



# **Dispense per il Corso di Reti di Telecomunicazioni**

**Ing. Giovanni Giambene**

# Indice

Capitolo 1: Introduzione alle reti di telecomunicazione .....	1
1.1 Caratteristiche generali dei segnali e dei sistemi di telecomunicazione .....	1
1.2. Tecniche di commutazione .....	4
1.3 Multiplex .....	12
Capitolo 2: Tecniche di accesso multiplo .....	16
2.1 Le risorse .....	16
2.2 Frequency Division Multiple Access (FDMA).....	16
2.3 Time Division Multiple Access (TDMA).....	17
2.4 Code Division Multiple Access (CDMA).....	17
2.5 Confronto fra le tecniche di accesso multiplo.....	24
Capitolo 3: Il modello OSI .....	26
3.1. Introduzione .....	26
3.2 Descrizione generale del modello OSI .....	27
3.3. Servizi senza connessione o con connessione.....	31
3.4 Livelli OSI .....	32
Capitolo 4: I Protocolli IP e TCP.....	48
4.1. Introduzione.....	48
4.2. Confronto tra il modello OSI e il modello TPC/IP .....	49
4.3. Il protocollo IP.....	50
4.4 Protocolli EGP .....	61
4.5 Protocolli IGP .....	62
4.6 I protocolli ARP e RARP.....	63
4.7 Protocollo IPv6 .....	67
4.8 Protocolli TCP e UDP .....	71
Capitolo 5: Le Reti locali.....	79
5.1. Introduzione.....	79
5.2. Struttura trasmissiva di una rete locale .....	81
5.3 Mezzi trasmissivi .....	85
5.4 La rete Ethernet.....	93
5.5 Caratteristiche dei diversi tipi di cablaggio.....	100
5.6 Configurazione di una LAN Ethernet in un singolo dominio di collisione.....	105
5.7 Calcolo della massima distanza tra due stazioni Ethernet.....	105
5.8 Fast Ethernet.....	108
5.9 Gigabit Ethernet.....	112
5.10 Token Ring .....	113
Capitolo 6: Teoria delle code ad applicazione alle reti di telecomunicazione .....	125
6.1 Elementi di ritardo in una rete di telecomunicazione.....	125
6.2 Teorema di Little .....	130
6.3 Nomenclatura per i sistemi a coda: la notazione di Kendall .....	134
6.4 Catene di Markov .....	136
6.5 Sistemi M/G/1.....	142
6.6 Sistemi a coda con priorità.....	145
6.7 Esercizi risolti sulla teoria delle code .....	147
6.8 Teoria del traffico .....	152
Riferimenti bibliografici .....	156

# Capitolo 1: Introduzione alle reti di telecomunicazione

## 1.1 Caratteristiche generali dei segnali e dei sistemi di telecomunicazione

I segnali che sono incontrati nelle applicazioni pratiche presentano spesso caratteristiche diverse tra loro, come è stato in parte già sottolineato nei precedenti capitoli. Per questo motivo la scelta e la realizzazione di un sistema di comunicazione deve sempre essere effettuata tenendo presenti le principali caratteristiche e requisiti dei segnali da trasmettere. Per alcuni segnali, come ad esempio il segnale telefonico o il segnale video, non sono accettabili ritardi troppo elevati e quindi il sistema di comunicazione deve garantire che il segnale sia ricevuto entro un massimo intervallo di tempo prefissato. Per altri segnali, quali ad esempio il traffico dati su Internet, il requisito essenziale è la correttezza dell'informazione ricevuta, mentre non esistono vincoli stringenti sul massimo ritardo.

Differenti tipi di traffico pongono requisiti diversi alla rete di comunicazione; per questo, una rete ottima per una certa classe di traffico può non risultare efficiente per altre classi di traffico.

La rete telefonica è stata ottimizzata per il traffico telefonico, ma è poco adatta per la trasmissione dei dati. Una rete o un sistema di comunicazione utilizzato in modo inefficiente non solo offre prestazioni non soddisfacenti, ma può comportare anche un costo maggiore per l'utente.

Una caratteristica fondamentale per ciascun segnale numerico è il numero di bit per secondo richiesti per rappresentarlo. Ad esempio, per trasmettere un segnale telefonico in forma numerica utilizzando un sistema PCM è necessaria una velocità di 64 Kb/s. Tuttavia, il numero di bit necessari per rappresentare o trasmettere un segnale è spesso un numero variabile con il tempo, poiché dipende dal contenuto informativo e dalla tecnica di codifica utilizzata per rappresentare il segnale.

Un esempio tipico del numero  $R$  di bit/s (o bit-rate) necessari per trasmettere un segnale al variare del tempo è mostrato nella Figura 1.1. Come si può mostrare il valore di  $R$  può variare notevolmente nel tempo.

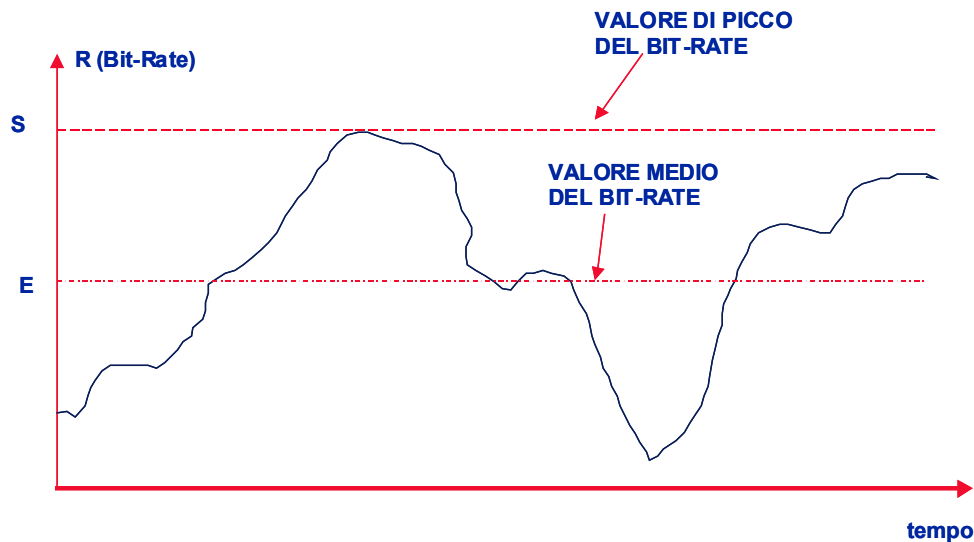


Figura 1.1. Esempio del bit rate  $R$  di un segnale in funzione del tempo.

In molti casi esiste una notevole differenza tra il valore massimo (o di picco)  $S$  e quello minimo. Il valore medio  $E$  del bit-rate  $R$  è un parametro caratteristico di ciascuna classe di segnali. Ad esempio, per il segnale telefonico si ha  $E = 32\text{Kb/s}$  e  $S = 64\text{Kb/s}$ , mentre per un segnale video di qualità standard  $E$  può essere  $20 - 30\text{ Mb/s}$  e  $S$  circa 2 – 3 volte più grande. Per trasmettere un segnale con un bit-rate variabile si possono adottare varie strategie.

Una soluzione possibile per trasmettere tale segnale è di utilizzare una rete con una velocità uguale al massimo valore di  $R$ . In questo caso si ha una riproduzione esatta del segnale numerico, tuttavia, in molti istanti si ha uno spreco della banda del sistema di comunicazione poiché in molti casi sarebbe necessaria una velocità di trasmissione più bassa (Figura 1.2).

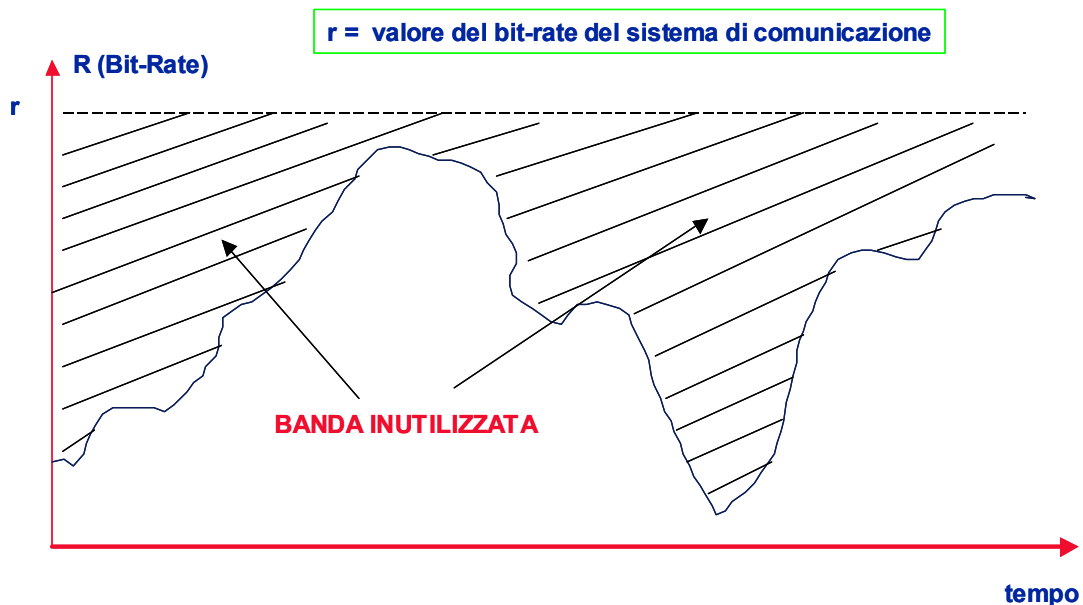


Figura 1.2. Situazione in cui la rete ha un bit-rate maggiore o uguale a  $S$ .

Per ovviare a questo inconveniente e tenendo conto che in molti segnali il valore massimo viene raggiunto solo raramente si può decidere di trasmettere ad una velocità  $V$  inferiore rispetto a quella massima. In questo caso, quando il segnale genera un bit – rate superiore a  $V$  si ha una riduzione della qualità del segnale. Tuttavia, anche in questo caso se  $R < V$  si ha uno spreco di banda del sistema di comunicazione. Per evitare che si verifichi in alcuni momenti uno spreco di banda, si può trasmettere ad ogni istante il numero di bit informativi contenuti effettivamente nel segnale.

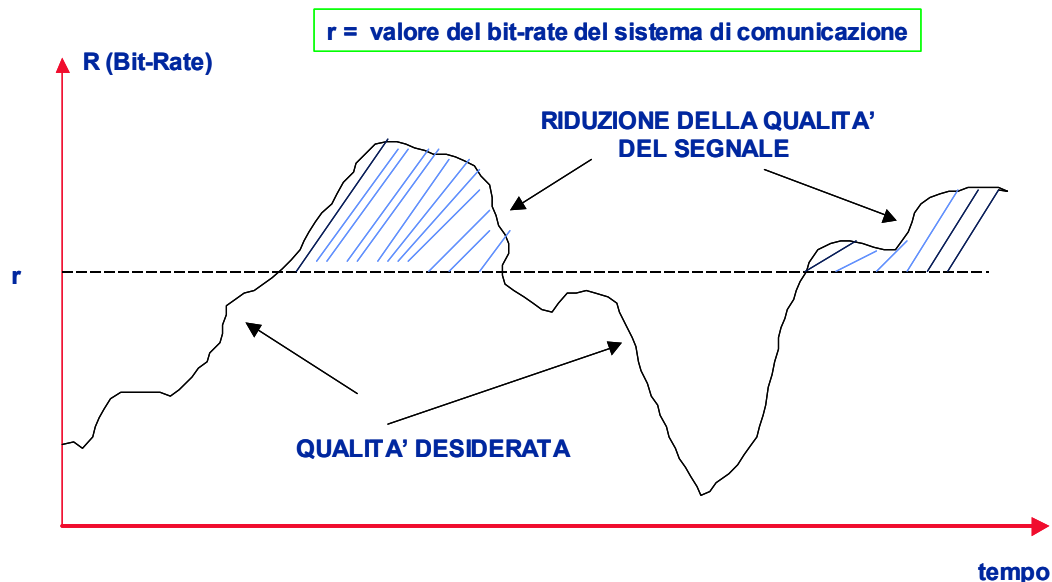


Figura 1.3. Situazione in cui la rete ha un bit-rate  $V$  minore di  $S$ .

In base a queste considerazioni i servizi possono essere divisi in due categorie:

- *Servizi isocroni o a bit rate fisso*: sono servizi con un bit – rate costante nel tempo. Un esempio tipico è il segnale telefonico codificato mediante un sistema PCM, che richiede una velocità fissa di 64 Kb/s.
- *Servizi asincroni o a bit rate variabile*: sono servizi in cui il numero di bit inviati nella rete varia nel tempo.

Il traffico dati generato da un computer è generalmente assimilabile ad un traffico asincrono: i messaggi sono generati ad istanti casuali e hanno lunghezza variabile, gli intervalli di tempo tra due messaggi consecutivi hanno generalmente una durata molto maggiore di quella dei messaggi (spesso di diversi ordini di grandezza). Come conseguenza, dedicare un canale di comunicazione soltanto alla trasmissione di un segnale di questo tipo comporta sia uno spreco di risorse di comunicazione (poiché per periodi di tempo significativi non si ha nessun segnale da trasmettere) sia un costo elevato per l'utente. Si tratta perciò di una situazione molto diversa rispetto al caso del segnale telefonico numerico in cui esiste ad ogni intervallo di tempo  $T = 125 \mu\text{sec}$  un gruppo di 8 bit (un campione) da trasmettere.

## 1.2. Tecniche di commutazione

Il trasferimento dell'informazione (voce, dati, ...) tra due (o più) stazioni attraverso una rete di comunicazioni può essere effettuato utilizzando diverse procedure, chiamate *tecniche di commutazione* che differiscono per l'uso delle risorse di comunicazione e possono essere divise in tre principali categorie:

- *Commutazione di circuito;*
- *Commutazione di messaggio;*
- *Commutazione di pacchetto.*

Ciascuna classe è ottima per la trasmissione di certi tipi di traffico, mentre può non risultare adatta a trasmettere altre categorie di traffico.

### *Commutazione di circuito*

In questo tipo di commutazione, un circuito è assegnato a due utenti per tutta la durata del collegamento; nessun altro utente può utilizzarlo in questo periodo. Il termine circuito è utilizzato in modo generico per indicare una risorsa di rete; esso può essere un circuito fisico (bidirezionale) effettivo, una porzione di banda, un intervallo di tempo.

La commutazione di circuito è stata utilizzata sin dall'inizio nella rete telefonica. Quando un utente effettua una chiamata verso un altro utente, la rete costruisce un collegamento fisico riservato soltanto ai due utenti per tutta la durata della chiamata.

Nella commutazione di circuito si possono distinguere tre fasi:

1. creazione del circuito. Nel caso del collegamento telefonico, questa fase inizia quando il primo utente compone il numero e termina quando l'altro utente risponde.
2. trasferimento dell'informazione da un utente all'altro. Nel caso telefonico, corrisponde alla conversazione tra i due utenti. Il trasferimento dell'informazione può avvenire soltanto dopo la conclusione della fase 1.
3. abbattimento del collegamento. Dopo la fine del trasferimento dell'informazione (uno dei due utenti chiude il collegamento), la rete effettua una serie di operazioni per liberare il circuito e renderlo nuovamente disponibile per altri utenti.

La commutazione di circuito è generalmente adatta alla trasmissione di segnali continui nel tempo e che presentano una durata temporale (fase di trasferimento dell'informazione) molto maggiore rispetto alle altre due fasi (creazione e abbattimento del collegamento). Un esempio tipico è rappresentato da una conversazione telefonica, in cui il segnale è (almeno in linea di principio) sempre presente fino a quando dura la conversazione tra i due utenti. Inoltre, la fase di conversazione è abbastanza grande (in base a misure effettuate una conversazione telefonica ha una durata media di circa 3 min) rispetto alla fase iniziale e finale che generalmente richiedono qualche decina di secondi).

La commutazione di circuito, una volta completata la fase di creazione del collegamento, non richiede alcuna operazione aggiuntiva per il trasferimento dell'informazione.

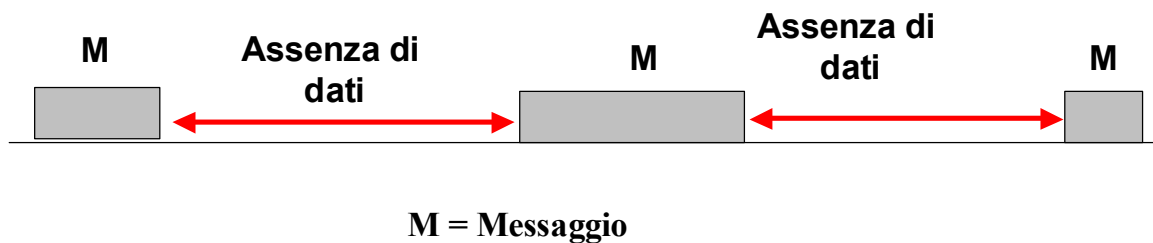


Figura 1.4 . Comportamento tipico di una sorgente dati.

### *Commutazione di messaggio*

Nella commutazione di messaggio, ogni messaggio è considerato un'unità informativa autonoma, e segue per arrivare a destinazione un percorso deciso volta per volta in base allo stato della rete. Un circuito (cioè una risorsa della rete) viene utilizzato soltanto per il tempo necessario per trasferire il messaggio; in questo modo, lo stesso circuito può essere utilizzato contemporaneamente da vari utenti.

Per spiegare il funzionamento della commutazione di messaggio, consideriamo l'esempio mostrato nella Figura 1.5 in cui il terminale A invia a B un insieme di messaggi (ad esempio tre messaggi indicati con M1, M2, M3). Ogni messaggio è composto da una testata (o header) H e dall'informazione, come mostrato nella Figura 1.6. La testata contiene tra l'altro gli indirizzi della stazione di destinazione (B) e della stazione che ha generato il messaggio (A); in questo modo ogni messaggio è autonomo, poiché contiene tutte le informazioni necessarie per portarlo a destinazione . Il messaggio viene inviato al nodo di commutazione che immagazzina il messaggio, lo inserisce nella coda dei

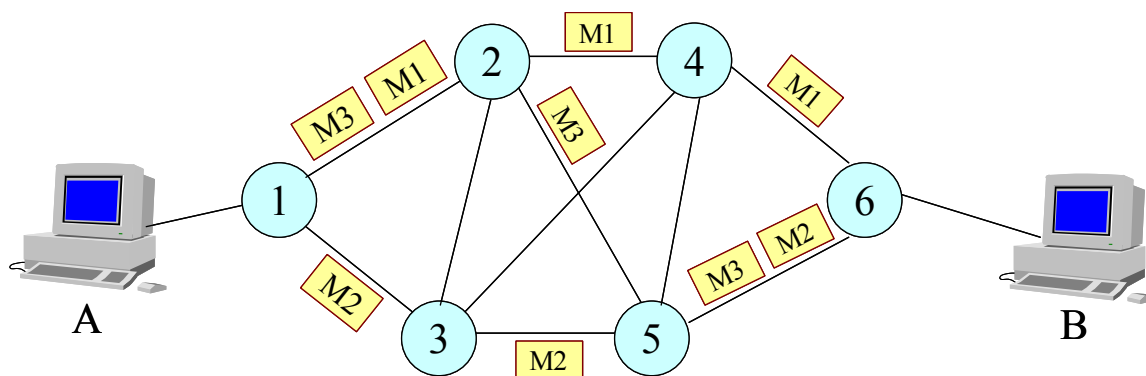


Figura 1.5. Esempio di collegamento tra due host.



Figura 1.6. Formato di un messaggio.

messaggi in attesa di essere trasmessi e, quando esso diventa il primo messaggio della coda, provvede ad instradarlo verso un nodo successivo della rete scelto in base al nodo di destinazione (contenuto nella testata) e utilizzando opportune tecniche di instradamento (o routing). Il funzionamento della rete è quindi basato sul concetto store and forward (memorizza e invia).

La commutazione di messaggio è molto più adatta alla trasmissione dati della commutazione di circuito; tuttavia è scarsamente utilizzata poiché la commutazione di pacchetto presenta prestazioni superiori. Una rete che utilizza la commutazione di messaggio è quella utilizzata per la distribuzione dei telegrammi.

### *Commutazione di pacchetto*

La commutazione di pacchetto rappresenta un'evoluzione di quella di messaggio ed è utilizzata in molte reti per la trasmissione dati. In questa tecnica, il messaggio generato da un terminale viene diviso in pacchetti di dimensioni più ridotte, come mostrato nella Figura 1.7. Ogni pacchetto è formato da una testata H e da una parte dei dati del messaggio.

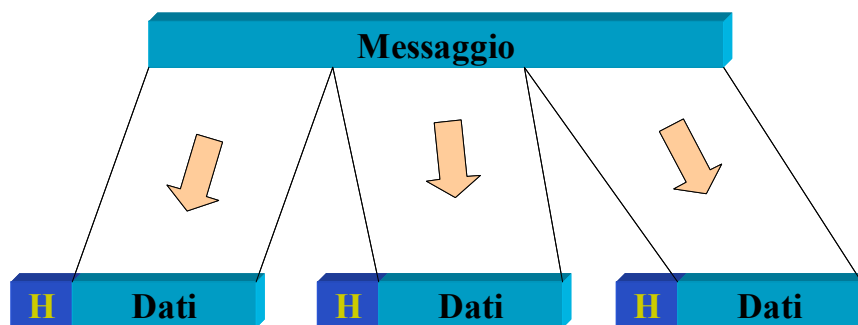


Figura 1.7 - Costruzione dei pacchetti.

La testata contiene numerosi campi utili per l'instradamento e la gestione dei dati, tra cui un numero progressivo che individua la posizione del pacchetto e gli indirizzi della stazione di destinazione e di trasmissione. In questo modo ogni pacchetto diventa un'entità autonoma.

La trasmissione dei pacchetti nella rete può essere effettuata utilizzando due diverse tecniche:

- datagram
- circuiti virtuali.

Nella commutazione di tipo datagram ogni pacchetto viene instradato nella rete in modo indipendente, per cui i pacchetti generati da un messaggio possono seguire strade diverse (Figura 1.8) e quindi i pacchetti possono arrivare al nodo di destinazione in ordine diverso rispetto a quello con cui sono stati generati. Il nodo terminale deve ricostruire l'ordine esatto dei pacchetti utilizzando il numero progressivo contenuto nella testata di ogni pacchetto.



Nella commutazione a circuiti virtuali i pacchetti generati a partire dallo stesso messaggio seguono tutti lo stesso percorso, come mostrato nella Figura 1.9. In questo modo i pacchetti sono sempre nell'ordine corretto con cui sono stati generati e quindi non è necessario al nodo terminale riordinare i pacchetti.

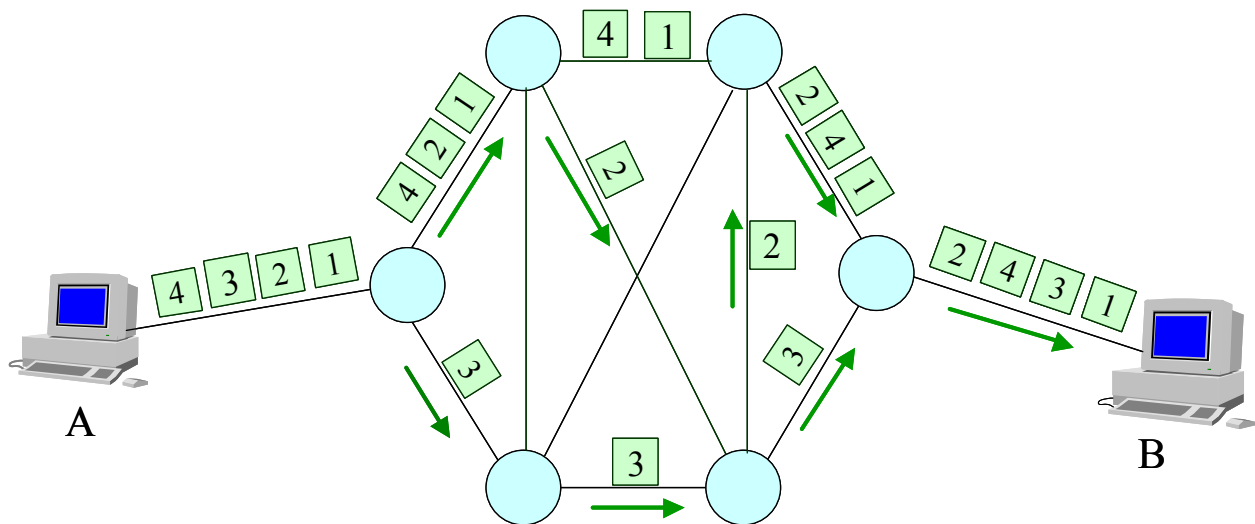


Figura 1.8. Commutazione di pacchetto di tipo datagram

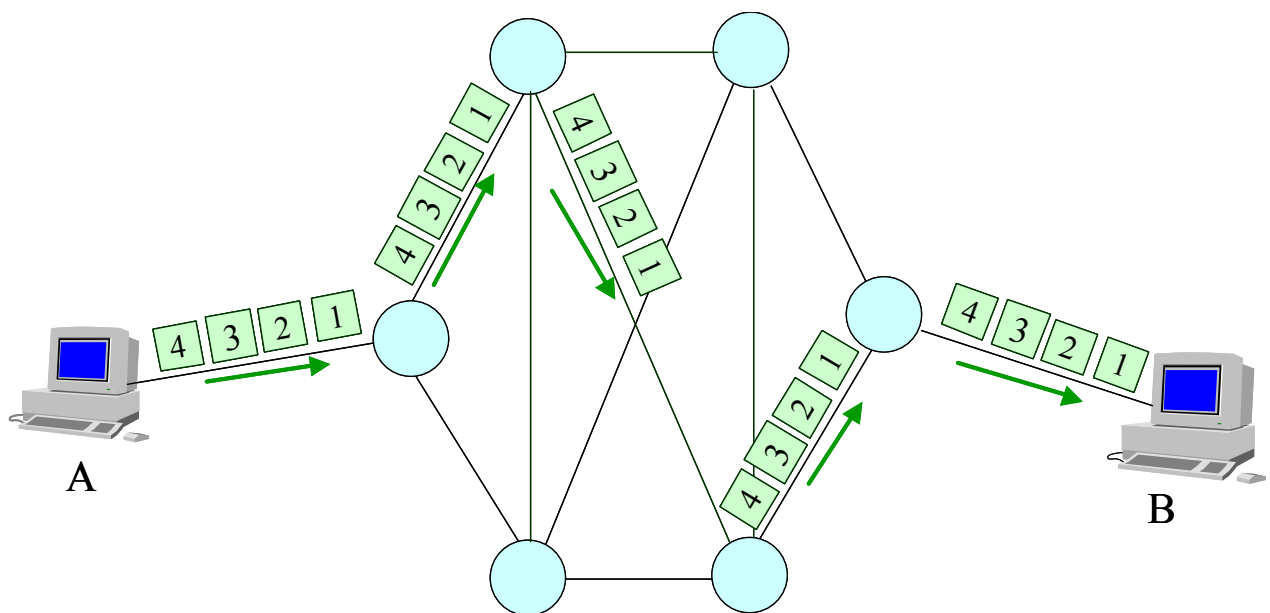


Figura 1.9. Commutazione di pacchetto di tipo a circuiti virtuali

Il termine circuito virtuale indica che, contrariamente a quanto accade nella commutazione di circuito, lo stesso circuito può essere condiviso tra diversi utenti.

Il circuito virtuale viene individuato prima della trasmissione dei pacchetti, per cui sono necessarie tutte le fasi presenti nella commutazione di circuito:

1. creazione del circuito virtuale;
2. trasmissione dei pacchetti;
3. abbattimento del circuito virtuale.

Una volta individuato il percorso, la trasmissione dei pacchetti è molto più veloce rispetto alla tecnica datagram poiché i diversi nodi non devono effettuare scelte o elaborare strategie di instradamento. Per questo motivo, la tecnica dei circuiti virtuali è molto utilizzata nelle moderne reti per la trasmissione di dati ad alta velocità

La tecnica datagram, utilizzata da Internet, presenta alcuni vantaggi rispetto alla tecnica a circuiti virtuali, quali:

- non è necessaria la creazione del circuito prima di iniziare la trasmissione;
- risulta molto più robusta a guasti e a malfunzionamenti; infatti, se un nodo o un link non funzionano correttamente il sistema a datagram identificherà percorsi alternativi, mentre nel caso di circuiti virtuali tutte le connessioni attive passanti per quel nodo o link sono interrotte;
- l'instradamento dei pacchetti della rete può essere progettato in modo da ridurre il periodo di congestione di un nodo o della rete.

La commutazione datagram richiede tuttavia che ogni pacchetto contenga l'indirizzo del nodo di destinazione di validità geografica e quindi con un numero consistente di bit. Ad esempio, Internet è una rete a commutazione di pacchetto di tipo datagram e utilizza indirizzi universali formati da 32 bit. Nella commutazione a circuiti virtuali, ogni pacchetto contiene un indirizzo relativo al circuito virtuale che ha una validità locale, per cui richiede un numero minore di bit.

#### *Confronti tra le diverse tecniche di commutazione*

Per illustrare in modo semplice le differenze tra i tre tipi di commutazione, consideriamo lo schema mostrato nella Figura 1.10, in cui viene disegnato il percorso scelto dal sistema per passare da A a B.

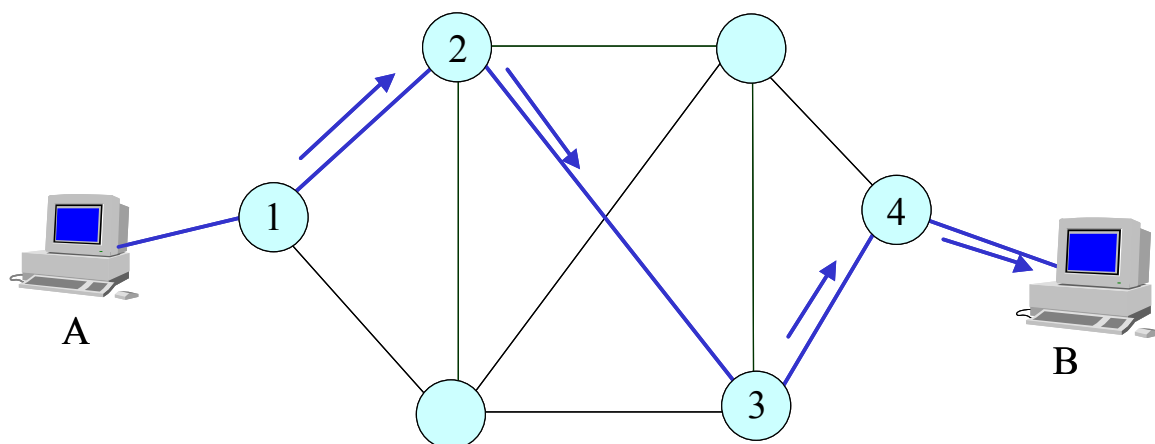


Figura 1.10. Esempio di collegamento tra due host.

Il diagramma temporale della trasmissione di un messaggio da A a B nel caso della commutazione di circuito è mostrato nella Figura 1.11, dove sono evidenziati i tempi di ritardo e di elaborazione incontrati dal messaggio nella rete. Nel disegno sono evidenziate le fasi necessarie per la costruzione del circuito, per il trasferimento del messaggio e per l'abbattimento del collegamento. Si possono evidenziare alcuni elementi caratteristici della commutazione di circuito:

- il ritardo totale con cui B riceve il messaggio è la somma dei tempi di ritardo introdotti dalle fasi 1 e 2;
- una volta terminata la costruzione del circuito (fase 1), il trasferimento del messaggio è immediato a parte il tempo richiesto al segnale per passare da A a B (ritardo di propagazione) e non è necessaria nessuna elaborazione ai nodi.

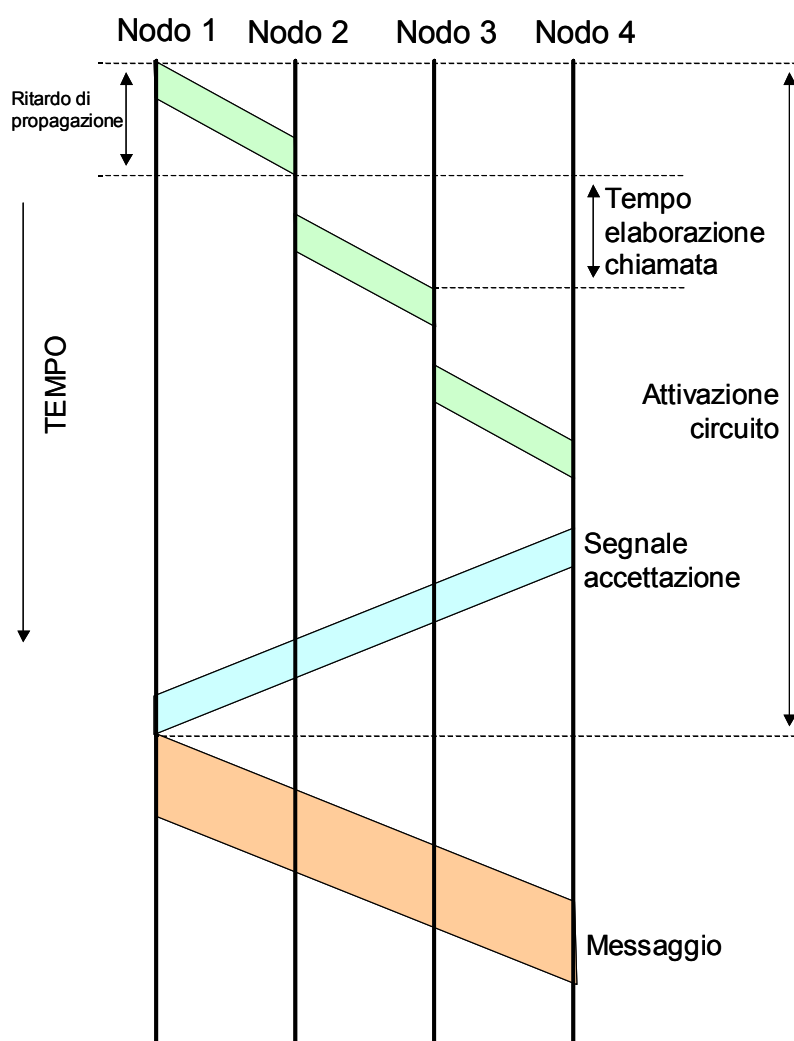


Figura 1.11. Diagramma temporale della commutazione di circuito per il caso di Figura 1.10.

- il ritardo introdotto dalle fasi 1 e 3 può essere superiore a quello dovuto alla trasmissione del messaggio;

- la fase 3 viene eseguita soltanto alla fine del collegamento una volta terminato il trasferimento di tutti i messaggi da A a B.

Nella commutazione di messaggio si ha una situazione abbastanza diversa. Consideriamo per questo il trasferimento del messaggio da A a B nella rete mostrata nella Figura 1.10 secondo il solito percorso evidenziato e utilizzando una commutazione di messaggio. Il diagramma temporale è mostrato nella Figura 1.12. In ogni nodo il messaggio subisce un ritardo dovuto al tempo di attesa in coda e al tempo di elaborazione necessario per identificare il nodo successivo di destinazione. Tuttavia, non c'è più il ritardo dovuto alla costruzione del circuito presente invece nella Figura 1.11. In generale, questo fatto consente di ottenere ritardi di trasmissione di un messaggio minori rispetto al caso della commutazione di circuito.

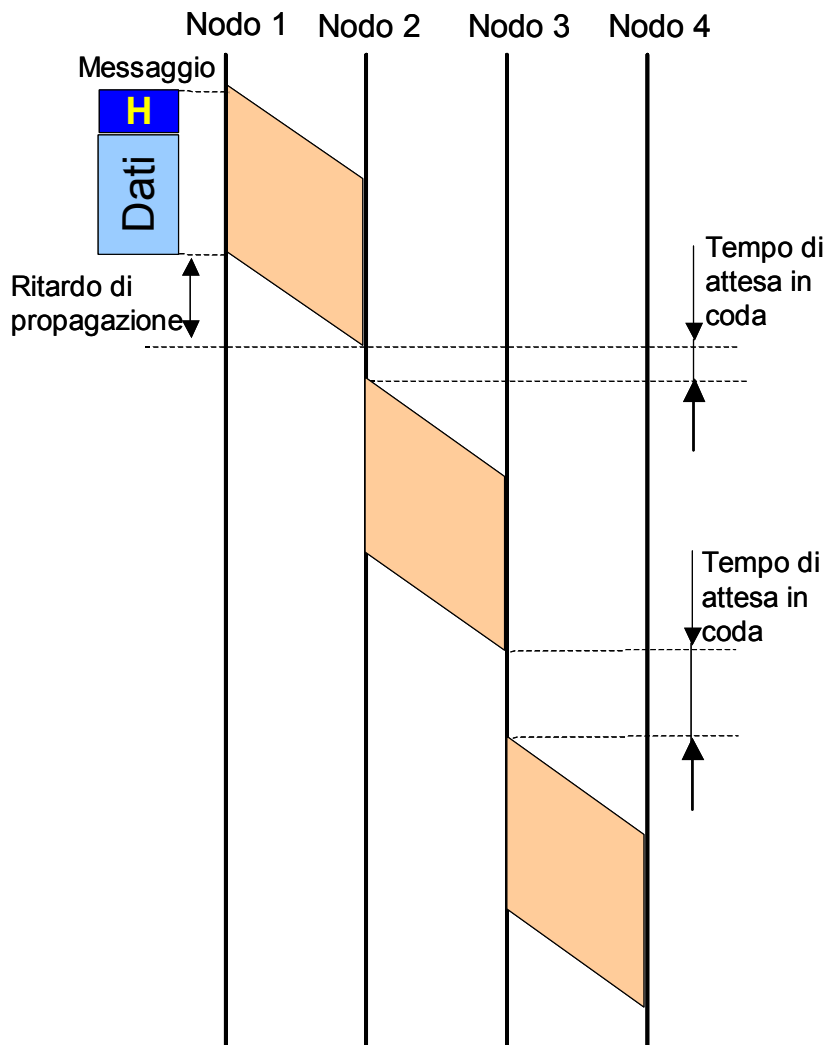


Figura 1.12. Diagramma temporale della commutazione di messaggio per il caso di Figura 1.10.

Nella commutazione di pacchetto, il messaggio viene diviso in pacchetti di dimensione ridotta e si può iniziare a trasmettere un pacchetto appena formato. In questo nodo della rete possono essere presenti contemporaneamente diversi pacchetti dello stesso

messaggio. Consideriamo anche in questo caso la rete della Figura 1.10 e supponiamo che il messaggio sia diviso in tre pacchetti, come nella Figura 1.7.

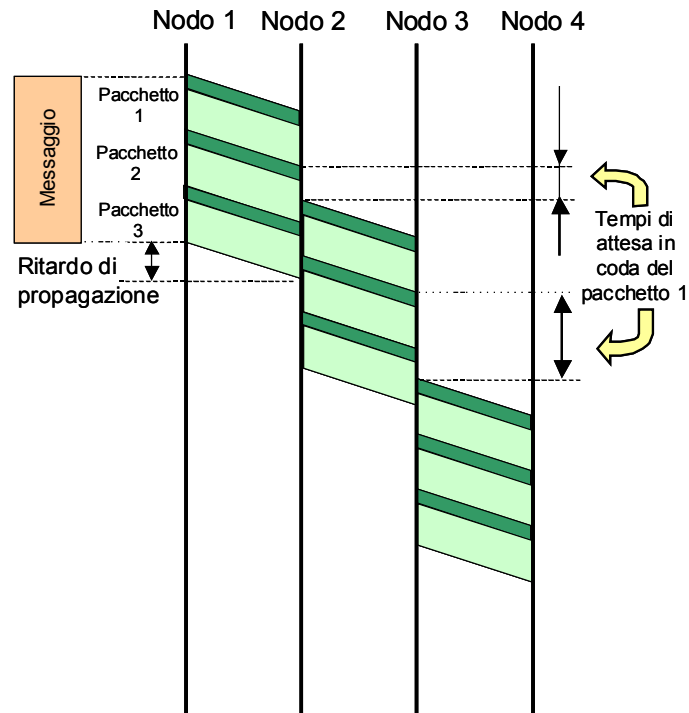


Figura 1.13. Diagramma temporale della commutazione di pacchetto di tipo datagram per il caso di Figura 1.10.

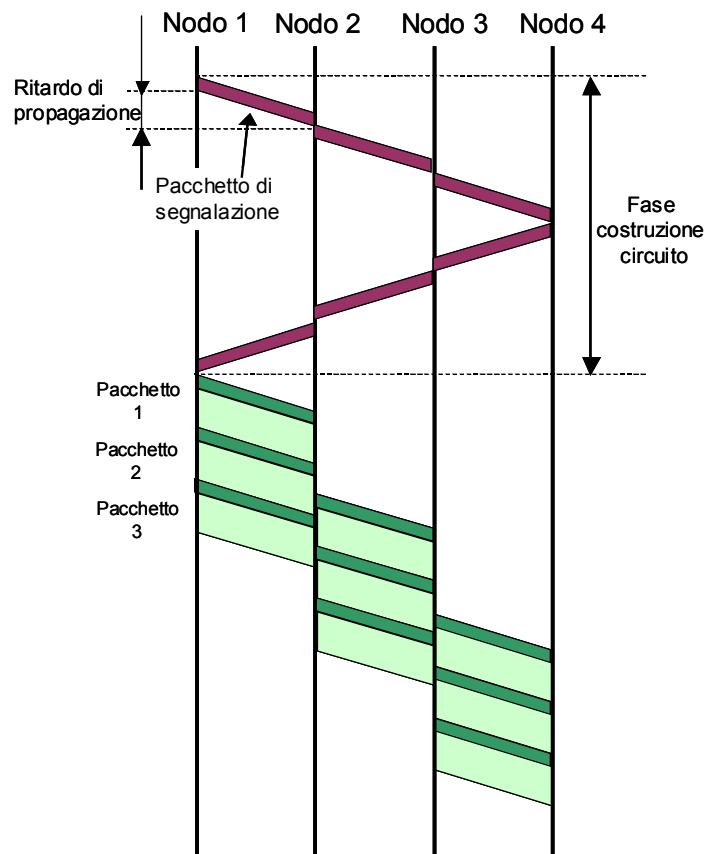


Figura 1.14. Diagramma temporale della commutazione di pacchetto di tipo a circuiti virtuali per il caso di Figura 1.10.

Il diagramma temporale dipende se la rete opera con una tecnica di tipo datagram o a circuiti virtuali. Nel caso di una rete di tipo datagram si ha il diagramma temporale mostrato nella Figura 1.13, mentre nel caso di una rete a circuiti virtuali si ha il diagramma mostrato nella Figura 1.14. Quest'ultimo tipo di commutazione presenta alcune caratteristiche simili alla commutazione di circuito (Figura 1.11) e in particolare la fase di costruzione del circuito. Tuttavia, in questo caso il circuito è virtuale e può quindi essere utilizzato da diversi utenti contemporaneamente.

### 1.3 Multiplex

Un canale di commutazione è capace spesso di trasportare contemporaneamente diversi segnali. Ad esempio, sui cavi telefonici o su un sistema satellitare possono essere trasmessi centinaia o migliaia di telefonate nello stesso istante. La possibilità di condividere le risorse e tra i diversi utenti consente di ridurre i costi di realizzazione della rete e quindi anche per l'utente. L'operazione con cui diversi segnali sono trasmessi sullo stesso canale (cavo, fibra, radio, ...) senza interferenze è chiamata multiplexing dei segnali e l'apparato che effettua tale operazione viene indicato con il nome di multiplex.

Un multiplex riceve  $N$  segnali distinti  $s_1(t)$ ,  $s_2(t)$ , ...,  $s_N(t)$  e li invia su un unico canale di uscita utilizzando opportune regole (o tecniche multiplex), come mostrato nella Figura 1.15.

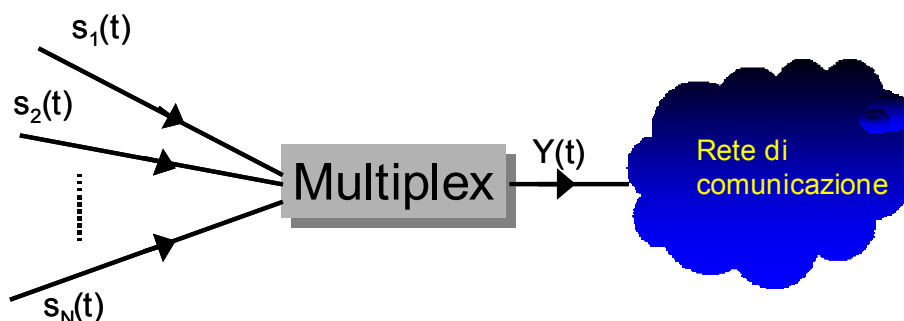


Figura 1.15. Un multiplex.

Il segnale in uscita  $Y(t)$  è una combinazione degli  $N$  segnali in ingresso e da esso è possibile recuperare i segnali di partenza attraverso un'operazione di demultiplexing.

Le tecniche multiplex attualmente utilizzate si dividono in due classi:

- *multiplex a divisione di frequenza; indicati con la sigla FDM (Frequency Division Multiplex);*
- *multiplex a divisione di tempo, indicati con la sigla TDM (Time Division Multiplex).*

Un multiplex a divisione di frequenza trasporta lo spettro dei segnali al suo ingresso su frequenze diverse. Per spiegare in modo semplice questo concetto, consideriamo il caso

in cui all'ingresso del multiplex siano presenti due segnali  $s_1(t)$  e  $s_2(t)$ , ambedue con lo spettro diverso da zero nell'intervallo  $(0, B)$ , come mostrato nella Figura 1.16.a.

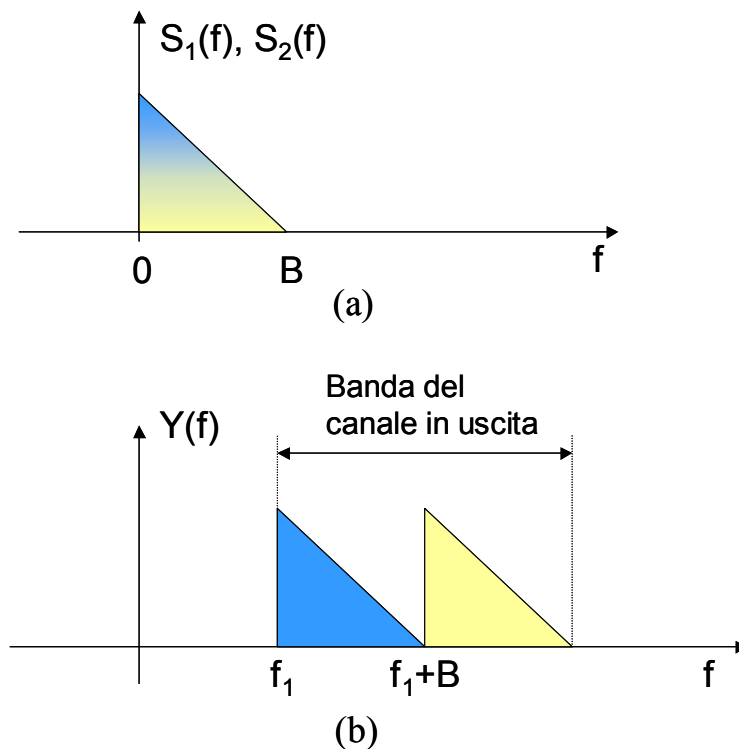


Figura 1.16. Esempio di multiplex FDM per due segnali.

Lo spettro del segnale  $s_1(t)$  viene traslato in frequenza di  $f_1$ , come mostrato nella Figura 1.16.b, mentre lo spettro del secondo segnale viene traslato di  $f_2$  con  $f_2 \geq f_1 + B$  (nella Figura 1.16.b si suppone  $f_2 = f_1 + B$ ). Il multiplex trasmette il segnale  $y(t)$  con lo spettro  $y(f)$  in Figura 1.16.b, il canale in uscita deve avere una banda doppia rispetto al caso di trasmissione di un solo segnale.

Il procedimento è facilmente generalizzato al caso di  $N > 2$  segnali; come mostrato nella Figura 1.17 in cui per semplicità si suppone che tutti i segnali in ingresso abbiano lo spettro diverso da zero nell'intervallo  $(0, B)$  mostrato nella Figura 1.16.a.

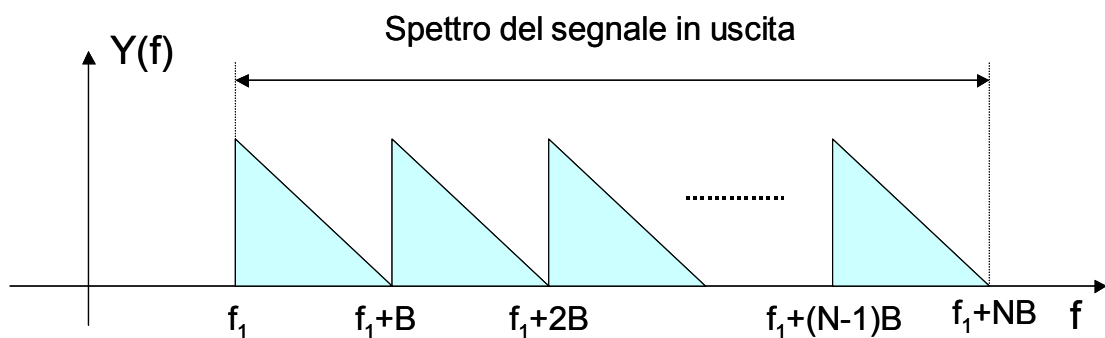
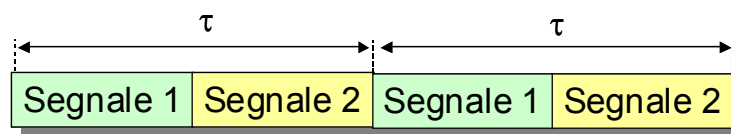


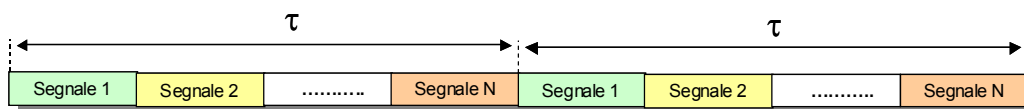
Figura 1.17. Multiplex a divisione di frequenza con  $N$  segnali.

Il canale di comunicazione in uscita, utilizzando per trasmettere il segnale  $y(t)$ , deve avere una larghezza di banda NB. I singoli segnali sono recuperabili senza distorsioni da  $y(t)$  poiché occupano zone di frequenza diverse. I multiplex a divisione di frequenza sono utilizzati soprattutto per la trasmissione di segnali analogici; ad esempio, essi sono molto diffusi nella telefonia.

Nel multiplex a divisione di tempo, utilizzati per i segnali numerici, i diversi segnali si differenziano sostanzialmente per l'intervallo di tempo utilizzato per la trasmissione. Per illustrare in modo semplice il funzionamento dei multiplex a divisione di tempo, consideriamo il caso di due segnali numerici ciascuno dei quali richiede ogni  $\tau$  secondi la trasmissione di  $m$  bit. Il multiplex opera come nella Figura 1.18.a. In questo caso il tempo viene diviso in intervalli di tempo  $\tau$ ; l'intervallo  $\tau$  viene suddiviso in due sotto intervalli: il primo viene utilizzato per trasmettere il primo segnale ed il secondo per trasmettere il secondo segnale.



(a)



(b)

Figura 1.18. Multiplex a divisione di tempo: a) caso di due segnali; b) caso di N segnali.

Il procedimento può essere facilmente generalizzato al caso di  $N$  segnali, come mostrato nella Figura 1.18.b. L'intervallo di tempo  $\tau$  è diviso tra gli  $N$  segnali, a ciascuno dei quali viene assegnato un determinato sotto intervallo per la trasmissione; la situazione si ripete negli intervalli successivi. L'intervallo di tempo  $\tau$  prende il nome di frame ed il suo valore può variare da centinaia di  $\mu\text{sec}$  a decine di  $\text{msec}$ .

I multiplex a divisione di tempo sono molto utilizzati nella telefonia numerica. In essa per ogni segnale telefonico si deve trasmettere un campione, rappresentato con 8 bit, ogni intervallo di  $125 \mu\text{sec}$ . Per questo nei multiplex per la telefonia, la durata del frame  $\tau$  viene scelta uguale a  $125 \mu\text{sec}$ .

Sistemi TDM per la telefonia sono stati standardizzati dal CCITT; si hanno due standard: il primo standard applicato in Europa ha  $N = 32$  canali; mentre il secondo applicato nel Nord America e Giappone usa  $N = 24$ .

Nella Figura 1.9 è riportato lo standard europeo con  $N = 32$ . Nell'intervallo  $\tau = 125 \mu\text{sec}$  devono essere trasmessi  $32 \times 8$  bit; in 1 secondo devono essere trasmessi  $32 \times 8 / 125 \times 10^{-6} = 2.048 \text{ Mb}$ . Il canale necessario per trasmettere il segnale multiplexato (canale all'uscita del multiplex) deve perciò avere una velocità di  $2.048 \text{ Mb/s} \simeq 2 \text{ Mb/s}$  o una banda di circa  $2 \text{ MHz}$ .



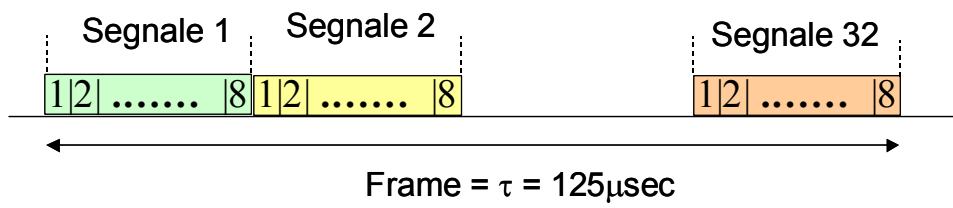


Figura 1.19. Multiplex a 32 canali.

Lo standard in uso in America del Nord e in Giappone è formato da 24 canali telefonici numerici (ciascuno a 64 Kb/s), per cui tali multiplex operano ad una velocità di 1.536 Mb/s.

## Capitolo 2: Tecniche di accesso multiplo

### 2.1 Le risorse

La descrizione seguente delle tecniche di accesso multiplo fa riferimento alle trasmissioni radio in sistemi wireless e cellulari in cui si hanno celle di copertura, ma può essere direttamente estesa ad altri scenari come la trasmissione su cavo o in fibra ottica. Il caso dei sistemi wireless e cellulari è stato prescelto data la sua importanza nell'attuale panorama delle telecomunicazioni. Tuttavia le considerazioni seguenti possono essere applicati anche ad altri scenari di telecomunicazioni, quali (ad esempio) i ponti radio e le comunicazioni satellitari.

Un utente mobile in una cella trasmette alla stazione base utilizzando opportune risorse radio. Una trasmissione nella cella si distingue dalle altre perché fa uso di risorse radio differenti.

Un risorsa trasmissiva viene contraddistinta (in generale) dall'intervallo temporale a disposizione per la trasmissione, la banda di frequenza disponibile, il codice usato per la trasmissione e il livello di potenza usato. Tutti e quattro questi aspetti (e cioè: tempo, frequenza, codice e potenza) concorrono ad identificare univocamente una risorsa.

A seconda della tecnica di accesso multiplo usata, le varie trasmissioni in una cella si differenzieranno per una o più di queste caratteristiche. Ad esempio, se le varie trasmissioni si differenziano solo per la banda di frequenza utilizzata si ha la tecnica di accesso multiplo a divisione di frequenza; se invece le trasmissioni si differenziano per il codice (ed il livello di potenza adottato) si ha la tecnica di accesso multiplo a divisione di codice.

In generale le tecniche di accesso multiplo si occupano di come ripartire le varie risorse tra le trasmissioni simultaneamente attive.

All'interno di una cella si hanno due direzioni di collegamento: il *collegamento uplink* dagli utenti mobili alla stazione base ed il *collegamento downlink* da stazione base agli utenti mobili. Nella tratta uplink si considera l'utilizzo di un protocollo di accesso multiplo per regolare l'accesso dei vari utenti al canale radiomobile; nella tratta downlink è la stazione base che ha da trasmettere con opportuna tecnica di multiplexing i segnali ai vari utenti che serve.

Di seguito sono descritte le principali tecniche di accesso multiplo usate nelle reti radiomobili.

### 2.2 Frequency Division Multiple Access (FDMA)

La banda del sistema viene divisa in sottobande, ogni sottobanda è un canale (Figura 2.1); i vari canali vengono così distribuiti fra le celle. Fra bande adiacenti sono lasciati degli spazi di guardia. I sistemi cellulari terrestri della prima generazione basati su trasmissioni analogiche (con modulazioni di frequenza) usavano questo tipo di tecnica di accesso multiplo. Con l'introduzione delle modulazioni digitali, oltre alla FDMA sono possibili le tecniche descritte nei paragrafi seguenti (TDMA e CDMA).

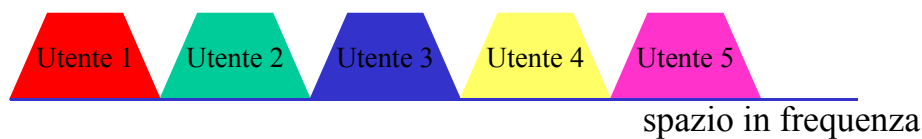


Figura 2.1: Tecnica di accesso FDMA.

### 2.3 Time Division Multiple Access (TDMA)

Ad ogni utente viene assegnato periodicamente un intervallo (=slot) in cui trasmette un insieme di bit (= pacchetto). La voce viene campionata ed ogni campione è quantizzato (ad esempio si prende un campione ogni  $125\ \mu\text{s}$  e si quantizza ad 8 bit, il flusso di bit risultante è di 64 Kbit/s; questa è la tecnica PCM classica). Si usano poi opportune codifiche di sorgente per ridurre il bit-rate fino a valori bassissimi (per i sistemi satellitari si prevede di scendere fino a valori di 2.4 Kbit/s). I bit informativi dell'utente sono raggruppati in pacchetti e la trasmissione è organizzata in trame (*frame*) ciascuna contenente un numero fissato,  $N_s$ , di intervalli temporali (*slot*) in ciascuno dei quali un utente trasmette un pacchetto (Figura 2.2). Quando un utente trasmette, ha a disposizione l'intera banda associata alla portante.

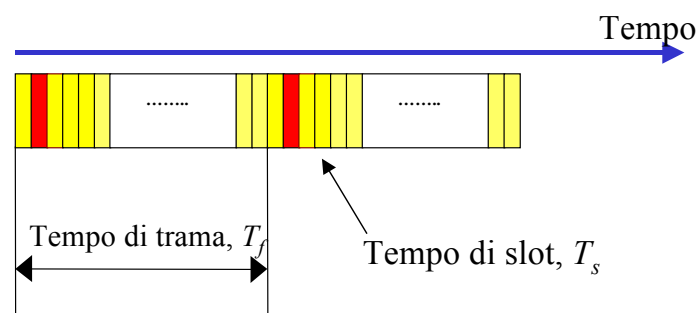


Figura 2.2: Struttura della trama di una portante TDMA.

Lo standard cellulare digitale americano IS-54 che usa TDMA ha triplicato, a parità di banda allocata, la capacità (= numero di utenti simultanei per cella) dello standard analogico AMPS basato su FDMA. Anche il sistema cellulare europeo di seconda generazione GSM (*Global System for Mobile Communications*) fa uso della tecnica di accesso TDMA. Più esattamente si tratta di una tecnica di tipo FDMA/TDMA in cui, infatti, la banda disponibile viene suddivisa in sotto-bande di 200 KHz e ciascuna di esse trasporta una portante GSM in cui l'accesso è TDMA.

### 2.4 Code Division Multiple Access (CDMA)

Le tecniche per l'allargamento dello spettro trasmesso ("*Spread Spectrum*", SS) sono state inizialmente introdotte in ambito militare (metà anni '50) per rendere le trasmissioni particolarmente immuni da disturbi e interferenze intenzionali ("*jamming*"). In trasmissione il segnale viene distribuito su una banda  $PG$  volte più grande di quella originaria tramite una

apposita modulazione ottenuta con un codice pseudocasuale (codice *PseudoNoise* - PN<sup>1</sup>); il fattore di allargamento di banda *PG* è detto “*processing gain*” e suoi valori tipici variano da 10 a 1000. Ogni utente ha un suo codice, tutti gli utenti attivi trasmettono nella stessa banda simultaneamente. Anche se nel canale sono introdotti disturbi intenzionali, l’operazione in ricezione che riporta il segnale nella sua banda originaria, distribuisce il disturbo su una banda molto più ampia, rendendolo praticamente influente. In ricezione si deve disporre di una sequenza di codice sincronizzata con quella usata in trasmissione per poter effettuare questa operazione.

Due sono le tecniche possibili per l’allargamento di spettro:

- *tecnica “Direct Sequence” DS* (a sequenza diretta), secondo cui il segnale trasmesso è moltiplicato per un segnale modulato dai bit (detti chip) della sequenza di codice PN con tasso molto più elevato (*PG* volte più elevato) di quello informativo;
- *tecnica “Frequency Hopping” FH* (a salti di frequenza), secondo cui la sequenza di codice PN va a variare la frequenza della portante.

La prima soluzione è preferita alla seconda, perché la tecnologia attuale non consente di ottenere economicamente sintetizzatori di frequenza capaci di effettuare le variazioni di frequenza della tecnica FH con la rapidità richiesta per ottenere elevati valori di *PG*.

Nella tecnica DS-CDMA ogni utente trasmette alla stazione base usando un proprio codice; il codice è come una firma dell’utente. Invece la stazione base trasmette a tutti i mezzi mobili della cella utilizzando un codice suo proprio. Il canale radiomobile è caratterizzato da forti disturbi fra i quali, in particolare, il fading (= fluttuazioni del segnale) prodotto da cammini multipli per la presenza di una miriade di ostacoli (terreno, edifici, vegetazione). Questo tipo di fading è selettivo in frequenza. Nelle reti cellulari terrestri come in quelle via satellite si è quindi pensato di usare tecniche DS-CDMA, perché queste trasmissioni a larga banda presentano un’intrinseca diversità di frequenza particolarmente adatta per combattere il fading veloce prodotto dalle riflessioni multiple e perché sono trasmissioni particolarmente insensibili all’interferenza derivante dalla presenza nella stessa banda di trasmissioni simultanee.

La capacità con CDMA è solo limitata dall’interferenza, mentre con FDMA e TDMA è limitata principalmente dall’ampiezza di banda. Con CDMA, qualsiasi riduzione di interferenza si traduce direttamente e linearmente in un incremento di capacità. Alcune tecniche per ottenere questo sono:

- “silenziamento” delle trasmissioni, nei periodi non attivi di una conversazione (*squelching*);
- uso di celle multisetore che limitano l’interferenza ricevuta alla stazione base a quella che proviene da una porzione della cella;
- uso di diverse polarizzazioni per il segnale trasmesso e di un’antenna in ricezione alla stazione base che le discrimina.

Inoltre la tecnica CDMA necessita di sistemi di controllo della potenza trasmessa da un utente mobile in relazione alla sua distanza dalla stazione base, per evitare che le

---

<sup>1</sup> I codici PN sono codici ciclici che ben approssimano la generazione casuale di bit 0 e 1 (ad esempio i codici di Gold). Questi codici devono essere caratterizzati da alti valori di auto-correlazione, in modo da distinguere il segnale utile da altri segnali interferenti con codici diversi, e da bassi valori per la correlazione incrociata.

trasmissioni di utenti più vicini impediscano la corretta ricezione di quelli più lontani (effetto “*near-far*”).

Con CDMA è possibile utilizzare una struttura di ricevitore denominata RAKE e cioè a più rami, uno per ciascun cammino che si riesce a risolvere nell’ampia banda di trasmissione. Ciò consente una tecnica a diversità appositamente per CDMA (nel ricevitore RAKE si hanno diversi blocchi demodulatori corrispondenti a repliche diversamente ritardate del segnale).

Infine, l’efficienza della tecnica CDMA non risente dell’introduzione di potenti codifiche a correzione (indispensabili per combattere i disturbi nel canale radiomobile), perché l’operazione di allargamento di spettro può essere opportunamente ripartita fra il processo di codifica e quello di DS. La codifica PN deve comunque rimanere per distinguere gli utenti. Questo consente di avvantaggiare molto il CDMA rispetto alle altre tecniche di accesso multiplo specie nelle reti radiomobili in cui occorre proteggere il segnale trasmesso con potenti codifiche.

Un altro vantaggio del protocollo CDMA è che esso può coesistere con trasmissioni a banda stretta (ad esempio altri sistemi cellulari che usano TDMA) rappresentando per questi solo un rumore accettabile.

Lo standard americano di seconda generazione per sistemi cellulari terrestri basato sul CDMA è lo standard IS-95 (cui corrisponde il sistema cellulare americano denominato cdmaOne); per i sistemi satellitari si può considerare che il sistema GLOBALSTAR fa uso della tecnica CDMA. Per i sistemi cellulari terrestri di terza generazione (3G) lo standard mondiale è basato su una versione di DS-CDMA a larga banda denominata Wideband-CDMA.

#### 2.4.1 Descrizione della tecnica di spreading a sequenza diretta

Facciamo riferimento ad uno schema di trasmissione DS-CDMA semplificato.

Per operare questa tecnica di *spreading* i bit informativi (di durata  $T_b$ ) che devono essere trasmessi vengono resi antipodali (e cioè, ad esempio, al bit 1 si fa corrispondere il valore +1 ed al bit 0 si fa corrispondere il valore -1). La sequenza di bit informativi viene moltiplicata per la sequenza di codice PN tipica della trasmissione. Tale sequenza produce dei bit antipodali (+1 e -1) detti *chip* di durata (durata  $T_c$ ) più breve di quella dei bit informativi. Tipicamente si assume che  $PG$  chip siano contenuti in un tempo di bit:

$$PG = T_b / T_c$$

$PG \gg 1$  rappresenta il *processing gain* (o *spreading gain*) e cioè il fattore di espansione della banda rispetto a quella del segnale originario.

Il segnale così prodotto va ad un modulatore prodotto che lo moltiplica per un’oscillazione ad alta frequenza.

Questo processo di spreading è descritto nella Figura 2.3.

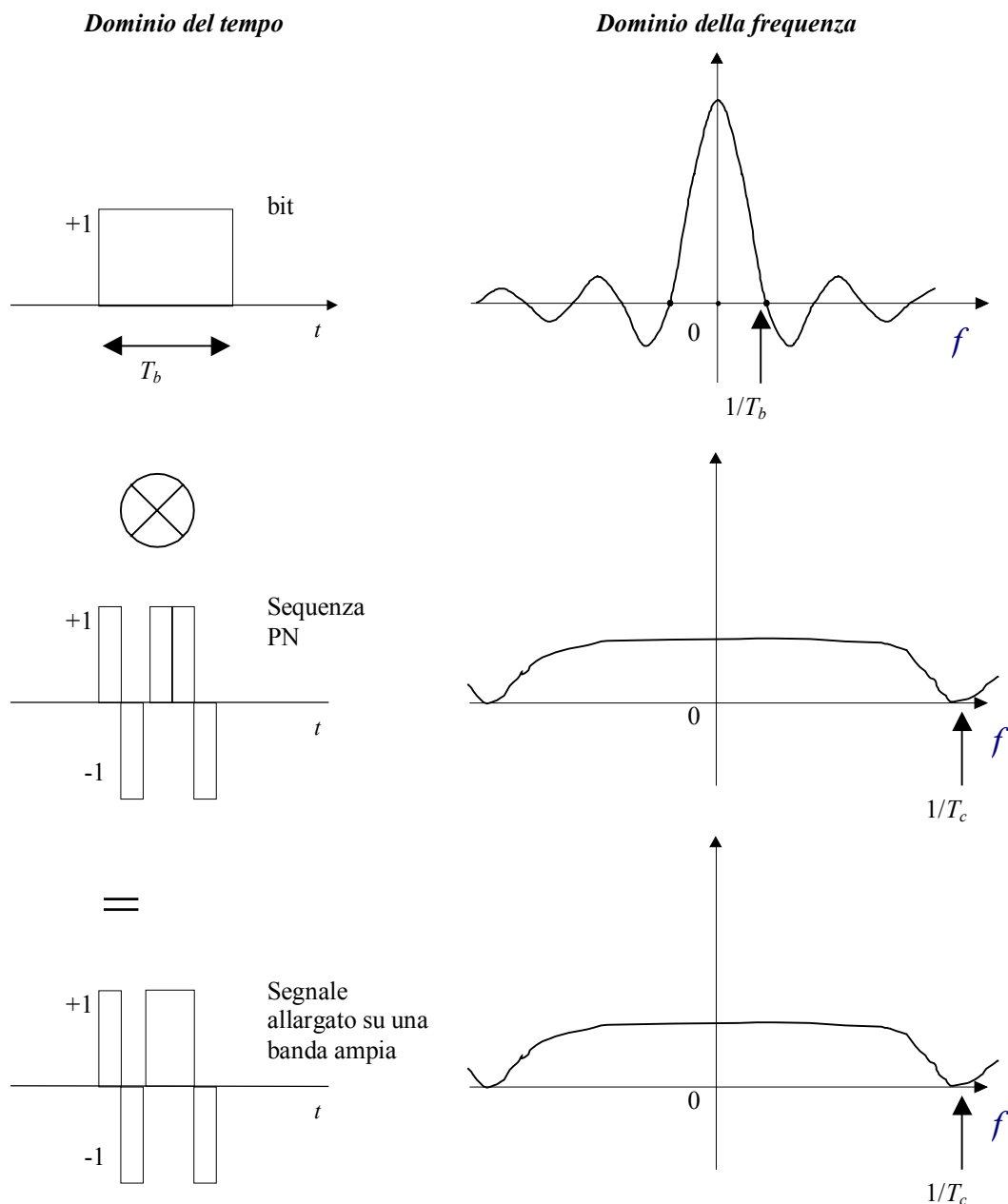


Figura 2.3: Processo di spreading con tecnica DS.

La sequenza PN è una data da un codice periodico: ogni  $L$  chip la sequenza si ripete. Di solito si fa sì che un periodo della sequenza coincida con un tempo di bit (cioè  $L = PG$ ).

Lo schema della trasmissione con questa tecnica può essere riassunto come indicato in Figura 2.4.

In ricezione si deve avere la stessa sequenza PN (e in fase) di quella trasmessa in modo che dal prodotto dei simboli PN uguali in trasmissione e in ricezione venga fuori un valore 1. Con questo prodotto si elimina il processo di spreading (operazione di *despreading*) e si riporta il segnale nella banda originaria. Lo schema della ricezione è stato riassunto in Figura 2.5.

Il vantaggio di questa tecnica è che un qualunque disturbo a banda stretta introdotto dal canale viene allargato in ricezione su tutta la banda di spreading e quindi la sua presenza ha un impatto ridotto.

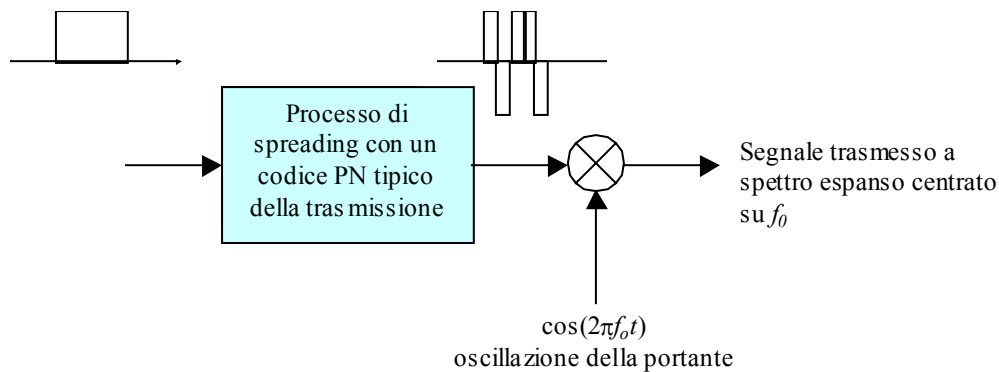


Figura 2.4: Trasmissione DS-CDMA.

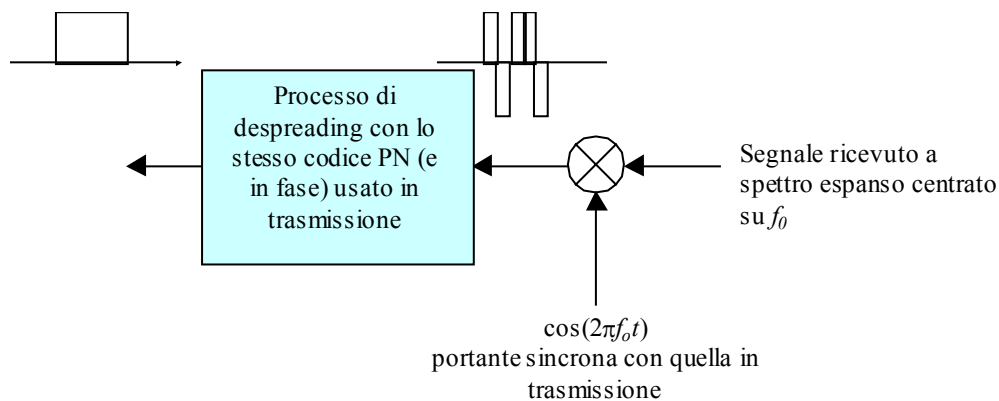


Figura 2.5: Ricezione DS-CDMA.

#### 2.4.2 Proprietà delle sequenze di codice PN

Idealmente il codice di spreading dovrebbe essere progettato in modo che i valori dei chip sono statisticamente indipendenti. Nella pratica il codice PN viene prodotto da registri a scorrimento opportunamente retroazionati e quindi la sequenza che si ottiene è periodica. Il prodotto (chip a chip) della parola di codice PN per una parola di codice ottenuta dalla precedente con un shift ciclico di  $k$  posizioni e la somma del risultato ottenuto (*autocorrelazione*) deve essere massima per  $k = 0$  (sequenze in fase) e praticamente nulla per  $k$  diverso da zero. In questo modo con tali sequenze si può recuperare in ricezione il sincronismo del segnale. Inoltre il prodotto (chip a chip) di due sequenze PN distinte e la somma dei risultati (*crosscorrelazione*) deve essere sufficientemente piccola (idealmente nulla) in modo che le trasmissioni di un utente che usa un codice siano separabili (ortogonali) rispetto alle trasmissioni di un altro utente che usa un altro codice.

Questa è una proprietà di fondamentale importanza nei sistemi radiomobili. Si faccia riferimento alla trasmissione dei mezzi mobili di una cella alla stazione base. Le trasmissioni DS-CDMA degli utenti usano due codici distinti. In questo modo la stazione base effettuando la procedura di despreading con il codice di un utente elimina totalmente il segnale dell'altro utente. Pertanto la proprietà della crosscorrelazione garantisce che le trasmissioni multiple a divisione di codice in una cella siano distinguibili alla stazione base.

Tuttavia, siccome le trasmissioni di due utenti non sono sincrone fra loro, si vengono a ridurre le capacità di ortogonalizzazione delle trasmissioni degli utenti con codici diversi. Pertanto, se la stazione base fa il despreading con un codice, rimane un contributo di interferenza dovuto alla trasmissione dell'altro utente con codice differente. Questa è l'*interferenza di multiaccesso*; pertanto la trasmissione di un utente in una cella subisce interferenza di accesso multiplo sia dagli altri utenti che trasmettono nella stessa cella sia dagli utenti nelle celle vicine. Questo fenomeno limita la capacità di utenti che possono trasmettere simultaneamente in una cella garantendo che il rapporto (alla stazione base) tra la potenza del segnale utile e la potenza del segnale interferente stia sopra una certa soglia. Altrimenti il segnale utile non può essere correttamente ricevuto e si dice che si ha un *evento di outage*.

Un esempio tipico di codice PN usato per trasmissioni DS-CDMA è dato dai codici di Gold.

#### 2.4.3 Il controllo di potenza

La tecnica CDMA fa sì che i segnali delle diverse comunicazioni siano distinti dall'uso di un codice diverso. Nella realtà, però, le condizioni di propagazione riducono le proprietà di ortogonalità delle sequenze di codice usate. Di conseguenza il numero delle conversazioni gestibile per cella con un accettabile livello del *rapporto segnale-interferenza* (SIR) è limitato dall'interferenza prodotta dalle altre trasmissioni nella stessa cella e dalle altre trasmissioni nelle celle adiacenti.

Se dunque una trasmissione ha un livello troppo basso di SIR essa può decidere di aumentare il livello della potenza trasmessa. In questo modo però, tale trasmissione può arrecare un livello di interferenza anche intollerabile alle altre trasmissioni nella stessa cella ed in quelle vicine. Inoltre, se un terminale mobile che si trova molto vicino alla stazione base decide di trasmettere con un livello di potenza troppo elevato, tutti gli altri segnali provenienti da mezzi mobili più distanti non possono essere ricevuti correttamente. Questo è il problema di *near-far*. In generale, è essenziale che nella tratta da terminali mobili a stazione base (*uplink*) i segnali vengano ricevuti alla stazione base dai diversi mezzi mobili con la stessa potenza. Ciò può essere ottenuto tramite un meccanismo di controllo della potenza trasmessa dal terminale mobile.

Un sistema cellulare CDMA si avvale di due sistemi di controllo di potenza: controllo ad anello aperto e controllo ad anello chiuso. Nel primo caso è il mobile che in base al livello di potenza di un segnale di riferimento trasmesso dalla stazione base (segnale pilota) autoregola la potenza trasmessa. Nel secondo caso è la stazione base che ricevendo il segnale trasmesso dal mezzo mobile comanda che esso alzi o abbassi la potenza trasmessa in modo di adeguare il livello ricevuto.

Il controllo di potenza è usato sia nella tratta da mezzi mobili a stazione base (*uplink*) sia nella tratta da stazione base ai mezzi mobili della cella (*downlink*). Il controllo di potenza è



essenziale in uplink dove molti utenti (ciascuno avente differenti condizioni di canale di comunicazione) trasmettono contemporaneamente alla stazione base. In downlink il controllo di potenza è meno critico in quanto il trasmettitore della stazione base “affascia” i vari segnali di utente e li trasmette simultaneamente ai vari utenti della cella. In questo caso, ciascun mezzo mobile riceverà i vari contributi (quello utile e quelli destinati agli altri mezzi mobili della cella) sincroni fra loro e con uguale livello di potenza. In base a queste considerazioni risulta evidente che la tratta uplink risulta la più critica e cioè quella che maggiormente limita la capacità di un sistema CDMA. Grazie ai meccanismi di controllo della potenza, l'interferenza dovuta agli utenti di una cella non dipende quindi dalla loro distanza dalla stazione base.

Da tutte queste considerazioni appare chiaro che la valutazione della capacità di un sistema CDMA deve essere basata sulla valutazione accurata del livello di interferenza del sistema e quindi dal valore del SIR garantito.

#### 2.4.4 La capacità di un sistema cellulare (tratta uplink)

Si consideri il caso di una cella isolata perfettamente dalle altre in cui la stazione base controlla perfettamente i livelli di potenza trasmessi dai terminali mobili: tutti i segnali sono ricevuti alla stazione base con lo stesso livello di potenza. Sia detto  $N$  il numero di utenti simultaneamente attivi nella cella e sia detto  $C$  il valore della potenza ricevuta alla stazione base da un generico mezzo. Per un utente mobile, i restanti  $N-1$  utenti della cella danno un segnale interferente con potenza  $C(N-1)$  alla stazione base. Pertanto il rapporto  $C$  su  $I$ , vale a dire il SIR della trasmissione dell'utente considerato si ottiene come segue:

$$\frac{C}{I} = \frac{1}{\rho(N-1)}$$

dove  $\rho$  è il coefficiente di cross-correlazione parziale per dei codici (si tenga conto che il processo di despreading consiste in una correlazione tra il segnale ricevuto e il segnale associato al codice di spreading). Per codici di Gold  $\rho = 2/3$ .

Al fine di garantire la qualità di servizio desiderata occorre che il SIR sia maggiore di un certo valore di soglia che dipende dal tipo di servizio considerato (altrimenti si verifica *outage*).

Generalmente si passa dal SIR al rapporto tra l'energia del bit d'informazione e la densità spettrale del segnale di interferenza (nell'ipotesi che il rumore additivo termico sia trascurabile),  $E_b/I_0$ , come segue:

$$\frac{E_b}{I_0} = \frac{C/R_b}{I/W} = \frac{W}{R_b} \frac{1}{\rho(N-1)} = \frac{PG}{\rho(N-1)}$$

dove  $W$  è la banda di trasmissione del segnale CDMA e  $R_b$  è il bit-rate informativo. Il rapporto  $W/R_b$  è praticamente il processing gain e si indica tipicamente con  $PG$ .

Noto il valore richiesto di  $E_b/I_0$  e noto  $PG$ , si può ricavare come segue il numero di utenti che la cella può supportare (per semplicità si è posto  $\rho = 1$  in questo studio):

$$N \approx \frac{PG}{\left. \frac{E_b}{I_0} \right|_{richiesto}}$$

Come si vede ci sono due termini che influenzano la capacità di utenti di una cella: il valore richiesto di  $E_b/I_0$  e il processing gain  $PG$ . Ogni tecnica che consente di diminuire il valore richiesto del rapporto  $E_b/I_0$  (a parità di qualità) comporta automaticamente un guadagno in termini di capacità.

Se durante le pause della conversazione, la sorgente non trasmette alcun segnale, si ha un aumento di capacità. Sia  $d$  la frazione di tempo per cui è mediamente attiva una sorgente (per una sorgente vocale  $d \approx 0.5$ ). Allora anche l'interferenza subita da una trasmissione si riduce di un fattore  $d$  e ciò porta direttamente ad un incremento della capacità.

In queste condizioni quindi la capacità di utenti per cella diventa:

$$N \approx \frac{1}{d} \frac{PG}{\left. \frac{E_b}{I_0} \right|_{richiesto}}$$

Si consideri ora l'estensione delle precedenti considerazioni al caso in cui gli utenti sono uniformemente distribuiti in più celle e richiedono tutti lo stesso servizio. Supponiamo che  $N$  utenti siano presenti per cella. L'effetto dell'interferenza delle celle esterne alla cella di interesse è tenuto in conto aumentando il numero degli utenti interferenti nella cella ( $N - 1$  utenti) con un altro contributo proporzionale al numero di utenti  $N$  per cella, secondo un fattore  $\varepsilon$ . Pertanto la capacità di utenti per un fissato valore di  $E_b/I_0$  diventa:

$$\frac{E_b}{I_0} = \frac{PG}{\rho(N-1)d + \varepsilon Nd} \xRightarrow{\rho=1} N \approx \frac{PG}{(1+\varepsilon)d} \frac{1}{\left. \frac{E_b}{I_0} \right|_{richiesto}}$$

Come si nota questa capacità è ridotta di un fattore  $1 + \varepsilon$  rispetto al caso di singola cella. In questa espressione della capacità compare il parametro  $\varepsilon$  che risulta di non facile valutazione. Valori tipici di  $\varepsilon$  in un ambiente microcellulare sono 0.5 – 0.6 (la tecnica di controllo di potenza, la legge dello shadowing, il tipo di attenuazione con la distanza ed il fading hanno impatto sulla determinazione del valore di  $\varepsilon$ ).

## 2.5 Confronto fra le tecniche di accesso multiplo

Inconveniente della tecnica TDMA è che tutti gli utenti devono essere sincronizzati. Inoltre uno slot deve contenere degli intervalli di guardia rispetto al tempo di trasmissione del pacchetto, per compensare i diversi ritardi di propagazione degli utenti all'interno di una cella (questo è importante soprattutto nel caso via satellite). Per elevati bit-rate in trasmissione è richiesto l'uso di equalizzatori in ricezione per combattere l'interferenza intersimbolica introdotta dal canale dispersivo.

Un altro svantaggio del protocollo TDMA rispetto a CDMA è il seguente. Siccome i terminali di utente hanno un ciclo  $1/N_s$ , essi hanno un inviluppo di potenza periodicamente pulsante. Questo rappresenta un problema nel progettare i componenti e gli amplificatori di potenza a radiofrequenza che devono essere capaci di supportare elevate potenze di picco.

Rispetto alla tecnica CDMA, il protocollo TDMA ha il vantaggio di necessitare di un controllo di potenza meno stringente, dal momento che l'interferenza fra utenti è controllata dall'allocazione in tempo ed in frequenza. Un altro importante vantaggio rispetto a FDMA e CDMA è che la struttura con slot temporali dà tempo per effettuare misurazioni di slot, frequenze e stazioni base alternativi al fine di supportare procedure di handover assistite o controllate dal mezzo mobile.

In termini di efficienza di utilizzo della banda disponibile le varie tecniche di accesso multiplo si confrontano in termini del seguente parametro misurato in bit/s/Hz:

$$\eta = \frac{MR_b}{W}$$

dove  $M$  è il numero di utenti simultanei supportabili per cella (il numero di utenti che trasmettendo simultaneamente hanno garantita una probabilità d'errore per bit minore o uguale ad un dato valore massimo accettabile),  $R_b$  è il bit rate informativo per utente e  $W$  la banda totale disponibile.

In base al parametro  $\eta$  è stato possibile dimostrare che la tecnica CDMA consente un'efficienza superiore nell'utilizzo delle risorse delle altre tecniche. I valori dell'efficienza  $\eta$  dipendono comunque fortemente dalle caratteristiche del canale di comunicazione, dalle tecniche trasmissioni utilizzate (es., codici, modulazione) e dai requisiti imposti sulla probabilità d'errore per bit.

# Capitolo 3: Il modello OSI

## 3.1. Introduzione

Il modello OSI (Open System Interconnection), sviluppato alla fine degli anni '70 dall'organismo internazionale ISO (International Standard Organization), ha come obiettivo principale la realizzazione di **sistemi aperti**, fra i quali sia possibile trasferire dati indipendentemente dal costruttore e dalla configurazione dei sistemi considerati.

Il modello OSI definisce come **sistema** un insieme di uno o più elaboratori con il relativo software, periferiche e terminali. **Un'applicazione** è invece l'elemento (es. programma software) che svolge effettivamente l'elaborazione dei dati.

Lo standard OSI si occupa dello scambio di informazione tra sistemi e tra gli altri elementi che contribuiscono alla connessione di tali sistemi (strutture ed apparati di telecomunicazioni), come mostrato nella Figura 3.1. Esso si propone i seguenti scopi:

- *Fornire una base comune per la realizzazione di standard nel settore dell'interconnessione di sistemi informatici e di telecomunicazione.*
- *Facilitare l'interconnessione tra apparati prodotti da diverse aziende.*
- *Costruire una struttura di riferimento per realizzare una rete aperta e trasparente per l'utente.*

L'architettura generale del sistema OSI è basata su tre componenti principali:

1. **I sistemi** che contengono le applicazioni.
2. **I processi applicativi** per lo scambio di informazione.
3. **Le connessioni** che permettono lo scambio di informazioni.

Per semplificare la descrizione e la progettazione di un sistema, lo standard OSI utilizza una **struttura a livelli**. Questo tipo di approccio è oggi comune a tutti gli standard per le architetture di rete, mentre possono variare il numero di livelli, il loro nome e le funzionalità.



Figura 3.1. Schema generale di un sistema di comunicazione tra due computer.

### 3.2 Descrizione generale del modello OSI

L'architettura di un qualunque sistema per il trasferimento dell'informazione viene divisa dal modello OSI nei seguenti sette livelli:

- 1 livello fisico
- 2 livello di collegamento (data link)
- 3 livello di rete
- 4 livello di trasporto
- 5 livello di sessione
- 6 livello di presentazione
- 7 livello di applicazione

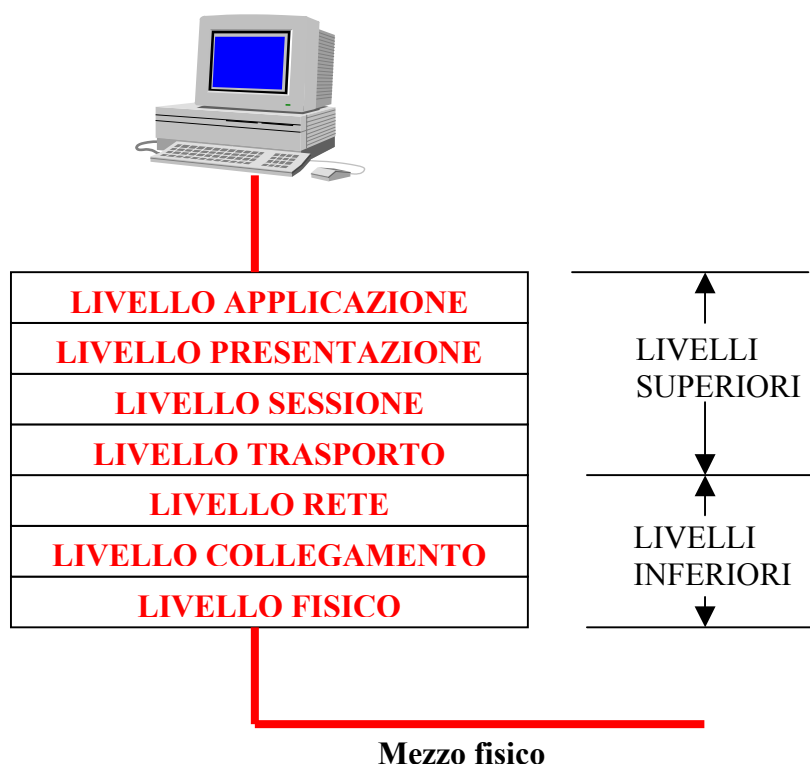


Figura 3.2. La struttura in livelli del modello OSI.

La struttura del modello, indicata anche con il nome di pila OSI, è mostrata nella Figura 3.2. Ciascun livello svolge compiti ben precisi ed interagisce con gli altri livelli mediante procedure definite ed universali. Ogni livello contiene:

- le **entità** che rappresentano gli elementi attivi di ogni livello e possono risultare sia di tipo software (ad esempio un processo), sia di tipo hardware (ad esempio un dispositivo di I/O). Ogni livello è composto da una o più entità.
- I **punti di accesso al servizio**, indicati con il simbolo **SAP (Service Access Point)**.

Lo scopo di ciascun livello è di fornire in modo trasparente servizi alle entità di livello superiore. Le entità del livello  $n$  forniscono perciò in modo trasparente servizi utilizzati dal livello  $n+1$ , ovvero senza che il livello  $n+1$  debba intervenire nelle operazioni svolte dal livello  $n$ . Il livello  $n$  è definito **fornitore di servizio** ed il livello  $(n+1)$  è denominato **utente del servizio**.

I servizi forniti dal livello  $n$  sono disponibili per il livello  $(n+1)$  nei SAP del livello  $n$ . Ciascun SAP ha un *indirizzo che lo identifica in modo univoco*. Per chiarire le idee consideriamo l'analogia con la rete telefonica: in questa analogia i SAP possono essere rappresentati dalle prese in cui sono inseriti i telefoni e l'indirizzo dei SAP dai numeri di quei telefoni. Le entità usano e forniscono i servizi tramite i SAP come mostrato nella Figura 3.3.

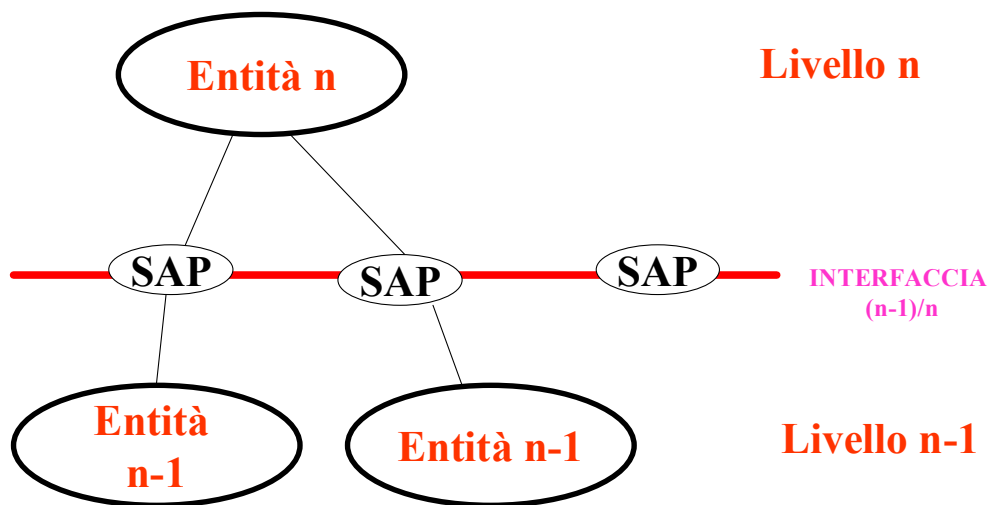


Figura 3.3. Realizzazione di servizi mediante le SAP tra il livello  $(n-1)$  e il livello  $n$ .

Due livelli possono scambiarsi informazioni se sono stabilite un insieme di regole relative al modo di operare dell'**interfaccia**. L'interfaccia definisce perciò quali operazioni primitive e quali servizi sono forniti da un livello superiore ad un livello inferiore.

Il livello  $n$  riceve dati dal livello superiore ed aggiunge una serie di dati di controllo, come mostrato nella Figura 3.4, in cui sono considerati il processo che trasmette i dati e il processo che li deve ricevere

Il processo che trasmette fornisce i dati al livello di applicazione; quest'ultimo effettua due operazioni:

- Aggiunge l'intestazione di applicazione (AH=Application Header) senza introdurre nessuna modifica nei dati forniti dal processo trasmittente.
- Fornisce il nuovo messaggio (AH + i dati) al livello inferiore.

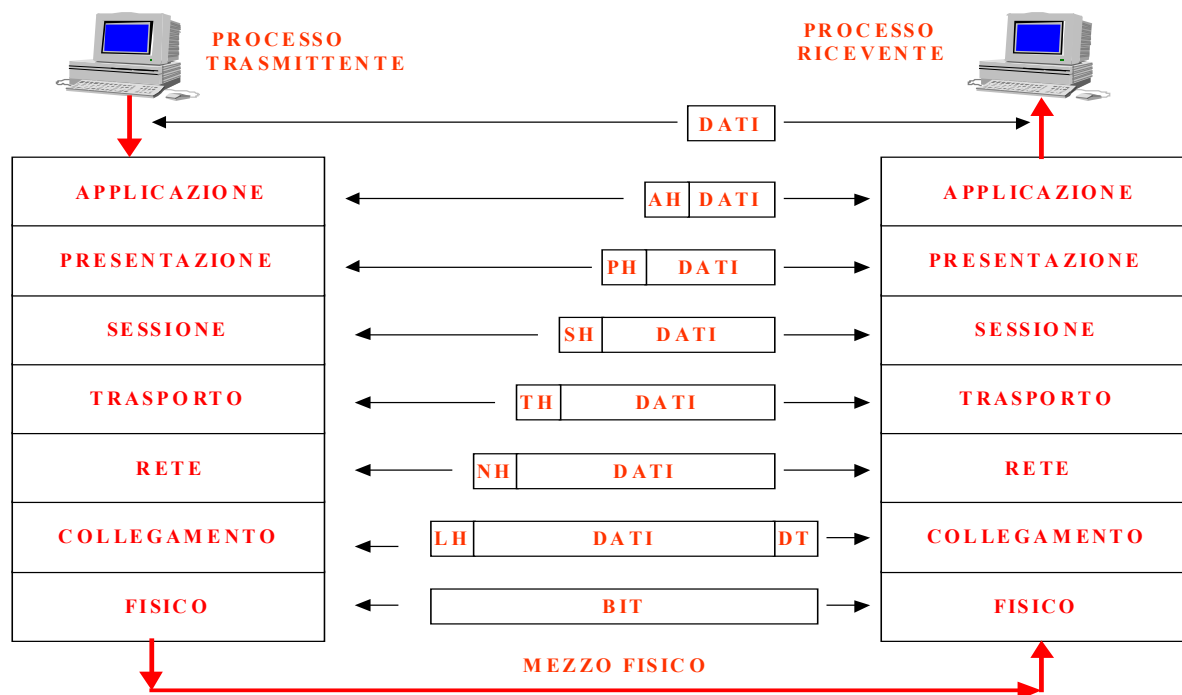


Figura 3.4. Gestione dei dati da parte dei livelli nel modello OSI.

Il processo si ripete in modo simile nei livelli successivi. Il livello  $n$  riceve i dati dal livello  $n+1$ , aggiunge un'intestazione senza modificare i dati provenienti dal livello superiore e passa il nuovo messaggio al livello inferiore. In questo modo il livello  $n$  non distingue tra i dati a livello  $n+2$  e l'intestazione aggiunta dal livello  $n+1$ . Nel livello 2 viene aggiunta anche una sequenza in coda per il controllo d'errore. Il livello fisico (livello 1) non aggiunge nessuna informazione ma trasforma i dati provenienti dal livello 2 in una sequenza di simboli. In ricezione il livello  $n$  analizzerà la testata introdotta in trasmissione dal livello corrispondente ed utilizzerà questi simboli per effettuare una serie di operazioni e controlli, dopodiché eliminerà la sua testata e passerà i "dati" al livello superiore.

Il concetto base nella struttura OSI è che *ciascun livello opera come se la trasmissione avvenisse in orizzontale* e quindi il livello  $n$  in ricezione interagisce solo con il livello  $n$  in trasmissione, utilizzando soltanto le informazioni aggiunte da quest'ultimo. In questo modo i livelli sono indipendenti ed isolati. *Questa struttura consente di cambiare un livello, ad esempio modificando i protocolli di tale livello, senza dover introdurre cambiamenti negli altri livelli.*

I dati generati dal protocollo di livello  $n$  sono detti **PDU (Protocol Data Unit)** del livello  $n$  (o  $n$ -PDU). Una volta attraversata nei SAP l'interfaccia tra il livello  $n$  ed il livello  $n-1$ , essi diventano una **SDU (Service Data Unit)** del livello  $n-1$  e sono indicati con  $(n-1)$ -SDU come mostrato nella Figura 5. Nell'ambito del livello  $(n-1)$  l'unità **PCI (Protocol Control Information)**, indicata anche come  $(n-1)$ -PCI, genera dei dati, che costituiscono l'header, del livello  $(n-1)$ . L'insieme dei dati  $(n-1)$ -PCI e  $(n-1)$ -SDU formano i dati da passare al livello inferiore.

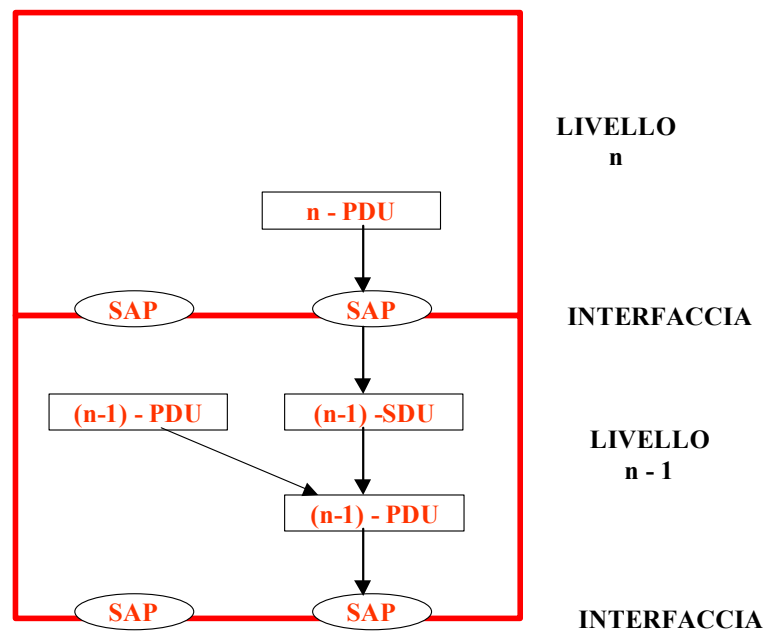


Figura 3.5. Gestione dei dati tra i livelli.

I sette livelli del modello OSI sono spesso divisi in due classi (Figura 3.2):

- **Protocolli di rete o di livello inferiore:** corrispondono ai primi tre livelli (fisico, link, network) e riguardano la rete di comunicazione; il compito di questi livelli è di far arrivare le informazioni al processo destinazione in modo corretto.
- **Protocolli di livello superiore:** corrispondenti ai 4 livelli superiori (trasporto, sessione, presentazione ed applicazione); questi livelli devono assicurare che i dati consegnati a destinazione siano correttamente interpretabili.



Figura 3.6 - Schema generale di un sistema di trasmissione dati.

Lo schema generale di un sistema per il trasferimento delle informazioni tra due terminali è mostrato nella Figura 3.6, in cui sono evidenziati i principali blocchi. I due calcolatori rappresentano i due sistemi finali (quello di trasmissione e di ricezione), mentre il nodo di rete (in generale saranno più di uno) serve a realizzare il collegamento tra i due sistemi. Nei due calcolatori devono essere presenti tutti i sette livelli del modello OSI, mentre nei nodi di comunicazione devono essere presenti soltanto i livelli che supportano il trasferimento dell'informazione sulla rete, cioè i primi tre livelli, come mostrato nella Figura 3.7. In alcuni casi il nodo della rete ha solo il livello 1 oppure solo i primi due livelli.



### 3.3. Servizi senza connessione o con connessione

I protocolli e i servizi dei diversi livelli OSI possono essere definiti con due modalità diverse:

- Modalità senza connessione.
- Modalità con connessione.

#### *Modalità con connessione*

Nella modalità con connessione lo scambio di dati è organizzato in tre fasi:

- 1 creazione della connessione tra le due stazioni;
- 2 trasferimento dei dati;
- 3 abbattimento del collegamento.

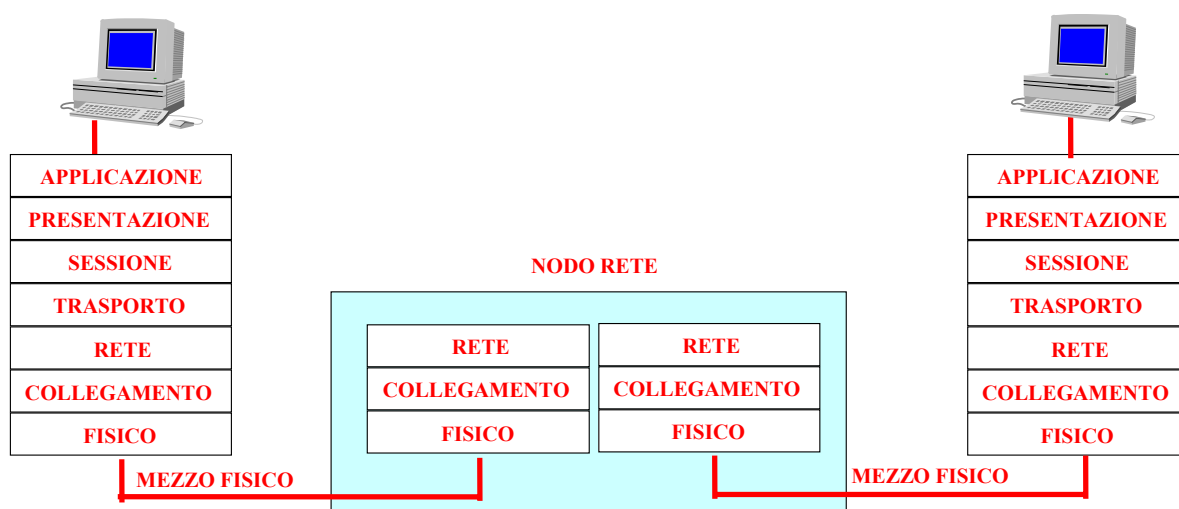


Figura 3.7 - Livelli OSI per i diversi componenti del sistema di trasmissione dati.

Questa tecnica è molto simile da un punto di vista concettuale a quella utilizzata nella telefonia. Durante la prima fase, la stazione chiamante deve specificare *gli indirizzi del mittente e del destinatario*. Alla fine di questa fase *viene realizzato un collegamento fisico* tra le due stazioni, che sarà utilizzato per il trasferimento di tutti i dati tra queste. Nella seconda fase le entità coinvolte dovranno specificare soltanto l'identificativo della connessione stabilita nella prima fase. Nella modalità con connessione le PDU sono ricevute nello stesso ordine con cui sono trasmesse. Alla fine della trasmissione, il sistema provvede ad abbattere il collegamento.

Le fasi di creazione ed abbattimento del collegamento possono introdurre ritardi significativi nella trasmissione di dati, specialmente se i dati da trasferire hanno una lunghezza limitata.

### Modalità senza connessione

Nella modalità senza connessione (o *datagram*) ogni pacchetto dati PDU segue un percorso autonomo nella rete; per questo ogni PDU deve contenere l'indirizzo del destinatario (e nella maggior parte dei casi anche del mittente). I pacchetti che formano un messaggio possono seguire strade diverse nella rete per raggiungere il ricevitore e possono perciò verificarsi i seguenti inconvenienti:

- i pacchetti di uno stesso messaggio possono avere ritardi diversi;
- i pacchetti possono essere ricevuti in ordine diverso da quello di trasmissione. Per questo motivo il ricevitore deve memorizzare i pacchetti ricevuti in un buffer e ristabilire l'ordine temporale dei pacchetti.

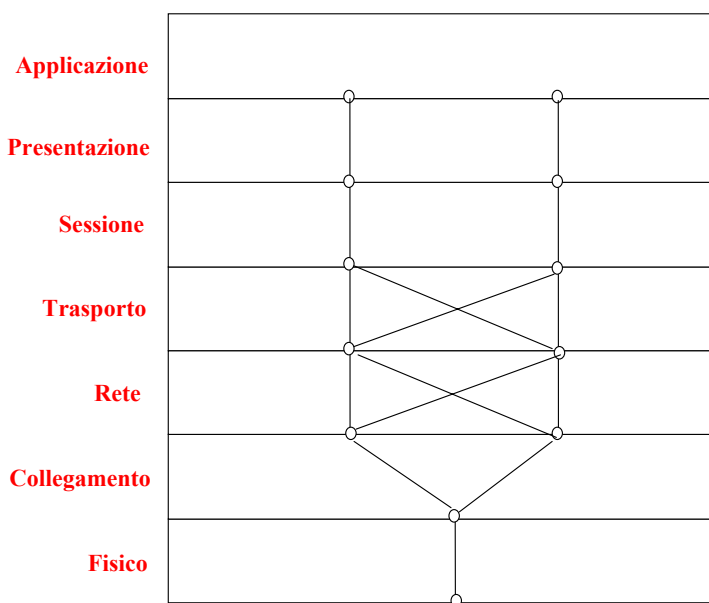


Figura 3.8. Scelte tra i servizi con e senza connessione.

### Confronti tra la modalità con e senza connessione

Lo standard OSI prevedeva inizialmente un servizio orientato alla connessione. Successivamente, a causa di discussioni e posizioni discordanti su questa problematica, l'ISO introdusse una modifica nello standard per includere ambedue i tipi di servizio. La scelta tra le due modalità di connessione deve essere fatta in tutti e tre i livelli, di collegamento, di rete e di trasporto, per cui alcuni livelli possono essere con connessione ed altri senza connessione. Nel modello OSI alla sommità di ciascuno dei livelli 2,3 e 4 esistono due SAP attraverso i quali il livello superiore può accedere ai servizi, che possono essere orientati alla connessione o senza connessione. La scelta tra i due può essere effettuata in uno qualunque dei SAP, come mostrato nella Figura 3.8. Si possono ottenere perciò varie possibilità e tipologie di servizi.

### 3.4 Livelli OSI

Il modello OSI specifica le attività e le operazioni che ogni livello deve effettuare, ma non definisce i servizi e i protocolli da utilizzare in ciascun livello. Per questo motivo *il modello*

OSI non è un'architettura di rete. In questo paragrafo descriviamo le principali caratteristiche di ogni livello.

## Livello fisico

Il livello fisico riguarda la trasmissione di bit attraverso il canale di comunicazione e specifica perciò le modalità di trasmissione dei simboli (bit) e le caratteristiche dei segnali utilizzati per trasmetterli (Figura 3.9)

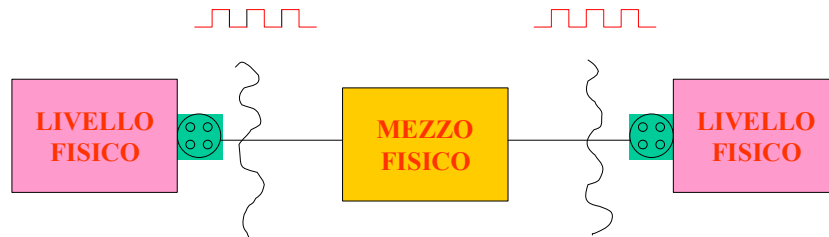


Figura 3.9 . Livello fisico.

Le due parti che colloquiano devono utilizzare gli stessi segnali, codici di linea e lo stesso tipo di modulazione. In particolare, i principali aspetti definiti dal livello fisico sono:

- le forme d'onda utilizzate per trasmettere i simboli;
- durata temporale di ciascun simbolo;
- regole per l'attivazione e la disattivazione del collegamento fisico tra due punti;
- caratteristiche dei cavi e dei connettori;
- interfaccia tra il DTE (Data Terminal Equipment) e il DCE (Data Communication Equipment);
- operazione di multiplazione;
- operazioni di modulazione.

### Interfaccia tra DTE e DCE

Gli aspetti progettuali a livello fisico riguardano essenzialmente le interfacce meccaniche, elettriche, procedurali e con il mezzo fisico di trasmissione, situato al di sotto del livello fisico.

Un esempio di protocollo del livello fisico è rappresentato dallo standard **EIA RS-232-C**, che con piccole modifiche è stato adottato successivamente dal CCITT con lo standard **V.24**. Esso definisce l'interfaccia elettrica, meccanica e funzionale tra il DTE e il DCE, in questo caso rappresentato da un modem. Lo standard RS-232 è stato adottato per velocità inferiori a 20 Kbit/s e per lunghezze del cavo tra DTE e DCE inferiori a 15 m; con l'evoluzione della tecnologia è stato sviluppato un nuovo standard nel caso di collegamenti mediante modem per tenere conto di sistemi a velocità superiori. Il nuovo standard, emanato dall'EIA, è indicato con la sigla **RS-449** ed è in realtà composto da tre standard:

- **RS-449**, che specifica le interfacce elettriche, meccaniche, funzionali e procedurali;

- **RS-423-A**, che specifica l'interfaccia elettrica. Questo standard utilizza una trasmissione sbilanciata, come nel RS-232-C, in cui tutti i circuiti condividono una massa elettrica comune.
- **RS-422-A**, che specifica l'interfaccia elettrica nel caso di trasmissione bilanciata, in cui ciascuno dei circuiti principali di collegamento tra DTE e DCE utilizza due fili senza una massa comune. In questo modo è possibile ottenere velocità fino a 2Mbit/s con un cavo di lunghezza massima uguale a 60 m.

### *Interfaccia digitale X.21*

Lo standard **X.21**, emanato nel 1976 dal CCITT, definisce l'interfaccia tra DTE e DCE nel caso di linee di comunicazioni digitali.

### **Livello di *data link* o di collegamento dati**

Il livello di *data link* organizza una struttura nei dati trasmessi dividendoli in **frame** o trame e provvede alla trasmissione in modo corretto di tali frame. Le principali funzioni svolte da questo livello sono:

- *suddivide in frame i bit forniti dal livello fisico;*
- *controlla la presenza di errori e può gestire meccanismi di correzione di tali errori;*
- *regola il flusso in trasmissione in modo che un ricevitore lento non risulti sommerso dai dati provenienti da un trasmettitore veloce.*
- *fornisce una serie di differenti classi di servizio al livello di rete.*

### *Suddivisione in frame*

I bit forniti dal livello fisico possono contenere errori, oppure il numero di bit ricevuti può essere diverso da quelli trasmessi. Il livello di data link ha lo scopo di rivelare e correggere questi errori. Per ottenere questi risultati, è necessario introdurre una struttura nei bit mediante la loro suddivisione in frame. Esistono vari metodi per dividere i dati in frame; nel seguito descriviamo i metodi più utilizzati.

### *Conteggio dei caratteri*

Nell'intestazione del frame viene inserito un campo che specifica il numero di caratteri che costituiscono il frame (Figura 3.10a). Attraverso tale informazione il livello di data link al ricevitore può determinare la lunghezza del frame ricevuto. Tuttavia, questo sistema è molto sensibile agli errori introdotti dal canale di comunicazione; infatti se un errore altera il campo iniziale di un frame il ricevitore perde il sincronismo e questa perdita si propaga ai frame successivi (Figura 3.10b).

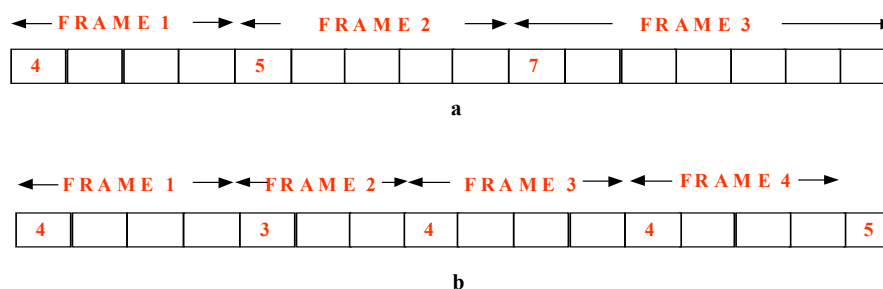


Figura 3.10 – Metodo di conteggio dei caratteri per delimitare il frame :  
a) suddivisione in frame; b) ricostruzione errata dei frame a causa di un errore.

### Introduzione dei caratteri di inizio e di fine frame

In questo sistema sono introdotti dei caratteri ASCII all'inizio ed alla fine del frame; il frame ha inizio con i due caratteri DLE STX, mentre termina con i caratteri DLE ETX. Naturalmente può accadere che i caratteri DLE STX o DLE ETX si presentino casualmente tra i dati e quindi si verifichino incertezze sull'inizio o la fine di un frame. Per ovviare a questo problema, il livello di collegamento inserisce un carattere DLE prima di un carattere DLE presente nei dati (Figura 3.11). Questo carattere sarà rimosso dal livello di collegamento in ricezione. Utilizzando questa tecnica non si ha più perdita di sincronismo, in quanto ciascun frame è un'entità individuata in modo autonomo.

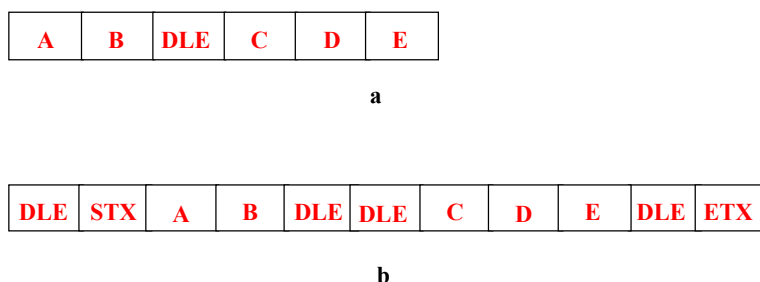


Figura 3.11. Formazione del frame mediante caratteri di inizio e fine: a) dati; b) frame.

### Tecnica di bit stuffing

La tecnica di riferimento dei bit (detta anche di **bit stuffing**) è la più usata nelle moderne reti di telecomunicazioni. In questa tecnica ogni frame inizia e termina con la sequenza di bit 01111110. Per evitare che queste sequenze siano confuse con dati informativi, il livello di collegamento analizza i bit informativi e se incontra cinque bit uguali ad 1 inserisce uno 0 (Figura 3.12).

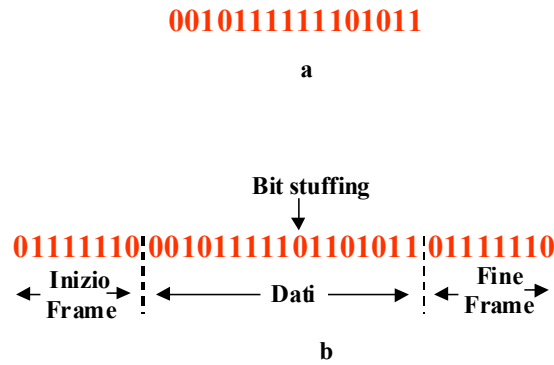


Figura 3.12. Esempio della tecnica di riempimento dei bit.

### Controllo degli errori

Un'operazione particolarmente importante realizzata dal livello di collegamento è il controllo della correttezza dei frame ricevuti. Durante la trasmissione possono verificarsi varie situazioni che producono errori alla stazione di ricezione A:

- un frame è ricevuto affetto da errori;
- un frame trasmesso viene perduto nella rete (ad esempio per un overflow in un buffer o per un errore nel campo che contiene l'indirizzo A della stazione ricevente);
- un frame viene ricevuto dalla stazione A anche se indirizzato ad un'altra stazione (a causa di un errore nel campo di indirizzo della stazione di ricezione).

Per ovviare a questi inconvenienti e garantire un'affidabilità ai dati che saranno forniti a livello di rete, il livello di collegamento contiene alcuni protocolli per il controllo degli errori. Tali protocolli utilizzeranno i seguenti meccanismi:

- il livello di collegamento in ricezione invia un riconoscimento positivo o ACK (acknowledgment) al trasmettitore per ogni frame ricevuto correttamente, oppure un riscontro negativo o NACK (negative acknowledgment) nel caso opposto. In quest'ultimo caso il trasmettitore deve inviare nuovamente il frame;
- il livello di collegamento in trasmissione contiene un timer, che viene attivato ogni volta che viene trasmesso un frame. Il timer è impostato per scadere dopo un tempo prefissato (generalmente il tempo di andata e ritorno del segnale più il tempo di elaborazione del frame). Se il frame o il riconoscimento (ACK o NACK) sono perduti nella rete, il trasmettitore invierà nuovamente il frame alla scadenza del tempo prefissato per il timer.

La rivelazione degli errori e i protocolli con il controllo delle ritrasmissioni (o protocollo ARQ) sono descritti in un capitolo precedente.

### Controllo del flusso

Il controllo del flusso informativo tra due computer, che possono avere velocità e caratteristiche diverse, è molto importante per il corretto funzionamento del collegamento, perché la velocità di invio di dati del trasmettitore deve essere adattata a quella del ricevitore. Il controllo di flusso avviene mediante un meccanismo di retroazione, in cui il ricevitore invia informazioni al trasmettitore sul numero di frame che ha elaborato.

### *Servizi forniti al livello di rete*

Il principale servizio è il trasferimento dei dati al livello superiore di rete. Tuttavia le modalità di esecuzione del servizio possono variare da sistema a sistema e possono essere divisi in:

- *Servizio senza connessione o senza riscontro*  
Non viene effettuata nessuna connessione in anticipo e il ricevitore non invia riconoscimenti (ACK o NACK) al trasmettitore sui frame ricevuti, per cui i frame sono accettati così come sono ricevuti. Questo sistema è adottato a linee con bassa probabilità di errore.
- *Servizio senza connessione e con riscontro*  
Il ricevitore invia un riconoscimento (ACK o NACK) per ogni frame e si utilizza un protocollo ARQ per la ritrasmissione dei frame ricevuti errati.
- *Servizio orientato alla connessione*  
Questo servizio è generalmente il più sofisticato e richiede che il trasmettitore e ricevitore identifichino un canale di comunicazione prima di attivare lo scambio dei dati.

### *Descrizione di alcuni protocolli del livello di collegamento dati per reti geografiche*

I principali protocolli di livello 2 nelle reti geografiche a commutazione di pacchetto sono :

- SDLC (Synchronous Data Link Control), protocollo sviluppato da IBM per la rete SNA;
- HDLC (High Level Data Link Control);
- LAP (Link Access Procedure);
- LPAB (Link Access Procedure Balanced);
- LAPD (Link Access Procedure D-Channel);
- LAPF (Link Access Procedure to Frame mode bearer services);
- LLC (Logical Link Control).

Questi protocolli sono molto simili tra loro; tuttavia, *lo standard OSI utilizza in modo esplicito il protocollo HDLC*. In questi protocolli le modalità di scambio di informazioni possono essere notevolmente diverse a seconda della configurazione del collegamento. I possibili modi operazionali possono essere divisi in due categorie:

- *Connessione bilanciata*; in questo caso il numero di stazioni è limitato a due e si riferisce perciò a collegamenti punto-punto. Viene utilizzato il modo operativo *ABM (Asynchronous Balanced Mode)*, che definisce un collegamento full-duplex, in cui entrambe le stazioni possono iniziare a trasmettere senza attendere alcuna autorizzazione reciproca. Il protocollo LAPB consente soltanto questa modalità di connessione.
- *Connessione sbilanciata*; questa procedura è tipica dei collegamenti multipunto con controllo centralizzato, in cui esiste una stazione primaria che gestisce il flusso dei dati e controlla la correzione degli errori. La stazione primaria emette degli ordini e riceve delle risposte. Esistono due diversi modi di operazione:
  - ❑ *NRM (Normal Response Mode)*: in cui una stazione secondaria risponde soltanto se interrogata (polling) dalla stazione primaria;
  - ❑ *ARM (Asynchronous Response Mode)*: in cui una stazione secondaria può iniziare a trasmettere in qualsiasi momento, anche se non interrogata dalla stazione

principale. Questa soluzione può provocare facilmente contese tra le stazioni secondarie.

Il formato del frame HDLC, che tuttavia è uguale a quello degli altri protocolli, è mostrato nella Figura 3.13. Descriviamo in dettaglio la funzione dei diversi campi presenti nel frame.

FLAG	INDIRIZZO	CONTROLLO	DATI	FCS	FLAG
------	-----------	-----------	------	-----	------

Figura 3.13. Formato del frame HDLC.

### Campo Flag

I due campi **FLAG** all'inizio e alla fine del frame servono ad identificare l'inizio e la fine del frame; essi contengono la sequenza di 8 bit 01111110. Il protocollo HDLC usa la tecnica di bit stuffing per evitare che nell'interno del campo dei dati possa comparire una sequenza uguale a quella utilizzata per i flag.

### Campo indirizzo

Il campo indirizzo, lungo 1 byte, contiene l'indirizzo della stazione ricevente; nel caso di un frame di risposta contiene l'indirizzo della stazione che sta rispondendo.

### Campo controllo

Il campo di controllo ha una lunghezza di 1 o 2 byte e viene utilizzato per vari scopi. In particolare esistono tre diversi formati di tale campo:

- *Frame Informativo o I-Frame*; servono a trasportare le informazioni dell'utente (i pacchetti forniti dal livello superiore). Il formato del campo di controllo è mostrato nella Figura 3.14a. La correzione degli errori viene effettuata in HDLC mediante una tecnica a rivelazione d'errore (ARQ) del tipo Go-Back-N. Il protocollo utilizza una finestra scorrevole di 3 bit e quindi possono essere presenti nel sistema fino a 7 frame non confermati. Il *campo NS* indica il numero di sequenza del frame, mentre il *campo NR* rappresenta il numero della trama confermata positivamente (ultima trama ricevuta correttamente). Il *campo P/F (Poll/Final)*, formato da 1 bit, serve per effettuare l'interrogazione ciclica (polling) di un gruppo di terminali. Se il bit è posto uguale a P, il computer che invia la trama sta invitando il terminale ad inviare i dati. Tutti i frame inviati dal terminale hanno il bit uguale a P, tranne l'ultimo frame in cui il bit è posto uguale a F.
- *Frame di Supervisione o S-Frame*; servono a fornire una serie di informazioni per la gestione del collegamento; non contengono il campo dati. Il formato del campo di controllo è mostrato nella Figura 3.14.b. Il *campo Tipo*, composto di 2 bit, serve a distinguere vari tipi di frame di supervisione:
  - RR (Receiver Ready): frame utilizzato per fornire un ACK in assenza di traffico; in presenza di traffico la conferma positiva viene inviata nel campo di controllo della trama informativa (tecnica di piggybacking).
  - RNR (Receiver Not Ready): questo frame viene utilizzato per indicare che la stazione non è momentaneamente in grado di ricevere nuove informazioni a causa di qualche problema. Quando il ricevitore è nuovamente operativo invia un frame RR.



- ❑ REJ (REject): questo frame viene utilizzato per richiedere la ritrasmissione di tutti i frame già trasmessi a partire da quello NR.
- ❑ SREJ (Selective REject): questo frame richiede la ritrasmissione del solo frame NR. Questo frame è presente in HDLC, ma non è supportato da LAPB.
- *Frame non numerato o U-Frame*; sono frame utilizzati per il controllo del collegamento e non contengono il campo dati. I vari protocolli orientati al bit differiscono soprattutto in questa parte. Il formato del campo di controllo è mostrato nella Figura 3.14c. Sono disponibili vari tipi di U-Frame definiti in base al valore del campo type (2 bit) e del campo Modificatore (3 bit). Descriviamo i principali tipi di U-Frame:
  - ❑ DISC (DISConnect): frame utilizzato per la disattivazione di una macchina.
  - ❑ SABM (Set Asynchronous Balanced Mode): frame utilizzato per inizializzare una connessione bilanciata full duplex tra due stazioni. Questa modalità di trasmissione è l'unica presente in LAPB. Viene utilizzata una finestra di 3 bit per la conferma dei frame ricevuti.
  - ❑ SABME (Set Asynchronous Balanced Mode Extended): è analoga alla precedente, ma viene utilizzata una finestra di 7 bit.
  - ❑ SNRM (Set Normal Response Mode): frame utilizzato per inizializzare una connessione sbilanciata o asimmetrica; la finestra di controllo è su 3 bit.
  - ❑ SNRME (Set Normal Response Mode Extended): frame analogo al precedente, in cui la finestra di controllo è basata su 7 bit.
  - ❑ UI (Unnumbered Information): trama utilizzata per inviare i dati in modalità non connessa.
  - ❑ UA (Unnumbered Acknowledge): frame utilizzato in risposta ad altri U-Frame, quali SABM, SABME, DISC,....
  - ❑ FRMR (FraME Reject): indica che è stato ricevuto un frame in cui il controllo d'errore è soddisfatto, ma che presenta altri problemi (ad esempio, lunghezza inferiore a 32 bit, frame di controllo illegale,...) per cui il frame non è accettabile.
  - ❑ DM (Disconnect Mode): frame che conferma la ricezione di un messaggio DISC.

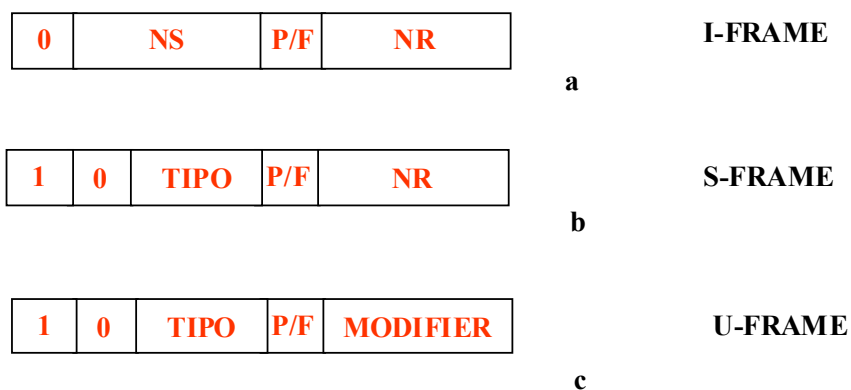


Figura 3.14. Formato del frame di controllo in HDLC : a. I-Frame; b. S.Frame; c. U-Frame

### Campo Dati

Il campo dati è usato per trasportare l'informazione e può essere arbitrariamente lungo. Esso contiene il pacchetto fornito dal livello superiore.

## Campo FCS

Il campo FCS, composto da 2 o 4 byte, contiene la ridondanza di un codice ciclico per rivelare eventuali errori introdotti dal canale di comunicazione. Il codice può avere 16 o 32 bit di ridondanza. La scelta del codice e quindi la ridondanza da utilizzare viene decisa dalle stazioni mediante opportuni messaggi.

## Esempio

Descriviamo attraverso un esempio molto semplice l'uso del protocollo HDLC considerando il caso in cui due sistemi DTE1 e DTE2 si devono scambiare informazioni mediante una rete a commutazione di pacchetto di tipo X.25 (Figura 3.15a). Nella Figura si considerano due DTE, ma la stessa procedura viene effettuata anche tra nodi della rete.

- *Fase di costruzione del collegamento*

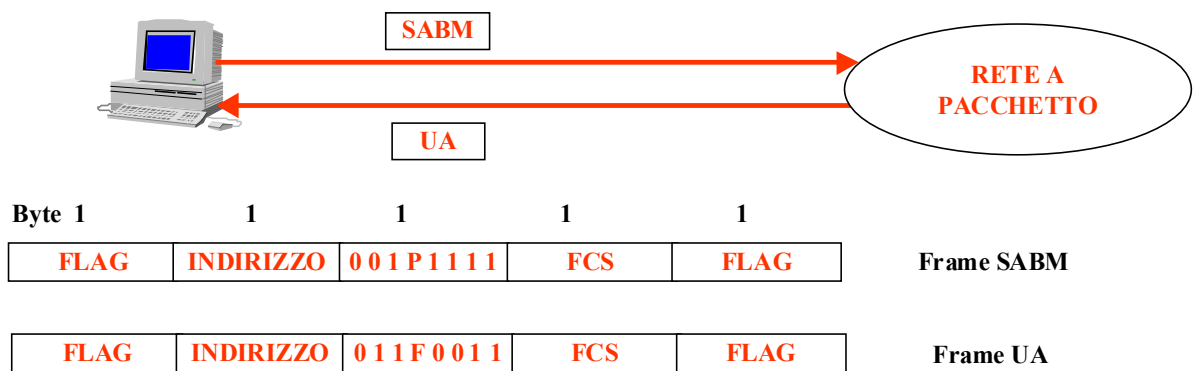
Il terminale DTE1 invia in primo luogo un U-Frame SABM per indicare una richiesta di trasmissione indicando nel campo "indirizzo" l'indirizzo della stazione con cui si vuole connettere. La rete, nel caso in cui la richiesta possa essere soddisfatta, invia un frame UA di controllo che fornisce una risposta affermativa (Figura 3.15a).

- *Fase di trasferimento dell'informazione*

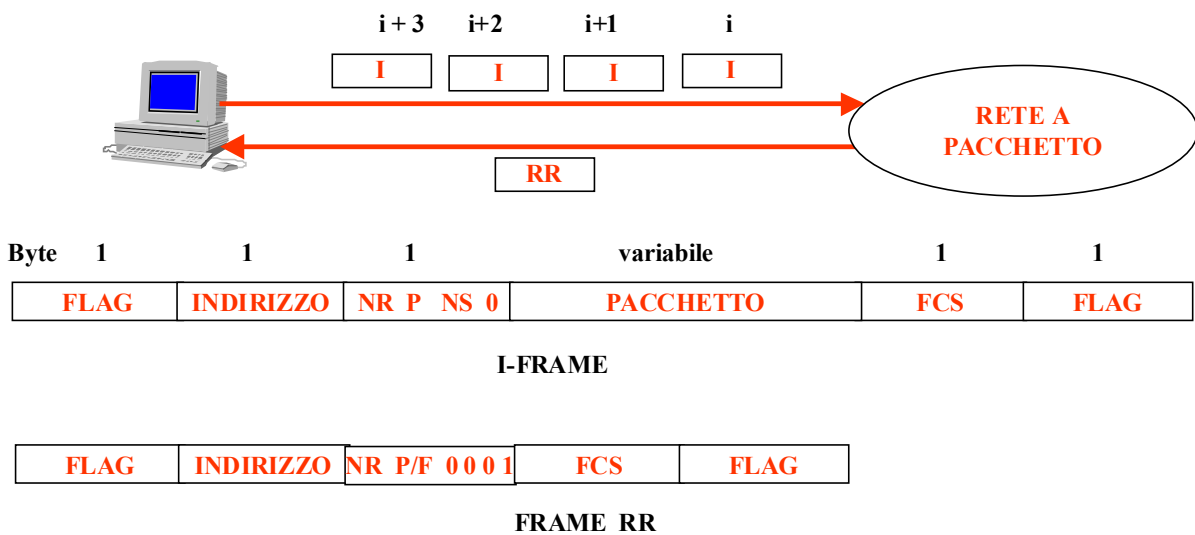
Il DTE1 inizia ad inviare frame informativi numerati da 0 a 7. Consideriamo ad esempio il caso in cui il DTE1 deve inviare il frame  $i$  e che tutti i precedenti frame siano stati correttamente confermati. Il DTE1 (o il nodo della rete) invia un I-frame che nel campo di controllo contiene  $NS=0$  e successivamente continua a trasmettere gli altri frame, se presenti, con valori di  $NS$  crescenti. Nella Figura 3.15b si suppone che il DTE1 trasmetta altri tre frame, indicati con  $i+1$ ,  $i+2$  e  $i+3$ . Il DTE2 invierà ad un certo istante una trama RR (Receiver Ready) contenente il numero  $i+4$ ; questo indica che i pacchetti fino a  $i+3$  sono stati ricevuti correttamente. Nel caso in cui uno dei pacchetti non sia ricevuto correttamente il DTE2 può inviare una trama REJ per richiedere la ritrasmissione del pacchetto e dei successivi (strategia Go-Back-N con finestra  $N=7$ ).

- *Fase di abbattimento del collegamento*

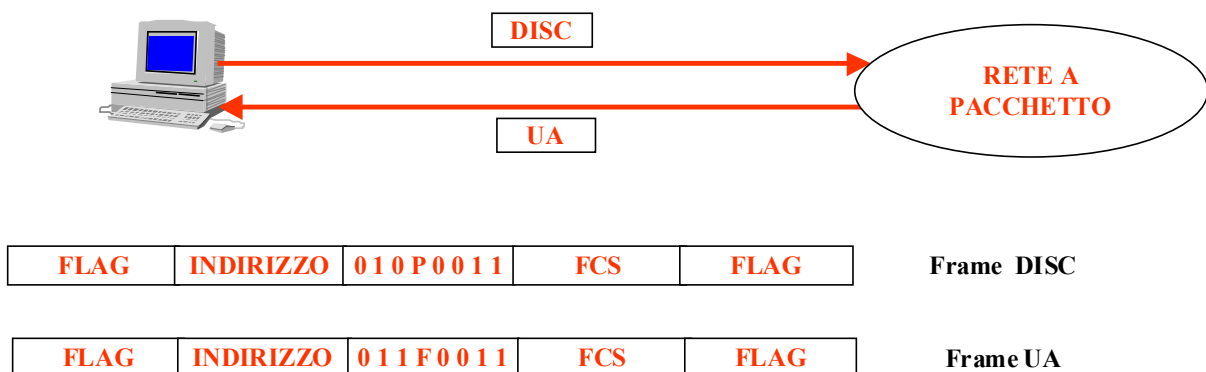
Alla fine del trasferimento dati, il DTE1 invia la trama DISC, che segnala l'abbattimento del collegamento, e il DTE2 risponde con una trama UA (Figura 3.15c).



a



b



c

Figura 3.15 – Esempio di funzionamento del protocollo X.25.

## Livello di rete

Il livello di rete gestisce l'instradamento dei messaggi attraverso la rete scelta dal livello di trasporto. Le funzioni principali svolte dal livello di rete sono le seguenti:

- *servizi offerti al livello di trasporto;*
- *multiplazione di due o più flussi di dati sullo stesso circuito fisico;*
- *instradamento o (routing) dei dati dalla stazione di partenza a quella di arrivo.*  
*L'instradamento può avvenire mediante due tecniche diverse:*
  - a. **circuiti virtuali**, in cui tutti i pacchetti utilizzano lo stesso percorso;
  - b. **datagram**, in cui i pacchetti possono utilizzare percorsi diversi.
- *controllo della congestione della rete;*
- *interconnessione di reti.*

### *Instradamento o routine*

Il protocollo di instradamento serve a scegliere il cammino su cui inviare un pacchetto per farlo arrivare alla stazione di destinazione. Nel caso in cui la rete operi con una tecnica datagram la scelta del cammino deve essere effettuata per tutti i pacchetti. Nel caso di circuiti virtuali, la scelta del cammino è effettuata soltanto nella fase di attivazione del collegamento.

Gli algoritmi di instradamento possono influenzare in modo significativo le prestazioni di una rete. I principali parametri che caratterizzano un algoritmo di instradamento sono:

- la semplicità;
- la robustezza, in presenza di guasti o malfunzionamenti;
- la stabilità;
- la minimizzazione del ritardo incontrato nell'attraversare la rete.

Gli algoritmi di instradamento possono essere divisi in due classi:

- algoritmi non adattabili, in cui il percorso per collegare due nodi è calcolato in anticipo;
- algoritmi adattabili, in cui il percorso per collegare due nodi viene deciso in base a misure o stime del traffico presente nella rete. Questi algoritmi presentano, in linea teorica, prestazioni ottimali, ma sono spesso complessi.

### *Congestione*

Quando il traffico all'ingresso di una rete è troppo elevato, le prestazioni della rete possono degradare rapidamente, determinando una congestione della rete stessa. Nella Figura 3.16 sono mostrate diverse situazioni in cui può trovarsi una rete. Definiamo time-slot la durata temporale di un pacchetto. Nella Figura 3.16 è riportato il traffico utile (throughput) all'uscita della rete in funzione del carico  $S$  (n.pacchetti/time-slot) all'ingresso della rete. In una rete ideale il throughput è uguale a quello in ingresso fino a quando  $S \leq 1$ , mentre si mantiene uguale a 1 per  $S \geq 1$ . I protocolli reali hanno ovviamente un comportamento diverso e all'aumentare del traffico possono innescarsi facilmente fenomeni di congestione della rete.

Per controllare il pericolo di congestione della rete sono stati sviluppati vari algoritmi basati su meccanismi di scarto dei pacchetti, sospensione di nuovi ingressi quando la rete è sovraccarica o mediante l'uso di algoritmi di controllo di flusso.

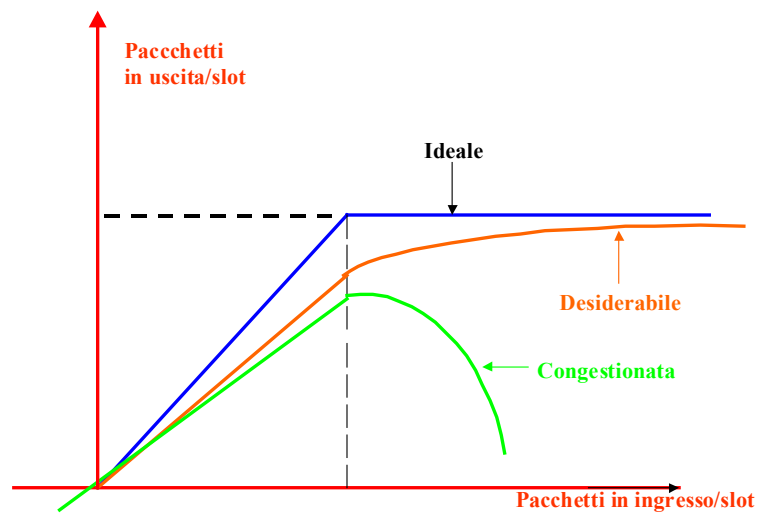


Figura 3.16. Vari comportamenti di una rete al variare del carico.

### Interconnessione di reti

L'interconnessione tra reti diverse (LAN, MAN, WAN,...) viene effettuata nel livello di rete.

### Livello di trasporto

Il livello di trasporto ha lo scopo di fornire un trasporto di dati affidabile, efficiente ed economico dalla macchina di partenza a quella di arrivo indipendentemente dalla rete utilizzata. Esso rappresenta il livello d'utente più basso e il primo livello che non si trova all'interno della rete, ma solo ai nodi terminali (Figura 3.7).

Il livello di trasporto effettua un *controllo end-to-end dei dati* per prevenire errori e malfunzionamenti e fornire perciò un servizio affidabile al livello di sessione.

Le principali funzioni svolte dal livello di trasporto sono:

- *servizi offerti al livello di sessione;*
- *definizione della qualità del servizio;*
- *rivelazioni e controllo di errori;*
- *controllo del flusso dei dati;*
- *segmentazione e assemblaggio dei dati;*
- *scelta della rete di trasporto.*

L'unità dei dati a questo livello non ha un nome specifico contrariamente ai due livelli precedenti (Figura 3.17).

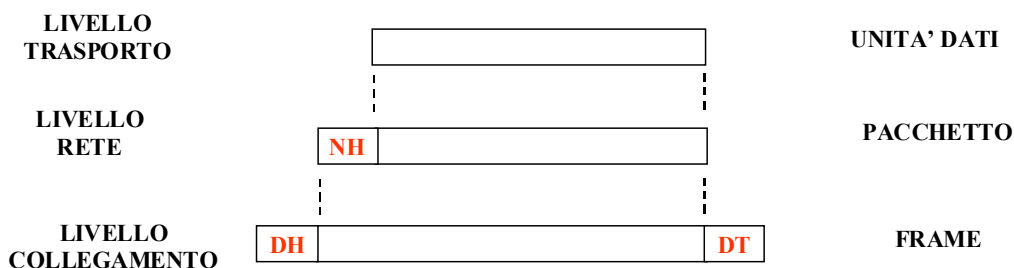


Figura 3.17. Le unità dati nei vari livelli.

### *Servizi forniti a livello di sessione*

I servizi forniti a livello di sessione possono essere divisi in:

- servizi orientati alla connessione;
- servizi senza connessione.

Ambedue questi servizi sono molto simili a quelli forniti a livello di rete. La necessità di introdurre questi due servizi anche nel livello di trasporto, oltre che in quello di rete, nasce dalla differente posizione dei due livelli; il livello di rete è posto nella rete di comunicazione e quindi la qualità del servizio dipende dal gestore di comunicazione nel caso di collegamenti su reti pubbliche. In questo modo l'utente non è in grado di controllare la qualità del servizio offerto dalla rete. Per ovviare a questo inconveniente, il livello di trasporto può consentire all'utente di scegliere la qualità di servizio.

### *Qualità di servizio*

Il livello di trasporto può migliorare la qualità di servizio (QoS) rivelando errori, pacchetti perduti o altri inconvenienti non rivelati dalla rete sottostante. La qualità di servizio può essere caratterizzata da un certo numero di parametri che possono essere specificati dall'utente. Il livello di trasporto deve determinare se le scelte dell'utente sono compatibili con le risorse disponibili e quindi se è in grado di fornire il servizio richiesto.

I principali parametri che caratterizzano la QoS di un servizio sono:

- Ritardo di attivazione di una chiamata  
Il tempo tra la richiesta di connessione da parte del livello di trasporto di trasmissione e la ricezione della conferma da parte del livello di trasporto di ricezione.
- Throughput
- Ritardo di transito
- Tasso errore residuo: Il tasso di errore residuo presente nei dati dopo il livello di trasporto in ricezione.
- Priorità: Indica la priorità da dare ad alcuni tipi di dati.
- Probabilità di fallimento del trasferimento

L'utente può specificare sia i valori desiderati, sia i valori minimi accettabili.

## Livello di sessione

Il livello di sessione è il più basso dei livelli di elaborazione e fornisce ai programmi applicativi un insieme di funzioni necessarie per la gestione ed il controllo di trasferimento dei dati.

Le principali funzioni svolte dal livello di sessione sono:

- *servizi offerti al livello di presentazione;*
- *formazione della connessione con un altro utente;*
- *sincronismo.*

La funzione principale svolta dal livello di sessione è quella di consentire agli utenti della sessione di stabilire una connessione tra loro, indicata con il termine **sessione**, e di trasferire dati tra loro. Una sessione può essere utilizzata per trasferire un file, per effettuare un collegamento di un terminale ad un computer, ....

### Sincronizzazione

Un servizio particolarmente importante svolto dal livello di sessione è la sincronizzazione del trasferimento dati tra due stazioni (quella di trasmissione e quella di ricezione).

Il sincronismo viene organizzato inserendo alcuni riferimenti facilmente riconoscibili detti **punti di sincronismo** nell'interno di un messaggio (Figura 3.18). Se durante una sessione si verificano dei problemi all'istante  $t$ , la sessione è in grado di essere ristabilita correttamente ripartendo dal punto di sincronismo precedente.



Figura 3.18. Inserimento dei punti di sincronismo in una sessione.

Gli standard internazionali prevedono due tipi di punti di sincronismo:

1. *punti principali di sincronismo*
2. *punti secondari di sincronismo.*

I dati sono generalmente divisi in *unità di dialogo*, ciascuna delle quali contiene dati indipendenti dalle altre unità. Un'unità di dialogo è individuata da due punti principali di sincronismo.

In molte applicazioni si introduce un'ulteriore struttura nei dati, considerando un insieme composto da varie unità di dialogo; tale insieme è chiamato *attività*.

Ogni attività è indipendente dalle altre. La struttura più generale di una sessione è perciò mostrata nella Figura 3.19.



Figura 3. 19. Organizzazione di una sessione.

I punti principali di sincronismo sono generalmente posti all'inizio e fine di ogni attività di dialogo. I punti secondari di sincronismo consentono di introdurre una struttura nei dati interni di unità di dialogo. L'introduzione di tali punti consente di ottimizzare la fase di recupero dei dati quando si verifica qualche inconveniente.

I punti principali di sincronismo sono particolarmente importanti ed il livello di sessione in ricezione provvede ad inviare una conferma per ogni punto principale al corrispondente livello di sessione del trasmettitore. In questo modo il trasmettitore è informato che le unità di dialogo fino a quella riscontrata positivamente possono essere scartate. Per i punti secondari di sincronismo non sono inviate conferme al trasmettitore.

Quando si deve effettuare una risincronizzazione è possibile ritornare indietro al massimo fino al punto principale di sincronismo precedente. Consideriamo ad esempio Figura 3.20. Una perdita di sincronismo tra i punti 12 e 13 può essere recuperata sincronizzandosi su 12, 11,10,9 o al massimo 8.

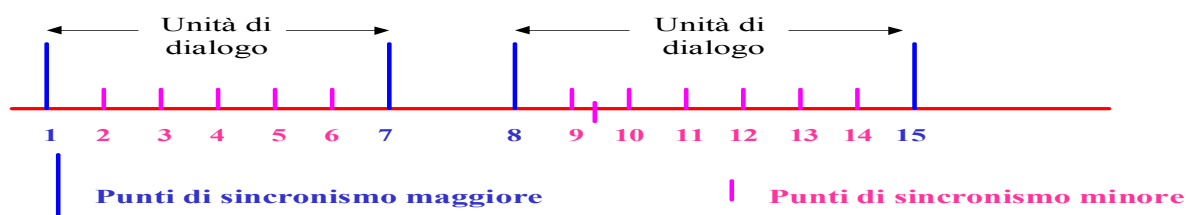


Figura 3.20. Punti di sincronismo maggiori e minori.

## Livello di presentazione

Il livello di presentazione ha il compito di consentire la corretta interpretazione dei dati scambiati tra due DTE indipendentemente dai codici, dai formati e da tutte le altre convenzioni impiegate da ciascun sistema. Per questo esso deve trasformare la rappresentazione dei dati interni del computer in una sequenza di bit adatti per essere trasmessi e in ricezione effettuare l'operazione opposta.

Il livello di presentazione svolge i seguenti servizi:

- *rappresentazione dei dati;*



- *compressione dei dati;*
- *cifratura dei dati.*

La compressione e la cifratura dei dati non saranno considerate in questo capitolo.

### *Rappresentazione dei dati*

I computer presentano diversi tipi di rappresentazione interna per i dati; perciò per far comunicare due computer è necessario effettuare un'opportuna conversione dei formati dei dati. Per questo ISO ha sviluppato uno standard noto come *notazione di sintassi astratta 1*, indicata con la sigla **ASN.1, (Abstrat Sytax Notation)** descritta nello standard 8824. Le regole per codificare le strutture di dati in una sequenza di bit da trasmettere sono specificate nello standard ISO 8825.

### **Livello di applicazione**

Il livello di applicazione contiene tutti i programmi di utente o **programmi applicativi** che consentono all'utente di svolgere le sue attività in rete. Questo livello contiene vari protocolli, tra cui i più importanti sono:

- *trasferimento, accesso e gestione dei file;*
- *posta elettronica;*
- *terminale virtuale.*

# Capitolo 4: I Protocolli IP e TCP

## 4.1. Introduzione

La rete Internet utilizza per il trasferimento dei dati un insieme di protocolli, di cui i più noti sono il **Transmission Control Protocol (TCP)** e l'**Internet Protocol (IP)**. L'insieme di questi protocolli consente di trasferire le informazioni attraverso un insieme di reti interconnesse ed è adatto per qualunque tipo di rete, per cui può essere utilizzato sia in reti locali, sia in reti geografiche. I protocolli utilizzati nella rete Internet sono specificati mediante standard noti con il nome di **RFC (Request For Comments)**.

Il modello TCP/IP può essere pensato, da un punto di vista concettuale, suddiviso in tre classi di servizi, come mostrato nella Figura 4.1.

Il livello inferiore fornisce il servizio di consegna dei dati senza connessione e senza riscontro, per cui non garantisce la corretta ricezione dei messaggi. *La rete è perciò inaffidabile* ed il corretto trasferimento dei dati è demandato al livello superiore. Il protocollo che definisce questo servizio è il **protocollo IP**; esso svolge le seguenti funzioni:

- definisce il **formato** dei dati che vengono trasmessi all'interno della rete.
- realizza la funzione di **routing**, ovvero il meccanismo con cui si sceglie il percorso per la trasmissione dei dati.
- prevede una serie di regole che determinano come devono essere processati i pacchetti, come e quando devono essere generati i messaggi di errore e le condizioni per le quali un pacchetto deve essere scartato.



Figura 4.1 – Struttura a livelli dei servizi in TCP/IP.

Il secondo livello in Figura 4.1 fornisce un *trasporto sicuro dell'informazione*, adottando una serie di regole e protocolli che consentono di recuperare eventuali malfunzionamenti o perdite di informazioni verificatosi nella rete. Il protocollo che realizza questo servizio è il **protocollo TCP**. Le principali funzioni svolte dal protocollo TCP/IP sono:

- controllare il flusso dell'informazione nella rete;
- fornire un trasporto sicuro dell'informazione assicurando che i dati arrivino senza errori e nell'ordine corretto;
- dividere i dati provenienti dal livello superiore in pacchetti.

Il controllo della correttezza delle informazioni è perciò realizzato **end-to-end** e non link-per-link, come in altre reti.

L'ultimo livello mostrato nella Figura 4.1 contiene i programmi applicativi (Telnet, FTP,...) che possono essere utilizzati su una rete TCP/IP. Ciascun applicativo sceglie la modalità di trasporto dei dati, che può essere nella forma di messaggi individuali o di uno stream di bit.

Un aspetto fondamentale di questa architettura, che rispecchia perfettamente la filosofia di Internet, è rappresentato dal fatto che i tre tipi di servizi vengono realizzati con protocolli software nettamente separati tra loro; in questo modo è possibile sostituire un servizio senza che gli altri ne risentano.

La struttura dei dati nei vari livelli del modello TCP/IP è mostrata nella Figura 4.2. Il livello applicativo contiene messaggi o stream continui di dati. Il livello di trasporto suddivide i dati in **pacchetti**, il livello IP in **datagram**. Le informazioni nei livelli inferiori sono strutturate secondo la rete utilizzata per il trasporto.

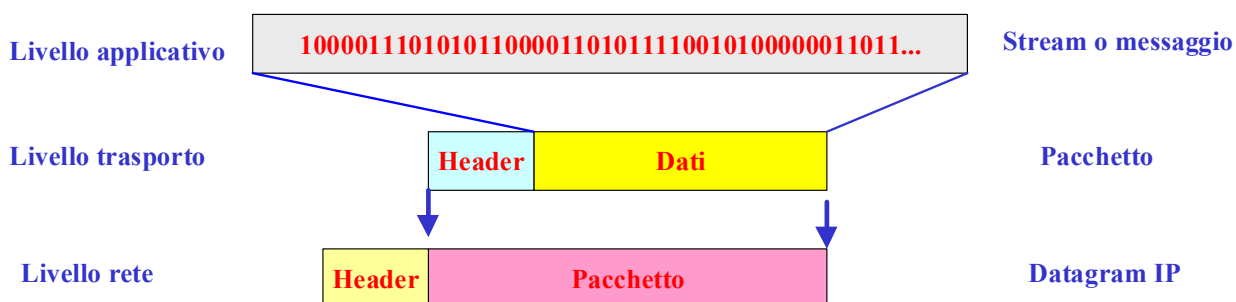


Figura 4.2 – Struttura dei dati nel protocollo TCP/IP.

## 4.2. Confronto tra il modello OSI e il modello TCP/IP

Il modello TCP/IP è distribuito su cinque livelli, che per la maggior parte corrispondono ai primi cinque livelli del modello OSI, come mostrato schematicamente nella Figura 4.3. Sono invece completamente assenti gli ultimi due livelli del modello OSI.

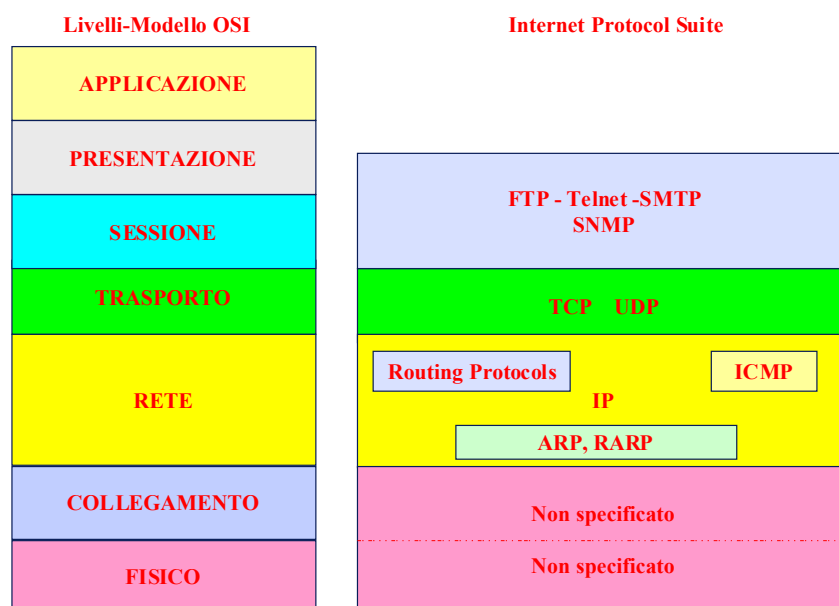


Figura 4.3 - Struttura a livelli del TCP/IP e del modello OSI.

L'architettura di rete TPC/IP non specifica il livello fisico e di collegamento, ma utilizza quelli disponibili sulla rete utilizzata. Ad esempio, nel caso di una rete LAN può utilizzare Ethernet, Token Ring, FDDI,..., mentre a livello geografico può essere utilizzata una qualunque rete geografica quale ATM, Frame Relay, X.25,....

### 4.3. Il protocollo IP

IP è il protocollo principale del livello di rete nell'architettura TCP/IP. Esso è stato specificato in RFC 791 e, come detto in precedenza, è di tipo *datagram*. Sono state sviluppate varie versioni del protocollo IP, che sono indicate generalmente con la sigla IPvN, dove N rappresenta il numero della versione. Attualmente è utilizzata la versione IPv4, mentre nei prossimi anni sarà introdotta la nuova versione IPv6, che fornirà nuove ed interessanti funzionalità. Nel seguito per protocollo IP si intende la versione IPv4, salvo un'esplicita dichiarazione. *Il formato del datagram* IPv4 è mostrato nella Figura 4.4. L'intestazione del datagram è formata da un insieme di campi a lunghezza fissa, ad eccezione del campo IP Option, che può essere portato fino ad una lunghezza massima di 32 bit. Il significato dei diversi campi sarà definito in dettaglio in un prossimo paragrafo.

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Length			
Identification			Flags	Fragment Offset		
Time to live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options					Padding	
DATI						
DATI						
....						
DATI						

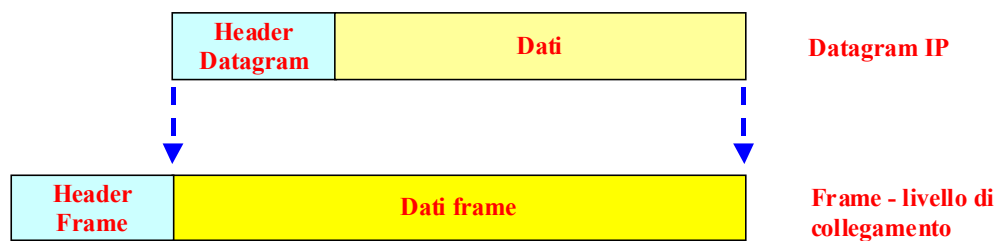
Figura 4.4 – Formato del datagram IPv4.

### Incapsulamento e frammentazione del datagram

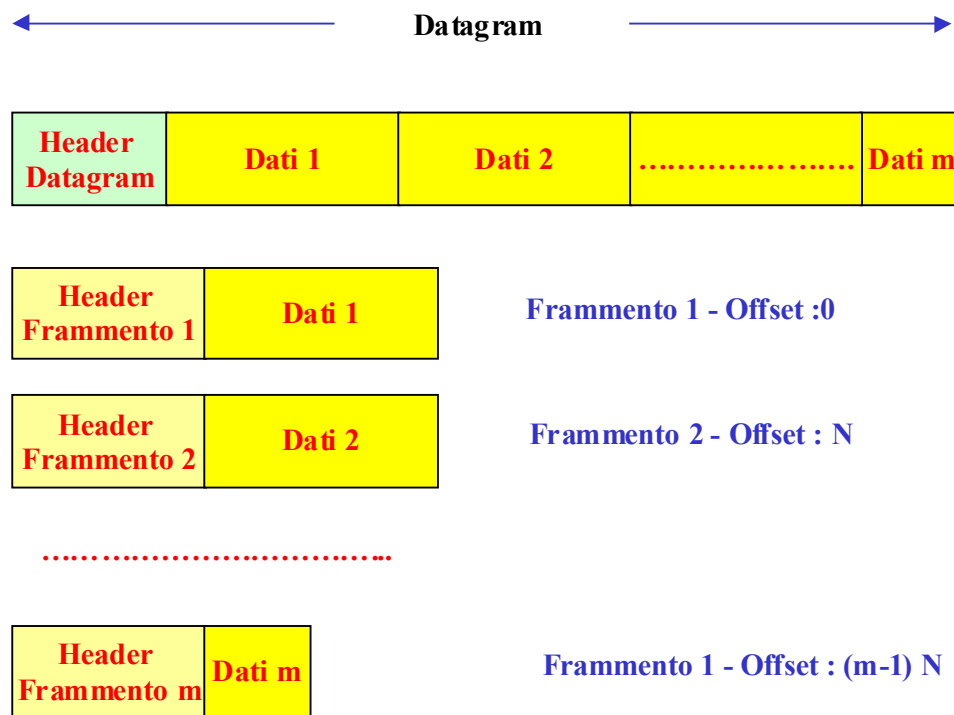
I datagram IP hanno una lunghezza massima uguale a 65.535 byte. Molte reti, che possono essere utilizzate a livello 1 e 2 per la trasmissione del datagram IP, accettano unità dati (frame) più piccole. Per questo motivo possono verificarsi varie situazioni (Figura 4.5):

- *Il datagram ha una lunghezza inferiore a quella del frame.* In questo caso il datagram è inserito direttamente nel frame (**incapsulamento del datagram**), come mostrato nella Figura 4.5.a.
- *Il datagram ha una lunghezza maggiore del frame.* Il datagram viene diviso in varie parti (**frammentazione del datagram**) e viene inserito in frame diversi, come mostrato nella Figura 4.5.b.

Ogni tipologia di rete ha una propria lunghezza massima di dati che il frame può trasportare; essa è spesso indicata come massima unità di trasferimento (**MTU = Maximun Tranfer Unit**)



a



b

Figura 4.5 – Incapsulamento e frammentazione di un datagram IP : a) incapsulamento; b) frammentazione.

Poiché Internet è composta da molte reti con caratteristiche diverse, non è possibile prevedere a priori la lunghezza massima accettabile del frame. La scelta di utilizzare MTU piccole non è ottimale, perché rende inefficiente le tratte in cui la rete può supportare frame di dimensioni maggiori. Non essendo possibile conoscere a priori nemmeno quali cammini saranno utilizzati per la comunicazione, la soluzione attualmente adottata da TCP/IP è quella di far fissare alla sorgente una lunghezza iniziale del datagram e prevedere che questo venga frammentato in pezzi più piccoli, quando deve attraversare una rete con un MTU più basso. Ogni frammento ha lo stesso formato del datagram originario. I frammenti possiedono tutti la stessa lunghezza, sono sempre multipli di un byte, ma l'ultimo sarà di lunghezza minore od uguale agli altri. La massima efficienza viene ottenuta quando il datagram è trasportato da un unico frame.

Il protocollo IP implementa dunque un meccanismo di frammentazione e ricomposizione dei frammenti in datagram. Al protocollo IP deve essere specificato l'MTU minimo, che viene utilizzato come limite superiore alla dimensione dei datagram generati. La frammentazione può avvenire in un punto qualsiasi del cammino di un datagram verso la stazione di destinazione.

#### Esempio

Consideriamo le tre reti mostrate nella Figura 4.6. La seconda rete ha un MTU uguale a 128 byte, per cui i datagram provenienti dalla rete 1 o 3 devono essere suddivisi in unità con lunghezza massima di 128 byte.

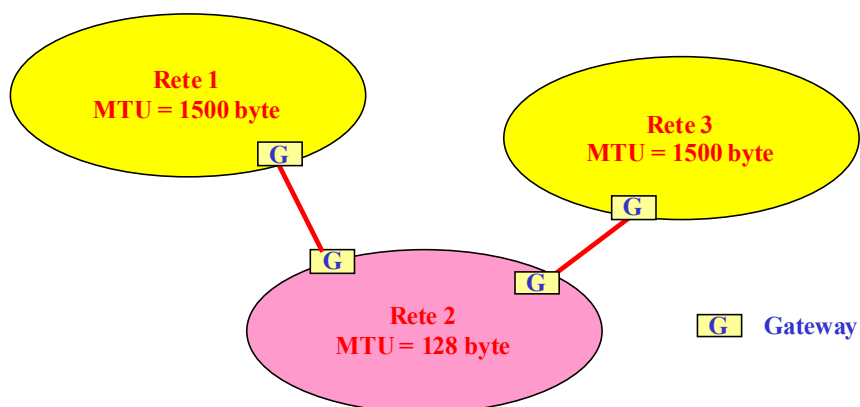


Figura 4.6 – Frammentazione di datagram in rete con diversi MTU.

Una volta che un datagram è stato frammentato, i frammenti sono trasmessi in modo del tutto indipendente attraverso la rete e vengono riassemblati solamente quando giungono a destinazione. Questa tecnica presenta i seguenti problemi:

1. I frammenti generati da una rete con un piccolo MTU potrebbero attraversare reti con grande MTU, causando quindi una perdita di efficienza;
2. Se un frammento viene perso, è necessario ritrasmettere tutto il datagram. Quando il computer in ricezione riceve un frammento, viene fatto partire un timer di riassemblamento. Se il timer si esaurisce prima che siano giunti tutti i frammenti, il computer ricevente scarta tutti i frammenti giunti fino a quel momento; per questo motivo all'aumentare del numero dei frammenti aumenta la probabilità di perdita di un datagram.

Nonostante questi svantaggi, la tecnica datagram presenta una notevole semplicità, per cui è stata adottata per la rete Internet.

## Formato del datagram IP

Descriviamo brevemente il significato dei diversi campi presenti nel formato del datagram IP mostrato nella Figura 4.4:

- Vers: composto da 4 bit, contiene la versione del protocollo IP usato per la creazione del datagram. Serve a verificare che il trasmettitore e il ricevitore utilizzino lo stesso formato. Attualmente è utilizzata la versione 4.
- Hlen: composto da 4 bit, fornisce la lunghezza dell'header del datagram IP (che può risultare variabile a causa del campo option), espressa come numero di parole da 32 bit. L'header più comune, che non presenta il campo option né il campo padding, misura 20 byte. In questo caso HLEN = 5.
- Service type: composto da 8 bit, specifica come un protocollo di livello superiore deve trattare il pacchetto. Questo campo è suddiviso in 4 sotto campi, come mostrato nella Figura 7 con il seguente significato:
- I bit di PRECEDENCE indicano il grado di importanza del datagram, con valori che vanno da 0 ( priorità normale) a 7 ( controllo della rete). Anche se spesso questo campo è ignorato dal software IP, tale valore fornisce un meccanismo per dare priorità ai pacchetti di controllo rispetto a quelli dati.
- I bit D, T e R specificano il tipo di trasporto richiesto per il datagram ed indicano:
  - campo D: Ritardo accettabile (1 = basso ritardo, 0 = valore non critico)
  - campo T: Throughput accettabile (1 = alto throughput, 0 = valore non critico)
  - campo R: Affidabilità (1 = alta affidabilità, 0 = valore non critico)Questi campi servono per il routing

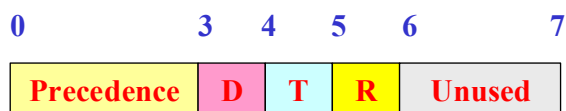


Figura 4.7 – Suddivisione del campo *Service type* del datagram IP

- Total length: composto da 16 bit, contiene la lunghezza del datagram o del frammento misurata in byte, inclusa l'intestazione. La massima lunghezza del datagram è 65.535 byte.
- Identification: composto di 16 bit; contiene un numero intero che identifica il datagram e quindi permette di individuare il datagram a cui appartiene un "frammento" che arriva a destinazione.
- Flags: composto da 3 bit. Il primo bit indica se il frammento è o no l'ultimo di un datagram. Il secondo bit indica se è possibile frammentare o no un datagram, mentre l'ultimo bit indica se il datagram è o no un frammento.
- Offset: composto da 13 bit; indica l'offset del frammento in multipli di 8 byte. Il primo frammento ha un offset uguale a 0. L'ultimo frammento ha un offset multiplo dei precedenti, ma con un total length minore od uguale ai precedenti.
- Time to live: composto da 8 bit; esprime il tempo in secondi che il datagram può rimanere nella rete Internet prima di essere scartato. Quando un datagram viene generato, questo campo viene posto uguale a 255 (massimo valore). Il valore del contatore viene diminuito con il passaggio del tempo; quando il contatore diviene uguale a 0, il datagram viene scartato. Questo contatore evita che un datagram permanga troppo a lungo nella rete a causa di malfunzionamenti.



- Protocol: composto da 8 bit; specifica il protocollo di livello superiore utilizzato per creare il pacchetto contenuto nel campo dati del datagram.
- Header checksum: composto da 16 bit; controlla se l'header del datagram contiene o no errori. Se l'header contiene errori, il datagram viene scartato. Il protocollo TCP dovrà provvedere al recupero del datagram.
- Source IP address: composto da 32 bit; contiene l'indirizzo IP della stazione che ha generato il datagram.
- Destination IP address: composto da 32 bit; contiene l'indirizzo IP della stazione a cui è diretto il datagram.
- Option: ha una lunghezza variabile; consente di fornire una serie di opzioni, quali la sicurezza e il source routing. Il source routing impone a un datagram un determinato percorso e può essere utile per analizzare il comportamento di una rete.
- Padding: questo campo ha una lunghezza variabile; serve a rendere l'header un multiplo di 32 bit.
- Dati: questo campo ha una lunghezza variabile; contiene i dati informativi.

## Indirizzi IP

Ogni computer connesso alla rete Internet ha un **indirizzo IP** che lo individua in modo univoco. L'indirizzo IP è costituito da un numero binario di **32 bit**, cioè da 4 byte. Per semplicità gli indirizzi IP sono generalmente espressi mediante i 4 numeri decimali corrispondenti ai 4 byte separati dal carattere punto.

### Esempio

L'indirizzo IP in binario 100000100000111000000001000011110 diventa in rappresentazione decimale 130.14.2.30

Per facilitare l'uso degli indirizzi, si ricorre spesso ad **indirizzi simbolici**.

### Esempio

L'indirizzo numerico del server informativo dell'Università di Siena è 193.205.4.2, mentre quello simbolico è unisi.it

I 32 bit che formano un indirizzo IP possono essere divisi in due campi (Figura 4.8):

- **Indirizzo della rete (netid)**, che identifica la rete su cui si trova il computer;
- **Indirizzo del computer (hostid)**, che identifica il computer all'interno della rete.



Figura 4.8 – Formato di un indirizzo IP.

**Gli indirizzi IP possono essere divisi in 5 classi** (Figura 4.9), denominate **classe A, B, C, D e E**. L'identificazione della classe avviene osservando i primi bit. Il formato degli indirizzi Internet per le diverse classi è mostrato nella Figura 4.9.

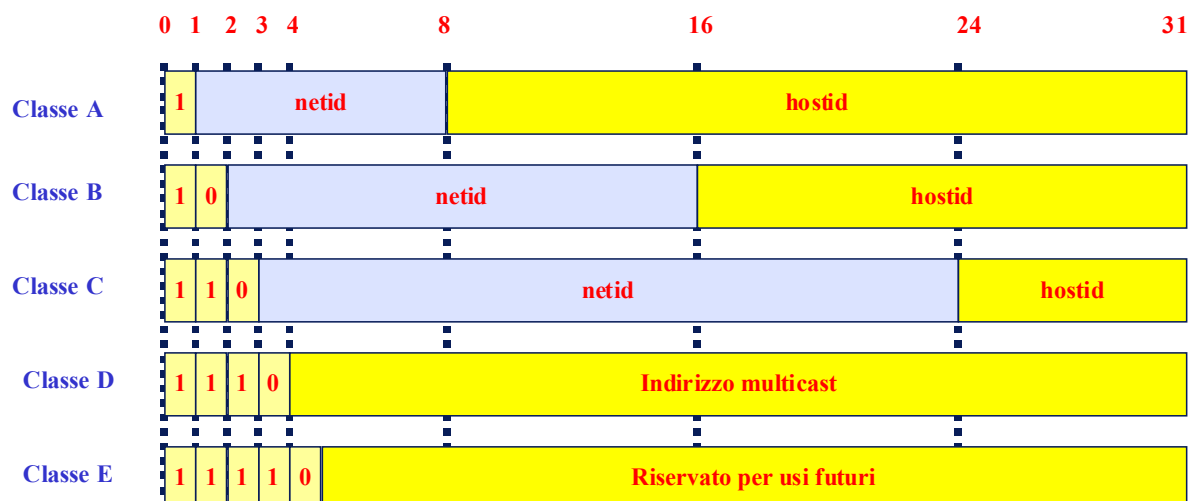


Figura 4.9 - Formato degli indirizzi Internet per le varie classi.

### Caratteristiche delle classi degli indirizzi IP

**Classe A:** utilizza 7 bit per netid e 24 per hostid. Possono perciò esistere un numero massimo di 128 reti di classe A, ciascuna delle quali può contenere al massimo  $2^{24} = 15.777.216$  computer.

**Classe B:** utilizza 14 bit per netid e 16 per hostid. La classe B è adatta a reti che hanno un numero di computer compreso tra 256 e  $2^{16} = 65536$ .

**Classe C:** utilizza 21 bit per netid e 8 bit per hostid. La classe C viene utilizzata per reti che hanno un numero di computer inferiore a 256.

**Classe D:** è riservata ad applicazioni di multicast.

**Classe E:** è stata definita per usi futuri. Gli indirizzi di questa classe sono facilmente riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 240 e 255.

Nella tabella 4.1 sono riassunte le dimensioni delle varie classi IP.

	N. MAX RETI	N. MAX COMPUTER PER RETE
<b>CLASSE A</b>	128	16777216
<b>CLASSE B</b>	16384	65536
<b>CLASSE C</b>	2097152	256

Tabella 4.1 - Dimensioni delle reti IP nelle varie classi.

Gli indirizzi IP sono stati realizzati in modo che sia possibile estrarre facilmente il **netid**, ovvero l'identificatore alla rete a cui appartiene un dato computer. Oltre che per le interfacce, gli indirizzi IP vengono usati anche per identificare una **rete**. Per convenzione, l'indirizzo di una rete è quello che ha l'**hostid con tutti 0**.

#### Esempio

L'indirizzo 10000001000001110000000000000000 corrisponde alla rete di classe B con il seguente indirizzo 130.14.0.0

## Indirizzi IP speciali

Un'altra convenzione utilizzata è quella che riguarda il **broadcast** su una rete (**directed broadcast**). Il broadcast su una rete si ottiene ponendo **tutti i bit dell'hostid a 1**.

## Sottoreti IP

Nello schema di indirizzamento IP originale (divisione dell'indirizzo IP in netid e hostid) si prevede che ad ogni rete fisica venga assegnato un unico indirizzo di rete. Questo aspetto e l'enorme crescita di Internet ha comportato i seguenti problemi:

- La più piccola rete prevista è quella di classe C (256 indirizzi): se una classe C viene assegnata ad una rete con pochi computer, la maggior parte degli indirizzi rimane inutilizzata.
- L'enorme numero di reti collegate ad Internet, molte delle quali di piccole dimensioni e ciascuna con un proprio indirizzo di rete, comporta l'aumento delle dimensioni delle tabelle di routing e dei compiti di gestione degli indirizzi.

Per ridurre il numero degli indirizzi di rete, è stato necessario trovare un meccanismo per far condividere lo stesso indirizzo di rete IP a più reti fisiche. Tale tecnica prende il nome di **subnet addressing** o **subnetting** ed è obbligatoria in ogni implementazione del protocollo IP.

### Esempio

Nella Figura 4.10 è mostrato un esempio di subnetting. Il router R utilizza lo stesso indirizzo in classe B (128.10.0.0) per le due reti fisiche ad esso collegate.

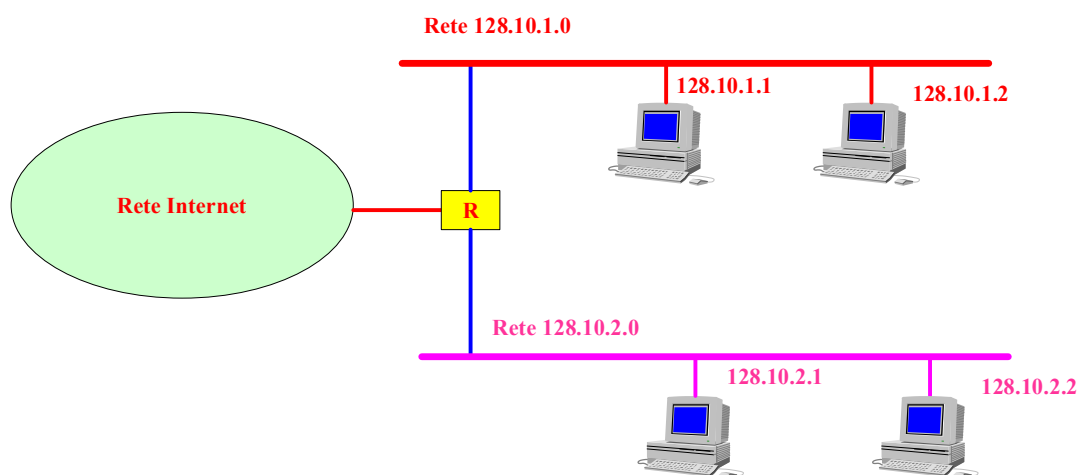


Figura 4.10 - Un sito con due reti fisiche che usa la subnettazione dell'indirizzo.

Tutti i router di Internet, tranne R, vedono le due reti come un'unica rete fisica di indirizzo 128.10.0.0. Quando un datagram arriva al router R, questo provvede ad inviarlo sulla rete fisica di destinazione. Per rendere più efficiente questa fase, l'amministratore di rete ha utilizzato il terzo byte dell'indirizzo per distinguere le due reti.

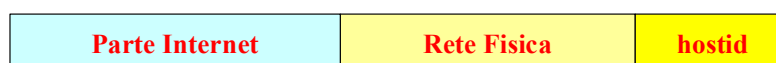
Le macchine sulla prima rete hanno un indirizzo che inizia con 128.10.1, mentre le macchine sulla seconda rete hanno l'indirizzo che inizia con 128.10.2. Per instradare il datagram il router R esamina i primi tre byte dell'indirizzo IP di destinazione.

Suddividere una rete in sottoreti significa interpretare l'indirizzo IP in modo leggermente diverso rispetto a quanto esposto fino ad ora (come mostrato nella Figura 4.11). Nella Figura 4.11.a è mostrato lo schema classico di un indirizzo IP, mentre nella Figura 4.11.b è mostrato uno schema di una possibile subnettizzazione. In esso il campo netid rimane inalterato, mentre il campo hostid viene suddiviso in due parti, cioè:

- subnet
- host



a



b

Figura 4.11 – Caratteristica dell'indirizzo IP nel caso di subnettizzazione : a) indirizzo IP standard; b) indirizzo IP nel caso di subnettizzazione.

L'ampiezza dei campi subnet e host può essere definita in modo molto flessibile tramite un parametro detto **netmask**. La netmask è composta da bit uguali ad 1 in corrispondenza dei campi di netid e subnet e uguale a 0 in corrispondenza del campo host. *Anche le netmask sono spesso rappresentate da una notazione dotted decimale.*

#### Esempio

La netmask 11111111 11111111 11111111 00000000 corrisponde all'indirizzo IP 255.255.255.0 ed indica che il campo host coincide con l'ultimo byte.

Dato un indirizzo IP, per estrarre l'indirizzo della rete e del subnet si effettua un'operazione *AND bit a bit* tra l'indirizzo IP e la netmask.

Esempio  
 Sia dato l'indirizzo IP 128.10.2.2; la sua rappresentazione binaria risulta:  
 100000000 00001010 00000010 00000010  
 Utilizzando la netmask 255.255.250.0 la cui rappresentazione binaria è:  
 11111111 11111111 11111010 00000000  
 ed effettuando l'operazione AND tra le due sequenze si ottiene la sequenza:  
 10000000 00001010 00000010 00000000  
 che corrisponde all'indirizzo:  
 128.10.2.0  
 e quindi l'indirizzo IP 128.10.2.2 appartiene alla rete 128.10.2.0. La rete 128.10.2.0 è una sottorete della rete in classe B 128.10.0.0. Utilizzando la netmask con l'indirizzo IP 128.10.3.4 si ottiene ancora 128.10.2.0 e quindi anche questo indirizzo IP appartiene alla stessa rete di 128.10.2.2

Con riferimento agli indirizzi di rete IP in classe C si possono definire le subnet mask contigue mostrate nella tabella 4.2.

Subnet mask (dotted decimal notation)	Subnet mask (ultimo byte)	N. reti/classe C	N. indirizzi IP/sottorete	N. host/sottorete
255.255.255.0	00000000	1	256	254
255.255.255.12	10000000	2	128	126
255.255.255.19	11000000	4	64	62
255.255.255.22	11100000	8	32	30
255.255.255.24	11110000	16	16	14
255.255.255.24	11111000	32	8	6
255.255.255.25	11111100	64	4	2

Tabella 4.2 – Subnet mask contigue.

## Protocolli di instradamento IP

Le tecniche di instradamento dei datagram possono essere divise in **routing diretto** e **routing indiretto**. Per **routing diretto** si intende la trasmissione di un datagram da una macchina direttamente ad un'altra. Il routing diretto si può avere solo se entrambe le macchine sono connesse alla stessa rete fisica. Viene utilizzato il **routing indiretto** quando le macchine comunicanti non si trovano sulla stessa rete fisica, costringendo il mittente ad inviare il datagram ad un router per la consegna.

### *Routing diretto*

La trasmissione di un datagram IP tra due macchine della stessa rete fisica non coinvolge i router. Il mittente incapsula il datagram in un frame fisico, mappa l'indirizzo IP con l'indirizzo fisico e invia il frame direttamente alla macchina destinazione. Poiché gli indirizzi IP di tutte le macchine che appartengono alla stessa rete fisica hanno lo stesso netid e poiché il netid può essere estratto dall'indirizzo IP con poche istruzioni, risulta semplice scoprire se una macchina può essere raggiunta direttamente. Il routing diretto può essere visto come consegna del datagram e rappresenta anche l'ultimo passo nella trasmissione del datagram. Infatti l'ultimo router del percorso è connesso alla stessa rete fisica della

macchina destinazione, dunque userà il routing diretto per consegnare il datagram alla macchina destinazione.

Il routing diretto può essere visto come un caso particolare del routing generico, in cui il datagram non transita in nessun router intermedio.

### *Routing indiretto*

Il routing indiretto presenta una complessità superiore al routing diretto, perché il mittente deve individuare il router a cui inviare il datagram; il router deve poi inoltrare il datagram verso la destinazione finale. Il percorso dalla sorgente alla destinazione è realizzato mediante la trasmissione del datagram da un router all'altro, fino a quando il datagram non arriva direttamente al router a cui la stazione di destinazione è collegata. Sulla rete Internet i router costituiscono una struttura cooperativa e interconnessa.

### *Tabelle di routing*

L'instradamento del traffico IP si basa sulle **tabelle di routing**, tabelle in cui vengono memorizzate le informazioni su come raggiungere una qualsiasi destinazione. Poiché sia gli host che i router instradano datagram, entrambi hanno le tabelle di routing; ogni volta che il protocollo IP deve inviare un datagram consulta la tabella di routing per decidere dove inviarlo. Se ogni tabella di routing contenesse le informazioni su ogni singolo indirizzo IP presente su Internet, avrebbe dimensioni enormi. Il concetto che si cerca di applicare è quello di avere un **routing con la minima informazione**. Per esempio, sarebbe preferibile confinare l'informazione sulle singole macchine nell'ambito locale in cui si trovano e consentire la loro raggiungibilità alle macchine remote senza che queste ne conoscano i dettagli. Per questo gli indirizzi IP sono assegnati in modo tale che tutte le macchine sulla stessa rete fisica abbiano lo stesso prefisso (il netid). Ciò consente di riportare nelle tabelle di routing solamente gli indirizzi identificativi delle reti e non gli indirizzi IP completi, riducendo quindi la dimensione delle tabelle, migliorando l'efficienza dell'informazione e confinando i dettagli sui singoli host nell'ambito locale in cui essi operano.

Tipicamente una routing table è costituita da una sequenza di coppie (**N,G**) dove:

- **N** indica l'indirizzo IP della rete di destinazione;
- **G** indica il **next hop**, ovvero l'indirizzo IP del prossimo router lungo il percorso verso la rete N.

Questo indirizzo deve riferirsi sempre ad una macchina direttamente raggiungibile dalla macchina a cui appartiene la tabella di routing.

Le tabelle di routing per gli host devono contenere la minima informazione possibile: l'idea è quella di costringere gli host ad affidarsi ai router per la maggior parte delle procedure di instradamento.

La scelta di effettuare un routing basato sul netid comporta tutta una serie di conseguenze, quali:

- Nella maggior parte dei casi tutto il traffico diretto ad una data destinazione prende la stessa strada, per cui, anche se esistono più percorsi per quella destinazione, non possono essere usati in modo concorrente.
- Poiché l'host di destinazione è connesso ad un router, solamente quest'ultimo può determinare se l'host esiste o è attivo. Quindi è necessario che il router implementi un meccanismo che segnali la situazione di errore alla sorgente.
- Poiché ogni router instrada il traffico in modo indipendente, i datagram che viaggiano da un host A ad un host B possono seguire un percorso completamente diverso di quelli che viaggiano da B a A. I router devono dunque collaborare per fare in modo che la comunicazione nei due sensi sia sempre possibile.

### *Autonomous system*

Le reti e i router collegati alla rete Internet sono divise in gruppi; ogni gruppo è controllato da un'unica autorità amministrativa, chiamata **Autonomous system (AS)**. Ogni AS è identificato da un numero univoco a livello internazionale e rilasciato dall'autorità che assegna gli indirizzi Internet. I router possono essere classificati in:

- ❑ **Router esterni:** se appartengono a diversi AS (Figura 4.12), in questo caso utilizzano per scambiare informazioni di instradamento un protocollo **EGP (Exterior Gateway Protocol)**.
- ❑ **Router interni:** se appartengono allo stesso AS; in questo caso utilizzano per scambiare informazioni di instradamento un protocollo **IGP (Interior Gateway Protocol)**. All'interno di un AS tutti i router utilizzano generalmente lo stesso IGP.

## **4.4 Protocolli EGP**

La rete Internet può utilizzare diversi tipi di protocolli EGP. In questo paragrafo descriviamo i principali tipi della classe di protocolli EGP; tra cui uno dei più noti è indicato con la sigla EGP.

### *Protocollo EGP*

Rappresenta il primo protocollo utilizzato in modo esteso all'interno della rete Internet. Questo protocollo, definito nel 1984, è simile ad un protocollo distance vector, ma non utilizza nessuna metrica per caratterizzare la raggiungibilità di una rete; per questo motivo esso è un algoritmo che opera in modo soddisfacente su reti ad albero, ma non su reti a maglia.

La costruzione e l'aggiornamento delle tabelle di routing viene effettuata dal protocollo EGP mediante la generazione di pacchetti di routing che contengono informazioni sulla raggiungibilità di una rete.

Il protocollo EGP presenta numerosi svantaggi e in particolare non ammette la presenza di una topologia a maglia, per cui tutti gli AS devono essere collegati in modo stellare ad un core system.

## Protocollo BGP

Border Gateway Protocol (BGP) è un protocollo che dovrebbe sostituire EGP, eliminandone i principali inconvenienti. BGP utilizza un algoritmo di routing del tipo distance vector, in cui al posto del fattore di costo per raggiungere una destinazione viene inviata la sequenza di AS da attraversare per raggiungere tale destinazione. Ogni router definisce una "via" preferita per una fissata destinazione e la comunica ai router BGP adiacenti tramite un distance vector.

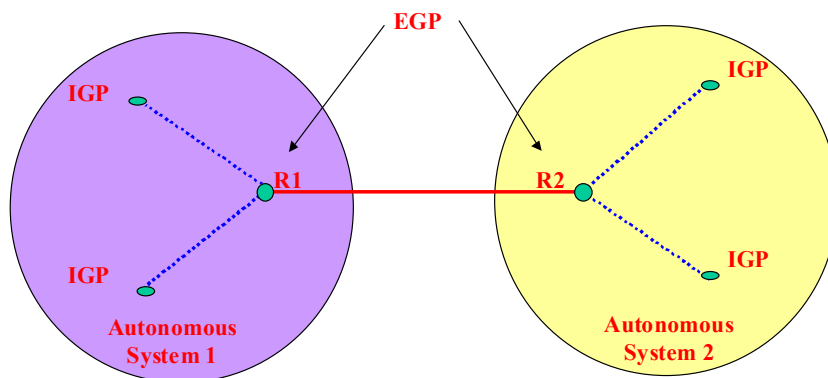


Figura 4.12 – Protocolli di routing.

## 4.5 Protocolli IGP

I protocolli IGP servono a facilitare lo scambio di informazioni tra router all'interno di un AS. I router all'interno di un AS si scambiano informazioni sulle proprie reti; quando la situazione dell'AS è stata completamente definita, un router (corrisponde all'exterior router di quel dominio) provvede a informare gli altri AS mediante un protocollo EGP. Come mostrato nella Figura 4.12, un router (ad esempio il router R1 o R2) può utilizzare contemporaneamente due diversi protocolli di routing: un protocollo IGP per comunicare all'interno del proprio AS e un protocollo EGP per comunicare con altri AS.

Descriviamo adesso le caratteristiche dei principali algoritmi IGP utilizzati sulla rete Internet.

### Protocollo RIP

**RIP (Routing Information Protocol)** è il più noto tra i protocolli IGP ed è conosciuto anche con il nome del programma routed. Il successo di questo protocollo è dovuto al fatto che il programma routed veniva incluso nella versione 4BSD di Unix, prodotto dall'università di Berkeley in California, per cui esso è diventato uno standard prima di apparire in un RFC.

Il RIP è un routing protocol di tipo distance vector. Suddivide le macchine in attive e passive. Le macchine attive informano le altre sul routing, quelle passive aggiornano le tabelle di routine, ma non diffondono informazioni sul routing. Tipicamente i **routers** sono **macchine attive** mentre gli **host** sono **macchine passive**.



## Protocollo OSPF

Per superare i problemi posti dai protocolli IGP IETF ha costituito nel 1988 un gruppo di studio per la realizzazione di un IGP basato sull'algoritmo SPF. In questo modo è stato definito il protocollo **Open Shortest Path Find (OSPF)**.

Le principali caratteristiche dell'OSPF sono:

- Le **specifiche** dell'OSPF sono **pubbliche**, per cui esso è un protocollo utilizzabile da chiunque in modo aperto senza costi.
- OSPF prevede un routing variabile in base al tipo di servizio; in questo modo possono essere previsti cammini multipli, ciascuno per un tipo di servizio (p.es basso ritardo o alto throughput).

## 4.6 I protocolli ARP e RARP

L'indirizzo IP assegnato ad un host (indirizzo di livello 3) non corrisponde all'indirizzo fisico (indirizzo di livello 2) della rete a cui l'host è realmente collegato. I protocolli **Address Resulotion Protocol (ARP)** e **Reverse Address Resolution Protocol (RARP)** consentono di rilevare in modo automatico la corrispondenza tra gli indirizzi IP e gli indirizzi fisici.

Il protocollo ARP viene utilizzato tutte le volte che una stazione collegata ad una LAN deve inviare un messaggio ad un nodo sulla stessa LAN di cui conosce solo l'indirizzo IP.

Il protocollo RARP viene utilizzato dalle stazioni senza memoria di massa per scoprire il loro indirizzo IP nella fase iniziale di avviamento. Il computer invia in broadcast una richiesta contenente il proprio indirizzo fisico; il server RARP risponde inviando al computer il suo indirizzo IP. I protocolli ARP e RARP si appoggiano direttamente sulle reti e non su IP.

*Il metodo più utilizzato per effettuare la mappatura tra indirizzo IP e fisico consiste nell'inviare un pacchetto speciale all'utente di cui si conosce solo l'indirizzo IP chiedendo di comunicare il proprio indirizzo fisico. Soltanto l'utente in possesso di quell'indirizzo IP può rispondere, comunicando il proprio indirizzo fisico alla stazione che ne aveva fatto richiesta. E' chiaro che questo protocollo di comunicazione in broadcast deve essere ripetuto il meno possibile, e quindi, una volta ottenuta la risoluzione dell'indirizzo, questo è posto in un'apposita memoria di cache, in modo da venire utilizzata successivamente senza dover ripetere tutta la procedura. Per evitare che l'utente a cui è stata indirizzata la richiesta di risolvere il proprio indirizzo debba ripetere tutta questa fase per comunicare con il suo interlocutore, si fa in modo che nel datagram ARP sia contenuta anche l'informazione relativa all'indirizzo fisico di chi sta trasmettendo. Per ottenere ulteriori miglioramenti, quando è in corso la comunicazione broadcast tutte le macchine presenti in quel momento sulla rete ricevono la richiesta di risoluzione e anche se non rispondono possono però prendere nota della risoluzione dell'indirizzo IP in indirizzo fisico del richiedente e memorizzarla in modo da realizzare un aggiornamento su tutte le macchine.*

Per lo stesso motivo, si può prevedere che ogni macchina che fa un boot sulla rete invii un messaggio broadcast ARP per presentarsi con il proprio indirizzo fisico a tutte le altre

macchine presenti. A questo punto, se una macchina ha nella propria cache l'indirizzo IP del nuovo arrivato, controlla che i due indirizzi fisici coincidano, ed in caso contrario aggiorna il contenuto della cache.

Prendiamo come riferimento le reti **Ethernet**. Nelle reti Ethernet, l'indirizzo fisico è associato all'**interfaccia hardware** (muovendo la scheda su un altro computer, l'indirizzo contenuto nella scheda viene associato al nuovo computer). Gli indirizzi Ethernet sono fissati a livello internazionale: ogni costruttore di schede ha a disposizione un proprio set di indirizzi. L'ARP nasconde la rete sottostante ai protocolli superiori, consentendo a questi di usare gli indirizzi IP.

### *Formato del pacchetto ARP*

Nella Figura 4.13 è mostrato il formato del pacchetto ARP. Vediamo in dettaglio il significato dei principali campi del pacchetto.

- Hardware type : indica il tipo di interfaccia hardware per cui il trasmettitore aspetta una risposta;
- Protocol type: specifica il tipo di protocollo utilizzato dal trasmettitore;
- HLEN: specifica la lunghezza dell'indirizzo hardware in modo da poter utilizzare diversi tipi di rete;
- PLEN: specifica la lunghezza dell'indirizzo IP utilizzato;
- Operation: specifica il tipo di operazione effettuata, cioè se è una richiesta ARP, una risposta RARP, una richiesta RARP oppure una risposta RARP;
- HA1: indica l'indirizzo hardware dell'apparecchiatura che ha inviato la richiesta;
- IP1: indica l'indirizzo IP dell'apparecchiatura che ha inviato la richiesta;
- HA2: indica l'indirizzo hardware dell'apparecchiatura a cui è inviata la richiesta;
- IP2: indica l'indirizzo IP dell'apparecchiatura a cui è inviata la richiesta.

### *Protocollo ICMP*

Il protocollo **ICMP (Internet Control Message Protocol)** permette ad un router di inviare messaggi di errore o di controllo ad altri router o host. ICMP fornisce un metodo per la comunicazione tra il protocollo IP su una macchina e il protocollo IP su un'altra macchina ed è considerato parte essenziale del protocollo IP, per cui deve essere presente in ogni sua implementazione. I messaggi ICMP viaggiano attraverso la rete nella parte dati del datagram.

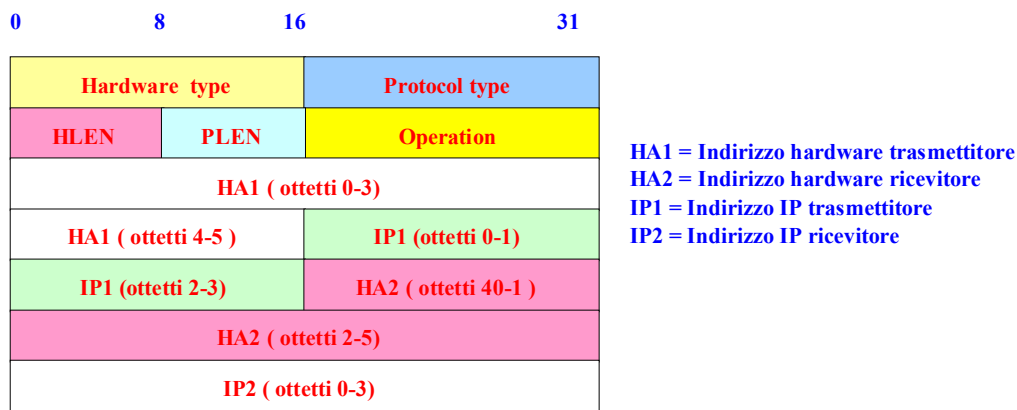


Figura 4.13 – Formato del pacchetto ARP.

Nonostante le linee guida raccomandino l'uso di alcuni messaggi ai soli router, in generale anche gli host possono scambiare messaggi ICMP; in questo modo è possibile utilizzare un solo meccanismo per tutti i messaggi di controllo.

ICMP serve solo a segnalare al mittente di un datagramm la presenza di un errore, ma non fornisce nessuna informazione sulla loro natura, per cui è compito del mittente individuare le cause di errore e intraprendere le azioni per correggerle.

Le cause di errore possono nascere in vari punti del sistema di trasmissione, ma ICMP può segnalare la condizione di errore soltanto al mittente, poiché il datagramm ricevuto contiene l'indirizzo del mittente e non l'indicazione del percorso effettuato.

Ogni messaggio ICMP è inserito nella parte dati del datagramm IP, che viene a sua volta trasportato da un frame, come mostrato nella Figura 4.14. I datagramm che trasportano messaggi ICMP sono instradati come gli altri datagramm nella rete.

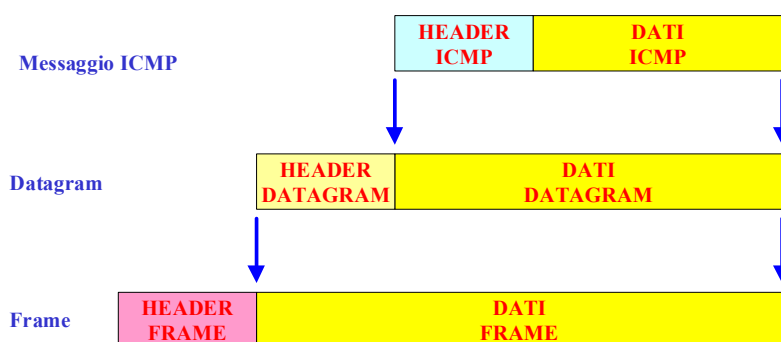


Figura 4.14 – Formato del datagramm ICMP.

## Messaggi ICMP

Il protocollo ICMP può inviare una serie di messaggi diversi, come mostrato nella tabella 4.3. Ogni messaggio ha un formato proprio. Descriviamo brevemente alcuni messaggi ICMP:

- Echo request e echo reply  
Attraverso questo messaggio una macchina A invia un echo request ad un'altra macchina B; quest'ultima risponde con un messaggio echo reply diretto alla macchina A. L'utilizzo più diffuso di questa procedura è legato all'applicazione **ping**, che serve a verificare se una stazione con cui ci si vuole collegare è raggiungibile ed attiva.
- Unreachable destination  
Questo messaggio viene inviato al mittente nel caso in cui un datagram non possa essere consegnato.
- Source quench  
Questo messaggio viene inviato per risolvere i problemi di congestione che si stanno verificando nella rete (ad esempio in un router). La condizione di congestione è quella in cui i datagram arrivano in un nodo ad un ritmo più elevato di quanto il nodo stesso riesca a trasmetterli. Un router invia un messaggio di source quench per ogni datagram scartato. Alcuni router utilizzano tecniche più sofisticate, monitorando i datagram ed inviando i source quench alle sorgenti con traffico più elevato. Una sorgente che riceve un messaggio di source quench deve ridurre la velocità di trasmissione fino a quando non cessa di ricevere tali messaggi.
- Redirect  
Questo messaggio può essere utilizzato tra router e host che si trovino sulla stessa rete e serve ad ottimizzare l'instradamento dei messaggi.
- Time exceed  
Quando un router invia un datagram, un contatore detto "time-to-live" viene messo ad un valore prefissato. Il contatore viene decrementato con il passare del tempo e quando raggiunge il valore 0 il datagram è scartato e un messaggio di time exceed è inviato al mittente del datagram. Questo meccanismo serve ad evitare ritardi troppo elevati nella consegna di un datagram e il fenomeno chiamato "routing cycle", in cui due o più router si inviano un datagram in circolo.
- Parameter problem  
Questo messaggio viene inviato quando il datagram ricevuto contiene gravi errori; in particolare, quando l'header del datagram non è corretto o non sono corretti i parametri relativi ad un'opzione contenuta in qualche campo dell'header.
- Timestamp  
Serve per sincronizzare gli orologi di più macchine.
- Address mask request e reply  
Servono per ottenere una subnet mask.

TIPO DI CAMPO	TIPO DI MESSAGGIO ICMP
0	Echo Replay
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
11	Time Exceeded for a Datagram
12	Parameter on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Reply (obsolete)
17	Address Mask Request
18	Address Mask Reply

Tabella 4.3 - Tipi di messaggio ICMP.

#### 4.7 Protocollo IPv6

La crescita enorme subita da Internet avvenuta a partire dai primi anni '90 ha posto in evidenza le limitazioni del sistema IPv4 attualmente utilizzato. Le previsioni indicano che lo spazio di indirizzamento disponibile con IPv4, in cui gli indirizzi IP sono composti da 32bit, sarà esaurito nel 2010. Per questo motivo *IETF (Internet Engineering Task Force)* ha elaborato nel 1994 un nuovo protocollo IP, noto con il nome di **IPv6**, descritto in **RCF 1752** "Raccomandazioni per il protocollo IP di prossima generazione". IPv6 introduce numerose modifiche rispetto a IPv4 e in particolare presenta indirizzi IP composti da 128 bit. Il numero di indirizzi in IPv6 è molto alto e seguendo la creazione di una gerarchia di indirizzi IPv6 può offrire 1500 indirizzi per ogni metro quadrato del pianeta. Questo numero così alto di indirizzi presenta numerosi vantaggi, quali:

- semplifica le procedure di instradamento;
- aumenta l'efficacia delle tabelle di instradamento;
- permette l'attuazione corretta delle procedure di configurazione automatica;
- consente di risolvere il problema degli indirizzi Internet per molti anni.

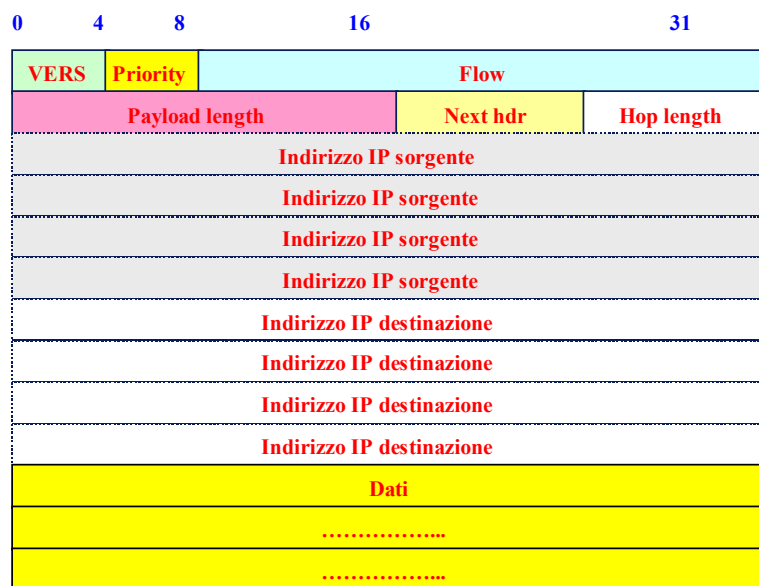


Figura 4.15 – Formato del datagram IPv6.

L'intestazione del datagram nel protocollo IPv6 è diversa rispetto a IPv4 e presenta le seguenti caratteristiche:

- il numero dei campi dell'header è ridotto da 10 a 6;
- la lunghezza dell'header in IPv6 è fissa; in questo modo l'elaborazione del pacchetto è più semplice e veloce;
- una parte dello spazio previsto per l'indirizzo in IPv6 è riservata dagli indirizzi IPv4. Inoltre è possibile scrivere gli indirizzi IPv4 come indirizzi compatibili IPv6. In questo modo il passaggio da IPv4 a IPv6 è notevolmente semplificato.

Il formato del pacchetto Ipv6 è mostrato nella Figura 4.15; vediamo in dettaglio la funzionalità dei diversi campi del pacchetto IPv6.

#### Vers

Il campo formato da 4 bit, indica il numero della versione del protocollo Internet. Nel caso di IPv6 questo campo assume il valore 6.

#### Priorità

Il campo è formato da 4 bit ed indica la priorità dei diversi pacchetti.

#### Flow label

Questo campo, formato da 28 bit, può essere utilizzato da un host per caratterizzare la qualità di servizio per ciascun pacchetto (ad esempio pacchetti da trasmettere in tempo reale).

#### Payload length

Questo campo, formato da 16 bit, indica la lunghezza in byte dei dati (payload), che seguono l'intestazione.

### Next header

Questo campo, formato da 8 bit, identifica il tipo di intestazione che segue quella dell'IPv6 ed usa gli stessi valori del campo analogo di IPv4.

### Hop limit

Il campo, formato da 8 bit, serve a limitare il numero di nodi attraversati per evitare problemi di "loop" o ritardi troppo elevati. Il valore del campo è inizializzato a 255 quando il pacchetto viene trasmesso e il suo valore è diminuito di 1 ogni volta che il pacchetto attraversa un nodo. Quando il campo assume il valore 0, il pacchetto viene scartato.

### Indirizzo di sorgente

Il campo, formato da 128 bit, rappresenta l'indirizzo IP della sorgente che ha generato il pacchetto.

### Indirizzo di destinazione

Il campo, formato da 128 bit, rappresenta l'indirizzo IP della stazione di destinazione.

## *Configurazione automatica di un indirizzo IP*

Una caratteristica molto interessante di IPv6 è rappresentata dalla sua capacità di configurare in modo automatico un host con un indirizzo IP: in altre parole un host può acquisire automaticamente l'informazione necessaria per la definizione del suo indirizzo IP.

Questa operazione, che consente di ridurre notevolmente la complessità ed il costo di gestione delle grandi reti e di configurare in modo semplice le piccole reti, può essere fatta con due modalità diverse:

- se l'host è collegato ad un router o a un server di indirizzi locali (ad esempio, in una rete locale), esso rivela l'indirizzo della rete su cui si trova, aggiunge una parte relativa al proprio indirizzo e invia un messaggio per verificare se esiste un altro indirizzo uguale. Se non esistono indirizzi uguali, il router o il server degli indirizzi viene aggiornato con questo nuovo indirizzo.
- se l'host è collegato ad una rete di grandi dimensioni, l'host invierà una richiesta ad un server di indirizzi, che provvederà a fornire l'indirizzo.

## *Coesistenza e transizione da IPv4 a IPv6*

Con l'introduzione di IPv6 sarà necessario garantire la convivenza tra IPv4 e IPv6 per un lungo periodo di tempo. La prima soluzione è quella di realizzare in un nodo ambedue gli algoritmi IPv4 e IPv6; questa soluzione, indicata con il nome **dual stack**, è mostrata nella Figura 4.16. I nodi di questo tipo sono indicati come IPv6 / IPv4.

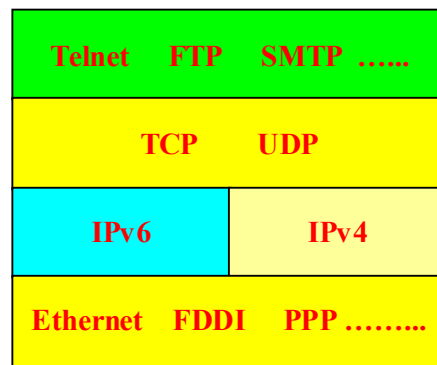


Figura 4.16 – Nodo dual stack IPV6/IPV4.

Un altro problema è rappresentato dal trasporto di un datagram IPv6 attraverso una rete IPv4; come mostrato nella Figura 4.17 in cui due nodi IPv6/IPv4 sono collegati attraverso una rete IPv4. Per risolvere questo problema si può utilizzare una tecnica di **tunneling**, in cui il datagram IPv6 viene incapsulato in un datagram IPv4 mediante l'inserimento di un header IPv4 (Figura 4.18).

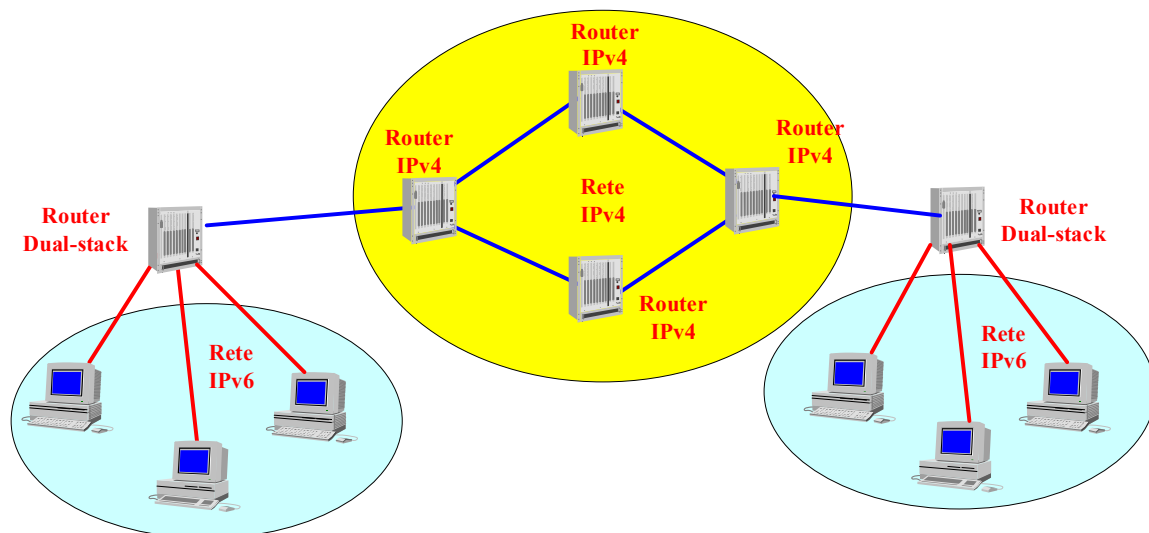


Figura 4.17. Collegamento tra due reti IPv6 mediante una rete IPv4.

### *Gestione della multimedialità e di applicazioni in tempo reale*

Il protocollo IPv6 consente una gestione migliore delle applicazioni multimediali e di quelle in tempo reale, quali videoconferenza o audio conferenza. Il campo priority, formato da 4 bit, classifica i pacchetti secondo la loro importanza per assicurare che, in caso di deterioramento della qualità della rete, i dati ad alta priorità arrivino a destinazione. Ad esempio, nel caso di una videoconferenza, l'audio è considerato più importante del video ed il video a bassa definizione avrà una priorità maggiore del video ad alta definizione.



## Sicurezza

Il protocollo IPv6 consente di avere un maggiore livello di sicurezza rispetto alle versioni precedenti; in particolare IPv6 considera la sicurezza della comunicazione, cioè:

- la convalida, che consente al destinatario di essere certo dell'origine di un messaggio;
- la crittografia, che rende il messaggio illeggibile da chiunque non sia il destinatario.

L'intestazione di convalida protegge le reti contro i rischi di instradamento di sorgente e di attacchi contro l'host, mentre la crittografia garantisce la riservatezza delle informazioni.



Figura 4.18 – Tecnica di tunneling: a) datagram IPv6; b) incapsulamento di un datagram IPv6 in un datagram IPv4.

## 4.8 Protocolli TCP e UDP

**TCP (Transmission Control Protocol)** e **UDP (User Datagram Protocol)** sono protocolli utilizzati nel livello di trasporto ed operano perciò a livello superiore rispetto a IP. Essi hanno caratteristiche diverse: il protocollo TCP garantisce un trasferimento affidabile dell'informazione, mentre UDP non garantisce l'affidabilità dei dati inviati ai livelli superiori.

I due protocolli sono in grado di trasferire i datagram IP tra computer utilizzando l'indirizzo IP. Tuttavia, un indirizzo IP identifica un computer e non è possibile effettuare distinzioni tra datagram diretti ad applicazioni sullo stesso computer. Il protocollo UDP aggiunge un meccanismo che consente di separare i datagram ricevuti da un computer tra le diverse applicazioni. In questo modo il protocollo di trasporto aggiunge alle funzioni dell' IP un meccanismo che permette alle singole applicazioni che sono eseguite su un computer di inviare e ricevere i datagram in modo indipendente l'una dall'altra.

Infatti, i sistemi operativi moderni supportano la multiprogrammazione, cioè permettono a più applicazioni di essere eseguite contemporaneamente. Ciascuna applicazione prende il nome di **processo** o di **task**. Per inviare un datagram ricevuto al processo a cui è destinato, UDP introduce un'astrazione che prende il nome di **porta**. Ogni porta è individuata da un numero intero positivo. Il sistema operativo locale fornisce un meccanismo di interfaccia che i processi utilizzano per specificare una porta o per accedervi. Generalmente il sistema operativo fornisce un accesso **sincrono** alle porte, nel senso che avvengono delle interruzioni di calcolo durante un'operazione di accesso ad una porta. Il protocollo UDP garantisce inoltre un processo di bufferizzazione dei pacchetti

per ciascuna porta. In questo modo i pacchetti in arrivo sono memorizzati in una coda di dimensioni finite, fino quando il processo non li estrae.

Per poter comunicare con una determinata porta, il mittente deve conoscere sia l'indirizzo IP della macchina destinazione che il numero della porta nella macchina destinazione; inoltre ciascun pacchetto contiene sia il numero della porta mittente che quella della porta destinazione. In questo modo è possibile per qualsiasi processo che riceve un messaggio di replicare al mittente.

Il protocollo TCP implementa il meccanismo delle porte, ma in modo diverso rispetto all'UDP. Infatti, nell'UDP una porta è considerata come un singolo oggetto, a cui può essere associata una coda. Nel TCP una porta non è un singolo oggetto e la connessione diventa l'astrazione principale. Una connessione è formata da una coppia di **endpoints**. Un endpoint è una coppia di interi (host, port) dove host è l'indirizzo IP di una macchina e port è la porta TCP su quella macchina. Dunque il TCP identifica una connessione con una coppia di endpoints. La conseguenza di ciò è che un dato numero di porta TCP su una macchina può essere condiviso da più connessioni.

#### *Esempio*

L'endpoint (150.217.11.23,25) rappresenta l'indirizzo IP 150.217.11.23 e la porta 25. Per rappresentare l'endpoint si può usare anche la notazione (150.217.11.23: 25).

Ad esempio un programma di gestione della posta elettronica su un server ha bisogno di una sola porta TCP, anche se consente l'accesso concorrente ai suoi servizi da parte di più utenti connessi in remoto.

### ***Il protocollo TCP***

Il TCP è un protocollo di livello trasporto. Anche se è stato introdotto come parte del TCP/IP, il TCP è di uso generale; infatti è stato preso come base per il protocollo TP-4 proposto dall'ISO nell'ambito del modello OSI.

A livello di collegamento il protocollo IP fornisce un servizio inaffidabile di distribuzione dei pacchetti. Infatti i pacchetti possono andare perduti od essere distrutti per una serie di cause. Le applicazioni, che si trovano ai livelli superiori, richiedono che il trasferimento dei dati sia affidabile. Nel caso della rete Internet il protocollo TCP assicura questo risultato.

Le principali caratteristiche del protocollo TCP sono:

- è orientato alla connessione, con conferma e controllo del flusso;
- fornisce un servizio full-duplex;
- utilizza una commutazione a circuiti virtuali.

Il protocollo TCP fornisce i seguenti servizi:

- definisce il formato dei dati e degli acknowledgement che due computer si devono scambiare per avere una trasmissione affidabile;
- definisce le procedure per assicurare la correttezza dei dati;
- implementa un meccanismo per distinguere le destinazioni multiple all'interno di una stessa macchina;

- implementa meccanismi per gestire la perdita e la duplicazione di pacchetti;
- specifica il modo in cui due computer iniziano la trasmissione della sequenza di bit e come questi si accordano sulla fine della trasmissione.

Il TCP non impone particolari limitazioni alla rete sottostante, per cui funziona su molte reti, quali collegamenti telefonici commutati, reti locali, reti ad alta velocità in fibra ottica, collegamenti punto-punto a bassa velocità, ecc.

### Formato del segmento TCP

L'unità informativa del TCP prende il nome di segmento. I segmenti vengono scambiati tra due computer per:

- stabilire la connessione;
- trasferire i dati;
- inviare gli ACK;
- inviare i window advertisement;
- chiudere la connessione.

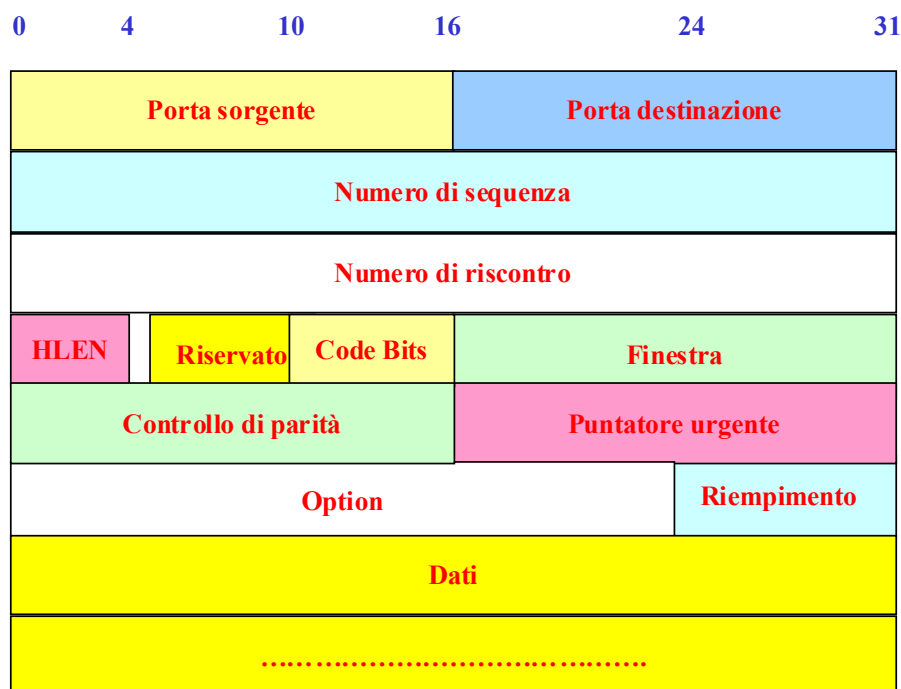


Figura 4.19 - Formato del segmento TCP.

Il formato di un segmento TCP è diviso in due campi, l'header e il campo dati ed è mostrato nella Figura 4.19. Descriviamo in dettaglio i diversi campi:

- porta sorgente: numero della porta TCP a cui sono associati gli applicativi;
- porta destinazione: numero della porta TCP di destinazione a cui sono associati gli applicativi;

- numero sequenza: numero di sequenza (posizione) del primo byte del campo dati del messaggio. Viene utilizzato anche come identificatore della "*sliding window*".
- numero di riscontro: contiene il numero di sequenza del primo byte che la stazione sorgente si aspetta di vedere confermato. Rappresenta perciò il campo di acknowledgment con tecnica di piggybacking della trasmissione nella direzione apposta.
- HLEN: indica la lunghezza dell'header TCP, misurata in multipli di 32 bit; questo valore è necessario perché il campo option ha una lunghezza variabile.
- Riservato: indica un campo riservato ad applicazioni future.
- Code bit: contiene informazioni sulle caratteristiche e finalità del segmento.
- Finestra : contiene la dimensione della finestra di ricezione TCP in trasmissione e quindi le dimensioni del buffer per il traffico in ingresso.
- Controllo di parità: viene utilizzato per rivelare errori sull'header.
- Puntatore urgente: indica il primo byte urgente del pacchetto.
- Option: serve per negoziare con il TCP dell'altra macchina vari parametri, quali la massima lunghezza di un segmento.
- Riempimento: è un campo fittizio la cui lunghezza dipende da quella del campo opzioni. La somma delle lunghezze dei due campi deve essere uguale a 32 bit.

### *Meccanismo per il controllo degli errori*

Il protocollo TCP garantisce l'affidabilità dell'informazione ricevuta mediante l'utilizzo di una appropriata tecnica ARQ. Esso utilizza una tecnica **sliding window** (finestra a scorrimento) per regolare le trasmissioni e le ritrasmissioni. La ricezione dei dati viene confermata dalla stazione ricevente; tale conferma può essere inviata in modo separato oppure essere inserita in un datagram in transito in direzione opposta con una tecnica di piggybacking. Il meccanismo a finestra del TCP risolve il problema di una trasmissione efficiente e del controllo di flusso. Il TCP vede la sequenza di bit da trasmettere come una sequenza di byte che viene trasmessa in gruppi detti **segmenti**. In genere ciascun segmento viaggia in Internet in un singolo datagram IP.

Come tutti i protocolli a finestra, TCP ha un numero massimo di dati in attesa di conferma; nel TCP tale dimensione massima è specificata come numero di byte e non come segmenti. I byte di una sequenza sono numerati e la stazione trasmittente utilizza tre puntatori per ciascuna connessione che svolgono le seguenti funzioni:

- il primo puntatore C1 separa, sulla sua destra, i byte che sono stati trasmessi e che hanno ricevuto un ACK;
- il secondo C2 individua l'ultimo byte che può essere trasmesso prima che venga ricevuto un ACK;
- il terzo C3 separa, all'interno della finestra, i byte che sono stati trasmessi da quelli da trasmettere.

Nella Figura 4.20 è mostrato un esempio di applicazione della finestra scorrevole del TCP. Nell'esempio i primi due byte sono stati trasmessi ed hanno ricevuto un riscontro positivo. I byte tra C1 e C2 (cioè i byte 3, 4 5,6) sono stati spediti e sono in attesa di riscontro mentre i byte tra C2 e C3 (cioè i byte 7, 8, e 9) devono essere ancora trasmessi, ma possono essere trasmessi anche senza ricevere un ACK. I bit successivi al contatore C3 (nell'esempio i byte dal 10 in poi) non possono essere trasmessi fino a quando non sarà ricevuto un ACK, che faccia scorrere la finestra verso sinistra.

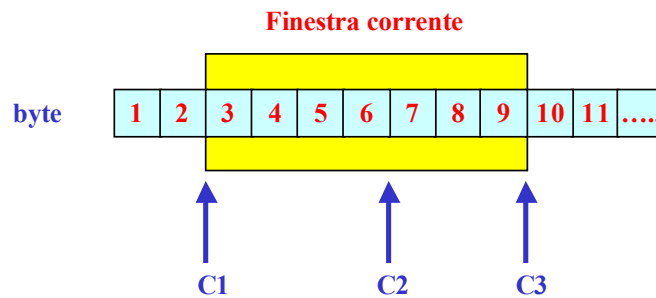


Figura 4.20 – Meccanismo a finestra utilizzato nel TCP per il controllo degli errori.

Il TCP risolve il problema del controllo di flusso rendendo variabili le dimensioni della finestra. Ciascun ACK specifica anche il **window advertisement**, ovvero quanti byte aggiuntivi saranno accettati dal destinatario. Se questo numero aumenta, il mittente aumenta la dimensione della finestra; se diminuisce, il mittente diminuisce la dimensione della finestra. In casi estremi, il destinatario può inviare un window advertisement di zero per bloccare completamente la trasmissione.

### **Il protocollo UDP**

Il protocollo UDP è un protocollo alternativo al TCP. UDP risulta molto più semplice del TCP, ma, contrariamente al TCP, non garantisce l'affidabilità dei dati ricevuti. UDP utilizza IP per la consegna dei pacchetti e, rispetto al livello IP, fornisce soltanto la possibilità di distinguere, attraverso il meccanismo delle porte, tra destinazioni multiple all'interno della stessa macchina. In particolare:

- non usa tecniche ARQ
- non ordina i pacchetti giunti a destinazione
- non fornisce feedback per controllare la velocità con cui scorre l'informazione tra le macchine

Per questo motivo i pacchetti UDP possono essere persi o duplicati e possono arrivare fuori ordine. Inoltre i pacchetti UDP possono arrivare più velocemente di quanto il destinatario riesca a processarli. Tutti questi aspetti devono dunque essere gestiti dai processi a livello superiore.

Spesso le applicazioni che si poggiano su un UDP funzionano bene in ambito locale, su reti affidabili e ad alta velocità, mentre non funzionano correttamente sulle reti geografiche.

### **Formato del pacchetto UDP**

Il pacchetto UDP è chiamato **user datagram (datagram di utente)** ed è mostrato nella Figura 21. L'header del pacchetto UDP è costituito dai seguenti **4 campi**, ciascuno lungo 16 bit:

- Porta sorgente UDP: questo campo è opzionale. Quando è presente indica la porta a cui devono essere inviate eventuali repliche. Se non è utilizzato viene messo uguale a 0.
- Porta di destinazione UDP: indica il numero della porta di destinazione.
- Lunghezza messaggio UDP: indica la lunghezza in byte del datagram UDP, incluso l'header e i dati. Il valore minimo è 8, corrispondente alla lunghezza della sola intestazione.
- Somma di parità UDP: questo campo è opzionale. Se non è usato, deve essere 0. Considerando che il protocollo IP non calcola il checksum sui dati (ma solo sull'header), questo è l'unico elemento che indichi se i dati siano giunti a destinazione in modo corretto. Il checksum viene calcolato dividendo i dati a gruppi di 16 bit e prendendo il complemento a 1 della somma dei complementi a 1.

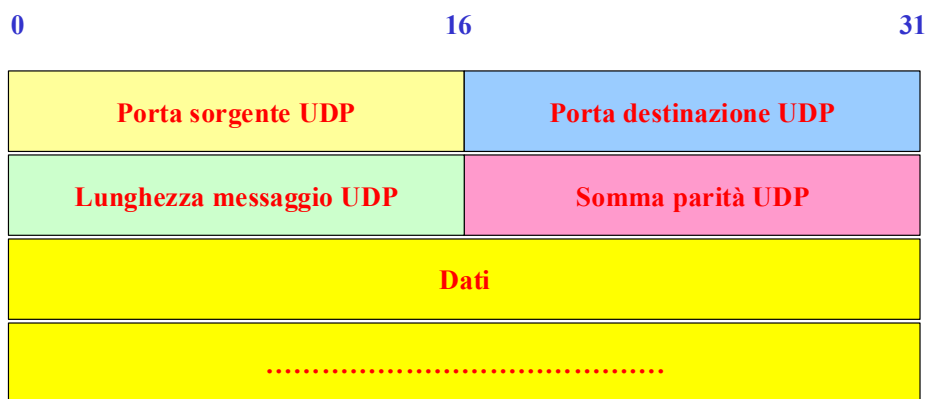


Figura 4.21 - Formato del datagram di utente nel protocollo UDP.

La somma di parità UDP consente anche di verificare che il datagram UDP ha raggiunto la destinazione corretta e viene effettuata utilizzando il datagram ricevuto e un pseudo-header, che non viene trasmesso, ma che il ricevitore è in grado di ricostruire dalle informazioni contenute nel datagram. L'UDP antepone una pseudo-intestazione al datagram UDP, aggiunge 8 bit uguali a zero per riempire il datagram in modo che il suo contenuto sia multiplo intero di 16, ed esegue la somma di verifica sull'intero oggetto (Figura 4.22). Il byte utilizzato per il riempimento e la pseudo-intestazione non sono trasmessi con il datagram UDP, e nemmeno vengono presi in considerazione per il calcolo della lunghezza nell'header UDP.

Per calcolare la somma di verifica, il software mette tutto a zero il campo della somma di verifica, e dopo aggiunge una somma in complemento ad uno dell'intero oggetto, compresi la pseudo-intestazione, l'intestazione dell'UDP e dei dati di utente. La chiave di interpretazione della pseudo-intestazione risiede nella comprensione che la destinazione è costituita da una macchina specifica e da una specifica porta di protocollo, all'interno della stessa macchina. L'intestazione dell'UDP specifica di per sé stessa soltanto il numero della porta di protocollo. In questo modo, per verificare la destinazione, l'UDP presente nella macchina mittente calcola una somma di verifica che comprende l'indirizzo IP di destinazione insieme al datagram UDP. All'arrivo alla destinazione finale, il software di UDP controlla la somma di verifica che comprende l'indirizzo IP di destinazione ricavato dall'intestazione del datagram IP che viene portato all'interno del messaggio UDP. Se la somma di verifica coincide, si può asserire che il datagram ha raggiunto l'host di destinazione voluto ma anche la corretta porta di protocollo all'interno dello stesso host.

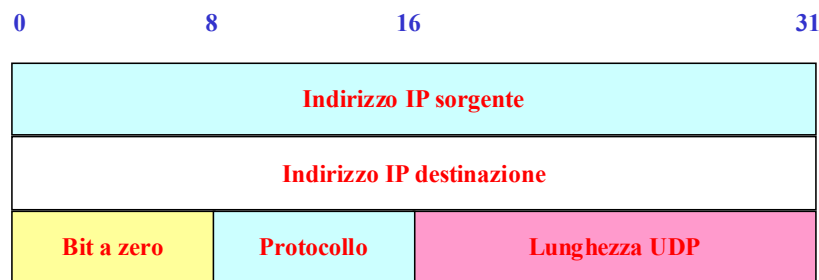


Figura 4.22. Formato del pseudo-header UDP.

Lo scopo dello pseudo-header è quello di verificare che l'UDP datagram abbia raggiunto la corretta destinazione, ovvero una specifica macchina e una specifica porta all'interno di quella macchina. Alla destinazione, il software deve ricostruire lo pseudo-header estraendo l'indirizzo IP di destinazione e deve ricalcolare il checksum. Lo pseudo-header consiste in **12 byte** in cui sono presenti:

- Indirizzo IP della sorgente (32 bit);
- Indirizzo IP di destinazione (32 bit);
- Bit uguali a zero (8 bit);
- Tipo di protocollo (8 bit);
- Lunghezza UDP (16 bit).

Il calcolo del checksum nel protocollo UDP rappresenta una **violazione** del modello ISO/OSI, che si basa sulla separazione delle funzioni di ciascun strato. Infatti, per il calcolo del checksum, il protocollo UDP deve interagire con il livello IP sottostante, per farsi fornire l'indirizzo IP destinazione, ma soprattutto l'indirizzo IP sorgente, che non può essere noto a priori dai livelli superiori all'IP, in quanto dipende dalla scelta di routing.

Il protocollo UDP, attraverso il meccanismo delle porte, implementa la funzione multiplexing e demultiplexing, tipica dei protocollo del livello di trasporto (Figura 4.23).

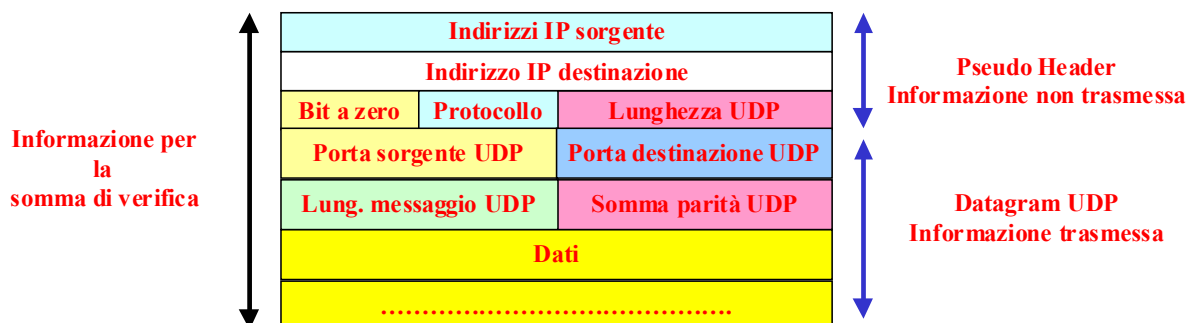


Figura 4.23 – Formato del datagram utilizzato per il calcolo del checksum nel protocollo UDP.

Nella pratica, ciascuna applicazione deve negoziare con il S.O. l'utilizzo di una porta prima di poter inviare UDP datagrams. Spesso in questa fase di negoziazione, il S.O. crea la coda associata a quella porta; l'applicazione può specificare o modificare la dimensione della coda.



# Capitolo 5: Le Reti locali

## 5.1. Introduzione

La crescente diffusione di sistemi informatici distribuiti e la disponibilità di grandi capacità elaborative a basso costo ha determinato la nascita e lo sviluppo delle reti locali (**LAN**) a partire dalla fine degli anni '70.

Nelle reti locali tutte le stazioni condividono lo stesso canale trasmissivo, generalmente ad alta velocità. Quando una stazione ottiene l'accesso alla trasmissione, essa occupa temporaneamente tutta la banda disponibile per il tempo necessario a trasmettere uno o più pacchetti. Tipicamente, i pacchetti immessi sulla rete sono ricevuti da tutte le stazioni presenti sulla LAN e perciò la trasmissione è di tipo "broadcast". Ogni pacchetto contiene l'indirizzo di destinazione, oltre a quello della stazione trasmittente, e può però essere recuperato dalla stazione ricevente.

Le principali proprietà e caratteristiche delle reti locali sono:

- *elevate velocità*. Infatti le reti LAN più diffuse oggi operano a velocità tra i 10 Mbit/sec e i 100 Mbit/sec;
- *basse probabilità di errore*. Le reti LAN, a causa delle estensioni ridotte, possono consentire di raggiungere velocità di trasmissione molto basse, per cui non sono generalmente utilizzate tecniche di controllo degli errori;
- *elevata affidabilità*. Le reti locali, se opportunamente progettate, possono continuare ad operare anche in presenza di guasti o malfunzionamenti;
- *espansibilità*. Le reti locali possono essere progettate in modo da crescere nel tempo secondo le esigenze dell'utente senza significativi cambiamenti nella rete;
- *basso costo*. Le reti locali hanno ormai raggiunto una elevata diffusione in tutti gli ambienti e presentano per questo motivo un costo complessivo abbastanza modesto.

Questi importanti vantaggi possono essere ottenuti mediante un'opportuna progettazione e realizzazione della rete. Le reti LAN non rispettano generalmente gli standard CCITT o ISO per una serie di motivi, tra cui i principali sono:

- le reti locali sono spesso nate in modo sperimentale;
- sono reti private;
- gli standard CCITT o ISO sono spesso troppo rigidi e talvolta richiedono troppo tempo per essere emanati.

Per consentire uno sviluppo non-proprietario e per garantire l'interconnessione di reti diverse, lo sviluppo di norme e di standard nelle reti locali è un aspetto essenziale. Per questo motivo, l'associazione degli ingegneri elettronici americani IEEE ha costituito il gruppo **IEEE 802**, composto da vari comitati, per lo sviluppo di standard per le reti LAN e MAN. Questo gruppo ha prodotto una serie di standard riportati nella tabella 5.1 e rappresenta oggi il punto di riferimento per tutte le attività nel settore delle reti locali. I comitati IEEE definiscono le caratteristiche dei prodotti e della rete locale. Il problema della realizzazione fisica della rete (**cablaggio**) è stato affrontato alla fine degli anni '80 e sono

state emanate dall'associazione EIA norme relative al cablaggio di una rete LAN; queste norme sono state raccolte nello standard EIA/TIA 568.

COMITATO IEEE	STANDARD LAN
802.1	Architettura, Gestione
802.2	LLC
802.3	CSMA/CD
802.bis	100 Baset
802.4	Token bus
802.5	Token ring
802.6	DQDB - rete MAN
802.7	Broadband technical advisory group
802.8	Fiber - optic technical advisory group
802.9	Reti fonia-dati integrate
802.10	Sicurezza
802.11	Wireless
802.12	100VG - Any LAN

Tabella 5.1: Comitati IEEE per le reti locali.

In sintesi, si può perciò affermare che la progettazione e realizzazione di una rete LAN investe due problematiche, come mostrato nella Figura 5.1:

- *la struttura trasmissiva ( protocolli, modalità di gestione dei collegamenti, ...) regolata dagli standard IEEE 802;*
- *il cablaggio della rete, regolato dalle norme EIA/TIA 568 e ISO/IEC 11801.*



Figura 5.1. Progettazione di una rete locale.

## 5.2. Struttura trasmissiva di una rete locale

Il gruppo IEEE 802 ha definito una struttura generale di una rete locale basata su una suddivisione in livelli, come nel caso del modello OSI. Tuttavia, per una serie di motivi, non è stato possibile mantenere una corrispondenza precisa tra il modello OSI e quello sviluppato per le reti locali.

Il concetto alla base dello sviluppo degli standard IEEE 802 è che le reti LAN o MAN devono fornire un'interfaccia unificata verso il livello di rete, anche se utilizzano tecnologie trasmissive diverse. Per questo motivo il gruppo IEEE 802 definisce soltanto i livelli inferiori, che corrispondono al livello fisico e di link del modello OSI, come mostrato nella Figura 5.2.

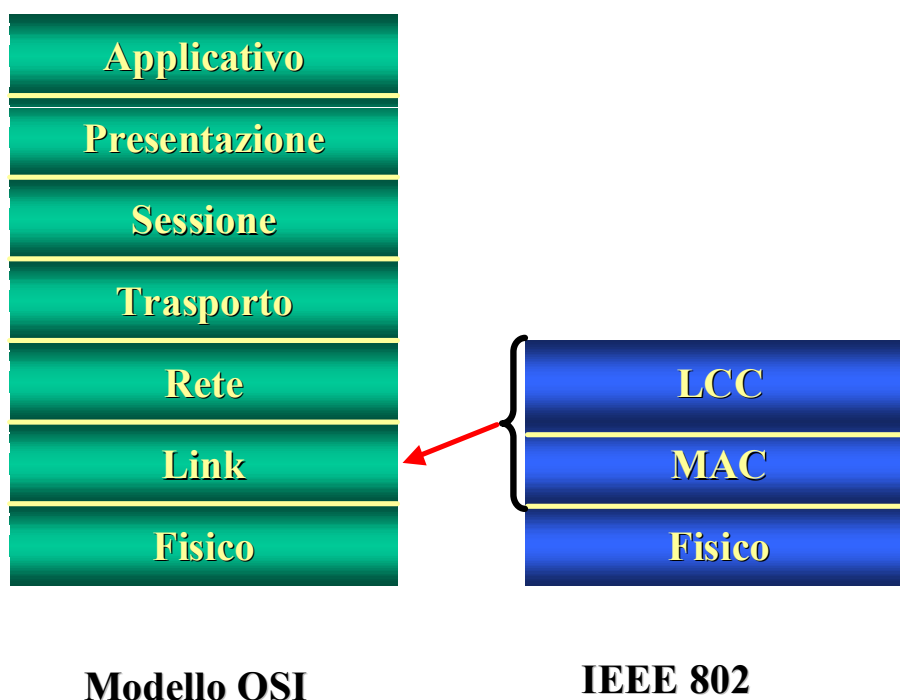


Figura 5.2. Modello OSI e IEEE 802.

Il modello proposto da IEEE 802 divide i due livelli inferiori (livelli fisico e di collegamento) in tre sottolivelli:

1. **livello fisico;**
2. **livello MAC (Medium Access Control);**
3. **livello LLC (Logical Link Control).**

Il livello fisico specifica le caratteristiche dei segnali per la trasmissione sul mezzo fisico (cavo coassiale, doppino, fibra ottica).

Il livello MAC caratterizza le modalità per la condivisione del mezzo trasmissivo tra gli utenti. *Questo livello è specifico per ogni LAN* ed esistono diversi protocolli di livello MAC. Il livello MAC è generalmente realizzato sulla scheda di rete e quindi mediante un'apposita struttura hardware.

*Il livello LLC è comune a tutte le reti locali*, poiché specifica l'interfaccia unificata verso il livello di rete. Il livello LLC è descritto dallo standard IEEE 802.2. Il livello LLC è realizzato generalmente via software.

### *Livello MAC*

Il livello MAC rappresenta l'elemento centrale nel funzionamento della rete locale, poiché gestisce l'accesso alla rete da parte degli utenti. Per questo motivo, a livello MAC viene definito un metodo di accesso multiplo in grado di evitare conflitti tra utenti e regolare la corretta trasmissione dei messaggi.

I protocolli di accesso multiplo utilizzati nelle reti locali possono essere divisi in due classi:

- *accesso multiplo casuale;*
- *accesso multiplo deterministico.*

Nelle reti LAN i protocolli più noti sono il CSMA/CD (di tipo casuale) e il token passing (di tipo deterministico).

*Il livello MAC, come il formato del frame, è specifico per ogni tipo di LAN* e quindi sarà descritto per ogni tipo di LAN nei prossimi capitoli. Tuttavia, alcuni campi essenziali per il funzionamento sono presenti in tutti i formati indipendentemente dal tipo di LAN. Questi campi essenziali, mostrati nella Figura 5.3, sono:

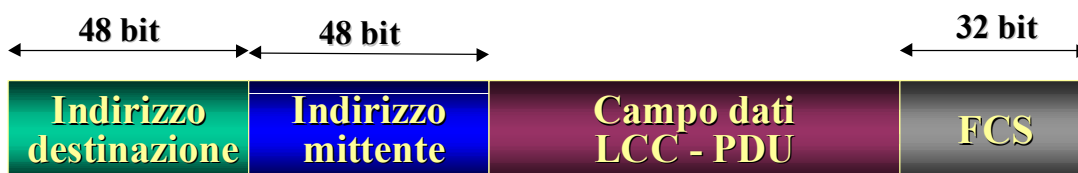


Figura 5.3. Formato dell'unità informativa a livello MAC (PDU-MAC).

- gli indirizzi della stazione di destinazione e del mittente. Questi indirizzi sono detti **indirizzi a livello MAC<sub>i</sub>**;
- il campo dati ha una lunghezza diversa a seconda del tipo di rete utilizzato;
- il campo FCS (Frame Control Sequence) contiene i bit di ridondanza di un codice per rivelare la presenza di errori nel frame.

### *Indirizzi a livello MAC*

L'uso degli indirizzi a livello MAC è stato standardizzato dal comitato IEEE 802. Questo comunicato consente di scegliere tra i seguenti valori di lunghezza:

- 16 bit
- 48 bit

Per le LAN IEEE 802.6 è possibile anche il valore di 60 bit.

La scelta di 16 bit presenta il vantaggio di ridurre la lunghezza dell'header del frame e quindi aumenta l'efficienza della LAN. Inoltre il numero di indirizzi è sufficiente per ogni singola LAN. Tuttavia, esso richiede la presenza di un gestore degli indirizzi di ciascuna LAN che assegna l'indirizzo alle singole apparecchiature al momento in cui sono connesse in rete. Inoltre lo spostamento di un'apparecchiatura da una rete all'altra implica che deve essere aggiornato l'indirizzo da parte del gestore.

Per evitare questi problemi oggi si utilizzano indirizzi MAC a 48 bit. Infatti in questo caso si possono fornire indirizzi validi globalmente per ogni dispositivo. Tale indirizzo è fornito direttamente dal costruttore ed è quindi indipendente dalla rete su cui viene inserito il dispositivo. In questo momento è possibile realizzare tecniche di *plug e play*, per cui il dispositivo può essere inserito in rete senza l'intervento di nessun operatore,

L'uso di **indirizzi universali** richiede la presenza di un'autorità che distribuisca gli indirizzi. Quest'autorità, inizialmente Xerox, è oggi rappresentata da IEEE. Il costruttore richiede un blocco di indirizzi composto  $2^{24}$  indirizzi, ciascuno composto da 6 byte (Figura 5.4) con la seguente struttura:

- i primi 3 byte identificano il costruttore;
- i rimanenti 3 byte ( $2^{24}$  indirizzi) sono a disposizione del costruttore per identificare i singoli dispositivi.

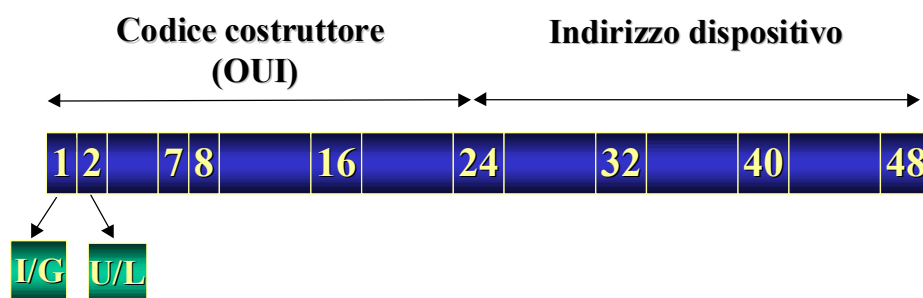


Figura 5.4. Struttura indirizzo MAC a 48 bit.

Nel primo byte dell'indirizzo MAC sono presenti bit che forniscono varie informazioni sul tipo di indirizzo:

- il primo bit o **I/G (Individual/Group)** serve a distinguere tra indirizzi individuali o di gruppo. Se il bit è 0 l'indirizzo si riferisce ad un singolo dispositivo, mentre se il bit è 1 l'indirizzo è relativo ad un gruppo logico di dispositivi. In questo modo il costruttore ha a disposizione  $2^{24}$  indirizzi individuali e  $2^{24}$  indirizzi di gruppo.
- Il secondo bit, **U/L (Universal/Local)** indica se l'indirizzo è globale (assegnato da IEEE) o deciso localmente.

A seconda del tipo di applicazione, l'indirizzo MAC di destinazione mostrato nella Figura 5.3 può essere di tre tipi:

- *singolo*, se è indirizzato ad un singolo dispositivo;
- *multicast*, se è indirizzato ad un gruppo di dispositivi;

- *broadcast*, se è indirizzato a tutti i dispositivi. L'indirizzo broadcast è FF-FF-FF-FF-FF-FF.

Quando il livello MAC di un dispositivo riceve un frame effettua una serie di controlli prima di passarlo a livello superiore. In particolare:

- controllo della lunghezza del frame per verificare se è ammissibile per la rete LAN su cui è stato trasmesso;
- controllo della presenza di errori mediante il campo FCS.

Nel caso in cui uno di questi controlli non risulti soddisfatto si procede alla ritrasmissione. In caso di esito positivo, il dispositivo analizza l'indirizzo MAC di destinazione ed effettua le seguenti operazioni:

- se l'indirizzo MAC è relativo ad un singolo dispositivo, e questo è uguale a quello memorizzato nella scheda del dispositivo (ROM) viene inviato il campo informativo del frame (LCC-PDU) al livello LLC. In caso opposto il frame non è analizzato;
- se l'indirizzo MAC è di tipo broadcast, LLC-PDU è passato al livello superiore;
- se l'indirizzo MAC è di tipo multicast, LLC-PDU è inviato a livello LLC solo se l'indirizzo è nel gruppo di multicast.

### *Livello LLC*

Il livello LLC, definito dallo standard IEEE 802.2, è unico per tutte le reti LAN. Poiché questo livello deve fornire un'interfaccia unica per le LAN verso il livello di rete e deve essere simile a quello delle reti geografiche, il livello LLC utilizza una variante del protocollo HDLC standardizzato nel modello OSI per le reti geografiche. Il frame LLC ha il formato mostrato nella Figura 5.5.

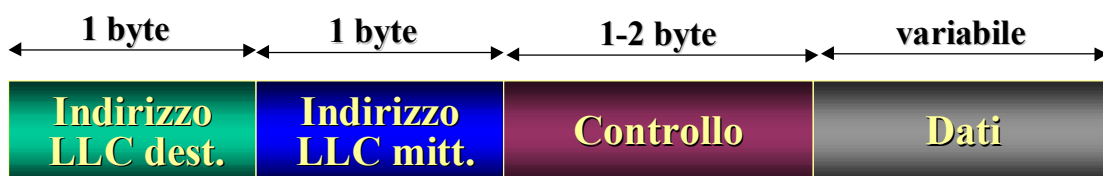


Figura 5.5. Formato della trama LLC.

Gli **indirizzi LLC** servono per individuare i protocolli del livello di rete su cui si appoggiano la rete locale che ha inviato il pacchetto (indirizzo LLC del mittente) e la rete locale a cui è diretto il pacchetto (indirizzo LLC del destinatario). Sono composti da 8 bit, di cui:

- bit **I/G (Individual/Group)** indica se l'indirizzo è rivolto ad ogni singolo utente o ad un gruppo di utenti;
- bit **U/L (Universal/Local)** indica se l'indirizzo è assegnato da IEEE e su base locale.

I rimanenti 6 bit consentono di individuare il protocollo di rete utilizzato scelti tra quelli standardizzati a livello internazionale.

Il livello LLC prevede tre modalità, o varianti, di servizio, e precisamente:

- **servizio senza connessione e senza conferma;**
- **servizio basato su una connessione logica;**
- **servizio senza connessione con conferma.**

Le differenti modalità sono anche chiamate LLC1, LLC2, e LLC3.

Il primo tipo di servizio invia le trame con una modalità di tipo datagram e non prevede alcuna forma di conferma sulla correttezza dei dati ricevuti. In questo caso devono essere i livelli superiori ad effettuare i controlli e garantire il corretto recupero dell'informazione.

Nel secondo tipo di servizio, che ha una stretta analogia con le modalità basate su circuito virtuale nelle reti a commutazione di pacchetto, è necessario che inizialmente venga stabilita una connessione tra i punti di accesso al servizio dell'utente chiamante o chiamato. Il livello LLC controlla poi che su questa connessione logica lo scambio dei dati avvenga in modo corretto e nella giusta sequenza di trame.

L'ultimo tipo di servizio, oltre a richiedere come il primo, la preventiva connessione logica, fornisce un servizio di acquisizione delle trame trasmesse a livello di singola trama e richiede quindi che ogni trama trasmessa sia confermata (correttamente ricevuta) prima di procedere all'invio della trama successiva.

### **5.3 Mezzi trasmissivi**

Il mezzo di trasmissione costituisce il collegamento fisico tra gli elaboratori e le apparecchiature di rete. Per assicurare le prestazioni migliori il mezzo deve essere poco dispersivo e poco dissipativo, deve avere, quindi, bassi valori di resistenza, capacità ed induttanza e deve essere il più possibile indeformabile quando sottoposto a trazione durante la posa per evitare il deterioramento delle sue qualità trasmissive. I valori di resistenza, capacità ed induttanza presenti sul cavo sono sintetizzati in un unico parametro detto impedenza. Sia il trasmettitore che il ricevitore devono adattarsi a questo valore per ottimizzare la trasmissione dati, cioè per aumentare il più possibile la potenza ricevuta. Inoltre l'impedenza deve essere invariante rispetto alla frequenza di utilizzo, o avere un range di oscillazione molto limitato.

I mezzi più comunemente usati sono: la coppia intrecciata o doppino in rame, attualmente il più diffuso; il cavo coassiale, quasi completamente abbandonato; le fibre ottiche. Nelle reti di ultimissima generazione, laddove non sia possibile effettuare il cablaggio, vengono realizzate delle connessioni wireless, che utilizzano le onde radio o i raggi infrarossi per il trasferimento di informazioni punto-punto.

La scelta del mezzo di trasmissione, volta ad ottimizzare le prestazioni della rete LAN che si vuole realizzare, deve essere effettuata confrontando il costo e la facilità di installazione; la banda di trasmissione del cavo, che può consentire una o più sessioni contemporaneamente; la massima velocità di trasmissione permessa; l'estensione della rete.

## Doppino telefonico (Cavo twisted pair)

La coppia intrecciata, solitamente detta doppino telefonico, è il mezzo trasmissivo più utilizzato per il cablaggio delle reti LAN. Come indicato dal nome, consiste di coppie di conduttori di rame, ciascuna delle quali è detta doppino, intrecciate l'una attorno all'altra per renderle particolarmente immuni ai disturbi elettromagnetici in quanto le correnti che attraversano i due conduttori sono di uguale intensità e verso opposto e quindi generano campi magnetici opposti che tendono ad annullarsi; si limita così il trasferimento di segnale tra coppie adiacenti (cross-talk).

Il doppino, nato per la telefonia in banda base (spettro del segnale di 3 KHz), è stato oggetto di un'evoluzione tecnica che lo ha portato ad essere un mezzo di trasmissione in grado di supportare segnali a frequenze dell'ordine di centinaia di MHz, rendendolo adatto alla realizzazione di collegamenti con velocità di trasmissione che va da 10 Mbps fino a 100 Mbps.

Esistono diversi tipi di doppino telefonico:

- *UTP (Unshielded Twisted Pair)*: doppino non schermato (il più diffuso, soprattutto per collegare le prese utente, è il cavo a 4 coppie da 24 AWG di diametro per conduttore ed impedenza pari a 100  $\Omega$ );
- *Screneed FTP (Foiled Twisted Pair)*: doppino con unico schermo per tutto il cavo;
- *STP (Shielded Twisted Pair)*: doppino con uno schermo per ogni coppia più uno schermo globale (la rete Token Ring di IBM usa un STP composto da due coppie singolarmente schermate da 150  $\Omega$ ).

La coppia intrecciata non schermata (UTP) è la coppia di fili telefonici standard. Ciascun filo è isolato ed avvolto attorno ad un altro filo in modo da formare una coppia. I collegamenti standard per ufficio prevedono solitamente da 2 a 4 coppie per cavo portante. Ciascuno di essi è ricoperto da uno schermo non metallico (solitamente plastica o PVC).

La scelta del tipo di mezzo da utilizzare è molto complessa, in quanto è necessario tenere conto di numerosi parametri elettrici a tutte le frequenze di funzionamento interessate dalle varie applicazioni.

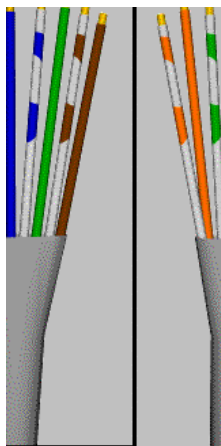


Figura 5.6. Esempio di doppino telefonico UTP a quattro coppie.



Per far fronte a questa esigenza l'Electronic Industries Association e la Telecommunications Industries Association (EIA/TIA) hanno definito le seguenti categorie standard per i doppini non schermati (UTP):

- Categoria 3 (High Speed Data): prima categoria di cavi adatta a realizzare reti locali fino a 10 Mbps, tale categoria è certificata fino a 16 MHz; sono cavi indicati per soddisfare gli standard 10base-T e Token-Ring fino a 4 Mbps;
- Categoria 4 (Low Loss, High Performance Data): cavi per LAN Token-Ring o 10base-T/100base-T fino a 16 Mbps; tale categoria garantisce ottime prestazioni per frequenze che raggiungono i 20 MHz;
- Categoria 5 (Low Loss, Extended Frequency, High Performance Data): comprende i migliori cavi disponibili, che supportano rate di trasmissione fino a 100 Mbps, con frequenze di funzionamento che arrivano a 100 MHz; questi cavi sono utilizzati largamente nella realizzazione di reti Ethernet.

Per ottenere maggiore ampiezza di banda, negli ultimi anni, è stata sviluppata la Categoria 6, in grado di operare alla frequenza di 200 MHz, ma per la quale non esistono ancora norme definitive, sebbene i cavi UTP di Cat.6 vengono comunque utilizzati.

I principali vantaggi dei cavi UTP sono: il basso costo, la possibilità di scegliere tra numerosi fornitori, la facilità di installazione e di testing, la rapidità di messa in opera e di sostituzione, la disponibilità delle interfacce hardware più diverse. I cavi UTP, inoltre, costituiscono lo standard per la telefonia, perciò, in molti edifici ad uso commerciale progettati o ristrutturati negli ultimi anni, si può sfruttare tale cablaggio per la realizzazione di reti LAN.

I limiti degli UTP sono dovuti alla bassa qualità dei cavi sia per quanto riguarda il metallo conduttore, sia per il dielettrico che costituisce il rivestimento protettivo. Essi, inoltre, sono sensibili alle interferenze elettriche o al rumore prodotti da altre sorgenti elettriche, come altri fili, cabine e macchine elettriche. Gli accoppiamenti, in cui i segnali di una coppia interferiscono con quelli di un'altra sono un tipico esempio. Le interferenze elettriche non sono un grosso problema in un ufficio, ma possono esserlo in una industria che utilizza macchine elettriche. I disturbi elettromagnetici costringono a ridurre la lunghezza dei cavi.

Il doppino intrecciato viene utilizzato per trasmissioni in banda base, utilizzando un solo canale, con velocità di trasmissione di 10 Mbps su distanze non superiori a 100 metri. In molte reti LAN ad alta velocità si utilizzano degli hub, e gli standard previsti dall'EIA/TIA consentono una distanza massima di 90 metri tra la porta dell'hub e la presa a muro, ed ulteriori 10 metri da quest'ultima al dispositivo di rete.

Il doppino schermato (STP), diversamente dal UTP, presenta un rivestimento costituito da uno schermo a lamina metallica che lo protegge dai disturbi; non è così largamente impiegato come il cavo non schermato in quanto più costoso.

I cavi sono caratterizzati da parametri elettrici che ne descrivono il comportamento al variare della frequenza di funzionamento. Il primo parametro è l'impedenza definita come:  $Z=R+j\omega L$ , che racchiude valori di resistenza, capacità ed induttanza del cavo. L'impedenza caratteristica viene definita come impedenza di ingresso di una linea di trasmissione di lunghezza infinita. Il valore varia con la frequenza, per i cavi di buona qualità l'impedenza deve restare stabile in un range di frequenze piuttosto ampio. Il cavo deve essere adattato

in impedenza con il ricevitore ed il trasmettitore per evitare riflessioni del segnale che comporta la riduzione del rapporto segnale rumore. Le irregolarità nella geometria del cavo producono variazioni nell'impedenza caratteristica, così come, trazioni eccessive e piegature che possono verificarsi in fase di posa. Tali variazioni determinano riflessioni del segnale, riducendone l'energia. Le perdite per riflessione sono misurate in decibel (dB) dal parametro return loss.

Altro parametro è la velocità di propagazione del segnale elettrico nel mezzo, espresso come percentuale rispetto alla velocità  $c$  di propagazione della luce nel vuoto ( $c=3 \cdot 10^8$  m/s). Tale valore è importante, ad esempio, nel calcolo di parametri di funzionamento del protocollo CSMA/CD usato dalla rete Ethernet; viene utilizzato per calcolare la distanza tra i due estremi di un cavo.

L'attenuazione misura l'indebolimento del segnale in dB, è il rapporto tra le tensioni:  $V_1$  in ingresso al cavo, e  $V_2$  che si misura all'uscita:

$$attenuazione(dB) = 20 \log \frac{V_1}{V_2}.$$

Il suo valore cresce con la lunghezza del cavo e con la radice quadrata della frequenza; è uno dei motivi per cui vengono fissate delle lunghezze limite per i cavi. Per esempio il valore massimo di attenuazione alla frequenza di lavoro di 100 MHz è di 22.04 dB per 100 m di cavo.

La vicinanza delle varie coppie determina il passaggio, per induzione elettromagnetica, dei segnali da un doppino ad uno contiguo, questo fenomeno è noto come cross-talk (diafonia), e viene espresso in dB attraverso due parametri: NEXT (Near End Cross-Talk), e FEXT (Far End Cross-Talk). Il NEXT o paradiafonia misura il segnale indotto da un cavo in un cavo vicino, utilizzando un solo strumento di misura costituito da un generatore di segnale, posto su un cavo, ed un misuratore di tensione posto sull'altro cavo, collegato ad una sola estremità del cavo, in prossimità del trasmettitore. Il minimo valore ammesso per il NEXT a 100 MHz è 32 dB per 10 m di cavo. Il FEXT o telediafonia, invece, misura il segnale indotto nel cavo adiacente a quello che trasporta il segnale, con il misuratore di tensione posizionato all'estremo opposto del cavo rispetto al generatore di segnale. Questo tipo di misurazione è di fondamentale importanza per la certificazione del cablaggio effettuato.

I nuovi standard di trasmissione (come il Gigabit Ethernet) utilizzano tutte e quattro le coppie di un cavo UTP/FTP sulle quali il segnale passa in entrambe le direzioni. Ciò aumenta le diafonie in gioco, che si sommano su ogni coppia. Con l'avvento delle nuove categorie le più importanti diafonie sono oggi le cosiddette ELFEXT e PSELFEXT. Il primo parametro, Equal Level FEXT, è la misura della tensione indotta dal segnale di un doppino in rapporto alla tensione d'uscita di un altro e questo per ogni possibile coppia, in altre parole è l'ACR (Attenuation to Cross-Talk Ratio) ottenuto sottraendo l'attenuazione dal FEXT. Per limitare gli effetti dovuti alla diafonia, i doppiini subiscono una torsione con passo variabile da una coppia all'altra.

Se si considera l'effetto complessivo, ossia prodotto da tutti e tre i doppiini su un quarto, otteniamo la PSELFEXT (Power Sum ELFEXT): in questo caso occorre misurare il rapporto  $(DIAF1 + DIAF3 + DIAF4)/OUT2$ . Come si nota, il valore di riferimento è sempre il segnale d'uscita sul cavo n.2. Entrambe le misure sono previste dai nuovi standard delle

nuove categorie, e devono essere controllate anche sui doppini di cat. 5 esistenti, prima di utilizzarli per standard come il Gigabit Ethernet.

Per valutare correttamente la qualità del segnale trasportato da un cavo, viene utilizzato un parametro che è la combinazione dei due appena esaminati. Tale parametro è l'ACR (Attenuation to Cross-Talk Ratio), anch'esso in dB, pertanto è espresso come:

$$\text{ACR(dB)} = \text{NEXT(dB)} - \text{Attenuazione(dB)}.$$

L'ACR di un cavo rappresenta il rapporto tra il segnale attenuato e quello indotto dalla coppia adiacente. Esso dipende dalla frequenza di lavoro e dalla lunghezza del cavo; al crescere della lunghezza del cavo aumenta l'attenuazione del segnale trasmesso, che diventa troppo debole rispetto a quello indotto per diafonia, determinando errori di trasmissione.

I parametri elettici visti consentono di valutare la bontà del cablaggio, e la sua rispondenza alle specifiche. I valori di riferimento sono ottenuti effettuando delle misure sul link, cioè sul percorso che dall'armadio di piano giunge fino alla presa utente, e sul channel o canale, che risponde maggiormente alle condizioni di lavoro reale, in quanto sono compresi anche i patch cord (cavetti di connessione di utente e di apparato), il permutatore di armadio e gli accoppiamenti presa-connettore.

Nella tabella 5.3 vengono riportati i valori massimi di attenuazione, la minima diafonia, l'ACR e le perdite per riflessione massime, utilizzando cavi di categoria 5, 5e (enhanced), valutati a 100 MHz, e per la nuova categoria 6 a 100 MHz ed a 200 MHz.

SPECIFICHE DI CANALE A 100MHz				200MHz
	Cat.5	Cat.5e	Cat.6	Cat.6
Attenuazione	24dB	24dB	24dB	29.2dB
NEXT	27.1dB	30.1dB	39.9dB	39.8dB
PSNEXT	24.1dB	27.1dB	37.1dB	37.8dB
ELFEXT	17dB	17.4dB	23.2dB	21.7dB
PSELFEXT	14.4dB	14.4dB	20.2dB	18.7dB
ACR	3.1dB		18.2dB	
PSARC	0.1dB		15.4dB	
RETURN LOSS	10dB	10dB	12dB	

Tabella 5.3. Specifiche dei parametri per i doppini telefonici.

## Cavo coassiale

Il cavo coassiale consiste di un conduttore centrale di rame ricoperto da un isolante, a sua volta circondato da una guaina di filo metallico o schermo. Il tutto è coperto da un rivestimento esterno, detto jacket, di plastica o gomma.

La schermatura che avvolge il conduttore interno rende il cavo coassiale meno sensibile al rumore o alle interferenze elettriche che provengono da altri cavi o sorgenti elettriche come i motori elettrici; l'attenuazione lungo il cavo, inoltre, è più bassa rispetto al cavo

intrecciato. In termini pratici ciò significa che il cavo coassiale permette velocità di trasmissione relativamente alte su distanze relativamente lunghe.

Esistono vari tipi di cavo coassiale, diversi a seconda del numero di conduttori interni, del materiale isolante utilizzato e del tipo di jacket. Il tipo maggiormente utilizzato nelle reti locali ha un'impedenza di  $50\ \Omega$ , ed è utilizzato per trasmettere il segnale in banda base in un range di frequenze compreso tra 50 e 100 MHz.

Il cavo coassiale è stato il mezzo di trasmissione originariamente utilizzato nelle LAN Ethernet, lo standard 10Base5 prevede l'uso del cavo thick (RG213) con impedenza di  $50\ \Omega$ , ed una attenuazione minima, su un segmento di 500 m, di 8.5 dB a 10 MHz. Tale tipo di cavo, oggi, è previsto dallo standard EIA/TIA-568 per il cablaggio delle dorsali. Per il cablaggio orizzontale, laddove ancora in uso, si preferisce il thin Ethernet (RG58), con le stesse caratteristiche del cavo thick, tranne che per la lunghezza massima del segmento che deve essere di 185 m.

Anche se maggiormente immune ai disturbi, il cavo coassiale è stato soppiantato dal doppino nelle reti di medie prestazioni e dalle fibre ottiche in quelle ad alte prestazioni, a causa del maggior costo e delle maggiori difficoltà di messa in opera. Il cavo coassiale ha come ulteriore limite quello di non essere adatto per realizzare alcune configurazioni di rete, come quella a stella o ad anello.

## Fibre ottiche

Le fibre ottiche sono uno dei mezzi di trasmissione più recenti, e stanno rivoluzionando il mondo delle telecomunicazioni.

La fibra si può considerare come una guida d'onda circolare costituita di un sottilissimo cilindro centrale (core), circondato da uno strato esterno (cladding) avente un diverso indice di rifrazione, realizzati entrambi con materiale dielettrico, generalmente ossido di silicio, il tutto ricoperto da una guaina protettiva. I cavi sono composti da più fibre raggruppate insieme in un'unica guaina contenitrice esterna.

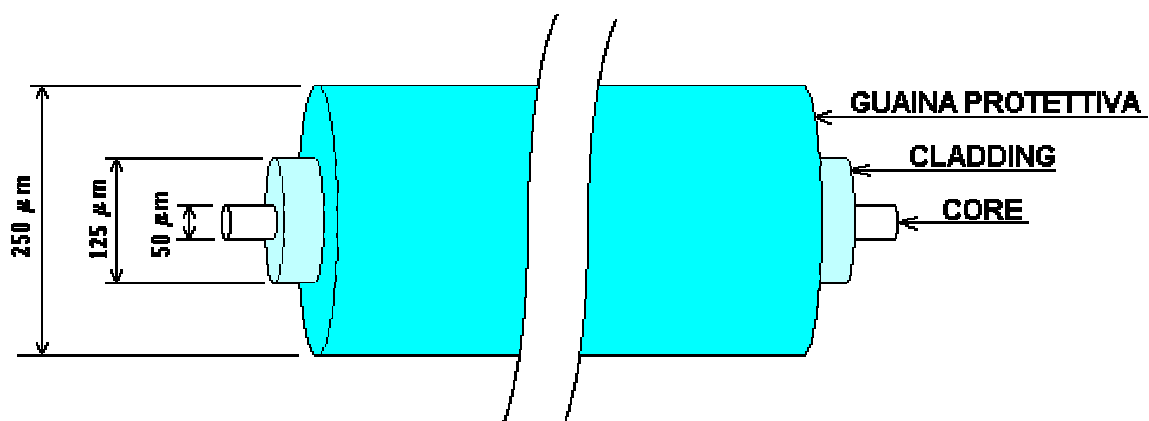


Figura 5.7. Cavo a fibre ottiche.

Le fibre trasportano i segnali attraverso il fenomeno della propagazione della radiazione luminosa, basato sulla variazione dell'indice di rifrazione all'interno del materiale

dielettrico. L'indice di rifrazione  $n$  è definito come il rapporto tra la velocità di propagazione del raggio luminoso nel vuoto ( $c=3 \cdot 10^8$  m/s) e la velocità di propagazione in un mezzo diverso dal vuoto ( $n=c/v$ ), dove  $v$  dipende, naturalmente, dalle caratteristiche e proprietà fisiche del mezzo stesso. Se il mezzo è isotropo e omogeneo allora  $n$  risulta un numero maggiore di uno e costante all'interno del dielettrico.

Quando un raggio luminoso incide su una superficie d'interfaccia tra due mezzi di indici diversi,  $n_1 > n_2$ , esso viene in parte riflesso e in parte rifratto o trasmesso, secondo la legge di Snell:

$$n_1 \sin(\alpha_1) = n_2 \sin(\alpha_2)$$

dove  $\alpha_1$  è l'angolo di incidenza del raggio rispetto la normale alla superficie nel punto di incidenza e  $\alpha_2$  è l'angolo che il raggio rifratto forma con la stessa normale nel secondo mezzo, come si vede nella Figura 5.8.

Poiché  $n_1 > n_2$ , ciò implica che  $\alpha_2$  aumenta all'aumentare di  $\alpha_1$ , fino ad arrivare alla condizione limite per cui  $\alpha_2 = \pi/2$ , in cui si ha il fenomeno di riflessione totale. In questa situazione si definisce l'angolo critico

$$\alpha_c = \sin^{-1} \left( \frac{n_2}{n_1} \right),$$

l'angolo di incidenza oltre il quale si ha assenza di rifrazione. I raggi giacenti su di un piano comprendente l'asse della fibra ottica, che incidono l'interfaccia vetro/aria con angolo maggiore di  $\alpha_c$ , vengono riflessi totalmente e, quindi, restano confinati all'interno della fibra indefinitamente. Il principio appena descritto è alla base del funzionamento di tutti i tipi di fibra ma nel campo delle telecomunicazioni è preferibile poter variare con precisione il valore dell'indice di rifrazione sia della fibra vera e propria (mezzo 1), sia del mezzo che la ricopre (mezzo 2). Entrambi i mezzi sono costituiti da materiale vetroso, gli indici di rifrazione vengono variati con precisione durante la costruzione, mediante l'aggiunta di droganti esterni, quali ossidi di germanio, piombo o alluminio. Il core ha indice di rifrazione  $n_1$  maggiore di quello del cladding  $n_2$ . In una fibra per telecomunicazioni il diametro esterno è tipicamente di  $125 \mu\text{m}$ , mentre il diametro del nucleo varia tra pochi  $\mu\text{m}$  e  $50 \mu\text{m}$  a seconda del tipo di fibra. La fibra così prodotta risulterebbe meccanicamente fragile; è allora necessario irrobustirla mediante ulteriori rivestimenti plastici.

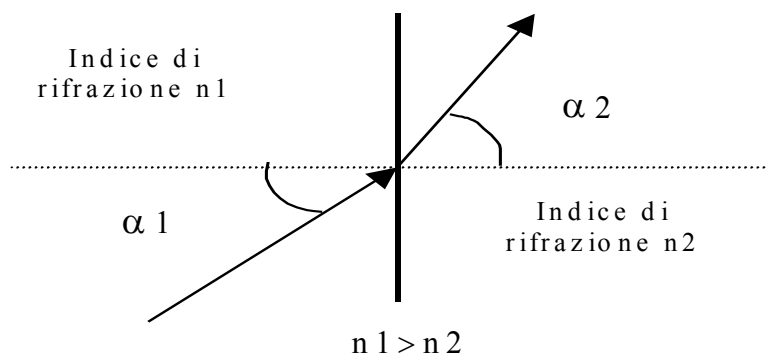


Figura 5.8. Legge di Snell.

Indipendentemente dal tipo, ogni fibra è caratterizzata da alcune grandezze che ne definiscono le proprietà fondamentali. Come si è visto, se un raggio luminoso viene inviato nella fibra con un angolo di incidenza tra core e cladding inferiore all'angolo critico, questo non viene accettato dalla fibra, attenuandosi dopo poche riflessioni. Per questo viene definito un cono d'accettazione, che contiene tutti i raggi che possono propagarsi nella fibra. Il vertice del cono è il centro della faccia d'ingresso della fibra, e l'angolo al vertice viene detto angolo d'accettazione  $\alpha_a$ ; spesso però al posto di  $\alpha_a$  viene fornito NA (apertura numerica), dove  $NA = \sin \alpha_a$ : maggiore è NA più è semplice accoppiare la fibra alla sorgente luminosa. L'angolo di accettazione può essere messo in relazione con i due indici di rifrazione  $n_1$  e  $n_2$  (rispettivamente del nucleo e del mantello) mediante la relazione:

$$\alpha_a = \arcsin[(n_1^2 - n_2^2)^{1/2}].$$

Il tipo di fibra più semplice è la fibra multimodale step-index, cioè con una discontinuità a gradino fra gli indici di rifrazione del core e del cladding. Essa è caratterizzata dal diametro del core molto maggiore della lunghezza d'onda utilizzata generalmente nei sistemi di telecomunicazione ( $1.55 \mu\text{m}$ ). All'interno di tale tipo di fibra l'energia luminosa si propaga per riflessioni successive dando luogo a più modi, ciascuno dei quali segue percorsi di lunghezza diversi, quindi con differenti tempi di propagazione.

La velocità di trasmissione delle fibre multimodali è limitata dalla dispersione modale: un impulso luminoso immesso in fibra, si scompone in vari raggi ognuno dei quali segue un percorso diverso, giungendo a destinazione in tempi leggermente diversi, leggermente deformato a breve distanza, e scomposto in vari impulsi più piccoli a grande distanza. Quando il ritardo tra due raggi diventa paragonabile con la durata dell'impulso inviato in fibra, la dispersione modale determina il fenomeno dell'interferenza intersimbolica, causa della degradazione delle prestazioni del sistema di trasmissione.

Per contrastare il fenomeno della dispersione intermodale sono state fabbricate delle fibre in cui i raggi vengono guidati, mediante la variazione dell'indice di rifrazione del nucleo tra un valore massimo ed uno minimo via via che ci si allontana dall'asse della fibra. Questo tipo di fibre sono indicate come graded-index, in esse i raggi vengono incurvati dalla variazione graduale di  $n$ . Una delle leggi più comuni di variazione di  $n$ , al variare della distanza radiale dall'asse, è detta a "profilo a", dove  $a$  è un parametro fissato in fase di fabbricazione.

Un'altra soluzione per evitare la dispersione modale è offerta dalle fibre monomodali, estremamente sottili, il core ha un diametro di  $8-10 \mu\text{m}$ , in cui i raggi seguono percorsi rettilinei, e permettono di coprire distanze superiori alle fibre multimodali, fino a  $30 \text{ Km}$ . Queste fibre, però, presentano il problema della dispersione cromatica, dovuta ad una proprietà fisica dei vetri silicei di cui la fibra è costituita. Il vetro è un materiale dispersivo, pertanto le componenti a frequenze diverse di cui il segnale modulato è composto si propagano con velocità di gruppo diverse, e, al ricevitore, si ricombinano con ritardi diversi, dando luogo ad una distorsione lineare di fase.

Le prime fibre fabbricate erano caratterizzate da un coefficiente di attenuazione intorno ai  $1000 \text{ dB/km}$  e, quindi, non ne consentivano l'uso pratico. Attualmente per le fibre convenzionali in materiale vetroso si arriva ad  $\alpha = 0.15 \text{ dB/km}$  con lunghezza d'onda  $\lambda = 1.55 \mu\text{m}$  per una fibra monomodale. Il coefficiente di attenuazione dipende dalla lunghezza

d'onda, e diminuisce all'aumentare della lunghezza d'onda, consentendo trasmissioni su distanze sempre maggiori.

Le fibre ottiche hanno ottime prestazioni: con le tecnologie attuali si raggiunge una velocità di trasmissione di circa 50 Gbit/s con un bassissimo tasso d'errore. La pratica attuale di usare velocità dell'ordine dei Gbit/s dipende dall'incapacità di convertire più velocemente segnali elettrici in luminosi. Esse offrono, inoltre, una bassissima attenuazione del segnale luminoso.

Rispetto agli altri mezzi di trasmissione le fibre consentono numerosi vantaggi: maggiore larghezza di banda, maggiore velocità di trasmissione, realizzazione di collegamenti più lunghi, bassissima attenuazione ed elevata immunità ai disturbi elettromagnetici. La realizzazione del cablaggio in fibra, inoltre, comporta minore ingombro, sia di spazio che di peso, dato che due fibre sono più capaci, in termini di banda, di mille doppini. D'altro canto le fibre sono più costose, anche perché richiedono, poi, apparati di rete e dispositivi dedicati; la messa in opera richiede personale specializzato ed attrezzature sofisticate, specie per la realizzazione delle giunzioni. Gli interventi successivi, sia di manutenzione, sia eventuali ampliamenti della rete richiedono interventi costosi e non semplici. Il cavo a fibre ottiche consente una comunicazione unidirezionale, pertanto la realizzazione delle connessioni tra trasmettitori e ricevitori di una rete richiede due fibre.

A causa del costo elevato, quindi, le fibre ottiche, oggi, nella realizzazione del cablaggio delle reti LAN vengono impiegate per collegare edifici distanti, o per le dorsali di edificio.

## **5.4 La rete Ethernet**

Ethernet rappresenta oggi la rete più nota e più diffusa in tutto il mondo. La nascita di Ethernet risale al 1976 quando Xerox utilizzò il protocollo CSMA/CD per realizzare una rete locale con una velocità di 2.94 Mbit/s per collegare oltre 100 stazioni. Ethernet incontrò subito un notevole successo per la sua semplicità realizzativa e le elevate prestazioni; per questo motivo Digital, Intel e Xerox formarono un consorzio DIX per elaborare le specifiche della rete Ethernet a 10 Mbit/s. Negli stessi anni il comitato IEEE 802 iniziò a sviluppare uno standard di rete locale basato su CSMA/CD e simile alla rete Ethernet, noto come IEEE 802.3.

Ethernet e IEEE 802.3 sono molto simili, anche se esistono differenze significative. Oggi si realizzano soltanto reti IEEE 802.3, ma in molti casi si continua ad utilizzare la denominazione di rete Ethernet. In questo capitolo i due termini saranno usati indifferentemente per indicare IEEE 802.3.

Le reti Ethernet e IEEE 802.3 si basano su una struttura a bus con una velocità di 10 Mbit/s. Lo standard IEEE 802.3 specifica il livello fisico e il livello MAC.

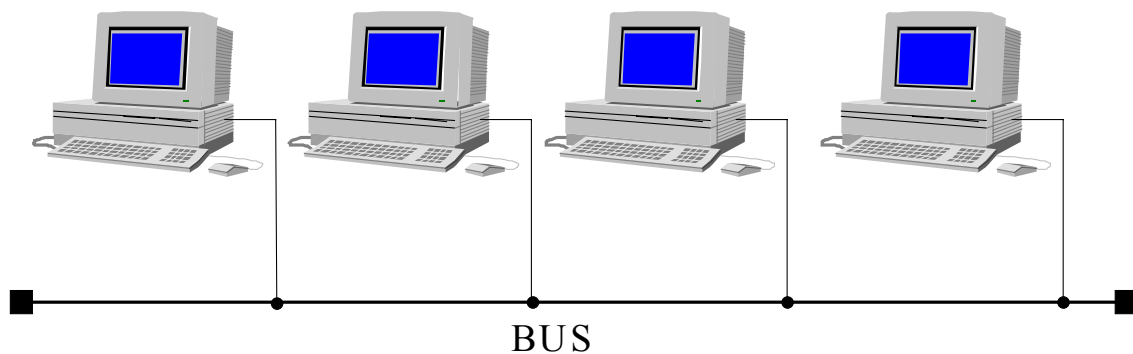


Figura 5.9. Struttura della rete Ethernet.

La topologia di una rete Ethernet o IEEE 802.3 è costruita, da un punto di vista concettuale, attorno ad un bus condiviso, come mostrato nella Figura 5.9. Il bus può essere costituito da vari tipi di cavo coassiale, quale cavo doppino telefonico e fibra ottica.

Il metodo di accesso multiplo CSMA/CD utilizza una struttura completamente distribuita, per cui non è necessaria la presenza di una stazione master.

Questa caratteristica, insieme alla semplicità del protocollo CSMA/CD, sono i motivi della grande diffusione di Ethernet.

#### *Caratteristiche del livello MAC in 802.3*

Il livello MAC in 802.3 definisce le caratteristiche del sistema di accesso multiplo CSMA/CD e la struttura dei dati. Nell'algoritmo CSMA/CD una stazione che deve inviare un pacchetto dati ascolta il canale o bus (carrier sense - CS): se il canale è libero, la stazione può iniziare a trasmettere. Nonostante il meccanismo di carrier sense, è possibile che due stazioni interferiscano tra loro (collisione). Questo inconveniente è determinato dal fatto che il tempo di propagazione del segnale nel bus non è nullo, per cui una stazione A non può sentire l'occupazione del canale da parte di un'altra stazione B fino a quando il segnale generato da B non arriva ad A.

Per rivelare il verificarsi di queste collisioni, una stazione in fase di trasmissione continua ad ascoltare i segnali sul bus, confrontandoli con quelli da lei generati. Nel caso in cui sia rivelata una collisione sono effettuate le seguenti azioni:

- la stazione trasmittente sospende la trasmissione e invia una sequenza di **jamming** composta da 32 bit per avvertire le altre stazioni della collisione;
- la stazione in ascolto, intercettando il jamming, scarta i bit ricevuti;
- la stazione trasmittente ripete il tentativo di trasmissione dopo un tempo generato in modo casuale utilizzando l'algoritmo di **back - off**. Il numero massimo di tentativi di ritrasmissione è 16.

Indichiamo con  $T$  il tempo di propagazione del segnale tra due qualsiasi stazioni presenti sulla rete A e B. Supponiamo che A inizi a trasmettere all'istante  $t$ . La stazione B non si accorgerà che il canale è occupato da un'altra stazione fino all'istante  $t+T$  e quindi può inviare un proprio messaggio prima di tale istante. All'istante  $t+T$  la stazione B rivela la



collisione, cessa di trasmettere il messaggio ed invia un pacchetto di jamming. La stazione A riceve il pacchetto di jamming all'istante  $t+2T$  e soltanto a questo istante, cioè dopo un intervallo di  $2T$ , essa è in grado di rivelare la sovrapposizione del proprio messaggio con quello generato da un'altra stazione.

Se indichiamo con  $T$  il tempo massimo di propagazione del segnale tra due qualsiasi stazioni presenti sulla rete,  $2T$  rappresenta il tempo massimo di trasmissione per una stazione prima di accorgersi di una collisione. La durata di un qualsiasi messaggio deve essere superiore a  $2T$  in modo che la stazione che trasmette sia in grado di rivelare una sua eventuale sovrapposizione con altri messaggi. Questa condizione impone, come vedremo successivamente, una limitazione sulla minima lunghezza consentita per un messaggio.

### Formato del frame IEEE 802.3

Il formato del frame nella rete IEEE 802.3 è mostrato nella Figura 5.10, in cui sono evidenziati i diversi campi che lo compongono:

- **Preambolo.** Questo campo ha una lunghezza di 7 byte, ognuno costituito dalla sequenza 10101010.
- **Delimitatore di inizio del frame.** Questo campo è formato dal byte 10101011 e serve ad indicare l'inizio del frame.

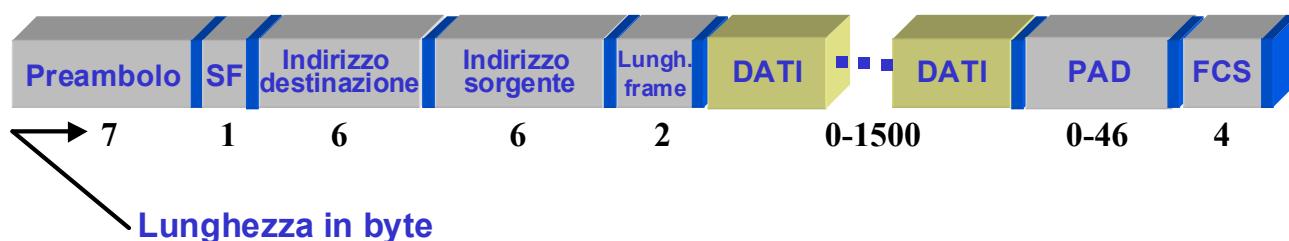


Figura 5.10. Formato del frame della rete IEEE 802.3.

- **Indirizzo della stazione di destinazione e sorgente.** Questo campo può avere una lunghezza di 2 o 6 byte; tuttavia, attualmente sono prevalentemente utilizzati indirizzi formati da 6 byte. Se il bit più significativo del campo indirizzo della stazione di destinazione è uguale a 0, il campo contiene un indirizzo MAC *ordinario*, mentre se tale bit è uguale a 1 allora si ha una trasmissione *multicast*. Al contrario, se l'indirizzo della stazione di destinazione è formato da bit uguali a 1, allora si ha una trasmissione *broadcasting*. Il bit 46 (accanto a quello più significativo) serve a distinguere indirizzi locali e globali (come indicato nel capitolo precedente).
- **Lunghezza del campo dati.** Questo campo indica la lunghezza in byte del campo dati contenuti nel pacchetto.
- **Campo Dati.** Questo campo ha una lunghezza variabile tra 0 e 1500 byte.
- **PDA.** Questo campo ha una lunghezza variabile tra 0 e 46 byte e viene introdotto per garantire che la lunghezza minima del pacchetto non sia inferiore a 64 byte. Come vedremo, questo valore minimo del pacchetto è necessario per un corretto funzionamento del protocollo CSMA/CD.

- **FCS.** Questo campo, formato da 2 byte, consente di effettuare il controllo degli errori sul pacchetto utilizzando un codice ciclico.

#### *Requisiti imposti a livello MAC dal CSMA/CD*

Per una corretta gestione delle collisioni, occorre rispettare nel caso della rete Ethernet 802.3 le seguenti regole fondamentali:

1. la trasmissione può essere iniziata soltanto quando il canale è sentito libero;
2. la collisione con un'altra stazione deve essere rivelata prima che il pacchetto sia stato completamente trasmesso;
3. la fine di un pacchetto è caratterizzato da un periodo di silenzio ITP (Inter Packet gap) uguale a 9.6  $\mu$ s.

Nella tabella 5.4 sono riportati i valori tipici per alcuni parametri della rete IEEE 802.3.

La seconda regola impone una condizione sulla lunghezza minima del messaggio, fissato il mezzo di propagazione (e quindi la velocità di propagazione) e la massima distanza della rete. Nella tabella 5.4 sono riportati i valori tipici per alcuni parametri della rete IEEE 802.3.

<b>ITP</b>	9.6 $\mu$ s
N. tentativi di ritrasmissione	16
N. tentativi prima di limitare il Back-off	10
Pacchetto di Jamming	32 byte
Lunghezza minima del pacchetto	64 byte
Massima lunghezza del pacchetto	1518 byte

Tabella 5.4. Alcuni parametri della rete IEEE 802.3.

Consideriamo ad esempio il pacchetto di lunghezza minima uguale a 512 bit. Il tempo necessario per la trasmissione di tale pacchetto è 51.2  $\mu$ s, che risulta uguale al round-trip delay 2T. Si ottiene perciò  $T \cong 25 \mu$ s e quindi con una velocità di trasmissione uguale a  $2 \times 10^9$  m/s (2/3 della velocità della luce), si ha una distanza massima uguale a 5 Km. Nelle applicazioni pratiche il valore di distanza massima deve essere diminuita a causa delle attenuazioni. Nel caso si desideri realizzare una rete con velocità maggiore di 10 Mbit/sec, è necessario aumentare la lunghezza minima del frame oppure diminuire la lunghezza massima del cavo. Ad esempio, se si vuole progettare una rete che operi ad una velocità di un 1 Gbit/s, la lunghezza minima del frame è 6400 byte se si vuole mantenere una

distanza massima di 2.5 Km, mentre se la lunghezza minima del frame è portata 640 byte la distanza massima è di 250 m.

### *Livello fisico*

Le principali funzioni svolte dal livello fisico sono:

- trasforma i bit da trasmettere in segnali elettrici codificati con il codice di Manchester;
- trasmette e riceve i bit.

Tutte le versioni di IEEE 802.3, definite per i diversi tipi di supporto fisico, utilizzano la codifica di Manchester. Ogni periodo di bit è diviso in due intervalli uguali e i segnali associati ai simboli 0 e 1 sono mostrati nella Figura 5.11. Questa codifica assicura che ogni periodo  $\tau$  di bit è presente una transizione nel mezzo di  $\tau$  e quindi facilita il sincronismo tra trasmettitore e ricevitore.

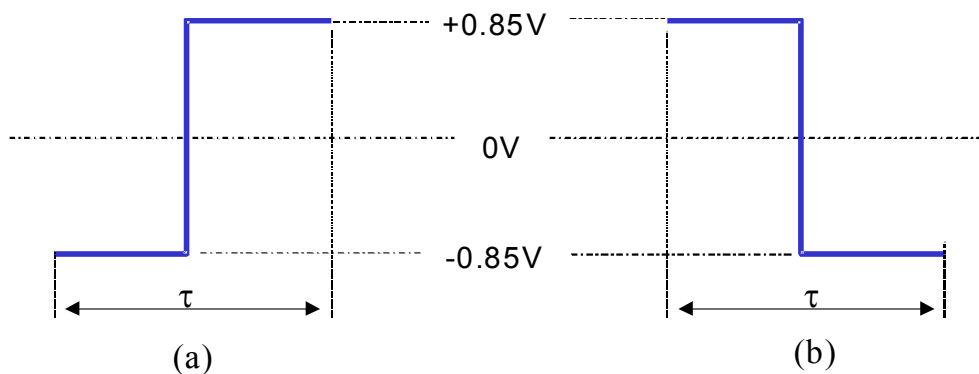


Figura 5.11. Codifica di Manchester : a) segnale associato a 0; b) segnale associato a 1.

### *Interfaccia o controller Ethernet*

Questo dispositivo, realizzato su un'apposita scheda, viene generalmente inserito nell'interno della apparecchiatura da connettere in rete. Esso svolge le seguenti funzioni:

- codifica (o decodifica) i singoli bit in segnali utilizzando il codice di Manchester;
- sincronizza il trasmettitore e il ricevitore utilizzando le transizioni del segnale dal livello alto al livello basso o viceversa contenute nella codifica di Manchester;
- gestisce il collegamento.

### *Cavo transceiver o AUI (Attachment Unit Interface)*

Questo cavo serve a collegare l'interfaccia Ethernet al transceiver e quindi alla rete Ethernet. La lunghezza massima del cavo è di 50 m. Il cavo è di tipo schermato con connettori a 15 poli.

## Transceiver

Il transceiver o MAU (Medium Access Control Unit) è un dispositivo che si collega alla presa AUI di una scheda Ethernet e al cavo di trasmissione; esso svolge le seguenti funzioni:

- trasmette e riceve i segnali della rete;
- rileva la portante ed eventuali collisioni;
- invia la sequenza di jamming quando viene rivelata una collisione.

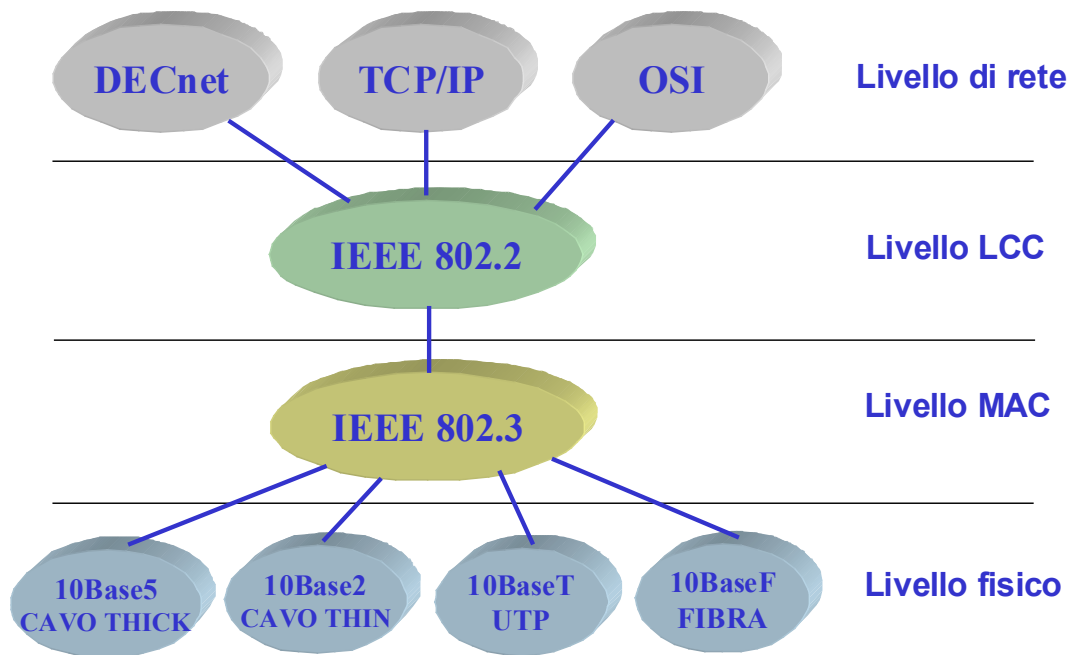


Figura 5.12. Differenti versioni dello standard IEEE 802.3 a seconda del tipo di mezzo trasmissivo utilizzato.

## Ripetitori

Un repeater serve ad estendere la lunghezza della rete superando i limiti imposti dagli standard per la singola rete locale a causa dell'attenuazione introdotta dai mezzi trasmissivi. Un repeater opera a livello fisico e ha lo scopo di ricevere, amplificare e ritrasmettere i segnali.

I repeater possono essere divisi in due classi:

- **Repeater di classe I.** Questo tipo di repeater rigenera i simboli ricevuti, per cui deve elaborare i segnali e quindi introduce un ritardo di trasmissione. Infatti il segnale analogico ricevuto da una porta viene trasformato in digitale, rigenerato e trasmesso sull'altra porta in forma analogica. Per realizzare queste operazioni di rigenerazione del segnale è necessario un buffer, che introduce un ritardo (circa 5 ms). Per evitare che il ritardo introdotto dai repeater possa portare alla sovrapposizione tra due pacchetti adiacenti eliminando l'Inter-Packet Gap di 9.6  $\mu$ s, è necessario imporre che tra due

qualunque transceiver si possono avere al massimo quattro repeater. Questo tipo di repeater può essere utilizzato per collegare tra loro due segmenti di rete realizzati con mezzi fisici diversi (cavo, doppino o fibra ottica).

- *Repeater di classe II.* Questo tipo di repeater amplifica il segnale ricevuto all'ingresso di una porta e lo ritrasmette su tutte le altre porte senza effettuarne una rigenerazione. Per questo motivo questi dispositivi possono collegare soltanto segmenti della rete realizzati con lo stesso tipo di mezzo fisico. Anche in questo caso il numero di repeater che si possono trovare tra due qualsiasi transceiver è limitato. Infatti quando un pacchetto viene ricevuto su una porta di ingresso, il repeater inizia a leggere il preambolo e a sincronizzare la sua trasmissione; una volta recuperato il sincronismo, il repeater inizia a trasmettere il segnale amplificato sulla porta di uscita, ma i simboli serviti per la sincronizzazione sono persi, per cui il repeater distrugge una parte del preambolo.

### *Collegamento di una stazione ad una rete Ethernet a 10 Mbit/s.*

La struttura generale del collegamento di una stazione terminale ad una rete Ethernet è mostrata nella Figura 5.13. In questo schema possono essere distinti i seguenti elementi:

- **Mezzo fisico:** rappresenta il mezzo trasmissivo, che può essere di vario tipo.
- **MDI (Medium Dependent Interface):** consente di collegare la stazione al mezzo fisico e quindi di ricevere o trasmettere i segnali sulla rete. Il dispositivo utilizzato dipende dal mezzo fisico utilizzato. Ad esempio MDI può essere un BNC o un attacco a vampiro nel cavo coassiale.
- **MAU o transceiver.**
- **Cavo AUI.**
- **Scheda Ethernet.**

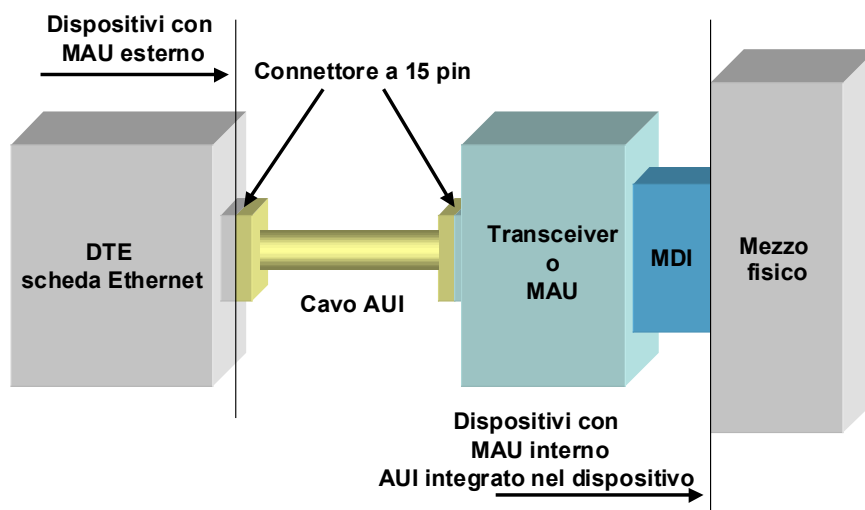


Figura 5.13. Schema del collegamento di una stazione terminale alla rete Ethernet.

## 5.5 Caratteristiche dei diversi tipi di cablaggio

### 10Base5

Il cablaggio 10Base5, indicato anche come **thick Ethernet**, utilizza un cavo coassiale RG8. Lo schema del collegamento di una stazione di rete è mostrato nella Figura 5.14. La struttura della rete è tipicamente a bus ed è mostrata nella Figura 5.15.

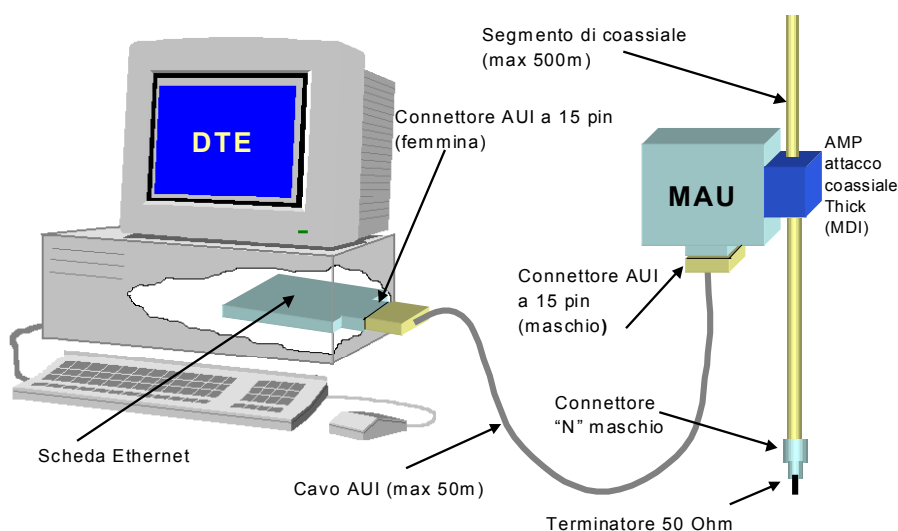


Figura 5.14. Schema del collegamento di una stazione ad una rete Ethernet 10Base5.

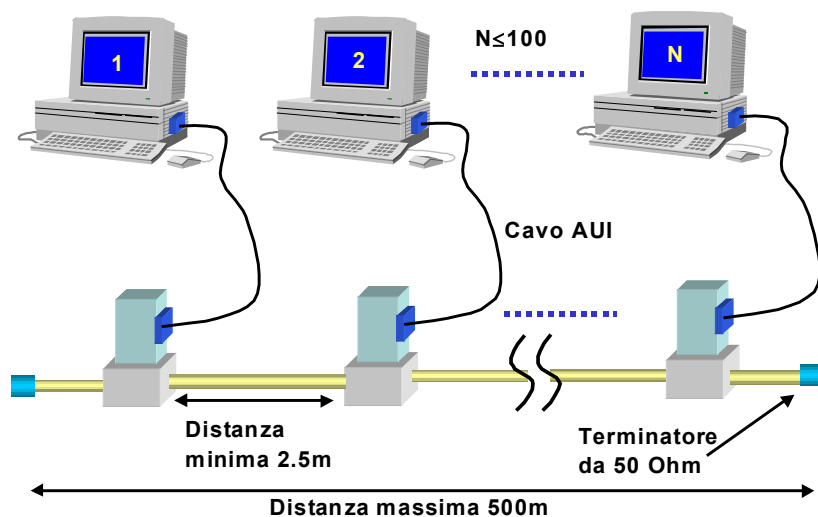


Figura 5.15. Configurazione di un sistema 10Base5.

Il transceiver o MAU è in grado di trasmettere e ricevere segnali su un segmento di cavo coassiale di 500 m. Il MAU è connesso al cavo coassiale mediante una connessione a vampiro, pertanto esso è a diretto contatto con l'anima del cavo. Questa connessione può

essere fatta ogni 2.5 m e per questo sul cavo giallo sono presenti dei segni neri che individuano tali punti. Il transceiver è un dispositivo che contiene tutta l'elettronica necessaria per il rilevamento della portante e delle collisioni. Quando si verifica una collisione, il transceiver invia la sequenza di jamming. Un transceiver può essere condiviso da vari computer (fino ad un massimo di 8). Il transceiver è connesso alla stazione mediante un cavo di transceiver o AUI, che non può essere più lungo di 50 m. il cavo AUI è connesso alla scheda di interfaccia mediante un apposito connettore con 15 piedini. Le principali attività svolte dall'interfaccia sono:

- ricezione e trasmissione dei frame;
- controllo degli errori.

Le principali caratteristiche dello standard 10Base5 sono le seguenti:

- *Mezzo di trasmissione:* cavo coassiale schermato ( RG8, cavo giallo), codifica di Manchester in banda base.
- *Velocità di trasmissione:* 10 Mbit/s.
- *Lunghezza di un segmento:* 500m.
- *Numero massimo di segmenti:* 5.
- *Numero massimo di stazioni per segmento:* 100.
- *Numero massimo di stazioni sulla rete:* 1023.
- *Distanza massima tra due stazioni sulla rete:* 2.8 Km.
- *Distanza minima tra due stazioni adiacenti sulla rete:* 2.5 m.
- *Numero massimo di repeater tra due qualsiasi stazioni sulla rete:* 2.

## 10Base2

Il cablaggio 10Base2, noto anche con il nome di thin Ethernet, utilizza un cavo coassiale fine RG-58A/U o coax thin. Ciascun segmento ha una lunghezza massima di 185 m. Lo schema del collegamento di una stazione alla rete è mostrato nella Figura 5.16.

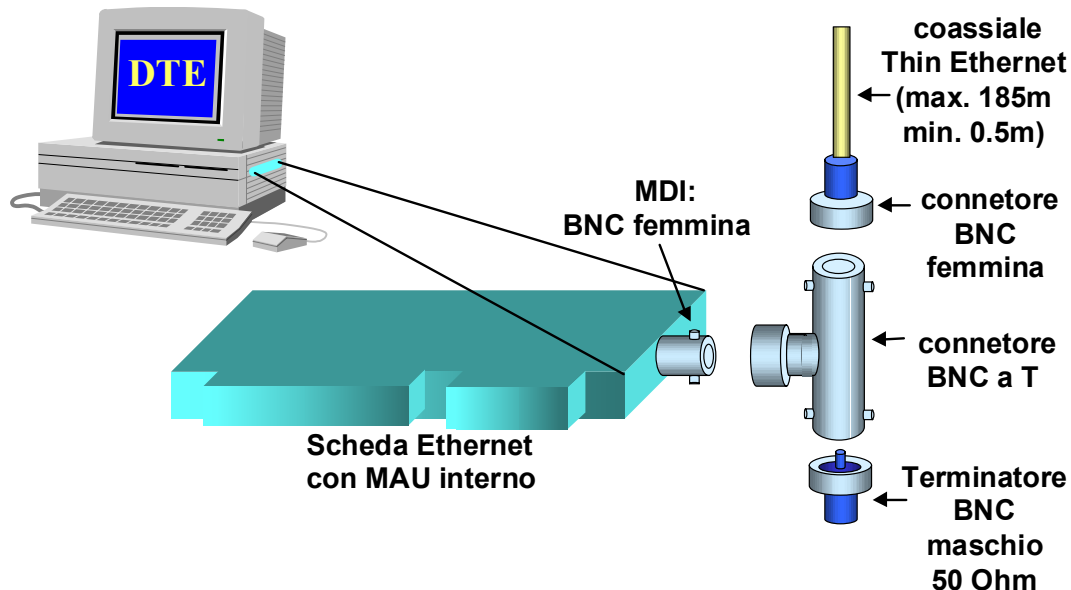


Figura 5.16. Schema del collegamento di una stazione ad una rete Ethernet 10Base2.

La connessione di ciascuna stazione al cavo è realizzata mediante connettori BNC passivi, formando una giunzione a T. La struttura della rete è di tipo a bus, come mostrato nella Figura 5.17.

Poiché il cavo ha uno spessore ridotto, le distanze sono minori (185 m per ogni spezzone) e può permettere la connessione di un numero minore di stazioni (30 per ogni segmento) rispetto alla rete 10Base5. Tuttavia, le dimensioni ridotte rendono il cavo più maneggevole e quindi facilitano il cablaggio.

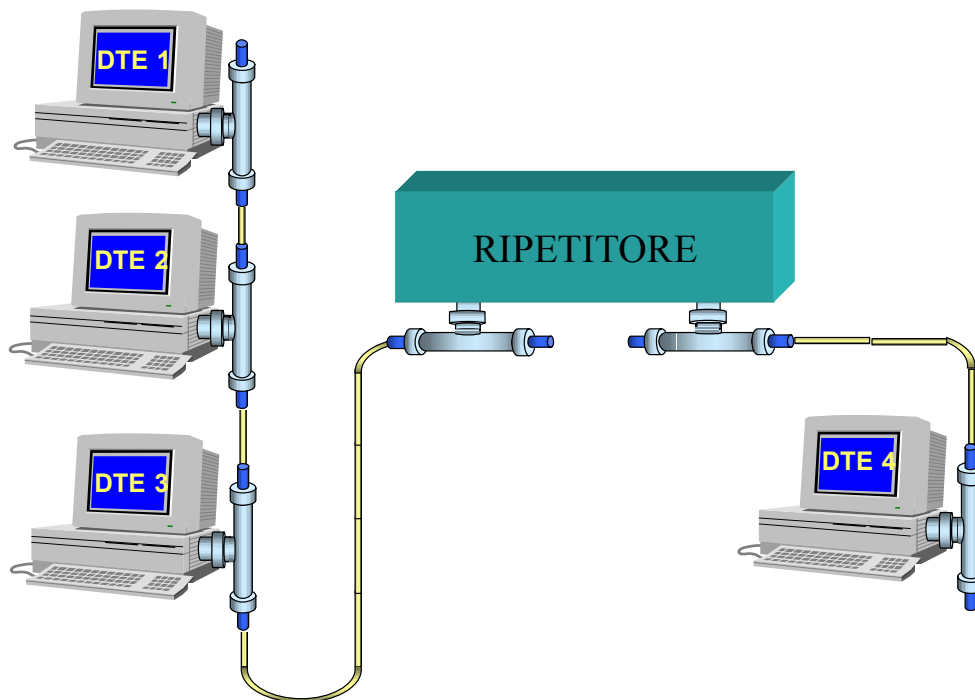


Figura 5.17. Configurazione della rete Ethernet 10Base2.

Le principali caratteristiche della rete 10Base2 sono le seguenti:

- *Topologia:* bus;
- *Mezzo di trasmissione:* cavo coassiale schermato (RG58), codifica di Manchester in banda base;
- *Velocità di trasmissione:* 10 Mbit/s;
- *Lunghezza massima del cavo di collegamento alla rete:* 50 m;
- *Lunghezza massima di un segmento:* 185 m;
- *Numero massimo di stazioni per segmento:* 30;
- *Distanza minima tra due stazioni adiacenti sulla rete:* 0.5 m.

## 10BaseT

Lo standard 10BaseT utilizza il doppino telefonico UTP per realizzare i collegamenti e secondo lo standard ammette la connessione di due sole stazioni nella modalità punto-punto. Lo schema per il collegamento di una struttura alla rete è mostrato nella Figura 5.18.



A causa delle caratteristiche dello standard, la struttura della rete 10BaseT è di tipo stellare (come mostrato nella Figura 5.19). Le diverse stazioni sono collegate ciascuna ad una porta di un HUB di un ripetitore multi-porta. La struttura 10BaseT ha incontrato un notevole successo per i numerosi vantaggi che offre, quali:

- il doppino telefonico è semplice da installare e presenta un ingombro e un costo ridotto;
- la connessione di tipo stellare consente di modificare in modo semplice la rete, poiché le diverse stazioni sono collegate in modo indipendente.

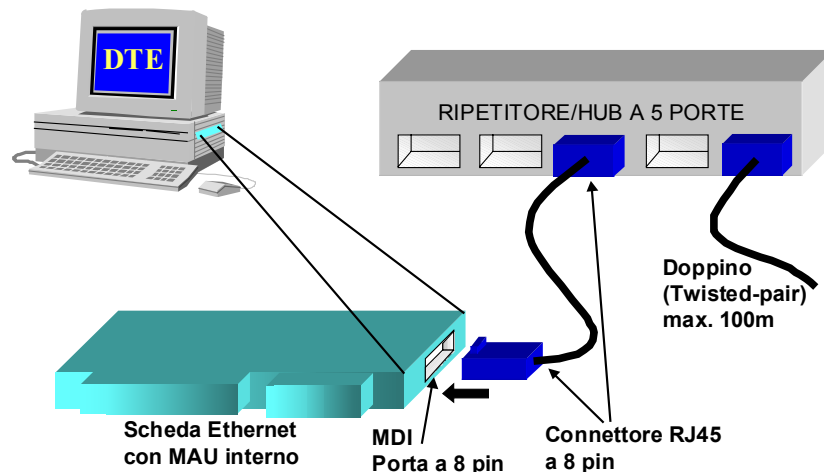


Figura 5.18. Schema del collegamento di una stazione ad una rete Ethernet 10BaseT.

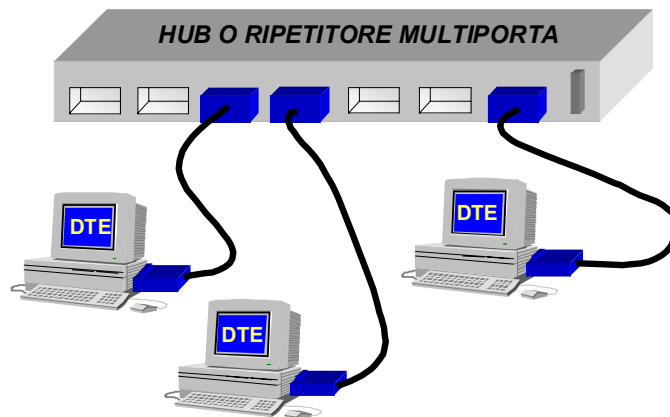


Figura 5.24. Configurazione di una rete Ethernet 10BaseT.

Le principali caratteristiche dello standard 10BaseT sono le seguenti:

- *Topologia della rete:* stella
- *Mezzo di trasmissione:* doppino telefonico non schermato (UTP) a due o quattro fili di categoria 3,4 e 5; codifica di Manchester in banda base;
- *Velocità di trasmissione:* 10 Mbit/s;
- *Lunghezza di un segmento:* 100 m.

## 10BaseF

Lo standard 10BaseF utilizza le fibre ottiche per la trasmissione del segnale e quindi garantisce elevate prestazioni e maggiori distanze. La distanza massima di un segmento è 2 Km. Il cablaggio 10BaseF è diviso in 3 standard:

- 10BaseFB (Fiber Backbone);
- 10BaseFL (Fiber Link);
- 10BaseFP (Fiber Passive).

### 10BaseFB

Questo standard è relativo a segmenti in fibra ottica per la connessione punto-punto di due ripetitori in una dorsale. Tuttavia spesso può essere utilizzato anche in una struttura stellare mediante ripetitori multiporta. Le regole di configurazioni impongono che il segmento di 10BaseFB può interconnettere due ripetitori e non stazioni terminali; ogni segmento può avere una lunghezza massima di 2 Km.

### 10BaseFL

Questo standard specifica le modalità di connessione tra un concentratore e una stazione periferica mediante un collegamento punto-punto. Per collegare più stazioni terminali è necessario utilizzare una configurazione a stella. Lo schema del collegamento di una stazione è mostrato nella Figura 5.20. Il segmento FL collega il concentratore o hub al MAU della stazione terminale e può avere una lunghezza massima di 2 Km. Il MAU, indicato in questo caso con FOMAU (Fiber Optic MAU), è connesso all'interfaccia Ethernet mediante un cavo AUI.

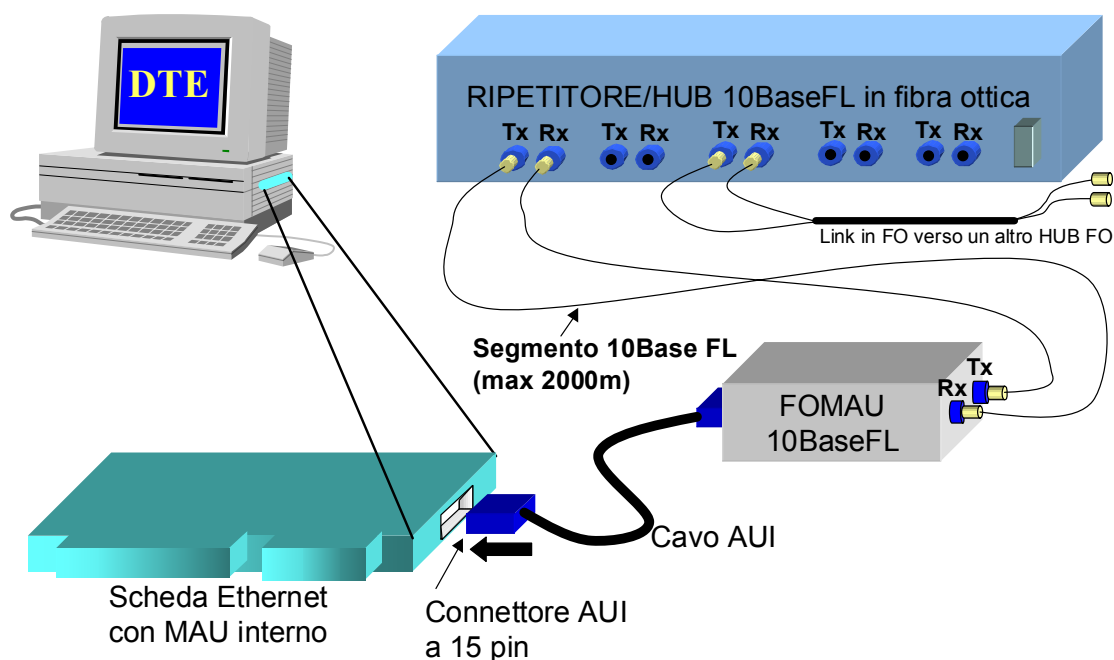


Figura 5.20. Schema del collegamento di una stazione ad una rete 10BaseFL.

Lo standard 10BaseFP definisce una rete a topologia stellare, costituita da vari segmenti in fibra ottica connessi ad un concentratore passivo. La stella passiva divide il segnale ottico entrante da una porta su tutte le altre porte di uscita. In questo modo a ciascuna uscita viene inviato un segnale uguale a quello incidente, ma fortemente attenuato rispetto a quello entrante.

## 5.6 Configurazione di una LAN Ethernet in un singolo dominio di collisione

La struttura di una LAN Ethernet è influenzata da vari parametri, quali:

- l'attenuazione dei cavi di trasmissione;
- i disturbi e i ritardi introdotti dai repeater;
- i parametri che definiscono il funzionamento del protocollo CSMA/CD quali *l'inter packet gap* e il *round-trip delay*.

Questi fattori, oltre ad imporre un valore massimo di lunghezza per ogni segmento della rete, limitano anche il numero dei segmenti, la loro configurazione e il numero di ripetitori che possono essere utilizzati.

In questo paragrafo descriviamo i principali parametri che limitano le dimensioni di una LAN Ethernet all'interno dello stesso dominio di collisione. Si definisce **dominio di collisione** una singola rete CSMA/CD in cui avviene una collisione se due computers trasmettono nello stesso istante. Un esempio di dominio di collisione è mostrato nella Figura 5.21. I repeater, gli hub e i transceiver sono dispositivi che operano a livello 1 e quindi non sono in grado di suddividere una LAN Ethernet in più domini di collisione. Per suddividere una LAN Ethernet in più domini di collisione è necessario utilizzare dispositivi in grado di operare a livelli OSI superiori e rispetto a primo, quali bridge, switch e router.

## 5.7 Calcolo della massima distanza tra due stazioni Ethernet

La massima distanza tra due stazioni è limitata dai seguenti parametri:

- un pacchetto ha una lunghezza minima di 64 byte = 512 bit;
- la fine di un pacchetto è marcata da un periodo di assenza di trasmissione (IGP) uguale a  $9.6 \mu\text{s}$ ;
- la collisione tra stazioni deve essere rivelata prima che il pacchetto sia stato trasmesso completamente.

Come abbiamo visto in precedenza, questi parametri determinano una distanza massima di circa 5 Km. In realtà a causa dei rumori e delle attenuazioni la distanza massima consentita per gli standard è molto minore (al massimo intorno a 2 Km).

### *Limiti sul massimo numero di repeater nell'interno di un dominio di collisione*

Il frame Ethernet non possiede un delimitatore di fine pacchetto; tuttavia, la presenza dell'intervallo IGP consente di effettuare tale riconoscimento. Una riduzione di tale intervallo tra due pacchetti successivi può portare a non riconoscere la fine del primo pacchetto ed alla loro fusione in un unico frame

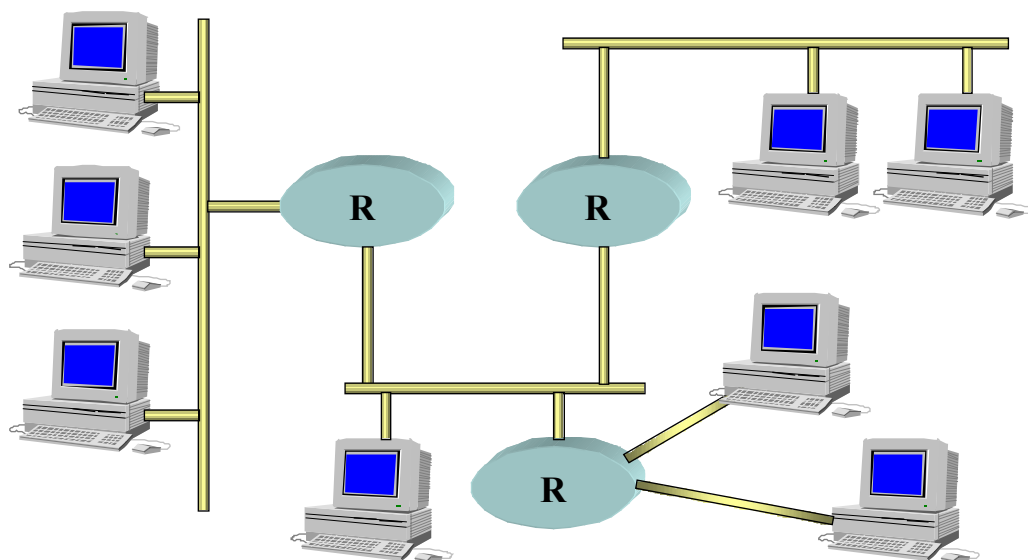


Figura 5.21. Esempio di un dominio di collisione Ethernet.

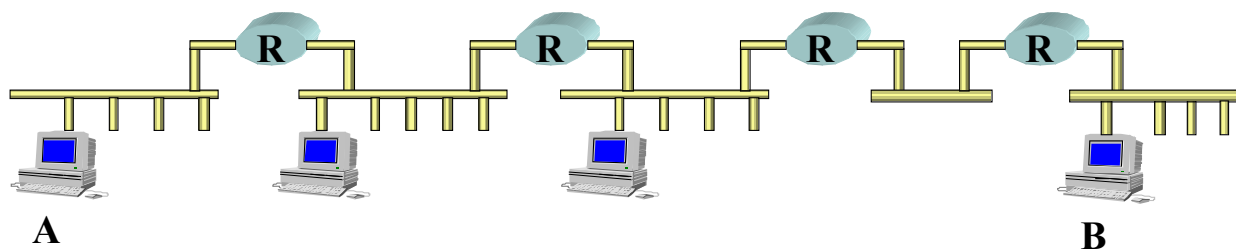
*I principali responsabili di una riduzione dell'IGP sono i repeater. Infatti ciascun repeater deve sincronizzarsi sul clock del trasmettitore e quindi può distruggere parte del preambolo prima di agganciare il sincronismo. Per eliminare questo inconveniente il repeater deve rigenerare il preambolo, per cui introduce un ritardo variabile da pacchetto a pacchetto. Per risolvere questo inconveniente, si limita il numero di repeater all'interno di uno stesso dominio di collisione. Occorre notare che i repeater che collegano fibre ottiche sono considerati nel conteggio come mezzo repeater.*

#### *Regole per la configurazione di una rete Ethernet in un dominio di collisione*

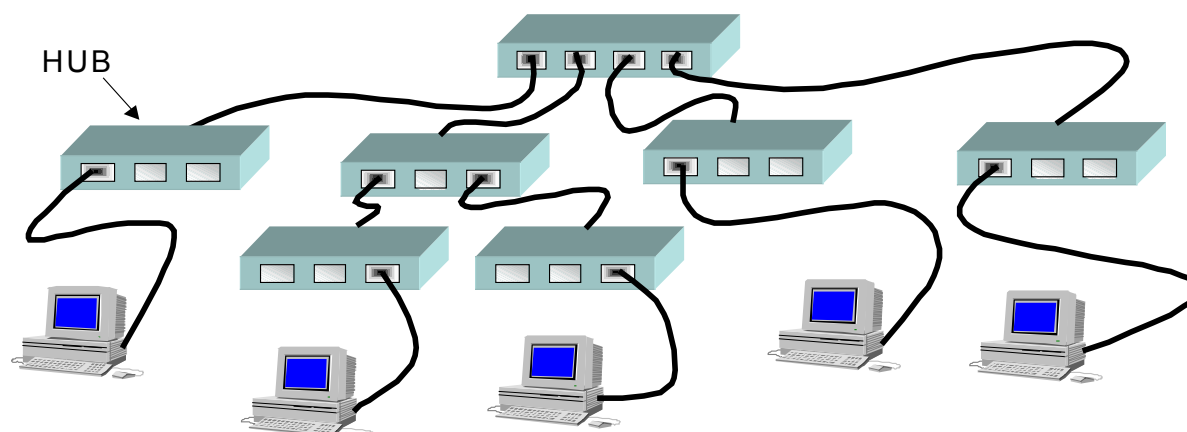
Le regole stabilite da IEEE 802.3 impongono un insieme di limiti nella progettazione di una rete Ethernet. Esistono sostanzialmente i seguenti due tipi di regole:

#### **Regola 1**

- il numero massimo di segmenti Ethernet tra due stazioni qualsiasi sulla rete LAN non deve essere superiore a 5, di cui tre al massimo in cavo coassiale.
- il numero massimo di repeater tra due stazioni qualsiasi sulla rete non deve essere superiore a 4. La rete può contenere anche un numero superiore di repeater, ma deve essere rispettata la regola precedente. L'insieme delle due regole precedenti, viene indicata anche con il nome di **regola 5-4-3**. Un esempio è mostrato nelle Figure 5.22.a e 5.22.b sono mostrati due esempi di rete correttamente progettata.
- se sono presenti 4 ripetitori ogni singolo segmento di cavo coassiale non deve superare i 500 m;
- se sono presenti 3 ripetitori, ogni singolo FOIRL non deve superare 1 Km.



a



b

Figura 5.22. Due configurazioni ammissibili per la rete Ethernet.

## Regola 2

Una serie di regole meno restrittive delle precedenti sono le seguenti:

- 4 repeater al massimo;
- 5 segmenti, di cui al massimo 3 mixing;
- i cavi AUI per i MAU 10BaseFB e FL non devono eccedere i 25 m.
- quando si ha un path con 5 segmenti in fibra ottica:
  - i segmenti FOIRL, 10BaseFB, 10BaseFL non possono superare i 500 m;
  - il segmento più lungo non deve eccedere i 300 m;
- se si hanno 4 segmenti e 3 ripetitori in un path
  - ogni segmento inter-repeater in fibra non deve superare i 1000 m per FOIRL, 10 Base FB o FL e 700 m per 10 Base FP;
  - la lunghezza massima di un segmento in fibra ottica che interconnette una stazione a un repeater non deve superare i 400 m nel caso 10 Base FL e 300 m nel caso 10 Base FP.

## 5.8 Fast Ethernet

La rapida crescita delle reti locali ed il crescente sviluppo di applicazioni e servizi multimediali ha portato all'esigenza di realizzare reti LAN di elevate velocità. All'inizio degli anni '90 sono state sviluppate e successivamente standardizzate da IEEE due differenti tecnologie a 100 Mbit/sec:

- **Fast Ethernet o IEEE 802.3u**
- **100 VG AnyLAN**

Fast Ethernet ha riscosso subito un grande successo poiché è compatibile con la rete Ethernet, e ne mantiene le caratteristiche di semplicità ed efficienza. In particolare, Fast Ethernet conserva tutti i parametri di Ethernet:

- utilizza lo stesso protocollo di accesso multiplo CSMA/CD di Ethernet;
- utilizza lo stesso meccanismo di gestione delle collisioni;
- utilizza lo stesso formato e la stessa lunghezza minima.

Nel funzionamento del protocollo CSMA/CD, la velocità di trasmissione ammissibile è legata alla lunghezza minima del pacchetto e al round-trip delay (e quindi alla massima distanza tra le stazioni sulla stessa rete). Poiché Fast Ethernet deve essere compatibile con Ethernet, la lunghezza minima e il formato del pacchetto devono essere mantenuti inalterati. Come conseguenza, per aumentare la velocità di trasmissione a 100 Mbit/s è necessario ridurre di un fattore 10 il round-trip delay e quindi la distanza massima.

### Struttura di base di Fast Ethernet

Gli elementi e i dispositivi necessari per collegare una stazione terminale ad una rete Fast Ethernet sono:

- il *mezzo fisico*, utilizzato nella realizzazione della rete;
- il dispositivo *MDI (Medium Dependent Interface)*, che consente di connettere la stazione al mezzo fisico e che può essere un connettore a 8-pin nel caso di doppino telefonico o un connettore per la fibra ottica;
- il dispositivo *PHY (Physical layer device)*, che svolge le stesse funzioni del transceiver nel caso di Ethernet a 10 Mbit/s. Esso può essere realizzato sia all'interno della porta Ethernet del dispositivo, sia in un piccolo contenitore esterno equipaggiato con cavo MII a 40 pin;
- il dispositivo *MII (Medium Independent Interface)* è un insieme di circuiti elettronici che serve a collegare la scheda Ethernet o Fast Ethernet, che genera le funzioni di controllo di accesso al mezzo, e il PHY, che invia il segnale sulla rete. Questo dispositivo può consentire di operare sia a 10 Mbit/s, sia a 100 Mbit/s e quindi può permettere il collegamento di segmenti 10Base-T e 100Base-T. Il suo compito è quello di convertire i segnali analogici ricevuti dal PHY in segnali digitali per qualunque dispositivo che può essere collegato in rete. Il dispositivo MII è opzionale;
- *Scheda di rete o interfaccia Fast Ethernet (o Ethernet)*, che contiene l'elettronica e il software necessari per eseguire i controlli di accesso al canale e per trasmettere i frame. Le schede Fast Ethernet differiscono da quelle di Ethernet solo per la velocità e

il tipo di cablaggio ammesso. Quasi tutte le schede Fast Ethernet o DTE ammettono la possibilità di operare a 10 o 100 Mbit/s.

Il passaggio da 10 a 100 Mbit/s viene fatto in modo automatico mediante un processo di *autonegoziazione*.

## Cablaggio

Il cablaggio di una rete Fast Ethernet è caratterizzato dai seguenti tre standard:

- 100Base-TX
- 100Base-T4
- 100Base-FX

### 100Base-TX

Il segmento 100Base-TX utilizza il *doppino telefonico UTP o STP* con le seguenti caratteristiche:

- due coppie di cavi bilanciati non schermati (UTP) di categoria 5;
- due coppie di cavi schermati (STP) bilanciati con impedenza caratteristica di 150  $\Omega$ .

In ambedue i casi una coppia è utilizzata per trasmettere e l'altra per ricevere, come in 10Base-T.

Il segnale è codificato mediante un codice 4B/5B con una frequenza di trasmissione uguale a 125 MHz. Lo schema completo del collegamento è mostrato nella Figura 5.23.

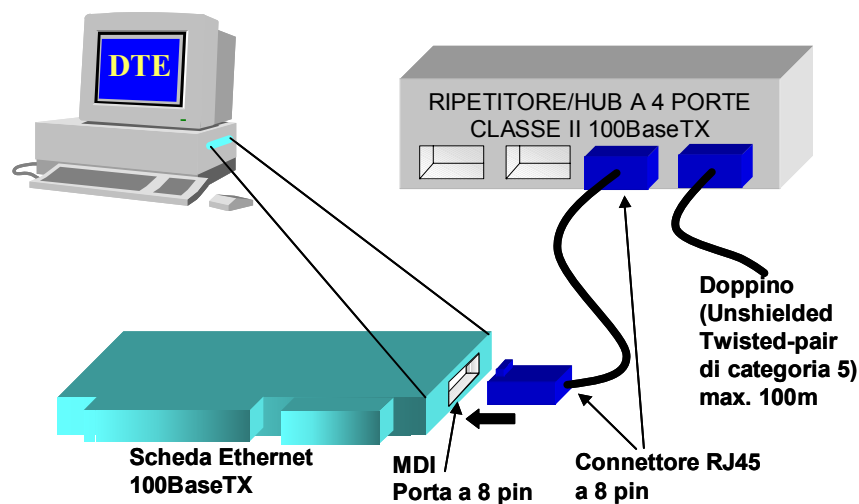


Figura 5.23. Schema del collegamento di un host con una rete 100 Base TX.

Il sistema 100BASE-TX permette collegamenti lunghi al massimo 100 metri. In cui la distanza può variare a seconda della potenza del segnale. Se ad esempio si usa un cavo di buona qualità in un segmento 10BASE-T, è possibile raggiungere distanze di 150 metri.

Questo non è vero con Fast Ethernet. Sono disponibili dei tester per i cavi che permettono di controllarne le caratteristiche elettriche che devono sottostare a certe specifiche. Ad esempio si può controllare il grado di accoppiamento tra la coppia di trasmissione e quella di ricezione, e l'attenuazione del segnale sul segmento.

Nel caso in cui sia necessario coprire distanze maggiori è necessario utilizzare ripetitori mediante una struttura a stella.

### **100BaseFX**

Questa soluzione utilizza due cavi in fibra ottica multimodale. Ogni segmento può raggiungere una *lunghezza massima di 412 m*, anche se le fibre ottiche potrebbero raggiungere distanze maggiori. Questo limite viene stabilito per garantire la temporizzazione dei segnali.

Le strutture di connessione sono le stesse del 100Base-TX. Tuttavia in questo caso le massime distanze permesse per ogni segmento variano a seconda del numero e del tipo di ripetitori usati nel link. Se viene usato un singolo ripetitore di Classe II la massima distanza tra due DTEs è di 320 metri. Nel caso di due ripetitori di Classe II la distanza si riduce a 228 metri. Nel caso invece di un ripetitore di classe I la distanza massima è di 272 metri.

### **100Base-T4**

Questo standard utilizza quattro coppie di cavi bilanciati della categoria 3 (UTP), come definito da ISO/IEC 11801. Questi cavi sono poco immuni al rumore sopra i 25 Mhz e non sarebbero compatibili con le specifiche degli standard europei. Per questo motivo per utilizzare cavi di categoria 3 si usano quattro coppie di cavi.

Il segnale è codificato con un codice a blocchi conosciuto come 8B/6T. *La massima distanza, come nel caso 100Base-TX, è uguale a 100m.*

### **Ripetitori e HUB**

I ripetitori sono utilizzati per estendere un segmento di una rete Fast Ethernet. Essi provvedono alla temporizzazione ed alla rigenerizzazione del segnale nel trasporto dei dati. Gli hub sono ripetitori multiporta e consentono di realizzare una topologia di tipo stellare. Esistono due classi di ripetitori: classe I e II. Lo standard Fast Ethernet impone le seguenti regole:

- *è ammesso un solo ripetitore di classe I tra due qualunque DTE;*
- *sono ammessi al massimo due ripetitori di classe II tra due qualunque DTE.*

I repeater di classe I hanno un ritardo di temporizzazione più lungo, ed operano trasformando il segnale analogico alla porta di ingresso, in digitale, rigenerandolo e ritrasformarlo in analogico per essere trasmesso sulla porta di uscita. Queste operazioni consentono di ripetere segnali tra segmenti Fast Ethernet che utilizzano tecniche di segnalazione diverse, come ad esempio 100Base-TX/-FX e 100Base-T4. Un repeater di



classe II presenta un ritardo più piccolo. Poiché esso ripete il segnale ricevuto su una porta di ingresso sulla porta di uscita, amplificando il segnale senza alcuna trasformazione. Per questo motivo, i ripetitori in questa classe non possono collegare due segmenti con caratteristiche diverse.

Nel caso di repeater di classe II *la massima distanza permessa tra ciascuna coppia di HUB è 5.*

### Switched Fast Ethernet

Per realizzare una rete Fast Ethernet con estensione superiore a quanto consentito dalle precedenti regole, si può utilizzare una struttura multi-segmento. In questo caso la LAN è divisa in vari sottodomini; tale operazione, detta di multisegmentazione, può essere realizzata mediante l'utilizzo di uno switch o di un dispositivo in grado di operare a livello MAC o superiore (switching hub, bridge, router).

Nella Figura 5.24.a è riportato lo schema della rete Fast Ethernet con un repeater di classe I o di classe II. In esso la massima distanza tra le stazioni o diametro D della rete è uguale a  $d_1 + d_2$ , dove  $d_1$  e  $d_2$  indicano la distanza del repeater dalle due stazioni più distanti. Nella Figura 5.24.b è mostrato l'utilizzo di due repeater di classe II utilizzati per estendere la rete Fast Ethernet. In questo caso  $D = d_1 + d_2 + d_3$ .

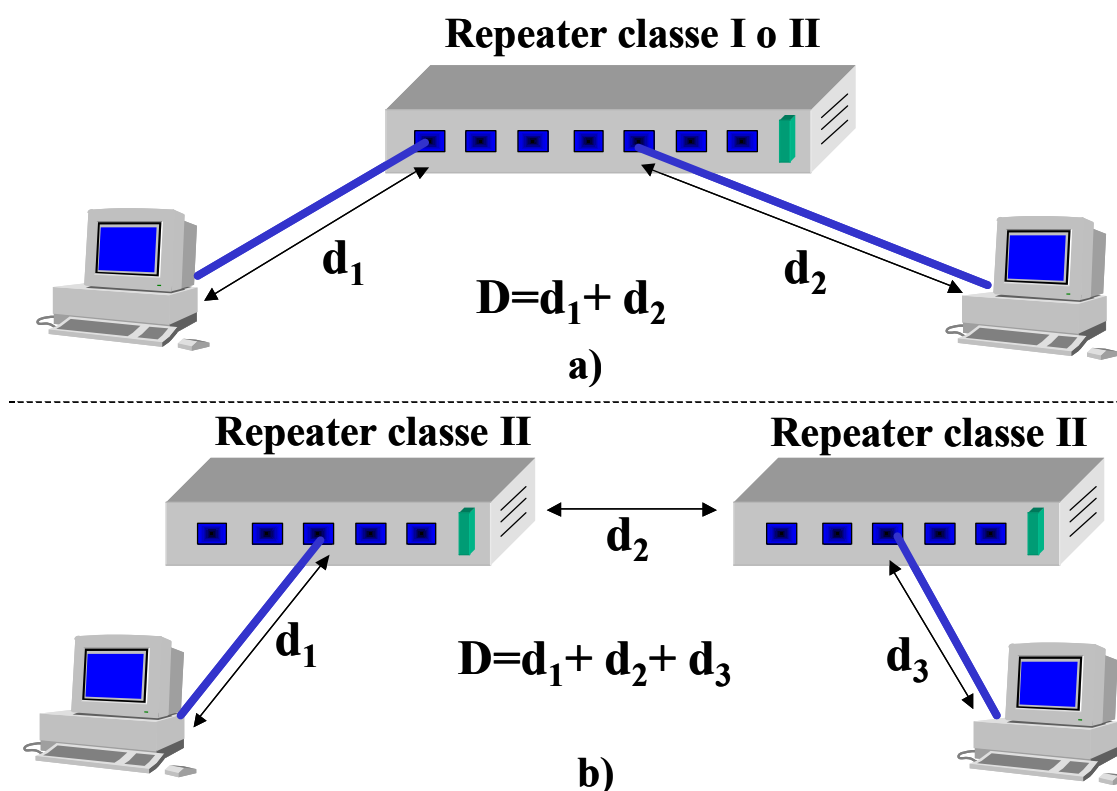


Figura 5.24. Configurazione di una rete Fast Ethernet: a) un solo repeater; b) due repeater.

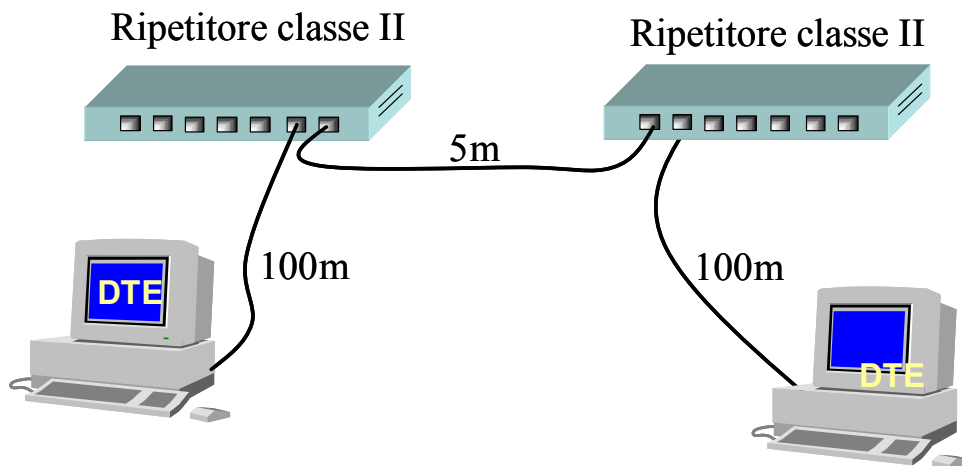


Figura 5.25. Configurazione di una rete Fast Ethernet utilizzando due repeater di classe II.

## 5.9 Gigabit Ethernet

La straordinaria crescita del traffico nelle reti LAN e lo sviluppo delle applicazioni multimediali ha determinato la necessità di realizzare reti locali con velocità elevate. Una delle tecnologie più interessanti è Gigabit Ethernet, che opera ad una velocità di 1 Gbit/s e che rappresenta un'estensione di Ethernet e Fast Ethernet, con le quali mantiene una completa compatibilità.

La rete Gigabit Ethernet nasce nel novembre 1995 quando Compaq Computer Communication propose al comitato IEEE 802 l'architettura base di una rete Ethernet a 1 Gbit/s. All'inizio del 1996 IEEE formò il gruppo IEEE 802.3z con lo scopo di definire uno standard per tale rete. Nell'aprile 1996 fu costituita "Gigabit Ethernet Alliance" da Compaq ed altre aziende per accelerare lo sviluppo di tale rete. Attualmente tale organismo è composto da oltre 70 enti.

La rete Gigabit Ethernet utilizza il protocollo CSMA/CD e per questo motivo è completamente compatibile con Ethernet e Fast Ethernet. Le sue principali caratteristiche sono:

- opera ad una velocità di 1 Gbit/s;
- utilizza un formato del frame identico a quello di Ethernet e Fast Ethernet;
- presenta gli stessi valori di lunghezza minima e massima per il frame delle reti Ethernet e Fast Ethernet;
- consente operazioni full duplex e half-duplex.

## Mezzi fisici

La rete Gigabit Ethernet può essere realizzata utilizzando vari tipi di cavi. Lo standard IEEE 802.3z ratificato nel giugno 1998, è stato definito per l'utilizzo su fibra ottica (standard 1000 Base SX e 1000 Base LX) o su doppino telefonico schermato (standard 1000 Base CX). Un altro gruppo IEEE 802.3ab sta definendo il livello fisico di una rete Gigabit Ethernet, realizzata mediante doppino telefonico UTP di categoria 5 (standard 1000 Base-T). Descriviamo in dettaglio le principali caratteristiche della rete Gigabit Ethernet a seconda del mezzo fisico utilizzato.

Standard	Tipo fibra	Diametro fibra $\mu\text{m}$	Banda (MHZ $\times$ Km)	Massima distanza (m)
1000 Base SX	Multimodale	62,5	160	220
	Multimodale	62,5	200	275
	Multimodale	50	400	500
	Multimodale	50	500	550
1000 Base LX	Multimodale	62,5	500	550
	Multimodale	50	400	550
	Multimodale	50	500	550
	Multimodale	9	NA	5000

Tabella 5.5. Caratteristiche delle fibre ottiche per realizzare Gigabit Ethernet.

### 5.10 Token Ring

I protocolli per l'accesso multiplo di tipo deterministico consentono di eliminare il problema delle collisioni tra stazioni presenti nelle reti locali che utilizzano protocolli casuali, quali ad esempio la rete Ethernet. Questo vantaggio è generalmente ottenuto a scapito della complessità realizzativa della rete. IBM ha sviluppato alcune reti locali che utilizzano la tecnica di accesso multiplo a **gettone** o **token**. Queste reti sono state successivamente standardizzate dal comitato IEEE 802 e rappresentano, dopo Ethernet, le reti più diffuse.

La prima rete basata sul token utilizzava una struttura a bus ed è stata standardizzata come rete **token bus** o **IEEE 802.4**. Tuttavia, essa non ha mai incontrato una grande diffusione ed attualmente è praticamente non utilizzata. Per questo motivo non sarà ulteriormente considerata. Nel 1976 IBM propose un'evoluzione basata su una tipologia ad anello e nota come *token ring*, che operava ad una velocità di 4 Mbit/s. Il comitato IEEE 802 ha elaborato lo standard **802.5** basato su tale rete introducendo alcune modifiche limitate e sviluppa una nuova versione della rete con una velocità di trasmissione di 16 Mbit/s.

La rete Token Ring utilizza una configurazione logica ad anello, come mostrato nella Figura 5.26. Ogni stazione è connessa all'anello mediante un apparato **MAU (Medium Access Unit)**.

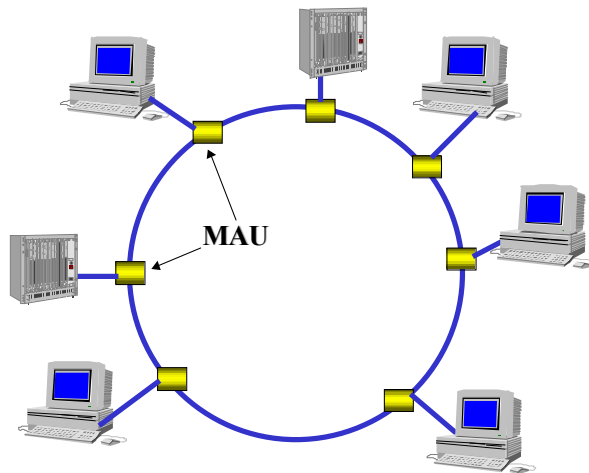


Figura 5.26. Configurazione logica di una rete token ring.

L'accesso della rete è gestito mediante un opportuno gettone: una stazione può trasmettere soltanto quando riceve il gettone. Esso è ricevuto sequenzialmente dalle stazioni sull'anello. Quando una stazione riceve il token, lo invia alla stazione successiva sull'anello se non ha dati da trasmettere. Nel caso opposto la stazione cattura il token, invia il pacchetto informativo sull'anello ed entra nello stato di attesa. Il pacchetto raggiunge la stazione di destinazione, ma non viene eliminato; esso continua il percorso sull'anello da stazione a stazione fino a ritornare alla stazione che lo ha generato. Quest'ultima provvede ad eliminarlo dall'anello e ad inviare il token alla stazione successiva.

Il token viene generato inizialmente da una *stazione master*; questa stazione controlla inoltre la presenza di errori od alterazioni. In questi casi o se il token viene perduto, la stazione master lo rigenera e lo ritrasmette sull'anello. In caso di malfunzionamento o rottura della stazione master, essa viene sostituita da un'altra stazione presente sulla rete in base all'indirizzo di rete.

#### *Livello MAC*

Il Token nella rete 802.5 ha il formato mostrato nella Figura 5.27. Esso è formato da tre campi, ciascuno dei quali di lunghezza 1 byte:

- **SD (Start Delimiter):** serve ad identificare l'inizio del token o di un frame informativo. Per questo contengono i bit J e K che violano il codice di Manchester.
- **AC (Access Control):** contiene le informazioni necessarie per l'accesso all'anello. *Il bit "T" indica se il frame ricevuto è un token o di tipo informativo. Se T=0 il frame è un token; se T=1 il frame è un pacchetto informativo. I bit PPP identificano un livello di priorità del pacchetto da 0 a 7, con 7 che indica la massima priorità. Il bit M indica se la trama è per il controllo del funzionamento dell'anello (M=0) oppure il tipo informativo (M=1). I bit RRR servono a prenotare il token utilizzando diversi livelli di priorità.*
- **ED (End Delimiter):** serve ad identificare la fine del token o di un frame informativo. Come SD, contiene i bit J e K che violano il codice di Manchester. Il bit I, detto

intermediate bit, serve ad indicare se la stazione che possiede il token ha altri pacchetti da trasmettere oppure no.

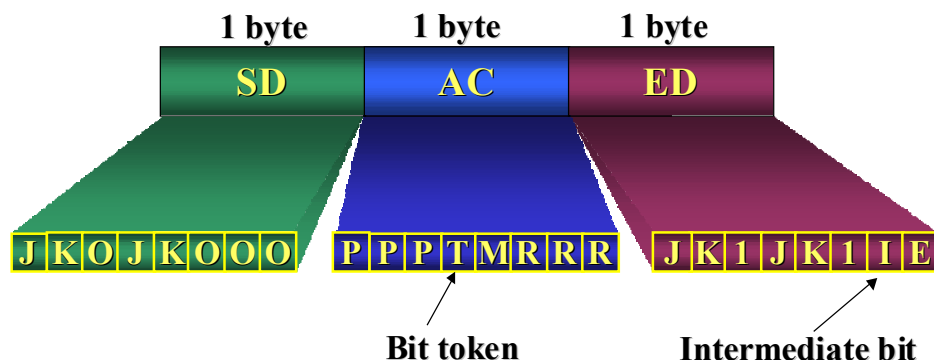


Figura 5.27. Formato del token.

#### *Caratteristiche della trama informativa*

La trama informativa presenta un numero maggiore di campi rispetto al token, come mostrato nella Figura 5.27. I campi presentano le seguenti caratteristiche:

- **SFS (Start Frame Sequence):** questo campo identifica l'inizio del frame ed è composto dai due campi SD e AC identici a quelli presenti nel token.
- **FC (Frame Control):** questo campo serve a controllare il frame. I primi 2 bit (FF) indicano il tipo della trama. Se FF=00, il pacchetto è un frame MAC utilizzato per scopi di management; se FF=01 il frame è stato generato a livello LLC. Nel primo caso (FF=0) il campo CCCCCC identifica le funzioni per cui è stato trasmesso il frame.
- **Destination address (DA):** questo campo identifica l'indirizzo della stazione di destinazione e può avere una lunghezza di 2 o 6 byte. Il primo bit del campo DA viene utilizzato per particolari funzioni di indirizzamento. Se tale bit è uguale a 0 il frame è diretto ad un solo utente il cui indirizzo è indicato dai bit successivi del campo DA. Se il bit è uguale ad 1, il frame è indirizzato ad un gruppo di utenti, mentre se tutti bit del campo DA sono uguali ad 1, il frame è indirizzato a tutte le stazioni connesse alla rete.
- **Source Address (SA):** questo campo contiene l'indirizzo della stazione che ha generato il frame. La lunghezza può essere di 2 o 6 byte.
- **Routing Information:** questo campo contiene le informazioni necessarie per instradare il messaggio dalla stazione sorgente a quella di destinazione.
- **Campo Dati:** questo campo contiene i dati informativi ed ha una lunghezza variabile (il massimo valore è 17749 byte).
- **FCS (Frame Check Sequence):** questo campo contiene i simboli di controllo del codice che serve a rivelare la presenza di errori nel frame.
- **EFS (End Frame Sequence):** questo campo, composto da due byte, serve ad identificare la fine del frame ed è composto dal sottocampo ED identico a quello presente nel token e dal sottocampo "Frame status". Questo sottocampo è costituito da una sequenza di bit viene seguita dal campo ACRR che serve a controllare la sua correttezza. I bit hanno il seguente significato:

- bit A: indica che l'indirizzo della stazione di destinazione è stato riconosciuto. La stazione che trasmette pone questo bit a 0, mentre la stazione che riconosce il proprio indirizzo nel campo "Destination address" pone tale bit a 1.
- bit C: indica che il frame è stato copiato dalla stazione di destinazione. Questo bit è posto a 0 dalla stazione di trasmissione ed è cambiato a 1 dalla stazione di destinazione.
- bit R: sono bit riservati per funzioni particolari.

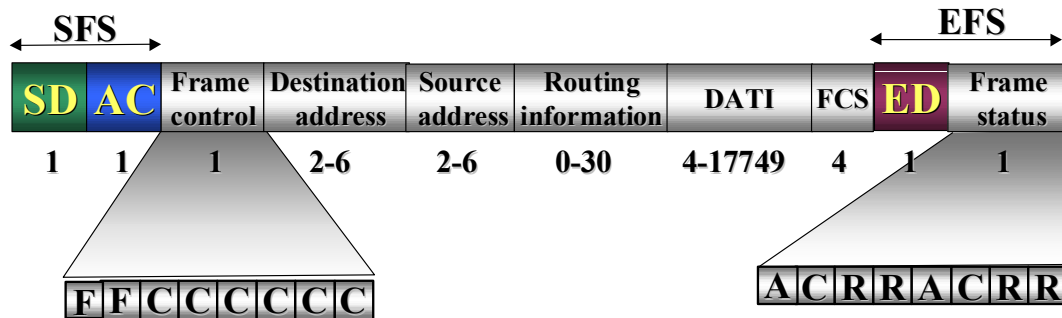


Figura 5.28. Formato della trama informativa in IEEE 802.5.

### Funzionamento della rete token-ring

L'accesso delle stazioni alla rete è gestito attraverso il token. Per spiegare il funzionamento della rete consideriamo l'esempio mostrato nella Figura 5.29. Il token arriva alla stazione S1 che deve trasmettere un pacchetto. Una stazione connessa alla rete riceve il token e deve inviare un pacchetto dati. La stazione opera nel seguente modo:

- il campo SD del token viene ritrasmesso inalterato all'uscita e costituisce il primo campo del frame.
- la stazione cattura il token cambiando da 0 a 1 il valore del bit T contenuto nel campo AC, che viene poi trasmesso in uscita.
- la stazione genera i campi successivi (FC, DA, SA, RI i dati e FCS) del frame o se la stazione non ha altri pacchetti da trasmettere oppure se è scaduto il tempo concesso alla stazione per la trasmissione (THT), l'intermediate bit del campo ED viene lasciato a 0 ed invia nel canale ED. Nel caso opposto il bit viene messo ad 1 e la stazione trasmette il pacchetto successivo.
- quando la stazione che ha trasmesso un pacchetto riceve lo stesso pacchetto e lo riconosce come proprio mediante il campo SA toglie il pacchetto dalla rete ed invia in rete il token.

*Ogni stazione deve leggere tutti i pacchetti che sono ricevuti al suo ingresso per verificare se l'indirizzo di destinazione contenuto nell'header del pacchetto coincide con il proprio indirizzo MAC. In caso positivo la stazione riceve il pacchetto e cambia i due bit "A e C" contenuti nel campo EFS; inoltre la stazione ritrasmette il pacchetto ricevuto sulla rete poiché esso dovrà essere controllato e gestito dalla stazione che lo ha trasmesso. Nel caso in cui la stazione non riconosca il proprio indirizzo, il pacchetto viene ritrasmesso inalterato sulla rete.*

Come indicato in precedenza, attraverso i primi tre (bit PPP) i bit del campo AC contenuto nel token o nella trama informativa, è possibile stabilire differenti priorità di accesso al canale in modo da consentire una maggiore priorità ad alcuni tipi di traffico. *Le singole stazioni possono effettuare la prenotazione con un certo valore di priorità mediante i tre bit RRR del campo AC. Una stazione può catturare un token soltanto se ha una priorità maggiore od uguale a quella scritta nel token.*

La stazione che possiede il token può alzare od abbassare il valore di priorità dei bit PPP. In assenza di richieste di priorità, i campi PPP e FFF sono posti uguali a 0. Soltanto la stazione che ha elevato il valore di priorità, può riabbassarlo successivamente. Per evitare che il livello di priorità aumenti progressivamente; quando una stazione invia il token in rete pone il campo PPP al valore che tale campo aveva quando è stato catturato.

### *Livello fisico*

La trasmissione dei segnali nello standard IEEE 802.5 avviene utilizzando una codifica di Manchester differenziata. La connessione di una stazione alla rete non viene realizzata direttamente, ma attraverso **un'unità di accesso (AU=Access Unit)**. Questa unità realizza le operazioni di inserzione o di esclusione della seconda in caso di guasto. In pratica varie unità AU sono raggruppate e insieme formano un concentratore **MAU (Multistation Access Unit)**.

Le MAU consentono di realizzare una struttura a stella, anche se da un punto di vista logico la rete è ad anello. Ogni MAU ha due porte speciali, chiamate *Ring In* e *Ring Out*, (Figura 5.29), *che possono essere utilizzate per collegare soltanto altre unità MAU e non collega altri dispositivi*. Ogni MAU ha anche almeno altre due porte (*Lobe ports*), che servono a collegare i dispositivi alla rete. Il collegamento di un dispositivo alla rete avviene attraverso una porta da cui partono due coppie di fili: una coppia per la trasmissione dal dispositivo alla rete ed una coppia per la ricezione.

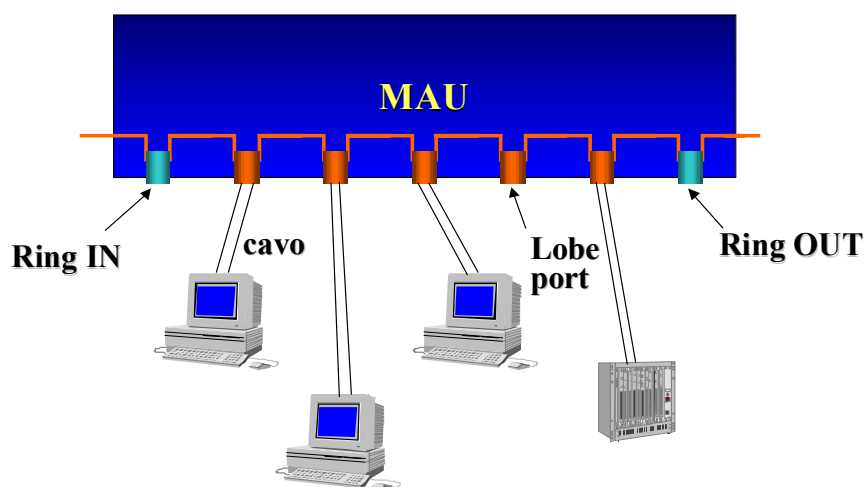


Figura 5.29. Unità MAU.

Nel caso in cui la rete sia realizzata con un'unica MAU (una rete con un numero limitato di dispositivi) le porte Ring In e Ring Out sono collegate tra loro, come mostrato nella Figura 5.30. Nel caso in cui la rete sia realizzata mediante diverse MAU, la porta di Ring di una MAU è connessa con la porta di Ring Out dell'altra MAU, come mostrato nella Figura 5.31. Ogni MAU può avere un numero di porte compreso tra 8 e 20 con velocità di 4 o 16 bit/s. esistono vari tipi di MAU con diverse caratteristiche:

- MAU passiva, che svolgono soltanto la funzione di connettere o disconnettere i dispositivi di rete. Oggi non sono più utilizzati.
- MAU attiva, che oltre a svolgere le funzioni di connessione, amplifica i segnali ricevuti o trasmessi sulle porte (lobo, Ring In e Out). Rappresentano un'ottima soluzione in molti cablaggi.
- MAU parzialmente attiva, che amplifica i segnali solo sulle porte di dorsale (Ring In e Out). Rappresentano una buona soluzione per i sistemi di cablaggio STP o UTP e impongono regole meno restrittive rispetto a MAU attivi.

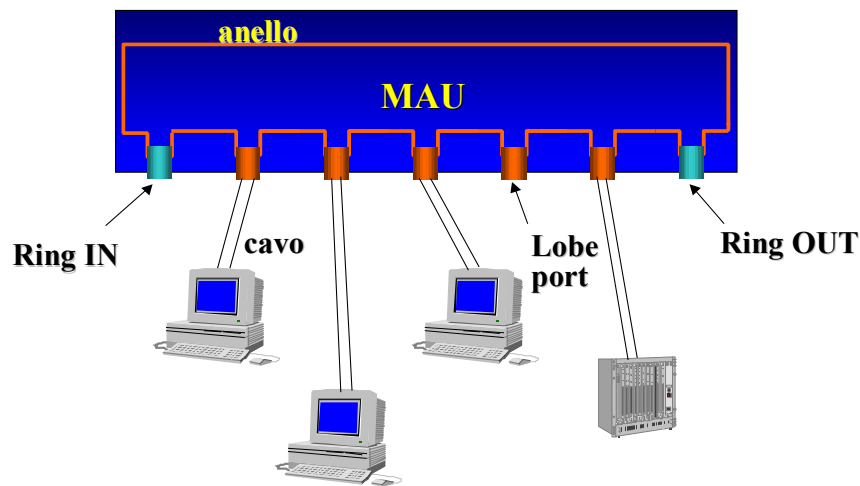


Figura 5.30. Rete token ring con una sola unità MAU.

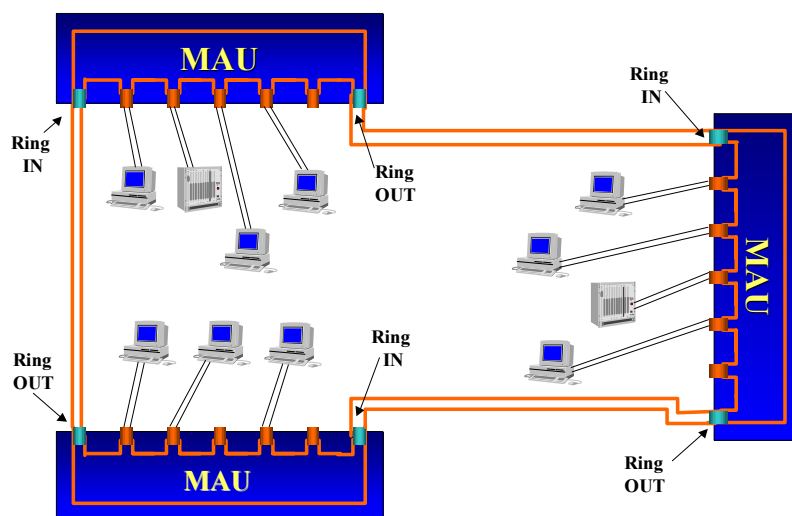


Figura 5.31. Rete token ring realizzata mediante diverse unità MAU.



## Cablaggio

Le reti Token Ring possono essere realizzate mediante tre tipi di cavi:

- *Doppino telefonico non schermato (UTP)*. Questa soluzione presenta il vantaggio di utilizzare un cavo a basso costo e grande flessibilità; tuttavia la lunghezza dell'anello è molto limitata. Possono essere utilizzati i cavi UTP di categoria 3, 4 e 5 per 4 Mbit/s e i cavi 4 e 5 per 16 Mbit/s.
- *Doppino telefonico schermato (STP9 "IBM Cabling System")*. Possono essere utilizzati diversi cavi per varie applicazioni.
- *Fibra ottica*.

In una rete token ring è possibile utilizzare nello stesso anello fibra ottica e UTP o STP. Tuttavia, non è possibile utilizzare sullo stesso anello UTS e STP, poiché presentano impedenze e caratteristiche diverse.

## FDDI (Fiber Distributed Date Interface)

La rete FDDI è stata progettata agli inizi degli anni '80 con lo scopo di realizzare una rete ad alta velocità (100 Mbit/s) su un'area di notevole estensione (decine di Km). FDDI è stata progettata per utilizzare la fibra ottica, anche se successivamente è stato introdotto l'uso dei doppini telefonici per le connessioni tra le stazioni ed i concentratori. Lo standard FDDI è stato definito da ANSI (American National Standard Institute); questo standard presenta una completa aderenza al modello OSI, di cui adotta la struttura a livelli.

Le principali caratteristiche della rete FDDI sono:

- la velocità di trasmissione è di 100 Mbit/s;
- la topologia della rete è ad anello, ma può essere ricondotta ad una configurazione a stella mediante concentratori attivi;
- la rete FDDI presenta una notevole tolleranza ai guasti ed ha una notevole affidabilità.

La struttura della rete FDDI è composta da due anelli concentrici in fibra ottica, come mostrato nella Figura 5.32. I due anelli trasferiscono l'informazione in senso opposto; tuttavia, in un dato istante solitamente un anello (detto anello primario) è effettivamente utilizzato per la trasmissione dei dati. L'altro anello (o anello secondario) entra in funzione soltanto nel caso di malfunzionamenti o guasti sull'anello o sulle stazioni connesse agli anelli.

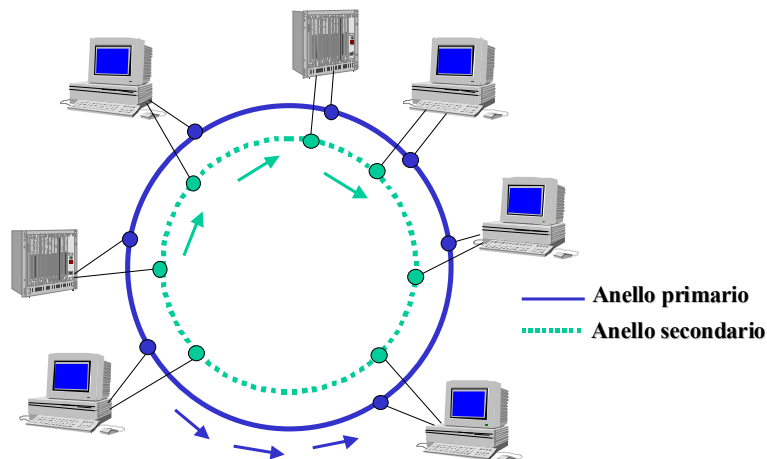


Figura 5.32. La rete FDDI.

#### *I livelli dello standard FDDI*

Lo standard FDDI è stato definito in accordo al modello OSI ed in particolare ai primi due livelli OSI, come mostrato nella Figura 5.33. Il livello fisico viene diviso in due sottolivelli:

- **PMD (Physical Medium Dependent Protocol)**, che descrive le specifiche hardware per la connessione delle stazioni alla rete FDDI, i segnali e le caratteristiche degli apparati e dei mezzi trasmissivi.
- **PHY (PHYsical layer protocol)** che definisce la codifica e decodifica dei dati scambiati tra PHY e MAC ed effettua la sincronizzazione dei dati. In particolare la codifica utilizza 25 simboli, ciascuno composto da 5 bit, di cui 16 simboli sono utilizzati per trasmettere 16 simboli esadecimali e 8 simboli sono utilizzati come codici fuori banda. In questo modo i dati e i segnali di temporizzazione possono essere trasmessi insieme.

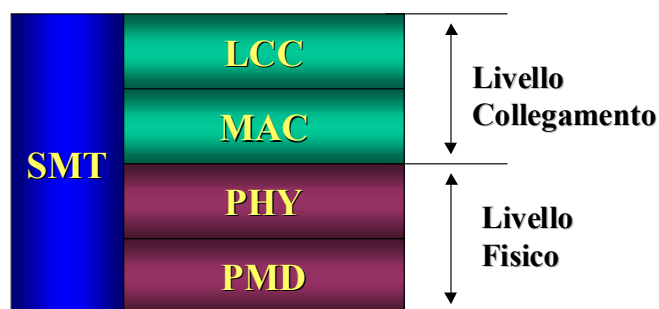


Figura 5.33. Livelli della rete FDDI.

Il livello di collegamento è diviso come per tutte le reti locali nei due sottolivelli:

- **MAC (Medium Access Control)**, che definisce le modalità di accesso delle stazioni della rete.
- **LLC (Logical Link Control)**, che effettua le operazioni di controllo del collegamento. Come per tutte le reti locali, il livello LLC segue lo standard IEEE 802.2.

### Il livello MAC nella rete FDDI

La rete FDDI utilizza un metodo di accesso multiplo di tipo token passing, in modo analogo alla rete token ring. I dati sono trasmessi sull'anello in modo seriale come stringhe di simboli, ciascuno di 5 bit, da una stazione all'altra; ogni stazione che riceve un simbolo lo ritrasmette alla stazione successiva.

Il formato del token utilizzato nella rete FDDI è mostrato nella Figura 5.34 e presenta numerose analogie con quello della rete token ring.



Figura 5.34. Formato del token nella rete FDDI.

Il formato di un pacchetto in una rete FDDI è mostrato nella Figura 5.34. La lunghezza del pacchetto è variabile. Descriviamo in dettaglio i diversi campi presenti nel token e nella trama informativa:

- **Preambolo.** Questo campo, composto da 16 simboli è necessario per sincronizzare il clock di una stazione con quello della stazione precedente nell'anello.
- **SD (Start Delimiter).** Questo campo, formato da 2 simboli, serve a delimitare l'inizio del token o di un frame. Per questo esso contiene due bit (bit J e K) che violano il codice di Manchester.
- **FC (Frame Control).** Questo campo formato da due simboli serve a specificare se il pacchetto ricevuto è un token o un frame. Nel caso di un frame informativo, il campo FC specifica se esso è di tipo *sincrono* (voce o video) o *asincrono* (dati) ed in quest'ultimo caso indica se il campo informativo contiene pacchetti di controllo (MAC PDU).
- **DA (Destination Address).** Questo campo, formato da 12 simboli, contiene l'indirizzo MAC della stazione di destinazione.
- **SA (Source Address).** Questo campo, formato da 12 simboli, contiene l'indirizzo MAC della stazione sorgente.
- **Informazione.** Questo campo, con una lunghezza variabile da 0 a 8956 simboli, contiene le informazioni o dati di controllo.
- **FCS (Frame Check Sequence).** Questo campo, composto da 8 simboli, contiene i bit di ridondanza di un codice ciclico per la rivelazione degli errori.
- **ED (End Delimiter).** Questo campo, formato da 2 simboli, identifica la fine del token o del frame. Esso contiene due bit, J e K, che violano il codici di Manchester.
- **FS (Frame Status).** Questo campo formato da 3 o più simboli, fornisce una serie di informazioni per caratterizzare lo stato della trama. In particolare esso contiene almeno tre simboli seguenti che servono a caratterizzare tale stato:
  - Bit error detected indicator, che indica che il pacchetto è errato. Questo bit è generalmente uguale a 0; una qualunque stazione che rilevi in errore la trama cambia il valore del bit.
  - Address recognized indicator, che viene impostato dalla stazione che riconosce il proprio indirizzo nel campo DA.

- Frame copied indicator, che viene impostato dalla stazione che ha copiato il pacchetto.

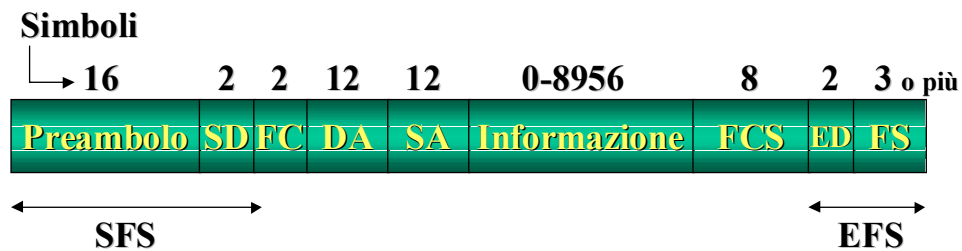


Figura 5.35. Formato del pacchetto FDDI.

### Servizio sincrono e asincrono

Il servizio di trasmissione sincrono utile per la trasmissione di segnali in tempo reale quali la voce e il video, prevede la trasmissione di pacchetti di lunghezza fissa ad intervalli regolari, assicurando una banda minima alle stazioni che devono trasmettere questo tipo di traffico.

*Il servizio di trasmissione asincrono è generalmente utilizzato per la trasmissione dati. Il servizio di trasmissione sincrono è prioritario rispetto a quello asincrono.* Infatti quando una stazione cattura il token trasmette per prima le trame sincrone e successivamente, se ha a disposizione un tempo sufficiente, provvede a trasmettere il traffico asincrono.

### Riconfigurazione di una rete FDDI

La rete FDDI utilizza in condizioni di funzionamento normale soltanto l'anello primario (Figura 5.36.a), mentre l'altro anello rimane in condizioni di riposo. Quando si verifica un guasto o un malfunzionamento (linea interrotta o stazione guasta), le stazioni DAS o DAC adiacenti al punto in cui si è verificato tale guasto rivelano questo inconveniente e provvedono attraverso uno switch interno che collega tra loro i due anelli, formando un unico anello che esclude la stazione o il punto di guasto, come mostrato nella Figura 5.36. b.

La riconfigurazione della rete può avvenire anche a causa di guasti multipli, creando anelli separati. Nella Figura 5.36.c. è mostrato il caso dei due guasti: la rete FDDI viene suddivisa a causa del processo di riconfigurazione in tre anelli separati. In questo modo la rete continua ad operare in modo parziale.

Una volta che guasti o malfunzionamenti sono stati riparati, la rete effettua in modo automatico una riconfigurazione e l'anello ritorna ad operare in modo normale.

### *Tipi di cavo*

Indipendentemente dal cavo utilizzato una rete FDDI non può avere una dimensione superiore a 200 Km, ma è fortemente consigliato di mantenere la lunghezza dell'anello inferiore a 100 Km.

A seconda del tipo di cavo utilizzato sono stati definite diverse configurazioni e parametri per la rete FDDI. In particolare sono attualmente definiti i seguenti quattro standard.

#### Fibra ottica multimodale

La fibra ottica multimodale è molto utilizzata per realizzare la rete FDDI. Sono stati definiti due standard. Lo Standard ANSI X3.166 e ISO/IEC 9314.3 è stato il primo ad essere stato emanato e rappresenta anche quello più noto. Esso utilizza fibre ottiche multimodali 6L/125  $\mu\text{m}$  e LED in seconda finestra. La massima distanza tra due stazioni FDDI può essere al massimo 2 Km. Lo standard ANSI X3.237 prevede una fibra ottica multimodale 62.5/125  $\mu\text{m}$  e LED in seconda finestra, come il precedente, ma utilizza componenti meno costosi. Per questo la distanza massima tra due stazioni FDDI è 500 m.

#### Fibra ottica monomodale

Questo standard, noto come ANSI X3.184, utilizza una fibra ottica monomodale 8.2/125  $\mu\text{m}$  e LESEG in seconda finestra. La distanza massima è 10 Km.

#### Doppino telefonico

Questo tipo di cavo viene utilizzato per collegare stazioni SAS al concentratore DAC. Il doppino telefonico può essere di tipo UTP e STP:

- Doppino telefonico UTP. Il cavo deve essere di categoria 5 e la massima distanza tra stazione e concentratore è 100 m.
- Doppino telefonico STP. Il cavo deve essere di tipo IBM. La massima distanza tra stazione e concentratore è 100 m.

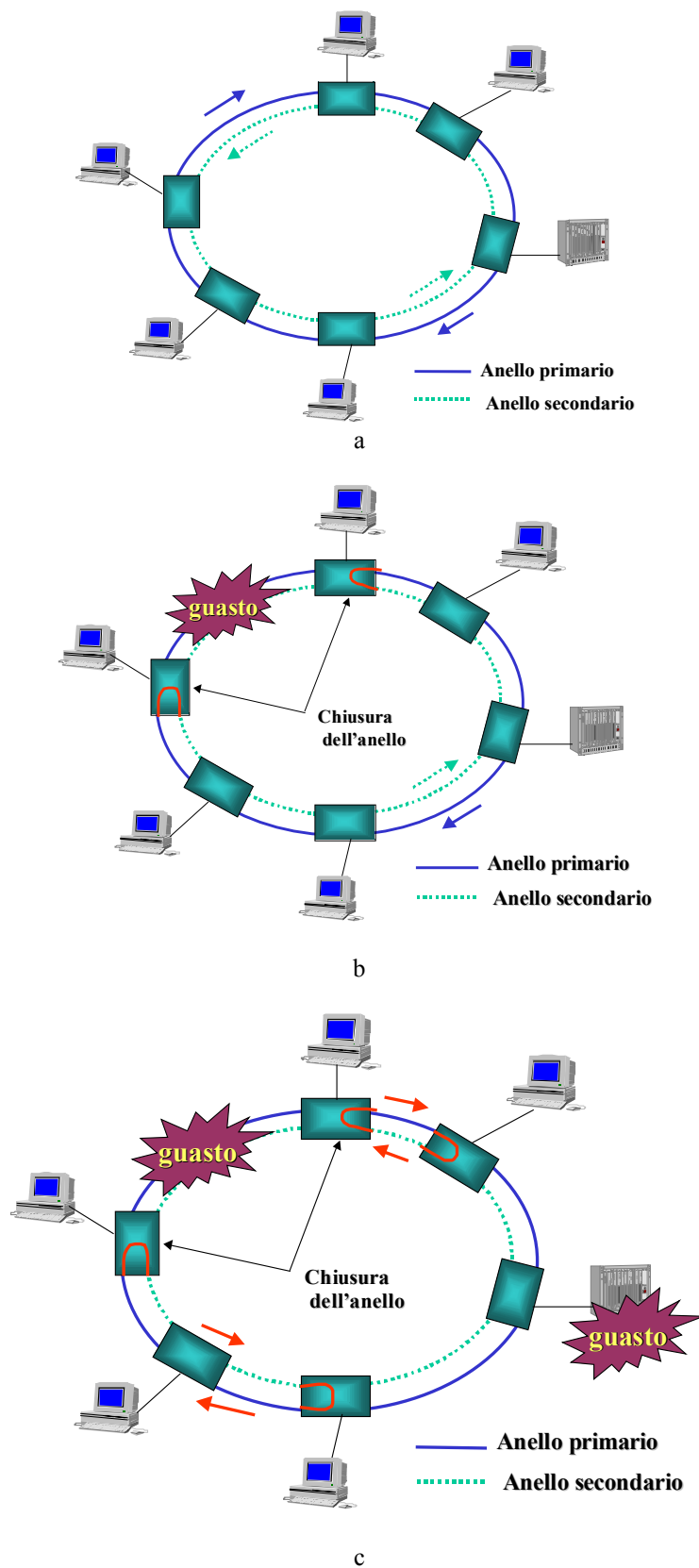


Figura 5.36. Riconfigurazione di una rete FDDI a causa di guasti: a) funzionamento normale; b) riconfigurazione a causa di un guasto; c) riconfigurazione a causa di due guasti.

## Capitolo 6: Teoria delle code ad applicazione alle reti di telecomunicazione

In questo capitolo, vedremo di analizzare in modo quantitativo e qualitativo i fenomeni di ritardo presenti in una rete di telecomunicazione. I parametri esaminati sono il ritardo medio che un pacchetto sperimenta nell'andare da una data sorgente ad una destinazione, ed il volume di traffico che la rete riesce a smaltire nell'unità di tempo (*throughput*).

La teoria delle code è uno strumento essenziale per:

- Caratterizzare le prestazioni di una rete di comunicazione;
- Dimensionare una rete o un apparato di comunicazione in modo da garantire le prestazioni desiderate in termini di ritardo medio.

### 6.1 Elementi di ritardo in una rete di telecomunicazione

Una rete di telecomunicazione consta di un insieme di nodi di smistamento del traffico (sotto forma di pacchetti di bit) inter-connessi da collegamenti. Il ritardo che subirà un generico pacchetto sarà dovuto alla somma dei ritardi accumulati su ogni link attraversato. Il ritardo associato ad ogni link, è costituito da quattro componenti:

1. **Processing delay**: tempo che trascorre da quando il pacchetto è correttamente ricevuto al nodo di testa del link e quando esso viene assegnato alla coda di trasmissione di un link d'uscita.
2. **Queueing delay**: tempo che trascorre tra l'istante in cui il pacchetto è assegnato ad una coda per la trasmissione e l'istante in cui il pacchetto inizia ad essere trasmesso.
3. **Transmission delay**: tempo che trascorre tra l'istante in cui il primo e l'ultimo bit del pacchetto sono spediti.
4. **Propagation delay**: tempo che impiega il segnale elettromagnetico a percorrere un collegamento. Questo tempo dipende dalle caratteristiche del mezzo trasmissivo, ed è proporzionale alla distanza che separa il *sender* dal *receiver*. Si ha ancora che tale ritardo risulta essere molto piccolo a meno del caso delle trasmissioni via satellite.

Da quanto detto sin ora, il nodo potrebbe essere schematizzato come in Figura 6.1, dal quale si deduce che il *processing delay* non è altro che la somma del tempo di attesa nella coda d'ingresso più il tempo di processamento nel server  $S_1$ , il *queueing delay* è il tempo di attesa nella coda d'uscita, mentre il *transmission delay* non è altro che il tempo di processamento o di servizio nel server corrispondente alla coda d'uscita.

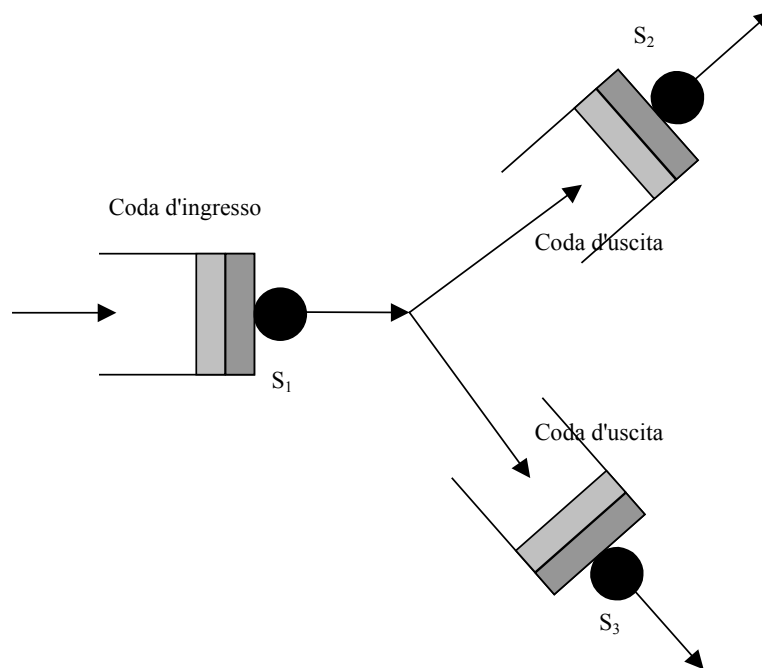


Figura 6.1: Schematizzazione delle code presenti nel generico nodo di una rete.

Quanto detto sin ora trascura la possibilità che un pacchetto debba essere ritrasmesso a causa di un errore o per qualche altra causa. In seguito, nel modellare il generico nodo, trascureremo sia il *propagation delay*, che il *processing delay*, in quanto il primo dipende dalle caratteristiche del mezzo e dalla distanza dei nodi connessi dal link, ma è del tutto indipendente dal traffico presente nella rete. Il processing delay, nelle reti a banda stretta, può essere trascurato, poiché incide poco sul ritardo totale. Esso rappresenta il tempo di lettura e di processamento del dato da parte del nodo di commutazione. Con l'ultima assunzione sparisce la coda d'ingresso ed il relativo server dalla Figura 6.1.

#### 6.1.1 Ritardo di trasmissione per traffico multiplexato

Abbiamo visto nel paragrafo precedente che uno degli addendi del ritardo di un pacchetto è costituito dal ritardo di trasmissione (*transmission delay*). Vedremo ora di valutare questo termine nel caso in cui la tecnica di multiplexing sia *TDM*, *FDM* o *Statistical Multiplexing*. Nel link possono essere trasmessi un certo numero di bit al secondo e questo valore, indicato tipicamente con  $C$  ed espresso in bps (bit/s), dipende sia dalle caratteristiche del mezzo fisico di cui il link è costituito, che dalle interfacce usate per la comunicazione.

#### 6.1.2 Statistical Multiplexing

In questo caso i pacchetti che arrivano dalle varie sorgenti sono posti in un'unica coda e vengono serviti con una politica di tipo FIFO.  $L$  bits sia la *lunghezza di un generico pacchetto* e  $C$  bit/s la *capacità del canale*; poiché la risorsa trasmissiva è allocata interamente ad un singolo pacchetto alla volta si ha:

$$t_d = L / C \quad (6.1)$$



### 6.1.3 Frequency Division Multiplexing (FDM)

Supponiamo di avere  $m$  sorgenti di traffico, le quali devono essere multiplexate mediante FDM sul nostro link. In tal caso, detta  $W$  la banda passante del canale, ad ogni stream di traffico verrà associato un canale avente banda circa pari a  $W/m$ . Detta  $C$  bit/s la capacità trasmissiva del canale, all' $i$ -esimo traffic stream sarà associato un canale di  $C/m$  bit/s circa. Quindi, il tempo necessario a trasmettere un pacchetto lungo  $L$  bits è pari a:

$$t_d = mL/C \quad (6.2)$$

Osserviamo come questo tempo sia  $m$  volte più grande rispetto a quello relativo allo statistical multiplexing.

### 6.1.4 Time Division Multiplexing (TDM)

Supponendo di avere sempre  $m$  stream di traffico, dobbiamo distinguere il caso in cui la dimensione degli slot è piccola rispetto alla lunghezza del pacchetto, dal caso in cui slot e pacchetto hanno la stessa dimensione. Nel primo caso, per trasmettere un pacchetto di  $L$  bits, si ha lo stesso tempo di trasmissione dato dalla (6.2). Infatti anche in questo caso è come se ogni stream avesse associato un canale di capacità  $C/m$ . Nel caso in cui la dimensione del pacchetto e quella dello slot coincidono, vale la relazione (6.1) ma bisogna aspettare un tempo pari a:

$$(m - 1) L/C$$

prima di poter trasmettere un altro pacchetto appartenente allo stesso stream.

Dalle relazioni ricavate sin ora si nota che lo *statistical multiplexing* è quello che garantisce il transmission delay più piccolo. Ciò è dovuto al fatto che le risorse allocate ai clienti dagli schemi di multiplexazione TDM ed FDM vengono sprecate nel caso in cui una sorgente non ha da trasmettere. Resta adesso da calcolare il *queueing delay*. Questa grandezza è più difficile da calcolare poiché è un parametro statistico e per il suo studio faremo uso della teoria delle code.

## 6.2 Sistemi a Coda

Un sistema a coda si può genericamente definire come un sistema in cui vi sono degli utenti (*clienti*) che arrivano e che vogliono utilizzare una risorsa finita (*servente*). I clienti (*customers*) richiedenti un dato servizio, sono generati nel tempo da una *sorgente*. Questi clienti entrando nel *queueing system* e formano una coda (= lista d'attesa). A certi istanti, un membro della coda viene scelto come prossimo cliente da servire, secondo una certa politica nota come *disciplina della coda*; per esempio la disciplina potrebbe essere *First In First Out* (FIFO), *Last In First Out* (LIFO), etc. Il servizio richiesto dal cliente viene quindi svolto dal *servente* e il *customer* può uscire dal sistema a coda. Questo processo è rappresentato in Figura 6.2.

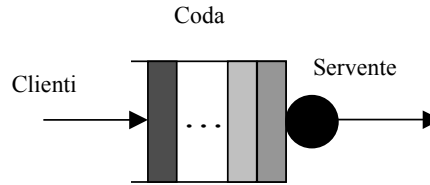


Figura 6.2: Schema di un sistema a coda.

Possono essere fatte svariate assunzioni sui vari elementi che costituiscono il queueing system. In generale, per caratterizzare un sistema a coda, deve essere specificata la *statistica dei tempi di interarrivo*, la *statistica dei tempi di servizio*, nonché la *disciplina usata per gestire la coda*.

In una rete di telecomunicazione i *customers* sono rappresentati dai pacchetti che arrivano e vengono assegnati ad un link per la trasmissione, mentre il *server* è rappresentato dalla linea di comunicazione. La *coda* corrisponde, invece, al buffer associato al link uscente dal nodo, tramite cui il pacchetto deve essere spedito.

Date le distribuzioni di probabilità dei tempi di interarrivo e dei tempi di servizio, il nostro obiettivo sarà quello di determinare le seguenti quantità:

- Il numero medio di clienti nel sistema;
- Il ritardo medio del generico cliente.

Per numero di clienti nel sistema si intende il numero di utenti presenti nella coda più il numero dei clienti che stanno usufruendo del servizio offerto dal sistema. Il ritardo di un cliente è costituito dal tempo di attesa in coda più il tempo di servizio.

Detta:

$p_n(t)$  = Probabilità che all'istante  $t$  vi siano  $n$  clienti nel sistema,

supposte note le informazioni statistiche necessarie per la determinazione delle probabilità  $p_n(t)$  per ogni  $t$ , definito:

$N(t)$  = Numero medio di clienti nel sistema al tempo  $t$ ,

si ha

$$E\{N(t)\} = N(t) = \sum_{n=0}^{+\infty} n \cdot p_n(t) \quad (6.3)$$

Osserviamo che sia  $p_n(t)$  che  $E\{N(t)\}$  dipendono dal tempo e dalla distribuzione delle probabilità al tempo  $t = 0$ , ossia,  $\{p_0(0), p_1(0), p_2(0), \dots, p_n(0), \dots\}$ . I sistemi con cui avremo a che fare saranno caratterizzati dal fatto di raggiungere una condizione di equilibrio, nel senso che:

$$\lim_{t \rightarrow \infty} p_n(t) = p_n$$

$$N = \sum_{n=0}^{+\infty} np_n = \lim_{t \rightarrow \infty} \overline{N}(t) \quad (6.4)$$

dove  $p_n$  e  $N$  sono indipendenti dalla distribuzione delle probabilità iniziale.

Detta  $N(t)$  una funzione di campionamento del numero dei clienti nel sistema, definiamo media temporale di tale funzione nell'intervallo  $[0, t]$  la grandezza:

$$N_t = \frac{1}{t} \int_0^t N(\tau) d\tau \quad (6.5)$$

Si definisce **ergodico**, un sistema per il quale vale la relazione:

$$\lim_{t \rightarrow \infty} N_t = \lim_{t \rightarrow \infty} \overline{N}(t) = N \quad (6.6)$$

Notiamo che se un sistema è ergodico, la media statistica e quella temporale coincidono.

Consideriamo ora il ritardo medio del generico cliente. Supposta nota la distribuzione di probabilità di ritardo di ciascun cliente, siamo in grado di calcolare il ritardo medio di ogni cliente. Sia  $E\{T_k\}$  il ritardo medio del  $k$ -esimo cliente.

Nel caso in cui il sistema converga ad un valore stazionario per  $k \rightarrow \infty$ , si ha che il ritardo medio del generico cliente sarà:

$$T = \lim_{k \rightarrow \infty} \overline{T}_k \quad (6.7)$$

Se il sistema è ergodico si ha che:

$$T = \lim_{k \rightarrow \infty} \overline{T}_k = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k T_i \quad (6.8)$$

dove  $T_i$  rappresenta il ritardo dell' $i$ -esimo cliente.

### 1.2.1 Applicazione dei sistemi a coda nelle reti

I sistemi a coda possono essere usati per modellare sia le reti a commutazione di pacchetto che le reti a commutazione di circuito. Nelle reti a commutazione di pacchetto i *clienti* sono i pacchetti da trasmettere. Supponendo che i pacchetti (= messaggi) abbiano dimensione variabile con media di  $L$  bit e che il canale trasmissivo abbia capacità di

trasmissione pari a  $C$  bit/s (singolo servente), il tempo medio di trasmissione di un pacchetto è dato da:

$$\frac{1}{\mu} = \frac{L}{C} \quad (6.9)$$

dove  $\mu$  (rate medio di servizio espresso in pacchetti/secondo) è il numero medio di pacchetti trasmessi dal servente in un secondo. Detto  $\lambda$  il numero medio di arrivi in un secondo, si definisce **fattore di utilizzazione del servente** o intensità di traffico (misurata in Erlang):

$$\rho = \frac{\lambda}{\mu} \quad (6.10)$$

e sostituendo la (6.9) nella (6.10) si ha:

$$\rho = \frac{\lambda \cdot L}{C} \quad (6.11)$$

Il numeratore della (6.11) rappresenta il carico medio nella rete ( $\lambda L$  [bit/s]), mentre il denominatore rappresenta la capacità di trasmissione della rete [bit/s]. Dunque il parametro  $\rho$  fornisce quantitativamente la misura di *quanto è caricato il sistema*. Se tale parametro è maggiore di 1, il sistema non riesce a smaltire il carico, poiché il numero medio di arrivi è superiore al numero medio di partenze (instabilità della relativa coda di attesa).

## 6.2 Teorema di Little

Il teorema di Little stabilisce che tra  $N$  e  $T$  intercorre una dipendenza lineare. Detta  $\lambda$  la costante di proporzionalità risulta:

$$N = \lambda T \quad (6.12)$$

dove:

$\lambda =$  *tasso medio degli arrivi*

ed è dato dalla relazione:

$$\lambda = \lim_{t \rightarrow \infty} \frac{\text{valore medio di arrivi in } [0, t]}{t} \quad (6.13)$$

Definiamo rispettivamente:

- $\alpha(t)$  = Numero degli arrivi nell'intervallo  $[0, t]$ ,
- $\beta(t)$  = Numero delle partenze nell'intervallo  $[0, t]$ .

Supposto  $N(0) = 0$ , dalla definizione di  $\alpha(t)$  e  $\beta(t)$  risulta chiaramente:

$$N(t) = \alpha(t) - \beta(t) \quad (6.14)$$

dove  $N(t)$  indica il numero di clienti presenti nel sistema all'istante  $t$ . Indichiamo con  $t_i$  l'istante in cui l' $i$ -esimo utente arriva nel sistema, mentre con  $T_i$  il tempo speso nel sistema dall' $i$ -esimo utente. Consideriamo ora ad un istante  $t$ , l'area racchiusa tra le due curve di Figura 6.3 che, in virtù della (6.14), è pari a:

$$\int_0^t N(\tau) d\tau$$

Ma d'altro canto risulta:

$$\int_0^t N(\tau) d\tau = \sum_{i=1}^{\beta(t)} T_i + \sum_{i=\beta(t)+1}^{\alpha(t)} (t - t_i) \quad (6.15)$$

Dividendo ambo i membri della (6.15) per  $t$  si ottiene:

$$\frac{1}{t} \int_0^t N(\tau) d\tau = \frac{\alpha(t)}{t} \frac{\sum_{i=1}^{\beta(t)} T_i + \sum_{i=\beta(t)+1}^{\alpha(t)} (t - t_i)}{\alpha(t)} \quad (6.16)$$

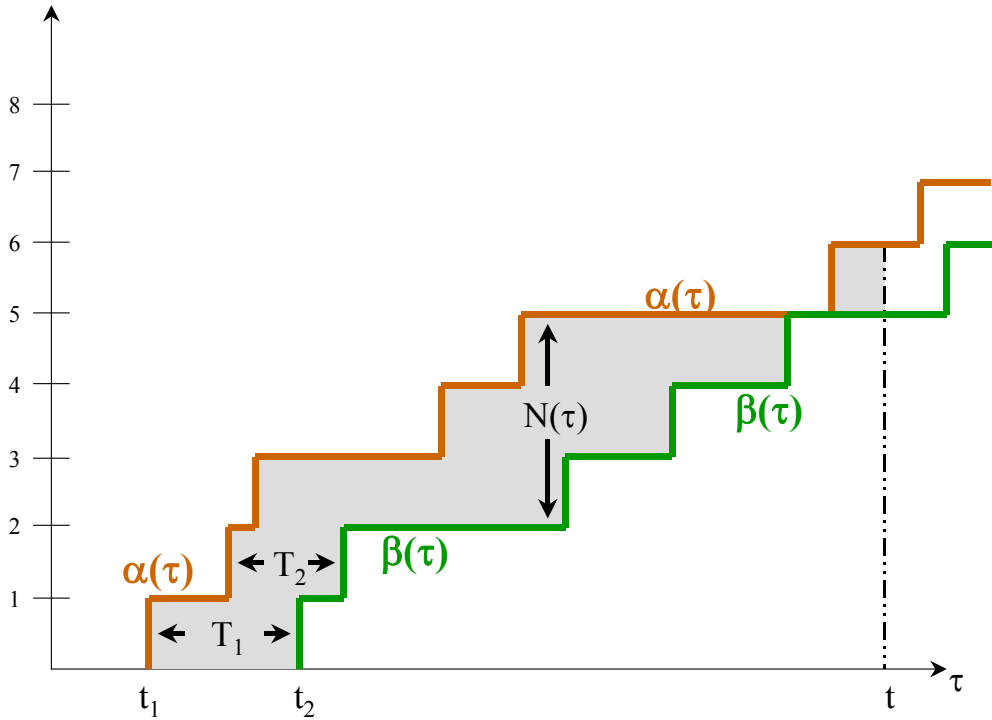


Figura 6.3: Schematizzazione degli arrivi e delle partenze in un sistema.

Osserviamo che il primo membro della (6.16) non è altro che la media temporale in  $[0, t]$  del numero di clienti presente nel sistema. D'altro canto si ha che:

$$\frac{\alpha(t)}{t} = \lambda_t$$

dove  $\lambda_t$  rappresenta la media temporale del tasso degli arrivi nell'intervallo  $[0, t]$ . Infine notiamo che risulta:

$$\frac{\sum_{i=1}^{\beta(t)} T_i + \sum_{i=\beta(t)+1}^{\alpha(t)} (t - t_i)}{\alpha(t)} = T_t$$

dove  $T_t$  rappresenta la media temporale del tempo che un cliente spende nel sistema nell'intervallo  $[0, t]$ . In virtù di queste osservazioni possiamo scrivere:

$$N_t = \lambda_t T_t \quad (6.17)$$

Se supponiamo che si abbia (processo ergodico):

$$\begin{aligned}\lim_{t \rightarrow \infty} N_t &= N \\ \lim_{t \rightarrow \infty} \lambda_t &= \lambda \\ \lim_{t \rightarrow \infty} T_t &= T\end{aligned}$$

segue subito la formula di Little  $N = \lambda T$ .

E' importante notare che  $T_t$  include il tempo speso nel sistema da tutti i clienti arrivati tra 1 e  $\beta(t)$ , ma traslascia il tempo speso dai clienti ancora nel sistema all'istante  $t$ . Se si suppone che  $N_t \rightarrow N < \infty$ , (il che implica che tutti i clienti sono serviti in un tempo finito) l'effetto dovuto ai clienti presenti nel sistema all'istante  $t$  diviene via via trascurabile, ed al crescere di  $t$ , così che  $T_t$  può effettivamente essere interpretato come la media temporale del tempo di sistema.

L'importanza del teorema di Little deriva dalla sua generalità. Esso può essere applicato ad un qualsiasi sistema a coda che raggiunga una condizione di equilibrio statistico. La cosa importante nell'applicare il teorema di Little è quella di interpretare nel modo appropriato  $N$ ,  $\lambda$  e  $T$ . Prendiamo in esame la parte di attesa della coda: la lunghezza media coda è data dalla relazione:

$$N_Q = \lambda W \quad (6.18)$$

dove  $W$  è il tempo medio di attesa in coda.

Analogamente, applicando il teorema di Little nella parte di uscita del sistema a coda (= lato servente), si ha che il numero medio di pacchetti in trasmissione  $\rho$  è dato dalla frequenza di arrivo dei pacchetti  $\lambda$  per il tempo medio di trasmissione,  $\bar{X} = \frac{1}{\mu}$ :

$$\rho = \lambda \bar{X} \quad (6.19)$$

Il parametro  $\rho$  è chiamato **fattore di utilizzazione** del sistema, perché è definito come il numero medio di pacchetti entranti nel servente per il tempo medio di trasmissione, ovvero rappresenta la porzione di tempo per il quale il sistema è occupato nella trasmissione di un pacchetto.

Gli **aspetti caratterizzanti** un sistema a coda sono:

- *Distribuzione del processo di arrivo delle richieste.* Si utilizza spesso anche la distribuzione del tempo che intercorre tra gli arrivi di richieste successive. Il numero medio o *tasso medio di arrivo delle richieste* in un secondo è generalmente indicato con  $\lambda$ ,
- *Distribuzione della durata o lunghezza di un arrivo,*
- *Capacità del buffer per la memorizzazione delle richieste* in attesa di servizio ovvero la

capacità della coda,

- **Capacità di fornire il servizio** ovvero *numero di serventi*,
- **Tempo di servizio**: tempo che occorre al servente per soddisfare la richiesta in servizio. Può essere fisso o caratterizzato statisticamente.
- **Disciplina di coda**. La disciplina con cui si regola l'accesso al servizio può avere varie modalità:
  - Disciplina **FIFO** (*First In First Out*): la prima richiesta che raggiunge il sistema è la prima ad essere servita;
  - Disciplina **LIFO** (*Last In First Out*): l'ultima richiesta arrivata è la prima ad essere servita;
  - Disciplina **Random**: le richieste sono servite in modo casuale con distribuzione uniforme;
  - Disciplina con **priorità**. In questo caso si possono adottare due strategie:
    - **Priorità con interruzione di servizio**: all'arrivo di una richiesta con priorità maggiore rispetto a quella della richiesta attualmente servita, il servizio viene concesso immediatamente, togliendolo a quella che ne usufruiva.
    - **Priorità senza interruzione di servizio**: all'arrivo di una richiesta con priorità maggiore rispetto a quella della richiesta attualmente servita, il sistema termina il servizio in atto e successivamente serve la richiesta con priorità maggiore.

I parametri più importanti per lo studio e la valutazione della bontà di un sistema a coda sono:

- **Tempo di attesa in coda**: tempo che intercorre da quando una richiesta entra in coda a quando viene servita. Questo parametro è ovviamente influenzato dal tempo medio di servizio di ciascuna richiesta, dalla frequenza degli arrivi delle richieste e dalla lunghezza della coda;
- **Tempo trascorso nel sistema**: somma del tempo trascorso dalla richiesta all'interno della coda e del tempo di servizio a questa dedicato;
- **Numero di richieste all'interno del sistema**: costituito dalla somma del numero delle richieste presenti in coda e all'interno del/dei servente/i;
- **Tempo di occupato/libero di ogni servente**. E' intuitivo che aumentando il numero di serventi, diminuisce il numero di richieste presenti in coda. Ogni servente implica, però, una spesa che deve essere ripagata da un suo utilizzo efficiente e continuativo. Un numero troppo elevato di serventi utilizzati per una piccola frazione del tempo complessivo, può diminuire molto i tempi di coda, ma aumentare considerevolmente i costi diminuendo, inoltre, l'efficienza del sistema.

### 6.3 Nomenclatura per i sistemi a coda: la notazione di Kendall

La nomenclatura, introdotta da Kendall per identificare i vari tipi di sistemi a coda fa uso di 5 simboli separati dal carattere "/":

1. La *prima lettera* indica la natura del processo degli arrivi. I valori tipici sono:
  - a. M: *memoryless*, indica che il processo degli arrivi è un processo di Poisson (distribuzione di probabilità dei tempi di interarrivo di tipo esponenziale e quindi senza memoria).



- b. G: *general*, indica che il processo degli arrivi è caratterizzato da una distribuzione di probabilità generale. In questo caso serve conoscere i momenti del 1° e del 2° ordine della distribuzione dei tempi di interarrivo.
  - c. D: *deterministic*, indica che il processo degli arrivi è deterministico e cioè con tempi di interarrivo costanti. Cioè i tempi di servizio sono costanti.
2. La *seconda lettera* indica la natura della distribuzione di probabilità dei *tempi di servizio*. I valori possibili, anche in questo caso, sono M, G, D e il significato è uguale a quello spiegato precedentemente con l'unica differenza che tali simboli si riferiscono alla distribuzione di probabilità del tempo di servizio di una richiesta.
  3. Il terzo simbolo indica il numero di serventi del sistema a coda.
  4. Il *quarto simbolo* indica il *numero massimo di clienti nel sistema*. Questo simbolo potrebbe non essere presente e per default è infinito.
  5. Il *quinto simbolo* indica il *numero massimo di sorgenti*. Anche questo simbolo potrebbe non essere presente e per default è infinito. Ogni sorgente (nel nostro caso sorgente di pacchetti) può immettere un solo pacchetto alla volta, e potrà produrne un altro solo quando il precedente è stato spedito.

Un sistema a coda di tipo M/M/1 è dunque caratterizzato da un solo servente (terzo simbolo), i clienti arrivano secondo un processo di Poisson con tasso medio  $\lambda$  e la distribuzione dei tempi di servizio è esponenziale con valor medio  $1/\mu$  sec. Il numero massimo di clienti nel sistema e il numero massimo di sorgenti attive nel sistema è infinito. I sistemi caratterizzati da processo di interarrivo e processo delle partenze a distribuzione esponenziale sono i più semplici da studiare e anche i più conservativi (come provato dal confronto con i sistemi M/G/1). I sistemi M/M/N possono essere studiati e risolti con la teoria delle *catene di Markov*. E' possibile, in particolare, calcolare la probabilità  $p_n$  che nel sistema vi siano  $n$  utenti e tramite essa è possibile ricavare il **numero medio di utenti** nel sistema ( $N$ ). Si ha infatti che:

$$N = \sum_{n=0}^{\infty} n \cdot p_n \quad (6.20)$$

Sfruttando il teorema di Little è facile ricavare anche il **tempo medio trascorso da un utente** nel sistema,  $T$ :

$$T = \frac{N}{\lambda} \quad (6.21)$$

In modo analogo è possibile ricavare il numero medio di utenti in coda ( $N_Q$ ) ed il tempo medio di attesa in coda di un utente ( $W$ ).

Qui di seguito si analizzeranno i sistemi a coda più importanti del tipo M/M/1, M/M/N, M/M/ $\infty$ , M/M/1/N, M/M/N/N e M/G/1.

## 6.4 Catene di Markov

I processi di Markov rivestono una particolare importanza nella teoria delle reti di telecomunicazione. In questa sezione sono elencate le proprietà generali delle catene di Markov. Consideriamo lo stato  $X(t)$  (= numero di messaggi in un buffer di trasmissione) di un sistema ad un certo istante  $t$  e supponiamo che  $X(t)$  possa assumere valori discreti da un insieme numerabile  $\{a_1, a_2, \dots\}$ .

L'occupazione degli stati nel tempo è un processo aleatorio che è molto importante per valutare il comportamento di un sistema di comunicazione. I processi di Markov possono essere divisi in due classi:

1. Processi di Markov tempo-discreto.
2. Processi di Markov tempo-continuo.

### 6.4.1 Catene di Markov tempo-continue e tempo-discrete

Il processo  $N(t)$  (utenti nel sistema all'istante  $t$ ) può essere studiato facendo uso delle catene di Markov tempo continue, dove la variabile  $t$  assume valori continui. E' possibile anche adottare la teoria (più semplice) delle catene di Markov tempo-discrete (la variabile  $t$  è discreta) utilizzando questo semplice artificio: consideriamo gli istanti di tempo

$$0, \delta, 2\delta, \dots, k\delta, \dots$$

dove  $\delta$  è un numero positivo *piccolo*. Indichiamo con:

$$N_k = \text{numero di utenti nel sistema all'istante } k\delta, N(k\delta).$$

Poiché  $N(t)$  è una catena di Markov tempo continua e  $N_k = N(k\delta)$ , si vede che:

$$\{ N_k \mid k = 0, 1, 2, \dots \}$$

è una catena di Markov tempo-discreta.

Detto questo, diamo una definizione più rigorosa alle catene di Markov tempo-discrete. Sia  $\{X_n \mid n = 0, 1, \dots\}$  un processo stocastico tempo discreto che assume valori interi non negativi. Gli stati in cui il processo può trovarsi sono:  $i = 0, 1, \dots$

Il processo è una **catena di Markov** se, c'è una probabilità fissa  $P_{ij}$  che il processo si troverà prossimamente nello stato  $i$  supponendo che si trovi nello stato  $j$  e tale probabilità è indipendente dalla storia che ha portato il processo nello stato  $i$ . Tale concetto è riassunto nelle equazioni sottostanti:

$$P_{ij} = P\{X_{n+1} = j \mid X_n = i, X_{n-1} = i_{n-1}, \dots, X_0 = i_0\} = P\{X_{n+1} = j \mid X_n = i\} \quad (6.22)$$
$$\forall n > 0, i_{n-1}, \dots, i_0, i, j$$

Le  $P_{ij}$  così definite sono dette *probabilità di transizione* dallo stato  $i$  allo stato  $j$ .

Ovviamente, essendo probabilità risulterà che:

$$P_{ij} \geq 0, \quad \sum_{j=0}^{\infty} P_{ij} = 1, \quad i = 0, 1, \dots \quad (6.23)$$

Si definisce matrice delle probabilità di transizione:

$$P = \begin{bmatrix} P_{00} & P_{01} & P_{02} & \dots \\ P_{10} & P_{11} & P_{12} & \dots \\ \dots & \dots & \dots & \dots \\ P_{q0} & P_{q1} & P_{q2} & \dots \end{bmatrix}$$

Possono essere definite anche le probabilità di transizione ad n passi:

$$P_{ij}^n = P\{X_{n+m} = j \mid X_m = i\} \quad n \geq 0, i \geq 0, j \geq 0$$

e può essere calcolata la matrice di transizione ad n passi  $P^n$ .

Date le probabilità di transizione ad n passi vale l'equazione di *Chapman-Kolmogorov*:

$$P_{ij}^{n+m} = \sum_{k=0}^{\infty} P_{ik}^n \cdot P_{kj}^m, \quad n, m \geq 0 \quad i, j \geq 0 \quad (6.24)$$

Introduciamo adesso alcune definizioni.

Si dice che due stati  $i$  e  $j$  **comunicano** tra loro se esistono due indici  $n$  e  $n'$  tali che:

$$P_{ij}^n > 0 \\ P_{ji}^{n'} > 0$$

Se tutti gli stati comunicano fra loro, la catena di Markov si dice **irriducibile**.

Una catena di Markov si dice aperiodica se esiste uno stato in cui è possibile ritornare solo dopo un numero di passi multiplo di  $d > 2$ .

Una distribuzione di probabilità  $\{p_j \mid j \geq 1\}$  si dice essere una **distribuzione stazionaria** per la catena di Markov se:

$$p_j = \sum_{i=0}^{\infty} p_i \cdot P_{ij}, \quad j \geq 0 \quad (6.25)$$

Per catene di Markov **irriducibili e aperiodiche** si ha che:

$$p_j = \lim_{n \rightarrow \infty} P_{ij}^n, \quad j \geq 0 \quad (6.26)$$

dove  $p_j$  rappresenta la probabilità, a regime, che il sistema si trovi in quello stato; essa rappresenta dunque anche la porzione di tempo in cui il processo *visita* in media lo stato  $j$ ;  $1/p_j$  rappresenta il **tempo medio di ricorrenza**, ovvero il numero atteso di transizioni tra due successive visite dello stato  $j$  (se  $p_j = 0$ , il tempo medio di ricorrenza è infinito).

Si può inoltre dimostrare che in una catena di Markov irriducibile e aperiodica possono verificarsi due possibilità:

1.  $p_j = 0$  per tutti gli stati  $j \geq 0$ . In questo caso la catena di Markov non ha distribuzione stazionaria (è il caso di un sistema M/M/1 in cui il tasso medio di arrivo è maggiore del tasso medio di servizio).
2.  $p_j > 0$  per tutti gli stati  $j \geq 0$ . In questo caso la distribuzione di probabilità:

$$p_j = \sum_{i=0}^{\infty} p_i \cdot P_{ij}, \quad j \geq 0$$

è **l'unica** distribuzione stazionaria della catena.

La distribuzione stazionaria di una catena di Markov, se esiste, può essere calcolata attraverso le **equazioni di bilanciamento globale**. Esse derivano dalla (6.23). Si ha infatti che:

$$\sum_{i=0}^{\infty} P_{ij} = P_{jj} + \sum_{i=0, i \neq j}^{\infty} P_{ij} = 1 \Rightarrow \sum_{i=0, i \neq j}^{\infty} P_{ij} = 1 - P_{jj}$$

moltiplicando ambo i membri per  $p_j$  si ha:

$$p_j \cdot \sum_{i=0, i \neq j}^{\infty} P_{ji} = p_j - p_j \cdot P_{jj}.$$

Sfruttando la (6.25) si ha che:

$$p_j \cdot \sum_{i=0, i \neq j}^{\infty} P_{ji} = \sum_{i=0}^{\infty} p_i \cdot P_{ij} - p_j \cdot P_{jj} \Rightarrow p_j \cdot \sum_{i=0, i \neq j}^{\infty} P_{ji} = \sum_{i=0}^{\infty} p_i \cdot P_{ij} - (p_i \cdot P_{ij})_{i=j}$$

da cui si ottiene:

$$p_j \cdot \sum_{i=0, i \neq j}^{\infty} P_{ji} = \sum_{i=0, i \neq j}^{\infty} p_i \cdot P_{ij} \quad (6.27)$$

La (6.27) indica che in condizioni di equilibrio, la probabilità di una transizione in partenza dallo stato  $j$  eguaglia la probabilità di una transizione in arrivo allo stato  $j$ .

Generalizzando il discorso ad un insieme di stati  $S$  si ottengono le equazioni di bilanciamento globale:

$$\sum_{j \in S} p_j \sum_{i \notin S} P_{ji} = \sum_{i \notin S} p_i \sum_{j \in S} P_{ij} \quad (6.28)$$

La (6.28) indica che la probabilità che si abbia una transizione in partenza da  $S$  è pari alla probabilità che si abbia una transizione verso  $S$ .

#### 6.4.2 Processi di nascita e morte

I processi di nascita e morte sono catene di Markov in cui due stati successivi differiscono solo di una unità, le transizioni dal generico stato  $k$  sono permesse solo verso gli stati adiacenti  $k + 1$  e  $k - 1$ . Tali processi sono ideali per caratterizzare l'evolvere di una coda. In essa, infatti, gli utenti arrivano uno alla volta e si accodano per ricevere il servizio. Nella trattazione seguente si fa sempre riferimento alla trattazione tempo-discreta equivalente.

Condizione necessaria e sufficiente affinché la catena sia irriducibile è che:

$$P_{i,i+1} > 0 \text{ e } P_{i+1,i} > 0 \text{ per ogni } i$$

Considerando l'insieme di stati  $S = \{0, 1, 2, \dots, n\}$ , le equazioni di bilanciamento parziali (6.28) danno:

$$p_n P_{n,n+1} = p_{n+1} P_{n+1,n} \quad n = 0, 1, \dots \quad (6.29)$$

ovvero, la probabilità di una transizione dallo stato  $n$  allo stato  $n + 1$  è pari alla probabilità di una transizione dallo stato  $n + 1$  allo stato  $n$ .

Generalizzando la (6.29) si ottengono le **equazioni di bilanciamento dettagliate**:

$$p_j \cdot P_{ji} = p_i \cdot P_{ij} \quad i, j \geq 0 \quad (6.30)$$

Queste equazioni permettono di calcolare facilmente la distribuzione stazionaria delle probabilità di stato  $\{p_j \mid j \geq 0\}$ . Osserviamo che **non sempre** valgono le equazioni di bilanciamento dettagliate per una data catena di Markov irriducibile e aperiodica. Un modo per verificare la loro validità è ipotizzarne la validità e tentare di risolvere il sistema che ne viene fuori per ottenere le probabilità  $p_j$  con la condizione al contorno che:

$$\sum_j p_j = 1$$

Esistono due possibilità:

1. l'assunzione non è vera, ed il sistema di equazioni è inconsistente;
2. l'assunzione è vera, e la distribuzione di probabilità  $\{p_j \mid j \geq 0\}$  trovata è l'unica distribuzione stazionaria del sistema (sicuramente essa soddisfa anche le equazioni di bilanciamento globali).

Valgono le equazioni di bilanciamento seguenti:

$$p_j \sum_{j \in S_j^m} P_{ji} = \sum_{j \in S_j^m} p_j \cdot P_{ji} \quad m = 1, 2, \dots, k \quad (6.31)$$

Le (6.31) vengono dette **equazioni di bilanciamento parziali**. Si può dimostrare che se la  $\{p_j \mid j \geq 0\}$  risolve un insieme di equazioni di bilanciamento parziali, allora risolve anche le equazioni di bilanciamento globali, e quindi è l'unica distribuzione stazionaria della catena di Markov irriducibile e aperiodica. E' quindi importante individuare il giusto insieme di equazioni parziali soddisfatte dalla distribuzione stazionaria per calcolare quest'ultima nel modo più semplice possibile.

Un metodo pratico per risolvere le catene di nascita-morte nel tempo-continuo è procedere come segue, facendo riferimento al generico processo nascita morte indicato in Figura 6.4 dove  $\lambda_i$  è il tasso medio di nascita dallo stato  $i$  e  $\mu_i$  è il tasso medio di morte dallo stato  $i$ .

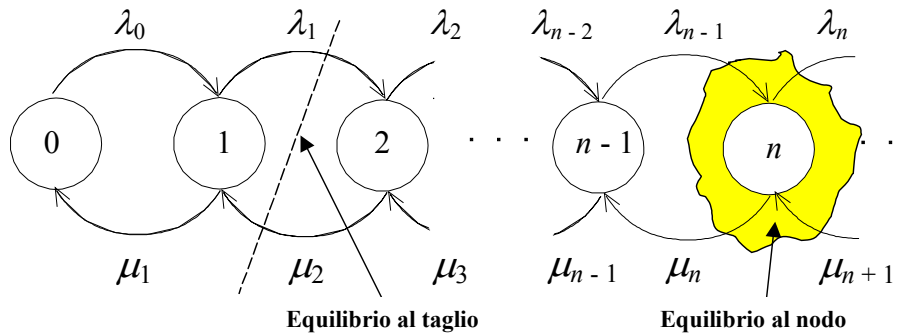


Figura 6.4: Generico processo di nascita morte.

Nell'ipotesi in cui la condizione " $\exists k$  tale che:  $\forall n \geq k, \lambda_n < \mu_n$ " (**condizione di ergodicità**) è soddisfatta, esiste un regime stazionario per la catena. A regime le probabilità  $P_n(t)$  (= probabilità di essere nello stato  $n$  al tempo  $t$ ) non dipendono dal tempo  $\Rightarrow dP_n(t)/dt = 0$  e  $P_n(t) = P_n$ . Allora valgono le seguenti equazioni di equilibrio ai nodi per caratterizzare le  $P_n$ :

$$\begin{aligned} \lambda_0 P_0 &= \mu_1 P_1 \\ (\lambda_n + \mu_n) P_n &= \lambda_{n-1} P_{n-1} + \mu_{n+1} P_{n+1}, \quad \forall n > 1 \\ \sum_{n=0}^{\infty} P_n &= 1 \quad (\text{normalizzazione}) \end{aligned}$$

La  $n$ -esima equazione può essere interpretata come **la condizione di equilibrio** tra il flusso entrante (=  $\lambda_{n-1} P_{n-1} + \mu_{n+1} P_{n+1}$ ) ed il flusso uscente (=  $\lambda_n P_n + \mu_n P_n$ ) attorno una generica superficie che circonda lo stato  $n$ . In Figura 6.4 è rappresentato l'equilibrio attorno al generico nodo  $n$ -esimo.

Analogamente è possibile risolvere le probabilità  $P_n$  facendo gli **equilibri ai tagli** ( $P_{n-1} \lambda_{n-1} = \mu_n P_n$ ) insieme alla condizione di normalizzazione. In Figura 6.4 è rappresentato l'equilibrio al taglio per  $n = 2$ .

## Sistemi M/M/1

I sistemi M/M/1 sono, come preannunciato, i sistemi a coda più semplici da studiare. Essi sono processi nascita morte  $\{N(t) \mid t \geq 0\}$  (numero di clienti nel sistema all'istante  $t$ ) in cui i tempi di interarrivo e di servizio sono distribuiti esponenzialmente, rispettivamente con tassi medi  $\lambda$  e  $\mu$ . Nella Figura 6.5 è rappresentato in forma grafica il sistema M/M/1, in cui gli archi sono etichettati con i tassi medi di transizione da uno stato all'altro.

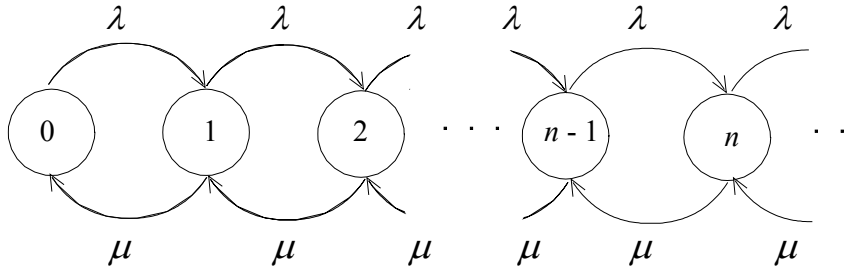


Figura 6.5: Rappresentazione in forma grafica di un sistema M/M/1.

La soluzione di questa catena è un caso particolare di quella in Figura 6.4.

Nel paragrafo precedente abbiamo visto come tale processo continuo può anche essere approssimato tramite una catena di Markov tempo-discreta  $N_k = N(k\delta)$ .  $\{N_k \mid k = 0, 1, 2\}$  o può essere risolto imponendo gli equilibri sulla catena tempo-continua.

### 6.4.3 Relazione tra carico e throughput (in sistemi singolo servente)

Per un sistema single-server il *throughput*  $\gamma$  rappresenta il traffico smaltito nell'unità di tempo. Osserviamo che il throughput sarebbe uguale al rate medio di servizio ( $\mu$ ) se la coda non fosse mai vuota, per cui si ha che:

$$\gamma = \mu(1 - p_0) \quad (6.32)$$

Nei sistemi G/G/1,  $\rho = (1 - p_0)$  è l'*intensità di traffico* che coincide con la probabilità che il servente sia occupato.

Nel caso ideale di sistema M/M/1, sostituendo a  $p_0$  il valore ottenuto precedentemente, e cioè  $1 - \rho$  ( $\rho = \lambda/\mu$ ), si ha che:

$$\gamma = \mu(1 - (1 - \rho)) = \mu\rho = \lambda$$

Per sistemi con buffer infinito, infatti, tutti i clienti che entrano nel sistema, prima o poi verranno serviti, dunque il throughput è uguale alla frequenza degli arrivi. Il *throughput normalizzato*  $\gamma/\mu$  è il *fattore di utilizzazione*  $\rho$  del servente ( $\rho < 1$  Erlang per la stabilità in presenza di un unico servente).

## 6.5 Sistemi M/G/1

I sistemi M/G/1 sono sistemi a singolo servente in cui i clienti arrivano secondo un processo di Poisson con tasso medio  $\lambda$  e i tempi di servizio seguono una distribuzione generica (non necessariamente esponenziale come accadeva nei sistemi M/M/1).

Sia  $X_i$  il tempo di servizio dell' $i$ -esimo cliente. Assumiamo che le variabili casuali ( $X_1, X_2, \dots$ ) siano identicamente distribuite e indipendenti dai tempi di interarrivo.

Indichiamo con:

$$\bar{X} = E\{X\} = \frac{1}{\mu}$$

il **tempo di servizio medio** (momento del primo ordine) e con:

$$\overline{X^2} = E\{X^2\}$$

il **momento del secondo ordine** del tempo di servizio.

Si può dimostrare che, per i sistemi M/G/1 vale la **formula di Pollaczek-Khintchine**:

$$W = \frac{\lambda \cdot \overline{X^2}}{2(1 - \rho)} \quad (6.33)$$

dove  $W$  è il tempo medio di attesa in coda, mentre risulta:

$$\rho = \frac{\lambda}{\mu} = \lambda \cdot \bar{X}$$

Il tempo medio di attesa nel sistema sarà pari alla somma del tempo medio speso nel servente più il tempo medio di attesa in coda dato dalla (6.33), dunque:

$$T = \bar{X} + \frac{\lambda \cdot \overline{X^2}}{2(1 - \rho)} \quad (6.34)$$

E' facile adesso calcolare il numero medio di clienti in attesa in coda e nel sistema, applicando il teorema di Little, si ottiene che:

$$N_Q = \frac{\lambda^2 \cdot \overline{X^2}}{2(1 - \rho)}$$
$$N = \rho + \frac{\lambda^2 \cdot \overline{X^2}}{2(1 - \rho)}$$

Calcoliamo ora il tempo medio di attesa in coda per sistemi M/M/1 come caso particolare della formula (6.33). Ricordiamo che il momento del secondo ordine (o valore quadratico medio) è dato dalla somma della varianza più il valor medio al quadrato:

$$\overline{X^2} = \sigma^2 + \bar{X}^2$$

In una distribuzione esponenziale  $\sigma^2 = 1/\mu^2$ , dove  $1/\mu$  è il valore medio, quindi:

$$\overline{X^2} = \frac{1}{\mu^2} + \frac{1}{\mu^2} = \frac{2}{\mu^2}$$



Sostituendo tale valore nella (6.33) si ha:

$$W = \frac{\rho}{\mu \cdot (1 - \rho)} = \frac{\rho}{\mu - \lambda} \quad (6.35)$$

Questo risultato indica che la formula (6.33) per i sistemi M/G/1 vale anche per i sistemi M/M/1, che, in fondo, sono un caso particolare di sistema M/G/1.

Analizziamo adesso un altro sotto caso dei sistemi M/G/1: i sistemi M/D/1. In tali sistemi il tempo di servizio è **deterministico**. Un caso pratico per questo tipo di sistemi può essere dato dalle reti in cui la lunghezza dei pacchetti è costante, quindi il tempo di servizio è costante per tutti i pacchetti. La varianza del tempo di servizio è dunque nulla ( $\sigma^2 = 0$ ) quindi:

$$\overline{X^2} = 0 + \frac{1}{\mu^2} = \frac{1}{\mu^2}$$

Dalla formula (6.33) si ottiene:

$$W = \frac{\rho}{2\mu \cdot (1 - \rho)} \quad (6.36)$$

Nel caso M/D/1, si ha il valore minimo del momento del secondo ordine, e quindi anche W, T,  $N_Q$ , e N hanno il valore minimo. In particolare, W e  $N_Q$  sono la metà dei corrispondenti valori per sistemi M/M/1 con uguale tasso medio di servizio e di arrivo.

I valori di T e N per i sistemi M/D/1 sono la metà dei corrispondenti in M/M/1 se  $\rho \approx 1$  Erlang e sono uguali ai corrispondenti M/M/1 per  $\rho$  piccolo. Ciò accade perché il tempo di servizio è circa lo stesso nei due casi e, per  $\rho$  piccolo, il tempo che incide di più è quello di servizio, mentre per  $\rho$  grande il termine più pesante è il tempo di attesa.

In genere, i valori di T e N per sistemi M/G/1 sono intermedi tra quelli di M/D/1 (che corrispondono al caso migliore) e quelli di M/M/1 (che corrispondono al caso peggiore).

Come conseguenza di quanto ricavato, osserviamo che, usare il multiplexing statistico suddividendo l'asse temporale in slots (in cui la durata dello slot coincide con il tempo di trasmissione di un pacchetto), implica il minimo tempo medio di attesa dei pacchetti in coda. Inoltre, bisogna evidenziare anche che, se per un dato sistema non è possibile conoscere il momento del primo e del secondo ordine del tempo di servizio, è giustificato l'utilizzo di un sistema M/M/1 come modello analitico, in quanto esso porta eventualmente al sovra-dimensionamento del sistema.

Dimostriamo adesso la formula di *Pollaczek-Khintchine* (PK), facendo riferimento al caso particolare della disciplina di servizio FIFO. Tale dimostrazione farà uso della definizione del **tempo residuo di servizio**.

Def:

*Si definisce **tempo residuo di servizio** relativamente all'i-esimo cliente, il tempo (rimanente) necessario affinché l'utente in servizio all'arrivo del cliente i-esimo, esaurisca il servizio stesso.*

Siano:

$W_i$  : Tempo di attesa in coda dell'i-esimo cliente.

$R_i$  : Tempo di servizio residuo visto dall'i-esimo cliente. Cioè, se nel servente è presente il cliente j-esimo quando il cliente i arriva, con  $R_i$  indichiamo il tempo rimanente affinché il cliente j completi il servizio. Se non vi sono clienti nel sistema quando i arriva (cioè il sistema è vuoto),  $R_i$  sarà zero.

$X_i$  : Tempo di servizio dell'i-esimo cliente.

$N_i$  : Numero di clienti trovati in attesa in di servizio nella coda all'arrivo dell'i-esimo cliente.

Si ha che il tempo di attesa in coda per l'i-esimo cliente è pari al tempo di servizio residuo (del cliente già nel servente quando i arriva) più la somma dei tempi di servizio degli  $N_i$  utenti in coda prima dell'arrivo di i:

$$W_i = R_i + \sum_{j=i-N_i}^{i-1} X_j$$

Essendo le variabili  $N_i, X_{i-1}, \dots, X_{i-N_i}$  indipendenti, si ha che:

$$E\{W_i\} = E\{R_i\} + E\left\{\sum_{j=i-N_i}^{i-1} E\{X_j\}\right\} = E\{R_i\} + \bar{X} \cdot E\{N_i\}$$

Facendo il limite ad ambo i membri per i che tende all'infinito si ha:

$$W = R + \frac{1}{\mu} N_Q \quad (6.37)$$

dove R è il *tempo residuo medio* ed è definito come:

$$R = \lim_{i \rightarrow \infty} E\{R_i\}$$

Usando la formula di Little per la parte di attesa, si ha che:  $N_Q = \lambda W$ , sostituendo nella (6.37) si ha:

$$W = R + \frac{1}{\mu} \cdot \lambda \cdot W \Rightarrow W \cdot (1 - \rho) = R$$

da cui:

$$W = \frac{R}{(1 - \rho)} \quad (6.38)$$

Per ottenere dunque il tempo medio di attesa in coda bisogna trovare il tempo medio residuo e sostituirlo nella (6.38). E' possibile risolvere questo problema tramite il teorema della vita residua che collega la distribuzione del tempo residuo con la distribuzione degli intertempi di arrivo e con quella di servizio. E' infatti possibile dimostrare che vale la seguente formula che fa riferimento ai valori medi:

$$R = \frac{1}{2} \cdot \lambda \cdot \overline{X^2}$$

Sostituendo dunque nella (6.38) si ha:

$$W = \frac{\lambda \cdot \overline{X^2}}{2(1-\rho)}$$

che è proprio la **formula di Pollaczzen-Khintchine(P-K)**.

Si noti che un sistema M/G/1 con  $\rho < 1$  Erlang può presentare tempi di attesa infiniti se il momento del secondo ordine tende ad infinito (es. questo vale in certe condizioni ad esempio con la distribuzione di Pareto del tempo di servizio). Quello che succede in questo caso è che una piccola quantità di utenti hanno un tempo di servizio molto lungo. Durante questo ampio intervallo di tempo, un numero molto elevato di clienti arrivano nel sistema e vengono accodati subendo dunque un elevato ritardo.

## 6.6 Sistemi a coda con priorità

Consideriamo un sistema M/G/1 in cui i clienti sono divisi in classi di priorità decrescente. Supponiamo inoltre che le priorità vengano gestite senza *preemption*. Cioè al cliente sotto servizio è permesso di completare il servizio senza interruzione anche se arriva un cliente a più alta priorità. Una coda separata è mantenuta per ogni classe di priorità. Quando un server diventa disponibile, viene servito il primo cliente in attesa nella coda non vuota a più alta priorità.

Indichiamo con:

- $\lambda_k$  : il tasso medio di arrivo degli utenti di classe k,
- $\overline{X_k} = 1/\mu_k$ : il momento del primo ordine del tempo di servizio relativo alla classe k,
- $\overline{X_k^2}$  : il momento del secondo ordine del tempo di servizio relativo alla classe k.

Calcoleremo adesso il tempo medio di attesa in coda per le varie classi di priorità.

Indichiamo con:

- $N_Q^{(k)}$  : il numero medio di utenti nella coda di priorità k,
- $W_k$  : il tempo medio di attesa nella coda con priorità k,
- $\rho_k = \lambda_k / \mu_k$ : l'utilizzazione del sistema per la priorità k,
- $R$ : il tempo residuo di servizio medio. Tale parametro non dipende dalla classe k perché stiamo supponendo che non ci sia preemption.

Per la classe di priorità più alta si ha che (dalla (6.37)):

$$W_1 = R + \frac{1}{\mu_1} N_Q^{(1)}$$

Ed usando il teorema di Little si ha:

$$W_1 = \frac{R}{(1-\rho_1)}$$

Per la seconda classe di priorità si ha:

$$W_2 = R + \frac{1}{\mu_1} N_Q^{(1)} + \frac{1}{\mu_2} N_Q^{(2)} + \frac{1}{\mu_1} \cdot \lambda_1 \cdot M_2$$

dove il quarto addendo del secondo membro rappresenta il ritardo aggiuntivo causato dai clienti con priorità più alta che arrivano quando il customer con priorità 2 è già in attesa in coda.

$$W_2 = R + \rho_1 \cdot W_1 + \rho_2 \cdot W_2 + \rho_1 \cdot W_2$$

$$W_2 = \frac{R + \rho_1 \cdot W_1}{1 - \rho_1 - \rho_2} = \frac{R}{(1 - \rho_1)(1 - \rho_1 - \rho_2)}$$

Analogamente si trova che:

$$W_k = \frac{R}{(1 - \rho_1 - \dots - \rho_{k-1})(1 - \rho_1 - \dots)} \quad (6.39)$$

Con un procedimento analogo al precedente si ottiene che:

$$R = \frac{1}{2} \cdot \lambda \cdot \overline{X^2} = \frac{1}{2} \cdot \left( \sum_{i=1}^n \lambda_i \right) \cdot \overline{X^2}$$

dove  $\overline{X^2}$  è il momento del secondo ordine mediato su tutte le classi di priorità:

$$\overline{X^2} = \frac{\lambda_1}{\sum_{i=1}^n \lambda_i} \cdot \overline{X_1^2} + \frac{\lambda_2}{\sum_{i=1}^n \lambda_i} \cdot \overline{X_2^2} + \dots + \frac{\lambda_n}{\sum_{i=1}^n \lambda_i} \cdot \overline{X_n^2}$$

Sostituendo nella (6.39) si ottiene:

$$W_2 = \frac{\sum_{i=1}^n \lambda_i \cdot \overline{X^2}}{2 \cdot (1 - \rho_1 - \dots - \rho_{k-1}) \cdot (1 - \rho_1 - \dots - \rho_k)} \quad (6.40)$$

$$T_k = \frac{1}{\mu_k} + W_k \quad (6.41)$$

Tali valori dipendono fortemente dalle distribuzioni dei tempi di servizio delle varie classi.

Si può facilmente dimostrare che il ritardo medio per cliente tende a ridursi quando si attribuisce priorità più alta ai clienti con tempi di servizio più brevi. Questo si traduce nelle reti a commutazione di pacchetto nell'attribuire priorità maggiore ai pacchetti di controllo che solitamente sono molto più brevi rispetto ai pacchetti dati.

## 6.7 Esercizi risolti sulla teoria delle code

A completamento di questo studio sulla teoria delle code vediamo due tipologie di esercizi che sono esemplificativi per l'applicazione di questi metodi analitici.

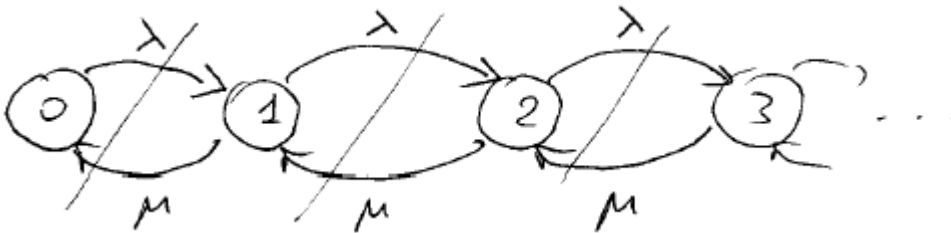
### Esercizio 1

Si consideri un multiplexer che raccoglie traffico formato da messaggi con intertempi di arrivo a distribuzione esponenziale. Il multiplexer è formato da un buffer e da una linea di trasmissione in uscita. Si consideri la seguente approssimazione: il tempo di trasmissione di un messaggio sulla linea è a distribuzione esponenziale con valore medio di  $E[x] = 10$  ms. Da misure effettuate sullo stato del buffer sappiamo che la probabilità che il buffer sia vuoto è  $P_0 = 0.8$ . Ricavare il ritardo medio di trasmissione di un messaggio.

### Soluzione

Il multiplexer è una coda con singolo servente. Il processo di arrivo è di Poisson con tasso medio  $\lambda$  da determinare. Il tempo medio di servizio è  $E[X] = 10$  ms. Il tempo di servizio è a distribuzione esponenziale con tasso medio  $\mu = 1/E[X]$ .

Il sistema si modella come una coda M/M/1:



Siccome  $P_0$  è positivo, il sistema è stabile perché è verificata la condizione di ergodicità.

Dalle equazioni ai tagli si ricava la probabilità degli stati:

$$P_0 \lambda = P_1 \mu \Rightarrow P_1 = \frac{\lambda}{\mu} P_0$$

$$P_1 \lambda = P_2 \mu \Rightarrow P_2 = \left( \frac{\lambda}{\mu} \right)^2 P_0$$

$\rho = \frac{\lambda}{\mu}$  è l'intensità di traffico offerta al multiplexer in Erlang.

$$\text{In generale } P_n = \left( \frac{\lambda}{\mu} \right)^n P_0 = \rho^n P_0$$

La probabilità di sistema vuoto si ricava con la condizione di normalizzazione:

$$P_0 = \frac{1}{1 + \sum_{n=1}^{\infty} P_n / P_0} = \frac{1}{1 + \sum_{n=1}^{\infty} \rho^n} = \frac{1}{\sum_{n=0}^{\infty} \rho^n} = 1 - \rho = 1 - \frac{\lambda}{\mu}$$

Siccome conosciamo  $P_0 = 0.8$  e  $\frac{1}{\mu} = E[X] = 10 \text{ ms}$ , da questa formula si ricava il tasso medio di arrivo  $\lambda$ :

$$P_0 = 1 - \frac{\lambda}{\mu} \Rightarrow 1 - 0.8 = \frac{\lambda}{\mu} \Rightarrow 1 - 0.8 = \lambda \cdot 10 \text{ ms}$$

$$\text{Quindi: } \lambda = \frac{1 - 0.8}{10} = 0.2 \left[ \frac{\text{messaggi}}{\text{ms}} \right]$$

Il numero medio di richieste nel sistema è  $N = \sum_{n=1}^{\infty} n \rho^n = P'(z)|_{z=1}$ , dove  $P(z)$  è la funzione generatrice del numero di messaggi nel sistema:

$$P(z) = \sum_{n=0}^{\infty} z^n (1 - \rho) \rho^n = \frac{1 - \rho}{1 - \rho \cdot z}$$

$$P'(z) = (1 - \rho) \cdot \frac{d}{dz} (1 - \rho \cdot z)^{-1} = (1 - \rho) \cdot (1 - \rho \cdot z)^{-2} \cdot (-\rho) = \frac{\rho(1 - \rho)}{(1 - \rho \cdot z)^2}$$

$$P'(z)|_{z=1} = \frac{\rho(1 - \rho)}{(1 - \rho)^2} = \frac{\rho}{1 - \rho} = N \Rightarrow N = \frac{0.2}{0.8} = 0.25 \text{ messaggi}$$

Il ritardo medio di messaggio è  $T = \frac{N}{\lambda}$ , in base al teorema di Little.

$$\text{Quindi } T = 0.25 \text{ messaggi} \cdot \frac{1}{0.02 \frac{\text{ms}}{\text{messaggi}}} = 12.5 \text{ ms} = \begin{matrix} 10 \text{ ms (tempo medio di servizio)} + \\ + 2.5 \text{ ms (tempo medio di attesa in coda)} \end{matrix}$$

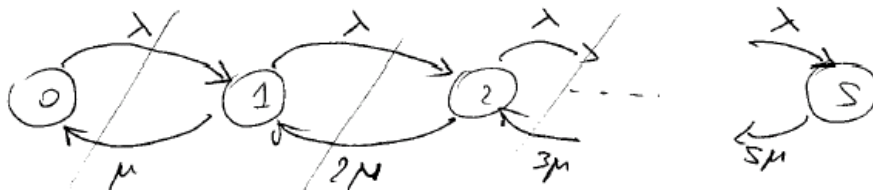
## Esercizio 2

*Si consideri un centralino telefonico che raccoglie le chiamate generate all'interno di una grande azienda in cui si hanno 1000 utenze telefoniche ciascuna generante un traffico di Poisson di 30 mErlang. Dimensionare il numero di linee telefoniche in uscita al centralino per collegarsi alla rete pubblica in modo da garantire una probabilità di blocco delle chiamate minore o uguale a 3% (si risolva formalmente il sistema in base al modello, ma si faccia uso della tabella allegata per trovare il risultato numerico). Cosa succede al numero di linee da prevedere in uscita per avere un blocco minore o uguale a 3% se il numero di utenti aumenta a 1300? Si confronti anche l'incremento percentuale di traffico offerto  $\Delta\rho\%$  con l'incremento percentuale di linee  $\Delta S\%$  che ne risulta.*

## Soluzione

Visto che si tratta di 1000 utenti ciascuno generante un traffico di Poisson di 30 mErlang, si fa lo studio per numero infinito di utenti. Trattandosi di traffico telefonico, sappiamo che il modello per la durata di ogni chiamata è a distribuzione esponenziale con durata media di 3 minuti.

Per studiare il blocco nel sistema, applichiamo un modello M/M/S/S con S da determinare in modo da soddisfare i requisiti di blocco. Il modello è:



dove  $\lambda$  è il tasso di arrivo totale degli utenti, che si calcola così:

- 1) Ogni utente contribuisce un tasso di arrivo pari a  $\frac{30 \cdot 10^{-3} \text{ Erlang}}{3 \text{ min}} = 10^{-2} \frac{\text{chiamate}}{\text{min}}$
- 2) Il tasso totale è la somma dei tassi di utente:  $\lambda = 1000 \cdot 10^{-2} \frac{\text{chiamate}}{\text{min}} = 10 \frac{\text{chiamate}}{\text{min}}$

Inoltre:

$$\frac{1}{\mu} = 3 \text{ min}$$

La distribuzione di probabilità degli stati si determina scrivendo gli equilibri ai tagli:

$$P_0 \lambda = P_1 \mu \Rightarrow P_1 = \frac{\lambda}{\mu} P_0$$

$$P_0 \lambda = P_2 \cdot 2\mu \Rightarrow P_2 = \frac{\lambda}{2\mu} \cdot \frac{\lambda}{\mu} P_0$$

$$\rho = \frac{\lambda}{\mu} = 1000 \cdot 30 \cdot 10^{-3} = 30 \text{ Erlang}$$

(è l'intensità di traffico *offerta* al sistema)

$$\text{In generale si ha: } P_n = \frac{1}{n!} \left( \frac{\lambda}{\mu} \right)^n P_0 = \frac{\rho^n}{n!} P_0$$

Ricaviamo  $P_0$  con la condizione di normalizzazione:

$$P_0 = \frac{1}{1 + \sum_{n=1}^S P_n / P_0} = \frac{1}{\sum_{n=0}^S \frac{\rho^n}{n!}}$$

non conoscendo  $S$  non possiamo calcolare  $P_0$ .

Nessuna nuova chiamata è accettata quando il sistema ha tutti e  $S$  i server occupati. Pertanto la probabilità di blocco è la probabilità di avere il sistema nello stato  $S$ :

$$P_B \equiv P_S = \frac{\rho^S}{S! \sum_{n=0}^S \frac{\rho^n}{n!}}$$

( FORMULA ERLANG-B )

In questa formula imponiamo  $P_S \leq 3\%$  e conosciamo  $\rho = 30$  Erlang, possiamo quindi ricavare  $S$ . Per via numerica ciò è complesso e si fa uso della tabella ERLANG-B riprodotta qui di seguito. Nella tabella prendiamo la colonna per  $P_B = 3\%$  e la scorriamo fino a prendere il valore di traffico immediatamente superiore ai 30 Erlang per fare un

dimensionamento cautelativo di  $S$ . Troviamo il valore di 30.53 Erlang a cui corrispondono  $S = 38$  serventi.

Se il numero di utenti incrementa a 1300, il carico di traffico *offerto* al centralino è  $\rho = 1300 \cdot 30 \cdot 10^{-3}$  Erlang = 39 Erlang. Per dimensionare  $S$  usiamo di nuovo la tabella e troviamo che in corrispondenza a 39.06 Erlang si devono usare  $S = 47$  serventi. L'incremento percentuale di serventi è ottenuto così:

$$38 + 38 \frac{\Delta S\%}{100} = 47 \Rightarrow \Delta S\% = \left( \frac{47 - 38}{38} \right) \cdot 100 = 23.68\%$$

L'incremento percentuale di carico offerto al sistema è:

$$38 \text{ Erlang} + 38 \text{ Erlang} \cdot \frac{\Delta S\%}{100} = 39 \text{ Erlang} \Rightarrow \Delta S\% = \left( \frac{39 - 30}{30} \right) \cdot 100 = 30\%$$

Si noti l'effetto di moltiplicazione statistica del traffico che fa sì che  $\Delta S\% < \Delta \rho\%$  pur mantenendo il requisito di  $P_B \leq 3\%$ .



## Tabella Erlang *B*

S	1.0%	1.2%	1.5%	2%	3%	5%	7%	10%
1	.0101	.0121	.0152	.0204	.0309	.0526	.0753	.111
2	.153	.168	.190	.223	.282	.381	.470	.595
3	.455	.489	.535	.602	.715	.899	1.06	1.27
4	.869	.922	.992	1.09	1.26	1.52	1.75	2.05
5	1.36	1.43	1.52	1.66	1.88	2.22	2.50	2.88
6	1.91	2.00	2.11	2.28	2.54	2.96	3.30	3.76
7	2.50	2.60	2.74	2.94	3.25	3.74	4.14	4.67
8	3.13	3.25	3.40	3.63	3.99	4.54	5.00	5.60
9	3.78	3.92	4.09	4.34	4.75	5.37	5.88	6.55
10	4.46	4.61	4.81	5.08	5.53	6.22	6.78	7.51
11	5.16	5.32	5.54	5.84	6.33	7.08	7.69	8.49
12	5.88	6.05	6.29	6.61	7.14	7.95	8.61	9.47
13	6.61	6.80	7.05	7.40	7.97	8.83	9.54	10.5
14	7.35	7.56	7.82	8.20	8.80	9.73	10.5	11.5
15	8.11	8.33	8.61	9.01	9.65	10.6	11.4	12.5
16	8.88	9.11	9.41	9.83	10.5	11.5	12.4	13.5
17	9.65	9.89	10.2	10.7	11.4	12.5	13.4	14.5
18	10.4	10.7	11.0	11.5	12.2	13.4	14.3	15.5
19	11.2	11.5	11.8	12.3	13.1	14.3	15.3	16.6
20	12.0	12.3	12.7	13.2	14.0	15.2	16.3	17.6
21	12.8	13.1	13.5	14.0	14.9	16.2	17.3	18.7
22	13.7	14.0	14.3	14.9	15.8	17.1	18.2	19.7
23	14.5	14.8	15.2	15.8	16.7	18.1	19.2	20.7
24	15.3	15.6	16.0	16.6	17.6	19.0	20.2	21.8
25	16.1	16.5	16.9	17.5	18.5	20.0	21.2	22.8
26	17.0	17.3	17.8	18.4	19.4	20.9	22.2	23.9
27	17.8	18.2	18.6	19.3	20.3	21.9	23.2	24.9
28	18.6	19.0	19.5	20.2	21.2	22.9	24.2	26.0
29	19.5	19.9	20.4	21.0	22.1	23.8	25.2	27.1
30	20.3	20.7	21.2	21.9	23.1	24.8	26.2	28.1
31	21.2	21.6	22.1	22.8	24.0	25.8	27.2	29.2
32	22.0	22.5	23.0	23.7	24.9	26.7	28.2	30.2
33	22.9	23.3	23.9	24.6	25.8	27.7	29.3	31.3
34	23.8	24.2	24.8	25.5	26.8	28.7	30.3	32.4
35	24.6	25.1	25.6	26.4	27.7	29.7	31.3	33.4
36	25.5	26.0	26.5	27.3	28.6	30.7	32.3	34.5
37	26.4	26.8	27.4	28.3	29.6	31.6	33.3	35.6
38	27.3	27.7	28.3	29.2	30.5	32.6	34.4	36.6
39	28.1	28.6	29.2	30.1	31.5	33.6	35.4	37.7
40	29.0	29.5	30.1	31.0	32.4	34.6	36.4	38.8
41	29.9	30.4	31.0	31.9	33.4	35.6	37.4	39.9
42	30.8	31.3	31.9	32.8	34.3	36.6	38.4	40.9
43	31.7	32.2	32.8	33.8	35.3	37.6	39.5	42.0
44	32.5	33.1	33.7	34.7	36.2	38.6	40.5	43.1
45	33.4	34.0	34.6	35.6	37.2	39.6	41.5	44.2
46	34.3	34.9	35.6	36.5	38.1	40.5	42.6	45.2
47	35.2	35.8	36.5	37.5	39.1	41.5	43.6	46.3
48	36.1	36.7	37.4	38.4	40.0	42.5	44.6	47.4
49	37.0	37.6	38.3	39.3	41.0	43.5	45.7	48.5
50	37.9	38.5	39.2	40.3	41.9	44.5	46.7	49.6

## 6.8 Teoria del traffico

In questo paragrafo concentreremo le nostre attenzioni sul dimensionamento e sull'analisi delle reti di telecomunicazione.

### 6.8.1 Intensità di traffico

L'intensità di traffico si definisce come la quantità media di unità di lavoro che viene offerta al sistema (o viene smaltita dal sistema) nell'unità di tempo. Pur essendo un numero puro, l'unità di misura attribuita convenzionalmente a tale grandezza è l'**Erlang** e la lettera usata per indicarla è (comunemente) la lettera  $A$  o  $\rho$ .

Viene definito dunque il **traffico offerto** (*utilizzazione del sistema*):

$$A_0 = \frac{\lambda}{\mu}$$

dove  $\lambda$  è il tasso medio totale degli arrivi e  $1/\mu$  è il tempo medio di servizio.

Si definisce **traffico smaltito**:

$$A_s = \frac{\gamma}{\mu}$$

dove  $\gamma$  è il tasso medio totale di richieste smaltite (= throughput) e  $1/\mu$  è il tempo medio di servizio.

Nel caso di reti a commutazione di circuito, la grandezza che indica quanto si impegnano le risorse della rete è:

$$\left[ \frac{\text{chiamate}}{\text{tempo}} \times \text{tempo di chiamata} \right]$$

Nel caso di reti a commutazione di pacchetto, si ha:

$$\left[ \frac{\text{pacchetti}}{\text{tempo}} \times \text{tempo di trasmissione} \right]$$

L'intensità di traffico dà anche:

- Il numero medio di sorgenti contemporaneamente attive (**traffico offerto**), cioè dà una misura del carico che bisogna prevedere per dimensionare il sistema;
- Il numero medio di risorse (serventi) contemporaneamente occupate (**traffico smaltito**), cioè una misura della capacità di smaltimento di traffico del sistema.

Si definisce, **traffico perso**:

$$A_p = \frac{\lambda \cdot P_B}{\mu}$$

In equilibrio statistico si ha che  $A_0 = A_S + A_P$ .

Il fattore di utilizzazione  $\rho$  indica l'intensità di traffico smaltita dal singolo servente (in un sistema con N serventi):

$$\rho = \frac{\lambda}{N \cdot \mu} = \frac{A_S}{N} < 1 \quad (6.42)$$

In condizione di stabilità  $\rho$  deve essere minore di 1 Erlang, dunque  $A_S$  deve essere minore di N. Dalla (6.42) si ricava che  $A_S = \rho N$ .

Per questo motivo, a volte con l'unità Erlang si indica la frazione di tempo per la quale una linea è impiegata, moltiplicata per il numero di linee in uscita al sistema.

### 6.8.2 Dimensionamento ed analisi delle reti di telecomunicazione

I passi da effettuare per realizzare e gestire una rete di telecomunicazione sono:

1. Dimensionare gli apparati all'interno della rete (in fase di realizzazione);
2. Gestire la rete di telecomunicazione, cioè decidere se accettare o meno le chiamate di richiesta di trasmissione. La decisione è presa cercando di garantire la *Qualità di Servizio* (QoS), note le caratteristiche delle sorgenti di traffico.

La QoS si caratterizza con parametri, quali:

- **Loss probability** (probabilità di perdita).
- **Delay** (ritardo).
- **Delay Jitter** (variazione del ritardo intorno la media).

Per quanto riguarda la probabilità di perdita, essa è particolarmente importante per traffici tempo reale in cui le *Unità Informative* (UI) hanno una certa CDT (*Cell Delay Tolerance*), mentre per traffici non tempo reale la *loss probability* è di scarsa rilevanza se non per mostrare i pacchetti scartati a causa di buffer saturi. La trattazione che segue farà riferimento a reti a pacchetto (di tipo ATM).

Le fasi della progettazione di una rete possono essere così classificate:

1. Caratterizzazione delle sorgenti.
2. Modellizzazione delle sorgenti.
3. Modellizzazione della rete.
4. Valutazione delle prestazioni.

Nel seguito ci focalizzeremo sulla caratterizzazione e modellizzazione delle sorgenti di traffico, perché questo è un aspetto fondamentale per dimensionare le reti di telecomunicazione.

### 6.8.3 Caratterizzazione e modellizzazione delle sorgenti di traffico

Caratterizzare una sorgente di traffico significa capirne statisticamente il comportamento. Vi sono 4 famiglie di sorgenti di traffico:

- *Sorgenti audio.*
- *Sorgenti video.*
- *Sorgenti dati.*
- *Sorgenti multimediali.* Esse sono un aggregato delle sorgenti precedentemente elencate, le quali risultano correlate fra loro. Ad esempio il movimento delle labbra di un parlatore è fortemente correlato con i dati audio, relativi alla voce dello speaker stesso.

Una prima classificazione delle sorgenti di traffico può essere effettuata in base alla modalità con cui i dati vengono emessi dal codificatore di sorgente. In particolare distinguiamo *Constant Bit Rate* (CBR) e *Variable Bit Rate* (VBR); nel primo caso la sorgente emette a bit-rate costante, nel secondo a bit-rate variabile. La trasmissione digitale PCM è di tipo CBR perché codifica la voce con bit/rate costante (64 Kbit/s). Essa è però poco efficiente in quanto trasmette anche quando si ha silenzio. Trasmettere con bit-rate costante è spesso poco conveniente, per cui si preferisce usare usualmente la tecnica VBR.

Caratterizziamo di seguito due delle sorgenti di traffico più comuni.

#### *Traffico vocale*

Il traffico vocale è real-time (= con requisiti stringenti sul ritardo di trasmissione) ed è prodotto campionando ad intervalli regolari, e poi comprimendo, il segnale proveniente da una sorgente vocale. Il parlato durante una conversazione non è continuo. Per questo si è pensato ad un modello che caratterizza tale traffico con una catena di Markov tempo discreto a due stati: ON e OFF. Come si può vedere nella Figura 6.6, una sorgente voce si può trovare alternativamente nello stato ON e nello stato OFF, nel primo caso c'è una generazione di traffico con bit-rate costante  $S$  bit/s, mentre la sorgente non produce traffico nel secondo caso.

Supponendo di campionare lo stato della sorgente voce ad intervalli regolari (slot), si ha che i tempi di permanenza in ogni stato sono geometricamente distribuiti con valore medio in slot pari a  $1/\xi$  per lo stato OFF e  $1/\theta$  per lo stato ON.

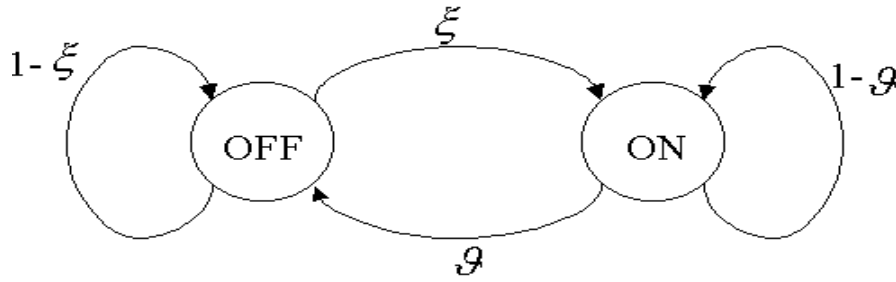


Figura 6.6: Modello di catena di Markov tempo-discreto per una sorgente voce.

Definiti  $k$  e  $h$  come:  $k = 1/\xi$  e  $h = 1/\theta$ , si può scrivere il fattore di attività di una sorgente voce (= probabilità che la sorgente voce sia nello stato ON) come segue:

$$\psi_s = \frac{h}{h + k} \quad (6.43)$$

#### Traffico dati di tipo Web browsing

Per il traffico di tipo Web browsing si fa riferimento ad un modello semplificato al livello di sessione. Infatti, una sorgente dati si può trovare in due fasi: *Packet Call*, durante la quale viene prodotto traffico (= datagrammi); e *Reading Time*, in cui non vengono generati dati (l'utente ha una pausa di navigazione perché legge le pagine che gli sono arrivate).

Il tempo di permanenza nello stato di Reading Time tra una Packet Call e l'altra è esponenzialmente distribuito con valor medio  $m_{Dpc}$ . Durante una Packet Call viene generato un numero di datagrammi che è geometricamente distribuito con valor medio  $m_{Nd}$ ; tra un datagramma e l'altro il tempo di interarrivo è esponenzialmente distribuito con valor medio  $m_{Dd}$ . Quindi la durata di una Packet Call dipende dal numero di datagrammi che vengono prodotti al suo interno e dai tempi di interarrivo dei datagrammi.

Il fattore di attività di una sorgente dati di tipo WWW può essere valutato come la probabilità che la sorgente si trovi nello stato di Packet Call:

$$\psi_w = \frac{m_{Nd} \cdot m_{Dd}}{m_{Nd} \cdot m_{Dd} + m_{Dpc}} \quad (6.44)$$

Il grado di burstiness della sorgente di traffico WWW è:

$$Bn_w = \frac{1}{\psi_w} \quad (6.45)$$

Ogni datagramma generato durante le Packet Call ha una lunghezza in bytes  $l_{w\_byte} = \lfloor x \rfloor$ , dove  $x$  è una variabile random con probabilità troncata di Pareto con parametri  $\gamma = 1.1$ ,  $k = 81.5$  bytes e  $m = 65$  Kbytes (max lunghezza di un datagram IP). La funzione di densità di probabilità troncata di Pareto è:

$$pdf(x) = \frac{\gamma \cdot k^\gamma}{x^{\gamma+1}} \cdot [u(x - k) - u(x - m)] + \left(\frac{k}{m}\right)^\gamma \delta(x - m) \quad (6.46)$$

dove  $u(\cdot)$  è la funzione di gradino unitario e  $\delta(\cdot)$  è la funzione delta di Dirac.

## Riferimenti bibliografici

- [1] A. S. Tanenbaum, "Reti di Calcolatori".
- [2] S. Gai, "Reti locali, dal cablaggio all'internetworking", Scuola Superiore G. Reiss Romoli (CD-ROM)
- [3] J. F. Hayes, "Modeling and Analysis of Computer Communication Networks". Plenum Press. New York, 1986.
- [4] L. Kleinrock, "Queuing Systems", Vol. I, J. Wiley & Sons, N.Y., 1976.
- [5] P. T. Brady, "A Model for On-Off Speech Patterns in Two-Way Conversation", *Bell Syst. Tech. Journal*, Vol. 48, No. 7, pp. 2445-2472, Sept. 1969.
- [6] ETSI, Selection Procedures for the Choice of Radio Transmission Technologies of the UMTS (UMTS 30.03 Version 3.1.0); *European Telecommunications Standards Institute*, Sophia-Antipolis, Cedex, France, Nov. 1997.
- [7] J. Kurose, "Internet e Reti", McGraw Hill.