

# LE RETI

## 1. Un po' di storia.

I primi computer erano *stand-alone*, questo termine indica computer non connessi con altri computer. Quando era necessario trasferire dati e/o programmi da un computer ad un altro, questo trasferimento doveva avvenire "fisicamente", caricando i dati su un supporto di memorizzazione (nastri, dischi, cartucce) da un computer, recarsi presso l'altro computer scaricare i dati su quest'ultimo.

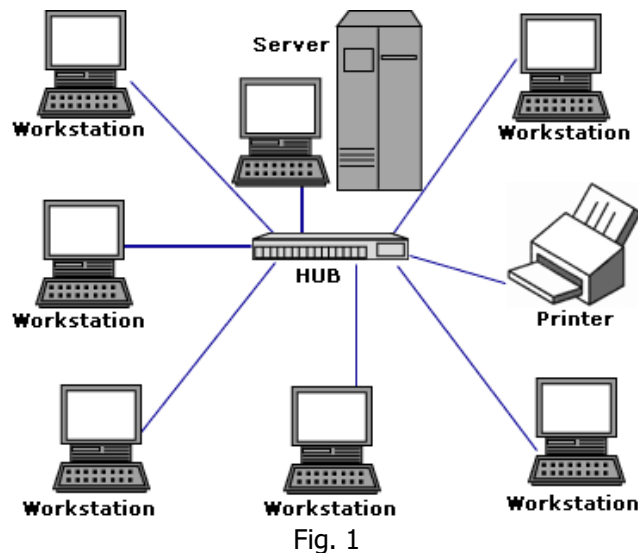
Agli inizi degli anni '60 il ministero della difesa USA commissionò uno studio a diverse università americane, per realizzare un sistema di trasferimento di dati. Questo sistema prese il nome di **ARPANET** (**A**dvan**R**esearch **P**roject **A**gency **N**ET). Il sistema era, ovviamente, segreto e solo anni più tardi si diffuse dando il via alle attuali reti di computer.

## 2. Definizione e classificazione delle reti su estensione geografica.

*Una rete è una connessione tra due e più dispositivi informatici per scambiare dati e risorse (hardware e software).*

La prima classificazione delle reti la facciamo su base geografica ossia in base alla grandezza della rete. Le reti vengono classificate in LAN, MAN, WAN e GAN.

**LAN** (Local Area Network) è una rete che ha un'estensione di al più qualche chilometro, privata, non può attraversare spazi pubblici.



**MAN** (Metropolitan Area Network) è una rete 'metropolitana' che si estende nell'ambito di un comprensorio (come ad esempio un comune).

**WAN** (Wide Area Network) è una rete molto estesa come, ad esempio un intero continente.

**GAN** (Global Area Network) la rete collega tutti i computer dislocati in tutto il mondo (internet).



Fig. 2

### 3. Come funziona la rete.

#### 3.1 I mezzi trasmissivi.

Innanzitutto cominciamo con il dire che affinché due o più computer possano comunicare tra di loro, devono essere in qualche modo collegati. Questo collegamento avviene tramite i cosiddetti *mezzi trasmissivi*.

I mezzi trasmissivi si dividono in tre gruppi principali:

- **mezzi elettrici**, cavi che sfruttano la conducibilità elettrica dei metalli per trasmettere le informazioni sotto forma di impulso elettrico;
- **onde radio** (wireless) sfruttano le onde elettromagnetiche per trasferire le informazioni;
- **mezzi ottici**, le informazioni vengono trasmesse tramite la luce.

I principali *mezzi elettrici* sono il *cavo coassiale* ed il *doppino telefonico* (twisted pair).

Il cavo coassiale ha al suo centro un singolo conduttore di rame. Uno strato di plastica (dielettrico) garantisce l'isolamento tra il centro del conduttore ed uno schermo di metallo intrecciato (in aggiunta, possiamo trovare uno schermo laminato). Lo schermo di metallo aiuta a bloccare qualsiasi interferenza esterna.



Fig. 3

Il tutto ricoperto da una guaina esterna.

Il doppino telefonico è in cavo che troviamo nella rete telefonica.

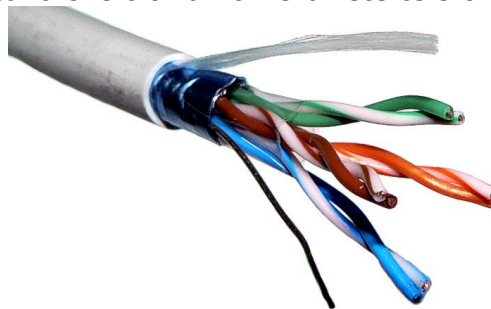


Fig. 4

È costituito da coppie di fili in rame intrecciati. I fili vengono intrecciati per diminuire le interferenze ed in base alle schermature che possono essere presenti o meno su ogni coppia intrecciata, i doppini vengono classificati in **STP** (shielded twisted pair) in cui ogni coppia di fili è schermata (come in fig. 4), **FTP** (Foiled twisted pair) in cui c'è solo una schermatura che ricopre tutte le coppie di fili e **UTP** (Unshielded Twisted Pair) privo di schermatura. Ovviamente i cavi migliori (e più costosi) sono gli STP, quindi gli FTP in ultimo gli UTP.

Le *onde radio* fanno uso, per trasportare le informazioni, delle onde elettromagnetiche. La televisione, radio, i cellulari ad esempio utilizzano le onde elettromagnetiche per ricevere/trasmettere le informazioni. Le onde elettromagnetiche sono composte dal campo elettromagnetico generato dalle cariche elettriche e dal loro movimento (corrente elettrica). L'oscillazione delle cariche elettriche in un conduttore (un'antenna, un filo di rame) produce due campi: elettrico e magnetico che si propagano sotto forma di onda elettromagnetica nello spazio (anche nel vuoto). Le onde elettromagnetiche, generate da una sorgente, vengono intercettate da un dispositivo, ricevitore, che le codifica in segnali elettrici.



Fig. 5

I *mezzi ottici* utilizzano la luce per trasmettere le informazioni. Anche la propagazione della luce può avvenire tramite cavo o wireless. I cavi per trasmettere la luce è la fibra ottica. Il cavo in fibra ottica per trasportare i dati utilizza segnali luminosi trasmessi sopra una sottile fibra in vetro. Il cavo in fibra ottica consiste infatti di una parte centrale in vetro (core) nella quale viaggia la luce, siccome la luce può rimbalzare all'interno del core, questo è rivestito da una sorta di materiale simile ad uno specchio (cladding) che consente alla luce di essere riflessa. Il core ed il cladding sono circondati da parecchi strati di materiali protettivi. Questo cavo trasmette luce anziché segnali elettrici, eliminando così il problema dell'interferenza elettrica; questo lo rende il mezzo trasmissivo ideale in ambienti che hanno un'elevata interferenza elettrica. Il cavo in fibra ottica ha la capacità di trasmettere segnali su distanze maggiori rispetto al cavo coassiale e al twisted pair, ed inoltre consente di trasferire l'informazione a velocità più elevate.

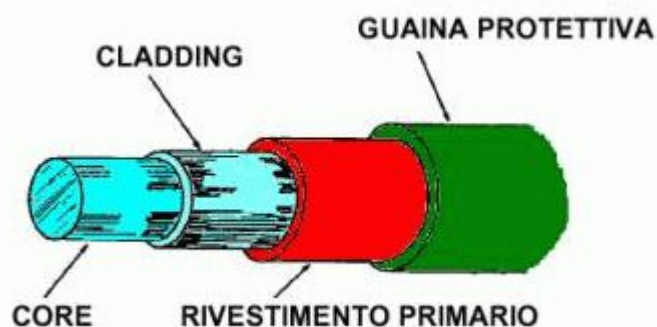


Fig. 6

I wireless ottici sono principalmente di due tipi: infrarossi, luce visibile, laser, raggi ultravioletti.

### **3.2 I Protocolli.**

Una volta che i computer ed i dispositivi informatici sono collegati tramite i mezzi trasmissivi, possono scambiare delle informazioni.

Il problema è che per "capirsi", i computer devono avere, un insieme di regole in modo che il flusso di informazioni che vengono inviate da una "sorgente" (ossia il dispositivo da cui partono le informazioni) siano comprese dalla "destinazione" (il dispositivo cui arrivano le informazioni).

Questo insieme di regole che servono per poter espletare i *servizi di rete* (indichiamo con questo termine il tipo di trasmissione di dati - posta elettronica, flussi di dati, pagine web, ecc.) si chiamano **protocolli**.

I protocolli sono suddivisi in strati chiamati *livelli*. Un messaggio (ossia l'informazione che deve essere inviata dalla sorgente e ricevuta da un destinatario) deve essere trasformato da qualcosa che è comprensibile ad un utente a qualcosa che possa viaggiare sul mezzo trasmissivo. Quando questo messaggio, così trasformato, arriva a destinazione deve subire il procedimento inverso, ossia da segnale che viaggia sul mezzo trasmissivo in qualcosa di comprensibile dall'utente destinatario. Questa trasformazione avviene facendo elaborare il messaggio dai vari livelli che compongono il protocollo.

Il protocollo usato nelle reti è attualmente il protocollo TCP/IP (**T**ransfer **C**ontrol **P**rotocol/**I**nternet **P**rotocol). Il protocollo TCP/IP è composto di quattro livelli: Application, Transport, Internet, Network Physical:

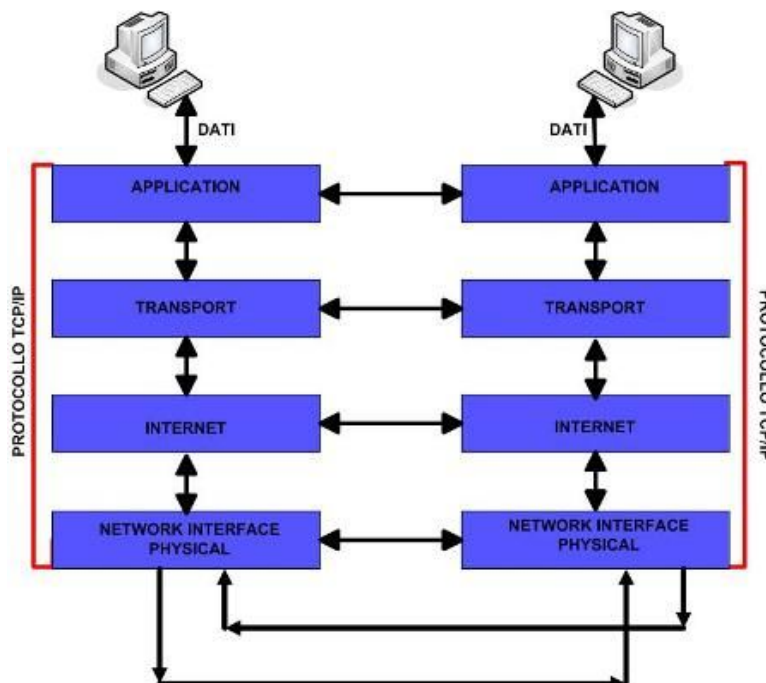


FIGURA 11

**Livello Network e Physical:** (physical) descrive l'interfaccia fisica fra il nodo della rete ed il mezzo trasmissivo e definisce le caratteristiche del mezzo stesso, i livelli del segnale, i tassi di trasmissione, lo schema di codifica dei dati e altri dettagli relativi alla trasmissione

e (network) descrive lo scambio di dati tra un nodo e la rete e definisce le modalità di individuazione del destinatario e il tipo di servizio.

**Livello internet:** descrive la trasmissione dati tra due nodi della rete (commutazione di pacchetto o trasmissione non affidabile) e definisce il formato dei pacchetti, il sistema di indirizzamento globale, il meccanismo di instradamento dei pacchetti. In questo livello viene utilizzato il protocollo IP, che fornisce un servizio di comunicazione non affidabile, cioè non garantisce la consegna dei pacchetti.

**Livello di trasporto:** descrive la comunicazione tra due nodi della rete e garantisce il corretto ordinamento/creazione dei pacchetti e la consegna affidabile dei dati. In questo livello viene utilizzato il protocollo TCP (o [UDP](#)), garantendo una comunicazione affidabile (trasmissione orientata alla connessione).

-**TCP:** Tcp fornisce un livello di trasporto affidabile e orientato alla connessione. Per affidabile s'intende che prima di inviare i dati il server esegue l'handshaking, cioè chiede al client se è pronto a riceverli. Per orientato alla connessione s'intende la numerazione dei pacchetti in modo che il client li riceva in modo ordinato. Viene utilizzato per la sua sicurezza.

-**UDP:** Udp fornisce un servizio di trasporto datagram-oriented (non affidabile) e non orientato alla connessione. I pacchetti quindi vengono inviati senza chiedere al client se è pronto e inviandoli in modo disordinato. Viene utilizzato per la sua velocità.

**Livello delle applicazioni:** è il più vicino all'utente e descrive la comunicazione tra processi su host differenti e le relative interfacce utente, fornisce vari servizi di rete, come login remoto, trasferimento file, posta elettronica e web.

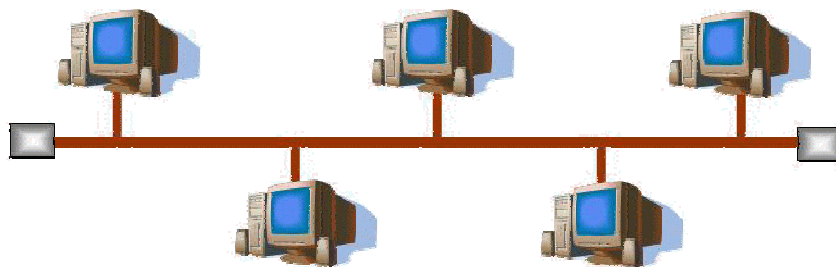
### 3.3 La Topologia.

Abbiamo classificato le reti in base alla loro estensione geografica. Ora le classificheremo in base alla disposizione fisica dei dispositivi del loro collegamento.

Abbiamo le seguenti *topologie*: topologia a **bus**, a **stella**, ad **anello**, ad **albero**, a **maglia**.

#### **Topologia a bus.**

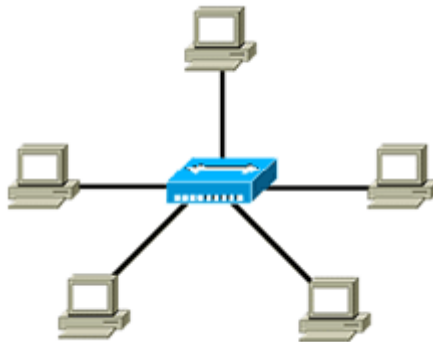
Una **topologia a bus** è l'organizzazione di rete più semplice. In effetti, in una topologia in bus tutti i computer sono collegati ad una stessa linea di trasmissione tramite un cavo, generalmente coassiale, alla fine del cavo sono inseriti dei terminatori che "assorbono" i messaggi presenti sulla linea che, altrimenti rimbalzerebbero, provocando disturbi. La parola «bus» designa la linea fisica che collega i terminali di rete:



Questa topologia ha il vantaggio della facile realizzazione e di avere un funzionamento semplice. Tuttavia, è estremamente vulnerabile dato che se una delle connessioni è difettosa, l'insieme della rete è compromesso.

**Topologia ad stella.**

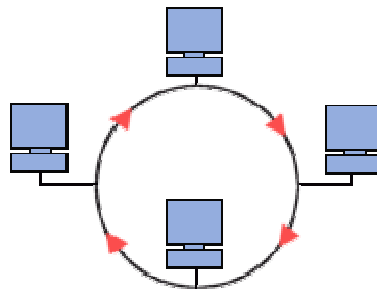
In una topologia a stella, i computer della rete sono collegati ad un dispositivo hardware centrale (es. Hub). Questi dispositivi hanno un certo numero di collegamenti nei quali è possibile inserire i cavi di rete dei computer ed hanno come ruolo quello di assicurare la comunicazione tra i diversi collegamenti:



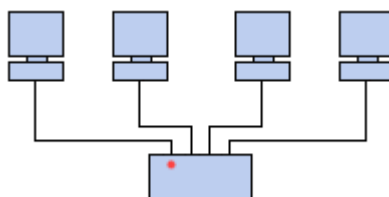
Contrariamente alle reti costruite su una topologia in bus, le reti con una topologia a stella sono molto meno vulnerabili dato che una delle connessioni può essere scollegata senza paralizzare il resto della rete.

**Topologia ad anello.**

In una rete con una topologia ad anello, i computer sono posti su un cerchio e comunicano ciascuno al loro turno:



In realtà, in una topologia ad anello, i computer non sono collegati in cerchio, ma ad un MAU (per Multistation Access Unit) che gestisce la comunicazione tra i computer a lui collegati impartendo ad ognuno di essi un intervallo di tempo di parola:





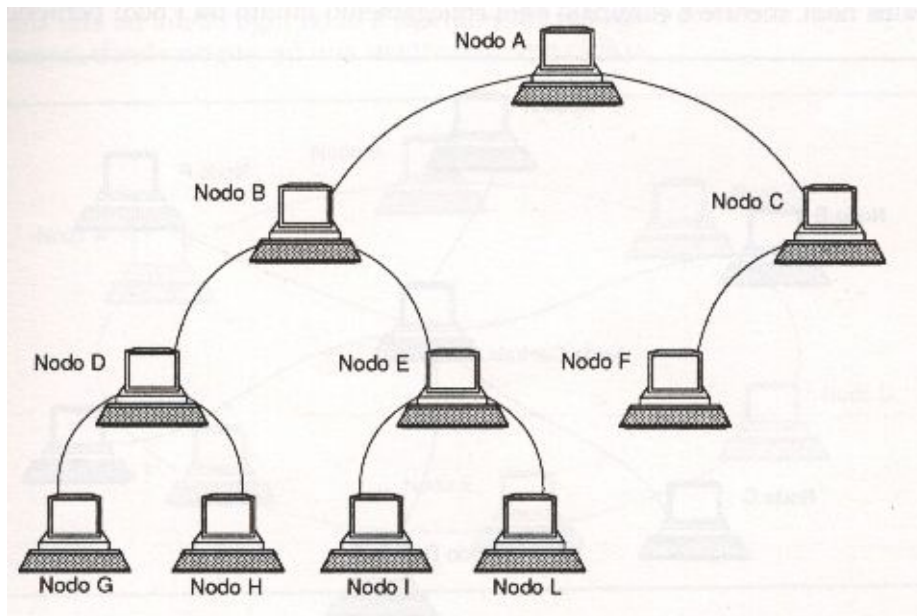
Le due principali topologie logiche che usano questa topologia fisica sono Token Ring e FDDI.

Il token (gettone) viene trasferito da un computer al successivo finché non raggiunge quello su cui sono disponibili dati da trasmettere. Il token viene modificato dal computer trasmittente che aggiunge al dato l'indirizzo del destinatario e quello del mittente e lo rinvia lungo l'anello.

I dati passano attraverso ciascun computer finché raggiungono quello il cui indirizzo corrisponde a quello indicato sui dati. Questo computer restituisce un messaggio di conferma al computer trasmittente il quale crea un nuovo token e lo immette nella rete. FDDI (Fiber Distributed Data Interface) è una rete Token ring in cui il mezzo trasmissivo è la fibra ottica.

### Topologia ad albero

Questo tipo di collegamento è di natura gerarchica. Ogni nodo (dispositivo) può rivolgersi ad un nodo superiore per connettersi agli altri. Qualora il collegamento desiderato non sia raggiungibile attraverso di esso, si ricorrerà al nodo ancora superiore e così via.



Se un nodo non è raggiungibile nemmeno attraverso la radice, si trova fuori dalla rete. È una tecnica indicata per le reti geograficamente estese, e per collegare più reti fra loro. Non però offre cammini alternativi in caso di interruzione di una linea o di guasto di un nodo.

### Topologia a maglia.

Una rete a maglia è un particolare in cui i nodi sono collegati tra loro più di una volta, così da creare canali di comunicazioni alternativi in caso che la rete sia congestionata, che la linea non funzioni bene o che uno dei nodi abbia malfunzionamenti.

Una rete a maglia può essere definita completa (fig. 7) se tutti i nodi sono connessi tramite percorsi alternativi in maniera diretta a tutti gli altri o parziale (fig. 8) se vengono implementati soltanto alcuni percorsi alternativi tra i nodi.



Ed è proprio la rete a maglia parziale ad essere particolarmente utilizzata in scenari reali, poiché il costo è relativamente contenuto rispetto a quanto impiegherebbe realizzare in toto una maglia totale – si sceglie, per la realizzazione, un buon compromesso tra i collegamenti richiesti ed il costo per implementarli.

Le reti a maglia, seppur costose, riducono sensibilmente il pericolo di malfunzionamento generale rispetto alle reti ad anello e alle reti a bus.

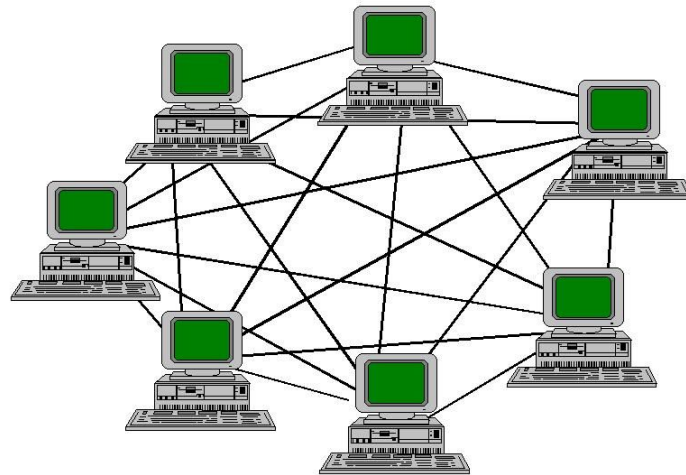


Fig. 7 - Maglia completa

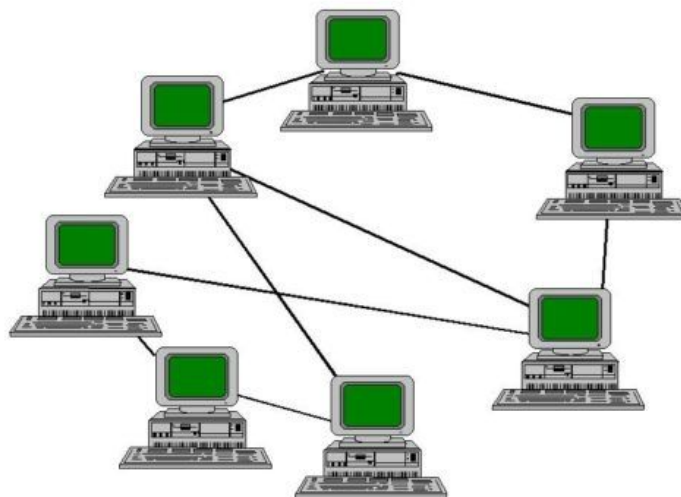


Fig. 8 - Maglia parziale.



Ci sono reti che sono un "miscuglio" delle topologie indicate. Queste reti prendono il nome di topologia mista.

Ogni dispositivo della rete viene definito **punto di connessione**.

### **3.4 I segnali ed i codici.**

Sul mezzo trasmissivo, per la trasmissione delle informazioni, viaggiano i *segnali*. I segnali si suddividono in segnali elettrici, ossia quelli che attraversano i mezzi trasmissivi elettrici, i segnali ottici, quelli che attraversano mezzi ottici. I segnali si distinguono, inoltre, in segnali analogici e segnali numerici o digitali. I segnali analogici sono i segnali che assumono con continuità i valori compresi in un determinato intervallo. I segnali che assumono valori discreti (ad esempio (0,1)) si dicono numerici o digitali.

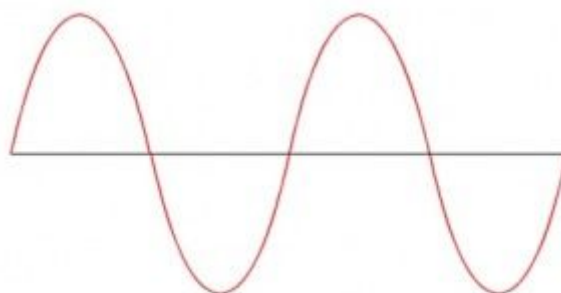


Fig. 9 - segnale analogico

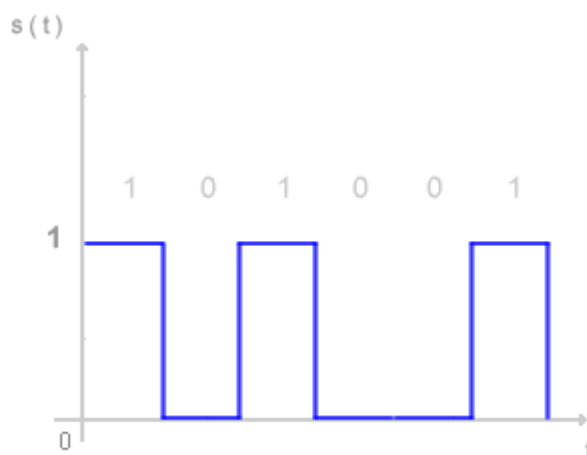


Fig. 10 - segnale numerico o digitale

I segnali durante il viaggio dal mittente al destinatario, possono essere trasformati da analogici a digitali e viceversa. Per effettuare tali conversioni si utilizzano due circuiti: l'**ADC** - converte i segnali da analogico a digitale e il **DAC** che converte i segnali da digitali ad analogici. I dispositivi che effettuano le due conversioni, si chiamano **modem** (modulatori-demodulatori). Questi dispositivi, convertono i segnali elettrici che viaggiano su rete telefonica di tipo analogico in segnali digitali (quando entrano nel computer collegato alla rete) e viceversa.

I messaggi che transitano sulla rete sono quindi formati da un insieme di segnali che viaggiano sui mezzi trasmissivi. Le reti possono essere:

- a **commutazione di pacchetto**: il messaggio viene diviso in pacchetti, ognuno contenente l'indirizzo del mittente e del destinatario ed altre informazioni per l'assemblaggio del messaggio una volta che tutti i pacchetti sono arrivati a destinazione. Ogni pacchetto, nel percorso dal mittente ad destinatario, può seguire una strada, sulla rete, diversa.

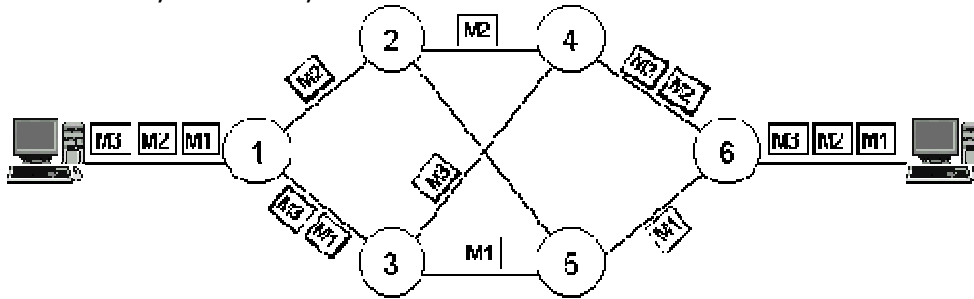


fig. 11

- a **commutazione di circuito**: prima di effettuare una trasmissione si deve stabilire a priori il percorso fisico tra sorgente e destinatario; questo tipo di trasmissione è utilizzata nella trasmissione telefonica tradizionale.

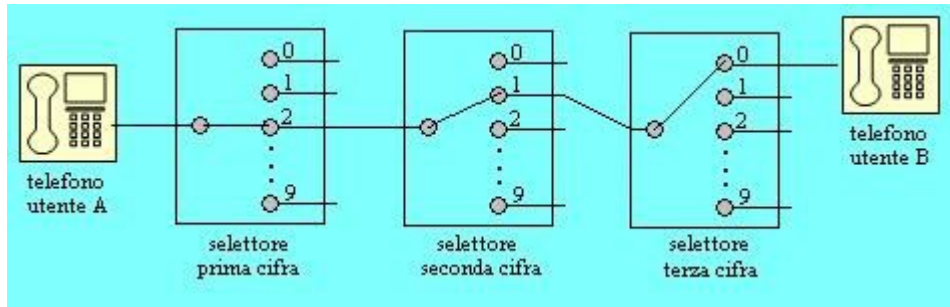


fig. 12

I mezzi trasmissivi vengono definiti anche con il termine *canali trasmissivi*; la caratteristica principale del canale è la **capacità** definita come la *quantità di informazione che può essere trasmessa dal quel canale nell'unità di tempo*. Il canale può essere affetto da disturbi, chiamati rumore, che fanno sì che il ricevente riceva un segnale diverso da quello trasmesso, pertanto il mezzo trasmissivo (canale) scelto deve rendere minima l'alterazione del messaggio trasmesso, tramite alcune tecniche (tecniche di ridondanza). L'entità dei danni subiti a causa dei disturbi viene misurata tramite il rapporto segnale-rumore (S/R) che rappresenta un indice di qualità del collegamento.

In definitiva nella trasmissioni delle informazioni abbiamo la **catena di Shannon**:

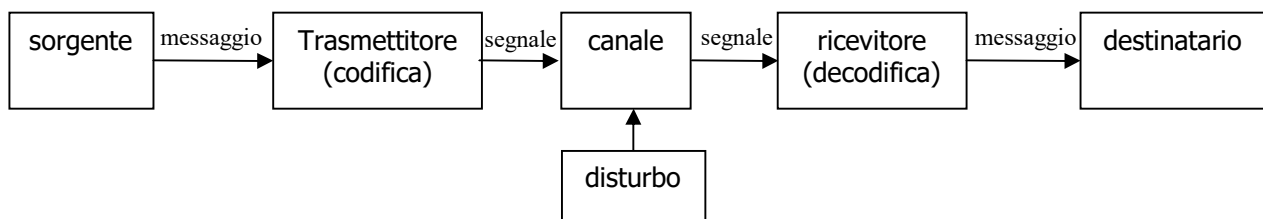


Fig.13

È ovvio che affinché la sorgente e la destinazione si "capiscano" quando si inviano messaggi, devono usare lo stesso **codice** (due dispositivi che vogliono scambiare delle informazioni devono usare gli stessi simboli la cui codifica rappresenta lo stesso carattere; ad esempio una sequenza di 1 e 0 disposti in un certo modo e di una certa determinata lunghezza rappresentano un carattere dell'alfabeto latino come la codifica ASCII). Durante la trasmissione di un messaggio, i vari dispositivi della rete possono utilizzare diverse codifiche:

**codifica di sorgente:** la codifica utilizzata per codificare il messaggio emesso dalla sorgente;

**codifica di canale:** sul canale, come detto, i segnali possono subire dei disturbi, per limitare i danni di questi rumori si utilizzano codici particolari, detti ridondanti, che possono:

- far capire al destinatario che il messaggio è arrivato errato,
- che consentono la correzione automatica del messaggio che ha subito errori durante la trasmissione sul canale;

**codifica di linea:** il processo di trasformazione del messaggio in segnali che transitano sul mezzo trasmissivo (canale).

Per tutte e tre le codifiche si dovrà prevedere un *decodificatore*.

In definitiva, per costruire un messaggio da immettere sulla rete sono necessari un **alfabeto** (esempio l'alfabeto latino o i 10 numeri interi) i cui caratteri in sequenza rappresentano una **parola**; i caratteri che compongono la parola vengono, quindi, codificati con un **codice**.

### **3.5 Codifica di canale ed errori.**

Quando due persone parlano, le onde sonore si propagano nell'aria e se siamo in un ambiente in cui ci sono dei rumori, ad esempio un martello pneumatico a lavoro, la comunicazione tra le due persone risulta difficile ad alcune volte, in parte, incomprensibile. La stessa cosa può accadere ad un segnale che attraversa un mezzo trasmissivo, già la propagazione del segnale stesso nel mezzo può, da solo, generare un disturbo. Quindi nella trasmissione il segnale è accompagnato da un altro segnale del tutto causale che prende il nome di **rumore** o **noise**.

I disturbi si dividono in:

**rumore bianco:** è il rumore che si genera dal mezzo trasmissivo stesso e dai circuiti elettrici, generato dall'attraversamento, ad esempio, degli elettroni nel conduttore, difficilissimo da eliminare;

**disturbo impulsivo:** è il disturbo che proviene dall'esterno del mezzo trasmissivo ma che lo influenza, come ad esempio la scarica elettrica generata da un fulmine che influenza le onde radio, o un campo magnetico che può influenzare una trasmissione su un cavo non adeguatamente schermato.

Il problema principale quando si genera un disturbo in una trasmissione, è che il destinatario si accorga che il messaggio originario è arrivato errato e se possibile correggere l'errore o chiedere alla sorgente di ripetere la trasmissione. Per ottenere ciò i codici di canale sono **ridondanti**.

Vediamo di capire cosa significa ridondanza.

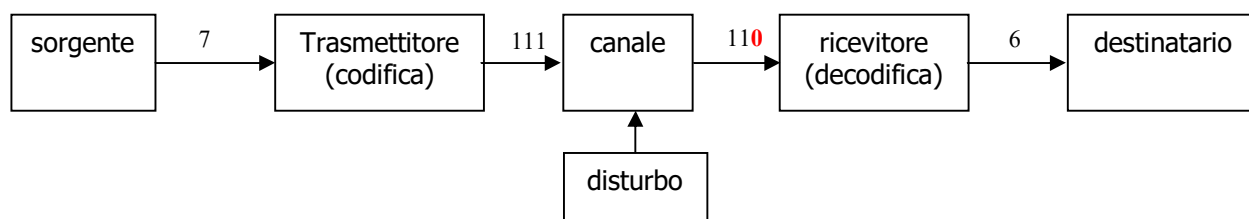
Sappiamo che per codificare un alfabeto di S caratteri in binario, abbiamo bisogno di n cifre binarie in modo tale che  $2^n = S$ .

Ad esempio per codificare un carattere ottale (un numero da 0 a 7) abbiamo bisogno di 3 cifre binarie.

ottale	binario
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

La codifica binaria di sopra utilizza il minimo numero di cifre binarie necessarie per rappresentare le otto cifre del sistema ottale.

Supponiamo che la sorgente voglia inviare il numero 7 ad un destinatario ma sul canale si verifichi un errore dovuto ad un disturbo impulsivo che modifica uno o più bit della codifica binaria del numero:



Il destinatario riceve una cifra (errata) dell'alfabeto ottale e non può accorgersi che la trasmissione è stata inficiata da un errore.

Utilizzando quindi una codifica con il numero di bit esattamente necessari per rappresentare un alfabeto e si verifica un errore durante la trasmissione, il destinatario non riesce ad accorgersi che si è verificato un errore. Per evitare questa situazione si utilizza una codifica con un maggiore numero di cifre. Questi codici si dicono ridondanti e sono formati da un certo numero ( $n$ ) di cifre per rappresentare il dato, **bit di dato**, e da un numero ( $k$ ) di bit (ridondanti) per controllare se si è verificato un errore, **bit di controllo**.

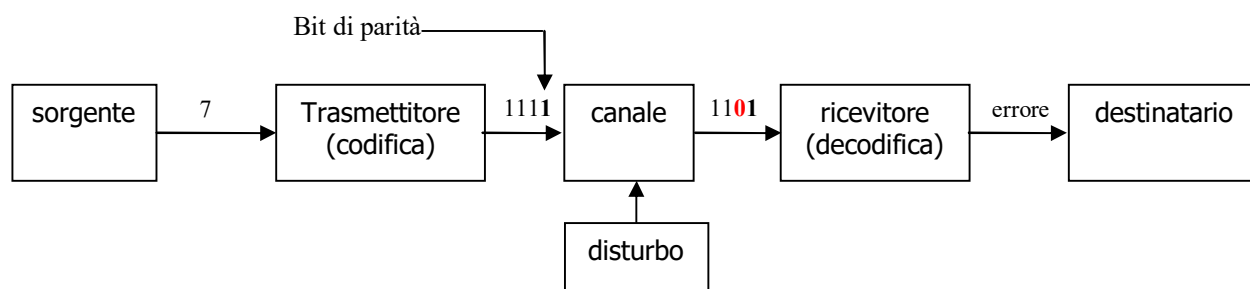
### 3.6 Codici a rilevazione e correzione di errore.

#### Controllo di parità.

Questo codice permette di individuare se solo su un bit del messaggio si verifica un errore. Il codice in questione ha un solo *bit di controllo* ( $k=1$ ) chiamato **bit di parità** e vale 1 se il numero di uno dei *bit di dato* sono dispari, 0 altrimenti. Ad esempio se volessimo codificare i numeri ottali, la codifica a *controllo di parità* sarebbe formata da 4 bit: 3 bit di dato ed un bit di controllo:

ottale	Controllo parità	
	Bit dato	Bit parità
0	000	0
1	001	1
2	010	1
3	011	0
4	100	1
5	101	0
6	110	0
7	111	1

Il destinatario controllando il bit di parità può accorgersi se durante la trasmissione si è verificato un errore su un bit e, quindi, richiedere, ad esempio, la ritrasmissione del messaggio alla sorgente:



Come si può notare, la sequenza (errata) 1101 non è presente nella tabella di codifica sopra indicata, quindi la fase di decodifica si accorge dell'errore.

### Controllo a ridondanza ciclica

Il **CRC (Cyclic Redundancy Check, controllo a ridondanza ciclica)** è un metodo a controllo polinomiale in cui i bit che formano un messaggio vengono visti come i coefficienti di un polinomio  $T(x)$  di grado  $n-1$  in  $x$ , dove  $n$  è il numero di bit del messaggio. Ad esempio se il messaggio da trasmettere è **10011101** il polinomio  $T(x)$  associato è:

$$T(x) = 1 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 = x^7 + x^4 + x^3 + x^2 + 1$$

Questo polinomio viene diviso per un altro polinomio,  $G(x)$ , detto **polinomio generatore**, di grado minore rispetto al polinomio  $T(x)$  e con il termine noto uguale ad 1.

La divisione tra  $T(x)$  e  $G(x)$  produce un polinomio resto  $R(x)$ .

Ora sia la sorgente che la destinazione posseggono il polinomio generatore  $G(x)$ . La sorgente trasforma il messaggio, prima d'inviarlo, in modo tale che sia divisibile per  $G(x)$ :

1. aggiunge al messaggio originale tanti 0 quanto è il grado di  $G(x)$  chiamiamo  $T'(x)$  questo messaggio
2. divide  $T'(x)$  per  $G(x)$  ottenendo il resto  $R(x)$
3. sottrae  $R(x)$  a  $T'(x)$ : sia  $T''(x)$  il polinomio risultante dalla divisione, tale polinomio è divisibile per  $G(x)$ .

$T''(x)$  in realtà è uguale a  $T(x)$  con l'aggiunta, alla fine, di alcuni bit detti crc che rendono il polinomio divisibile per  $G(x)$ .

La sorgente invia, quindi,  $T''(x)$  quando il destinatario  $T''(x)$ , lo divide per  $G(x)$ . Se il resto della divisione è 0 il messaggio è arrivato in modo corretto altrimenti si è verificato un errore durante la trasmissione.

### **Controllo trasversale e longitudinale.**

Questo codice è simile al bit di parità solo che si applica su insiemi di 8 byte (ogni byte sappiamo che è formato da 8 bit) di caratteri, che disposti l'uno sotto l'altro formano una matrice 8x8, in cui si controlla sia in orizzontale che in verticale in numero di 1 presenti.

Supponiamo ad esempio che sono stati inviati i caratteri C1, C2, C3 e C4 (per semplicità ogni carattere è di 4 bit ossia un semi byte) che formano la matrice sottostante:

	CONTROLLO LONGITUDINALE				
C1	1	0	1	0	<b>0</b>
C2	1	1	1	0	<b>1</b>
C3	1	1	0	0	<b>0</b>
C4	1	0	0	0	<b>1</b>
<b>CONTROLLO TRASVERSALE</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Se durante la trasmissione di questi quattro caratteri si verifica *un* errore il codice ci permette anche di individuare dove si è verificato:

	CONTROLLO LONGITUDINALE				
C1	1	0	1	0	<b>0</b>
C2	1	1	0	0	<b>0</b>
C3	1	1	0	0	<b>0</b>
C4	1	0	0	0	<b>1</b>
<b>CONTROLLO TRASVERSALE</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	

L'incrocio tra i bit di controllo diversi (segnati in rosso) rispetto a quelli inviati, ci dicono dove si è verificato l'errore ed effettuare l'opportuna correzione.

### **Distanza di Hamming e rilevazione degli errori .**

Diamo alcune definizioni:

**Peso:** il numero di uno presenti in una parola, ove per parola indichiamo un byte es. 10011100 ha peso 4.

- ✓ **Distanza tra due parole:** è il numero di posizioni in cui due parole hanno valori diversi nei corrispondenti bit es.  $P1 = 10010001$  e  $P2 = 10000101$  ha distanza 2, infatti i bit indicati in rosso in  $P1$  e  $P2$  hanno valori differenti.
- ✓ **Molteplicità dell'errore:** è la distanza tra la parola trasmessa e quella ricevuta. Ad esempio se  $P1$  è il messaggio inviato e  $P2$  quello ricevuto, la molteplicità dell'errore è 2.



- ✓ **Distanza minima di Hamming (h)**: se M è un messaggio con N parole, h è la distanza minima tra due qualsiasi parole del messaggio se h è uguale ad 1 il codice è efficiente se h è maggiore di 1 è ridondante.

Codici in cui  $h > 1$  permettono di rilevare la presenza di errori.

### Codice di Hamming.

Il codice di Hamming è un codice a correzione di errore e si ottiene inserendo dei bit di parità in posizioni specifiche all'interno del messaggio che si vuole trasmettere.

Per determinare quanti bit di controllo (R) si devono usare, deve essere verificata la seguente relazione:

$2^R \geq M + R + 1$  ove M è la lunghezza del messaggio ed R sono i bit ridondanti.

Ad esempio se abbiamo un messaggio con 4 bit da trasmettere si deve trovare il più piccolo R in modo che sia soddisfatta la disuguaglianza di sopra:

$2^R \geq 4 + R + 1$  è facile verificare R = 3 soddisfa la disuguaglianza.

Vediamo adesso dove devono essere posti questi bit di controllo all'interno del messaggio da trasmettere.

Questi bit devono essere posti nelle posizioni delle potenze di due che vanno da  $2^0, 2^1, \dots, 2^{R-1}$ .

Nel nostro esempio siccome R = 3, le posizioni ove porre i bit di controllo sono in

$2^0 = 1$  posizione,  $2^1 = 2$  posizione,  $2^2 = 4$  posizione.

Ad esempio se il messaggio è formato dai bit dati  $D_1 D_2 D_3 D_4$  e se indichiamo con  $P_0, P_1, P_2$  i bit di parità, il messaggio da trasmettere assumerà la forma:

messaggio	$P_0$	$P_1$	$D_1$	$P_2$	$D_2$	$D_3$	$D_4$
posizione	1	2	3	4	5	6	7

I bit del messaggio originale ( $D_1 D_2 D_3 D_4$ ) vengono posti nelle posizioni "libere" 3, 5, 6, 7.

Vediamo ora come assegnare un valore 0 o 1 ai bit di parità supponiamo che il messaggio che vogliamo trasmettere sia  $D_1 D_2 D_3 D_4 = 0101$

messaggio	$P_0$	$P_1$	0	$P_2$	1	0	1
posizione	1	2	3	4	5	6	7

Consideriamo le posizioni dove sono presenti degli 1. Le posizioni in cui sono presenti degli uno sono la posizione 7 e la posizione 5. trasformiamo in binario le posizioni coinvolte:  $7_{10} = 111_2$  e  $5_{10} = 101_2$

Facciamo XOR tra i due numeri (se fossero state coinvolte più posizioni si faceva XOR a due a due, prima tra le prime due posizioni il risultato con la terza e così via). Otteniamo:  $111 \text{ xor } 101 = 010$ . Assegniamo, dalla posizione meno significativa, i bit del risultato dell'xor ai bit di parità:  $P_0 = 0, P_1 = 1, P_2 = 0$ . Il messaggio diventa, in definitiva:

messaggio	0	1	0	0	1	0	1
posizione	1	2	3	4	5	6	7

Una volta trasmesso, il destinatario fa la medesima operazione. Gli 1 ora si trovano in posizione 2, 5 e 7; analogamente 2 = 010, 5 = 101 e 7 = 111. Facciamo gli xor:  $010 \text{ xor } 101 = 111 \Rightarrow 111 \text{ xor } 111 = 000$ . Siccome il risultato è 0 significa che la trasmissione è avvenuta correttamente. Supponiamo che il destinatario riceva invece un messaggio con errori:

messaggio	0	1	0	0	<b>0</b>	0	1
posizione	<b>1</b>	<b>2</b>	3	<b>4</b>	5	6	7

(in posizione 5 si è verificato un errore).

Gli 1, ora, sono in posizione 2 ed in posizione 7:  $010 \text{ xor } 111 = 101$ .  
Ma  $101 = 5$  ossia la posizione del bit errato che viene corretto.