
RETI DI CALCOLATORI

Corso A

Autore

Giuseppe Acocella

2025/26

<https://github.com/Peenguino>

Ultima Compilazione - September 27, 2025

Contents

1	Introduzione alle Reti	3
1.1	Tipi di Rete per Dimensione	4
1.2	Gestione di Internet come Rete di Reti	4
1.3	Reti e Mezzi d'Accesso	4
1.3.1	Schema dell'Accesso DSL	4
1.3.2	Tipi d'Accesso - Cavo, Aziendale, Domestico, Mobile e Satellitare . . .	5
1.4	Nucleo della Rete - Commutazione Circuito vs Pacchetto	6
1.5	Metriche - Prestazioni della Rete (Latenza, Throughput, Prod. Rate/Ritardo)	7
1.6	Modello Stratificato	8
1.6.1	Stack Protocollore TCP/IP	8
1.6.2	Stack Protocollore ISO/OSI - Cenno Storico	9
1.7	Breve Introduzione alla Sicurezza di Reti	9
2	Livello Applicazione	10
2.1	Introduzione a Paradigmi, Protocolli e Tipi d'Utilizzo	10

1 Introduzione alle Reti

Come facciamo a costruire una rete di computer che sia scalabile e che supporti **svariati tipi di applicazioni** come streaming, messaggistica e videochiamate? Internet ci permette di farlo, e tecnicamente è un insieme di miliardi di host (servers, laptops, smartphones) connessi tra loro.

Internet - Vista dei Componenti Questa connessione è permessa da specifici componenti:

1. **Link di Comunicazione:** Fibra ottica, rame, onde radio, microonde.
2. **Dispositivi di Interconnessione:** I più comuni sono:
 - (a) **Switch:** Dispositivo che collega tra loro **più host**.
 - (b) **Router:** Dispositivo che collega tra loro **più reti**.
3. **Reti:** Insieme di host, dispositivi di interconnessione e link gestiti da una stessa organizzazione.

Internet - Vista dei Servizi Da un punto di vista di servizi offerti invece Internet:

1. E' un **infrastruttura** che offre servizi alle **applicazioni distribuite**.
2. Offre un **interfaccia di programmazione** (socket) che permette alle applicazioni, distribuite su **host diversi**, di scambiarsi informazioni.

Internet - Vista delle Entità Software

1. **Applicazioni:** Elaborano e si scambiano informazioni.
2. **Protocolli:** Regolano la trasmissione di queste informazioni, definendo quindi il formato e l'ordine dei messaggi scambiati tra due o più entità in comunicazione. Due esempi noti di protocolli internet sono:
 - (a) **Transmission Control Protocol (TCP)**
 - (b) **Internet Protocol (IP)**

Standardizzazione di Protocolli I protocolli di Internet vengono standardizzati da diversi enti, come:

1. Internet Engineering Task Force (IETF). Si basano su una procedura detta RFC (Request for Comments) che seguendo passi rigorosi definisce gradualmente nuovi standard per Internet.
2. IEEE 802 LAN Standards.
3. World Wide Web Consortium (W3C): Comunità internazionale che sviluppa standard aperti per favorire lo sviluppo del Web.

1.1 Tipi di Rete per Dimensione

Descrizione dei tipi di rete per estensione fisica:

1. **Personal Area Network (PAN)**: Connessione personale, ad esempio una Bluetooth.
2. **Local Area Network (LAN)**: Reti circoscritte ad un'area limitata, utilizzano cavi o mezzi wireless per connettersi e sono solitamente proprietarie.
3. **Metropolitan Area Network (MAN)**: Rete di calcolatori che non supera mai l'estensione fisica indicativa di una "città".
4. **Wide Area Network (WAN)**: Reti che cercano di interconnettere host separati da distanze geografiche tramite cavi in fibra ottica o ponti radio.

1.2 Gestione di Internet come Rete di Reti

Ogni rete locale si espone alle altre reti grazie agli **Internet Service Provider (ISP)**. Come possiamo immaginare però non connettiamo ogni punto terminale ad ogni altro punto terminale perchè provocherebbe un'alta complessità da un punto di vista di collegamenti. Di conseguenza saranno presenti dei **Global ISP** che si occupano della gestione del route della comunicazione. Non esiste un solo **Global ISP** ma **molteplici** e questi si connettono tra loro con dei **Peering Point** su punti d'incontro tra le reti detti **Internet Exchange Point (IXP)**.

Content Provider Network Idealmente si segue lo schema descritto sopra, ma a volte grandi aziende (Amazon, Google) si posizionano trasversalmente a questa organizzazione descritta, in modo tale da gestire la propria rete per avvicinare i propri servizi all'utente finale.

1.3 Reti e Mezzi d'Accesso

Descriviamo questi elementi caratterizzanti dell'accesso ad una rete:

1. **Rete d'Accesso**: Rete che connette fisicamente un sistema terminale al **edge router**, ossia il primo router da sorgente a destinazione.
2. **Mezzi d'Accesso**: Come passiamo fisicamente dal calcolatore al edge router:
 - (a) **Cablati (Vincolati)**: Doppino, coassiale, fibra.
 - (b) **Wireless (Non Vincolati)**: Onde Radio, microonde, infrarossi.

1.3.1 Schema dell'Accesso DSL

Uno dei primi schemi d'accesso è stato quello Digital Subscriber Line (DSL), dove la compagnia telefonica rappresentava l'ISP. Risultava quindi necessario splittare la linea telefonica già esistendo, suddividendo il traffico in bande di frequenze diverse:

1. **Canale Telefonico**: $0 - 4kHz$
2. **Upstream**: $4 - 50kHz$
3. **Downstream**: $50kHz - 1MHz$

In questo modo sarà necessario un multiplexer di accesso alla linea digitale (DSLAM) che permetta di separare i due tipi di comunicazione. Esistono **versioni diverse** di **questo schema**, riferiremo infatti allo schema **xDSL**, proprio perchè è possibile migliorare le caratteristiche della connessione ad esempio basandosi su una connessione in **fibra** tra DSLAM ed ISP, ad esempio:

1. **Fibre To The Cabinet (FTTC)**: Standard VDSL e VDSL2.
2. **Fibre To The Derivation Point**.
3. **Fibre To The House (FTTH)**: Caratterizzato dai seguenti elementi:
 - (a) Fibra ottica fino all'interno delle abitazioni.
 - (b) Fibra uscente dalla centrale locale con terminatore ottico di linea **OLT** viene condivisa da diverse abitazioni.
 - (c) Il terminatore ottico di rete **ONT** invece è connesso ad uno splitter tramite fibra dedicata, questo permette la gestione fino al centinaio di abitazioni.
 - (d) L'**OLT** si connette al router dell'ISP e tramite questo ad Internet.

1.3.2 Tipi d'Accesso - Cavo, Aziendale, Domestico, Mobile e Satellitare

Descriviamo queste tipologie di accesso alla rete:

1. **Accesso Via Cavo**: Il segnale ottico viene convertito in segnale elettromagnetico e inviato sulle linee di cavi coassiali per la distribuzione del segnale alle varie abitazioni. La velocità potrebbe degradare a causa della distanza o della congestione del canale condiviso tra più abitazioni.
2. **Accesso Aziendale**: Nelle aziende i sistemi sono collegati al router di frontiera con una LAN.
3. **Accesso Domestico**: Utilizzate tecnologie Ethernet o WiFi per creare LAN domestiche.
4. **Accesso Mobile**: Infrastruttura radio mobile definita dagli ISP, può subire degrado di prestazioni a causa di distanza oppure ostacoli.
5. **Accesso Satellitare**: Accesso permesso da trasmettitori terrestri che si connettono a satelliti geostazionari (GEO) oppure satelliti a bassa quota (LEO). Questo sistema risulta essere il più duttile e non richiede complesse installazioni, ma potrebbe risultare inferiore da alcuni punti di vista come la latenza più alta.

1.4 Nucleo della Rete - Commutazione Circuito vs Pacchetto

Come determiniamo il percorso effettuato da un messaggio? Come trasferiamo dalla porta di uscita a quella di ingresso di due calcolatori? A queste domande risponde il tipo di commutazione.

Commutazione di Circuito Si instaura un cammino tra gli host in comunicazione e tutte le risorse del canale sono dedicate a loro. Questo causa un utilizzo esclusivo del canale e conseguente spreco di risorse. Per poter permettere molteplici comunicazioni utilizzando questo tipo di commutazione esistono due politiche:

1. **Frequency Division Multiplexing (FDM)**: Divido il canale in bande di frequenze e le dedico alle diverse comunicazioni.
2. **Time Division Multiplexing (TDM)**: Dedico tutto il canale alla coppia di host ma per una finestra di tempo limitata.

Commutazione di Pacchetto Il flusso dati di una comunicazione viene suddiviso in **pacchetti**, e gli viene assegnato un **header** che mantenga dei metadati riguardanti il flusso dati originale. Questo tipo di instradamento segue queste fasi:

1. **Suddivisione in pacchetti ed assegnamento header.**
2. **Instradamento** del singolo **pacchetto indipendentemente** dagli altri. Pacchetti di flussi dati diversi possono condividere i canali di comunicazione.
3. Fase di **Store and Forward**, ossia prima che il commutatore (router) consegni i pacchetti dovrà prima aspettare che siano del tutto arrivati. Il tipo di Multiplexing quindi è statistico e non prefissato. Seguendo questa politica potremmo incorrere anche in problemi di **perdita di pacchetti** in base al tipo di gestione del buffer di ciascun commutatore. Non abbiamo quindi alcuna garanzia sulle prestazioni utilizzando questa tecnica.

Confronto Caratteristiche Commutazione Circuito/Pacchetto Elenchiamo pro e contro di ciascuna tecnica:

1. **Commutazione Circuito - Pro:**
 - (a) Prestazioni garantite.
 - (b) Tecnologie di switching efficienti.
 - (c) Tariffazioni per ISP semplici da definire.
2. **Commutazione Circuito - Contro:**
 - (a) Segnalazione e configurazione delle tabelle di switching.
 - (b) Poca ottimizzazione del uso di risorse.

3. Commutazione Pacchetto - Pro:

- (a) Utilizzo ottimale delle risorse.
- (b) Non richiede fase di setup e tabelle di switching predefinite.

4. Commutazione Pacchetto - Contro:

- (a) Tecnologie di inoltro non efficienti.
- (b) Ritardi variabili.
- (c) Rischio di congestione.

1.5 Metriche - Prestazioni della Rete (Latenza, Throughput, Prod. Rate/Ritardo)

Descriviamo due metriche fondamentali delle prestazioni della rete:

1. **Latenza:** Tempo richiesto dal primo bit partito dalla sorgente fino all'arrivo a destinazione. Questa definizione è ideale, infatti dipende anche dal tipo di commutazione, quella di pacchetto con Store & Bound introduce altre difficoltà. Nello specifico le **cause specifiche di ritardo nella commutazione di pacchetto** sono:

(a) Ritardo di Elaborazione del Nodo

- i. Controllo errori sui bit.
- ii. Determinazione porta di uscita.

(b) Ritardo di Accodamento

Componente di ritardo più complessa da stabilire, si basa su una **condizione di stabilità** ossia un rapporto $\rho = \frac{L \cdot a}{R}$ dove a è velocità media di arrivo, R velocità di trasmissione ed L lunghezza media dei pacchetti in bit. La condizione $\rho < 1$ è detta **condizione di stabilità**.

- i. Attesa di trasmissione.
- ii. Dipende da intensità e tipo di traffico.

(c) Ritardo di Trasmissione L/R

Tempo impiegato dal router per trasmettere un pacchetto sul link, con $R(bit/sec)$ indichiamo il rate, ossia la velocità di trasmissione del collegamento mentre con $L(bit)$ la lunghezza del pacchetto. Il ritardo sarà quindi $d_{trasm} = \frac{L}{R}$. Quindi rappresenta il ritardo di passaggio nel commutatore.

(d) Ritardo di Propagazione

Quanto un bit ci mette per spostarsi fisicamente, rappresenta il ritardo di passaggio nel link.

Il ritardo complessivo è calcolato come somma di tutti i ritardi calcolati sopra.

2. **Throughput** Rappresenta la capacità effettiva di un link da host A verso host B , difficile da definire formalmente, ma diamo questi due riferimenti:

- (a) **Throughput Istantaneo**: Velocità in *bit/sec* a cui host B riceve in ogni istante.
- (b) **Throughput Medio**: Rapporto tra quantità L di dati trasferiti e il tempo T impiegato per il loro trasferimento, ovvero $\frac{L}{T}$.

Un potenziale bottleneck influenzerebbe pesantemente questa metrica, in caso quindi di più di un collegamento q_i il calcolo sarà $\min(q_1, \dots, q_n)$. Il Throughput quindi è differente dalla velocità di trasmissione del collegamento che si pone come upper bound alla metrica del Throughput.

3. **Prodotto Rate per Ritardo** Il prodotto rate per ritardo rappresenta il "volume" del collegamento, ossia il massimo numero di bit che possono riempire il collegamento ad un certo istante.

1.6 Modello Stratificato

Lo schema base di gestione delle reti è di tipo **stratificato**, ossia ciascun livello ha le proprie caratteristiche e responsabilità seguendo i due criteri di:

- 1. **Separation of Concern**: Divisione di interessi e responsabilità tra i livelli.
- 2. **Information Hiding**: Si espone solo l'interfaccia di ciascun livello ma non la sua implementazione.

Quindi ogni livello fornisce **servizi** al livello superiore e scambia informazioni con i livelli adiacenti tramite **interfacce**. In questo caso anche in caso di rifattorizzazione di un livello gli altri livelli sarebbero indipendenti dalle modifiche apportate a meno di modifica dell'interfaccia. Bisogna quindi definire dei protocolli che guidino la gestione di questi livelli.

Cosa è un Protocollo In protocollo si specificano **sintassi** di un messaggio, la **semantica** di un messaggio e **azioni** da intraprendere in caso di ricezione di messaggio.

1.6.1 Stack Protocollare TCP/IP

Si compone di 5 livelli (ciascun livello sarà guidato a sua volta da protocolli):

- 1. **Livello Applicazione**: Rappresenta delle applicazioni di rete, oppure collegamenti logici e scambi di messaggi end-to-end tra due processi su host diversi.
 - (a) **Protocolli**: **ftp, smtp, http**.
 - (b) **Entità Informazione del Livello**: L'informazione a questo livello è detta **messaggio**.

2. **Livello Trasporto:** Trasferimento dati end-to-end tra processi su host remoti.
 - (a) **Protocolli:** tcp, udp.
 - (b) **Entità Informazione del Livello:** L'informazione a questo livello è detta:
 - i. **Segmento** se in **Protocollo TCP**.
 - ii. **Datagramma Utente** se in **Protocollo UDP**.
3. **Livello Rete:** Trasferimento e instradamento di **datagrammi** dalla sorgente alla destinazione.
 - (a) **Protocolli:** IP o ICMP.
 - (b) **Entità Informazione del Livello:** L'informazione a questo livello è detta **datagramma**.
4. **Livello Link:** Trasferimento dati in **frame** attraverso il collegamento tra elementi di rete vicini.
 - (a) **Protocolli:** PPP o Ethernet.
 - (b) **Entità Informazione del Livello:** L'informazione a questo livello è detta **frame**.
5. **Livello Fisico:** Trasferimento dei bit di un frame sul mezzo trasmissivo.

1.6.2 Stack Protollare ISO/OSI - Cenno Storico

A differenza dello Stack TCP/IP, che era stato definito dall'IETF, l'ISO/OSI voleva essere uno standard effettivo e formale, definito invece dall'ISO. Si differenziava dall'TCP/IP perchè aggiungeva due livelli ossia Presentazione e Sessione (compresi nel livello Applicazione nel TCP/IP). Non dimostrò nessun pratico vantaggio al TCP/IP quindi viene solo usato come riferimento formale.

1.7 Breve Introduzione alla Sicurezza di Reti

Un software malevolo può penetrare in un host e può rendere questo host parte di una botnet che distribuisce richieste spam. Esistono varie tecniche:

1. **DDoS** (Distributed Denial of Service):
 - (a) **Bandwidth Flooding:** Inondazione di pacchetti
 - (b) **Connection Flooding:** Inondazione di richieste TCP
2. **Sniffing:** Man in the middle host C collegato ad un mezzo condiviso può ottenere copia di ogni pacchetto trasmesso tra due host A e B.
3. **Spoofing:** Man in the middle host C che immette pacchetti spacciandosi per un altro utente tra due host A e B.

Parametri e Criteri di Sicurezza Esistono dei metodi per difendersi da potenziali attacchi:

1. **Autenticazione:** Dimostrazione della propria identità.
2. **Crittografia:** Garantisce confidenzialità delle informazioni.
3. **Integrità ed Autenticità:** Assicurare che i dati non siano stati alterati e provengano da fonti affidabili.
4. **Controllo Accessi:** Limitare l'uso di risorse in base ai ruoli.
5. **Utilizzo di Firewall:** Filtrare il traffico tramite dispositivi hardware o software dedicato.

2 Livello Applicazione

2.1 Introduzione a Paradigmi, Protocolli e Tipi d'Utilizzo

Livello che definisce programmi applicativi che comunicano tra i vari host. Si seguono in genere due paradigmi di comunicazione tra host in questo livello:

1. **Client/Server:** Host server sempre attivo che attende richieste dei vari host client.
2. **Peer to Peer:** Tutti i client alla pari, spesso utilizzato nella condivisione di file.

Protocolli La comunicazione si basa su protocolli aperti (HTTP, SMTP) oppure proprietari. Una web app ad esempio si basa sul protocollo HTTP, invece un client di posta elettronica può utilizzare il protocollo SMTP.

Socket e API Ogni processo, essendo che comunicherà con **processi di altre macchine**, dovrà essere **identificato** dall'**IP della macchina** (da 32 bit) e dalla **porta dedicata al processo** (da 16 bit). Questo avviene grazie all'astrazione dei socket, che utilizzando IP e porta permettono ai processi di scrivere/leggere da ciascun lato.

Caratterizzazione di un Applicazione Ciascuna applicazione dovrà scegliere un protocollo da utilizzare in base alla sua caratterizzazione ed in base a specifici criteri:

1. **Throughput:** Tasso effettivo di trasferimento dati, ad esempio un client di mail non avrà bisogno di un alto Throughput.
2. **Integrità dei Dati:** Richiesta d'integrità del flusso dei dati, ad esempio una stream potrebbe non richiedere un'integrità assoluta.
3. **Sensibilità ai Ritardi:** Richiesta di una bassa latenza, ad esempio un videogioco multiplayer potrebbe richiedere una bassa latenza.

L'analisi di questi criteri in relazione all'applicazione permette la scelta del protocollo di trasporto (livello inferiore), quindi nel nostro caso se TCP (orientato allo stream) o UDP (orientato al messaggio).