



*Corso di Laurea Triennale in Informatica
Università degli Studi della Basilicata*

Reti di Calcolatori

Docente: Ugo Erra

ugo.erra+reti@unibas.it

3° Lezione – Livelli di protocollo

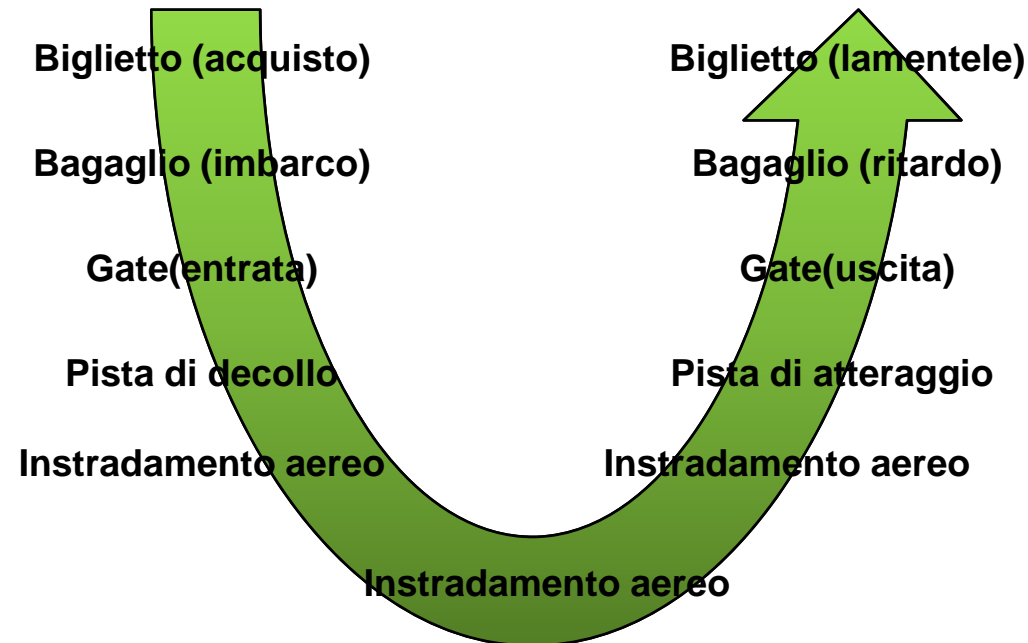
Livelli di protocollo



- Le reti sono complesse
 - ▣ Diversi mezzi di trasmissione
 - ▣ Diverse applicazioni
 - ▣ Diversi protocolli
 - ▣ Diversi componenti hardware (router, host, etc...)
- Questa complessità impone una organizzazione architettonica

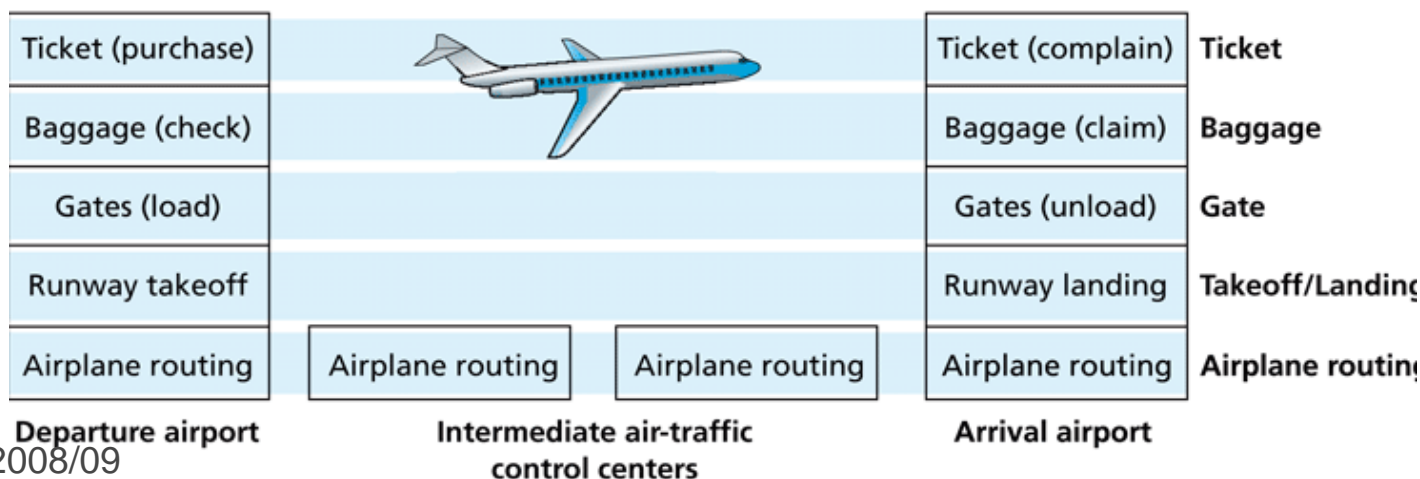
Come organizziamo un viaggio aereo?

- Organizzare un volo è complesso ma procedendo attraverso una serie di passi diventa più semplice



Livelli di servizio

- Ciascun livello realizza un servizio nel seguente modo:
 - ▣ All'interno dello stesso livello vengono effettuate determinate azioni
 - ▣ Ogni livello utilizza i servizi del livello immediatamente inferiore



Stratificare un sistema complesso

- Una struttura a livelli 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
 - ▣ Modifiche implementative al servizio di uno dei livelli risultano trasparenti al resto del sistema
 - es.: modifiche nelle procedure effettuate al gate non condizionano il resto del sistema

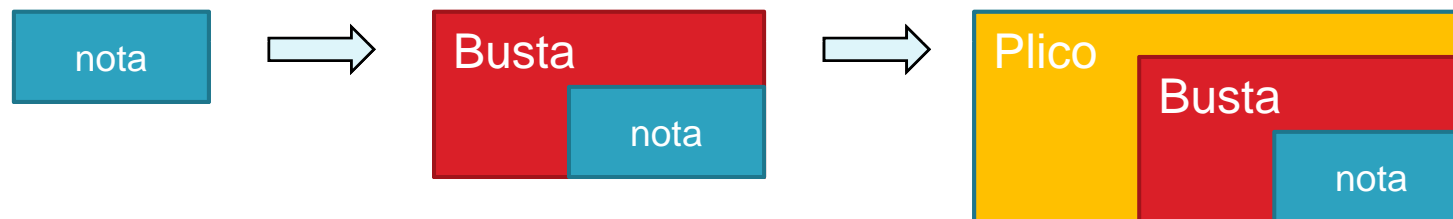
Pila di protocolli Internet

- **Applicazione**
 - ▣ Supporto alle applicazioni di rete (FTP, SMTP, HTTP)
- **Trasporto**
 - ▣ Trasferimento dei messaggi a livello di applicazione tra il modulo client e server di un'applicazione (TCP, UDP)
- **Rete**
 - ▣ Instradamento dei datagrammi dall'origine al destinatario (IP, protocolli di instradamento)
- **Link** (collegamento)
 - ▣ Instradamento dei datagrammi attraverso una serie di commutatori di pacchetto (PPP, Ethernet)
- **Fisico**
 - ▣ Trasferimento dei singoli bit



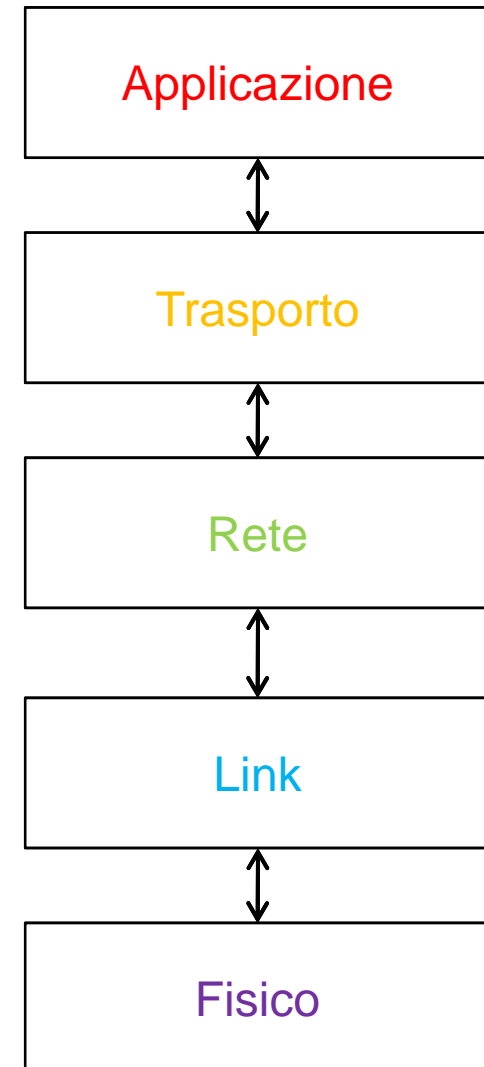
Incapsulamento

- L'incapsulamento descrive il processo con il quale un livello concatena delle informazioni aggiuntive prima di passare il "pacchetto" al livello successivo
- Alla ricezione i dati vengono spaccettati in ordine inverso
- Ad esempio supponiamo di dover inviare una nota da un ufficio all'altro

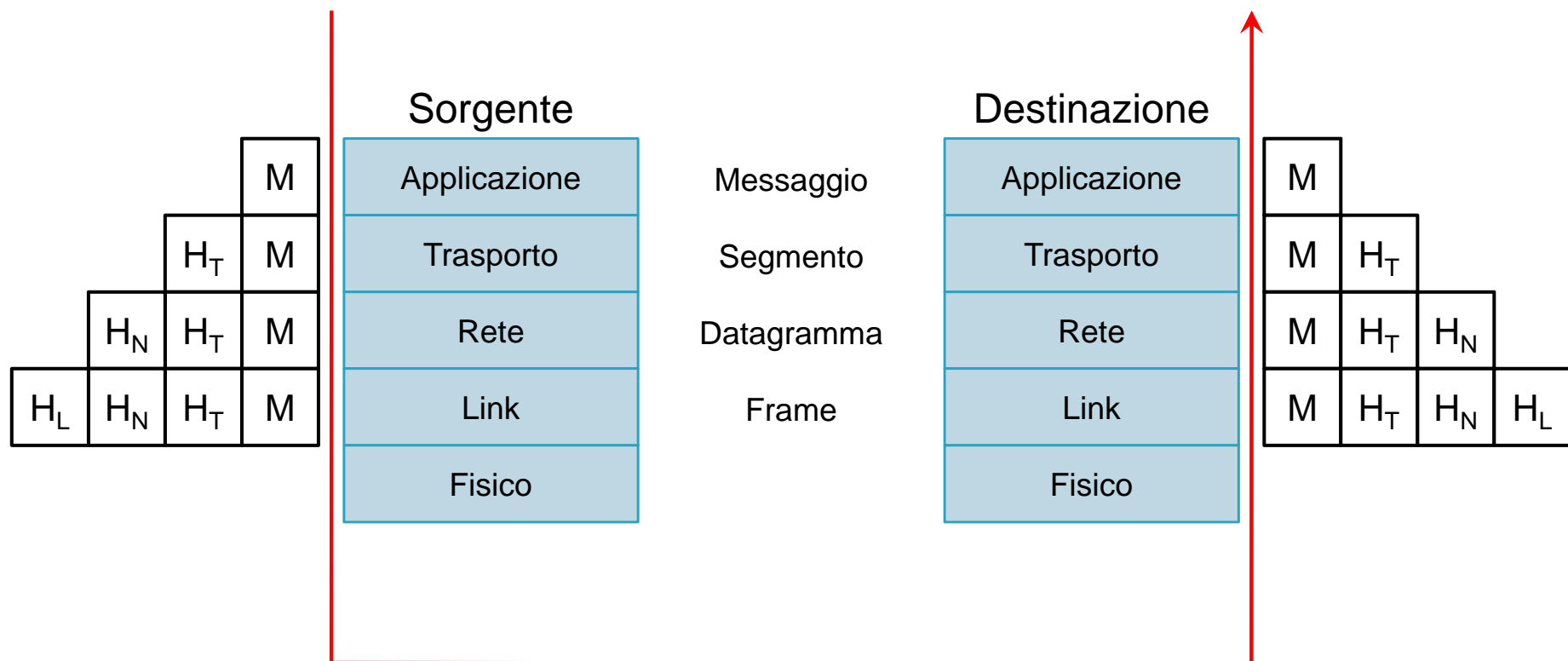


Messaggi, segmenti, datagrammi e frame

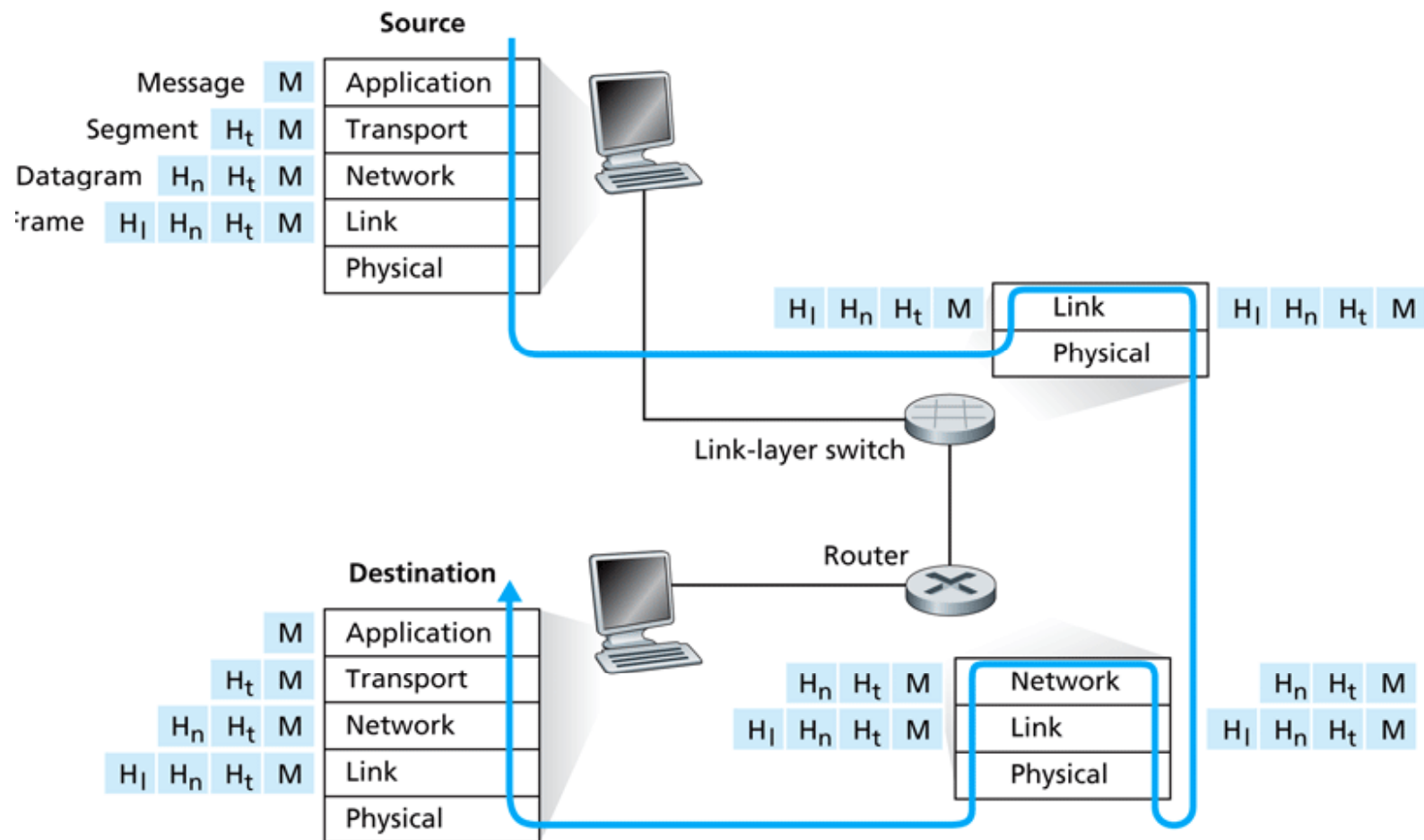
- Un **messaggio al livello applicazione** viene passato al livello trasporto
- Il livello trasporto concatena alcune informazioni al messaggio che diventa un **segmento al livello di trasporto**
- Il livello di rete concatena alcune informazioni al segmento che diventa un **datagramma al livello di rete**
- Il livello di collegamento aggiunge le proprie informazioni al segmento che diventa un **frame a livello di collegamento**



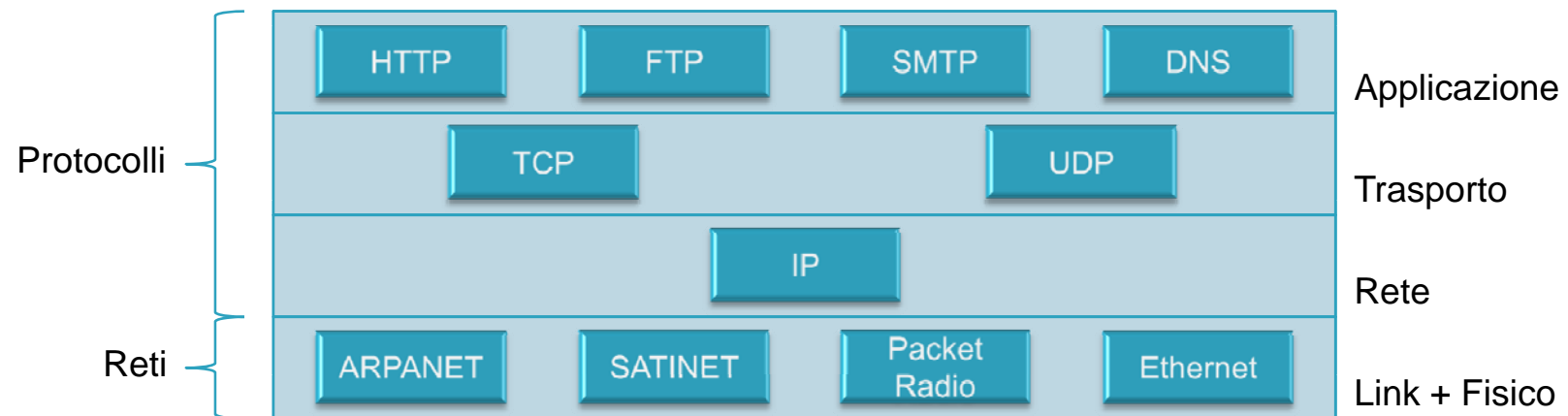
Incapsulamento pila dei protocolli



Pila di protocolli in Internet



Protocolli e Reti nel modello TCP/IP



Throughput

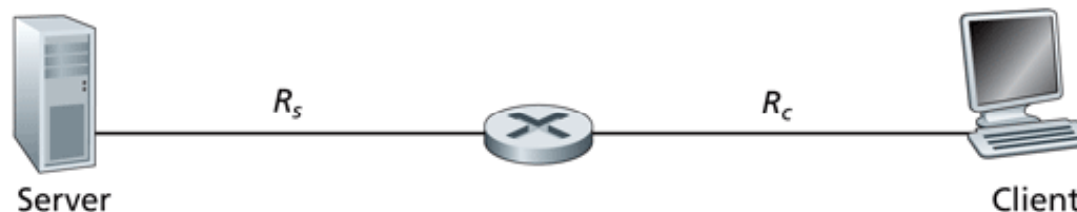


- Il **throughput** misura la velocità in bps con il quale trasferiamo i bit da una sorgente alla destinazione
 - ▣ Quando è misurato in un istante di tempo preciso è definito **throughput istantaneo**
 - ▣ Quando è misurato su di un periodo più lungo è definito **throughput medio**

Un semplice scenario - 1

- Consideriamo il trasferimento di un file tra client e server
 - ▣ Un solo router separa il client dal server
 - ▣ Il server ha una frequenza di collegamento di R_s
 - ▣ Il client ha un frequenza di collegamento di R_c
- Cosa avviene se $R_s < R_c$?
 - ▣ I bit inviati dal server arriveranno ad un frequenza R_s
- Cosa avviene se $R_c < R_s$?
 - ▣ I bit inviati dal server arriveranno ad un frequenza R_c
- In generale la frequenza di trasmissione end-to-end e quindi il **collo di bottiglia** o (*bottleneck*) sarà

$$\min (R_s, R_c)$$



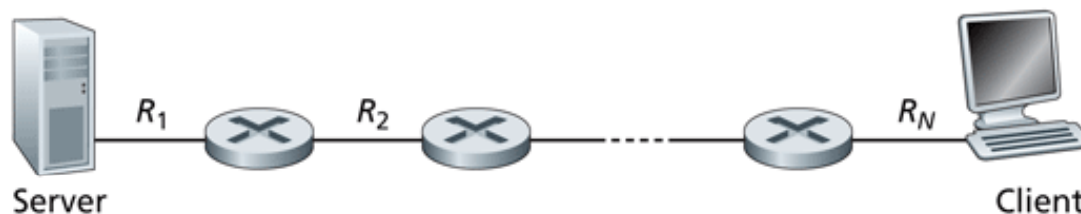
Un semplice scenario - 2

- Consideriamo N collegamenti tra server e client con frequenze di trasmissioni

$$R_1, R_2, \dots, R_N$$

- Il throughput end-to-end tra server e client sarà di

$$\min (R_1, R_2, \dots, R_N)$$

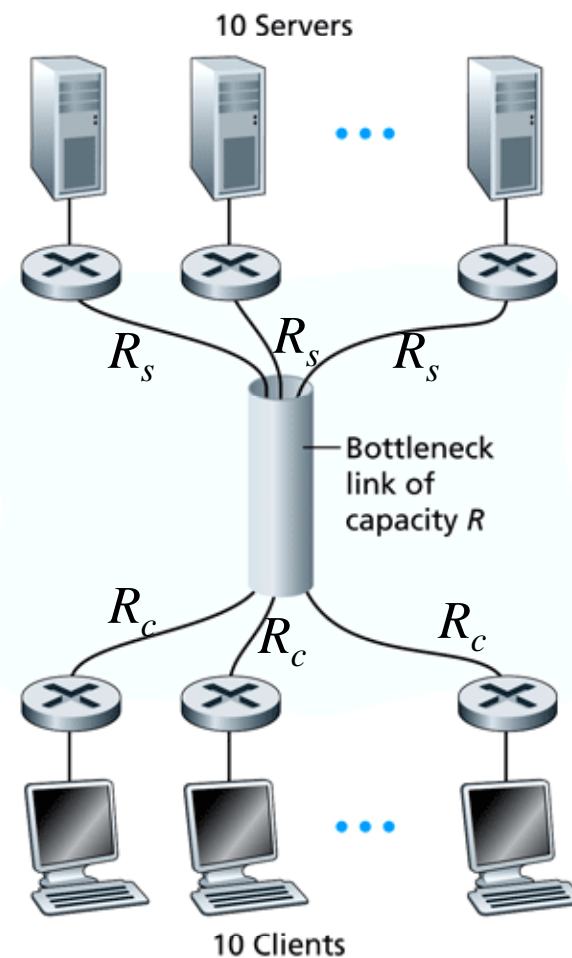


Un semplice scenario - 3

- Su internet il throughput è influenzato dalle connessioni condivise
- Il throughput è in questo caso

$$\min (R_s, R_c, R/10)$$

- Ad esempio se $R_s=2\text{Mbps}$, $R=5\text{Mbps}$, $R_c=1\text{Mbps}$ di quanto sarà il throughput?
 - 500kbps



Sicurezza di internet

- Quando parliamo di sicurezza su internet studiamo
 - ▣ In che modo i malintenzionati possono attaccare una rete
 - ▣ In che modo possiamo difenderci dagli attacchi
 - ▣ In che modo progettare reti immuni dagli attacchi
- Internet non è nata inizialmente con il “pallino” della sicurezza
 - ▣ Nella visione originale era basata sul modello “gruppo di utenti mutuamente fidati collegati a una rete trasparente”
 - ▣ Negli ultimi anni i progettisti stanno recuperando il terreno perso sul fronte della sicurezza
 - ▣ In ogni livello dello stack TCP/IP vengono analizzati possibili problemi di sicurezza

Malware



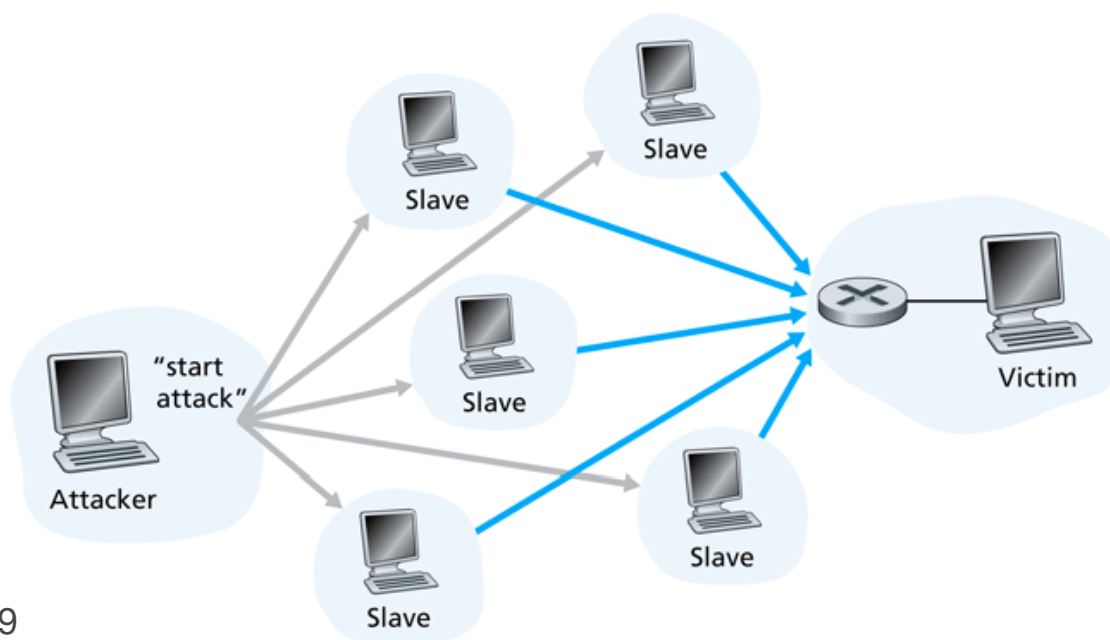
- Un *malware* è un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito
 - ▣ Un malware ha la capacità di autoreplicarsi e diffondersi su altri host
- Uno *spyware* è un malware che può registrare cosa digitiamo, i siti web visitati o prelevare informazioni dalla nostra macchina
- Una *botnet* è una rete costituita da diverse macchine infettate utilizzate per scopi non leciti
 - ▣ Utilizzate per fare spam o attacchi DDoS

Tipi di malware

- Cavalli di Troia
 - ▣ Nascosto all'interno di software apparentemente innocuo
 - ▣ Oggi molto diffuso tra le pagine web
- Virus
 - ▣ L'infezione normalmente avviene aprendo email o lanciando applicazioni
 - ▣ Normalmente si auto-replicano propagandosi ad altri host
- Worm
 - ▣ Letteralmente "verme" è una particolare categoria di malware in grado di auto-replicarsi
 - ▣ È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi

DoS: Negazione del servizio

- La **negazione del servizio** o *denial-of-service* (DoS) consiste nell'attaccare una risorsa rendendola non disponibile agli utenti legittimi
 - ▣ Normalmente una botnet viene ingaggiata per portare avanti il DoS



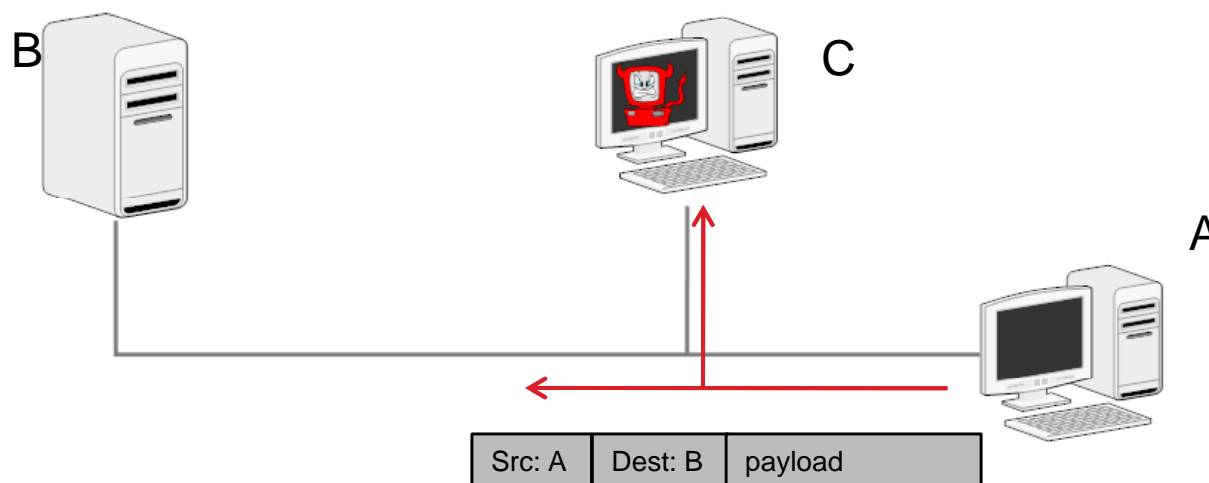
Tipi di attacchi DoS



- Attacchi alla vulnerabilità dei sistemi
 - ▣ Invia di messaggi costruiti ad-hoc per bloccare il servizio
- Flooding di banda
 - ▣ Inondare il bersaglio di pacchetti in modo da ostruire il collegamento di accesso
- Flooding di connessione
 - ▣ Aprire un gran numero di connessioni TCP impedendogli di aprire le connessioni legittime

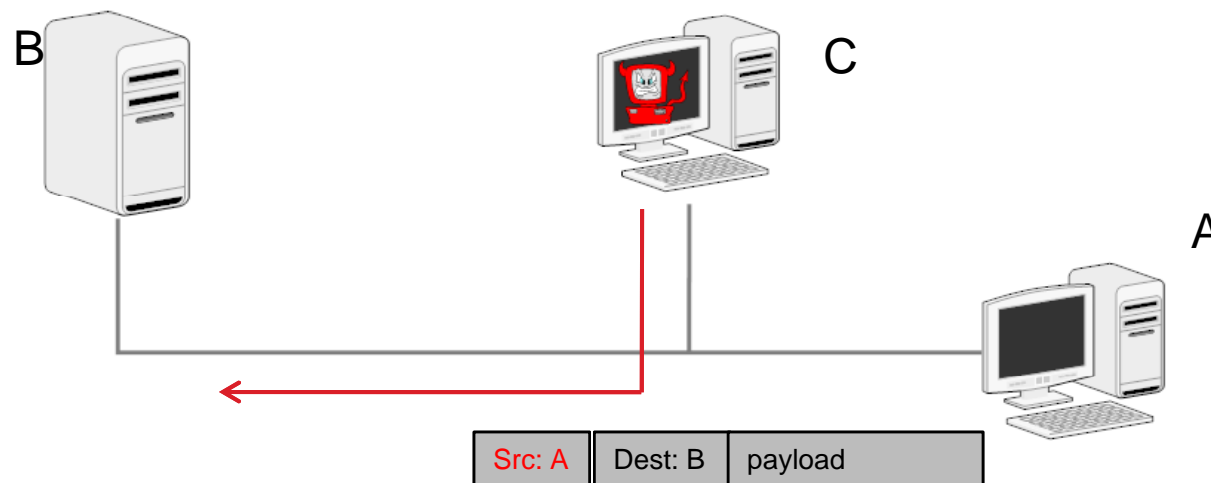
Analisi dei pacchetti

- Un **analizzatore di pacchetti** o *packet sniffer* memorizza una copia di ciascun pacchetto che transita su un mezzo di trasmissione
 - ▣ Utilizzati anche per scopi didattici
 - ▣ Sono passivi quindi difficilmente individuabili
 - ▣ Una possibile soluzione è usare la crittografia



Mascheramento

- Il **mascheramento** o *IP spoofing* consiste nel creare dei pacchetti con un falso indirizzo sorgente
 - Il TCP/IP per sua natura permette di realizzare facilmente un pacchetto del genere
- Un utente può cambiare identità senza che la destinazione si accorga di nulla
- Una soluzione consiste in una autenticazione end-to-end
 - Avere certezza che la sorgente sia esattamente quella che ci aspettiamo



Cancellazione e modifica

- Nell'attacco **uomo nel mezzo** o *man-in-the-midde* un malintenzionato si inserisce nel cammino tra due host
 - ▣ Ad esempio potrebbe sostituirsi ad un router compromesso immettendo, modificando o cancellando i pacchetti

