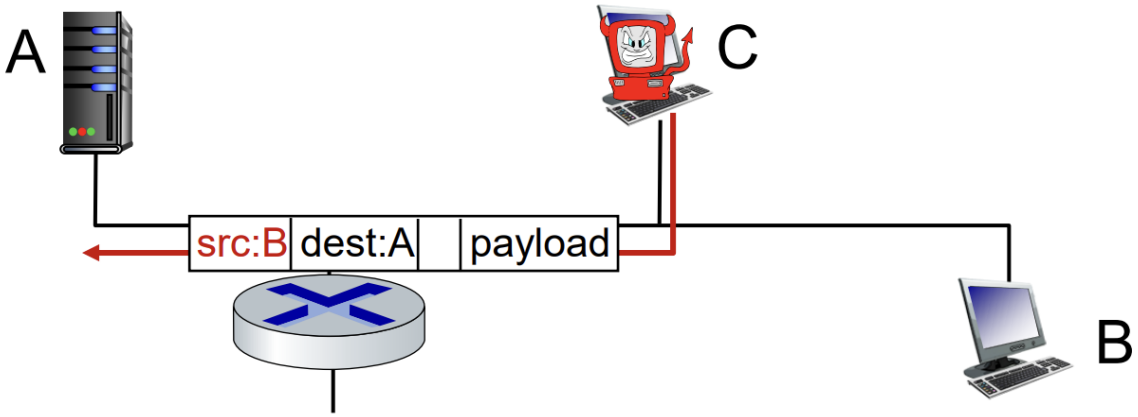
Lezione 3

Sicurezza di rete

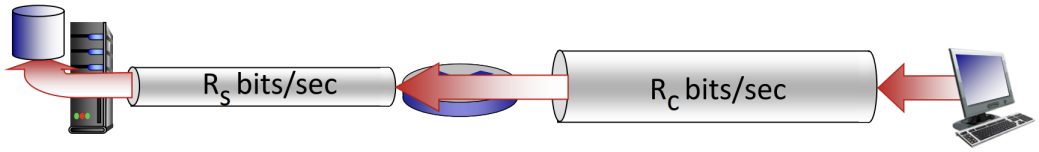
- **Analisi dei pacchetti** (packet sniffing): - media broadcast (Ethernet condivisa, wireless); - un'interfaccia di rete promiscua legge/registra tutti i pacchetti che l'attraversa. ![[Pasted image 20240312104714.png]]

- **Identità falsa** : *Ip spoofing*, iniezione di pacchetti con indirizzo sorgente falso.



  - **Usi** :
  - Ostacolare identificazione/blocco di una sorgente di attacco.
  - Sfruttare relazione di fiducia tra host.
  - Indirizzare messaggi di risposta verso B, montando un attacco di negazione di servizio contro B, basato sull'amplificazione del traffico generato da C.
- **Negazione del servizio** : aggressori rendono una rete, host o altro elemento infrastrutturale non disponibile per gli utenti legittimi.
  - ***3 categorie di attacchi DoS*** :
    - *Attacchi alla vulnerabilità dei sistemi*: invio di (pochi) pacchetti costruiti ad arte per causare il blocco di un servizio o lo spegnimento di un host, sfruttando vulnerabilità delle applicazioni o dei sistemi operativi.

- *Bandwidth flooding* (inondazione di banda) : invio massimo di pacchetti all'host obiettivo impedendo al traffico legittimo di raggiungerlo.
  Quindi l'attaccante invia traffico a una velocità prossima a R_S (Velocità di accesso ai server)



- *Connection flooding* (inondazione di connessioni) : stabilire un gran numero di connessioni TCP con l'host obiettivo, impedendogli di accettare le connessioni legittime.

- Quindi i passi sono :
  1. Selezionare l'obiettivo;
  2. irrompere negli host attraversi la rete;
  3. Inviare pacchetti verso l'obiettivo da host compromessi.

Linee di Difesa

- Autenticazione : dimostrare che siete chi dite di essere.
- Riservatezza : attraverso cifrature.
- Integrità : le firme digitali prevengono/rilevano le manomissioni.
- Restrizione di accesso : VPN protette da password.
- Firewalls : "middlebox" specializzate nelle reti di accesso e di base:
  - off-by-default: filtra i pacchetti in entrata per limitare i mittenti, i destinatari e le applicazioni.
  - rileva/reagisce agli attacchi DoS.

Livelli di protocollo e modelli di riferimento

Perché la stratificazione?

- Una struttura esplicita consente l'identificazione dei vari componenti di un sistema complesso e delle loro interrelazioni.
- La modularizzazione facilita la manutenzione e l'aggiornamento di un sistema

Potenziali svantaggi

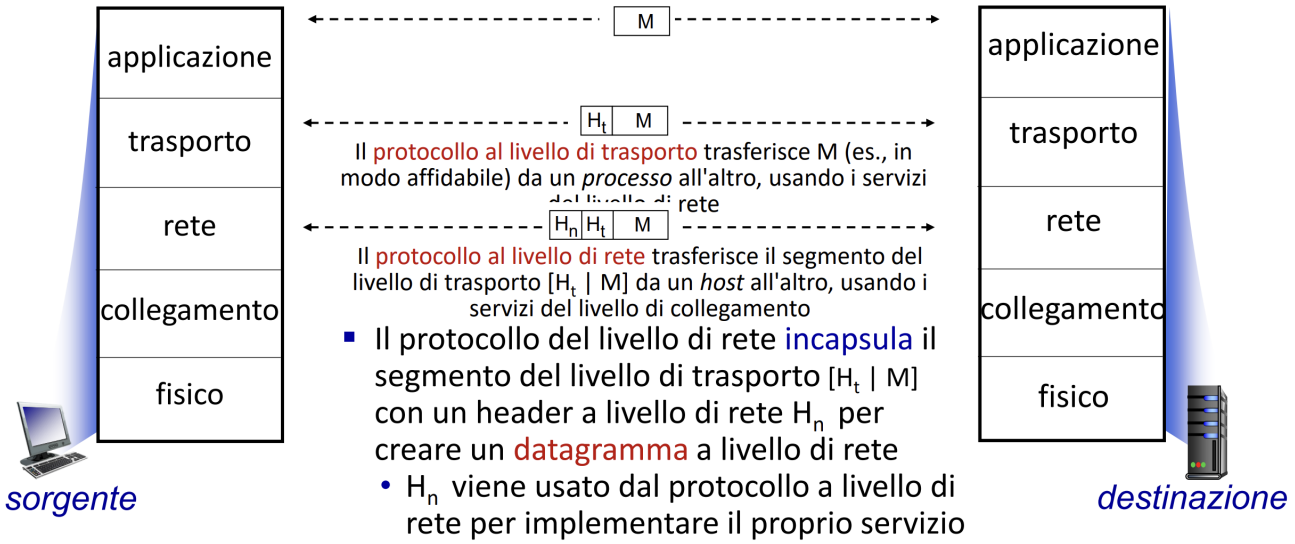
- Un livello può duplicare funzionalità del livello inferiore (es. correzione degli errori implementata spesso sia a livello di trasporto sia a livello di collegamento).
- Necessità di violare la separazione tra livelli, perché un livello ha bisogno di una informazione disponibile solo all'interno del livello inferiore.

Pila di Protocolli (Protocol stack) di Internet

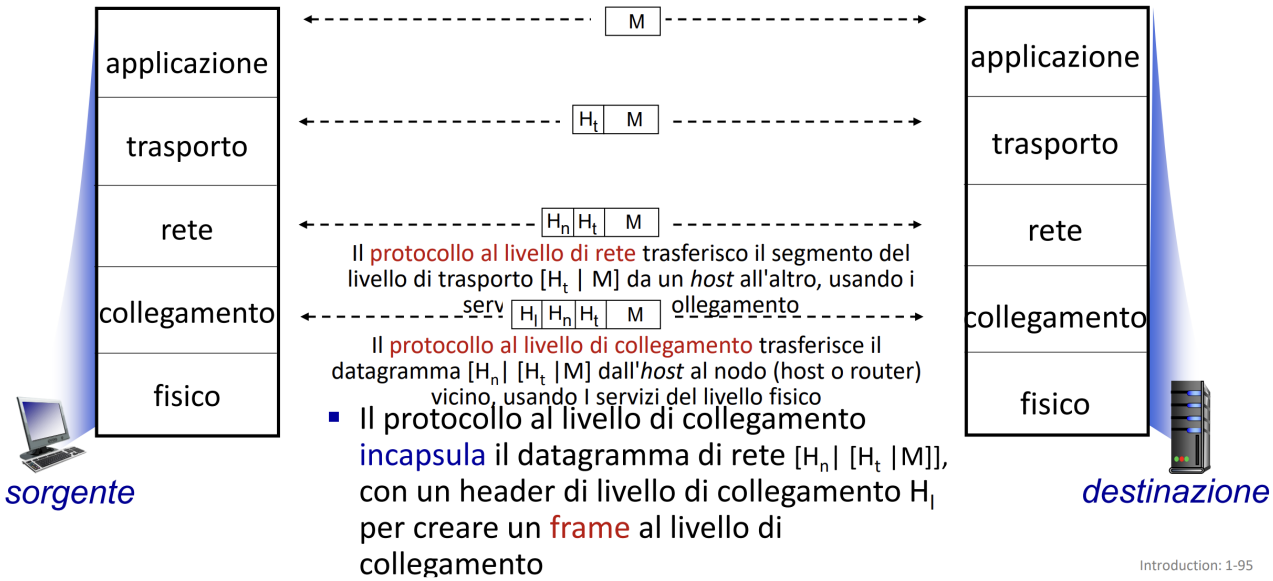
- Applicazione : supporto alle applicazioni di rete
  - HTTP, IMAP, SMTP, DNS.
- Trasporto : trasferimento di dati tra processi (in esecuzione su host differenti)
  - TCP, UDP.
- Rete : trasferimento di pacchetti di rete, detti datagrammi, da un host all'altro
  - IP, protocolli di instradamento.
- Collegamento : trasferimento di dati tra elementi di rete vicini
  - Ethernet, 802.11(WiFi), PPP.
- Fisico : bit sul filo.

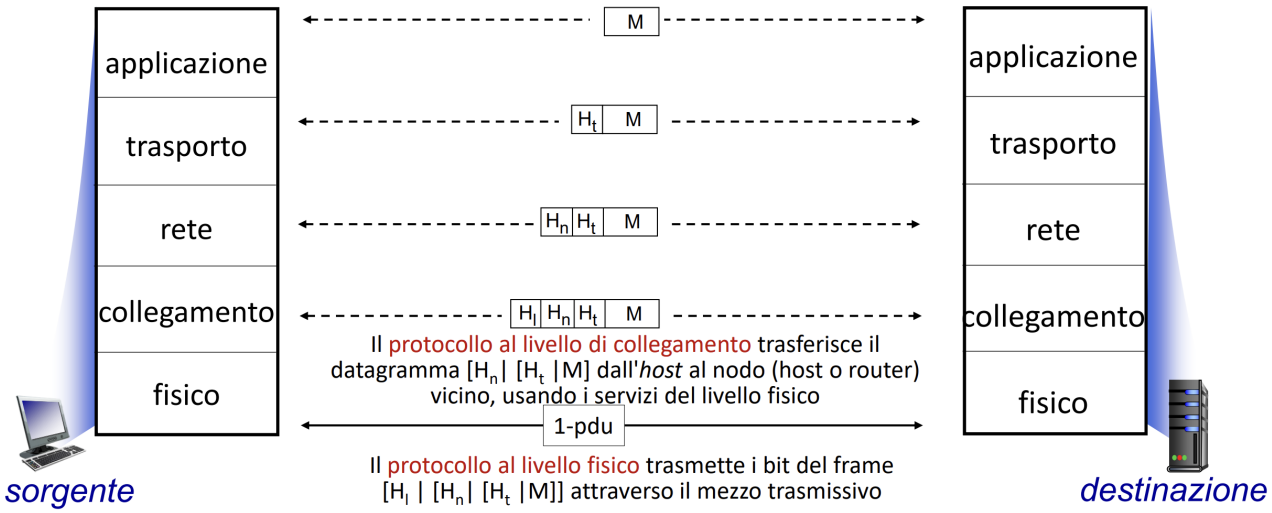
Servizi, Stratificazione e Incapsulamento

- Il protocollo di livello di trasporto incapsula il messaggio di livello applicativo, M, con un header H_t di livello di trasporto per creare un segmento a livello di trasporto
  - H_t viene usato dal protocollo di livello di trasporto per implementare il proprio servizio



- Il protocollo del livello di rete incapsula il segmento del livello di trasporto [H_t | M] con un header a livello di rete H_n per creare un datagramma a livello di rete
  - H_n viene usato dal protocollo a livello di rete per implementare il proprio servizio



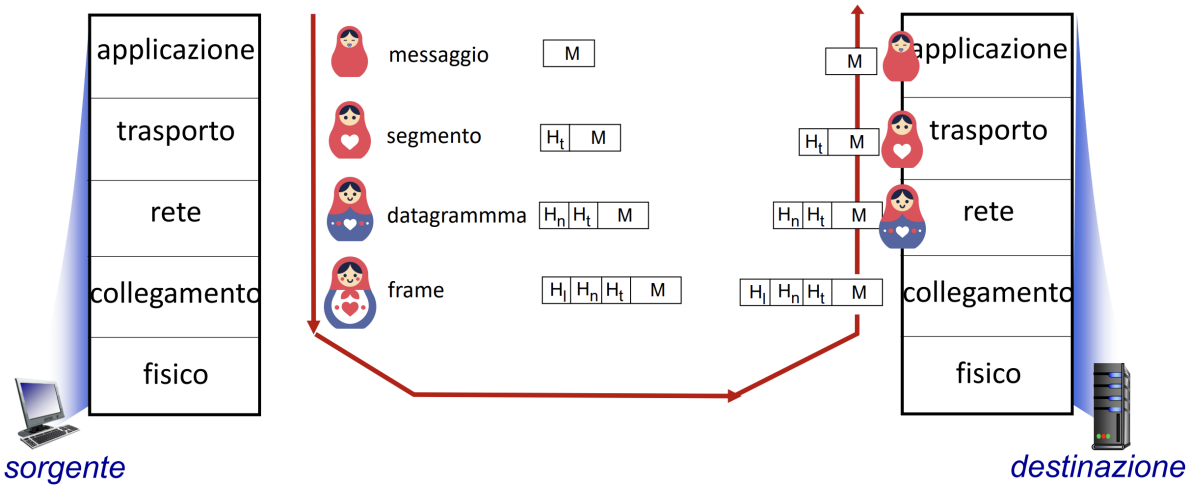


modello di servizio

- Insieme dei servizi offerti da un livello a quello superiore.
- I diversi servizi possono essere implementati da protocolli diversi.
- Il livello di collegamento può offrire servizi diversi in base al protocollo impiegato sul link.
- Inoltre, un protocollo a livello di collegamento può prevedere diversi protocolli a livello fisico dipendentemente dalla tecnologia di trasmissione e dal mezzo trasmissivo del link.

Incapsulamento

- **Bambole matrioska**



Modello di riferimento ISO/OSI

Sono due strati non presenti nella pila di protocolli di internet.

- Presentazione : consente alle applicazioni di interpretare il significato dei dati ad esempio, crittografia, compressione, convenzioni specifiche della macchina.
- Sessione : sincronizzazione, checkpointing, ripristino dello scambio di dati.