Livello di Rete: Indirizzamento IPv4, DHCP, indirizzi privati e NAT, Forwarding, ICMP

Prof.ssa Gaia Maselli

maselli@di.uniroma1.it

Parte di queste slide sono state prese dal materiale associato ai libri:

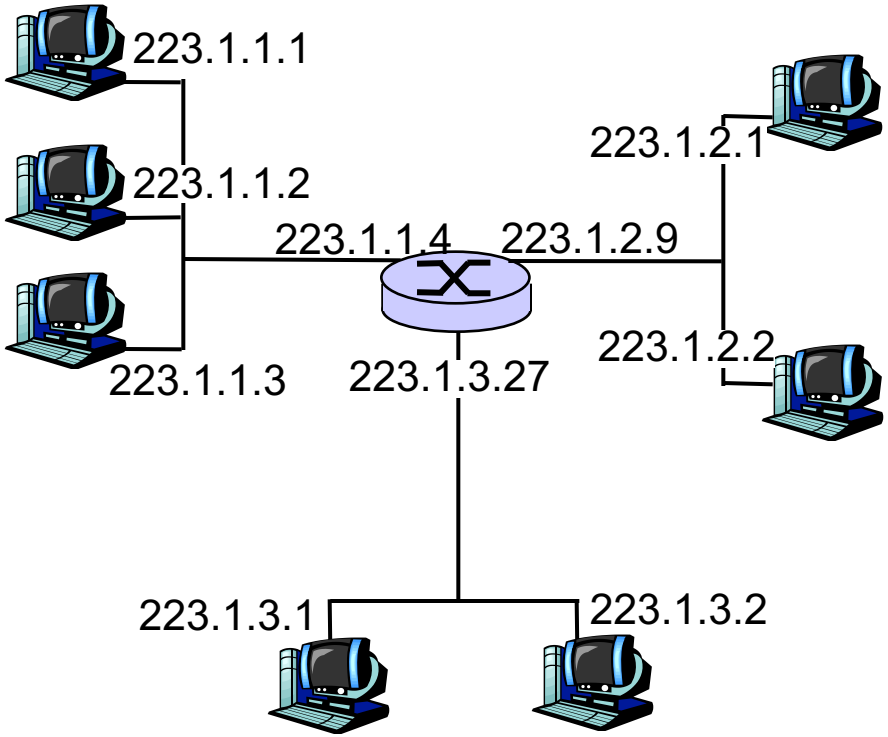
1) B.A. Forouzan, F. Mosharraf – Reti di calcolatori. Un approccio top-down. Copyright © 2013 McGraw-Hill Education Italy srl. Edizione italiana delle slide a cura di Gabriele D'Angelo e Gaia Maselli
2) Computer Networking: A Top Down Approach , 6th edition. All material copyright 1996-2009 J.F Kurose and K.W. Ross, All Rights Reserved

Livello di rete

- Forwarding e routing
- Struttura dei router
- IPv4
  - Formato dei datagrammi IPv4
  - Frammentazione
  - Indirizzamento IPv4 (con classi e senza classi)
  - DHCP
  - NAT
- Forwarding dei datagrammi IP
- ICMP
- Routing (RIP, OSPF, BGP)

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

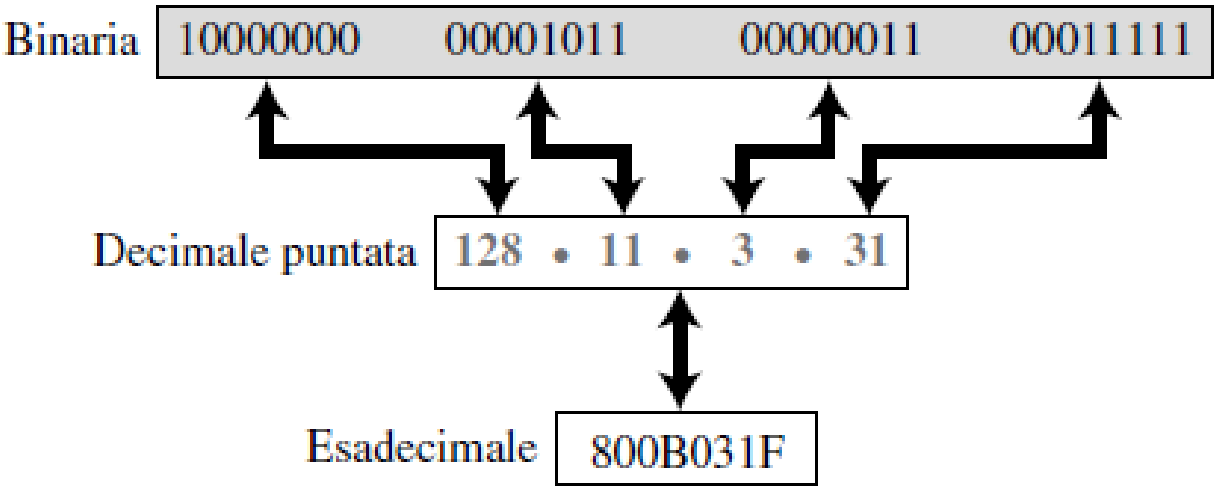


223.1.1.1 = 11011111 00000001 00000001 00000001

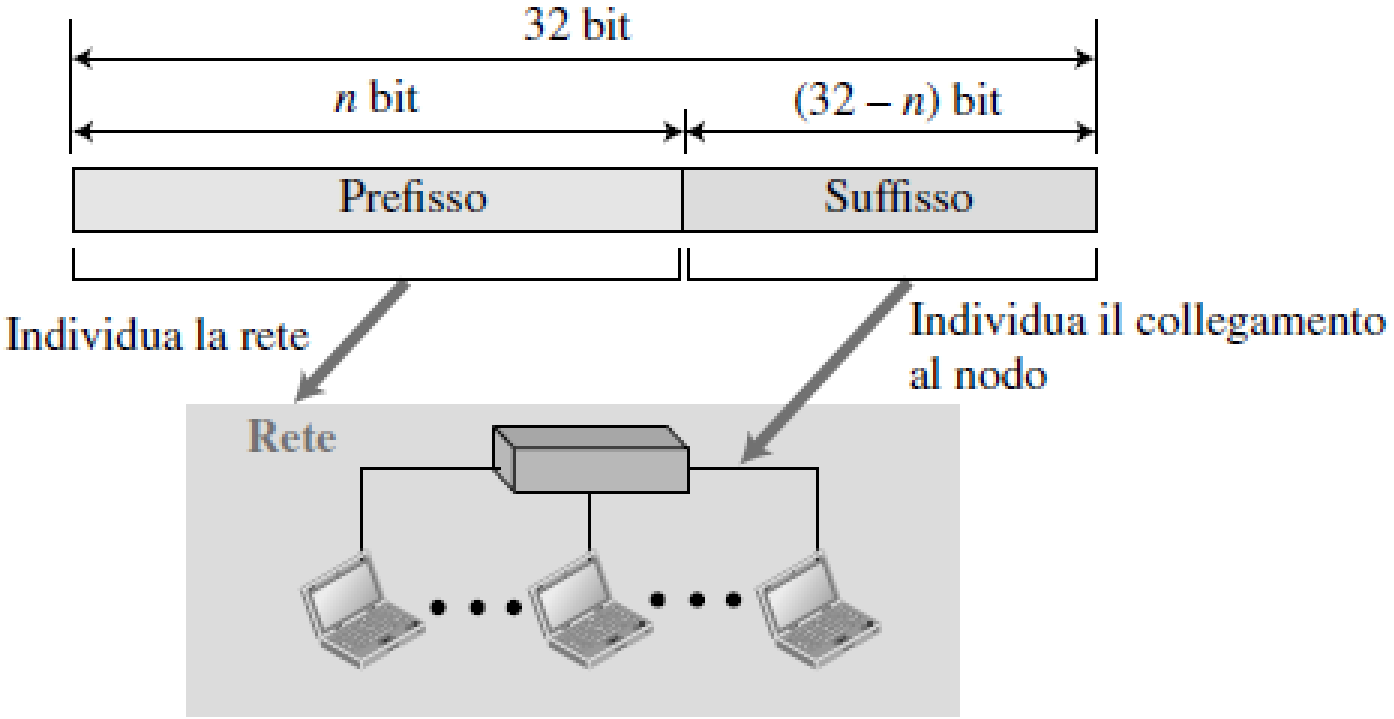
223 1 1 1

Spazio degli indirizzi

- Numero totale indirizzi 2^{32} ovvero più di 4 miliardi
- Notazione
  - Binaria
  - Decimale puntata
  - Esadecimale (usata nella programmazione di rete)



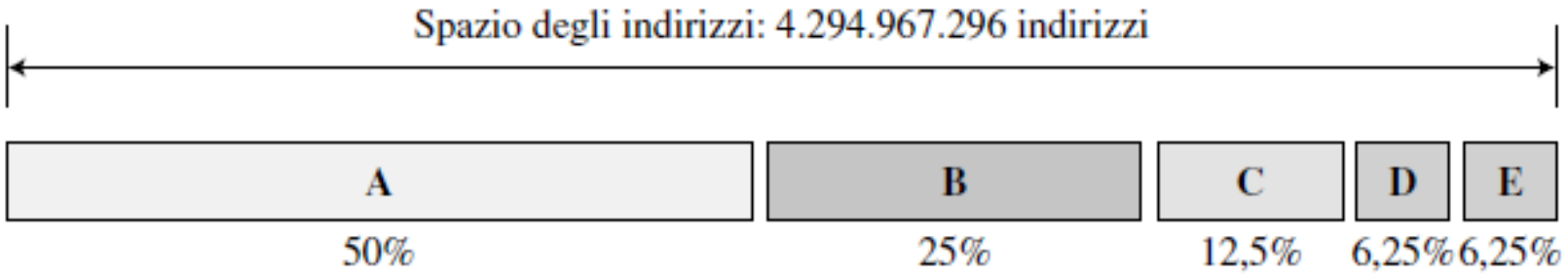
Gerarchia nell'indirizzamento

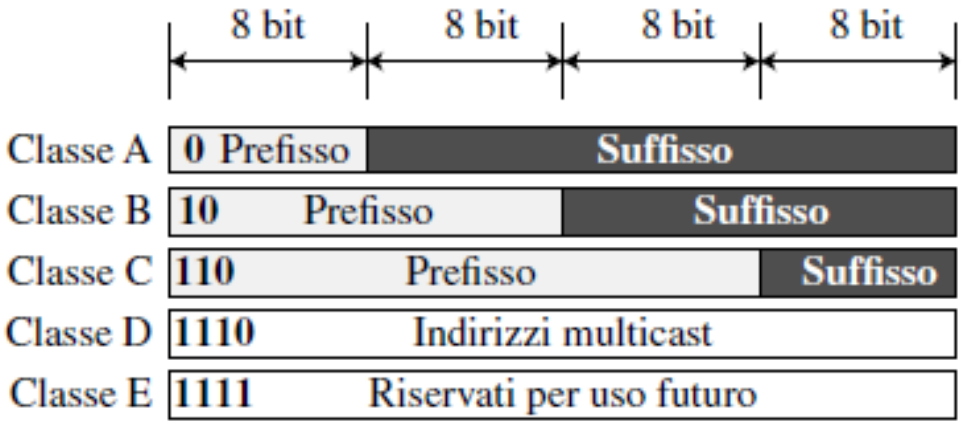


- Il prefisso può avere lunghezza
  - Fissa: indirizzamento con classi
  - Variabile: indirizzamento senza classi

Indirizzamento con classi

- Necessità di supportare sia reti piccole che grandi
- 3 lunghezze di prefisso (8,16,24)





Classe	Prefissi	Primo byte
A	$n = 8$ bit	Da 0 a 127
B	$n = 16$ bit	Da 128 a 191
C	$n = 24$ bit	Da 192 a 223
D	Non applicabile	Da 224 a 239
E	Non applicabile	Da 240 a 255

Pros and cons

- Una volta individuato un indirizzo si può facilmente risalire alla classe e la lunghezza del prefisso

Problema dell'esaurimento degli indirizzi

- La classe A può essere assegnata solo a 128 organizzazioni al mondo, ognuna con 16.777.216 nodi
  - La maggior parte degli indirizzi andava sprecata
  - Poche organizzazioni (solo 128) potevano usufruire di indirizzi di classe A
- Classe B: stessi problemi della A
- Classe C: pochi indirizzi (256) per rete

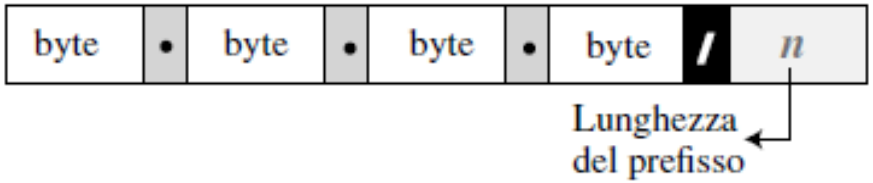
Indirizzamento senza classi

- Necessità di maggiore flessibilità nell'assegnamento degli indirizzi
- Vengono utilizzati blocchi di lunghezza variabile che non appartengono a nessuna classe
- Un indirizzo non è in grado di definire da solo la rete (o blocco) a cui appartiene
- La lunghezza del prefisso è variabile (da 0 a 32 bit) e viene aggiunta all'indirizzo separata da uno slash

Notazione 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/n, dove n indica il numero di bit nella prima parte dell'indirizzo.

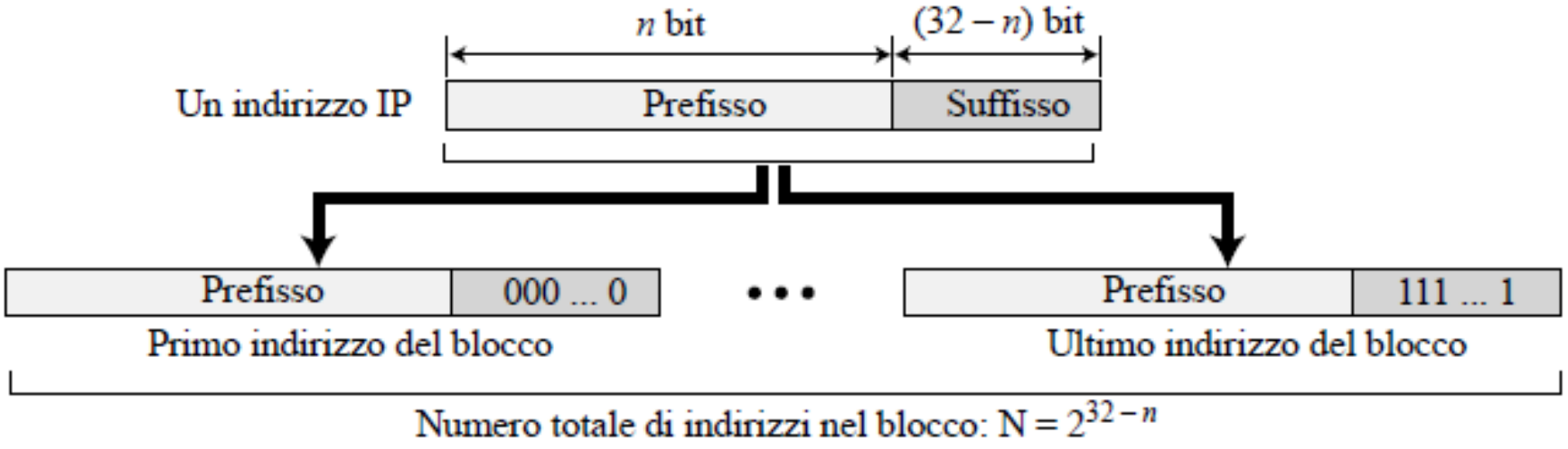


200.23.16.0/23

Estrazione delle informazioni

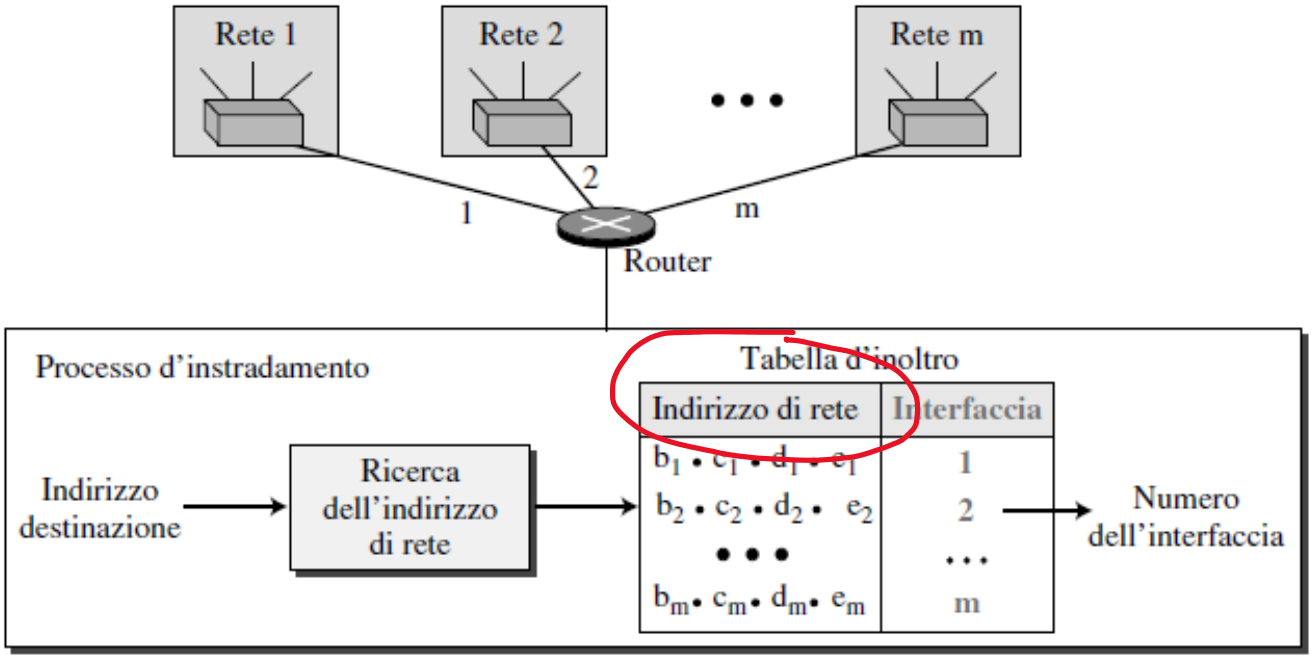
- Se *n* è la lunghezza del prefisso

1. Il numero di indirizzi nel blocco è dato da $N = 2^{32-n}$
2. Per trovare il primo indirizzo si impostano a 0 tutti i bit del suffisso (32-n)
3. Per trovare l'ultimo indirizzo si impostano a 1 tutti i bit del suffisso (32-n)



Maschera e indirizzo di rete

- 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
- Mediante la maschera si ottiene l'indirizzo di rete che è usato nell'instradamento dei datagrammi verso la destinazione



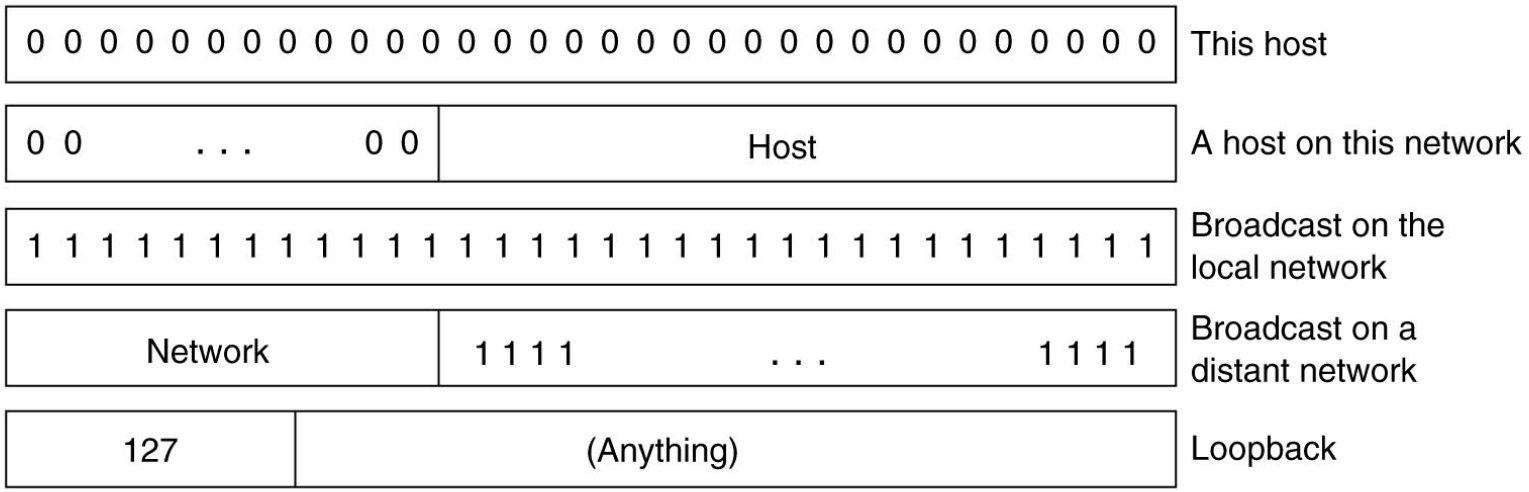
Perchè la maschera?

- 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=NOT(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))

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 sono distribuiti gli indirizzi all'interno di una rete (LAN)?

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

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

Dynamic Host Configuration Protocol (DHCP)

- Assegnazione automatizzata degli indirizzi ai singoli host o router
- Programma client/server di livello applicazione
- Quando un host vuole entrare a far parte di una rete necessita di
  - Indirizzo IP
  - Maschera di rete
  - Indirizzo del router
  - Indirizzo DNS

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:

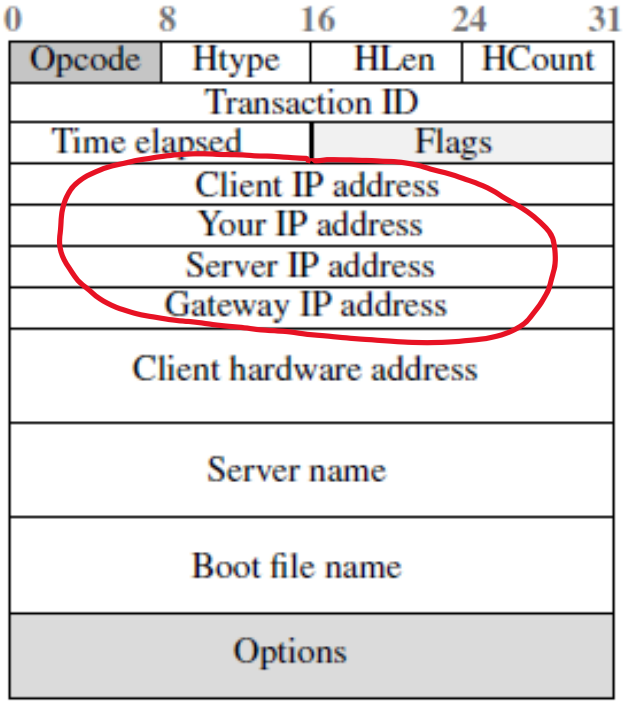
- ogni sottorete in genere dispone di un server DHCP
- Altrimenti router fa da agente di appoggio DHCP, conosce un server DHCP per quella rete

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"

Formato messaggi DHCP

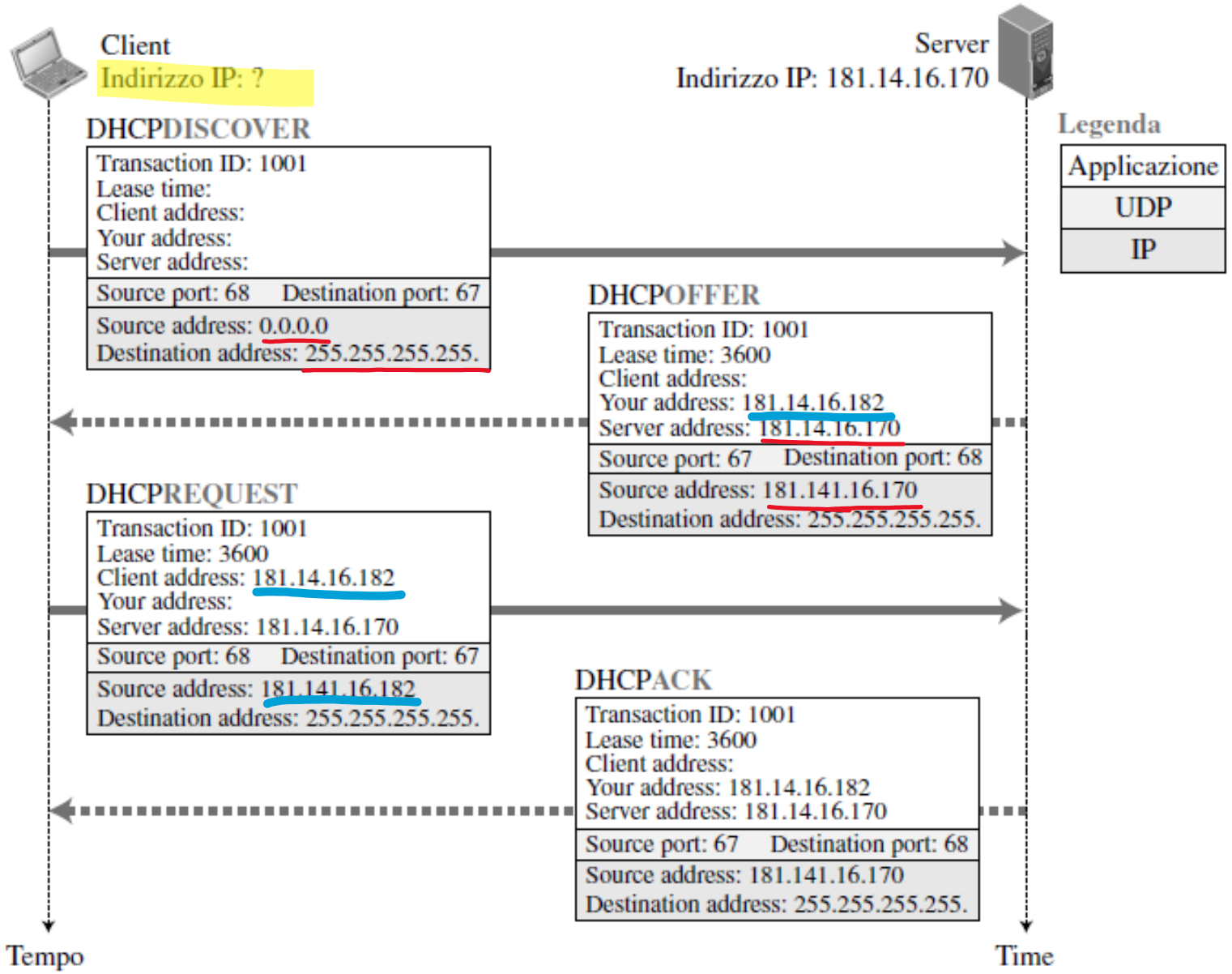
- Il client invia un messaggio di richiesta, il server di risposta



Campi:

Opcode: codice operazione, richiesta (1) o risposta (2)
Htype: tipologia dell'hardware (Ethernet, …)
HLen: lunghezza dell'indirizzo hardware
HCount: numero massimo di hop che il pacchetto può compiere
Transaction ID: un numero intero impostato dal client e ripetuto dal server
Time elapsed: il numero di secondi da quando il client ha inviato il primo messaggio di richiesta
Flags: il primo bit definisce l'unicast (0) o il multicast (1): gli altri 15 bit non vengono utilizzati
Client IP address: l'indirizzo IP del client, impostato a 0 se il client non lo conosce
Your IP address: l'indirizzo IP del client, inviato dal server
Server IP address: l'indirizzo IP del server, impostato ad un indirizzo IP di broadcast se il client non lo conosce
Gateway IP address: l'indirizzo del router di default
Server name: il nome di dominio del server (64 byte)
Boot file name: un nome di file (128 byte) usato per informazioni aggiuntive
Options: un campo da 64 byte con un duplice scopo, come descritto nel testo

DHCP


Client
Indirizzo IP: ?
Server
Indirizzo IP: 181.14.16.170
Legenda
Applicazione
UDP
IP
DHCPDISCOVER
Transaction ID: 1001
Lease time:
Client address:
Your address:
Server address:
Source port: 68 Destination port: 67
Source address: 0.0.0.0
Destination address: 255.255.255.255.
DHCPOFFER
Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.141.16.170
Destination address: 255.255.255.255.
DHCPREQUEST
Transaction ID: 1001
Lease time: 3600
Client address: 181.14.16.182
Your address:
Server address: 181.14.16.170
Source port: 68 Destination port: 67
Source address: 181.141.16.182
Destination address: 255.255.255.255.
DHCPACK
Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.141.16.170
Destination address: 255.255.255.255.
Tempo
Time

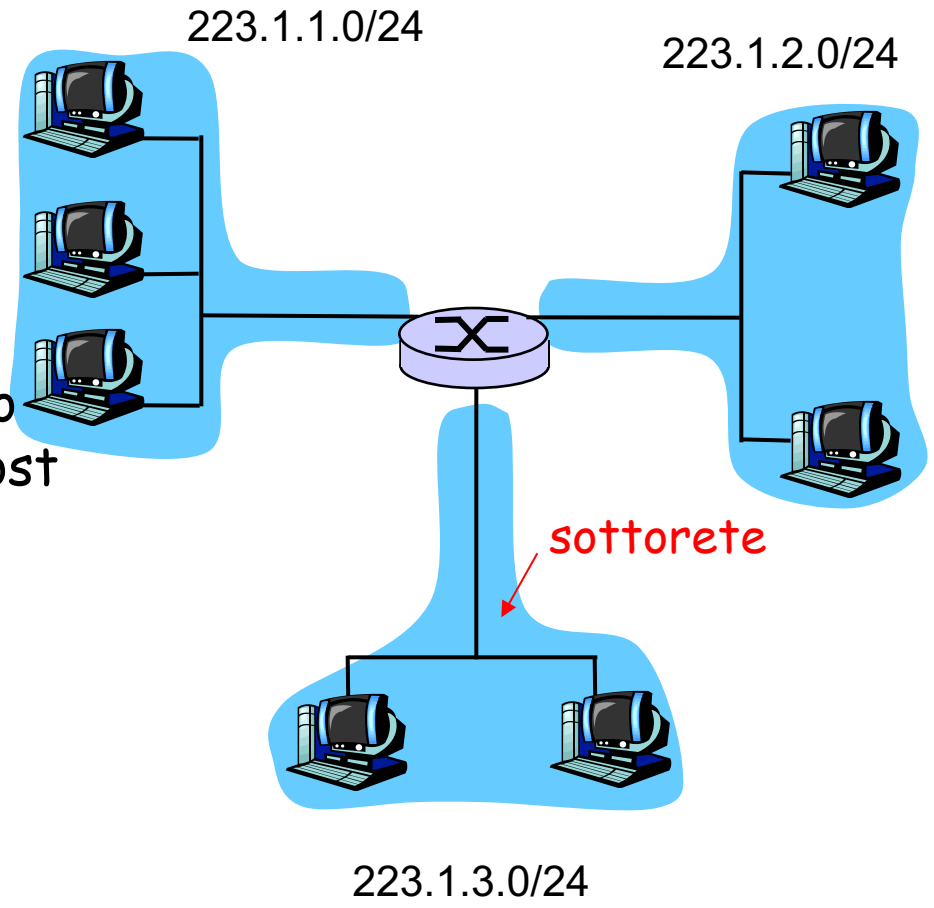
DHCP

- D: Usa porte well-known (client: 68, server: 67), perchè?
- R: La risposta del server è broadcast
- Il server invia solo l'indirizzo IP al client.
- D: Come può il client ottenere le altre info (maschera, server DNS, router)?
- R: Nel DHCPACK il server inserisce il pathname di un file contenente le info mancanti. Il client usa FTP per ottenere il file.

Livello di rete

- Forwarding e routing
- Struttura dei router
- IPv4
  - Formato dei datagrammi IPv4
  - Frammentazione
  - Indirizzamento IPv4 (con classi e senza classi)
  - DHCP
  - NAT
- Forwarding dei datagrammi IP
- ICMP
- Routing

Sottorete



Definizione

- È detta *sottorete* una rete isolata i cui punti terminali sono collegati all'interfaccia di un host o di un router.
- *Indirizzo IP*
  - Parte di sottorete (prefisso)
  - Parte dell'host (suffisso)

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

N.B.

- Dato un indirizzo IP e la sua maschera di rete, come faccio a sapere a quale blocco appartiene?
- Il prefisso di rete ha una lunghezza variabile
  - Multiplo di 8 bit

    esempio: a.b.c.d/24

    allora gli indirizzi degli host vanno da

    a.b.c.**0** a a.b.c.**255**
  - Non multiplo di 8 bit

    esempio a.b.c.d/26

    Allora bisogna vedere la rappresentazione binaria di d

    Se per esempio d=10xyznls allora gli indirizzi degli host nella sottorete vanno da 10000000 (128) a 10111111 (191)

Problema

- La notazione CIDR ha reso molto più flessibile l'assegnazione di blocchi di indirizzi (di dimensione variabile) a aziende, istituzioni, utenti privati
- Una volta assegnato un blocco, cosa succede se l'entità che ha ricevuto il blocco ha bisogno di un numero maggiore di indirizzi? (aumentano i dipendenti, aumento i computer in una famiglia)
- Il blocco successivo può essere stato assegnato a un'altra entità
- Soluzione?

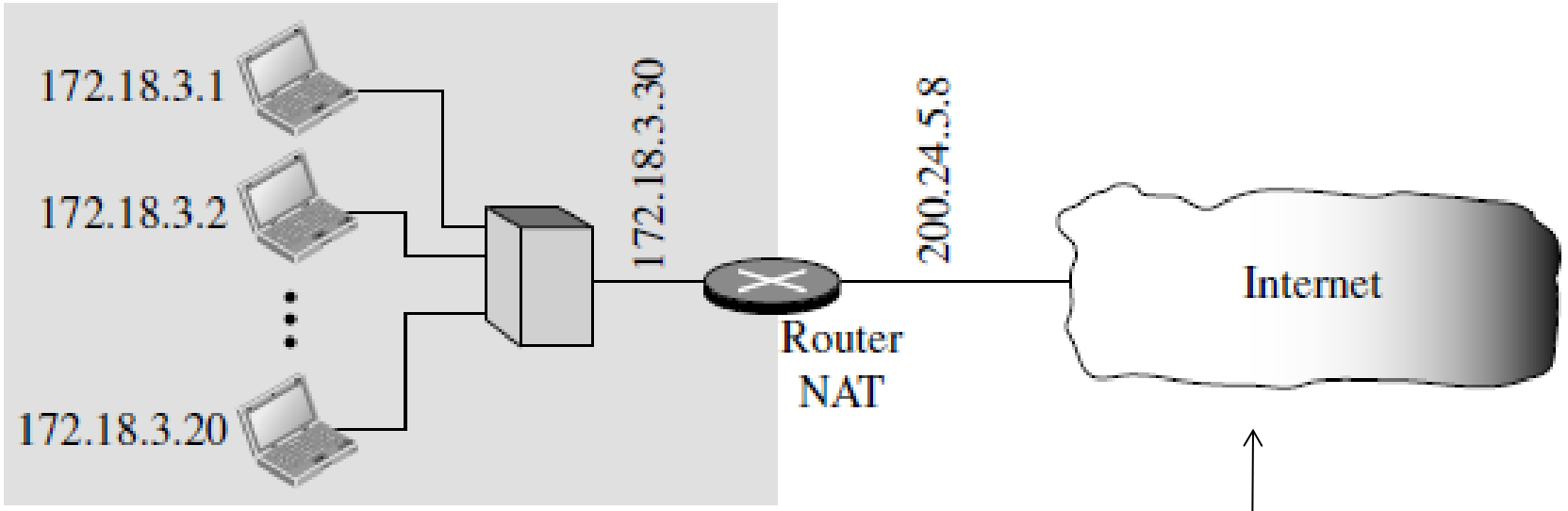
Indirizzi privati

- 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 usano indirizzi privati

Indirizzi	CIDR
10.0.0.0 - 10.255.255.255	10.0.0.0/8
172.16.0.0 - 172.31.255.255	172.16.0.0/12
192.168.0.0 - 192.168.255.255	192.168.0.0/16

  - si adotta la traduzione degli indirizzi di rete (NAT, network address translation)

Traduzione degli indirizzi di rete (NAT)



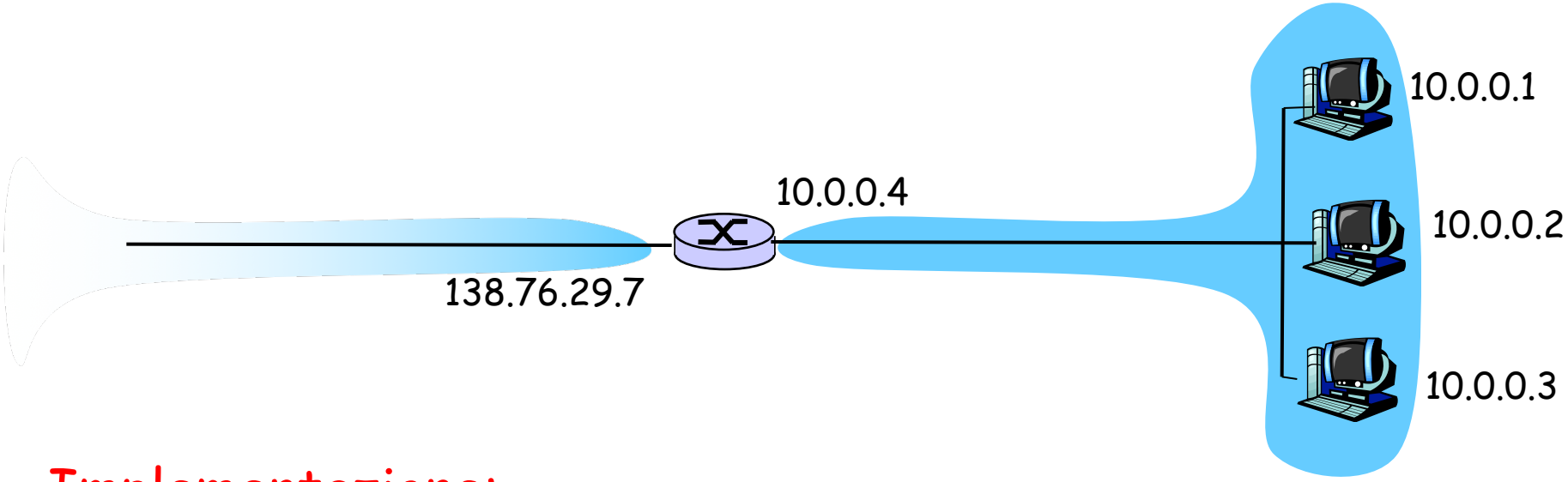
Spazio di indirizzi riservato alle reti private, molte delle quali usano un identico spazio, 172.18.3/24 per scambiare pacchetti tra i loro dispositivi

I router abilitati al NAT non appaiono al mondo esterno come router ma come un *unico* dispositivo con un *unico* indirizzo IP. Indirizzo IP origine: 200.24.5.8, e tutto il traffico verso Internet deve riportare lo stesso indirizzo.

Traduzione degli indirizzi di rete (NAT)

- Il router abilitato al 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 (garantisce maggiore sicurezza)

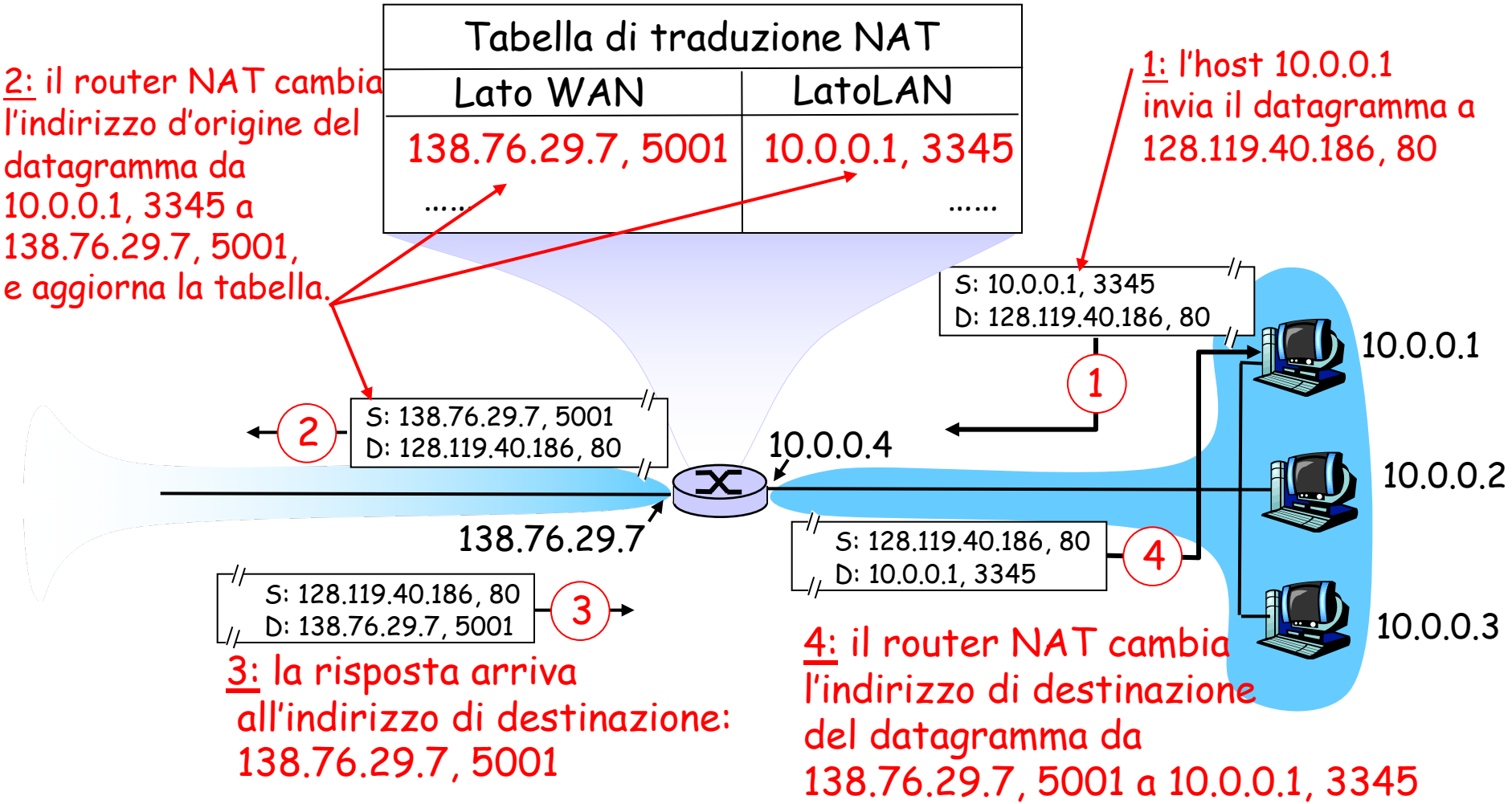
Traduzione degli indirizzi di rete (NAT)



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.

Livello di rete

- Forwarding e routing
- Struttura dei router
- IPv4
  - Formato dei datagrammi IPv4
  - Frammentazione
  - Indirizzamento IPv4 (con classi e senza classi)
  - DHCP
  - NAT
- Forwarding dei datagrammi IP
- ICMP
- Routing

Forwarding datagrammi IP

- Inoltrare significa collocare il datagramma sul giusto percorso (porta di uscita del router) che lo porterà a destinazione (o lo farà avanzare verso la destinazione)
- Inviare il datagramma al prossimo hop
- Quando un host ha un datagramma da inviare lo invia al router della rete locale
- Quando un router riceve un datagramma da inoltrare, accede alla tabella di routing per trovare il successivo hop a cui inviarlo
- L'inoltro richiede una riga nella tabella per ogni blocco di rete

esempio

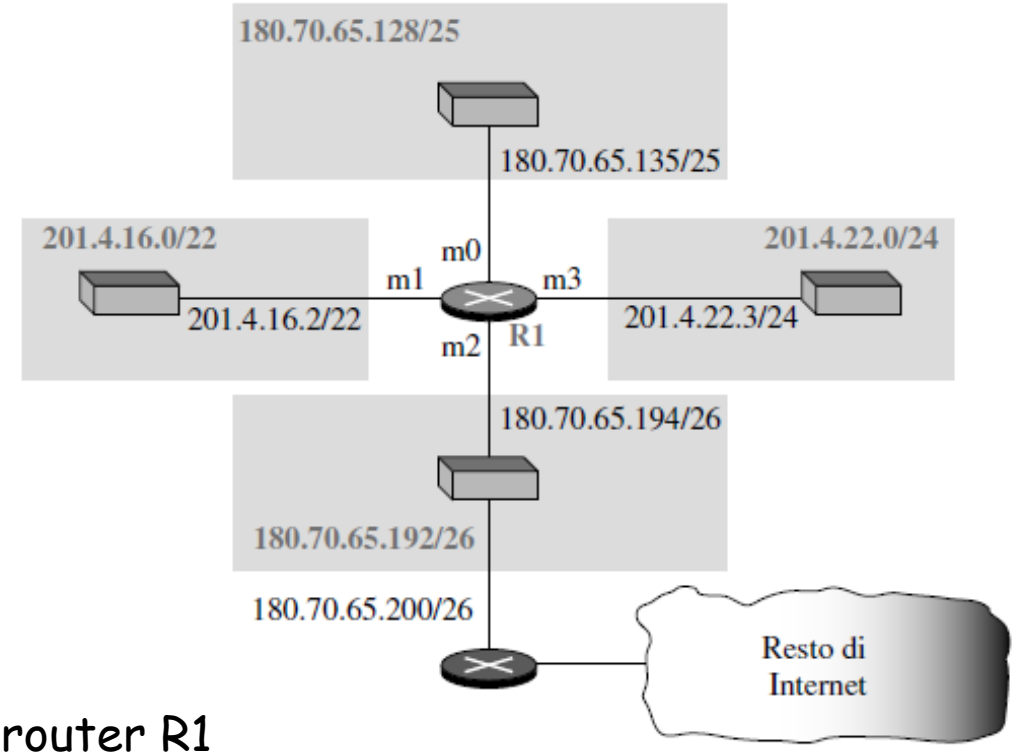


Tabella di inoltro per il router R1

Indirizzo di rete	Hop successivo	interfaccia
180.70.65.192/26	-	m2
180.70.65.128/25	-	m0
201.4.22.0/24	-	m3
201.4.16.0/22	-	m1
default	180.70.65.200	m2

Altra rappresentazione della tabella d'inoltro

Bit a sinistra nell'indirizzo di destinazione	*Salto successivo*	*Interfaccia*
10110100 01000110 01000001 11	–	m2
10110100 01000110 01000001 1	–	m0
11001001 00000100 00011100	–	m3
11001001 00000100 000100	–	m1
Default	180.70.65.200	m2

- All'interno della tabella di routing sono presenti indirizzi di rete (lunghezza inferiore a 32 bit)
- Ma un datagramma contiene l'indirizzo IP dell'host di destinazione (pari a 32 bit) e non indica la lunghezza del prefisso di rete
- Come si esegue l'instradamento?

Altra rappresentazione della tabella d'inoltro

Bit a sinistra nell'indirizzo di destinazione	*Salto successivo*	*Interfaccia*
10110100 01000110 01000001 11	–	m2
10110100 01000110 01000001 1	–	m0
11001001 00000100 00011100	–	m3
11001001 00000100 000100	–	m1
Default	180.70.65.200	m2

Quando arriva un datagramma in cui i 26 bit a sinistra nell'indirizzo di destinazione combaciano con i bit della prima riga, il pacchetto viene inviato attraverso l'interfaccia m2. Analogamente negli altri casi.

La tabella mostra chiaramente che la prima riga ha un prefisso più lungo (che matcha con il successivo) che indica uno spazio di indirizzi più piccolo

esempio

Bit a sinistra nell'indirizzo di destinazione	*Salto successivo*	*Interfaccia*
10110100 01000110 01000001 11	–	m2
10110100 01000110 01000001 1	–	m0
11001001 00000100 00011100	–	m3
11001001 00000100 000100	–	m1
Default	180.70.65.200	m2

Mostrare il processo d'inoltro di un datagramma, con indirizzo di destinazione 180.70.65.140 (10110100 01000110 01000001 10001100), nel caso arrivi a R1.

Soluzione

Il router esegue i seguenti passaggi:

1. La prima maschera (**/26**) ovvero 10110100 01000110 01000001 11 è applicata all'indirizzo di destinazione.

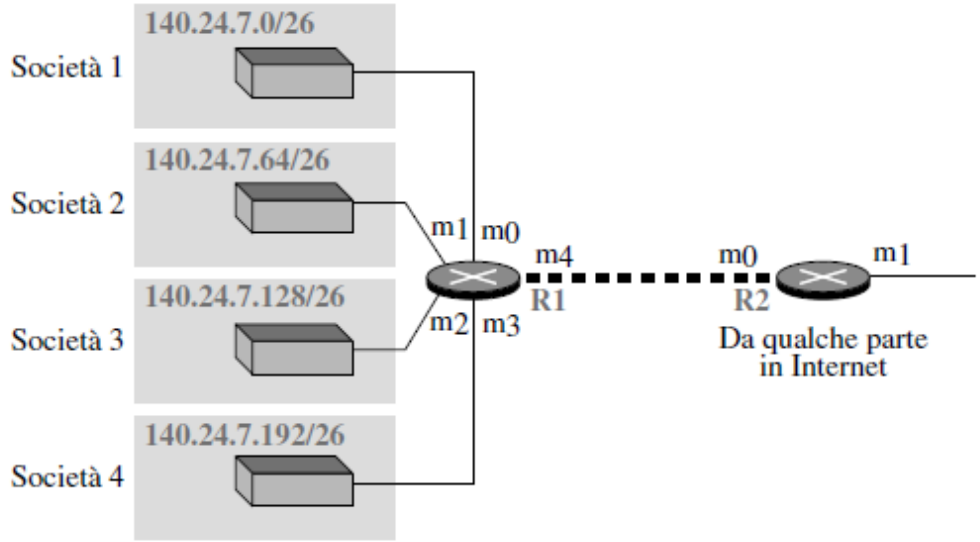
10110100 01000110 01000001 10001100 (indirizzo destinazione)
10110100 01000110 01000001 10000000 (indirizzo di rete della destinazione)

Il risultato è 180.70.65.128, che non combacia con l'indirizzo di rete corrispondente.

2. La seconda maschera (**/25**) è applicata all'indirizzo di destinazione. Il risultato è 180.70.65.128 che combacia con l'indirizzo di rete corrispondente. L'indirizzo del salto successivo e il numero di interfaccia m0 vengono estratti dalla tabella e usati per inoltrare il datagramma.

Aggregazione degli indirizzi

- Inserire nella tabella una riga per ogni blocco può portare a tabelle molto lunghe, con aumento del tempo necessario per fare la ricerca
- Soluzione: aggregazione degli indirizzi



Aggregazione di indirizzi nella tabella di R2

Tabella d'inoltro per R1

Indirizzo di rete/maschera	Indirizzo del salto successivo	Interfaccia
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
140.24.7.192/26	----------	m3
0.0.0.0/0	Indirizzo di R2	m4

Corrispondenza con la maschera più lunga

- Cosa accade se l'organizzazione 4 è connessa al router R2?

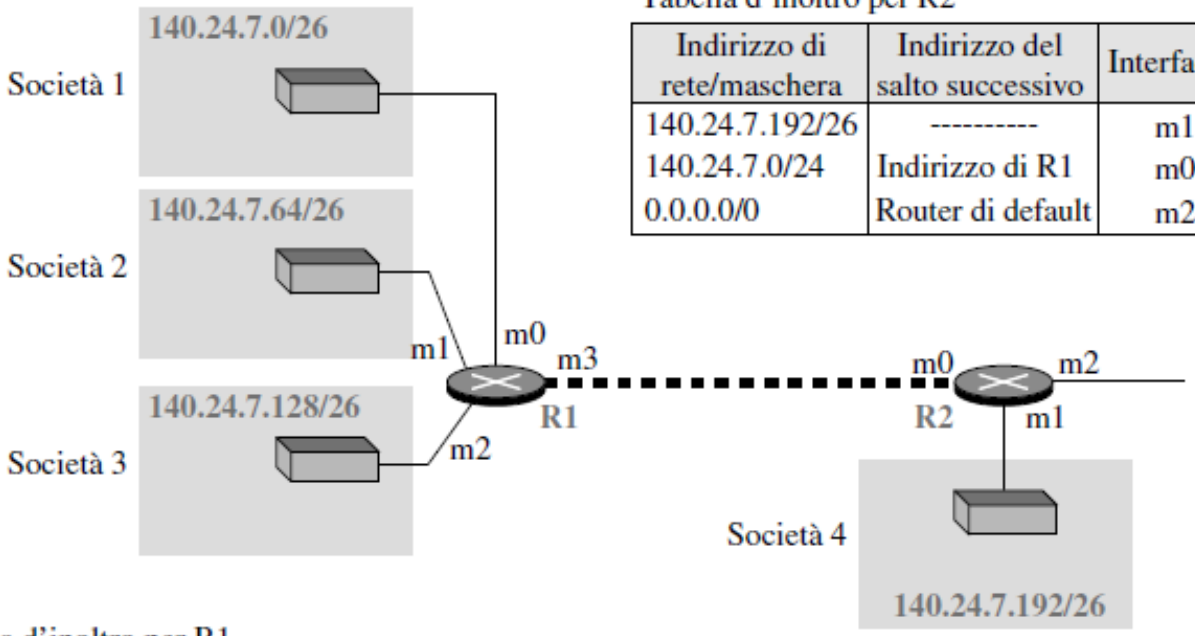


Tabella d'inoltro per R2

Indirizzo di rete/maschera	Indirizzo del salto successivo	Interfaccia
140.24.7.192/26	----------	m1
140.24.7.0/24	Indirizzo di R1	m0
0.0.0.0/0	Router di default	m2

Tabella d'inoltro per R1

Indirizzo di rete/maschera	Indirizzo del salto successivo	Interfaccia
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
0.0.0.0/0	Router di default	m3

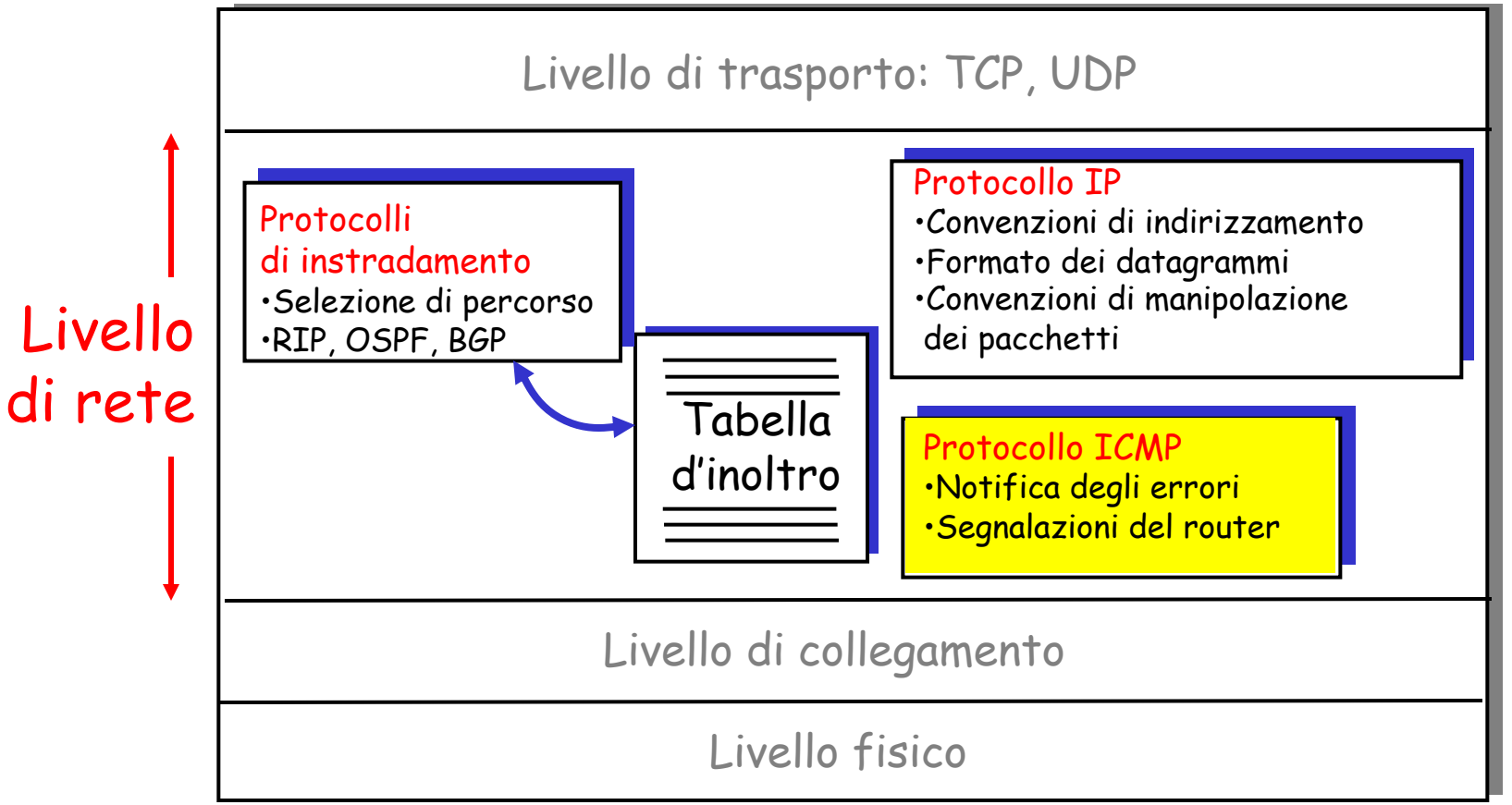
Corrispondenza con la maschera più lunga!!!

Livello di rete

- Forwarding e routing
- Struttura dei router
- IPv4
  - Formato dei datagrammi IPv4
  - Frammentazione
  - Indirizzamento IPv4 (con classi e senza classi)
  - DHCP
  - NAT
- Forwarding dei datagrammi IP
- ICMP
- Routing

Livello di rete

Uno sguardo al livello di rete Internet:



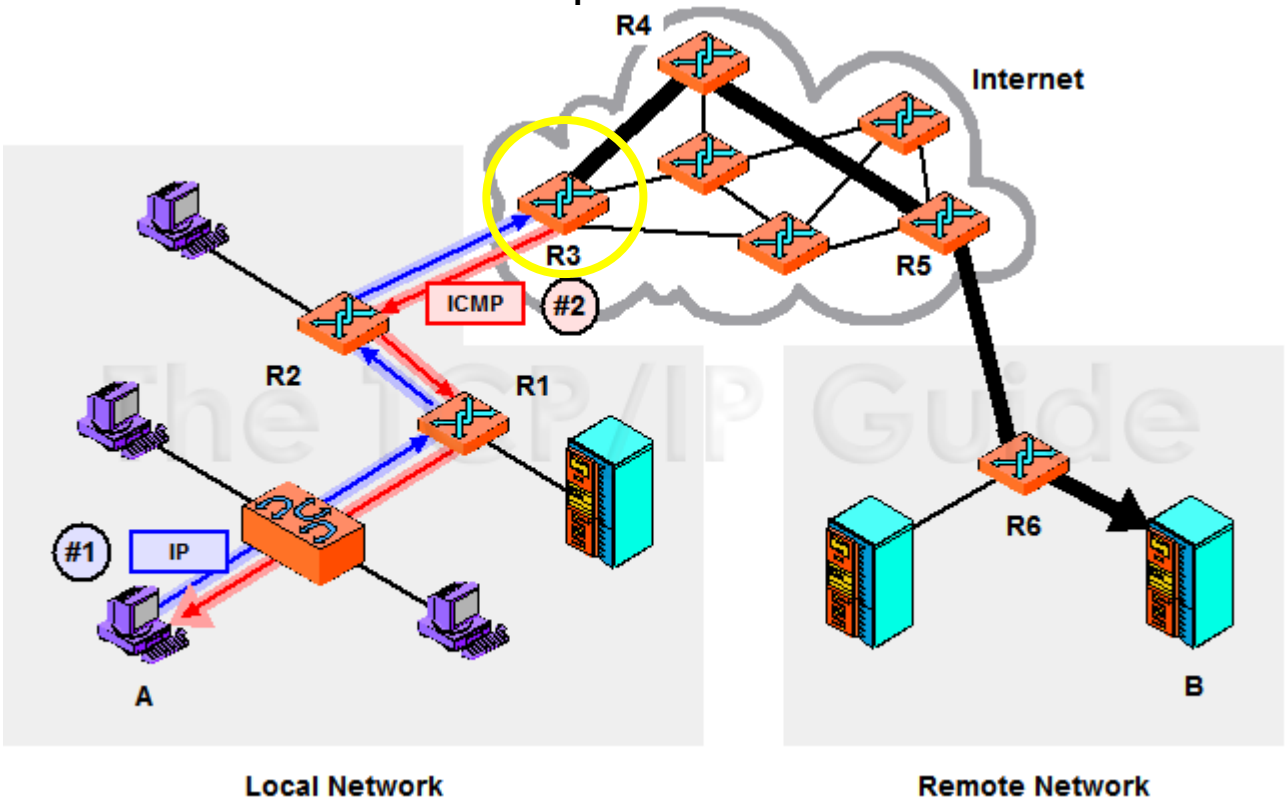
Il campo dati dei datagrammi IP può contenere un messaggio ICMP

Gestione errori?

- Cosa accade se un router deve scartare un datagramma perché non riesce a trovare un percorso per la destinazione finale?
- Cosa accade se un datagramma ha il campo TTL pari a 0?
- E se un host di destinazione non ha ricevuto tutti i frammenti di un datagramma entro un determinato limite di tempo?
- Situazioni di errore che IP non gestisce!

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

Ping

- Il programma *ping* si basa sui messaggi di richiesta e risposta *echo* di ICMP

```
$ ping pads.cs.unibo.it
PING chernobog.pads.cs.unibo.it (130.136.132.11) 56(84) bytes of data.
64 bytes from chernobog.pads.cs.unibo.it (130.136.132.11): icmp_req=1 ttl=52 time=34.2 ms
64 bytes from chernobog.pads.cs.unibo.it (130.136.132.11): icmp_req=2 ttl=52 time=33.1 ms
64 bytes from chernobog.pads.cs.unibo.it (130.136.132.11): icmp_req=3 ttl=52 time=34.0 ms
64 bytes from chernobog.pads.cs.unibo.it (130.136.132.11): icmp_req=4 ttl=52 time=33.9 ms
64 bytes from chernobog.pads.cs.unibo.it (130.136.132.11): icmp_req=5 ttl=52 time=33.3 ms
--- chernobog.pads.cs.unibo.it ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 33.177/33.758/34.220/0.417 ms
```

Traceroute e ICMP

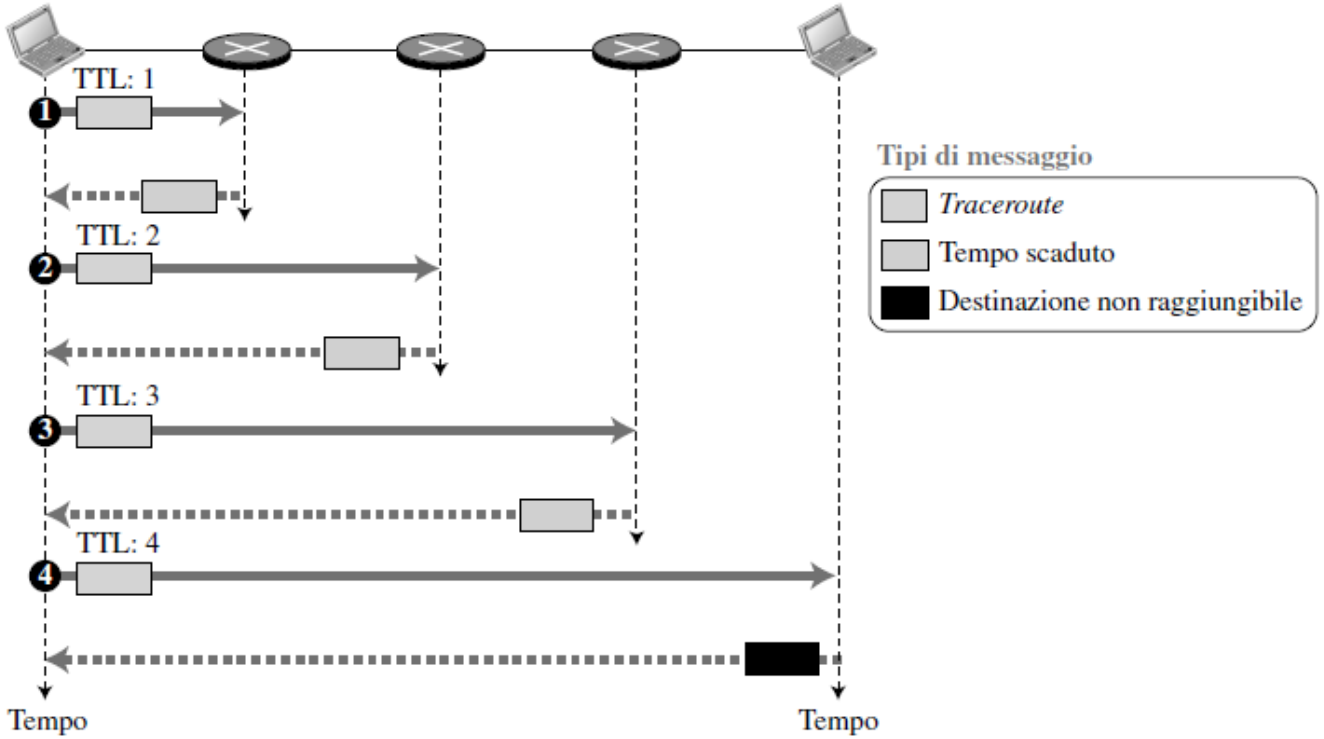
- Il programma invia una serie di datagrammi IP alla destinazione ciascuno contenente un segmento UDP con un numero di porta inutilizzata.
  - Il primo pari a TTL =1
  - Il secondo pari a TTL=2, ecc.
  - Numero di porta improbabile
  - L'origine avvia un timer per ogni datagramma
- Quando l'*n*-esimo 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.

traceroute

- Non c'è un programma server (ma solo un client)
- Le risposte arrivano da ICMP (tempo scaduto dai router intermedi e porta non raggiungibile dall'host di destinazione)



Livello di rete

- Forwarding e routing
- Struttura dei router
- IPv4
  - Formato dei datagrammi IPv4
  - Frammentazione
  - Indirizzamento IPv4 (con classi e senza classi)
  - DHCP
  - NAT
- Forwarding dei datagrammi IP
- ICMP
- Routing

Esercizio

- Quali protocolli/applicazioni sono generatori di pacchetti?