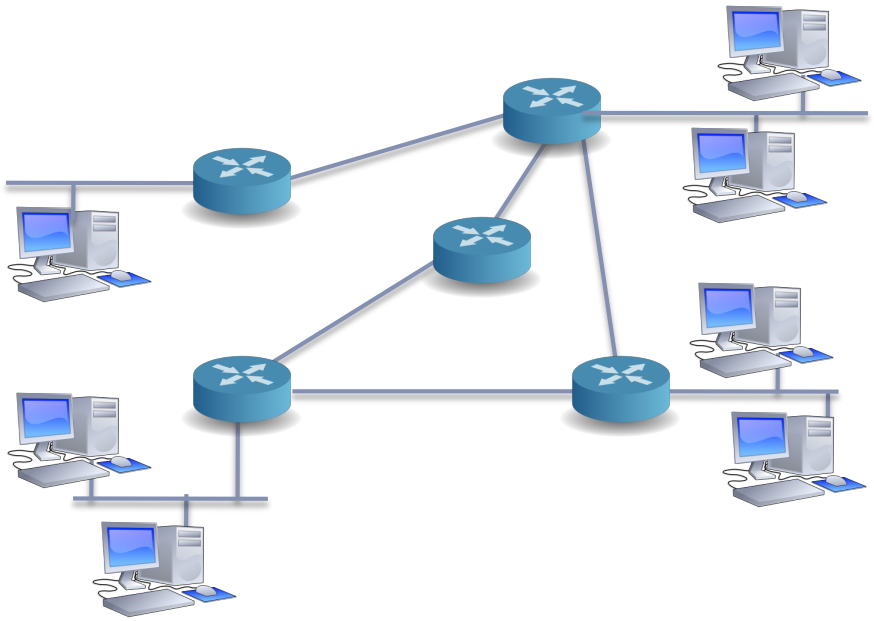
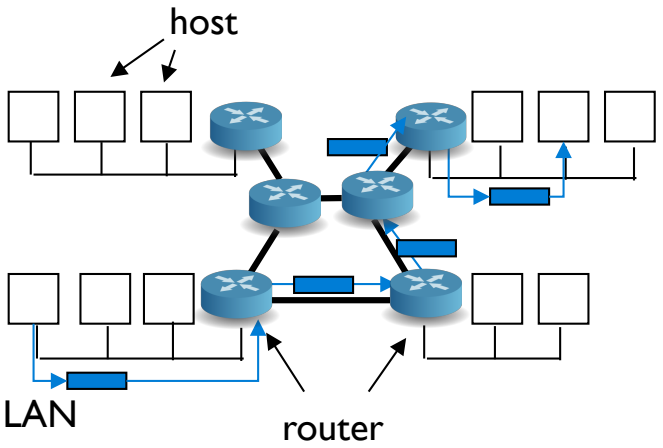


Reti di Calcolatori

Network Layer & IP

Il livello di rete

- Trasmissione host-to-host di pacchetti dati
- Connessione di reti fisiche basate su tecnologie anche diverse (internetworking)
  - Definizione di uno schema di indirizzamento logico globale degli host (indirizzi pubblici di rete)
  - Uso di nodi intermedi di instradamento (router) per connettere le reti fra loro
    - Ogni nodo router connette due o più reti fisiche
    - La rete ha una struttura a grafo
    - L'instradamento è possibile se è nota la topologia del grafo
    - I router instradano i pacchetti sulle loro linee di uscita in modo da indirizzarli verso la destinazione
    - I percorsi sono scelti in modo ottimale (es. per evitare sovraccarichi)



Tipologie di instradamento

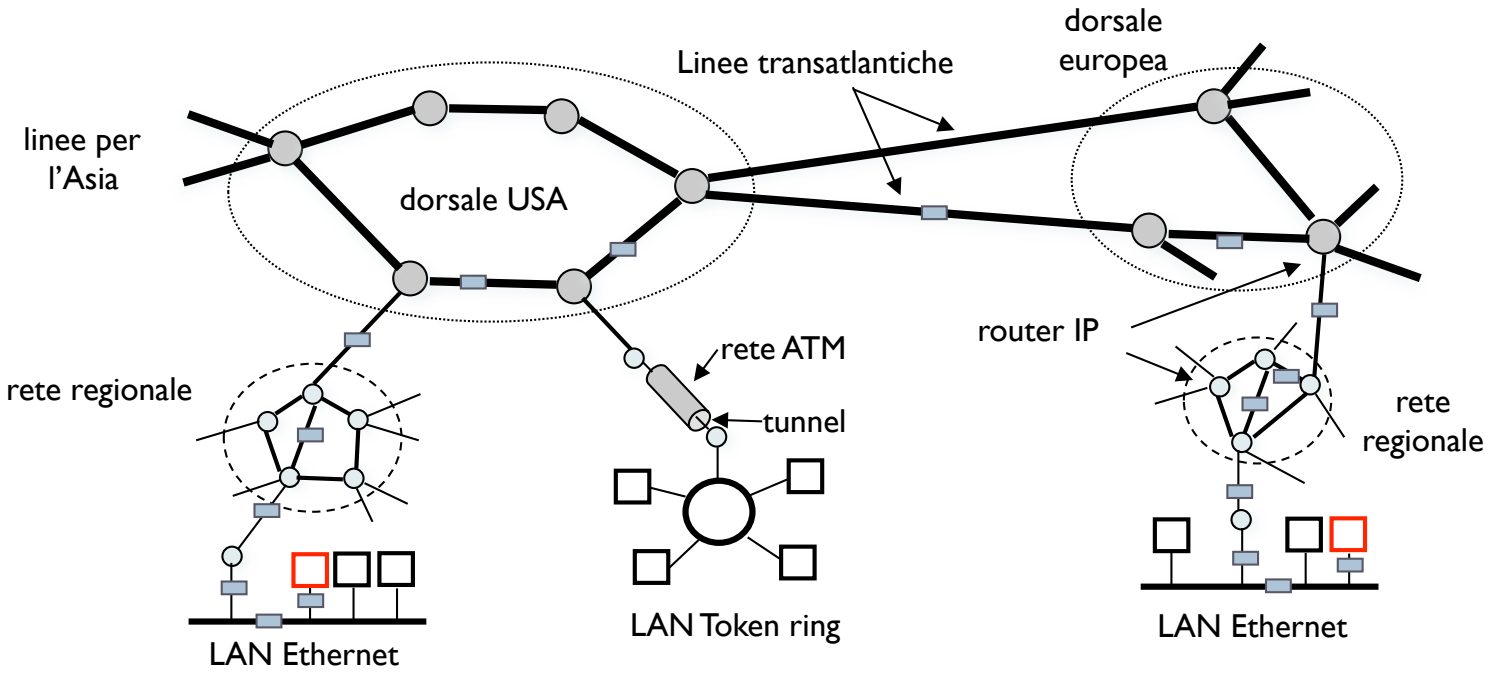
- Con connessione (circuiti virtuali) (es. ATM)
  - Prevede una fase di connessione per la definizione del percorso di consegna dalla sorgente alla destinazione
    - Si configura ogni router associando all'identificatore (indirizzo) del circuito virtuale l'uscita su cui instradare i pacchetti appartenenti al circuito
    - I router devono mantenere memoria dei circuiti virtuali che passano attraverso di essi
  - Il percorso è lo stesso per tutti i pacchetti associati al circuito virtuale
    - I pacchetti contengono indicazione del circuito virtuale a cui appartengono
- Senza connessione (datagram) (es. Internet)
  - La decisione di instradamento viene presa per ogni pacchetto
    - Il percorso da un host sorgente ad un host destinazione non è predefinito ma dipende dalle scelte fatte dai nodi via via attraversati
    - I pacchetti fra due host possono seguire anche percorsi diversi
    - I pacchetti contengono l'indirizzo dell'host destinatario (e del mittente)
  - I router hanno tabelle che indicano quale linea di uscita utilizzare per ogni possibile "destinazione"

Datagram vs Circuiti Virtuali

Caratteristica	**Reti basate su datagrammi**	**Reti basate su circuito virtuale**
Creazione circuito	Non richiesto	Richiesto
Indirizzamento	Ogni pacchetto contiene gli indirizzi sorgente e destinazione completi	Ogni pacchetto contiene un piccolo numero VC (Virtual Circuit)
Informazioni di stato	La sottorete non conserva informazioni di stato	Ogni circuito virtuale richiede spazio nelle tabelle dei router nella sottorete
Instradamento	Ogni pacchetto è instradato indipendentemente	Percorso scelto alla creazione del circuito virtuale: tutti i pacchetti seguono questo percorso
Effetti dei guasti nei router	Nessuno, a parte i pacchetti persi durante il guasto	Tutti i circuiti virtuali che passano attraverso il router guasto vengono terminati
Controllo di congestione	Complesso	Semplice se può essere allocato spazio sufficiente in anticipo per ogni circuito virtuale
Ordine dei pacchetti	Non è garantito che l'ordine di consegna sia lo stesso dell'ordine di invio	I pacchetti arrivano nello stesso ordine con cui sono stati inviati

Internet

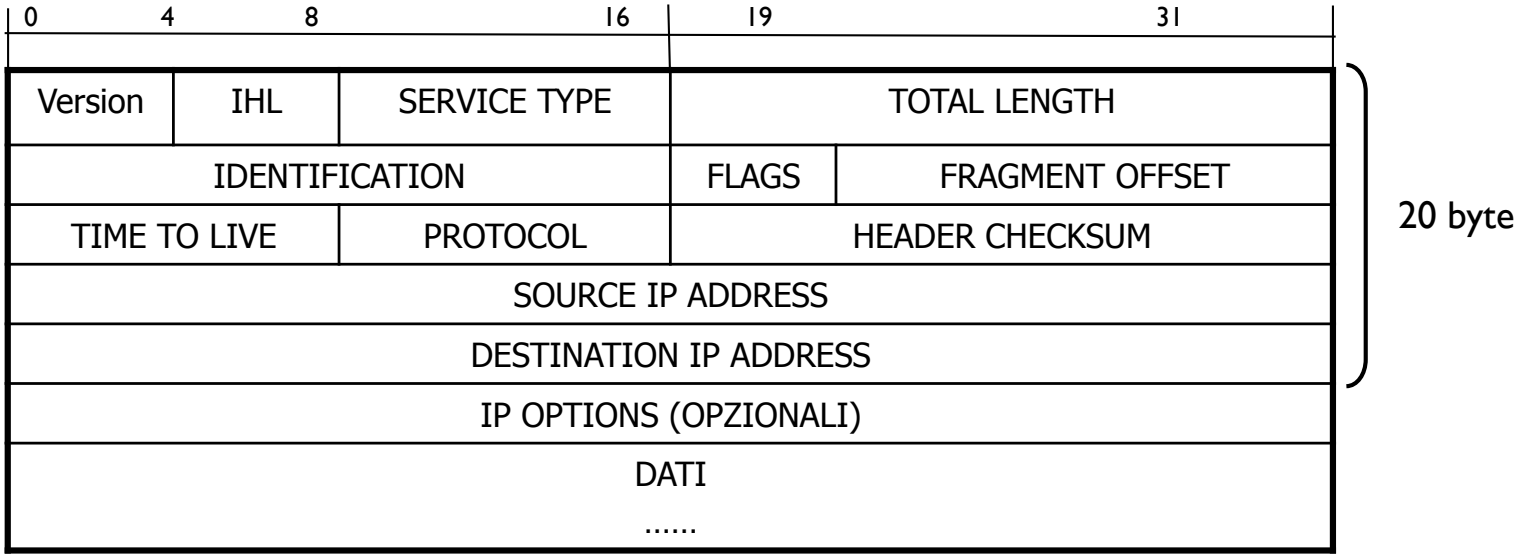
- E' una collezione di sottoreti connesse insieme
  - Backbone (dorsali) ad alta capacità con router veloci
  - Reti regionali
  - Reti locali



Internet Protocol (IP)

- Standardizzato in RFC 791 è la base di Internet
- E' un protocollo senza connessione best-effort
  - I datagrammi contengono l'identità della destinazione
  - Ogni datagramma viene spedito/gestito indipendentemente
  - Non è garantita la consegna

datagram IP



Header IP – word 1

Version	IHL	SERVICE TYPE	TOTAL LENGTH	
IDENTIFICATION			FLAGS	FRAGMENT OFFSET
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM	

- Version permette di mantenere compatibilità fra le versioni
- IHL è la lunghezza del preambolo in parole da 32 bit (su 4 bit)
  - Al massimo il preambolo è 15x4 = 60 byte
  - Il campo opzionale può contenere fino a 40 byte (60-20)
- SERVICE TYPE individua il tipo di servizio desiderato in termini di affidabilità, velocità e ritardo
  - Può influenzare le scelte di routing
- TOTAL LENGTH riguarda l'intero datagram (header e dati)
  - La lunghezza massima del datagram è di 2^{16}-1=65535 byte

Header IP – word 2

Version	IHL	SERVICE TYPE	TOTAL LENGTH	
IDENTIFICATION			FLAGS	FRAGMENT OFFSET
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM	

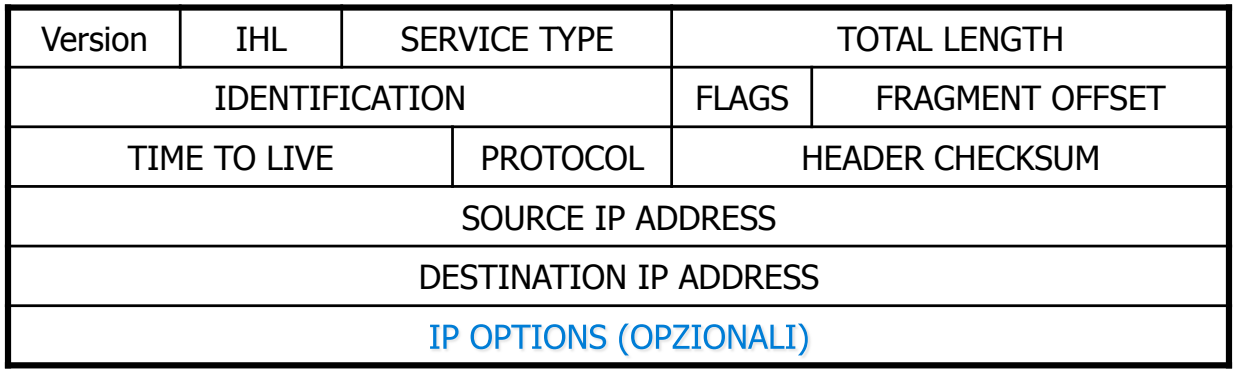
- Gestione della frammentazione dei datagram
  - Può essere necessaria se si invia un datagram su reti con protocolli datalink basati su pacchetti di lunghezza massima minore (es. Ethernet con 1500 byte/pacchetto)
  - I frammenti (eccetto l'ultimo) sono multipli di 8 byte
  - IDENTIFICATION è l'identificatore del datagram a cui appartiene il frammento
  - FRAGMENT OFFSET (13 bit) identifica il numero d'ordine del frammento
    - Si possono avere un massimo di 8192 frammenti
  - FLAGS permettono di indicare che il pacchetto non è frammentabile (Don't Fragment) e che ci sono ulteriori frammenti (More Fragments)

Header IP – word 3

Version	IHL	SERVICE TYPE	TOTAL LENGTH	
IDENTIFICATION			FLAGS	FRAGMENT OFFSET
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM	

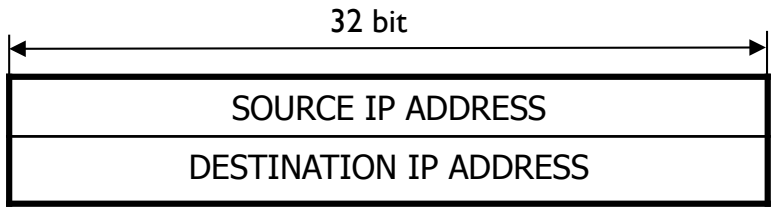
- TIME TO LIVE è un contatore utilizzato per limitare la vita dei pacchetti
  - E' in secondi (0-255)
  - Dovrebbe essere decrementato ad ogni salto (hop) su un router (o se rimane per più tempo in coda)
  - Quando il contatore si azzera il pacchetto è scartato e si invia una notifica al mittente
- PROTOCOL individua il protocollo di trasporto (es. TCP o UDP)
- HEADER CHECKSUM verifica solo l'header
  - deve essere ricalcolato ad ogni hop se cambia il campo TIME TO LIVE

Header IP Options



- Ogni opzione inizia con 1 byte che la identifica
  - Può essere seguito da 1 byte che ne indica la lunghezza
  - Seguono i dati relativi all'opzione attivata
  - Alcuni esempi
    - Strict source routing – specifica il percorso dalla sorgente alla destinazione con una sequenza di indirizzi IP
    - Record route – forza i router ad aggiungere i loro IP nel campo opzione del pacchetto (max 9 router)
    - Timestamp – aggiunge oltre all'IP dei router sul percorso anche un timestamp a 32 bit

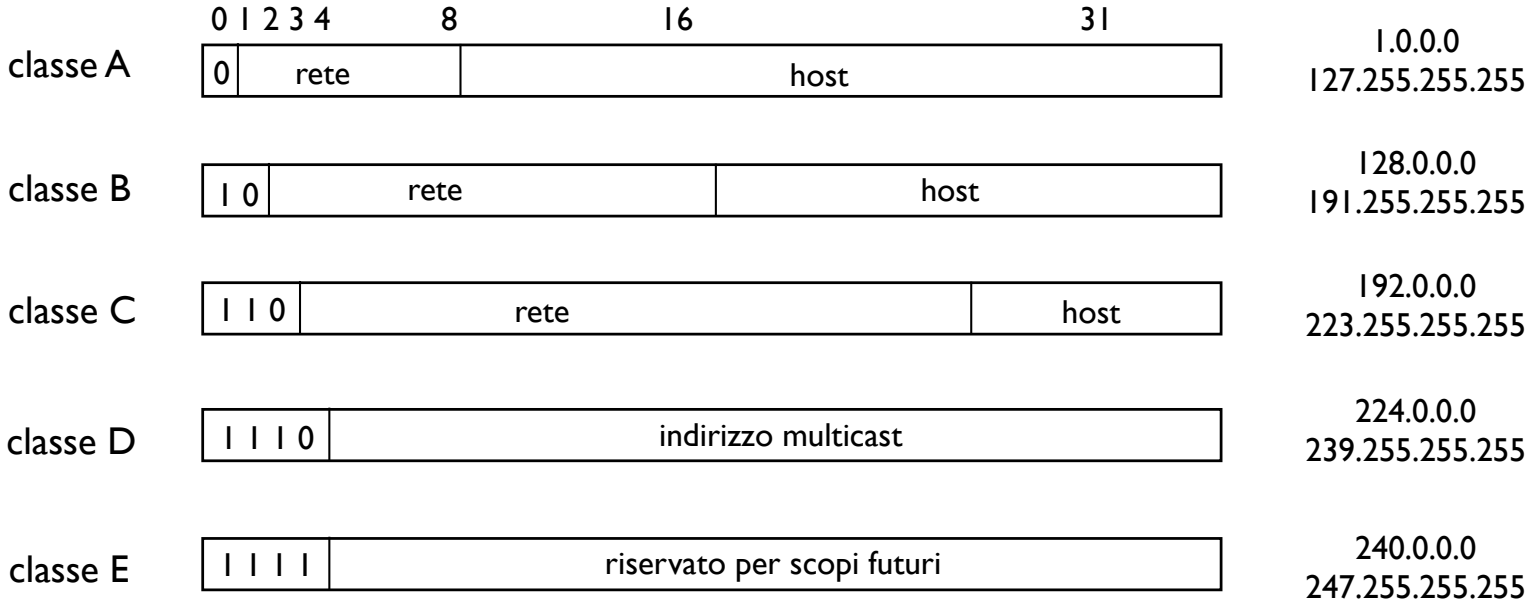
Indirizzamento IP



- L'indirizzo IP a 32 bit identifica univocamente un dispositivo (host o router) sulla rete
  - Gli indirizzi IP pubblici sulla rete Internet sono assegnati dal NIC (Network Information Center)
  - Due dispositivi connessi alla rete Internet non possono avere lo stesso IP
- L'indirizzo può essere scomposto in due parti
  - Indirizzo di rete
  - Indirizzo di host nella rete

Classi di indirizzi IP

- In base alla divisione rete – host sono state definite classi di indirizzi standard



Dimensioni delle reti

classe	bit nel prefisso	numero massimo di reti	bit nel suffisso	numero massimo di host per rete
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

- Non tutte le configurazioni sono indirizzi utilizzabili per host
  - Sono definiti indirizzi speciali
- Dimensioni delle reti
  - A grosse organizzazioni
  - B medie organizzazioni
  - C piccole organizzazioni

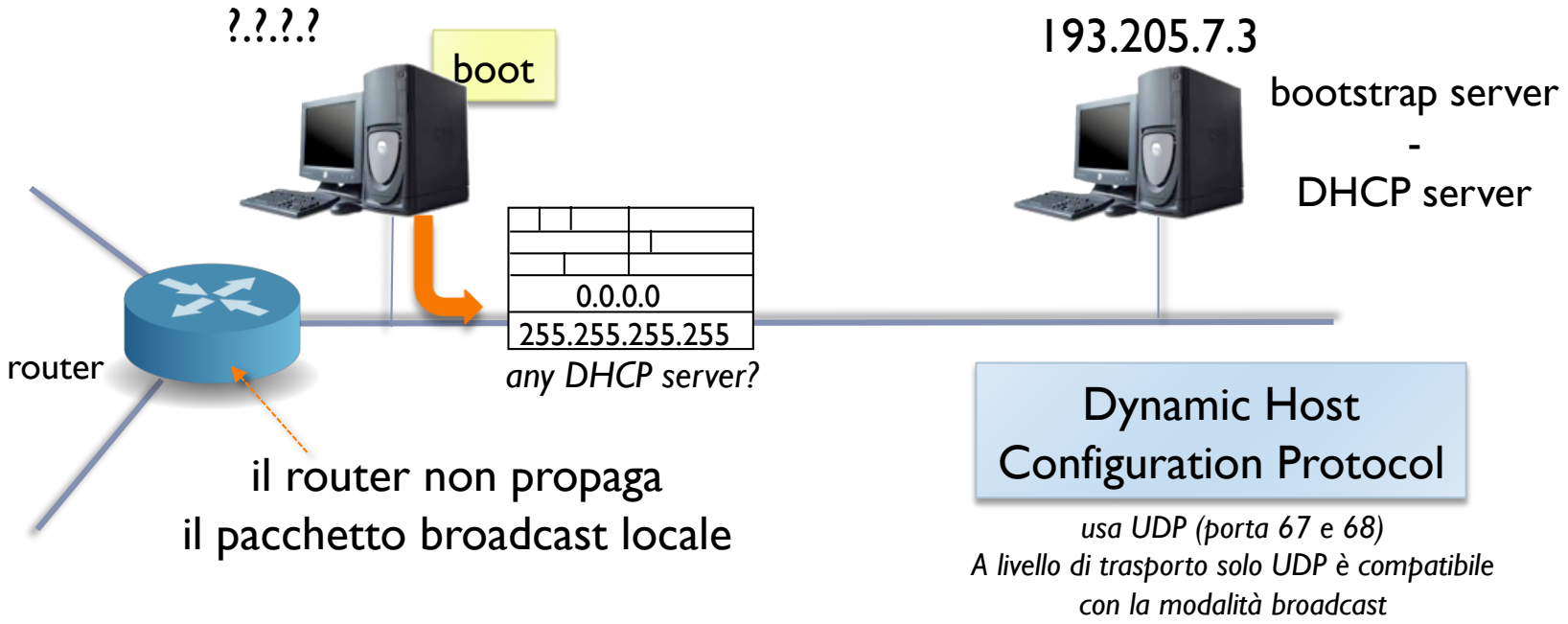
Indirizzi speciali

prefisso	suffisso	tipo di indirizzo	scopo
tutti 0	tutti 0	questo computer	utilizzato nel boot
rete	tutti 0	la rete	identifica una rete
rete	tutti 1	broadcast diretto	broadcast su una rete specifica
tutti 1	tutti 1	broadcast limitato	broadcast sulla rete locale
127	qualsiasi	loopback	test

- I pacchetti di broadcast limitato sono confinati alla sottorete dal router che non li propaga all'esterno
- Con gli indirizzi di loopback il pacchetto non viene immesso sulla rete
  - Il pacchetto viene smistato localmente nel modulo del livello rete (non viene passato al livello fisico)

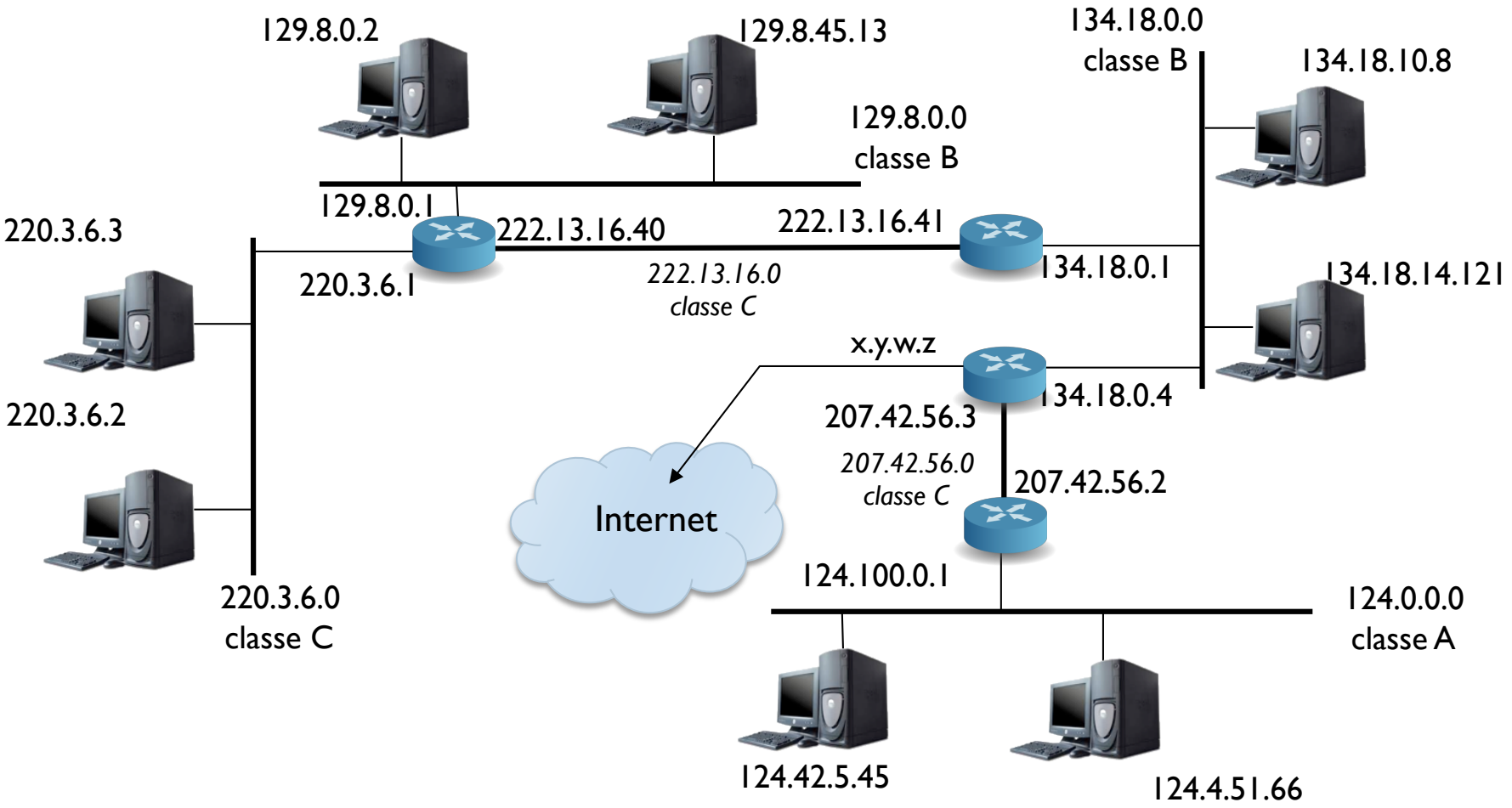
0.0.0.0 e 255.255.255.255

0.0.0.0 – questo host su questa rete
255.255.255.255 – broadcast limitato sulla rete corrente



- La modalità broadcast UDP può essere utilizzata per fare discovery di servizi su una rete locale

Un esempio di inter-rete



Indirizzi privati

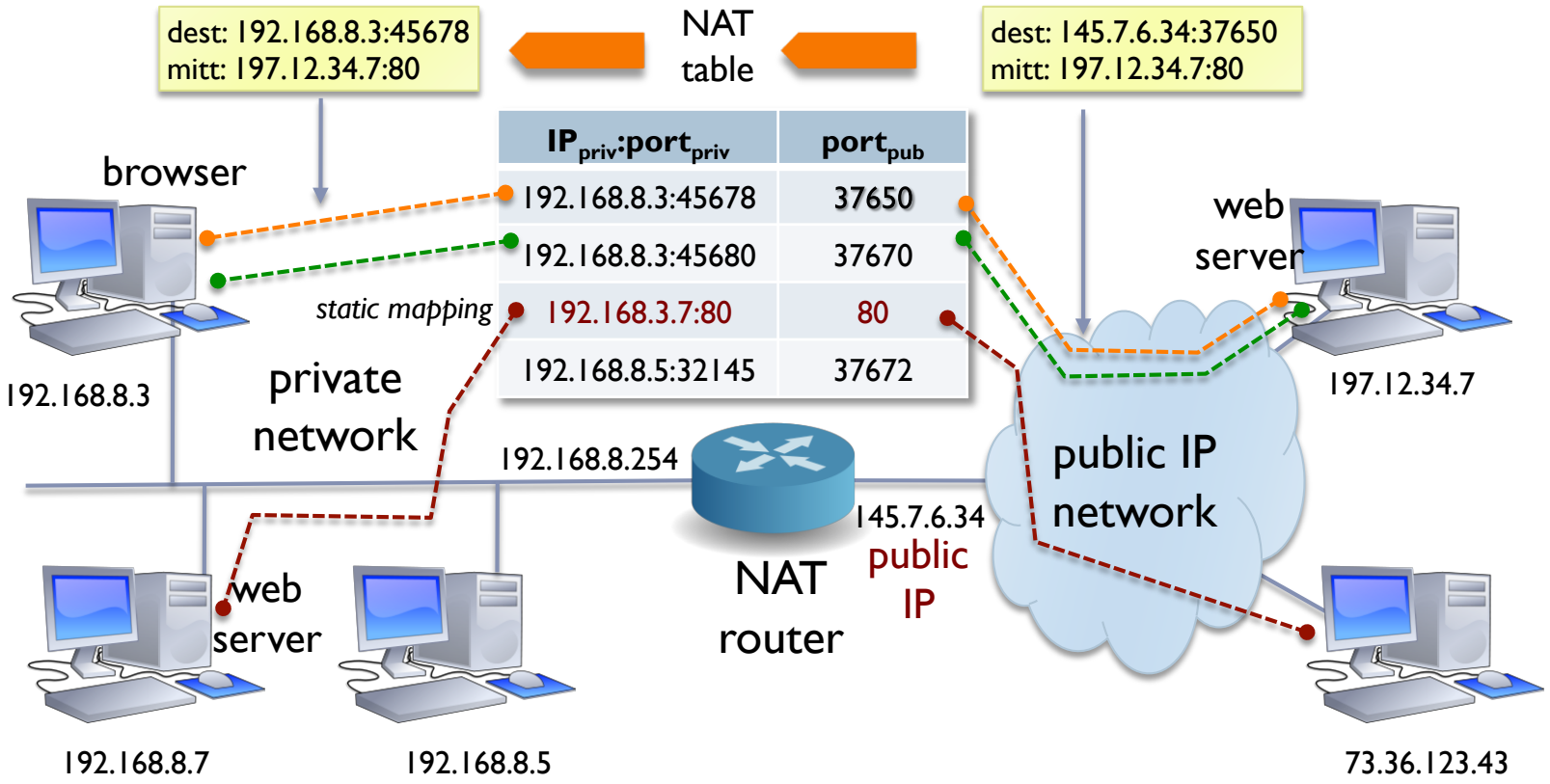
- Sono stati riservati indirizzi per reti non connesse direttamente alla rete Internet
  - Sono indirizzi locali e non pubblici
  - Devono rimanere confinati alla sottorete
  - La rete può accedere alla rete Internet pubblica per mezzo di un gateway che implementa una tecnica di Network Address Translation (NAT)

classe	rete	numero reti
A	10.0.0.0	1
B	Da 172.16 a 172.31	16
C	Da 192.168.0 a 192.168.255	256

NAT

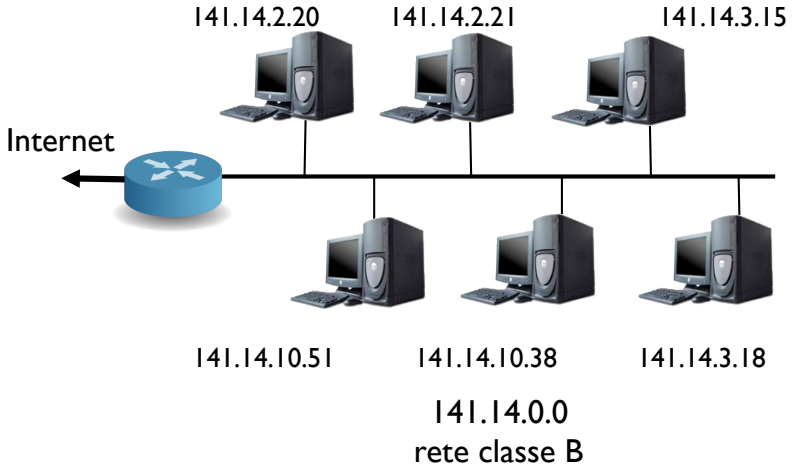
- Permette l'accesso alla rete pubblica da una rete privata
  - Il mapping è one-to-many ovvero tutti gli host della rete privata accedono alla rete pubblica condividendo un unico IP pubblico
    - Il mapping richiede di modificare le intestazioni sia a livello di rete che a livello di trasporto (TCP/UDP)
    - Il meccanismo NAT permette la comunicazione in automatico attraverso un router quando la comunicazione origina dall'interno
      - Le coppie IP_{priv}:$port_{priv}$ sono mappate in coppie IP_{pub}:$port_{pub}$ dal router NAT
      - Il router mantiene una tabella NAT che permette di instradare all'host/porta della rete privata i pacchetti ricevuti dall'esterno
    - E' possibile anche configurare manualmente le tabelle del NAT per rendere pubblici dei servizi in esecuzione su host della rete privata (port forwarding)
      - Ad esempio si può associare la porta 80 del router alla porta 80 di un host interno per rendere accesibile dalla rete pubblica il server Web

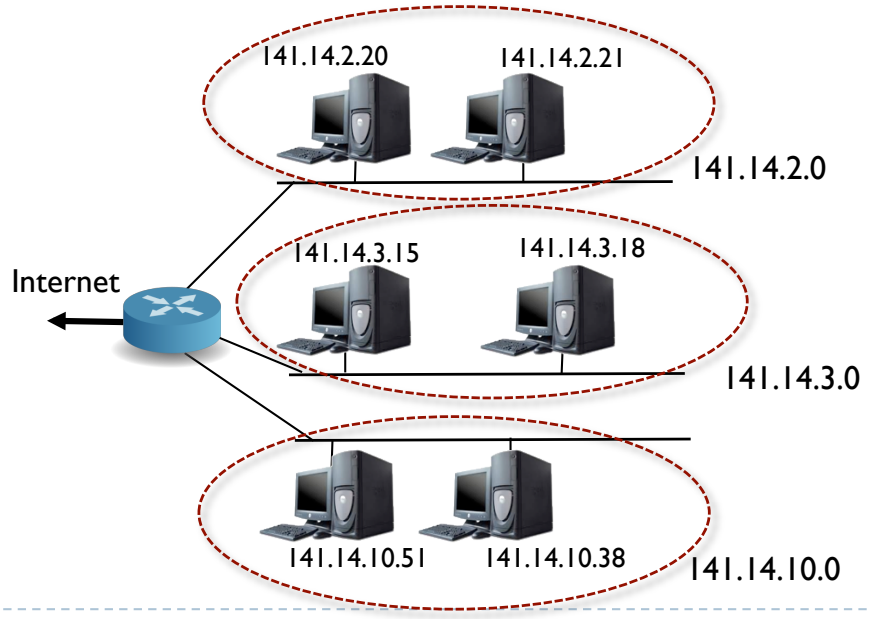
Rete privata con NAT



Subnetting

- Le classi standard definiscono una gerarchia a 2 livelli
  - Rete
  - Host
- Può essere utile suddividere la rete in sottoreti per gestire separatamente un numero minore di host
  - Si crea una gerarchia a più livelli (>2)

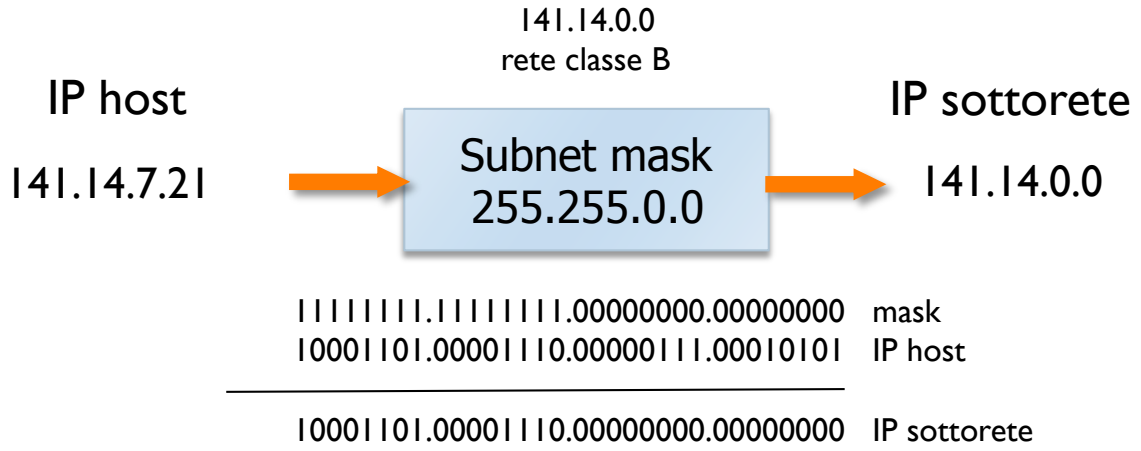




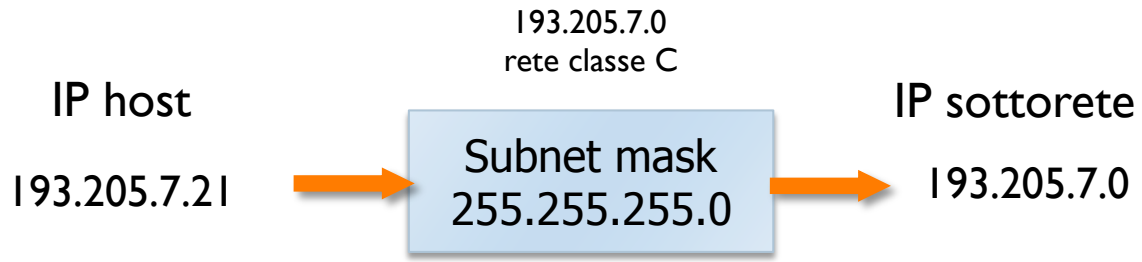
Subnet Mask

- Si utilizza un maschera di bit a 1 nelle posizioni corrispondenti alla parte di indirizzo riferita alla rete
  - Permette di verificare se un indirizzo destinazione appartiene alla propria sottorete calcolando l'AND bit a bit

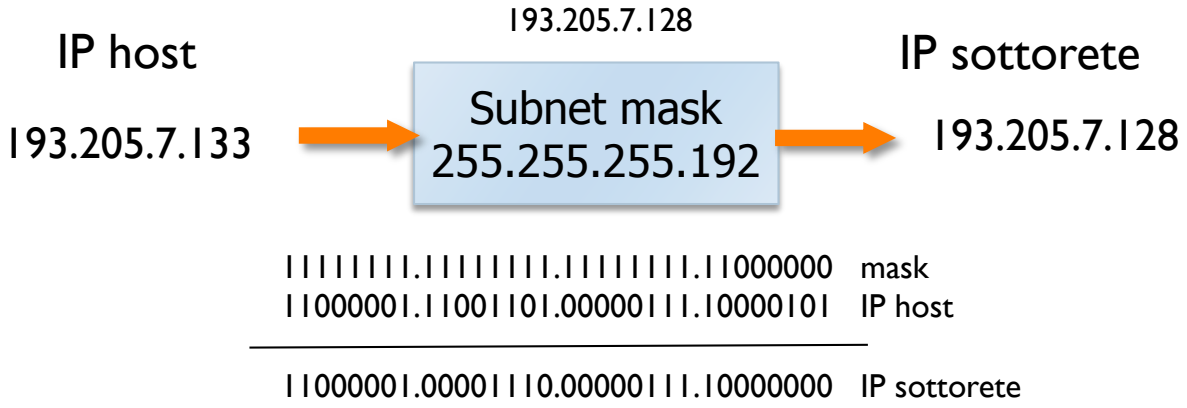
```
if((address & subnet_mask) == mynetwork_address)
  {.. stessa sottorete .. }
```



Subnet mask per classe C



- Si può suddividere una rete di classe C in sottoreti
  - Ad esempio sottoreti di 62 host (6 bit) – 4 sottoreti possibili



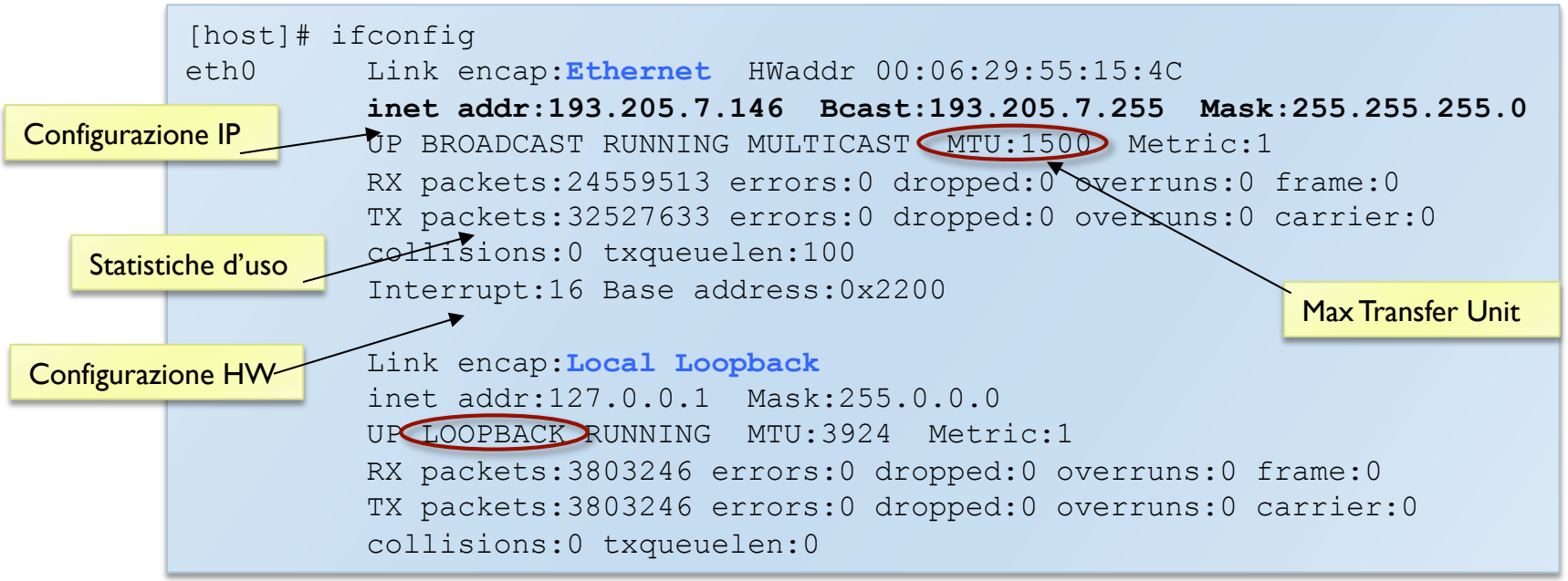
Subnet mask per sottoreti

- Le subnet mask per le classi standard sono
  - classe A 255.0.0.0
  - classe B 255.255.0.0
  - classe C 255.255.255.0
- Se si creano sottoreti, la sottorete è individuata da bit aggiuntivi nella parte prevista per l'host

n bit	bit netmask	valore decimale	numero sottoreti	indirizzi sottorete	range indirizzi
1	10000000	128	2	128	0-127, 128-255
2	11000000	192	4	64	0-63,64-127,128-191, 192-255
3	11100000	224	8	32	0-31,32-63,.....,192-223,224-255
4	11110000	240	16	16	0-15,16-31,...,224-239,240-255
5	11111000	248	32	8	0-7,8-15,.....,240-247,248-255
6	11111100	252	64	4	0-3,4-7,....,248-251,252-255
7	11111110	254	128	2	0-1,2-3,....,252-253,254-255
8	11111111	255	256	1	0,1,2,.....,253,254,255

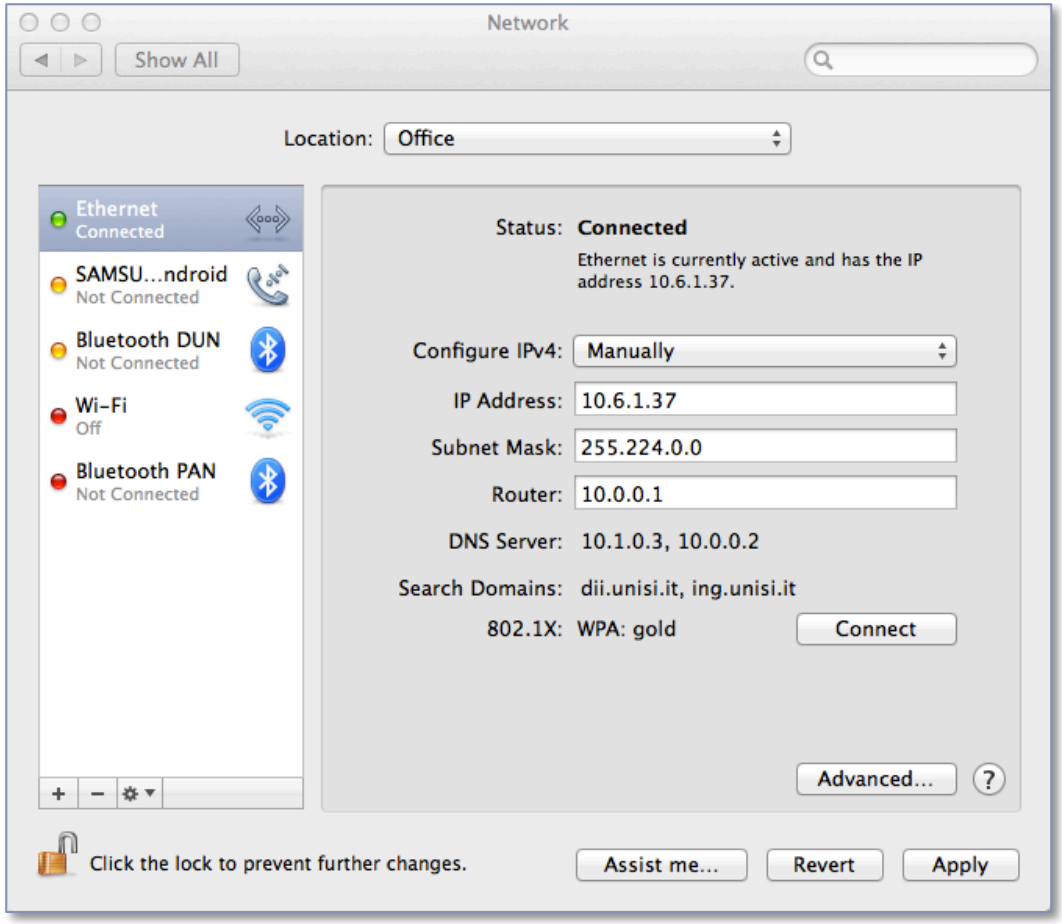
Configurare la scheda di rete

- Su Unix il comando ifconfig configura la scheda di rete
  - La abilita/disabilita (up/down)
  - Definisce i parametri hardware (es. irq, io_addr)
  - Definisce i parametri della connessione di rete (indirizzo, netmask,..)
  - Abilita funzionalità particolare (modo promiscuo – promisc)



Configurazione da pannello

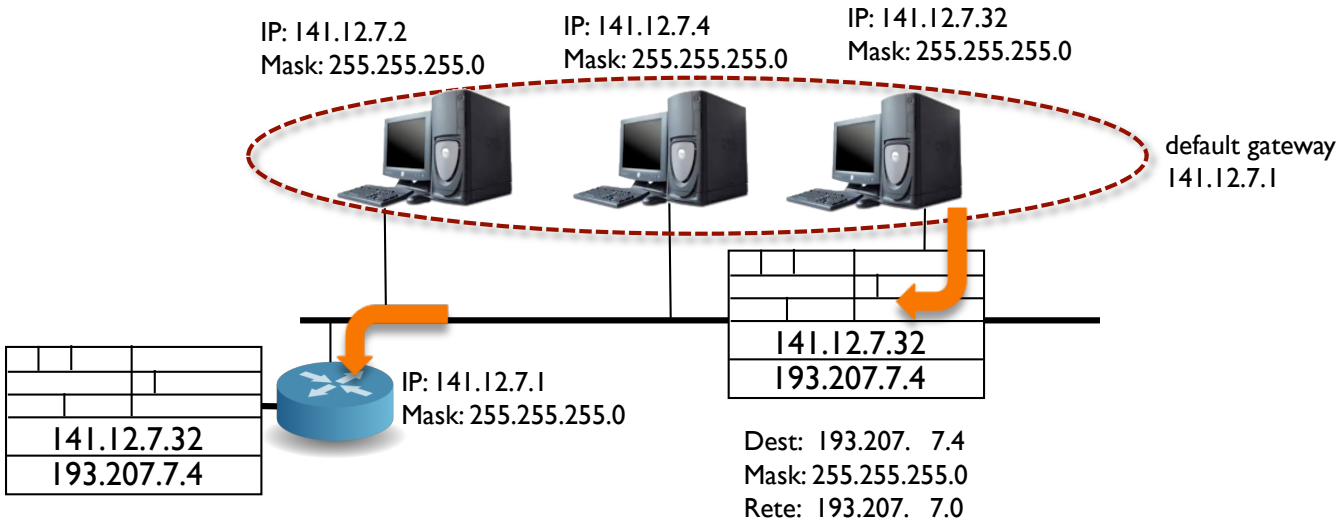
- Il pannello delle preferenze per la rete permette di configurare l'indirizzo
  - configurazione manuale
    - IP
    - netmask
    - default gateway (router)
    - DNS server
  - configurazione automatica
    - uso di DHCP server
- La configurazione si può effettuare per ogni dispositivo di rete



Subnet mask e instradamento

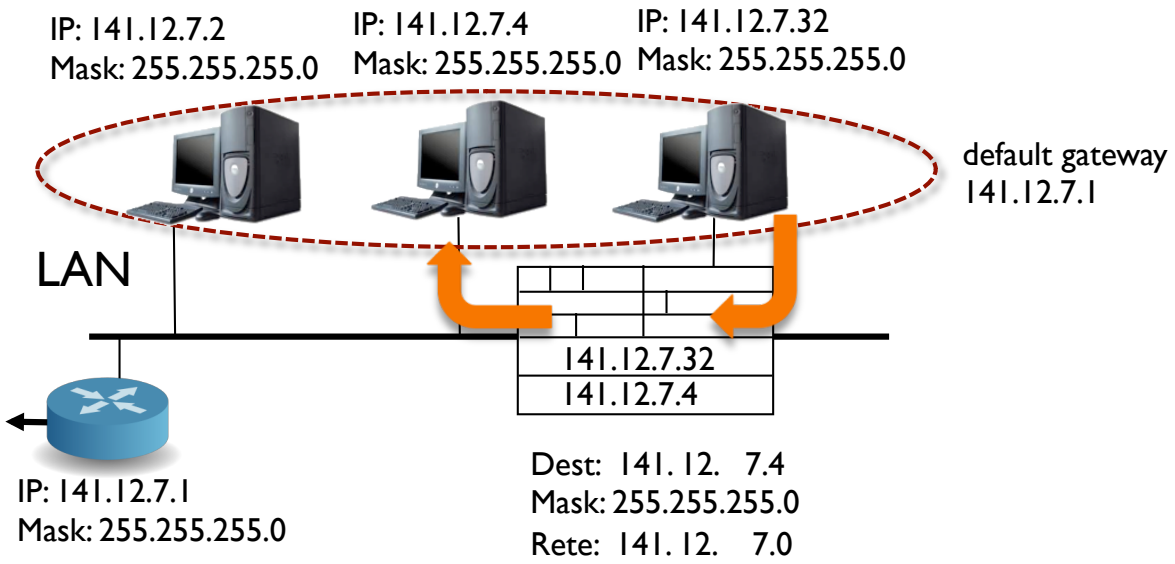
- La subnet mask permette di verificare se l'indirizzo destinatario di un pacchetto IP appartiene alla stessa sottorete del mittente
  - Se l'host destinatario non è nella stessa sottorete il pacchetto deve essere instradato verso il router (gateway)

```
if(!((address & subnet_mask) == mynetwork_address))
  {.. send to default gateway (router) .. }
```



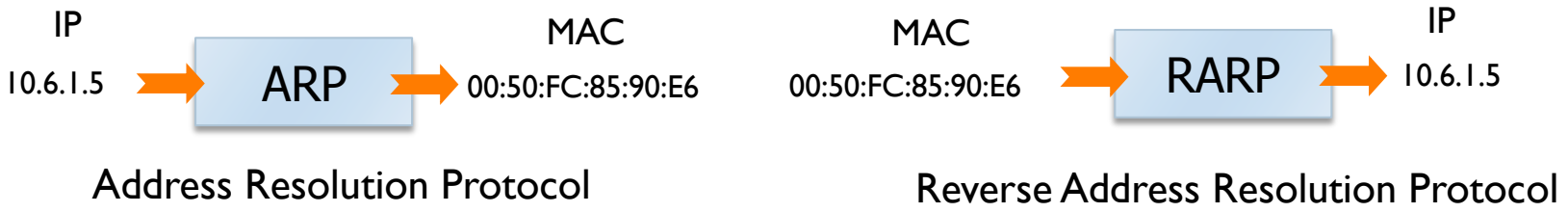
Consegna diretta

- Il destinatario è un host sulla stessa sottorete LAN del mittente
- Si verifica se l'indirizzo della rete è lo stesso usando la netmask
  - Occorre associare all'indirizzo IP del destinatario il suo **indirizzo fisico**
  - Esempio: **conversione IP→Indirizzo ethernet** (indirizzo MAC a 48 bit)
  - Si usa il protocollo **ARP** (Address Resolution Protocol)



Protocolli ARP e RARP

- L'associazione IP-Indirizzo fisico può essere
  - Statica
    - Si compila una tabella con le associazioni che deve essere memorizzata su tutti i dispositivi della sottorete
    - Richiede di aggiornare periodicamente le tabelle
    - E' poco flessibile
  - Dinamica
    - Permette di ricavare l'associazione inoltrando una richiesta su rete

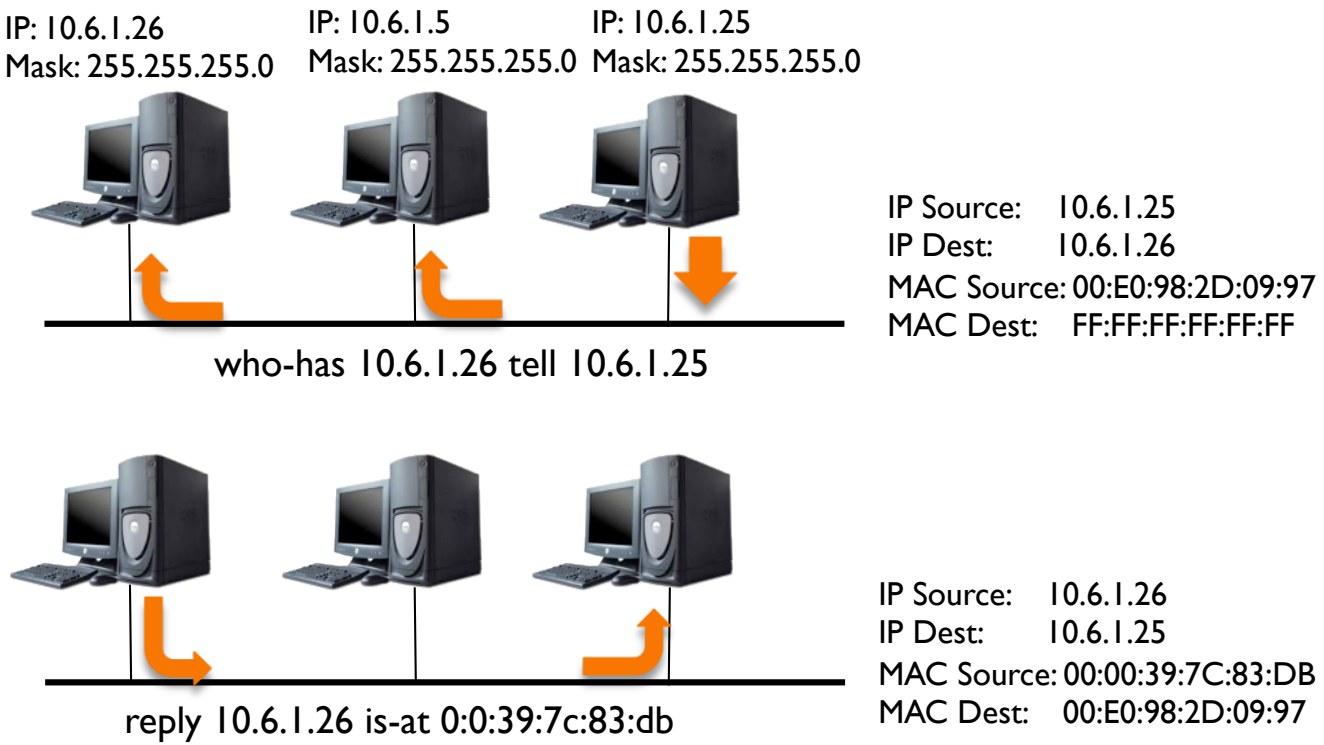


Address Resolution Protocol

Reverse Address Resolution Protocol

Protocollo ARP

- La richiesta è inoltrata in broadcast sulla sottorete
- La macchina che ha l'indirizzo IP risponde col suo indirizzo MAC (Media Access Control)
  - nel caso della rete LAN Ethernet è un indirizzo a 48 bit



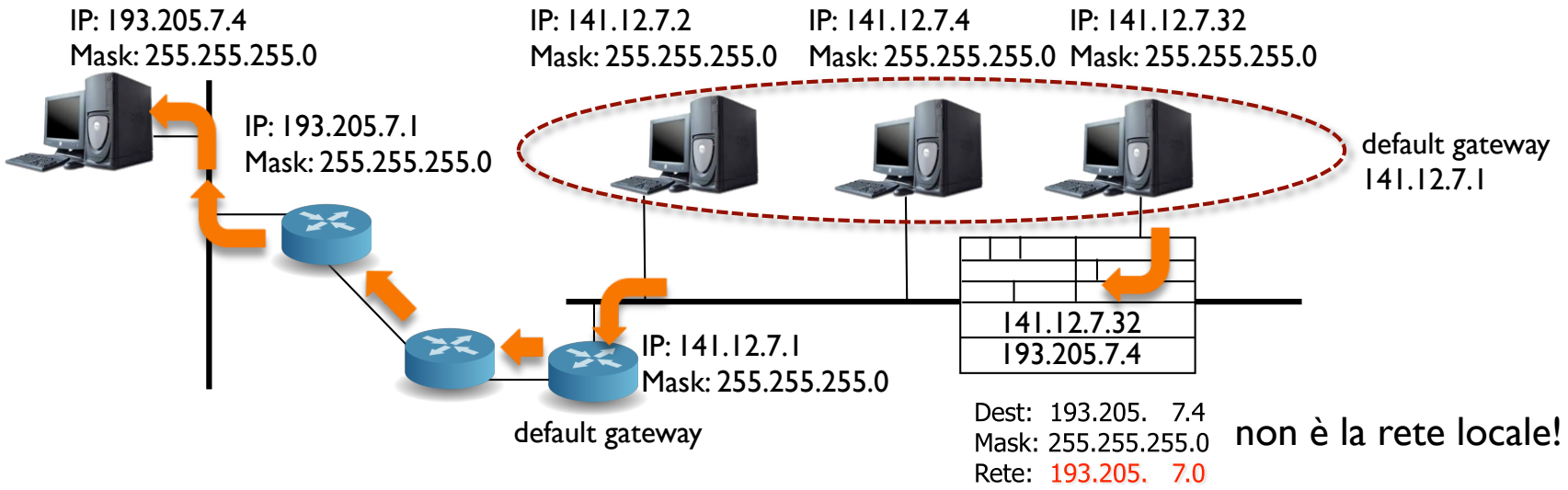
Cache ARP

- Per evitare di risolvere l'IP in indirizzo MAC per ogni pacchetto si mantiene una cache locale
- Su Unix si può gestire la cache col comando arp
  - Consultare la cache
  - Aggiungere o cancellare elementi

```
[host]# arp -n
Address       HWtype  HWaddress           Flags Mask  Iface
193.205.7.1   ether   00:00:0C:3A:99:C6   C           eth0
193.205.7.2   ether   00:10:5A:2E:5A:CE   C           eth0
```

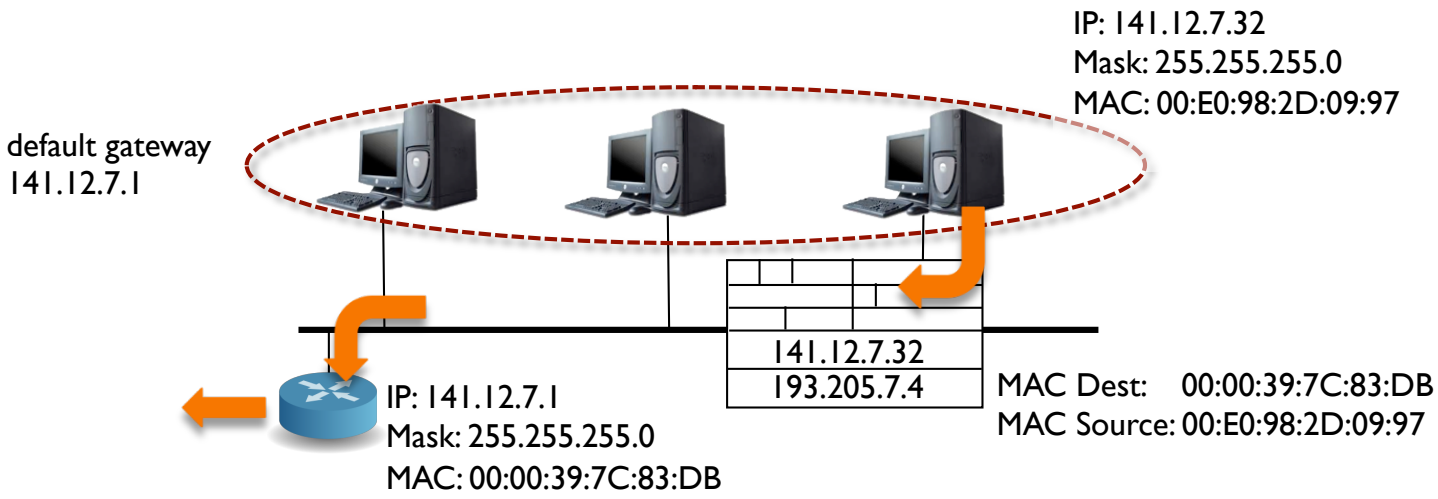
Consegna indiretta

- La destinazione finale è un host connesso ad una rete fisica LAN diversa da quella in cui si trova il mittente
  - Il mittente verifica che la destinazione non è sulla sua sottorete e usa le informazioni di routing (tabella di routing)



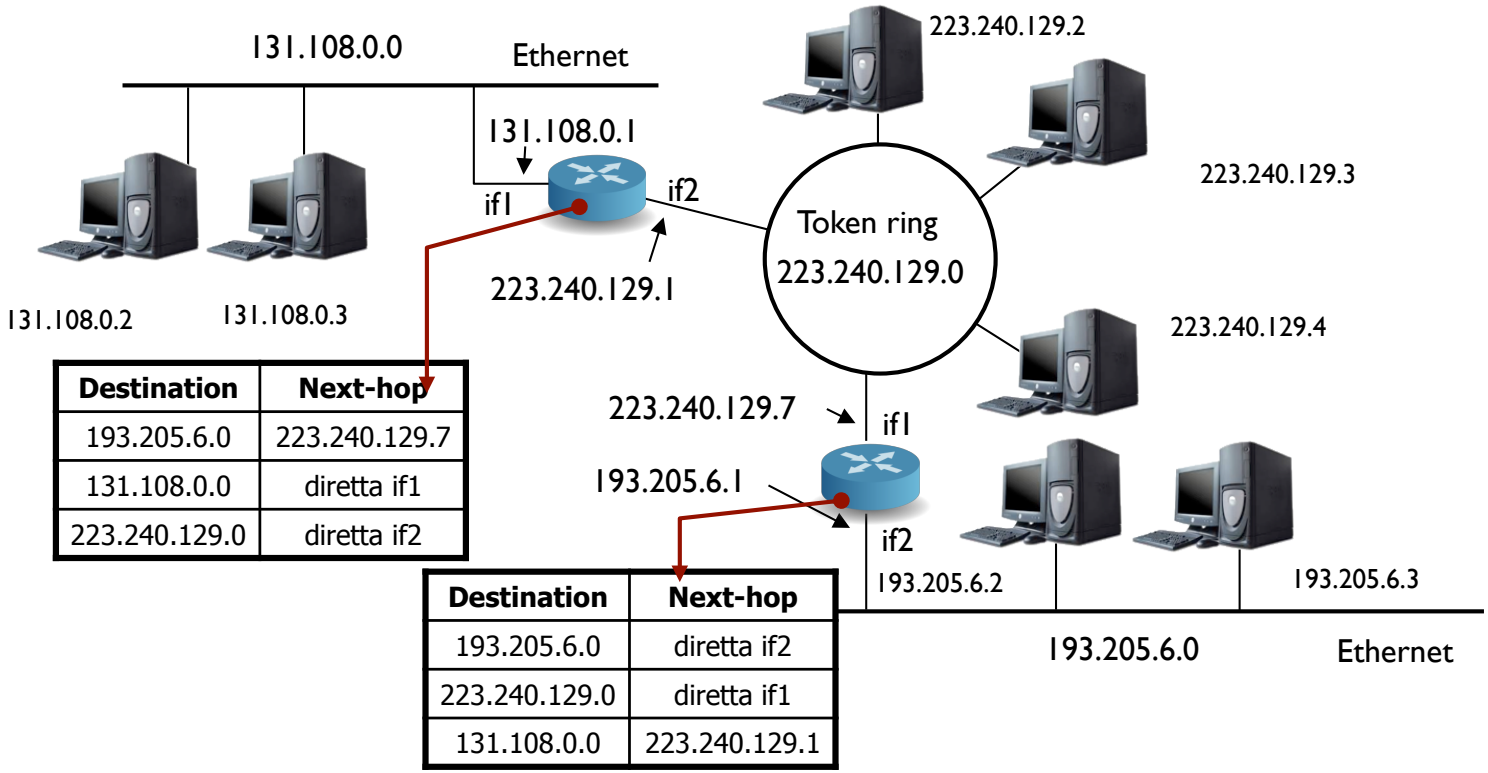
Default gateway

- Sull'host può essere definita una tabella di routing che specifica il gateway a cui inviare i pacchetti per ogni specifica destinazione
- Di solito si specifica un gateway di default che è l'IP del router sulla sottorete (se c'è un solo router)
- Il pacchetto viene inviato direttamente al gateway utilizzando il suo indirizzo MAC



Instradamento next-hop

- Il router utilizza le tabelle di routing per individuare il percorso verso la destinazione finale
  - Non si memorizza l'intero percorso ma solo il prossimo "salto" (hop)
  - Le entry della tabella sono sottoreti (l'instradamento è in genere per gruppi di IP)

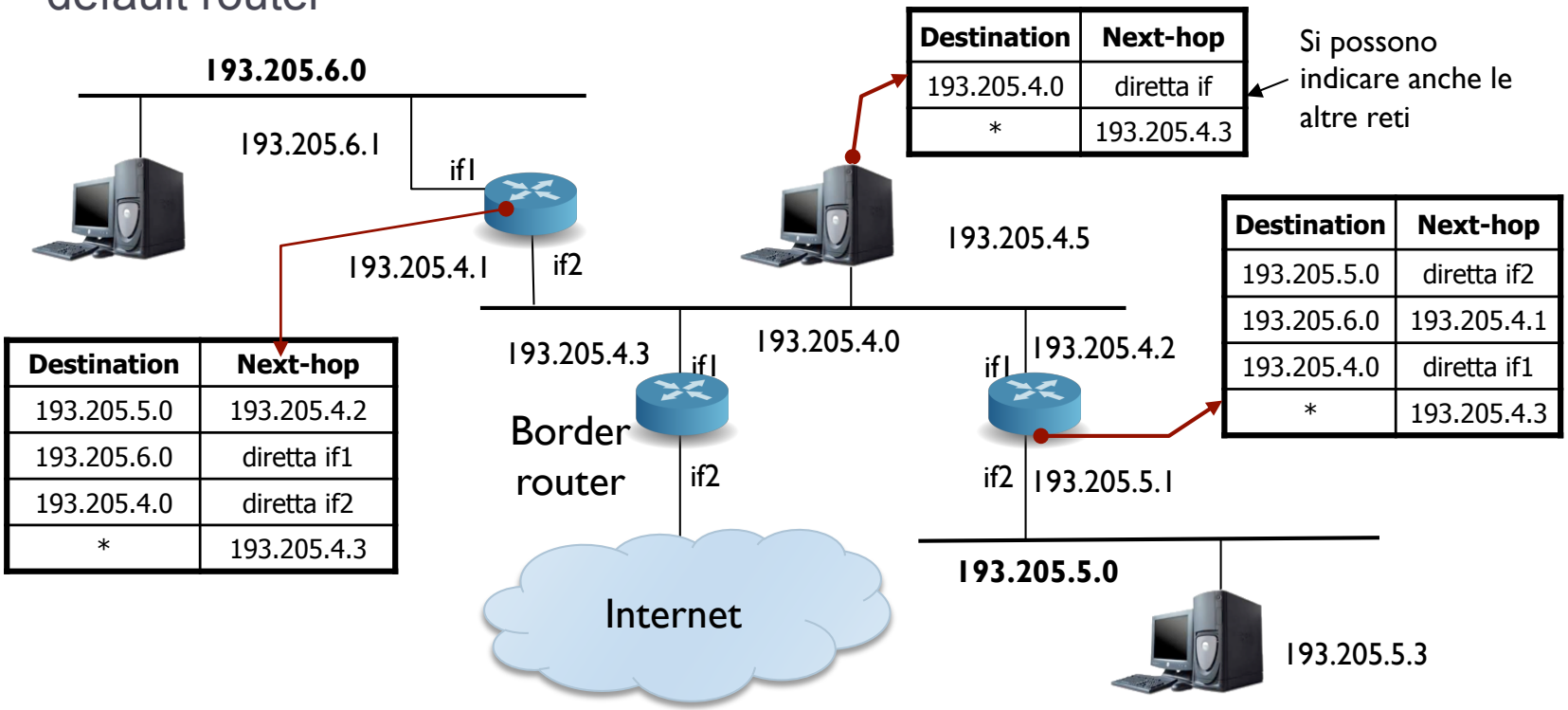


Destination	Next-hop
193.205.6.0	223.240.129.7
131.108.0.0	diretta if1
223.240.129.0	diretta if2

Destination	Next-hop
193.205.6.0	diretta if2
223.240.129.0	diretta if1
131.108.0.0	223.240.129.1

Routing di default

- Il routing di default permette di instradare pacchetti verso reti che non sono gestite localmente
  - I pacchetti sono indirizzati verso un router “di confine” della rete
  - Tutti i pacchetti con IP non appartenente alle reti note sono inviati dal default router



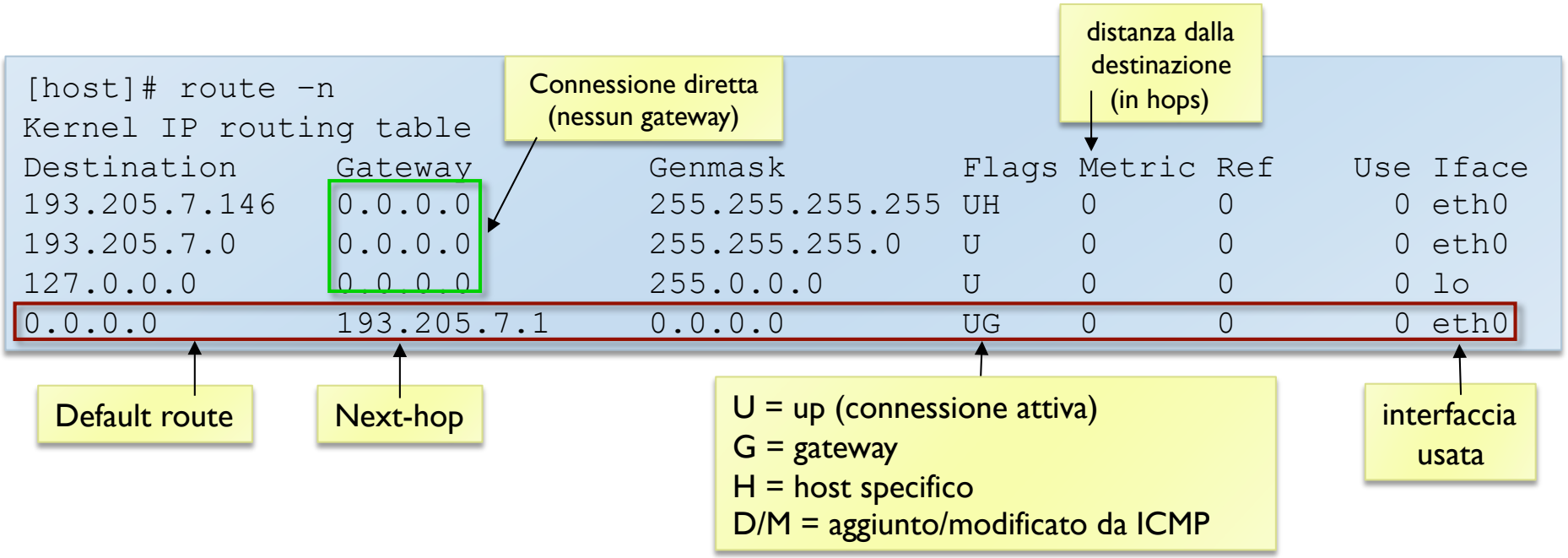
Destination	Next-hop
193.205.4.0	diretta if
*	193.205.4.3

Destination	Next-hop
193.205.5.0	193.205.4.2
193.205.6.0	diretta if1
193.205.4.0	diretta if2
*	193.205.4.3

Destination	Next-hop
193.205.5.0	diretta if2
193.205.6.0	193.205.4.1
193.205.4.0	diretta if1
*	193.205.4.3

Tabella di routing

- La tabella di routing definisce il next-hop per un pacchetto da instradare
  - Le entry (linee) sono scandite in sequenza
  - Si applica la prima regola verificata `(Ipdest & Genmask)==Destination`
  - L'ultima entry è l'instradamento di dafault che è verificato da ogni IP



Routing

- Spedizione di un pacchetto con IP destinazione IPdest
  - Si cerca IPdest nelle tabelle di routing (diretta/host/rete/default)
  - Si ricava il prossimo “hop” ovvero l’indirizzo IP del prossimo nodo sul percorso (e l’interfaccia da usare)
  - Si spedisce il datagram al prossimo nodo

- Nel pacchetto inviato l’unico indirizzo che compare è quello dell’ultima destinazione
- Si devono definire le tabelle di routing
  - Instradamento statico (costruzione manuale – piccole reti)
  - Instradamento dinamico (aggiornamento periodico in base a informazioni scambiate fra i router con protocolli RIP, OSPF o BGP)

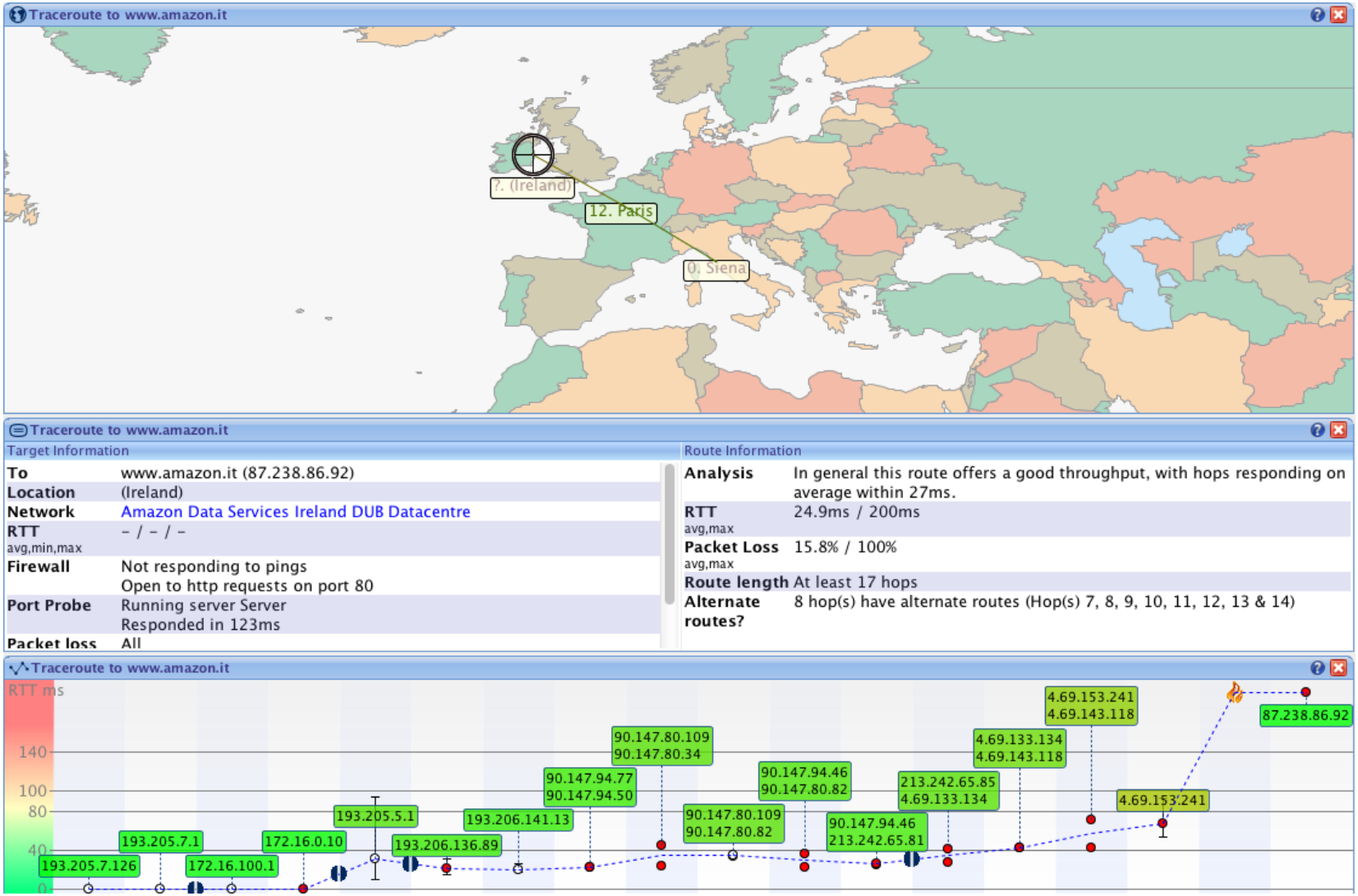
Il comando traceroute

- Traccia il percorso dei pacchetti verso una data destinazione mostrando i nodi attraversati
- Utilizza il campo TIME TO LIVE utilizzando il messaggio di notifica ICMP TIME_EXCEEDED inviato dai gateway quando il pacchetto scade
- Per default sono inviati 3 pacchetti “sonda” per ogni TTL e viene mostrato il tempo di round-trip per ciascuno di essi
- Il messaggio di notifica è atteso per un tempo massimo (5 s) altrimenti si stampa “*” per il relativo pacchetto sonda
- Il numero massimo di hop è 30 (lo stesso delle connessioni TCP)
- Non tutti i gateway inviano il messaggio TIME_EXCEEDED
  - Compare “*” in tal caso

Un esempio di route

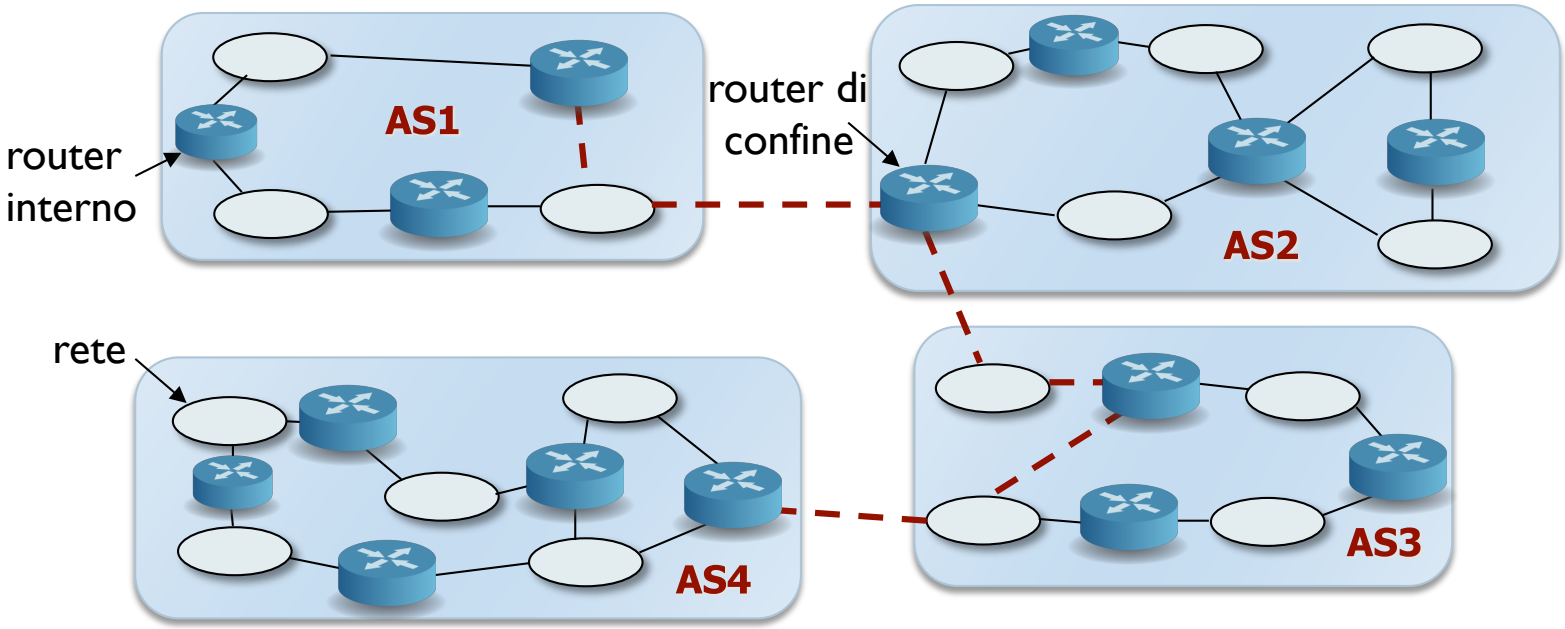
```
[host]# traceroute www.virgilio.it
traceroute to www.virgilio.it (212.48.10.150), 30 hops max, 38 byte packets
 1  ringe (193.205.7.1)  2.685 ms  1.665 ms  1.662 ms
 2  cuces-ing.link.unisi.it (193.205.5.101)  70.407 ms  32.951 ms  70.588 ms
 3  rcuces.unisi.it (193.205.4.1)  43.928 ms  130.064 ms  125.421 ms
 4  rc-unisi.fi.garr.net (193.206.136.89)  125.552 ms  119.365 ms  103.817 ms
 5  bo-fi.garr.net (193.206.134.93)  70.092 ms  38.814 ms  20.001 ms
 6  rtg-rt-1.bo.garr.net (193.206.134.198)  19.653 ms  105.629 ms  14.991 ms
 7  rm-bo-g.garr.net (193.206.134.49)  32.389 ms  60.269 ms  25.866 ms
 8  cw-nap.inroma.roma.it (194.242.224.3)  45.573 ms  54.386 ms  88.611 ms
 9  s3-0-r2-ROM2.cwitaly.net (195.94.140.173)  37.144 ms  27.868 ms  42.471 ms
10  194.79.199.35 (194.79.199.35)  26.232 ms  25.961 ms  33.669 ms
11  pos0-1-0-r5-MIL3.cwitaly.net (194.79.192.5)  49.560 ms  33.136 ms  81.481 ms
12  fe0-0-r3-MIL1.cwitaly.net (213.233.14.75)  164.763 ms  71.242 ms  107.814 ms
13  * matrix-mi.ar1.mi1.cwitaly.net (195.250.255.102)  45.349 ms  79.267 ms
14  212.48.4.241 (212.48.4.241)  71.192 ms  59.393 ms  43.822 ms
15  212.48.4.174 (212.48.4.174)  59.138 ms  83.495 ms  39.530 ms
16  * * *
17  * * *
```

Visual route



Sistemi autonomi

- La dimensione di Internet rende impossibile gestire centralmente tutti router
  - La rete è divisa in sistemi autonomi (Autonomous Systems)
  - Il routing è esterno o interno se esce o rimane confinato in un AS



Costruzione delle tabelle di routing

- La costruzione delle tabelle di routing deve garantire
  - Robustezza rispetto ai guasti
  - Imparzialità rispetto ai mittenti
  - Ottimalità rispetto ad un data metrica (minimo ritardo, massimo throughput della rete, minimo numero di hop)
    - Ad ogni passo di instradamento è associata una metrica
    - La metrica del percorso è la somma delle metriche associate alle reti attraversate
- Gli algoritmi per il calcolo delle tabelle di routing possono essere
  - Non adattivi - calcolano i percorsi off-line (routing statico)
  - Adattivi - modificano le tabelle di routing in base a variazioni della topologia e del traffico

Limiti dell'indirizzamento IPv4

- Gli indirizzi IP (o meglio le sottoreti) si stanno esaurendo
  - Esistono circa 2.000.000.000 di indirizzi "usabili" per host
  - L'organizzazione in classi porta ad uno spreco
    - Acquisire una rete di classe B implica acquisire 65536 indirizzi
    - Una rete di classe C è troppo piccola per molte organizzazioni
    - Le reti di classe A sono troppo grandi
- Le tabelle di routing sono molto grosse
  - i router devono conoscere tutte le reti
  - il problema sono le reti di classe C (sono 2.097.152)
  - CIDR (Classless Interdomain Routing – RFC 1519) prevede di allocare le reti di classe C in blocchi di reti contigue
    - Sono definite regole di allocazione "geografica" per intervalli di indirizzi
      - es. 194.0.0.0 – 195.255.255.255 sono per l'Europa

Il protocollo ICMP

- I messaggi ICMP (Internet Control Message Protocol – RFC 792) servono per la gestione di funzionalità del livello di rete
  - Segnalazione di errore (inviati al mittente)
    - Destination Unreachable – Il pacchetto non può essere consegnato
    - Time exceeded – TTL ha raggiunto il valore 0 oppure non si sono ricevute tutte le parti di un pacchetto frammentato entro un tempo limite
    - Parameter Problem – Errore nei parametri dell'header
    - ….
  - Messaggi di richiesta
    - Echo request/Echo reply – Richiesta/risposta di eco (verifica se un host risponde)
    - Timestamp request/Timestamp reply – Richiesta/risposta con timestamp
    - ….

Destination unreachable

- Messaggio di errore
  - Inviato (eventualmente) da
    - Router che non riesce ad instradare un pacchetto
    - Host che non riesce a consegnarlo
  - Un codice indica il motivo (host/rete non raggiungibile, porta TCP non aperta,…)
  - Al messaggio è allegato l'inizio del pacchetto per capire a chi notificare l'errore (porta del mittente)

Tipo: 3	Codice: 0-15	checksum
0 (non usato)		
Header e primi 8 byte del datagram IP ricevuto		

Il comando ping

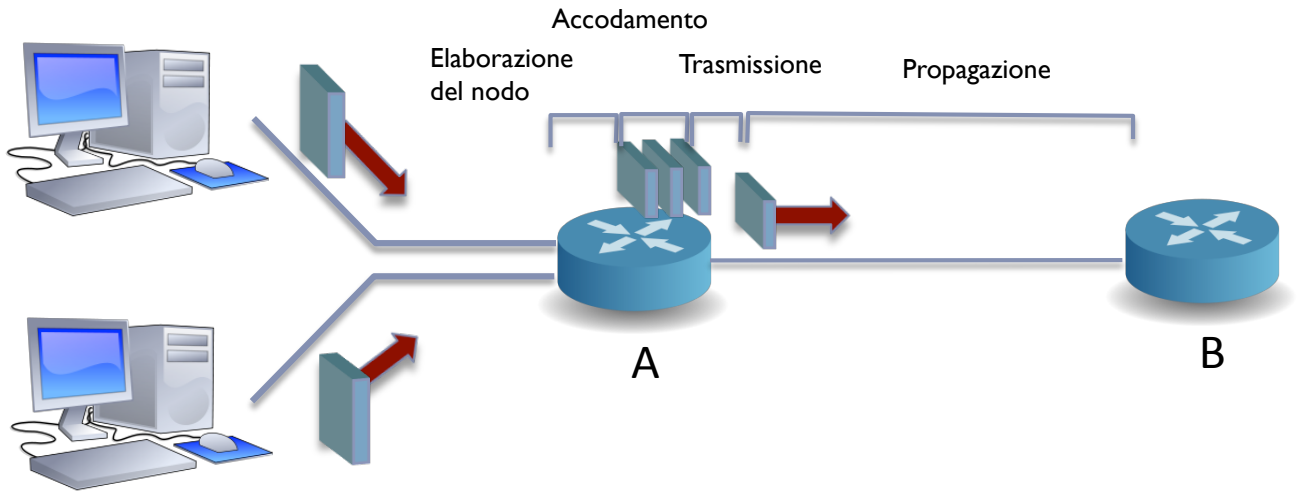
- Invia pacchetti ICMP ECHO REQUEST ad un host o gateway
- Attende le risposte ICMP ECHO REPLY
- Il pacchetto contiene un timestamp per misurare il tempo di round-trip

```
[host]# ping -v cuces.unisi.it
PING cuces.unisi.it (193.205.4.2): 56 data bytes
64 bytes from 193.205.4.2: icmp_seq=0 ttl=252 time=28.6 ms
64 bytes from 193.205.4.2: icmp_seq=1 ttl=252 time=45.1 ms
64 bytes from 193.205.4.2: icmp_seq=2 ttl=252 time=61.8 ms
64 bytes from 193.205.4.2: icmp_seq=3 ttl=252 time=62.8 ms
64 bytes from 193.205.4.2: icmp_seq=4 ttl=252 time=78.0 ms

--- cuces.unisi.it ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 28.6/55.2/78.0 ms
```

Ritardo di trasferimento di un pacchetto

- Il ritardo totale di un nodo della rete è dato da
  - Ritardo di elaborazione
  - Ritardo di accodamento
  - Ritardo di trasmissione
  - Ritardo di propagazione



Tipi di ritardo 1

- Ritardo di elaborazione
  - Tempo per elaborare l'intestazione e prendere la decisione di routing
    - eventuale controllo di errori
    - controllo dell'indirizzo destinazione
    - accesso alle tabelle di routing per determinare la coda di uscita in cui memorizzare il pacchetto
- Ritardo di accodamento
  - Il ritardo effettivo dipende dal numero di pacchetti in coda
    - Se la coda è vuota il ritardo è nullo
    - Il numero di pacchetti in coda dipende dal traffico in un certo istante verso l'uscita associata alla coda
    - La coda implementa la strategia First Come First Served. In alternativa si prevedere di assegnare una priorità ai pacchetti e usare una coda con priorità
    - Il ritardo di accodamento può essere molto diverso da pacchetto a pacchetto

Tipi di ritardo 2

- **Ritardo di trasmissione**
  - Se L è la lunghezza del pacchetto in bit e R bit/s la frequenza di trasmissione della linea di uscita il ritardo è L/R
  - Corrisponde al tempo necessario a trasmettere tutti i bit sul canale di uscita
- **Ritardo di propagazione**
  - E' il tempo che impiega il segnare relativo a ciascun bit ad arrivare alla destinazione propagandosi sul collegamento
    - Dipende dal mezzo fisico
    - Il ritardo di propagazione è d/v dove d è la lunghezza del mezzo di trasmissione e v la velocità di propagazione (è dell'ordine della velocità della luce – 3×10^8 m/s)
    - Può essere dell'ordine dei ms per reti estese

Ritardo di accodamento

- Viene descritto mediante misure statistiche
  - media e varianza
  - probabilità che superi una certa soglia

- Dipende dai seguenti fattori
  - frequenza di arrivo del traffico nella coda (*a* pacchetti/secondo)
    - numero delle linee di ingresso e probabilità che i pacchetti in ingresso siano diretti verso la coda in oggetto
  - frequenza di trasmissione in uscita alla coda (R bit/secondo)
  - natura del traffico entrante (costante o a burst)
  - lunghezza dei pacchetti (si suppone una lunghezza fissa L)

Intensità del traffico

- L'intensità del traffico è il rapporto fra la frequenza dei bit in arrivo nella coda e quella con cui si riescono a smaltire

$$I = \frac{La}{R}$$

  - Se I>1la frequenza di arrivo dei bit è superiore alla capacità di trasmetterli e la coda tende a crescere facendo aumentare il ritardo
  - Il sistema va progettato in modo che l'intensità "media" nel tempo non sia superiore a 1
    - Se I≤1 e i pacchetti arrivano a cadenza costante, la coda è sempre vuota
    - Se I≤1 e i pacchetti arrivano a burst, la coda si riempie durante il burst (il pacchetto t-esimo ha un ritardo di (t-1)L/R secondi)

Perdita di pacchetti

- Le code dei router sono di dimensioni limitate
  - Quando l'intensità di traffico rimane maggiore di 1 per troppo tempo la coda si riempie e i pacchetti in arrivo vengono scartati
  - La probabilità di perdita dei pacchetti è un parametro relativo alle prestazioni di un router