 3 volte

Criteri di arresto dell'invio

- Quando un segmento UDP arriva all'host di destinazione.
- L'host di destinazione restituisce un messaggio ICMP di porta non raggiungibile (tipo 3, codice 3).
- Quando l'origine riceve questo messaggio ICMP, si blocca.