ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Internet e IP

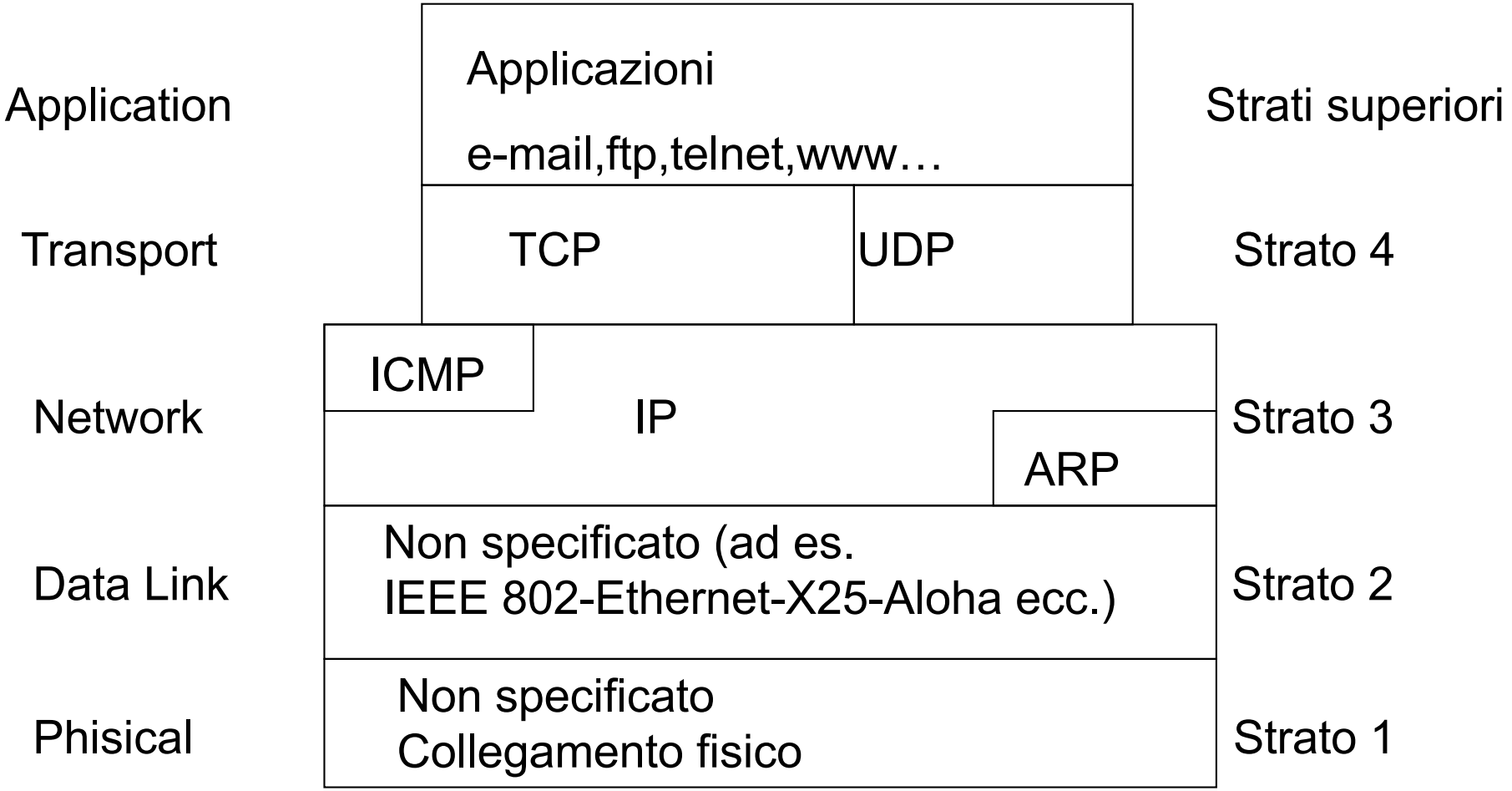
Franco CALLEGATI
Dipartimento di Informatica: Scienza e Ingegneria

A.A. 2018-2019

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

I protocolli di Internet

Architettura



Internet Protocol (IP) - RFC 791

- Progettato per funzionare a **commutazione di pacchetto** in modalità **connectionless**
- Si prende carico della trasmissione di **datagrammi** da sorgente a destinazione, attraverso reti eterogenee
- Identifica **host** e **router** tramite indirizzi di **lunghezza fissa**, ragruppandoli in **reti IP**
- **Frammenta** e **riassembla** i datagrammi quando necessario
- Offre un servizio di tipo **best effort**, cioè non sono previsti meccanismi per
  - aumentare l'affidabilità del collegamento end-to-end,
  - eseguire il controllo di flusso e della sequenza.

Struttura degli indirizzi IP

- Indirizzi di lunghezza fissa pari a **32 bit**
- Scritti convenzionalmente come sequenza di 4 numeri decimali, con valori da **0** a **255**, separati da punto (rappresentazione **dotted decimal**)

`10001001.11001100.11010100.00000001`

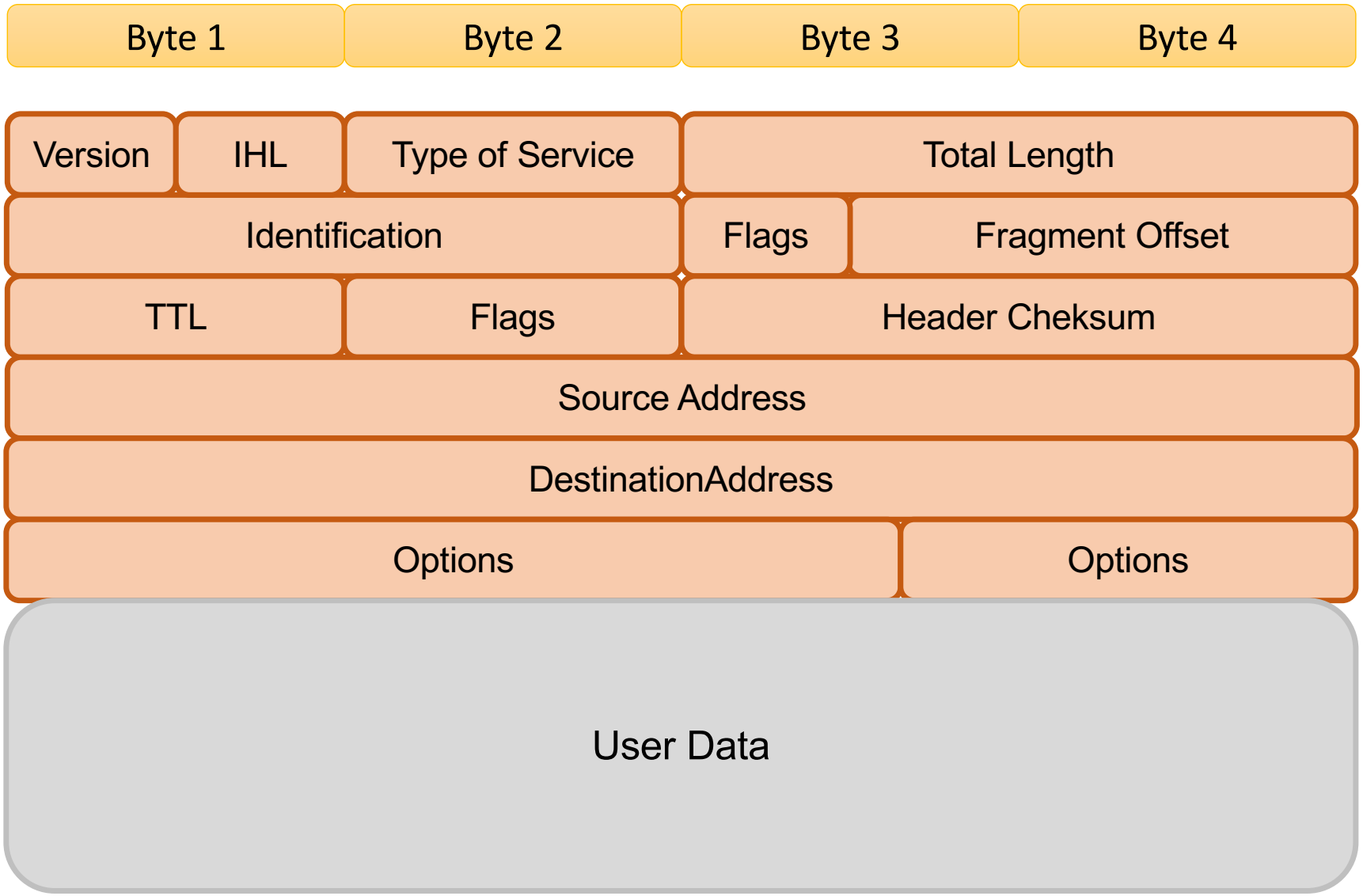
`137.204.212.1`

- Numero teorico max. di indirizzi

$$2^{32} = 4.294.967.296$$

  - In realtà si riesce a sfruttare un numero molto inferiore
- Assegnati dalla **IANA** (**I**nternet **A**ssigned **N**umbers **A**uthority)

Formato pacchetto



Significato delle PCI

- **Version :** indica il formato dell'intestazione, attualmente la versione in uso è la 4
- **IHL :** lunghezza dell'intestazione, espressa in parole di 32 bit; lunghezza minima = 5
- **Type of service :** indicazione sul tipo di servizio richiesto, usato anche come sorta di priorità
- **Total length :** lunghezza totale del datagramma, misurata in bytes; lunghezza masima = 65535 bytes, ma non è detto che tutte le implementazioni siano in grado di gestire questa dimensione

Significato delle PCI

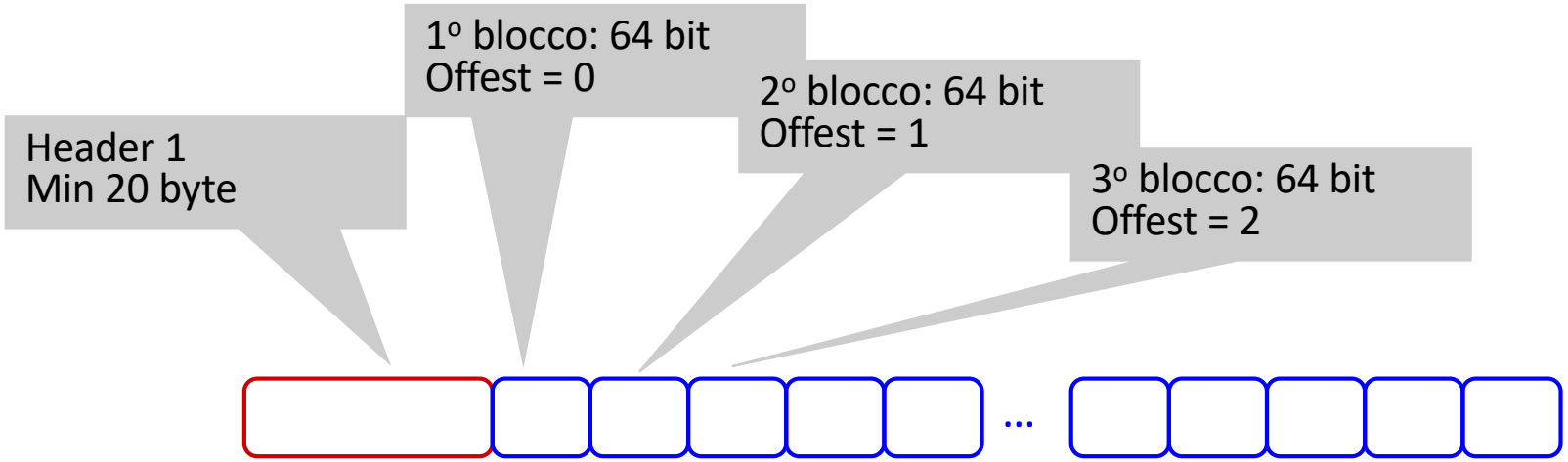
- **Identification** : valore intero che identifica univocamente il datagramma
  - Indica a quale datagramma appartenga un frammento (fragment)
- **Flag** :
  - bit 0 — sempre a 0
  - bit 1 — don't fragment (DF)
    - DF = 0 si può frammentare
    - DF = 1 non si può frammentare
  - bit 2 — more fragments (MF)
    - MF = 0 ultimo frammento
    - MF = 1 frammento intermedio
- **Fragment offset**: indica quale è la posizione di questo frammento nel datagramma, come distanza in unità di 64 bit dall'inizio

Fragment offset

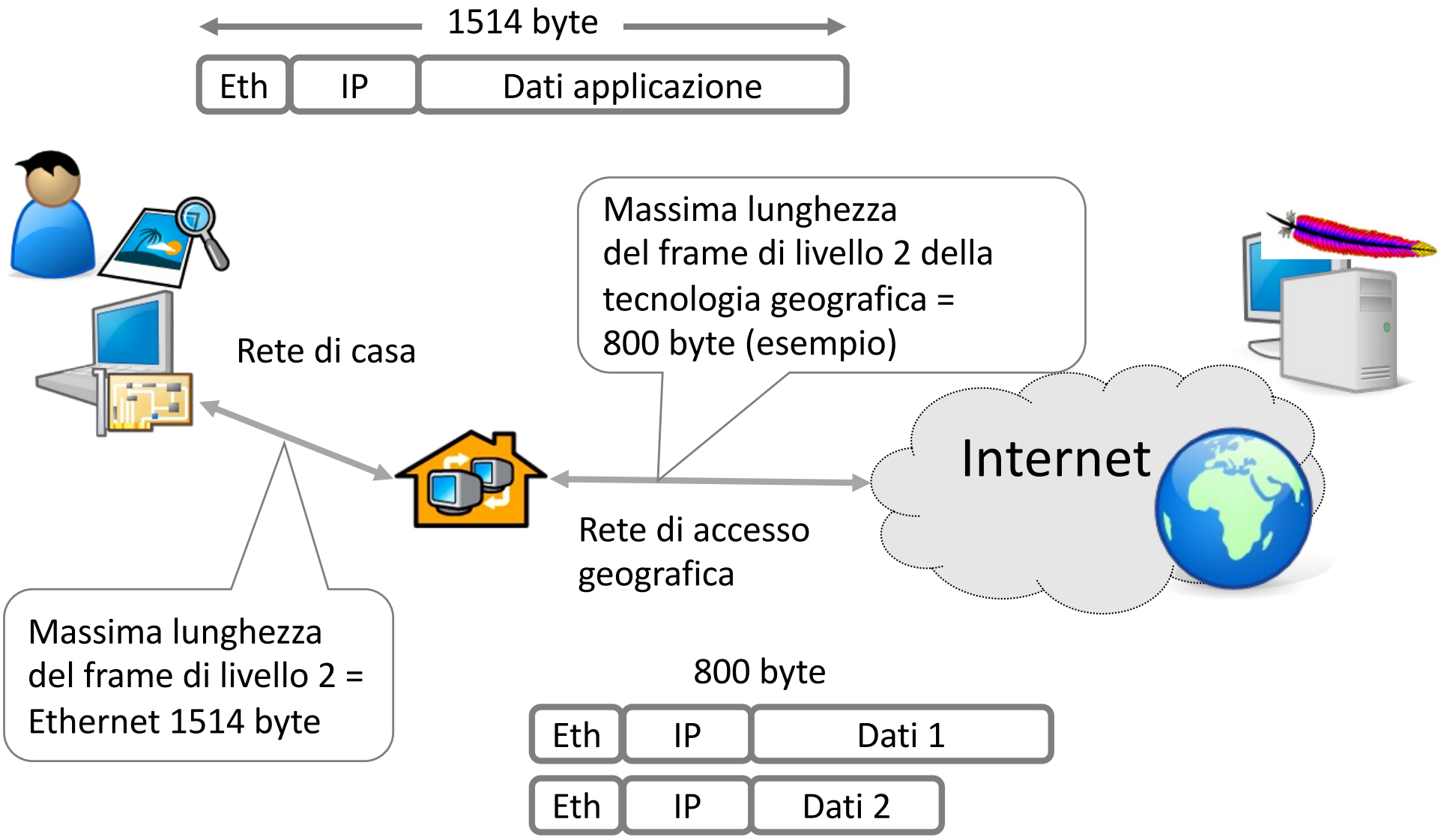
- Il datagramma IP viene virtualmente suddiviso in sotto-blocchi di 8 byte (64 bit)
- Per l'IP che trasmette (non necessariamente la sorgente dei dati ma anche un nodo intermedio)
  - Il primo blocco del datagramma è il numero 0
  - I blocchi successivi sono logicamente numerati sequenzialmente
- Il numero logico del primo blocco viene scritto nel Fragment Offset del datagramma

Implementazione

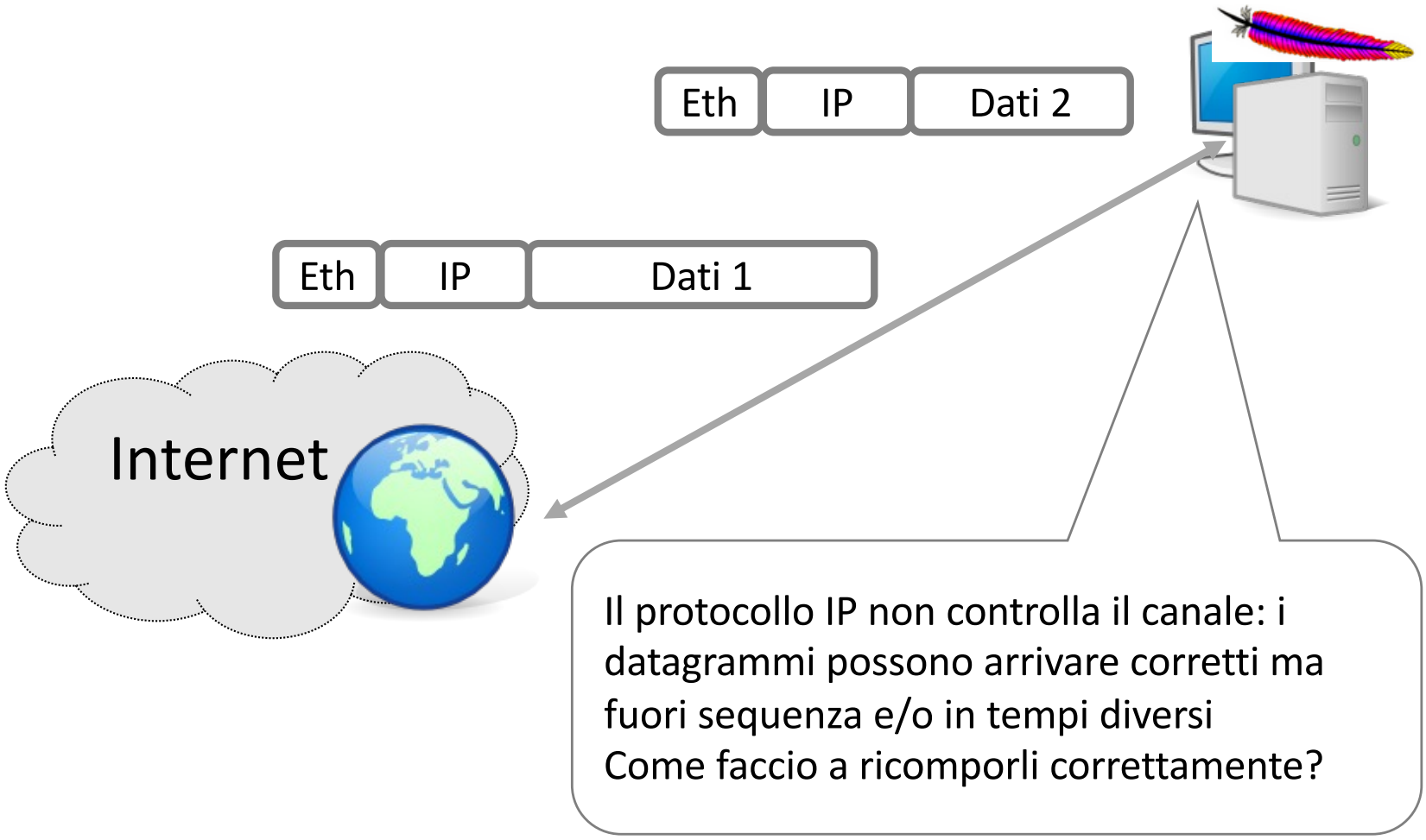
- Chi frammenta i datagrammi?
  - Qualunque apparato di rete dotato di protocollo IP può frammentare un datagramma
  - Tipicamente i nodi intermedi non riassemblano, ma lo fa solamente il terminale ricevente
- Frammentazioni multiple
  - Un datagramma può essere frammentato a più riprese in nodi successivi
- La numerazione tramite "offset" permette di rinumerare facilmente frammenti di un frammento



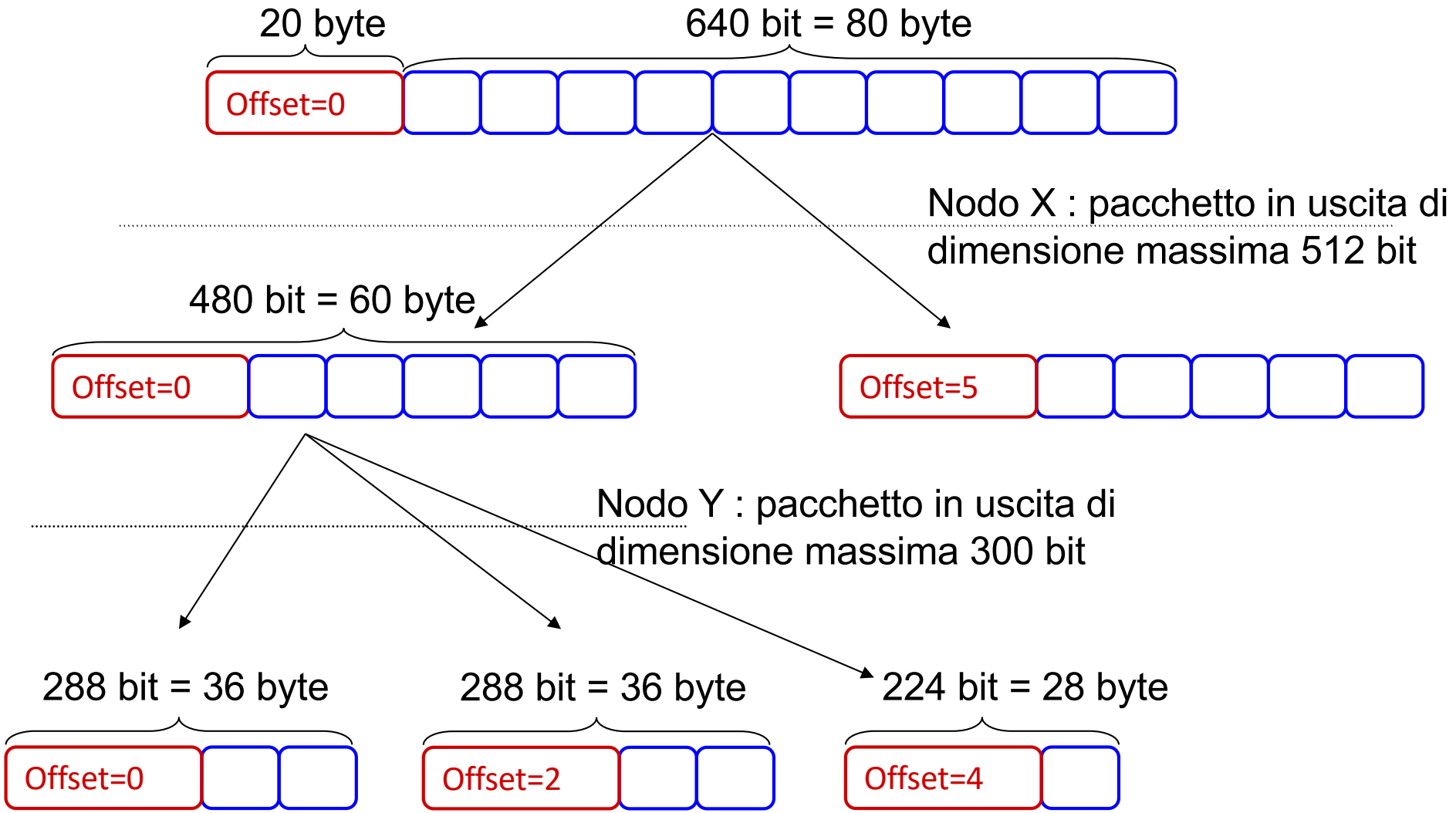
Perché la segmentazione?



Il riassemblamento



Calcolo dell'offset



Formato del pacchetto IP (4)

- **Time to live (TTL)** : max numero di nodi attraversabili
  - Il nodo sorgente attribuisce un valore maggiore di 0 a TTL (tipicamente TTL = 64, al massimo 255)
  - Ogni nodo che attraversa il datagramma pone TTL = TTL - 1
  - Il primo nodo che vede TTL = 0 distrugge il datagramma
- **Protocol** : indica a quale protocollo di livello superiore appartengono i dati del datagramma
- **Header checksum** : controllo di errore della sola intestazione, viene ricalcolato da ogni nodo attraversato dal datagramma
- **Source and Destination Address** : indirizzi sorgente e destinazione

Formato del pacchetto IP (5)

- **Options :** contiene opzioni relative al trasferimento del datagramma (registrazione del percorso, meccanismi di sicurezza), è perciò di lunghezza variabile

- **Padding :** bit privi di significato aggiunti per fare in modo che l'intestazione sia con certezza multipla di 32 bit

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

L’instradamento IP

Instradamento

- La rete Internet è una rete a commutazione di pacchetto
  - Oggi un sistema molto complesso
- In generale esistono più modi per raggiungere una destinazione da una certa sorgente

- Chi decide quale percorso seguire e come lo fa?
- Si decide pacchetto per pacchetto o per flusso di dati applicativi?
- …

Come funziona Internet

- Internet è una grande “rete di reti”
- La componente elementare è la **network IP**
  - Ogni network IP è una sorta di isola
    - L’isola tipicamente contiene calcolatori che fungono da nodi terminali della rete detti **host**
  - Le isole sono interconnesse da apparati che svolgono la funzione di “ponte”
    - Si tratta di calcolatori specializzati detti **router** o **gateway**

Internet: reti di reti

Tante Network IP isolate

La tecnologia

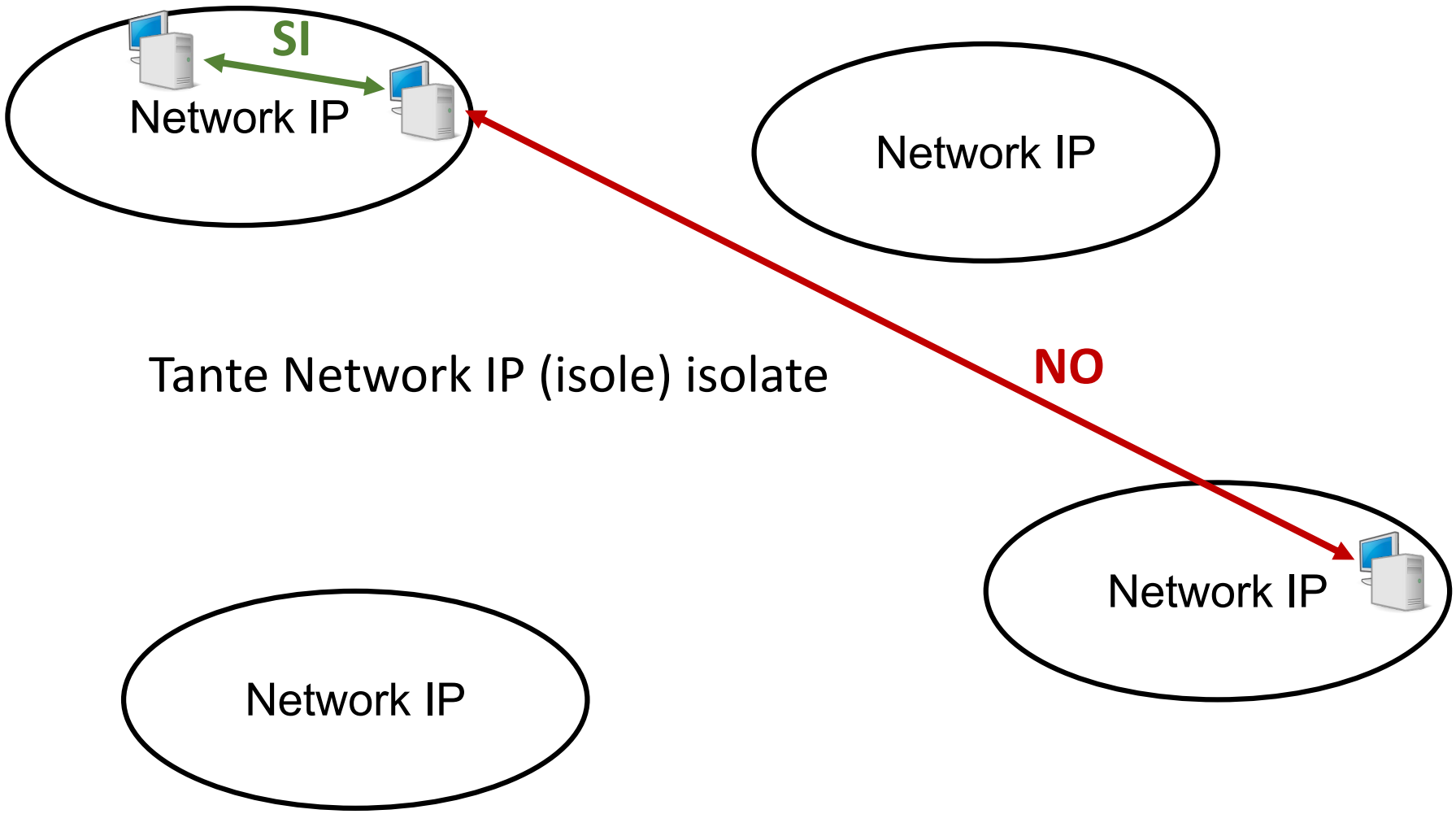
- Ogni network IP può essere implementata con una **tecnologia specifica**
- Esempio
  - Wi-Fi : Network realizzata con tecnologia wireless in area locale
  - ADSL e xDSL: Network realizzata con tecnologia a media distanza via cavo tramite infrastruttura di uno specifico fornitore di servizio pubblico
  - Ethernet: Network realizzata con tecnologia a breve distanza via cavo privata in area locale
  - GPRS/EDGE/LTE: Network realizzata con tecnologia radio a media distanza tramite infrastruttura di uno specifico fornitore di servizio pubblico

La network IP

- I calcolatori di una network IP sono connessi dalla medesima infrastruttura di rete fisica (livelli 1 e 2)

- Ipotesi fondamentale
  - Tutti gli host appartenenti alla medesima network IP sono in grado di parlare tra loro grazie alla tecnologia con cui essa viene implementata

Internet: reti di reti



Rete logica e rete fisica

- Nella terminologia di Internet si definisce
  - Rete logica: la network IP a cui un Host appartiene logicamente
  - Rete fisica: la rete (tipicamente LAN) a cui un Host è effettivamente connesso
- La rete fisica normalmente ha capacità di instradamento e può avere indirizzi locali (es. indirizzi MAC)
- L'architettura a strati nasconde gli indirizzi fisici e consente alle applicazioni di lavorare solo con indirizzi IP

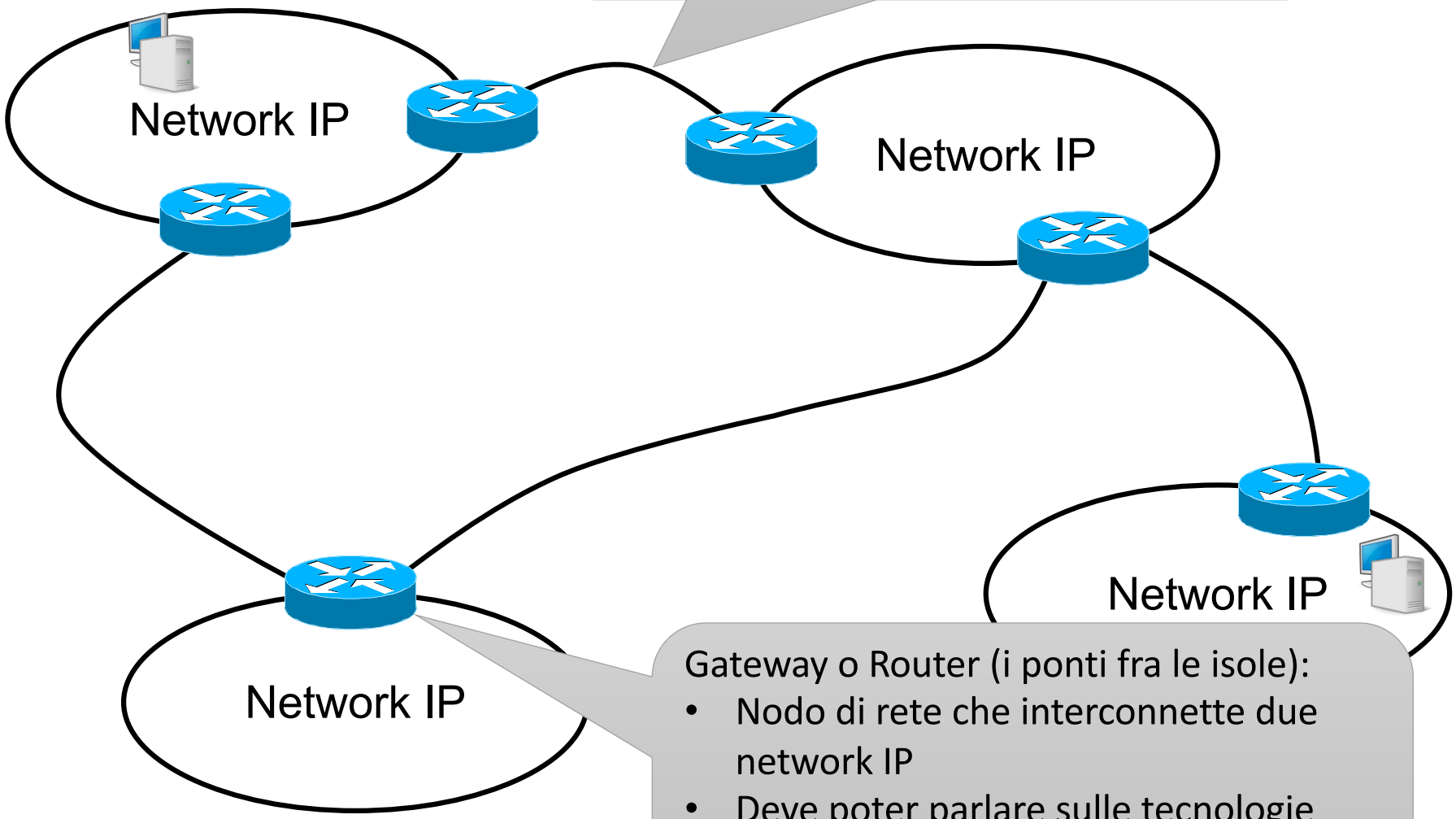
Interconnettere le isole

- Per far parlare tra loro le isole (network IP) è necessario che
  - Vi siano dei collegamenti fra le isole stesse, spesso realizzati con tecnologie diverse da quelle dell'isola
  - Vi siano degli apparati che permettono di usare questi collegamenti nel modo opportuno
  - Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere

I router

Collegamento fra router:

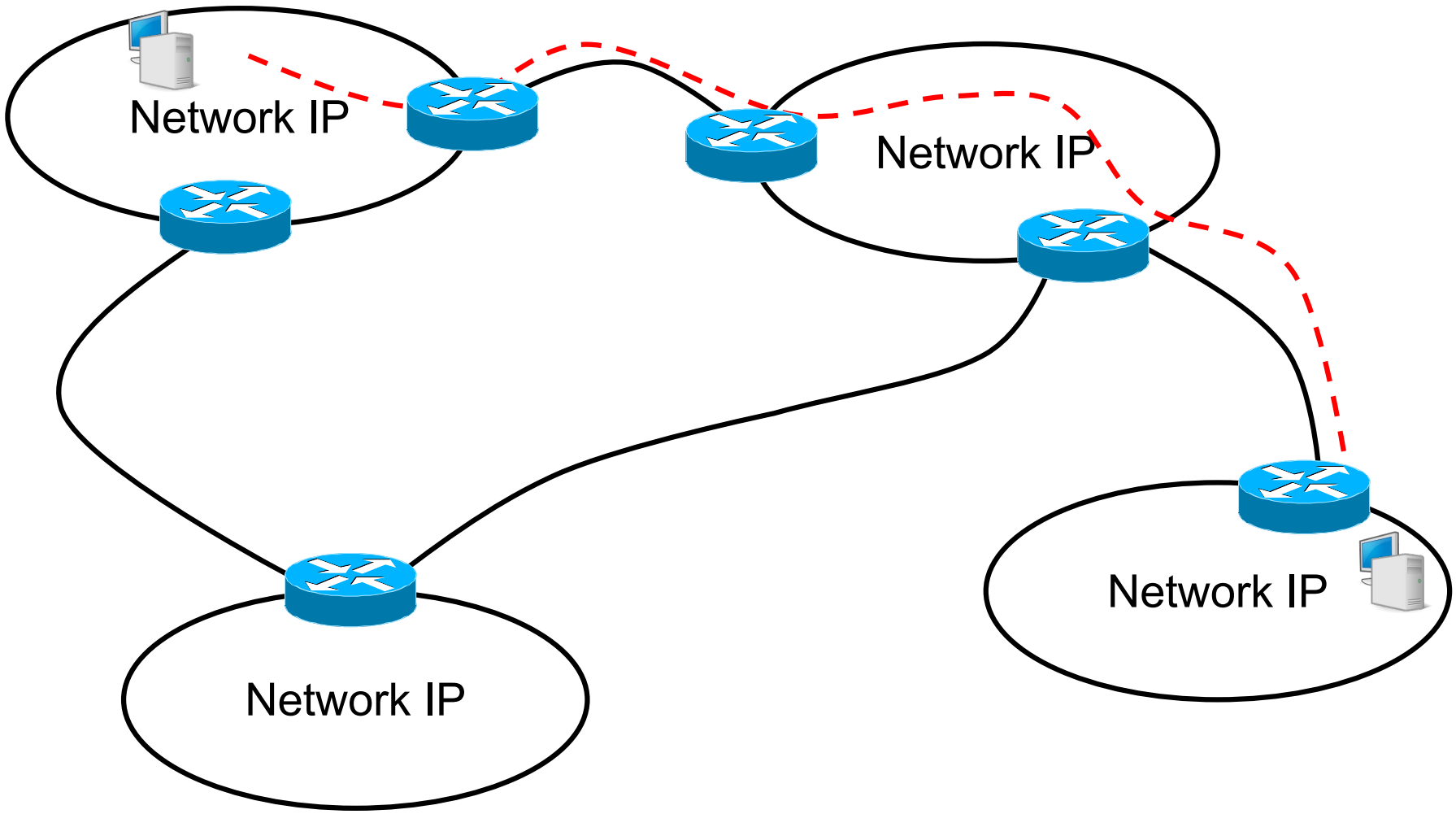
- Può essere una tecnologia simile a quella delle network oppure molto diversa



Gateway o Router (i ponti fra le isole):

- Nodo di rete che interconnette due network IP
- Deve poter parlare sulle tecnologie specifiche delle due Network
- Ha funzioni dal livello 1 al livello 3 OSI

Il percorso end-to-end

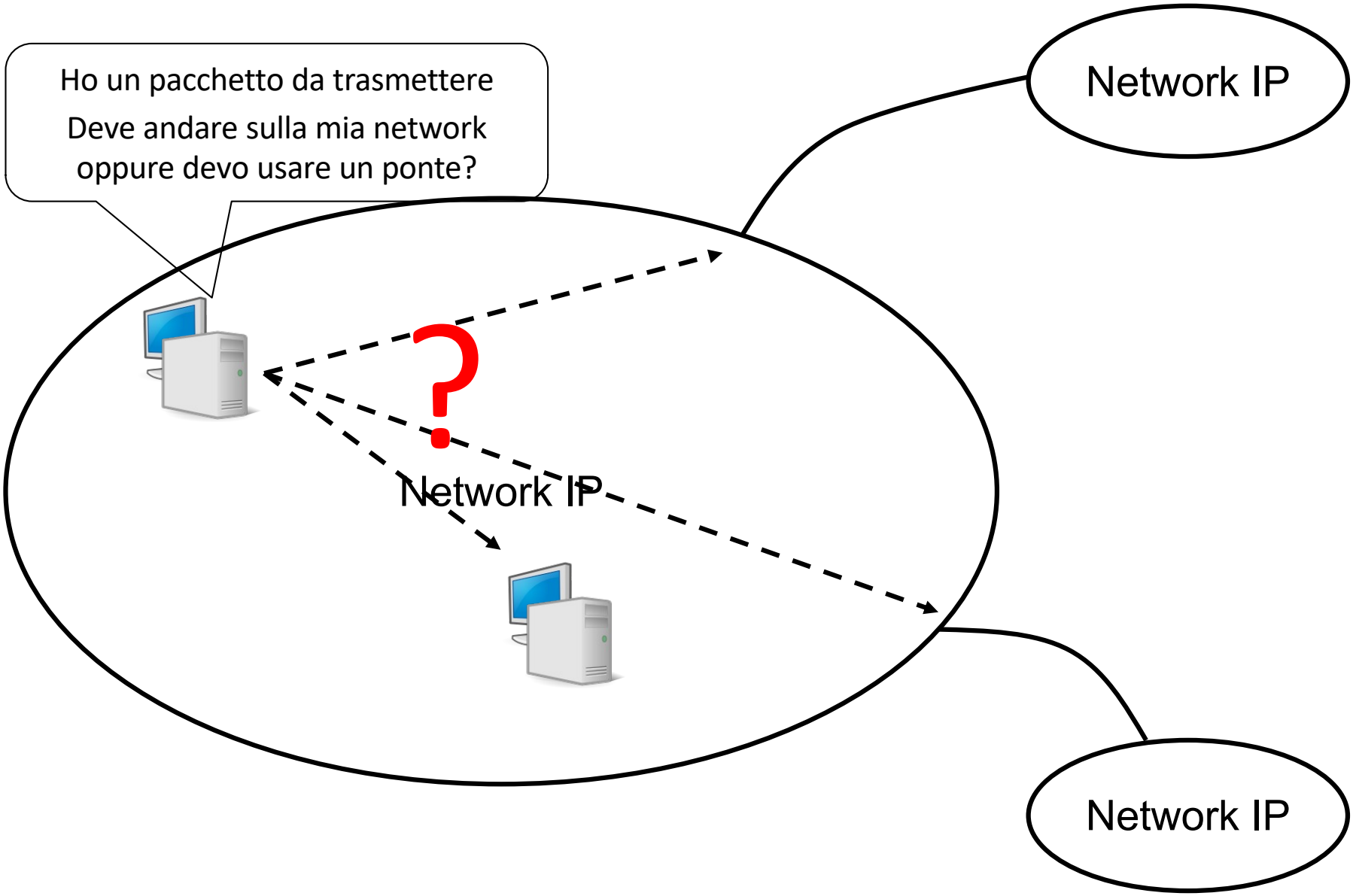


Cosa fa IP

- La tecnologia IP è agnostica rispetto alla tecnologia con cui sono realizzate le network
  - Il protocollo IP è concepito per lavorare indifferentemente su tecnologie diverse

- L'obiettivo di IP è quello di rendere possibile il dialogo fra network a prescindere dalla loro implementazione e localizzazione

La domanda cruciale

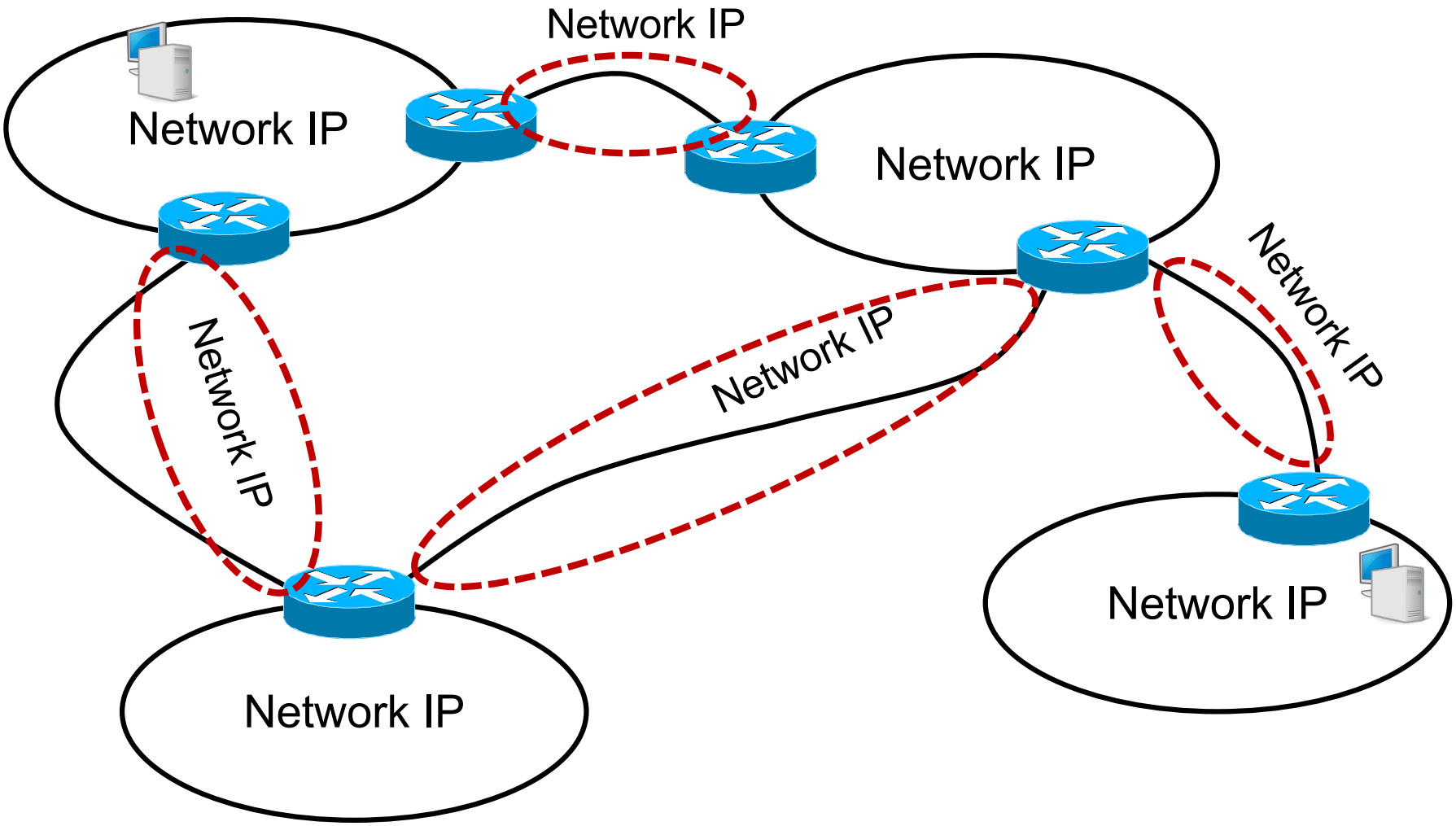


La risposta

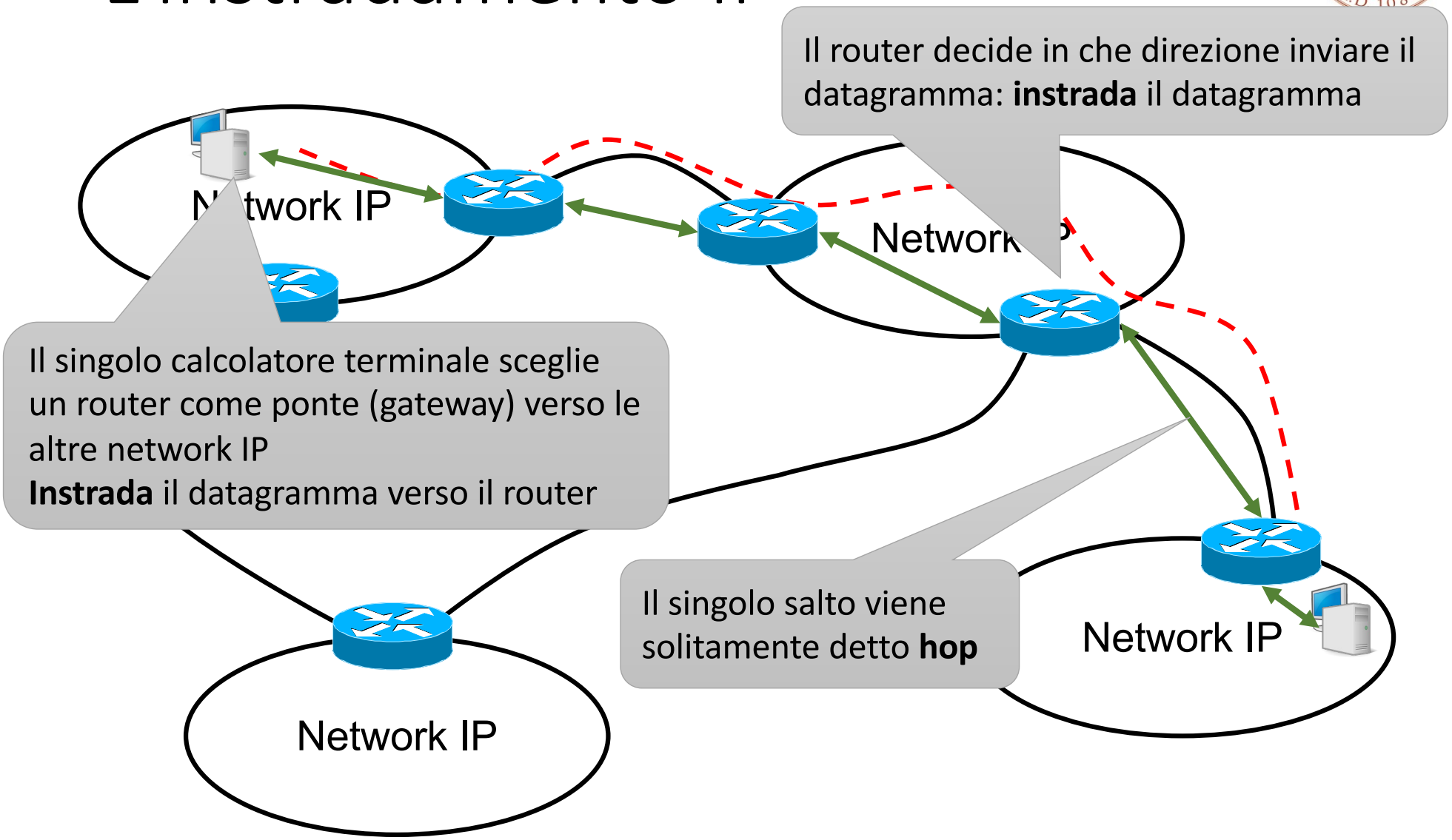
- Ogni nodo di Internet ha una base dati di destinazioni possibili
- Quando deve inviare un datagramma
  - Parte dall'indirizzo IP di destinazione
  - Legge la base dati
  - Decide quale azione intraprendere

- La tecnologia della propria network può essere utilizzata:
  - Per raggiungere la destinazione finale
  - Per raggiungere il primo ponte da attraversare

Le network fra i router



L'instradamento IP



Semantica dell'indirizzo IP

- L'indirizzo IP è logicamente suddiviso in due parti:
  - Network (Net) ID
    - Prefisso che identifica la **Network IP** a cui appartiene l'indirizzo
    - Tutti gli indirizzi di una medesima **Network IP** hanno il medesimo *Network ID*
  - Host ID
    - Identifica l'host (l'interfaccia) vero e proprio di una certa Network
- Per Net e Host ID vengono utilizzati bit contigui
  - Net ID occupa la parte *sinistra* dell'indirizzo
  - Host ID occupa la parte *destra* dell'indirizzo

Reti IP private (RFC 1918)

- Alcuni gruppi di indirizzi sono riservati a reti IP private
- Essi non sono raggiungibili dalla rete pubblica
- I router di Internet non instradano datagrammi destinati a tali indirizzi
- Possono essere riutilizzati in reti isolate

- **da 10.0.0.0 a 10.255.255.255**
- **da 172.16.0.0 a 172.31.255.255**
- **da 192.168.0.0 a 192.168.255.255**

Come si distingue net-ID da host-ID?

- Si usa la netmask
  - Al numero IP viene associata una maschera di 32 bit

```
137.204.191.25
10001001.11001100.10111111.00011001
11111111.11111111.11111111.11000000
```

Net-ID	Host-ID

- I bit a 1 della netmask identificano i bit dell'indirizzo IP che fanno parte del net-ID
- La netmask si può rappresentare
  - In notazione dotted-decimal
    - `11111111.11111111.11111111.11000000 = 255.255.255.192`
  - In notazione esadecimale
    - `11111111.11111111.11111111.11000000 = ff.ff.ff.c0`
  - Utilizzando la notazione abbreviata
    - `11111111.11111111.11111111.11000000 = /26`

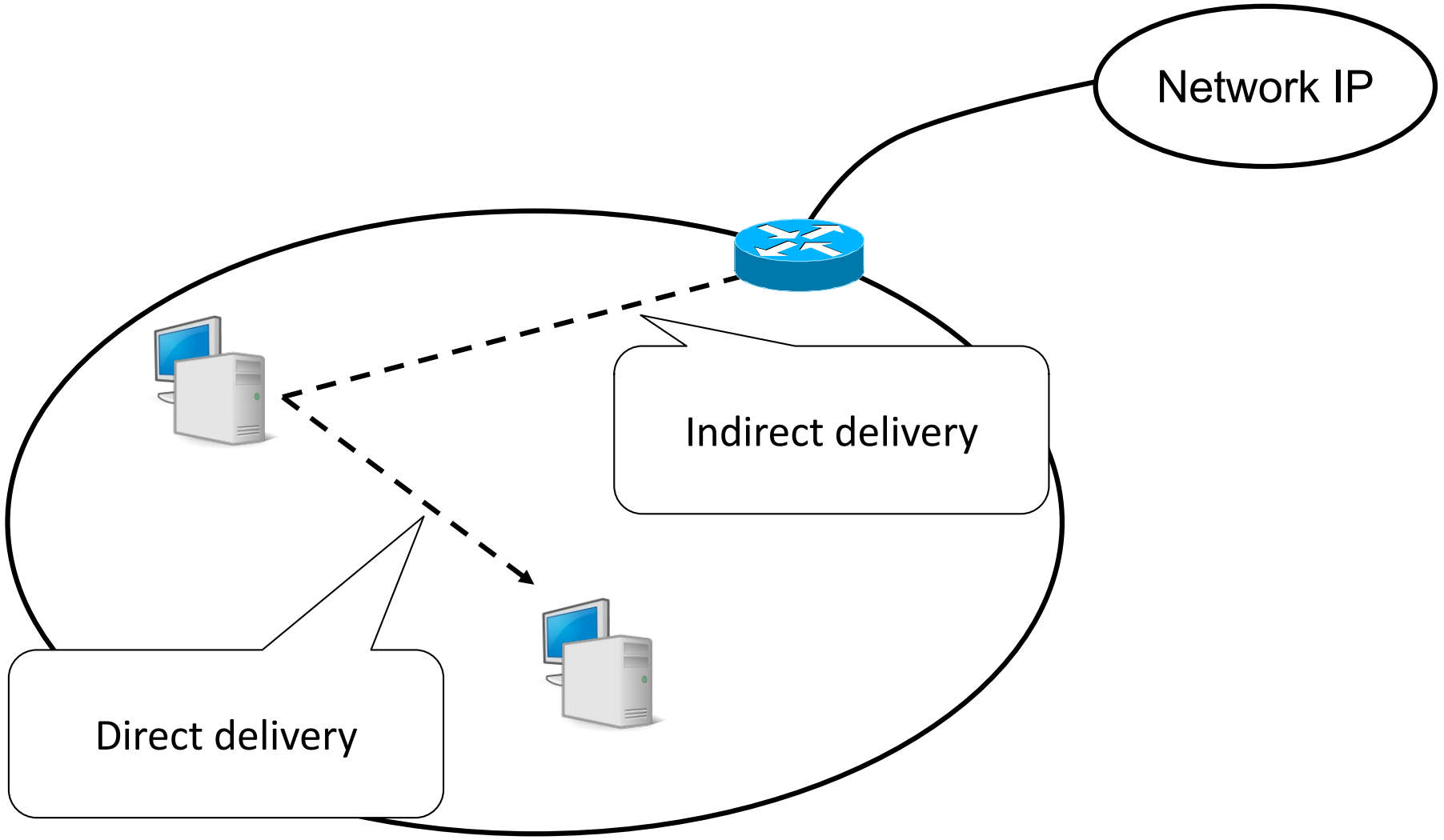
Netmask

- Esempio:
  - Network 192.168.1.0
    - Network privata con Net-ID = 3 byte = 24 bit
  - Subnetting in 2 sottoreti
    - Net-ID+subnet-ID = 25 bit
    - Netmask = `11111111. 11111111. 11111111.10000000`
  - Notazione
    - Net-ID = 192.168.1.0 Netmask = 255.255.255.128
    - Net-ID = 192.168.1.128 Netmask = 255.255.255.128
      - oppure
    - 192.168.1.0/25
    - 192.168.1.128/25

Esempio: Università di Bologna

- Net ID = 137.204
  - La network corrispondente ha indirizzo **137.204**.*0.0*
  - Tutti i numeri IP dell'Università di Bologna hanno il medesimo prefisso
- Host ID
  - Qualunque combinazione dei rimanenti 16 bit
    - Escluso 137.204.0.0 e 137.204.255.255
  - Server web UniBO
    - 137.204.24.35
  - Server web del DEIS
    - 137.204.24.40
  - Server web DEISNet
    - 137.204.57.85

La domanda cruciale

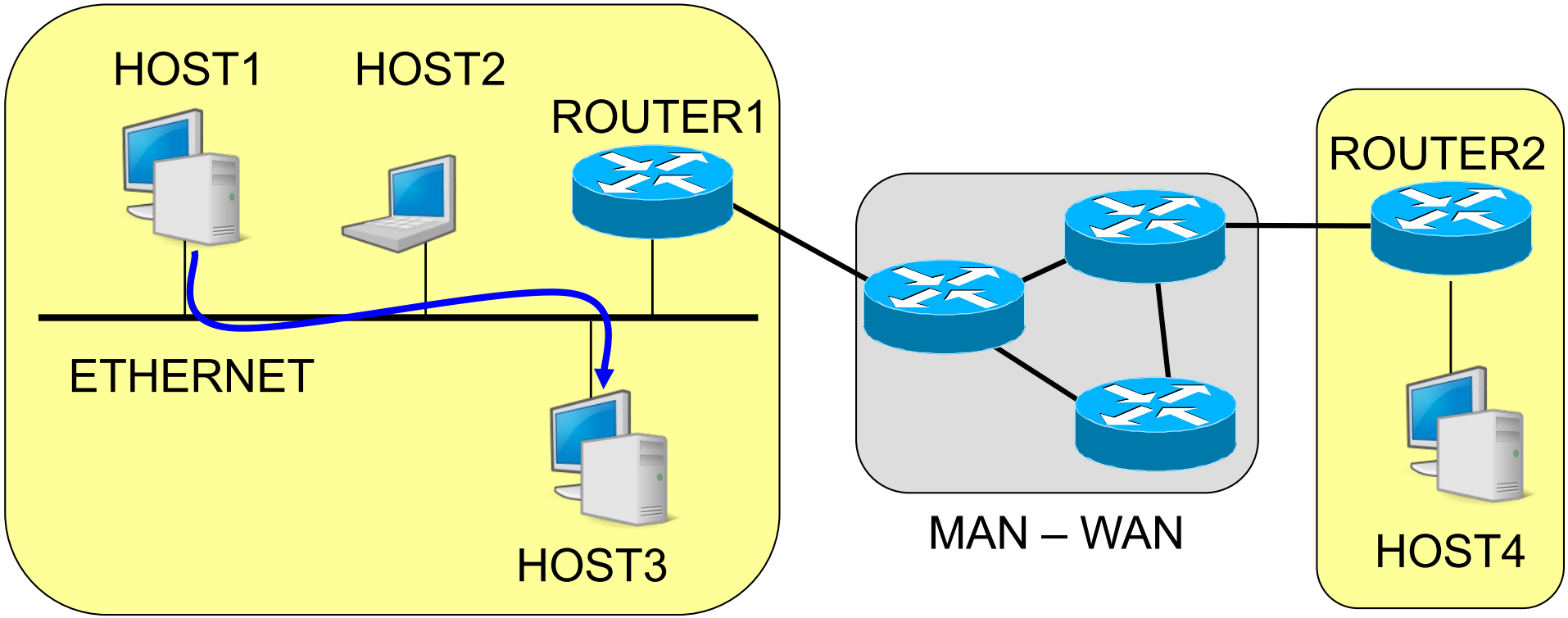


Instradamento diretto e indiretto

- **Direct delivery :**
  - IP sorgente e IP destinatario sono sulla stessa network
  - L'host sorgente spedisce il datagramma direttamente al destinatario
- **Indirect delivery :**
  - IP sorgente e IP destinatario non sono sulla stessa network
  - L'host sorgente invia il datagramma ad un router intermedio

- **Routing :** scelta del percorso su cui inviare i dati
  - i router formano struttura interconnessa e cooperante:
    - i datagrammi passano dall'uno all'altro finché raggiungono quello che può consegnarli direttamente al destinatario

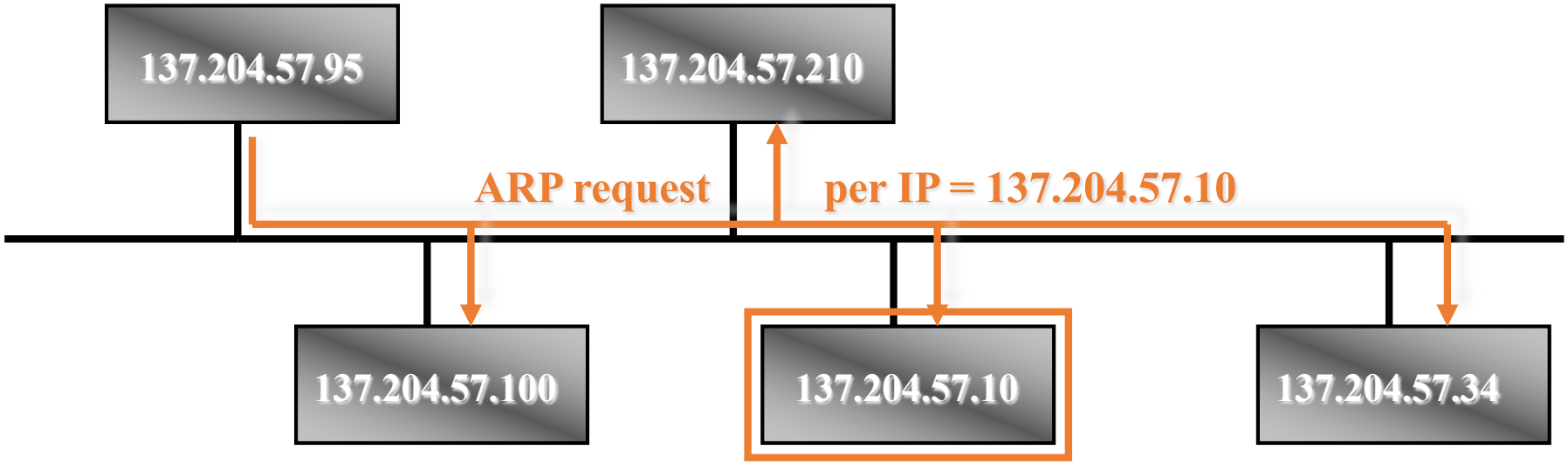
Direct Delivery



Relazione Indirizzi Fisici – Indirizzi IP

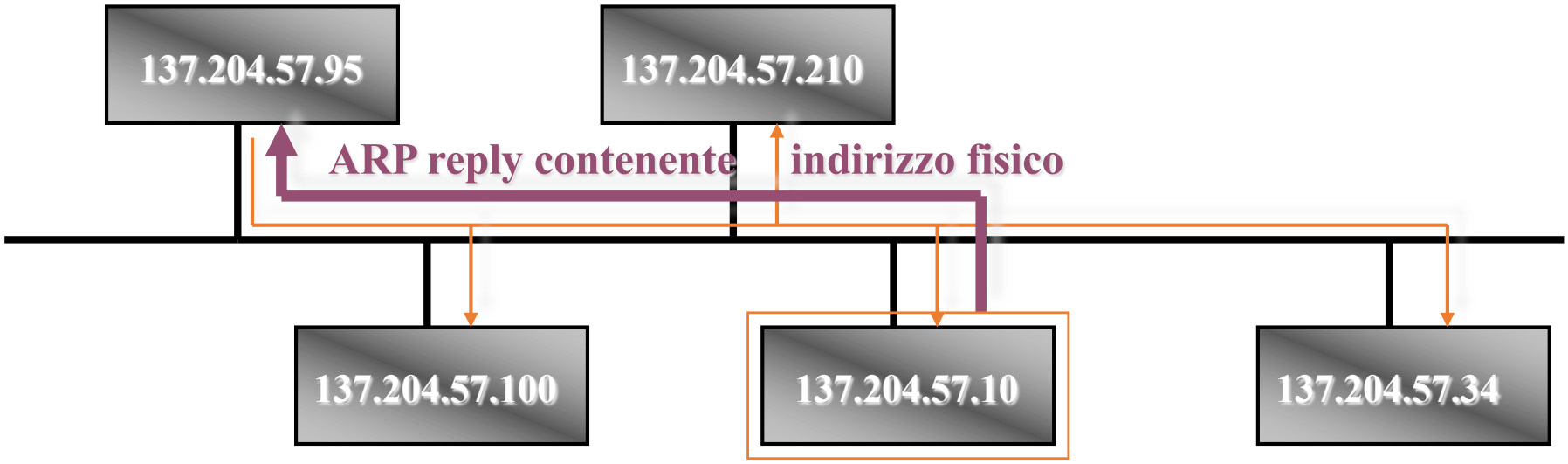
- Software di basso livello nasconde gli indirizzi fisici e consente ai livelli superiori di lavorare solo con indirizzi IP
- Gli host comunicano attraverso una **rete fisica** (ad es. LAN) quindi devono conoscere reciprocamente gli indirizzi fisici
- L'host A vuole mandare datagrammi a B, che si trova sulla stessa rete fisica e di cui conosce solo l'indirizzo IP
- Come si ricava l'indirizzo fisico di B dato il suo indirizzo IP?

Address Resolution Protocol – ARP (RFC 826)



- Il nodo sorgente invia una trama broadcast (**ARP request**) contenente l'indirizzo IP del nodo destinazione
- Tutte le stazioni della rete locale leggono la trama broadcast

Address Resolution Protocol - ARP (3)



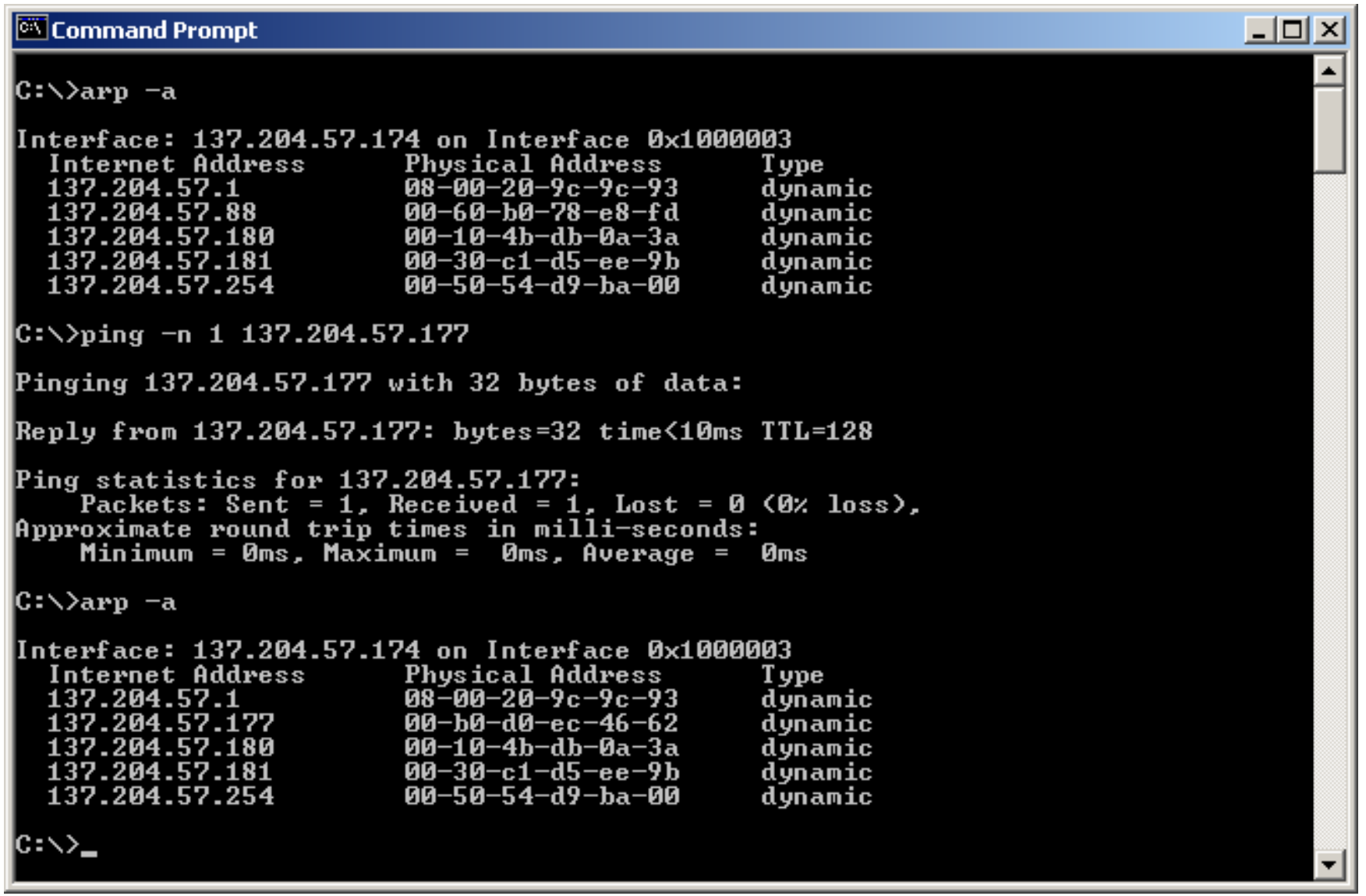
- Il destinatario risponde al mittente, inviando un messaggio (**ARP reply**) che contiene il proprio indirizzo fisico
- Con questo messaggio host sorgente è in grado di associare l'appropriato indirizzo fisico all'IP destinazione
- Ogni host mantiene una tabella (**cache ARP**) con le corrispondenze fra indirizzi logici e fisici

Comando ARP

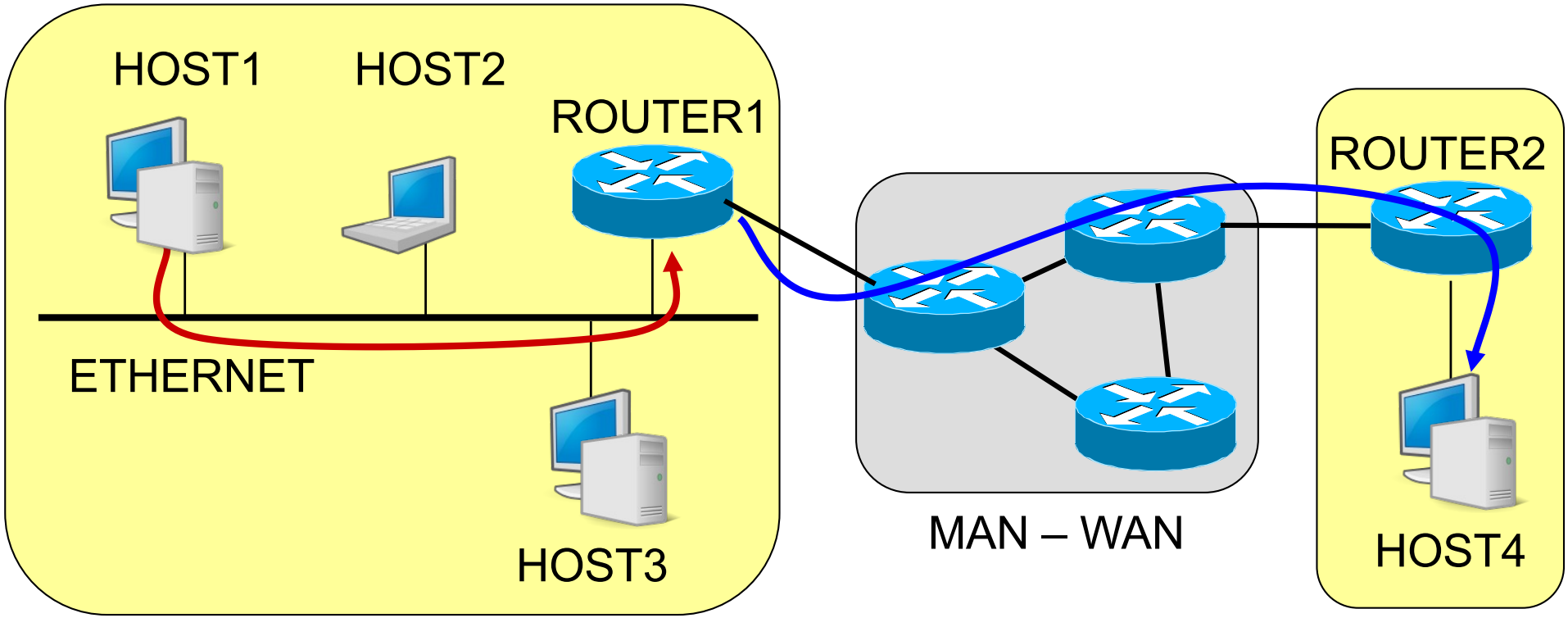
`arp -a`

visualizza il contenuto della cache ARP con le diverse corrispondenze tra indirizzi IP e MAC

Comando ARP – Esempio

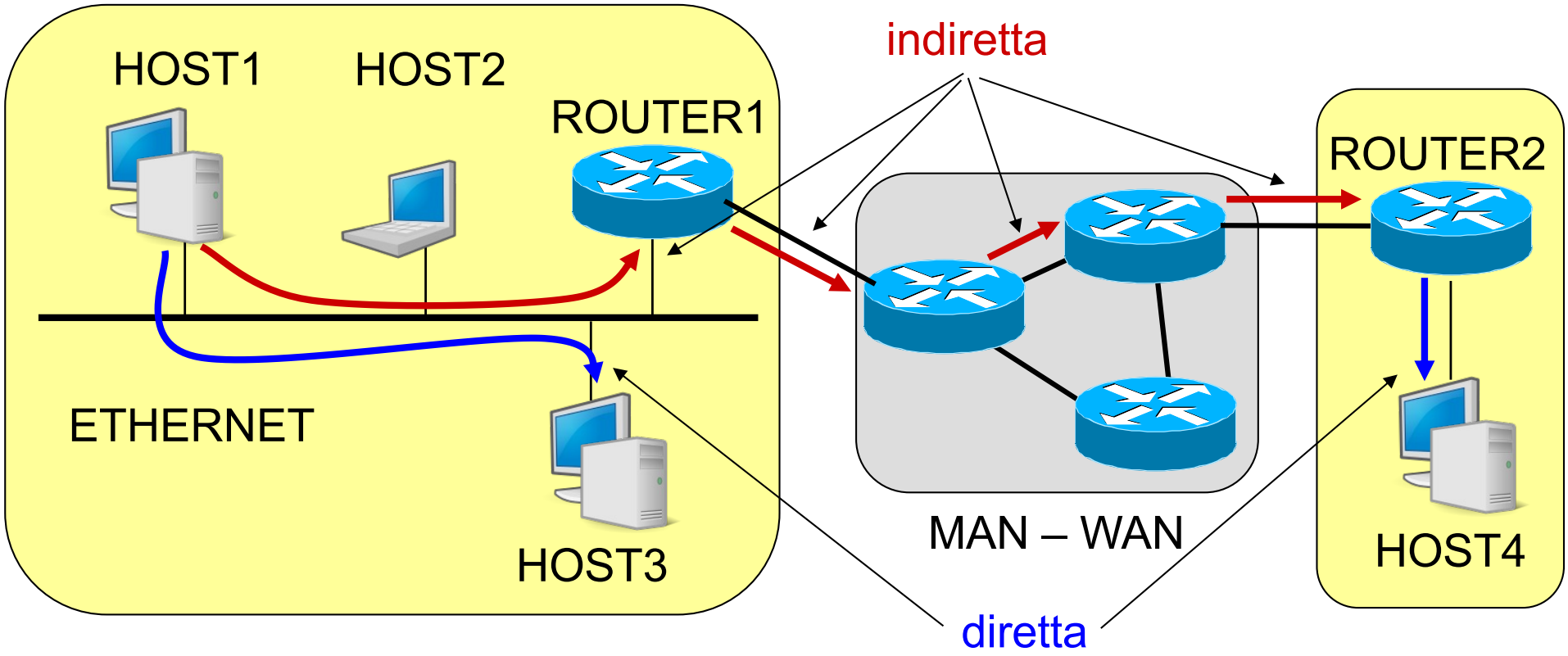


Indirect Delivery

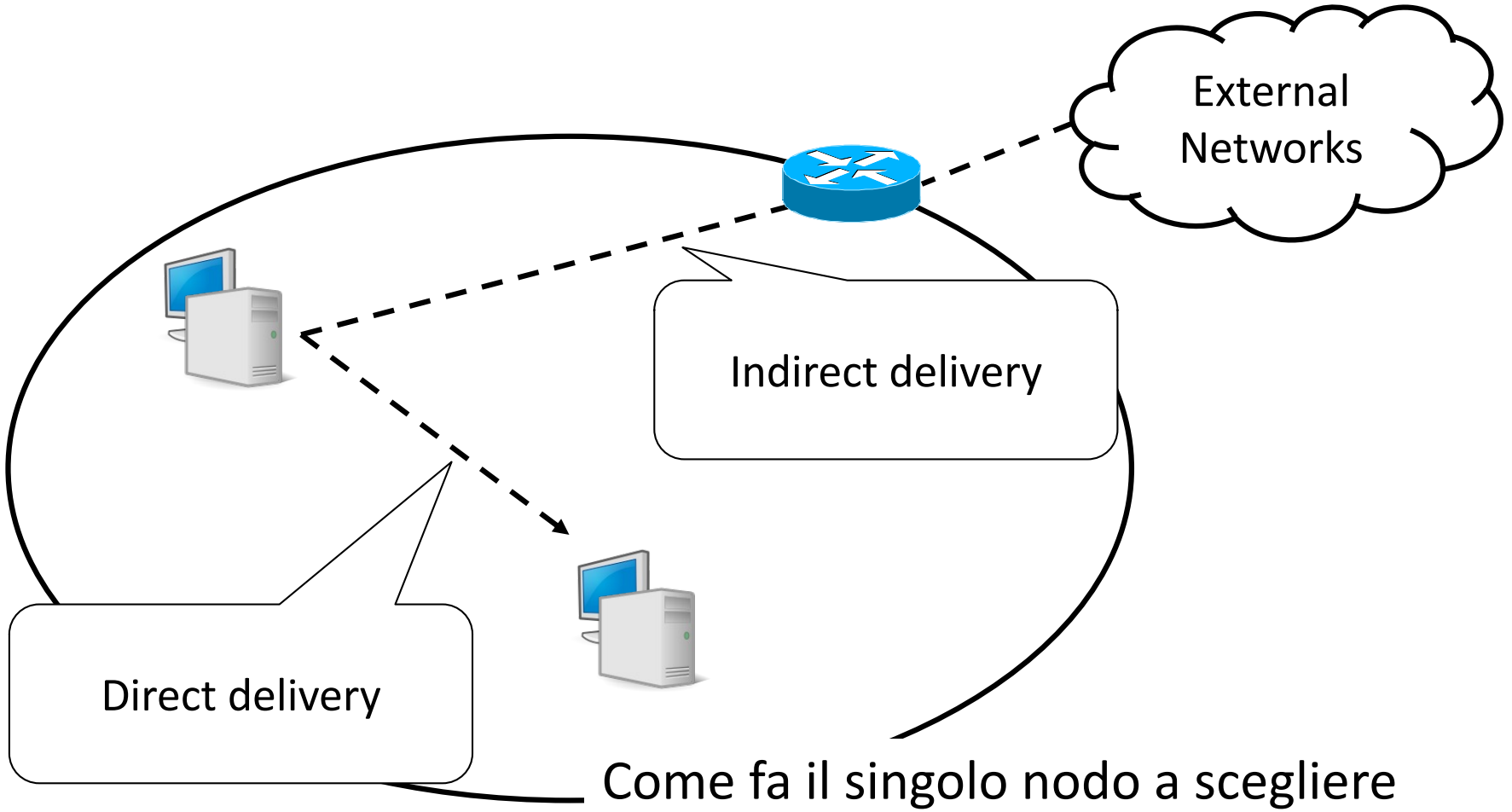


Da mittente a destinatario

- C’ è sempre una consegna diretta
- Può non esserci alcuna consegna indiretta
- Possono esserci una o più consegne indirette



Come scegliere?



Come fa il singolo nodo a scegliere

- fra instradamento diretto e indiretto?
- il gateway giusto qualora ve ne siano molteplici?

La tabella di instradamento IP

- Base dati in forma di tabella
  - Righe (dette anche route, rotte, entry, record)
    - Insieme di informazioni relative alla singola informazione di instradamento
  - Colonne (dette campi)
    - Informazioni del medesimo tipo relative a diverse opzioni di instradamento

- Formato della tabella
  - Dipende dal sistema operativo e dall'implementazione
    - Le informazioni sono le medesime
    - Il modo di presentarle ed elaborarle può essere diverso

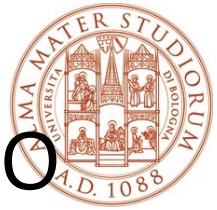
Route

- Tipici campi della singola rotta sono:
  - **Destinazione (D):** numero IP valido
    - Può essere un indirizzo di network o di host
  - **Netmask (N)**: maschera di rete valida
    - Identifica il Net-ID
  - **Gateway (G)**: numero IP a cui consegnare il datagramma
    - Indica il tipo di consegna da effettuare
  - **Interfaccia di rete (IF)**: interfaccia di rete utilizzare (loopback compreso) per la consegna del datagramma
    - Seleziona il dispositivo hardware da utilizzare per l'invio del datagramma
  - **Metrica (M)**: specifica il "costo" di quel particolare route
    - Possono esistere più route verso una medesima destinazione

La tabella

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	ppp0	1
137.204.64.0	255.255.255.0	137.204.64.254	en0	1
137.204.65.0	255.255.255.0	137.204.65.254	en1	1
137.204.66.0	255.255.255.0	137.204.66.254	en2	1
137.204.67.0	255.255.255.0	137.204.67.254	en3	1
192.168.10.0	255.255.255.252	192.168.10.2	ppp0	1

Uso della tabella di instradamento



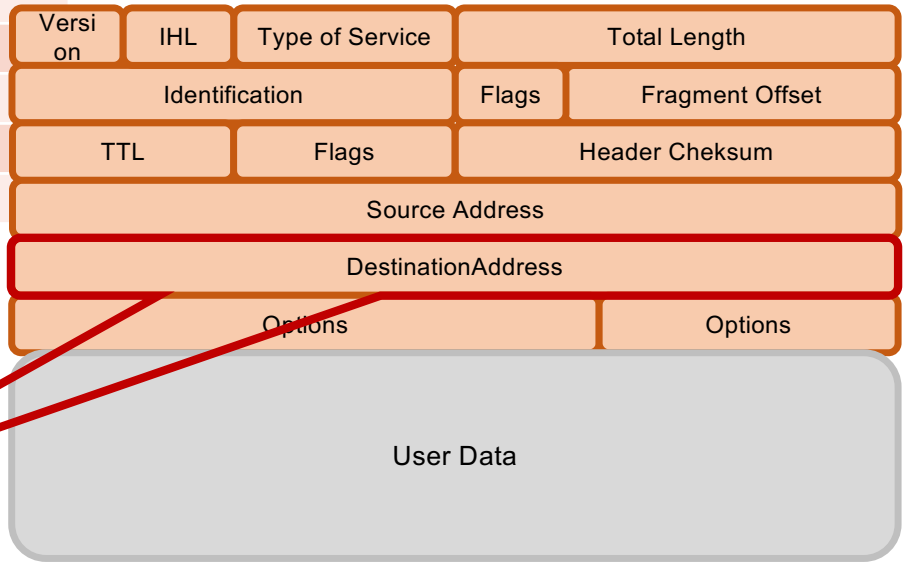
- Il singolo nodo riceve un datagramma:
  - Estrae dall'intestazione IP_D = indirizzo IP di destinazione
  - Seleziona il route per tale IP_D, confrontandolo con i campi D presenti nella tabella
    - Processo di "**table lookup**"
  - Se il route esiste
    - Esegue l'azione di instradamento suggerita dai campi G e IF
  - Se il route non esiste genera un messaggio di errore
    - Tipicamente notificato all'indirizzo sorgente (ICMP - Destination Unreachable)

Table lookup

- La ricerca nella tabella avviene confrontando
  - Indirizzo IP di destinazione IP_D del datagramma
  - Destinazione (D) di ciascun route
  - Utilizzando la netmask (N) del route
- La procedura viene detta di "longest prefix match"
  - IP_D **AND** N = R
    - Indirizzo di destinazione del datagramma e netmask di ciascuna riga
  - R = D ?
    - SI : la route viene selezionata e il processo termina
    - NO : si passa al route successivo
- In quale ordine leggere i route
  - dalla riga che presenta una netmask con un numero maggiore di bit a uno

Il lookup

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	ppp0	1
137.204.64.0	255.255.255.0	137.204.64.254	en0	1
137.204.65.0	255.255.255.0	137.204.65.254	en1	1
137.204.66.0	255.255.255.0	137.204.66.254	en2	1
137.204.67.0	255.255.255.0	137.204.67.254	en3	1
192.168.10.0	255.255.255.252	192.168.10.2	ppp0	1



Destination Address

Netmask **AND**

Result

==

Destination

YES/NO

Esempio di lookup – 1

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 192.168.2.18
- Confronto prima con riga 3, poi con riga 2 e poi riga 1

```
192.168.002.018          bitwise AND
255.255.255.255
192.168.002.018 == 192.168.002.018
```

- La riga 3 è quella giusta (host specific)

Esempio di lookup – 2

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 192.168.2.22

```
192.168.002.022
255.255.255.255
192.168.002.022 != 192.168.002.018

192.168.002.022
255.255.255.000
192.168.002.000 == 192.168.002.000
```

- La riga 2 è quella giusta (network specific)

Esempio di lookup – 3

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 80.48.15.170

```
080.048.015.170
255.255.255.255
080.048.015.170 != 192.168.002.018

080.048.015.170
255.255.255.000
080.048.015.000 != 192.168.002.000

080.048.015.170
000.000.000.000
000.000.000.000 == 000.000.000.000
```

- La riga 1 è quella giusta (default gateway)

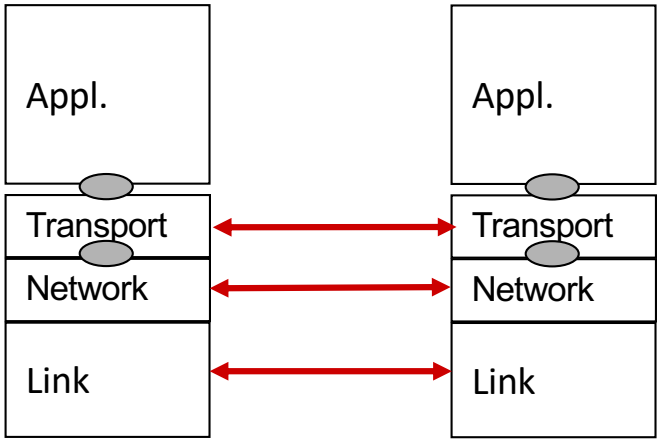
Gateway

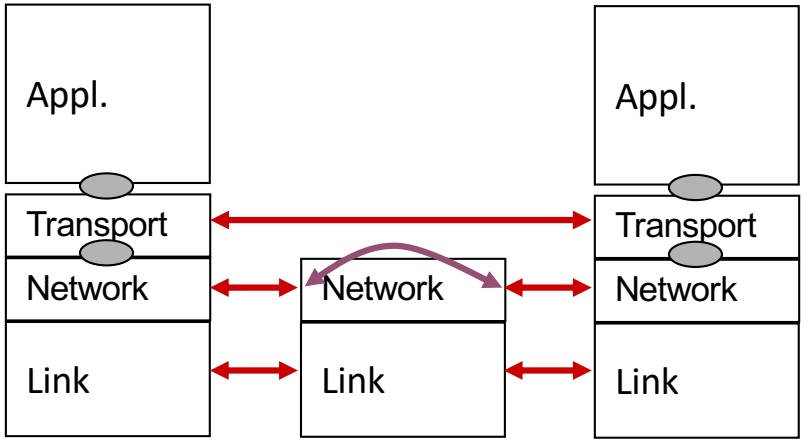
- Nella tabella di instradamento compaiono
  - Gateway
  - Interfaccia
- Perché due informazioni distinte?
- Chi è il gateway?

Il ruolo del Gateway

- Il table look-up sceglie la D i-esima = D_i
- La funzione di instradamento invia il datagramma a IF_i
- Con l'obiettivo di consegnarlo al gateway G_i
- Perché non è sufficiente IF_i?
- L'instradamento IP è basato sull'appartenenza alla network
  - Host della medesima network possono comunicare direttamente
  - Host di network diverse comunicano tramite gateway

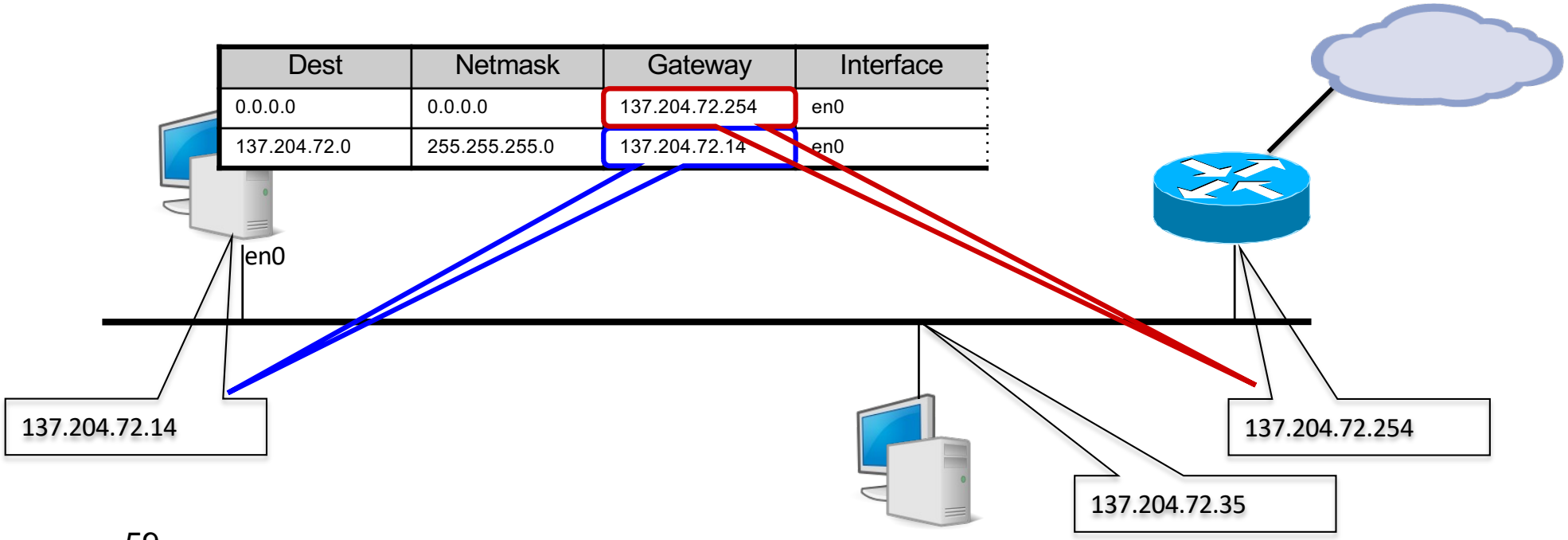
- *Gateway* = responsabile della consegna del datagramma



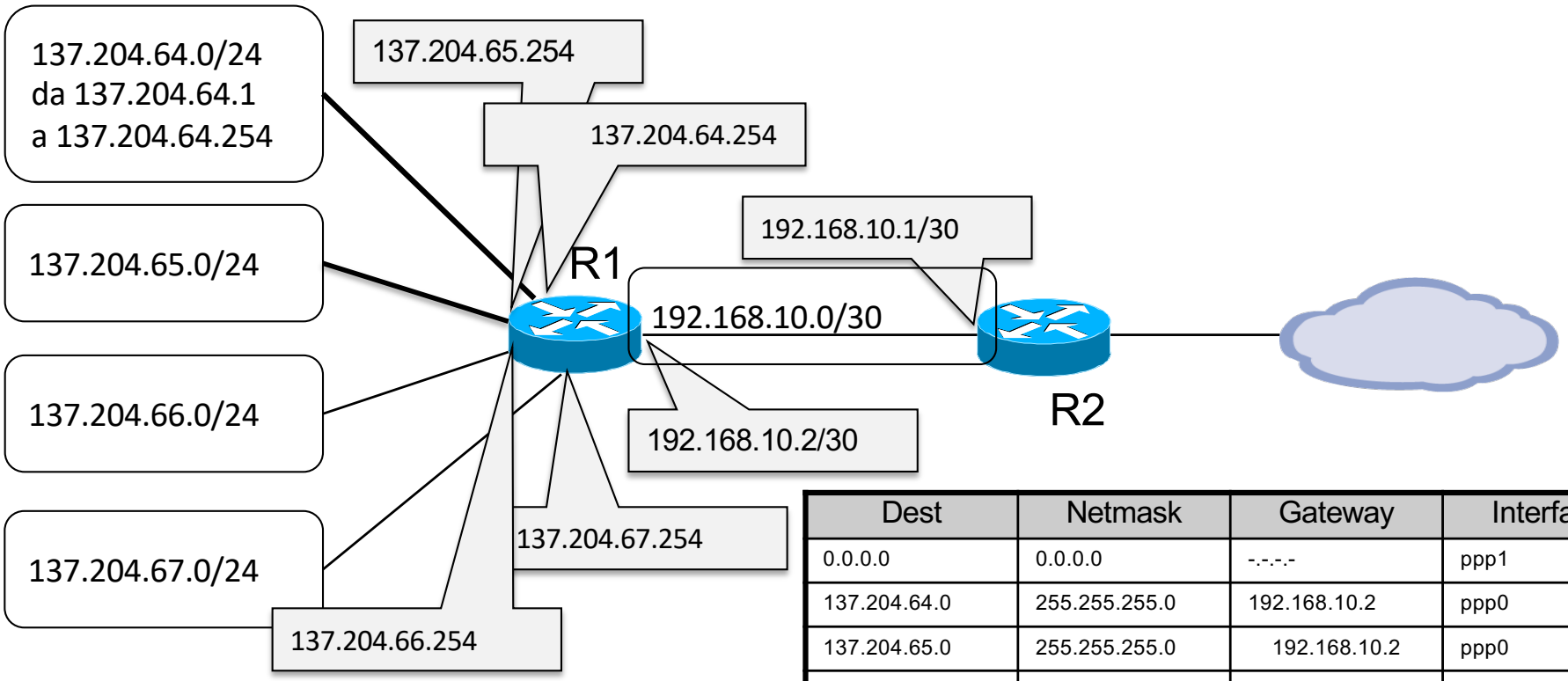


Uso del Gateway

- Il campo gateway della tabella di routing serve per specificare il tipo di instradamento
  - Instradamento diretto: la sintassi dipende dall'implementazione
    - In Windows: instradamento diretto se gateway = IP locale
    - In Linux/Unix: instradamento diretto se gateway = 0.0.0.0
  - Instradamento indiretto
    - Gateway = numero IP del router da contattare



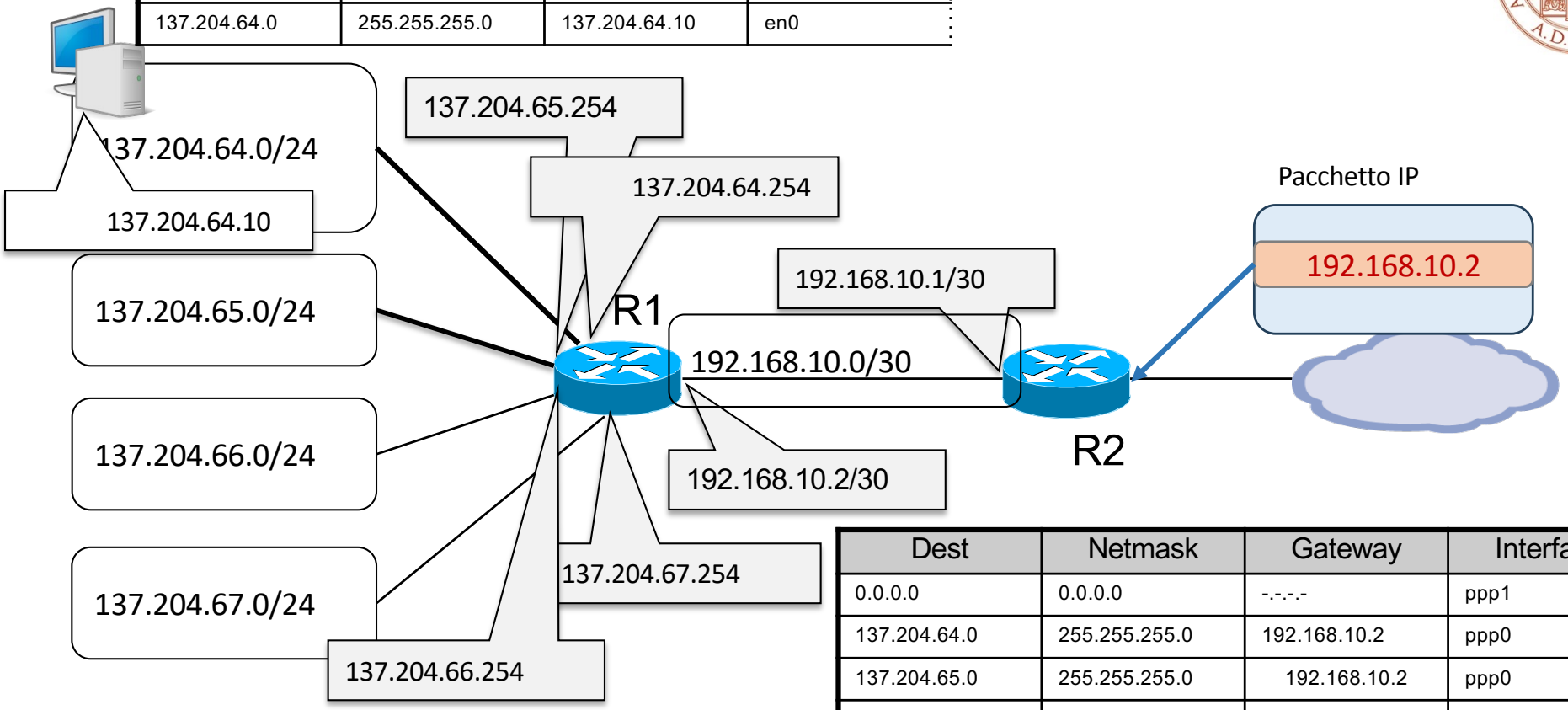
Esempio



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.66.0	255.255.255.0	137.204.66.254	en2
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.255.0	192.168.10.2	ppp0
137.204.65.0	255.255.255.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	192.168.10.2	ppp0
137.204.67.0	255.255.255.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	137.205.64.254	en0
137.204.64.0	255.255.255.0	137.204.64.10	en0



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.255.0	192.168.10.2	ppp0
137.204.65.0	255.255.255.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	192.168.10.2	ppp0
137.204.67.0	255.255.255.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	
137.204.65.0	255.255.255.0	137.204.65.254	
137.204.66.0	255.255.255.0	137.204.66.254	
137.204.67.0	255.255.255.0	137.204.67.254	
192.168.10.0	255.255.255.252	192.168.10.2	

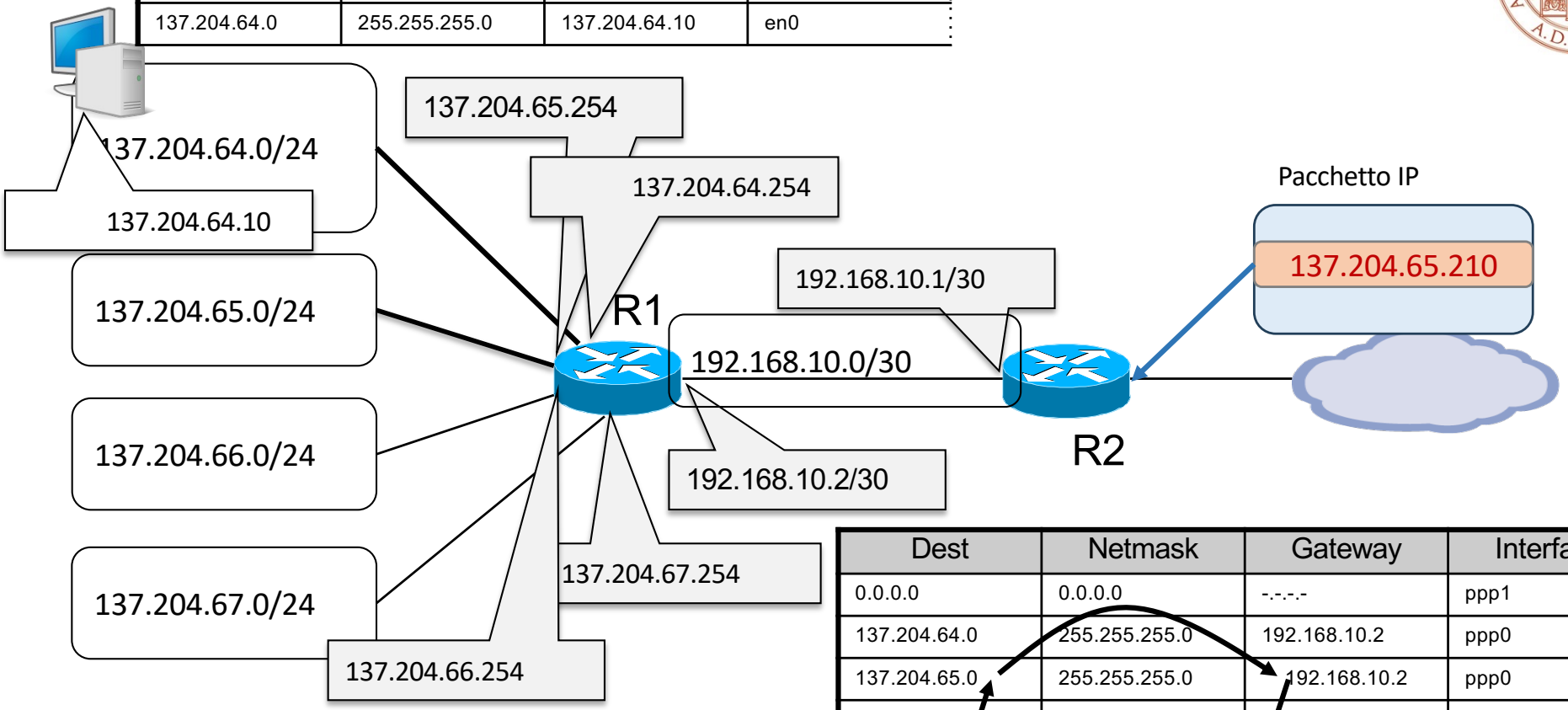
Longest prefix match

192.168-10.2 AND
255.255.255.252 =
192.168.10.0

Gateway 192.168.10.1 = me stesso

Consegna diretta a 192.168.10.2
sulla network **192.168.10.0/30**
Direct delivery su **ppp0**

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	137.205.64.254	en0
137.204.64.0	255.255.255.0	137.204.64.10	en0



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.255.0	192.168.10.2	ppp0
137.204.65.0	255.255.255.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	192.168.10.2	ppp0
137.204.67.0	255.255.255.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	
137.204.65.0	255.255.255.0	137.204.65.254	
137.204.66.0	255.255.255.0	137.204.66.254	
137.204.67.0	255.255.255.0	137.204.67.254	
192.168.10.0	255.255.255.252	192.168.10.2	

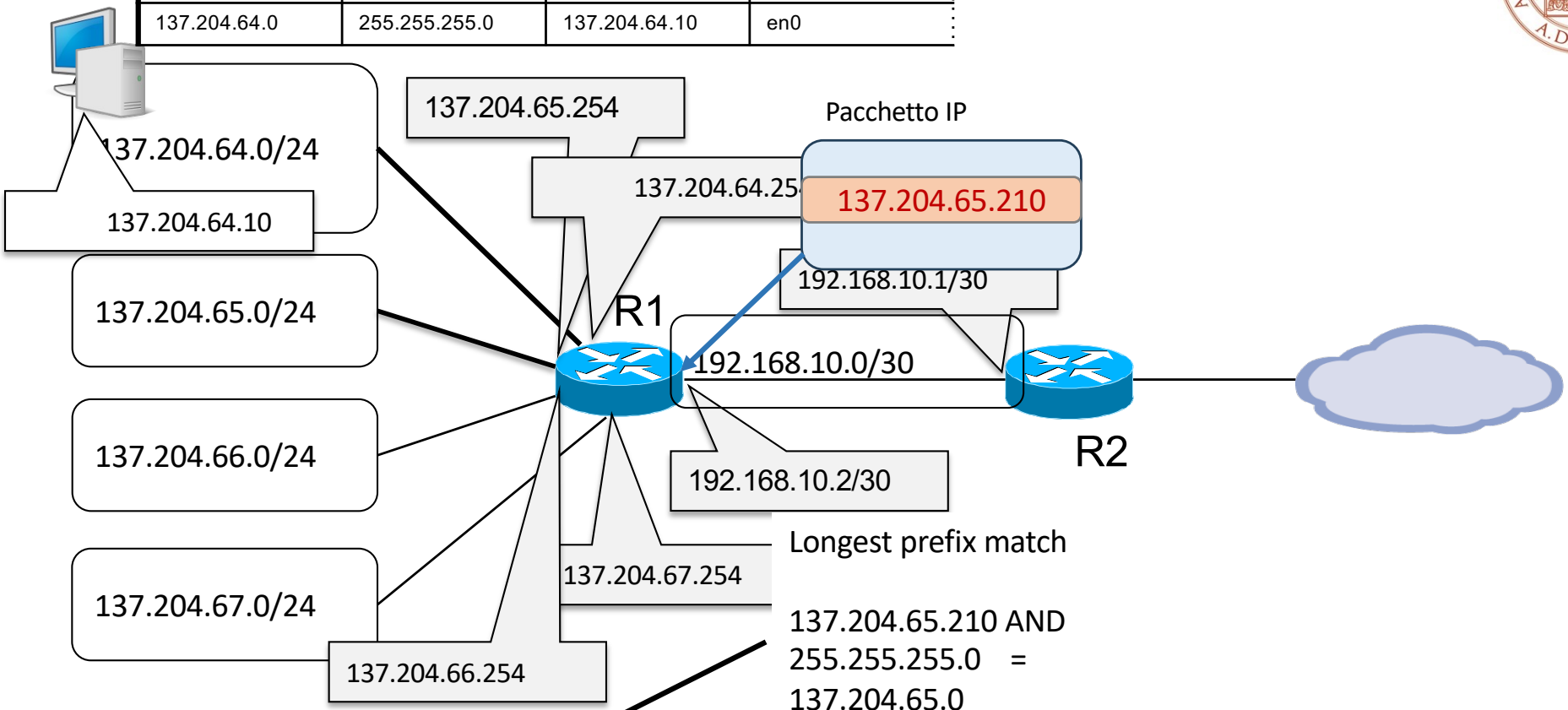
Longest prefix match

137.204.65.210 AND
255.255.255.0 =
137.204.65.0

Gateway 192.168.10.2

Consegna indiretta tramite 192.168.10.2 sulla network **192.168.10.0/30** utilizzando **ppp0**

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	137.205.64.254	en0
137.204.64.0	255.255.255.0	137.204.64.10	en0



Longest prefix match

137.204.65.210 AND
255.255.255.0 =
137.204.65.0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.66.0	255.255.255.0	137.204.66.254	en2
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

Gateway 137.204.65.254 me stesso

Consegna indiretta tramite
sulla network **137.204.65.0/24**
utilizzando **en1**

Analizziamo gli indirizzi delle 4 reti

- 137.204.64.0 il terzo byte è 01000000
- 137.204.65.0 il terzo byte è 01000001
- 137.204.66.0 il terzo byte è 01000010
- 137.204.67.0 il terzo byte è 01000011

  - I primi 2 byte ed i primi 6 bit del terzo byte sono comuni a tutte e quattro le network. Se usiamo NETMASK=255.255.252.0

```
10001001.11001100.01000000.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000000.00000000
```

137 204 **64**

```
10001001.11001100.01000001.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000000.00000000
```

137 204 **65**

```
10001001.11001100.01000010.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000000.00000000
```

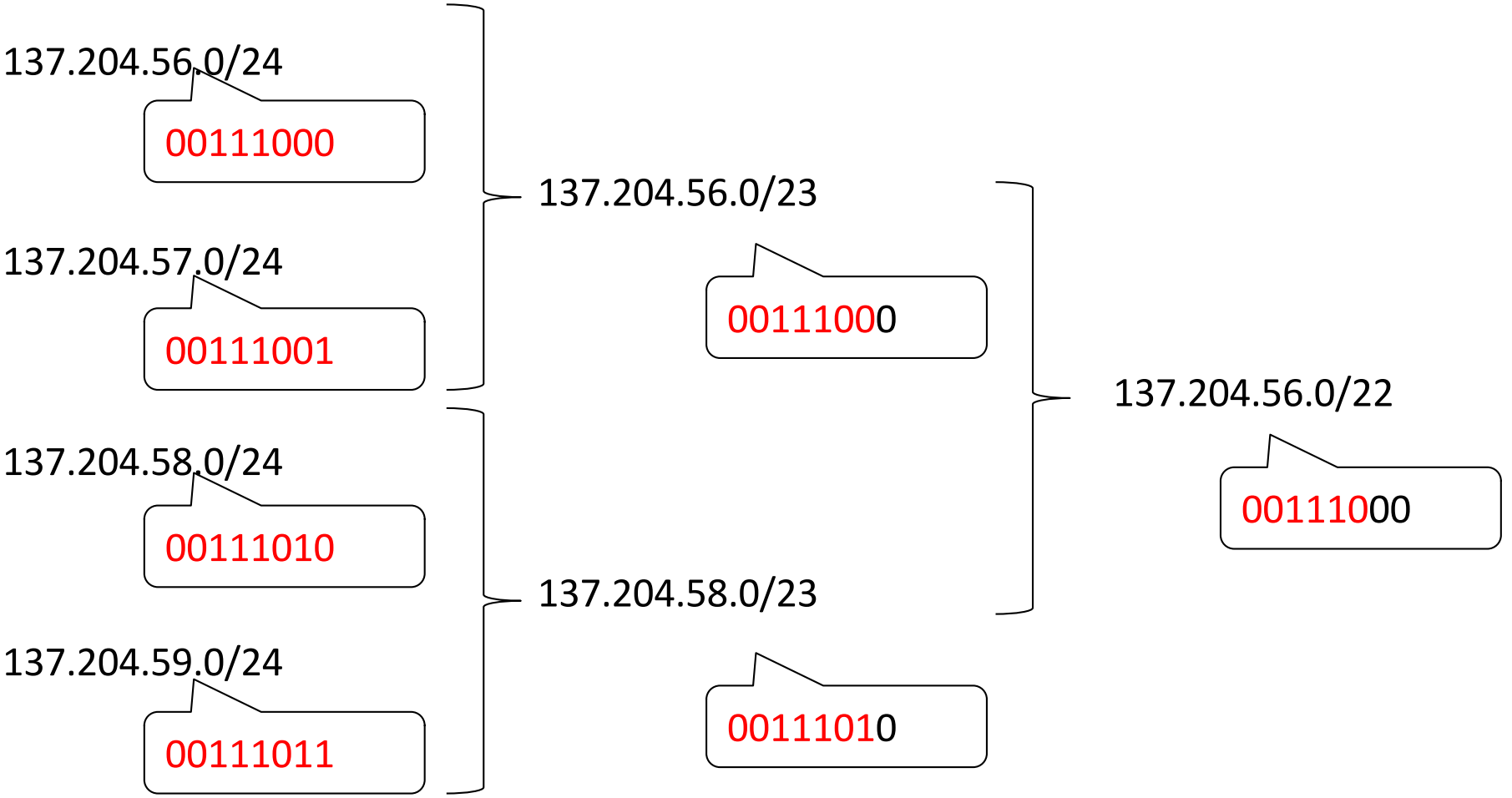
137 204 **66**

```
10001001.11001100.01000011.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000000.00000000
```

137 204 **67**

- Otteniamo il medesimo risultato in tutti e quattro i casi:
  - Il prefisso di rete è sempre 137.204.**64**.0

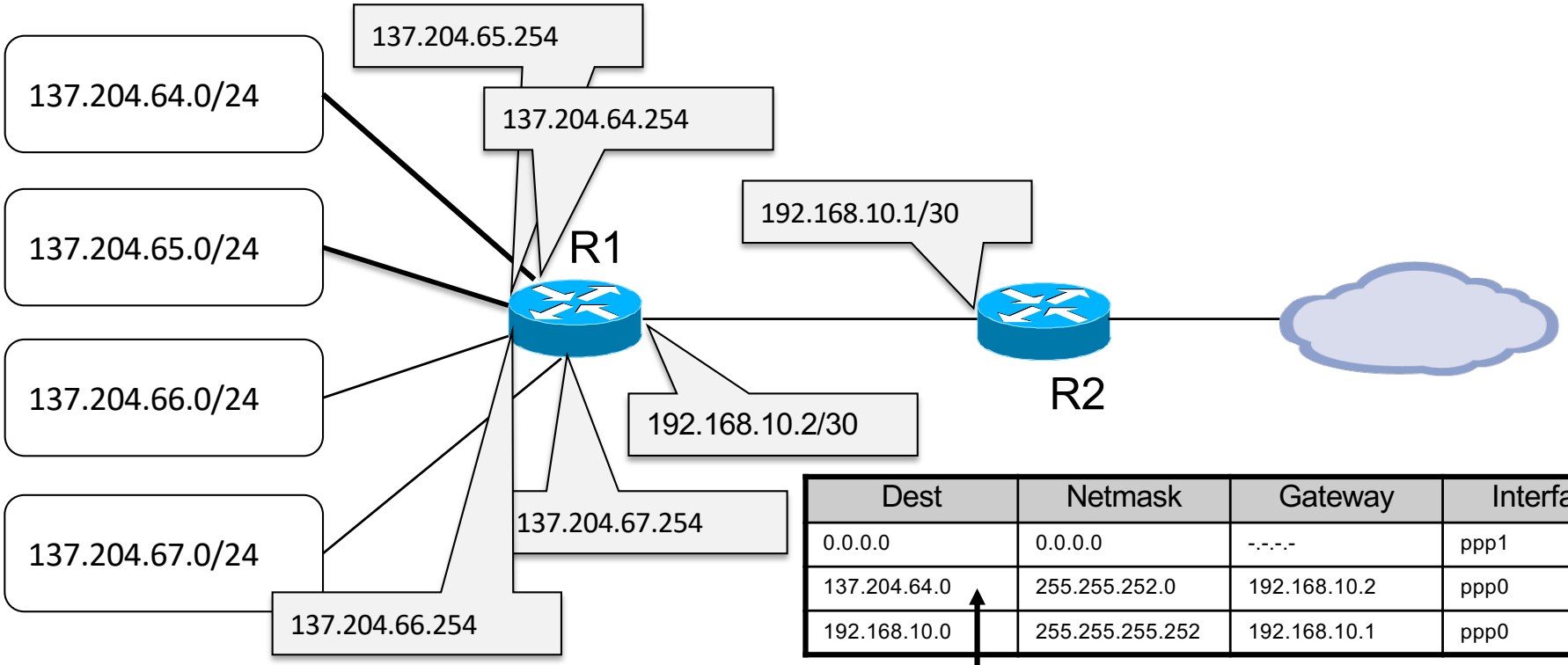
Un altro esempio



Semplificazione delle tabelle

- È necessario che R2 conosca il dettaglio di come le reti sono connesse a R1?
  - R2 invia comunque i datagrammi tramite R1
  - È sufficiente un'informazione più "riassuntiva"
- I route verso le 4 network possono essere aggregate in una sola
- R2 vede le 4 reti come una sola
  - Il gateway verso quelle destinazioni è R1

Aggregazione

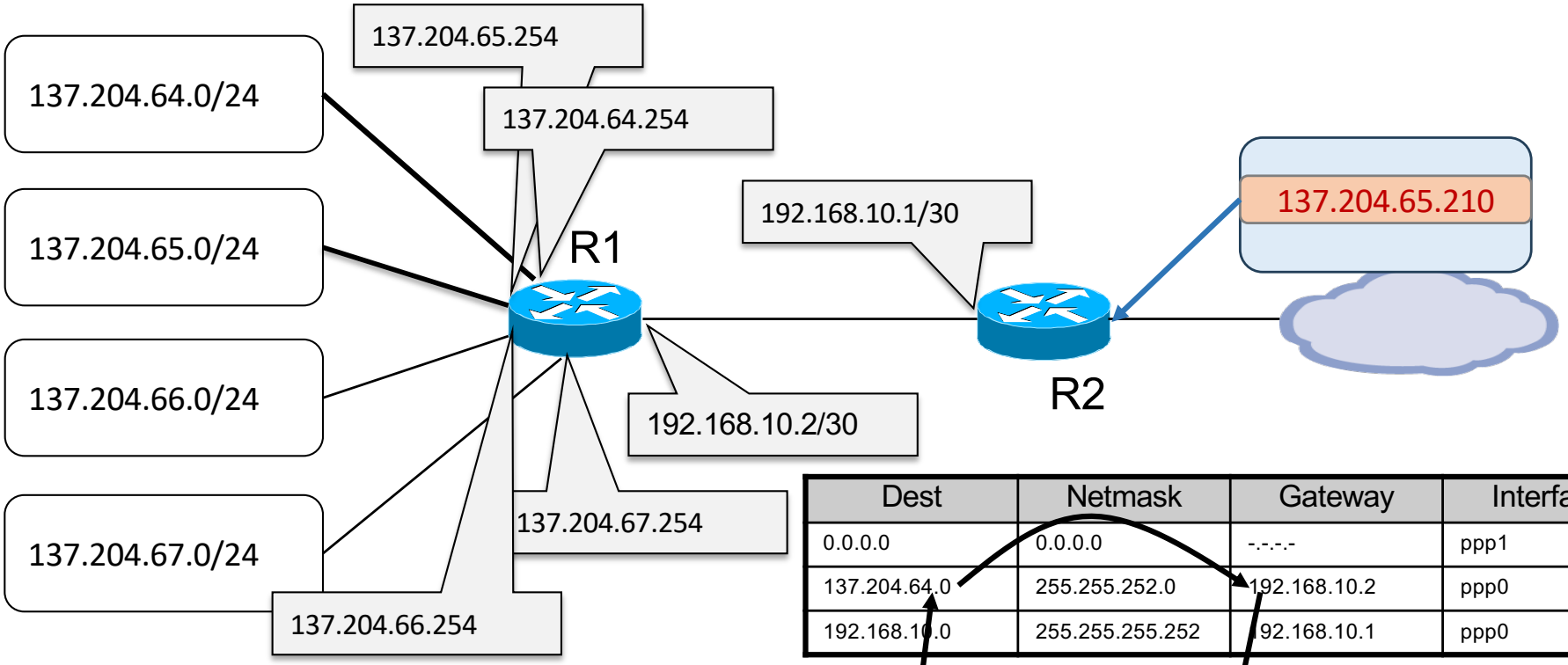


Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interfa
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.66.0	255.255.255.0	137.204.66.254	en2
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

Le network
137.204.64.0/24
137.204.65.0/24
137.204.66.0/24
137.204.66.0/24
Vengono aggregate in un'unica destinazione
137.204.64.0/22

Aggregazione



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	
137.204.65.0	255.255.255.0	137.204.65.254	
137.204.66.0	255.255.255.0	137.204.66.254	
137.204.67.0	255.255.255.0	137.204.67.254	
192.168.10.0	255.255.255.252	192.168.10.2	

Longest prefix match

137.204.65.210 AND
255.255.252.0 =
137.204.64.0

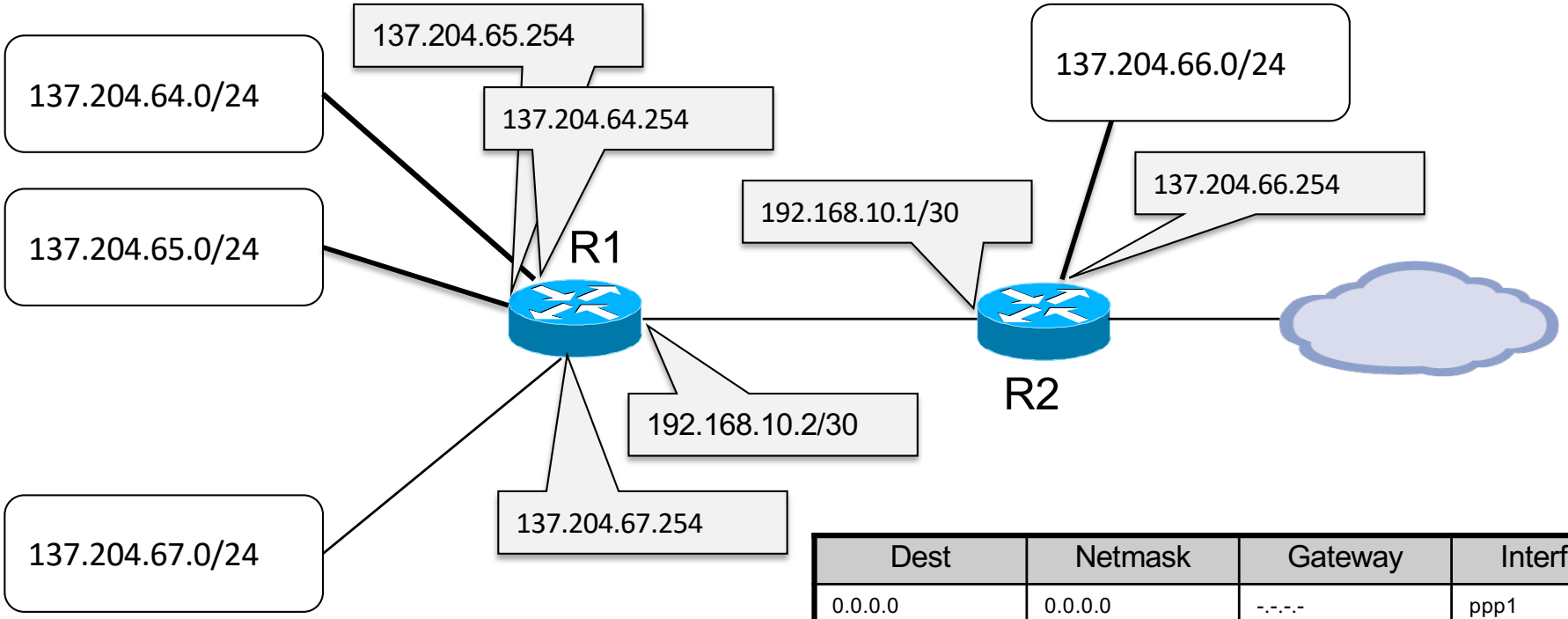
Gateway 192.168.10.2

Consegna indiretta tramite 192.168.10.2 sulla network **192.168.10.0/30** utilizzando **ppp0**

Perché ordinare i route?

- Dare priorità alle route più specifiche
- L'ordinamento in funzione della Netmask decrescente garantisce di considerare in ordine
  - singoli host
  - reti piccole
  - reti grandi
- È possibile implementare eccezioni a regole generali che possono convivere nella medesima tabella

Eccezioni

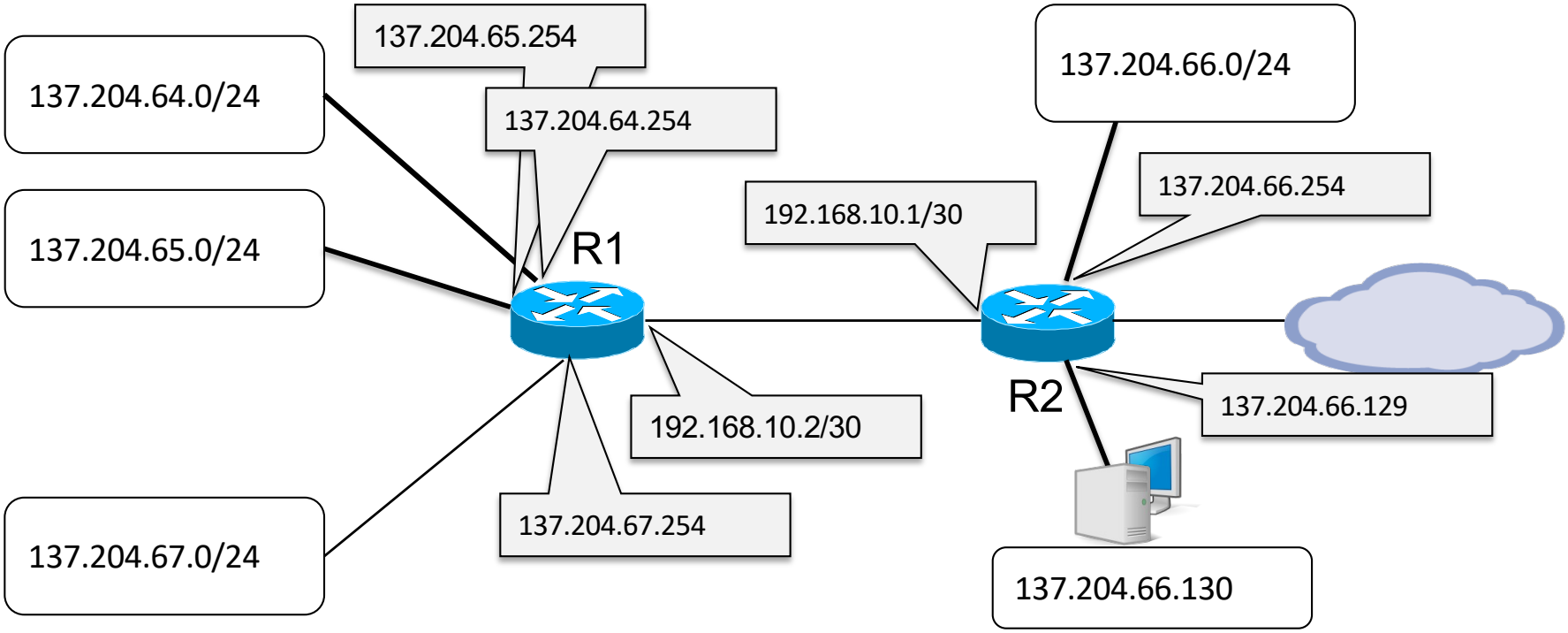


Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	137.204.66.254	en0
192.168.10.0	255.255.255.252	192.168.10.1	Ppp0

La rotta per 137.204.66.0/24 viene cancellata e non è necessario modificarla perché adesso viene assorbita dalla rotta di default

Eccezioni



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	137.204.66.254	en0
192.168.10.0	255.255.255.252	192.168.10.1	Ppp0
137.204.66.128	255.255.255.252	137.204.66.129	en1

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Classless VS Classfull
la logica degli indirizzi IP

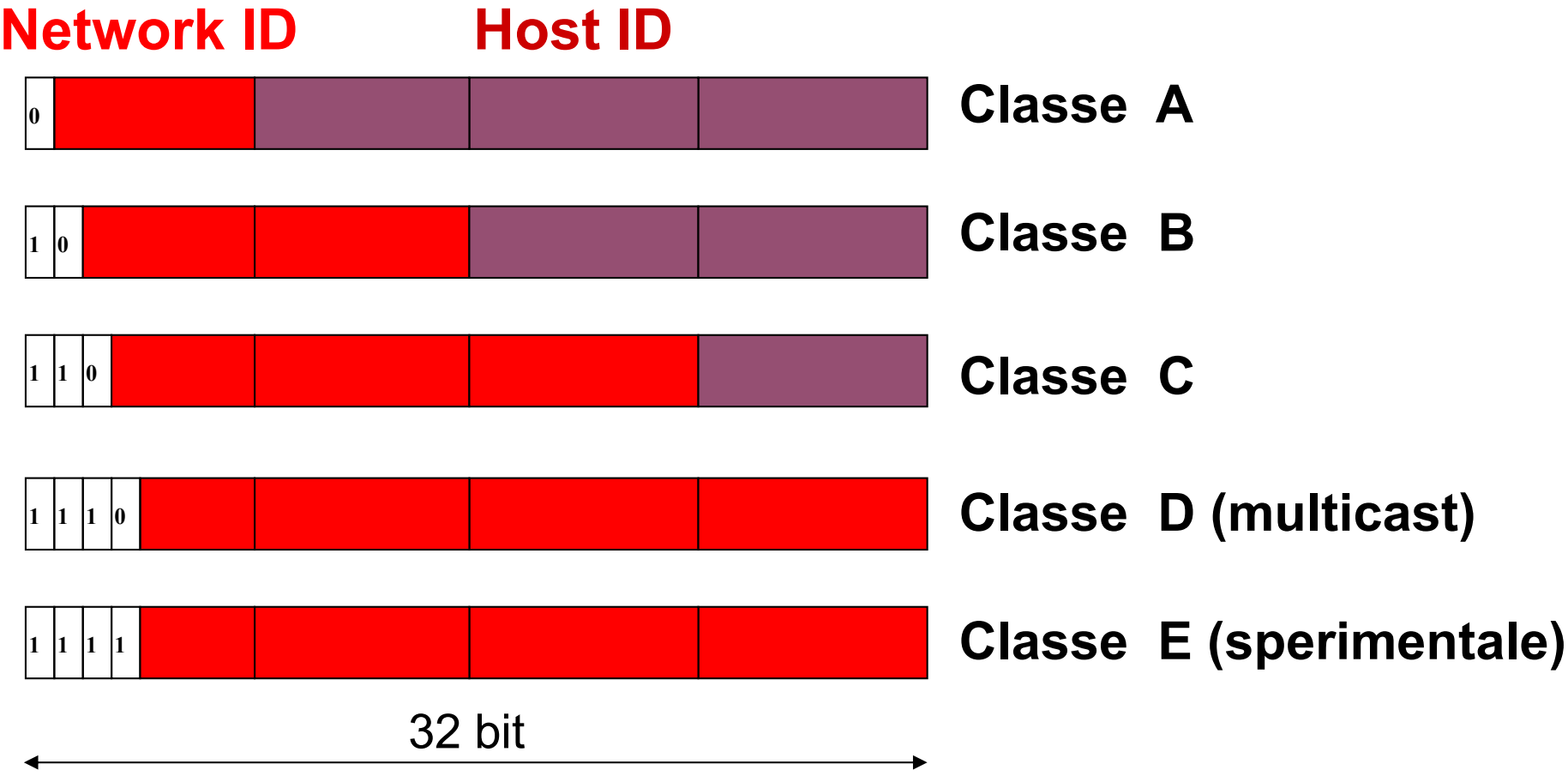
IP e netmask

- Il numero IP ha valore assoluto in rete
  - Un numero IP pubblico deve essere unico su Internet
  - I numeri IP sorgente e destinazione caratterizzano il datagramma in quanto parte della sua intestazione
- La netmask è relativa al singolo nodo
  - Non viene trasportata nell'intestazione del datagramma
  - È parte della tabella di routing dei singoli nodi
  - Ai medesimi indirizzi possono corrispondere netmask diverse in nodi diversi (route aggregation)
- È sempre stato così?
  - NO: inizialmente la suddivisione net-ID e host-ID era assoluta

Classe delle reti

- Durante la fase iniziale di Internet furono definite diverse “classi” di network differenziate per dimensione
  - La parte iniziale del Net-ID differenzia le classi
    - 0 classe A
    - 10 classe B
    - 110 classe C
  - La definizione delle classi è standard e quindi nota a tutti
  - I router riconoscono la classe di una rete dai primi bit dell’indirizzo
    - Ricavano di conseguenza il Net-ID

Classi di indirizzi



Network ID : identifica una rete IP

Host ID : identifica i singoli calcolatori della rete

Intervalli di indirizzi

- Classe A: **da 0.0.0.0 a 127.255.255.255**
- Classe B: **da 128.0.0.0 a 191.255.255.255**
- Classe C: **da 192.0.0.0 a 223.255.255.255**
- Classe D: **da 224.0.0.0 a 239.255.255.255**
- Classe E: **da 240.0.0.0 a 255.255.255.255**

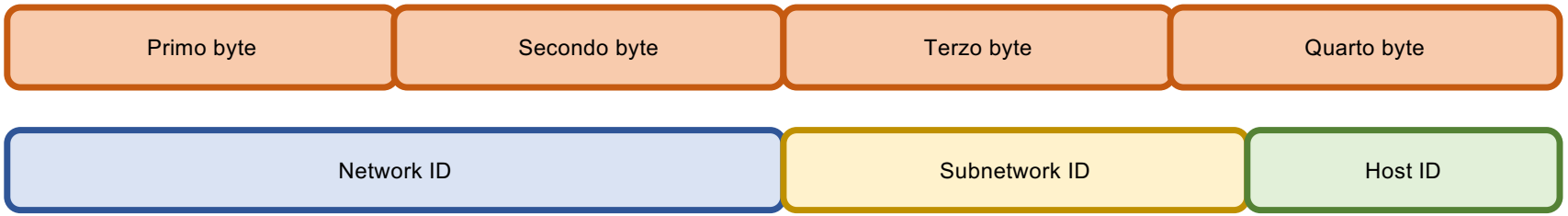
- Indirizzi riservati (RFC 1700)
  - **0.0.0.0** indica l'host corrente senza specificarne l'indirizzo
  - **Host-ID tutto a 0** viene usato per indicare la rete
  - **Host-ID tutto a 1** è l'indirizzo di broadcast per quella rete
  - **0.x.y.z** indica un certo Host-ID sulla rete corrente senza specificare il Net-ID
  - **255.255.255.255** è l'indirizzo di broadcast su Internet
  - **127.x.y.z** è il **loopback**, che redirige i datagrammi agli strati superiori dell'host corrente

Le sottoreti

- A un'amministrazione è assegnata una network
  - L'amministrazione potrebbe essere suddivisa in sotto-amministrazioni *logicamente separate*
  - Converrebbe "*frammentare*" la network in "*sub-network*" da assegnare alle sotto-amministrazioni
- Si decide localmente una sotto-ripartizione Net/Host ID indipendente dalle classi
- Si frammenta l'Host-ID in due parti:
  - la prima identifica la sottorete (subnet-ID)
  - la seconda identifica i singoli host della sottorete
- La ripartizione deve essere *locale* e *reversibile*
  - Tutta Internet vede comunque una certa network come un'entità unitaria

Subnetting

- La suddivisione è locale alla singola interfaccia
  - Deve essere configurabile localmente
- Si personalizza la ***Netmask***




```
11111111 11111111  1111111111 000000
Netmask /26
```

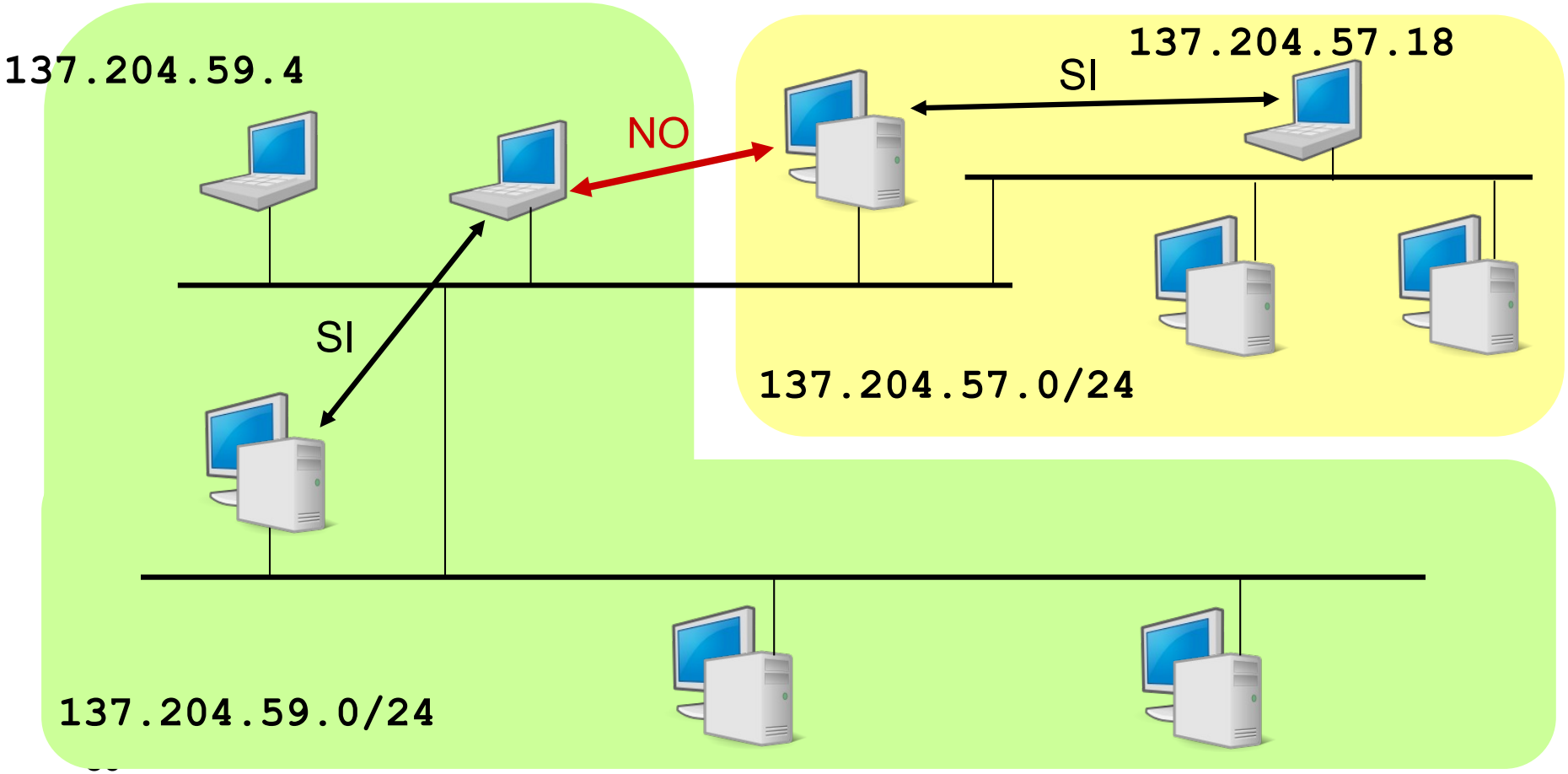
Esempio: Università di Bologna

- Una network di classe B (137.204.0.0)
  - Numerose entità distinte nella stessa amministrazione
    - Facoltà, Dipartimenti, Centri di ricerca ecc.
  - Si suddivide la rete (network) in sottoreti (subnetwork)
- Il primo byte del Host-ID viene utilizzato come indirizzo di sottorete
  - Dalla network di classe B si ricavano 254 network della dimensione di una classe C

Netmask = 255.255.255.0

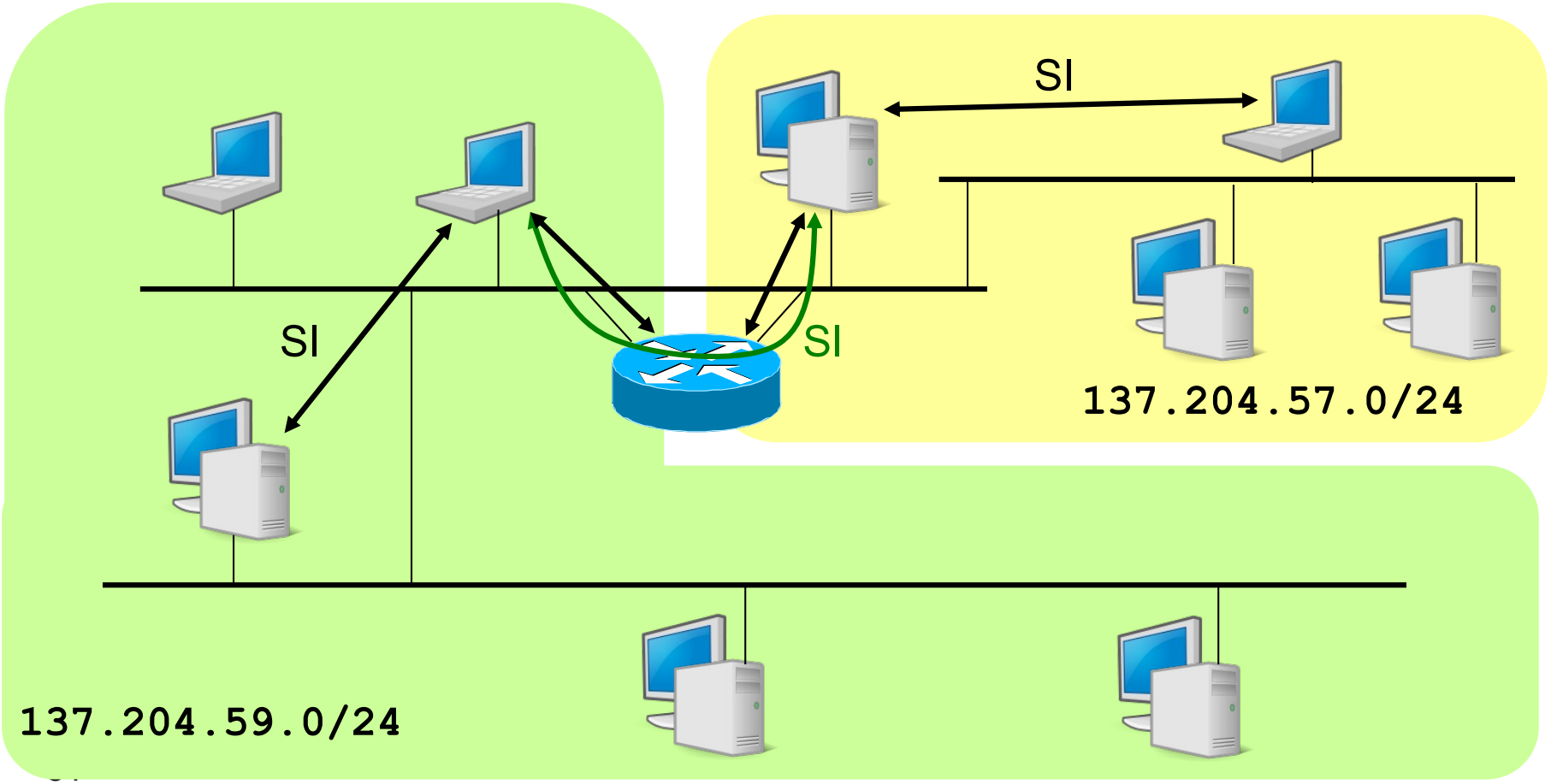
Subnetting

- Subnet diverse sono di fatto Network diverse e quindi non comunicano
- È necessario un gateway



Subnetting

- Il Gateway permette instradamento indiretto fra le Subnetwork



CIDR

- Con la grande diffusione di Internet la rigida suddivisione nelle 3 classi rendono l'instradamento poco flessibile e scalabile
- CIDR (RFC 1519) Classless InterDomain Routing
  - Si decide di rompere la logica delle classi nei router
  - La dimensione del Net-ID può essere qualunque
  - Le tabelle di routing devono comprendere anche le Netmask
  - Generalizzazione del subnetting/supernetting
    - reti IP definite da **Net-ID/Netmask**

Obiettivi del CIDR

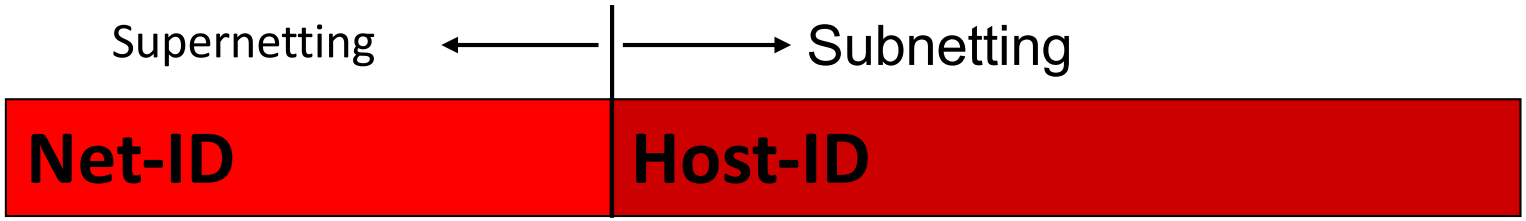
- Allocazione di reti IP di dimensioni variabili
  - utilizzo più efficiente dello spazio degli indirizzi
- Accorpamento delle informazioni di routing
  - più reti contigue rappresentate da un'unica riga nelle tabelle di routing
- Miglioramento di due situazioni critiche
  - Limitatezza di reti di classe A e B
  - Crescita esplosiva delle dimensioni delle tabelle di routing

Supernetting

- Raggruppare più reti con indirizzi consecutivi
  - Indicarle nelle tabelle di routing con una sola entry accompagnata dalla opportuna Netmask
- Es. Un ente ha bisogno di circa 2000 indirizzi IP
  - una rete di classe B è troppo grande (64K indirizzi)
  - meglio 8 reti di classe C (8 × 256 = 2048 indirizzi) dalla 194.24.0.0 alla 194.24.7.0
- **Supernetting**: si accorpano le 8 reti contigue in un'unica super-rete:
  - Identificativo: 194.24.0.0/21
  - Supernet mask: 255.255.248.0
  - Indirizzi: 194.24.0.1 – 194.24.7.254
  - Broadcast: 194.24.7.255

Supernetting

- Subnetting e Supernetting sono operazioni duali
  - Subnetting → **n** bit del Host-ID diventano parte del Net-ID
  - Supernetting → **n** bit del Net-ID diventano parte dell'Host-ID

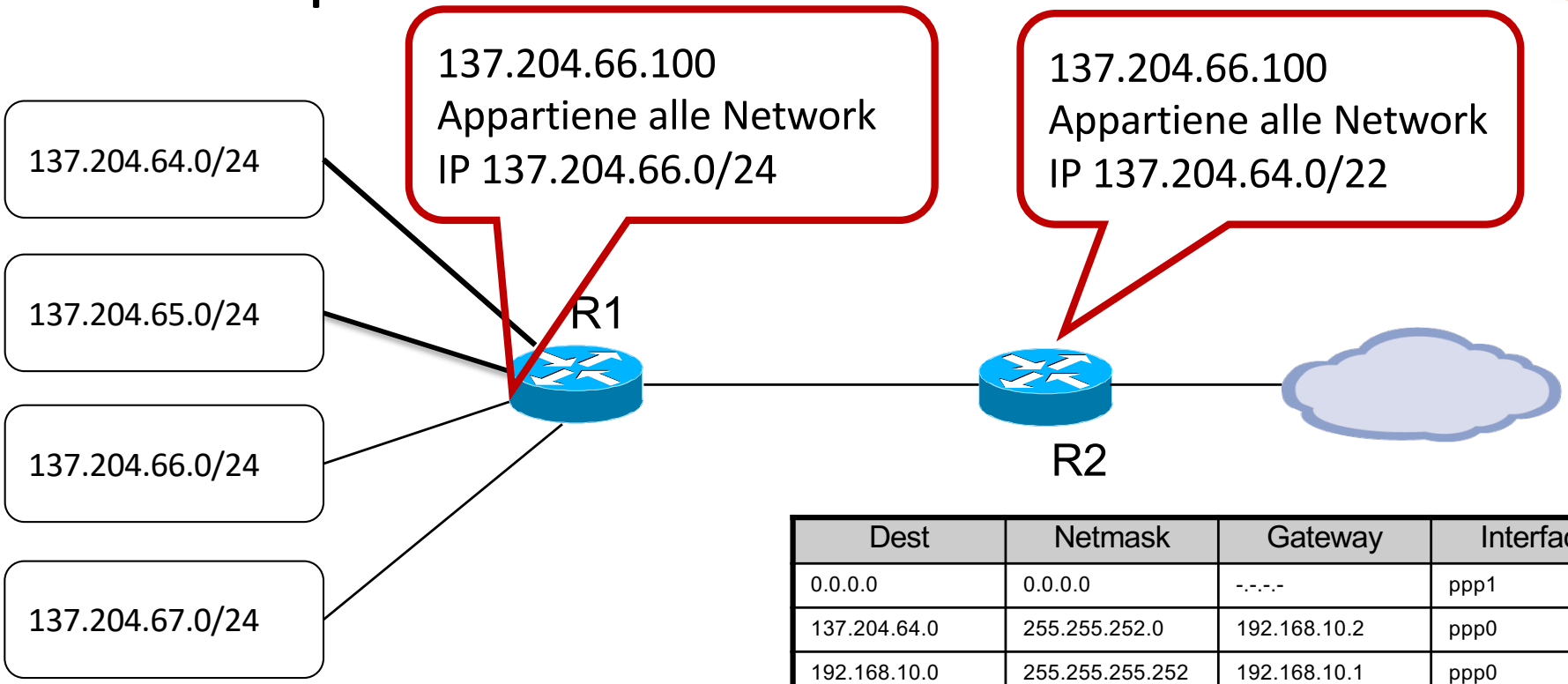


- Accorpamento di **N** reti IP (**$N = 2^n$**)
  - **contigue**:
    - 194.24.0.0/24 + 194.24.1.0/24 = 194.24.0.0/23
    - 194.24.0.0/24 + 194.24.2.0/24 = non contigue
  - **allineate** secondo i multipli di 2^n
    - 194.24.0.0/24 + .1.0/24 + .2.0/24 + .3.0/24 = 194.24.0.0/22
    - 194.24.2.0/24 + .3.0/24 + .4.0/24 + .5.0/24 = non allineate

Oggi

- La distinzione fra Net-ID e Host-ID è locale funzione della Netmask
- Lo stesso indirizzo può essere interpretato in modo diverso in punti diversi della rete
- Tutte le tabelle di instradamento devo contenere la colonna delle Netmask

Esempio



Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.66.0	255.255.255.0	137.204.66.254	en2
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

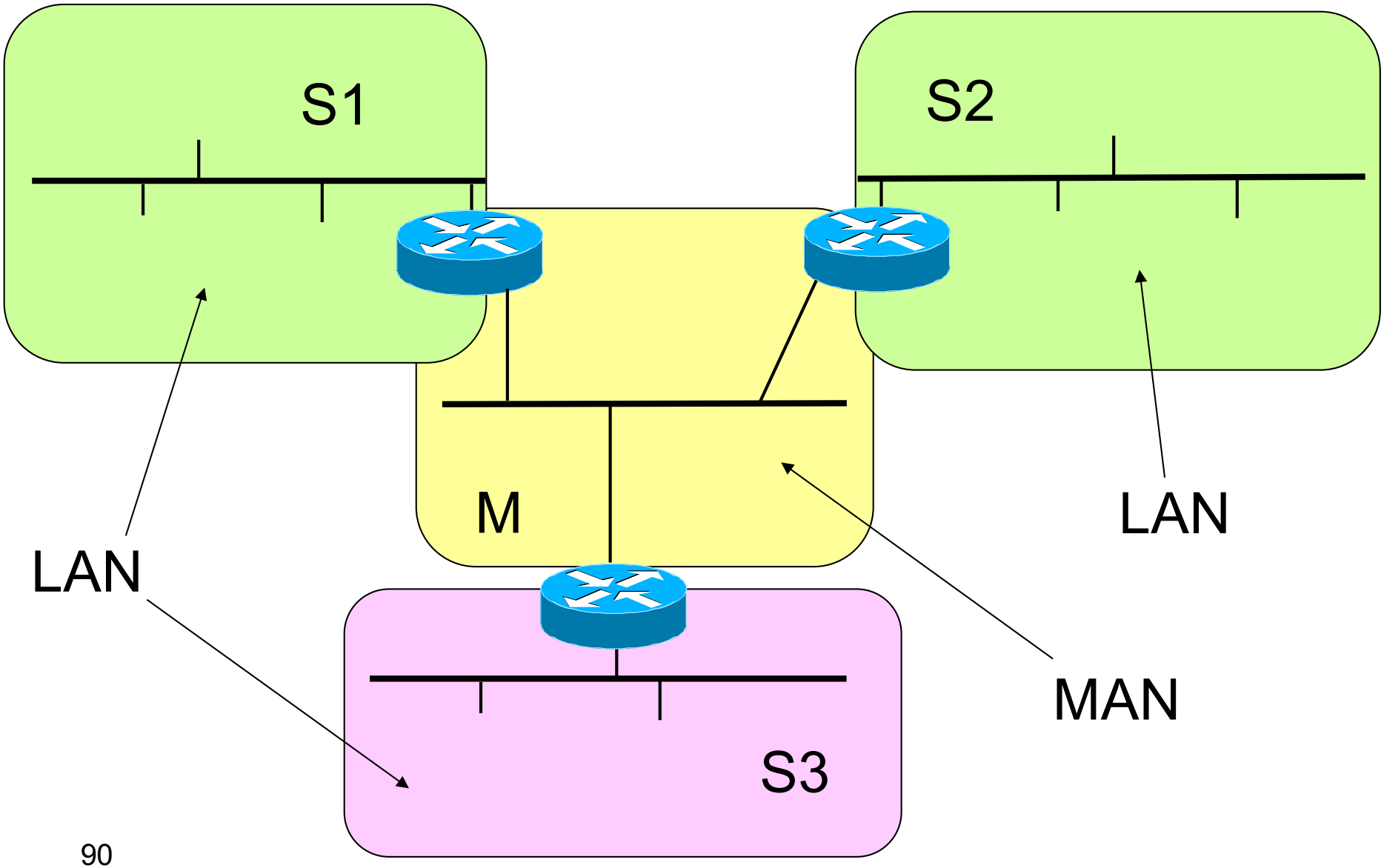
ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Pianificare la numerazione di reti IP

Esempio

- Un’azienda possiede tre siti distribuiti su una grande area urbana: S1, S2, S3.
- Ciascun sito aziendale è dotato di infrastrutture informatiche comprendenti, tra l'altro, una LAN ed un router di uscita verso il mondo esterno. Tutti i siti devono essere interconnessi tra loro con una rete a maglia completa.
- I siti sono così divisi:
  - S1, S2: 50 host
  - S3: 20 host
- Si richiede di progettare una rete di classe C a cui viene assegnato l’indirizzo 196.200.96.0/24 comprensiva della numerazione dei router, definendo le relative netmask

Architettura



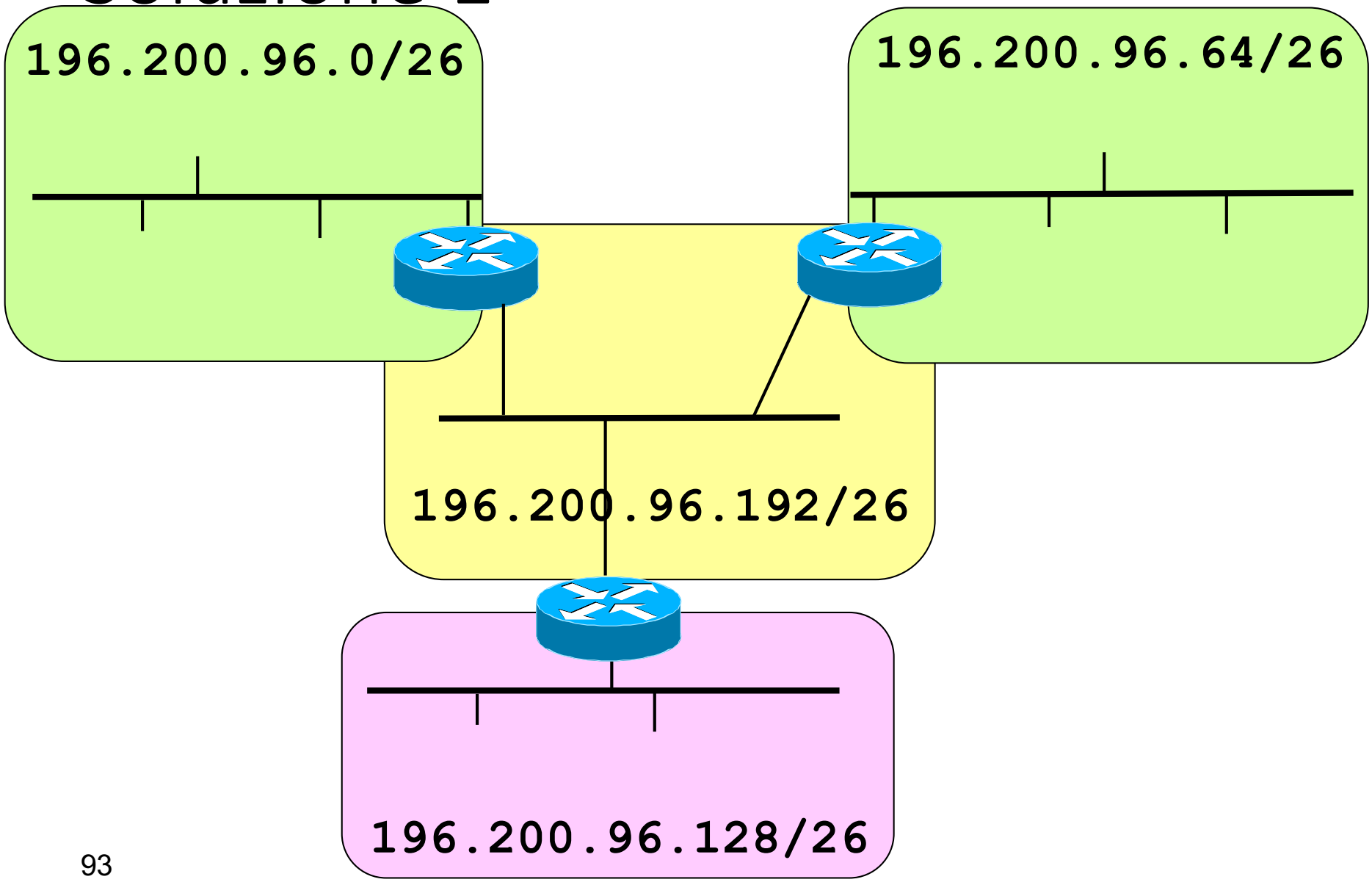
La scelta della netmask

Ultimo byte netmask	# host	# subnets
00000000	254	1
10000000	126	2
11000000	62	4
11100000	30	8
11110000	14	16
11111000	6	32
11111100	2	64

Soluzione 1

- Subnets:
  - **196.200.96.0/26** **(S1)**
  - **196.200.96.64/26** **(S2)**
  - **196.200.96.128/26** **(S3)**
  - **196.200.96.192/26** **(M)**
- Netmask: **255.255.255.192**
- Broadcast:
  - **196.200.96.63** **(S1)**
  - **196.200.96.127** **(S2)**
  - **196.200.96.191** **(S3)**
  - **196.200.96.255** **(M)**

Soluzione 1



Soluzione 1

- Routers LAN: **196.200.96.62 (S1)**
  196.200.96.126 (S2)
  196.200.96.190 (S3)

- Routers MAN: qualunque indirizzo tra:
  196.200.96.193 e **.254 (M)**

- IP Hosts: qualunque indirizzo tra:
  196.200.96.1 e **.61 (S1)**
  196.200.96.65 e **.125 (S2)**
  196.200.96.129 e **.189 (S3)**

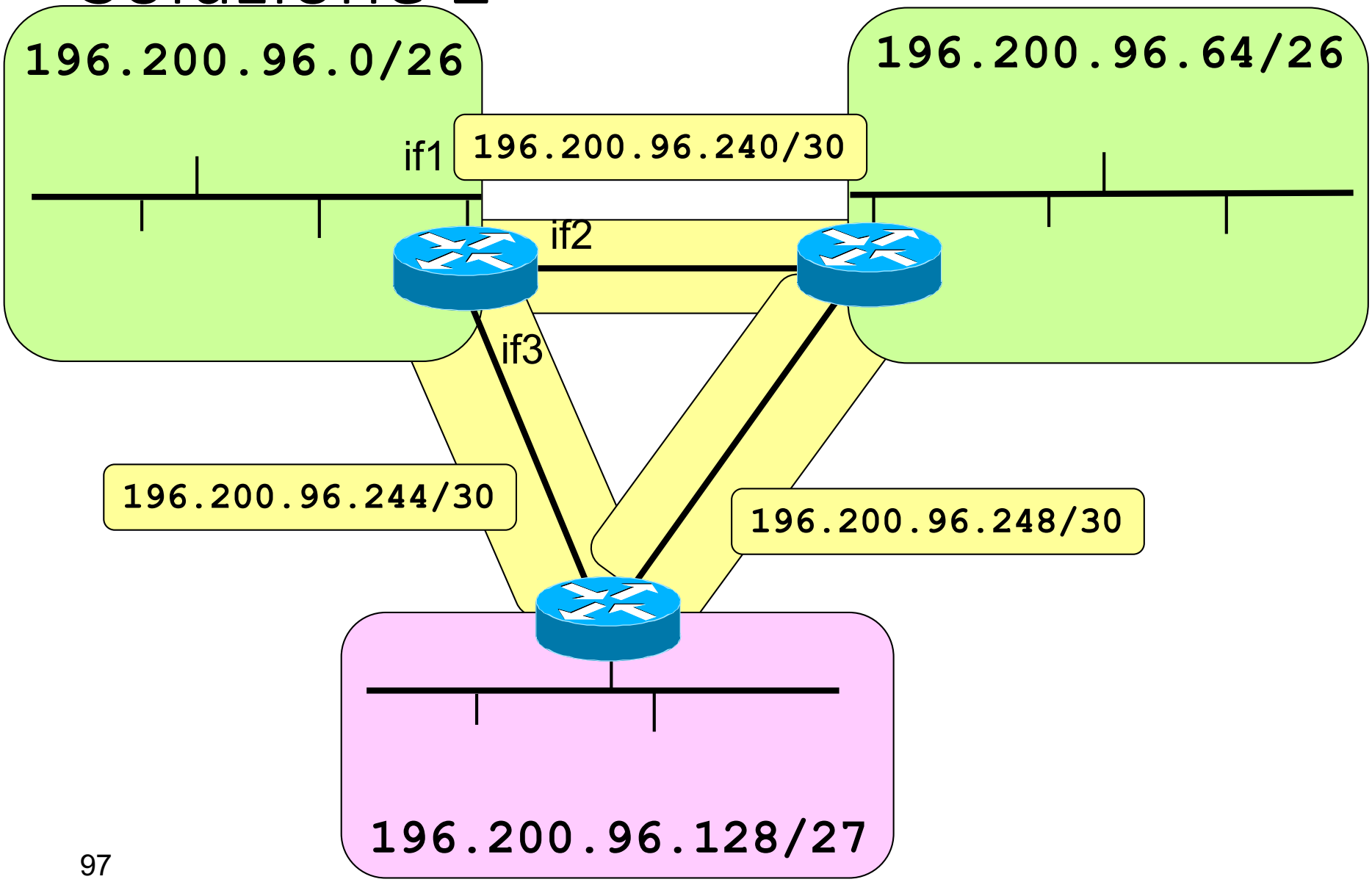
Scelta di netmask diverse

Ultimo byte netmask	# host	# subnets
00000000	254	1
10000000	126	2
11000000	62	4
11100000	30	8
11110000	14	16
11111000	6	32
11111100	2	64

Soluzione 2

Subnet	# host	Indirizzi	Broadcast
196.200.96.0/26	62	1 – 62	63
196.200.96.64/26	62	65 – 126	127
196.200.96.128/27	30	129 – 158	159
196.200.96.160/27	30	161 – 190	191
196.200.96.192/27	30	193 – 222	223
196.200.96.224/28	14	225 – 238	239
196.200.96.240/30	2	241 – 242	243
196.200.96.244/30	2	245 – 246	247
196.200.96.248/30	2	249 – 250	251
196.200.96.252/30	2	253 – 254	255

Soluzione 2


196.200.96.0/26
196.200.96.64/26
if1
196.200.96.240/30
if2
if3
196.200.96.244/30
196.200.96.248/30
196.200.96.128/27

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Il protocollo ICMP

Il protocollo IP…

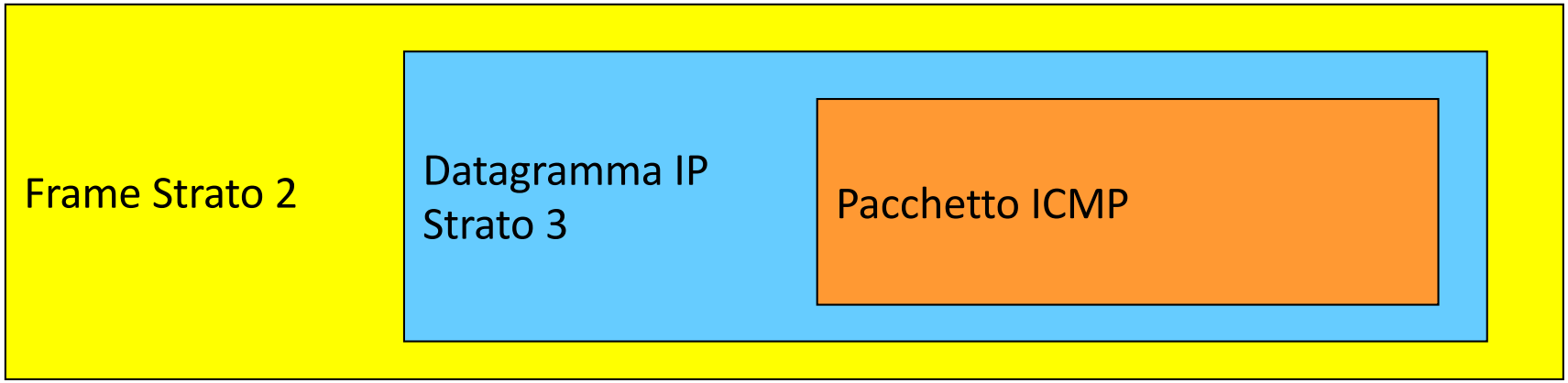
- offre un servizio di tipo best effort
  - non garantisce la corretta consegna dei datagrammi
  - se necessario si affida a protocolli affidabili di livello superiore (TCP)
- è comunque necessario un protocollo di controllo
  - gestione di situazioni anomale
  - notifica di errori o di irraggiungibilità della destinazione
  - scambio di informazioni sulla rete

→ **ICMP (Internet Control Message Protocol)**

- ICMP segnala solamente errori e malfunzionamenti, ma non esegue alcuna correzione
- ICMP **non rende affidabile** IP

ICMP

- **Internet Control Message Protocol** (RFC 792) svolge funzioni di controllo per IP
  - IP usa ICMP per la gestione di situazioni anomale, per cui ICMP offre un servizio ad IP
  - i pacchetti ICMP sono incapsulati in datagrammi IP, per cui ICMP è anche utente IP



Pacchetto ICMP

IP header	20 - 60 byte
Message Type	1 byte
Message Code	1 byte
Checksum	2 byte
Additional Fields (optional)	variabile
Data	variabile

- **Type** definisce il tipo di messaggio ICMP
  - messaggi di errore
  - messaggi di richiesta di informazioni
- **Code** descrive il tipo di errore e ulteriori dettagli
- **Checksum** controlla i bit errati nel messaggio ICMP
- **Add. Fields** dipendono dal tipo di messaggio ICMP
- **Data** intestazione e parte dei dati del datagramma che ha generato l'errore

Tipi di errori

- **Destination Unreachable** (Type = 3)
  - Generato da un gateway quando la sottorete o l'host non sono raggiungibili
  - Generato da un host quando si presenta un errore sull'indirizzo dell'entità di livello superiore a cui trasferire il datagramma
- Codici errore di Destination Unreachable
  - 0 = sottorete non raggiungibile
  - 1 = host non raggiungibile
  - 2 = protocollo non disponibile
  - 3 = porta non disponibile
  - 4 = frammentazione necessaria ma bit don't fragment settato

Tipi di errori

- Time Exceeded (Type = 11)
  - generato da un router quando il Time-to-Live di un datagramma si azzera ed il datagramma viene distrutto (Code = 0)
  - generato da un host quando un timer si azzera in attesa dei frammenti per riassemblare un datagramma ricevuto in parte (Code = 1)
- Source Quench (Type = 4)
  - i datagrammi arrivano troppo velocemente rispetto alla capacità di essere processati: l'host sorgente deve ridurre la velocità di trasmissione (obsoleto)
- Redirect (Type = 5)
  - generato da un router per indicare all'host sorgente un'altra strada più conveniente per raggiungere l'host destinazione

Informazioni

- Echo (Type = 8)
- Echo Reply (Type = 0)
  - l'host sorgente invia la richiesta ad un altro host o ad un gateway
  - la destinazione deve rispondere immediatamente
  - metodo usato per determinare lo stato di una rete e dei suoi host, la loro raggiungibilità e il tempo di transito nella rete
- Additional Fields:
  - Identifier: identifica l'insieme degli echo appartenenti allo stesso test
  - Sequence Number: identifica ciascun echo nell'insieme
  - Optional Data: usato per inserire eventuali dati di verifica

Informazioni

- Timestamp Request (Type = 13)
- Timestamp Reply (Type = 14)
  - l'host sorgente invia all'host destinazione un Originate Timestamp che indica l'istante in cui la richiesta è partita
  - l'host destinazione risponde inviando un
    - Receive Timestamp che indica l'istante in cui la richiesta è stata ricevuta
    - Transmit Timestamp che indica l'istante in cui la risposta è stata inviata
  - serve per valutare il tempo di transito nella rete, al netto del tempo di processamento = $T_{Transmit} - T_{Receive}$

Informazioni

- Address Mask Request (Type = 17)
- Address Mask Reply (Type = 18)
  inviato dall'host sorgente all'indirizzo di broadcast (255.255.255.255) per ottenere la subnet mask da usare dopo aver ottenuto il proprio indirizzo IP tramite RARP o BOOTP

- Router Solicitation (Type = 10)
- Router Advertisement (Type = 9)
  utilizzato per localizzare i router connessi alla rete

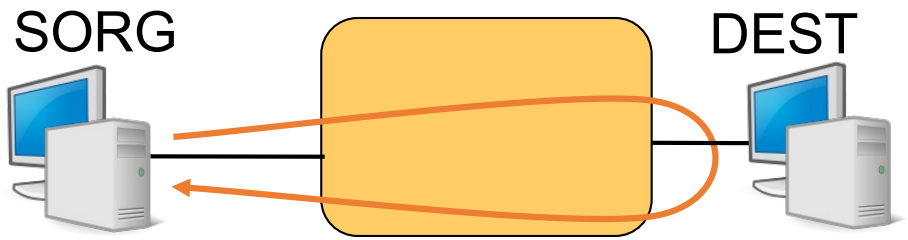
ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Applicazioni di ICMP

Comando PING

`ping DEST`

Permette di controllare se l'host DEST è raggiungibile o meno da SORG



- SORG invia a DEST un pacchetto **ICMP** di tipo **"echo"**
- Se l'host DEST è raggiungibile da SORG, DEST risponde inviando indietro un pacchetto ICMP di tipo **"echo reply"**

Opzioni

- **`-n N`** permette di specificare quanti pacchetti inviare (un pacchetto al secondo)
- **`-l M`** specifica la dimensione in byte di ciascun pacchetto
- **`-t`** esegue **`ping`** finché interrotto con **`Ctrl-C`**
- **`-a`** traduce l'indirizzo IP in nome DNS
- **`-f`** setta il bit *don't fragment* a 1
- **`-i T`** setta *time-to-live* = **`T`**
- **`-w` T_{out}** specifica un timeout in millisecondi

- Per maggiori informazioni consultare l'help: **`ping /?`**

Comando PING – Output

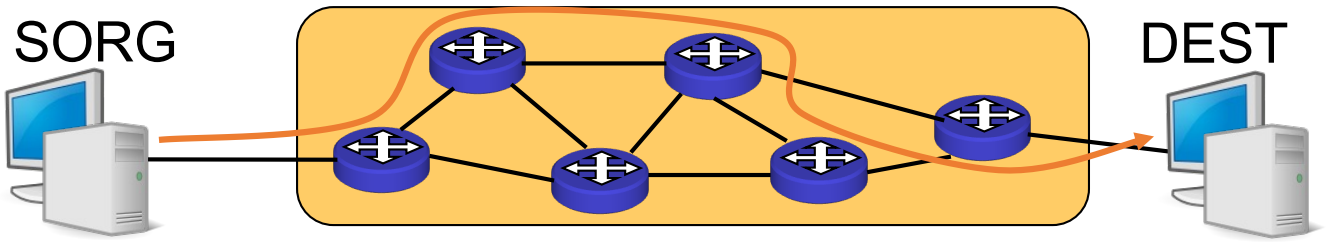
L'output mostra

- la dimensione del pacchetto "echo reply"
- l'indirizzo IP di DEST
- il numero di sequenza della risposta (solo UNIX-LINUX)
- il "time-to-live" (TTL)
- il "round-trip time" (RTT)
- alcuni risultati statistici: N° pacchetti persi, MIN, MAX e media del RTT

Comando TRACEROUTE

`tracert DEST`

Permette di conoscere il percorso seguito dai pacchetti inviati da SORG e diretti verso DEST



- SORG invia a DEST una serie di pacchetti **ICMP** di tipo **ECHO** con un **TIME-TO-LIVE (TTL)** progressivo da **1** a **30** (per default)
- Ciascun nodo intermedio decrementa **TTL**
- Il nodo che rileva **TTL = 0** invia a SORG un pacchetto **ICMP** di tipo **TIME EXCEEDED**
- SORG costruisce una lista dei nodi attraversati fino a DEST
- L'output mostra il **TTL**, il nome **DNS** e l'indirizzo **IP** dei nodi intermedi ed il **ROUND-TRIP TIME (RTT)**

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Gestione della numerazione

Dispositivi di rete

- DHCP
  - Permette ad un Host di ottenere una configurazione IP
- Packet Filter
  - Permette/blocca l'invio di pacchetti da/verso determinati indirizzi
  - Protegge la rete dal traffico "vagante"
- Application Layer Gateway (ALG) / Proxy
  - Controlla la comunicazione a livello applicativo
- Firewall
  - Combinazione dei dispositivi descritti sopra
  - Protegge le risorse interne da accessi esterni
- Network Address Translator (NAT)
  - Riduce la richiesta dello spazio di indirizzamento Internet
  - Nasconde gli indirizzi IP interni
  - Esegue un packet filtering per il traffico sconosciuto

DHCP – RFC 2131,2132

Dynamic Host Configuration Protocol

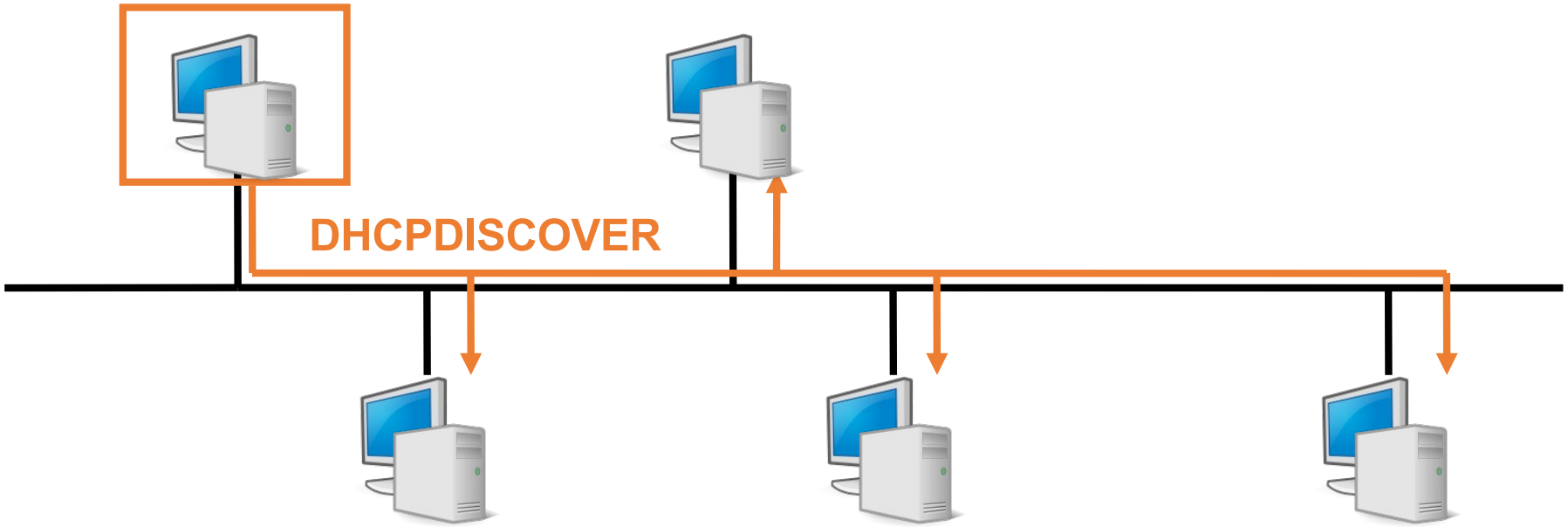
Configurazione **automatica** e **dinamica** di

- Indirizzo IP
- Netmask
- Broadcast
- Host name
- Default gateway
- Server DNS

Server su porta **67** UDP

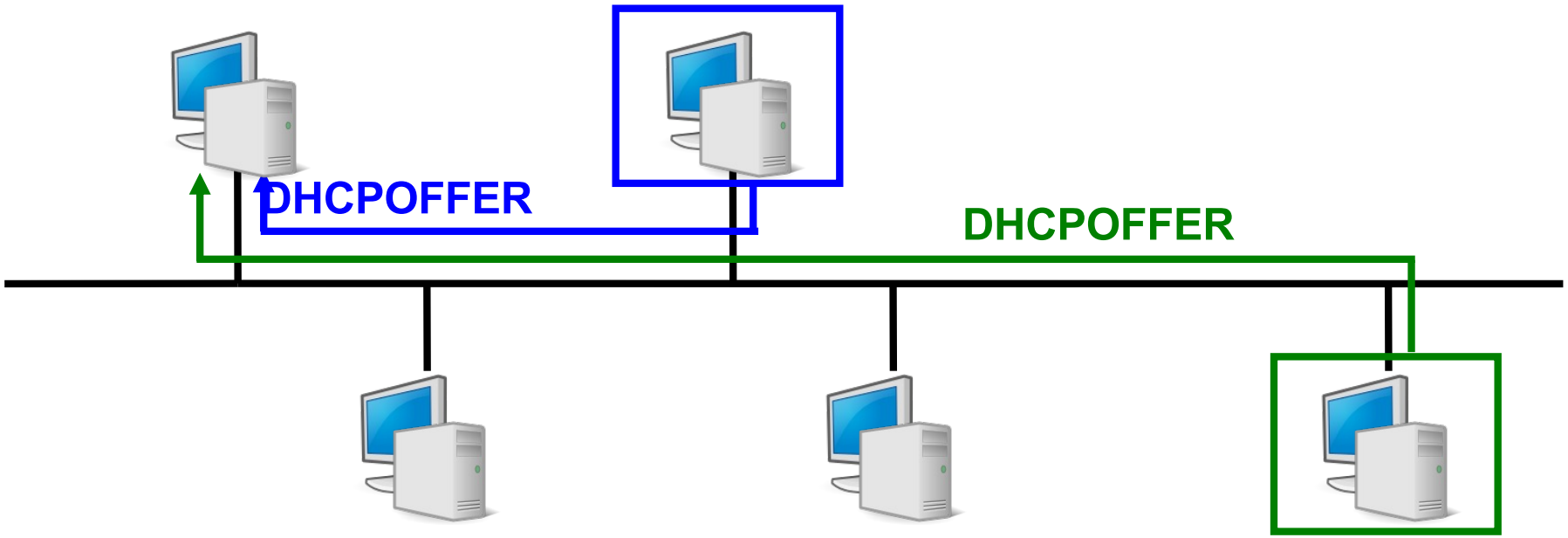
DHCP – 1

- Quando un host attiva l'interfaccia di rete, invia in modalità broadcast un messaggio **DHCPDISCOVER** in cerca di un server DHCP



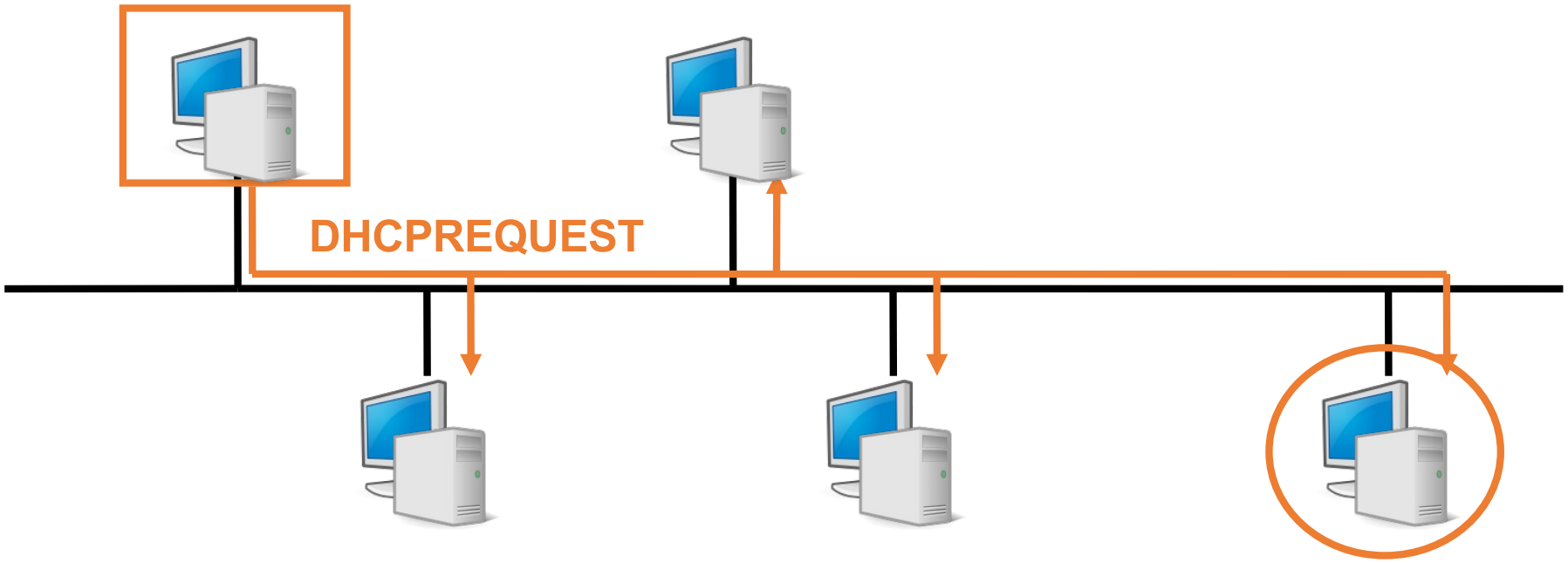
DHCP – 2

- Ciascun server DHCP presente risponde all'host con un messaggio **DHCPOFFER** con cui propone un indirizzo IP



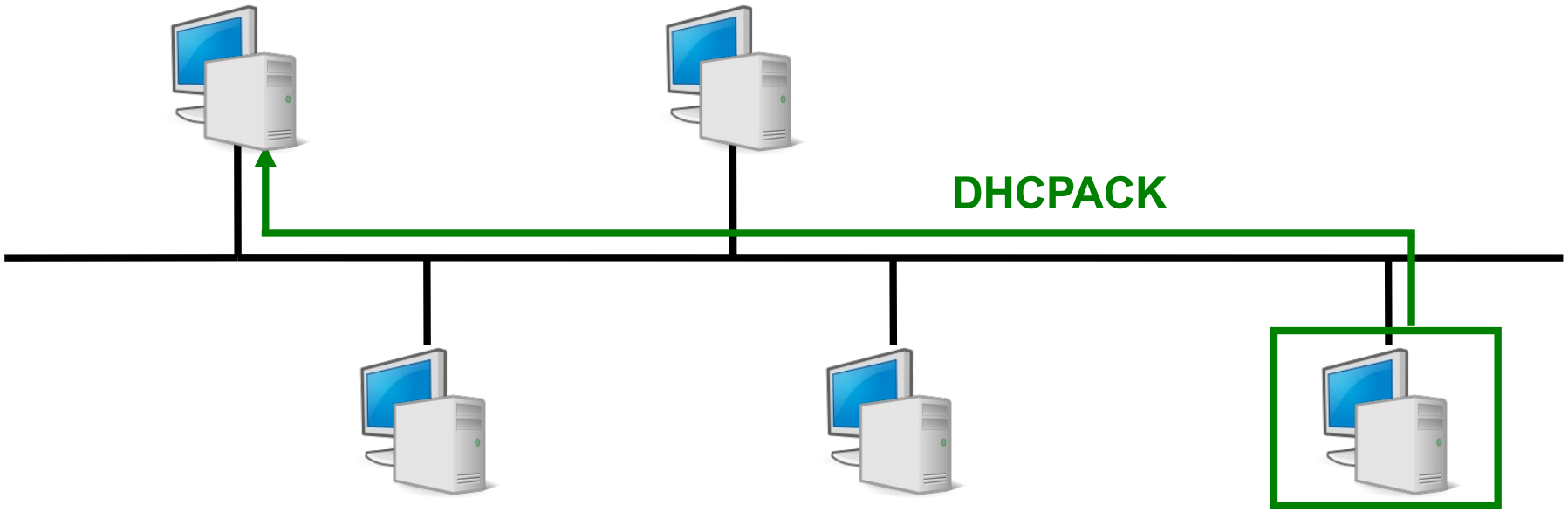
DHCP – 3

- L'host accetta una delle offerte proposte dai server e manda un messaggio **DHCPREQUEST** in cui richiede la configurazione, specificando il server



DHCP – 4

- Il server DHCP risponde all'host con un messaggio **DHCPACK** specificando i parametri di configurazione



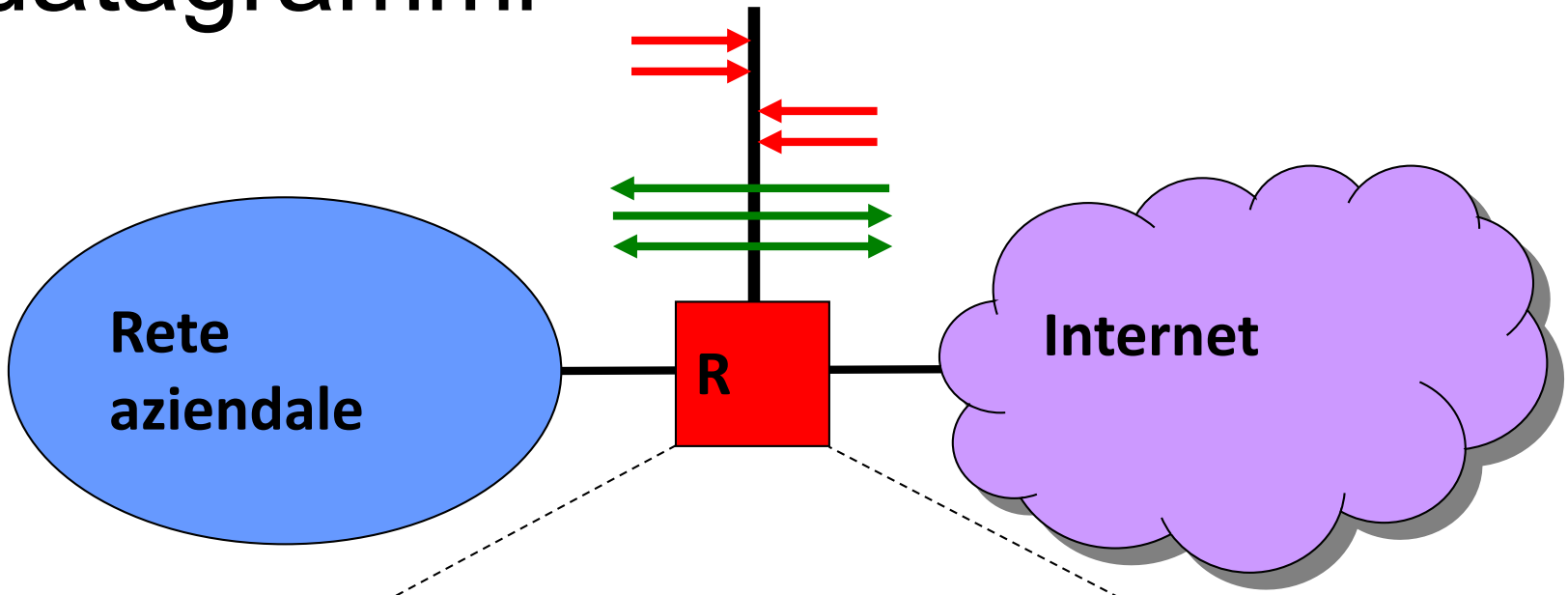
Ulteriori dettagli

- Un’analisi dettagliata del protocollo DHCP che include:
  - Esempi operativi
  - Catture di traffico
- Si può trovare su virtuale

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Packet Filter e Firewall

Metodologie di filtraggio dei datagrammi

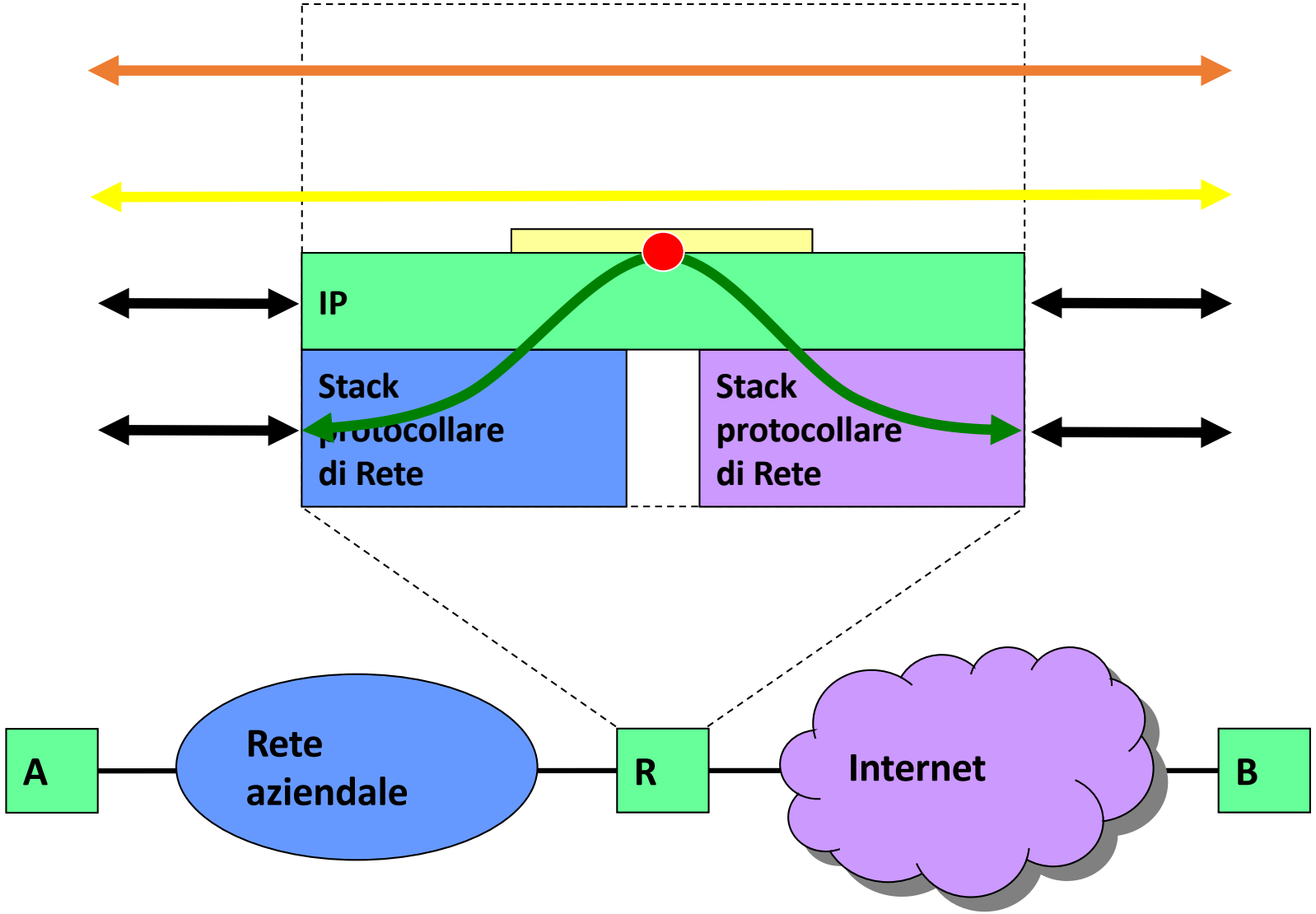


Impostazioni del Packet Filter

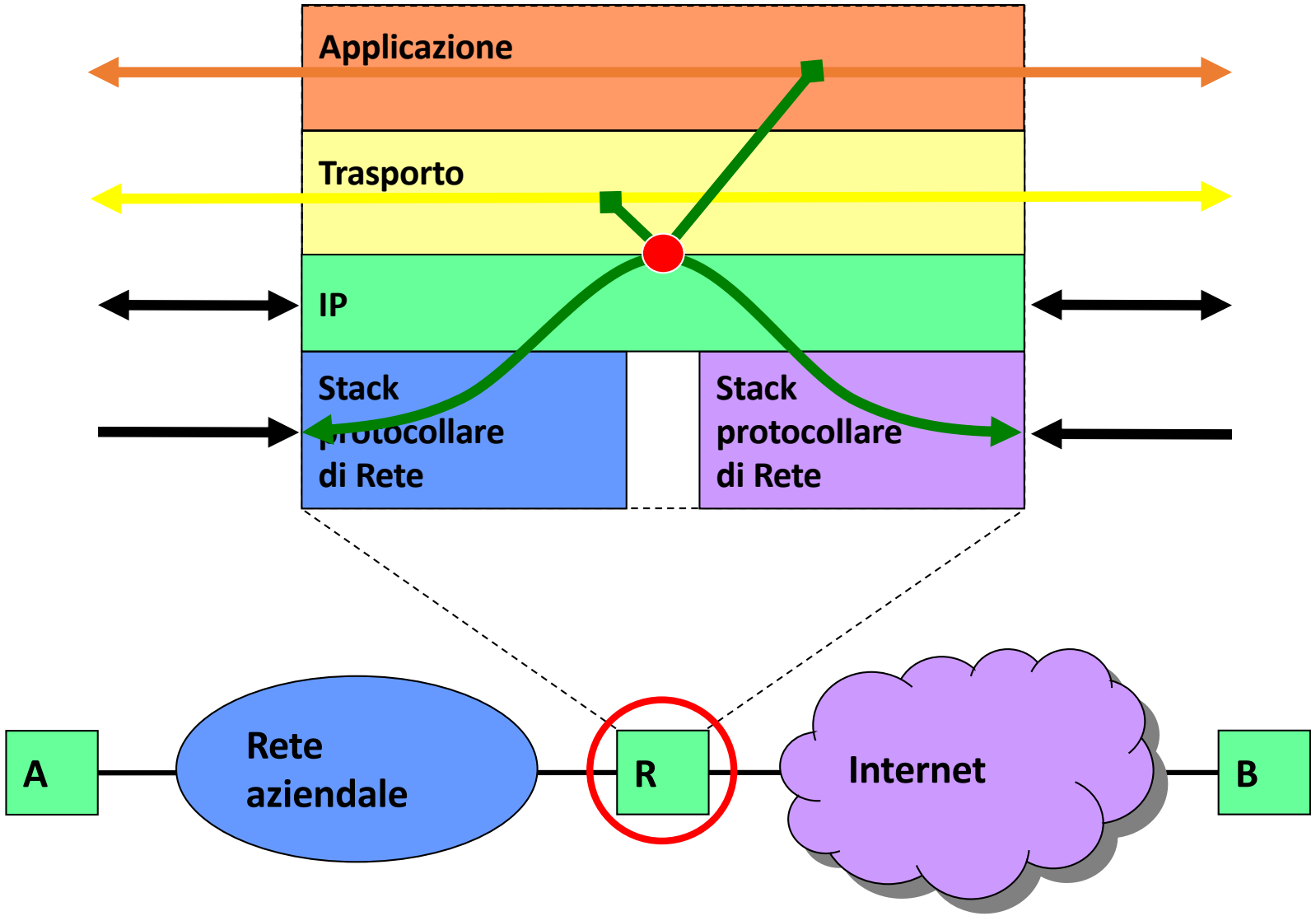
- **Indirizzo IP sorgente e destinazione**
- **Protocollo (TCP, UDP, ICMP)**
- **Porta sorgente e destinazione**
- **Direzione del traffico**

Può essere configurato dinamicamente

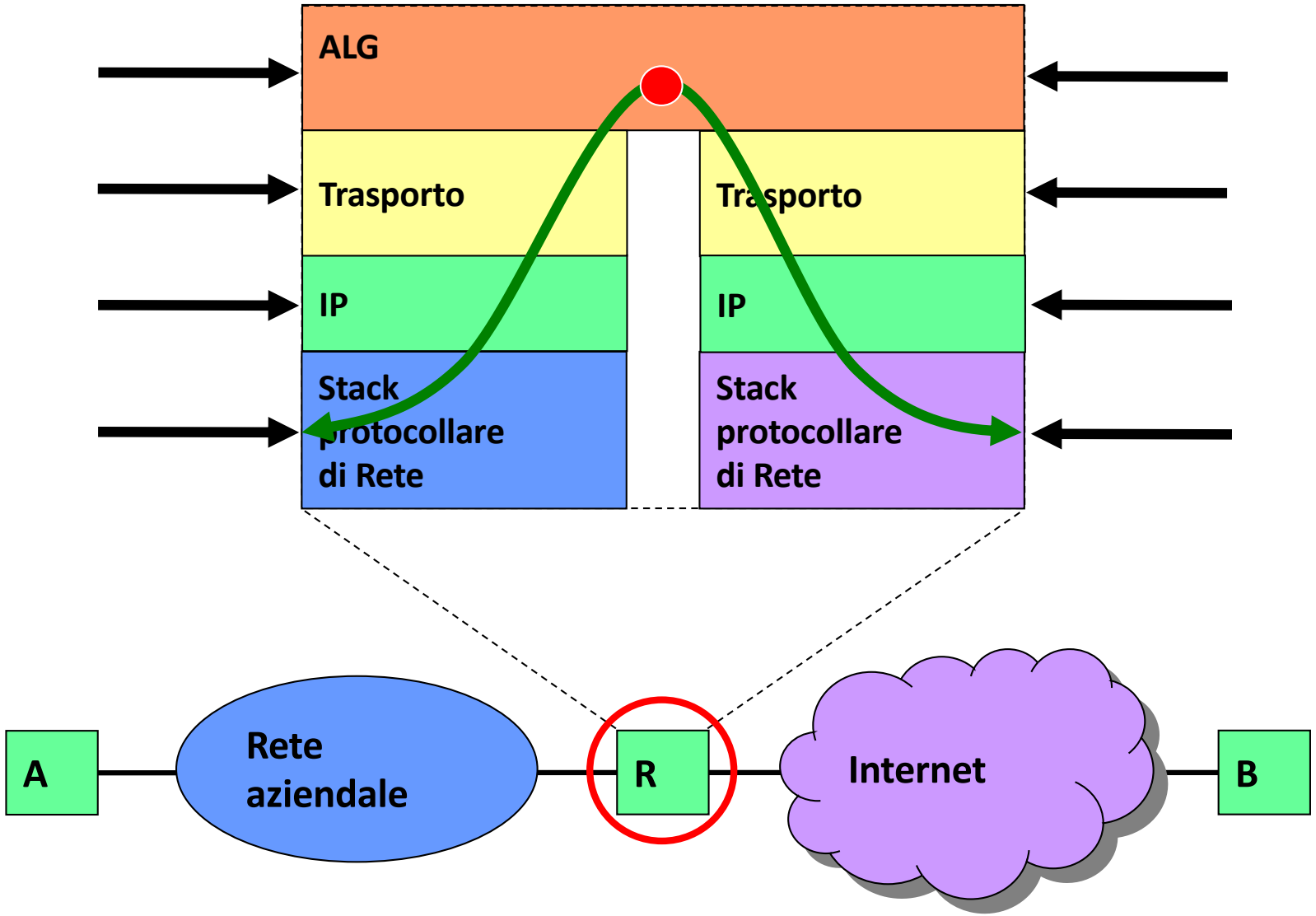
Instradamento selettivo: packet filter



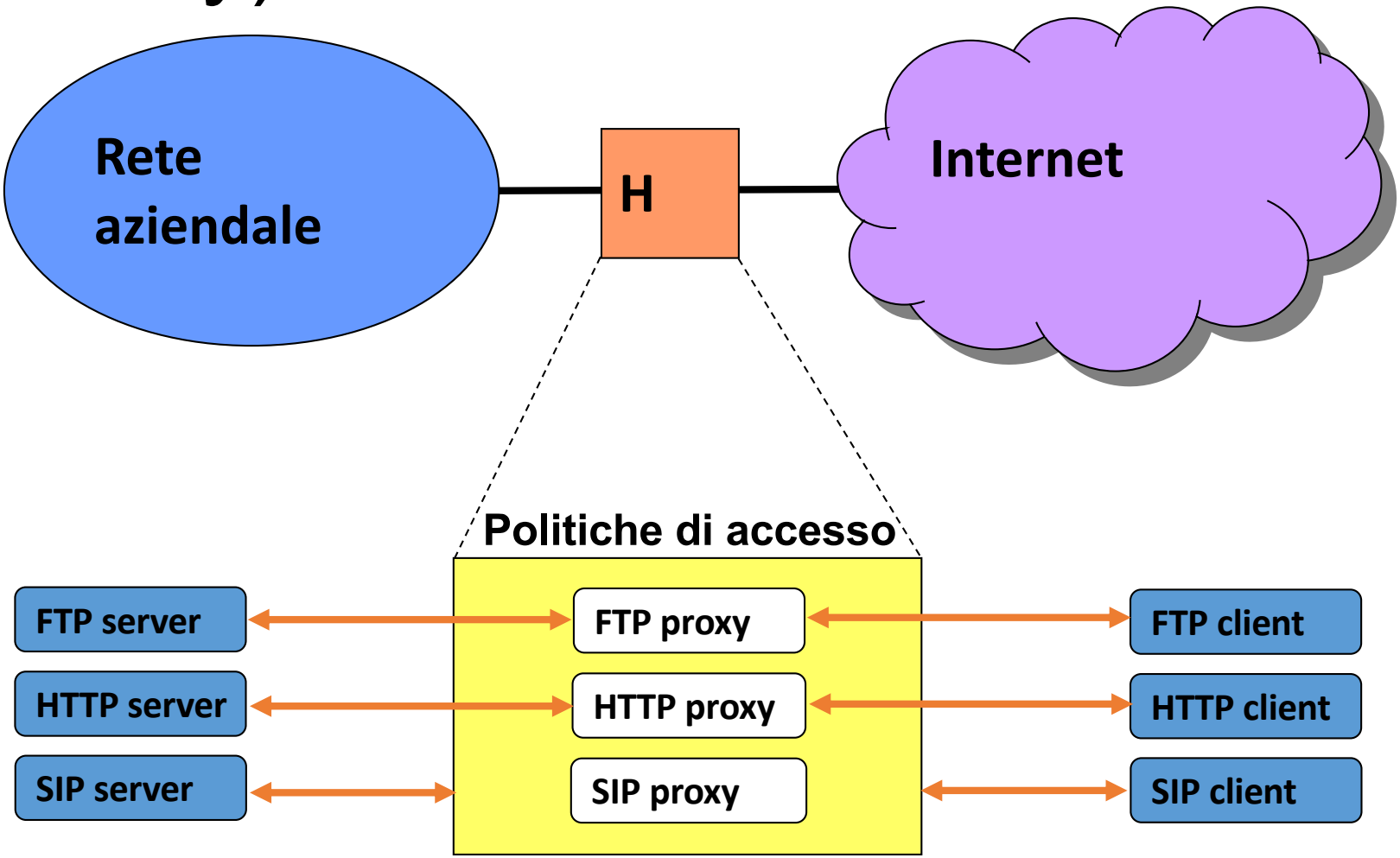
Stateful Packet Inspection



Application Layer Gateway (Proxy)



Application Layer Gateway (Proxy)



Firewall

- Packet Filter: filtra i pacchetti seguendo la politiche stabilite
  - Filtri: generalmente configurati staticamente
  - La maggioranza delle configurazioni non permettono pacchetti per porte "non-standard" (Internet Assigned Numbers Authority – IANA)

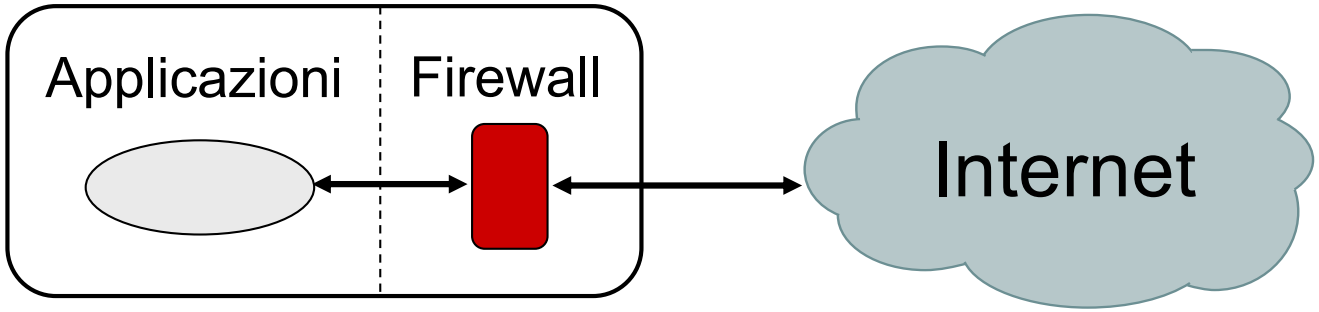
- Stateful Packet Inspection
  - Mantiene il contesto dei pacchetti sia nel trasporto che nello strato applicativo
  - Adatta dinamicamente le specifiche dei filtri

- Application Layer Gateway (trasparente o proxy esplicito)
  - Monitora le connessioni: analizza il contenuto dei protocolli applicativi
    - A scapito della sicurezza di comunicazione end-to-end
  - Adatta dinamicamente le specifiche dei filtri

- Per ogni strato (layer) dello stack possono essere applicate politiche (policies) differenti

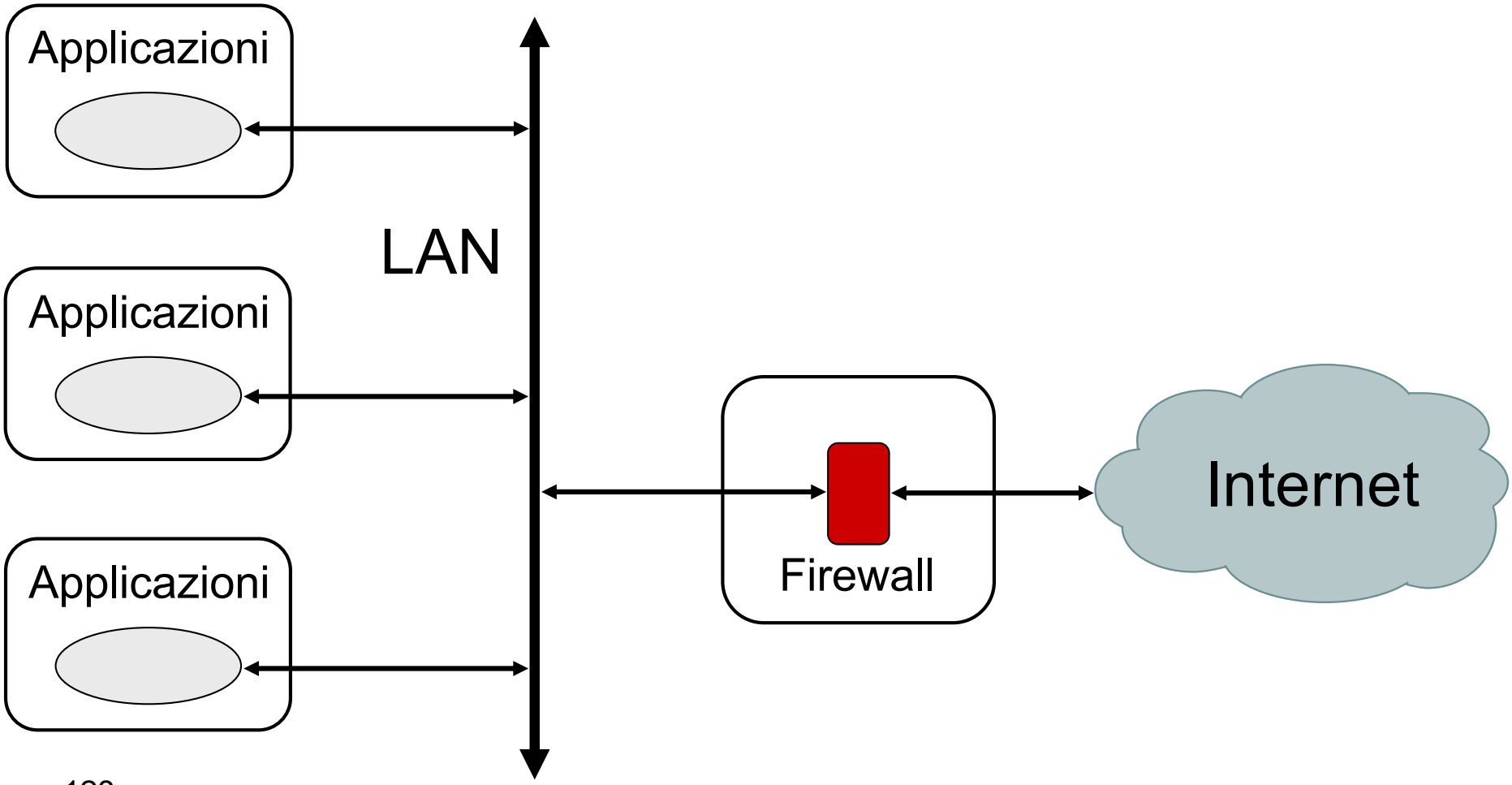
Protezione di host: firewall

- Un firewall è un filtro software/hardware che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete
- Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni
  - tipicamente usato in accessi domestici a larga banda (ADSL, FTTH)



Protezione di rete: firewall

- Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale



Protezione di rete: firewall

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
- Solo il traffico autorizzato deve attraversare il firewall
- Si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti
- Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host
- In fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete
  - **default deny**: tutti servizi non esplicitamente permessi sono negati
  - **default permit**: tutti i servizi non esplicitamente negati sono permessi

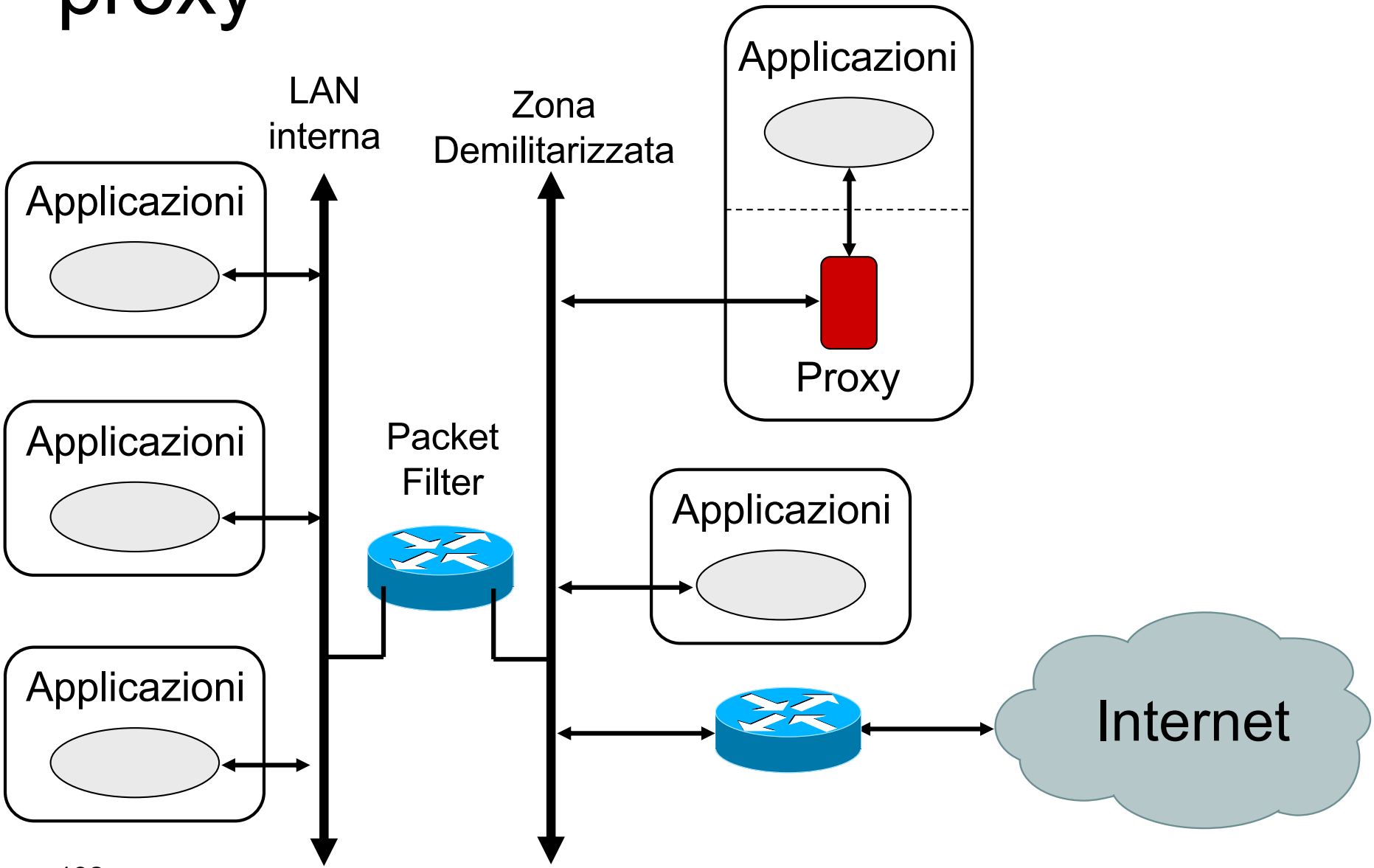
Livelli di implementazione

- Un firewall può essere implementato come
  - packet filter
  - proxy server
    - application gateway
    - circuit-level gateway
- **Packet filter**
  - si interpone un router fra la rete locale ed Internet
  - sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
  - il filtro scarta i datagrammi sulla base di
    - indirizzo IP sorgente o destinazione
    - tipo di servizio a cui il datagramma è destinato (porta TCP/UDP)
    - interfaccia di provenienza o destinazione

Livelli di implementazione

- **Proxy server**
  - nella rete protetta l'accesso ad Internet è consentito solo ad alcuni host
  - si interpone un server apposito detto proxy server per realizzare la comunicazione per tutti gli host
  - il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale
  - **application level**
    - viene impiegato un proxy server dedicato per ogni servizio che si vuole garantire
  - **circuit level gateway**
    - è un proxy server generico in grado di inoltrare le richieste relative a molti servizi

Configurazione di packet filter e proxy

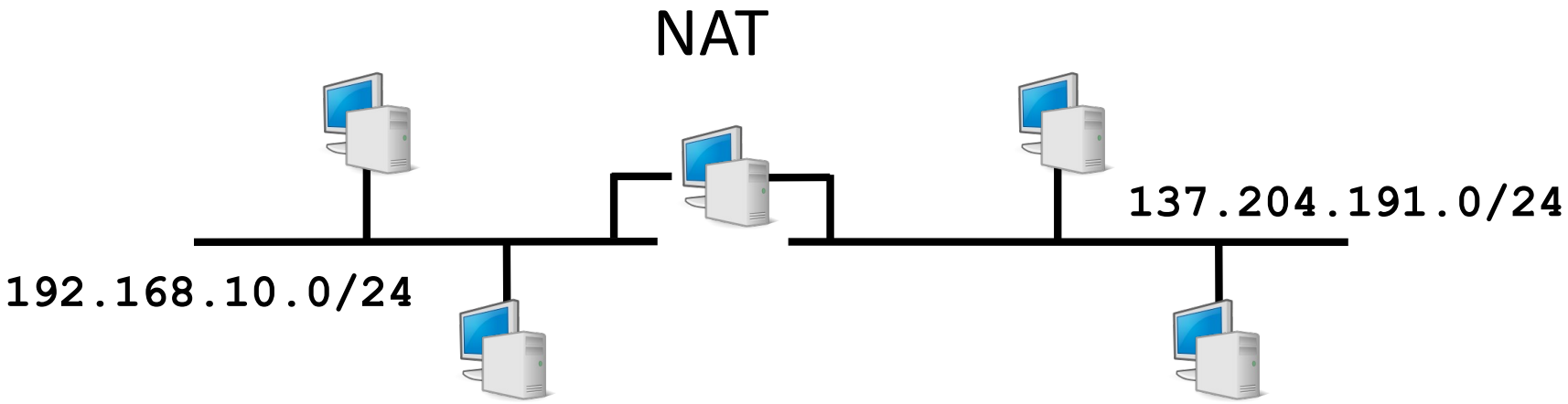


ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Network Address Translation

Network Address Translation (NAT)

- Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento)
  - Indirizzi e porte
- Definito nella RFC 3022 per permettere a reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway
- Utile per il risparmio di indirizzi IP pubblici e il riutilizzo di indirizzi IP privati



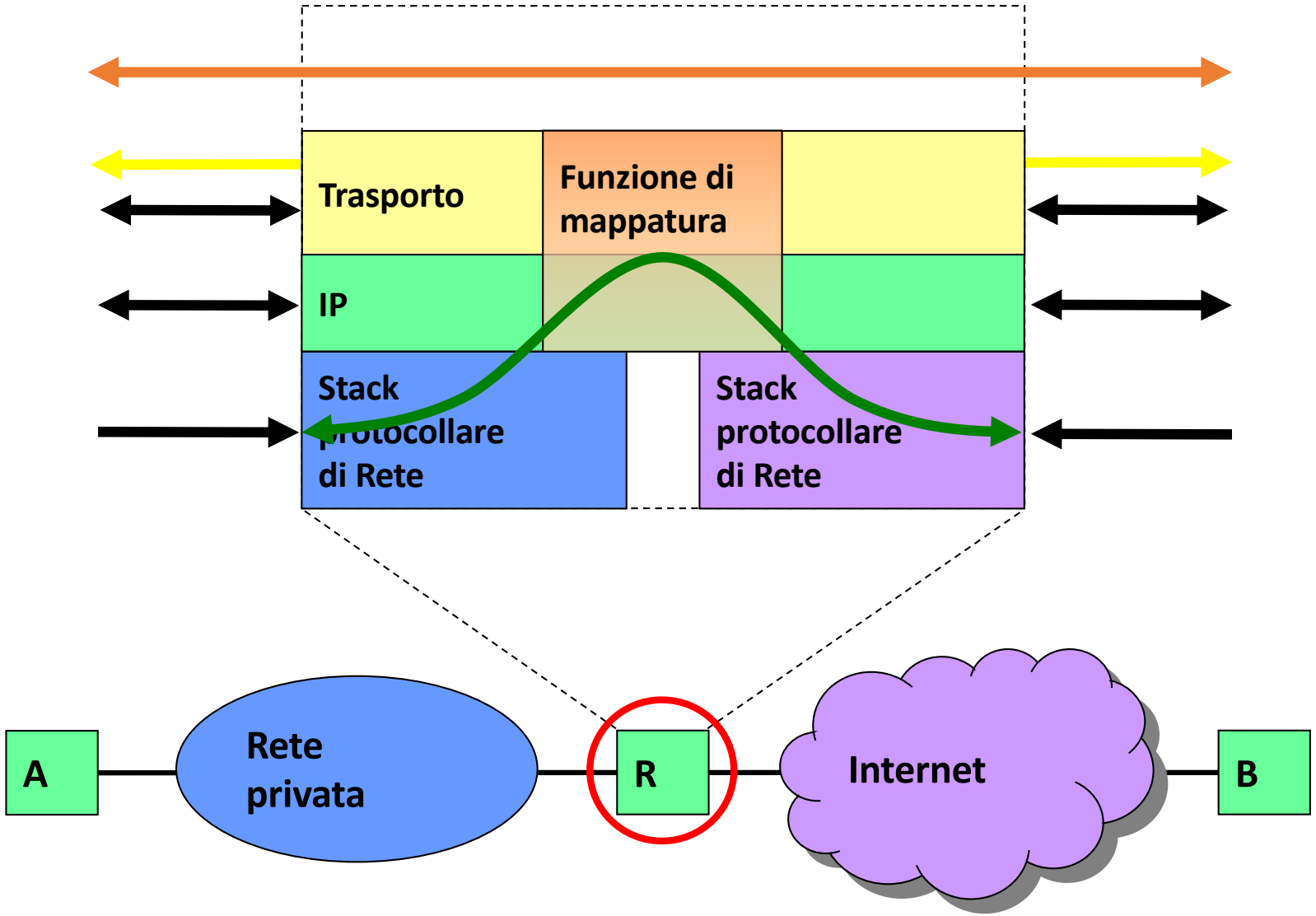
NAT: motivazioni

- Efficiente uso della spazio degli indirizzi
- Condividere uno o pochi indirizzi
- Uso di indirizzi privati nella LAN locale (10.x.x.x, 192.168.x.x, …)

- Security
  - Rendere gli host interni non accessibili dall'esterno
  - Nascondere gli indirizzi e la struttura della rete

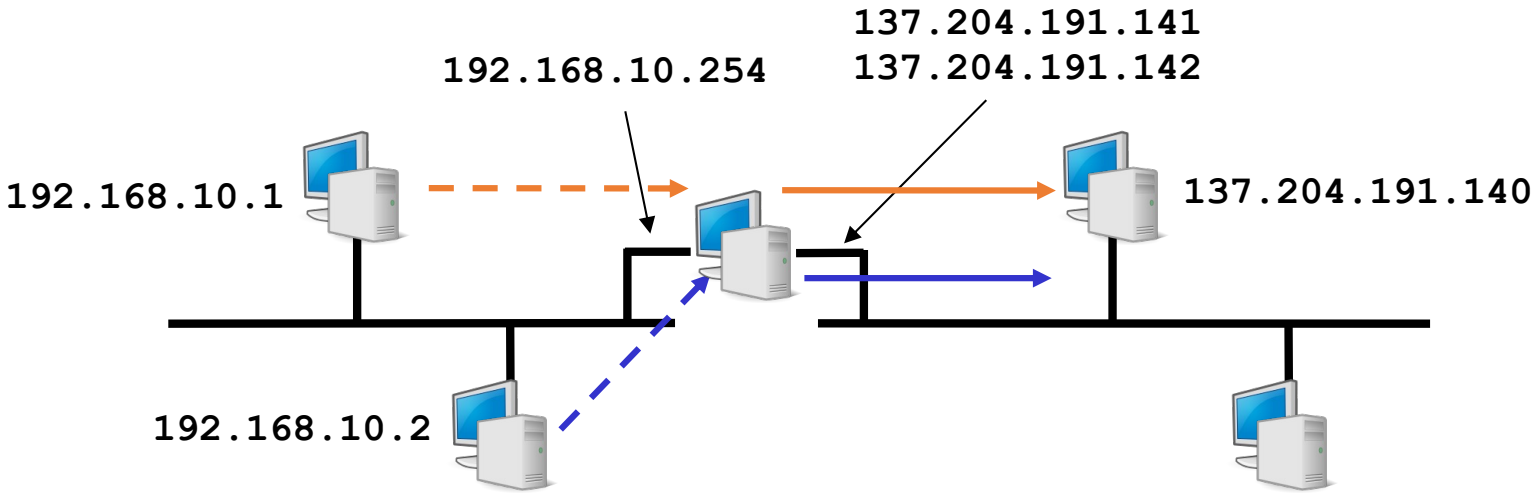
- Include un packet filter, stateful packet inspection configurati dinamicamente

Network (+Port) Address Translator (NAT)



Basic NAT – Conversione di indirizzo

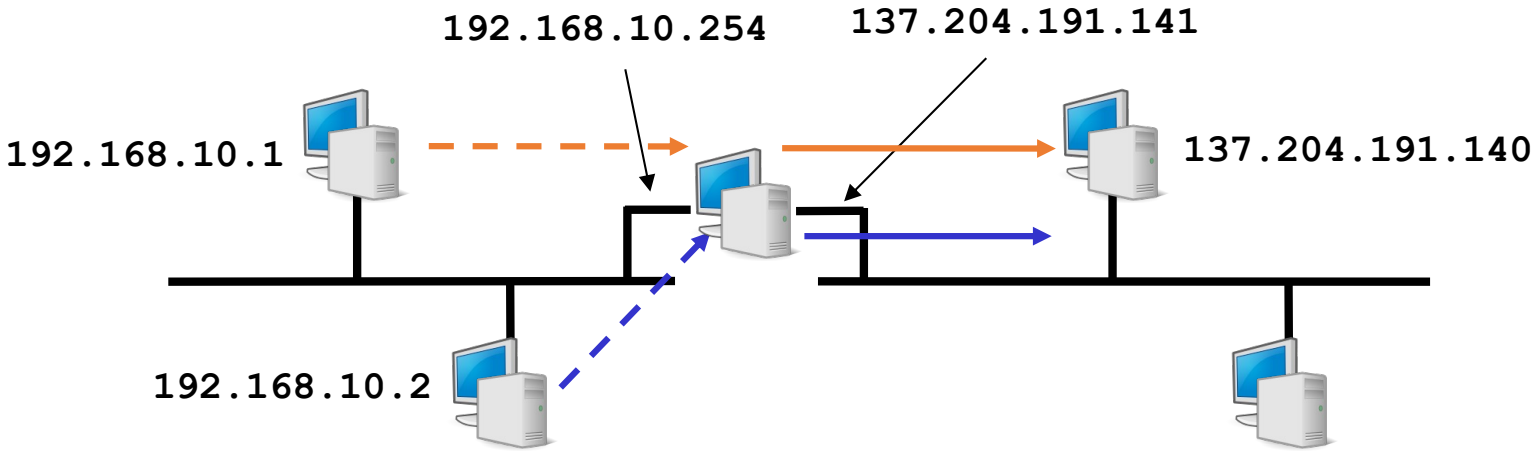
- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



192.168.10.1:3123	--->	137.204.191.140:80
137.204.191.141:3123	--->	137.204.191.140:80
192.168.10.2:5039	--->	137.204.191.140:22
137.204.191.142:5039	--->	137.204.191.140:22

Conversione di indirizzo e porta

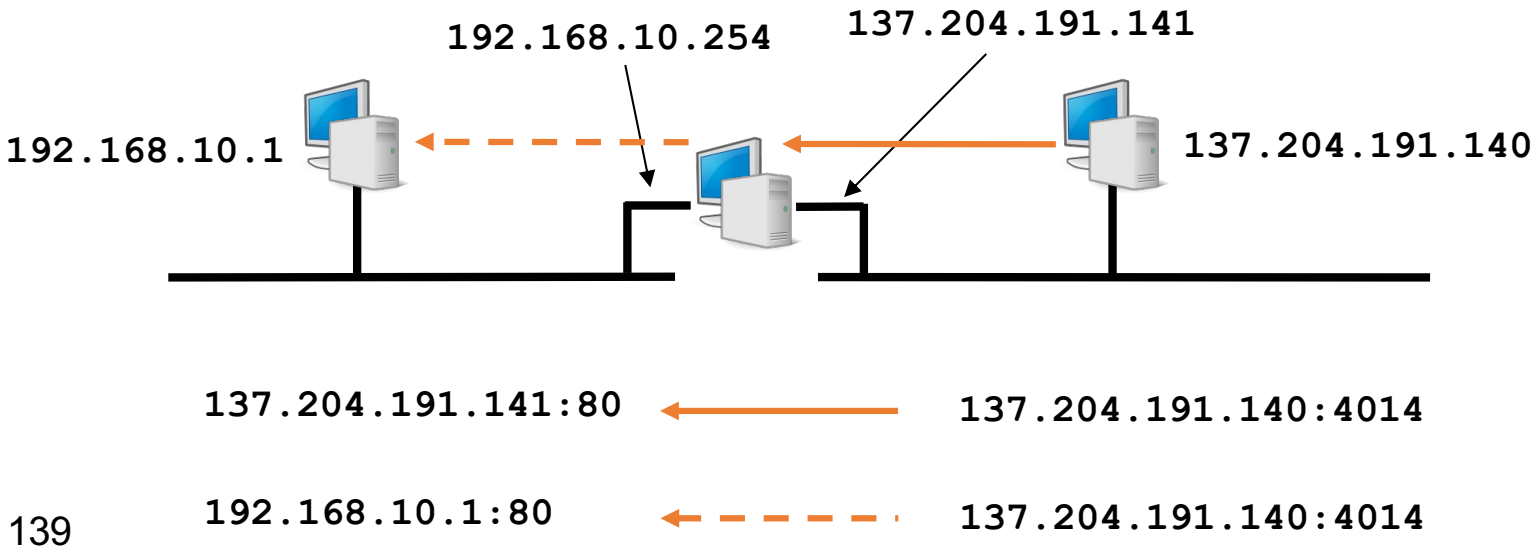
- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



192.168.10.1:3123	--->	137.204.191.140:80
137.204.191.141:3123	--->	137.204.191.140:80
192.168.10.2:3123	--->	137.204.191.140:22
137.204.191.141:4131	--->	137.204.191.140:22

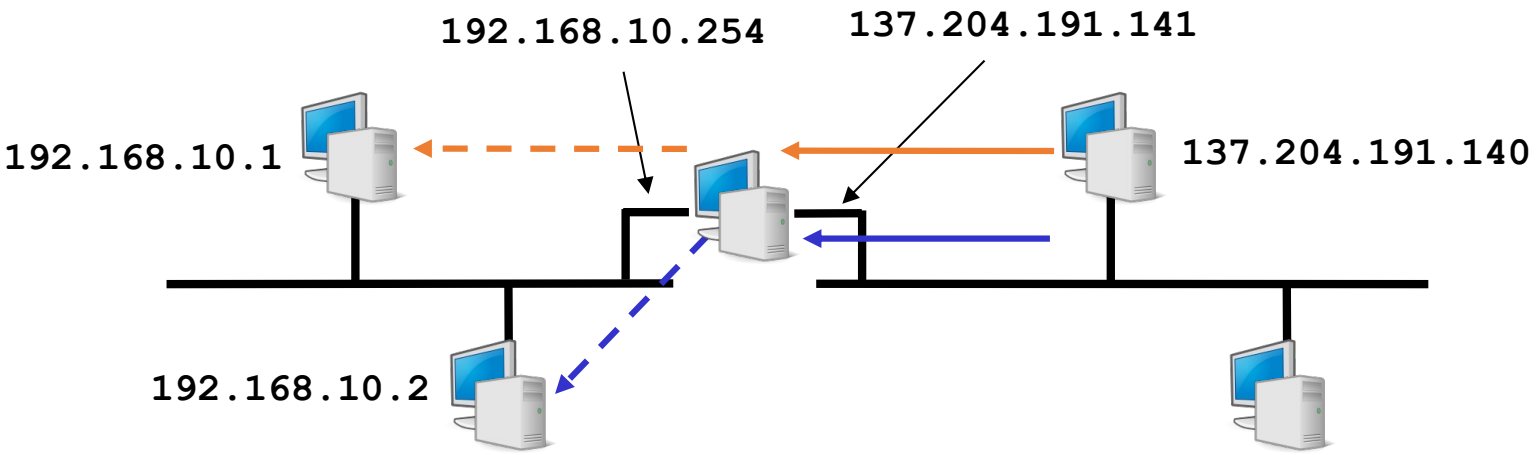
Direzione delle connessioni

- Tipicamente da rete privata verso rete pubblica
  - Il NAT si preoccupa di effettuare la conversione inversa quando arrivano le risposte
  - Registra le corrispondenze in corso in una tabella
- E' possibile contattare dalla rete pubblica un host sulla rete privata?
  - Dipende dal tipo di NAT e dalla relativa configurazione



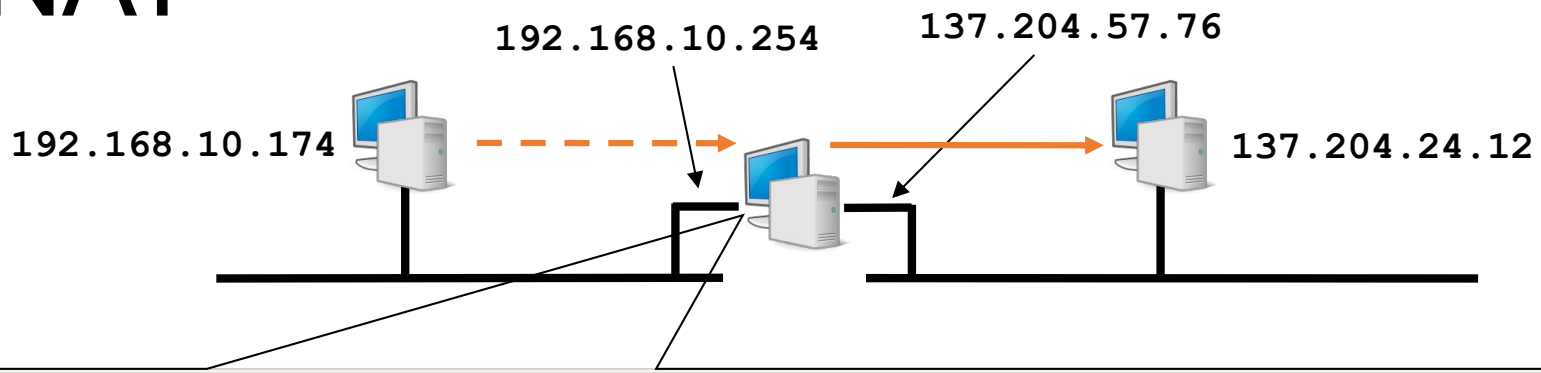
Port forwarding

- Il NAT permette l'ingresso di pacchetti destinati a porte specifiche effettuando la traduzione opportuna



137.204.191.141:80	←	137.204.191.140:4014
192.168.10.1:80	←	137.204.191.140:4014
137.204.191.141:8080	←	137.204.191.140:4015
192.168.10.2:8080	←	137.204.191.140:4015

Analisi di connessioni attraverso NAT

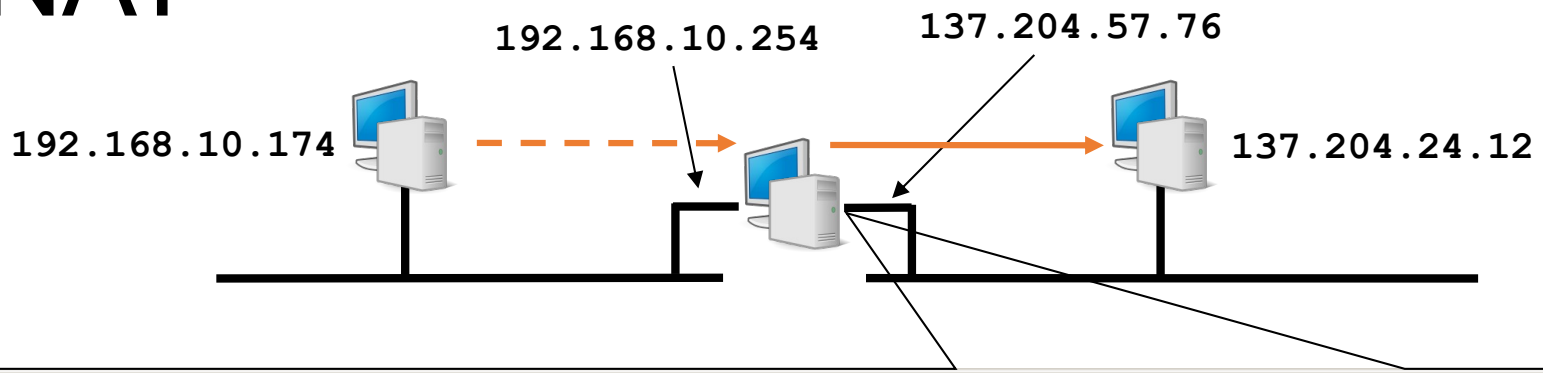


NAT-int.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.174	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034608	137.204.24.12	192.168.10.174	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1
3	0.896816	137.204.24.12	192.168.10.174	HTTP	HTTP/1.1 200 OK
4	0.896908	137.204.24.12	192.168.10.174	HTTP	Continuation
5	0.898068	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6
6	0.899848	137.204.24.12	192.168.10.174	HTTP	Continuation
7	0.899971	137.204.24.12	192.168.10.174	HTTP	Continuation
8	0.900095	137.204.24.12	192.168.10.174	HTTP	Continuation
9	0.900913	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6
10	0.901066	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6
11	0.902676	137.204.24.12	192.168.10.174	HTTP	Continuation
12	0.902798	137.204.24.12	192.168.10.174	HTTP	Continuation
13	0.902921	137.204.24.12	192.168.10.174	HTTP	Continuation
14	0.903045	137.204.24.12	192.168.10.174	HTTP	Continuation
15	0.903168	137.204.24.12	192.168.10.174	HTTP	Continuation
16	0.903846	192.168.10.174	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903848	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6
18	0.903850	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6
19	0.904022	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6
20	0.905643	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6

Analisi di connessioni attraverso NAT



NAT-ext.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	137.204.57.76	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034559	137.204.24.12	137.204.57.76	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1128
3	0.896736	137.204.24.12	137.204.57.76	HTTP	HTTP/1.1 200 OK
4	0.896859	137.204.24.12	137.204.57.76	HTTP	Continuation
5	0.898045	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6424
6	0.899803	137.204.24.12	137.204.57.76	HTTP	Continuation
7	0.899925	137.204.24.12	137.204.57.76	HTTP	Continuation
8	0.900050	137.204.24.12	137.204.57.76	HTTP	Continuation
9	0.900889	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6424
10	0.901042	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6424
11	0.902630	137.204.24.12	137.204.57.76	HTTP	Continuation
12	0.902752	137.204.24.12	137.204.57.76	HTTP	Continuation
13	0.902875	137.204.24.12	137.204.57.76	HTTP	Continuation
14	0.903000	137.204.24.12	137.204.57.76	HTTP	Continuation
15	0.903122	137.204.24.12	137.204.57.76	HTTP	Continuation
16	0.903836	137.204.57.76	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903847	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6424
18	0.903855	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6424
19	0.903999	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6424
20	0.905619	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6424

NAT e applicazioni di rete

- Il NAT è trasparente per l'applicazione
  - Modifica l'intestazione IP e TCP/UDP ma non il payload
- Questo è un problema in alcuni casi specifici
  - Applicazioni non sono trasparenti al NAT
    - Contengono indirizzi IP e numeri di porta nel payload
    - FTP utilizza due connessioni parallele
      - connessione per l'interazione con il server tramite linea di comando (porta TCP 21)
      - connessione per il trasferimento dei dati da e verso il server
      - i parametri della seconda sono specificati nei dati trasmessi dalla prima
  - Il tipo di traffico permesso dipende dal tipo di NAT
    - Full Cone NAT
    - (Port) Restricted Cone NAT
    - Symmetric NAT