

## Capitolo 5:

# Le reti locali

Le reti locali (Local Area Networks-LAN) sono reti di telecomunicazione tra entità paritetiche pensate ed ottimizzate per connettere numerosi e differenti tipi di utenti in un'area geografica limitata (un edificio, una fabbrica, un campus). La rete locale di solito appartiene, viene usata e gestita da una singola organizzazione.

Le prime LAN sono nate agli inizi degli anni '70 negli Stati Uniti per soddisfare la crescente richiesta di interconnessione tra computer dalla crescente capacità di calcolo. Fino a quel momento le comunicazioni tra elaboratori erano state di tipo master-slave con un mainframe collegato a numerosi terminali senza capacità di elaborazione autonoma. Le LAN introducono per la prima volta nella comunicazione locale il concetto di colloquio tra entità paritetiche alla base del modello a strati OSI nel quale la risorsa di comunicazione è condivisa tra tutti i computer collegati. Ogni computer collegato ha capacità di elaborazione e lavoro autonome, ma condivide informazioni con gli altri computer e condivide l'uso di risorse preziose come ad esempio stampanti ed altre periferiche.

Le prime reti locali e quelle in esercizio utilizzano un mezzo trasmissivo condiviso. La ragione di questa scelta è legata al fatto che nelle fasi iniziali di sviluppo delle LAN era molto facile in ambito di rete locale avere a disposizione tecniche di trasmissione ad alta velocità e a basso costo, ma non era altrettanto agevole disporre a basso costo di apparati che svolgessero funzioni di nodi di commutazione all'interno di una rete magliata. Per questo motivo la scelta obbligata è stata quella di usare tecniche di trasmissione ad alta velocità su un mezzo trasmissivo condiviso che quindi eliminava la necessità di ricorrere a nodi di commutazione.

Nelle reti locali moderne, le motivazioni che hanno spinto alla definizione di reti senza nodi di commutazione non sono più applicabili in quanto oggi è possibile disporre di apparecchi a basso costo in grado di effettuare la commutazione anche su collegamenti ad alta velocità. Per questo la struttura delle LAN è attualmente in veloce evoluzione, anche se le tecniche di trasmissione e di accesso al mezzo trasmissivo tendono ad essere conservate.

L'utilizzo di un mezzo trasmissivo condiviso richiede che le trasmissioni delle diverse stazioni vengano regolate da opportune procedure di accesso multiplo. All'interno del modello a strati OSI, tali funzioni sono implementate in un sottolivello di accesso (Medium Access Control - MAC) del livello 2 di linea che ha il compito di implementare i protocolli e le procedure atte a regolare l'accesso al mezzo condiviso. Il livello 2 risulta dunque diviso in due sottolivelli: il MAC e il LLC (Logical Link Control) cui sono di solito delegate le funzioni di controllo d'errore e di flusso.



Figura 1: divisione del livello 2 di linea nei sottolivelli MAC ed LLC

Particolare rilevanza nell'ambito delle LAN assumono i primi protocolli per reti locali standardizzati dall'IEEE nel comitato 802 a partire dai primi anni '80. Tali protocolli sono pensati per differenti ambienti e reti fisiche, ma mantengono, per quanto possibile, una struttura comune. La struttura dei protocolli sviluppata dal comitato 802 è mostrata in Figura 2. Il protocollo 802.2 definisce il livello LLC, mentre i protocolli inferiori definiscono diversi protocolli MAC alternativi che vengono usati in reti locali differenti e che possono essere supportati su differenti configurazione del livello fisico. Di particolare interesse sono l'802.3 che definisce il MAC usato nelle reti *ethernet*, l'802.5 che definisce il MAC usato nelle reti *Token Ring*, e l'802.11 che definisce il MAC usato nelle reti locali wireless. Tutti i MAC dello stack 802 usano un indirizzo MAC della lunghezza di 48 bit la cui assegnazione avviene in modo statico (normalmente è memorizzato nella scheda di rete del PC) e univoco a livello mondiale sulla base del costruttore dell'interfaccia di rete. I protocolli della serie 802.1 definiscono delle funzionalità di commutazione per reti locali il cui uso verrà analizzato nella parte finale del capitolo.

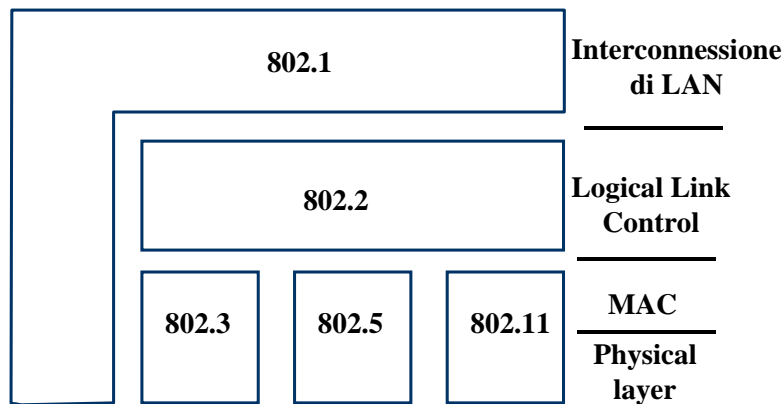


Figura 2: protocolli IEEE 802.x

## 1. Topologia

Nelle reti locali senza nodi di commutazione la topologia definisce il modo nel quale viene configurata la risorsa trasmissiva condivisa dagli utenti. Per tutti i tipi di topologie la rete risulta comunque intrinsecamente broadcast, ovvero un pacchetto trasmesso da una stazione raggiunge sul mezzo condiviso tutte le altre stazioni.

E' opportuno distinguere tra topologia logica delle reti locali e topologia fisica. La prima discrimina il modo nel quale un segnale emesso da una stazione raggiunge tutte le altre, mentre la seconda descrive la reale topologia descritta dai cavi che collegano le stazioni.

Per la topologia logica sono di interesse le topologie a bus, ad anello e a stella.

La topologia a bus (Figura 3) richiede un mezzo trasmissivo intrinsecamente bidirezionale, cioè che ammetta la propagazione del segnale in entrambe le direzioni in modo broadcast. I bus sono realizzati tipicamente con cavi coassiali ai quali le stazioni sono collegati con agganci passivi (*tap*). Il segnale alla fine del bus da entrambe i lati viene assorbito da opportuni *terminatori*. Il bus consente topologie fisiche molto flessibili in relazione alla posizione dei punti di accesso che occorre servire.

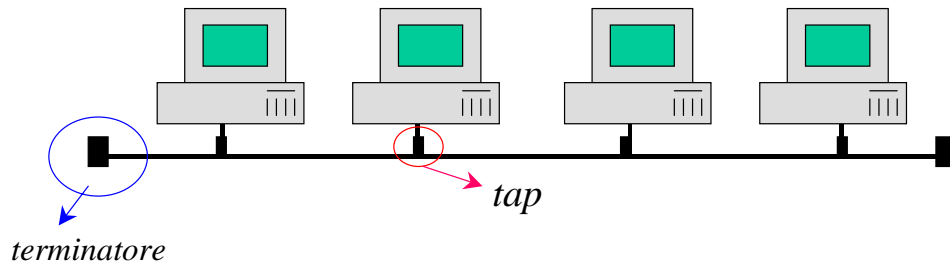


Figura 3: topologia a bus

La topologia ad anello è ottenuta collegando ogni stazione con due vicine in modo da formare un cerchio (Figura 4). La trasmissione nell'anello avviene solo in un verso e quindi i collegamenti usati tra le stazioni sono di tipo monodirezionale. I punti di collegamento tra le stazioni e l'anello, quindi, non sono passivi ma attivi in quanto devono ricevere da un lato il segnale dalla stazione a monte e ritrasmetterlo, rigenerandolo, verso la stazione a valle; i dispositivi che effettuano questa operazione sono detti *repeater*. La topologia fisica adottata nel caso di anello può essere una reale topologia ad anello che attraversa in modo ordinato tutti i punti da collegare oppure può essere di tipo ad anello ripiegato a formare una stella (Figura 5). Quest'ultima configurazione consente di avere una maggiore affidabilità in quanto in caso di cattivo funzionamento da parte di una stazione è possibile la sua immediata esclusione dall'anello mediante l'inserimento di un connettore di bypass.

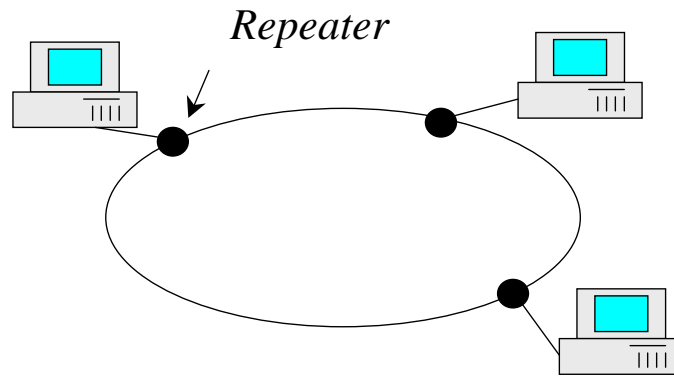


Figura 4: topologia ad anello

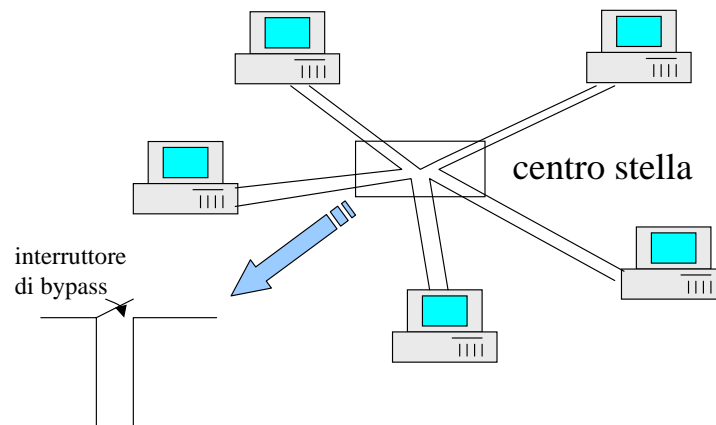


Figura 5: topologia con anello ripiegato a stella

Per la topologia a stella (Figura 6) è necessaria la presenza di un centro stella costituito da un dispositivo attivo in grado di replicare il segnale ricevuto da un ramo verso tutti gli altri. Nell'ipotesi che, come detto, non vi siano dispositivi di commutazione nella rete, il centro stella è costituito da un repeater multiporta che riceve i bit dalle porte e li replica su tutte le altre implementando quindi la rete broadcast a livello fisico. Come si vedrà nel seguito, la topologia a stella è anche la topologia più adatta per una evoluzione della rete che preveda l'uso di elementi di commutazione che sostituiscano il centro stella.

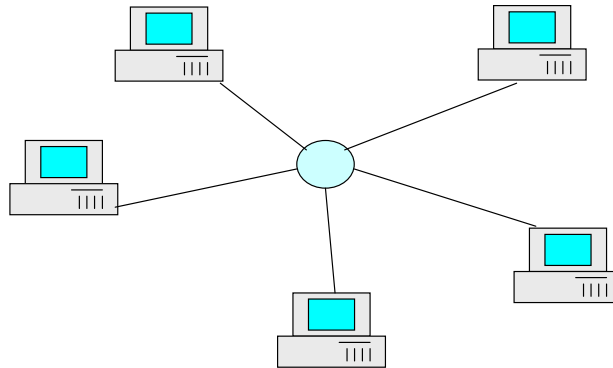


Figura 6: topologia a stella

## 2. Indirizzamento

La funzione di indirizzamento a livello 2 di linea, come già accennato nel capitolo 3, non è strettamente necessaria quando il collegamento è di tipo punto-punto. Al contrario l'indirizzamento è necessario quando sono possibili configurazioni di tipo punto-multipunto.

Le reti broadcast, quali sono appunto le reti locali, ricadono in quest'ultimo caso, e il sotto-livello che si occupa di fare l'indirizzamento è il MAC. Quindi mittente e destinatario devono essere esplicitamente indicati nella trama di livello MAC (MAC-PDU), che viene consegnata a tutti gli utenti connessi alla rete broadcast. Il MAC di questi utenti riceve tutte le trame, ma passa al livello superiore solo quelle che rispondono a determinati criteri di indirizzo. Sono possibili indirizzamenti *unicast* in cui l'indirizzo di destinazione MAC identifica una sola stazione collegata alla rete, *broadcast*, ottenuti con un indirizzo particolare che consente di raggiungere tutte le stazioni collegate, e indirizzi *multicast* che consentono di raggiungere un gruppo di stazioni.

Gli indirizzi MAC vengono chiamati spesso indirizzi fisici, perché associati ai SAP fisici, e per distinguerli dagli indirizzi logici, a livello di rete, che identificano la stazione destinataria di una comunicazione a livello di rete geografica. Benché i due tipi di indirizzi possano coincidere, l'indirizzo fisico nasce esplicitamente con un significato puramente locale e ciò li ha portati ad essere distinti. Tale distinzione, inoltre, porta una grande flessibilità perché gli indirizzi fisici, spesso legati agli apparati, cambiano con gli apparati stessi.

Si noti, infine, che se il livello 2 deve effettuare moltiplicazione, ossia inviare l'informazione che proviene da più SAP di livello 2 in un SAP di livello 1, allora per demoltiplicare in modo corretto occorre anche associare un indirizzo ad ogni SAP di livello 2 (si ricordi la differenza tra TEI e SAPI nell'ISDN). Questo indirizzo può avere significato solo all'interno del nodo dal momento che l'indirizzo globale è rappresentato dall'insieme degli indirizzi dei due SAP.

### 3. Accesso multiplo

I protocolli di accesso multiplo sono lo strumento con cui varie stazioni possono accedere alla rete fisica sottostante che è per ipotesi di tipo broadcast. Tali protocolli hanno come compito quello di regolare la trasmissione delle stazioni in modo tale che non si sovrappongano sul mezzo condiviso.

Nel capitolo 2 si è già presentato il problema dell'accesso multiplo come tecnica per suddividere le risorse in modo statico tra stazioni fisicamente distanti. Il problema dell'accesso multiplo nell'ambito delle reti locali, però, non viene normalmente risolto con tecniche statiche di divisione come ad esempio il TDMA a causa principalmente della natura del traffico presente su tali reti. Tipicamente, infatti, il traffico sulle LAN è molto variabile ed ogni stazione è caratterizzata da periodi di attività nei quali genera pacchetti ad un ritmo sostenuto e periodi di silenzio durante i quali non emette pacchetti. La tecnica TDMA suddivide in modo rigido le risorse tra le stazioni e quindi durante i periodi di silenzio gli slot di una stazioni rimarrebbero inutilizzati, mentre altre stazioni potrebbero averne necessità per smaltire più velocemente i pacchetti in attesa di essere trasmessi (Figura 7).

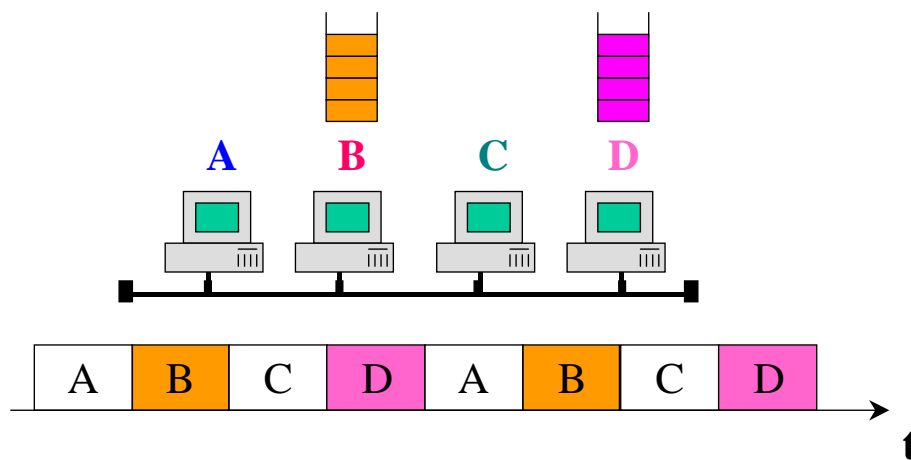


Figura 7: accesso multiplo TDMA con traffico intermittente

Nelle tecniche di accesso multiplo usate nelle reti locali, invece, la suddivisione della risorsa condivisa avviene in modo dinamico e quindi in modo più adatto alle esigenze della modalità a pacchetto con la quale sono gestite le comunicazioni nelle reti locali. Compito, quindi, del protocollo di accesso multiplo è quello di coordinare le trasmissioni delle stazioni che hanno qualcosa da trasmettere per evitare le trasmissioni contemporanee (dette spesso collisioni), o almeno per limitarne l'effetto.

I protocolli di accesso multiplo trovano collocazione nella pila OSI nel sotto-livello MAC. Oltre alla funzione di accesso multiplo, lo scopo del MAC è anche quello di effettuare le funzioni tradizionali di livello 2 richieste dal livello fisico, come per esempio predisporre una trama ed eventualmente un preambolo di sincronismo.

In linea di principio un approccio possibile al problema dell'accesso multiplo è quello di utilizzare un controllore centralizzato in grado di ricevere le richieste di trasmissione e di dare i permessi alle stazioni in funzione delle esigenze ed evitando sovrapposizioni. In questo caso un problema è rappresentato dalla necessità di definire le modalità con le quali le stazioni e il controllore si scambiano le informazioni di servizio (coda piena o coda vuota, permessi di trasmissione, ecc.). Tale informazione di servizio dovrà necessariamente utilizzare il mezzo condiviso stesso per la trasmissione. Anche se questo approccio di tipo centralizzato è potenzialmente in grado di effettuare una efficace gestione della risorsa trasmissiva, non è in pratica usato nelle reti locali a causa della complessità di gestione derivante dalla presenza del controllore centralizzato e dalla scarsa affidabilità in caso di guasti. Questi protocolli centralizzati, però, sono comunemente adottati nei nuovi sistemi di trasmissione dati a pacchetto per sistemi radiomobili (ad esempio nel GPRS, General Packet Radio Service, il servizio dati a pacchetto del GSM).

I protocolli di accesso multiplo comunemente adottati nelle reti locali sono di tipo *distribuito*, ovvero il coordinamento delle trasmissioni avviene mediante processi di decisione effettuati dalle stazioni in base a regole prestabilite.

I protocolli distribuiti sono intrinsecamente più robusti nei confronti di guasti o malfunzionamenti, ma sono realizzabili semplicemente solo se si rinuncia alla conoscenza completa dello stato del sistema (stato delle code, tempi di attesa, ecc.) e si accettano gestioni che possono non essere le migliori. La segnalazione necessaria al coordinamento può essere più schematica che nel caso centralizzato, e l'efficienza del protocollo (massimo grado di utilizzo delle risorse) più alta.

Una importante classificazione dei protocolli di accesso li distingue in protocolli ad *accesso ordinato*, in cui la sequenza d'accesso al canale da parte delle stazioni avviene seguendo regole deterministiche e prevedibili, e in protocolli ad *accesso casuale* nei quali la scelta effettuata da ogni stazione su quando effettuare una trasmissione avviene sulla base di estrazioni casuali e sulla base della conoscenza degli eventi di collisione precedentemente verificatisi sul canale.

### 3.1 Accesso ordinato

Tra le procedure di accesso ordinato, la più semplice e praticamente utilizzata prende il nome di *polling o round-robin*. Il polling è un insieme di protocolli ad accesso ordinato in cui le stazioni ricevono un messaggio di polling, che rappresenta l'abilitazione a trasmettere sul canale, in successione ciclica. Alla fine della sua trasmissione la stazione segnala il rilascio del canale di modo che il messaggio di polling possa essere inviato ad altra stazione.

La procedura di polling usa le risorse trasmissive del sistema stesso, e quindi riduce la banda disponibile per i messaggi di informazione degli utenti.

Nei protocolli distribuiti il passaggio del messaggio di polling avviene da una stazione alla successiva, ma possono essere necessarie procedure che impediscano che la catena del passaggio del messaggio si interrompa a causa di malfunzionamenti.

Il messaggio di polling può essere un messaggio indirizzato alla stazione successiva nella catena. Ma, se il canale è sequenziale, ossia prevede già un ordinamento fisico fra le stazioni come nel caso della topologia ad anello, allora il passaggio del controllo può non essere esplicitamente indirizzato. Basta, infatti, un solo simbolo logico, spesso chiamato *token*, che venga fermato dalla stazione che ne ha bisogno e poi rilasciato verso la successiva.

Fra le caratteristiche logiche dei sistemi di polling una molto importante riguarda il tempo di servizio, ossia il tempo consecutivo per cui una stazione può tenere il token prima di rilasciarlo. Se non esistono limiti a tale tempo allora si parla di *servizio esaustivo*. Altrimenti si parla di *servizio limitato* e *k-limitato* se si consente la trasmissione di  $k$  pacchetti consecutivi prima di rilasciare il controllo.

Anche se l'accesso ordinato ha come pregio quello di consentire un perfetto coordinamento tra le stazioni senza possibilità di sovrapposizione nelle trasmissioni, ha anche problemi legati all'efficienza nel caso di reti con molte stazioni che generano poco traffico in modo molto intermittente. Si immagini che nell'accesso venga coinvolto un grande numero  $M$  di stazioni e che il traffico fornito da ciascuna di queste sia costituito da pacchetti estremamente rari. Come risultato, ad ogni istante il numero di stazioni che ha qualcosa da trasmettere è solo una piccola frazione del totale. In questo caso quello che accade è che il token viene passato tra un gran numero di stazioni che non ne hanno bisogno, e quindi la risorsa trasmissiva viene sprecata per questo inutile passaggio di token tra stazioni che non hanno pacchetti da trasmettere. Di conseguenza l'efficienza può divenire molto bassa e i tempi di attesa delle poche stazioni che devono trasmettere molto elevati.

## 3.2 Accesso casuale

L'accesso casuale nasce per evitare, o in qualche modo limitare, gli effetti negativi dell'accesso ordinato nel caso di stazioni numerose e con basso traffico. Come caratteristica base si accetta il fatto che, a seguito della mancanza di coordinamento, stazioni diverse possano trasmettere in modo tale che le loro trasmissioni vengano a sovrapporsi, anche parzialmente, al ricevitore (*collisioni*).

In caso di collisione viene qui fatta l'assunzione che i pacchetti vadano tutti distrutti. Questa assunzione è ben verificata nel caso di reti cablate, mentre può non essere vera per reti wireless. I pacchetti collisi devono venire in qualche modo scoperti e ritrasmessi. Le assunzioni e le regole che sovrintendono a tali procedure sono appunto i protocolli d'accesso casuale.

Le informazioni su cui il protocollo opera possono essere molteplici. L'informazione minima è quella del riscontro (ACK) dell'avvenuta corretta ricezione. Il riscontro può essere fornito da osservazione diretta (ad esempio nel caso di canale broadcast o con eco) o indiretta (è il ricevente che segnala la corretta ricezione). Altre informazioni tipiche sono quelle fornite dal cosiddetto *feedback di canale*, che sono le informazioni che una stazione può ottenere da un'osservazione, più o meno articolata, del canale.

### 3.2.1 ALOHA

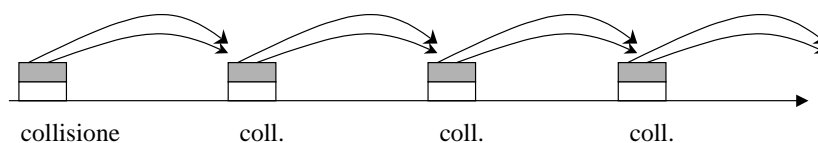
È il protocollo più semplice e fa a meno di ogni forma di coordinamento fra le stazioni. Come informazione di servizio necessita solo del riscontro dell'avvenuta corretta trasmissione, solitamente supposta ottenuta dalla stazione ricevente, e viene perciò classificato come protocollo "senza feedback di canale".

Le regole del protocollo possono essere così schematizzate:

- ✓ i pacchetti nuovi vengono trasmessi appena generati.
- ✓ i pacchetti collisi vengono ritrasmessi dopo un tempo  $X$  variabile casuale di opportune caratteristiche

La seconda regola è evidentemente dettata dalla necessità di evitare che due stazioni che hanno colliso continuino a ricollidere nella ritrasmissioni successive. Leggi deterministiche di trasmissione (ritrasmettere subito, dopo un tempo fisso, ecc.), portano inevitabilmente al ripetersi della situazione di collisione (Figura 8).

ritrasmissione dopo un tempo fisso  $t$ :



ritrasmissione dopo un tempo casuale  $T [t, 2t]$ :

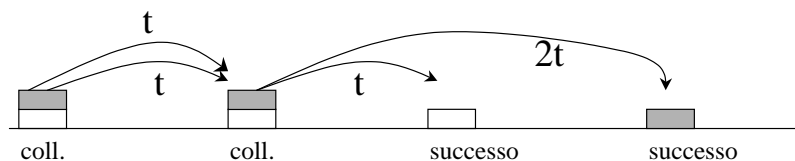


Figura 8: modalità di ritrasmissione in ALOHA

Sicuramente le prestazioni in termini di efficienza del sistema dipendono dalla frequenza con la quale si presentano le trasmissioni. Qui di seguito viene presentata una semplice valutazione delle prestazioni del protocollo sotto ipotesi molto semplificate.

Si assuma che il processo del traffico di canale, ossia il processo puntuale dell'inizio delle trasmissioni che si possono osservare sul canale, sia assimilabile ad un processo di Poisson<sup>1</sup> la cui frequenza è indicata con  $G$  trasmissioni nell'unità di tempo  $T$ , pari al tempo di trasmissione dei pacchetti supposti di lunghezza costante.

La probabilità che un pacchetto venga trasmesso senza essere disturbato da altri è pari alla probabilità che nessun altro pacchetto venga trasmesso  $T$  secondi prima e  $T$  secondi dopo l'inizio della trasmissione del pacchetto in oggetto (in caso contrario le trasmissioni si sovrapporrebbero come mostrato in Figura 9).

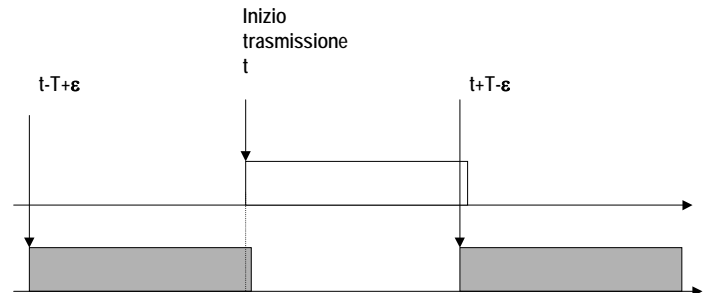


Figura 9: sovrapposizione delle trasmissioni in ALOHA

Per l'assunzione sul processo di Poisson sul traffico, la probabilità che una trasmissione non venga interferita da altre è data dalla probabilità che nell'intervallo  $2T$  non vi siano altre trasmissioni e quindi:

$$P_s = e^{-2G} \quad (1)$$

Il numero medio di pacchetti trasmessi con successo in un intervallo di tempo  $T$  risulta allora essere:

$$S = Ge^{-2G} \quad (2)$$

Tale valore definisce quello che viene indicato come *throughput* del sistema, espresso appunto in pacchetti trasmessi nell'unità di tempo  $T$  (varia quindi tra 0 e 1).

L'analisi della curva riportata in Figura 10 mostra che il massimo throughput trasportato è  $1/2e=0.1839$  pacchetti per tempo  $T$  in  $G=1$ , ma soprattutto che la curva non cresce monotonicamente e che al crescere di  $G$  scende asintoticamente a zero.

Si noti che l'ipotesi alla base del modello, prima ancora di assumere la distribuzione di trasmissioni e ritrasmissioni assume che queste costituiscano un processo stazionario a media  $G$ . Resta da vedere se  $S$  nuove trasmissioni per tempo  $T$  originano un processo che unito alle ritrasmissioni si stabilizza nel processo stazionario ipotizzato. Quest'analisi è fuori dagli scopi di queste dispense, ma occorre sottolineare che l'ipotesi non è verificata se non si adottano opportuni meccanismi di ritrasmissione che rendano il processo sul canale effettivamente stazionario.

In alternativa all'ALOHA puro si può assumere un parziale coordinamento fra le stazioni, consistente nel sincronismo dei possibili istanti di trasmissione, che distano  $T$  (*slotting* del tempo). Le stazioni dunque hanno in comune un riferimento temporale e possono trasmettere solo iniziando al tempo  $0, T, 2T, \dots$  Tale protocollo è detto *slotted-ALOHA* e per il resto delle regole opera come l'ALOHA puro.

Appare chiaro che il sincronismo evita il caso di sovrapposizioni parziali delle trasmissioni e quindi la collisione si ha solo se altri pacchetti partono nello stesso istante del pacchetto scelto. Dunque, col modello semplificato visto prima, la probabilità di non avere collisione è data da:

<sup>1</sup> E' utile richiamare le nozioni di base sui processi di Poisson. La probabilità che ci sia un punto di Poisson in un intervallo infinitesimo  $dt$  è pari a:  $P[n(t,t+dt)=1]=\lambda dt$ , dove il parametro  $\lambda$  rappresenta la frequenza del processo (in punti per unità di tempo). La probabilità che ci siano più punti in un intervallo infinitesimo  $dt$  è nulla  $P[n(t,t+dt)>1]=0$ . Il numero di punti presenti in intervalli di tempo disgiunti sono variabili causali indipendenti. La probabilità che vi siano  $k$  punti di Poisson in un intervallo temporale  $\tau$  è pari a:

$$P[n(t,t+\tau) = k] = \frac{(\lambda\tau)^k}{k!} e^{-\lambda\tau}$$



$$P_s = e^{-G} \quad (3)$$

e quindi il throughput:

$$S = Ge^{-G} \quad (4)$$

Il massimo throughput è questa volta  $1/e = 0.3678$ , (Figura 10) raddoppiato rispetto al precedente caso. Resta però sempre il problema della stazionarietà del processo di traffico sul canale e quindi della stabilità del protocollo.

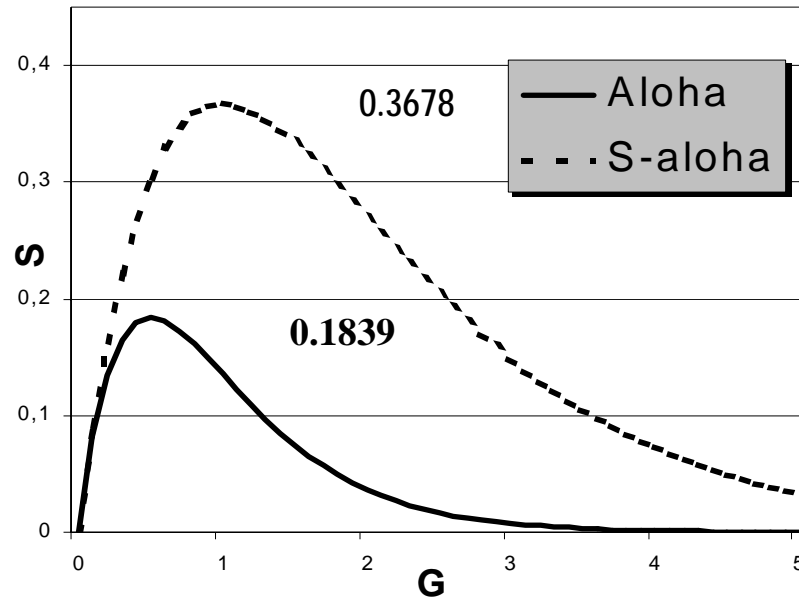


Figura 10: curve S-G per ALOHA e slotted-ALOHA

### 3.2.2 CSMA e CSMA-CD

Il Carrier Sensing Multiple Access (CSMA) è il protocollo che direttamente deriva dall'ALOHA base, con l'aggiunta del feedback che riguarda l'occupazione del canale stesso. Lo strumento che rivela l'occupazione del canale viene chiamato *Carrier Sensing* e dà il nome al protocollo.

L'operazione del CSMA consiste nel monitorare il canale e nell'astenersi da ogni trasmissione se il Carrier Sensing indica che il canale è già occupato. Se il canale è libero il protocollo agisce come l'ALOHA e trasmette appena pronto il messaggio. In caso di collisione, viene effettuato un nuovo tentativo dopo un ritardo casuale. Si noti che nonostante l'ascolto del canale le collisioni sono ancora possibili se il tempo di propagazione fra una stazione e l'altra ( $\tau$ ) è maggiore di 0, come avviene in pratica. Ciò è mostrato in Figura 11 dove sono indicate le attività del canale come viste dal Carrier sense di due stazioni poste a una distanza corrispondente ad un ritardo di propagazione di  $\tau$ . Con riferimento alla trasmissione effettuata in una stazione, si vede che esiste un *periodo di vulnerabilità* nel quale le altre stazioni a distanza  $\tau$  sono "cieche". Queste non possono aver trasmesso prima di questo periodo perché altrimenti la prima stazione avrebbe visto il canale occupato e non avrebbe trasmesso. Non possono nemmeno trasmettere dopo questo periodo perché la trasmissione della prima stazione arriva e alza il Carrier Sense. Ma il protocollo non può impedire trasmissioni durante il periodo vulnerabile, e ciò rende dunque le collisioni possibili.

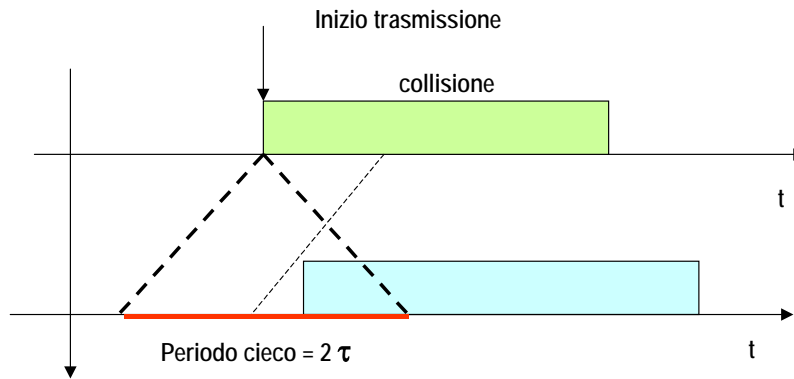


Figura 11: periodo di vulnerabilità del CSMA

E' intuibile, dunque, che le prestazioni del protocollo dipendano dal valore di  $\tau$  e migliorano al decrescere di questo (per  $\tau=0$  non si avrebbero collisioni ed il throughput massimo potrebbe raggiungere il 100%). Si può far vedere che in realtà il parametro che influenza le prestazioni è il rapporto  $a=\tau/T$ , con  $T$  tempo di trasmissione del pacchetto. E' chiaro comunque che nel caso estremo di  $\tau=T/2$  il Carrier Sense non può dare informazioni e le prestazioni non possono che essere pari o peggiori di quelle dell'ALOHA.

Riguardo al meccanismo base CSMA sono possibili diverse varianti:

- ✓ *non-persistent CSMA*: quando, al momento individuato per la trasmissione o ritrasmissione, il canale è sentito occupato dal Carrier Sense, la trasmissione viene rimandata a un nuovo tempo scelto in modo casuale, come nel caso di una collisione.
- ✓ *persistent CSMA*: quando, al momento individuato per la trasmissione o ritrasmissione, il canale è sentito occupato dal Carrier Sense, la trasmissione viene trattenuta finché il canale viene sentito libero e da questo momento viene rilasciata.

Esistono poi le varianti chiamate *p-persistent* in cui, quando al momento della trasmissione o ritrasmissione il canale è sentito occupato, la modalità di funzionamento persistent viene applicata con probabilità  $p$  e con  $1-p$  si usa la modalità non-persistent.

Le prestazioni di un tale sistema nel caso non-persistent possono essere valutate utilizzando il modello semplificato già usato per l'ALOHA. Tuttavia le prestazioni dipendono dalla topologia delle varie stazioni connesse al bus. Un caso semplice è quello di un sistema a topologia stellare (nei riguardi della propagazione del segnale) in cui tutte le stazioni distano egualmente dal centro stella e in cui  $\tau$  denota il tempo di propagazione da una stazione all'altra, uguale per tutte le coppie.

Utilizziamo di nuovo come unità il tempo  $T$  di trasmissione di un pacchetto e indichiamo con  $G$  il numero medio di trasmissioni e ritrasmissioni, supposte di Poisson, in un tale tempo unitario. Si dimostra che il throughput  $S$  è dato da:

$$S = \frac{Ge^{-aG}}{G(1+2a) + e^{-aG}} \quad (5)$$

Le curve di throughput per diversi valori di  $a$  sono riportate in Figura 12. Si vede che il massimo valore di throughput sale al decrescere di  $a$ , come ovvio, ma che in ogni caso, al crescere di  $G$  il throughput tende a zero. Ciò suggerisce, come già nel caso ALOHA, che un protocollo di tal genere sia instabile, anche se l'instabilità ha effetti diversi al variare di  $a$ .

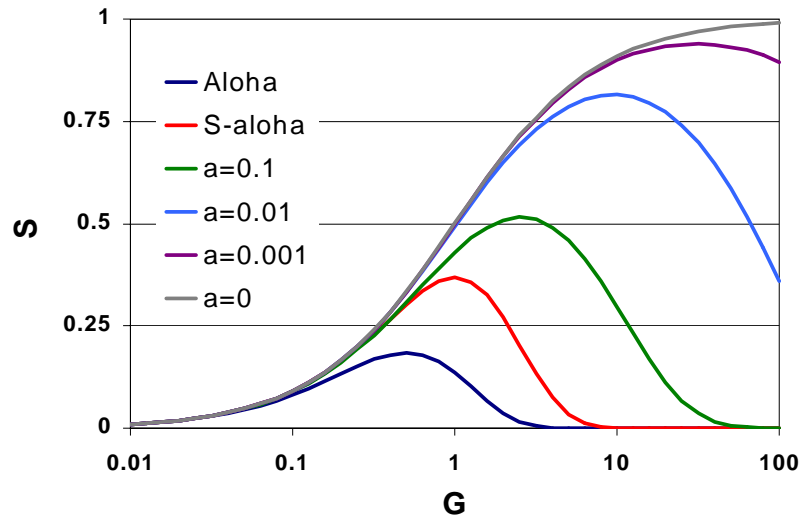


Figura 12: curve S-G del CSMA confrontate con quelle dell'ALOHA al variare del parametro  $a$

Il protocollo CSMA ha lo svantaggio di sprecare tutto il tempo di trasmissione quando una collisione è in atto. In alcuni casi è possibile avere un rivelatore di collisioni quando la trasmissione è ancora in corso (Collision Detection (CD)). In questo caso, appena scoperta una collisione, la trasmissione viene abortita. Una variante di questo genere prende il nome di CSMA-CD (Carrier Sense Multiple Access with Collision Detection).

Dal punto di vista pratico, per come è operativamente fatto il rivelatore di collisioni, può essere necessario continuare la trasmissione per un tempo  $\delta < 1$  dopo la scoperta di una collisione. Ciò per permettere a tutte le stazioni di verificare con sicurezza una collisione. Evidentemente, se fosse  $\delta=1$  si ritorna all'efficienza del CSMA.

Anche con questo protocollo sono possibili le diverse versioni già viste per il CSMA, a titolo di confronto viene data l'espressione del throughput del solo caso non persistente col modello semplificato e con la topologia stellare già usata per il CSMA:

$$S = \frac{Ge^{-aG}}{G(1+2a) + e^{-aG} - G(1-\delta)(1-e^{-aG})} \quad (6)$$

Le curve di throughput sono simili a quelle già viste per il CSMA, ma a pari valori di  $a$  hanno il massimo più alto, più piatto e più spostato verso destra, mostrando una stabilità accresciuta. In Figura 13 è mostrato il throughput massimo in funzione di  $a$  nel caso più favorevole in cui  $\delta=0$ .

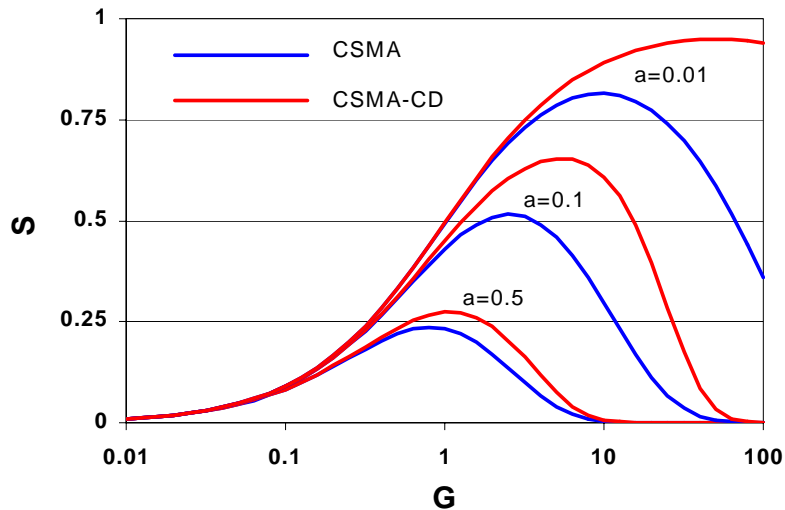


Figura 13: curve S-G del CSMA-CD al variare del parametro  $a$  confrontate con quelle del CSMA

#### 4. Il livello LLC 802.2

La trama LLC del protocollo 802.2 è mostrata in Figura 14 ed è praticamente derivata da quella dello HDLC, senza gli indicatori di trama e FCS, e con l'aggiunta di un ulteriore campo di indirizzamento. E' a questo sotto livello che è demandato l'eventuale ARQ, il set-up della eventuale connessione e le altre funzionalità tipiche del livello 2 ma non svolte dal MAC..

I campi di indirizzo LLC servono per moltiplicare e demoltiplicare fra i loro diversi SAP che lo standard ha destinato come accessi a diversi tipi di protocolli che usano il LLC, sia protocolli di rete che di servizio. Ecco per esempio alcune corrispondenze in esadecimale:

- ✓ [02] Individual LLC sublayer Management
- ✓ [06] Internet Protocol
- ✓ [42] il protocollo 802.1d (MAC bridge)

I servizi operativi, e le conseguenti primitive di servizio, definiti sono di tre tipi. Il tipo 1 prevede trasferimenti senza connessione (datagram) e senza riscontro ed è quello normalmente utilizzato nelle architetture TCP/IP. Questo tipo di servizio è favorito dal fatto che le moderne reti locali presentano una piccolissima probabilità d'errore, per cui ha poco senso caricare il LLC con servizi di acknowledgment dal momento che è sempre presente un controllo d'errore fra utenti finali. Si noti che con questo tipo servizio, il servizio vero e proprio del livello LLC si limita ad identificare i SAP.

Il servizio di tipo 2 prevede trasferimenti a connessione derivati dalla modalità ABME dell'HDLC. I controlli di sequenza d'errore sono quelli dell' HDLC.

Il servizio di tipo 3 prevede trasferimenti senza connessione (datagram) ma con riscontro. E' una modalità pensata per protocolli da utilizzarsi in ambito fabbrica.

1	1	1 o 2	variabile
SAP sorgente	SAP destinaz.	controllo	dati

Figura 14: trama del protocollo 802.2

## 5. Le reti Ethernet e il protocollo 802.3

Il protocollo 802.3 è lo standard IEEE che deriva dalla rete Ethernet. La versione standard del protocollo e la versione Ethernet presentano delle piccole differenze che verranno evidenziate in seguito. La velocità di trasmissione è pari a 10 Mbit/s nella versione base del protocollo.

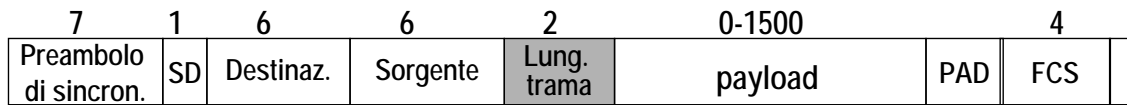
Il protocollo d'accesso utilizzato è una variante del CSMA-CD 1-persistent, nota come *truncated binary exponential backoff*, che funziona come segue. Viene definito uno *slot time* corrispondente a 512 bit, che è la base dei tempi del protocollo e che corrisponde anche al pacchetto più piccolo trasmissibile. Questo asse dei tempi discreto ha solo importanza locale e non richiede la sincronizzazione fra le stazioni. Se al momento della richiesta di trasmissione il canale è libero si trasmette. Altrimenti, si attende la discesa del Carrier Sense e quindi si trasmette. Se da questo istante il Collision Detect (CD) segnala collisione si abortisce la trasmissione, si trasmette una sequenza di *jamming* lunga 32 bit per rafforzare la collisione cosicché tutti la sentano bene, e si inizia la procedura di ritrasmissione. Questa consiste nello scegliere un numero intero  $r$  di slots trascorso il quale la procedura viene ripetuta. Il numero  $r$  è scelto uniformemente nell'intervallo  $0 \leq r \leq 2^k$ , dove  $k$  è posto a zero all'inizio di ogni nuova procedura ed incrementato di uno ad ogni fallimento fino al raggiungimento di un massimo valore pari a 10. Sono ammessi 16 tentativi di trasmissione, dopodiché il MAC segnala al LLC il fallimento della trasmissione.

La filosofia che ispira questo protocollo è quella della rapidità, da qui la scelta della modalità 1-persistent. Il numero crescente di tentativi falliti indica però affollamento di trasmissioni sul canale e l'aumento del campo di  $r$  è un tentativo di ridurlo. E' stato dimostrato che, anche qualora la legge esponenziale di aumento del backoff crescesse senza il vincolo di  $k=10$ , il protocollo sarebbe perfettamente stabile.

La lunghezza dello slot coincide con il parametro  $2\tau$  tipico delle reti CSMA che vincola la massima distanza end-to-end fra due stazioni. Infatti la condizione affinché pacchetti di lunghezza minima che collidono vengano visti collisi da ogni posizione in rete è che sia  $T > 2\tau$ , ossia  $a < 0.5$ . Alla velocità del segnale pari a  $2 \times 10^8$  m/s e alla frequenza di 10 Mbit/s la distanza  $2\tau$  percorsa in un tempo di slot vale  $d = (2 \times 10^5 \times 512) / 10^7 \approx 10$  km. Poiché la durata dello slot è il massimo tempo di andata e ritorno ammesso, ne segue che il diametro massimo della rete è pari alla metà, ossia 5 km. In pratica questo valore viene dimezzato dal momento che i ritardi che giocano non sono solo quelli di propagazione ma anche quelli di attraversamento delle varie unità hardware quali i trasmettitori ed i ripetitori.

Il formato della trama MAC è mostrato in Figura 15 insieme col formato della trama Ethernet da cui lo standard IEEE deriva. Quest'ultimo è tuttora utilizzato, nelle schede standard, per supportare ad esempio il protocollo di rete IP.

## 802.3



## Ethernet

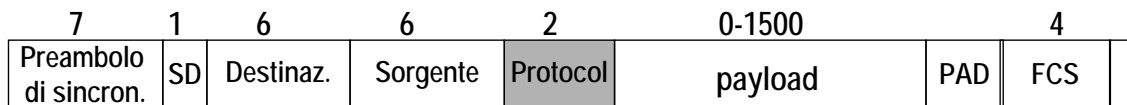


Figura 15: formato delle trame MAC di 802.3 e di Ethernet

La codifica di linea utilizzata è la codifica Manchester che rappresenta il simbolo 0 con una transizione dal livello alto a quello basso e il simbolo 1 con una transizione dal livello basso a quello alto (Figura 16). Il campo SD (Start Delimiter) è una particolare sequenza che viola il codice di linea (Manchester) per indicare in modo inequivocabile l'inizio della trama.

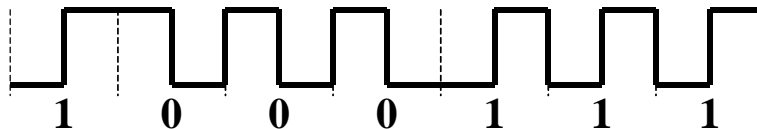


Figura 16: codifica Manchester

Il campo di lunghezza di trama specifica la lunghezza del campo dati mentre il campo PAD viene appeso solo quando occorre portare la lunghezza della trama alla lunghezza minima pari a 64 byte. La massima lunghezza ammessa è di 1518 byte (preambolo e SD esclusi). Nel protocollo Ethernet non vi è un livello LLC superiore e il campo lunghezza di trama è sostituito dal campo protocol che indica l'indirizzo del SAP del livello di rete superiore (IP, IPX, ecc.). In molte reti i due protocolli convivono e quindi per consentire il riconoscimento i valori che il campo protocol può assumere partono da quello che rappresenta la massima lunghezza di trama. In questo modo se il campo contiene un valore fino a 1512 definisce un campo lunghezza dell'802.3 se invece contiene valori superiori definisce il campo protocol di Ethernet.

Viene inoltre definito un tempo di guardia di 9.6  $\mu$ s a partire dall'ultima trasmissione osservata, durante la quale il Carrier Sense (CS) continua a segnalare la presenza di portante; ciò ha lo scopo di separare i pacchetti sul canale anche nel caso di trasmissione di una sequenza di pacchetti.

Il livello fisico ammette dei *repeater* che hanno lo scopo di connettere i cablaggi fisici in modo da estendere il raggio della rete fino al limite consentito dallo standard. Oltre a copiare le trame ricevute su una porta su tutte le altre, i repeater svolgono anche altre funzioni necessarie al funzionamento trasparente della LAN. Fra queste

- ✓ rigenera il preambolo, mangiato durante l'acquisizione del sincronismo, e lo SD, introducendo così un ritardo
- ✓ propaga le collisioni scoperte su una porta inviando una sequenza di jamming su tutte le altre porte;
- ✓ riporta i segnali fisici che non rispettino i vincoli di lunghezza agli stessi vincoli;
- ✓ può escludere porte in cui si presentino troppe collisioni.

Poiché i repeater non fanno commutazione e non hanno bisogno di leggere i campi della trama, il ritardo che introducono è molto limitato e per lo più dovuto alla necessità di ricostruire il preambolo di sincronizzazione.

La configurazione topologica e fisica delle prime reti Ethernet era a bus con il mezzo trasmissivo costituito da un cavo coassiale. Tra queste configurazioni ricordiamo la 10BASE2 e la 10BASE5 dove il "10" indica la velocità in Mbit/s, la sigla BASE indica la trasmissione in banda base e l'ultimo numero la massima dimensione della rete in centinaia di metri.

Particolarmente usata oggi è la configurazione fisica su doppino di classe 3, indicata con la sigla 10BaseT, e topologia a stella a più livelli (detta ad albero), dove gli utenti costituiscono le foglie e i repeater multiporta, detti *hub*, i nodi (Figura 17). I repeater di livello più basso presentano una porta per ogni utente cui sono collegate. Possono esserci configurazioni miste nelle quali i repeater possono avere anche porte su coassiale o su fibra. La massima lunghezza del segmento è di 100 m ed il numero di repeater in cascata (livelli dell'albero) sono limitati a quattro. Il cavo tipico è costituito da un cavo UTP a 4 coppie di cui la LAN ne usa solo 2, una per trasmettere e una per ricevere. Con questa configurazione di cablaggio il funzionamento fisico potrebbe anche essere full duplex (trasmissione e ricezione contemporanea), ma il funzionamento del CSMA-CD lo impedisce perché ci sarebbero comunque collisioni sulle altre porte dei repeater. Dunque il segnale di collisione è comunque attivato quando si riceve un segnale mentre si sta trasmettendo.

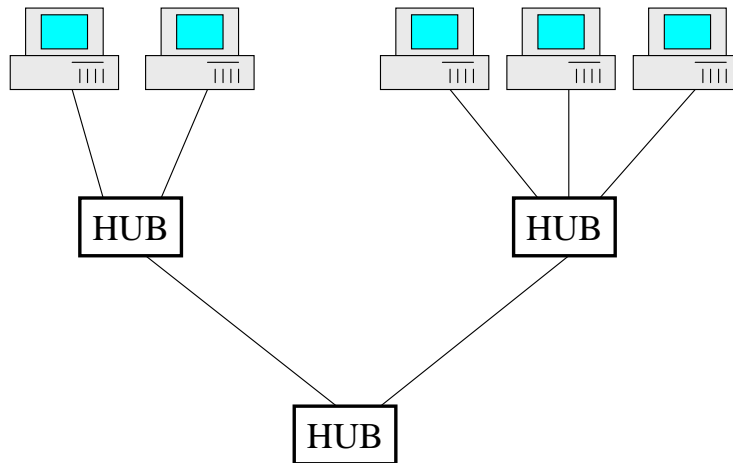


Figura 17: topologia ad albero per il 10BASET

Esiste anche la possibilità di usare fibre ottiche (10BaseF).

Recentemente il protocollo 802.3 è stato esteso per ottenere velocità in linea di 100 Mbit/s, con i vincoli però che la trama MAC e le regole che la determinano restassero le stesse in modo da facilitare l'interoperabilità fra spezzoni di rete a velocità diverse.

Poiché, come detto, il protocollo d'accesso CSMA-CD impone un rapporto costante fra il tempo di trasmissione della minima trama e il massimo ritardo di propagazione sulla rete, riducendosi il primo per via dell'aumento di velocità di linea occorre ridurre anche il secondo. Dunque, anche con solo uno spezzone di rete a 100 Mbit/s, la rete totale non può superare un'estensione massima di circa 250 m, cosa accettabile visto che comunque anche la 10BaseT prevede tratte d'utente non più lunghe di 100 m. Naturalmente, una tale variazione di velocità cambia pesantemente lo strato fisico. Questo standard ha due varianti, la prima 100Base4T prevista per funzionare con i vecchi cavi di categoria 3 adatti alla 10BaseT, e la seconda, 100BaseX prevista per cavi di categoria 5 e fibra (100BaseTX e 100BaseFX).

Nello standard il livello fisico viene suddiviso in due sottostrati in cui quello più basso, il Physical Medium Dependent (PMD) sublayer, cambia con il mezzo usato ma presenta un'interfaccia con lo strato superiore indipendente dal mezzo. Il sottostrato più alto utilizza questa interfaccia per trasformare i segnali come quelli che si aspetta il MAC CSMA-CD e viene chiamato Convergence Sublayer.

La variante 100Base4T utilizza tutti e quattro i doppini presenti nel cavo. I primi due sono usati per trasmissione dati in modo unidirezionale (simplex) e per collision detect come nello 10BaseT, mentre gli altri due, non usati nel precedente standard, sono usati insieme per trasmissione dati in modo half-duplex (come il coassiale). Dunque la trasmissione dati avviene su tre coppie in parallelo, riducendo la velocità su ciascuna coppia a 33.3 Mb/s. Tuttavia va cambiato anche lo schema di codifica di linea, dato che col Manchester encoding la velocità risulta ancora troppo alta per doppini di categoria 3. Si ricorre a una codifica di linea chiamata 8B6T, che traduce otto simboli binari in 6 simboli ternari, riducendo la velocità in linea a 25 Msimboli/s. Il meccanismo è alquanto complesso e non viene ulteriormente descritto in queste dispense.

Nel 100BaseX, dove il mezzo non è vincolante rispetto alla velocità, la codifica è di tipo 4B5B che trasforma gruppi di 4 bit in codifica a 5 bit.

Alla fine del 1998 è giunto a conclusione il lavoro di definizione del protocollo 802.3z, noto come Gigabit Ethernet, in cui, come dice il nome, le funzionalità dello 802.3 sono state estese alla velocità di 1 Gb/s. Il nuovo standard prevede sia il funzionamento tipico CSMA-CD su mezzi di tipo condiviso basato su una configurazione a stella e su repeater, sia un tipo di funzionamento punto-punto full duplex che non presenta problemi di accesso. Quest'ultimo tipo di funzionamento è previsto per connettere fra loro nodi di commutazione di livello 2 (bridge). Per ora lo standard prevede il funzionamento su un livello fisico che usa fibre ottiche, multimodo e monomodo, e cavo schermato. In futuro è prevista l'estensione dello standard a cavo UTP di categoria 5.

Per evitare di ridurre ulteriormente il massimo diametro consentito per la rete, che mantenendo le regole della rete a 10 e 100 Mb/s si ridurrebbe a 20 m., si è deciso di mantenere le dimensioni della rete a 100 Mbit/s e di aumentare di 10 volte la dimensione della trama di lunghezza minima. Ciò complica la connessione di spezzoni a velocità diversa a livello 2, in quanto i bridge dovrebbero riformattare completamente la trama. Ad evitare il problema si è trovata un'ingegnosa soluzione, ossia la tecnica nota come *carrier extension*.

La soluzione consiste nell'aumentare la dimensione dello slot, ossia la minima lunghezza in cui è presente attività di trasmissione sul canale, da 512 bit a 512 byte, ma mantenendo la minima lunghezza di trama di 512 bit. Se alla fine della trasmissione della trama questa risulta di lunghezza inferiore a 512 byte, si continua la trasmissione con una sequenza particolare di simboli di canale, noti come Carrier Extension (CE) fino a che la minima lunghezza dello slot viene raggiunta.

Naturalmente, la soluzione trovata non può evitare una forte perdita di efficienza quando le trame da trasmettere siano di lunghezza minima.

## 6. Le reti Token Ring 802.5

Le reti Token Ring implementano un accesso multiplo a token su una topologia ad anello monodirezionale. Il meccanismo a token sui canali di tipo ad anello fisico è di più semplice costruzione rispetto all'anello logico (ad esempio sistemi a token su bus come l'802.4) perché l'anello logico, appunto, non va costruito in quanto il token passa naturalmente attraverso tutte le stazioni.

Uno dei problemi più pressanti del token ring, che non esiste nelle strutture a bus, è la rimozione dei segnali immessi e dei segnali che eventualmente si trovano a circolare per errore. La rimozione dei segnali immessi potrebbe avvenire sulla base del riconoscimento dell'indirizzo, ma questo comporterebbe di inserire un ritardo in ciascun ripetitore, pari al tempo necessario a riconoscere l'indirizzo voluto.

In alternativa, si può utilizzare il metodo detto single token, schematizzato in Figura 18 e che si può riassumere nel seguente modo: quando una stazione riceve il token da quella che la precede sul ring, apre l'anello, trasmette il suo messaggio, drenando nel frattempo tutto quello che riceve dal ring finché riceve anche il proprio messaggio. Quando il messaggio è stato estratto in modo totale dal ring, l'anello viene richiuso e il token trasmesso a valle. Questa tecnica consente di ritardare al minimo il segnale transitante e cioè di un tempo di bit, necessario a riconoscere lo stato del flag di token e ad alterarlo, (porlo occupato) in modo che la stazione a valle non lo possa usare.



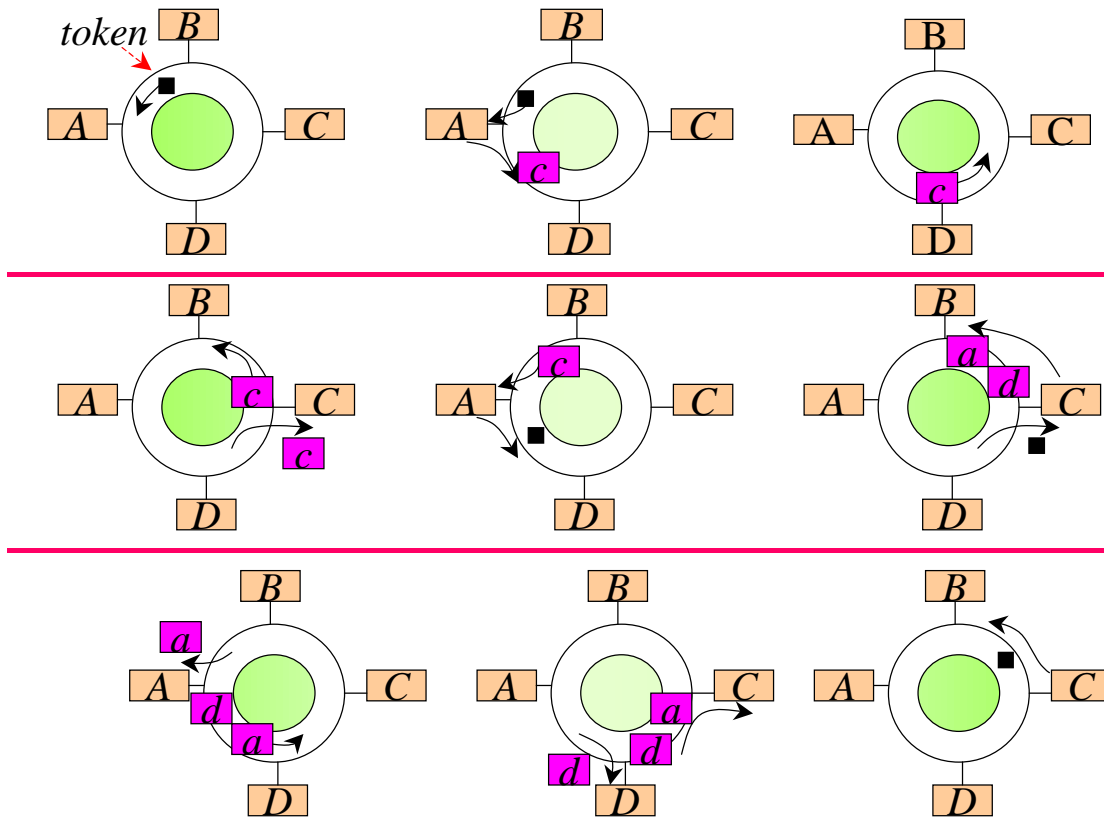


Figura 18: schema di funzionamento del single token; cattura del token da parte della stazione A e trasmissione di un pacchetto verso C; passaggio del token a D e poi a C che trasmette un pacchetto verso A e uno verso D; l'anello viene mantenuto aperto da parte della stazione trasmittente fino alla completa ricezione dei pacchetti trasmessi

Lo standard IEEE 802.5, originato nei primi anni 80, recepisce una tecnica di tipo token ring originata dall'IBM nel 1976. L'anello utilizza collegamenti sequenziali punto-punto, inizialmente progettato per coppie STP, e sincronismo continuo generato da una delle stazioni che assume il ruolo di *master* e una velocità di 4 Mb/s. Il massimo numero di stazioni ammesso è di 260 a causa delle limitazioni dovute all'accumulazione di jitter nella rigenerazione del sincronismo da parte delle stazioni a valle del master. Successivamente lo standard è stato perfezionato introducendo la possibilità di utilizzare cavi UTP, ripetitori attivi ed aumentando la velocità a 16 Mb/s. Per una migliore efficienza in condizioni estreme, il protocollo utilizzato in questo caso è una variante single token detta di *early token release* che prevede che il token venga rilasciato quando si inizia a ricevere il pacchetto trasmesso e non alla fine della ricezione.

In questo standard il problema dell'alimentazione dei ripetitori viene risolto attraverso dei relais di bypass che quando sono alimentati fanno passare il segnale verso gli apparati di ricezione della stazione (Figura 4). Quando una stazione si spegne il relais si disaccetta richiudendo un circuito di bypass fra ingresso e uscita. Per facilitare la gestione e la ricerca dei guasti, la rete viene configurata in modo stellare tramite dei "cabinets" in cui vengono concentrati i relais di bypass e i ripetitori. Nello topologia stellare il "lobo" formato da ciascuna stazione può arrivare al centinaio di metri.

In Figura 19 è mostrata la trama MAC utilizzata dall'802.5. I delimitatori di trama sono formati da ottetti in cui compaiono delle violazioni di codice di linea, in modo da identificare univocamente l'inizio della trama. Il campo di Frame Control distingue il tipo di trama (controllo o dati), mentre il campo Access Control contiene 3 bit di priorità, il token (1 bit), un bit di monitor e 3 bit di prenotazione. Il campo Routing Information è stato aggiunto in seguito e contiene informazione per la tecnica source routing (vedi paragrafo successivo). Il campo Frame Status viene utilizzato dal ricevente, se acceso, per indicare se ha riconosciuto

la trama (2 bit) e se l'ha copiata (2 bit). L'End Delimiter contiene anche un bit di "more", ossia un bit che viene usato quando la stazione ha più trame da trasmettere.

La trasmissione di una o più trame viene regolata da un contatore chiamato Token Holding Time (THT), stabilito al momento dell'inizializzazione della rete, che limita il tempo di trattenimento del token presso una stazione. Il THT ha un valore massimo consentito di 8.9 ms.

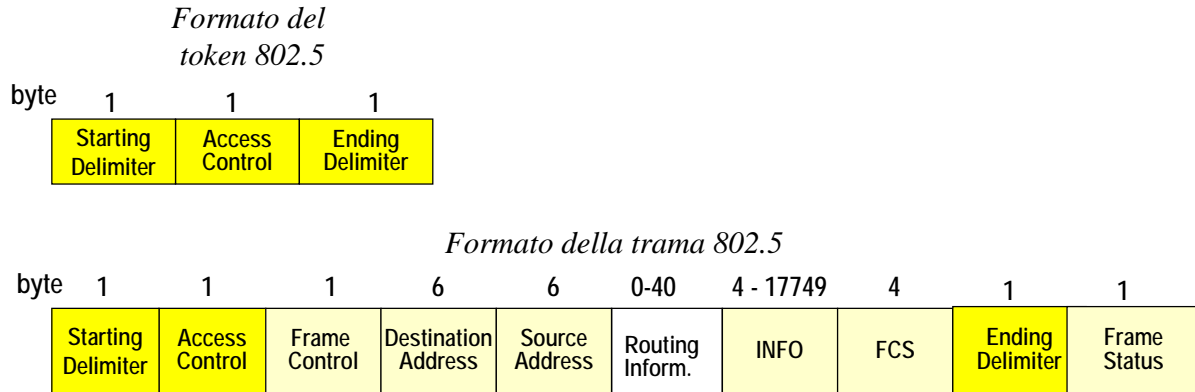


Figura 19: formato delle trame e dei token 802.5

## 7. I bridge (layer 2 switch)

Il forte aumento di traffico ha messo in luce i limiti di non scalabilità presentati dalle prime strutture di reti locali puramente broadcast. La tecnologia ha messo successivamente a disposizione degli apparati di commutazione/instradamento a basso costo, cosa che ha reso conveniente il frazionamento di reti broadcast in diversi *domini di collisione* disgiunti, a loro volta connessi da tali apparati, denominati *bridge*, e che presentano due o più porte connesse alle diverse reti locali.

I bridge operano una interconnessione delle lan a livello 2, come mostrato in Figura 20. Le LAN collegate possono essere dello stesso genere o addirittura possono adottare meccanismi MAC differenti. Su ogni LAN il bridge si comporta, nei confronti del protocollo di accesso multiplo, come una normale stazione per la trasmissione dei pacchetti ricevuti dalle altre LAN e che devono essere trasmessi.

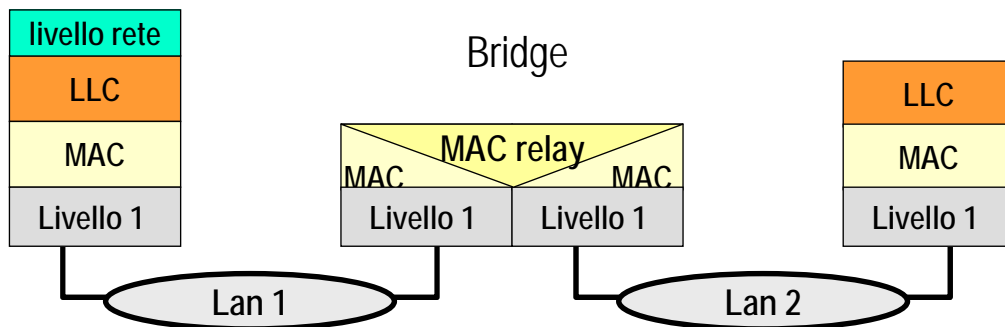


Figura 20: interconnessione a livello 2 con bridge

Si noti qui in modo esplicito che l'interconnessione di spezzoni di rete locale mediante repeater non elimina la possibilità di collisione tra pacchetti trasmessi su spezzoni differenti in quanto l'interconnessione avviene

a livello fisico e dunque il trasferimento sulle porte avviene commutando il singolo bit. Al contrario l'interconnessione tramite bridge configura una vera e propria funzionalità di rete in cui i pacchetti vengono ricevuti dal bridge, memorizzati e trasmessi sull'uscita opportuna sulla base delle regole di instradamento adottate (Figura 21).

In uno scenario di commutazione a livello 2 l'efficienza dell'instradamento non è di primaria importanza rispetto alla velocità e al basso costo, per cui le tecniche di instradamento sviluppate per i bridge si basano su principi abbastanza semplici.

L'introduzione della commutazione a livello 2 è avvenuta rispettando i principi su cui si basano le reti locali, ossia la capacità di indirizzare in modo broadcast con una sola trama, e la mobilità, ossia la capacità di comunicare con un unico indirizzo MAC in qualunque punto della rete ci si metta (struttura di indirizzamento piano).

Due differenti tipologie di bridge sono state considerate per le reti locali di comune utilizzo.

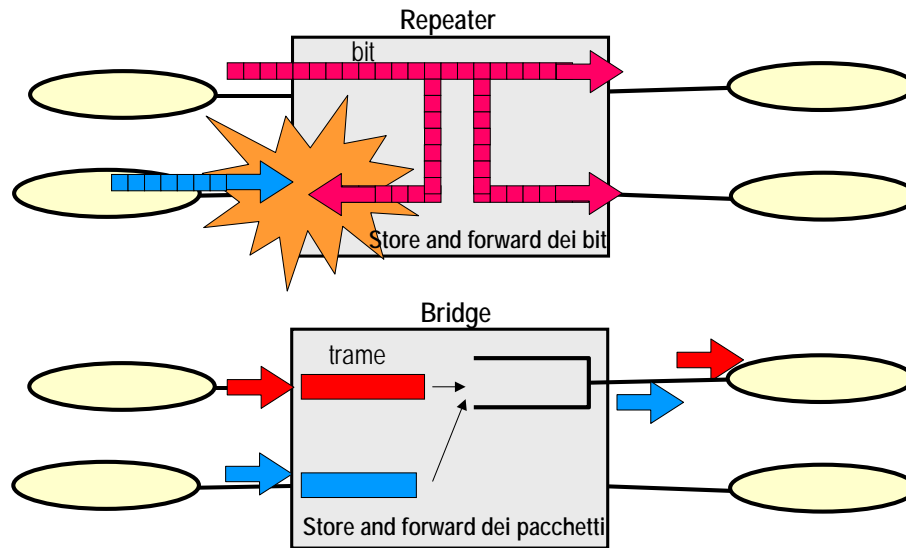


Figura 21: interconnessione mediante repeater e mediante bridge

## 7.1 Bridge trasparenti

In questo standard il bridge opera l'instradamento degli indirizzi MAC delle trame che transitano su una porta sulla base di tabelle che associano tale indirizzo a una porta di destinazione, tramite la quale l'indirizzo stesso possa essere raggiunto. Se la porta associata è la stessa su cui la trama è stata ricevuta, il bridge non interviene. Altrimenti copia la trama sulla porta di destinazione.

Tali tabelle si configurano dinamicamente tramite una procedura detta di *backward learning* che consiste nel leggere tutte le trame che sono ricevute dal bridge su una porta e nell'associare tale porta all'indirizzo MAC nel campo sorgente.

Questo approccio è sufficiente a garantire un corretto instradamento in condizioni statiche nelle quali l'associazione tra indirizzi e porte non muta nel tempo. Per permettere cambiamenti dinamici, e quindi la mobilità, l'associazione tra indirizzo e porta è caratterizzata da un tempo di validità trascorso il quale viene eliminata.

Resta il problema di effettuare l'instradamento verso stazioni che non hanno ancora l'associazione. In questo caso le trame vengono inviate a tutte le porte del bridge secondo la tecnica detta del *flooding*.

Con questo tipo di bridge un eventuale segmentazione di una rete broadcast non viene avvertita dagli utenti, se si eccettuano i brevi ritardi di configurazione dei bridges. Per questo motivo questi bridge sono chiamati trasparenti.

Il meccanismo di flooding adottato dai bridge trasparenti è utilizzabile solo in topologie della rete non magliate, ovvero solo quando la topologia è descritta da un albero. Se, infatti, fosse adottato il flooding in una rete con almeno una maglia chiusa si andrebbe incontro al fenomeno detto di *broadcast storm* che blocca il normale funzionamento della rete. Con riferimento alla semplice rete magliata di Figura 22, si consideri il caso in cui B invia un pacchetto ad A ed A non è nelle tabelle dei bridge. In accordo alle regole dei bridge trasparenti, i bridge inviano il pacchetto sull'altra porta in uscita verso la LAN 1. Ogni bridge riceve il pacchetto trasmesso sulla LAN 1 dall'altro bridge e, di nuovo, effettua l'instradamento verso l'altra LAN. La situazione si ripete all'infinito e i pacchetti continuano a circolare tra le due LAN.

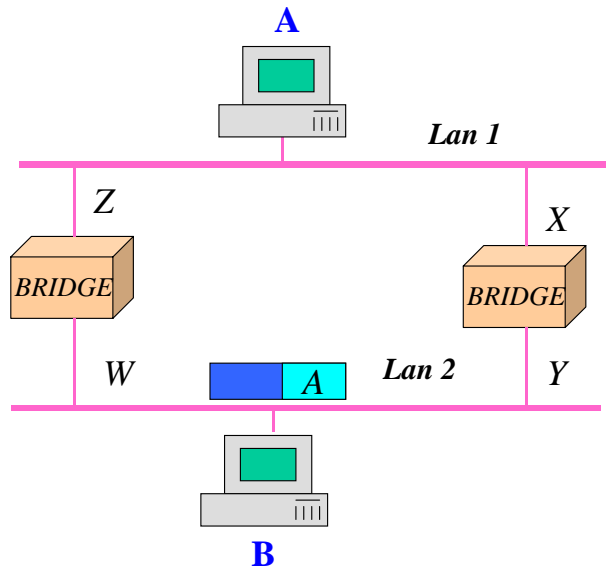


Figura 22: esempio di rete magliata dove si può presentare il broadcast storm

Lo spanning tree (IEEE 801.1d) è una variante introdotta per evitare i problemi di ricircolo dei pacchetti nelle reti magliate. L'idea alla base è semplice: definire sul grafo della topologia originale un sotto-grafo che sia un albero, ed usare solo i rami dell'albero per il meccanismo di flooding. Nell'albero (detto spanning tree perché contiene tutti i nodi) non vi sono cicli dove possa avvenire il ricircolo e quindi il meccanismo dei bridge trasparenti funziona correttamente.

Per determinare uno spanning tree i bridge devono scambiare pacchetti di controllo tra di loro. La prima operazione da fare è eleggere la radice dell'albero. Ciò viene fatto sulla base del serial number di ogni bridge e viene eletto radice dell'albero il bridge con il serial number minimo.

La procedura prevede che ogni bridge trasmetta dei messaggi di servizio sulle LAN alle quali è connesso che vengono catturati solo dai bridge connessi alle stesse LAN. In tali messaggi è indicato:

- ✓ S/N del mittente
- ✓ S/N della radice provvisoria
- ✓ numero di hop fino alla radice

Ogni bridge all'inizio considera se stesso come radice e pone a zero il numero di hop. Quando riceve un messaggio da un altro bridge con un S/N della radice più basso aggiorna la sua informazione e ritrasmette il messaggio. Se la topologia della rete non varia la procedura converge all'albero con il minimo numero di hop.

## 7.2 Bridge source routing

Un altro metodo, che evita gli inconvenienti del broadcast storm è quello noto come source-routing bridge, sviluppato nel comitato IEEE 802.5.

Il metodo source-routing richiede la cooperazione delle stazioni nello scoprire e indicare ai bridge il cammino da seguire. I bridge devono pertanto solo seguire le istruzioni di instradamento che vengono inserite nello header dei pacchetti. In questo modo l'operazione di inoltramento è estremamente semplificata e sveltita. Le trame che devono passare dai bridge devono contenere un campo di routing addizionale (Routing Information) a sua volta costituito da  $n$  campi di due ottetti, il primo dei quali (Routing Control) indica il tipo di trama, la sua lunghezza massima e il numero  $n-1$  dei successivi campi (Route Designator) indicanti ciascuno la strada da seguire, composta da un identificativo di rete di 12 bit e da un identificativo di bridge di 4 bit.

L'instradamento viene operato se il bridge scopre il proprio numero affiancato dai due numeri di rete che connette. Naturalmente, la stazione sorgente deve conoscere tutta la strada verso il destinatario e fornire il campo RI. Per le ragioni già spiegate, occorre prevedere una modalità di ricerca della strada stessa.

Supponiamo che la stazione A debba effettuare la ricerca della strada verso la stazione B. La ricerca della strada è effettuata mediante la trasmissione un pacchetto particolare (single route broadcast) indirizzato alla stazione di destinazione B. Questo pacchetto è inoltrato su tutte le reti seguendo una tecnica di tipo spanning-tree o flooding, e raggiunge per questa via la destinazione. In risposta a questo pacchetto B invia un pacchetto particolare (all route broadcast) con campo di instradamento vuoto. Questa trama viene inoltrata dai bridge lungo tutte le vie possibili, registrando il passaggio sul campo di instradamento. Quando più copie di questa trama raggiungono A, portano conoscenza ad A di tutte le strade possibili per raggiungere B e dunque A può scegliere sfruttando la strada migliore o, persino, più strade.

I vantaggi del source routing sono legati ovviamente alla possibilità di sfruttare per ogni pacchetto un solo cammino, scelto con criteri di ottimizzazione, verso la destinazione evitando di occupare risorse su LAN non presenti nel cammino, come invece in generale avviene nel transparent bridging. Di contro questa tecnica non è "trasparente" in quanto richiede che i nodi collaborino nel processo di bridging e, quindi, necessita della modifica di eventuali nodi già installati.