

# Reti di Elaboratori

## INDICE

1. Introduzione alle Reti
  - a. Tipologie di Reti di accesso
  - b. Store and Forward
  - c. Struttura di Internet
  - d. Latenza e Perdita di Pacchetti
2. Stack Protocolare
  - a. Multiplexing e Demultiplexing
3. Introduzione alla Sicurezza
  - a. Attacchi alla Rete

## Introduzione

Definiamo come rete una interconnessione di dispositivi che tra loro scambiano informazioni.

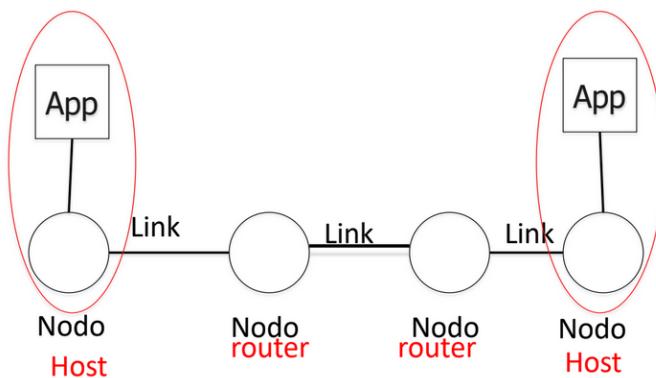
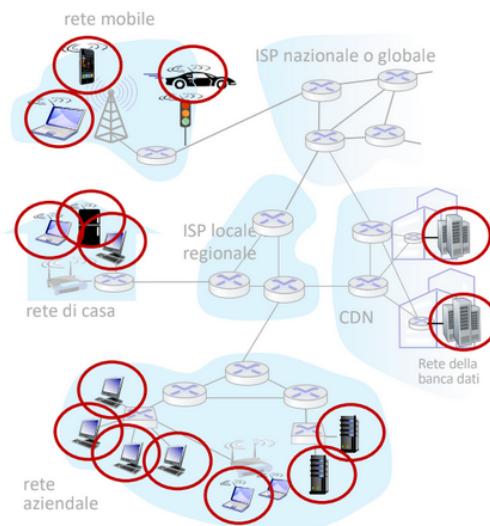
Questi dispositivi possono essere di due tipi:

- Terminali (end devices): sono quelli che effettivamente comunicano e fanno partire i messaggi o li ricevono, come computer, cellulari, tablet, server ecc.
- Dispositivi che consentono a più end devices di comunicare: router, switch ecc.

I dispositivi terminali possono essere di due tipi:

- Host: richiedono una risorsa (es. una pagina internet)
- Server: rispondono alla richiesta dell'host inviando una risposta (es. un web server in cui tu ricerchi dei contenuti)

Diremo che i dispositivi terminali saranno situati alla periferia della rete:



Come possiamo vedere in queste immagini, gli host si trovano agli "estremi" della rete e tra di loro vi sono dei router che si passano il dato che vogliono comunicare, finché non raggiungono l'host a cui il messaggio era destinato.

I dispositivi di connessione possono essere di tre tipi principali:

- Router: collegano una rete ad una o più reti
- Switch (commutatori): collegano due host della stessa rete tra di loro, senza comunicare con l'esterno
- Modem: ottiene effettivamente la connessione, trasforma il segnale da analogico e digitale, lo passa al router (molte volte modem e router sono messi insieme nello stesso device)

Definiamo con access network dei collegamenti che connettono il sistema al primo edge router, ovvero il router che ti mette in contatto con la rete esterna ed altri router.

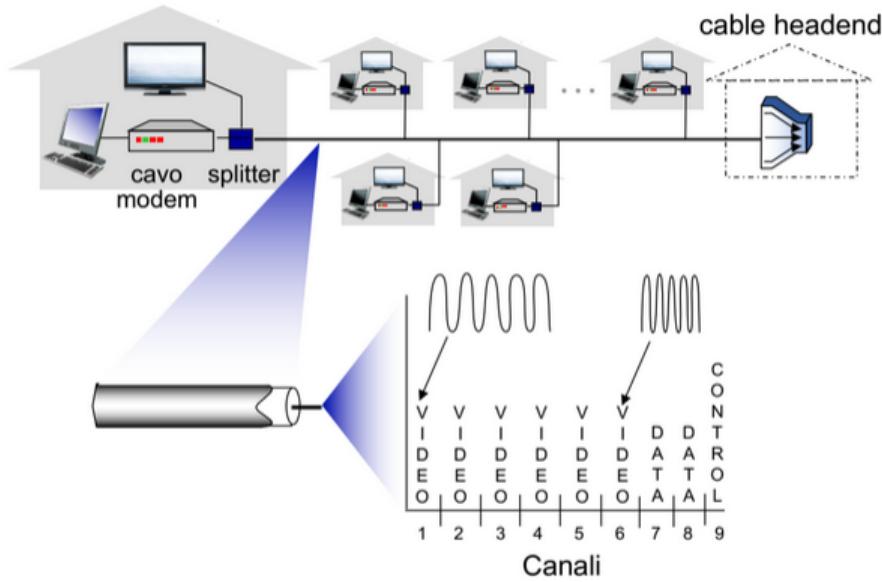
Possiamo collegare un sistema periferico al edge router tramite vari modi, tra cui:

- Reti di accesso aziendale
- Reti di accesso istituzionali (scuole, laboratori)
- Reti di accesso mobile (Wifi, 4G)

## ▼ Tipologie di reti di accesso

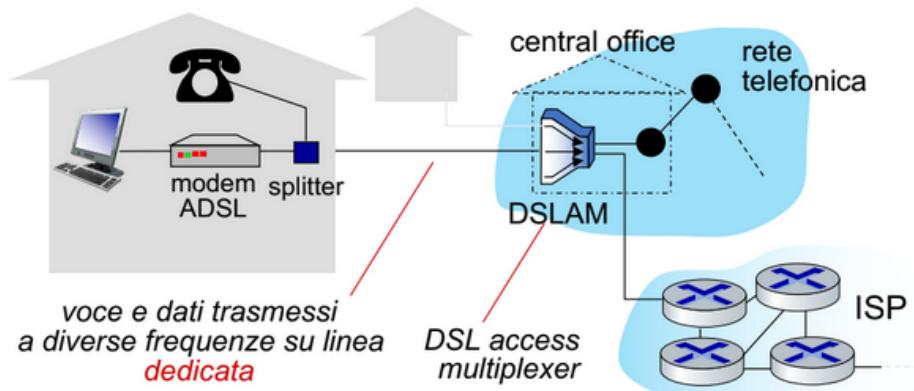
### **Accesso via cavo:**

Tutte le case/uffici si collegano allo stesso cavo, e viene effettuato un FDM (multiplexing a divisione di frequenza) tramite il quale i diversi canali di comunicazione (ogni casa) trasmette in frequenze diverse, in modo da riconoscere "chi è chi"



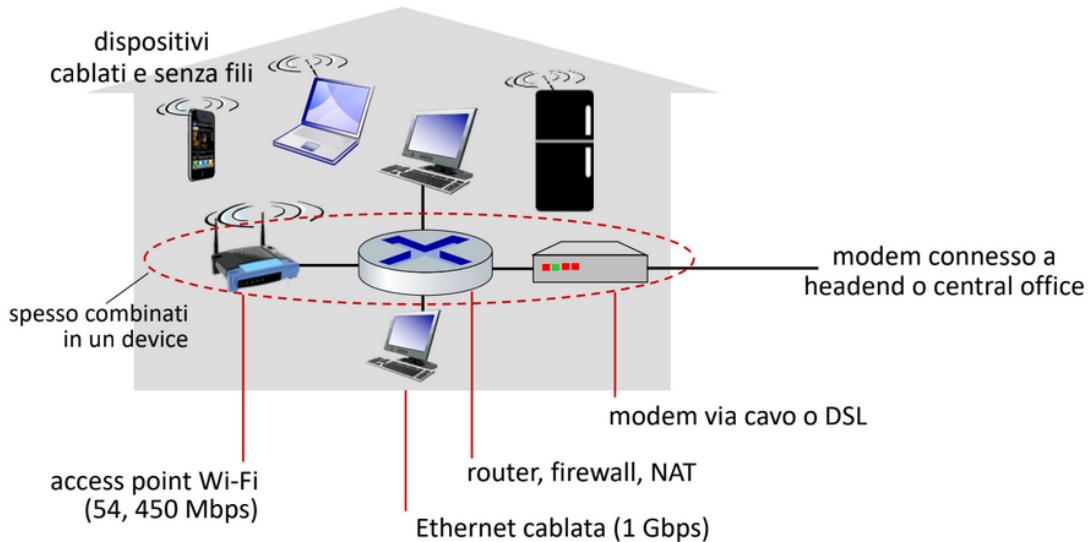
### Digital Subscriber Line (DSL):

L'ISP fornisce la connessione alle varie abitazioni sfruttando la linea telefonica, assieme ai segnali vocali



### Reti domestiche:

Un modem, connesso al router, riceve la connessione



### Reti wireless:

Vi è una connessione wireless che collega il nostro end devices al router, possiamo avere due sottotipi di reti wireless:

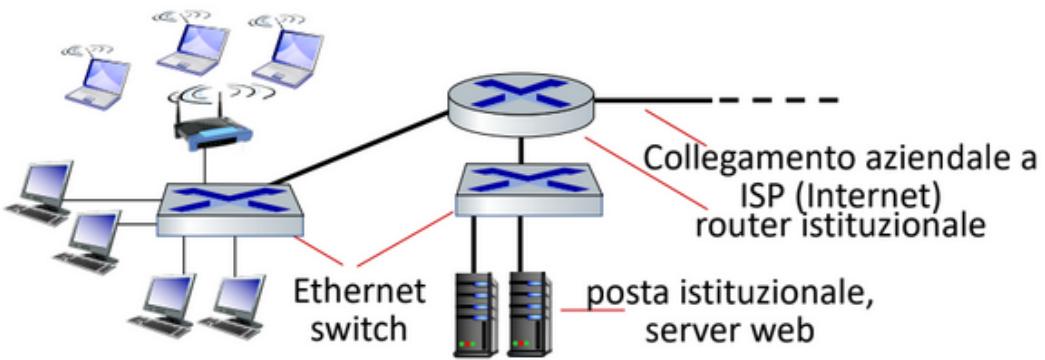
- WLAN (Wireless Local Area Network) ad esempio quella di una casa, in cui l'end devices è lontano massimo 30m dal router
- WAN (Wide Area Network) in cui un operatore di rete cellulare fornisce la rete tramite 4G o 5G



A sinistra possiamo vedere una WLAN, a destra una WAN

### Reti aziendali:

Servono per connettere dispositivi terminali di università, aziende ecc. e fanno affidamento su un mix di tecnologie cablate e wireless, facendo uso di vari switch e router usando quindi sia tecnologia ethernet che wifi



Come fa un host ad inviare i dati?

Innanzitutto riceve da un'applicazione il messaggio che deve essere inviato e lo suddivide in pacchetti di lunghezza  $L$  bit

Successivamente trasmetterà ogni pacchetto ad una velocità di trasmissione (ovvero la larghezza di banda, quanti bit/s vengono inviati) ,di  $R$ , per cui il pacchetto non sarà inviato tutto insieme, ma le sue varie parti verranno inviate secondo la velocità di transsmissione.

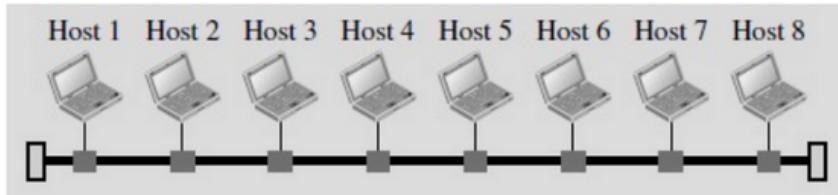
Il ritardo di trasmissione di un pacchetto si misurerà quindi con  $\frac{L(\text{bit})}{R(\text{bit/s})} = X$  secondi

## Reti LAN

Una rete LAN è una rete locale, usata ad esempio da aziende o università, in cui ogni dispositivo ha un indirizzo che lo identifica univocamente all'interno della rete (non fuori).

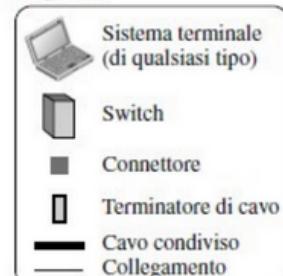
Una rete LAN non ha specifiche sul numero massimo o minimo di dispositivi che può ospitare.

Le LAN possono essere implementate con un cavo condiviso (broadcast) ma c'è il problema delle collisioni: non si può fare come l'accesso via cavo in cui si riconoscono le varie frequenze, quindi se più host usano il cavo contemporaneamente non si possono evitare collisioni.



a. LAN con cavo condiviso (obsoleta)

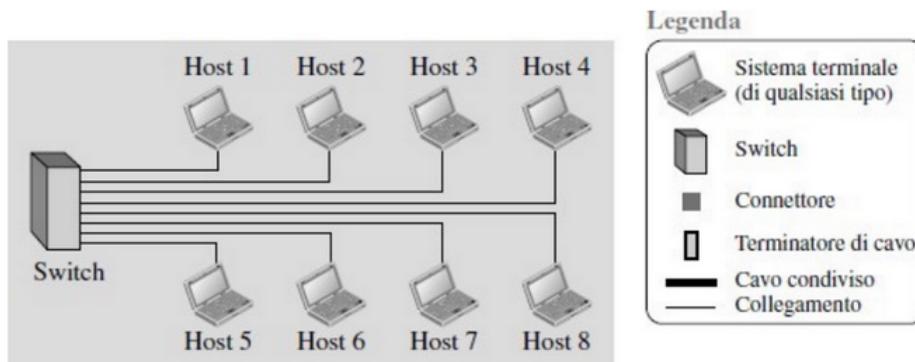
Legenda



- Il pacchetto inviato da un dispositivo viene ricevuto da tutti gli altri
- Solo il destinatario elabora il pacchetto, tutti gli altri lo ignorano

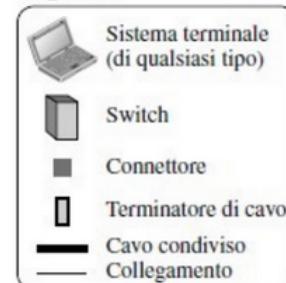
Ovviamente più persone sono connesse e minore è la velocità dato che si devono evitare le collisioni

Dato che questo tipo di LAN è obsoleto, illustriamo un tipo più moderno, ovvero le LAN con switch di interconnessione:



b. LAN con switch (moderna)

Legenda



Ogni host è collegato allo switch tramite un cavo dedicato, e lo switch sa a chi inviare il messaggio, evitando quindi che il messaggio venga trasmesso a tutti.

Lo switch riduce anche il traffico della LAN e permette a più coppie di host di comunicare tra loro, a patto che non vi siano sorgenti e destinazioni in comune, questo perché se hai un host che comunica con due host contemporaneamente hai comunque delle collisioni dato che lo switch invia i messaggi a questo host tramite un cavo solo, quindi sarà possibile che un messaggio verrà inviato dall'host mentre ne riceve un altro.

## Reti WAN

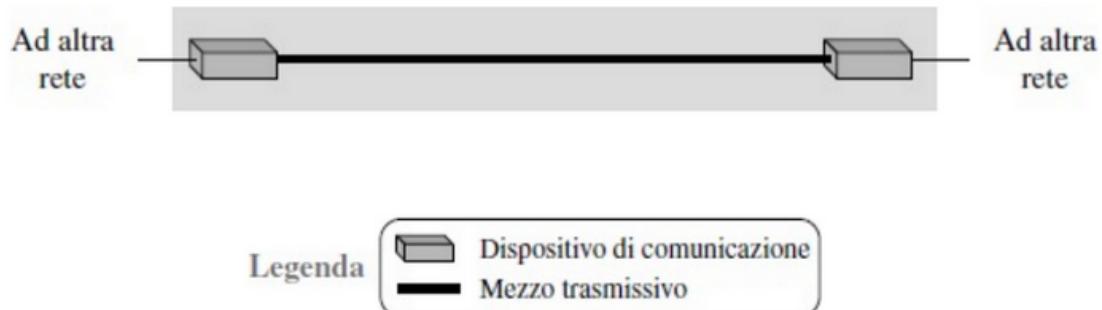
WAN sta per Wide Area Network ed indica reti che operano su una area geografica molto vasta, come ad esempio città regioni o nazioni.

Ovviamente una WAN fa uso di più modem, switch e router per funzionare, è impossibile pensare che vi sia un unico router a cui tutti facciano riferimento

Le reti WAN funzionano grazie agli ISP (Internet Service Provider) che permette a reti lontanissime tra loro di comunicare.

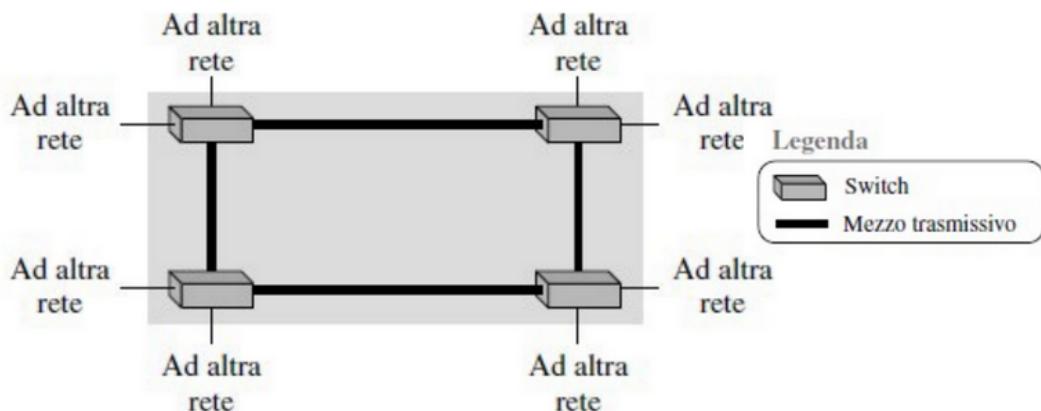
Le WAN possono essere di due tipi:

- Punto-punto:



Collega due reti tra di loro tramite un mezzo trasmissivo che può essere cavo o wireless

- A commutazione (o switched)

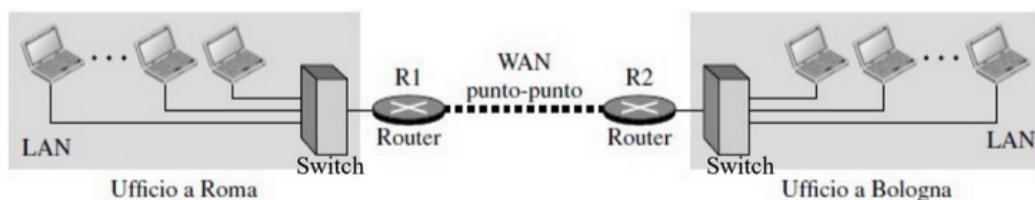


Usata nelle dorsali (backbone) di internet, ad esempio quando si connettono tra loro più router di smistamento.

Come possiamo vedere ci sono più punti di terminazione, per cui se due router vogliono comunicare non hanno una singola opzione, aumentando la sicurezza dato che se un solo mezzo trasmissivo è malfunzionante si possono usare gli altri.

## Wan punto-punto ed internet private

Spesso LAN e WAN non sono isolate: ad esempio una azienda vuole connettere più uffici che sono lontanissimi tra loro e per farlo avrà bisogno di una WAN punto-punto.

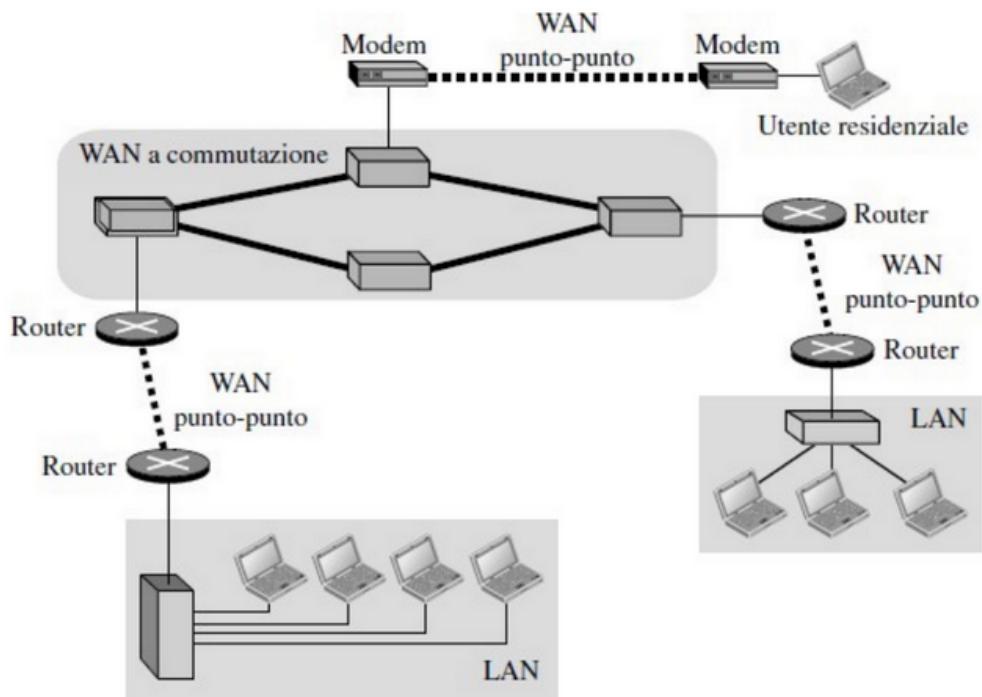


Questa WAN punto-punto sarà affittata da un ISP, che avrà i messi fisici per connettere queste due LAN.

In questa maniera l'azienda avrà realizzato una internet (rete di reti) privata.

Nota che la wan punto-punto è solo quella compresa tra i due router, non c'entrano le LAN

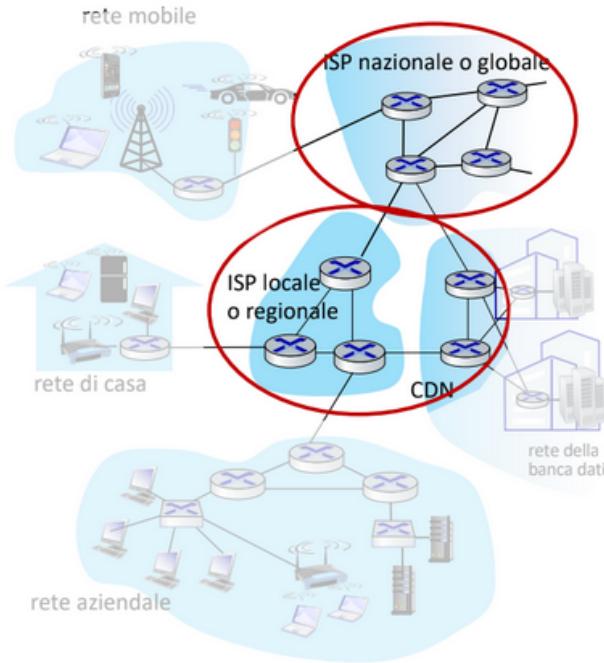
Esempio:



Abbiamo qui una internet privata formata da 4 WAN (una a commutazione e 3 p-p) e 3 LAN (la terza LAN è composta dalla residenza dell'utente residenziale)

## Nucleo e funzioni della rete

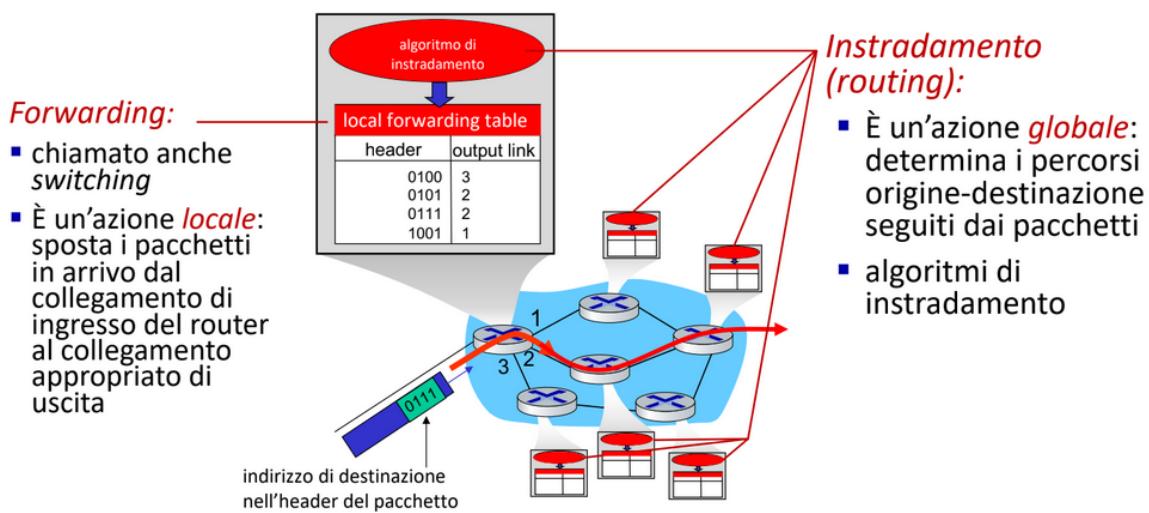
Il nucleo della rete è composto da router che si scambiano i pacchetti che devono raggiungere destinazioni remote, nota che i router in questione sono molto più grandi e performanti dei router che abbiamo a casa dato che elaborano quantità enormi di dati da host diversi.



Una rete esegue due funzioni molto importanti:

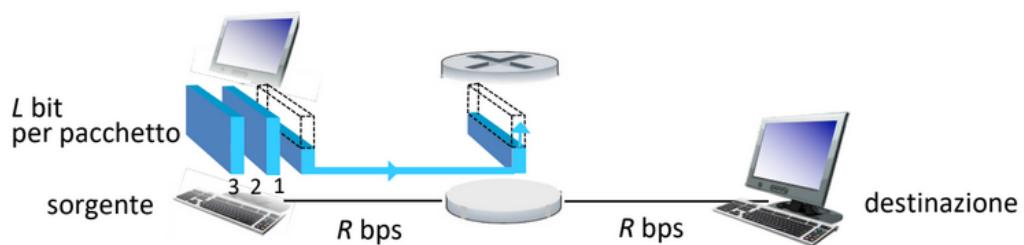
- Forwarding (o switching) : è un'azione locale tramite la quale si riceve un pacchetto su una porta e lo si invia su un'altra (ad esempio su un altro router)
- Routing: vengono determinati i percorsi origine e destinazione che i pacchetti devono seguire, fa uso di algoritmi di instradamento

Includo la slide intera per far capire bene a cosa è collegato il forwarding e a cosa il routing



## Store and Forward

Quando un host invia un pacchetto ad un router, non lo invia interamente, ma invia i suoi dati uno dopo l'altro ed il router "ricostruirà" il pacchetto:



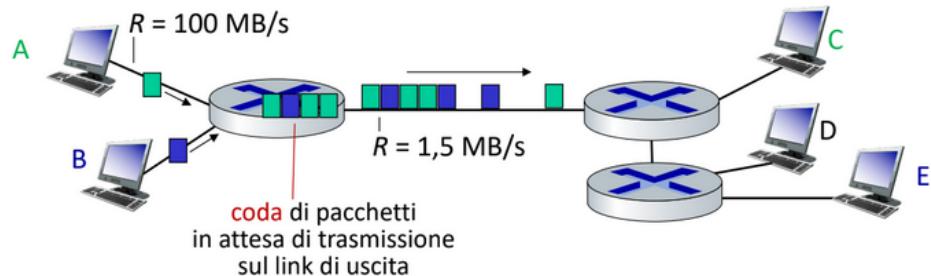
Dobbiamo ora però dare alcune importanti definizioni:

- Ritardo di trasmissione: ci vogliono  $\frac{L}{R}$  secondi per trasmettere il pacchetto all'altro dispositivo
- Store and forward: la pratica tramite la quale il pacchetto deve prima essere ricostruito e quindi essere presente sul router interamente prima di essere inviato al collegamento (es. cavo) successivo
- Ritardo end-end: quanto tempo ci mette il dispositivo di interconnessione a mettere il pacchetto sul mezzo di trasmissione,  $2 \frac{L}{R}$  secondi se assumiamo un ritardo di propagazione uguale a 0

## Commutazione di pacchetto

Con la commutazione di pacchetto, gli host invieranno i pacchetti al router tre lui li smisterà ai destinatari, ma non esistono linee dedicate, il router invia tutti i pacchetti tramite lo stesso canale di comunicazione

Possiamo avere delle code quando eseguiamo il packet switching:

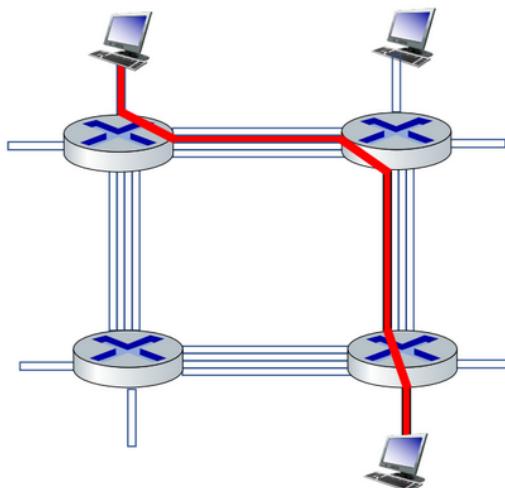


In questo caso abbiamo due host che inviano pacchetti ad una velocità di 100MB/s mentre il router esegue il forwarding ad una velocità di 1.5 MB.

Il router ha però una memoria (buffer) che conserva i pacchetti non ancora inviati, ma se la memoria si riempie i pacchetti verranno scartati

## Commutazione di circuito

In questa modalità di comunicazione ogni dispositivo ha una sua linea dedicata:



Notiamo che in condizioni ottimali non si ha condivisione dello stesso mezzo di comunicazione (chiedi al prof se è un cavo o cosa dato che abbiamo dei router) in quanto abbiamo più circuiti sui quali passano i dati.

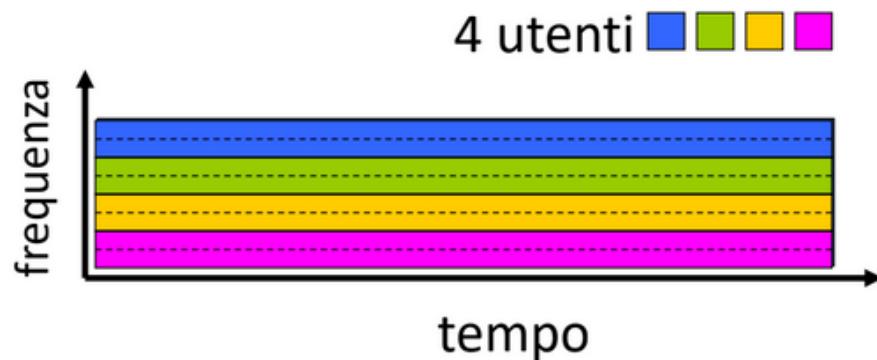
Se un segmento di circuito non viene utilizzato da nessuna chiamata rimane inutilizzato: non viene usato per trasmettere i dati del dispositivo che sta comunicando in quel momento, si attua quindi una politica no-sharing.

Che succede quando due o più host condividono lo stesso canale di comunicazione? Come facciamo a sapere a chi appartiene un certo segnale?

Abbiamo due metodi:

CHIEDI: Viene applicato all'ethernet o solo alle chiamate?

- FDM (Frequency Division Multiplexing): le frequenze sono suddivise in varie bande e sono assegnate ai vari host, in modo che ognuno trasmetta ad una certa frequenza.

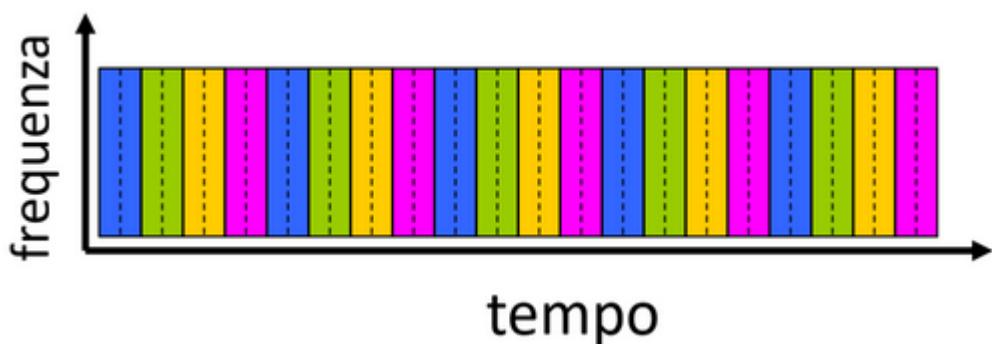


Possiamo anche vedere che ogni dispositivo può trasmettere alla velocità di banda massima, ma la banda è stretta

Contro: costo alto, difficile da implementare

Pro: molto efficiente

- TDM (Time Division Multiplexing): ogni host ha dei quanti temporale a disposizione durante i quali inviare i messaggi e può trasmettere alla velocità massima della banda (larga)



Contro: turni diversi

Pro: costo basso

E' importante chiarire un concetto: un sistema di comunicazione a commutazione di pacchetto è più scalabile dal momento che anche se abbiamo molti host che usano lo stesso mezzo di comunicazione, possiamo suddividerli in turni inviano una volta un pacchetto dell'host x ed una volta uno dell'host y.

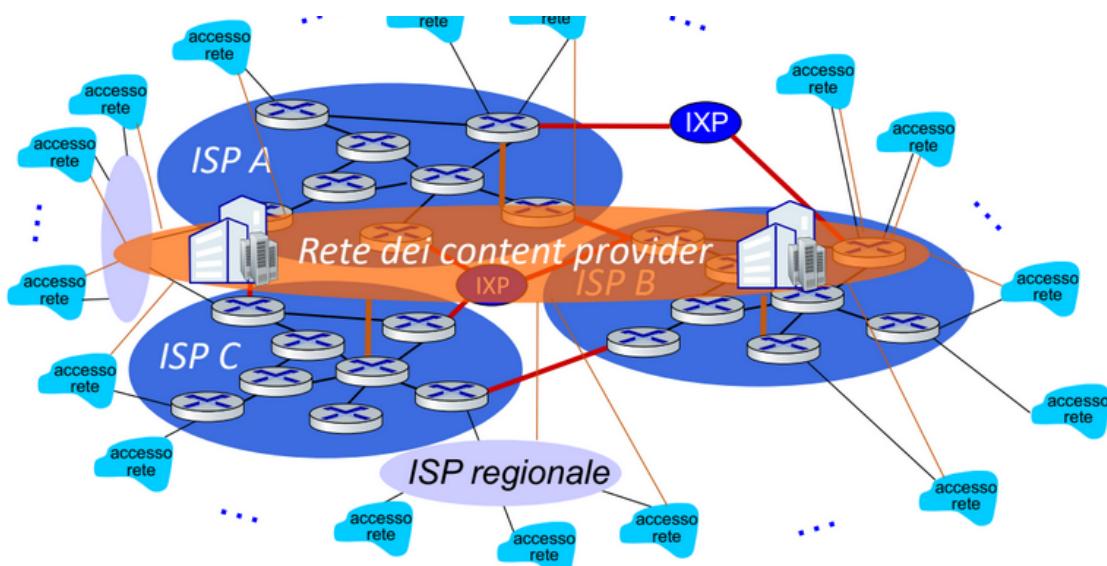
Un sistema a commutazione di circuito non può fare ciò dal momento che ogni host utilizza il suo mezzo di comunicazione, quindi non possiamo avere più di  $n$  host.

Per questo motivo la comunicazione a commutazione di pacchetto è migliore, in quanto è adatta a dati bursty, ovvero che hanno uno spike di dati e poi sono silenziosi per lunghi periodi di tempo.

Però si ha il rischio di congestione dato il possibile overflow del buffer, quindi va gestito tramite appositi protocolli

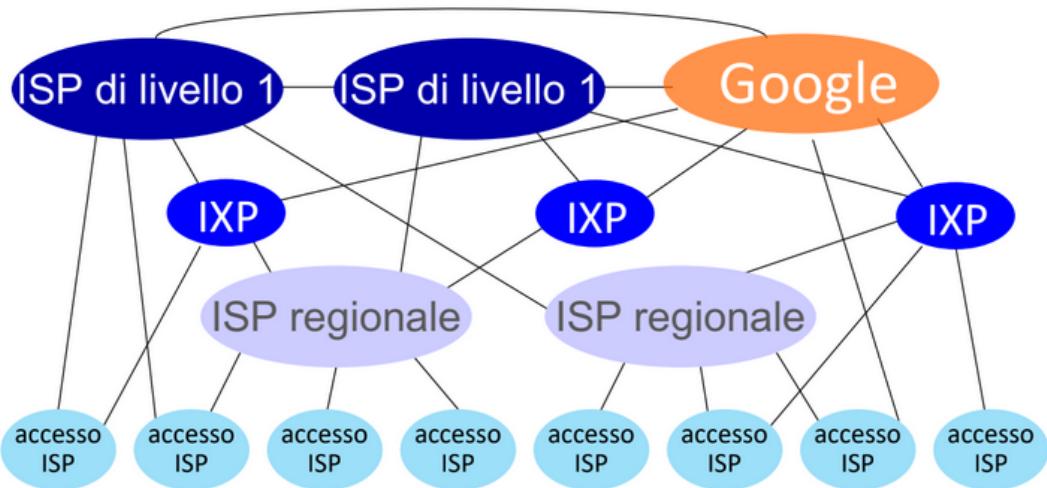
## Struttura di internet: una rete di reti

Ogni nodo si connette ad internet tramite un ISP, ma anche questi ISP tra di loro devono essere connessi per permettere la creazione della rete internet per come la conosciamo e ciò viene fatto tramite gli IXP: internet exchange point



Qui vediamo che ogni dispositivo di accesso alla rete è connesso ad un isp, che sia un ISP di una grossa azienda o un ISP regionale che connetterà a quest'ultimo ISP.

Molti content provider (es. google, netflix) utilizzano una tecnica per permettere di raggiungere velocemente gli utenti "sorpassando" gli ISP, connettendosi direttamente agli IXP e bypassando gli ISP:



### Aampiezza di banda (bitrate)

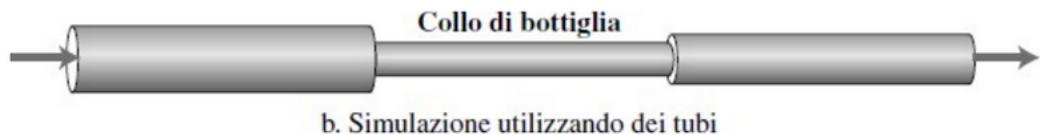
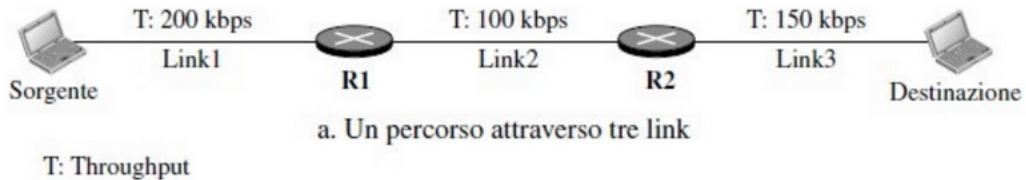
Con il termine "ampiezza di banda" si intende la quantità di bit al secondo che un link garantisce di poter inviare

### Throughput

Rappresenta il numero di bit che effettivamente passano attraverso un link, mentre il bitrate indica un numero di bit potenziale, es. 100Mb/s

Es. c'è una strada che è progettata per far passare 1000 auto al minuto (bitrate), ma c'è traffico e la strada fa passare 100 auto al minuto (throughput)

**Nota:** quando hai dei dispositivi che comunicano attraverso più link, il throughput sarà il throughput del link che ha il throughput minore:

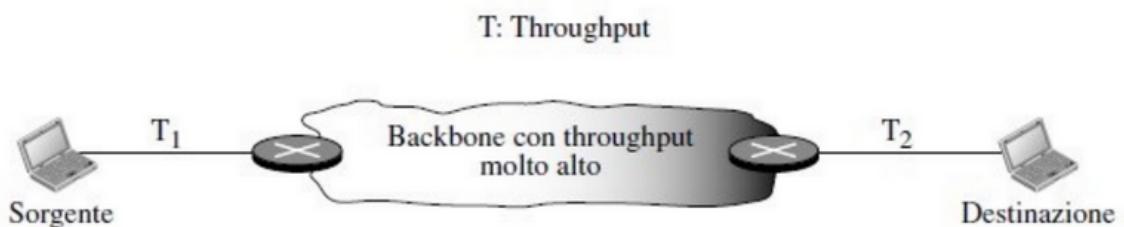


Il throughput del percorso è 100 kbps:

Noi tramite il link 1 inviano 200kbps, ma il link 2 ne invia solo 100 al secondo, quindi l'host sorgente dovrà aspettare.

Però anche il link 3, per inviare i dati a 150kbps deve aspettare che gli siano inviati a 100kbps, quindi il rallentamento c'è sempre.

### Caso realistico:



Molto spesso due host comunicano attraverso le dorsali di internet, che hanno un throughput molto alto, per cui i colli di bottiglia sono dati dai due host: la dorsale può anche avere un T di 1Gbps, ma se il sorgente glieli invia a 100Mbps non sfrutta il suo T molto alto.

Per cui il T in questo caso sarà il minimo tra T<sub>1</sub> e T<sub>2</sub> (i T dei due link que conectan los hosts a la dorsal)

## Latenza e perdita di pacchetti (todo)

## Stack protocollare

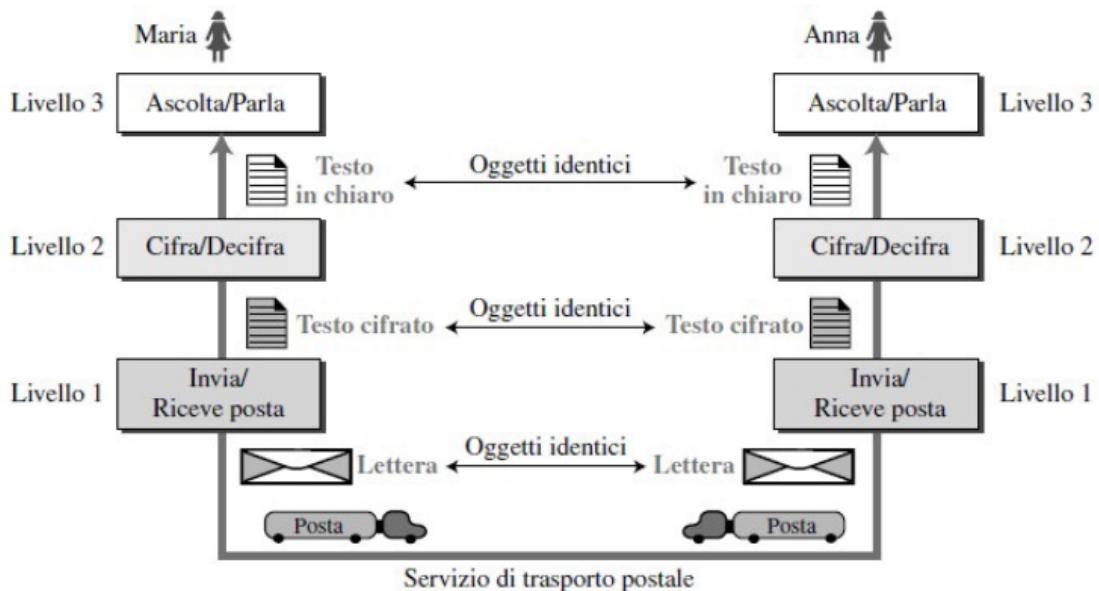
Un protocollo è un set di regole che due end point devono utilizzare per permettere la comunicazione, similmente a quando due persone parlano al telefono: ci sono dei protocolli, ovvero dire pronto, chiedere chi è, poi l'altro si presenta ecc.

Queste regole sono utili e necessarie in quanto permettono a dispositivi di natura diversa (televisioni, pc, telefoni, server, orologi smart ecc.) di comunicare tra loro a prescindere appunto da come sono costruiti.

Sulla rete internet, i protocolli sono layerizzati, ovvero suddivisi per layer: un layer (livello) si occupa di mostrare il messaggio all'utente, l'altro di instaurare una connessione, l'altro del trasporto messaggi ecc.

Ciò è utile in quanto costruisce l'architettura protocollare in una maniera modulare: ogni protocollo è un modulo a sé e se vogliamo cambiare un protocollo es. crittografia, dobbiamo modificare solo il nostro protocollo di crittografia, senza toccare tutto il resto, cosa che accadrebbe se usassimo un protocollo unico per fare tutto.

Esempio di comunicazione a livelli:



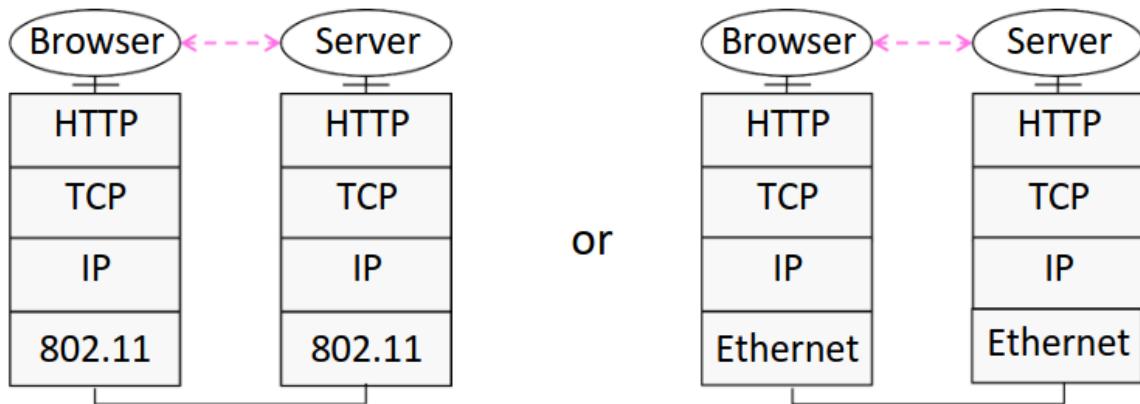
Maria ed Anna al livello 3 si occupa di ascoltare e parlare, mentre al livello 2 cifrano e decifrano, per poi inviare/ricevere al livello 1.

Se Maria vuole inviare un messaggio, parla (livello 3) ed il testo in chiaro del messaggio viene inviato al livello 2 (lo cifra) per poi inviarlo al livello 1.

Anna riceverà il messaggio al livello 1, lo decifrerà al livello 2 ed al livello 3 lo ascolterà.

All'interno di una strutturazione a livelli, ogni modulo (livello) non si preoccupa di ciò che avverrà nel livello successivo o in quello sottostante, ma solo di ciò che farà lui.

Esempio in cui il layering può essere utile:

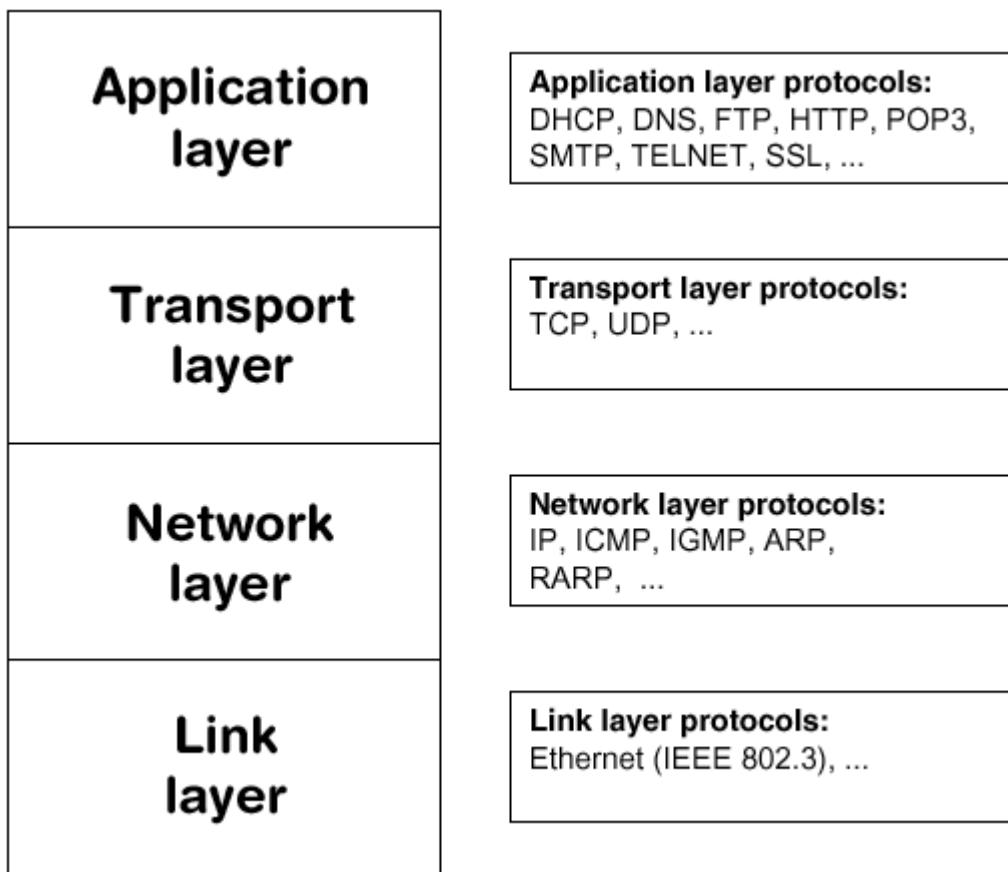


Noi qui abbiamo un browser ed un server che comunicano (sx) usando lo standard 802.11 (standard delle reti WLAN).

Nel caso il browser volesse cambiare standard di comunicazione mettendo ethernet andrebbe modificato solo un modulo (livello), ovvero quello che si occupa della connessione fisica, senza toccare tutti gli altri livelli. Abbiamo quindi come un puzzle, in cui puoi togliere un pezzo e metterne un altro senza dover interferire con gli altri.

### Struttura dello stack TCP/IP

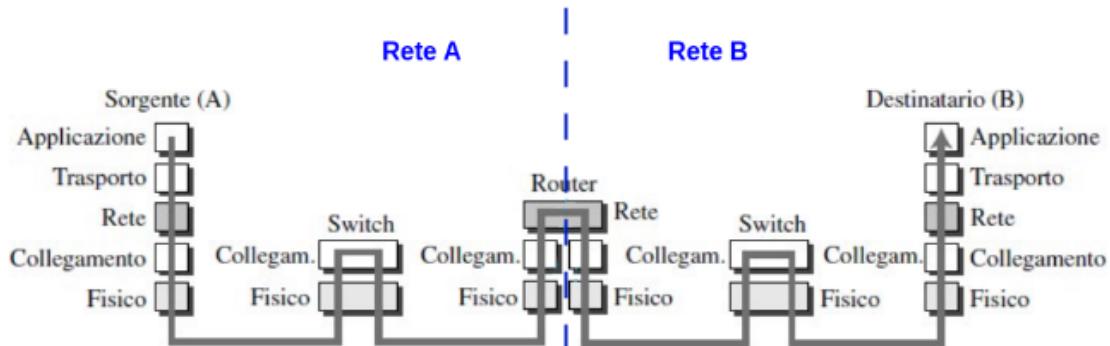
Lo stack TCP/IP è lo stack standard di livelli utilizzato sulla rete internet, ed è composto da cinque livelli (di cui a volte gli ultimi 2 sono raggruppati in uno solo):



- Applicazione:** serve a fornire un servizio applicativo al client, ci fornisce ciò che abbiamo richiesto o ci permette di fare ciò che abbiamo richiesto di fare, es. HTTP serve per richiedere e ricevere pagine web, FTP per trasportare file su un server, POP3 per le email, il DNS ci comunica l'IP di un host che cerchiamo (es. [google.com](http://google.com) - 123.25.6.111)
- Trasporto:** serve per il trasferimento vero e proprio dei dati, perché tu con HTTP ricevi la pagina web oppure la richiedi, ma questa pagina viene inviata al livello applicazione tramite il livello di trasporto, e quando richiedi una pagina la richiesta HTTP passa al livello di trasporto per essere appunto poi trasportata all'altro host
- Rete:** serve per instradare (indicare un percorso) un pacchetto dal mittente al destinatario, es. indirizzi IP che identificano un host sulla rete ed algoritmi di instradamento (routing) che calcolano quale sarà il percorso del pacchetto
- Collegamento-fisico:** due collegamenti che talvolta sono accorpati in uno, collegamento serve per stabilire il collegamento tramite il quale i messaggi passeranno e quello fisico si occupa del trasferimento dei singoli bit.

Nota che più si scende e più saremo tendenzialmente vicini all'HW.

Quando due host comunicano, il messaggio può passare attraverso switch e router, secondo la seguente modalità:



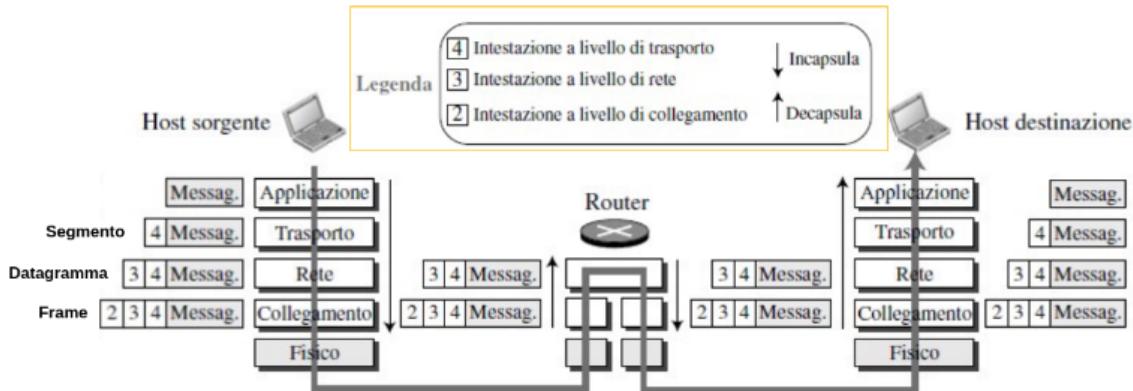
L'host sorgente (A) invia il suo pacchetto completo allo switch, che lo decapsula ma solo fino al livello di collegamento, non operando sui livelli successivi

Successivamente lo switch lo passa al router, che lo decapsula e poi ricapsula fino al livello di rete, in quanto non è competente per i livelli successivi e nemmeno gli servono, per poi inviarlo allo switch ecc. fino ad arrivare al destinatario.

Nota che ogni volta che un messaggio viene inviato al livello sottostante, vengono aggiunti degli header (intestazioni) che contengono informazioni sul lavoro svolto dal livello in questione e forniscono informazioni al livello successivo (quello sottostante).

Un messaggio può assumere 4 denominazioni diverse in base al livello in cui si trova:

- Messaggio (livello di applicazione), è uguale al pacchetto originale, ancora non ci sono intestazioni
- Segmento (livello di trasporto), messaggio ricevuto dal livello superiore + header di trasporto
- Datagramma (livello di rete), segmento + header di rete
- Frame (livello di collegamento), datagramma + header di collegamento



Come possiamo vedere, più scendiamo e più si aggiungono gli header, mentre più saliamo e più gli header vengono rimossi.

### Multiplexing e demultiplexing

Dato che ogni livello dello stack può operare con protocolli diversi, ogni livello deve poter eseguire due operazioni:

- Multiplexing: i protocolli devono essere in grado di incapsulare il pacchetto ricevuto dal livello superiore ed inviarlo al livello inferiore
- Demultiplexing: i protocolli devono essere in grado di decapsulare il pacchetto ricevuto dal livello sottostante ed inviarlo al livello superiore

## Introduzione alla Sicurezza

Esiste un modello referenziale per descrivere gli strati/livelli della comunicazione chiamato **modello OSI**, che ai 5 precedenti aggiunge 2 livelli interposti fra applicazione e trasporto, ossia presentazione (si occupa della crittografia) e sessione (si occupa della sincronizzazione).

Definiamo **campo della sicurezza**, l'ambito che si occupa di capire come le reti potrebbero subire attacchi, e quali potrebbero essere eventuali difese. Internet in origine, alla sua nascita, non è stato pensato per essere "sicuro", in quanto **Arpanet** era una rete confidenziale condivisa fra utenti che si fidano fra loro, ed ogni livello dello stack è soggetto ad attacchi.

## Attacchi alla Rete

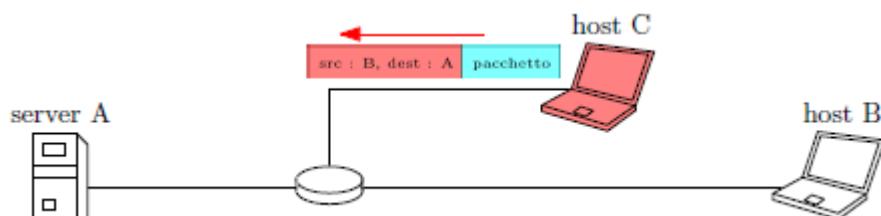
Un **malware** è un software malevolo che può entrare in una rete, ed infettare gli host tramite un meccanismo "autoreplicante" mediante la ricezione/esecuzione di oggetti, come allegati di posta elettronica o file eseguibili.

Uno **spyware** è un tipo di malware che ha lo scopo di registrare gli input dell'host infetto, e le sue tracce sulla rete, come i siti web visitati. L'host infetto può diventare parte di una **botnet**, utilizzata per scopi malevoli.

Uno degli attacchi tipici che possono arrivare da una botnet è l'attacco **DOS (Denial of Service)**, tale attacco viene eseguito sovraccaricando un servizio (bersaglio), inviando un numero elevato di pacchetti in modo da creare traffico sulla rete e rendere il servizio non disponibile.

Un altro attacco tipico è il **packet sniffing**, ossia l'intercettazione di pacchetti da parte di un terzo utente alla quale tali pacchetti non erano destinati. Viene spesso perpetrato tramite mezzi di trasmissione fisici come il cavo Ethernet o Wireless. L'utente malevolo legge e registra i pacchetti, che possono contenere informazioni confidenziali.

L'**IP spoofing** è un attacco che ha lo scopo di inviare pacchetti ad un destinatario, fingendosi una sorgente falsa, ovvero utilizzando un indirizzo di origine falso, convincendo il destinatario ad avviare una comunicazione, facendogli credere di star comunicando con un utente fidato.



Ci sono diverse forme di difesa agli attacchi presentati, l'**autenticazione** (dimostrare che il destinatario è effettivamente chi dichiara di essere), la **confidenzialità** (cifrare i messaggi tramite la crittografia), il **controllo integrità** (associare delle firme digitali ad un messaggio per prevenire o riconoscere eventuali manomissioni), le **restrizioni di accesso** (VPNs protette da password), e l'utilizzo di un **firewall** (programmi che si trovano nel nucleo dell'access point, con lo scopo di filtrare i pacchetti e riconoscere eventuali attacchi DOS).