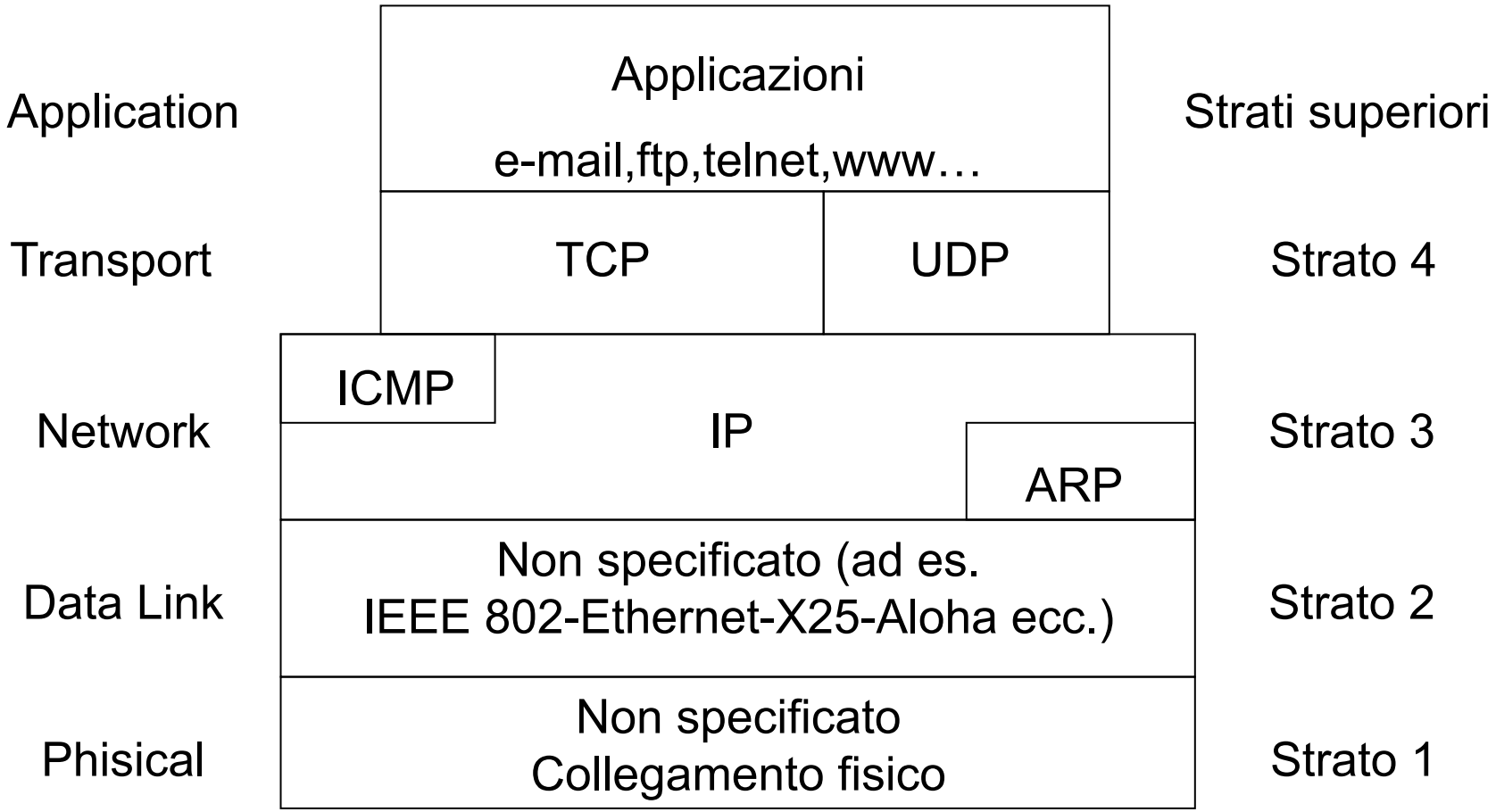
Il protocolli di Internet

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

La famiglia dei protocolli TCP/IP



La famiglia dei protocolli TCP/IP (2)

- Nessuna specifica per gli strati sotto a IP, in quanto relativi alla singola sottorete
- IP: funzioni di rete, instrada i pacchetti
- TCP: trasporto connection oriented
  - controllo della connessione end-to-end
- UDP: trasporto connectionless
- ICMP: gestione e controllo delle funzionalità di IP
- Lo strato di applicazione contiene applicativi utilizzati per fornire servizi all'utente

Il protocollo IP

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Internet Protocol (IP) - RFC 791

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

Struttura degli indirizzi IP

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

`10001001.11001100.11010100.00000001`

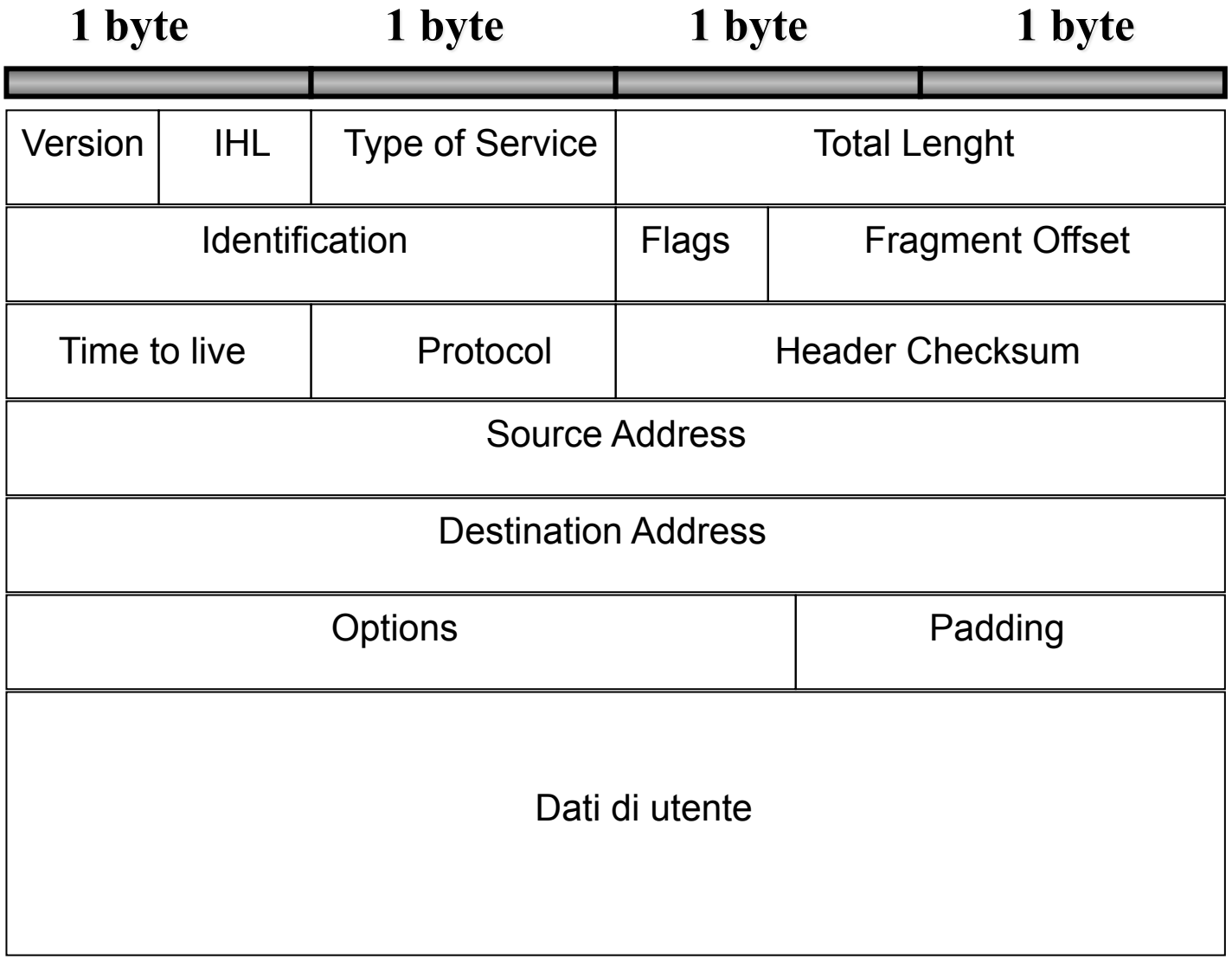
`137.204.212.1`

- Numero teorico max. di indirizzi

$$2^{32} = 4.294.967.296$$

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

Formato del pacchetto IP



Formato del pacchetto IP (2)

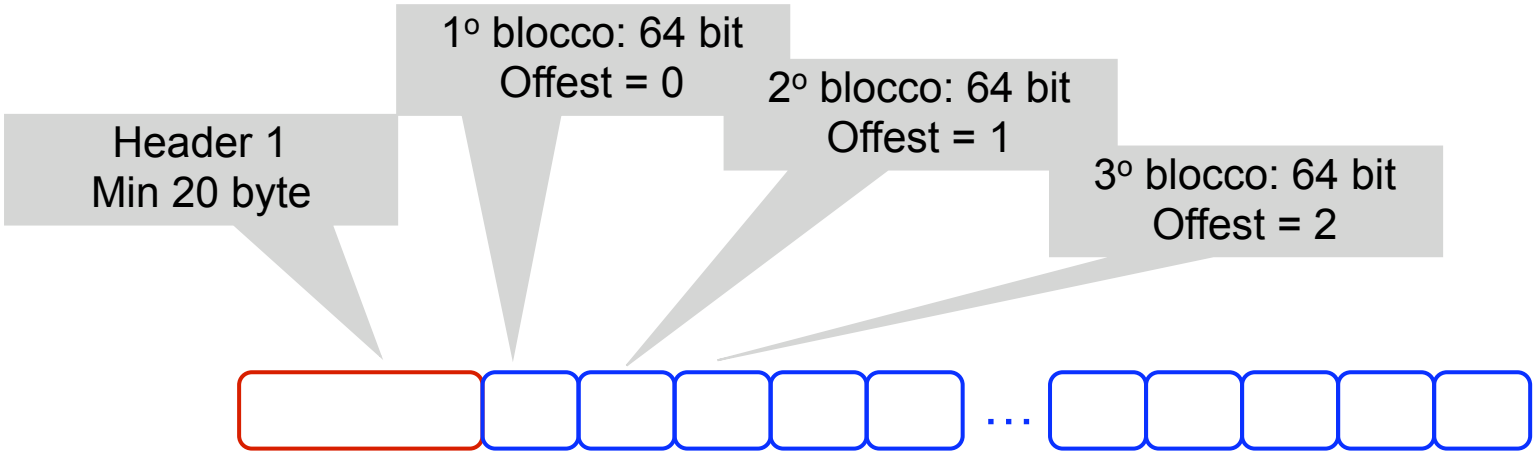
- **Version :** indica il formato dell'intestazione, attualmente la versione in uso è la 4
- **IHL :** lunghezza dell'intestazione, espressa in parole di 32 bit; lunghezza minima = 5
- **Type of service :** indicazione sul tipo di servizio richiesto, usato anche come sorta di priorità
- **Total length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

Formato del pacchetto IP (3)

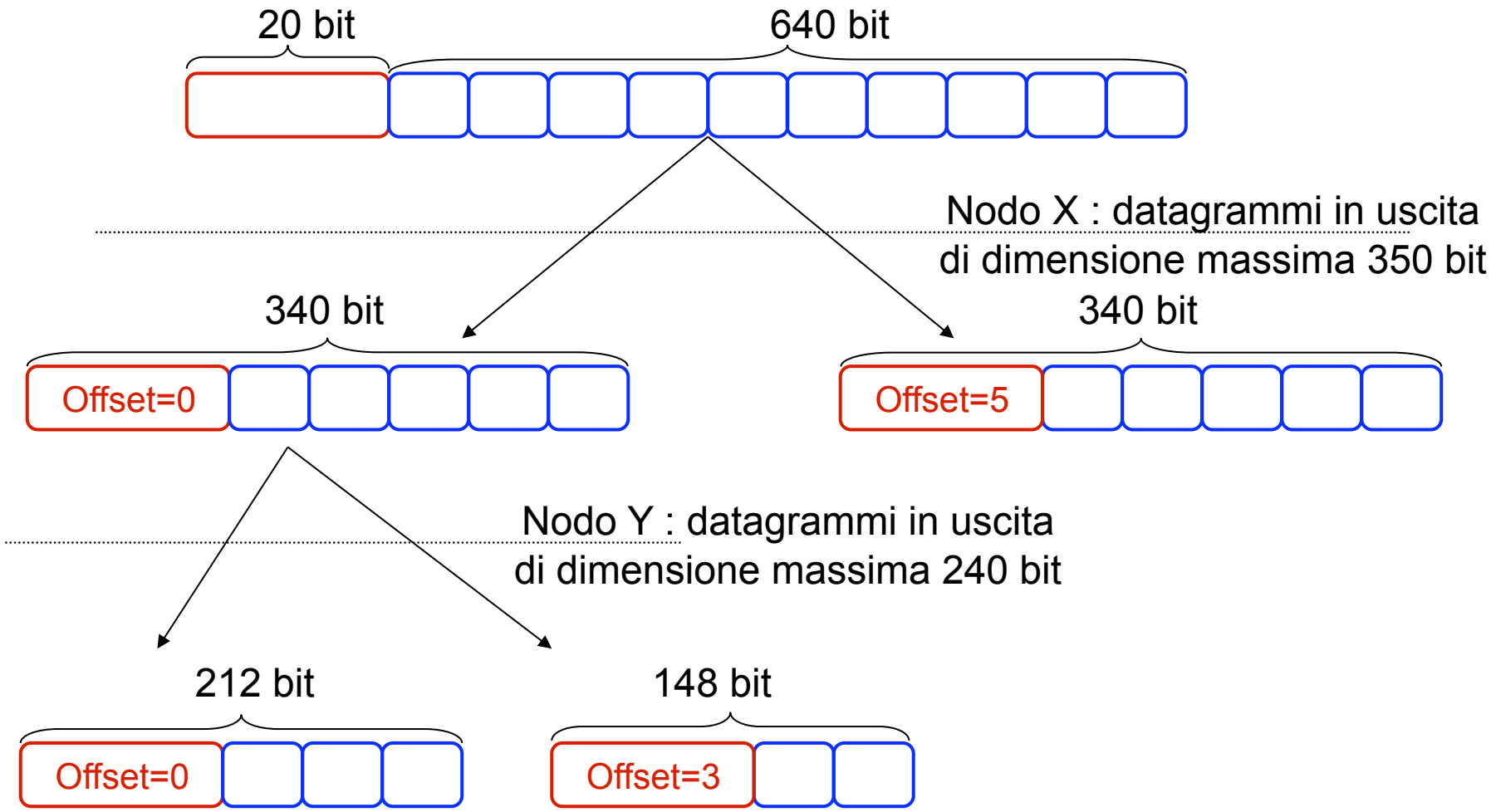
- **Identification :** valore intero che identifica univocamente il datagramma
  - Indica a quale datagramma appartenga un frammento (fragment)
- **Flag :** bit 0 sempre a 0
  bit 1 don't fragment (DF)
  DF = 0 si può frammentare
  DF = 1 non si può frammentare
  bit 2 more fragments (MF)
  MF = 0 ultimo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

La segmentazione in IP

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



Frammentazione e calcolo dell'offset



Formato del pacchetto IP (4)

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

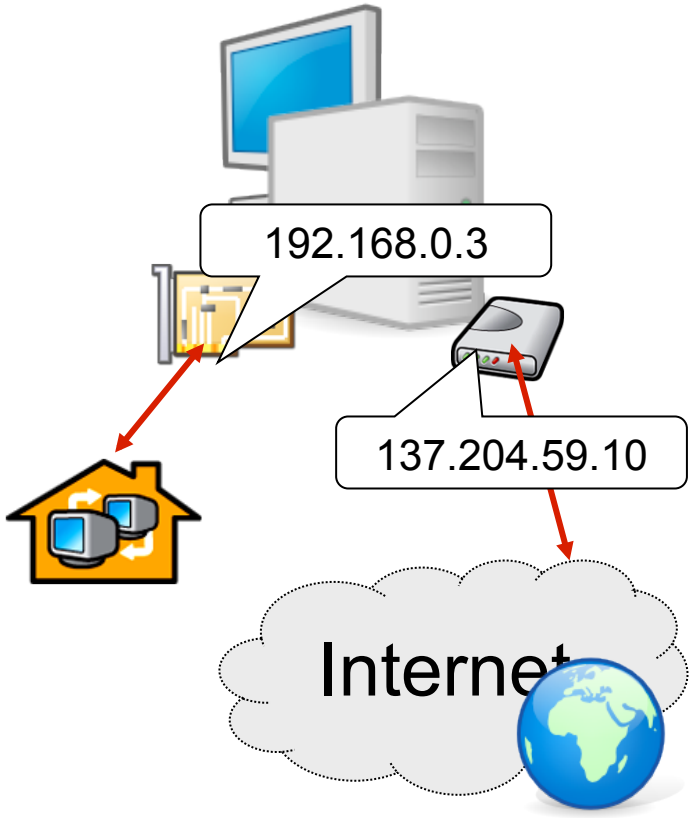
Formato del pacchetto IP (5)

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

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

Indirizzi e interfacce di rete

- L'indirizzo identifica i punti di interconnessione di un host con la rete
  - Non identifica un host individuale, ma una delle sue interfacce di rete
- **Multi-homed hosts**
  - host con due o più interfacce di rete
- Esempio: un router che collega *N* reti ha
  - *N* interfacce di rete
  - *N* distinti indirizzi IP, uno per ogni interfaccia di rete



Semantica dell'indirizzo IP

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

Reti IP private (RFC 1918)

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

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

Netmask

- Come si distingue net-ID da host-ID?
- Si usa la netmask
  - Al numero IP viene associata una maschera di 32 bit

```
137.204.191.25
10001001.11001100.10111111.00011001
11111111.11111111.11111111.11000000
```

- 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.60`
  - Utilizzando la notazione abbreviata
    - `11111111.11111111.11111111.11000000 = /26`

Netmask

- Esempio:
  - Network 192.160.1.0
    - Network privata di classe C 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

IP: Instradamento

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Tabella di instradamento IP

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

- Formato della tabella
  - Dipende dal sistema operativo e dall'implementazione
    - La tipologia di informazione è la medesima
    - Il modo di presentarle ed elaborarle può essere diverso

Entry

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

Uso della tabella di routing

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

Table lookup

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

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
255.255.255.255
192.168.002.018 == 192.168.002.018
```

- La riga 3 è quella giusta (host specific)

Esempio di lookup – 2

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

- Datagramma con IP dest. = 192.168.2.22

```
192.168.002.022
255.255.255.255
192.168.002.022 != 192.168.002.018

192.168.002.022
255.255.255.000
192.168.002.000 == 192.168.002.000
```

- La riga 2 è quella giusta (network specific)

Esempio di lookup – 3

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

- Datagramma con IP dest. = 80.48.15.170

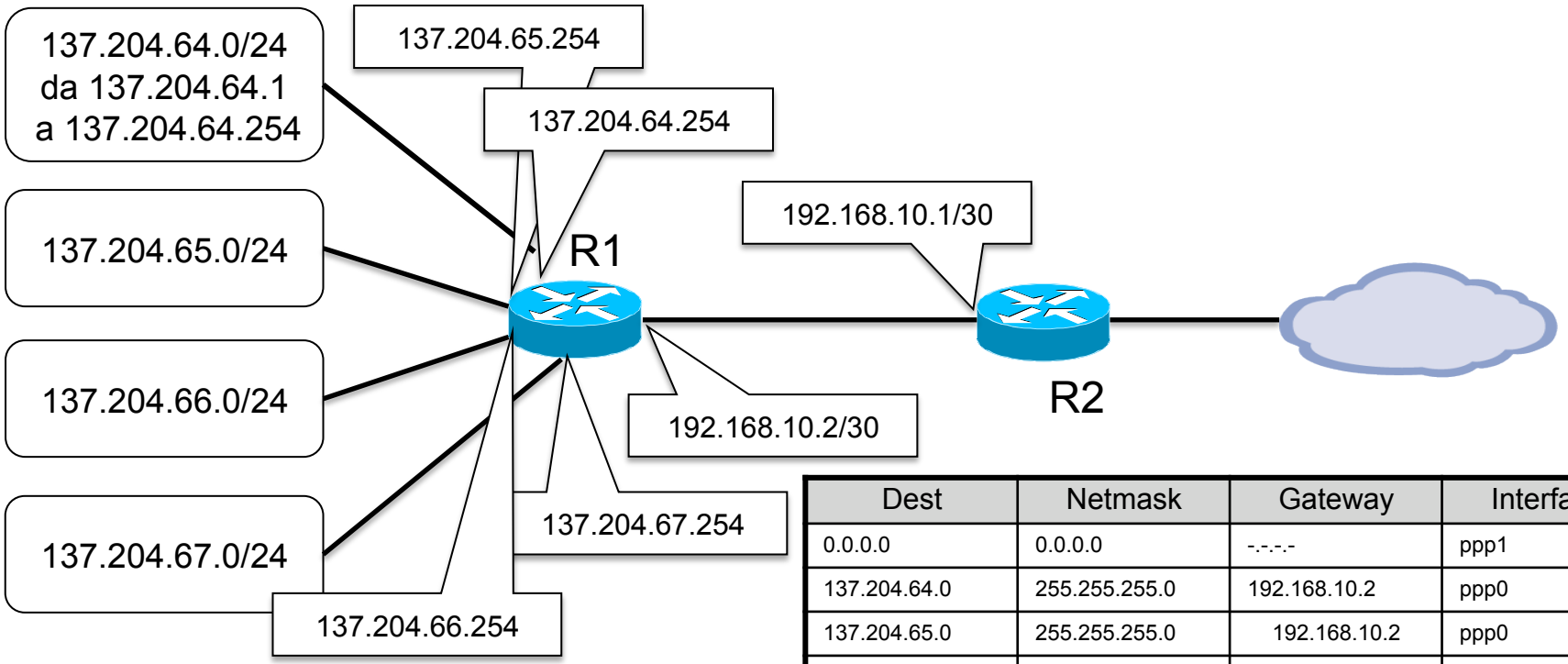
```
080.048.015.170
255.255.255.255
080.048.015.170 != 192.168.002.018

080.048.015.170
255.255.255.000
080.048.015.000 != 192.168.002.000

080.048.015.170
000.000.000.000
000.000.000.000 == 000.000.000.000
```

- La riga 1 è quella giusta (default gateway)

Esempio



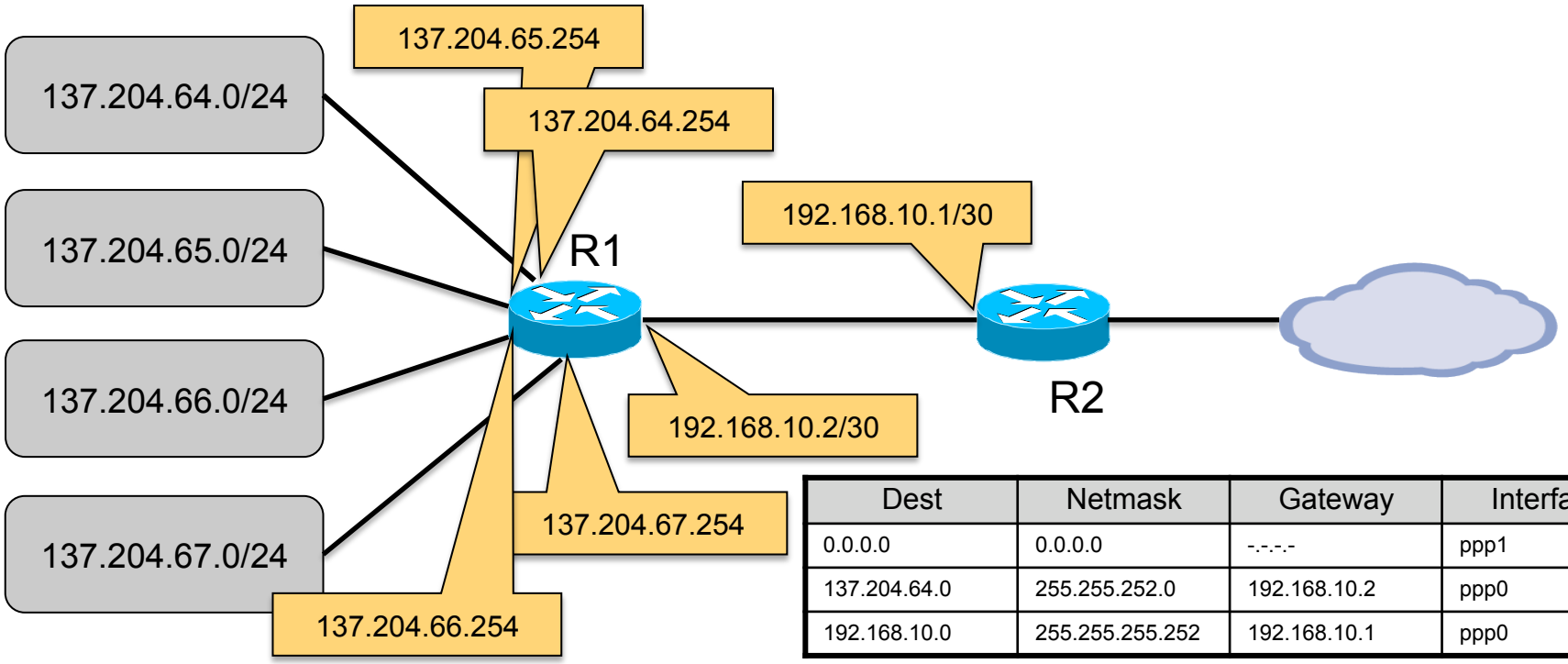
Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.10.1	ppp0
137.204.64.0	255.255.255.0	137.204.64.254	en0
137.204.65.0	255.255.255.0	137.204.65.254	en1
137.204.66.0	255.255.255.0	137.204.66.254	en2
137.204.67.0	255.255.255.0	137.204.67.254	en3
192.168.10.0	255.255.255.252	192.168.10.2	ppp0

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

Semplificazione delle tabelle

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

Aggregazione



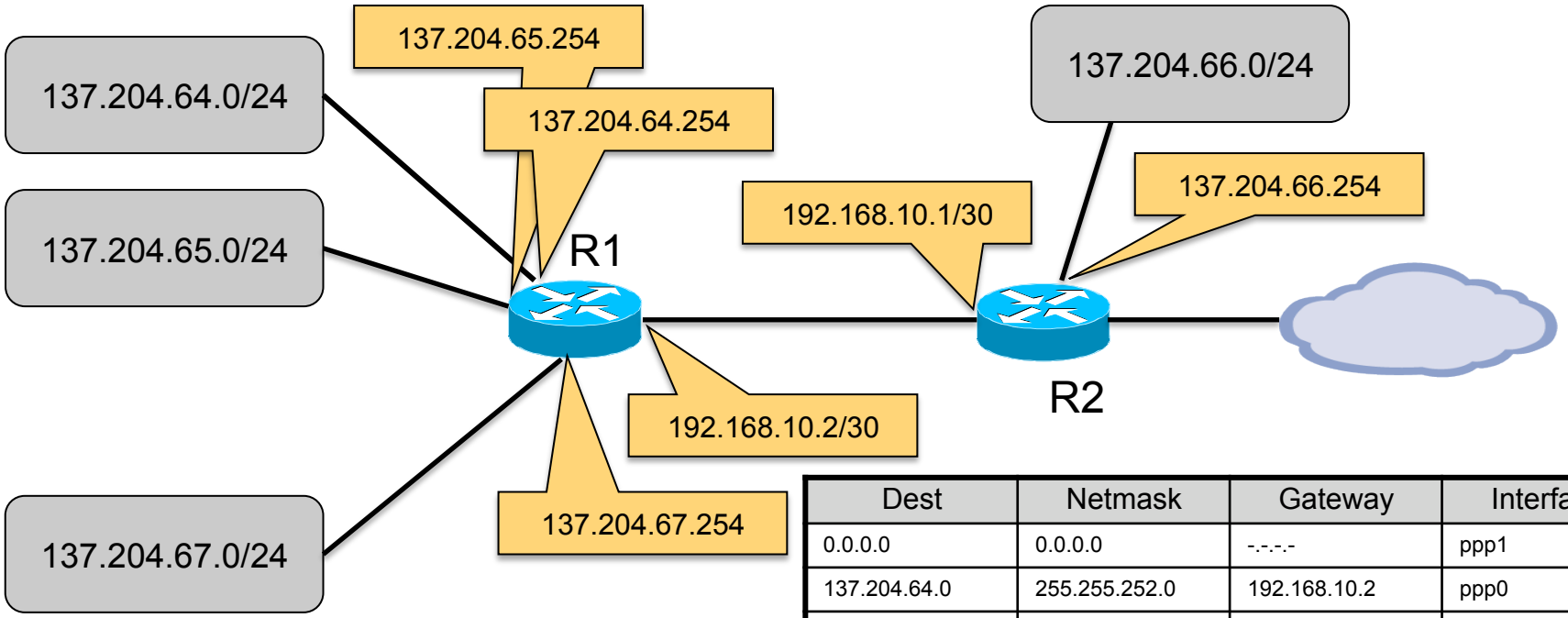
Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

Dest	Netmask	Gateway	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

Perché ordinare i route?

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

Eccezioni



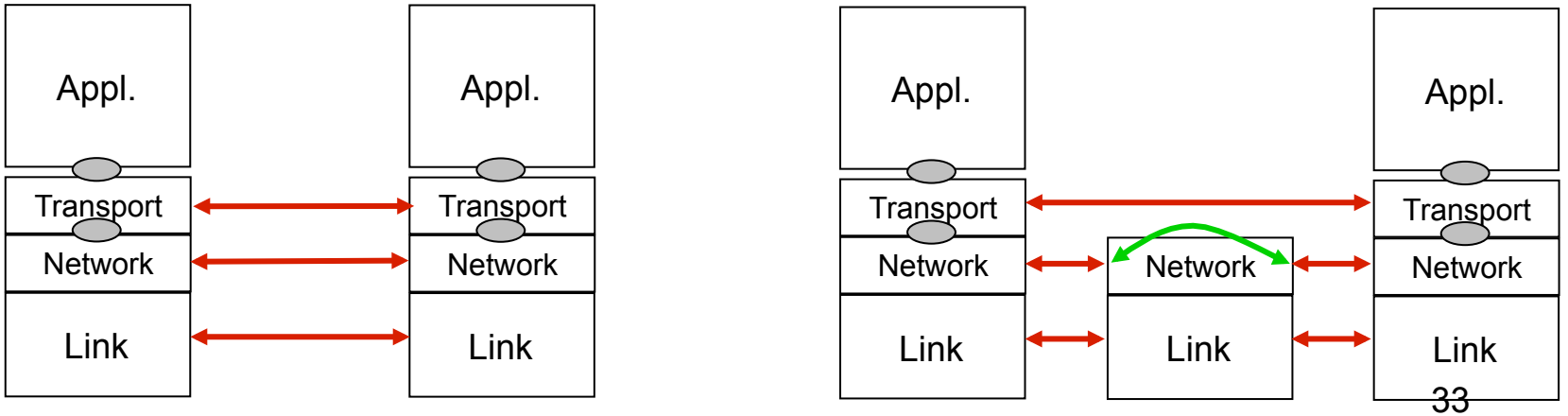
Dest	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	-.-.-.-	ppp1
137.204.64.0	255.255.252.0	192.168.10.2	ppp0
137.204.66.0	255.255.255.0	137.204.66.254	en0
192.168.10.0	255.255.255.252	192.168.10.1	ppp0

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

Instradamento (forwarding)

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

- *Gateway* = responsabile della consegna del datagramma



Rete logica e rete fisica

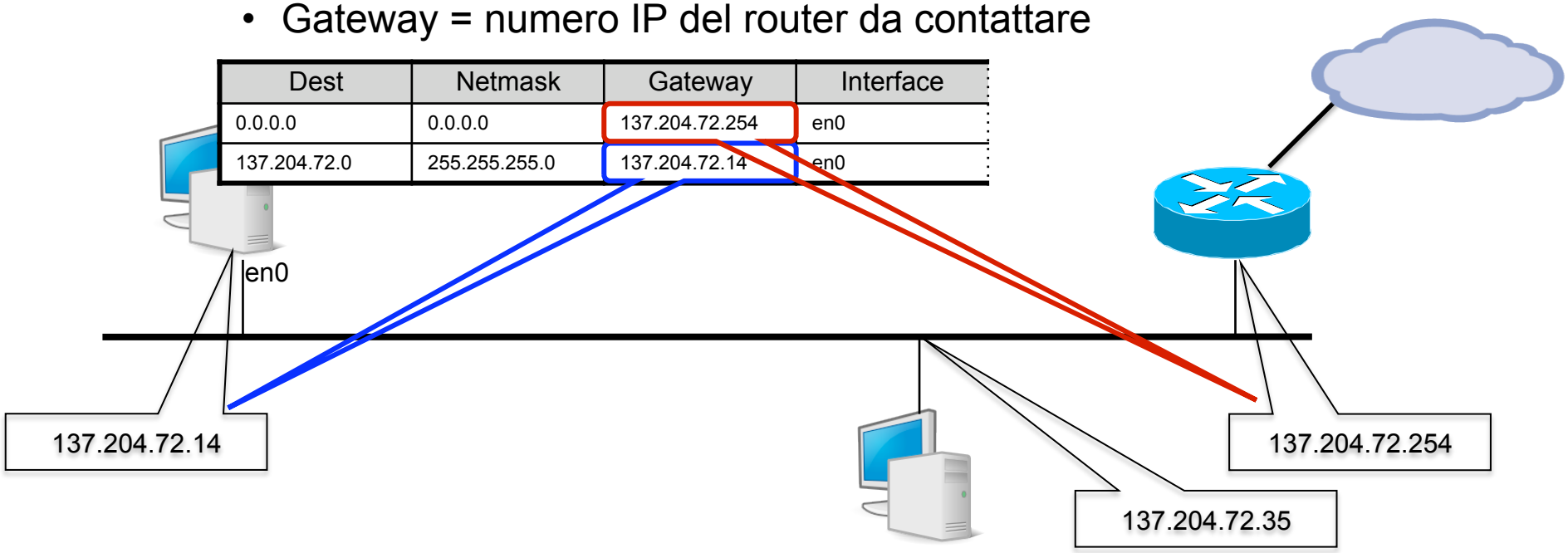
- Nella terminologia di Internet si definisce
  - Rete logica: la network IP a cui un Host appartiene logicamente
  - Rete fisica: la rete cui è effettivamente connesso
- La rete fisica normalmente ha capacità di instradamento e può avere indirizzi locali (indirizzi fisici)
- L'architettura a strati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

Rotuing: instradamento diretto e indiretto

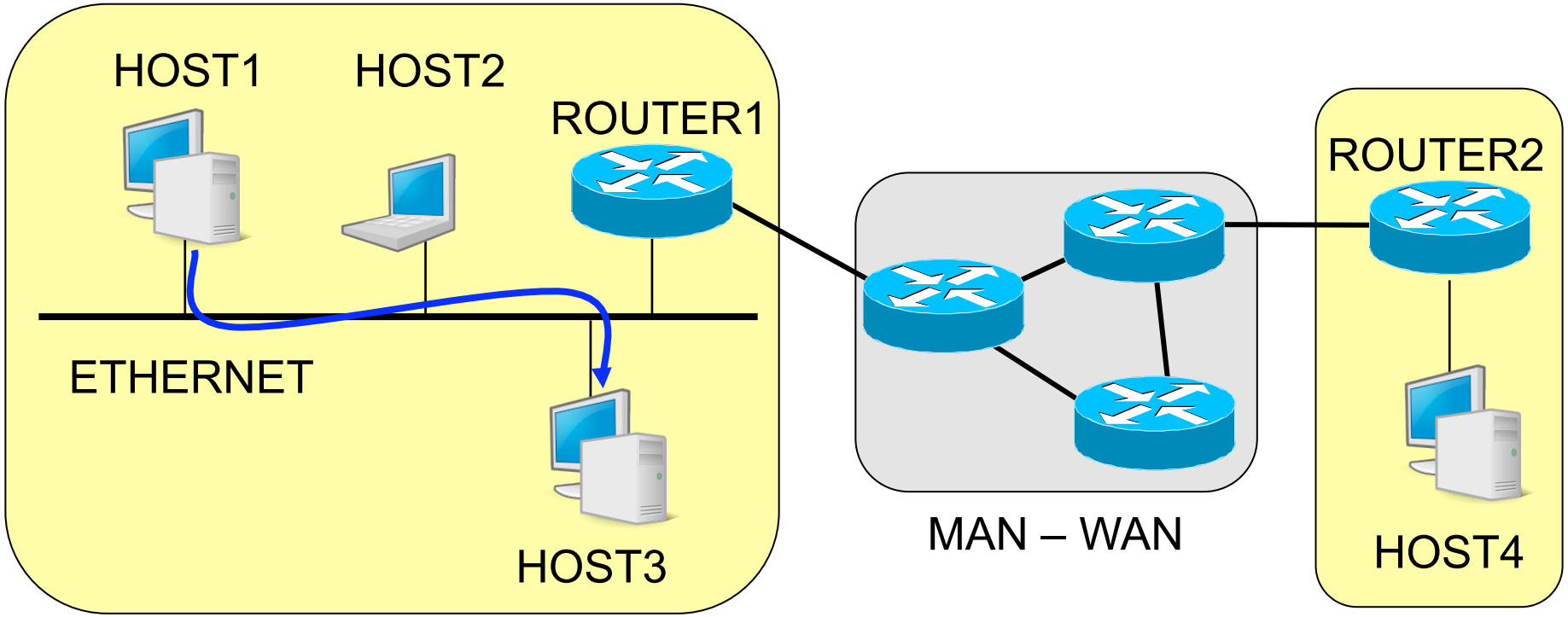
- **Routing** : scelta del percorso su cui inviare i dati
  - i router formano struttura interconnessa e cooperante:
    - i datagrammi passano dall'uno all'altro finché raggiungono quello che può consegnarli direttamente al destinatario
- **Direct delivery** :
  - IP sorgente e IP destinatario sono sulla stessa rete fisica
  - L'host sorgente spedisce il datagramma direttamente al destinatario
- **Indirect delivery** :
  - IP sorgente e IP destinatario non sono sulla stessa rete fisica
  - L'host sorgente invia il datagramma ad un router intermedio

Uso del Gateway

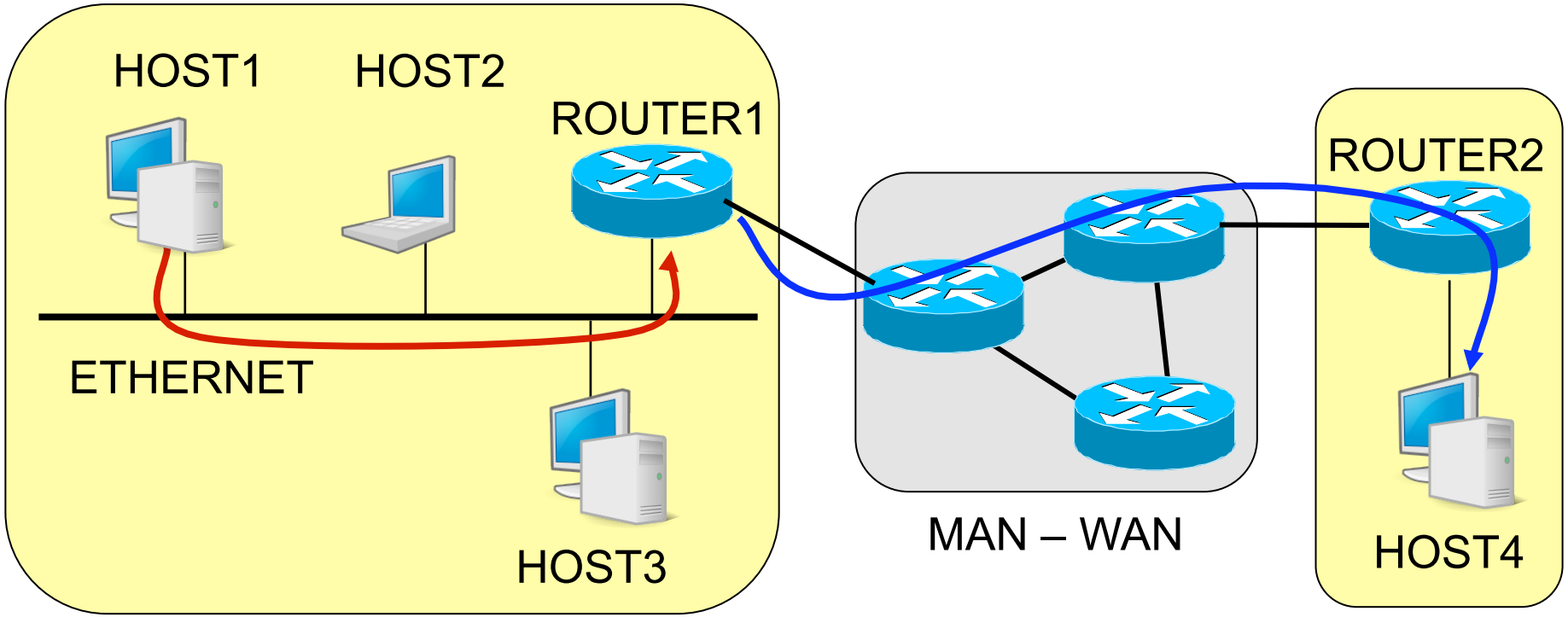
- Il campo gateway della tabella di routing serve per specificare il tipo di instradamento
  - Instradamento diretto: la sintassi dipende dall'implementazione
    - In Windows: instradamento diretto se gateway = IP locale
    - In Linux/Unix: instradamento diretto se gateway = 0.0.0.0
  - Instradamento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



Direct delivery: da Host 1 a Host 3



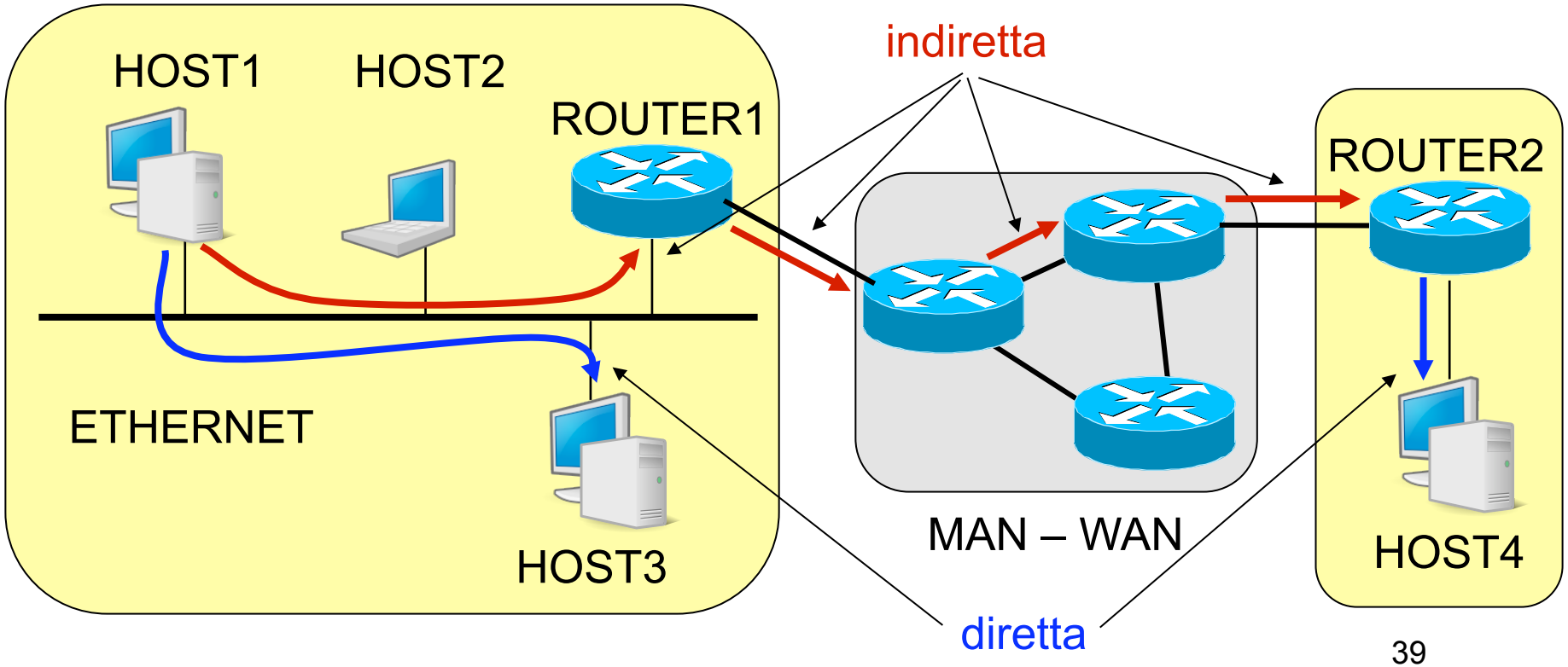
Indirect delivery: da Host 1 a Host 4



L2 ADDRESS: ROUTER1	IP ADDRESS: HOST4	DATI

Da mittente a destinatario

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



Indirizzamento Classfull e Classless

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

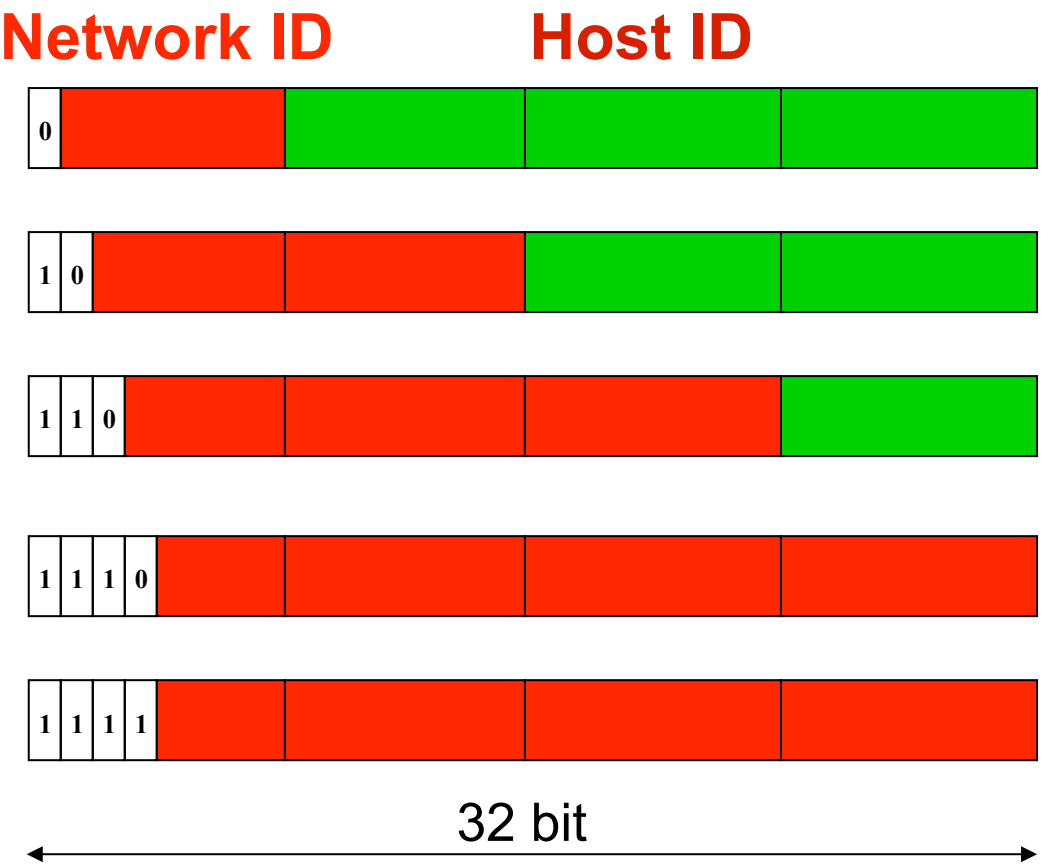
IP e netmask

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

Classe delle reti

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

Classi di indirizzi



Network ID : identifica una rete IP

Host ID : identifica i singoli calcolatori della rete

Intervalli di indirizzi

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

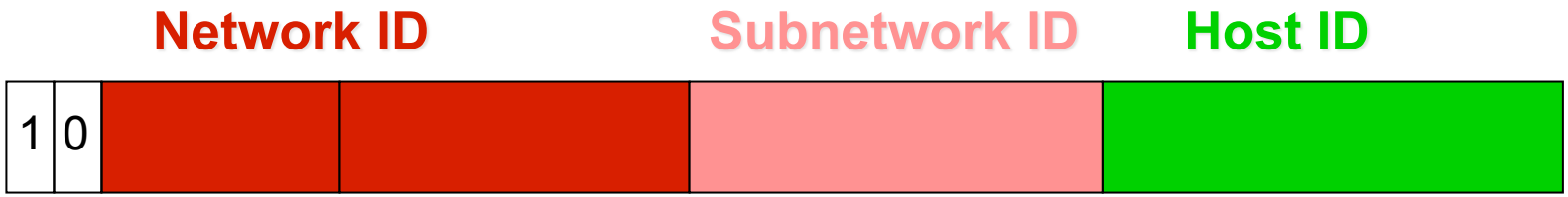
- Indirizzi riservati (RFC 1700)
  - **0.0.0.0** indica l'host corrente senza specificarne l'indirizzo
  - **Host-ID tutto a 0** viene usato per indicare la rete
  - **Host-ID tutto a 1** è l'indirizzo di broadcast per quella rete
  - **0.x.y.z** indica un certo Host-ID sulla rete corrente senza specificare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

Le sottoreti

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

Subnetting

- La suddivisione è locale alla singola interfaccia
  - Deve essere configurabile localmente
- Si fa uso della ***Netmask***
  - La nestmask tutti i bit utilizzati come prefisso
    - Net-ID e subNet-ID



Netmask

11111111 11111111 11111111 00000000

Netmask notazione dotted decimal : 255.255.255.0

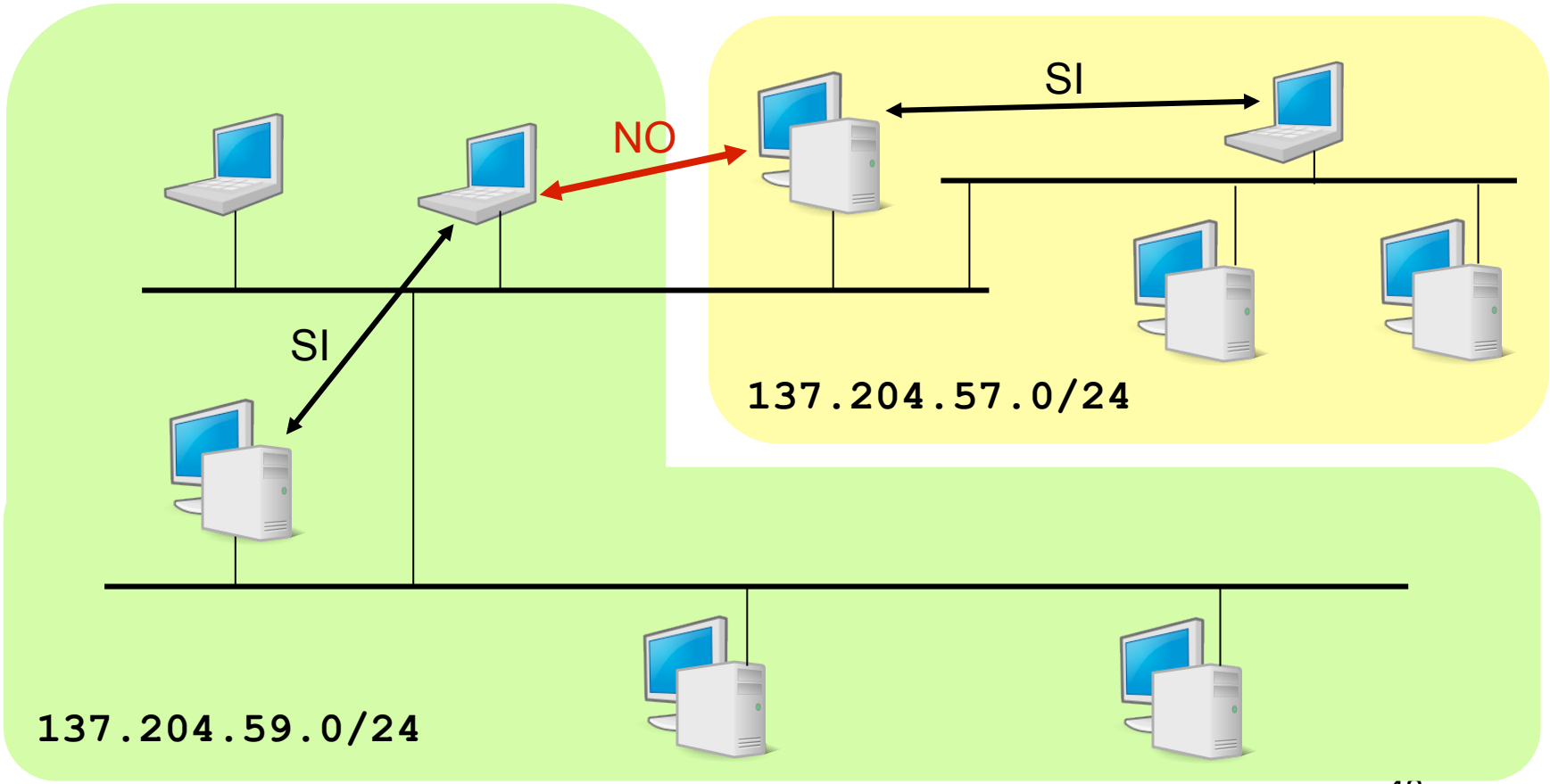
Esempio: Università di Bologna

- 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

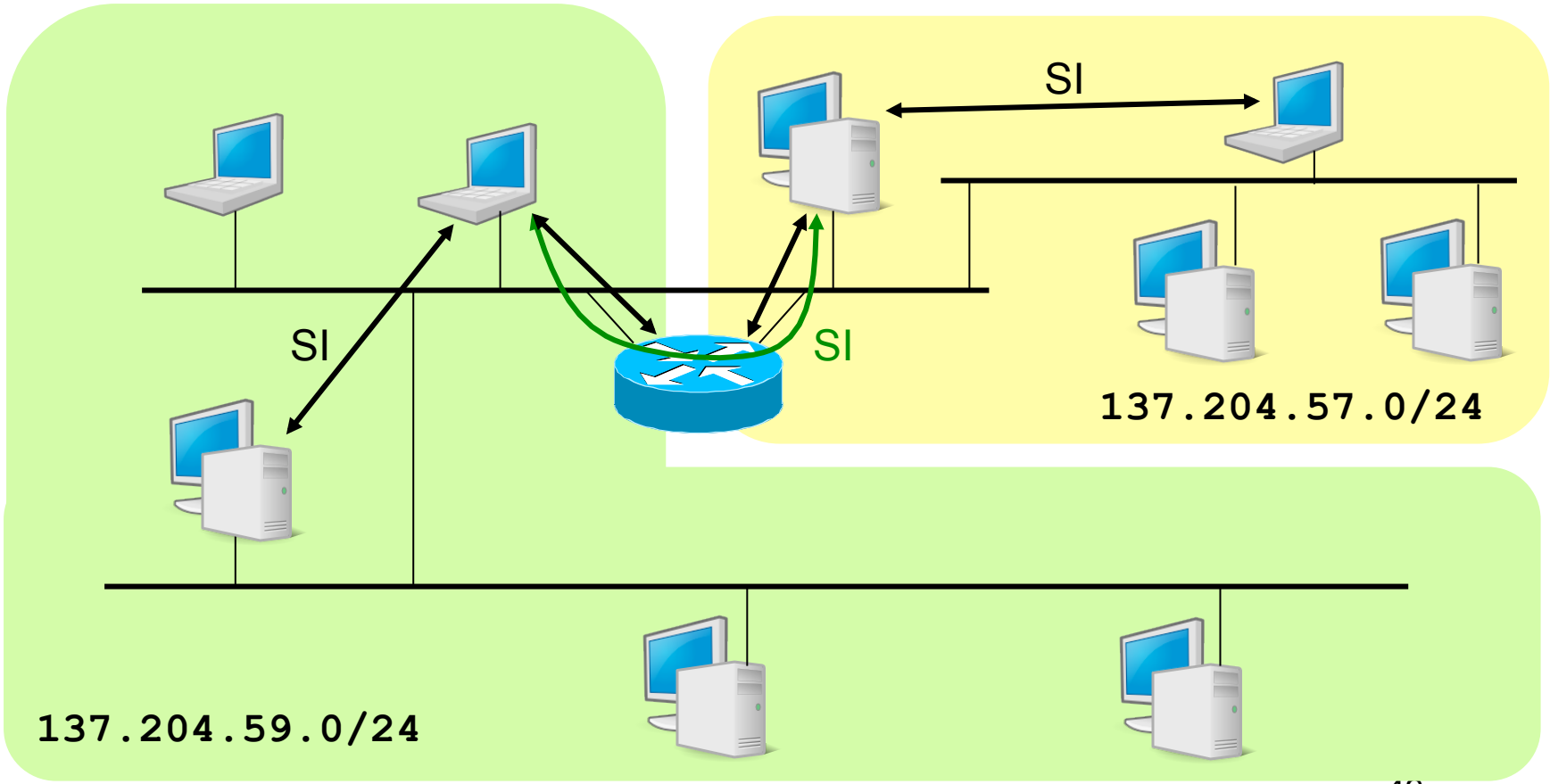
Subnetting: ripartizione logica e fisica

- La configurazione della netmask è necessaria per il corretto funzionamento dell'instradamento
  - Riconoscere il proprio Net-ID
  - Decidere fra instradamento diretto e indiretto



Subnetting: ripartizione logica e fisica

- La configurazione della netmask è necessaria per il corretto funzionamento dell'instradamento
  - Riconoscere il proprio Net-ID
  - Decidere fra instradamento diretto e indiretto



CIDR = Classless InterDomain Routing

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

Obiettivi del CIDR

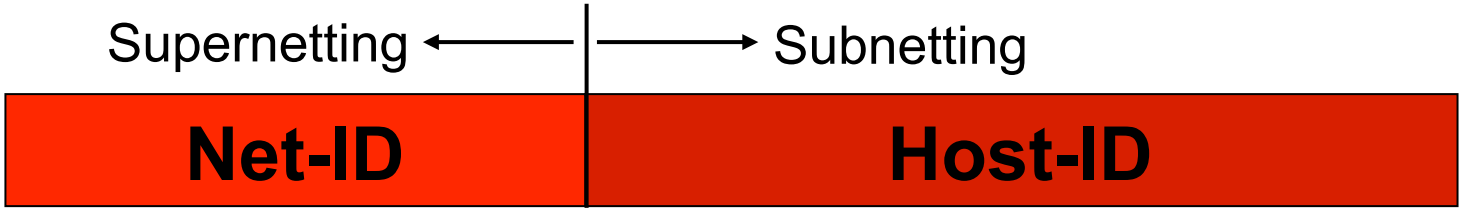
- Allocazione di reti IP di dimensioni variabili
  - utilizzo più efficiente dello spazio degli indirizzi
- Accorpamento delle informazioni di routing
  - più reti contigue rappresentate da un'unica riga nelle tabelle di routing
- Miglioramento di due situazioni critiche
  - Limitatezza di reti di classe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

Supernetting

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

Supernetting

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



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

Configurazione dell'interfaccia IP nell'host

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Configurazione delle interfacce di rete

`ipconfig /all` `(Windows 2X)`

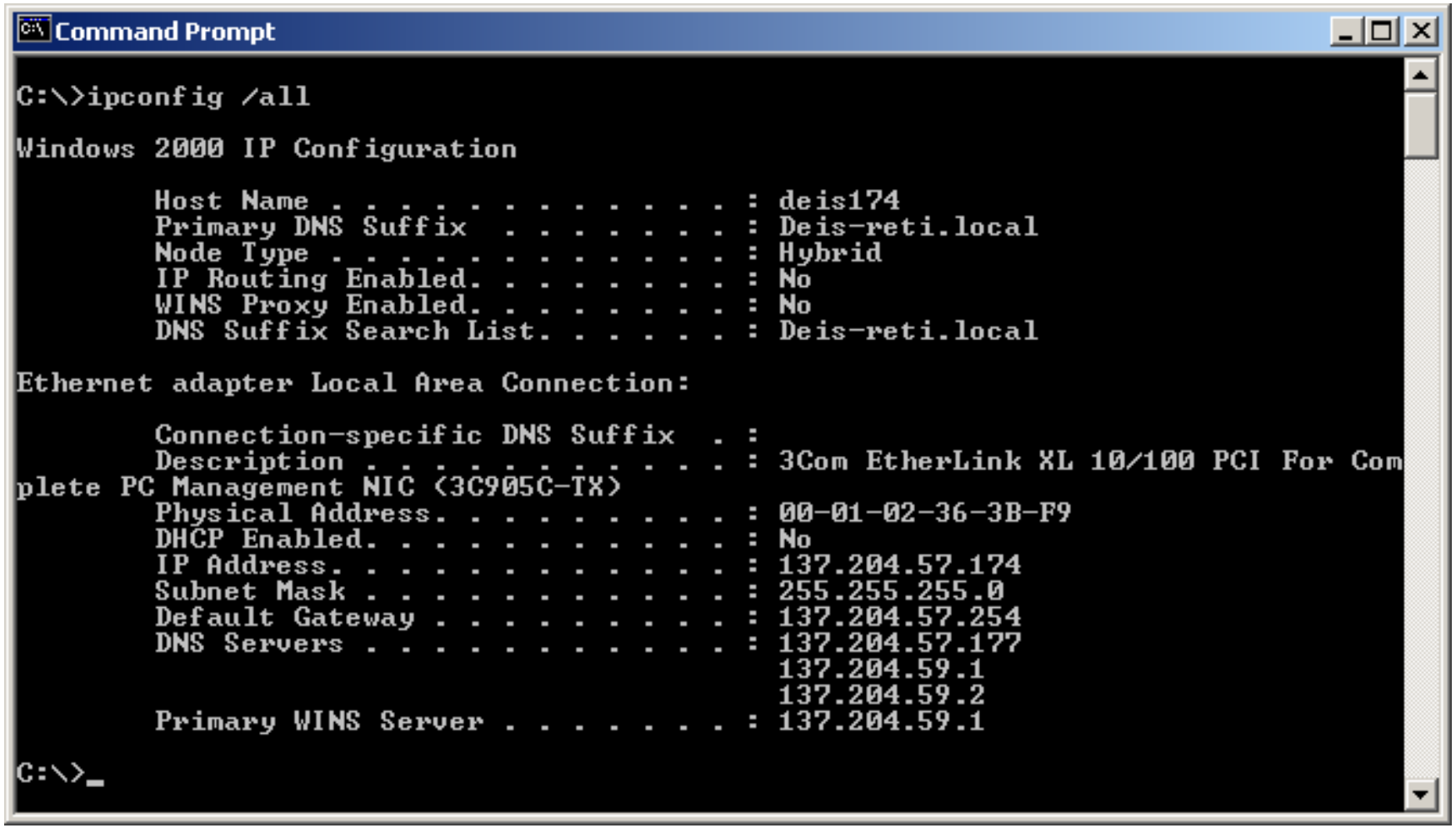
visualizza la configurazione IP corrente di ciascuna interfaccia di rete presente nella macchina:

- indirizzo MAC
- indirizzo IP
- subnet mask
- default gateway
- server DNS
- …

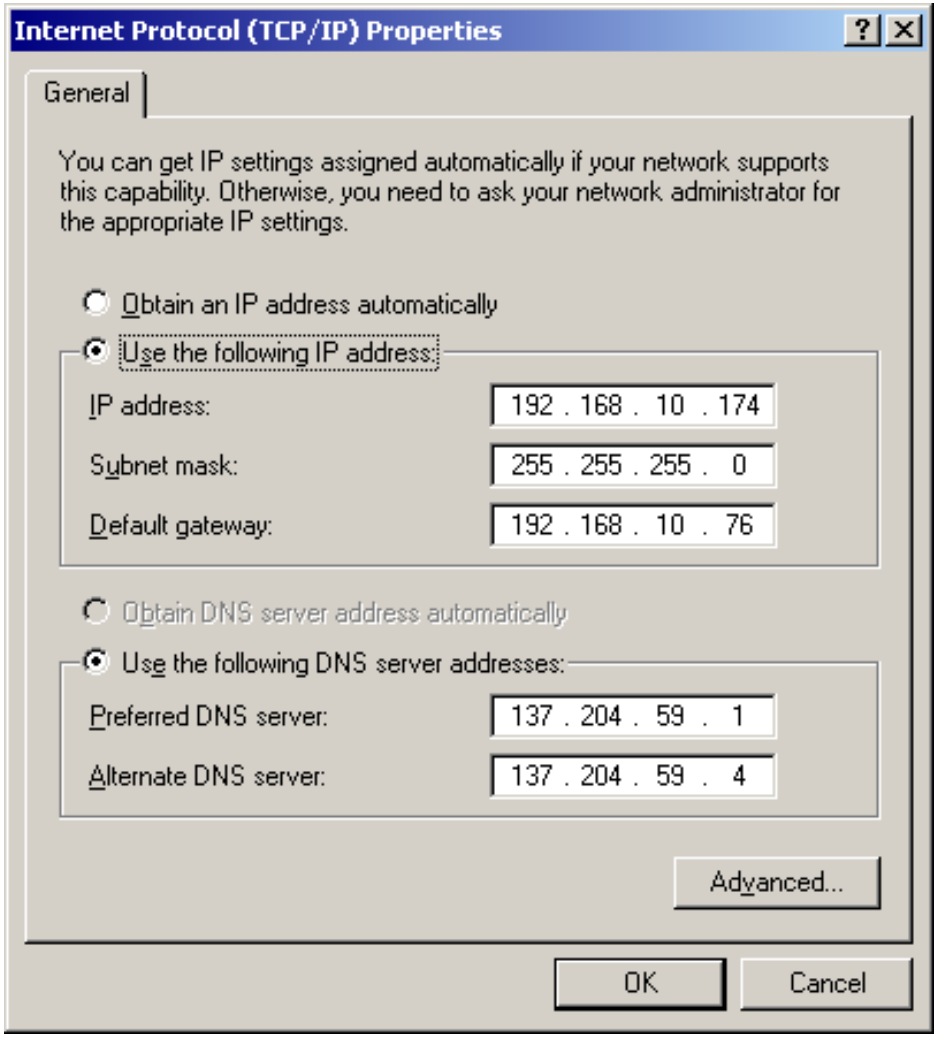
Su Windows 9x: **`winipcfg`**

Su UNIX/LINUX: **`ifconfig`**

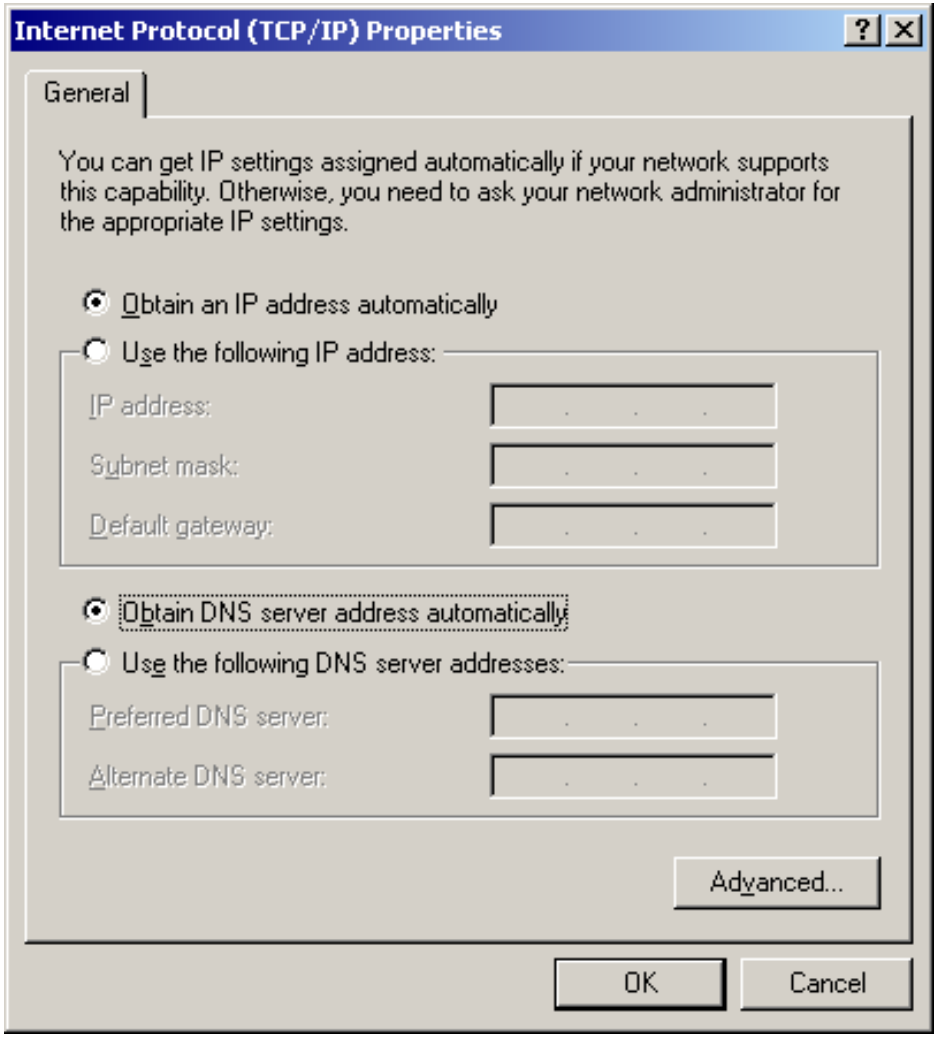
Comando IPCONFIG – Esempio



Configurazione manuale dei parametri IP



Configurazione automatica dei parametri IP



Comando ROUTE

`route print` (Windows)

`route -n` (Linux/Unix)

visualizza la tabella di routing dell'host

`route -p add DEST mask NETMASK GATEWAY`

aggiunge alla tabella di routing Windows una entry permanente relativa alla destinazione **`DEST`** indicandone la **`NETMASK`** e il **`GATEWAY`** attraverso il quale raggiungerla

Esempio 1: host semplice (Windows)

```
===========================================================================
Elenco interfacce
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 d0 59 ce 68 16 ...... Intel 8255x-based Integrated Fast Ethernet
===========================================================================
===========================================================================
Route attive:
Indirizzo rete            Mask              Gateway       Interfac.  Metric
          0.0.0.0          0.0.0.0    192.168.10.76   192.168.10.90       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
    192.168.10.0    255.255.255.0    192.168.10.90   192.168.10.90       1
   192.168.10.90  255.255.255.255        127.0.0.1       127.0.0.1       1
  192.168.10.255  255.255.255.255    192.168.10.90   192.168.10.90       1
        224.0.0.0        224.0.0.0    192.168.10.90   192.168.10.90       1
  255.255.255.255  255.255.255.255    192.168.10.90   192.168.10.90       1
Gateway predefinito:     192.168.10.76
===========================================================================
Route persistenti:
  Nessuno
```

Gateway = IP locale → consegna diretta

Gateway = loopback → consegna agli strati superiori

Altrimenti → consegna indiretta tramite il gateway indicato

Esempio 1: host semplice (Linux)

```
[walter@deis73 walter]$ /sbin/route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.10.76   0.0.0.0         UG    0      0        0 eth0
[walter@deis73 walter]$
```

Gateway = 0.0.0.0 & Iface = eth*n* → consegna diretta

Gateway = 0.0.0.0 & Iface = lo → agli strati superiori

Altrimenti → consegna indiretta tramite quel gateway

Esempio 2: multi-homed host (Linux)

```
[walter@deis76 walter]$ /sbin/route  -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
137.204.57.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         137.204.57.254  0.0.0.0         UG    0      0        0 eth0
[walter@deis76 walter]$
```

Tabella di routing

- Nell'host la tabella di routing si ottiene delle configurazione delle interfacce
  - Numero IP e netmask identificano la network di appartenenza
  - Default gateway identifica il router per la connessione fuori dalla propria network
- E nei router?
  - Le tabelle di routing devono contenere informazioni su più destinazioni dipentemente dalla topologia di rete
    - In casi semplici possono essere create a mano (statiche)
    - Vengono create in modo automatico utilizzando protocolli di routing

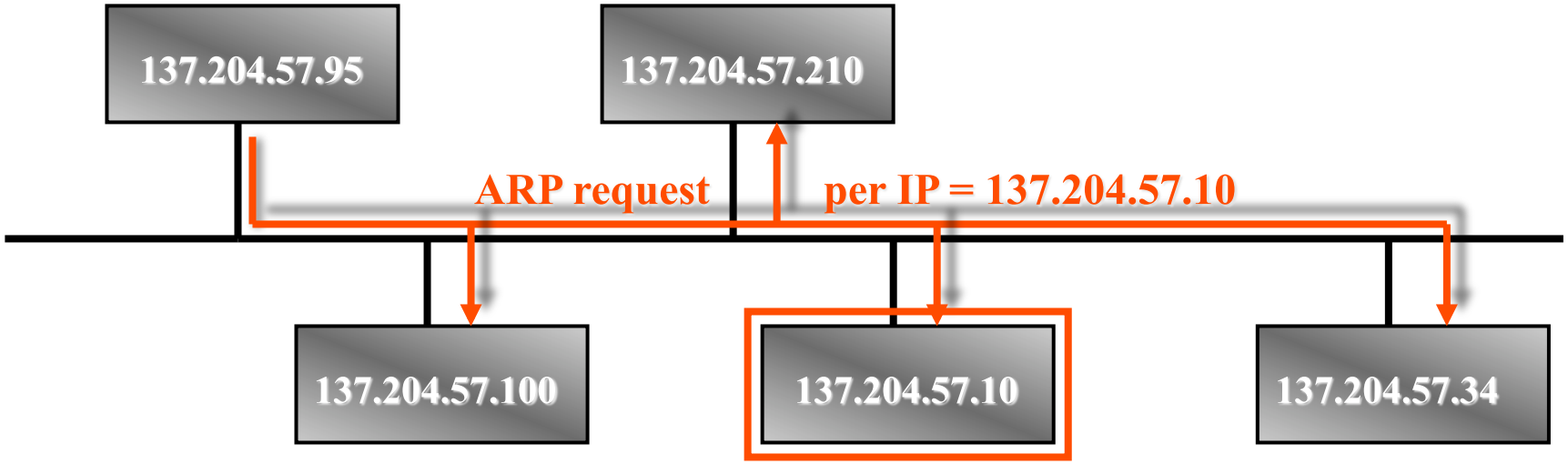
Address Resolution Protocol

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Relazione Indirizzi Fisici – Indirizzi IP

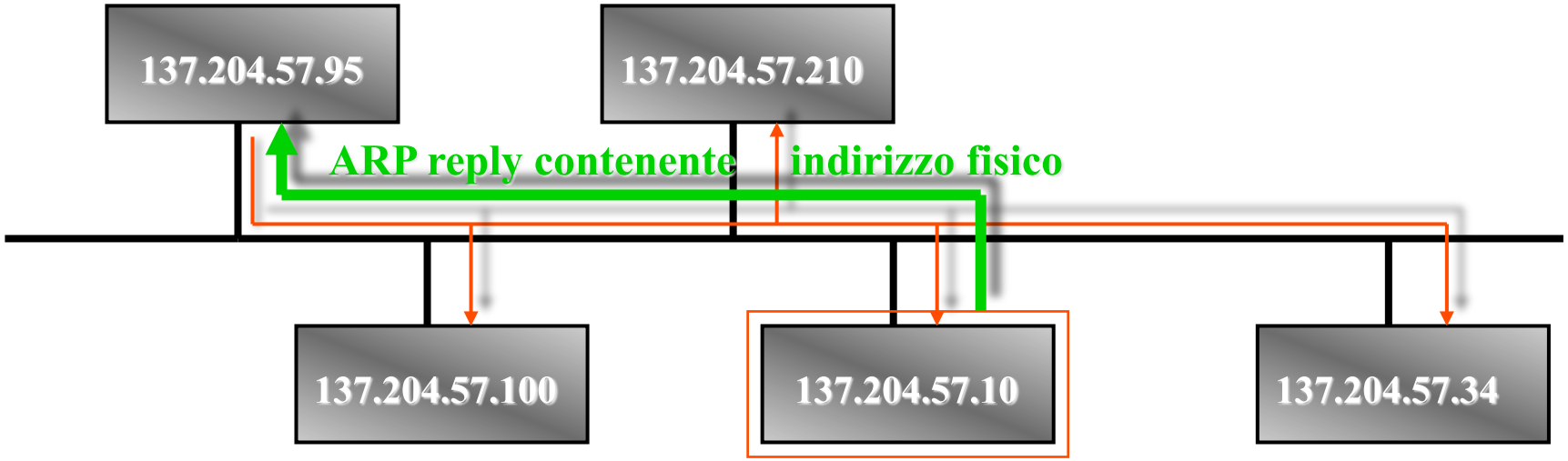
- Software di basso livello nasconde gli indirizzi fisici e consente ai livelli superiori di lavorare solo con indirizzi IP
- Gli host comunicano attraverso una **rete fisica** (ad es. LAN) quindi devono conoscere reciprocamente gli indirizzi fisici
- L'host A vuole mandare datagrammi a B, che si trova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

Address Resolution Protocol – ARP (RFC 826)



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

Address Resolution Protocol - ARP (3)



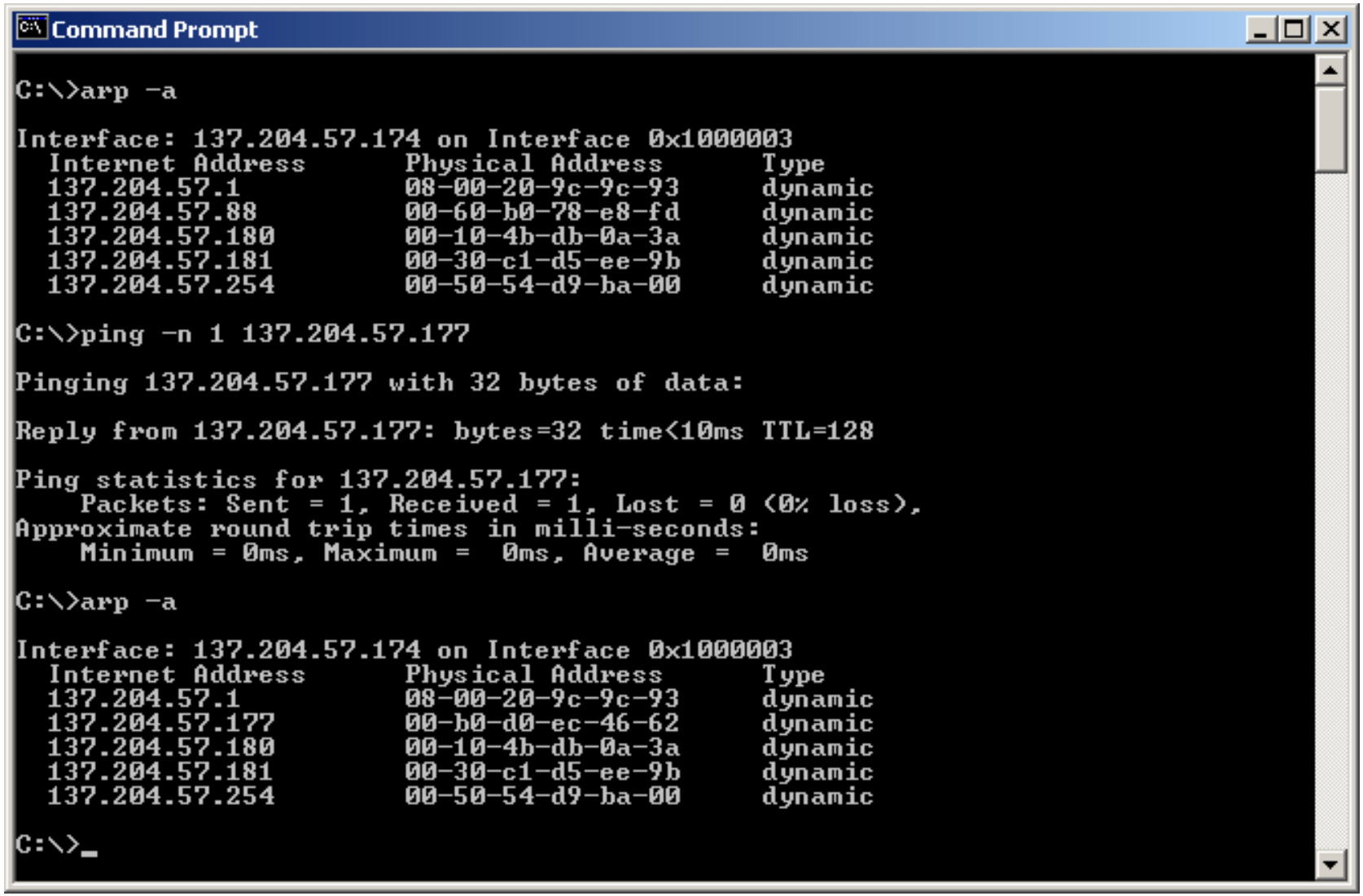
- Il destinatario risponde al mittente, inviando un messaggio (**ARP reply**) che contiene il proprio indirizzo fisico
- Con questo messaggio host sorgente è in grado di associare l'appropriato indirizzo fisico all'IP destinazione
- Ogni host mantiene una tabella (**cache ARP**) con le corrispondenze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

Comando ARP

`arp -a`

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

Comando ARP – Esempio



Il protocollo ICMP

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Il protocollo IP…

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

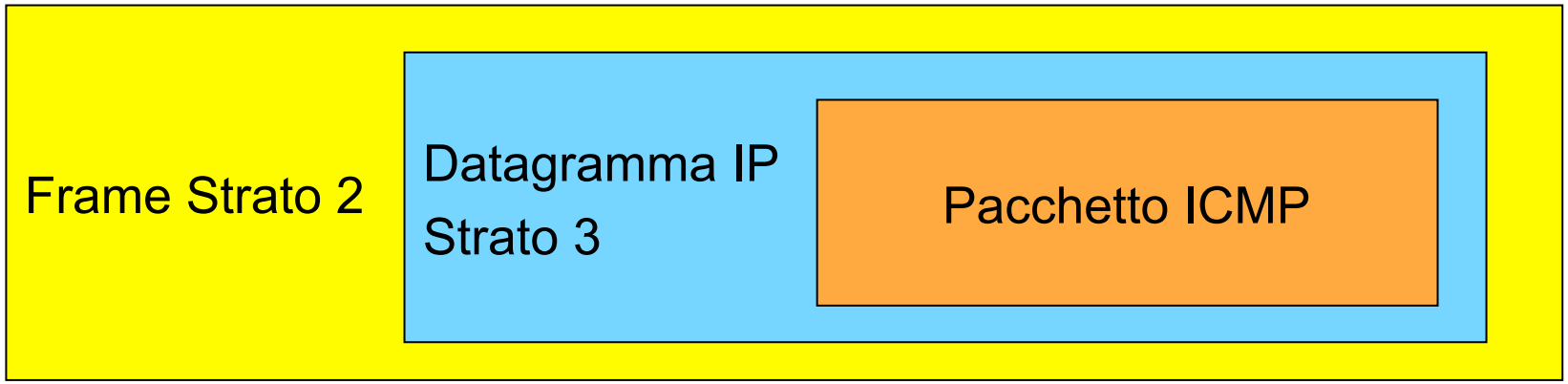
→ **ICMP (Internet Control Message Protocol)**

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

Internet Control Message Protocol (ICMP)

ICMP (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



Formato del pacchetto ICMP

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

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

Messaggi di errore (1)

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

Messaggi di errore (2)

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

Messaggi di richiesta di informazioni (1)

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

Messaggi di richiesta di informazioni (2)

- **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 = $T_{Transmit} - T_{Receive}$

Messaggi di richiesta di informazioni (3)

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

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

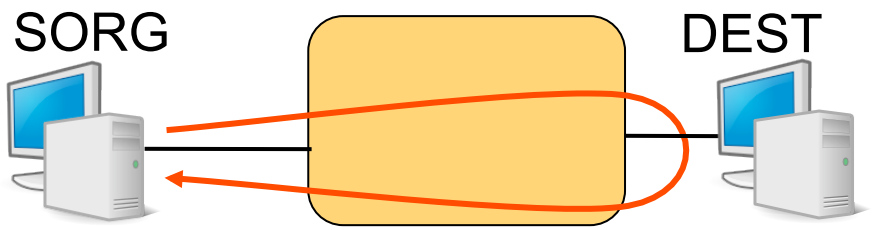
Applicazioni di ICMP

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

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"**

Comando PING – Opzioni

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

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

Comando PING – Output

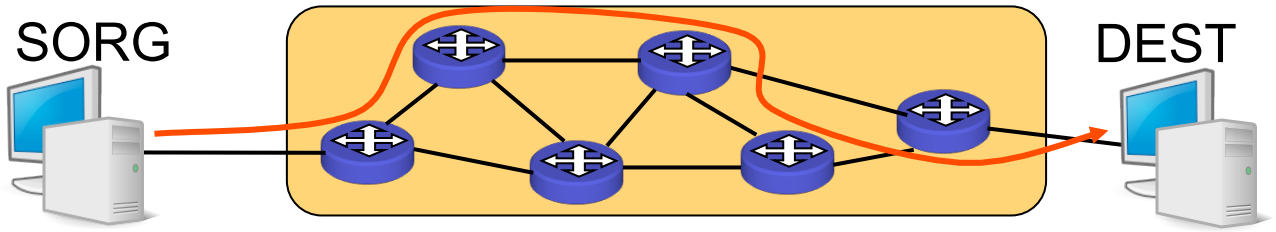
L'output mostra

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

Comando TRACEROUTE

`tracert DEST`

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



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

IPv6

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Problematiche dell'indirizzamento IP

- Mobilità
  - Indirizzi riferiti alla rete di appartenenza
  - Se un host viene spostato in un'altra rete, il suo indirizzo IP deve cambiare
    - Configurazione automatica con DHCP
    - Mobile IP
- Sicurezza
  - Scarsa protezione del datagramma IP (intestazione in chiaro)
    - IPSec applicabile anche a IPv4
- Dimensioni delle reti prefissate
  - Subnetting e CIDR
- Data l'enorme diffusione di Internet, il numero di indirizzi possibili è troppo basso
  - Reti IP private NAT

IPv6

- Stanti i problemi dell'IPv4 attualmente in uso si è lavorato su una nuova versione con i seguenti obiettivi
  - Supportare molti miliardi di host
  - Semplificare il routing
  - Offrire meccanismi di sicurezza
  - Offrire qualità di servizio (multimedialità)
  - Gestire bene multicast e broadcast
  - Consentire la mobilità
  - Fare tutto questo consentendo future evoluzioni e garantendo compatibilità col passato

IPv6: principali caratteristiche

- Indirizzi più lunghi: 16 byte (4 righe o 128 bit)
- Semplificazione dell'intestazione obbligatoria
  - Meno campi che nella v4
  - Non permessa frammentazione
  - Lunghezza minima comunque 10 righe
- Possibilità di diversi header opzionali
  - Alcuni router, per esempio quelli di transito possono ignorare le intestazioni che non li riguardano
- Meccanismi per la sicurezza e qualità di servizio

Non è ancora chiaro se e quando verrà veramente adottato