

MAC (Medium Access Control): sottolivello del livello data link

Problema delle reti **broadcast**: a quale elaboratore (**stazione**) assegnare il mezzo trasmissivo in caso di più richieste simultanee.

E' compito dei protocolli del **sottolivello MAC** decidere chi deve essere il prossimo a trasmettere su un canale broadcast.

Usati soprattutto nelle reti broadcast (tipo le LAN e le connessioni WAN basate su satelliti) i protocolli MAC possono assegnare i canali attraverso un'allocazione:

statica - l'allocazione viene decisa in anticipo;

dinamica - l'allocazione viene stabilita in base alle esigenze del momento.

Allocazione statica: *suddivisione della banda del canale fra gli N utenti* (a ciascuno utente viene assegnata una frazione della banda totale).

Esempio: *nell'FDM a ciascun utente si assegna una banda di frequenze diversa da quelle assegnate agli altri* (tecnica accettabile se il numero di utenti non varia rapidamente e se tutti trasmettono con data rate più o meno costante)

Svantaggi:

- *spreco di banda quando uno o più utenti non trasmettono;
- *la natura ***bursty*** del traffico non consente un'adeguata gestione dei picchi.

L'allocazione dinamica, che cerca invece di adeguarsi alle esigenze trasmissive, si basa su un modello:

a stazioni: N stazioni indipendenti generano frame da trasmettere. Una stazione che ha generato un frame si blocca finché non viene trasmesso;

a singolo canale: tutte le stazioni (con pari priorità) possono trasmettere e ricevere frame da un singolo canale;

con collisioni: se due frame vengono trasmessi contemporaneamente

- * il segnale risultante è rovinato (si ha una collisione e tutte le stazioni possono rilevare la collisione);

- * i frame devono essere ritrasmessi;

Rispetto al **tempo** si può avere:

continuous time: la trasmissione di un frame può iniziare in un qualunque istante;

slotted time: il tempo è diviso in intervalli discreti (**slot**), e la trasmissione può iniziare solo all'inizio di uno slot. In uno slot si possono avere zero (slot vuoto), uno (slot con frame) o più frame (collisione).

Ascolto del canale

carrier sense (tipico delle LAN): le stazioni, prima di trasmettere, ascoltano il canale; la trasmissione ha inizio solo se il canale non è occupato;

no carrier sense (tipico dei canali via satellite, nei quali vi è un elevato round trip time): le stazioni trasmettono comunque (non ascoltano); solo dopo si preoccupano di rilevare eventuali collisioni.

Protocollo *ALOHA*: nato negli anni '70 per collegare, via radio al suolo, gli elaboratori sparsi nelle isole Hawaii (*Pure Aloha* e *Slotted Aloha*).

Pure Aloha: le stazioni trasmettono quando vogliono; durante la trasmissione ascoltano il canale e confrontano ciò che ricevono con ciò che hanno spedito.

In caso di collisione, lasciano passare un intervallo di tempo casuale e ritrasmettono il frame.

Analisi delle prestazioni del protocollo Aloha

Detto *Frame time* il tempo necessario alla trasmissione di un frame di lunghezza fissa, ed ipotizzando una generazione media di frame con una distribuzione di Poisson di S frame per *frame time*, è ovvio che:

se $S \geq 1$ si hanno quasi sempre collisioni.

mentre per $0 < S < 1$: il numero di collisioni diviene più o meno accettabile.

Conseguentemente, per i frame che complessivamente bisogna trasmettere (quelli nuovi più quelli da ritrasmettere a causa delle collisioni precedenti) è possibile ipotizzare una distribuzione di Poisson di G frame per *frame time*.

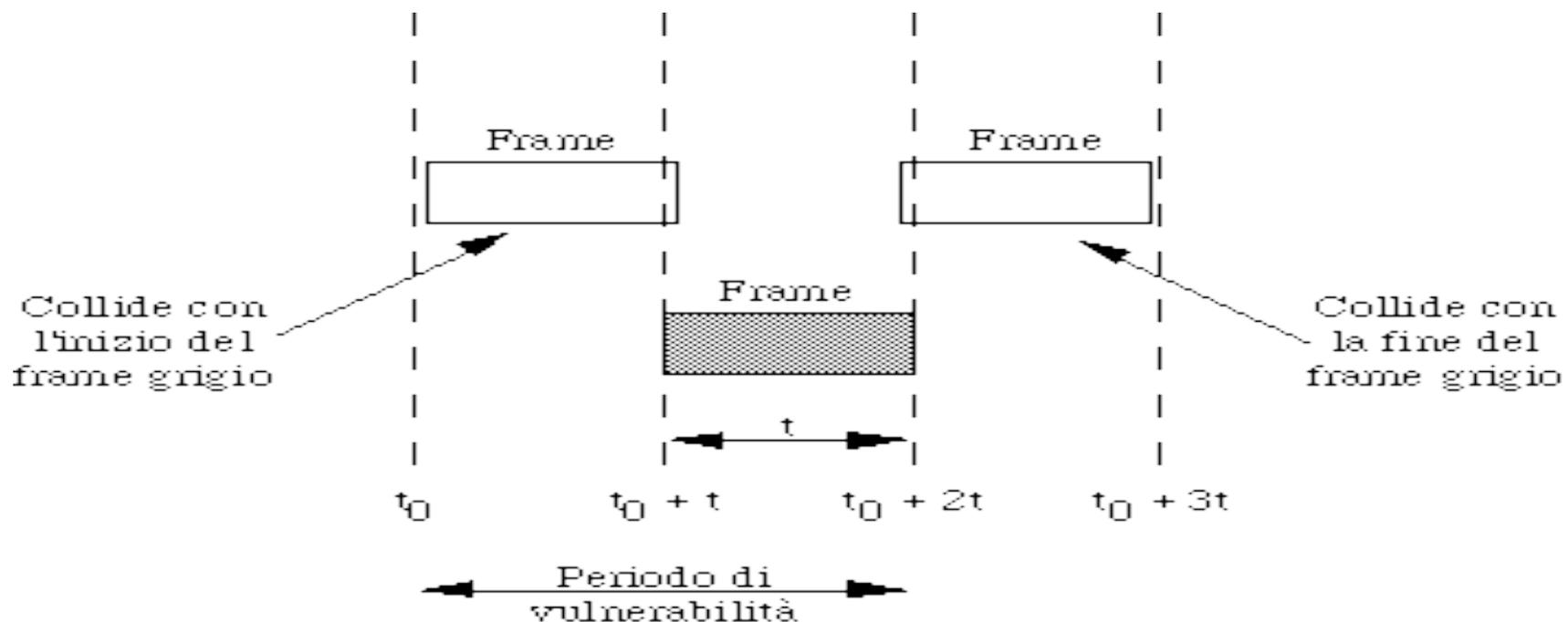
A basso carico G è circa uguale ad S mentre ad alto carico (aumentando le collisioni) G sarà maggiore di S .

Se G è il numero di frame da trasmettere per frame time, la **quantità di pacchetti che arriva a destinazione** è data da G per la probabilità che vi siano zero collisioni **Throughput** = $G * P(0)$

Poiché nel caso di distribuzione di Poisson la probabilità $P(k)$ è data dalla formula:

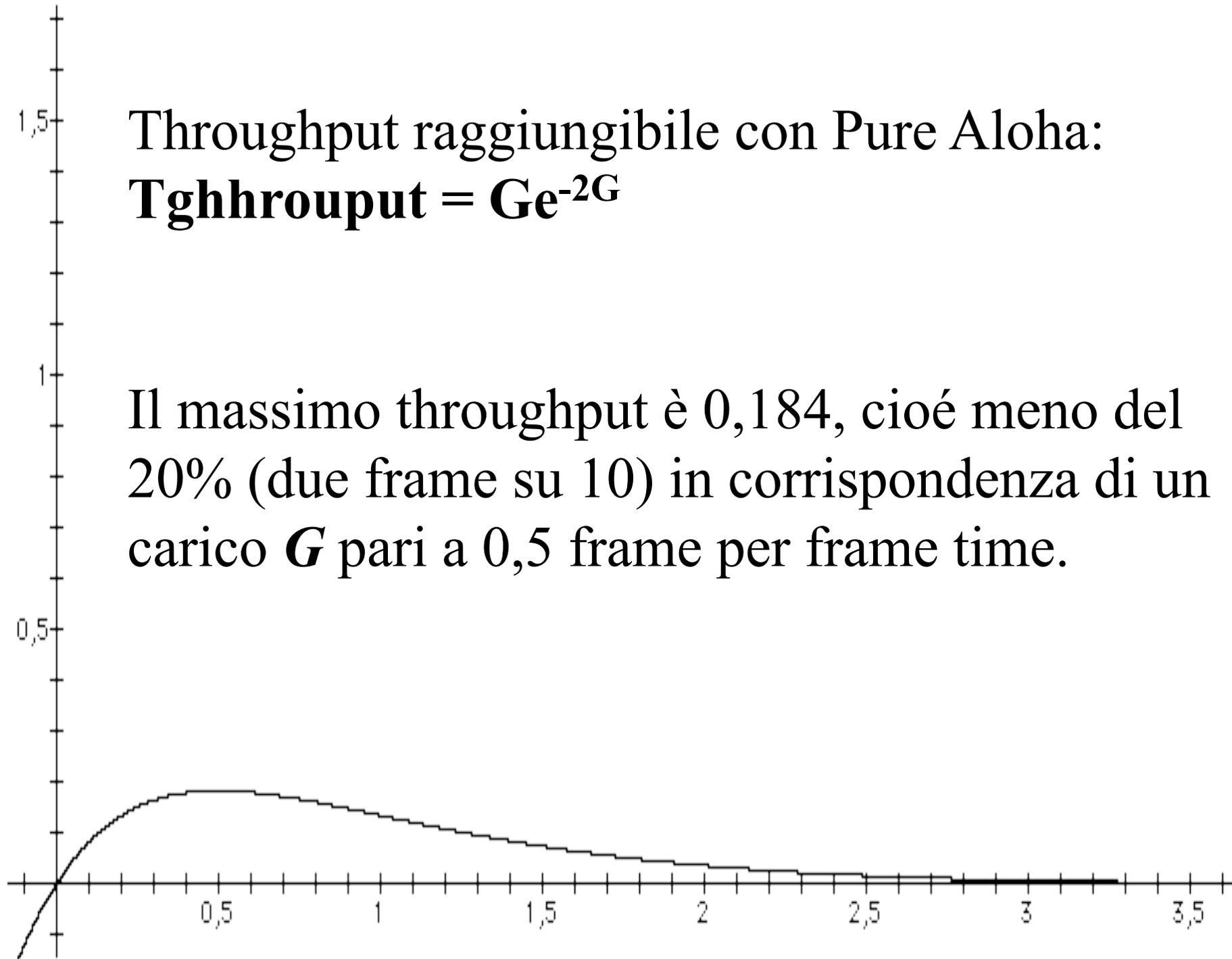
$$P(k) = \frac{G^k e^{-G}}{k!} \Rightarrow P(0) = e^{-G}.$$

Essendo il **periodo di vulnerabilità** (tempo a rischio di collisioni) di un frame 2 volte il frame time si ottiene: **$P(0) = e^{-2G}$**



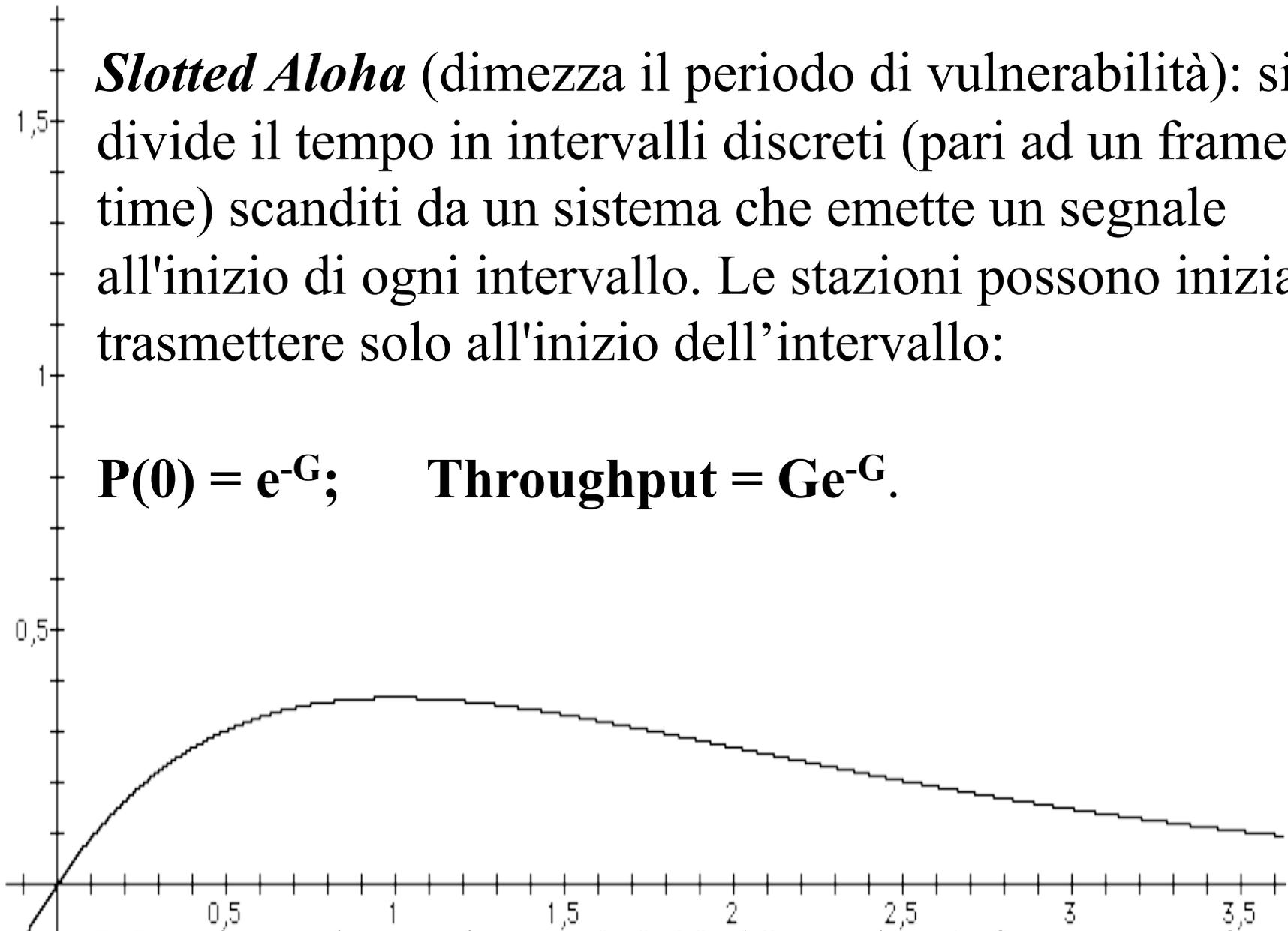
Throughput raggiungibile con Pure Aloha:
Throughput = $G e^{-2G}$

Il massimo throughput è 0,184, cioè meno del 20% (due frame su 10) in corrispondenza di un carico G pari a 0,5 frame per frame time.



Slotted Aloha (dimezza il periodo di vulnerabilità): si divide il tempo in intervalli discreti (pari ad un frame time) scanditi da un sistema che emette un segnale all'inizio di ogni intervallo. Le stazioni possono iniziare a trasmettere solo all'inizio dell'intervallo:

$$P(0) = e^{-G}; \quad \text{Throughput} = Ge^{-G}.$$



Massimo throughput 0,368 (G pari a 1 frame per frame time).

Protocolli **CSMA** (*Carrier Sense Multiple Access*)

Protocolli **carrier sense**: le stazioni ascoltano il canale prima di iniziare a trasmettere.

Protocolli **carrier sense**:

1-persistent

Non-persistent

P-persistent

Protocolli *carrier sense 1-persistent*:

Quando una stazione deve trasmettere, ascolta il canale:

**se è occupato, aspetta finché si libera e quindi trasmette*

**se è libero, trasmette (con probabilità 1, da cui il nome).*

Se avviene una collisione, la stazione aspetta un tempo random e riprova tutto da capo.

Si ha una collisione se:

* una stazione **A** trasmette, e prima che il suo segnale arrivi a **B** anche **B** inizia a trasmettere;

* **A** e **B** ascoltano contemporaneamente durante la trasmissione di **C**, e non appena quest'ultima termina iniziano entrambe a trasmettere

Più alto è il tempo di propagazione fra **A** e **B**, più alta è la probabilità di collisioni.

Protocolli *carrier sense Nonpersistent*

Quando una stazione deve trasmettere, ascolta il canale:

- *se è occupato, attende che si liberi, quindi, aspetta un tempo random e ripete tutto il procedimento da capo;

- *se è libero trasmette.

Intuitivamente, ci si aspettano meno collisioni ma maggiori ritardi prima di riuscire a trasmettere un frame.

Protocolli *carrier sense P-persistent* (si adottano per canali slotted)

Quando una stazione deve trasmettere, ascolta il canale:

*se è occupato, aspetta il next slot e ricomincia da capo; * se è libero:

- con probabilità p trasmette subito;

- con probabilità $1 - p$ aspetta il prossimo slot e riapplica tale procedimento;

In caso di collisione la stazione aspetta un tempo random e ricomincia da capo.

Intuitivamente, al diminuire di p ci si aspettano crescenti ritardi prima di riuscire a trasmettere un frame ed una progressiva diminuzione delle collisioni.

Protocolli *CSMA/CD* (*CSMA* with *C*ollision *D*etection)

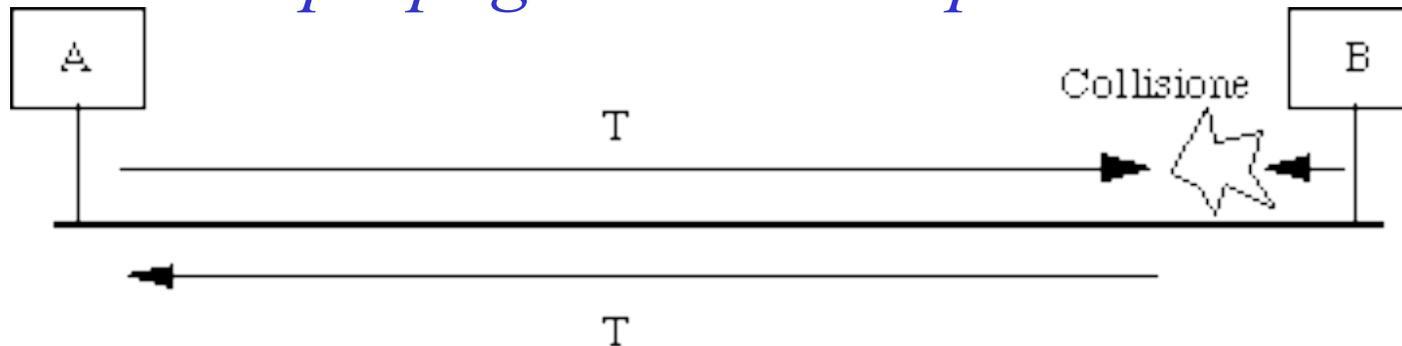
Le stazioni, che rilevano una collisione, interrompono istantaneamente la loro trasmissione.

Una stazione per rilevare le collisioni ascolta il canale durante le proprie trasmissioni.

Se la potenza del segnale ricevuto (processo analogico) è superiore a quella trasmessa si è verificata una collisione.

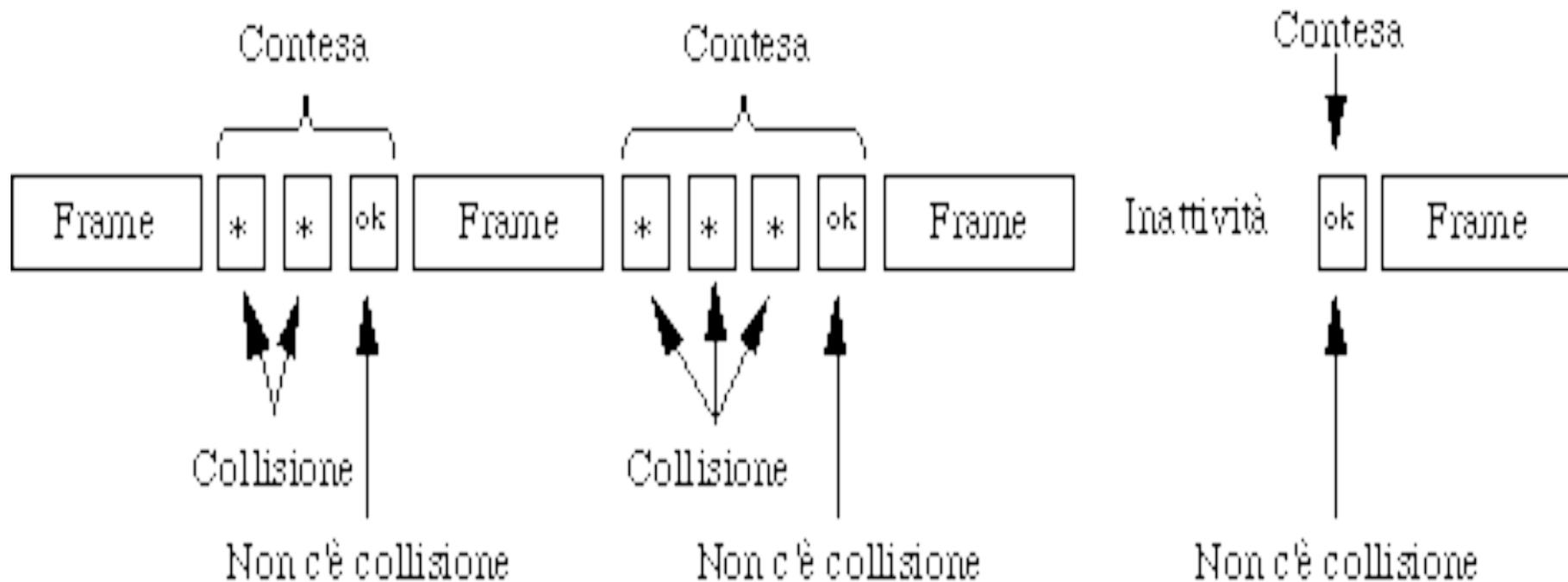
Quando si verifica una collisione, la stazione ritenta la trasmissione dopo un intervallo di tempo casuale.

- Ipotesi :1) *A e B sono le due estremità della rete;*
2) *T è il tempo impiegato dal segnale per propagarsi da un capo all'altro della rete.*



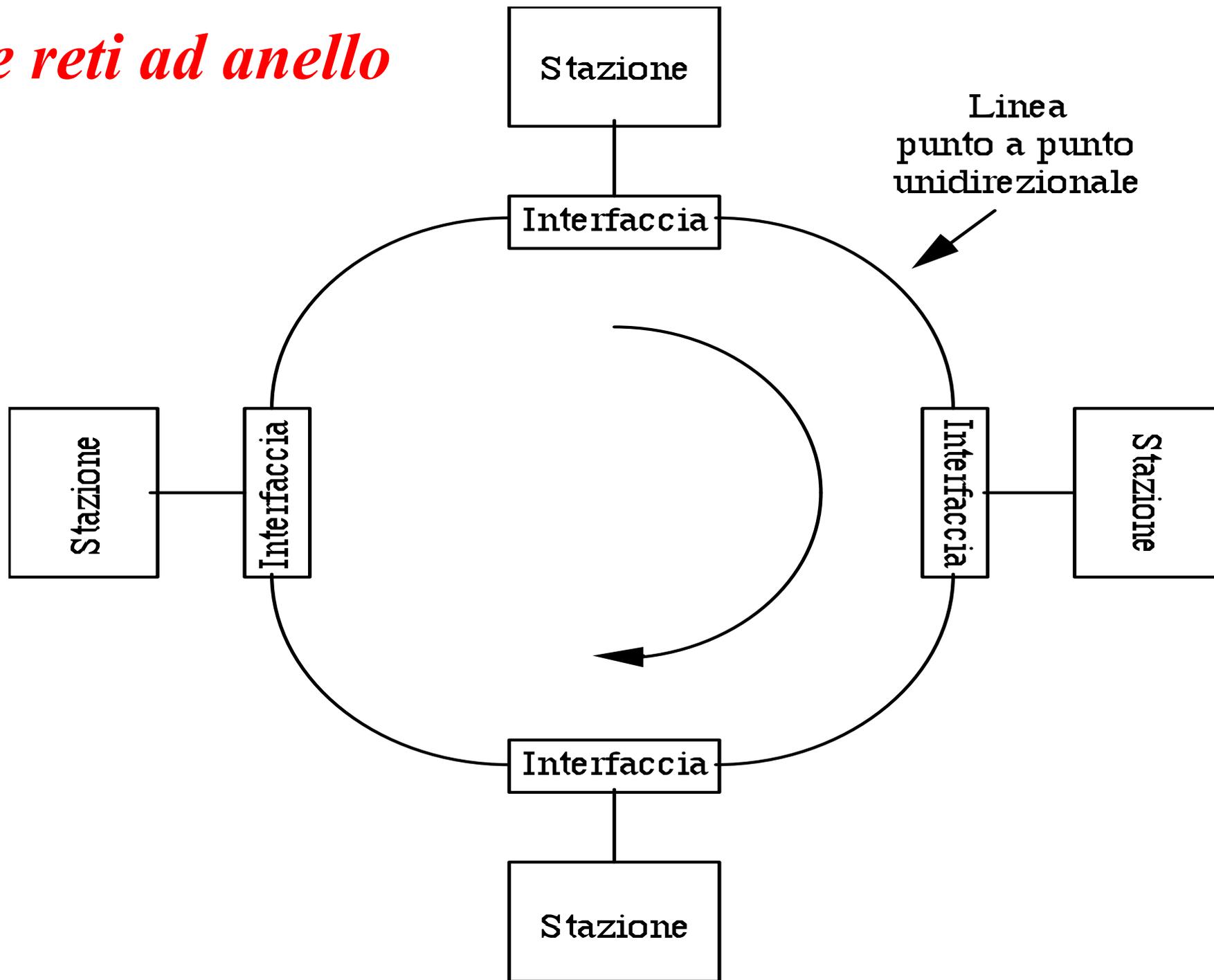
- *A inizia a trasmettere al tempo t_0 ;
- *B avverte la trasmissione solo al tempo $t_0 + T$;
- *se B inizia a trasmettere un attimo prima di $t_0 + T$;
- *A rileva che anche B sta trasmettendo (collisione) solo nell'istante $t_0 + 2T$.

Modello concettuale: alternanza di periodi di *contesa*, *trasmissione* e di *inattività* (il periodo di contesa è modellato come uno Slotted Aloha con slot di durata $2T$):



Per un cavo di 1 km T vale circa $5 \mu\text{s}$

Le reti ad anello

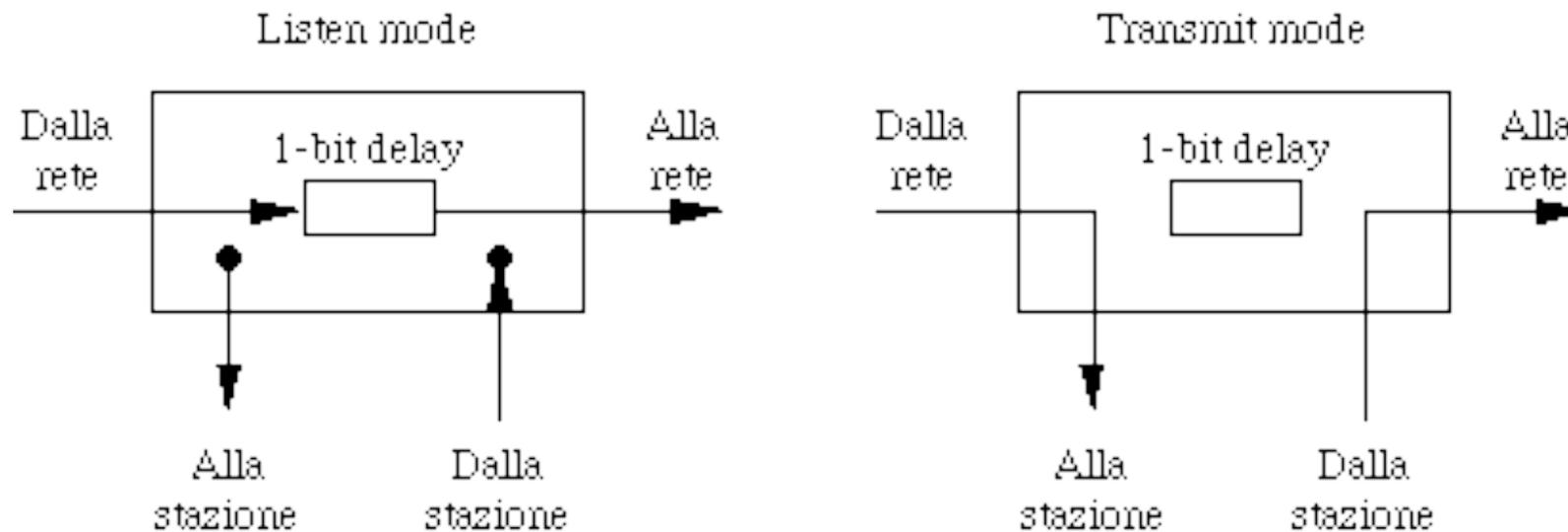


Le reti ad anello:

- * non si basano su un mezzo trasmissivo broadcast;*
- * manca la componente analogica (inutile perchè le collisioni non possono verificarsi);*
- * l'anello è intrinsecamente equo.*

Ogni bit che arriva all'interfaccia è copiato in un buffer interno, poi rigenerato e ritrasmesso sul ring (può essere modificato prima di essere ritrasmesso).

Due diverse modalità operative:



listen mode: *i bit in ingresso vengono copiati nel buffer interno e quindi ritrasmessi con un ritardo di un bit (1-bit delay).*

transmit mode (l'anello è aperto): *i bit in arrivo vengono rimossi ed una nuova copia di bit viene trasmessa sull'anello.*

Token (gettone): speciale configurazione binaria trasmessa lungo l'anello in assenza di trasmissioni.

Una stazione che vuole trasmettere:

- *aspetta che arrivi il token (listen mode);*
- *lo rimuove dal ring (listen mode);*
- *trasmette i dati (transmit mode);*
- *rigenera il token (transmit mode);*
- *passa in listen mode.*

Poiché c'è un solo token, questo meccanismo risolve senza conflitti il problema dell'accesso al mezzo.

Time Holding Token (THT): *tempo massimo entro il quale, una volta preso il token, si deve completare la trasmissione (schedulazione round-robin delle trasmissioni).*

Perché il token sia completamente distribuito lungo l'anello, la sua dimensione non può essere arbitraria.

Diversa è la situazione per la dimensione del frame che, immesso nell'anello dal mittente e rimosso dal destinatario (anello aperto), non presenta particolari limiti;

Problema: ***qual'è la lunghezza di un bit ?***

Velocità di propagazione nel rame $\sim 205 \text{ m}/\mu\text{s}$.

Poiché 1 Mbps genera un bit ogni μs , ed in $1 \mu\text{s}$ il bit percorre circa 205 metri, per contenere 10 bit l'anello deve essere lungo almeno 2 km.

Sul ring trovano quindi posto:

x bit sull'anello, in funzione della sua lunghezza totale;

y bit nei buffer delle interfacce delle y stazioni.

$x + y >$ del numero di bit del token.

Nella stazione **monitor** dell'anello si può ricavare un ritardo addizionale aggiungendo appositi buffer.

Reti ad anello

Quando tutte le stazioni hanno qualcosa da trasmettere, l'efficienza si avvicina al 100%.

Quando non c'è traffico, una stazione per trasmettere deve attendere un pò più che in CSMA/CD (mediamente, per ricevere il token, dovrà attendere il tempo di attraversamento di mezzo anello).

Gli standard IEEE per le LAN, indicati come ***IEEE 802***, includono:

Specifiche generali del progetto (802.1);

Logical Link Control, LLC (802.2);

CSMA/CD (802.3);

Token bus (802.4);

Token ring (802.5);

DQDB (802.6);

.....

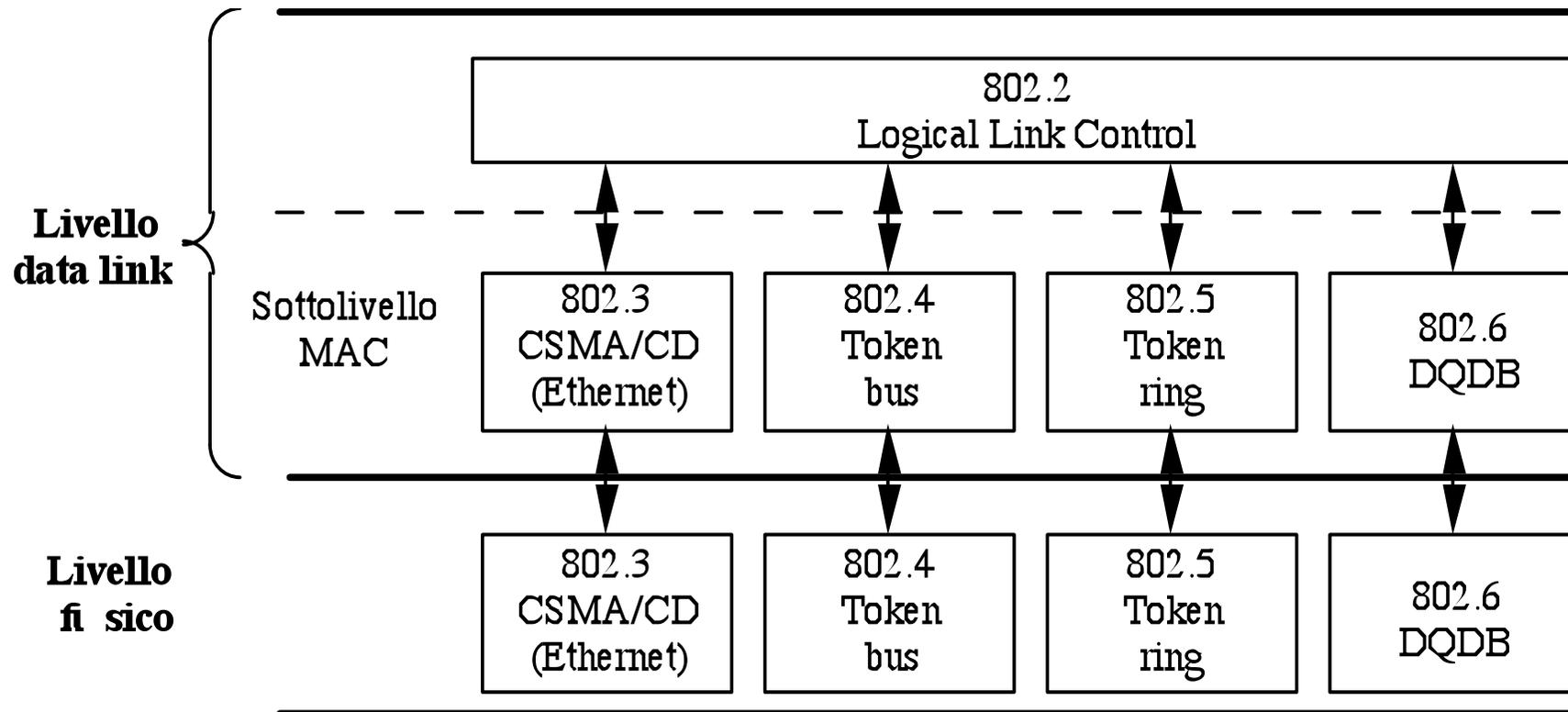
Wireless Networks (802.11);

.....

Bluetooth (802.15);

.....

I vari standard differiscono a livello fisico e nel sottolivello MAC, ma sono compatibili a livello data link.



LLC, che costituisce la parte superiore del livello data link, viene usata da tutti i protocolli standard del sottolivello MAC.

IEEE 802.3: evoluzione dello standard ***Ethernet*** (proposto da Xerox, Dec e Intel) è un protocollo ***CSMA/CD, 1-persistent, 10 Mbps.***

Cablaggio ***10Base5 (Thick ethernet)***

Cablaggio ***10Base2 (Thin ethernet)***

Cablaggio ***10BaseT (doppino telefonico)***

IEEE 802.3 ed ***Ethernet*** presentano alcune differenze, ma sono largamente compatibili

Cablaggio *10Base5* (*Thick Ethernet*)

Realizzato con cavo coassiale (detto *cavo giallo* per il colore della guaina esterna) ufficialmente noto come *cablaggio 10Base5*:

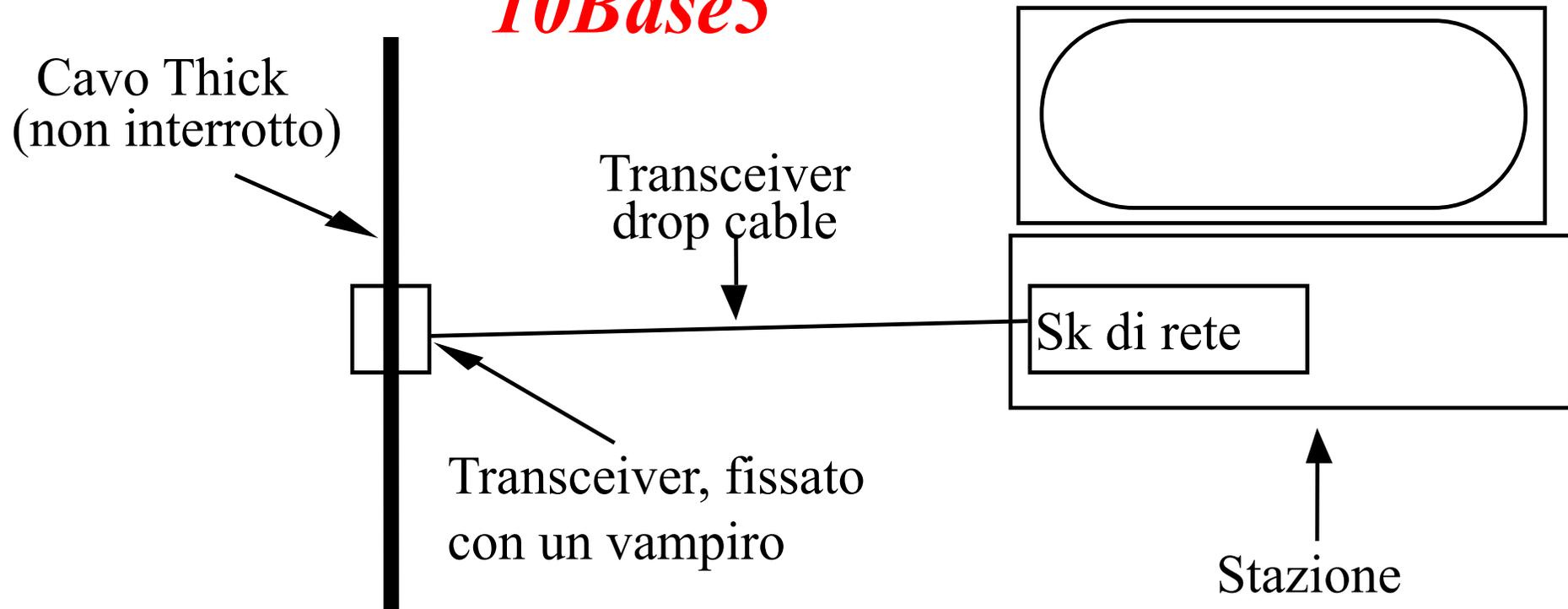
10 Mbps;

*Base*band signaling;

500 metri di lunghezza massima.

Massimo 100 macchine su un segmento.

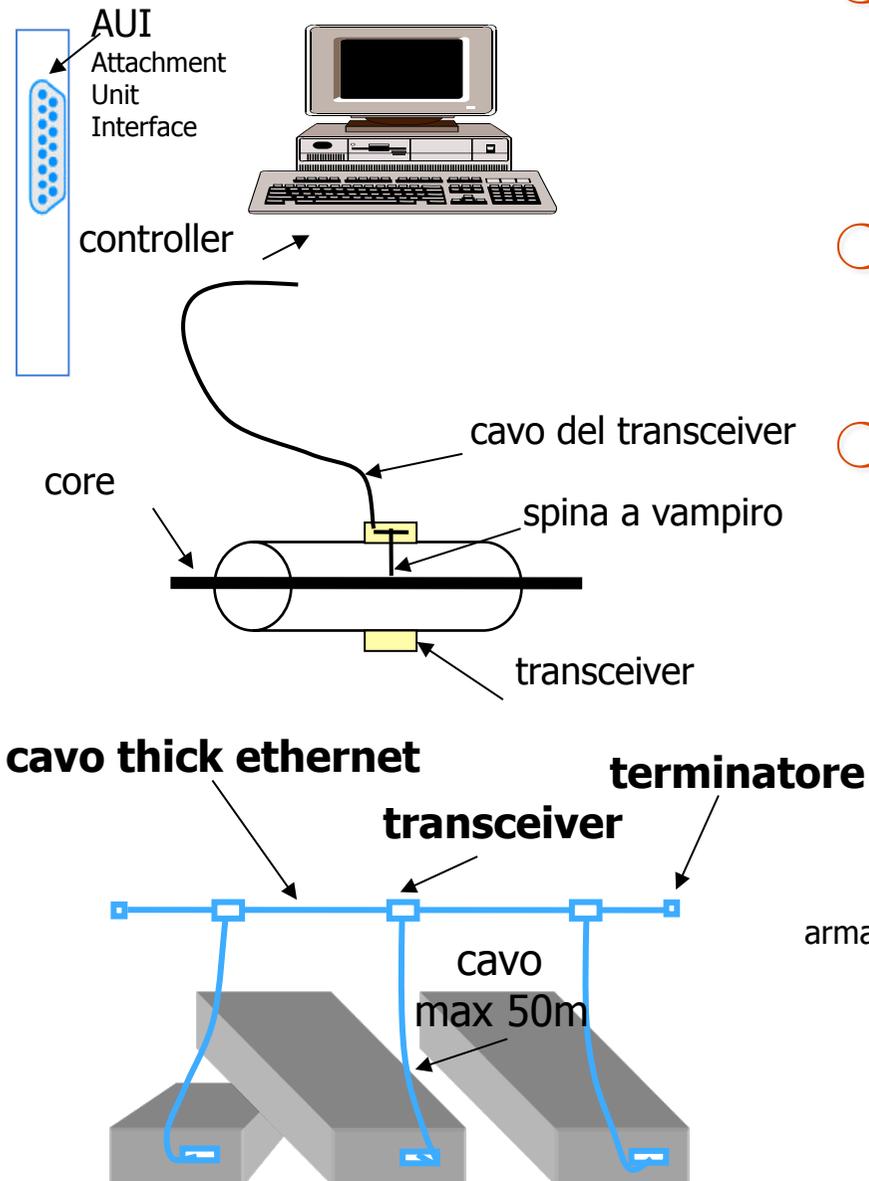
10Base5



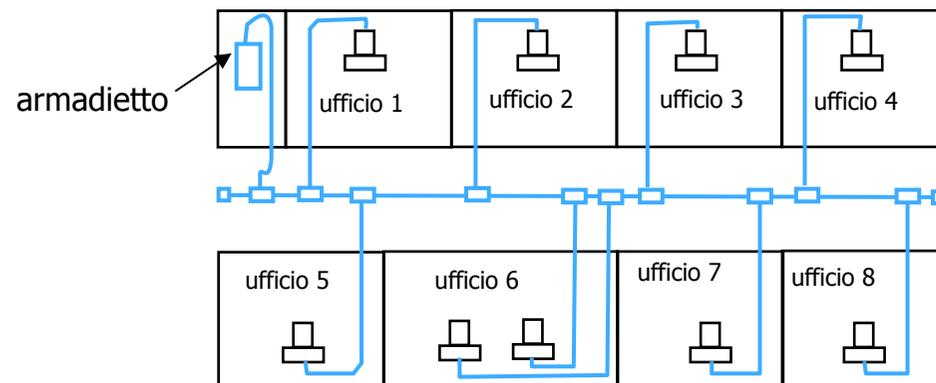
Drop cable (pochi metri) collega la Sk di rete al **transceiver** che a **vampiro** si aggancia (senza interromperlo) al cavo **thick**.

Il **transceiver** (che contiene la **circuiteria analogica per l'ascolto del canale e la rilevazione delle collisioni**) in caso di collisione informa l'interfaccia ed invia sulla rete un **jamming sequence** (una stringa di 32 bit, utilizzata per segnalare alle stazioni connesse di scartare quanto già ricevuto)

10Base5



- **Thick Ethernet:** Cavo giallo con tacche ogni 2.5 m a indicare i punti di aggancio delle spine
- **Transceiver:** circuito elettronico che rileva la portante e le collisioni
- **Cavo del transceiver:** 5 doppini schermati (*dati in ingresso, dati in uscita, controllo in e out, alimentazione*)



Cablaggio 10Base2 (Thin ethernet)

Realizzato con un cavo coassiale più sottile (si piega più facilmente) è ufficialmente noto come:

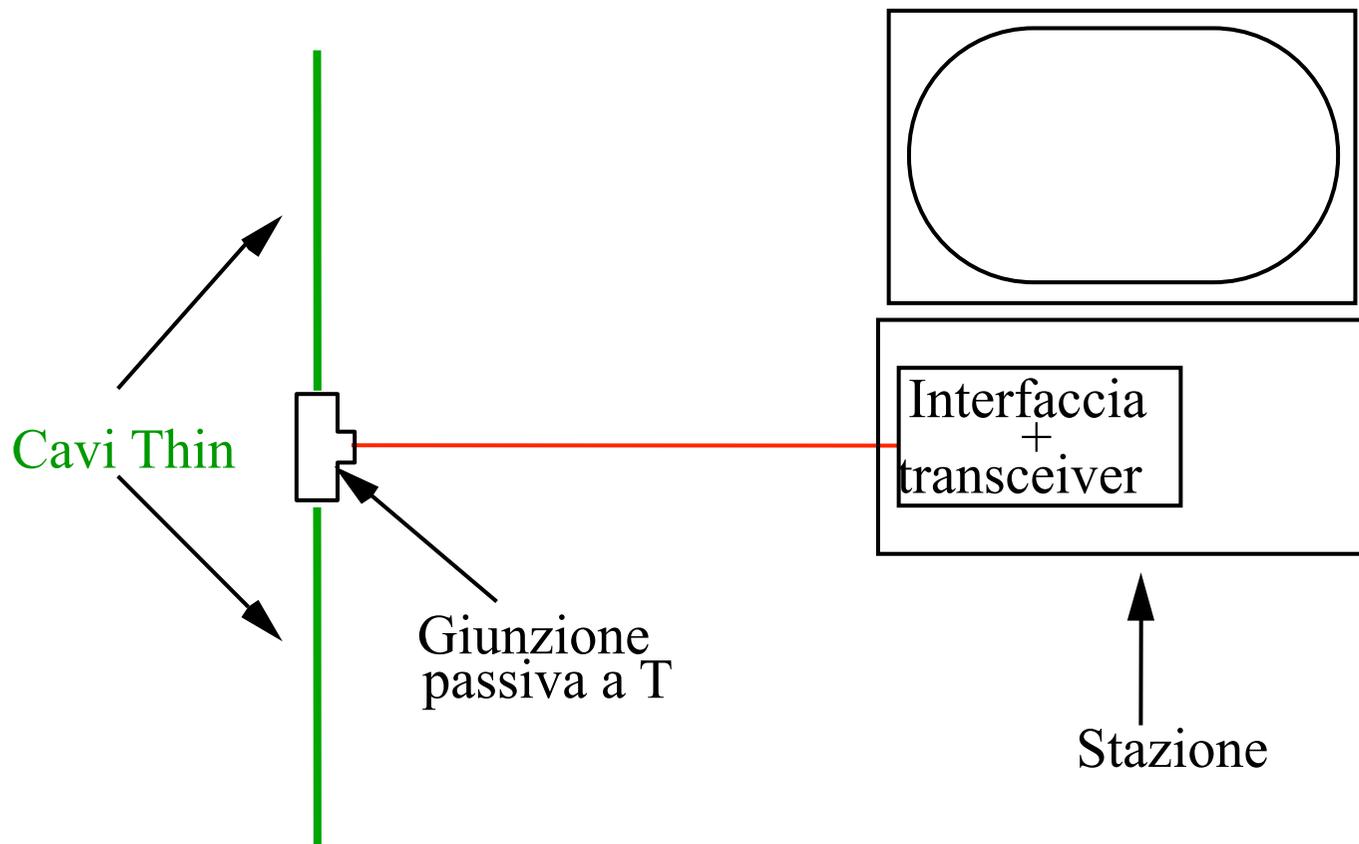
10 Mbps;

*Base*band signaling;

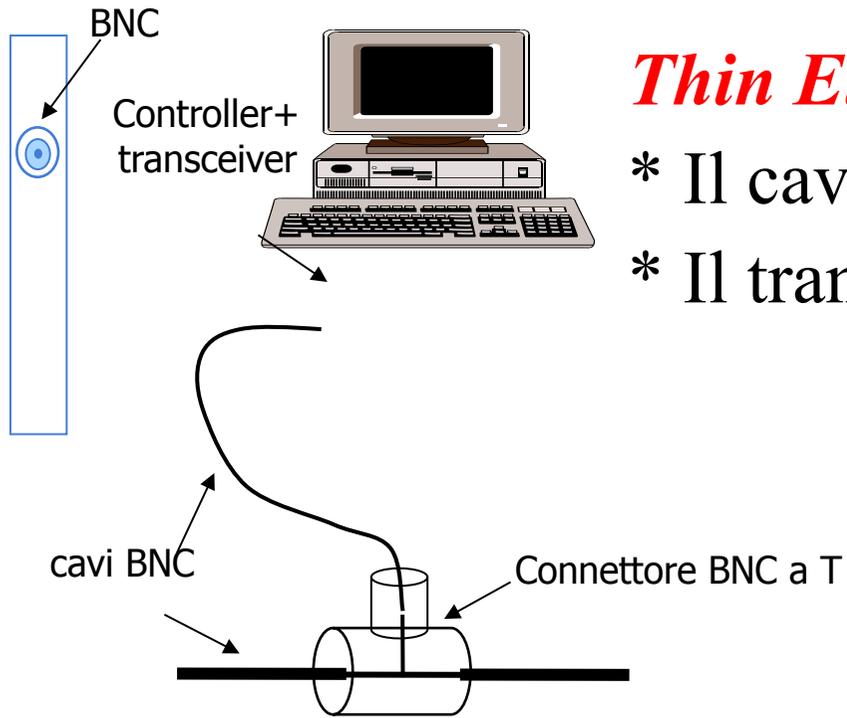
200 mt per un singolo segmento.

Possono essere installate sino a 30 macchine su un segmento.

10Base2: Di norma l'interfaccia di rete contiene anche il transceiver. Le stazioni sono collegate in cascata (*daisy-chain*), ed il collegamento alla rete avviene con una *giunzione a T*, alla quale sono collegati il **cavo** che porta alla stazione e **due cavi thin**, che costituiscono una porzione del segmento.

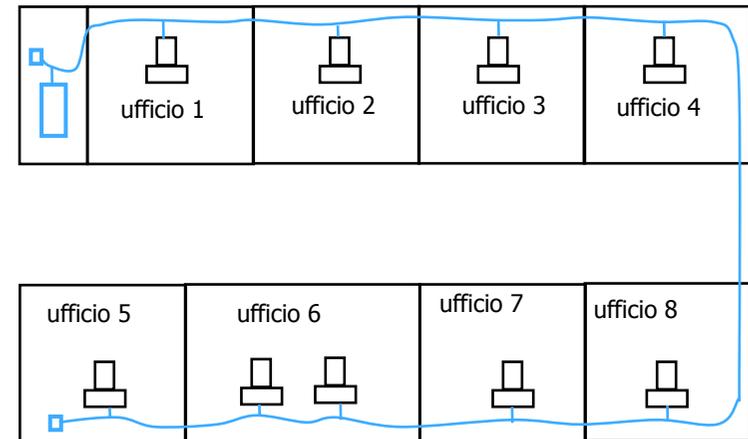
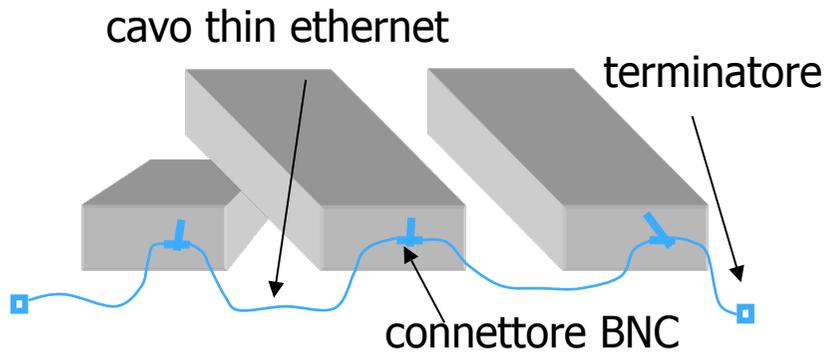


10Base2



Thin Ethernet

- * Il cavo è flessibile
- * Il transceiver è in genere sul controller





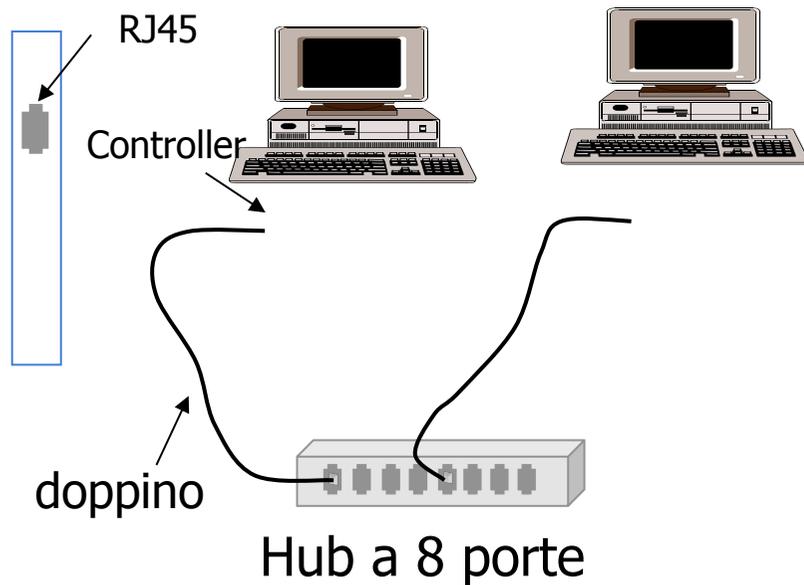
Cablaggio 10BaseT (doppino telefonico)

Lo standard per il doppino telefonico, noto come ***10BaseT*** (***T***wisted), prevede il collegamento fra una sola coppia di stazioni.

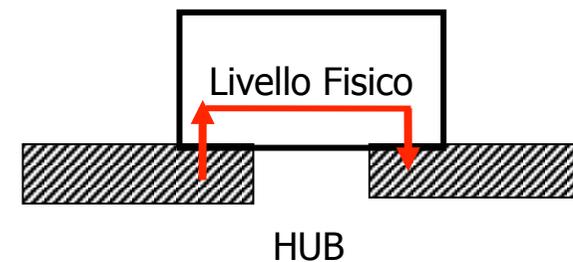
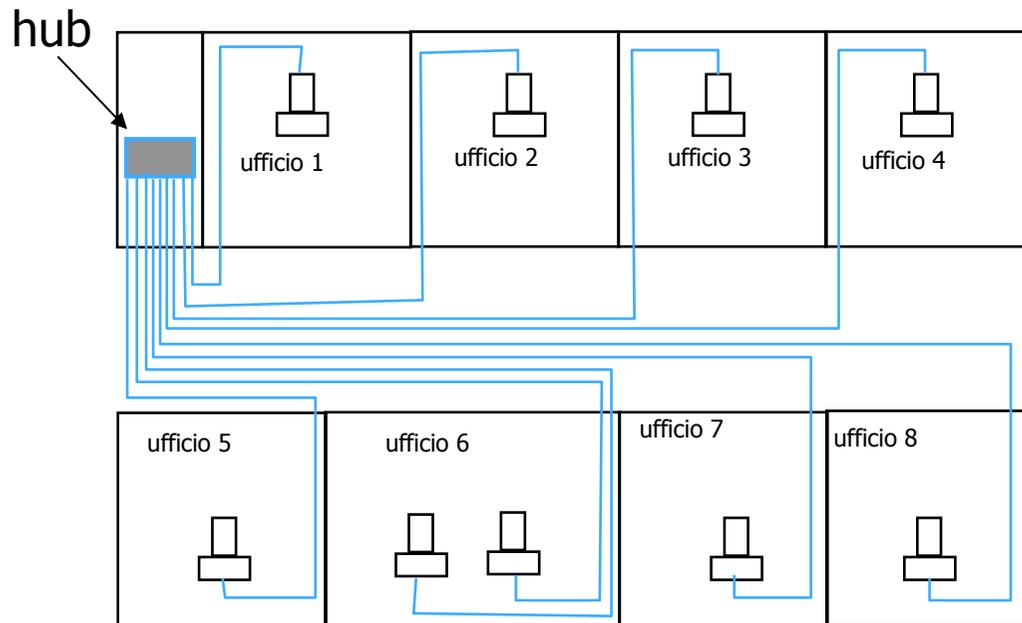
La lunghezza massima è 100 metri per cavi UTP cat. 5 (maggiore se il doppino è di classe superiore).

Per connettere più di due stazioni serve o un ripetitore multiporta (HUB) o uno SWITCH

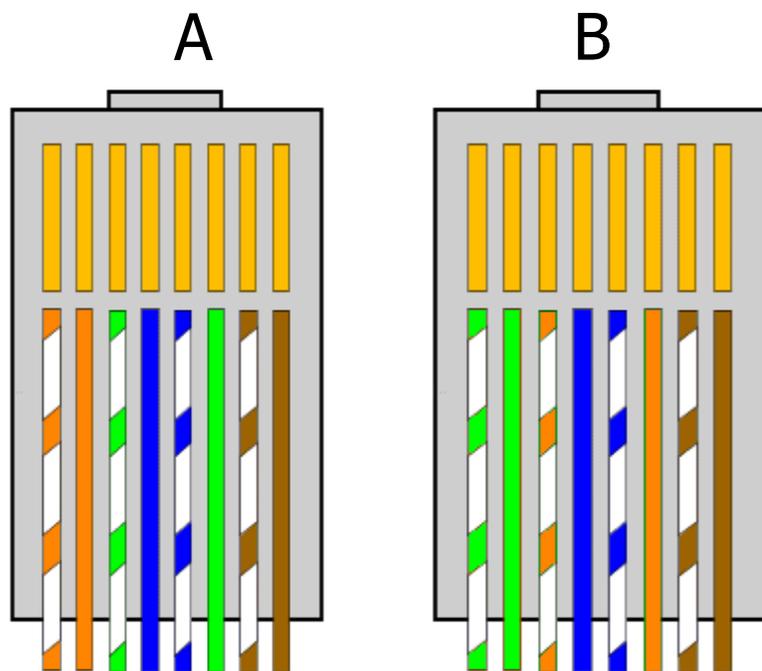
10BaseT



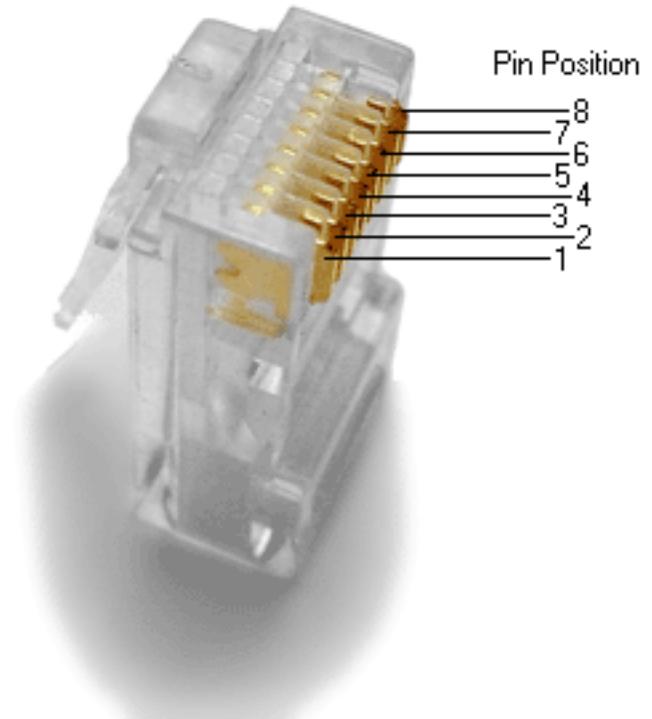
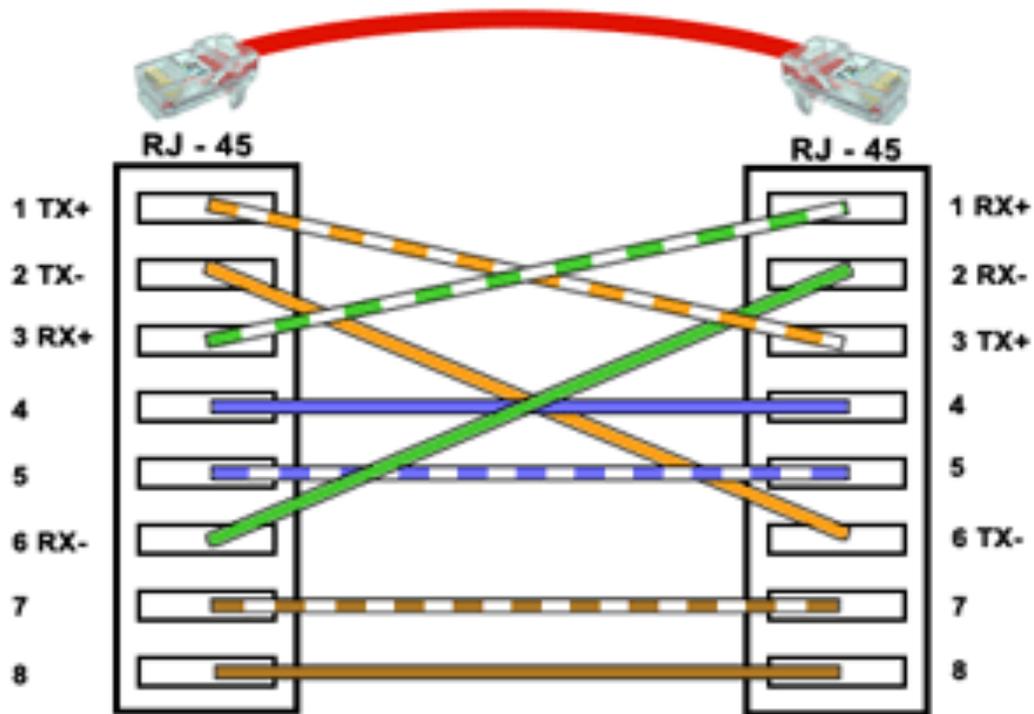
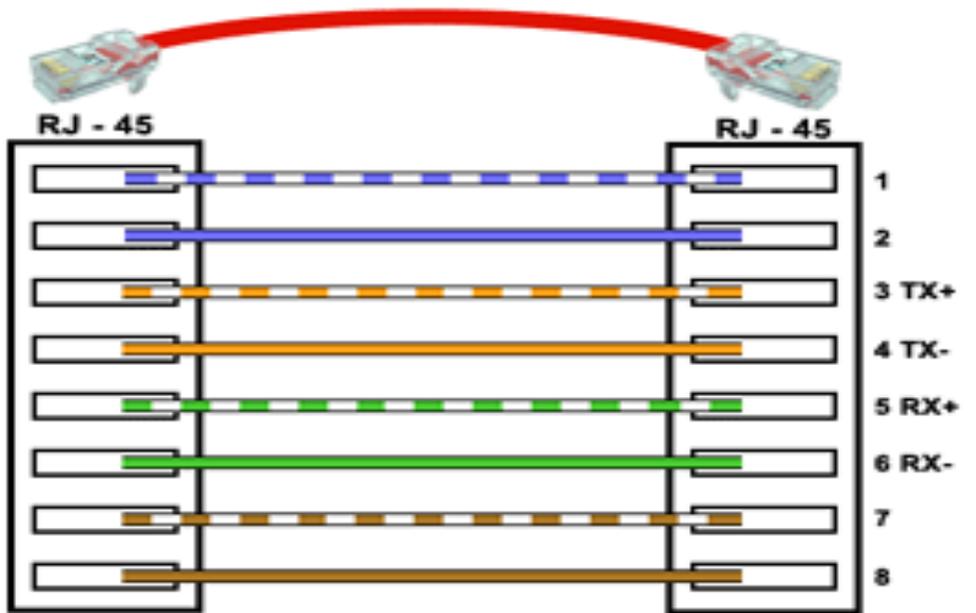
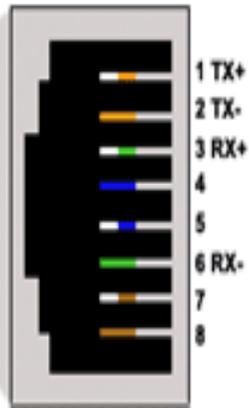
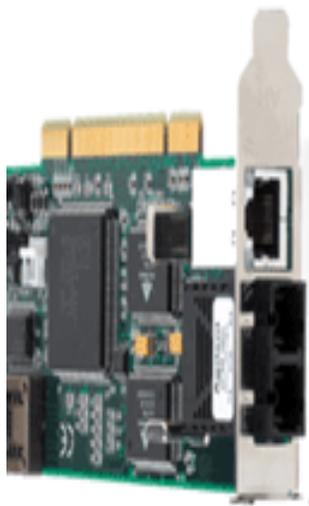
- * Topologia a stella
- * Semplicità di manutenzione
- * Distanza massima dall'hub: 100m
- * Tutte le stazioni collegate ad un hub sono nello stesso **dominio di collisione**
- * **Gli hub** sono solo ripetitori del segnale (**lavorano al livello fisico**)



Connettore RJ-45 (doppino)



Pin	Signal	Description
1	RxD (+)	Receive Data (+)
2	RxD (-)	Receive Data (-)
3	TxD (+)	Trasmit Data (+)
4	NC	
5	NC	
6	TxD (-)	Transmit Data (-)
7	NC	
8	NC	



Codifica dei dati

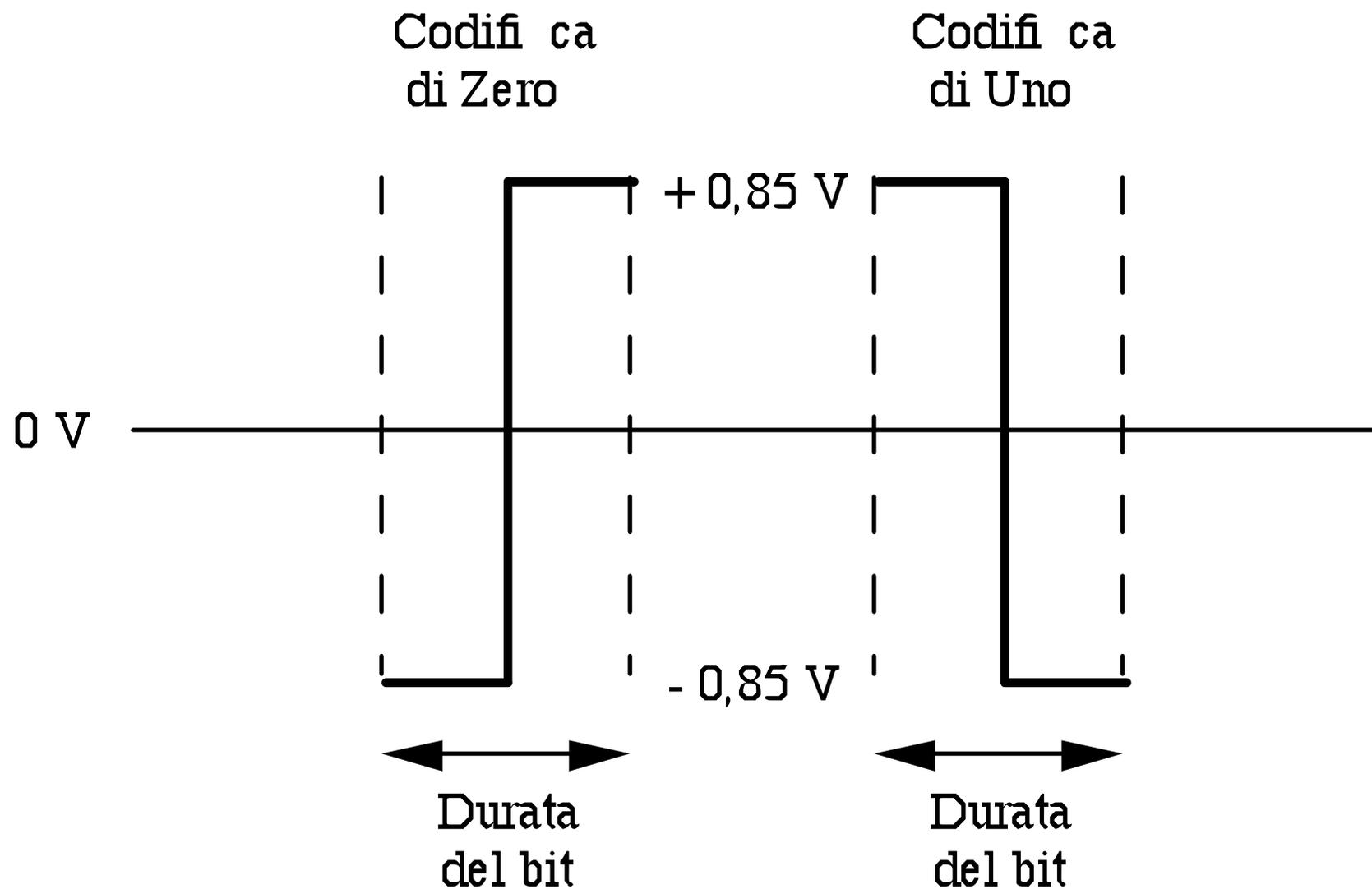
IEEE 802.3 non usa una codifica diretta dei dati (*zero* volt per **0** e *cinque* volt per **1**), perché sarebbe difficile rilevare le collisioni.

Binary o Non-Return To Zero (NRZ) encoding

La codifica deve facilitare l'individuazione dell'inizio e della fine del singolo bit.

Si usa una codifica, detta *Manchester*, che prevede una transizione del valore del segnale nel mezzo di ogni bit, **0** o **1** che sia.

Codifica *Manchester*



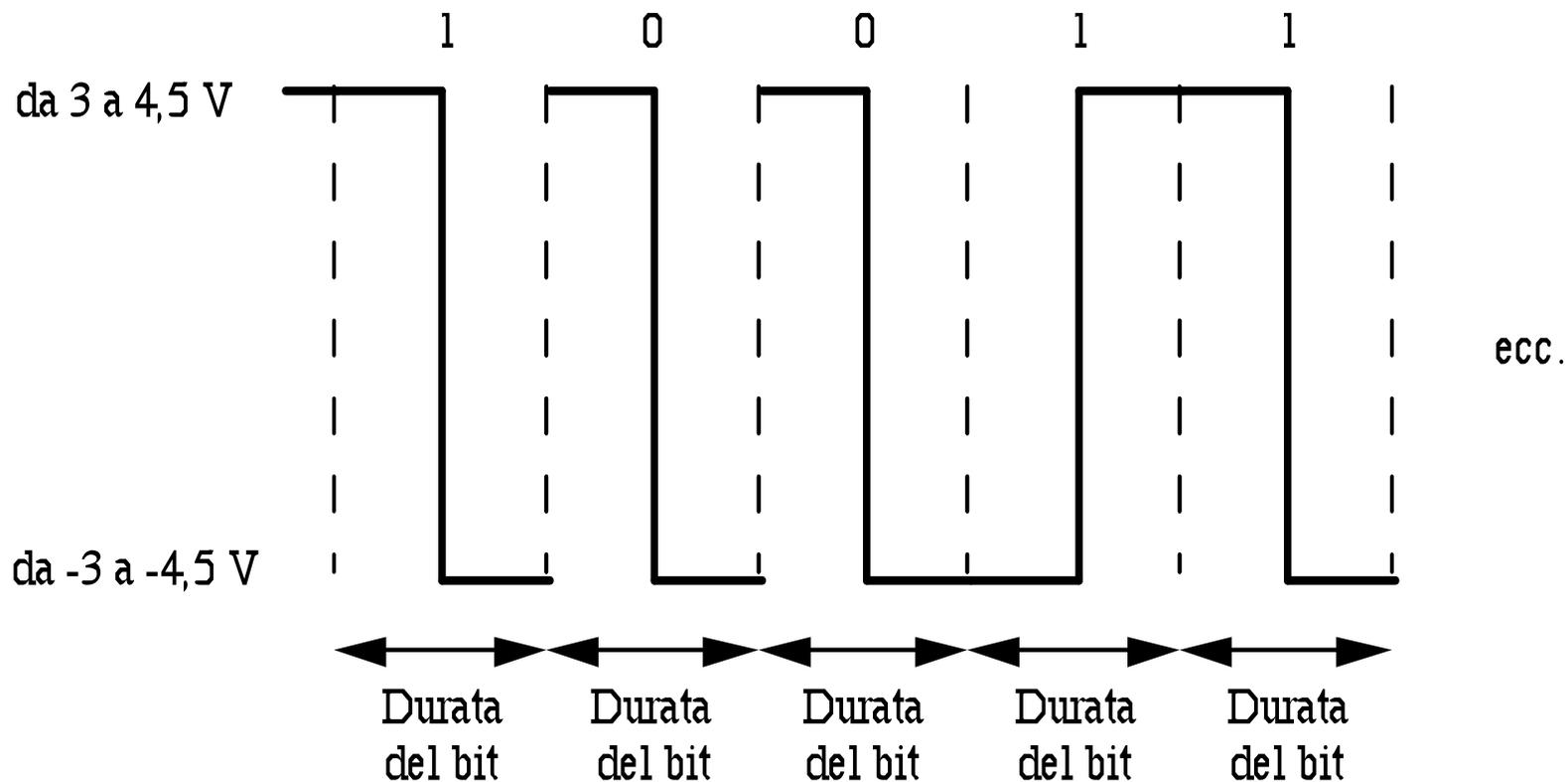
Livelli standard IEEE 802.3: **-0.85**, **+0.85**

Differential Manchester Encoding:

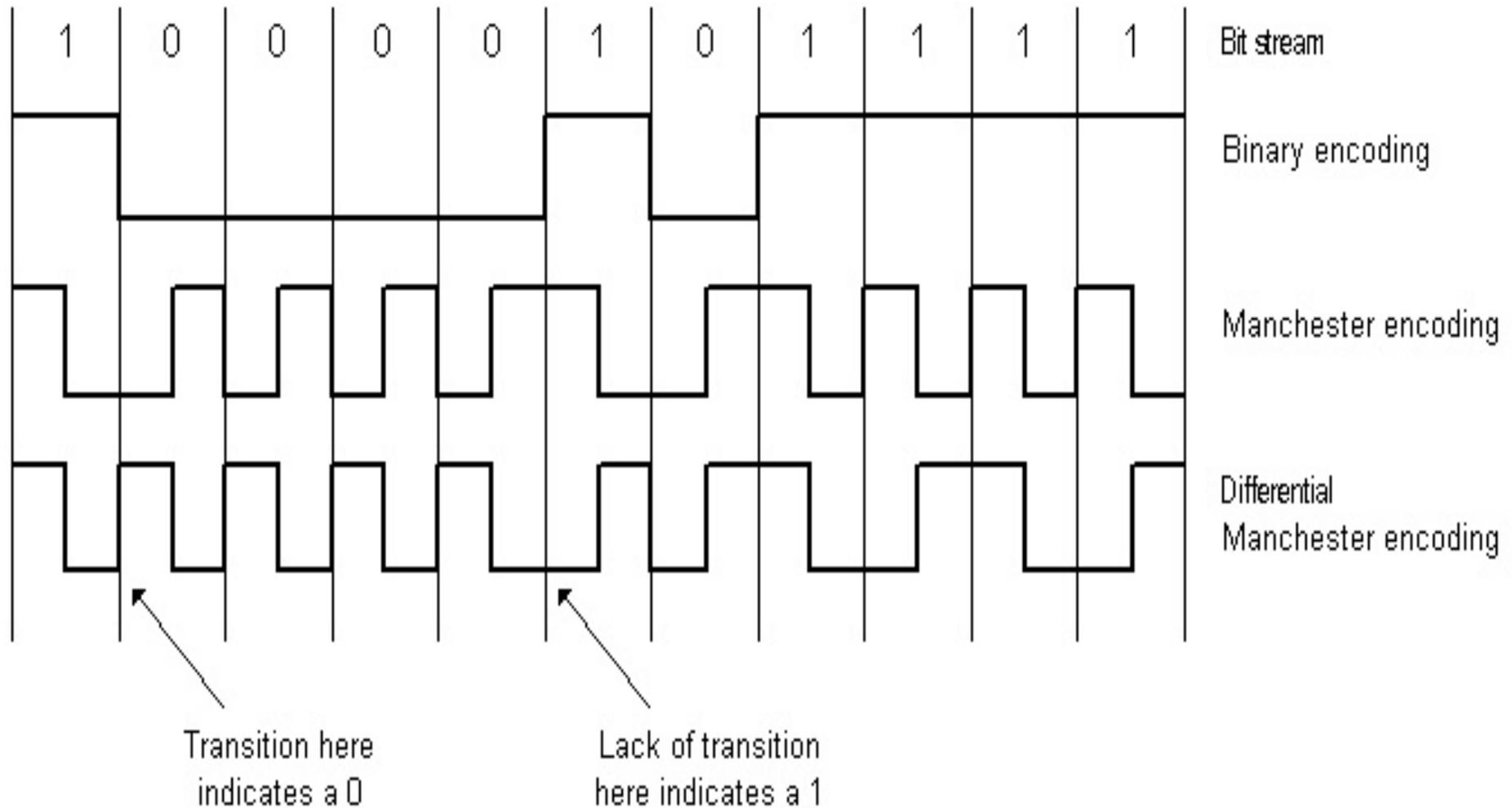
0: transizione all'inizio del bit;

1: non c'è transizione all'inizio del bit;

0, 1: c'è transizione a metà del bit.



Data Link Bit Encoding



Nei modelli *Carrier Sensitive*, che fanno uso della codifica *Manchester*, l'assenza di portante può essere codificata con segnale nullo

Con la codifica *Manchester* si ha una facile:

- * **sincronizzazione** fra mittente e destinatario;
- * rilevazione delle **collisioni**.

Il codice è *bilanciato* (uguale energia per **0** e **1**) e la trasmissione di più **0** o più **1** consecutivi non produce componenti in corrente continua (dannose nella trasmissione dei segnali).

A parità di velocità di trasmissione, la codifica Manchester richiede una **banda doppia** rispetto alla codifica diretta (ogni bit richiede la trasmissione di due valori distinti).

Formato del Frame IEEE 802.3

Byte:	7	1	6	6	2	0 - 1500	0 - 46	4
	Preamble	Start of frame	Indirizzo destinaz.	Indirizzo sorgente	Lunghezza dei dati	Dati	Pad	Checksum

* **Preambolo:** 7 byte **10101010**.

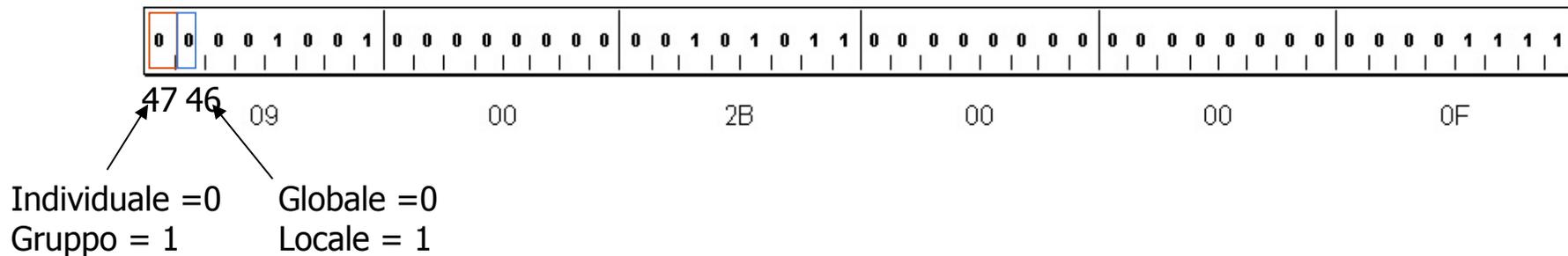
Trasmettendo 7 byte 10101010 si produce un'onda quadra per $5.6 \mu\text{s}$ ($7 \cdot 8 \text{ bit}$, $10 \text{ bit}/\mu\text{s}$), impiegata per sincronizzare il clock del destinatario con quello del mittente

* **Start of frame:** 1 byte **10101011**

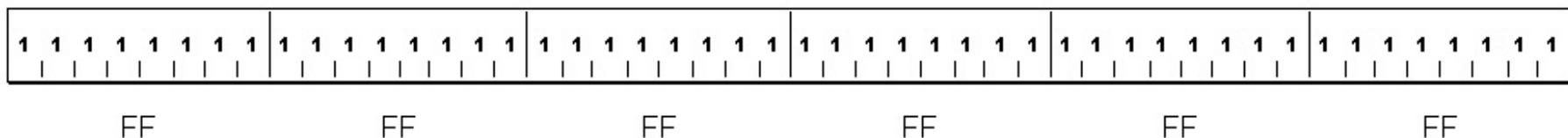
* Indica l'inizio del pacchetto

Byte:	7	1	6	6	2	0 - 1500	0 - 46	4
	Preamble	Start of frame	Indirizzo destinat.	Indirizzo sorgente	Lunghezza dei dati	Dati	Pad	Checksum

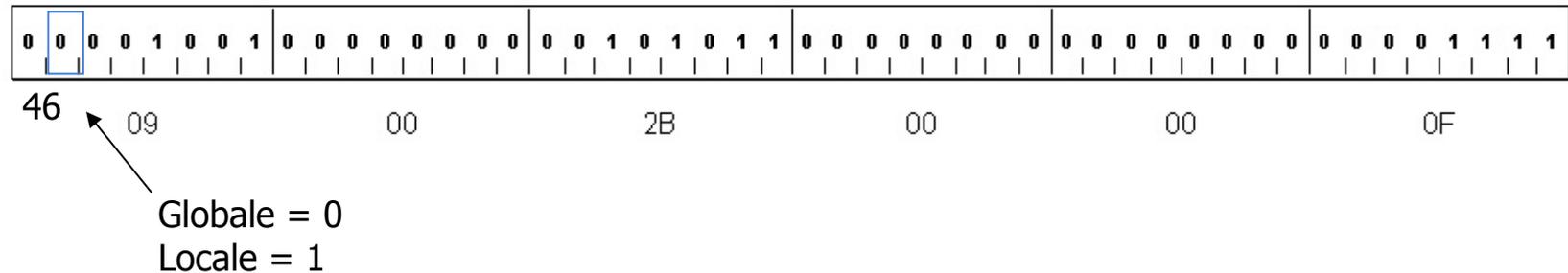
Il frame contiene l'indirizzo del mittente e del destinatario rappresentati su 6 byte (48 bit)



- * Il bit 47 (Individual, Group) definisce se il frame è indirizzato ad una singola stazione (**unicast**) o a un gruppo di stazioni (**multicast**)
- * Un indirizzo composto da tutti 1 è riservato per il **broadcast** (il frame è ricevuto da tutte le stazioni)



Indirizzi Ethernet



Il bit 46 distingue gli indirizzi locali da quelli globali

Gli indirizzi globali sono assegnati dalla IEEE per assicurare l'unicità degli indirizzi

Sono disponibili $2^{46} \approx 7 \times 10^{13}$ indirizzi globali

- * Tutte le stazioni ricevono il frame e lo accettano se l'indirizzo destinazione è compatibile con quello a loro assegnato
- Se la trasmissione è *unicast* solo la stazione con l'indirizzo specificato nel campo destinazione del frame accetta il pacchetto. Le altre stazioni lo scartano
- Il riconoscimento dell'indirizzo è a livello hardware
- * Se l'interfaccia è configurata in **modo promiscuo**, accetta tutti i pacchetti

Byte: 7 1 6 6 2 0 - 1500 0 - 46 4

Preamble	Start of frame	Indirizzo destinaz.	Indirizzo sorgente	Lunghezza dei dati	Dati	Pad	Checksum
----------	----------------	---------------------	--------------------	--------------------	------	-----	----------

Lunghezza dei dati: indica il numero di byte (tra **0** e **1500**) del campo dati.

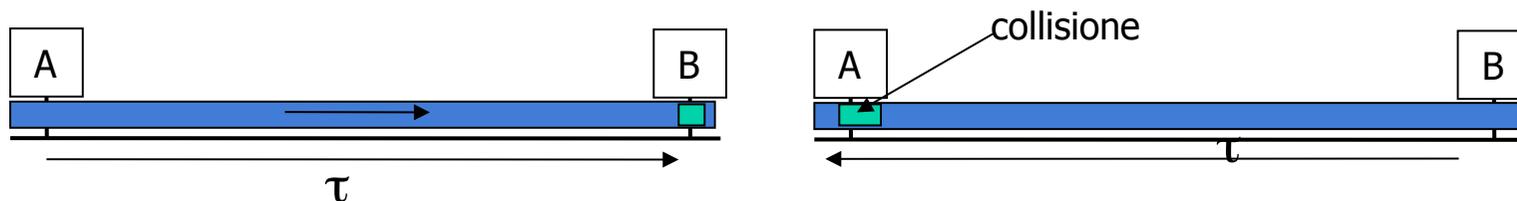
Dati: contiene il payload del livello superiore.

Pad: Se il frame (esclusi preambolo e delimiter) è più corto di 64 byte, con questo campo lo si porta alla lunghezza di 64 byte.

Checksum: codice CRC.

Lunghezza del frame: occorre evitare che la trasmissione termini prima che il primo bit abbia raggiunto l'estremità più lontana e sia tornata indietro.

Per una LAN a 10 Mbps di 2.5 Km (4 ripetitori) un pacchetto deve durare almeno 51.2 μ s (64 byte). Velocità maggiori sono possibili limitando la lunghezza del cavo



Byte:	7	1	2 opp. 6	2 opp. 6	2	0 - 1500	0 - 46	4
	Preamble	Start of frame	Indirizzo destinaz.	Indirizzo sorgente	Lunghezza dei dati	Dati	Pad	Checksum

Escludendo i (6 + 6) byte per gli indirizzi, i 2 del campo length e i 4 del checksum, occorrono *almeno altri 46 byte* (eventuale padding)

Estensione massima teorica

Trasmettendo a 10 Mbps si ha un bit ogni 100 ns. Se il pacchetto minimo è di 64 byte (512 bit) la trasmissione di (7+1+64) byte (576 bit) richiede 57.6 μ s

Poiché un bit percorre circa 200 m/ μ s, i metri percorsi (andata/ritorno) in 57 μ s sono $(57*200)/2 \cong 5.7$ Km

Estensione massima in pratica

Poiché ogni repeater introduce un delay di circa 5.3 μ s, in una rete con 4 repeater si introduce un delay (andata/ritorno) tale per cui la massima estensione non deve superare i 2 Km.

Estensione massima $L_{max} \cong 2$ Km.

L'802.3 adotta il CSMA/CD di tipo 1-persistent

Una stazione che deve trasmettere ascolta il canale:

- * se è libero, avvia la trasmissione;*
- * se è occupato, aspetta, ed appena libero inizia a trasmettere;*

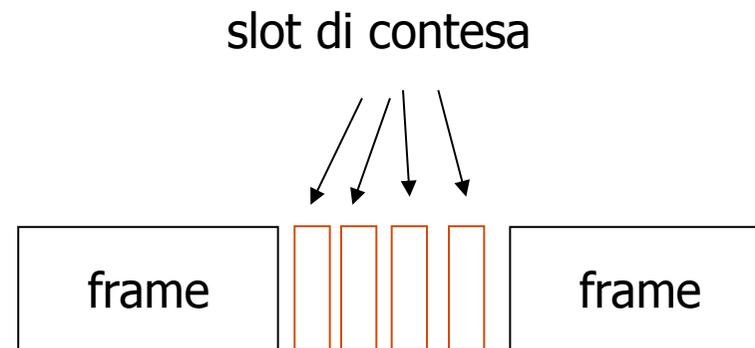
Se durante la trasmissione si verifica una collisione

******la circuiteria contenuta nel transceiver *invia una sequenza di jamming di 32 bit*, per avvisare le altre stazioni;

******attende una quantità di tempo casuale e poi riprova.

Binary backoff exponential algorithm: Algoritmo per il calcolo del tempo di attesa dopo una collisione

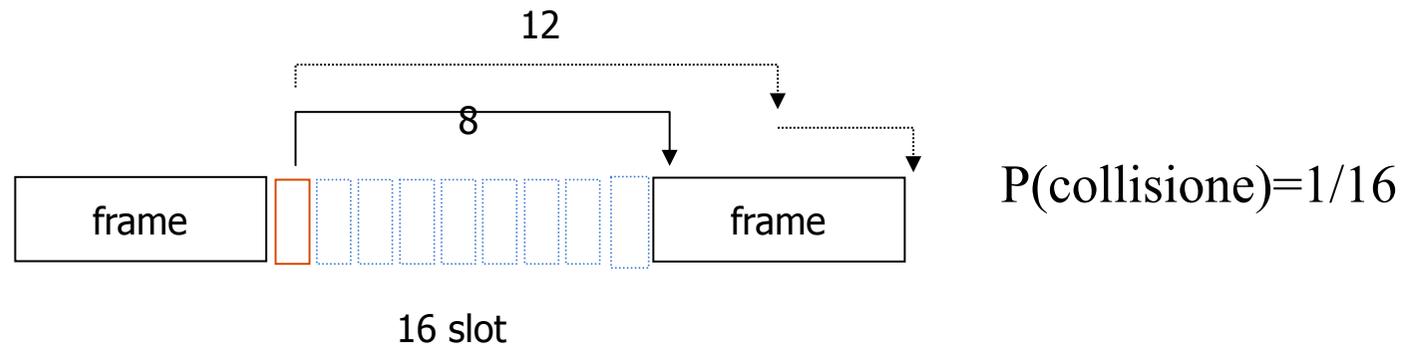
Slot di contesa: 512 bit a 10 Mbps \Rightarrow 51.2 μ s



- * **Prima collisione**: aspetta **0** o **1** slot
- * **Seconda collisione**: aspetta **0, 1, 2** o **3** slot
- * **Collisione n**: aspetta **r** slot con **r** scelto in modo casuale nell'intervallo $0 \leq r \leq 2k-1$ dove $k = \min(\mathbf{n}, \mathbf{10})$
- * **Collisione n = 16**: si notifica l'errore di trasmissione

Il *Binary backoff exponential algorithm* adatta l'attesa al numero di stazioni che vogliono trasmettere

- Un numero alto di slot di attesa diminuisce la probabilità che due stazioni collidano di nuovo ma introduce un ritardo medio elevato



- Un numero basso di slot di attesa rende improbabile la risoluzione della collisione quando molte stazioni collidono

Nell'ipotesi di k stazioni sempre pronte a trasmettere con probabilità di trasmissione p costante per ogni slot, **la probabilità A che sul canale vi sia una trasmissione è:**

$$A = k p (1-p)^{k-1}$$

Probabilità che:

- una stazione trasmetta
- le altre $k-1$ no
- per ogni stazione disponibile (k)

mentre **la probabilità che la trasmissione avvenga nel j -esimo slot è:**

$$A (1-A)^{j-1}$$

Probabilità che la trasmissione:

- avvenga nello slot j
- sia fallita nei $j-1$ slot precedenti

Nel caso di carico costante il numero medio di slot di contesa è $1/A$, e poiché ogni slot ha durata 2τ , l'intervallo medio di contesa è $2\tau/A$.

Per un frame di F bit la trasmissione attraverso un canale di banda B richiederà T secondi, con $T = F/B$.

Conseguentemente l'efficienza del canale

$$E = T/(T + 2\tau/A)$$

- * Diminuisce con la lunghezza della linea (τ)
- * Aumenta con la dimensione F del frame ($T = F/B$)
- * Decresce al crescere del numero di stazioni pronte a trasmettere (aumentando le stazioni aumenta la probabilità di collisione).

Poiché il modello di traffico nelle LAN non è **poissoniano** ma **bursty** e **self similar** (su un lungo periodo l'andamento è simile a quello su un breve periodo), ***prestazioni accettabili si ottengono per un carico medio del 30% con picchi del 60% (3 ÷ 6 Mbps)***

In situazioni di **carico medio**:

- *il **2-3%** dei pacchetti ha una collisione;

- ***qualche pacchetto su 10.000** ha più di una collisione.

Riepilogando

Ethernet nasce all'inizio degli anni 80:

- * topologia a bus su cavo coassiale
- * 10 Mbs (throughput massimo 4 Mbs)
- * protocollo ***MAC CSMA/CD***

successivamente:

- * topologia a stella (cablaggio strutturato)
- * doppini in rame e fibra ottica evoluzione a 100 Mbs (***802.3u***), 1 Gbs (***802.3z***) e 10 Gbs (***802.3ae***)

Fast Ethernet : standard ***802.3u*** (approvato nel 1995) passa da ***10 Mbps*** a ***100 Mbps***.

Doppino cat. 3 (100BaseT4) - si usano quattro doppini fra l'hub ed ogni stazione:

- * uno per il traffico dall'hub alla stazione;*
- * uno per il traffico dalla stazione all'hub;*
- * 2 usati di volta in volta nella direzione della trasmissione in corso;*

100BaseT4: non utilizza la codifica Manchester

Codifica ***8B6T*** (8 bit codificati con 6 ***trit***)

trit = simboli ternari [+ - 0]

La velocità di segnalazione è **25 Mhz** (contro i 20 Mhz dell'802.3) e **si inviano sui 3 doppini 3 trit (27 simboli: 4 bit + ridondanza)** per volta.

Poiché 3 trit => convogliano 4 bit otteniamo:

$$4 * 25 = \mathbf{100 Mbps.}$$

Si ha un canale nell'altro verso a 33.3 Mbps

Standard *802.3u*: *Doppino cat. 5 (100BaseT)*

- * codifica *4B5B* (4 bit codificati con 5 bit);
- * velocità di segnalazione *125* Mhz;

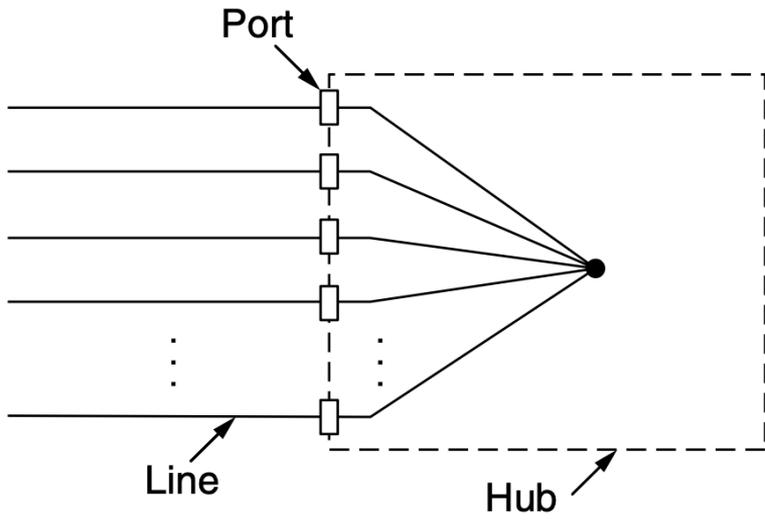
Hub tradizionale:

- * lunghezza massima di un ramo è 100 mt;
- * il diametro della rete è (100+100) metri.

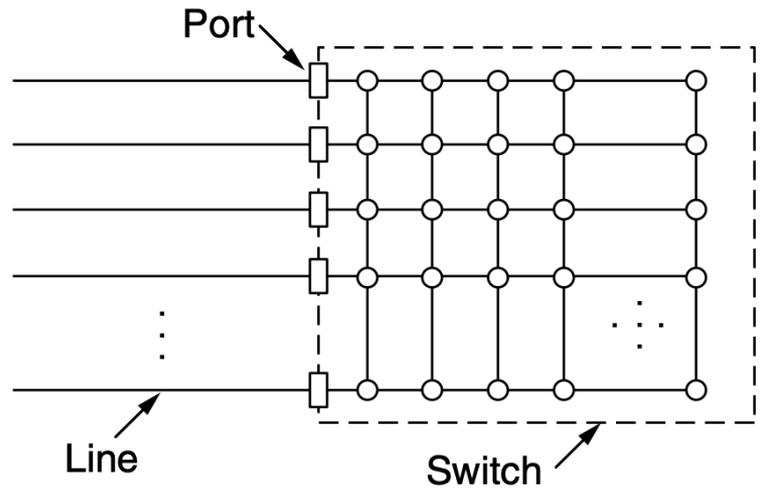
Switched hub:

- * ogni ramo è un dominio di collisione separato (non possono aversi collisioni);
- * resta il limite di 100+100 metri.

Codifica <i>4B/5B</i> :	<u>Sorgente</u>	<u>Mezzo fisico</u>
	0000	11110
	0001	01001
	0010	10100
I 4 bit della sorgente sono	0011	10101
mappati su pattern	0100	01010
FISSO di 5 bit sul	0101	01011
mezzo fisico (codeword)	0110	01110
	0111	01111
Non esistono codeword	1000	10010
con una sequenza	1001	10011
di valori 0 maggiore di tre	1010	10110
	1011	10111
	1100	11010
	1101	11011
	1110	11100
	1111	11101



(a)



(b)

Standard 802.3u

100BaseFX (fibra ottica):

- * velocità di segnalazione **125** Mhz;
- * codifica **4B5B**
- * obbligatorio switched hub;

Lunghezza rami fino a **2 km** (con uno switched hub non c'è il problema delle collisioni).

Prima finestra: etichettata 850 nm, con *sorgente LED*, viene utilizzata per le *fibre multimodali* in applicazione *LAN con distanze medio-piccole*.

Seconda finestra: etichettata 1300 nm, con *sorgente LED*, è utilizzata con *fibre multimodali* in applicazione *LAN con distanze medie*. Questa stessa finestra viene portata a 1310 nm, con sorgente laser, costituendo la prima finestra per la **fibra monomodale** per applicazioni LAN e trasmissione dati su distanze medio-lunghe.

Terza finestra: etichettata 1550nm, con *sorgente LASER*, è utilizzata con *fibre monomodali* per trasmissione dati su distanze lunghe.

1000Base-X (Gigabit Ethernet)

A seconda del supporto fisico, si distinguono:

–1000Base-SX

- ***Fibra ottica multimodale*** in prima finestra, distanze fino a 275m o 550m a seconda del tipo di fibra.

–1000Base-LX

- ***Fibra ottica monomodale*** in seconda finestra, distanze fino a 5km (secondo lo standard) o 10km (secondo molti produttori).

1000Base-T Gigabit ethernet su UTP cat. 5

standardizzata come IEEE 802.3ab, usa tutte e 4 le coppie di conduttori di un cavo UTP (distanza max 100m)

1000Base-TX Gigabit ethernet su UTP cat. 6

standardizzata come IEEE 802.3z, usa solo 2 coppie di conduttori. (distanza max 100m)

1000Base-LLX o 1000Base-LH o 1000BASE-ZX

Fibra ottica monomodale, con trasmissione in terza finestra, distanze fino 70km. Non standardizzata ma offerta da molti produttori.

10GBASE-X (10Gbps) A seconda del supporto fisico, si distinguono:

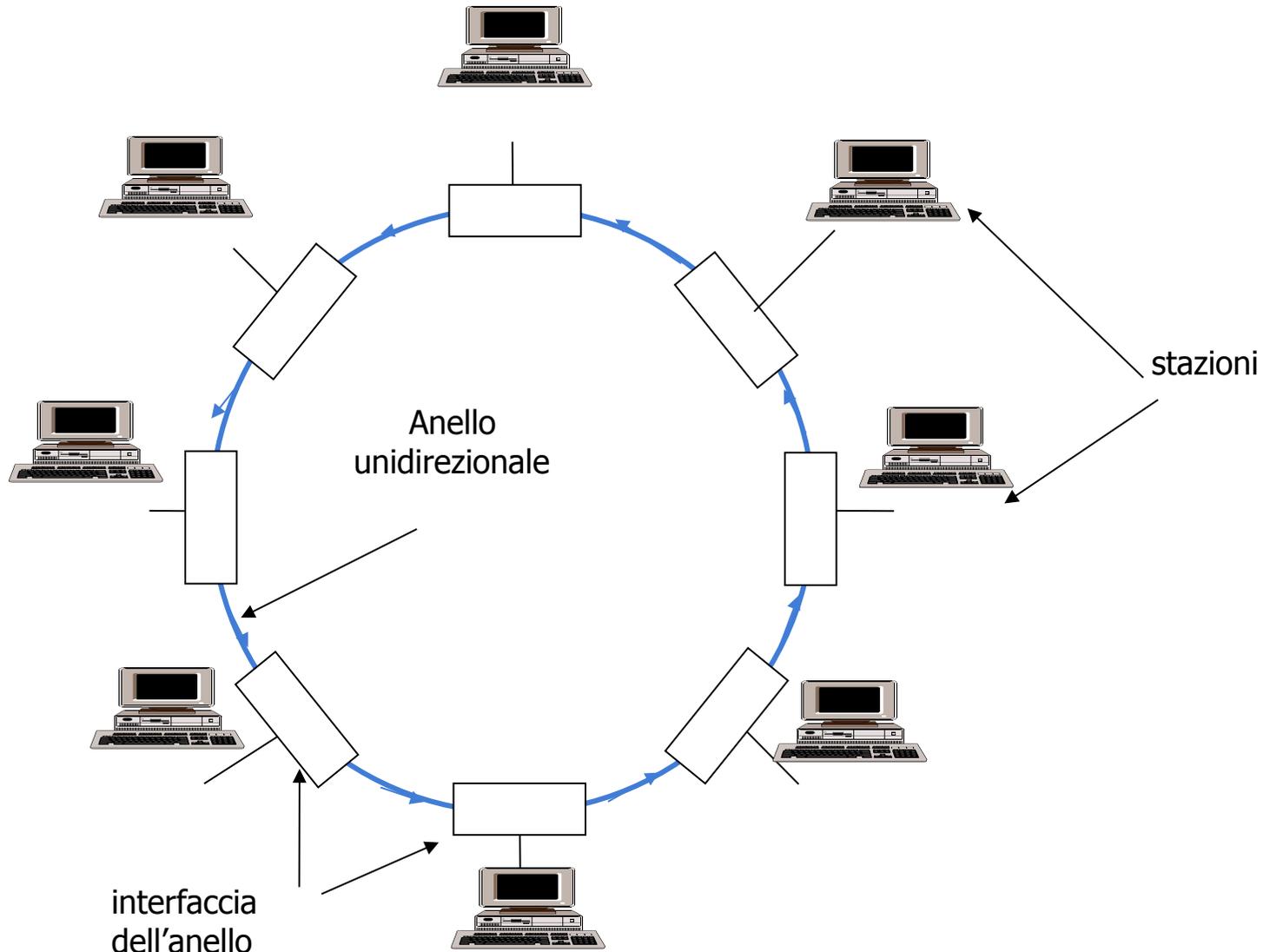
10GBASE-S: fibra multimodale (fino a 65m)

10GBASE-LX4: (trasmissione CWDM su fibra multimodale (fino a 300m), oppure fibra monomodale in seconda finestra (fino a 10km))

10GBASE-L: fibra monomodale in seconda finestra (fino a 10km)

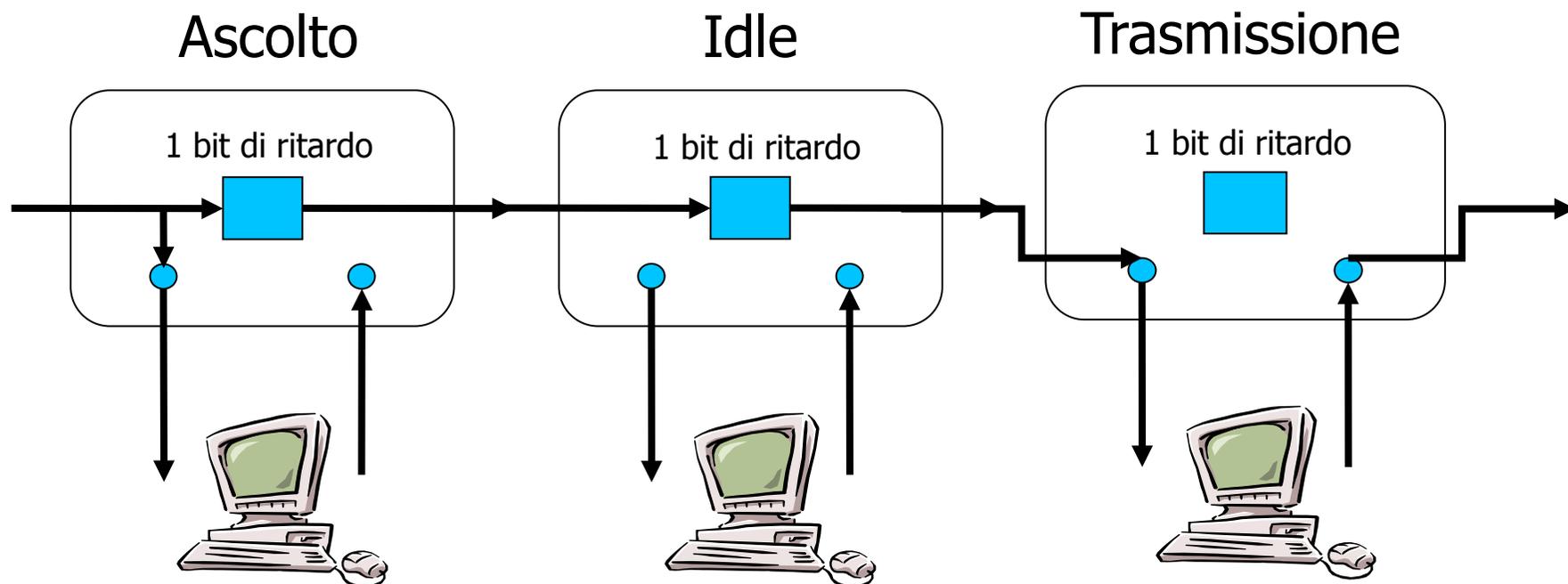
10GBASE-E: fibra monomodale in terza finestra (fino a 40km)

Token Ring: Utilizza un insieme di collegamenti punto-punto



Interfaccia Token Ring

- Ogni bit che raggiunge l'interfaccia è copiato in un buffer di 1 bit
- Il bit viene ritrasmesso sull'anello dopo un'eventuale controllo (**ascolto**) o modifica (**trasmissione**)
- Si ha un ritardo di 1 bit per ogni interfaccia



Problema dell'*Anello*

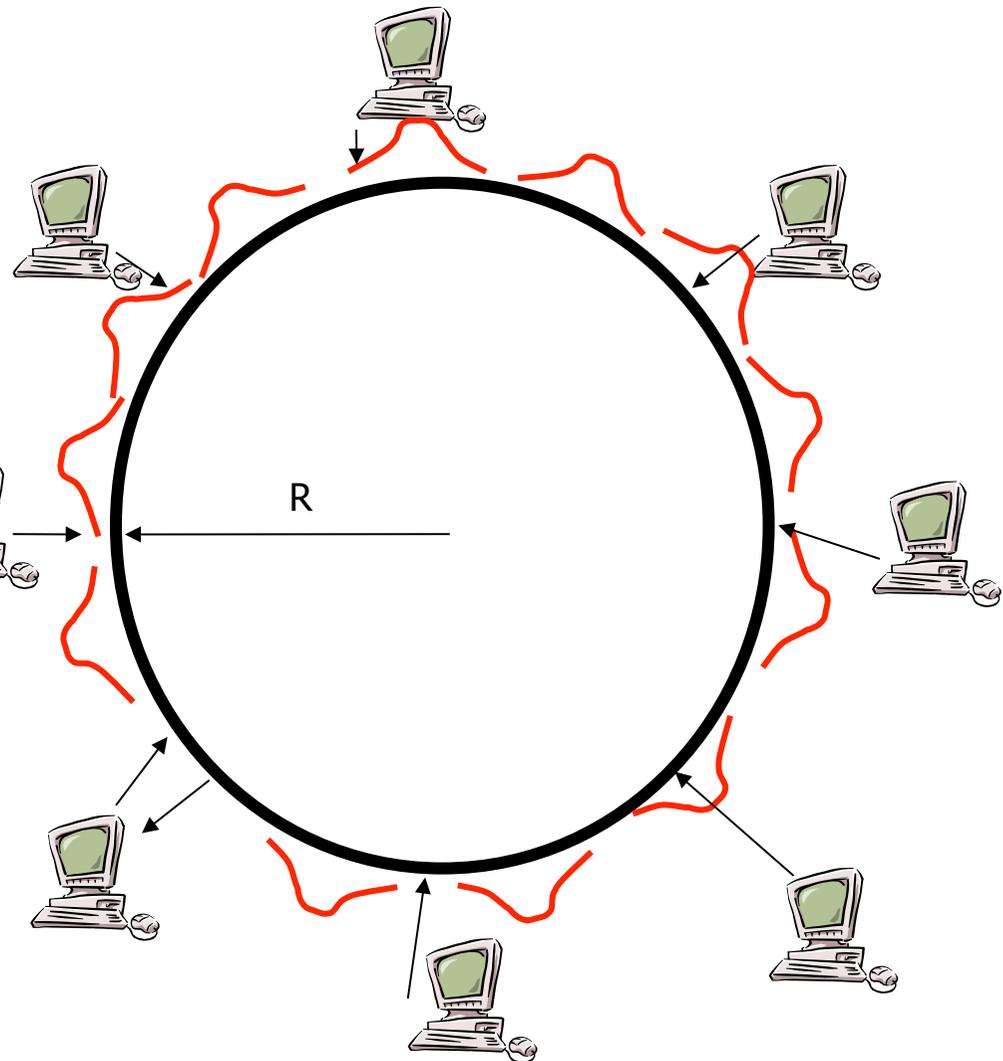
Ipotesi:

Velocità della rete: V Mbps (nell'anello viene iniettato un bit ogni $\frac{1}{V} \mu\text{s}$)

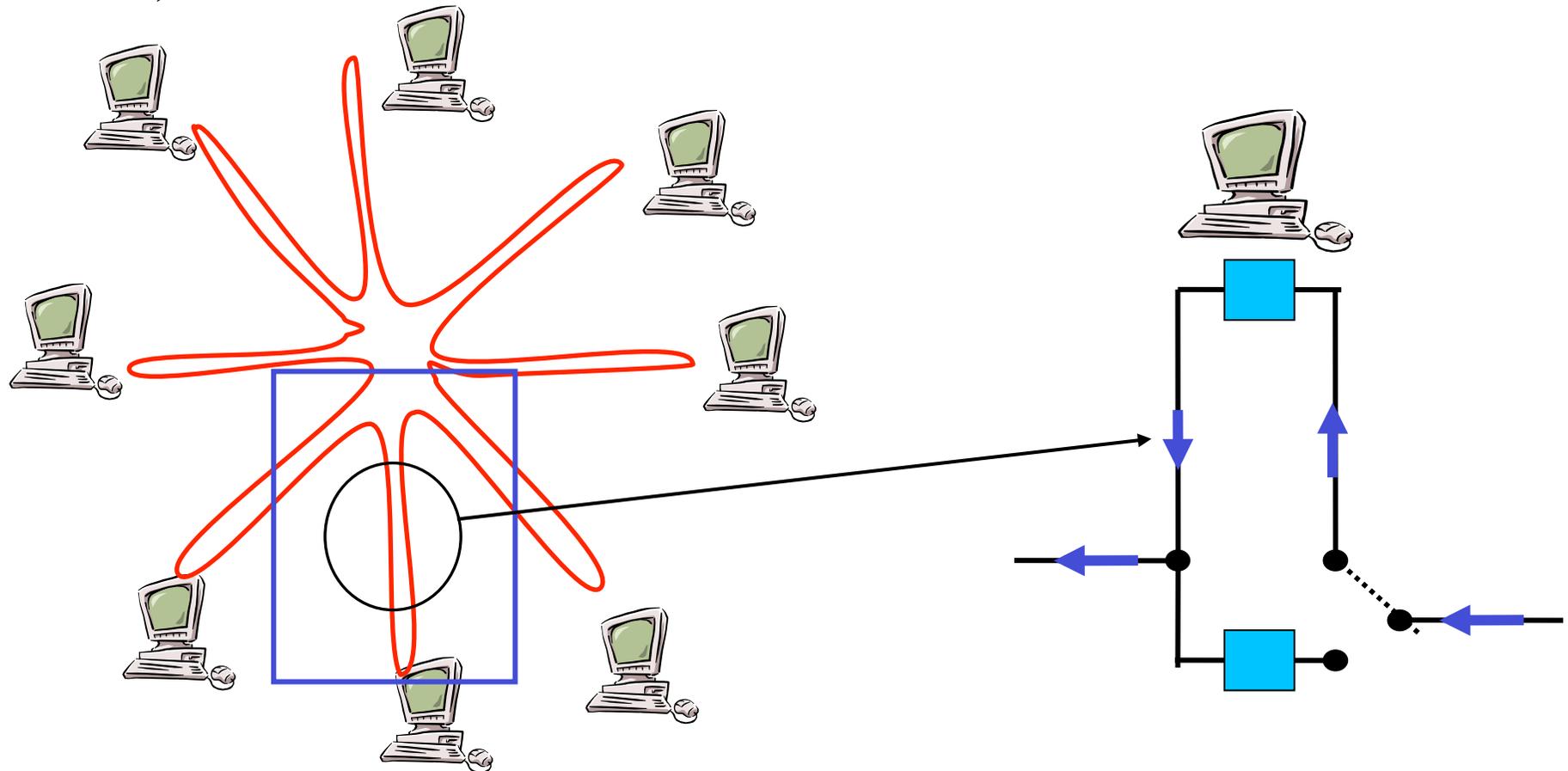
Velocità del segnale: $205 \text{ m}/\mu\text{sec}$
(in $\frac{1}{V} \mu\text{s}$ un bit percorre:
 $l_{\text{bit}} = \frac{205}{V} \text{ m}$)

Il massimo numero di bit presenti su un anello di raggio R è quindi:

$$n_{\text{bit}} = \frac{2\pi R V}{205}$$

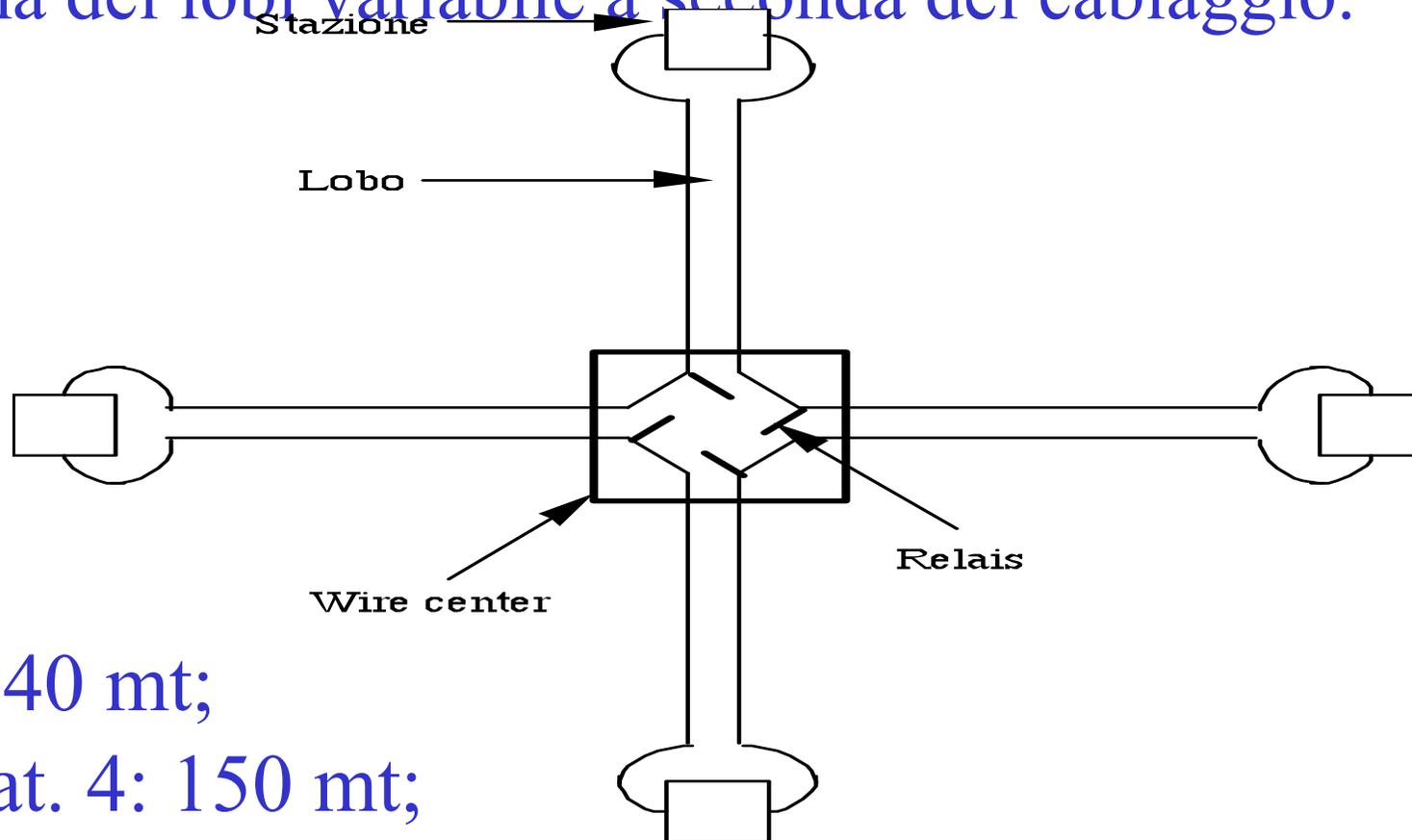


Problema: poiché l'anello deve contenere tutto il token, oltre il problema della lunghezza sono necessarie interfacce di rete che restino attive anche a terminale spento (interfacce con alimentazione autonoma).



*Si realizza un anello virtuale (**wire center**), accentrato in un singolo apparato di controllo e comunicazione, una specie di HUB ma più complesso.*

Nel cablaggio *wire center*, l'assenza della corrente su un lobo causa la chiusura del corrispondente relais e conseguentemente l'esclusione di tale lobo). Lunghezza massima dei lobi variabile a seconda del cablaggio.



STP: 340 mt;

UTP cat. 4: 150 mt;

UTP cat. 5: 195 met. Massimo 260 stazioni.

IEEE 802.5 (Token Ring di IBM 1972)

Principali differenze:

Token Ring prevede velocità di 4 e 16 Mbps;

IEEE 802.5 prevede 1, 4 e 16 Mbps.

Cablaggio (più diffuso) su doppino telefonico:

- * schermato (STP);
- * non schermato (UTP):
- * categoria 3, 4 o 5 per 4 Mbps;
- * categoria 4 o 5 per 16 Mbps.

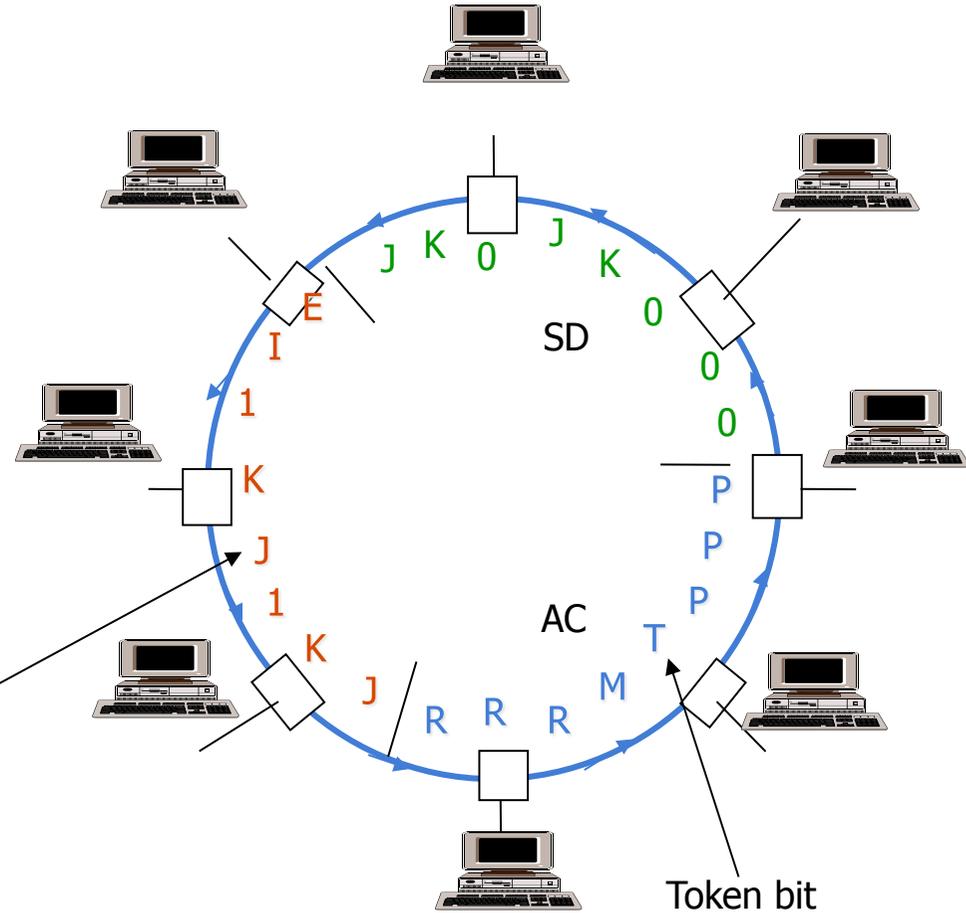
Il Token Frame



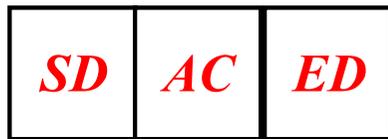
- J and K - Code Violations
- PPP - Priority Bits
- T - Token Bit
- M - Monitor Bit
- RRR - Reserved Bits
- I - Intermediate Frame Bit
- E - Error Bit

Quando nessuna stazione trasmette, il token frame viaggia di continuo sull'anello.

Protocollo *MAC 802.5*



Byte: 1 1 1



Struttura del token

Byte: 1 1 1 2 opp. 6 2 opp. 6 Da 0 a 17.747 4 1 1



Struttura del frame

AC (Access Control): utilizzato per il controllo dell'accesso, è costituito dagli 8 bit:

PPPTMRRR

PPP: indicano la ***priorità attuale***;

T (token bit): identifica un token se vale **0** e un frame se vale **1**;

M: serve per il controllo di ***frame orfani***. Il monitor lo setta ad **1** al passaggio del frame, e se lo ritrova ad **1** al passaggio successivo il frame è orfano e viene tolto dall'anello;

RRR: indicano la priorità richiesta.

FC (Frame Control): distingue frame dati e controllo.

Indirizzi: come 802.3.

Dati: contiene il payload del livello superiore.

Checksum: codice CRC.

Frame Status

A	C	r	r	r	r	r	r
---	---	---	---	---	---	---	---

A: Indirizzo riconosciuto

C: Frame copiato

Questi due bit segnalano al mittente del messaggio se il destinatario ha ricevuto tutto il pacchetto.

Le possibili situazioni sono 3:

$A = 0, C = 0$: Destinatario non esistente o non attivo

$A = 1, C = 0$: Destinatario esistente ma frame non copiato

$A = 1, C = 1$: Destinatario esistente e frame copiato

Funzionamento di 802.5

Quando una stazione (in listen mode) vuole trasmettere:

- * aspetta che arrivi il token;
- * lascia passare SD;
- * lascia passare i bit PPP di AC;
- * cambia in 1 il token bit T (trasformando il token in un frame) e lo invia sul ring;
- * passa in transmit mode;
- * invia il resto del frame;
- * finché non esaurisce il ***THT (Token holding time)*** può trasmettere altri frame;
- * rigenera un nuovo token e lo trasmette;
- * trasmesso l'ultimo bit del token ripassa in listen mode.

Stazione monitor: ogni stazione può funzionare da monitor.

Se una stazione si accorge che non c'è monitor, trasmette un frame di controllo **Claim Token**. Se il frame ritorna, essa diviene il monitor

Il monitor annuncia periodicamente la sua presenza con un frame di controllo **Active Monitor Present**

Funzioni del monitor:

- * controlla che il token non vada perso (utilizza un timer)
- * ripulisce l'anello da frame corrotti o orfani (frame di stazioni divenute inattivate prima di ritirarlo)
- * introduce ritardi se l'anello non riesce a contenere i 24 bit del token

IEEE 802.3

Vantaggi

- * ha un'enorme diffusione;
- * esibisce un buon funzionamento a dispetto della teoria.

Svantaggi

- * ha sostanziose componenti analogiche (per il rilevamento delle collisioni);
- * il funzionamento peggiora con forte carico.

IEEE 802.5

Vantaggi

- * è totalmente digitale;
- * va molto bene sotto forte carico.

Svantaggi

- * c'è ritardo anche senza carico (attesa token);
- * ha bisogno di un monitor.

In definitiva, nessuna delle due può essere giudicata la migliore in assoluto.

IEEE 802.2 *Logical Link Control (LLC)*

Il ***Logical Link Control*** definisce la parte superiore del livello data link, fornendo al livello network un'interfaccia unica (nasconde al livello network le differenze fra i vari sottolivelli MAC).

A differenza del sottolivello MAC che fornisce solo servizi datagram, l'***LLC*** a secondo della richiesta fornisce:

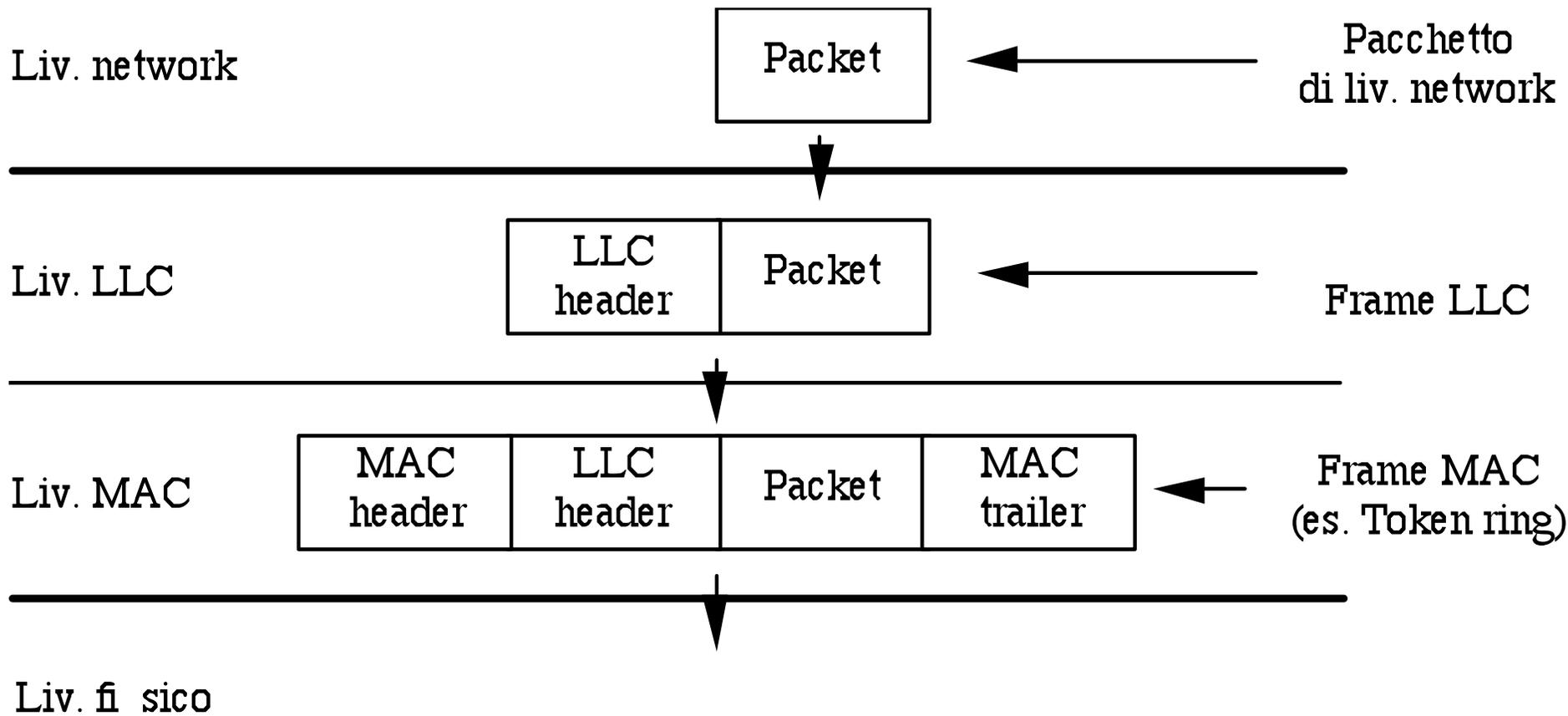
- servizi datagram;
- servizi datagram confermati;
- servizi affidabili orientati alla connessione.

Logical Link Control



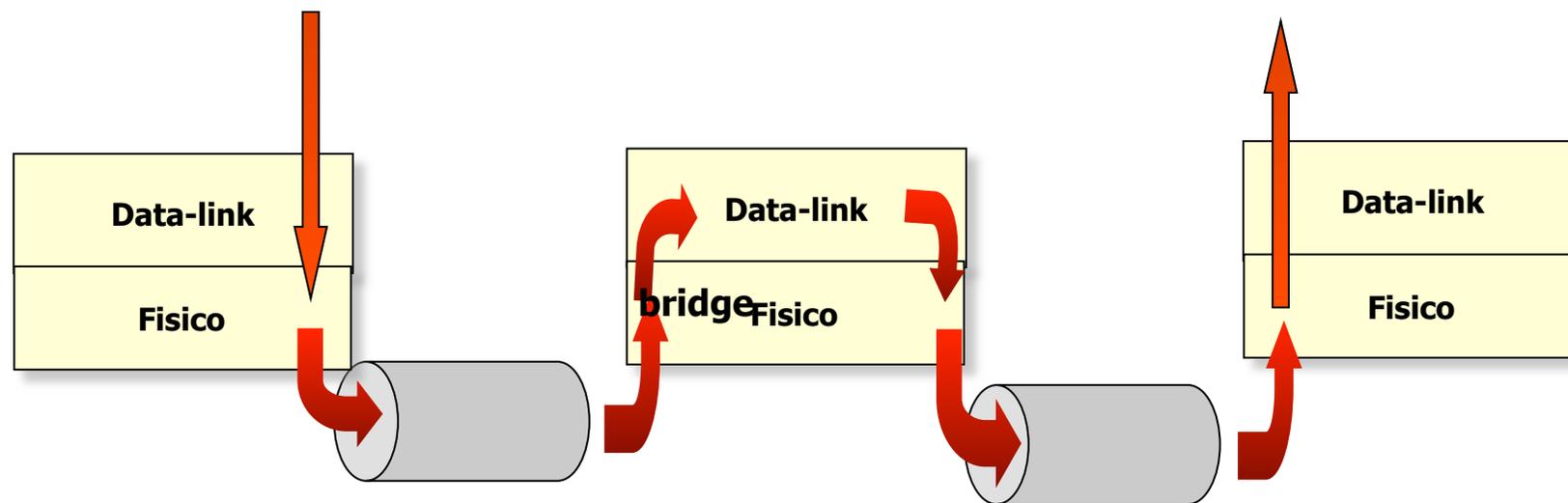
Gli indirizzi **LLC**, lunghi un byte (SSAP e DSAP Source e Destination Service Access point), indicano il protocollo di livello superiore che deve ricevere quel pacchetto (**LLC** offre un supporto **multiprotocollo**).

In trasmissione il frame LLC viene imbustato nel frame del sottolivello MAC impiegato (e deimbustato in ricezione).

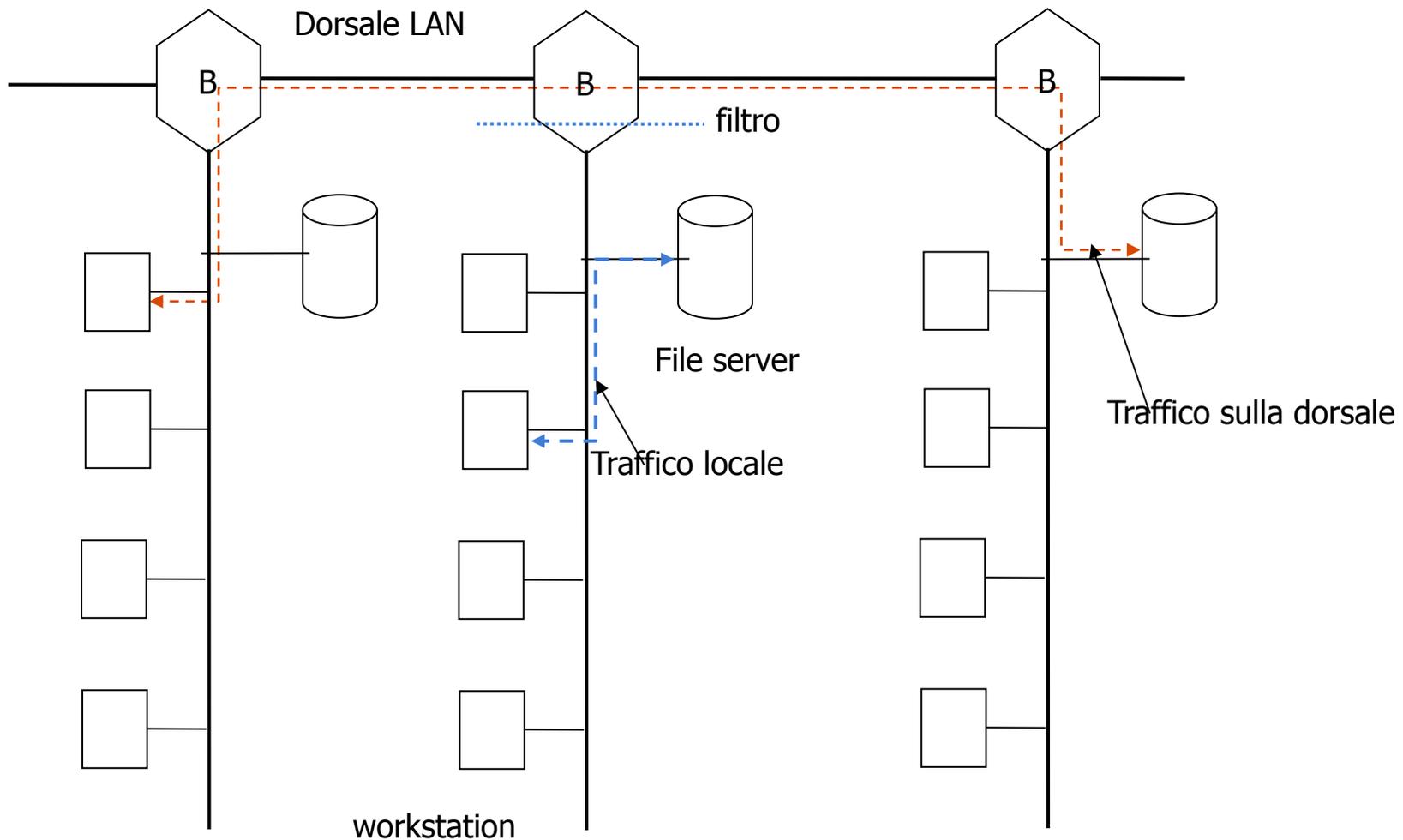


Bridge: *connettono più segmenti di una stessa LAN (omogenee e/o eterogenee) mantenendo la suddivisione a livello data link*

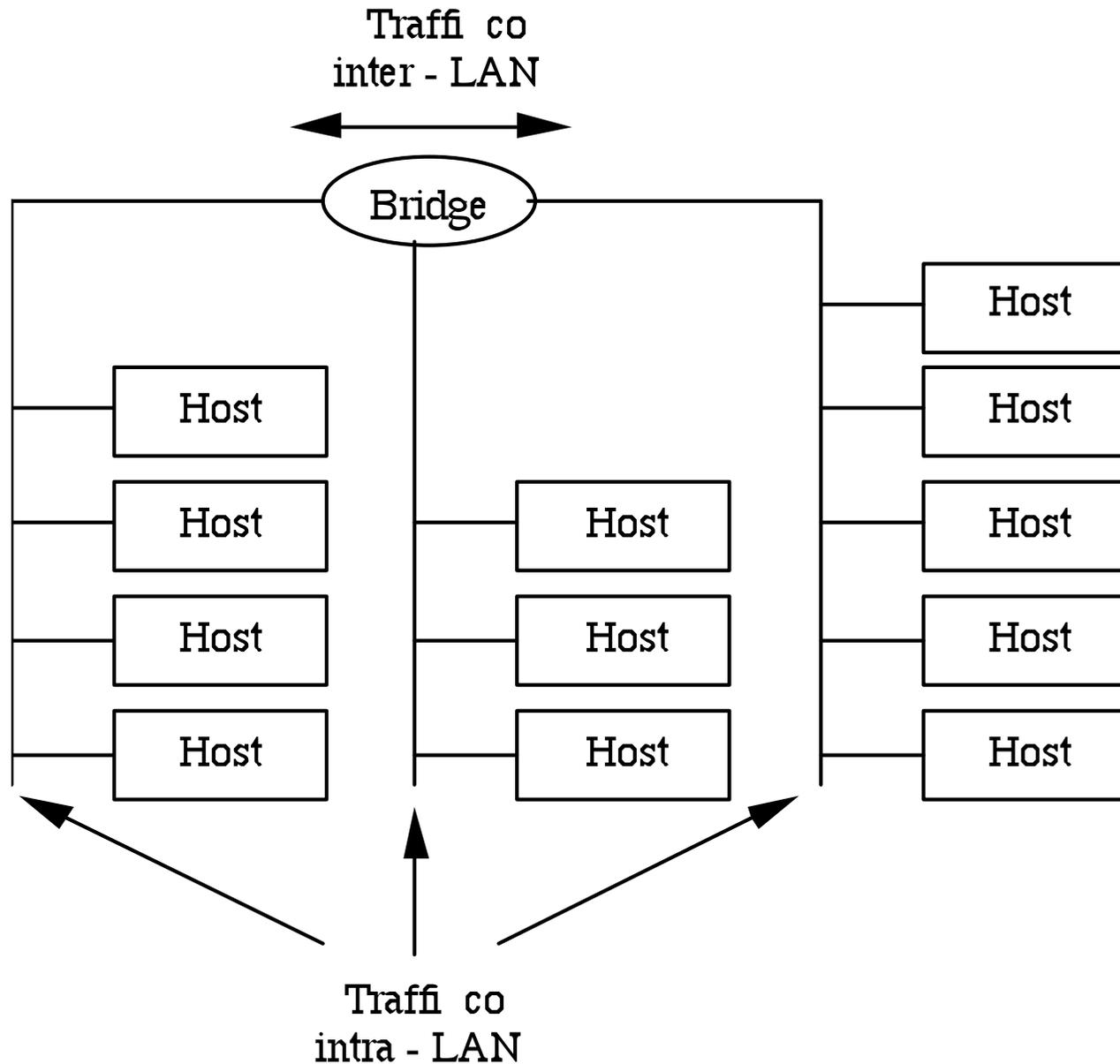
- * Possono collegare segmenti operanti con protocolli diversi
- * Frazionano la rete in segmenti creando domini di collisione separati (il traffico locale rimane confinato nella sottorete)
- * Confinano i malfunzionamenti dovuti a stazioni difettose
- * Aumentano la sicurezza dei dati - uso “malizioso” del modo promiscuo (il traffico su un segmento non è visibile alle altre)



Tiene confinati i traffici sui singoli segmenti, consentendo il passaggio solo alle comunicazioni che hanno mittente e destinatario su segmenti distinti.



Un bridge ha tante interfacce di rete quanti sono i segmenti ad esso collegati.



Quando una delle interfacce riceve un frame:

** lo passa al relativo software di livello MAC, che lo de-imbusta e lo passa al software di livello LLC del bridge;*

** sulla base dell'indirizzo MAC di destinazione, il bridge decide a quale segmento inviarlo:*

◦ se destinazione e provenienza si trovano sullo stesso segmento il frame viene scartato;

◦ altrimenti, il frame LLC viene passato al livello MAC dell'interfaccia collegata al segmento di destinazione

◦ il livello MAC lo imbusta e lo invia su tale LAN.

DIFFERENZA TRA RIPETITORE E BRIDGE

Un ripetitore copia pedissequamente tutto ciò che riceve da una linea su tutte le altre.

Il bridge, acquisito un frame, lo analizza, lo ricostruisce e lo inoltra, quindi può anche essere configurato in modo da *filtrare* (non far passare) traffico di uno specifico protocollo.

Il filtraggio avviene in funzione dei due ottetti SSAP e DSAP del LLC, che identificano il protocollo del mittente e quello del destinatario di livello superiore.

I bridge progettati per l'interconnessione di segmenti di tipo diverso (ad es. token ring ed ethernet) devono risolvere vari problemi:

- * *diversi formati dei frame;*

- * *differenti data rate;*

- * *diverse lunghezze massime.*

Funzioni previste dalla LAN mittente non necessariamente sono supportate da quella destinataria (ad esempio, il concetto di priorità ed i bit A e C presenti in 802.5 non hanno un equivalente in 802.3)

Bridge IEEE Standard

Transparent bridge: opera in modo trasparente, richiede solo l'alimentazione e la connessione fisica (le *tabelle d'instradamento* gestite dai *bridge*).

Source-routing bridge: il mittente indica esplicitamente il cammino (sequenza di bridge e reti) che il frame deve attraversare (*tabelle d'instradamento* gestite dai sistemi connessi alle LAN) .

Transparent bridge (IEEE 802.1 part D)

Appena attivato, il bridge esamina tutti i frame che gli arrivano dalle varie LAN, e sulla base di questi costruisce progressivamente le sue tabelle di instradamento.

Quando arriva un frame, inviato da un mittente non presente in tabella (sconosciuto), il bridge aggiunge una nuova riga in tabella in cui registra la porta (rete), attraverso cui il frame gli è pervenuto, ed il MAC address del relativo mittente.

Per ogni frame ricevuto il bridge consulta le tabelle di instradamento :

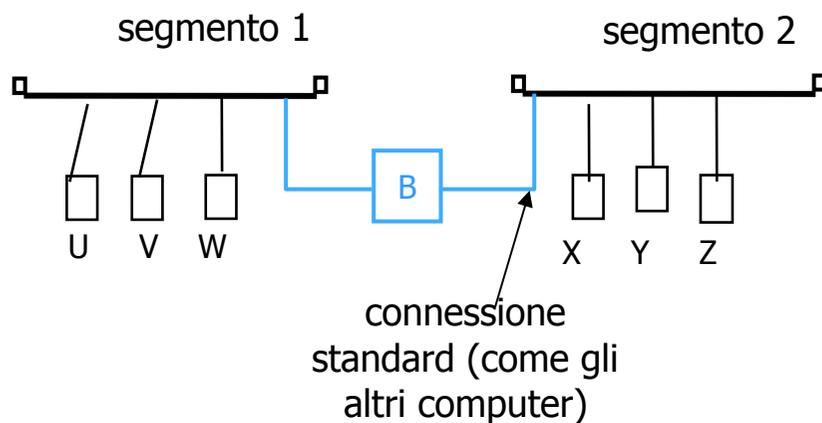
- * se la porta di destinazione è la stessa di quella di arrivo, lo scarta;

- * se la porta di destinazione è diversa da quella di arrivo, invia il frame sulla LAN ad essa associata;

- * se la porta di destinazione non è presente in tabella, invia il frame a tutte le LAN tranne quella di provenienza (**flooding**).

Bridge trasparenti: dispositivi “*plug-and-play*” non richiedono alcuna configurazione

- * Operando in modo promiscuo il bridge riceve tutto il traffico delle LAN a cui è connesso;
- * Osservando il traffico costruisce una tabella hash interna, in cui associa ad ogni indirizzo MAC la porta del bridge su cui ha ricevuto il frame che lo conteneva (*back learning*);



Evento	Lista segmento 1	Lista segmento 2
boot del bridge	-	-
U invia a V	U	-
V invia a U	U,V	-
broadcast di Z	U,V	Z
Y invia a V	U,V	Z,Y
Y invia a X	U,V	Z,Y
X invia a W	U,V	Z,Y,X
W invia a Z	U,V,W	Z,Y,X

Backward learning

*Al boot le tabelle sono vuote

*Dopo brevissimo tempo le tabelle sono complete e la struttura raggiunge la piena efficienza

Gestione dinamica: per una corretta gestione di topologie dinamiche (nuove stazioni e/o spostamenti da una rete all'altra), le tabelle sono continuamente aggiornate.

*Accanto ad ogni indirizzo in tabella, viene memorizzato in quale istante è arrivato l'ultimo frame inviato.

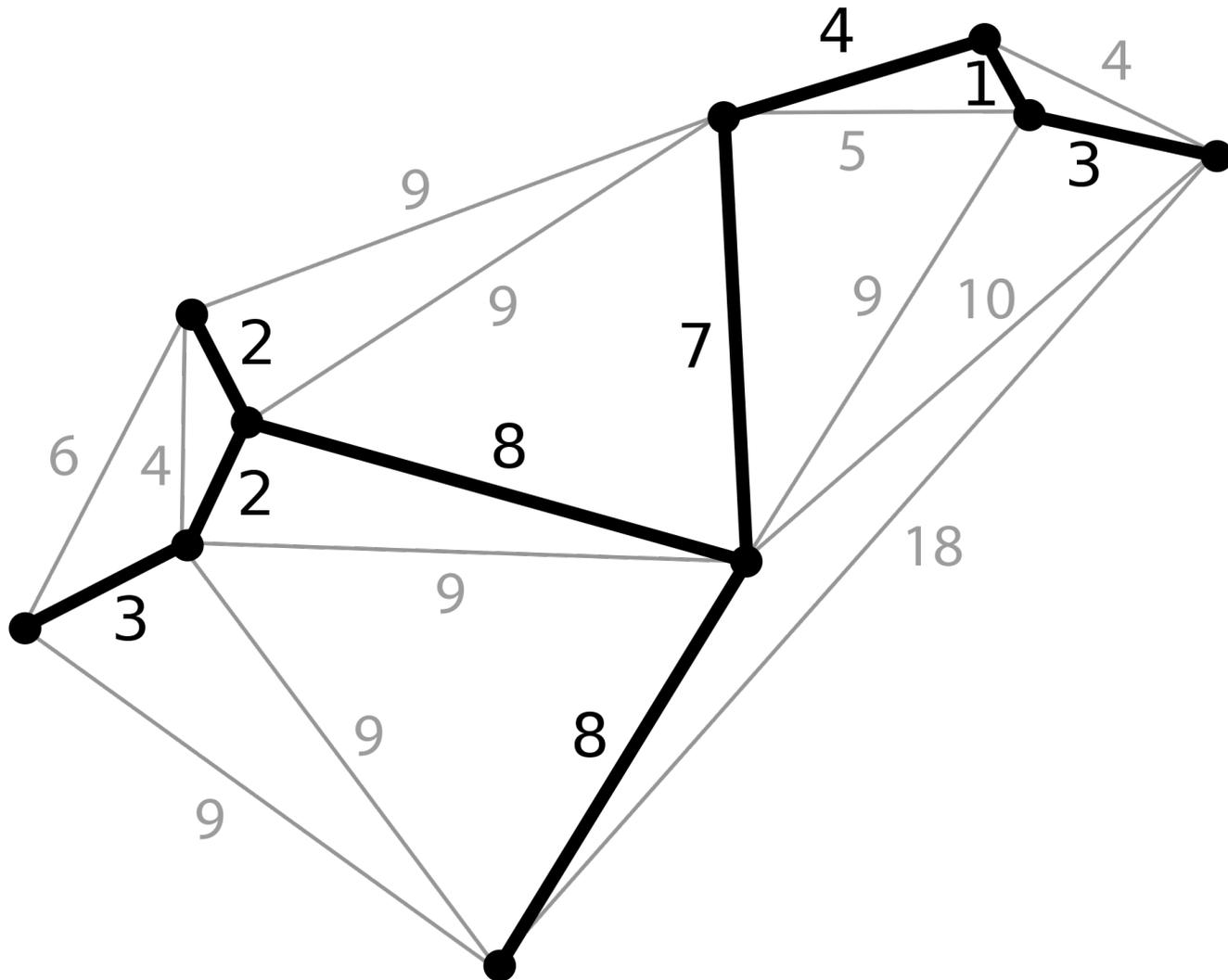
*Periodicamente vengono eliminati dalla tabella gli indirizzi che non hanno comunicato nell'ultimo periodo (pochi minuti).

Problema *Broadcast Storm*: in presenza di maglie nella topologia delle LAN, durante il *flooding* si possono creare dei loop che in pochi attimi bloccano tutti i sistemi connessi in rete.

Soluzione: si integra il learning process con un algoritmo di spanning tree

Spanning tree (albero di ricoprimento): riporta (dinamicamente) una topologia “magliata” ad una topologia ad albero escludendo nel flooding alcune porte

Esempio di *Spanning tree*



Source-routing bridge

Il mittente indica esplicitamente il cammino (sequenza di bridge e reti) che il frame deve percorrere.

Ad esempio la presenza di tali informazioni nel campo **RI** (**Routing Information**) del frame 802.5, è indicata dal valore 1 del bit più significativo dell'indirizzo sorgente. Quindi nelle reti **802.5** il *bridge* *esamina solo i frame che hanno tale bit a 1*

Ogni host memorizza, in una propria ed apposita struttura dati, le informazioni riguardo la topologia delle connessioni.

Quando un host non sa come raggiungere una destinazione, invia un *discovery frame*;

Il *discovery frame*, inviato in *flooding* da ogni bridge a tutti gli altri, raggiunge tutti gli host.

Poiché lungo il percorso ogni bridge aggiunge nel discovery frame il proprio ID, a destinazione il discovery frame contiene l'intero percorso mitt >>> dest.

Quando l'host di destinazione riceve un discovery frame lo reinvia al mittente.

Il mittente, aggiorna le proprie tabelle, inserendovi il path ritornato dal primo discovery frame ricevuto (ritenendolo il più conveniente), quindi invia il frame.

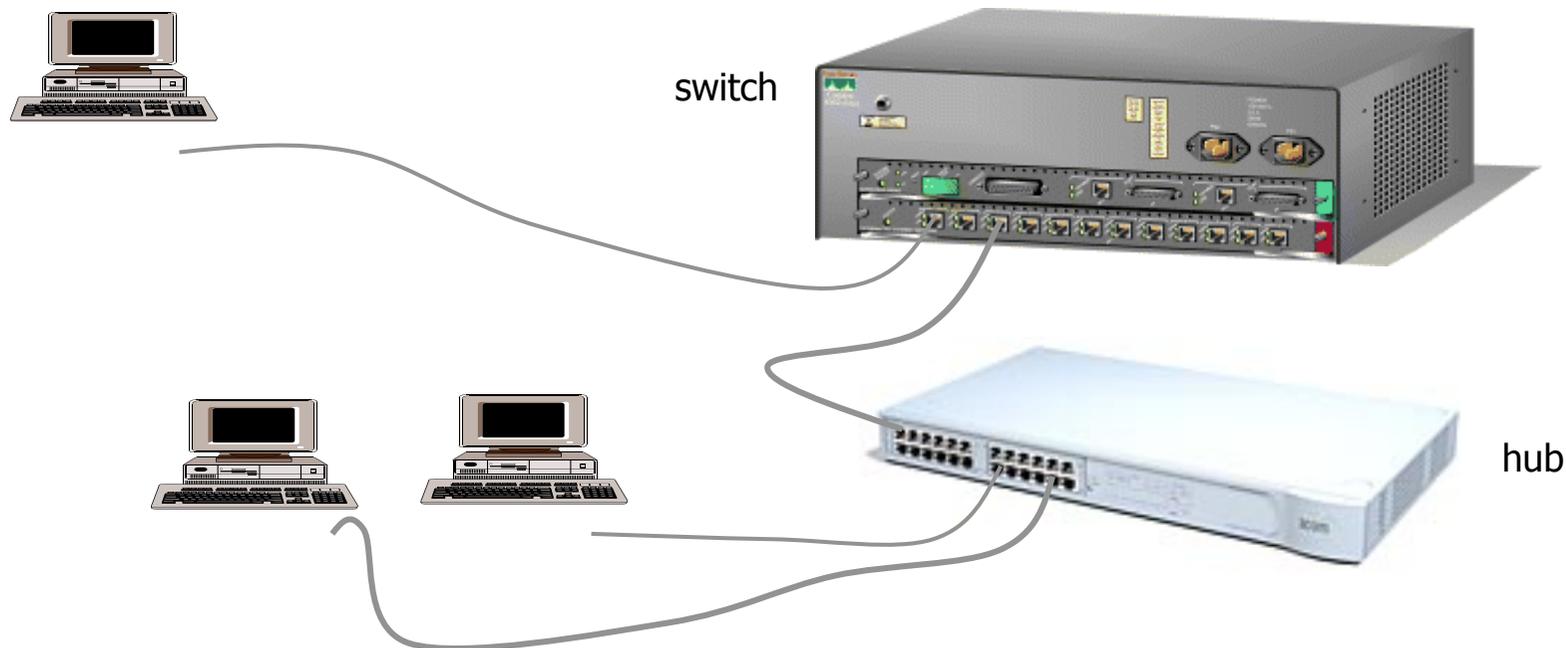
Vantaggio: si trova sempre il cammino ottimo.

Svantaggio: esplosione del numero di discovery frame

Dopo un un primo periodo in cui entrambi gli standard sopra descritti erano abbastanza diffusi, *oggi praticamente tutti i bridge costruiti sono di tipo transparent, ed al più offrono la funzionalità source-routing come un'opzione supplementare.*

Switch

- *Stessa modalità di funzionamento del bridge
- *Ha un numero di porte > 2 (8, 12, 24, ...)
- * Ogni porta può essere collegata a un segmento della rete o a una stazione singola



Tecnologia degli Switch

Shared Memory:

Memorizza i pacchetti in una memoria comune a tutte le porte.

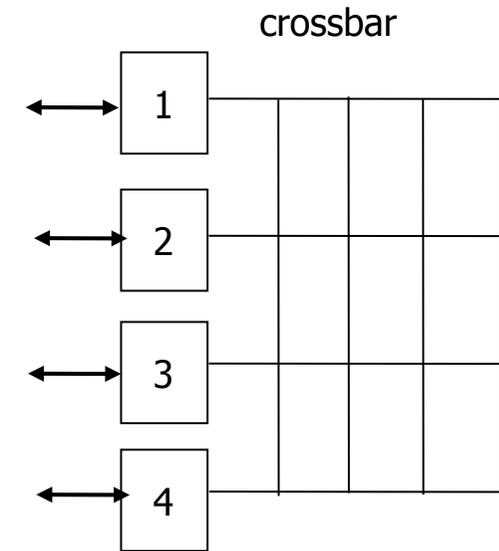
Invia i pacchetti in memoria alla porta destinazione

Matrix

Utilizza una matrice di commutazione

In base all'indirizzo e al contenuto della tabella viene attivata la connessione

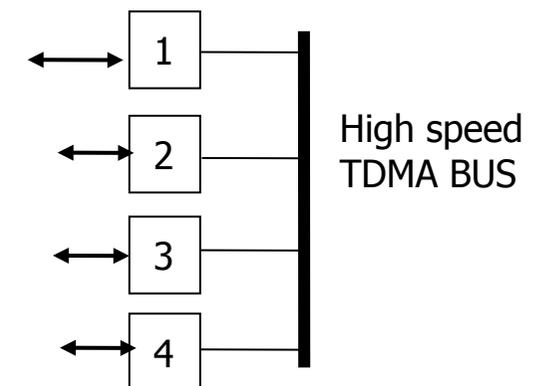
necessaria



Bus-Architecture

Ha un BUS interno condiviso ad alta velocità

La comunicazione interna usa TDMA



Tipi di switch

Cut-through switching

Il frame è subito reindirizzato sulla porta corretta

Store-and-forward

- * Il frame è letto completamente dallo switch
- * Viene controllato il CRC prima di inviarlo
- * In caso di errore il frame è scartato
- * Permette di filtrare il traffico

Port-based switching

Ad ogni porta corrisponde un solo indirizzo Ethernet

Segment-based switching

Ad ogni porta corrispondono più indirizzi (ad esempio è collegata ad un hub)