POLITECNICO DI MILANO

Impianti Informatici





Reti

Cos'è una rete

Rete: insieme di sistemi per l'elaborazione delle informazioni interconnessi tra loro

- Terminali: host
- Edge (isp…)
- Core (router…)
- Interconnessione: Ethernet, wireless,…gsm, umts,…

Obiettivi:

- condividere il software/hardware
  - Stampante
  - NFS, **NAS**,…
- consultare archivi comuni
  - DB remoto,…
- comunicare dati fra i sistemi stessi
  - **Mail**, instant messeging,…

Tipologie di reti

Estensione rete

LAN (Local Area Network)

- Estensione limitata, elevata velocità di trasferimento dei dati (edificio, edifici adiacenti, ~100m)

MAN (Metropolitan Area Network)

- Trasferimento dati ad alta velocità (città, ~ 10 Km), ad esempio utilizzando cavi in F.O. (fibra ottica)
- Può connettere varie LAN all'interno della stessa città

WAN (Wide Area Network)

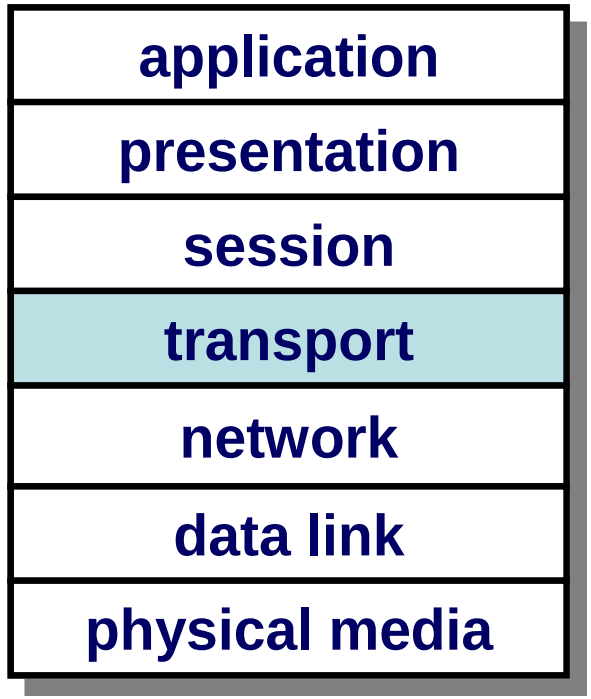
- Consiste solitamente in più LAN e MAN distribuite in un'ampia area geografica
- La più ampia è Internet

- Dimensione
- Tecnologia
  - Velocità
  - Latenza
- Eterogeneità/omogeneità (es.: cluster vs grid computing)

Modello ISO-OSI 1978

OSI (Open System Interconnection) è un modello **teorico** di riferimento definito dalla ISO (International Standard Organization) che definisce le caratteristiche della comunicazione multilivello

- I tre livelli più alti sono application-oriented
- I tre livelli più bassi sono network-oriented
- Il livello di trasporto fa da intermediario



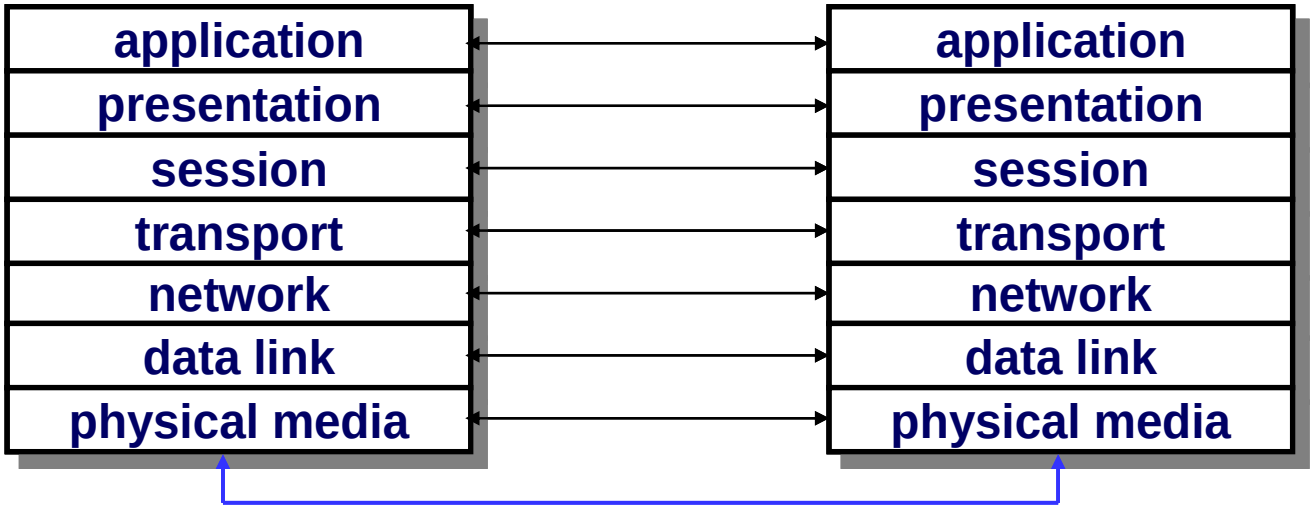
Non è l'implementazione → IETF
→ es.: RFC 793 (tcp)

RFC=request for comments
IETF=Internet Engineering Task Force

Stratificazione

Protocollo: insieme di regole per gestire la comunicazione tra entità che scambiano informazioni

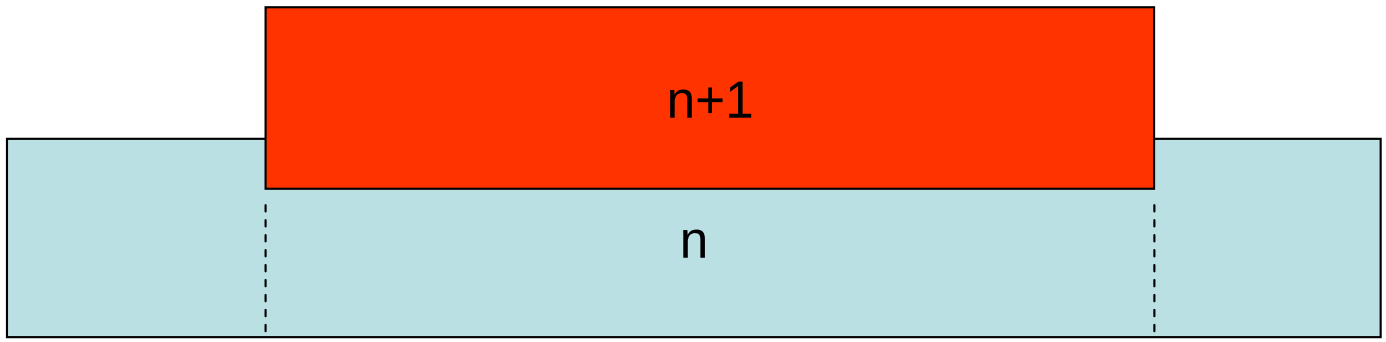
Il livello *n* di un sistema comunica **virtualmente** con il livello *n* di un altro



Principio dell'incapsulamento

Principio dell'**incapsulamento**

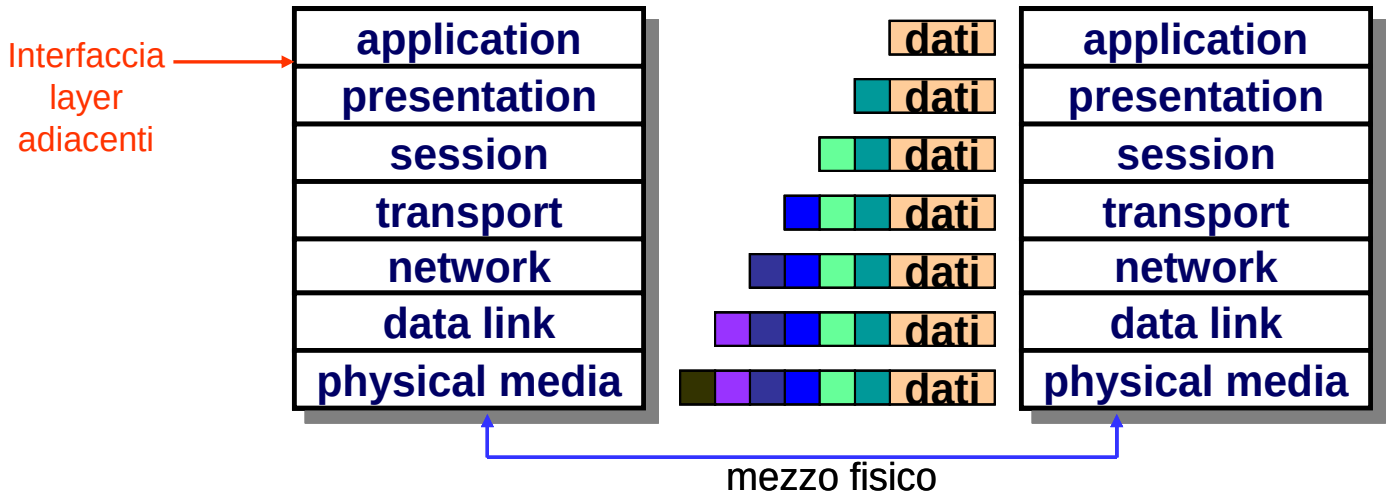
- i messaggi dei livelli superiori vengono *incapsulati* nel campo dati del livello inferiore e trasmessi in maniera *trasparente*
  - non vengono né interpretati né modificati
- Garantisce l'**indipendenza tra layer**



Header e payload di un messaggio

Ogni livello aggiunge ai dati (*payload*) le proprie informazioni di controllo (*header*)

Per ogni coppia di livelli adiacenti esiste un'**interfaccia** per lo scambio delle informazioni



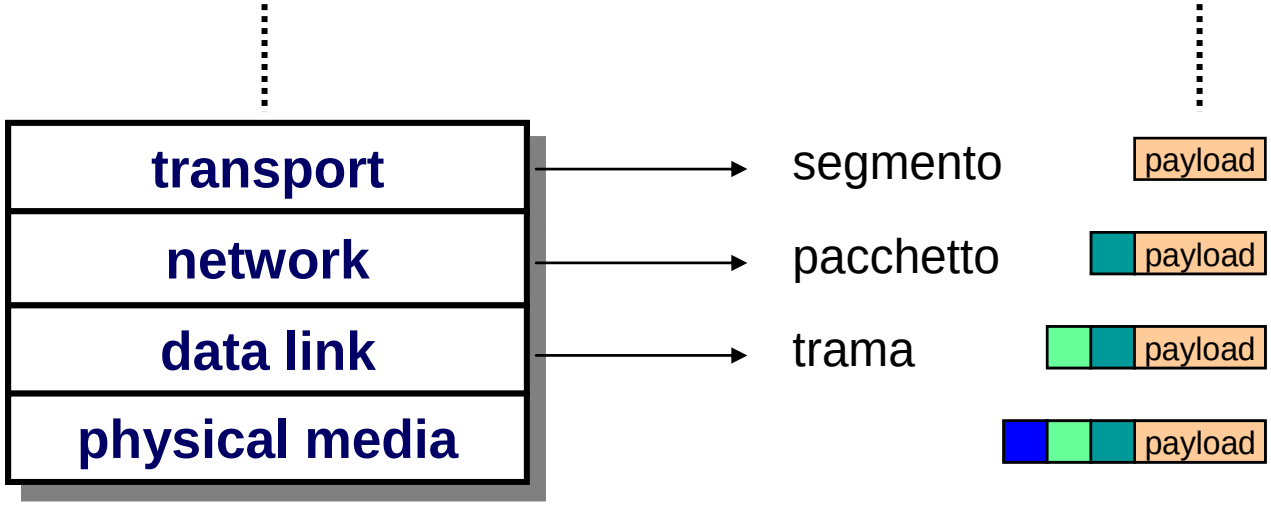
Funzioni dei 7 livelli OSI

Physical Layer: interfaccia con il mezzo fisico

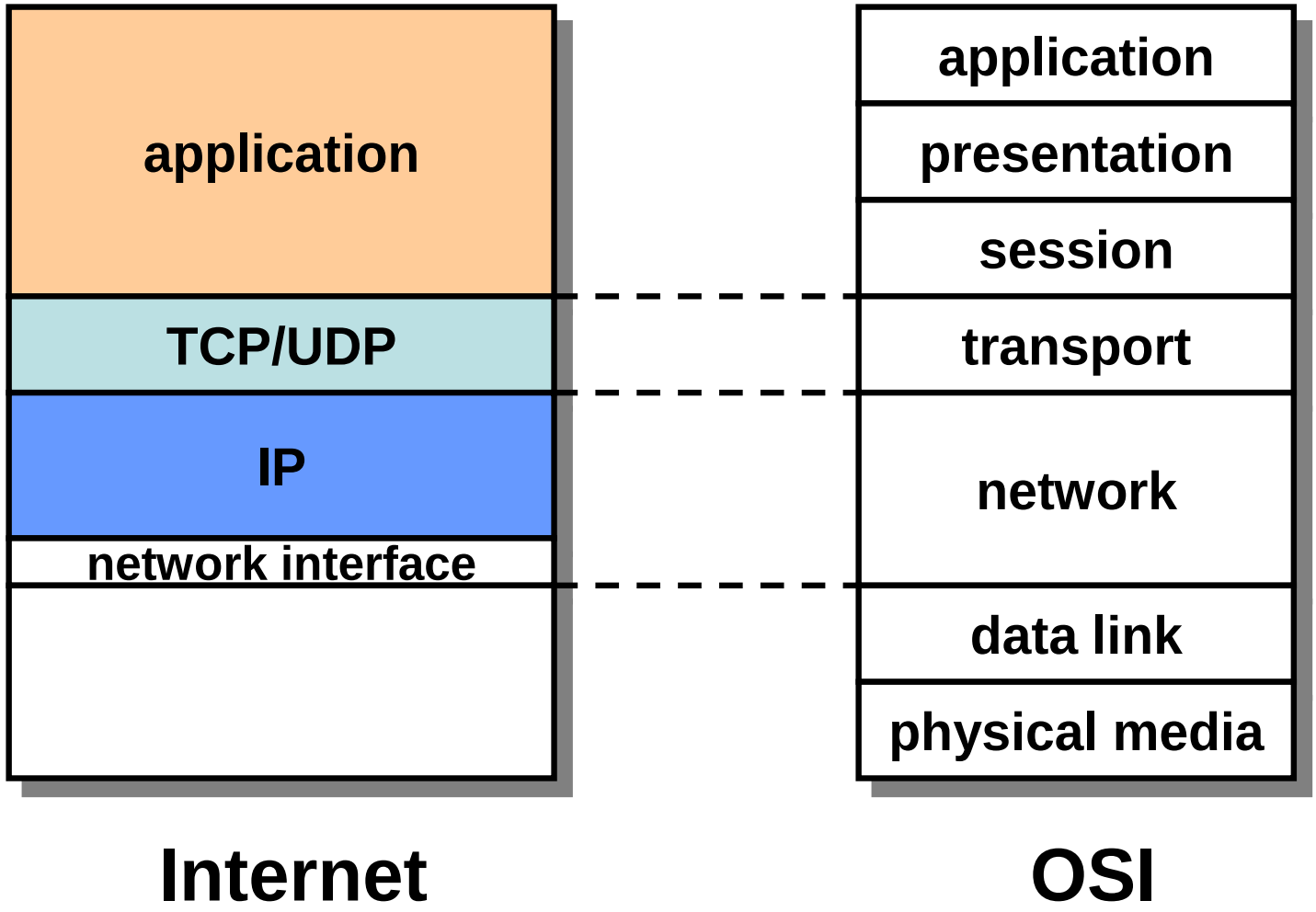
Data Link Control: comunicazione *point-to-point*

Network Layer: instradamento dei *pacchetti* da sorgente a destinazione

Transport Layer: crea la connessione logica *end-to-end*



I protocolli Internet nel modello OSI



Indirizzo IP

Ogni nodo della rete è identificato da un indirizzo IP.

- Un nodo che è collegato a più reti (multi homed host) ha un indirizzo per ogni interfaccia

Un indirizzo è una stringa lunga 32 bit (nel caso IPv4)

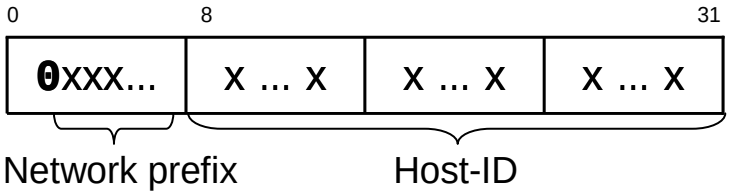
L'indirizzo IP è solitamente espresso nella notazione decimale a gruppi di 8 bit (*dotted decimal notation*):

8 bit . 8 bit . 8bit . 8 bit

- Ad esempio: 131.175.54.140

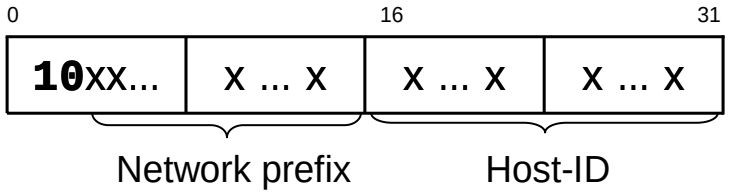
Indirizzi IP classful

Classe A



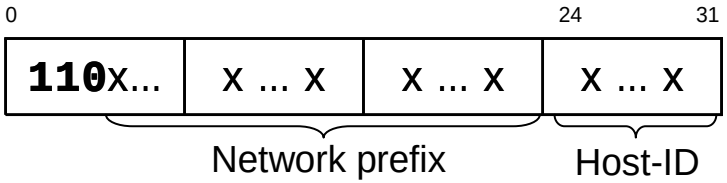
2^7 reti
2^{24} indirizzi in ogni rete

Classe B



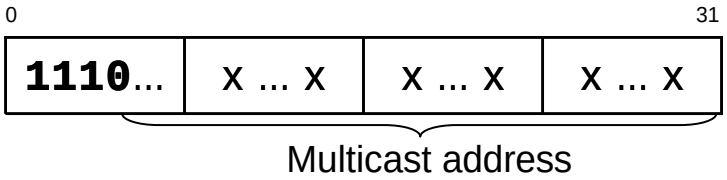
2^{14} reti
2^{16} indirizzi in ogni rete

Classe C



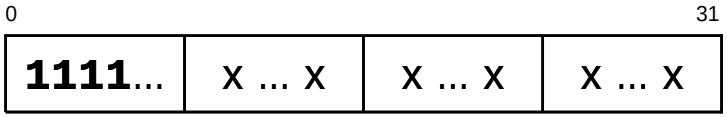
2^{21} reti
2^{8} indirizzi in ogni rete

Classe D



2^{28} gruppi multicast

Classe E



destinato per usi futuri

Internet Protocol

È un protocollo di rete (livello 3 modello OSI) a pacchetto

- Si occupa della consegna dei pacchetti tra due nodi della rete
- È un protocollo di *interconnessione tra reti* (*Inter-Net*working *Protocol*), nato per collegare reti eterogenee per tecnologia, prestazioni, gestione.

Caratteristiche Internet Protocol

Servizio *unreliable*

- È compito dei livelli superiori fornire particolari garanzie

Funzioni di *instradamento e indirizzamento*

- Identifica i nodi sorgente e destinazione mediante un indirizzo IP
- Consente ad un pacchetto di circolare dalla sorgente alla destinazione

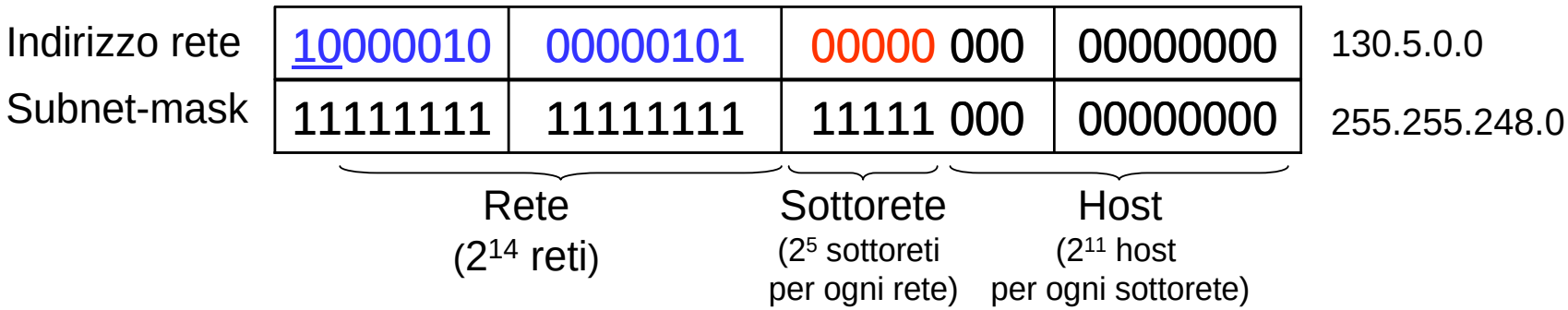
Esegue *frammentazione* e riassemblamento dei pacchetti

Subnetting

Consente di partizionare lo spazio degli indirizzi per creare delle *sottoreti*

Mediante una **subnet-mask** si allunga il *network prefix* con un nuovo campo che individua la sottorete (*subnet prefix*)

La lunghezza della subnet-mask viene solitamente indicata con **/n** (ad es: 175.16.1.5/16)

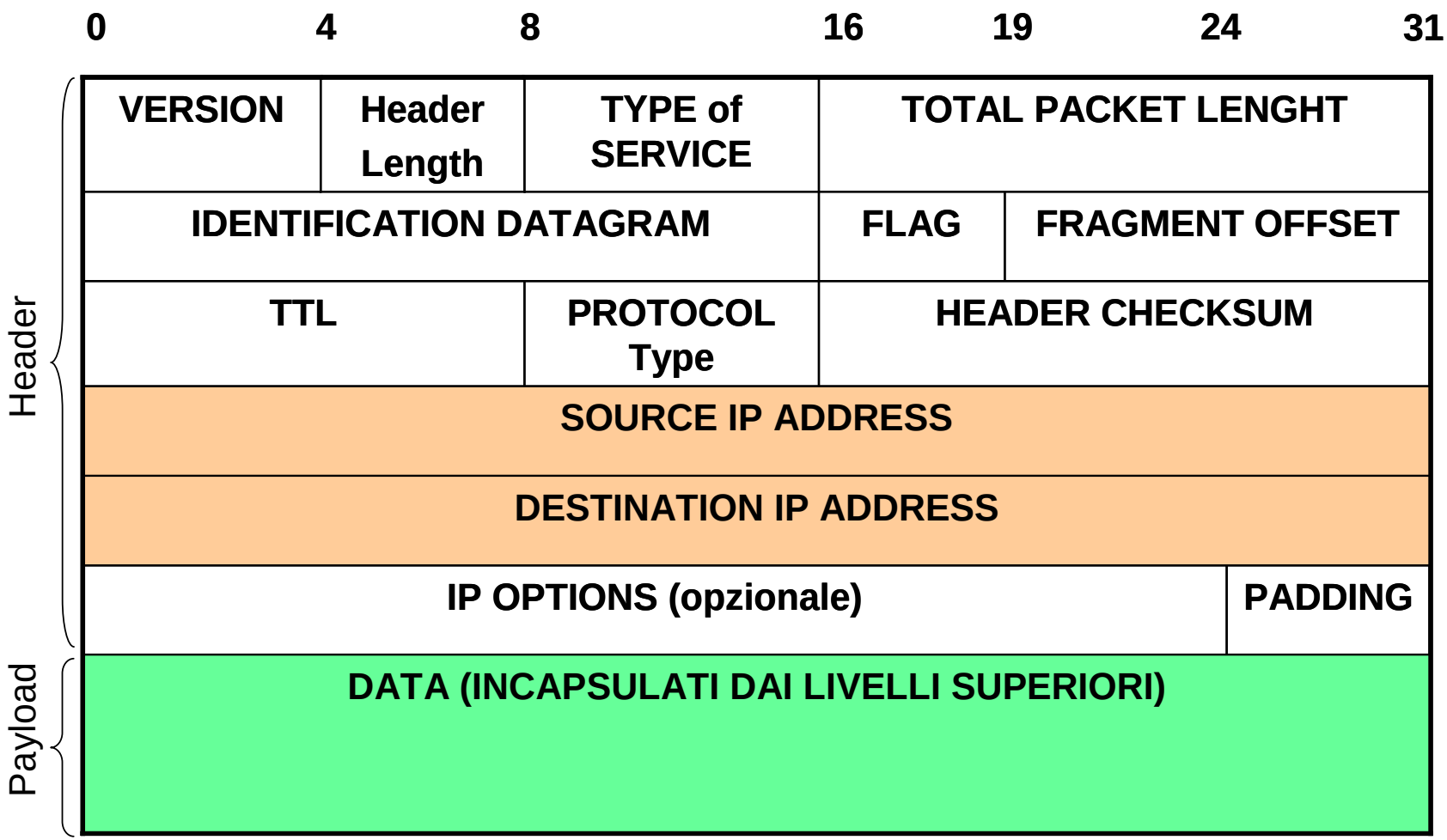


Indirizzi IP ad uso “privato”

Esistono degli intervalli di indirizzi “privati”

- Questi indirizzi non possono essere utilizzati su internet, ma chiunque è libero di utilizzarli per una rete privata, che sia domestica o di una grande azienda:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 169.254.0.0/16
- Un computer che utilizzi uno di questi indirizzi non potrà collegarsi direttamente ad un computer su un indirizzo pubblico, a meno di utilizzare particolari meccanismi:
  - NAT (o NAPT)
  - Proxy

Struttura di un pacchetto IP

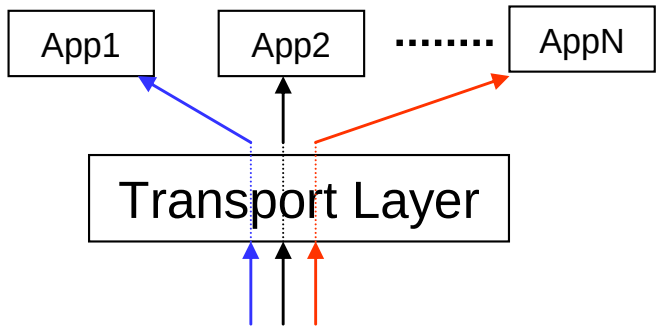


Protocolli di trasporto

Creano una connessione logica (end-to-end) tra sorgente e destinazione

La sorgente, così come la destinazione, è identificata da un *socket* (indirizzo IP + porta)

- L'IP identifica il nodo
- La porta identifica il *servizio* richiesto
  - il livello di trasporto esegue la *demultiplazione* (e *multiplazione*) per inviare i dati alla corretta applicazione



Protocolli TCP e UDP

La connessione logica è descritta in modo completo da una coppia di socket

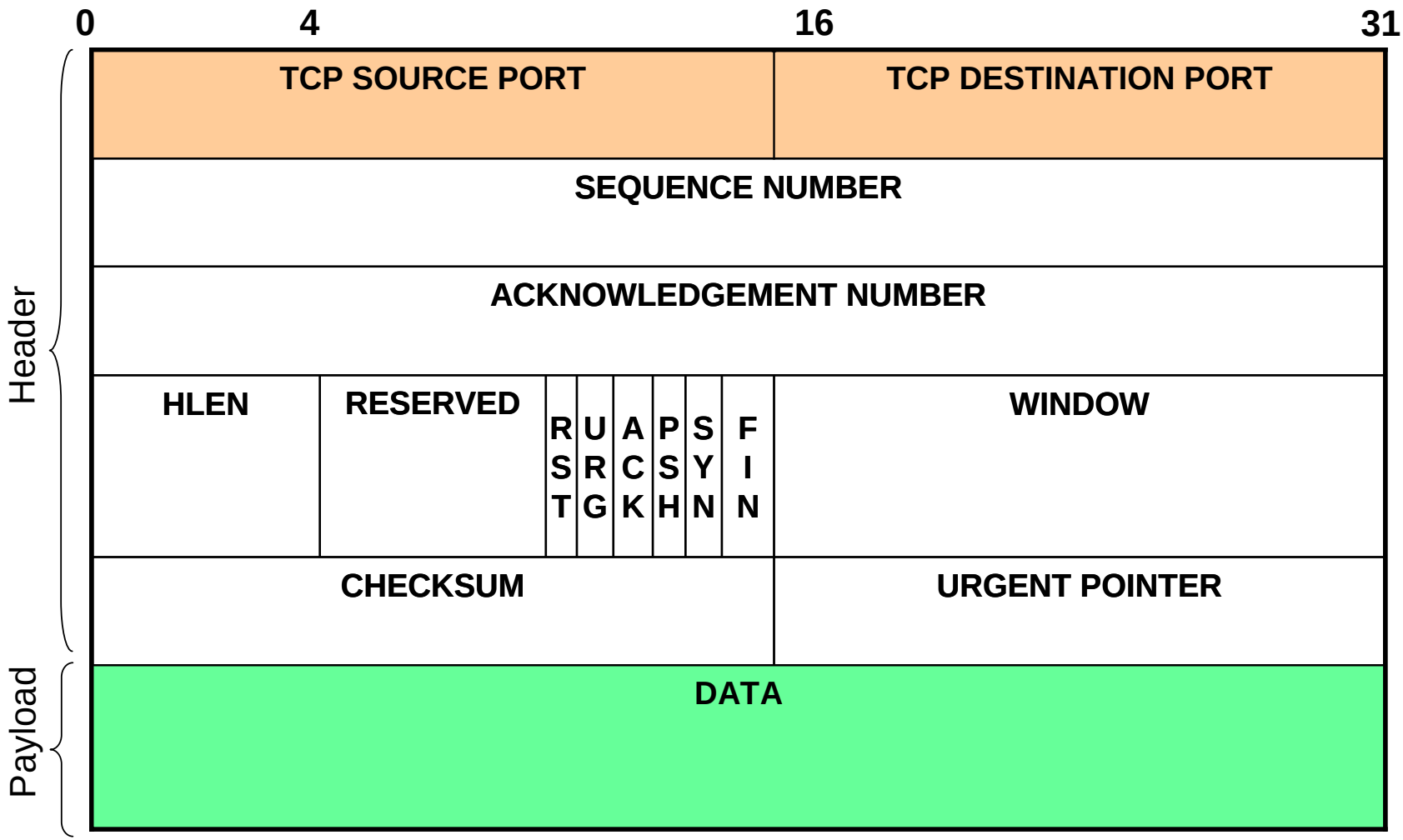
UDP (User Datagram Protocol):

- *Segmentazione*
- Multiplazione/demultiplazione

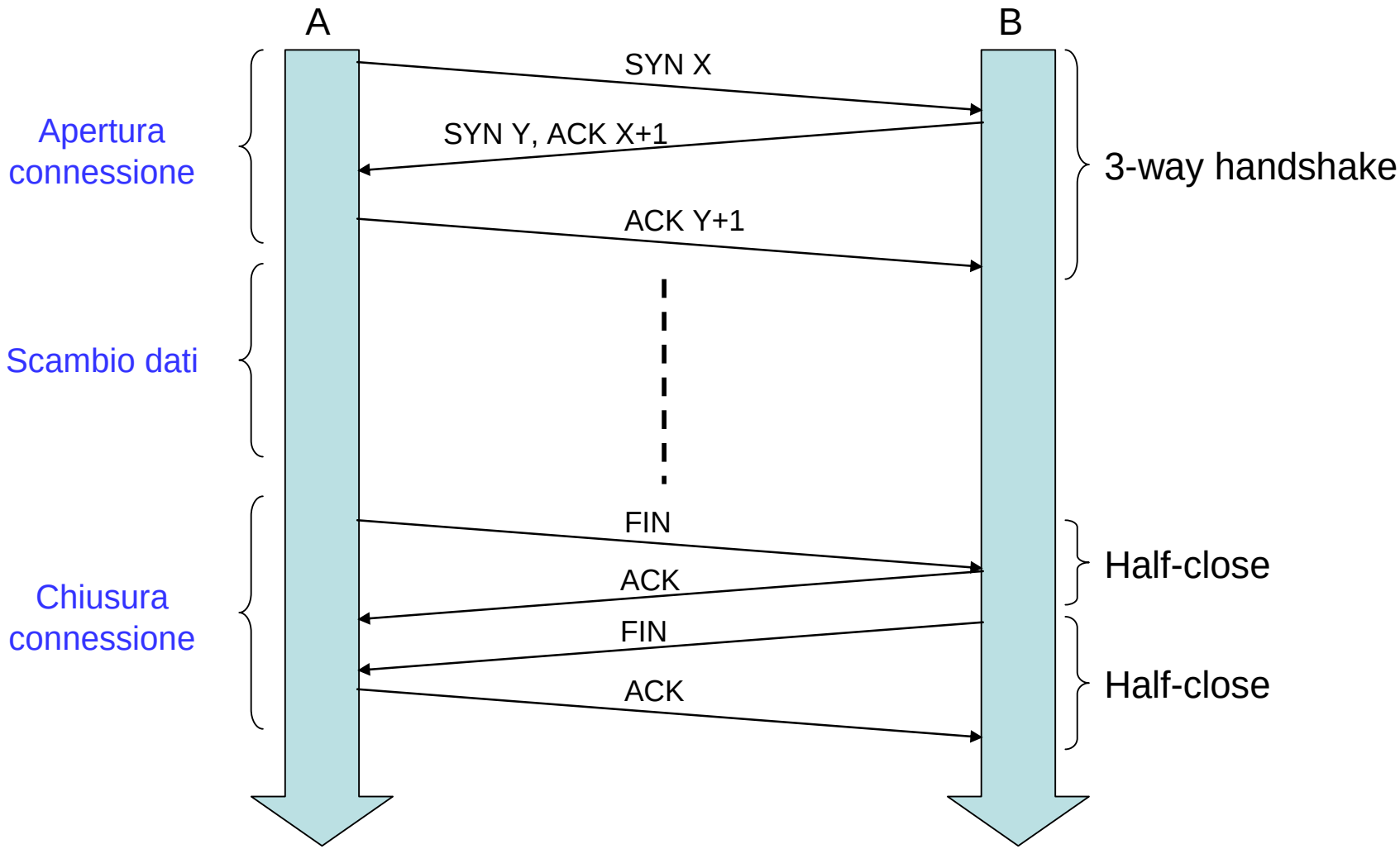
TCP (Trasmission Control Protocol):

- È *connection-oriented* (virtual circuit)
- Offre le stesse funzioni di UDP + un servizio *reliable:*
  - Controllo di flusso
  - Controllo di sequenza
  - Controllo di congestione
  - Correttezza delle informazioni (gestisce perdite e duplicazioni)

Struttura di un segmento TCP



Apertura e chiusura di una connessione TCP



Impianti Informatici

POLITECNICO DI MILANO





Reti

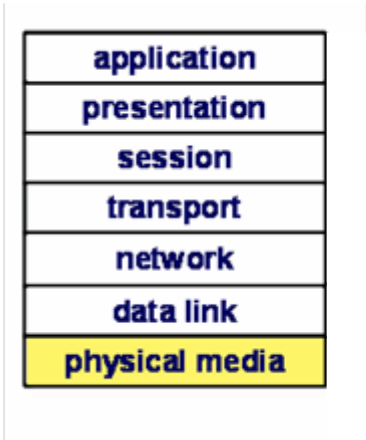
HUB **(livello 1)**

Opera al livello fisico dello stack ISO-OSI

È un semplice *ripetitore* di segnale

- Anche denominato *accentratore di rete*

Unisce LAN perfettamente identiche tra loro (con stesso protocollo MAC)

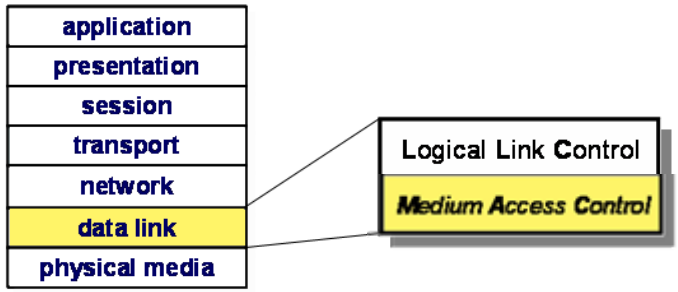


BRIDGE/SWITCH **(livello 2)**

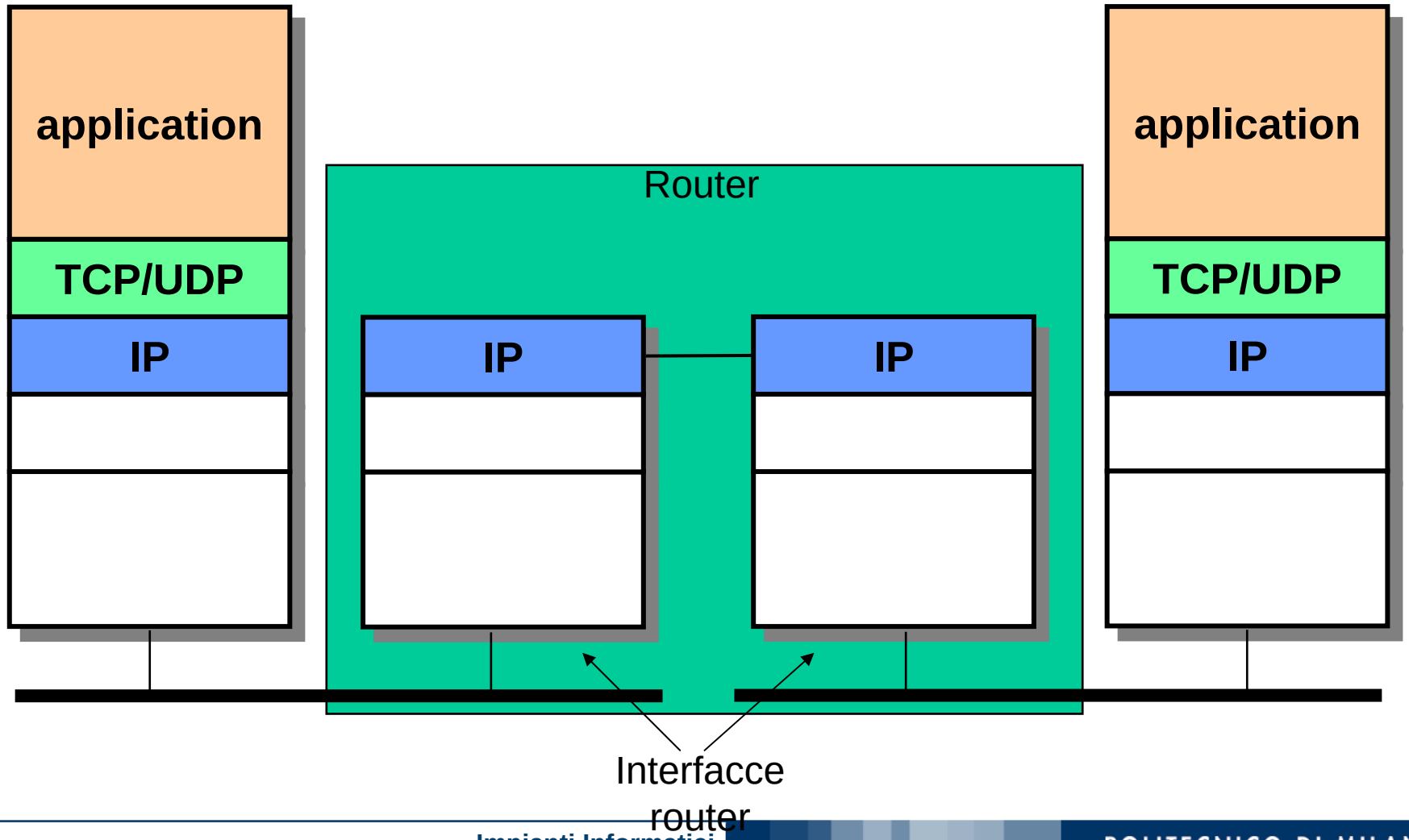
Opera a livello MAC (Medium Access Control) del Data Link Layer

Ha nozioni di *trama*, quindi non replica semplicemente il segnale

Unisce LAN che usano gli stessi protocolli nei layer superiori a quello MAC



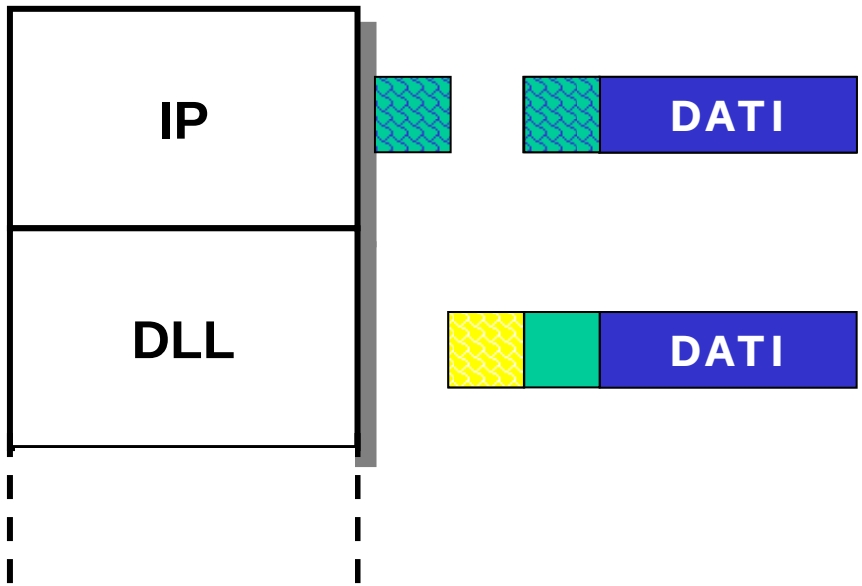
ROUTER **(livello 3)**



Funzionalità dei router

I router eseguono il routing dei pacchetti IP tra le reti ad essi connesse:

- Rimuovono l'intestazione di livello 2
- Esaminano l'intestazione di livello 3 per eseguire l'instradamento
- Modificano l'intestazione di livello 3 (ad es. TTL)
- Inseriscono una nuova intestazione di livello 2



Funzionalità dei router

Hanno algoritmi di instradamento sofisticati

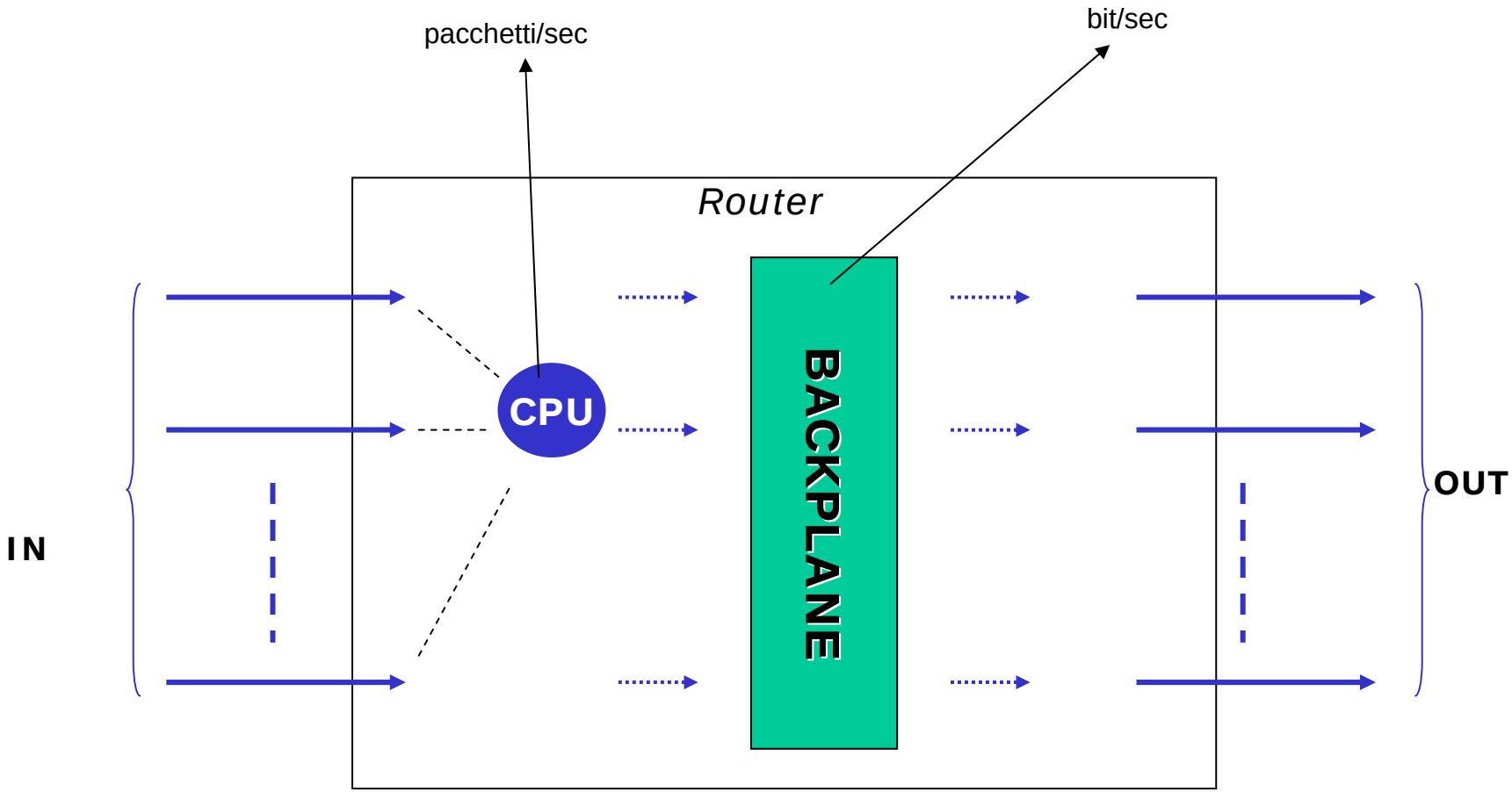
Se necessario, frammentano ulteriormente i pacchetti per adattarsi alla rete fisica su cui trasmette

Si utilizzano solitamente per interconnessioni MAN/WAN

I router attuali offrono generalmente anche funzioni aggiuntive al puro instradamento,

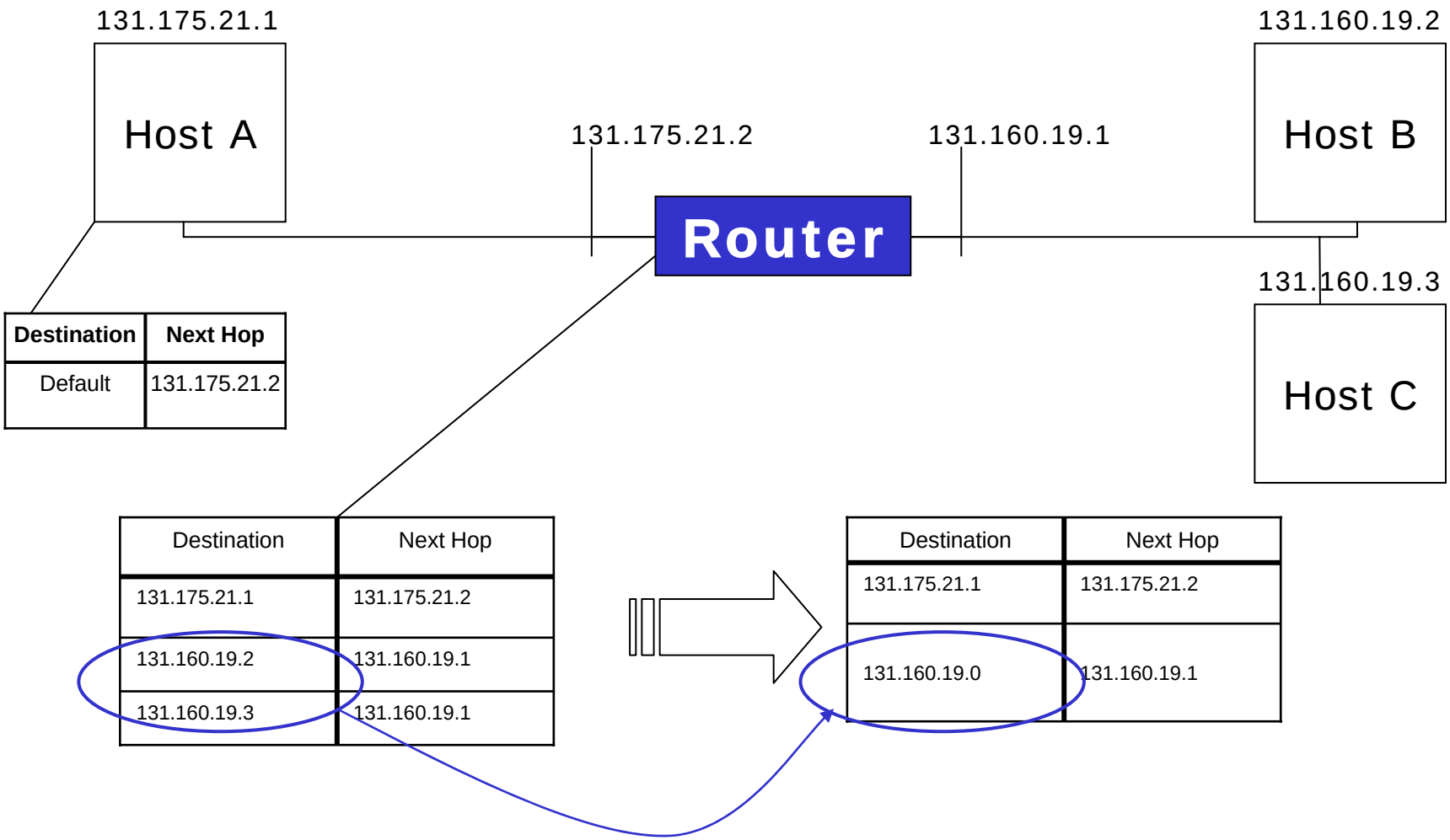
- Esse richiedono l'integrazione di protocolli superiori al livello di rete (ad esempio quando fungono da NAT-BOX)

Struttura router



A seconda del traffico, bottleneck in
- cpu
- backplane

Esempio tabella di routing



Router: Migrazione IPv4 → IPv6

Migrazione istantanea non fattibile

Tecniche di migrazione:

- Dual Protocol
  - Ogni nodo deve implementare sia IPv4 che IPv6

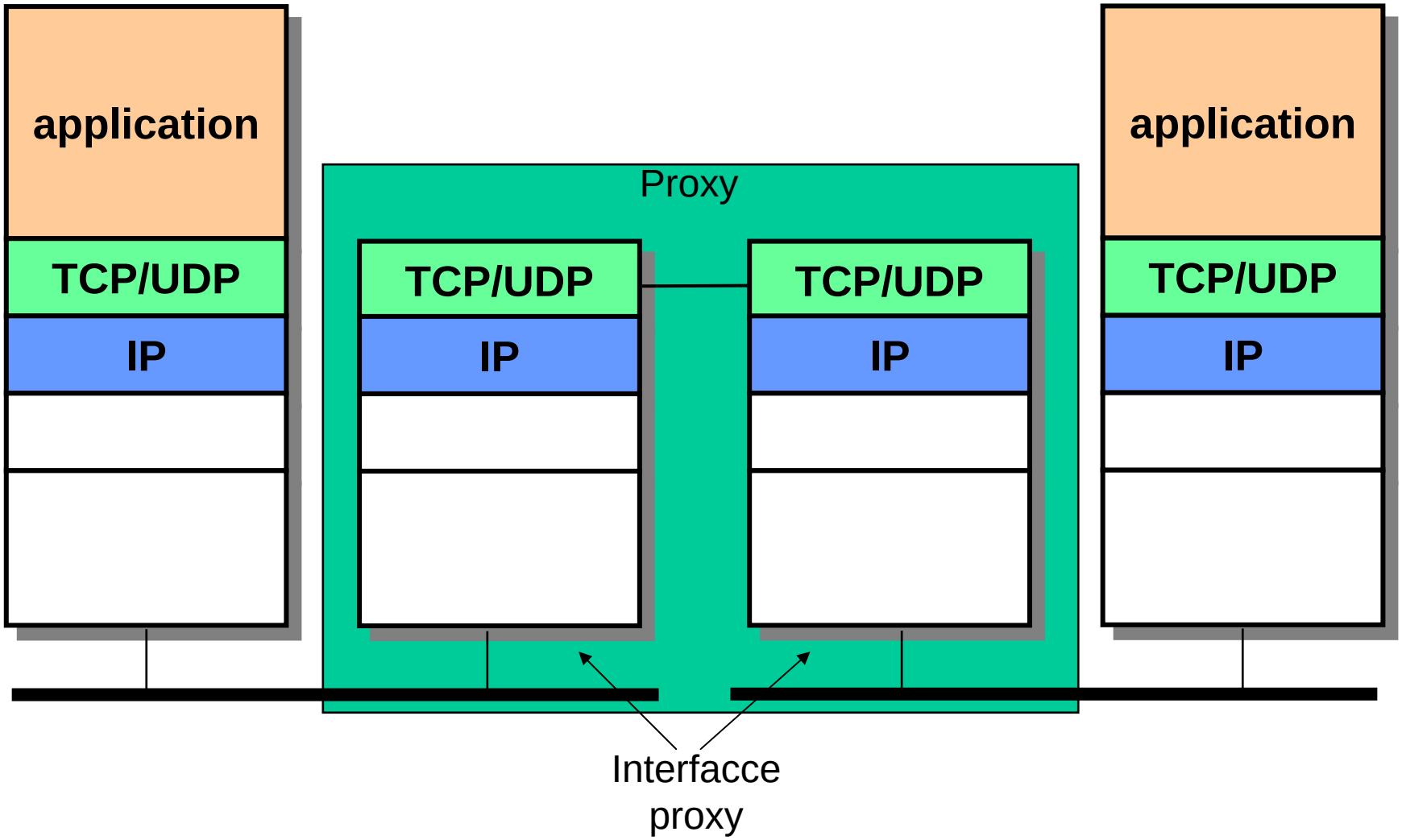
  - Costi implementazione
  - Configurazione
  - Amministrazione/manutenzione

- IPv4 Tunnelling
  - Edge router con stack IPv4 e IPv6

  Soluzione ibrida

- Protocol Translation
  - Incompatibilità tra gli header
  - Impossibilità di usare i nuovi campi di IPv6

PROXY **(livello 4)**



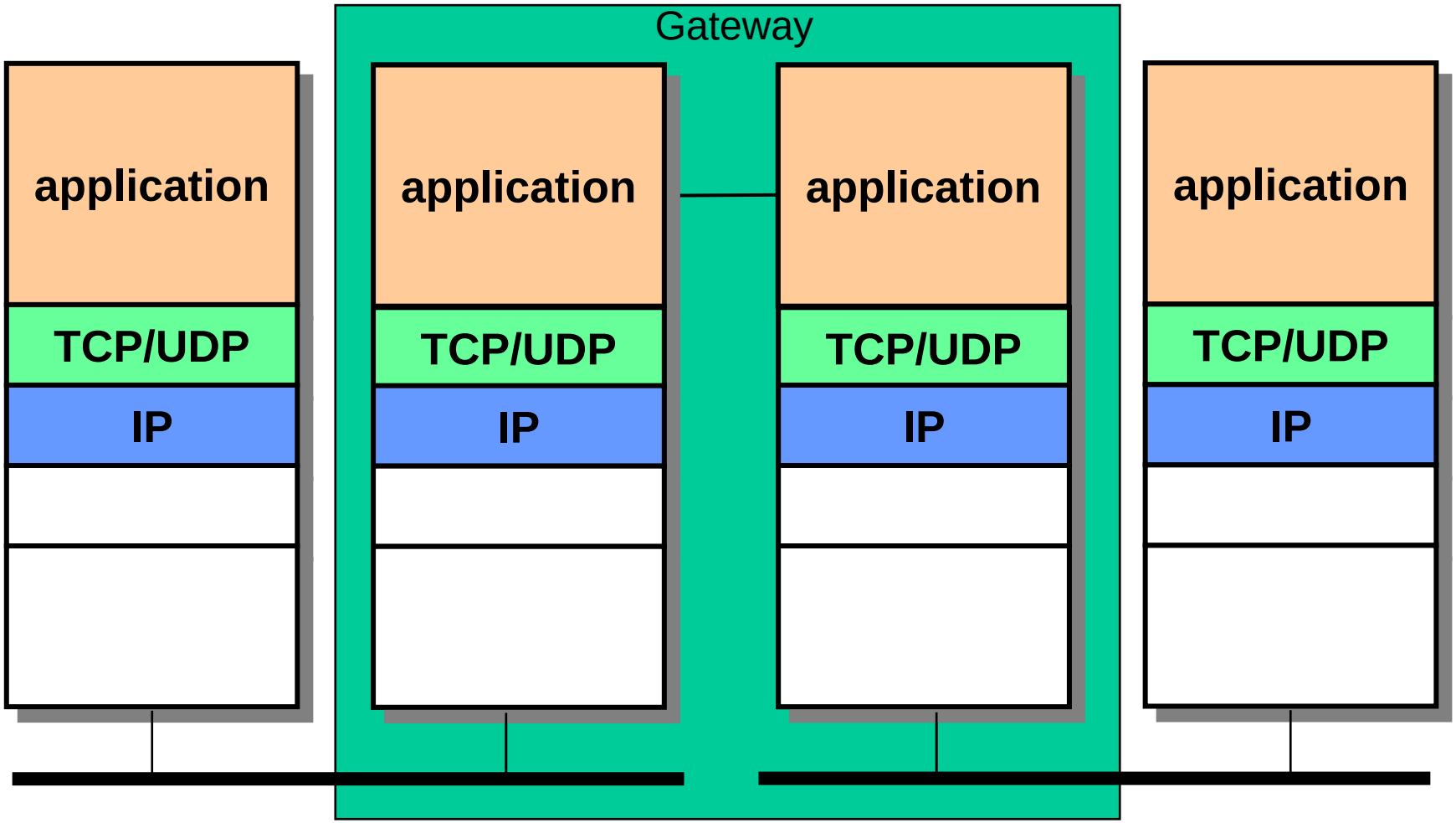
PROXY

Sono in grado di ricostruire un intero messaggio o flusso di dati scambiato tra due reti

Possono (limitatamente e con eventuali “plugin”) analizzare e modificare il flusso informativo tra due reti o stazioni

- a livello di proxy è possibile applicare un antivirus alle e-mail in transito
- a livello di proxy è possibile decidere se un utente ha il diritto di visualizzare una certa pagina Web
- intermediario tra nodi
  - **Web caching** (pagine + connessioni)
  - **Web replication** (CDN)
  - **User proxy** (single sign-on, delegation)
  - In alternativa al NATTING

GATEWAY APPL. **(livello 7)**



GATEWAY APPLICATIVO

I gateway applicativi interconnettono applicazioni diverse (agiscono da interfaccia tra protocolli differenti)

Esempio: posta elettronica (via web mail)

- L'e-mail si avvale di protocolli applicativi (SMTP, POP, IMAP) e di applicazioni client/server adatte a questi protocolli
- Un gateway Web permette di leggere e inviare e-mail usando un protocollo applicativo totalmente diverso (HTTP) e applicazioni client/server totalmente diverse (Web browser/Web server)

Esempio: sistemi legacy

Differenza tra gateway e router

Il gateway opera a livello 7 dello stack ISO-OSI

- È in grado di interpretare i dati ricevuti e in parte di modificarli prima di trasmetterli

Il router opera a livello 3 dello stack ISO-OSI

- Instrada i pacchetti
- Non modifica il flusso di dati

NB: l'apparato convenzionalmente chiamato "default gateway" è quindi un *default* router

Network Address (and Port) Translation

Il NAT è una tecnica, che consiste nel modificare gli indirizzi IP di un pacchetto in transito

IP *masquerading*

- Particolare utilizzo del NATTING che consente ai molteplici computer di una rete privata di utilizzare un singolo indirizzo IP (pubblico) per accedere ad Internet
- Risolve il problema del “limitato” numero di indirizzi IP disponibili
- Nasconde dall’esterno la rete privata

Funzionamento di NAT

Cambia alcune informazioni negli header dei messaggi:

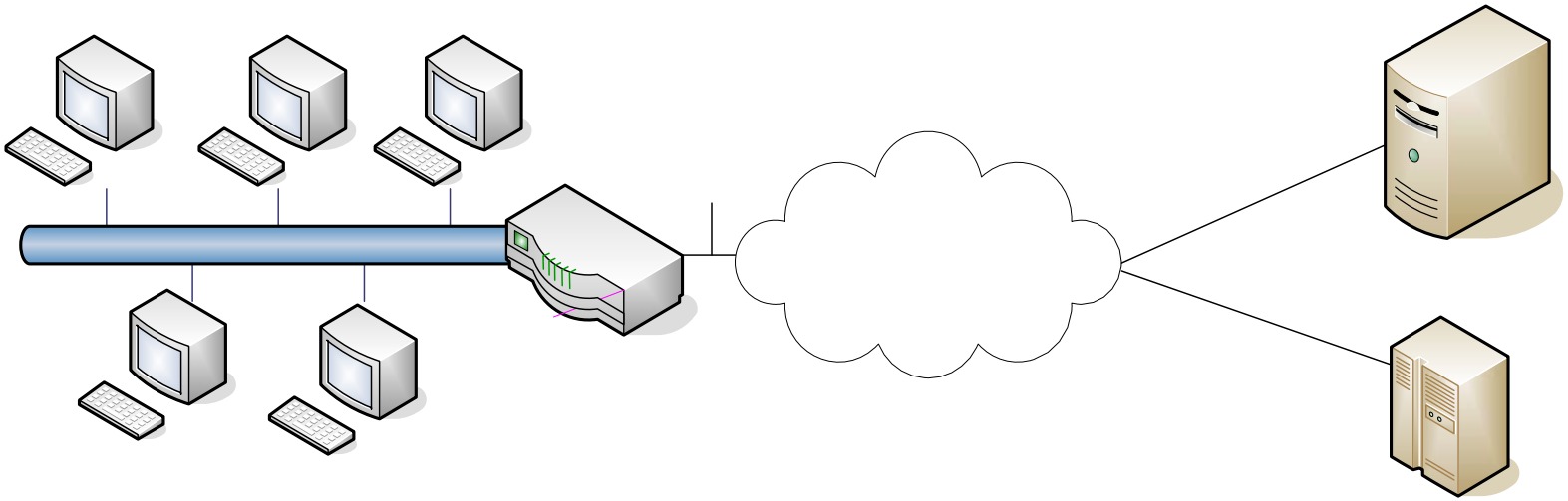
- Source address -> Indirizzo IP pubblico
- Source port -> Una porta qualsiasi disponibile

Memorizza in apposite tabelle le modifiche apportate

- Tali informazioni vengono utilizzate per traslare i messaggi di risposta, così da farli pervenire all'host (e al servizio) corretto
- A seconda che si stia modificando l'indirizzo IP sorgente o destinazione, si parla di:
  - Source NAT
  - Destination NAT

Esempio di NAT

Private Address	Private Port	External Address	Ext. Port	Protocol Used	NAT Address	NAT Port
192.168.0.1	13	81.231.110.1	80	TCP	91.168.0.15	231
192.168.0.6	66	81.231.110.1	80	TCP	91.168.0.15	115
192.168.0.4	12	211.1.9.115	21	TCP	91.168.0.15	231



IPv6 (Next Generation Protocol)

Limitazioni IPv4:

- Numero di indirizzi limitato (2^{32} indirizzi non sono più sufficienti)
  - Espansione del numero di utenti della Rete
  - Sottosfruttamento degli indirizzi potenzialmente disponibili
    - le più vecchie assegnazioni disponevano solo di indirizzi classful (/8 /16 /24)
  - Parte dei 2^{32} indirizzi è destinata per:
    - Reti private
    - Indirizzi multicast
- Esplosione delle tabelle di routing
- Esigenza di nuove funzionalità:
  - Applicazioni Real Time
  - QoS
  - Security (autenticazione, crittografia)
  - Supporto per il roaming

Caratteristiche IPv6

Servizio connectionless (come IPv4)

Indirizzo a 128 bit

- Solitamente in 8 gruppi da 4 cifre esadecimali (2001:0db8:85a3:08d3:1319:8a2e:0370:7344)
- Introduce gli indirizzi *anycast*
- Elimina gli indirizzi *broadcast*

Indirizzamento gerarchico (indirizzo strutturato)

Sicurezza integrata: autenticazione, cifratura

Header flessibile:

- Base header
- Extension headers: fragment, routing, authentication,…

Funzionalità per l'allocazione delle risorse (QoS):

- Classe / priorità
- Flow label

Supporto per il roaming

Amministrazione della rete: autoconfigurazione (plug&play)

Domain Name System

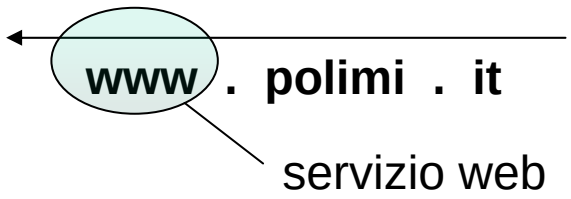
È un protocollo **applicativo** che si appoggia su **UDP**

Consente di utilizzare stringhe, anziché indirizzi IP, per identificare un host

Associa all'indirizzo numerico di un host un nome simbolico (ad esempio **www.polimi.it**) composto da una serie di *label* (www, polimi e it sono label)

Ogni *label* è assegnata da una *naming authority*

- Ciascuna di esse è strettamente inclusa in una o più authority più grandi, così da creare una *gerarchia* di nomi
- Tale gerarchia di inclusione va da destra a sinistra: la prima label (a sinistra) identifica il nome della macchina (o del servizio)



Domain Name System

Ogni nome corrisponde ad un *dominio*

- La gerarchia dei nomi è sia geografica che organizzativa
- I domini di livello 1 sono, ad es:
  - com, edu, org, gov, it, fr, de…
- I *server DNS* consentono la risoluzione (restituendo l'indirizzo IP corrispondente ad un dato dominio)
  - Se un server DNS non sa risolvere un indirizzo manda la richiesta ad un server di livello superiore
  - La risoluzione degli indirizzi può essere:
    - Iterativa
    - Ricorsiva

Il nome di dominio va registrato presso l'InterNIC (Internet Network Information Center)

- Ciò assicura l'unicità del nome e la sua associazione ai numeri che identificano le macchine usate dal richiedente

Domain Name System