



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

di rete

Application

Transport

Garantisce la trasmissione affidabile dei dati da un'applicazione all'altra.

Network

È responsabile dell'instradamento (routing) dei pacchetti attraverso reti diverse.

Data Link

Gestisce la trasmissione dei dati tra due nodi direttamente connessi.

Physical

Si occupa del collegamento fisico tra i dispositivi. Include cavi, fibre ottiche, onde radio, connettori e tutto ciò che permette il trasferimento di segnali elettrici o ottici.

Applicazioni

e-mail,ftp,telnet,www...

Connessione orientata, garantisce che i dati arrivino completi e in ordine.

TCP

Connessione non orientata, più veloce ma meno affidabile.

UDP

Messaggi di controllo e segnalazione di errori.

ICMP

IP

Instradamento dei pacchetti.

Traduzione degli indirizzi IP in indirizzi MAC.

ARP

Non specificato (ad es.
IEEE 802-Ethernet-X25-Aloha ecc.)

Non specificato
Collegamento fisico

Strati superiori

Strato 4

Strato 3

Strato 2

Strato 1



Internet Protocol (IP) - RFC 791

- Progettato per funzionare a **commutazione di pacchetto** in modalità **connectionless**
(ovvero non richiede una connessione stabile tra il mittente e il destinatario. Ogni pacchetto è indipendente e può seguire percorsi diversi.)
 - Si prende carico della trasmissione di **datagrammi** da sorgente a destinazione, attraverso reti eterogenee → cioè reti con tecnologie diverse, garantendo l'interoperabilità.
 - L'IP Identifica **host** e **router** tramite indirizzi di **lunghezza fissa**, raggruppandoli in **reti IP** → Gli indirizzi IP sono raggruppati in reti IP, permettendo una gerarchia per l'instradamento e la suddivisione in sottoreti.
 - **Frammenta** e **riassembla** i datagrammi quando necessario → Quando un datagramma è troppo grande per essere trasmesso in una rete specifica (ad esempio, a causa della dimensione massima di un pacchetto accettata dalla rete), IP frammenta il datagramma in pezzi più piccoli. I frammenti vengono poi riassemblati dal destinatario per ricostruire il messaggio originale.
 - 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.
- L'IP offre un servizio best effort, il che significa che:
Non garantisce la consegna dei pacchetti.
Non garantisce l'ordine di arrivo dei pacchetti.
Non rileva né corregge gli errori durante la trasmissione.
Non implementa meccanismi per:
Migliorare l'affidabilità della trasmissione end-to-end (es. ritrasmissioni in caso di errore).
Eseguire il controllo di flusso o mantenere l'ordine dei pacchetti.
Queste funzioni sono demandate a protocolli di livello superiore, come TCP.



Struttura degli indirizzi IP

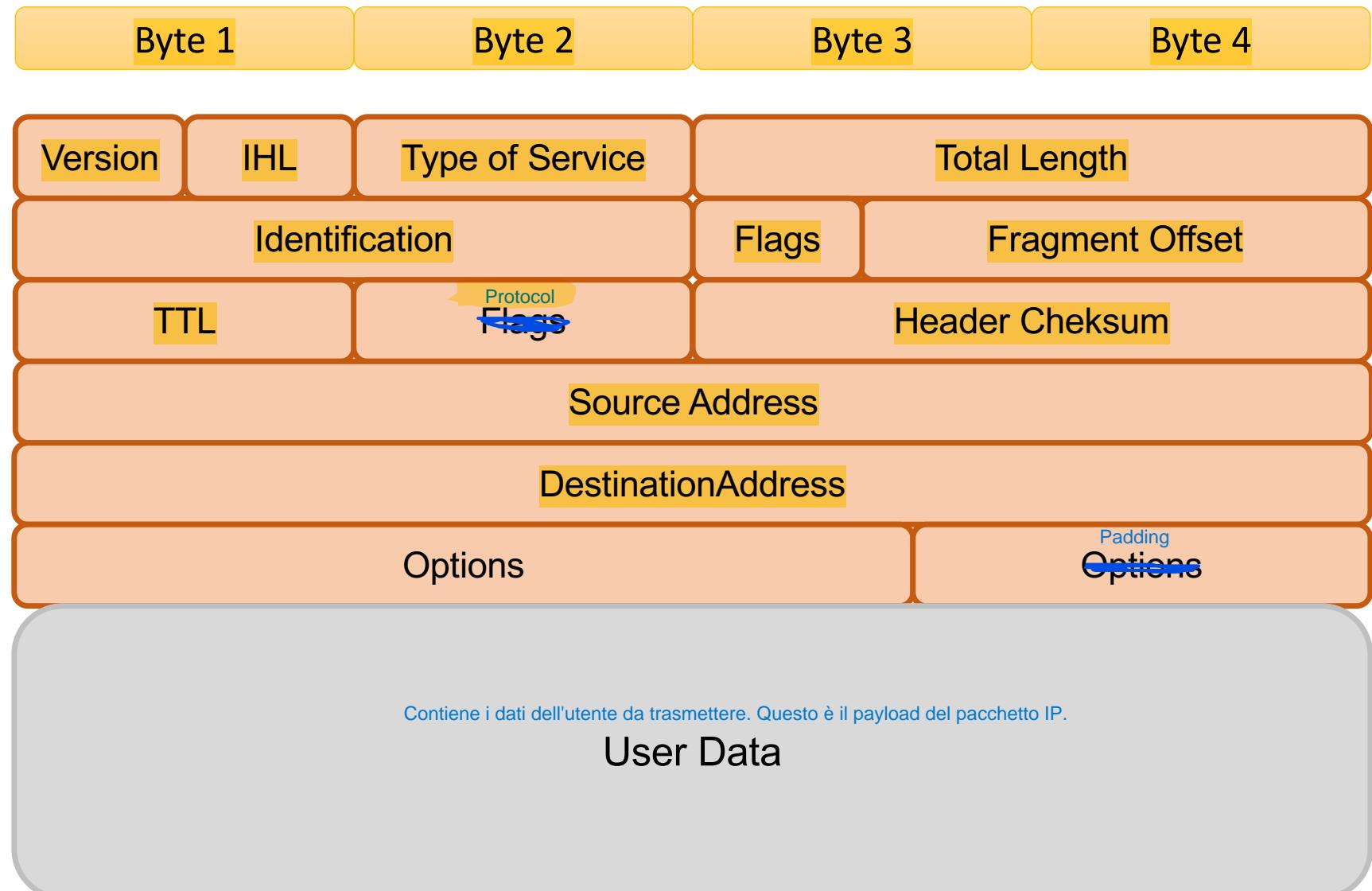
- Indirizzi di lunghezza fissa pari a **32 bit**
- Scritti convenzionalmente come sequenza di 4 numeri decimali, con valori da **0** a **255**, separati da punto (rappresentazione **dotted decimal**)

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** (Internet Assigned Numbers Authority)



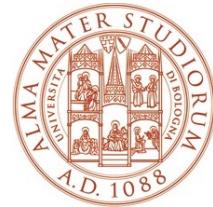
Formato pacchetto





Significato delle PCI

- **Version** : indica il formato dell' intestazione, attualmente la versione in uso è la 4
Indica la versione del protocollo IP in uso.
- **IHL** : lunghezza dell' intestazione, espressa in parole di 32 bit; lunghezza minima = 5
(5 parole da 32 bit sono 20 byte)
- **Type of service** : indicazione sul tipo di servizio richiesto, usato anche come sorta di priorità
Determina la priorità del pacchetto e il trattamento preferenziale che dovrebbe ricevere (es. velocità, affidabilità, costo).
→ Lunghezza totale del pacchetto IP, inclusa l'intestazione e i dati, espressa in byte.
- **Total length** : lunghezza totale del datagramma, misurata in bytes; lunghezza massima = 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 Identifica univocamente il datagramma, utile nel caso in cui sia stato frammentato.
 - Indica a quale datagramma appartenga un frammento (fragment)

Campi di controllo per la frammentazione



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 Indica la posizione del frammento rispetto all'inizio del datagramma originale. Misurato in blocchi di 8 byte (64 bit).

La frammentazione è il processo tramite cui un datagramma IP viene suddiviso in frammenti più piccoli per poter essere trasmesso su collegamenti con una dimensione massima del pacchetto (MTU, Maximum Transmission Unit) inferiore alla dimensione del datagramma originale.



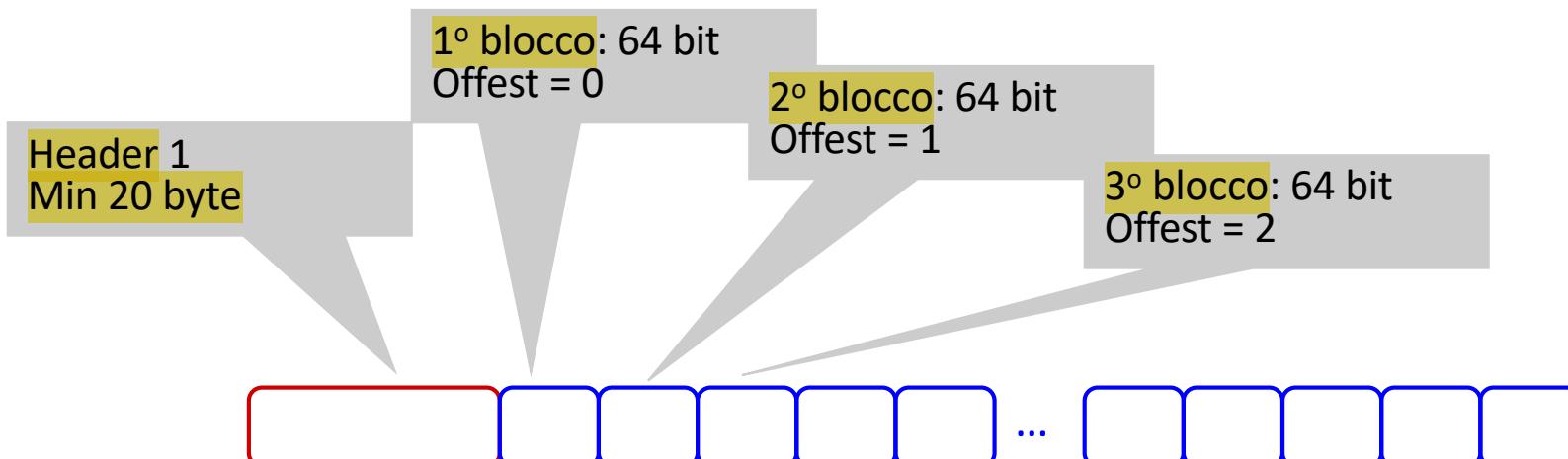
Fragment offset

L'intero datagramma IP è suddiviso virtualmente in blocchi di 8 byte.

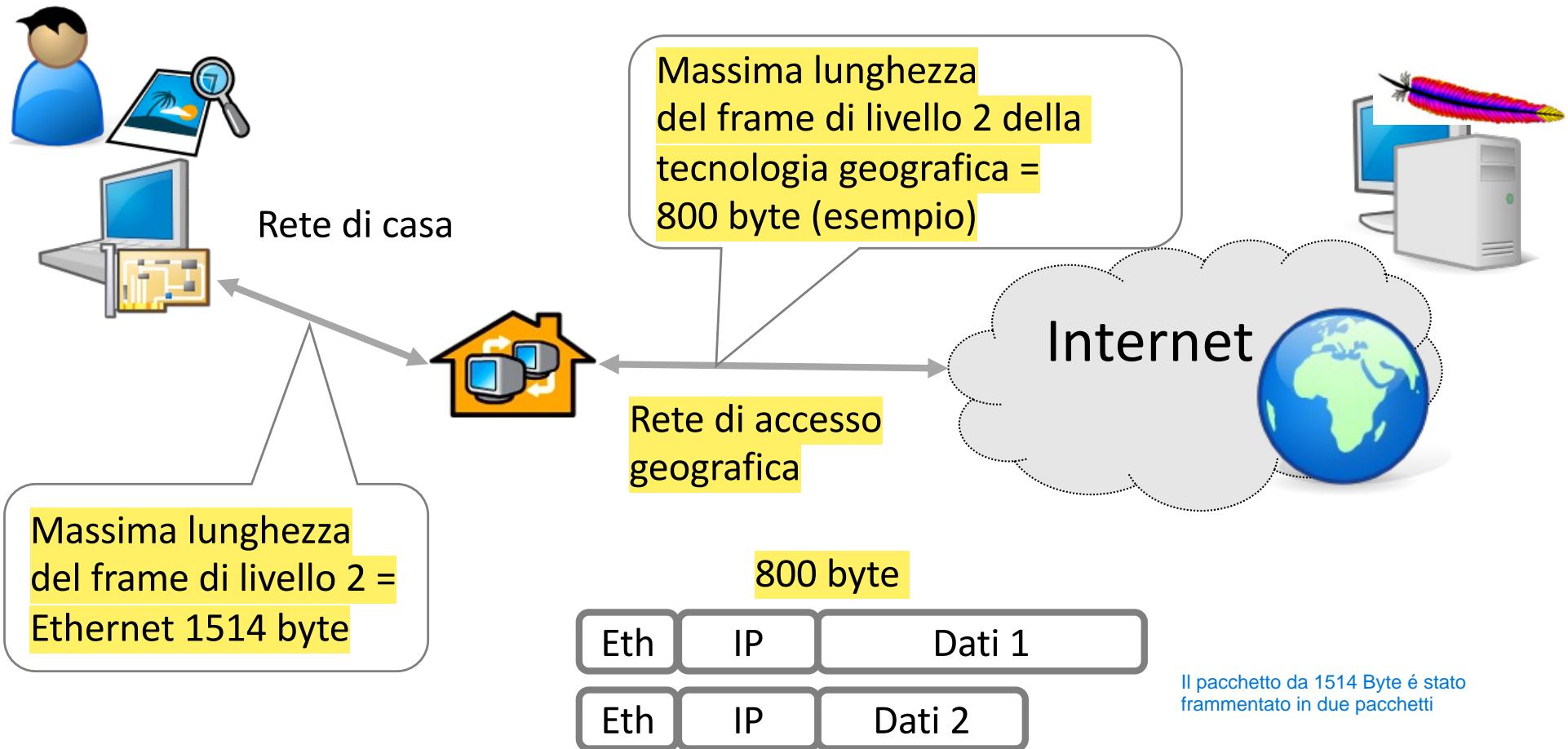
- Il datagramma IP viene virtualmente suddiviso in sotto-blocchi di 8 byte (64 bit)
- Per l'IP che trasmette (non necessariamente la sorgente dei dati ma anche un nodo intermedio)
 - Il primo blocco del datagramma è il numero 0
 - I blocchi successivi sono logicamente numerati sequenzialmente
- Il numero 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 quando la dimensione del pacchetto supera la MTU (Maximum Transmission Unit) del collegamento successivo.
 - Tipicamente i nodi intermedi non riassemlano, ma lo fa solamente il terminale ricevente (Questa operazione è demandata esclusivamente all'host destinatario)
- Frammentazioni multiple → Un datagramma può essere frammentato più volte durante il transito in diversi nodi.
Esempio: un datagramma frammentato in due parti può essere ulteriormente suddiviso in tre frammenti se il collegamento successivo ha un MTU più piccolo.
 - 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?





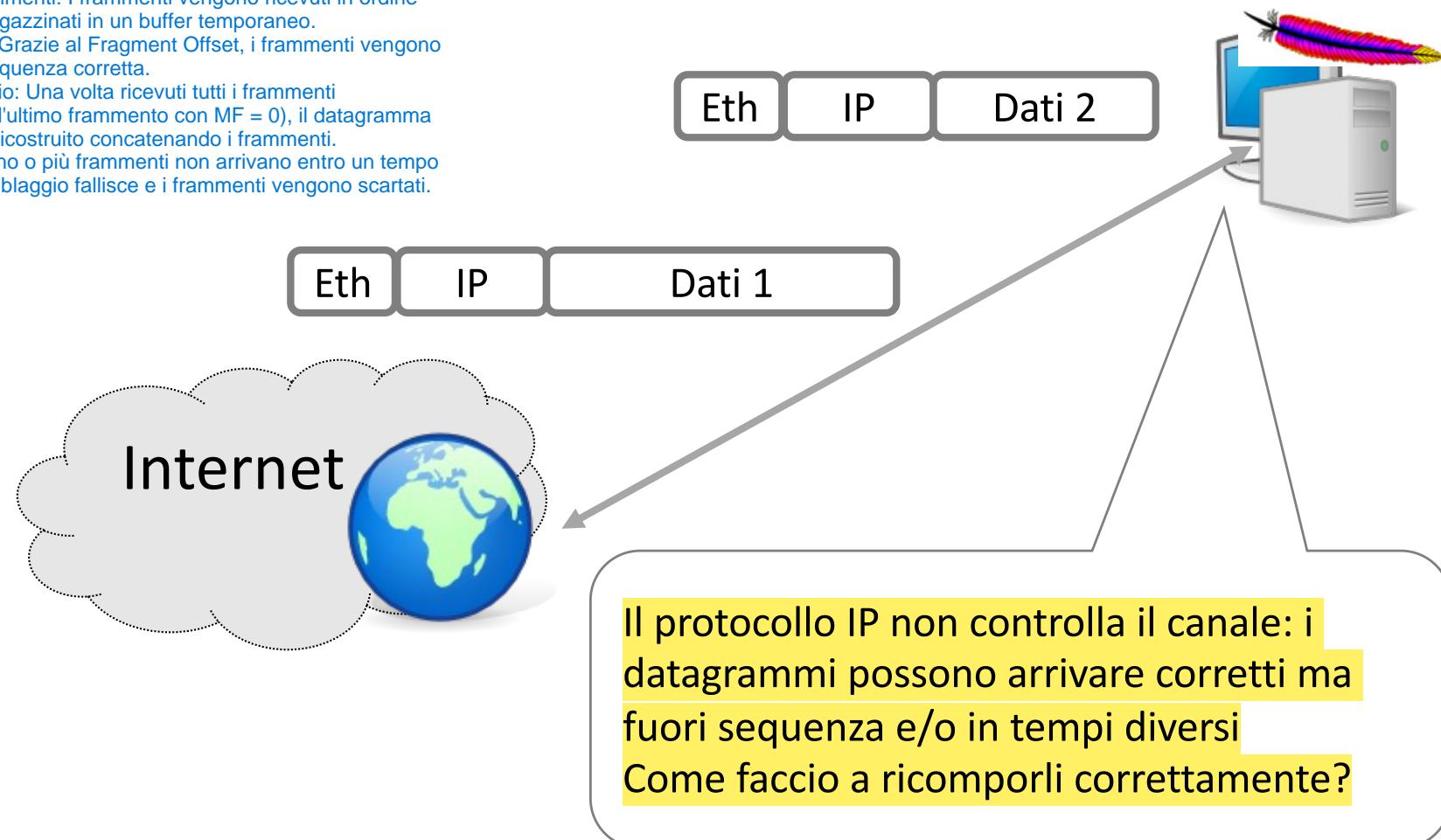
Il protocollo IP è connectionless (ogni pacchetto è indipendente e può seguire percorsi diversi) e non garantisce l'arrivo dei datagrammi né il loro ordine di ricezione.

Il riassemblamento

Non esiste un meccanismo intrinseco nel protocollo IP per garantire la consegna.

Ecco come avviene il riassemblamento:

- Ricezione frammenti: I frammenti vengono ricevuti in ordine casuale e immagazzinati in un buffer temporaneo.
- Ordinamento: Grazie al Fragment Offset, i frammenti vengono ordinati nella sequenza corretta.
- Riassemblaggio: Una volta ricevuti tutti i frammenti (confermato dall'ultimo frammento con MF = 0), il datagramma originale viene ricostruito concatenando i frammenti.
- Timeout: Se uno o più frammenti non arrivano entro un tempo limite, il riassemblaggio fallisce e i frammenti vengono scartati.



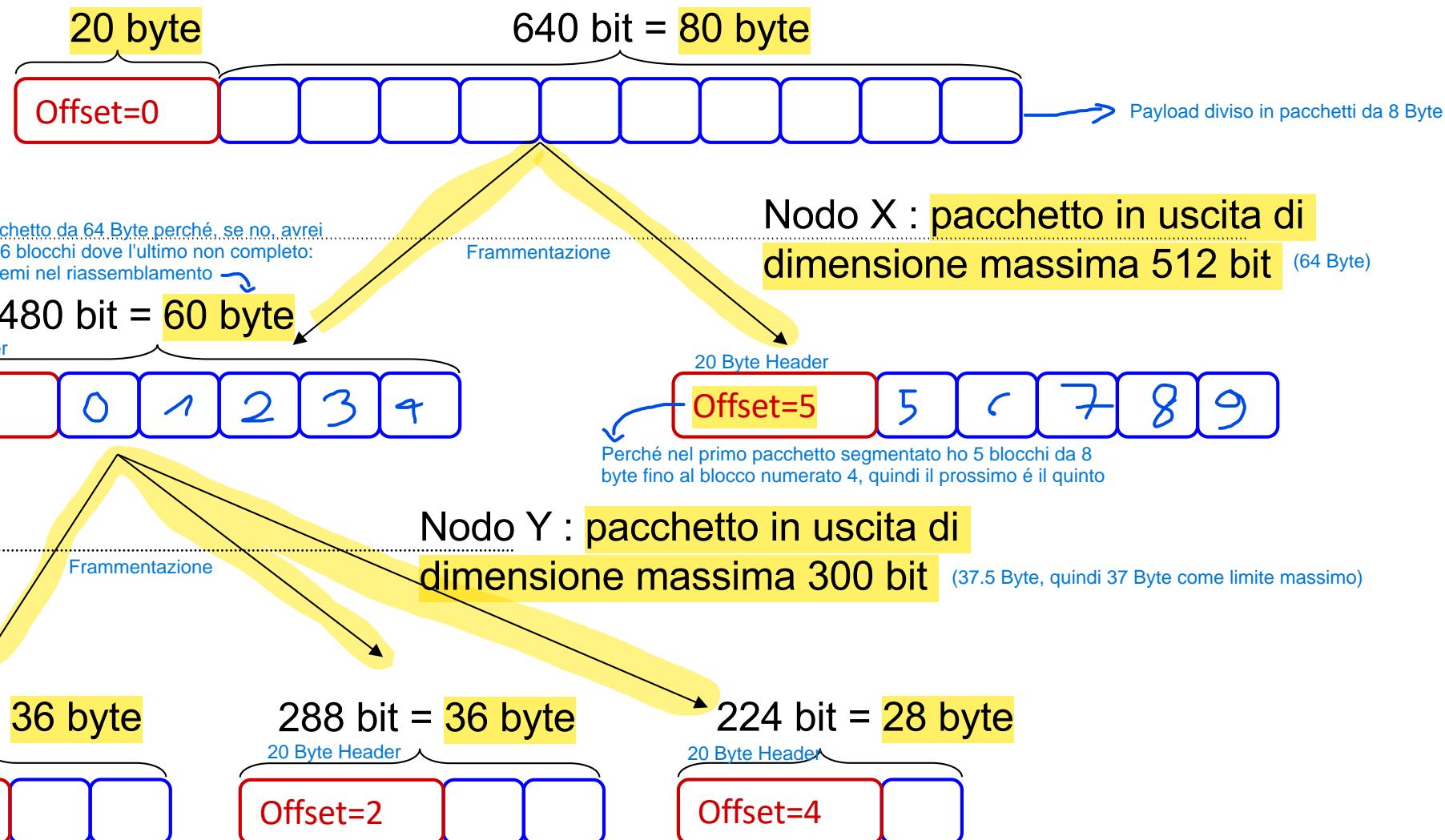
Un Pacchetto, per essere segmentato, deve avere almeno un payload di 8 byte (64 bit)

Se il pacchetto è piú grande della MTU del collegamento attraverso cui deve passare, segmenta il pacchetto in piú pacchetti che sono \leq a MTU



Calcolo dell'offset

Solo l'ultimo pacchetto frammentato, può avere l'ultimo blocco con meno di 8 Byte all'interno





Formato del pacchetto IP (4)

→ È un campo utilizzato per limitare la durata di un datagramma IP nella rete. Contiene un valore numerico che rappresenta il massimo numero di nodi (router) che il pacchetto può attraversare.

• **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

→ Indica come interpretare i dati del payload.

Per evitare che pacchetti persi rimangano in circolazione indefinitamente, consumando risorse della rete.

• **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 per verificare l'integrità dell'intestazione del pacchetto IP.
- **Source and Destination Address** : indirizzi sorgente e destinazione



Formato del pacchetto IP (5)

→ Campo opzionale che consente di includere informazioni aggiuntive per il controllo e la gestione del trasferimento dei datagrammi.

- **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

Quando il campo Options non occupa multipli di 32 bit, il padding viene aggiunto per "riempire" lo spazio rimanente.



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

L'instradamento IP



Instrandamento

- 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?
- ...

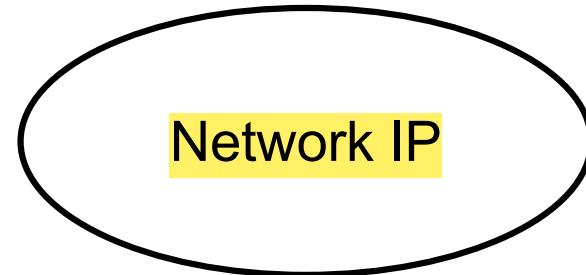
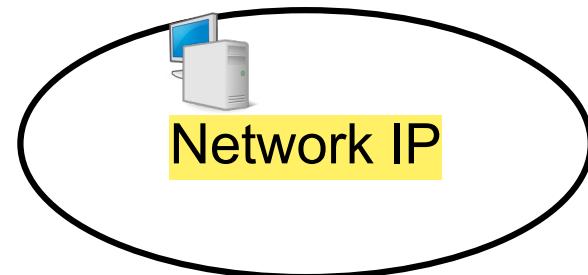


Come funziona Internet

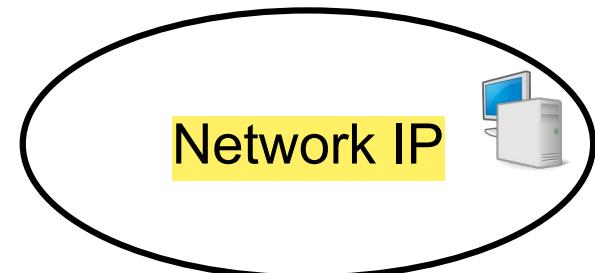
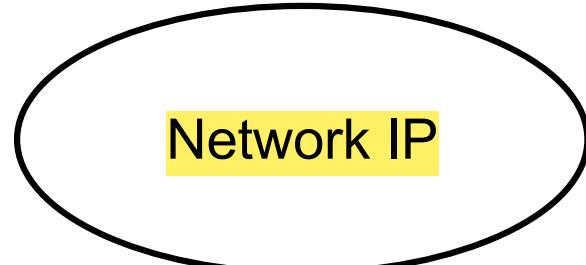
- Internet è una grande “rete di reti”
- La componente elementare è la **network IP**
 - Ogni network IP è una sorta di isola
 - L'isola tipicamente contiene calcolatori che fungono da nodi terminali della rete detti **host**
 - Le isole sono interconnesse da apparati che svolgono la funzione di “ponte”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



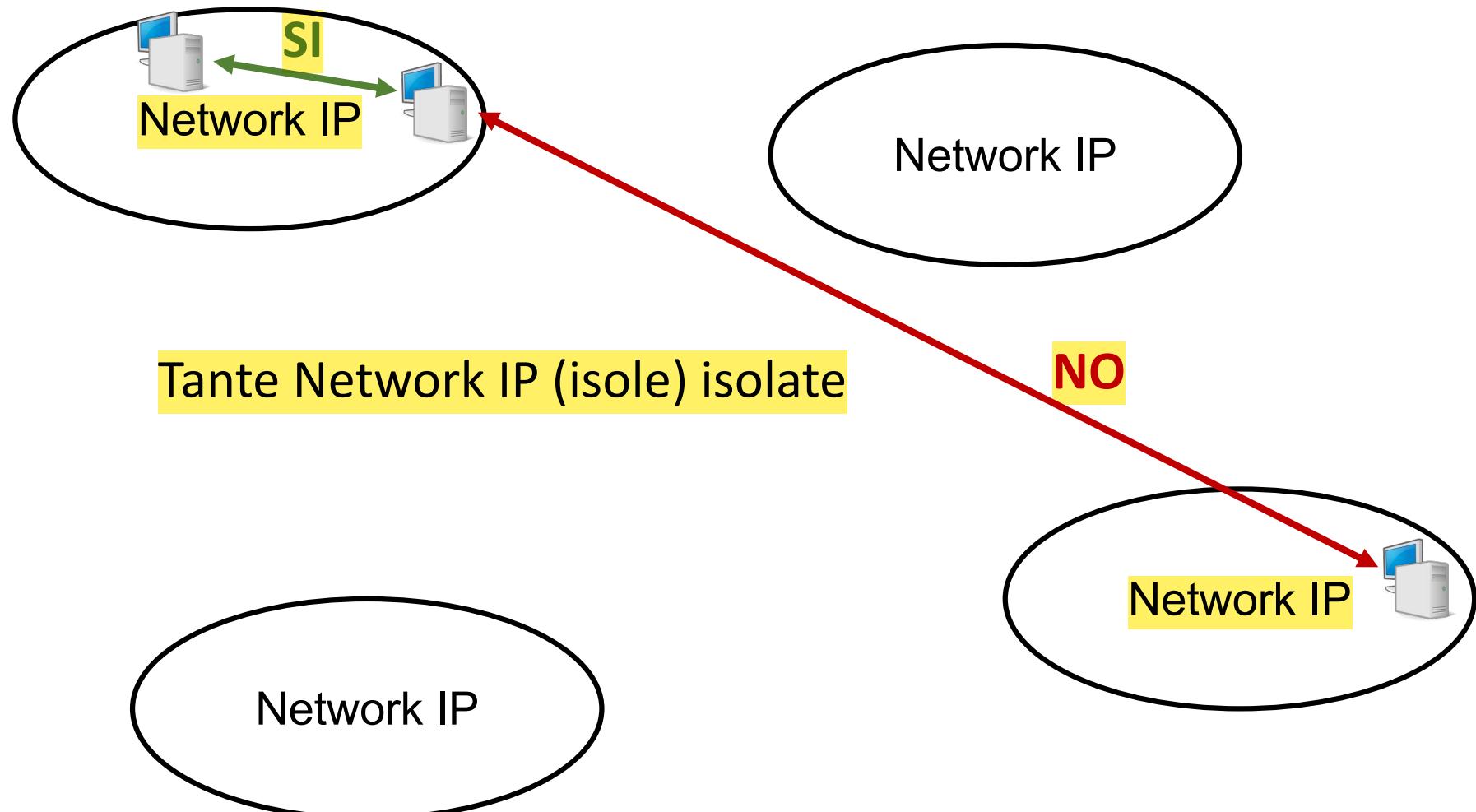
La network IP

- 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



Due host appartengono alla stessa RETE FISICA se possono comunicare direttamente attraverso l'infrastruttura di rete condivisa, senza necessità di instradamento tramite router.
Due host appartengono alla stessa RETE LOGICA se condividono lo stesso identificatore di rete (Net ID), determinato dall'indirizzo IP e dalla subnet mask.



Rete logica e rete fisica

La rete logica è indipendente dalla topologia fisica.

Due host appartenenti alla stessa rete logica possono comunicare direttamente senza l'uso di un router.

- Nella terminologia di Internet si definisce
 - **Rete logica:** la network IP a cui un Host appartiene logicamente → È definita dagli indirizzi IP e dalla subnet mask, che determinano quali dispositivi sono considerati nella stessa rete logica.
 - **Rete fisica:** la rete (tipicamente LAN) a cui un Host è effettivamente connesso → È la rete effettivamente connessa fisicamente.
La rete fisica opera a livello 1 (fisico) e 2 (data link) del modello OSI.
Utilizza indirizzi MAC per identificare i dispositivi nella comunicazione locale (livello 2).
- La rete fisica normalmente ha capacità di instradamento e può avere indirizzi locali (es. indirizzi MAC)
 - Ogni dispositivo collegato a livello fisico ha un indirizzo univoco (indirizzo MAC), utilizzato per la comunicazione locale prima che il traffico venga instradato a livello IP.
- L'architettura a strati nasconde gli indirizzi fisici e consente alle applicazioni di lavorare solo con indirizzi IP

Grazie all'architettura a strati, le applicazioni lavorano con indirizzi IP (logici) senza preoccuparsi dei dettagli fisici.
La traduzione tra indirizzi logici (IP) e fisici (MAC) avviene tramite protocolli come ARP (Address Resolution Protocol).

Comunicazione tra gli host:

- Stessa rete fisica: Se gli host sono sulla stessa rete fisica, possono comunicare direttamente utilizzando dispositivi di livello 2, come switch o bridge.
- Reti fisiche diverse: Se gli host sono su reti fisiche differenti, la comunicazione richiede l'uso di un router o di un dispositivo di livello 3 per instradare il traffico tra i segmenti fisici.



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 Servono dispositivi capaci di trasferire pacchetti da un'isola all'altra.
 - Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere → Devono esistere regole o configurazioni che permettano di determinare quale collegamento usare per raggiungere una specifica isola.

1) Stessa rete logica, reti fisiche diverse (ARCHITETTURA SBAGLIATA):

Questo scenario si verifica quando due host condividono lo stesso indirizzo di rete IP (definito dalla subnet mask), ma sono collegati attraverso segmenti fisici distinti.

Esempio:

Host A: Indirizzo IP 192.168.1.10, situato in un edificio.

Host B: Indirizzo IP 192.168.1.20, situato in un altro edificio.

Sembra che Host A e Host B condividano la stessa rete logica (192.168.1.0/24), potrebbero essere collegati a reti fisiche diverse, come segmenti Ethernet separati o diverse VLAN.

Due host possono appartenere alla stessa rete logica (ovvero condividere lo stesso intervallo di indirizzi IP) ma essere situati dietro dispositivi NAT (Network Address Translation) differenti.

Non è necessario un Router per comunicare perché stessa rete logica, ma bisogna avere un nodo di rete per rimpingere l'arp request e pacchetto

2) Stessa rete fisica, reti logiche diverse:

In questo caso, due host sono collegati alla stessa infrastruttura fisica ma appartengono a subnet IP differenti.

Esempio:

Host C: Indirizzo IP 192.168.1.30, subnet mask 255.255.255.0.

Host D: Indirizzo IP 192.168.2.40, subnet mask 255.255.255.0.

Entrambi gli host sono collegati allo stesso switch fisico, ma appartengono a reti logiche diverse (192.168.1.0/24 e 192.168.2.0/24). In questo scenario, la comunicazione tra Host C e Host D richiede l'uso di un router per instradare il traffico tra le due subnet.

Due host possono essere gestiti dallo stesso dispositivo NAT (Network Address Translation) ma appartengano a reti logiche diverse.



Un router è un dispositivo di rete che:
Instrada i pacchetti tra diverse reti IP.

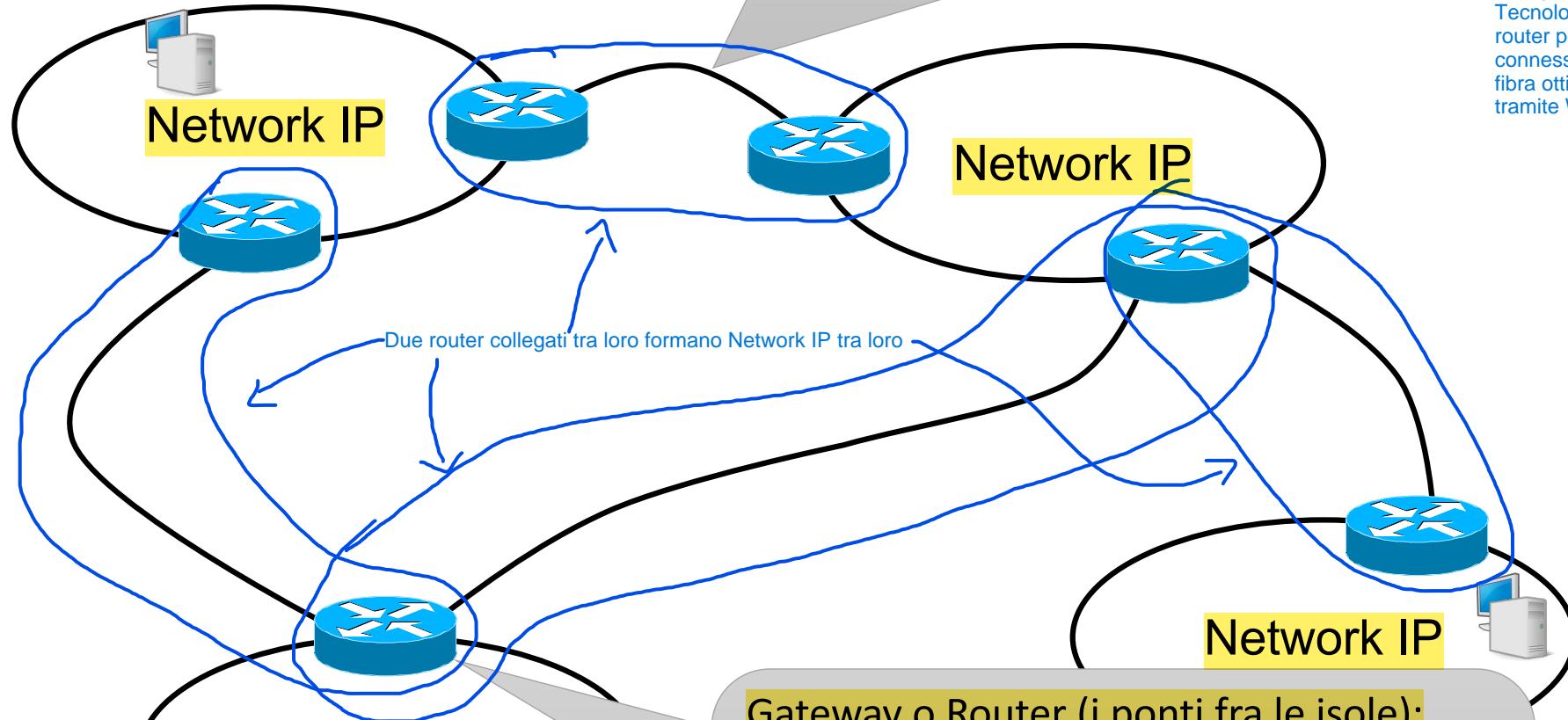
Funziona al livello 3 del modello OSI (strato di rete), utilizzando gli indirizzi IP per determinare la destinazione.
Gestisce protocolli di routing per decidere il percorso ottimale verso altre reti.

I router

Collegamento fra router:

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

Tecnologie simili: Per esempio, due router collegati via Ethernet.
Tecnologie diverse: Un router potrebbe essere connesso a uno tramite fibra ottica e a un altro tramite WAN.



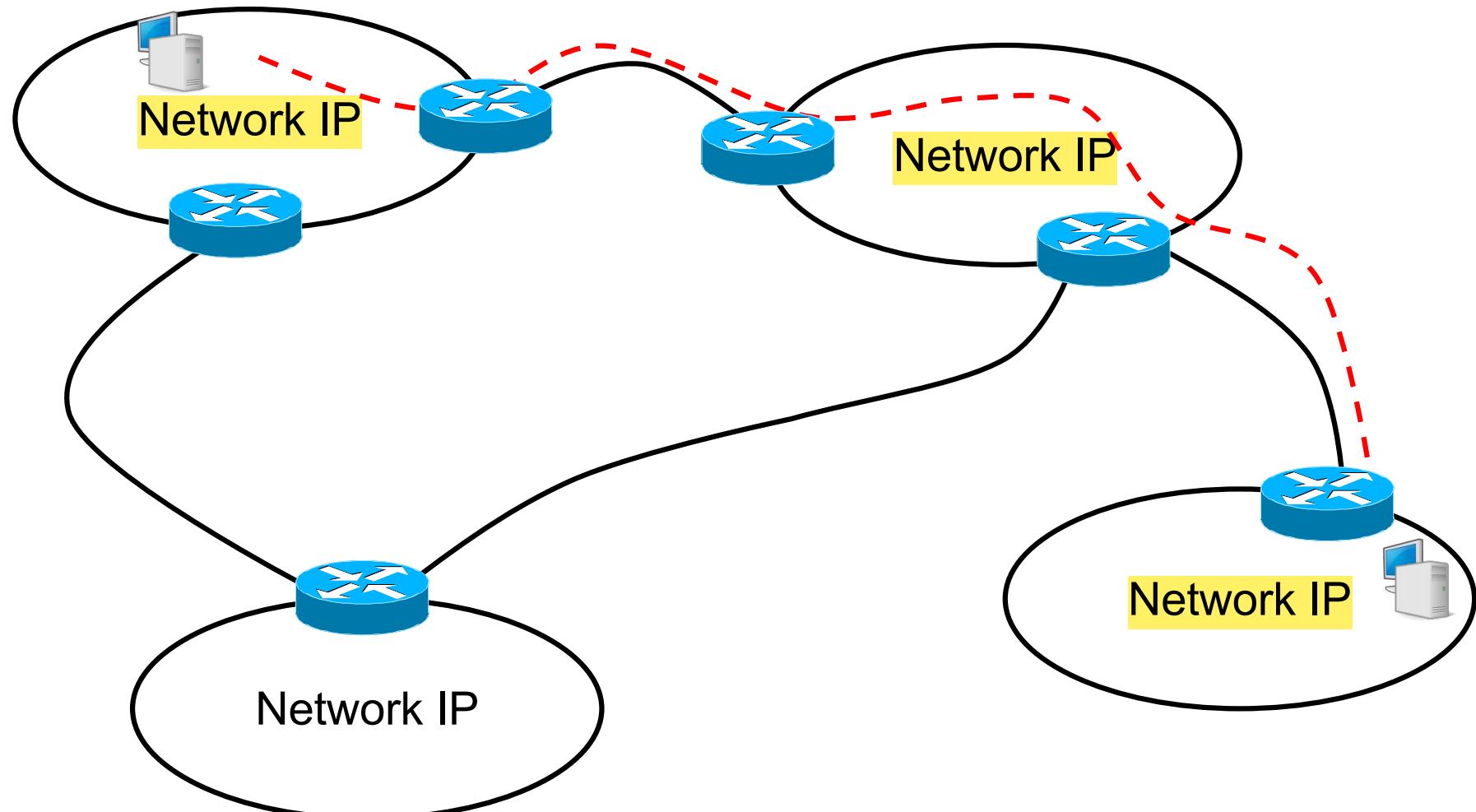
Per ogni collegamento, un router ha una interfaccia di rete (router sono dotati di interfacce fisiche che supportano diverse tecnologie di connessione)

Deve "parlare" le tecnologie di entrambe le reti che collega. Ad esempio, può tradurre pacchetti provenienti da una rete Ethernet per trasmetterli su una rete MPLS.

Gateway o Router (i ponti fra le isole):

- Nodo di rete che interconnecta 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



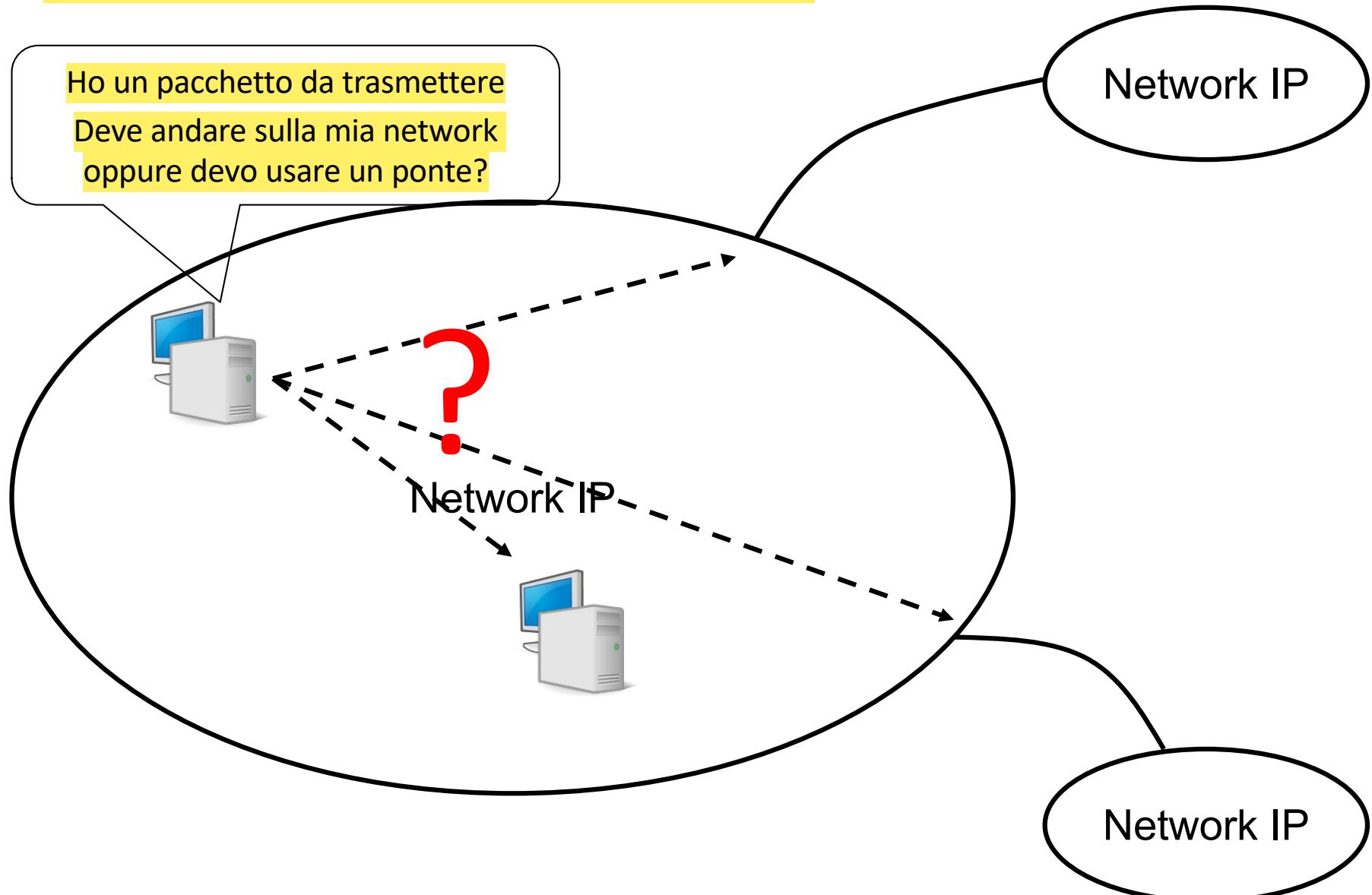


Cosa fa IP

- La tecnologia IP è agnostica rispetto alla tecnologia con cui sono realizzate le network → Il protocollo IP è progettato per essere indipendente dalla tecnologia di rete sottostante. Può operare su reti realizzate con tecnologie diverse
 - 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



Ho un pacchetto da trasmettere
Deve andare sulla mia network
oppure devo usare un ponte?

La risposta



Questa tabella è essenziale per decidere se:
Il pacchetto può essere consegnato localmente (all'interno della propria rete).
Deve essere inoltrato a un ponte (un router o gateway).

- Ogni nodo di Internet ha una base dati di destinazioni possibili

un nodo

→ Ogni nodo (sia host che router) mantiene una tabella di routing che contiene:
Destinazioni conosciute: Reti o host specifici raggiungibili.
Percorso predefinito (gateway di default): Utilizzato per pacchetti destinati a reti non esplicitamente elencate.

- Quando ^Vdeve inviare un datagramma
 - Parte dall'indirizzo IP di destinazione
 - Legge la base dati
 - Decide quale azione intraprendere

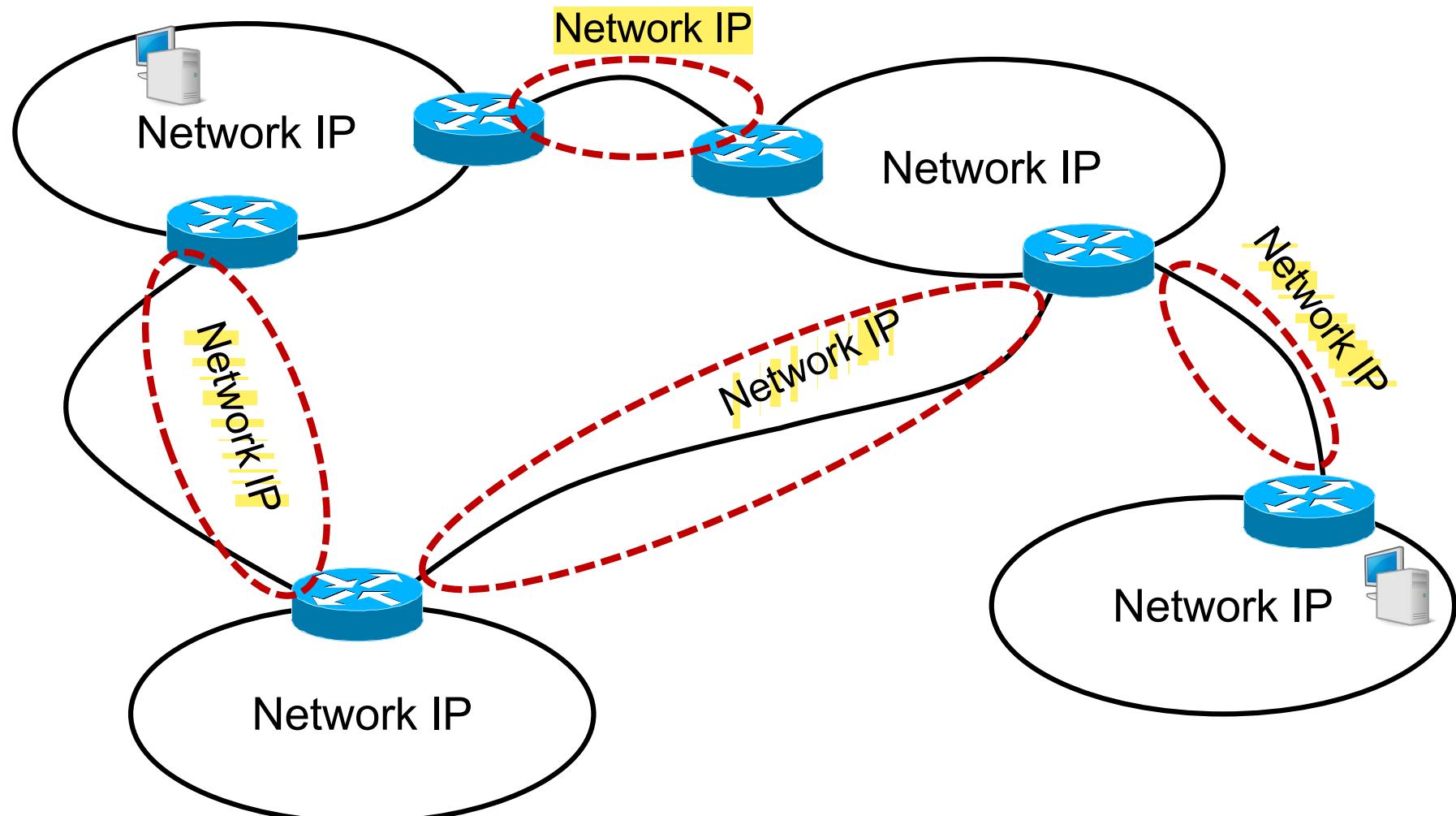
Per gli host una Tabella di routing locale: Gli host possiedono una tabella di routing che indica come raggiungere le destinazioni, specificando se un pacchetto deve essere inviato direttamente a un altro dispositivo nella stessa rete locale o inoltrato a un gateway predefinito per raggiungere reti esterne. Per i router una Tabella di routing estesa: I router mantengono tabelle di routing più complesse, contenenti informazioni su numerose reti e sottoreti. Queste tabelle vengono aggiornate dinamicamente attraverso protocolli di routing, permettendo ai router di instradare i pacchetti verso la destinazione più efficiente.

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

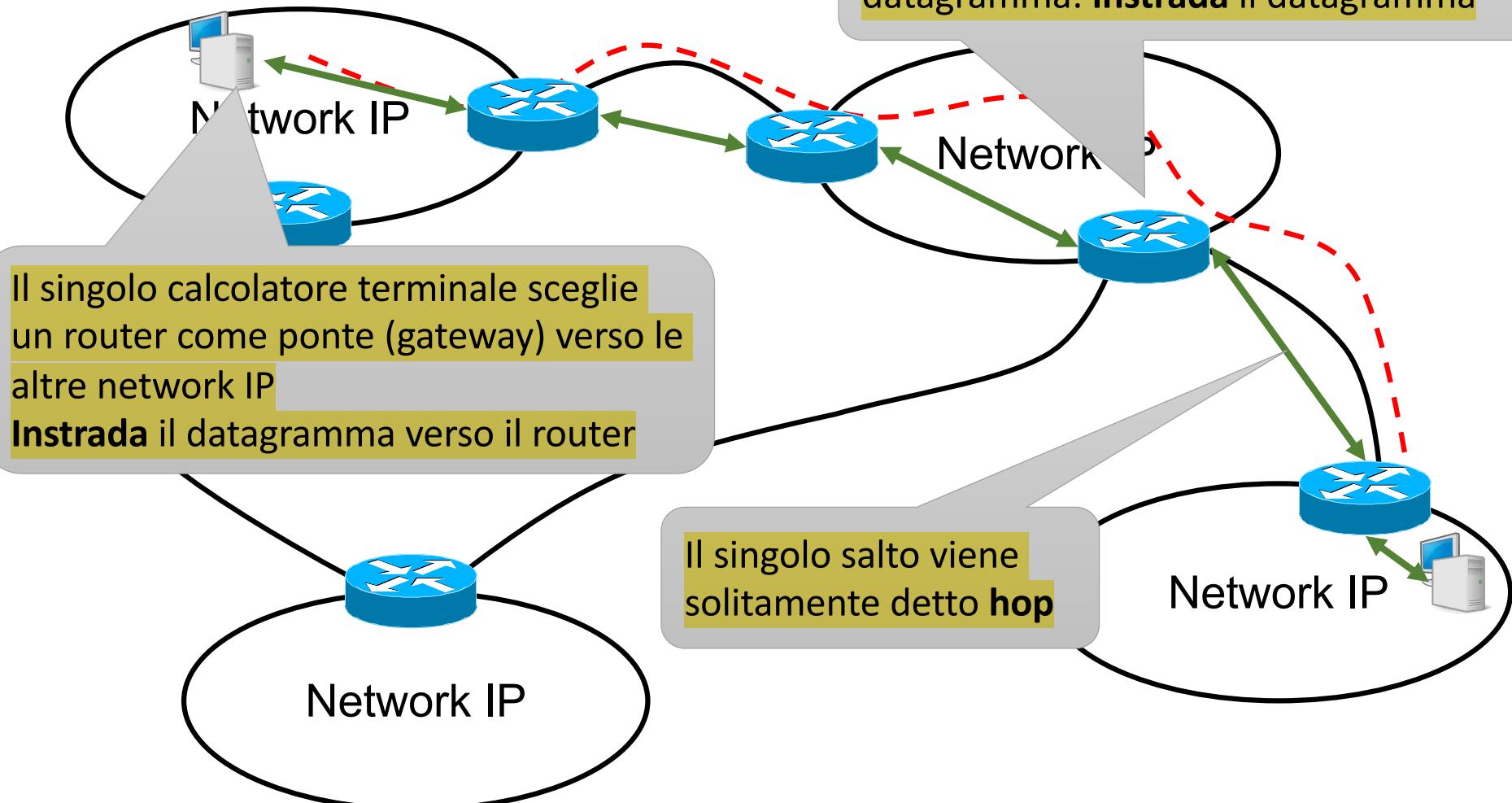
→ Se la destinazione è locale: Viene utilizzata la tecnologia della rete interna

→ Se è necessario un ponte: La tecnologia usata per connettersi al ponte dipende dal tipo di connessione al router

Le network fra i router



L'instradamento IP





Semantica dell'indirizzo IP

- L' indirizzo IP è logicamente suddiviso in due parti:
 - **Network (Net) ID** Identifica la rete IP a cui un host appartiene.
 - 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 un host (o dispositivo) specifico all'interno della rete (l'Host ID di un indirizzo IP identifica specificamente l'interfaccia di rete di un dispositivo all'interno di una rete.).
 - 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 → Non sono instradabili sulla rete pubblica. Ciò significa che i router di Internet scartano i pacchetti con questi indirizzi come destinazione.
- Possono essere riutilizzati in reti isolate → Possono essere utilizzati da più reti isolate senza rischio di conflitti, poiché sono validi solo all'interno della rete privata.

Gli IP privati consentono di ridurre il consumo di indirizzi pubblici, utilizzando una singola connessione pubblica per più dispositivi privati (tramite NAT). Il NAT traduce gli indirizzi privati in un indirizzo pubblico condiviso.

- 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

10001001.11001100.1011111.00011001

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

La più utilizzata



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

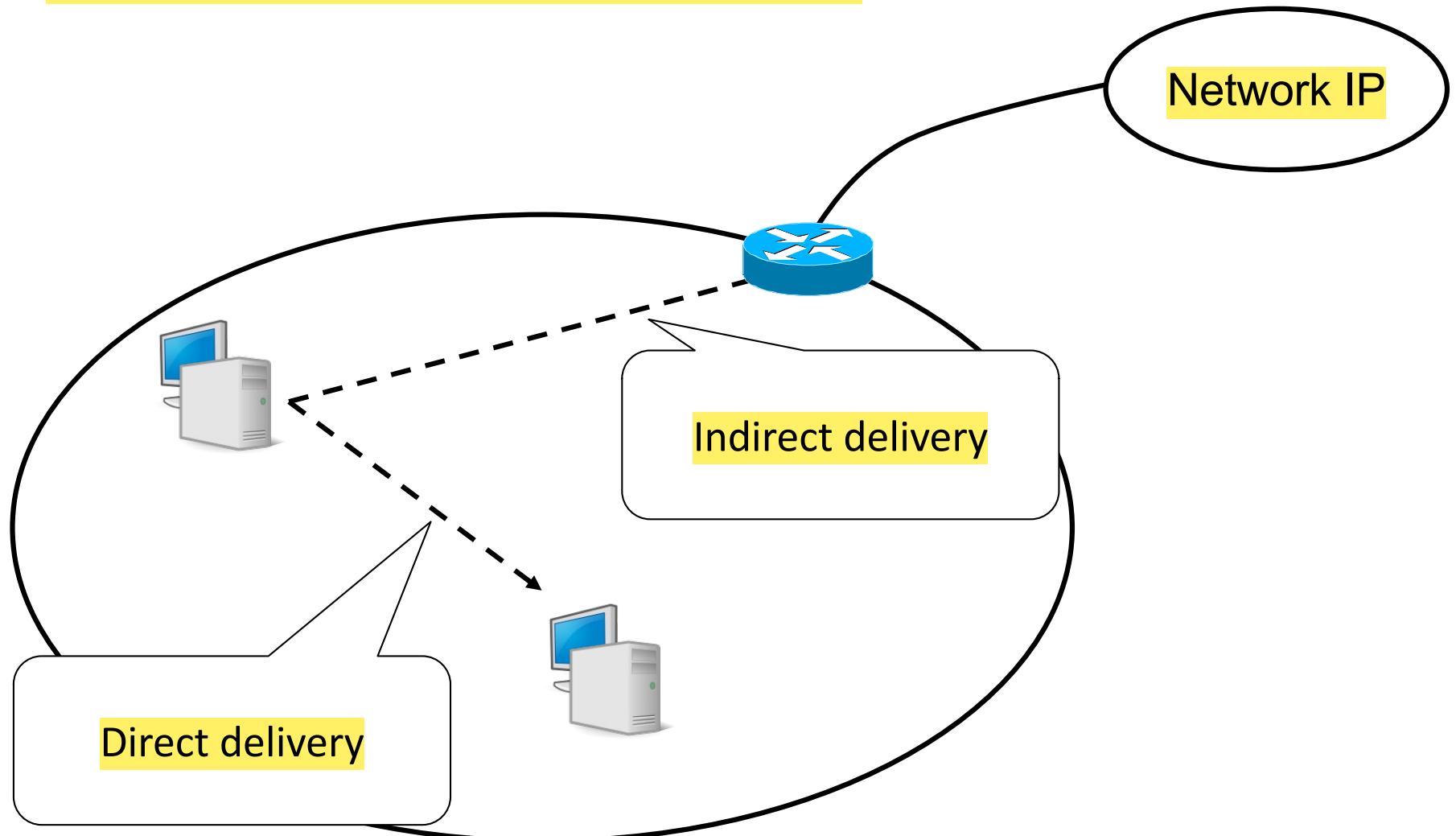


Esempio: Università di Bologna

- **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





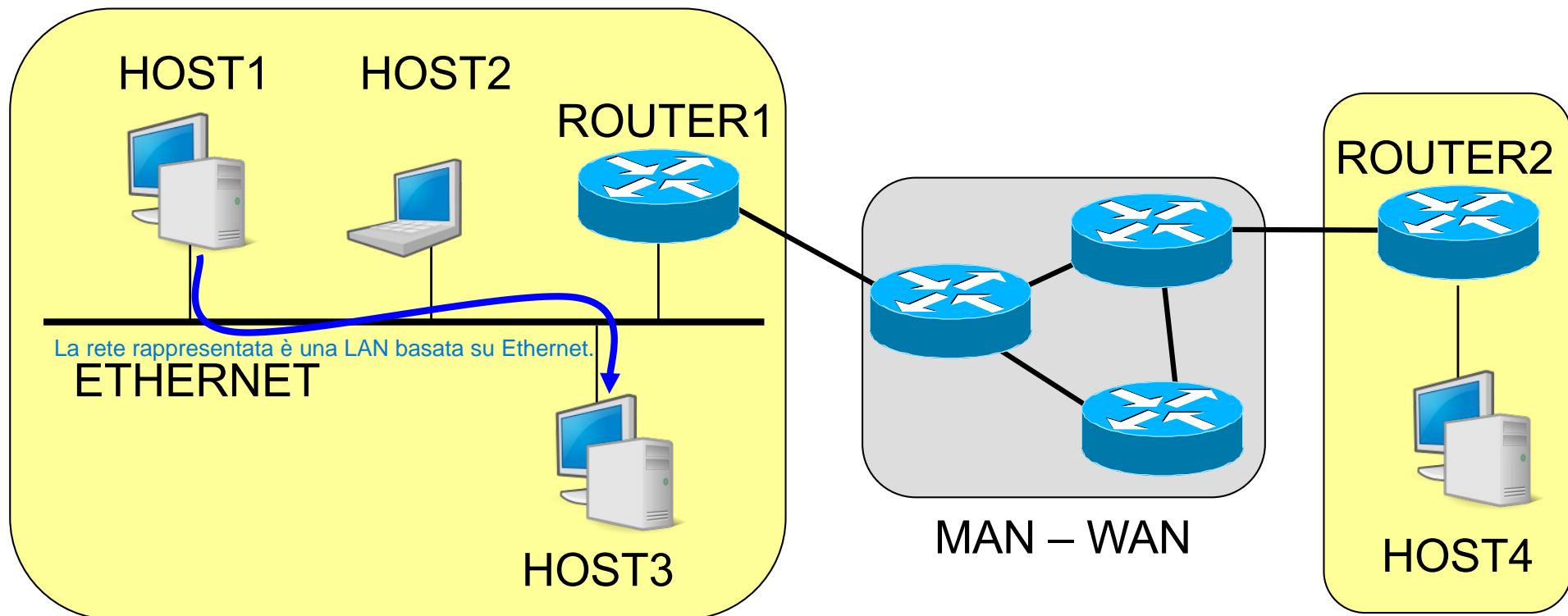
Instradamento diretto e indiretto

- **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

Il Direct Delivery avviene quando la destinazione si trova sulla stessa rete locale, e quindi l'indirizzo MAC del destinatario è utilizzato direttamente per il trasferimento dei dati senza necessità di inoltro tramite un router.



Direct Delivery



Relazione Indirizzi Fisici – Indirizzi IP

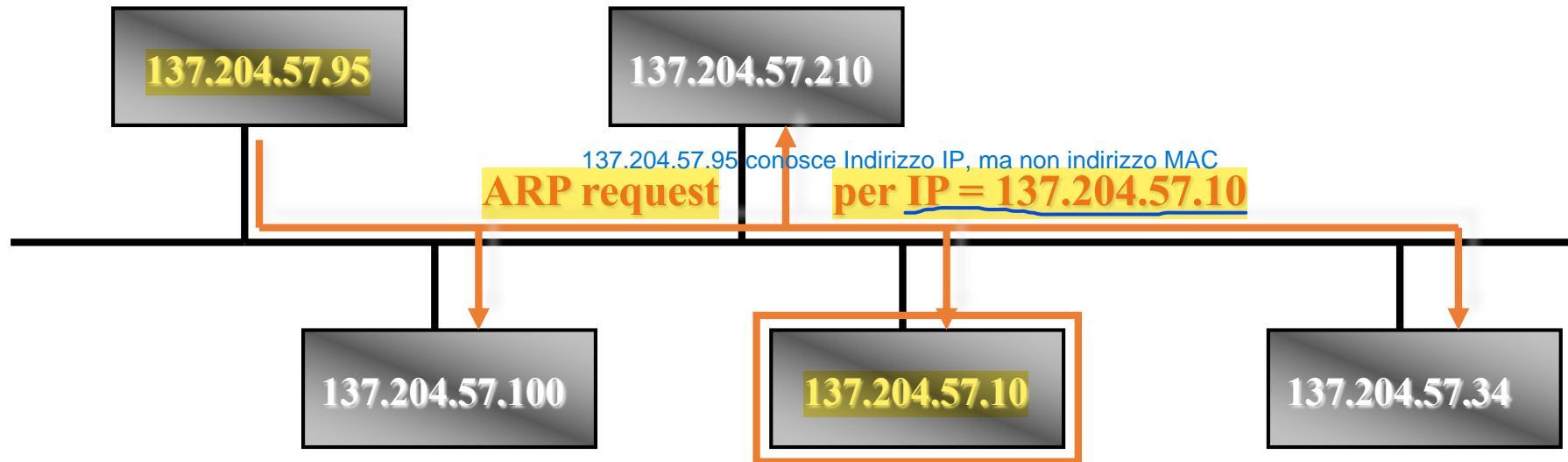
Il sistema operativo o il software di rete

- Software di basso livello nasconde gli indirizzi fisici e consente ai livelli superiori^(alle applicazioni) di lavorare solo con indirizzi IP
(indirizzi MAC)
- Gli host comunicano attraverso una **rete fisica** (ad es. LAN) quindi devono conoscere reciprocamente gli indirizzi fisici
(In una rete fisica come una LAN, gli host devono conoscere gli indirizzi fisici (MAC address) degli altri dispositivi per poter comunicare)
- L'host A vuole mandare datagrammi a B, che si trova sulla stessa rete fisica e di cui conosce solo l' indirizzo IP
Quando Host A vuole inviare dati a Host B, sa solo il suo indirizzo IP. Tuttavia, per inviare effettivamente i dati sulla rete fisica, ha bisogno dell'indirizzo fisico (MAC address) di Host B.
- Come si ricava l' indirizzo fisico di B dato il suo indirizzo IP?
Questo processo avviene tramite un protocollo chiamato ARP (Address Resolution Protocol).

Le richieste ARP funzionano esclusivamente tra host connessi alla stessa rete fisica o segmento di rete.

Address Resolution Protocol – ARP (RFC 826)

ARP è un protocollo che fa parte della suite di protocolli di livello 3

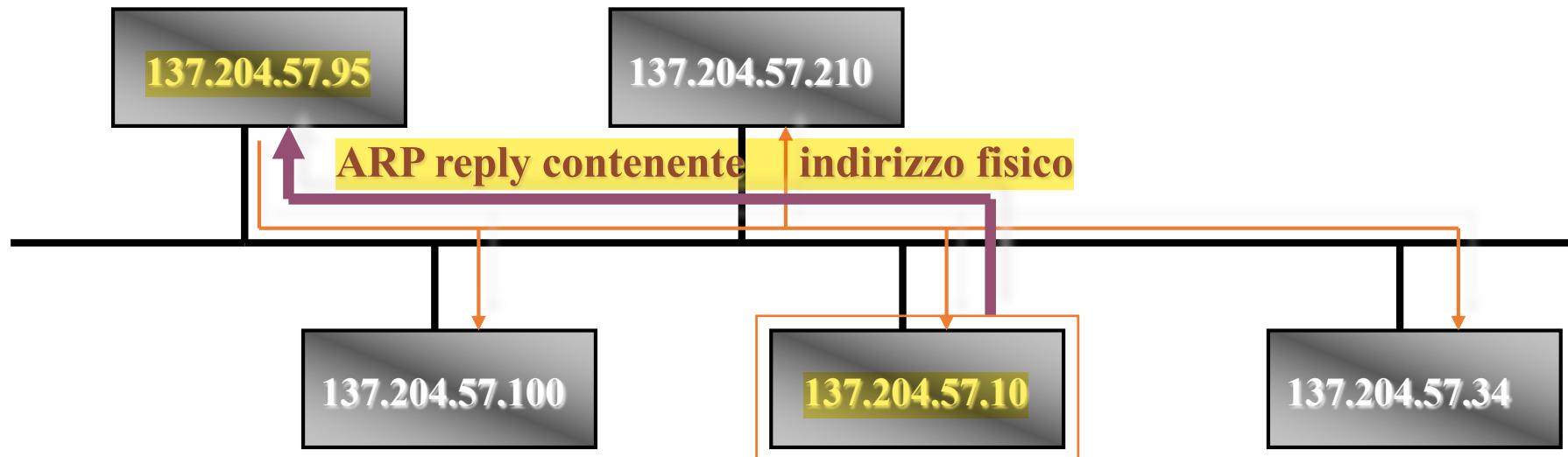


sulla rete fisica, un pacchetto di livello 2 in modalità

- 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

Tutti i dispositivi sulla rete leggono la richiesta. Solo il dispositivo con l'indirizzo IP corrispondente risponde.

Address Resolution Protocol - ARP (3)



- Il destinatario risponde al mittente, inviando un messaggio (**ARP reply**) che contiene il proprio indirizzo fisico (ARP reply è una trama mandata in modo non broadcast)
- 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 → Il dispositivo mittente memorizza la mappatura tra l'indirizzo IP e l'indirizzo MAC nella sua cache ARP. Questo evita la necessità di effettuare un'altra richiesta ARP per comunicazioni successive.

Comando ARP

arp -a

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

Comando ARP – Esempio

```
Command Prompt

C:\>arp -a
Interface: 137.204.57.174 on Interface 0x10000003
  Internet Address      Physical Address      Type
  137.204.57.1           08-00-20-9c-9c-93    dynamic
  137.204.57.88          00-60-b0-78-e8-fd    dynamic
  137.204.57.180         00-10-4b-db-0a-3a    dynamic
  137.204.57.181         00-30-c1-d5-ee-9b    dynamic
  137.204.57.254         00-50-54-d9-ba-00    dynamic

C:\>ping -n 1 137.204.57.177
Pinging 137.204.57.177 with 32 bytes of data:
Reply from 137.204.57.177: bytes=32 time<10ms TTL=128
Ping statistics for 137.204.57.177:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a
Interface: 137.204.57.174 on Interface 0x10000003
  Internet Address      Physical Address      Type
  137.204.57.1           08-00-20-9c-9c-93    dynamic
  137.204.57.177          00-b0-d0-ec-46-62    dynamic
  137.204.57.180         00-10-4b-db-0a-3a    dynamic
  137.204.57.181         00-30-c1-d5-ee-9b    dynamic
  137.204.57.254         00-50-54-d9-ba-00    dynamic

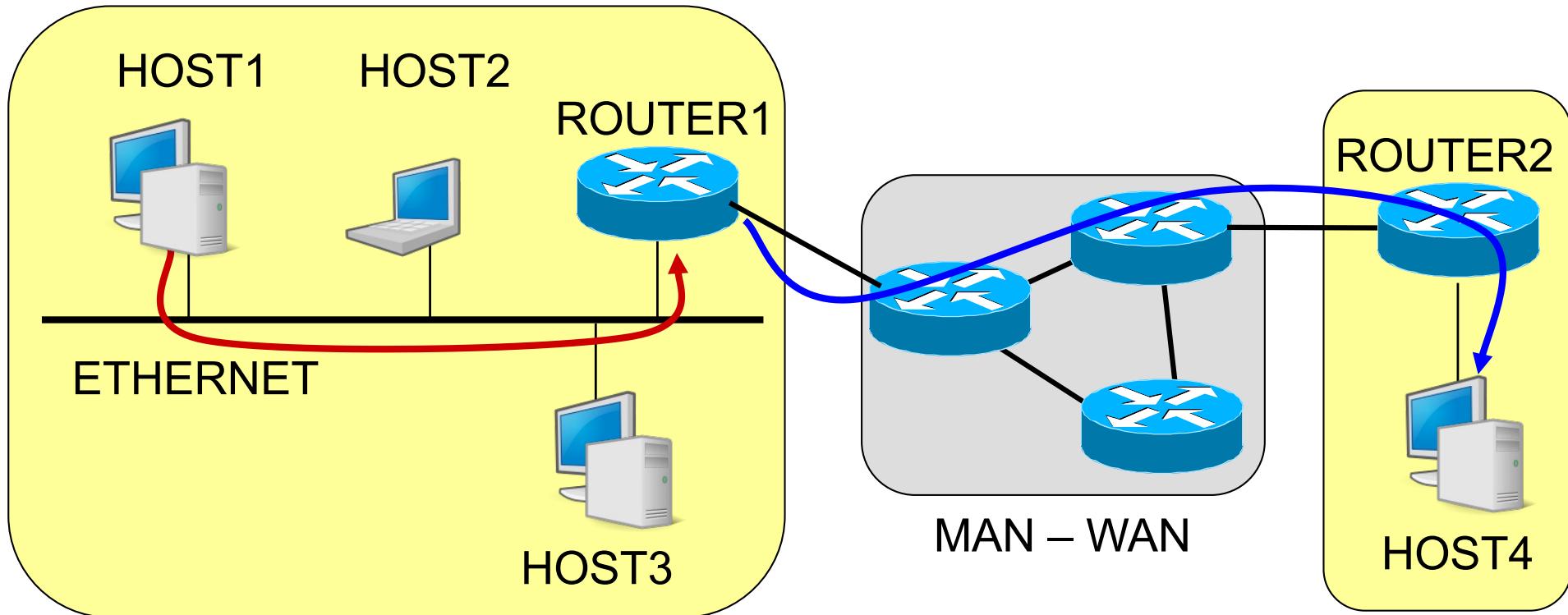
C:\>_
```



Consegna indiretta di pacchetti tra due host che appartengono a reti diverse.

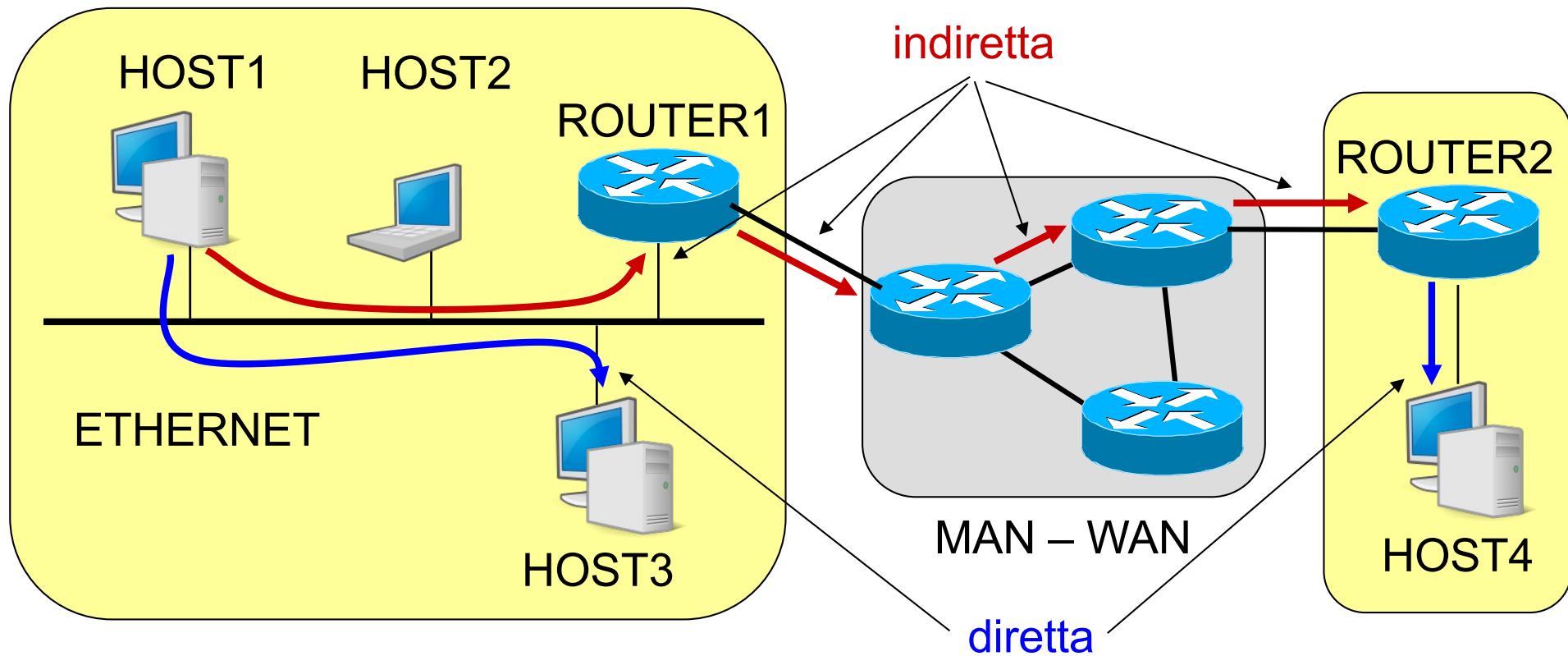
Indirect Delivery

A Livello 3 (IP), il pacchetto mantiene come indirizzo di destinazione l'indirizzo IP di HOST4 per tutto il tragitto. A Livello 2 (Ethernet), l'indirizzo MAC cambia a ogni salto: ad esempio, da HOST1 a ROUTER1, e successivamente tra i router fino alla destinazione.



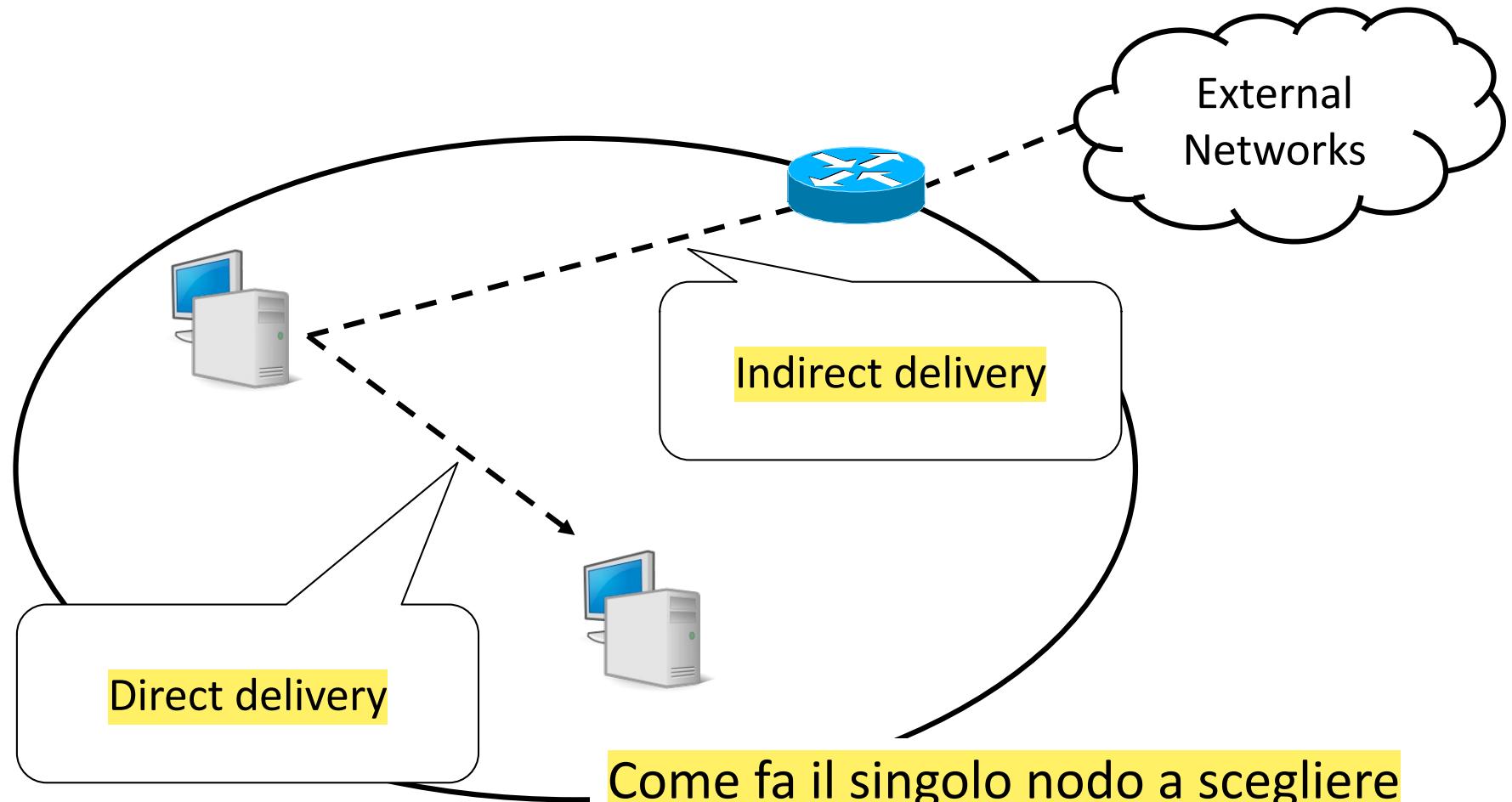
Da mittente a destinatario

- 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

Ogni riga rappresenta una singola rotta verso una determinata destinazione o un insieme di destinazioni. Contiene tutte le informazioni necessarie per instradare un pacchetto su quella rotta (destinazione, gateway, interfaccia, metrica).
 - 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

Informazioni comuni: Indipendentemente dalla piattaforma, le informazioni essenziali sono sempre le stesse.
Presentazione e gestione: Cambiano solo il modo in cui le tabelle vengono visualizzate e gestite.

Questa tabella contiene informazioni sulle rotte disponibili, consentendo al dispositivo di decidere a quale "hop" successivo inviare il pacchetto.



Route

Rotte Direttamente Connesse: Indicano reti a cui il dispositivo è direttamente collegato.
Rotte Statiche: Configurate manualmente da un amministratore per specificare percorsi fissi.
Rotte Dinamiche: Apprese automaticamente tramite protocolli di routing come OSPF o RIP.

- Tipici campi della singola rotta sono:

- **Destinazione (D):** numero IP valido

- Può essere un indirizzo di network o di host

Specifica l'indirizzo IP della rete o dell'host di destinazione.

- **Netmask (N):** maschera di rete valida

- Identifica il Net-ID Definisce la porzione dell'indirizzo IP che identifica la rete.

- **Gateway (G):** numero IP a cui consegnare il datagramma

- Indica il tipo di consegna da effettuare Indica l'indirizzo IP del router successivo a cui inviare il pacchetto per raggiungere la destinazione finale o indica di fare instradamento diretto.

- **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 Specifica l'interfaccia di rete attraverso la quale il pacchetto deve essere inviato.

- **Metrica (M):** specifica il “costo” di quel particolare route

- Possono esistere più route verso una medesima destinazione

Rappresenta il costo associato alla rotta; percorsi con metriche inferiori sono preferiti.



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^(destinazione) 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**)

Il nodo confronta IP_D con le voci nella tabella di instradamento.

Se viene trovata una rotta corrispondente:

Il pacchetto viene instradato secondo i campi Gateway (G) e Interfaccia di rete (IF) della rotta selezionata.

Se non viene trovata alcuna rotta:

Viene generato un messaggio di errore, tipicamente notificato al mittente come 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”
 - $(\text{IP_D AND N}) = R$
 - 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 (netmask più grande)

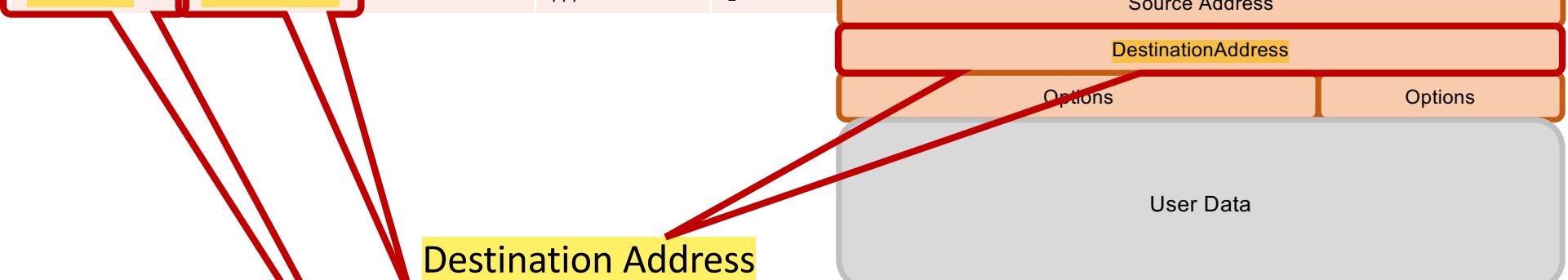
Se $R = D$ (il risultato del confronto corrisponde al campo Destinazione), quella rotta viene selezionata.

In caso contrario, si passa alla riga successiva della tabella.



II 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

Bitwise

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 (vengono presi solo i BIT ad 1 in quella posizione)
255.255.255.255
192.168.002.018 \equiv 192.168.002.018

- La riga 3 è quella giusta (host specific) (indirizzo IP di un Host)



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) (indirizzo IP di una Network)



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)

Il gateway predefinito in una tabella di instradamento IP è l'indirizzo del router a cui un dispositivo invia i pacchetti destinati a reti esterne alla propria rete locale. In altre parole, è il percorso utilizzato quando non esiste una rotta specifica per la destinazione desiderata.



Gateway

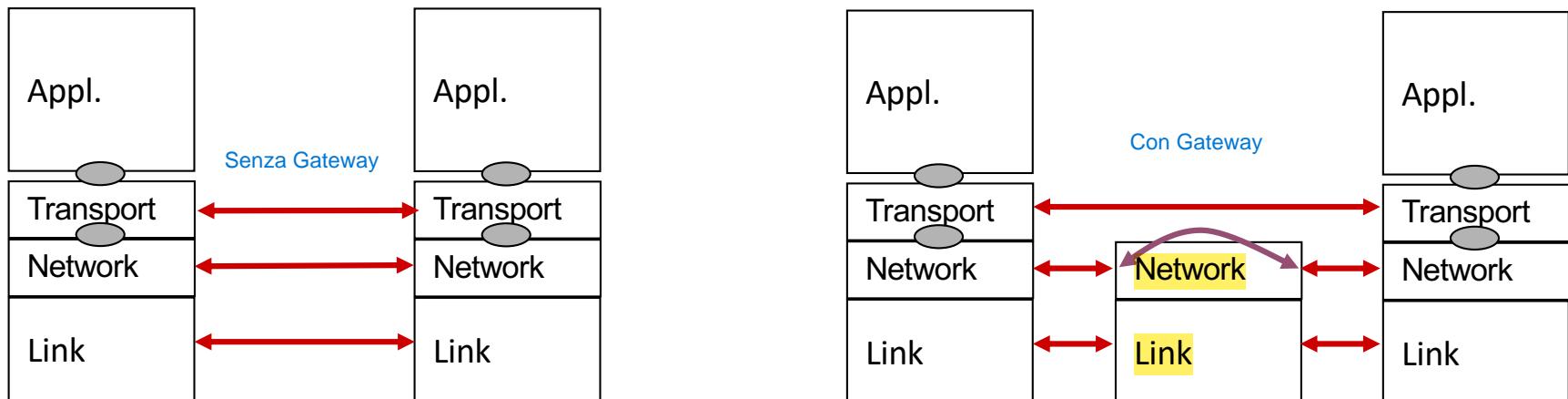
- Nella tabella di instradamento compaiono
 - Gateway
 - Interfaccia
- Perché due informazioni distinte?
- Chi è il gateway?



Il ruolo del Gateway

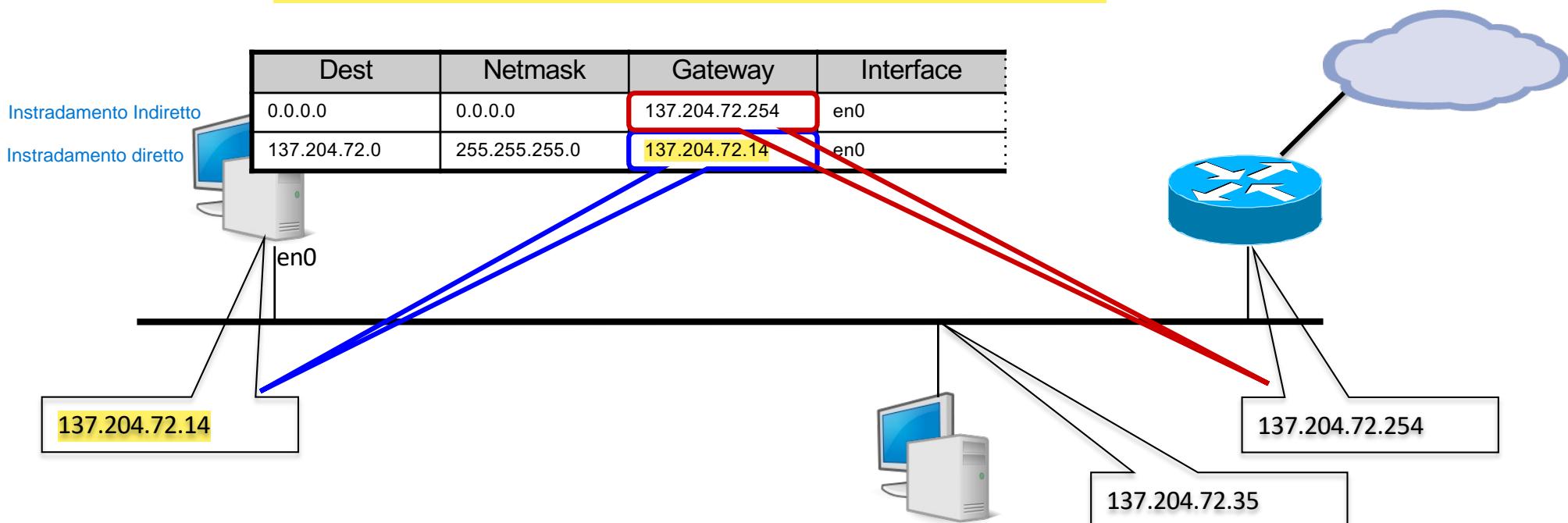
Un gateway è responsabile della consegna dei datagrammi quando due host appartengono a reti differenti. La funzione principale del gateway è quella di collegare reti diverse, garantendo la comunicazione tra dispositivi che altrimenti non sarebbero in grado di interagire direttamente.

- Il table look-up sceglie la $D^{\text{(destinazione)}}$ -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

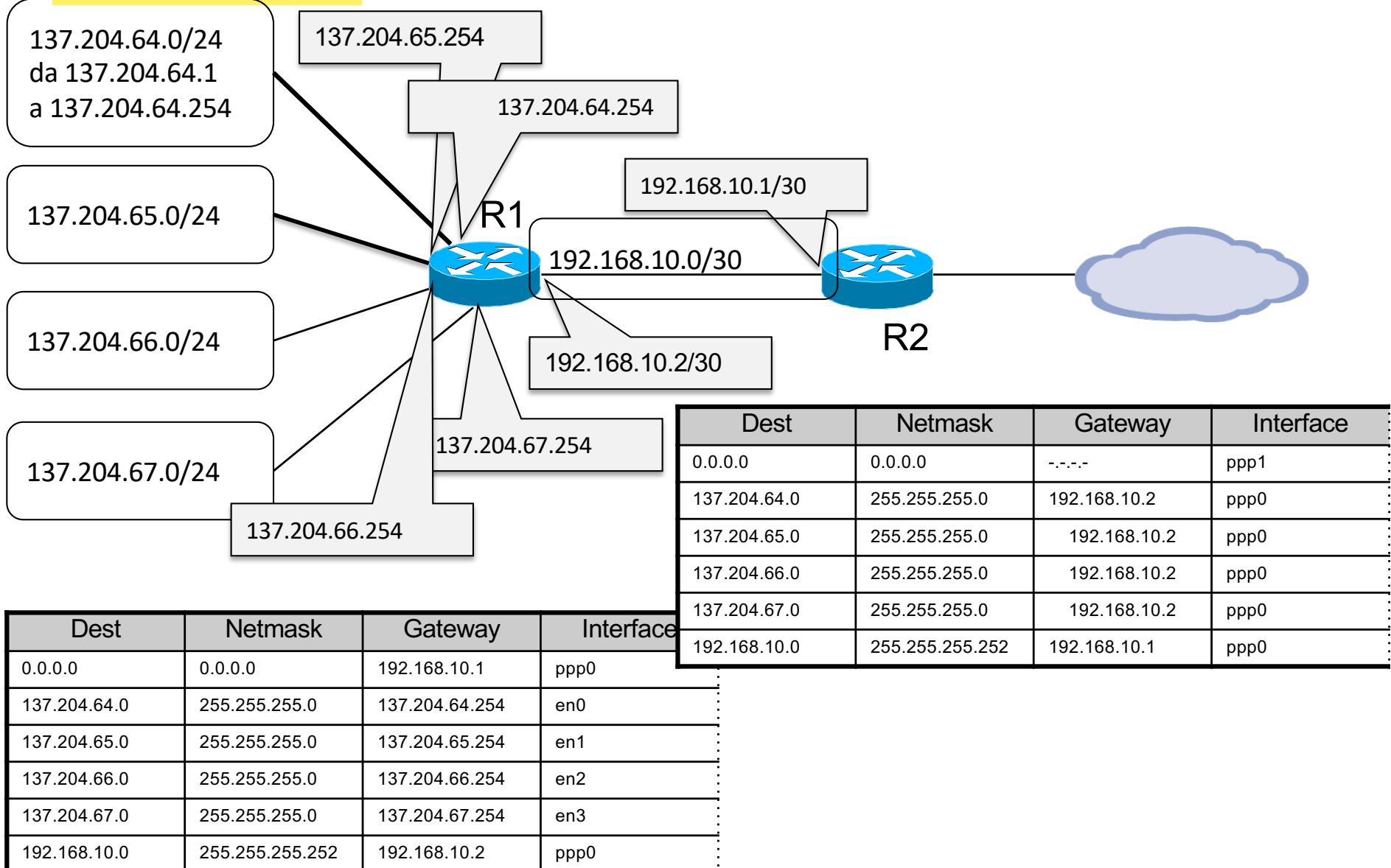


Uso del Gateway

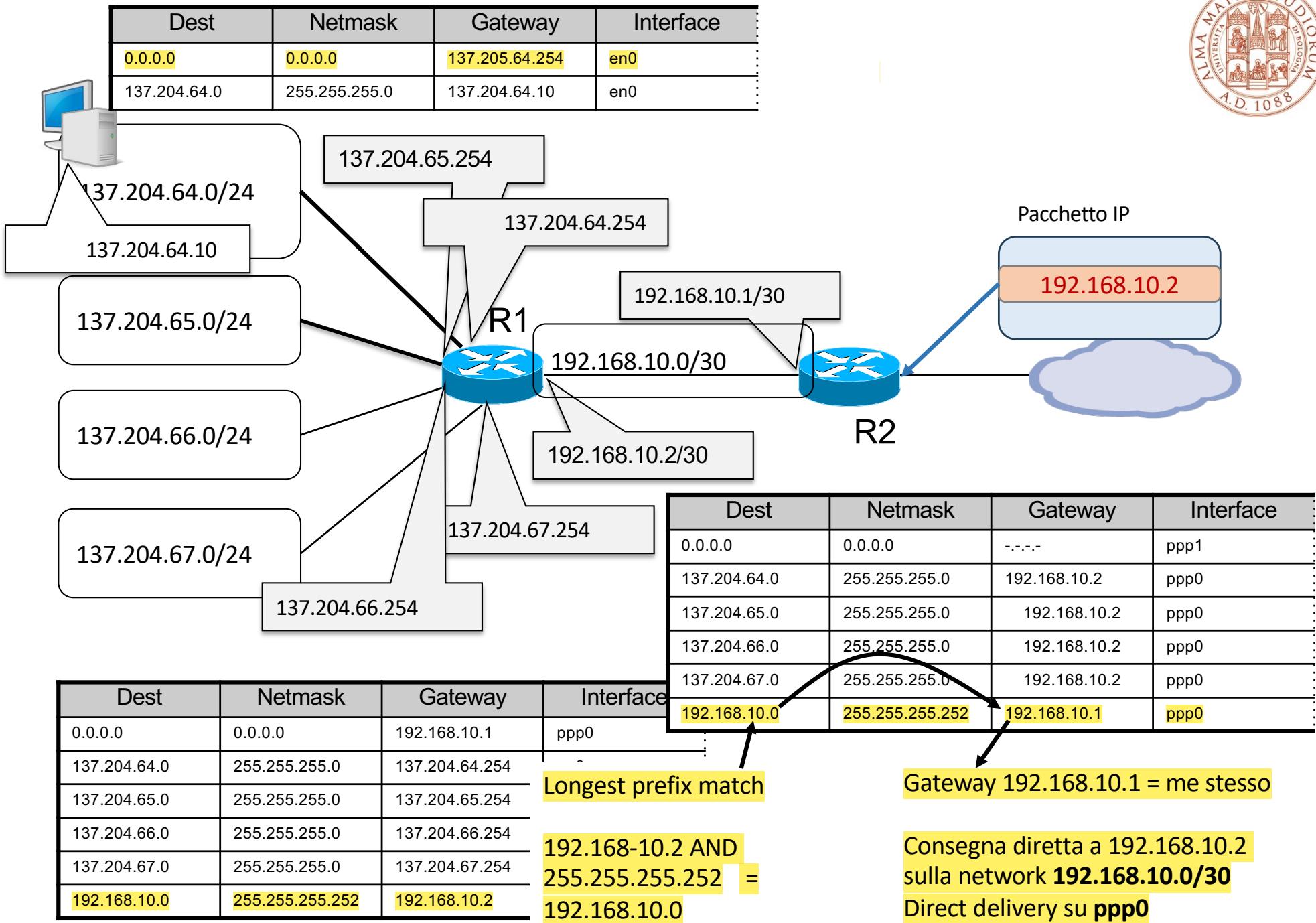
- Il campo gateway della tabella di routing serve per specificare il tipo di instradamento
 - Instradamento diretto: la sintassi dipende dall'implementazione
 - In Windows: instradamento diretto se gateway = IP locale (cioè l'IP del proprietario della tabella)
 - In Linux/Unix: instradamento diretto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

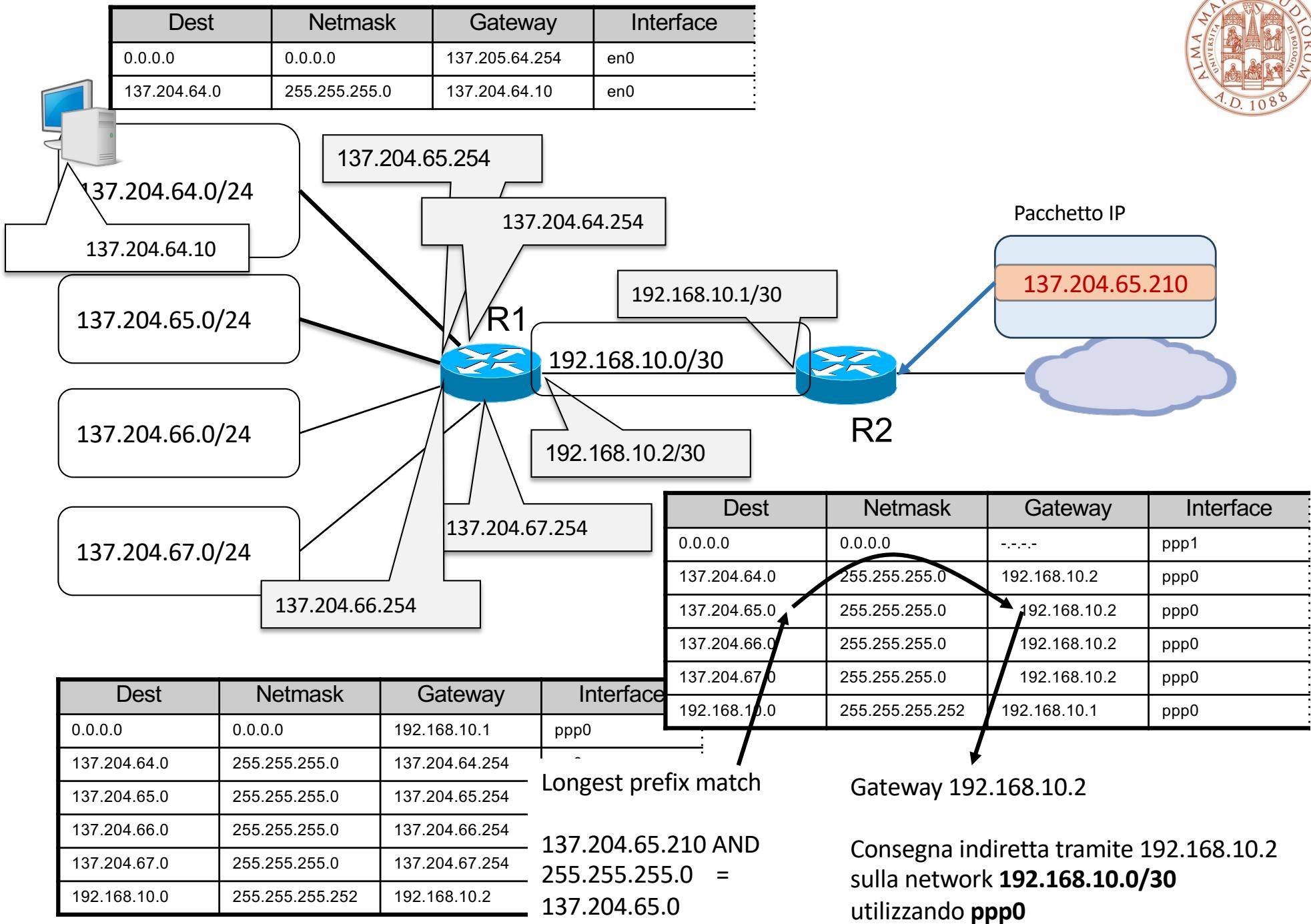


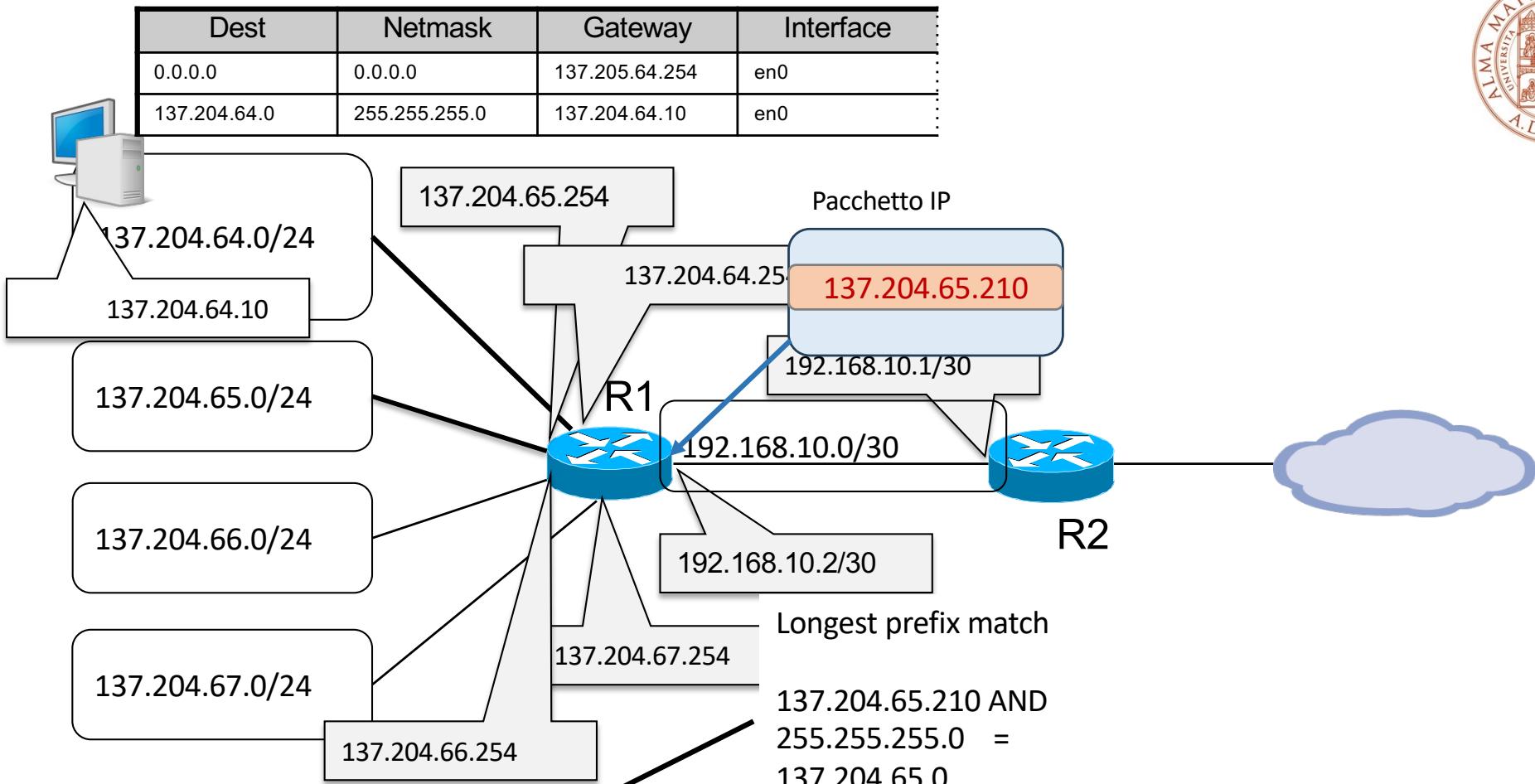
Esempio



Dalle Network più specifiche a quelle più generali (da network con meno numeri IP a network con più numeri IP)







Router R1 Routing Table:

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



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**

10001001.11001100.01000010.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000010.00000000
137 204 **66**

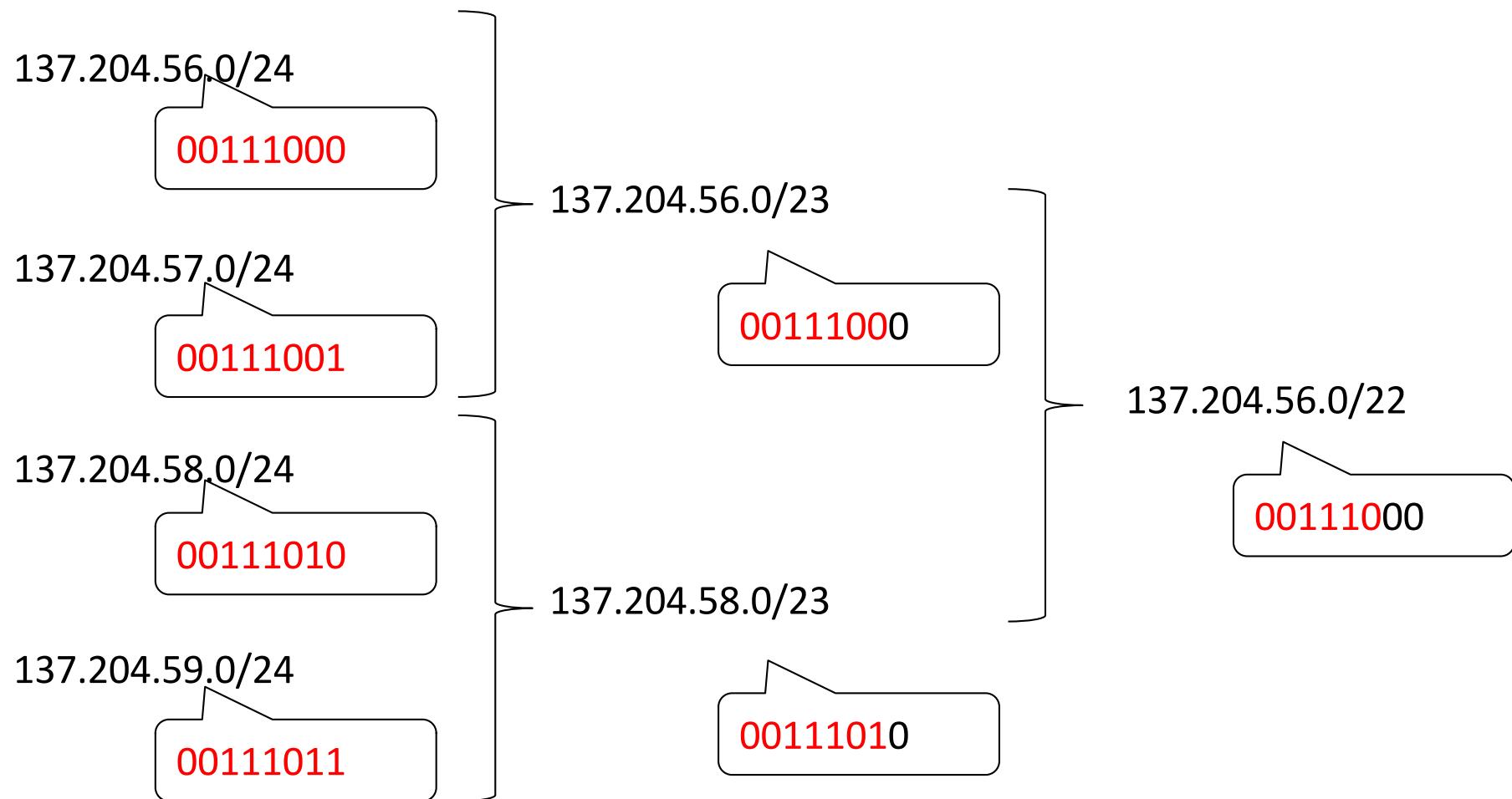
10001001.11001100.01000001.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000001.00000000
137 204 **65**

10001001.11001100.01000011.xxxxxxxx
11111111.11111111.11111100.00000000
10001001.11001100.01000011.00000000
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

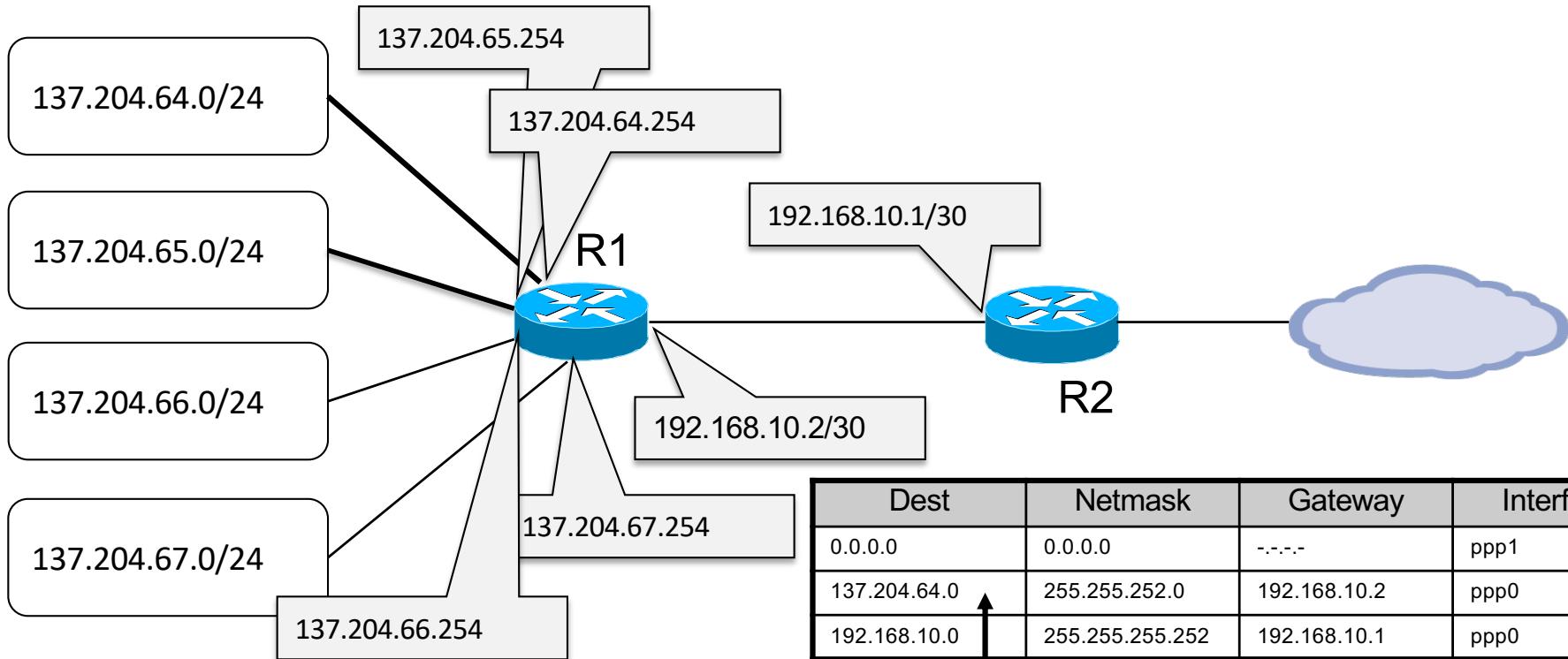




Semplificazione delle tabelle

- 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 (Cambiando la Netmask: da 255.255.255.0 a 255.255.252.0)
- 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	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

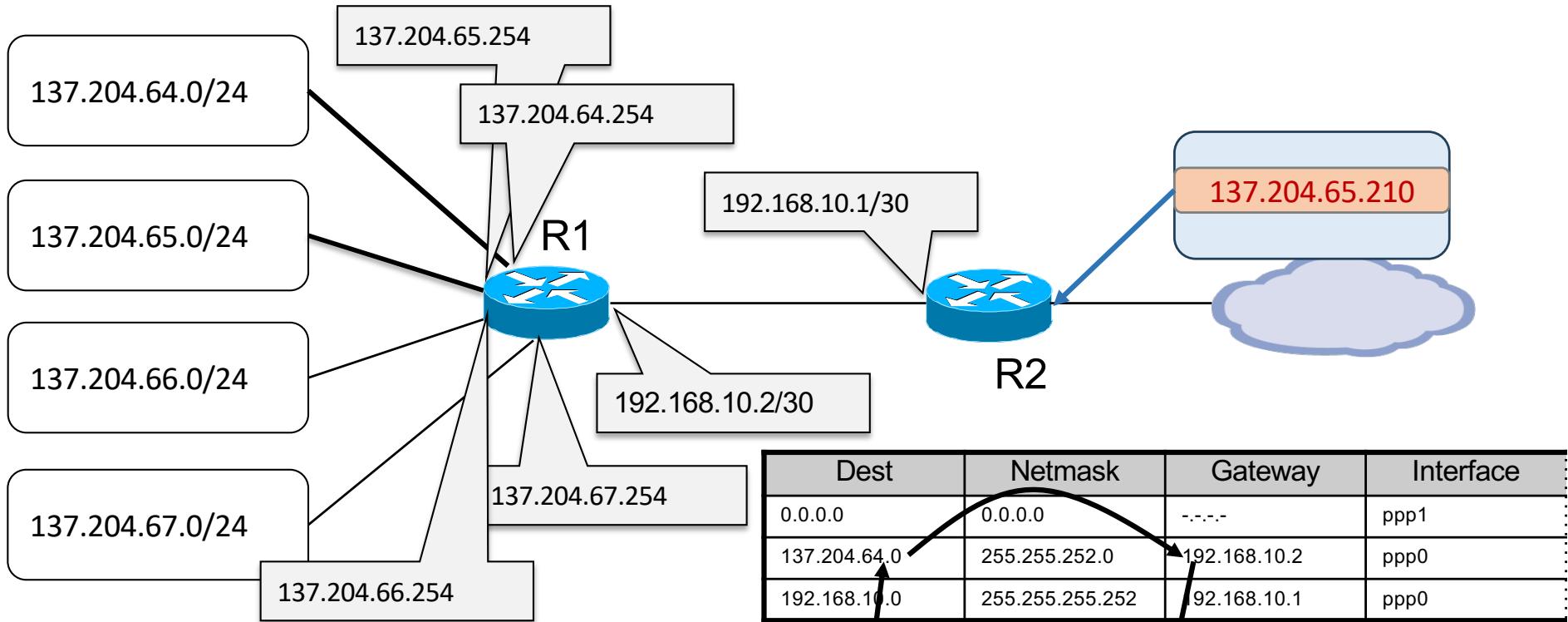
Le network

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	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

Le route con una Netmask più lunga (quindi più specifica) vengono considerate prioritarie rispetto a quelle generali.

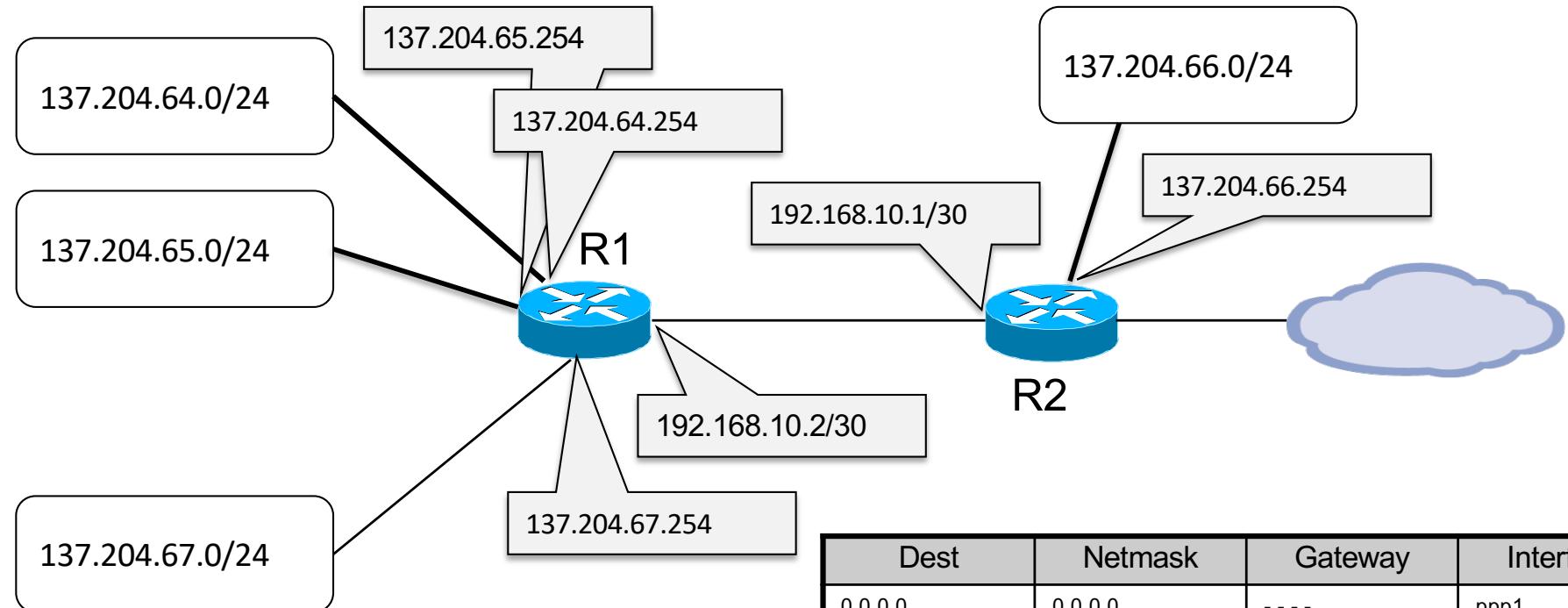
Le route nella tabella vengono organizzate in base alla lunghezza della maschera di rete, in ordine decrescente:

- Route per singoli host: La Netmask è 255.255.255.255 (/32), quindi il match è estremamente specifico.
- Route per reti piccole: La Netmask potrebbe essere, ad esempio, 255.255.255.0 (/24), che include una sottorete di 256 indirizzi.
- Route per reti grandi: La Netmask è più corta, come 255.0.0.0 (/8), e copre un range molto ampio di indirizzi.

Questo approccio assicura che, quando un pacchetto corrisponde a più route nella tabella, venga selezionata quella con il match più lungo (il "longest prefix match").

È possibile implementare regole specifiche accanto a quelle generali. Ad esempio:
Una regola generale per tutto il traffico Internet (default route: 0.0.0.0/0).
Una regola specifica per una determinata destinazione.

Eccezioni

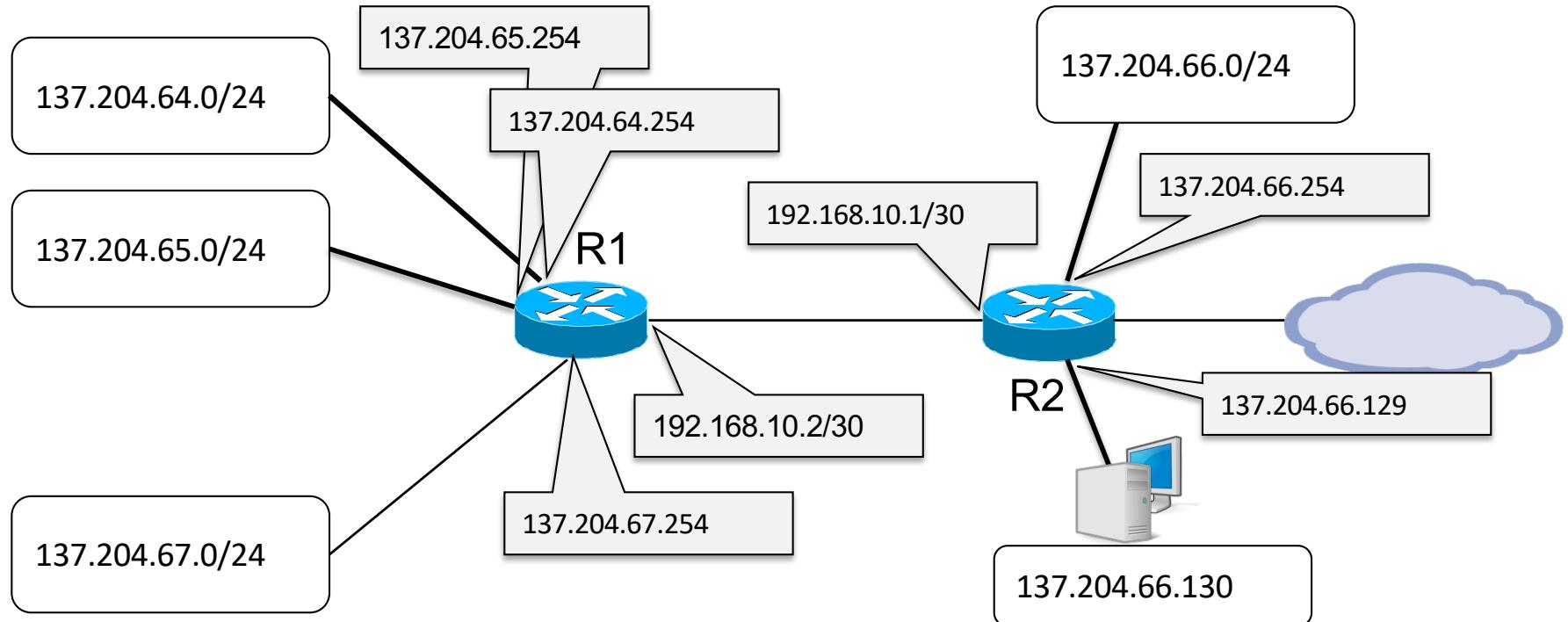


Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

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



Introduce CIDR (Classless Inter-Domain Routing), dove la subnet mask è espressa in formato prefisso (es. /24 invece di 255.255.255.0). Consente flessibilità nella suddivisione degli indirizzi IP, riducendo lo spreco grazie al subnetting e supernetting.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Classless VS Classfull

la logica degli indirizzi IP

Nella logica Classful, gli indirizzi IP sono suddivisi in tre principali classi (A, B e C) basate sul primo ottetto. Ogni classe ha una dimensione di rete e host predefinita.

Limiti:
Rigido nella struttura, portando a spreco di indirizzi IP.
Nessun concetto di subnetting.



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

In una rete, i router possono aggregare (riassumere) più reti in una singola entry nella tabella di routing. Questo permette una gestione più efficiente delle tabelle di routing.

Lo stesso indirizzo IP può essere visto con netmask diverse in base al nodo (router o dispositivo) in cui viene interpretato.

Classe delle reti

Le classi sono state introdotte per soddisfare le esigenze di reti di dimensioni diverse, assegnando blocchi di indirizzi IP in base al numero di dispositivi (host) che ogni rete avrebbe dovuto supportare:



Reti molto grandi (come reti di grandi aziende o organizzazioni governative).

Reti di medie dimensioni (università, aziende di dimensioni medie). Reti più piccole (piccole organizzazioni o uffici locali).

Questa suddivisione ha creato un modo standardizzato per distinguere tra reti grandi, medie e piccole, e facilitare il routing degli indirizzi.

- 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 Il primo bit dell'indirizzo è sempre 0. La subnet mask predefinita è 255.0.0.0 (o /8), dove i primi 8 bit identificano la rete (Net-ID).

- 10 classe B I primi due bit sono sempre 1 0. Subnet mask: 255.255.0.0 (o /16), con i primi 16 bit riservati al Net-ID.

- 110 classe C I primi tre bit sono sempre 1 1 0. Subnet mask: 255.255.255.0 (o /24), con 24 bit riservati al Net-ID.

- 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

I router utilizzano i bit iniziali di un indirizzo IP per determinare la classe e quindi estrapolare il Net-ID. Questo sistema è standard, cioè universalmente conosciuto, permettendo a tutti i dispositivi di comprendere la struttura dell'indirizzo IP.



Classi di indirizzi

I bit iniziali comunicavano al Router quanto é grande la Network ID, così da poterla identificare

Network ID

Host ID



Classe A

/8



Classe B

/16



Classe C

/24



Classe D (multicast)



Classe E (sperimentale)

32 bit

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

Gli indirizzi che iniziano con 127. sono riservati per il loopback, una funzione che consente a un dispositivo di inviare pacchetti a sé stesso.

In una rete con una specifica subnet mask, un indirizzo con tutti i bit dell'Host-ID impostati a 1 rappresenta il broadcast per quella particolare rete.

Questo indirizzo è riservato per inviare pacchetti a tutti gli host all'interno della stessa rete locale.



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

Quindi

- 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

Subnet-ID: Identifica la sottorete specifica.
Host-ID (rimanente): Identifica i dispositivi all'interno di quella sottorete.

La decisione su come suddividere una rete in sottoreti è fatta a livello locale, all'interno di un'organizzazione o amministrazione. Per il resto di Internet, l'intera rete rimane visibile come un'unità (grazie all'aggregazione delle rotte).

Scopo:

Ottimizzare l'uso degli indirizzi IP.

Separare logicamente sezioni della rete per motivi di organizzazione o sicurezza.

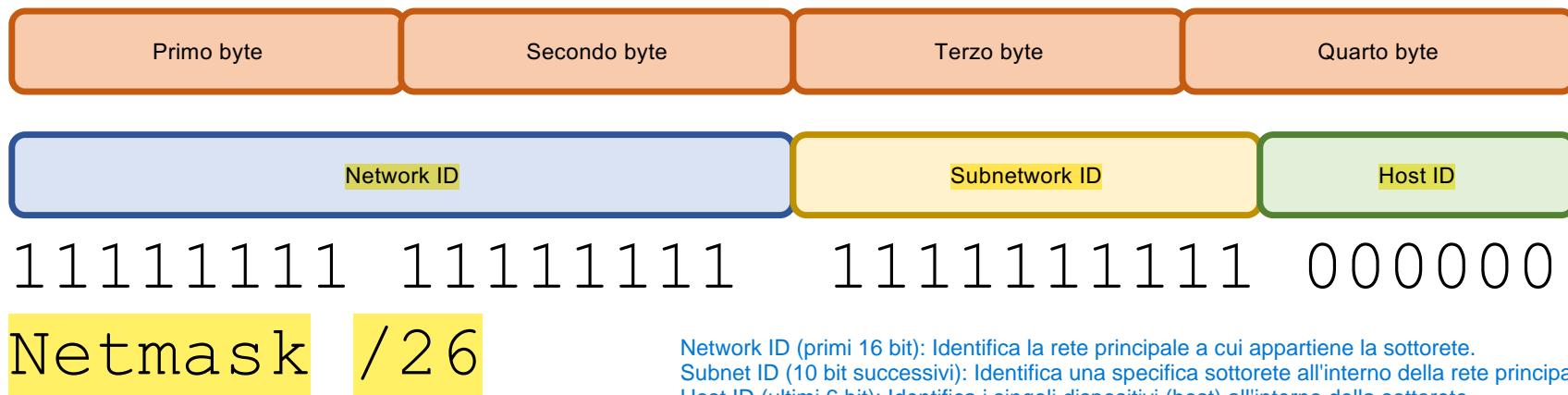
Limitare il traffico broadcast.



Subnetting

È la tecnica utilizzata per dividere una rete più grande in sottoreti più piccole e gestibili. Questa divisione avviene localmente, cioè all'interno dell'amministrazione della rete, e non è visibile dall'esterno (Internet vede ancora l'intera rete come un'unità unica).

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





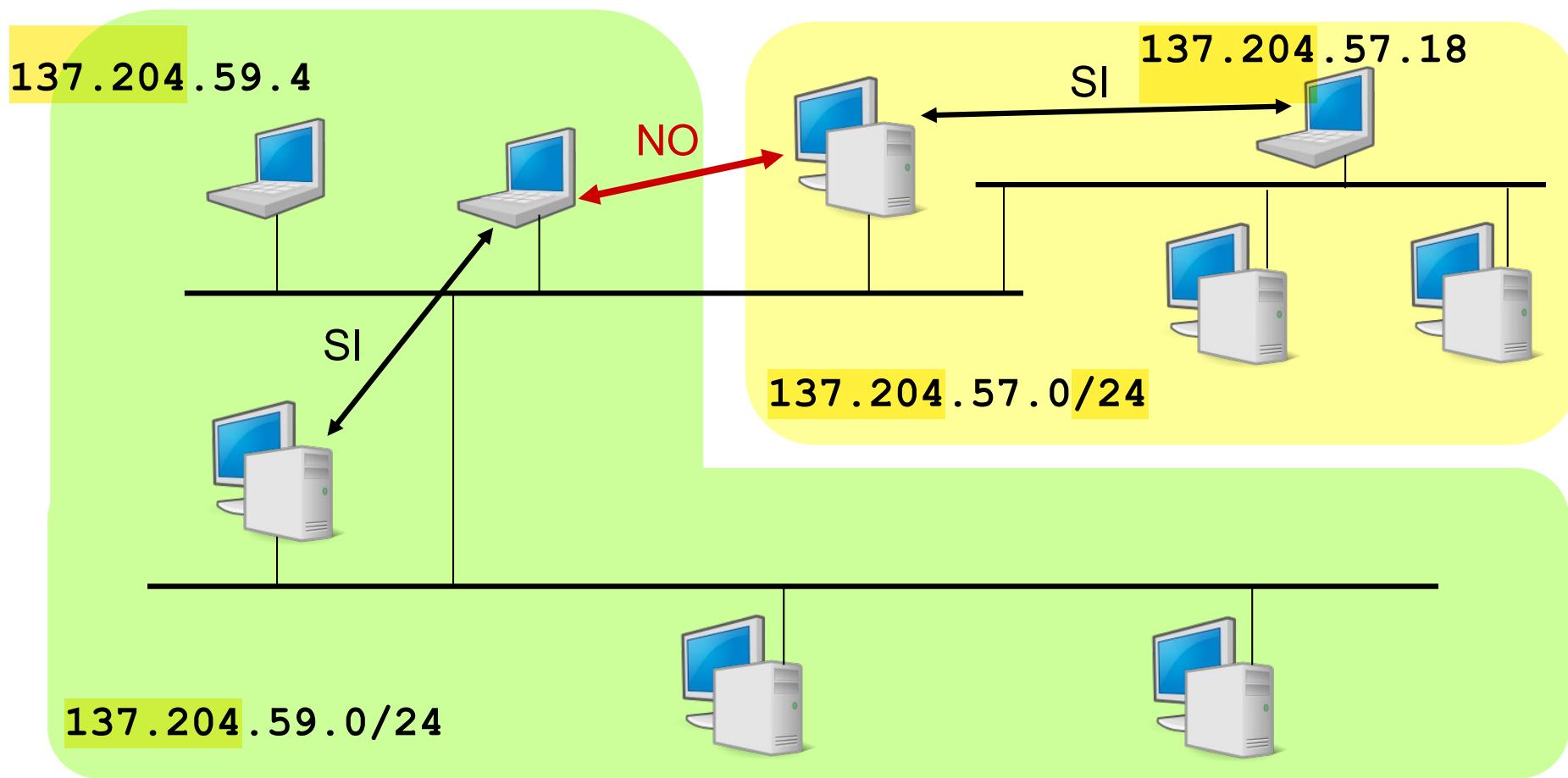
Esempio: Università di Bologna

- 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

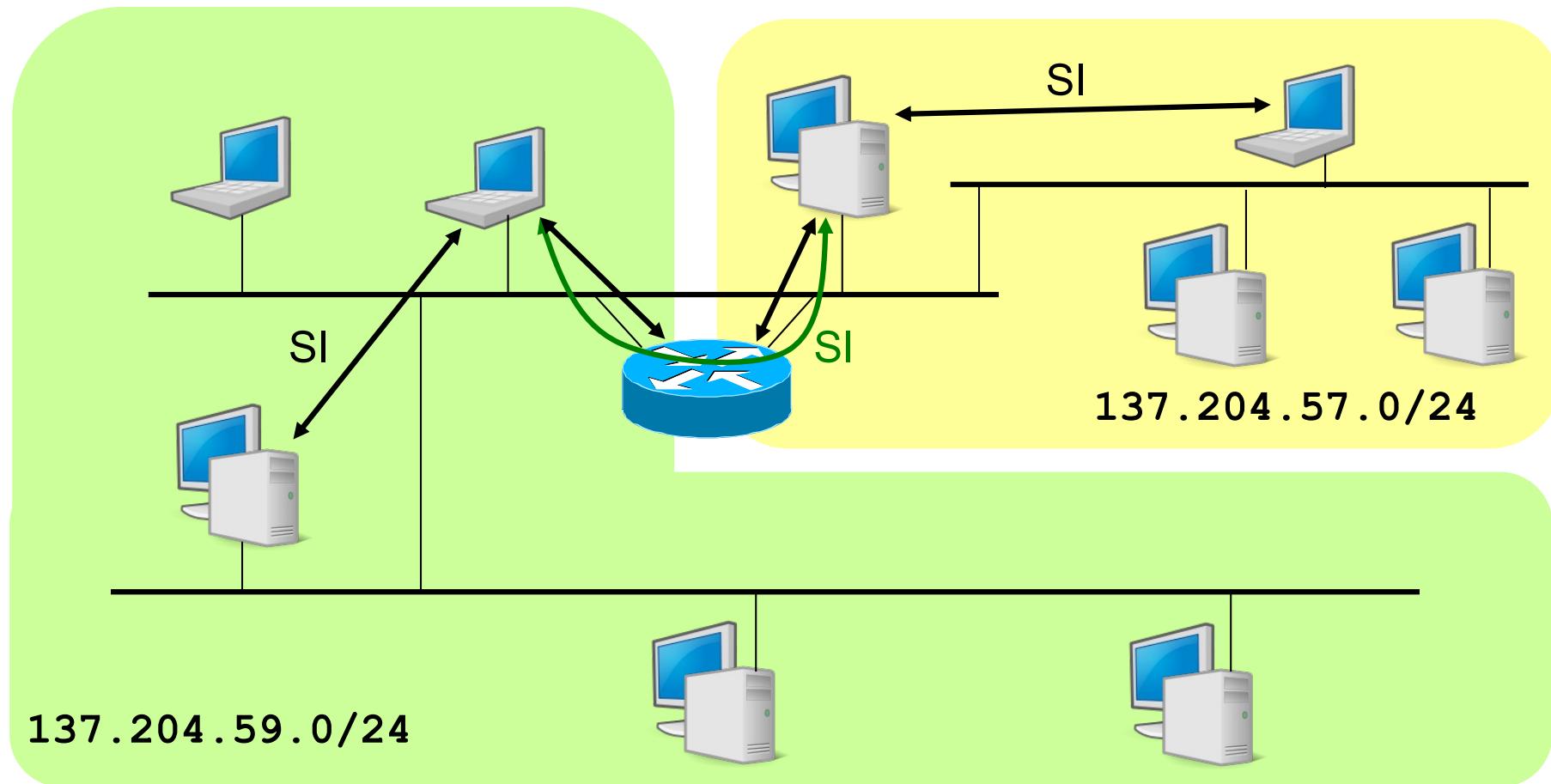
Subnetting

- 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

CIDR (definito nell'RFC 1519) è un sistema di indirizzamento IP introdotto nei primi anni '90 per risolvere i problemi legati al Classful Addressing. La necessità di un nuovo approccio è nata a causa della rigidità delle classi IP (A, B, C) che portava a uno spreco significativo di indirizzi IP.

Con il CIDR: Si rompe la rigida suddivisione in classi (Class A, B, C) e Si utilizza una netmask flessibile, rappresentata con il formato Net-ID/Prefisso, per definire in modo preciso l'ambito della rete e degli host.

- 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**

I router, per effettuare l'instradamento, devono considerare anche la Netmask associata a ciascun indirizzo IP.

- Generalizzazione del subnetting/supernetting

• reti IP definite da **Net-ID/Netmask**

Non è più necessario che un indirizzo appartenga a una specifica classe (A, B, C).

Le reti sono definite come Net-ID/Netmask.

Esempio: 192.168.1.0/24 indica che i primi 24 bit rappresentano il Net-ID e i restanti 8 bit sono usati per gli host.

→ Subnetting: Suddivisione di una rete più grande in sottoreti più piccole.
Supernetting: Aggregazione di reti adiacenti per ridurre la complessità delle tabelle di routing.



Obiettivi del CIDR

Ad esempio, una rete con 300 dispositivi può ricevere un blocco /23 (512 indirizzi), ottimizzando l'uso dello spazio IP.

- Permette di assegnare blocchi di indirizzi di dimensioni variabili, definiti da una Netmask personalizzata.
 - 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

Introduce il concetto di supernetting, ovvero la possibilità di aggregare reti contigue in una singola voce di routing (Senza CIDR, non era possibile).
 - Miglioramento di due situazioni critiche
 - Limitatezza di reti di classe A e B
 - Crescita esplosiva delle dimensioni delle tabelle di routing

L'accorpamento (supernetting) riduce il numero di rotte necessarie, aggregando più reti in un'unica voce.
- Rende l'allocazione degli indirizzi indipendente dalle classi, permettendo di assegnare blocchi più piccoli (es. /28, /30) o più grandi (/20, /18), in base alle necessità.



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 ($8 \times 256 = 2048$ 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

Supernetting ←————→ Subnetting



- 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

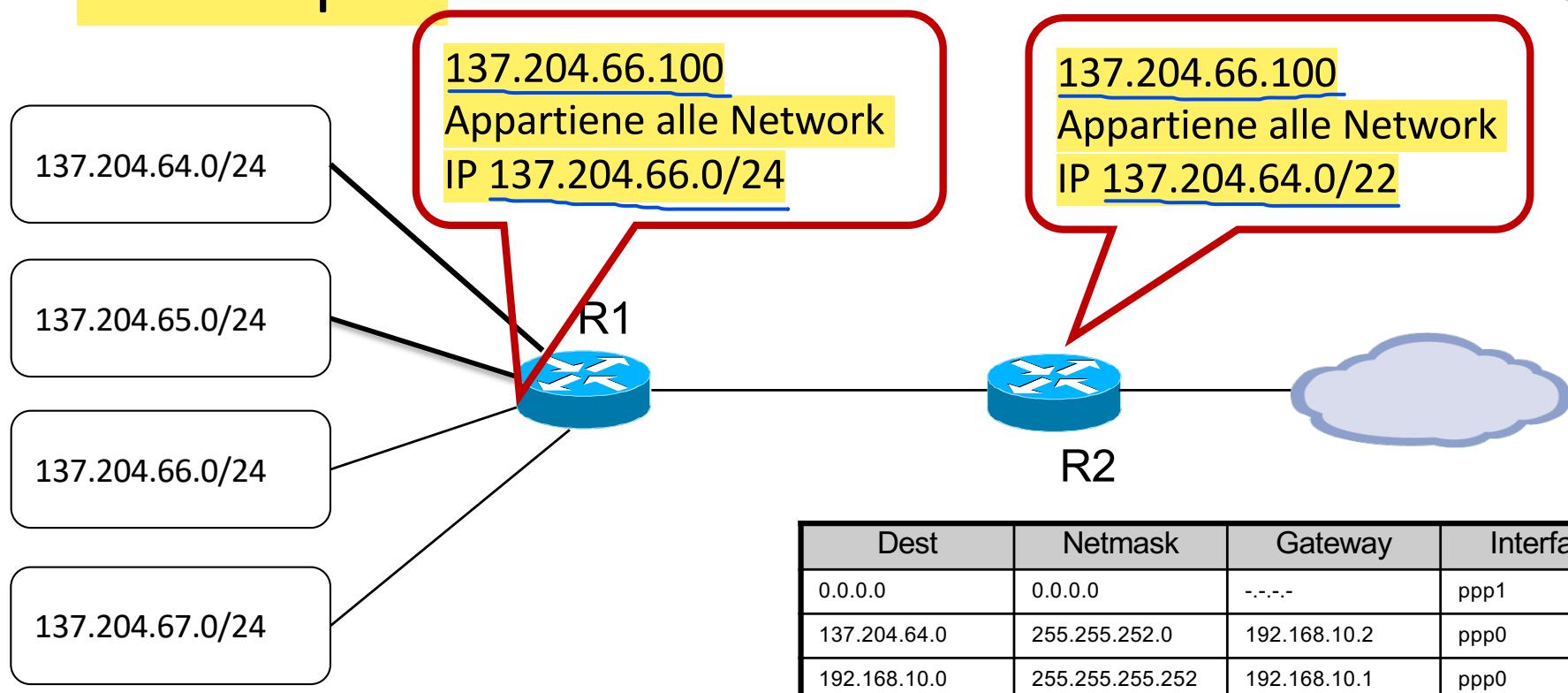


Oggi

- 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 (a causa di netmask diverse)
- Tutte le tabelle di instradamento devo contenere la colonna delle Netmask

Esempio

Stesso Indirizzo, Netmask Diverse, Interpretazioni Diverse



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

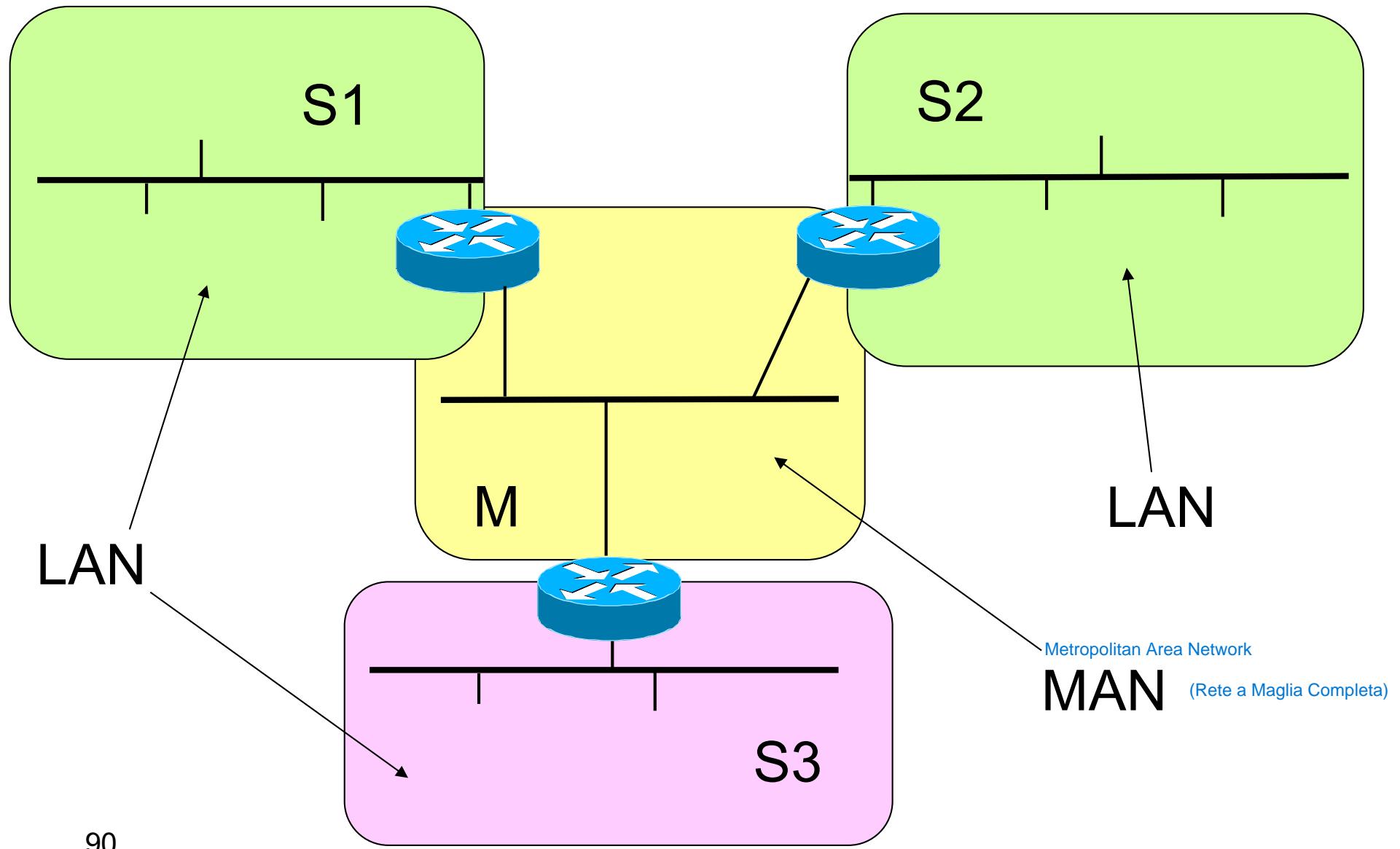
Pianificare la numerazione di reti IP



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 (a disposizione 256 indirizzi IP)

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

non 64 perché
ogni subnet ha
un indirizzo IP
per broadcast
(Host-ID tutti a 1)
e network (Host-
ID tutti a 0)

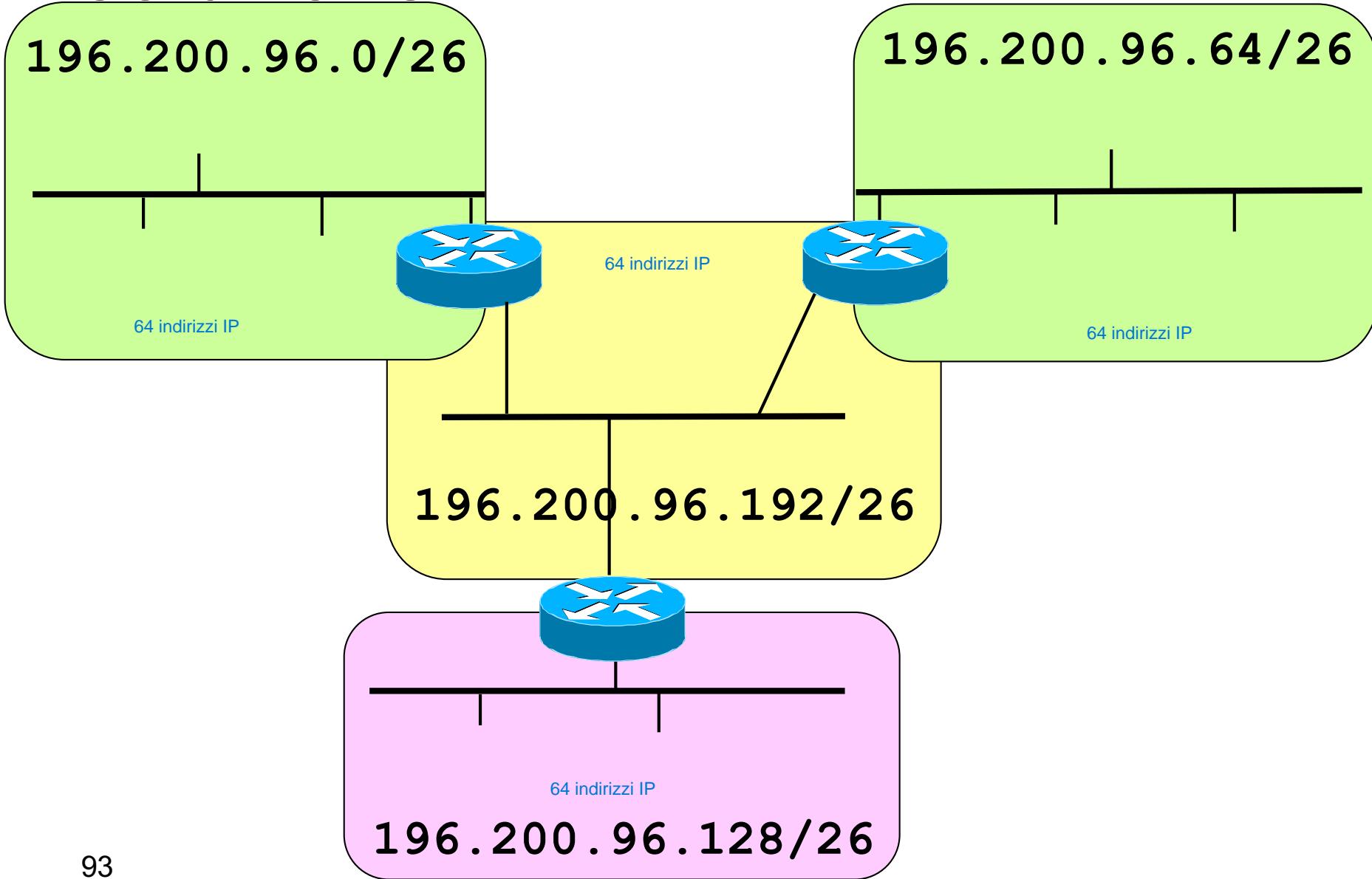


Soluzione 1

- 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

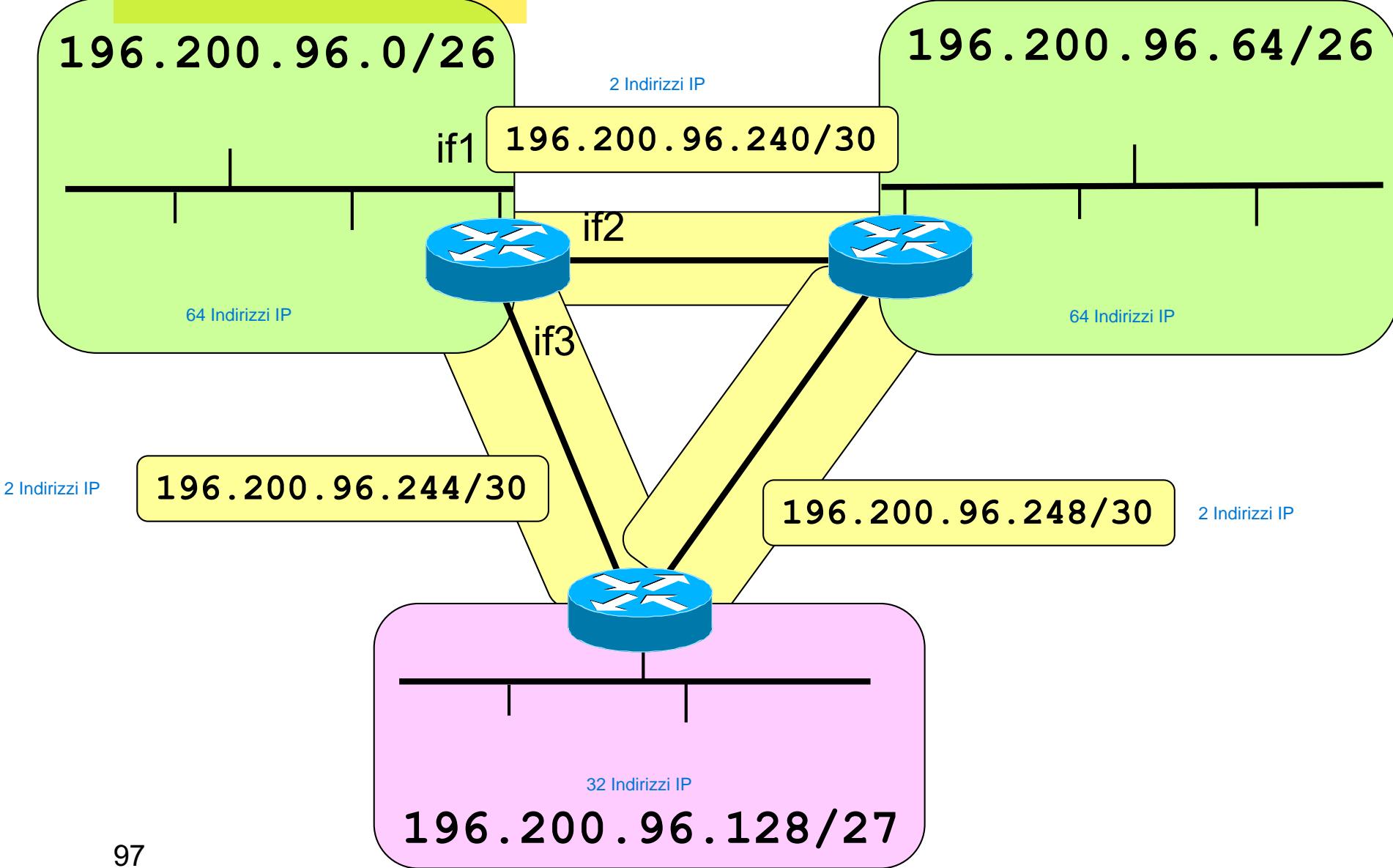
Soluzione 2

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



Ho cambiato l'architettura della rete centrale tra le 3 reti, risparmiando 58 indirizzi IP
Inoltre, aumento la netmask di 1 della Network sotto e risparmio altri 32 Indirizzi IP

Soluzione 2





ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Il protocollo ICMP

Il protocollo IP ...

Il protocollo IP tenta di consegnare i dati nella rete nel miglior modo possibile ("best effort"), ma non garantisce:

La consegna dei pacchetti (potrebbero andare persi).
L'ordine dei pacchetti ricevuti (potrebbero arrivare in un ordine diverso da quello di invio).
L'assenza di errori nei dati trasmessi.

- 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) (quindi non fa rilevazione e correzione di errore)
 - 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 si limita a segnalare errori o malfunzionamenti; non corregge problemi.

È un protocollo di controllo utilizzato per comunicare errori, avvisi e informazioni diagnostiche relative alla rete.

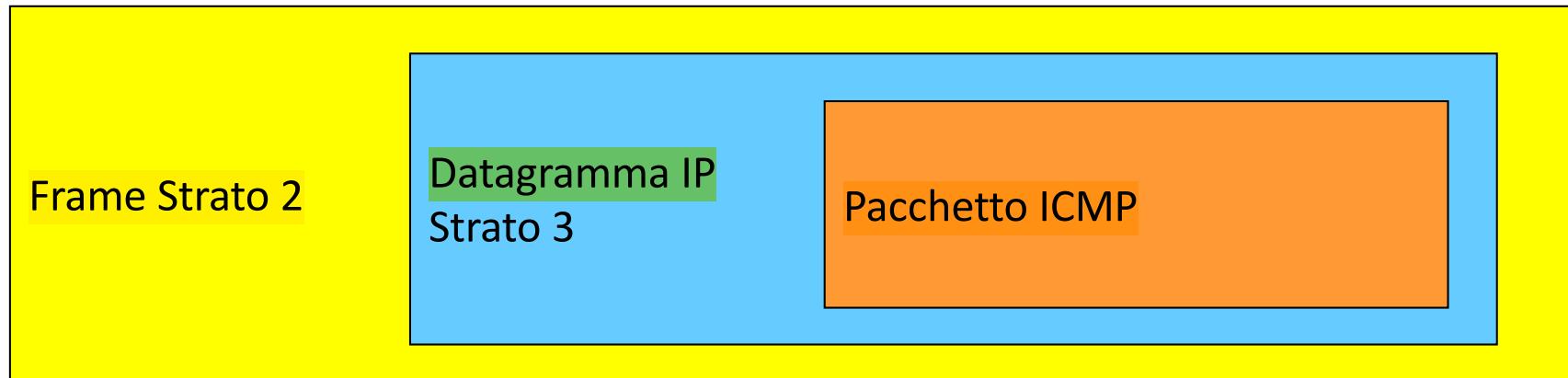


ICMP

Permette a dispositivi di rete (router, host) di segnalare errori, anomalie o fornire informazioni diagnostiche. È essenziale per la gestione e il monitoraggio delle reti.

- **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
Message Type
Message Code
Checksum
Additional Fields (optional)
Data

20 - 60 byte

1 byte

1 byte

2 byte

per verificare che non sia stato corrotto durante la trasmissione.

variabile

variabile

Type

definisce il tipo di messaggio ICMP

- messaggi di errore
- messaggi di richiesta di informazioni

come "Echo Request" o "Echo Reply" (usati da ping).

Code

descrive il tipo di errore e ulteriori dettagli

Controlla l'integrità del messaggio ICMP.

Checksum

controlla i bit errati nel messaggio ICMP

Add. Fields

dipendono dal tipo di messaggio ICMP

Campo opzionale che contiene informazioni aggiuntive, a seconda del tipo di messaggio.

Data

intestazione e parte dei dati del datagramma

IP

che ha generato l' errore

Include i dati originali del datagramma IP che ha causato l'errore.
Questo aiuta il mittente a identificare quale pacchetto ha generato il problema.



Tipi di errori

Questo messaggio ICMP viene generato quando un dispositivo (router o host) non è in grado di inoltrare un pacchetto verso la destinazione prevista.

- **Destination Unreachable (Type = 3)**

- Generato da un gateway quando la sottorete o l'host non sono raggiungibili Non esiste un percorso valido verso la destinazione.
- Generato da un host quando si presenta un errore sull'indirizzo dell'entità di livello superiore a cui trasferire il datagramma L'applicazione o il protocollo di livello superiore non può essere raggiunto

- Codici errore di Destination Unreachable

- 0 = sottorete non raggiungibile
- 1 = host non raggiungibile
- 2 = protocollo non disponibile L'host di destinazione non supporta il protocollo specifico richiesto dal pacchetto
- 3 = porta non disponibile L'host di destinazione ha ricevuto il pacchetto, ma la porta specifica non è aperta o non è in ascolto.
- 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)
 - Viene inviato quando un dispositivo riceve pacchetti a una velocità superiore a quella che può gestire, causando un sovraccarico. Il messaggio notifica al mittente di ridurre la velocità di trasmissione per prevenire ulteriori congestioni.
- 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 Echo
 - la destinazione deve rispondere immediatamente Echo Reply
 - 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 Identifica il set di messaggi Echo che appartengono allo stesso test.
Utile per distinguere richieste e risposte in caso di test multipli simultanei.
 - Sequence Number: identifica ciascun echo nell'insieme Fornisce un numero progressivo per ciascun messaggio Echo.
Aiuta a rilevare pacchetti persi o ricevuti fuori ordine.
 - 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 = $T_{Transmit} - T_{Receive}$

Tempo di andata: Receive Timestamp - Originate Timestamp

Tempo di ritorno: Transmit Timestamp - Receive Timestamp

Tempo totale di andata e ritorno (RTT): Transmit Timestamp - Originate Timestamp



Informazioni

Questo messaggio viene inviato da un host per richiedere la subnet mask (maschera di rete) da utilizzare per la configurazione IP.
Generalmente viene inviato in broadcast all'indirizzo 255.255.255.255.
Utilizzo:
È spesso utilizzato in reti dove l'host ha già ottenuto il proprio indirizzo IP tramite protocolli come RARP o BOOTP, ma non conosce ancora la subnet mask.

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

Questo messaggio è la risposta a una richiesta Address Mask.
Contiene la subnet mask che l'host deve utilizzare.

Router Solicitation (Type = 10)

- Router Advertisement (Type = 9)

utilizzato per localizzare i router connessi alla rete

Gli host utilizzano questo messaggio per scoprire quali router sono disponibili nella rete locale.
Inviato dagli host all'indirizzo multicast o broadcast per cercare router nelle vicinanze.

Utilizzo:
È utile per gli host che vogliono configurarsi automaticamente, ad esempio, per conoscere il router predefinito.

I router rispondono a una Router Solicitation con un messaggio di Router Advertisement.
Questo messaggio include:
L'indirizzo del router.
Informazioni aggiuntive come il tempo di validità per l'indirizzo del router come gateway.



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

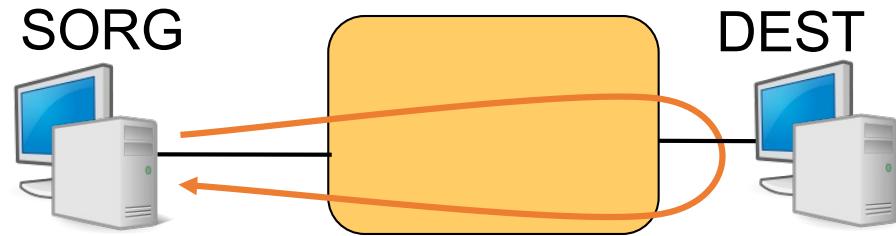
Applicazioni di ICMP



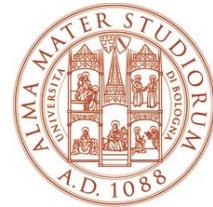
Comando PING

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**
Ctrl-C esegue **ping** finché interrotto con

• **-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

Traduce l'indirizzo IP nel relativo nome DNS (se disponibile).
Esempio: ping -a 8.8.8.8 potrebbe restituire un nome come dns.google.

Specifica un timeout in millisecondi per attendere una risposta (rispetto al valore predefinito).
Esempio: ping -w 5000 8.8.8.8 aspetta al massimo 5 secondi per la risposta.

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

Risposta da 8.8.8.8: byte=32 durata=20ms
TTL=117
Risposta da 8.8.8.8: byte=32 durata=22ms
TTL=117
Risposta da 8.8.8.8: byte=32 durata=19ms
TTL=117

Statistiche:
Pacchetti: Inviati = 4, Ricevuti = 4, Persi = 0 (0% persi)
Tempo approssimativo in millisecondi:
Minimo = 19ms, Massimo = 22ms, Medio = 20ms

Comando PING – Output

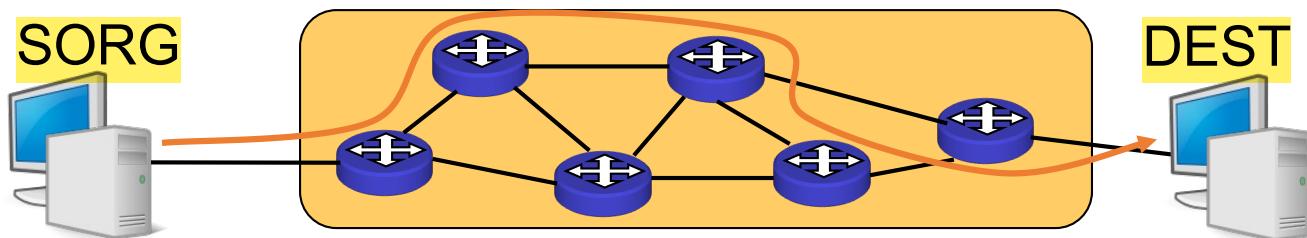
L' output mostra

- la dimensione del pacchetto “echo reply”
- l' indirizzo IP di DEST
- il numero di sequenza della risposta
(solo UNIX-LINUX) ogni pacchetto è numerato con un ID sequenziale per identificare l'ordine delle risposte ricevute.
- 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** Questo messaggio contiene l'indirizzo IP (e, se possibile, il nome DNS) del router.
- SORG costruisce una lista dei nodiattraversati fino a DEST
- L'output mostra il **TTL**, il nome **DNS** e l'indirizzo **IP** dei nodi intermedi ed il **ROUND-TRIP TIME (RTT)**

Traccia instradamento verso google.com [142.250.74.206]
su un massimo di 30 punti di passaggio:

1 <1 ms <1 ms <1 ms 192.168.1.1
2 5 ms 6 ms 5 ms 10.0.0.1
3 14 ms 15 ms 14 ms ae1-1120.edge1.milano1.level3.net [4.68.37.201]
4 20 ms 19 ms 19 ms 142.250.74.206

Non tutti gli indirizzi IP
hanno il nome DNS



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**

Un ALG o Proxy opera a livello applicativo del modello OSI (livello 7) per analizzare e controllare il traffico di rete.

 - Controlla la comunicazione a livello applicativo
- **Firewall**

Un firewall combina funzionalità di packet filtering, ALG, e altre tecnologie per proteggere una rete.
Funziona come una barriera tra una rete privata (interna) e una rete esterna (come Internet), consentendo solo traffico autorizzato.

 - Combinazione dei dispositivi descritti sopra
 - Protegge le risorse interne da accessi esterni
- **Network Address Translator (NAT)**

Traduce gli indirizzi IP privati utilizzati all'interno di una rete locale (LAN) in un indirizzo IP pubblico utilizzato per comunicare su Internet.

 - Riduce la richiesta dello spazio di indirizzamento Internet
 - Nasconde gli indirizzi IP interni
 - Esegue un packet filtering per il traffico sconosciuto



Fornisce in modo dinamico i parametri di rete ai dispositivi connessi (host), senza la necessità di configurazione manuale.

DHCP – RFC 2131,2132

Dynamic Host Configuration Protocol

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

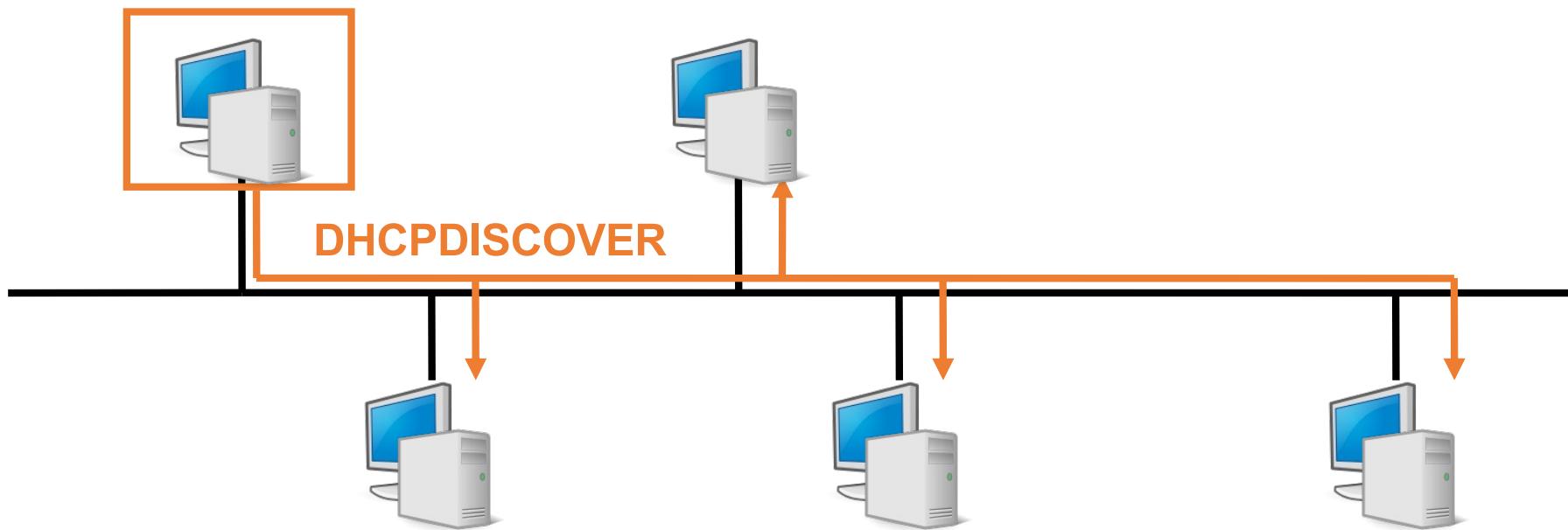
- Indirizzo IP L'IP è assegnato per un determinato periodo di tempo (detto lease).
- Netmask Specifica la dimensione della rete. Serve per distinguere la parte di rete dall'indirizzo e la parte dedicata agli host.
- Broadcast L'indirizzo per inviare pacchetti a tutti i dispositivi sulla rete (esempio: 192.168.1.255 in una rete 192.168.1.0/24).
- Host name Alcuni server DHCP possono assegnare un nome host al dispositivo, che può essere utile per la risoluzione dei nomi in reti locali.
- Default gateway Specifica il router predefinito che permette ai dispositivi di accedere a reti esterne
- Server DNS Indica quali server Domain Name System (DNS) utilizzare per risolvere i nomi di dominio (esempio: tradurre "google.com" nell'indirizzo IP 142.250.74.206).

Server su porta **67 UDP**

- Ascolto delle richieste dei client: Il server DHCP rimane in ascolto sulla porta 67 UDP per rilevare i messaggi inviati dai client DHCP che necessitano di configurazione di rete.
- Invio delle risposte: Il server utilizza la stessa porta 67 per inviare i messaggi di configurazione ai client DHCP.

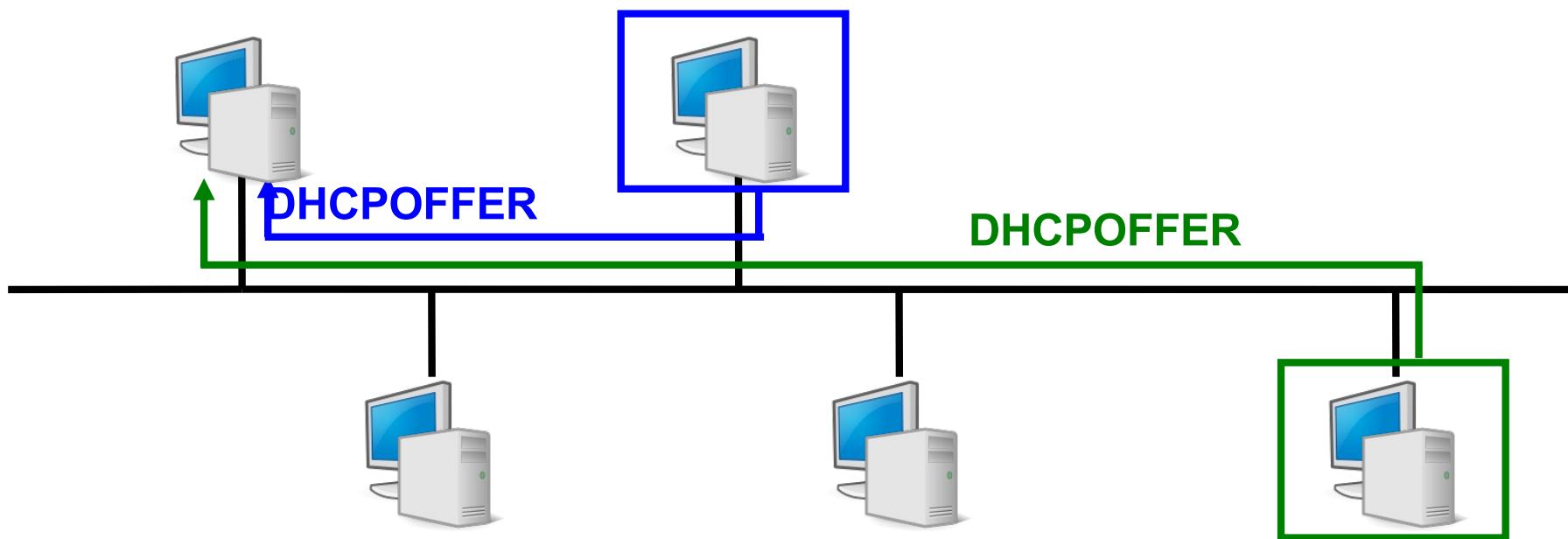
DHCP – 1

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



DHCP – 2

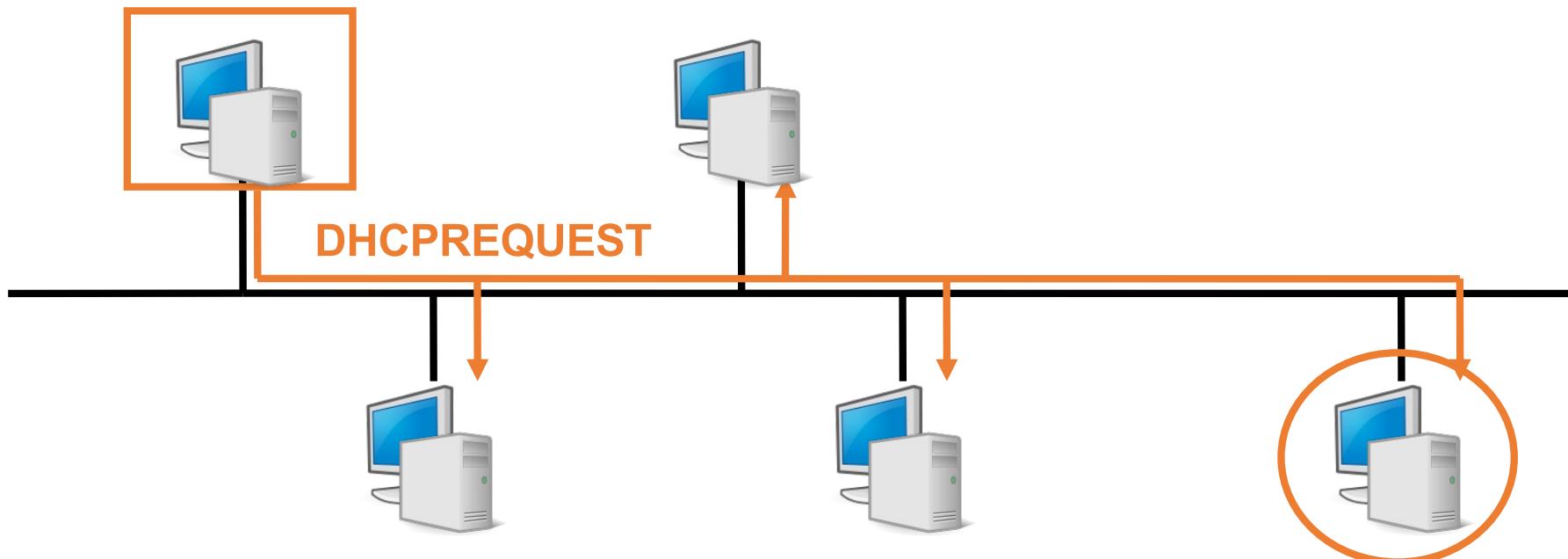
- Ciascun server DHCP presente risponde all'host con un messaggio **DHCPOFFER** con cui propone un indirizzo IP



DHCP – 3

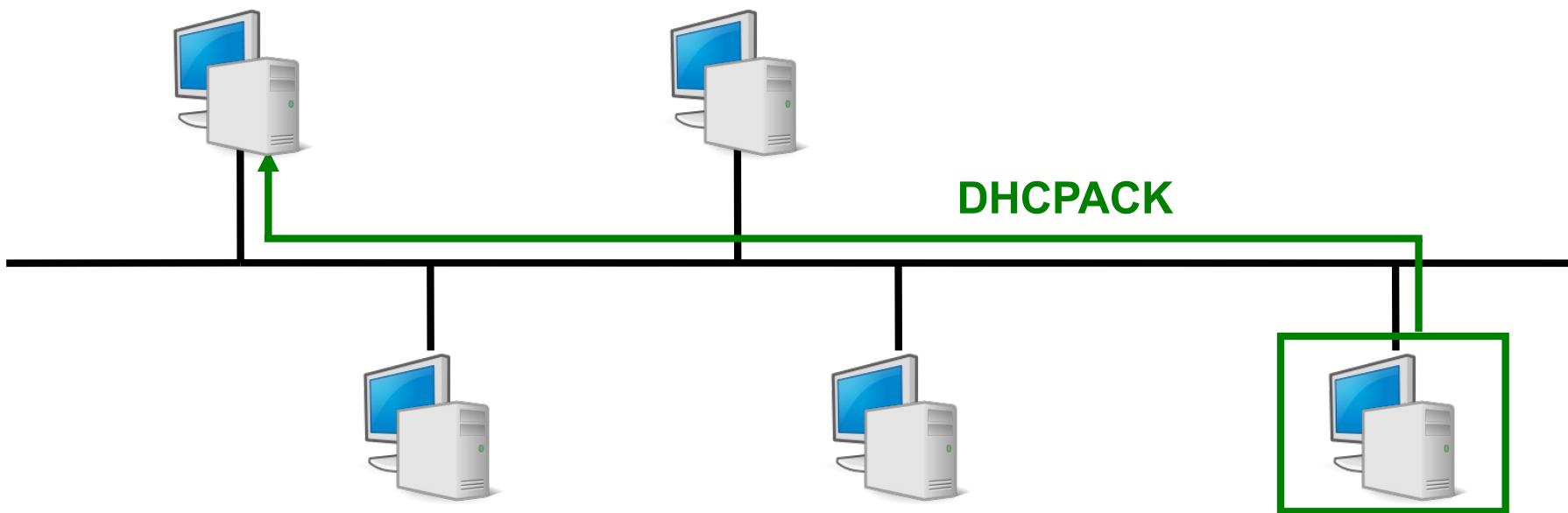
(DHCPREQUEST mandato in modalità broadcast per informare a TUTTI i server DHCP che il client ha selezionato un server specifico)

- 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

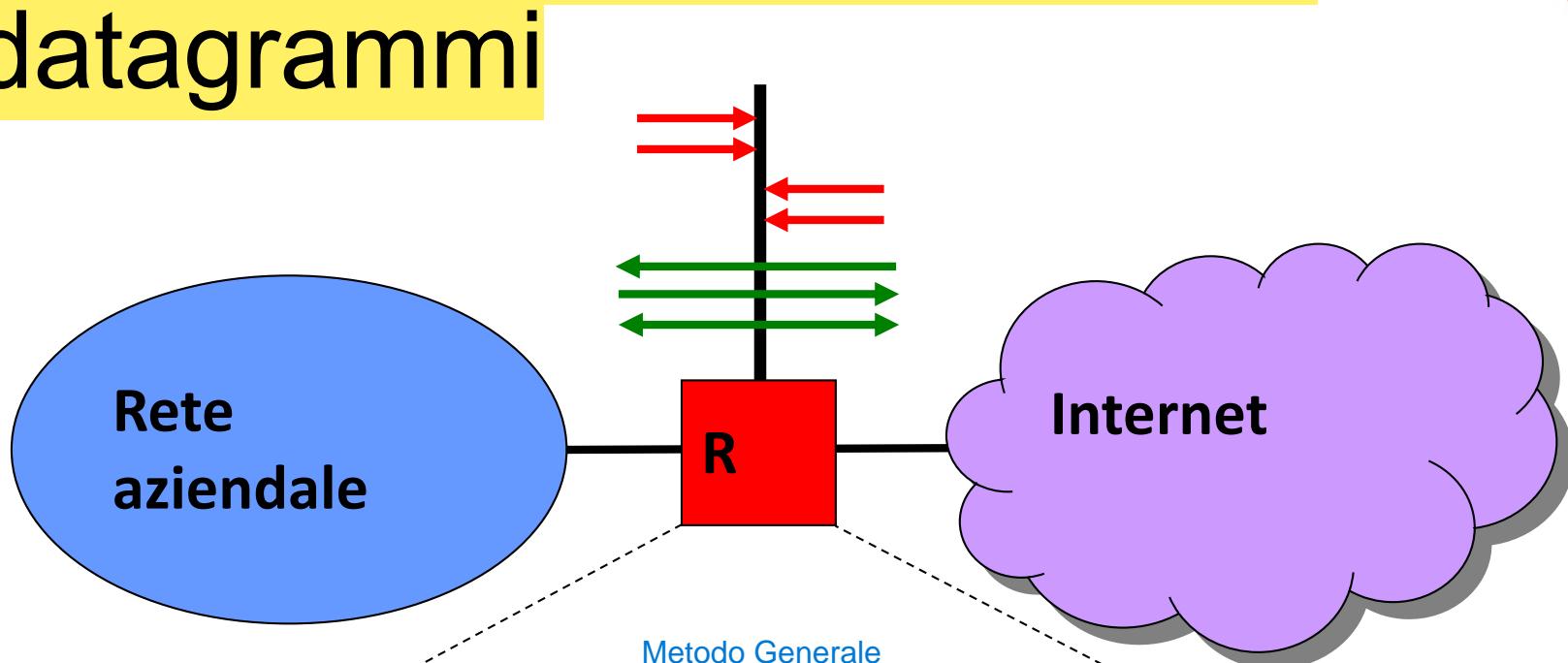
- Un'analisi dettagliata del protocollo DHCP che include:
 - Esempi operativi
 - Catture di traffico
- Si può trovare su virtuale



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Packet Filter e Firewall

Metodologie di filtraggio dei datagrammi



Packet Filtering e Stateful Packet Inspection sono considerate tecniche di filtraggio del traffico di rete, non dei nodi di rete. Vengono implementate tipicamente su dispositivi che fungono da gateway/router/firewall tra diverse reti. Il PROXY è un dispositivo di rete che implementa specifiche tecniche di filtraggio del traffico di rete e protezione. Un proxy si comporta come un intermediario tra un client e un server, gestendo direttamente le comunicazioni a livello applicativo.

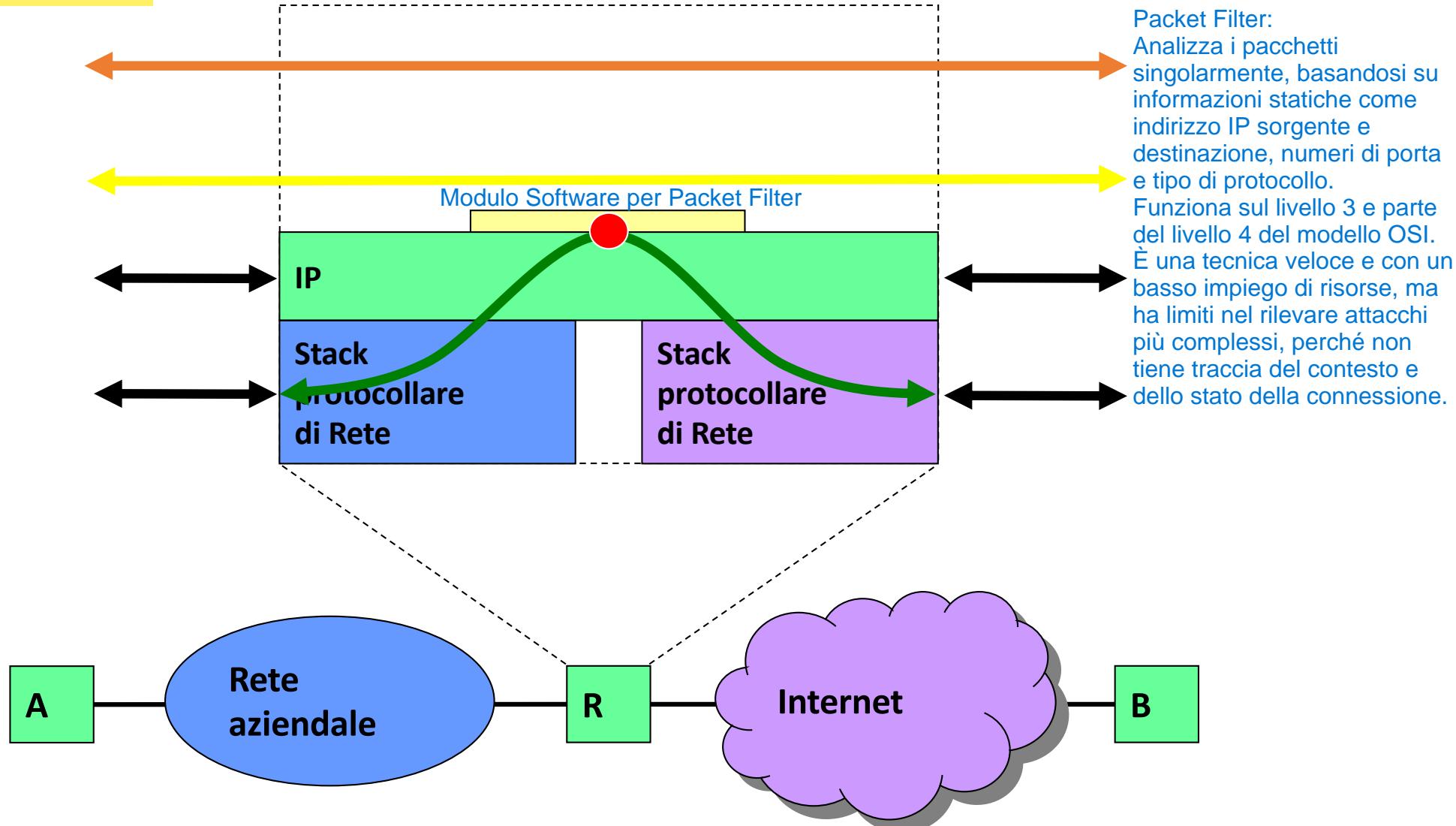
Impostazioni del Packet Filter

Si decide su cosa far passare e cosa non:

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

Può essere configurato dinamicamente

Instradamento selettivo: packet filter



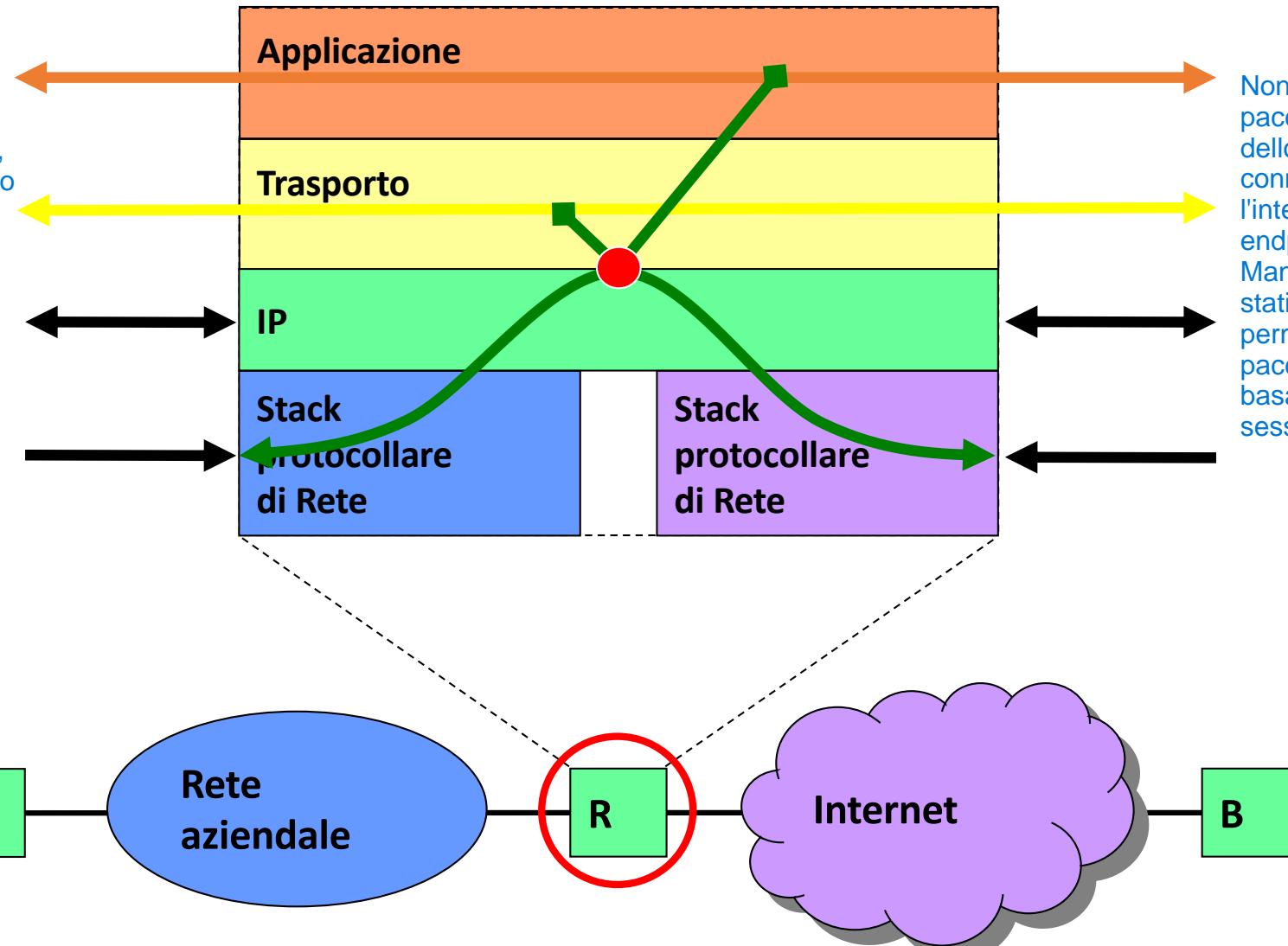


Prende informazioni dai livelli superiori, leggendo Header, però non conosce la semantica dei protocolli superiori: per questo è in grado di leggere solo Header, non il payload (dati)

2

Stateful Packet Inspection

A differenza del semplice "Packet Filtering", lo SPI tiene traccia dello stato delle connessioni attive. Legge le informazioni dai livelli superiori dello stack, ovvero dal livello Trasporto e, dal livello Applicativo. Il modulo è in grado di leggere gli header dei pacchetti fino a questi livelli, per determinare se un pacchetto fa parte di una connessione già esistente o è una nuova connessione, ma non comprende la semantica dei protocolli di livello superiore al livello 4.

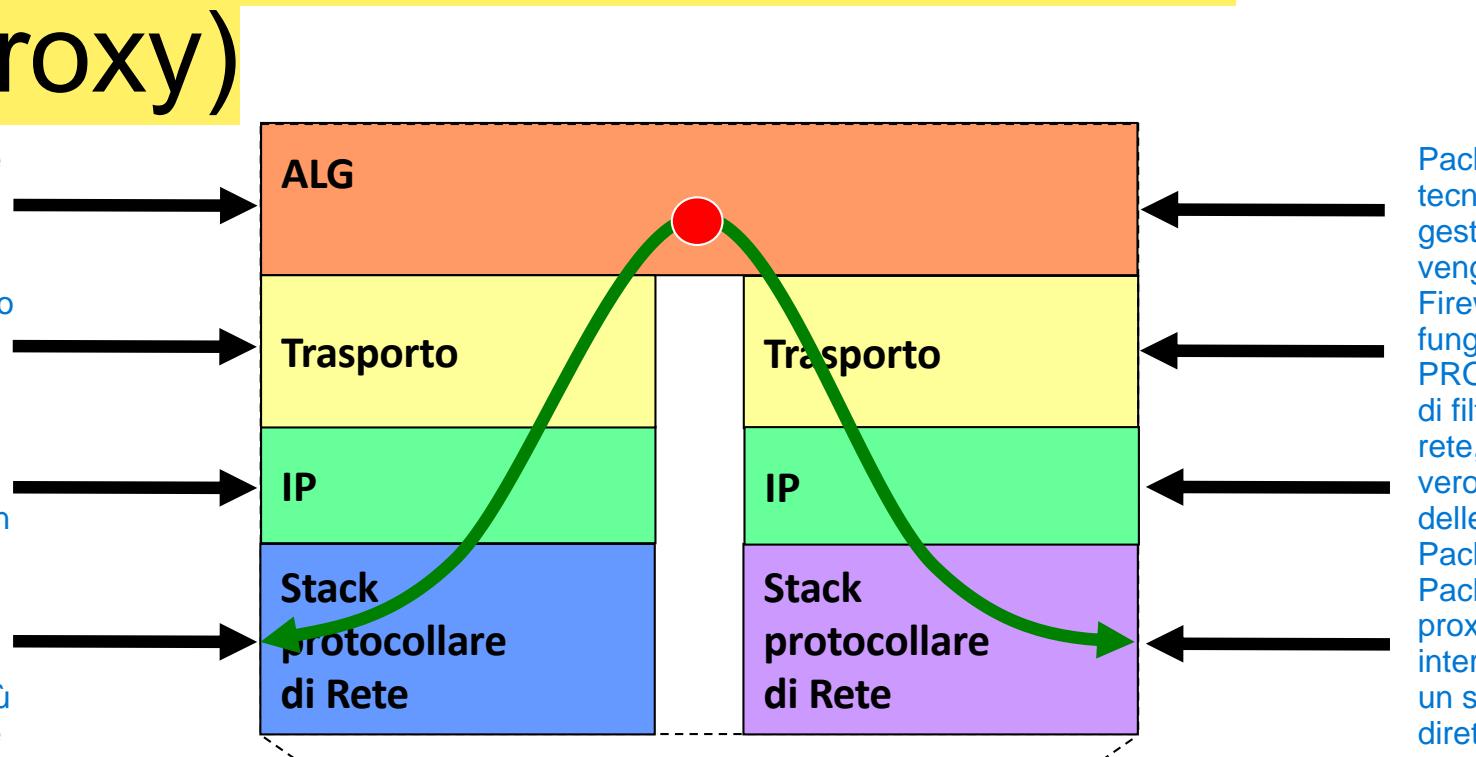


Non solo esamina i pacchetti, ma tiene traccia dello stato della connessione, monitorando l'intero flusso di dati tra due endpoint.
Mantiene una tabella degli stati delle connessioni, che permette di rilevare pacchetti sospetti o anomali basati sul contesto della sessione.

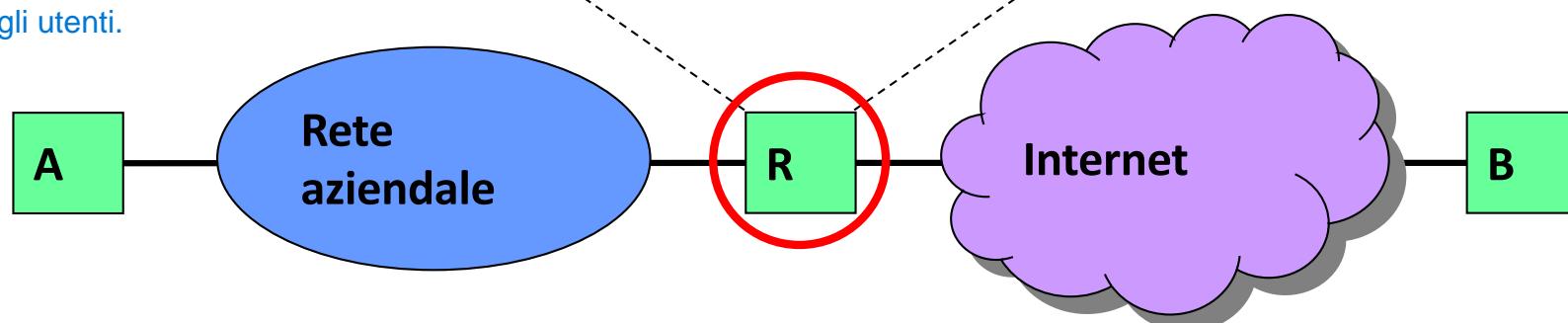
3

Application Layer Gateway (Proxy)

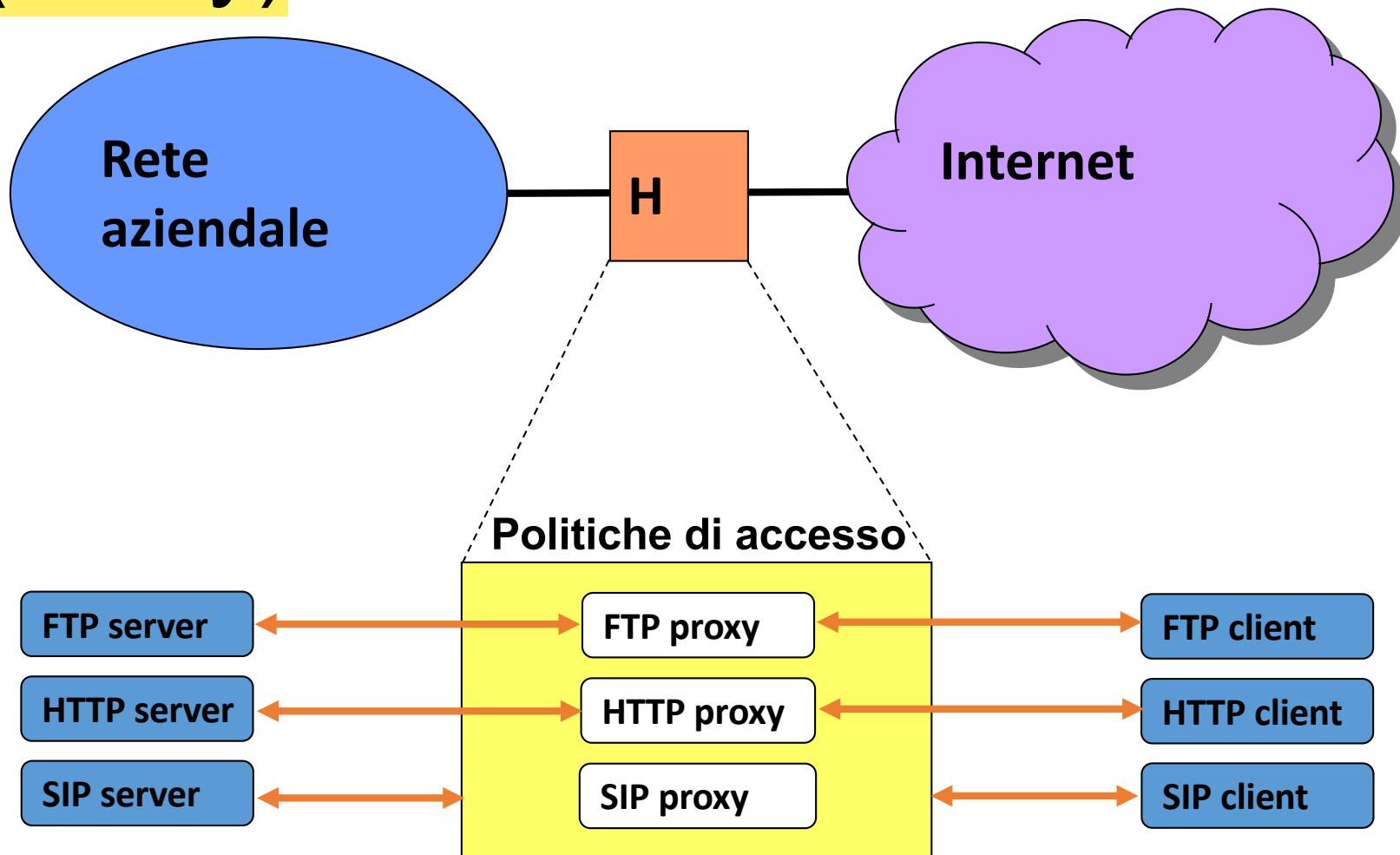
Differenza tra Proxy e altre tecniche:
Packet Filtering e Stateful
Packet Inspection filtrano il traffico a livello di pacchetto o di connessione, basandosi principalmente sulle informazioni di intestazione del pacchetto IP, porte e protocolli.
Il proxy, invece, lavora a un livello più alto, a livello di applicazione, e può analizzare e modificare il contenuto del traffico stesso. Questo lo rende più adatto per applicazioni che richiedono una protezione e un controllo approfondito, come il filtraggio dei contenuti web o l'autenticazione degli utenti.



Packet Filtering e SPI sono tecniche di filtraggio e gestione della rete e vengono implementate su Firewall o Router che fungono da Gateway. Il PROXY è sia una tecnica di filtraggio del traffico di rete, sia un nodo di rete vero e proprio. A differenza delle tecniche come il Packet Filter o la Stateful Packet Inspection, un proxy si comporta come un intermediario tra un client e un server, gestendo direttamente le comunicazioni a livello applicativo (Layer 7 del modello OSI).



Application Layer Gateway (Proxy)



PROXY MultiProtocollo che fanno passare dei protocolli ed altri no



Il Packet Filter controlla solo le intestazioni dei pacchetti, concentrando su informazioni come:

Indirizzo IP (origine e destinazione)
Numero di porta (origine e destinazione)
Protocollo

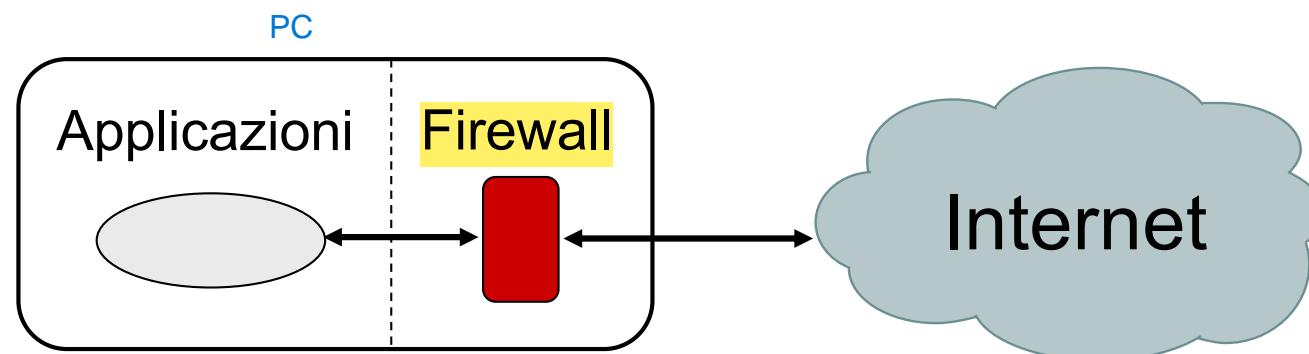
Firewall

Un firewall è un dispositivo o un software di sicurezza che controlla e gestisce il traffico di rete in entrata e in uscita, applicando regole di sicurezza predefinite per proteggere una rete o un sistema dagli accessi non autorizzati, da attacchi informatici e da altri tipi di minacce. Il firewall agisce come un filtro tra una rete sicura (come una rete interna o aziendale) e una rete meno sicura o non sicura (come Internet).

- **Packet Filter:** filtra i pacchetti seguendo la politiche stabilite
 - Filtri: generalmente configurati staticamente cioè le regole vengono impostate manualmente e non cambiano automaticamente.
 - La maggioranza delle configurazioni non permettono pacchetti per porte “non-standard” (Internet Assigned Numbers Authority – IANA)
- **Stateful Packet Inspection** Oltre a esaminare i pacchetti individuali, un firewall stateful tiene traccia delle connessioni di rete attive.
 - Mantiene il contesto dei pacchetti sia nel trasporto che nello strato applicativo
 - Adatta dinamicamente le specifiche dei filtri Le regole di filtraggio possono cambiare dinamicamente a seconda dello stato delle connessioniCiò significa che i pacchetti non vengono filtrati solo in base al loro contenuto statico, ma anche in base allo stato della connessione.
- **Application Layer Gateway (trasparente o proxy esplicito)** ↗ il client non sa dell'esistenza del proxy.
 - Monitora le connessioni: analizza il contenuto dei protocolli applicativi
 - A scapito della sicurezza di comunicazione end-to-end ALG analizza il contenuto effettivo della comunicazione.
 - Adatta dinamicamente le specifiche dei filtri↗ il client sa che sta utilizzando un proxy e deve configurare esplicitamente il proprio software per far passare il traffico attraverso di esso
- Per ogni strato (layer) dello stack possono essere applicate politiche (policies) differenti

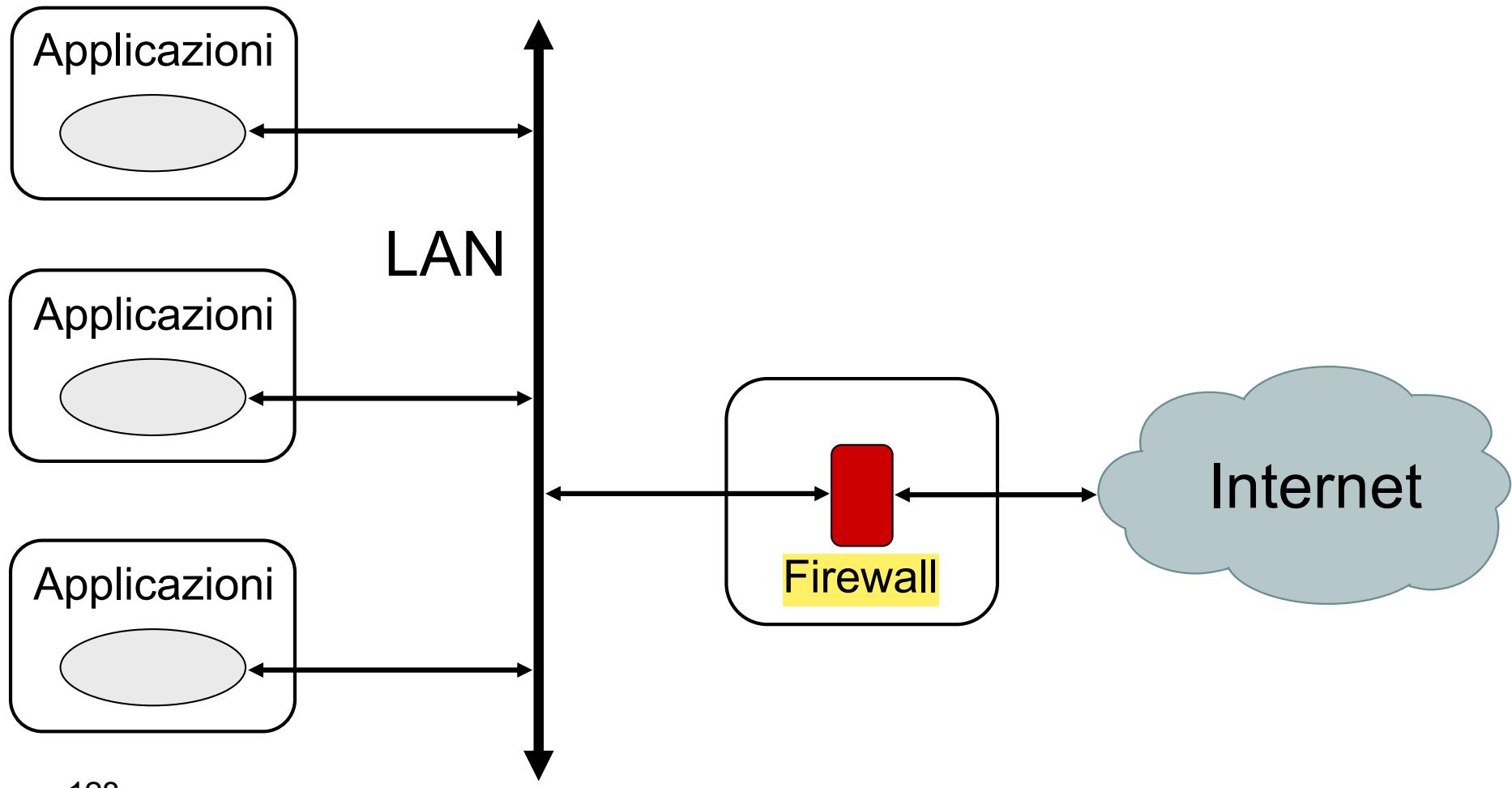
Protezione di host: firewall

- 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



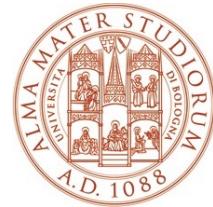


Protezione di rete: firewall

- 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 i servizi non esplicitamente permessi sono negati
 - **default permit**: tutti i servizi non esplicitamente negati sono permessi

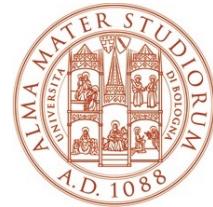
Nonostante le restrizioni, il firewall deve consentire che i servizi fondamentali per l'operatività aziendale continuino a funzionare senza interruzioni.

Il firewall stesso deve essere sicuro e non vulnerabile ad attacchi.



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



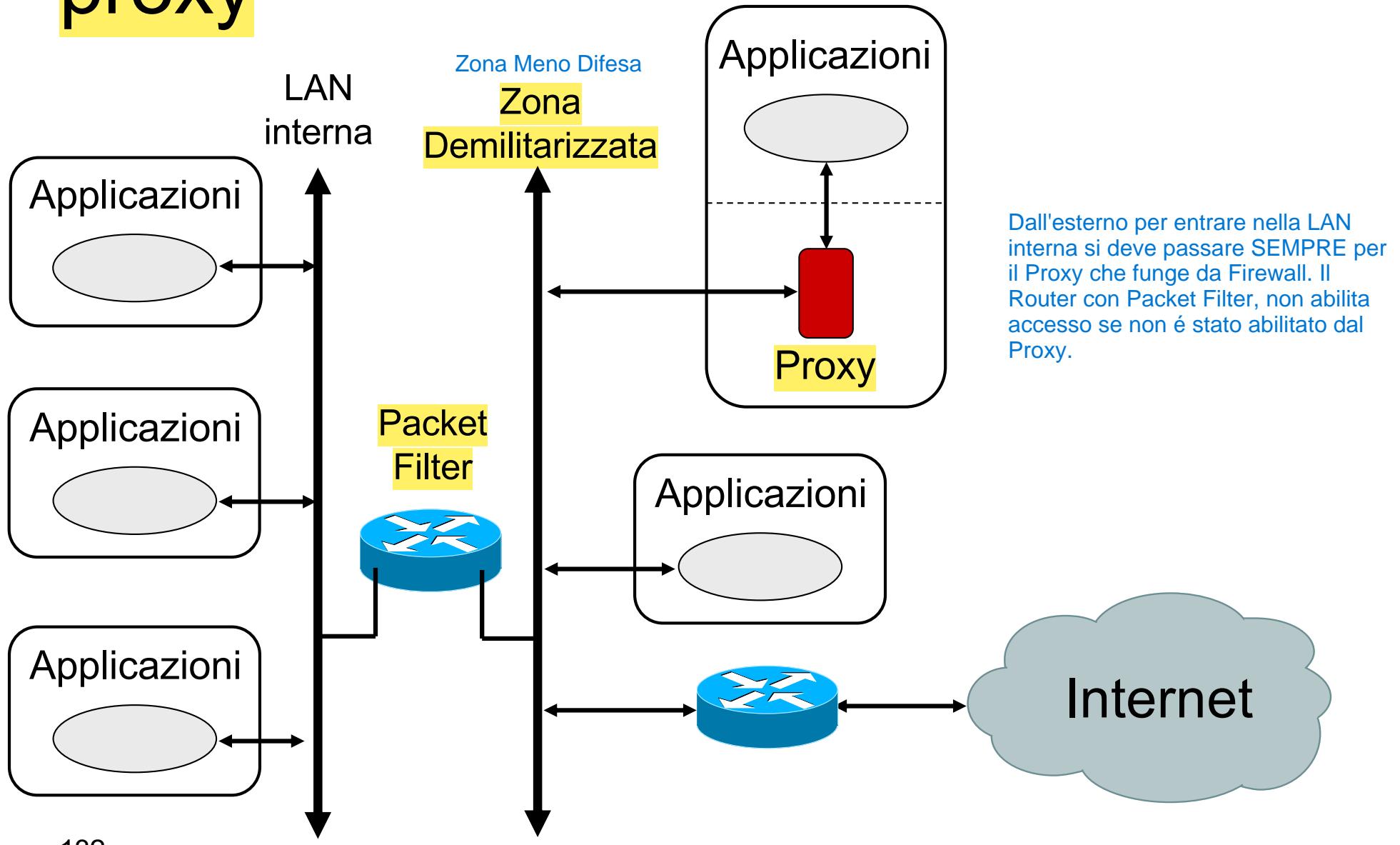
Livelli di implementazione

• 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 Ogni servizio ha il suo proxy dedicato. Questi proxy sono specifici per un'applicazione e spesso includono funzionalità di filtraggio e controllo su quello specifico servizio.
- **circuit level gateway**
 - è un proxy server generico in grado di inoltrare le richieste relative a molti servizi ma senza il livello di ispezione dei proxy applicativi.

L'host non comunica direttamente con il server esterno, ma invia la richiesta al proxy server. Questo server poi si collega a Internet, ottiene la risposta e la inoltra all'host.

Configurazione di packet filter e proxy





ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Network Address Translation



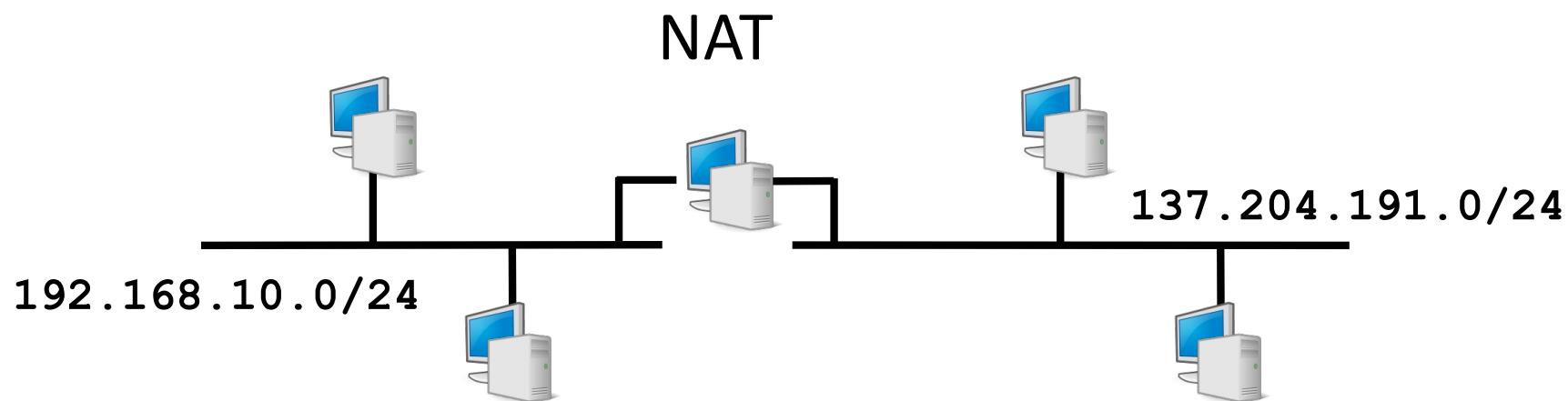
Network Address Translation (NAT)

(Nasconde Calcolatori Locali dall'esterno)

- 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

Quando un pacchetto dati lascia la rete interna (LAN) e si dirige verso Internet, l'indirizzo IP di origine del pacchetto viene sostituito (mascherato) con l'indirizzo IP pubblico del gateway NAT. Questo processo avviene in modo trasparente per i dispositivi all'interno della rete locale. Inoltre, NAT può anche modificare la porta di origine (non solo l'indirizzo IP), in modo da tracciare le comunicazioni provenienti da dispositivi interni che utilizzano lo stesso indirizzo IP pubblico.

Un gateway NAT è un router o un firewall che gestisce il traffico tra una rete privata (tipicamente una rete domestica o aziendale) e una rete pubblica (come Internet).





NAT: motivazioni

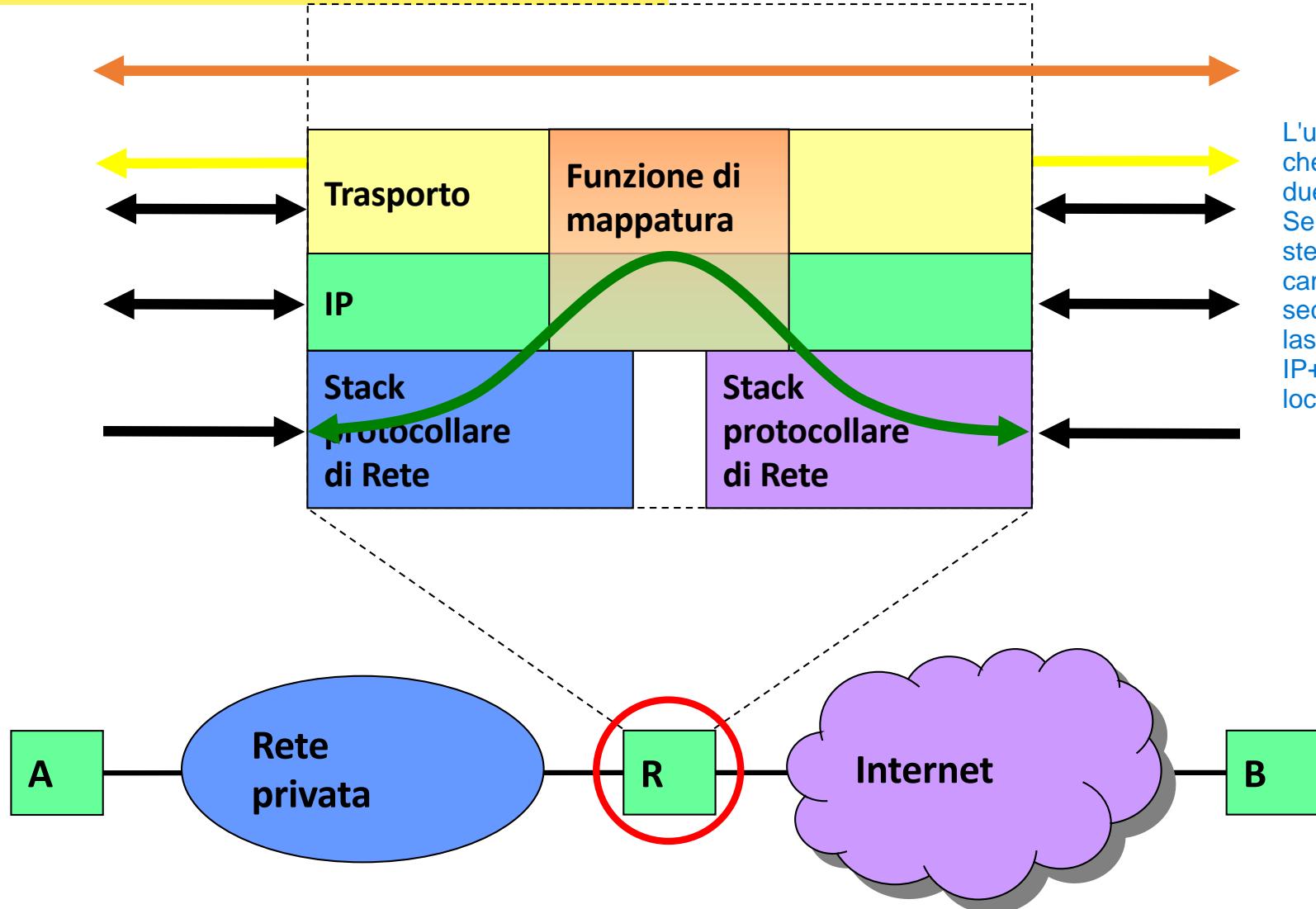
NAT utilizza una tabella di traduzione per tenere traccia delle associazioni tra gli indirizzi IP privati e quelli pubblici. Memorizza Indirizzo IP Pubblico, Privato e Numero di Porta.

- **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**

NAT (Network Address Translation) è una tecnologia di rete che consente a più dispositivi in una rete locale di condividere un singolo indirizzo IP pubblico per comunicare con Internet. Questo è particolarmente utile per risparmiare indirizzi IP pubblici, che sono limitati.

Quando un dispositivo all'interno di una rete privata vuole comunicare con un server su Internet, il router NAT cambia l'indirizzo IP privato del dispositivo in un indirizzo IP pubblico prima di inviare i pacchetti di dati all'esterno. Quando il server risponde, il router NAT intercetta la risposta, cambia l'indirizzo IP pubblico nel corrispondente indirizzo IP privato e inoltra i pacchetti al dispositivo corretto nella rete interna. Questo processo è trasparente per i dispositivi coinvolti.

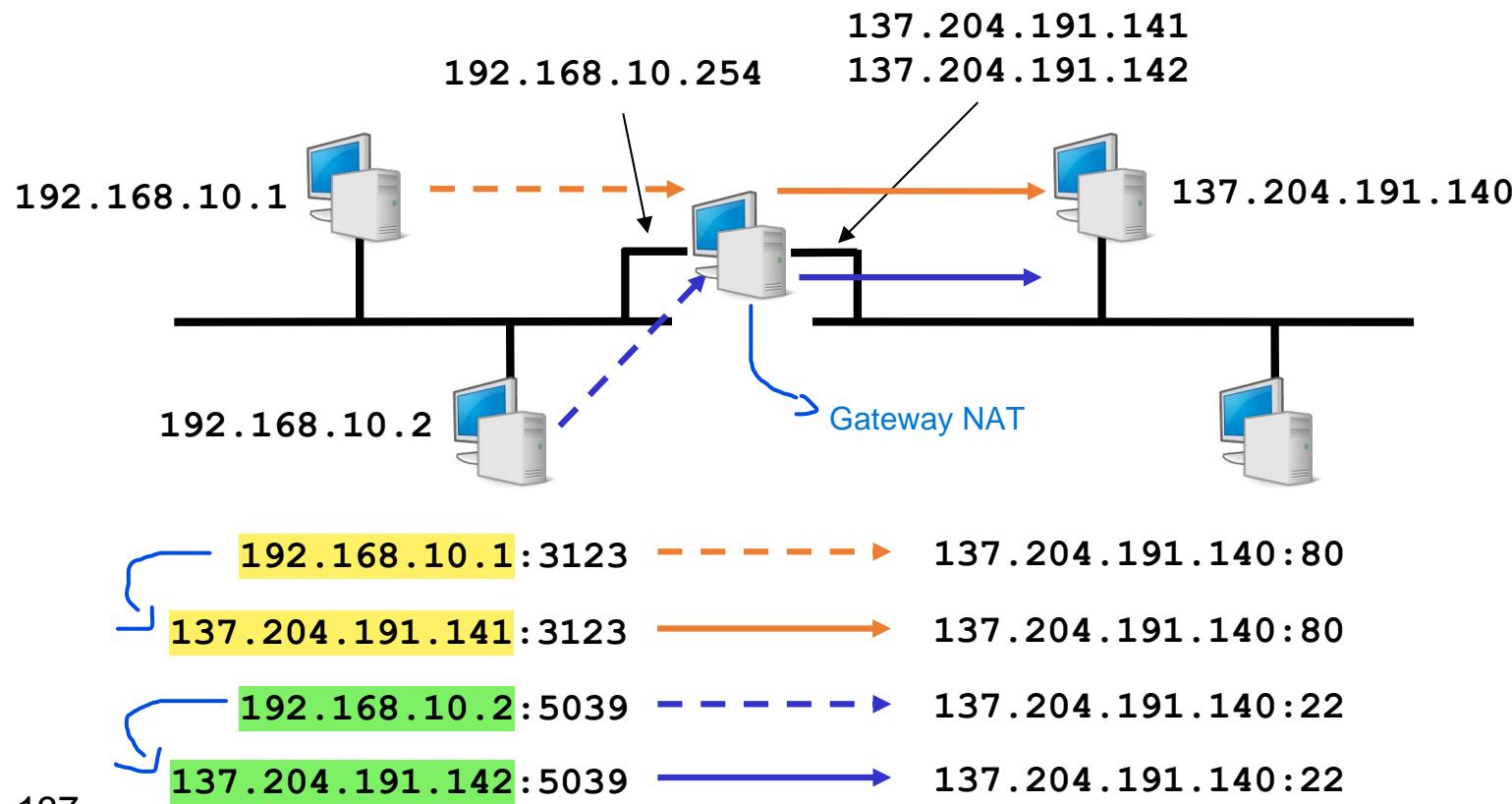
Network (+Port) Address Translator (NAT)



L'unico problema è evitare che si usi stessa porta in due connessioni diverse. Se ho 2 connessioni con stessa porta, il NAT cambia la porta della seconda connessione, lasciando invariato IP+Porta del calcolatore locale.

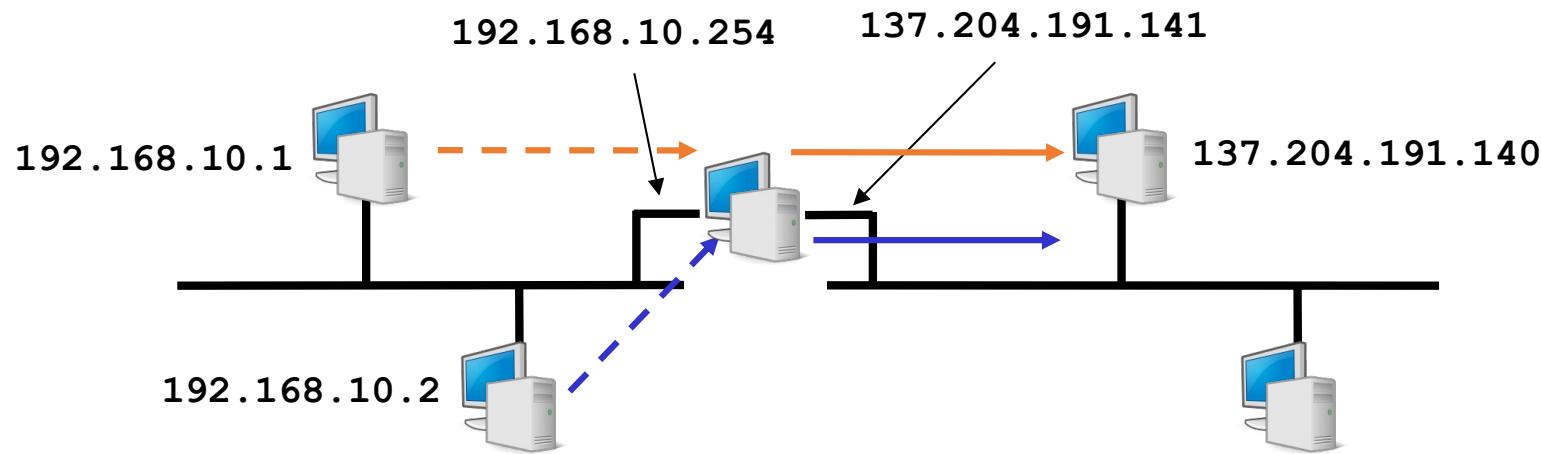
Basic NAT – Conversione di indirizzo

- 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



Conversione di indirizzo e porta

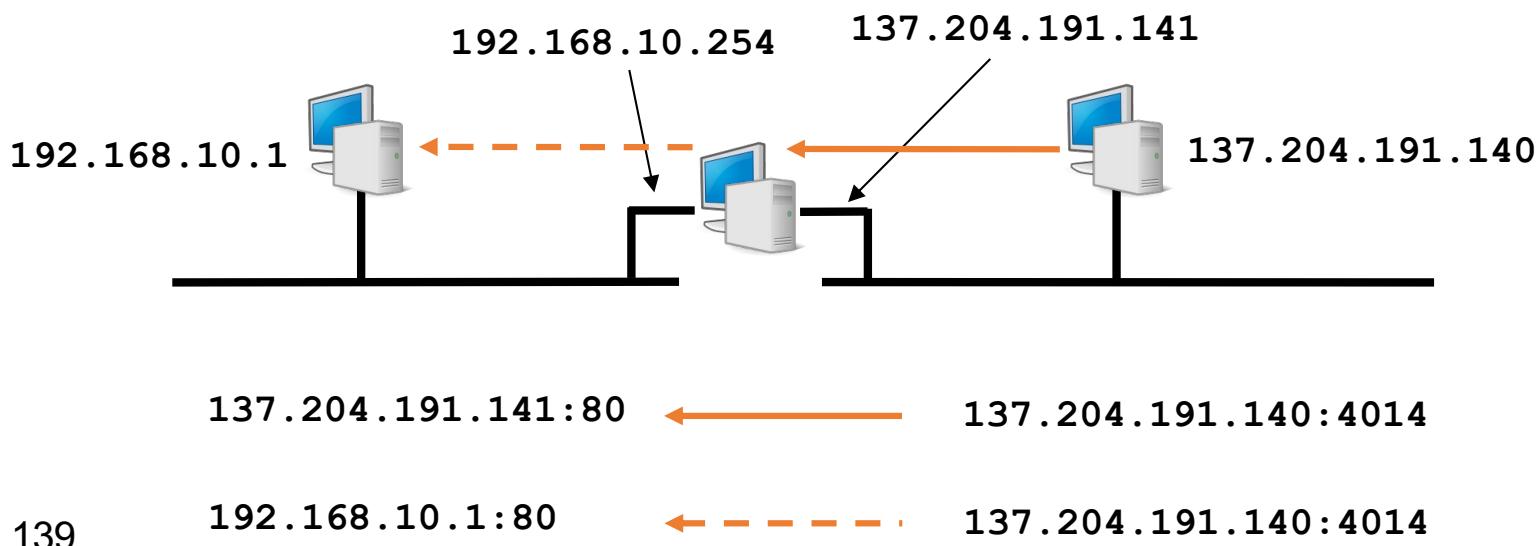
- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



Cambio solo IP	192.168.10.1:3123	→	137.204.191.140:80
	137.204.191.141:3123	→	137.204.191.140:80
Cambio IP e Porta perché ho già una connessione sulla porta 3123 138	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





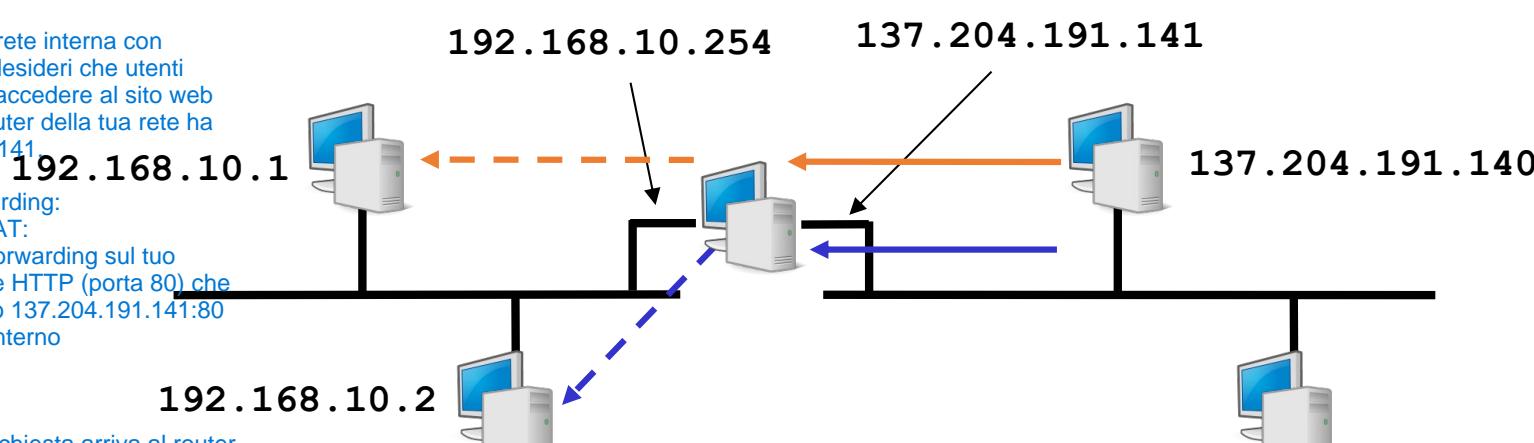
Port forwarding

Il Port Forwarding è una tecnica utilizzata nel NAT per consentire l'accesso a servizi specifici all'interno di una rete privata da dispositivi esterni su Internet. In pratica, il router NAT riceve pacchetti destinati a un determinato indirizzo IP pubblico e porta, quindi li inoltra a un dispositivo specifico nella rete interna, traducendo l'indirizzo e la porta secondo la tabella di traduzione.

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

Scenario:

Hai un server web nella tua rete interna con indirizzo IP 192.168.10.1 e desideri che utenti esterni su Internet possano accedere al sito web ospitato su quel server. Il router della tua rete ha un IP pubblico 137.204.191.141.



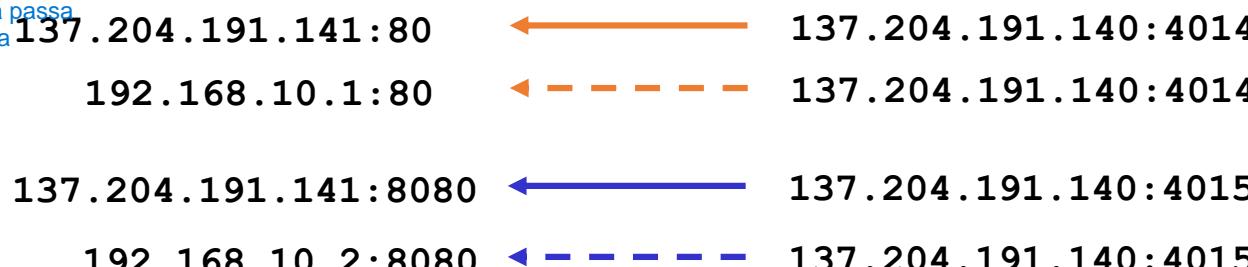
Come funziona il Port Forwarding:

Configurazione del router NAT:
Imposta una regola di Port Forwarding sul tuo router, in cui tutte le richieste HTTP (porta 80) che arrivano all'indirizzo pubblico 137.204.191.141:80 vengono inoltrate al server interno 192.168.10.1:80.

Flusso di dati:

Un utente su Internet visita <http://137.204.191.141>. La richiesta arriva al router NAT, che la intercetta e la inoltra al server interno sulla rete locale con IP 192.168.10.1, che ascolta sulla porta 80.

Il server web risponde con il contenuto richiesto (ad esempio, una pagina web). La risposta passa di nuovo attraverso il router, che la rimanda all'utente esterno.



Vantaggi:

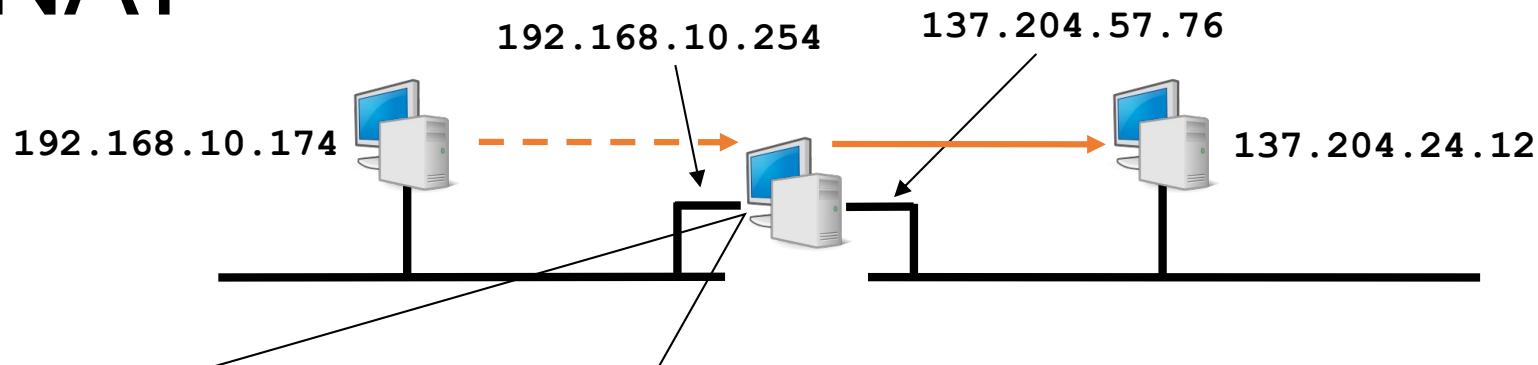
Sicurezza: Non esponi tutta la rete interna a Internet, ma solo il server e le porte specifiche che desideri aprire.

Accessibilità: Gli utenti esterni possono accedere a servizi specifici sulla rete interna senza che i dispositivi della rete privata siano direttamente visibili.

140

Con il Port Forwarding, solo le porte esplicitamente configurate sono accessibili dall'esterno, migliorando la sicurezza e il controllo.

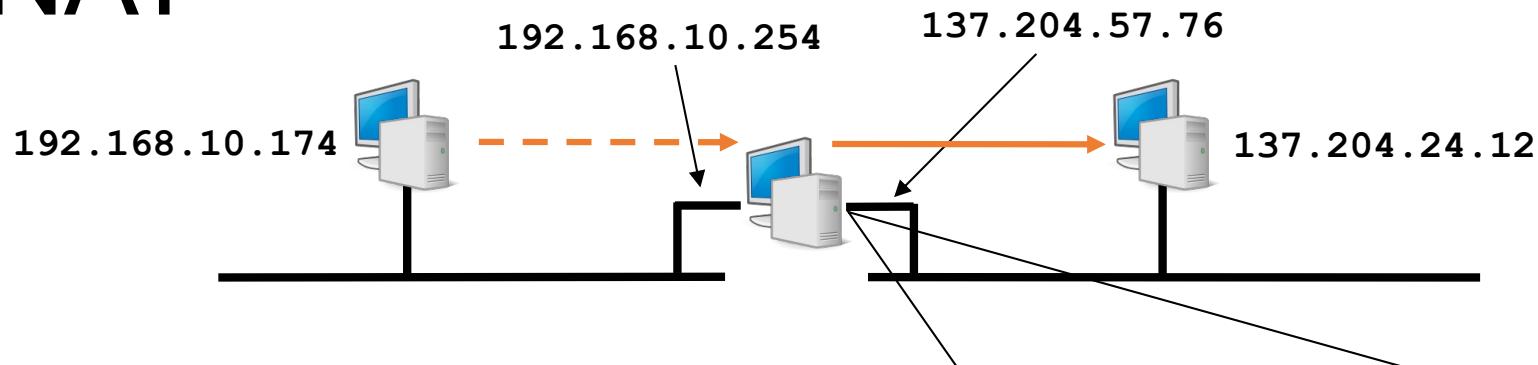
Analisi di connessioni attraverso NAT



NAT-int.cap - Ethereal

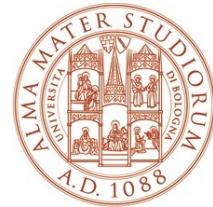
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.174	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034608	137.204.24.12	192.168.10.174	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1
3	0.896816	137.204.24.12	192.168.10.174	HTTP	HTTP/1.1 200 OK
4	0.896908	137.204.24.12	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

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 solo IP+Porta
 - 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