

Università degli Studi di Roma "Tor Vergata"
Laurea in Informatica

Sistemi Operativi e Reti
(modulo Reti)
a.a. 2023/2024

Introduzione (parte3)

dr. Manuel Fiorelli

manuel.fiorelli@uniroma2.it

<https://art.uniroma2.it/fiorelli>

Basate sulle slide del libro di testo:

https://gaia.cs.umass.edu/kurose_ross/ppt.php

Capitolo 1: tabella di marcia

- Cos'è Internet?
- Cos'è un protocollo?
- Ai confini della rete: host, reti di accesso, mezzi trasmissivi
- Il nucleo della rete: commutazione di pacchetto e commutazione di circuito, struttura di Internet
- Prestazioni: perdite, ritardi, throughput
- **Sicurezza**
- Livelli di protocollo, modelli di servizio
- Un po' di storia



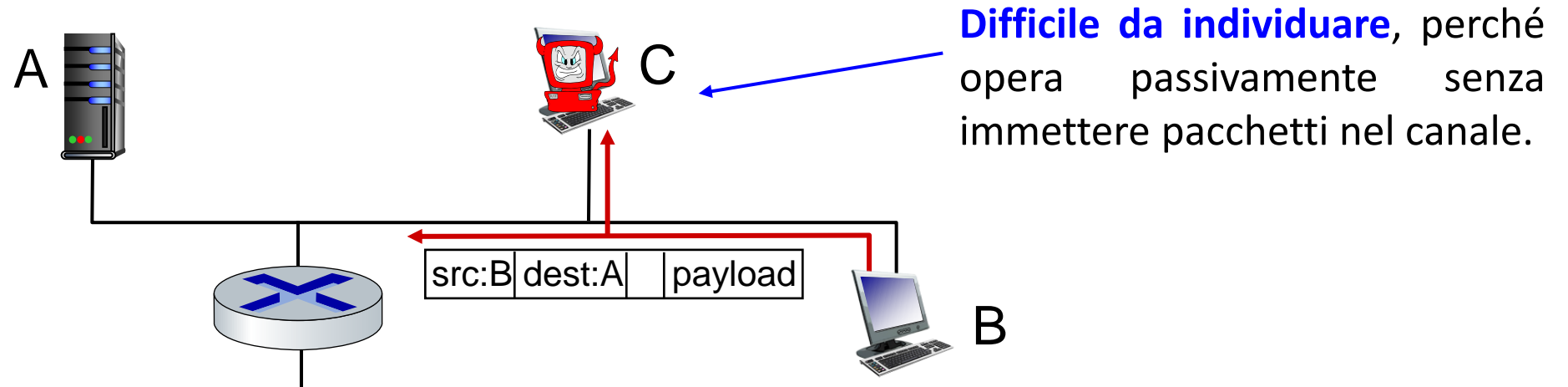
Sicurezza di rete

- Internet non è stata originariamente progettata pensando (molto) alla sicurezza
 - *visione originale*: “gruppo di utenti mutuamente fidati collegati a una rete trasparente” [Blumenthal 2001]
- Ora dobbiamo pensare a:
 - come i malintenzionati possono attaccare le reti informatiche
 - come possiamo difendere le reti dagli attacchi
 - come progettare architetture immuni agli attacchi

Malintenzionati: intercettazione dei pacchetti

Analisi dei pacchetti (packet sniffing):

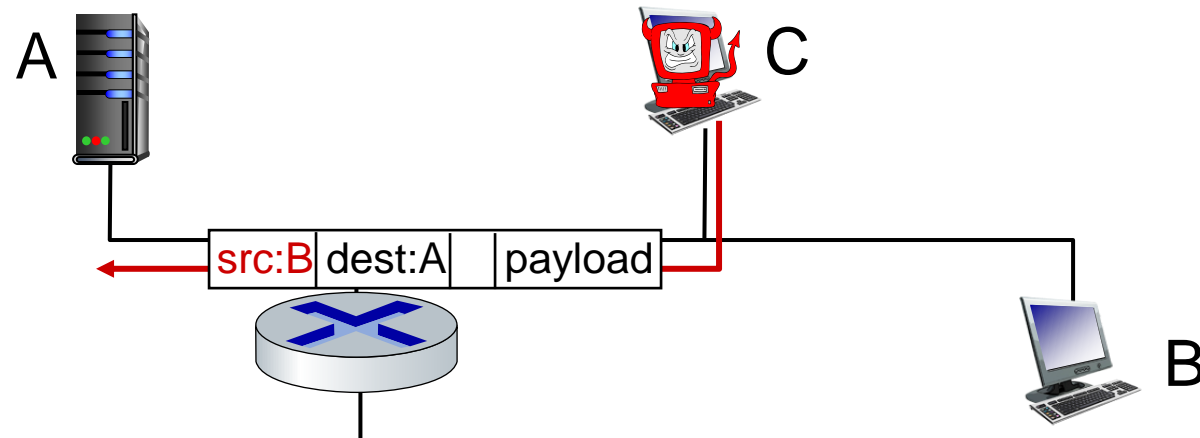
- media broadcast (Ethernet condivisa, wireless)
- un'interfaccia di rete promiscua legge/registra tutti i pacchetti (ad esempio, anche le password!) che l'attraversa



Il software Wireshark è un packet sniffer (gratuito)

Malintenzionati: identità falsa

IP spoofing: iniezione di pacchetti con indirizzo sorgente falso



Usi:

- ostacolare identificazione/blocco di una sorgente di attacco (vedi DoS dopo, sebbene meno rilevante nel caso di DDoS)
- sfruttare relazione di fiducia tra host (es. accesso senza autenticazione da host nella medesima rete locale)
- indirizzare messaggi di risposta verso B, montando un attacco di negazione di servizio contro B (vedi dopo), basato sull'amplificazione del traffico generato da C (vedi DNS Amplification Attack, in cui una richiesta a un DNS produce una risposta più grande indirizzata verso la vittima)

Malintenzionati : negazione del servizio (denial-of-service, DoS)

Negazione del servizio (Denial of Service (DoS)): gli aggressori rendono una rete, un host o altro elemento infrastrutturale non disponibili per gli utenti legittimi.

3 categorie di attacchi DoS:

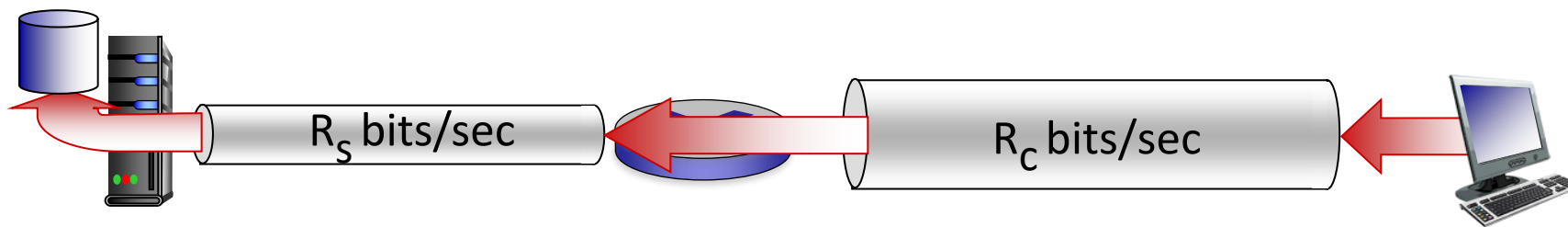
- *attacchi alla vulnerabilità dei sistemi*: invio di (pochi) pacchetti costruiti ad arte per causare il blocco di un servizio o lo spegnimento di un host, sfruttando vulnerabilità delle applicazioni o dei sistemi operativi.
- *bandwidth flooding* (inondazione di banda): invio massivo di pacchetti all'host obiettivo impedendo al traffico legittimo di raggiungerlo.
- *connection flooding* (inondazione di connessioni): stabilire un gran numero di connessioni TCP con l'host obiettivo, impedendogli di accettare le connessioni legittime.

Malintenzionati : negazione del servizio (denial-of-service, DoS)

Negazione del servizio (Denial of Service (DoS)): gli aggressori rendono una rete, un host o altro elemento infrastrutturale non disponibili per gli utenti legittimi.

bandwidth flooding:

L'attaccante invia traffico a una velocità prossima a R_s (velocità di accesso del server)



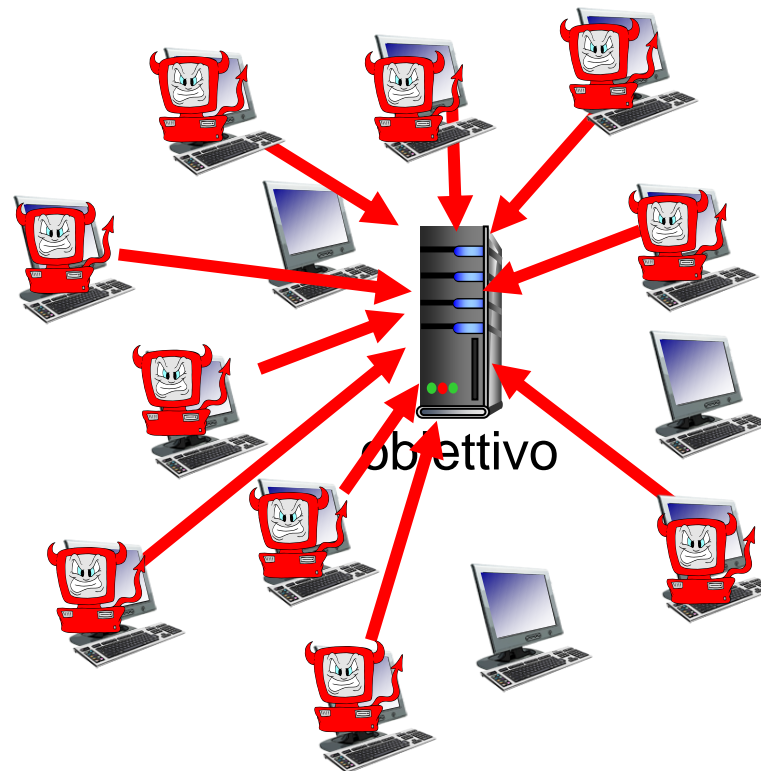
Una singola sorgente di attacco potrebbe avere una velocità di accesso insufficiente (tipicamente $R_c \ll R_s$) e sarebbe comunque facile da identificare e bloccare.

Malintenzionati : negazione del servizio (denial-of-service, DoS)

Negazione del servizio (Denial of Service (DoS)): gli aggressori rendono una rete, un host o altro elemento infrastrutturale non disponibili per gli utenti legittimi.

Distributed denial-of-service (DDoS)


1. selezionare l'obiettivo
2. irrompere negli host attraverso la rete (vedi botnet)
3. inviare pacchetti verso l'obiettivo da host compromessi



Linee di difesa

- **autenticazione:** dimostrare che siete chi dite di essere
 - Le reti cellulari forniscono un'identità hardware attraverso la carta SIM; in Internet tradizionale non esiste un'assistenza hardware di questo tipo.
- **riservatezza:** attraverso la cifratura
- **integrità:** le firme digitali prevengono/rilevano le manomissioni
- **restrizioni di accesso:** VPN (Virtual Private Network) protette da password
- **firewalls:** "middlebox" specializzate nelle reti di accesso e di base:
 - off-by-default: filtrare i pacchetti in entrata per limitare i mittenti, i destinatari e le applicazioni
 - rilevare/reagire agli attacchi DOS

Firewall implementato spesso anche negli host in software (es. nel sistema operativo)

- 
- protezione da IP spoofing (es. impedire l'ingresso in una LAN di pacchetti provenienti da altre reti ma il cui mittente dichiarato appartiene alla LAN)
 - impedire connessioni a applicazioni
 - etc.

... e molto altro si potrebbe dire ancora

Capitolo 1: tabella di marcia

- Cos'è Internet?
- Cos'è un protocollo?
- Ai confini della rete: host, reti di accesso, mezzi trasmissivi
- Il nucleo della rete: commutazione di pacchetto e commutazione di circuito, struttura di Internet
- Prestazioni: perdite, ritardi, throughput
- Sicurezza
- Livelli di protocollo, modelli di servizio
- Un po' di storia



Livelli di protocollo e modelli di riferimento

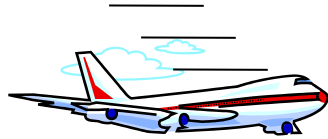
Le reti sono complesse,
con molti “pezzi”:

- host
- router
- svariate tipologie di mezzi trasmissivi
- applicazioni
- protocolli
- hardware, software

Domanda: c'è qualche speranza di organizzare l'architettura delle reti?

- e/o la nostra trattazione sulle reti?

Esempio: organizzazione di un viaggio aereo



——— *trasferimento end-to-end di persona e bagaglio* ———→

biglietto (acquisto)

bagaglio (imbarco)

gate (entrata)

pista di decollo

instradamento aereo

biglietto (proteste)

bagaglio (ritardo)

gates (uscita)

pista di atterraggio

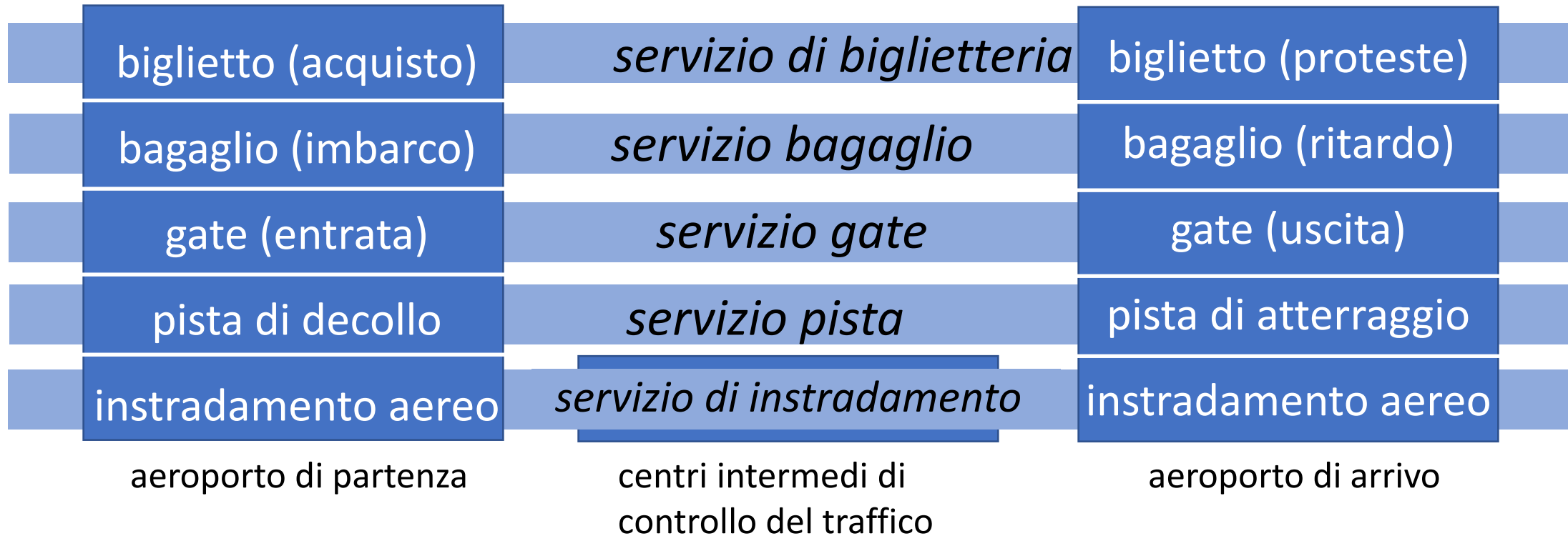
instradamento aereo

instradamento aereo

Come *definireste/discutereste* il *sistema* dei viaggi in aereo?

- una serie di passaggi che coinvolgono molti servizi

Esempio: organizzazione di un viaggio aereo



livelli o strati (layer): ogni livello implementa un servizio

- effettuando determinate azioni all'interno del livello
- utilizzando i servizi del livello immediatamente inferiore

Perché la stratificazione?

Approccio alla progettazione/discussione di sistemi complessi

- una struttura esplicita consente l'identificazione dei vari componenti di un sistema complesso e delle loro inter-relazioni
 - analisi del *modello di riferimento a strati*
- la modularizzazione facilita la manutenzione e l'aggiornamento di un sistema
 - modifica dell'implementazione del servizio del livello: trasparente al resto del sistema
 - es. le modifiche alla procedura di gate non influiscono sul resto del 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 (es. un valore di natura temporale) disponibile solo all'interno di un livello inferiore

Pila di protocolli (protocol stack) di Internet

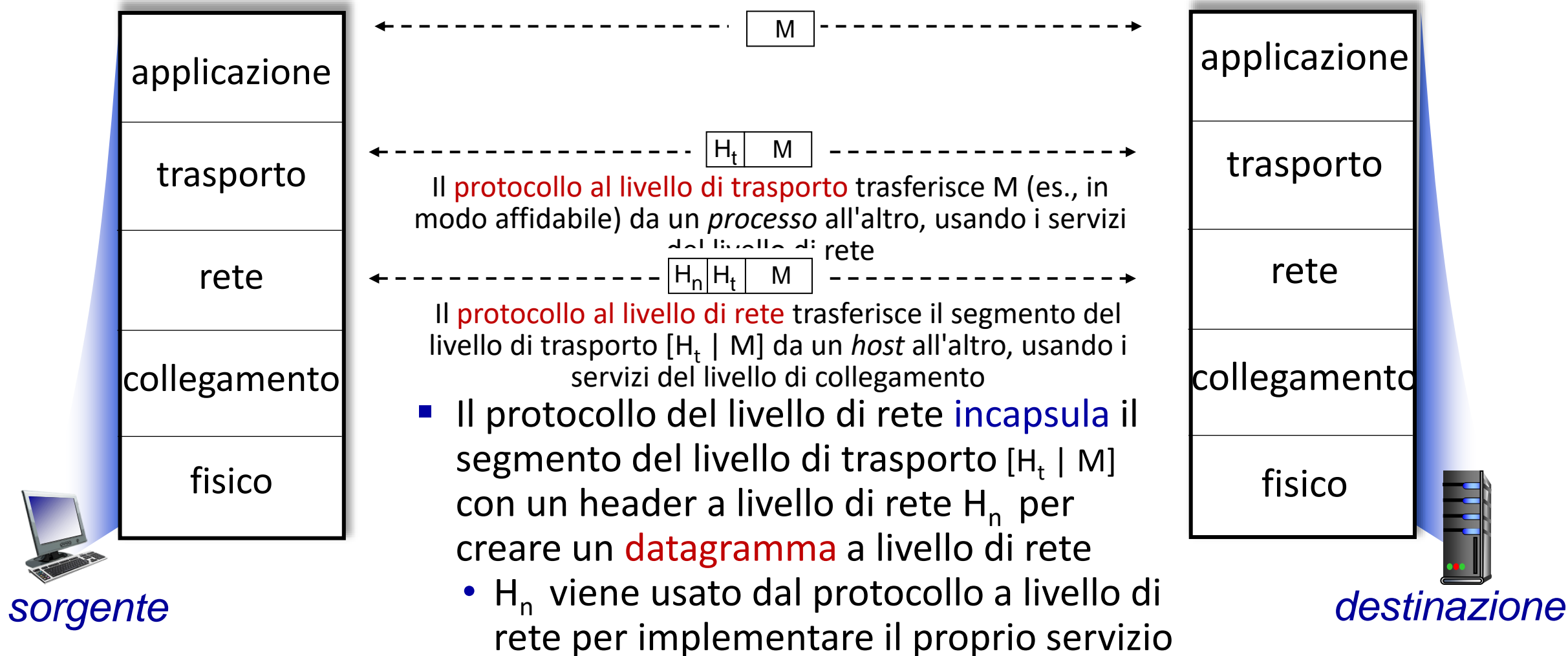
- **applicazione (application layer):** supporto alle applicazioni di rete
 - HTTP, IMAP, SMTP, DNS, *funzionalità critica ma implementata a livello applicativo negli host*
- **trasporto (transport layer):** trasferimento di dati tra processi (in esecuzione su host differenti)
 - TCP, UDP
- **rete (network layer):** trasferimento di pacchetti di rete, detti datagrammi, da un host all'altro
 - IP, protocolli di instradamento
- **collegamento (link layer):** trasferimento di dati tra elementi di rete vicini
 - Ethernet, 802.11 (WiFi), PPP
- **fisico (physical layer):** bit “sul filo”



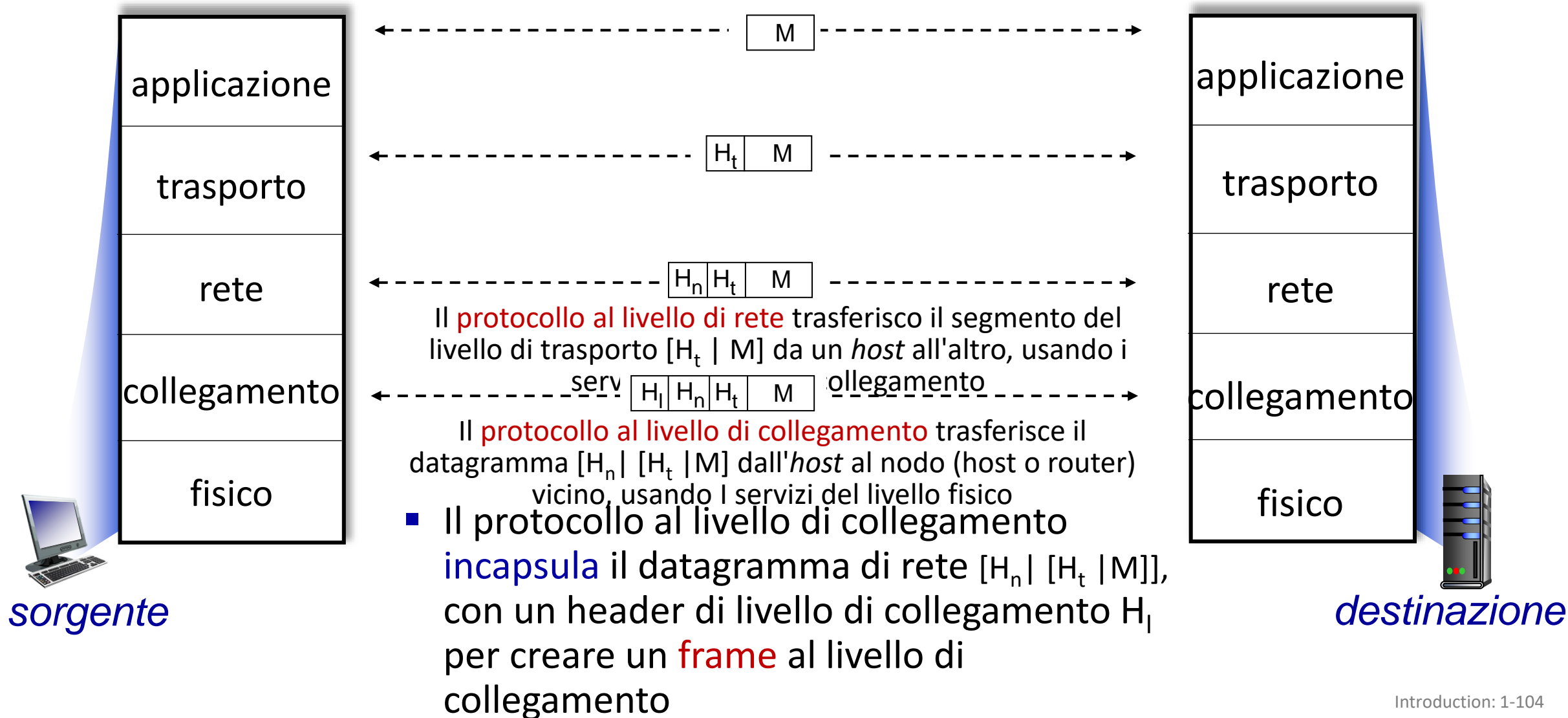
Servizi, Stratificazione e Incapsulamento



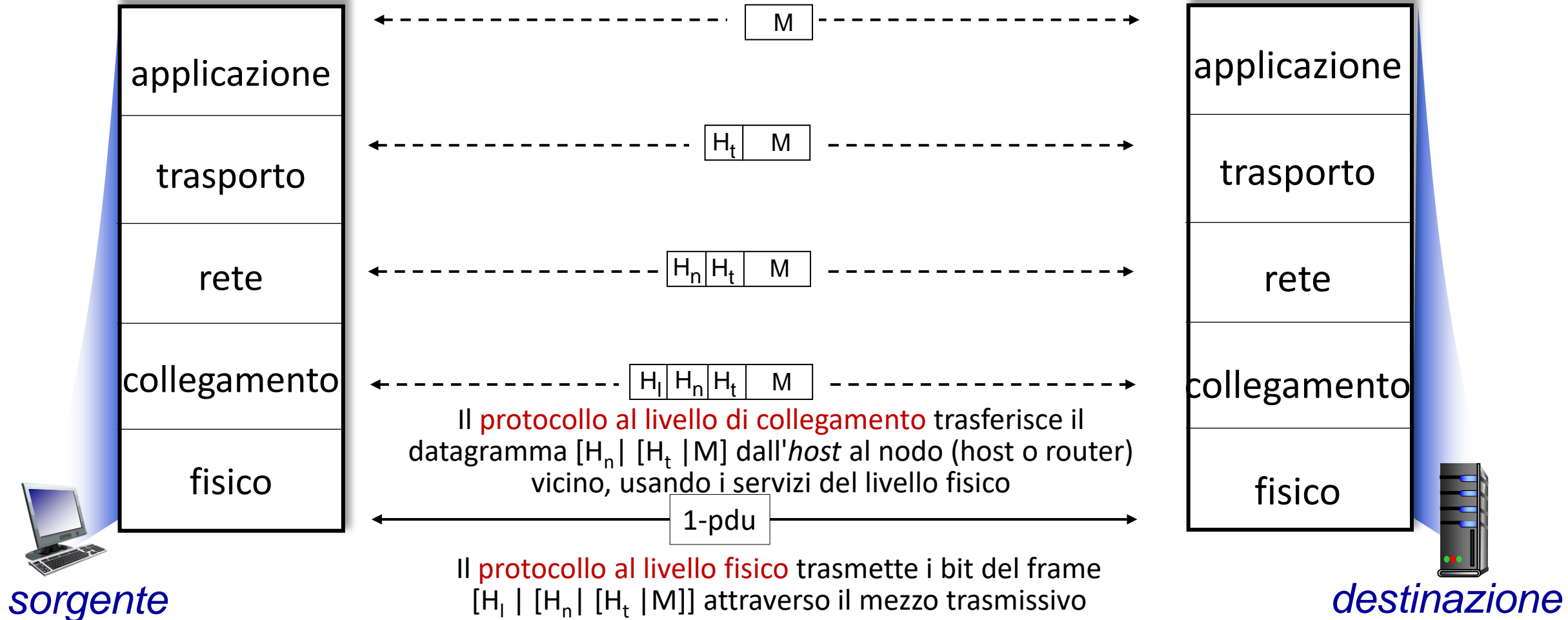
Servizi, Stratificazione e Incapsulamento



Servizi, Stratificazione e Incapsulamento



Servizi, Stratificazione e Incapsulamento

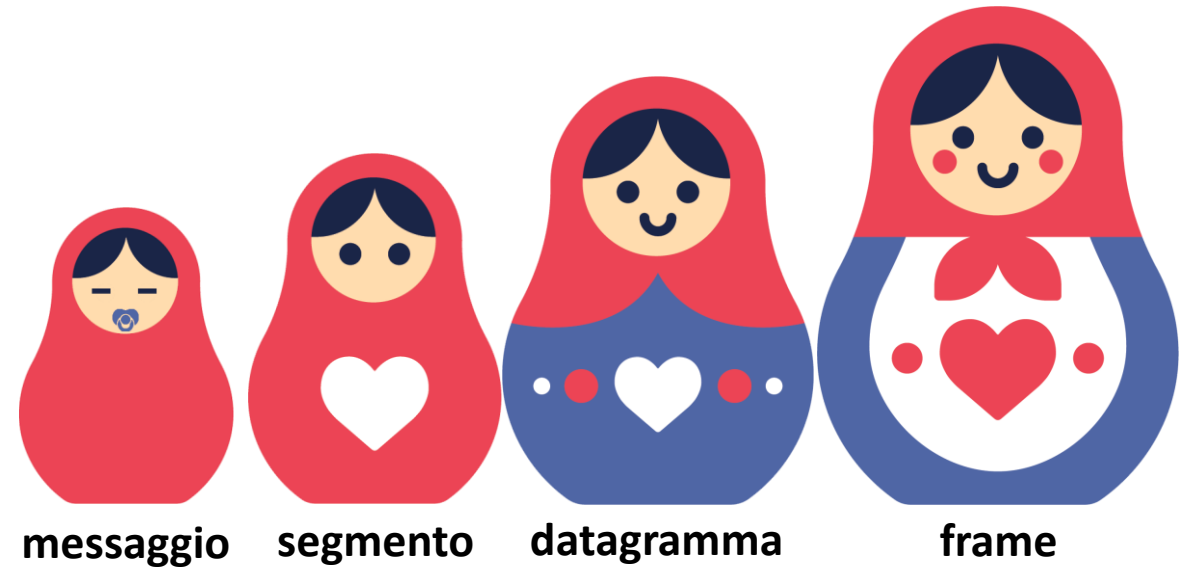


Modello di servizio (*service model*)

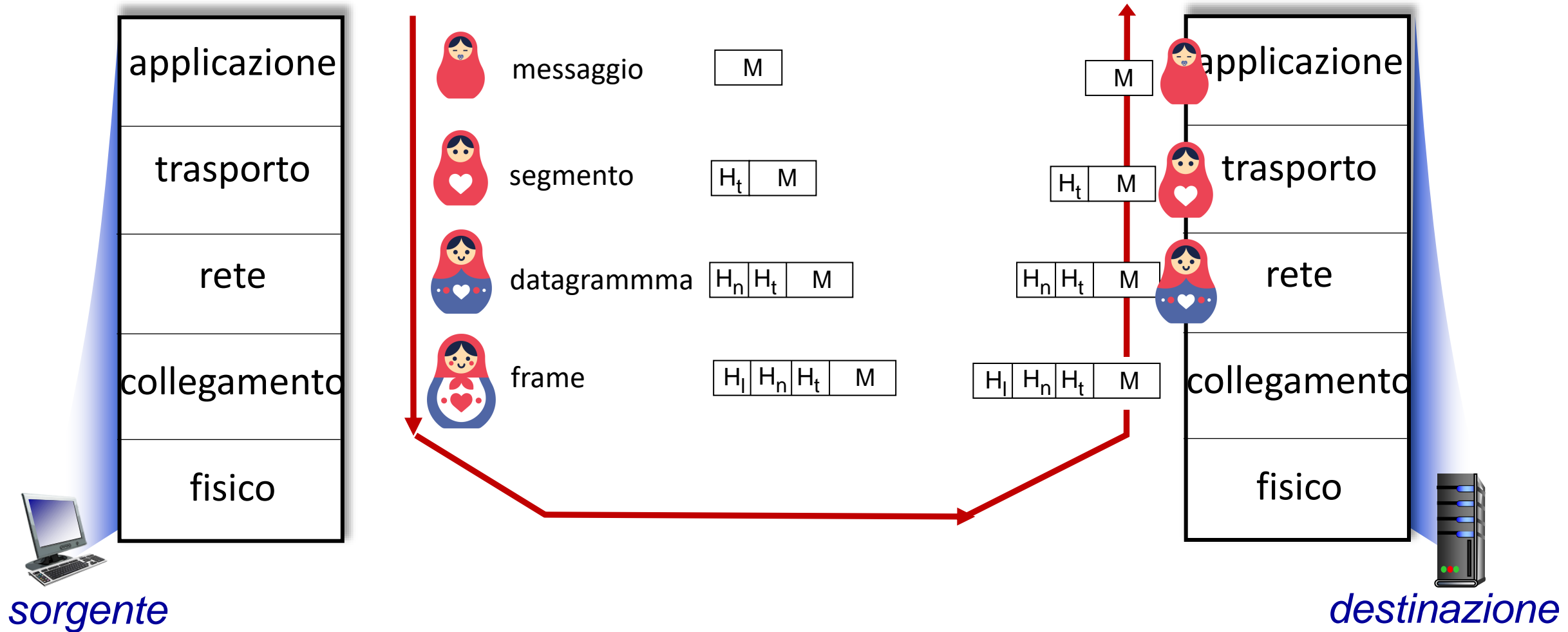
- Insieme dei servizi offerti da un livello a quello superiore
- I diversi servizi possono essere implementati da protocolli diversi
- Il livello di collegamento può offrire al servizio di rete servizi diversi lungo ciascun collegamento nel percorso dalla sorgente alla destinazione in base al protocollo impiegato su ciascun collegamento (es. Ethernet, Wi-Fi, PPP).
- 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. Ethernet, ad esempio, ha molti protocolli dello strato fisico: es. uno per doppino intrecciato, uno per la fibra ottica, uno per il cavo coassiale.

Incapsulamento

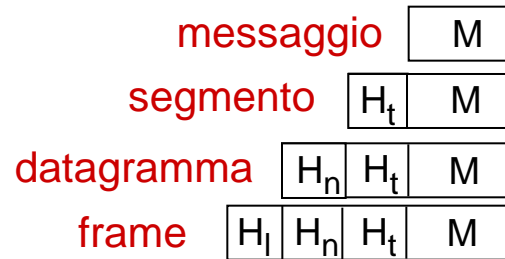
Bambole matrioska (bambole impilabili)



Servizi, Stratificazione e Incapsulamento



Incapsulamento: una visione end-to-end

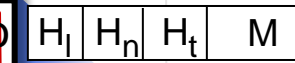
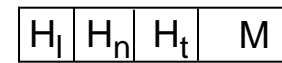
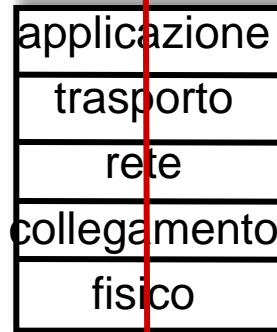


Un protocollo di livello n può essere **distribuito** tra sistemi periferici, commutatori di pacchetto e altri elementi di rete.

Si noti che host, router e switch implementano ciascuno solo i livelli adeguati alle loro funzionalità.

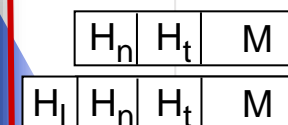
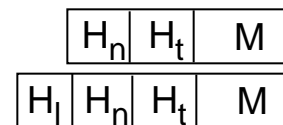


sorgente



switch

A seguito dell'inoltro, l'intestazione H_n può cambiare (es. decremento *Time to live*)



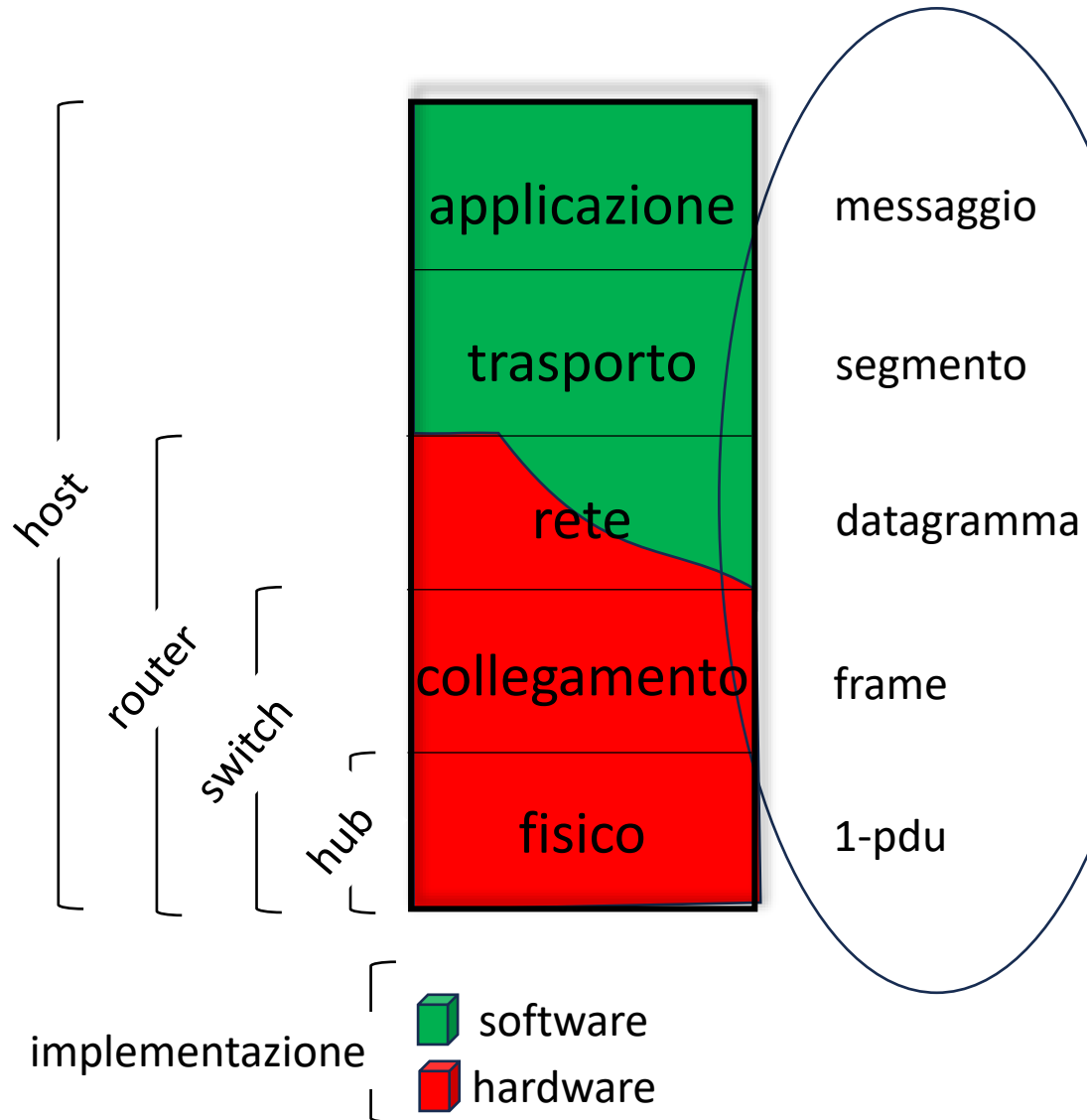
router

Il livello di rete può ricevere un servizio diverso dai protocolli del livello di collegamento, man mano che un datagramma attraversa collegamenti di tipo diverso.

Incapsulamento: una visione end-to-end

- L'intestazione del datagramma contiene gli indirizzi a livello di rete (indirizzi IP) dell'host sorgente e dell'host destinazione. Questi indirizzi non cambiano mentre il pacchetto attraversa la rete a meno di alcuni casi che vedremo durante il corso.
- Ad ogni salto (hop) lungo il percorso, l'intestazione del frame di livello 2 viene aggiornata con gli indirizzi a livello di collegamento (MAC) del dispositivo sorgente (ad esempio, la scheda di rete dell'host o del router che sta inviando il frame) e del dispositivo destinazione immediatamente adiacente (il router successivo o l'host di destinazione finale, se è nella stessa rete).
- Gli switch sono trasparenti (non vengono mai indirizzati esplicitamente)
- Dal punto di vista del livello di rete, due nodi sono adiacenti se possono comunicare direttamente tra loro tramite il livello di collegamento, *senza* dover passare per un router.

n-PDU, implementazione dei livelli



n-PDU (*protocol data unit*): è la singola unità di informazione scambiata tra pari attraverso un protocollo di livello n.

- specifiche informazioni di controllo per il protocollo
- carico utile (payload): in genere una (n+1)-PDU

Gli host implementano tutti e 5 livelli: maggiore complessità nella periferia della rete!

I dispositivi che non implementano un livello non ne interpretano/elaborano la PDU.

Modello di riferimento ISO/OSI

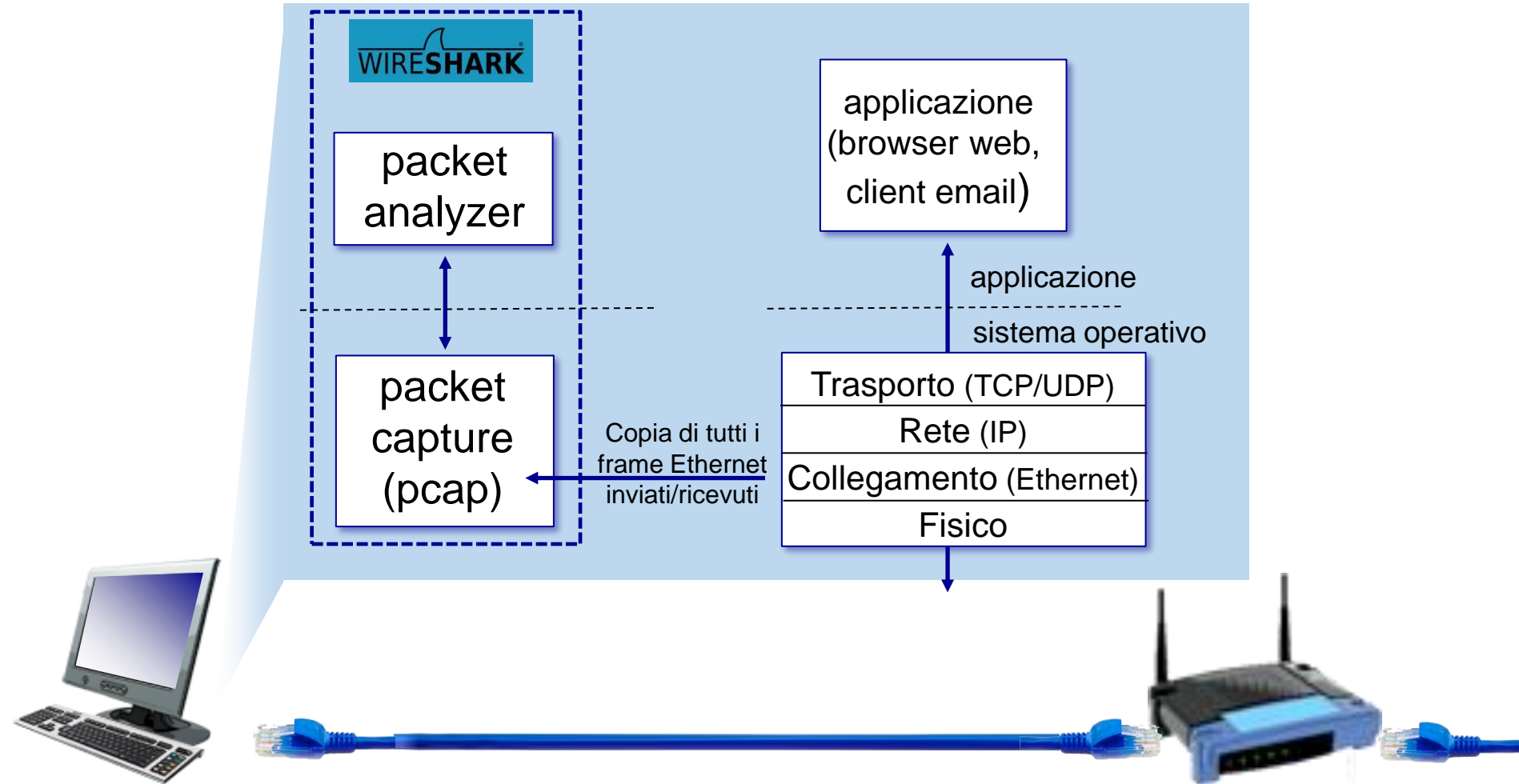
Due strati non presenti nella pila di protocolli di Internet!

- *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
- La pila di Internet "manca" di questi strati!
 - questi servizi, *se necessari*, devono essere implementati nelle applicazioni
 - necessari?



Il modello di riferimento ISO/OSI a 7 strati

Wireshark



Capitolo 1: tabella di marcia

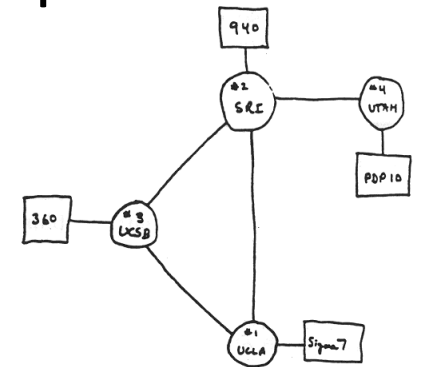
- Cos'è Internet?
- Cos'è un protocollo?
- Ai confini della rete: host, reti di accesso, mezzi trasmissivi
- Il nucleo della rete: commutazione di pacchetto e commutazione di circuito, struttura di Internet
- Prestazioni: perdite, ritardi, throughput
- Sicurezza
- Livelli di protocollo, modelli di servizio
- Un po' di storia



Storia di Internet

1961-1972: Sviluppo della commutazione di pacchetto

- **1961:** Kleinrock – usando la teoria delle code, dimostrò l'efficacia dell'approccio a commutazione di pacchetto per sorgenti di traffico intermittenti
- **1964:** Baran – investigò l'uso della commutazione di pacchetto nelle reti militari
- **1967:** il progetto ARPAnet viene concepito dall'Advanced Research Projects Agency
- **1969:** primo nodo operativo ARPAnet
- **1972:**
 - dimostrazione pubblica di ARPAnet
 - NCP (Network Control Protocol) primo protocollo host a host
 - Primo programma di posta elettronica
 - ARPAnet ha 15 nodi



THE ARPA NETWORK

Storia di Internet

1972-1980: Internetworking e reti proprietarie

- **1970:** rete satellitare ALOHAnet nelle Hawaii
- **1974:** Cerf e Kahn – architettura per l'interconnessione delle reti
- **1976:** Ethernet allo Xerox PARC
- **Fine anni '70:** architetture proprietarie: DECnet, SNA, XNA
- **1979:** ARPAnet ha 200 nodi

I principi di Cerf e Kahn sull'internetworking:

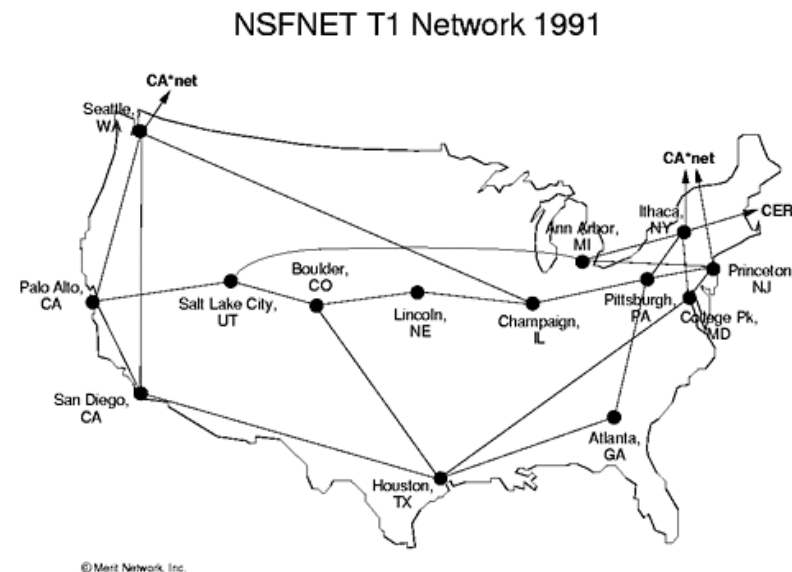
- minimalismo, autonomia – per collegare le varie reti non occorrono cambiamenti interni
- modello di servizio best effort
- router stateless
- controllo decentralizzato

definiscono l'attuale architettura di Internet

Storia di Internet

1980-1990: nuovi protocolli, proliferazione delle reti

- **1983:** rilascio di TCP/IP
- **1982:** definizione del protocollo SMTP per la posta elettronica
- **1983:** definizione del DNS per la traduzione degli indirizzi IP
- **1985:** definizione del protocollo FTP
- **1988:** controllo della congestione TCP
- nuove reti nazionali: CSnet, BITnet, NSFnet, Minitel
- 100,000 host collegati alla confederazione delle reti



Storia di Internet

1990, 2000s: commercializzazione, Web, nuove applicazioni

- primi anni '90: ARPAnet viene dismessa
- 1991: NSF lascia decadere le restrizioni sull'uso commerciale di NSFnet (dismessa nel 1995)
- primi anni '90: Web
 - ipertestualità [Bush 1945, Nelson 1960's]
 - HTML, HTTP: Berners-Lee
 - 1994: Mosaic, poi Netscape
 - fine anni '90: commercializzazione del web

Fine anni '90 – inizi 2000:

- arrivano le "killer application": messaggistica istantanea, condivisione di file P2P
- sicurezza di rete in primo piano
- stimati 50 milioni di host, 100 milioni+ di utenti
- velocità nelle dorsali dell'ordine di Gbps

Storia di Internet

2005-presente: scala, SDN, mobilità, cloud

- diffusione aggressiva dell'accesso domestico a banda larga (10-100 Mbps)
- 2008: software-defined networking (SDN)
- la crescente ubiquità dell'accesso wireless ad alta velocità: 4G/5G, WiFi
- i fornitori di servizi (Google, FB, Microsoft) creano le proprie reti
 - scavalcare l'Internet commerciale per connettersi "vicino" all'utente finale, fornendo un accesso "istantaneo" ai social media, alla ricerca, ai contenuti video, ...
- le imprese gestiscono i loro servizi in "cloud" (es., Amazon Web Services, Microsoft Azure)
- ascesa degli smartphone: più dispositivi mobili che fissi su Internet (2017)
- ~15 miliardi di dispositivi connessi a Internet (2023, statista.com)

Capitolo 1: riassunto

Abbiamo coperto una "tonnellata" di materiale!

- Internet overview
- cos'è un protocollo?
- ai confine della rete, reti di accesso, nucleo
 - commutazione di pacchetto versus commutazione di circuito
 - struttura di Internet
- prestazioni: perdite, ritardi, throughput
- stratificazione, modelli di servizio
- sicurezza
- storia

Ora avete

- contesto, visione d'insieme, vocabolario, "sensazione" di rete
- più profondità, dettaglio e *divertimento* da seguire!