

10

INTERCONNESSIONE DI LAN TRAMITE BRIDGE

10.1 INTRODUZIONE

Le reti locali sinora esaminate hanno dei limiti in termini di distanze massime ammesse, carico massimo sopportato e numero massimo di sistemi collegabili. Quando si vuole oltrepassare uno o più di tali limiti, bisogna creare una *rete locale estesa* (a volte indicata con le sigle ELAN, XLAN o BLAN) interconnettendo tra loro più LAN per mezzo di *bridge*.

Nella figura 10.1 è rappresentato lo schema logico di una BLAN. I due sistemi* (End Station), connessi alle due LAN, sono messi in grado di comunicare dal bridge.

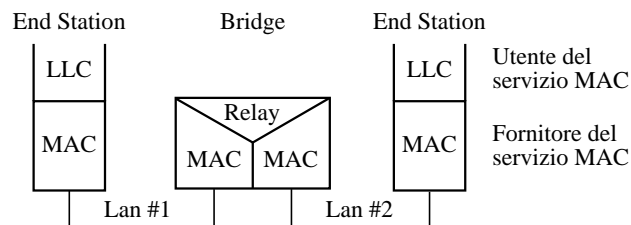


Fig. 10.1 - Impiego di un bridge per interconnettere due LAN.

I bridge ritrasmettono solo i pacchetti che devono effettivamente transitare da una LAN ad un'altra LAN, mantenendo separati i traffici locali delle singole LAN che interconnettono. Questa funzionalità, detta di "filtraggio" (*filtering*), permette

* Nel seguito il termine *sistema*, di derivazione OSI, e il termine *stazione* (station o end station), di derivazione IEEE 802, verranno usati come sinonimi.

di ottenere un traffico globale sulla BLAN superiore a quello massimo ammesso per ogni singola LAN.

Tale ritrasmissione avviene con una modalità di "*store and forward*", cioè il pacchetto è ricevuto dal bridge, e poi eventualmente ritrasmesso. Questo permette di superare i limiti sulle distanze massime e sul numero massimo di sistemi collegabili in una rete locale, in quanto tali limiti sono tipicamente dettati dal livello fisico.

I bridge possono interconnettere LAN con lo stesso MAC (es: 802.3 con 802.3) oppure con MAC differenti (es: FDDI con 802.3, FDDI con 802.5, 802.3 con 802.5). In questo secondo caso devono tradurre la busta di livello 2, ricevuta da una LAN, nella busta di livello 2 da trasmettere all'altra LAN. In figura 10.2 viene illustrato l'utilizzo di un bridge 802.3-FDDI e le relative operazioni di traduzione delle buste, che risultano semplici poiché entrambe le LAN utilizzano il protocollo IEEE 802.2/LLC (si veda paragrafo 5.7).

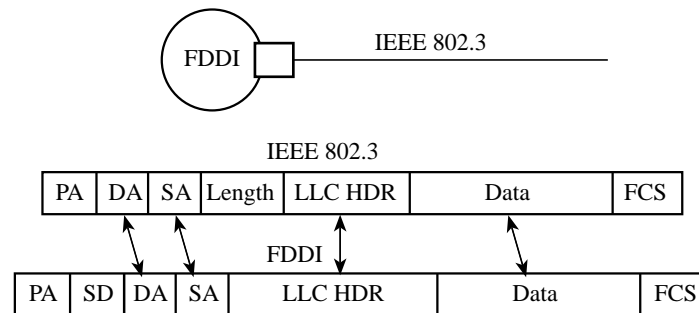


Fig. 10.2 - Bridge 802.3-FDDI.

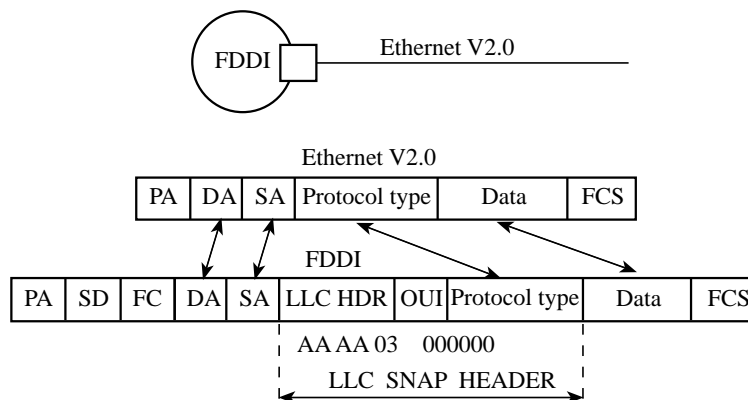


Fig. 10.3 - Bridge Ethernet-FDDI.

I bridge sono molto spesso utilizzati anche per interconnettere LAN proprietarie (non conformi allo standard IEEE 802). Il caso più tipico è quello dei bridge verso Ethernet. La figura 10.3 illustra un bridge Ethernet-FDDI e le relative problematiche di traduzione delle buste, che risultano più complesse poiché Ethernet non utilizza il protocollo IEEE 802.2 e il bridge deve inserire un header LLC SNAP (si veda il paragrafo 5.7.4).

10.1.1 Caratteristiche generali

I bridge hanno le seguenti caratteristiche generali:

- operano al livello 2 del modello di riferimento OSI, sottolivello MAC, e per questo sono molto spesso detti MAC-Bridge;
- hanno algoritmi di instradamento molto semplici: ogni bridge calcola autonomamente le sue tabelle di instradamento senza interagire con gli altri bridge, con un algoritmo di routing isolato (si veda il paragrafo 14.5.2);
- si utilizzano normalmente per interconnessioni locali, anche se sono stati usati nel passato, in modo un po' problematico, anche per interconnessioni geografiche.

I bridge possono essere realizzati secondo due filosofie diverse che differiscono nel luogo ove vengono memorizzate le *tabelle di instradamento* (nel seguito usato come sinonimo di *tabelle di filtraggio*):

- *transparent bridge*: sono i bridge conformi allo standard 802.1D (trattato in questo capitolo), di derivazione Ethernet. Hanno le tabelle di instradamento a bordo e sono trasparenti, nel senso che i sistemi interconnessi alle LAN ignorano la loro esistenza;
- *source routing bridge*: sono i bridge di derivazione token-ring. Non hanno tabelle di instradamento a bordo, le tabelle sono invece mantenute dai sistemi connessi alle LAN che in fase di trasmissione del pacchetto devono specificare esplicitamente il cammino che il pacchetto dovrà fare per giungere a destinazione, indicando tutti i bridge da attraversare (che quindi vengono indirizzati esplicitamente).

Nel seguito verranno descritti prima i transparent bridge e poi i source routing bridge. Quanto detto da questo punto in poi, quando non diversamente specificato, vale per i transparent bridge.

10.1.2 Spanning Tree

Come già visto, i bridge devono instradare pacchetti sulla rete e quindi hanno bisogno di costruirsi delle tabelle di instradamento. Se la topologia della BLAN è ad albero, la costruzione di tali tabelle può avvenire con un algoritmo molto semplice, in modo automatico, tramite un processo di apprendimento (*learning process*).

Poiché è tuttavia preferibile avere topologie magliate per ragioni di affidabilità, occorre integrare il learning process con un algoritmo di *spanning tree* (si veda paragrafo 10.18) per riportare dinamicamente una topologia magliata ad una topologia ad albero, escludendo dall'operatività opportune porte di opportuni bridge.

Tale problema non esiste nei source routing bridge, in quanto il pacchetto, quando viene generato, contiene la specifica completa del cammino che dovrà seguire.

10.1.3 Frammentazione

I bridge che operano tra LAN eterogenee hanno il problema aggiuntivo della diversa lunghezza massima del campo dati (INFO) del pacchetto MAC. La dimensione massima del campo INFO del pacchetto varia a seconda degli standard, ad esempio è di 1.500 byte per 802.3, 17.749 byte per 802.5 e 4.478 byte per FDDI.

Poiché è impossibile violare tali dimensioni massime, quando un bridge deve ritrasmettere un pacchetto di dimensione superiore a quella massima ammessa ha due possibilità: scartare il pacchetto o frammentarlo.

La frammentazione è un tipico compito del livello 3 (network) e non può essere realizzata da un bridge in modo generalizzato per tutti i protocolli. Fortunatamente molti di questi, tra cui ISO 8473 (si veda paragrafo 17.5) e DECnet fase IV (si veda paragrafo 15.2), non generano mai pacchetti più lunghi di 1500 byte e quindi il problema non si pone. Il protocollo TCP/IP invece genera sistematicamente pacchetti di dimensioni maggiori e molti bridge, limitatamente al protocollo IP (si veda paragrafo 16.4), realizzano la frammentazione, in accordo con lo standard RFC 791.

10.1.4 Prestazioni di un Bridge 802.3

Le prestazioni di un bridge sono importanti in quanto determinano le prestazioni globali della BLAN. I parametri più importanti sono:

- numero massimo di pacchetti al secondo che un bridge può filtrare (cioè ricevere e processare);

- numero massimo di pacchetti al secondo che un bridge può ritrasmettere;
- *tempo medio di latenza*, cioè tempo di attraversamento del bridge da parte di un pacchetto.

Per minimizzare la possibilità di perdita di pacchetti è preferibile che un bridge sia *full-speed*, cioè che i primi due parametri siano uguali al massimo teorico. Questo è tanto più difficile da realizzare quanto più i pacchetti sono corti (massimizza il numero di decisioni sul filtraggio che un bridge deve prendere nell'unità di tempo), per cui la proprietà di *full-speed* deve essere verificata con pacchetti tutti di lunghezza minima.

Nel caso di 802.3, un bridge è *full-speed* quando è in grado di inoltrare 14880 pps (packet per second) da 64 byte (pacchetti più corti). Tale numero si può calcolare partendo dalla lunghezza del pacchetto, aggiungendo preambolo e delimitatori e considerando la necessità di rispettare un *inter packet gap* tra i pacchetti, fissato da IEEE 802.3 in 9,6 microsecondi. La tabella 10.1 illustra le prestazioni di un bridge 802.3.

Dimensione pacchetto	Pacchetti al secondo	
	carico 50%	carico 100%
1.518	403	812
1.024	603	1.206
512	1.192	2.385
256	2.332	4.664
128	4.464	8.928
64	8.223	14.880

Tab. 10.1 - Prestazioni di un bridge 802.3-802.3.

Il tempo di latenza di un bridge esprime il tempo che intercorre da quando il pacchetto incomincia ad entrare nella porta ricevente a quando esso incomincia ad uscire dalla porta trasmittente. Il tempo di latenza non è fisso, ma varia a seconda della dimensione del pacchetto ricevuto: valori medi sono compresi tra 80 microsecondi e 1,2 millisecondi.

10.1.5 Bridge remoti

Nel progetto OSI i bridge sono stati concepiti per interconnettere LAN su base locale, mentre l'interconnessione di LAN su scala geografica è stata demandata ai

router, cioè a commutatori di pacchetto operanti al livello 3 del modello di riferimento OSI. Tuttavia, poiché i bridge sono assolutamente trasparenti ai protocolli di livello 3 (nel senso che trasportano qualsiasi pacchetto MAC valido, ignorandone il contenuto), e poiché si sono resi disponibili sul mercato prima dei router multi-protocollo, essi sono stati modificati per operare anche su scala geografica e sono nati i cosiddetti *bridge remoti*.

I bridge remoti vengono utilizzati per interconnettere le LAN anche geograficamente distanti e comunque implicano l'attraversamento di suolo pubblico. Essi utilizzano principalmente:

- linee telefoniche a velocità maggiore o uguale a 64 Kb/s;
- reti veloci a commutazione di pacchetto, quali Frame Relay e SMDS (si vedano i paragrafi 13.5 e 13.6);
- portanti non convenzionali, quali raggi laser, fibre ottiche e fasci di microonde.

Lo standard 802.1D non specifica le modalità ed i protocolli da usare per trasportare i pacchetti attraverso le linee pubbliche. Per questa ragione è consigliabile che la coppia di bridge remoti sia dello stesso costruttore e del medesimo modello. I protocolli più usati sulle linee sono HDLC e PPP (si vedano i paragrafi 13.2 e 13.3).

I bridge remoti non si prestano a realizzare strutture magliate, in quanto l'algoritmo di spanning tree mette in backup (stato di blocking) costose linee pubbliche sino a ridurre la rete ad un albero (figura 10.4), con evidente spreco di denaro.

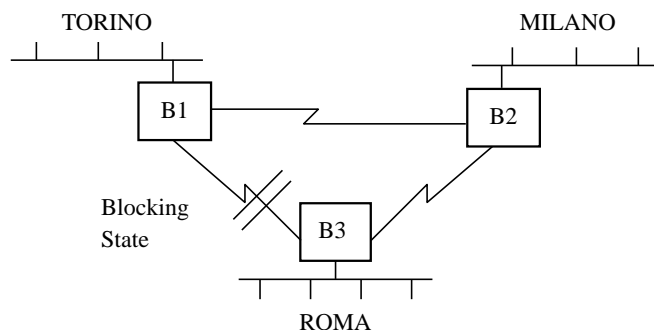


Fig. 10.4 - Bridge remoti

Alcuni costruttori, per utilizzare appieno tutte le linee, comprese quelle di backup, adottano il DLS (*Distributed Load Sharing*). Il DLS permette di usare

anche le linee dichiarate in blocking state dallo spanning tree, per il traffico tra due LAN. I due problemi principali che devono essere risolti dal DLS sono il comportamento FIFO e la non generazione dei duplicati, e questo è particolarmente critico durante le fasi di transizione dello spanning tree.

10.2 ARCHITETTURA FISICA DI UN BRIDGE

I bridge sono costituiti da una o più CPU, una memoria e due o più interfacce che interconnettono le LAN (figura 10.5).

La ROM contiene il software che realizza tutte le funzionalità del bridge in conformità allo standard IEEE 802.1D. La memoria RAM contiene le tabelle di instradamento, i buffer per i dati ed un'area di memoria utilizzata dal software per le strutture dati interne.

L'interfaccia è costituita per una parte da dispositivi elettronici conformi ai diversi standard per le LAN (ad esempio, 802.3, 802.5, FDDI) e per la restante parte da dispositivi per la connessione ai diversi mezzi trasmissivi (ad esempio: UTP, STP, fibra ottica, cavo coassiale).

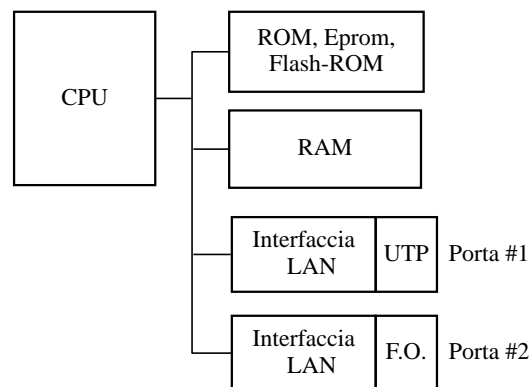


Fig. 10.5 - Architettura fisica di un bridge.

10.3 ARCHITETTURA LOGICA DI UN BRIDGE

Oltre a tale organizzazione fisica si può considerare un bridge costituito, da un punto di vista logico, dai seguenti tre elementi (figura 10.6):

- le *porte*, che possono essere due o più;
- l'entità di ritrasmissione e filtraggio chiamata *MAC relay entity*;
- le entità di livello superiore chiamate *higher layer entities*.

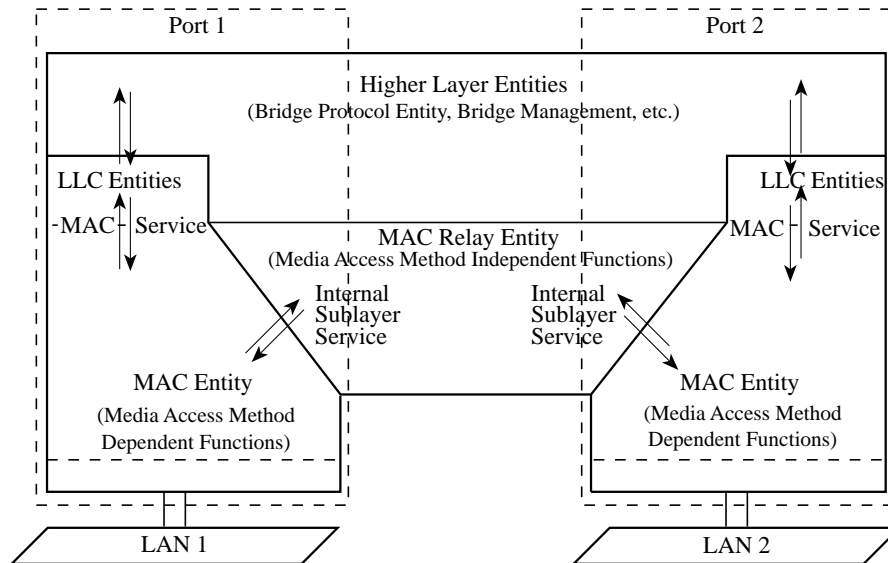


Fig. 10.6 - Architettura logica di un bridge.

Ogni porta riceve/trasmette i pacchetti dalla/alla LAN a cui è connessa usando il servizio fornito dall'entità MAC associata a tale porta. L'entità MAC di ogni porta tratta tutte le funzioni di metodo di accesso nel modo specificato dai relativi standard IEEE 802.

L'entità di ritrasmissione (MAC relay entity) si occupa di ritrasmettere i pacchetti tra due porte, filtrare i pacchetti ed apprendere le informazioni di filtraggio.

Le entità di livello superiore (higher layer entities), che fanno uso delle procedure di Logical Link Control (LLC), fornite separatamente per ogni porta, sono principalmente due:

- *bridge protocol entity* che si occupa del calcolo e della configurazione della topologia della BLAN (algoritmo di spanning-tree);
- *bridge management entity* che si occupa di governare e controllare le funzioni del bridge.

10.4 PRINCIPALI FUNZIONI DI UN BRIDGE

Le funzioni principali di un bridge sono:

- ricevere, filtrare e ritrasmettere i pacchetti;
- mantenere le informazioni richieste per prendere le decisioni di filtraggio;
- governare e controllare (*management*) quanto sopra citato.

La figura 10.7 riporta il diagramma di flusso relativo alle prime due funzioni.

10.4.1 Filtraggio

I pacchetti trasmessi da un sistema S1 verso un sistema S2 vengono confinati dai bridge nelle LAN che formano il percorso tra S1 e S2. Questo tipo di filtraggio è il più comune e serve a ridurre il traffico globale.

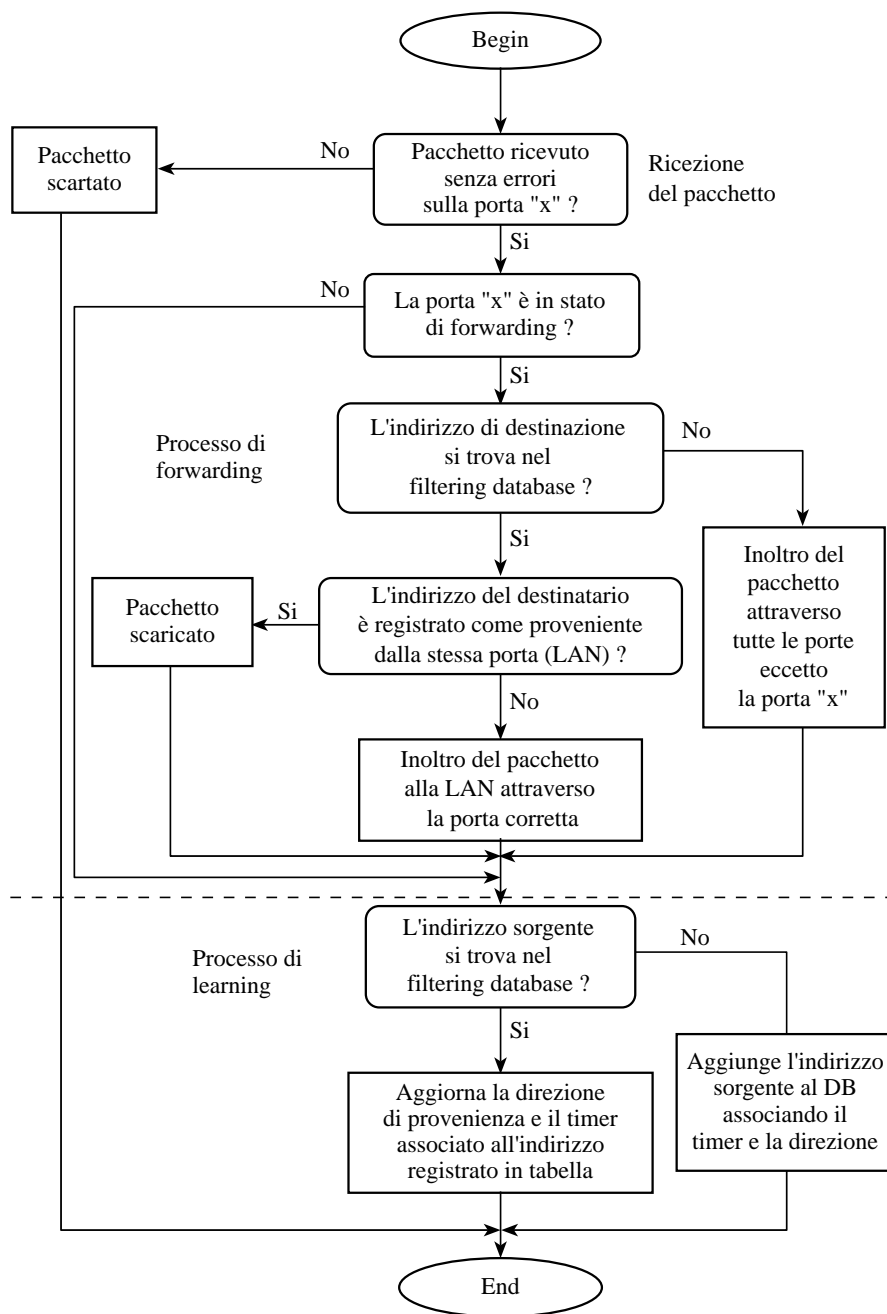
Qualora esistano più percorsi per raggiungere S2, i bridge operano un ulteriore filtraggio per prevenire la duplicazione di pacchetti.

Altri tipi di filtraggio possono essere effettuati intervenendo direttamente sul bridge con sistemi di management e definendo filtri inclusivi e filtri esclusivi. I filtri esclusivi limitano l'apprendimento del learning process, imponendo classi di pacchetti che devono essere sempre filtrati, cioè non ritrasmessi. I filtri inclusivi includono invece classi di pacchetti che non devono essere filtrati. Tali filtri possono agire su combinazioni dei seguenti parametri:

- indirizzo di mittente (MAC-SSAP) del pacchetto;
- indirizzo di destinatario (MAC-DSAP) del pacchetto;
- filtri basati sul tipo di protocollo di livello 3 contenuto nel campo dati della MAC-PDU.

Le funzioni che riguardano il mantenimento delle informazioni di filtraggio sono le seguenti:

- configurazione delle informazioni relative al filtraggio statico, cioè ai filtri inclusivi o esclusivi impostati da management;
- apprendimento automatico (learning process) delle informazioni relative al filtraggio dinamico, attraverso l'osservazione del traffico della BLAN;
- definizione dell'età massima (*ageing time*) delle informazioni di filtraggio che sono state apprese automaticamente, oltre la quale le informazioni stesse vengono invalidate;
- calcolo e configurazione della topologia della BLAN (tramite algoritmo di spanning-tree).

**Fig. 10.7** - Diagramma di flusso delle principali operazioni del bridge.

10.4.2 Ritrasmissione (Relay)

I pacchetti che superano il filtraggio sono ritrasmessi sulla LAN di destinazione con il protocollo di livello MAC proprio di tale rete e mantenendo la sequenza con cui i pacchetti sono stati ricevuti.

10.5 INFORMAZIONE DI STATO DELLE PORTE

L'informazione di stato associata ad ogni porta del bridge governa la sua partecipazione alla BLAN. A livello di management si dichiara la porta attiva (*enabled*) o non attiva (*disabled*). Le porte attive possono trovarsi in vari sottostati in funzione delle decisioni prese dall'algoritmo di spanning tree. Una porta attiva si dice in un stato di *forwarding* se partecipa alla ritrasmissione di pacchetti, di *learning* se si limita ad apprendere, di *listening* se si limita ad ascoltare il traffico e di *blocking* se è stata definita come porta di backup dall'algoritmo di spanning tree (per una descrizione più dettagliata si veda il paragrafo 10.18.3).

10.6 TABELLA DI INSTRADAMENTO

La tabella di instradamento, detta anche tabella di filtraggio o filtering database, è costituita da un insieme di righe (*entry*), contenenti le informazioni di filtraggio che sono esplicitamente configurate tramite operazioni di management (*entry statiche*) oppure sono state registrate automaticamente dal processo di apprendimento (*entry dinamiche*).

La tabella di instradamento fornisce le informazioni al processo di inoltramento, per decidere se inoltrare un pacchetto avente un certo indirizzo di destinazione su una data porta.

Una entry dinamica non viene creata se esiste già una entry statica relativa allo stesso indirizzo MAC. All'atto della creazione di una entry statica, una eventuale entry dinamica relativa allo stesso indirizzo MAC viene rimossa.

Le entry dinamiche sono soggette ad un meccanismo di timeout: se l'entry non viene aggiornata per un tempo superiore al parametro ageing time (valore di default cinque minuti), la entry viene automaticamente rimossa.

Le entry statiche non sono soggette a timeout.

10.7 RICEZIONE DEI PACCHETTI

L'entità MAC associata ad ogni porta riceve ed esamina tutti i pacchetti trasmessi sulla LAN cui è connessa.

La prima analisi riguarda il campo FCS per determinare se il pacchetto è corretto o errato. I pacchetti errati sono scartati.

I pacchetti indirizzati effettivamente alle entità di livello superiore del bridge (che sono normalmente una piccola parte) vengono affidati al livello LLC associato alla porta di ricezione. Questi pacchetti contengono nel campo destination (MAC-DSAP) l'indirizzo MAC di una porta del bridge o un indirizzo di gruppo (multicast) cui appartiene almeno una porta del bridge (ad esempio, l'indirizzo di multicast usato dal protocollo spanning tree).

Gli altri pacchetti vengono passati all'entità MAC di inoltro.

10.8 TRASMISSIONE DI PACCHETTI

L'entità MAC associata ad una porta trasmette i pacchetti che le sono stati affidati dall'entità MAC di inoltro dei pacchetti (MAC relay entity).

Essa trasmette inoltre i pacchetti generati dalle entità di livello superiore del bridge stesso.

10.9 INOLTRO DEI PACCHETTI

Il processo di inoltro dei pacchetti (frame forwarding) realizza la MAC relay entity e compie le seguenti funzioni:

- inoltro dei pacchetti ricevuti da una porta alle altre porte;
- filtraggio dei pacchetti in base alle informazioni contenute nella tabella di filtraggio;
- filtraggio dei pacchetti in base allo stato delle porte.

La figura 10.8 illustra l'utilizzo, da parte del processo di forwarding, dell'informazione di stato delle porte, allo scopo di determinare se il pacchetto debba essere ritrasmesso verso le altre porte del bridge.

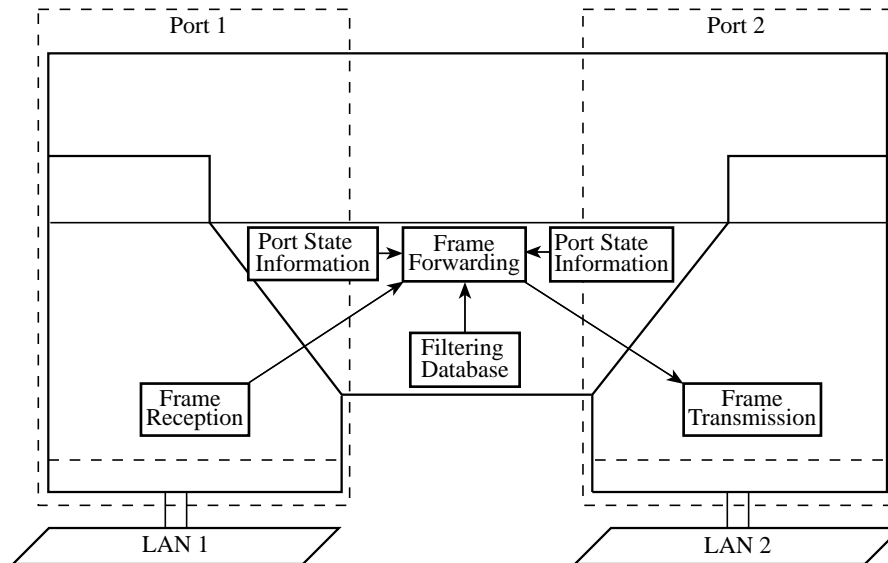


Fig. 10.8 - Inoltro dei pacchetti (bridge forwarding).

10.9.1 Condizioni di inoltro

Un pacchetto ricevuto su una porta di un bridge viene affidato al processo di inoltro che deve deciderne un eventuale accodamento per la trasmissione su altre porte. Condizione necessaria è che sia la porta di ricezione sia le porte di destinazione si trovino in stato di forwarding.

Il processo di inoltro accoda il pacchetto su una singola porta se questo ha un indirizzo di destinazione MAC (MAC-DSAP) di tipo singolo, su tutte le porte se il MAC-DSAP è multicast o broadcast.

Il processo di inoltro consulta la tabella di instradamento per determinare su quale porta eventualmente accodare il pacchetto in funzione del suo indirizzo di destinazione (MAC-DSAP).

È inoltre indispensabile che la dimensione del pacchetto da trasmettere non superi la dimensione massima ammessa dalla LAN di destinazione. Ad esempio, se il pacchetto ricevuto ha una dimensione di 2.052 byte ed è destinato ad una LAN 802.3, il pacchetto non verrà inoltrato, poiché la dimensione massima del campo dati nelle LAN 802.3 è di 1500 byte.

10.9.2 Accodamento dei pacchetti

Il processo di inoltramento si occupa di accodare i pacchetti rispettando l'ordine di arrivo, operando cioè in modalità FIFO (*First-In First-Out*).

Un pacchetto viene rimosso dalla coda della porta a cui è associato a seguito di una delle seguenti condizioni:

- dopo la trasmissione del pacchetto stesso, indipendentemente dal fatto che sia avvenuta correttamente;
- nel caso in cui venga superato il tempo massimo di transito del pacchetto (*maximum bridge transit delay*);
- nel caso in cui la porta abbandoni lo stato di forwarding.

La rimozione di un pacchetto dalla coda di trasmissione di una porta non implica la rimozione del medesimo dalla coda di trasmissione di altre porte.

10.9.3 Ricalcolo della FCS

Quando un pacchetto viene inoltrato tra due LAN omogenee non viene effettuato il ricalcolo del FCS, qualora invece le due LAN siano eterogenee (ad esempio, un pacchetto ricevuto su una porta associata ad una LAN IEEE 802.3 e ritrasmesso ad una LAN FDDI) viene ricalcolato il campo FCS.

10.10 PROCESSO DI APPRENDIMENTO

Il processo di apprendimento (*learning*) osserva l'indirizzo MAC sorgente (MAC-SSAP) dei pacchetti ricevuti su ogni porta e crea o aggiorna le entry dinamiche della tabella di instradamento, condizionatamente allo stato delle porte.

Il MAC-SSAP indica al processo di apprendimento che la stazione con quell'indirizzo è raggiungibile attraverso la porta che ha ricevuto il pacchetto. Tale metodologia di apprendimento è anche detta di *routing isolato - backward learning* (si veda il paragrafo 14.5.2) in quanto un indirizzo di sorgente attuale crea o aggiorna una entry dinamica della tabella di instradamento relativamente ad una destinazione che potrà essere utilizzata in futuro.

La figura 10.9 illustra il ruolo dell'informazione di stato relativa alla porta che riceve il pacchetto, allo scopo di determinare se l'informazione relativa alla locazione della stazione possa essere incorporata nel filtering database. In caso

positivo, nella tabella di instradamento viene inserito l'indirizzo MAC della stazione trasmittente e la direzione, cioè la porta del bridge da cui è stato ricevuto il pacchetto.

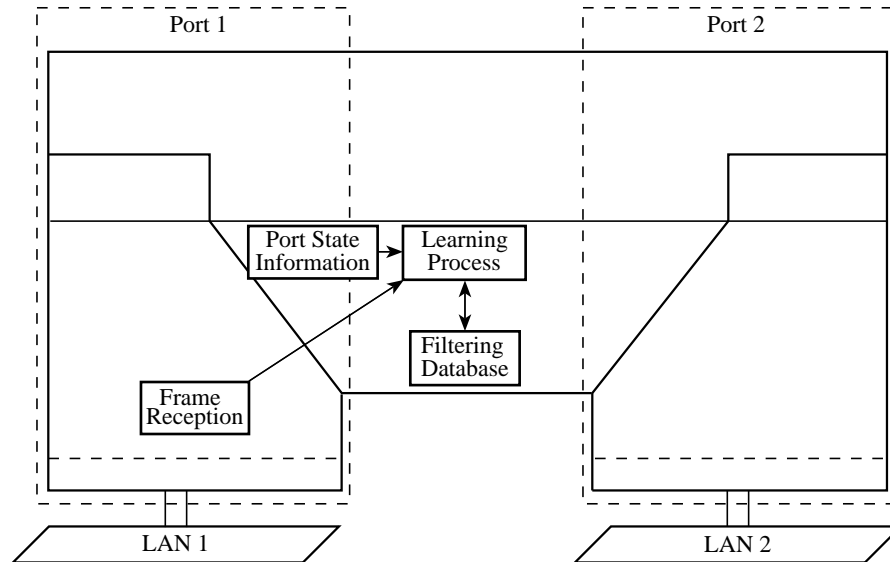


Fig. 10.9 - Processo di apprendimento.

Le condizioni in cui è possibile creare o aggiornare una entry dinamica sono:

- la porta da cui è stato ricevuto il pacchetto deve essere in uno stato che permetta l'apprendimento dell'indirizzo MAC (stato di learning o di forwarding);
- non esiste già una entry statica per quell'indirizzo MAC.

Se il numero risultante di tutte le entry supera la capacità massima della tabella di instradamento, una entry più vecchia viene rimossa per far spazio alla nuova entry.

10.11 BRIDGE MANAGEMENT

Lo standard IEEE 802.1B specifica i protocolli e le operazioni relative al management remoto dei bridge. I protocolli di bridge management fanno uso del servizio fornito dai sottolivelli LLC del bridge.

10.12 INDIRIZZAMENTO

Le entità MAC che comunicano attraverso una BLAN adottano il classico indirizzo MAC su 48 bit (si veda il paragrafo 5.6.7). In particolare, sia le porte dei bridge, sia i bridge stessi devono avere un indirizzo MAC. Gli indirizzi delle porte sono utilizzati dai protocolli di spanning tree e di management. Le porte vengono inoltre identificate all'interno del bridge con un numero progressivo a partire da 1. L'indirizzo del bridge coincide con l'indirizzo MAC della porta 1.

10.13 ENTITÀ DI PROTOCOLLO DEI BRIDGE

Le entità di protocollo dei bridge (*bridge protocol entities*) realizzano l'algoritmo di spanning tree. Esse operano tramite le BPDU (*Bridge Protocol Data Unit*) trasmesse in multicast all'indirizzo MAC denominato *bridge group address* (tabella 10.2).

Assignment	Value
Bridge group address	01-80-C2-00-00-00
Reserved for future standardization	01-80-C2-00-00-01÷ 01-80-C2-00-00-0F

Tab. 10.2 - Indirizzi di gruppo dei bridge.

Lo Standard 802.1D definisce inoltre il valore del LLC-SAP per il protocollo di spanning tree in 042H (in binario 01000010 è un numero palindromo e questo risolve alcuni problemi di incompatibilità tra gli standard relativamente a MSB e LSB).

La figura 10.10 illustra le operazioni effettuate dalle entità di protocollo dei bridge ed in particolare la modifica delle informazioni di stato delle porte e della tabella di instradamento. Tale modifica viene elaborata dall'algoritmo di spanning tree quando sia necessario determinare una nuova topologia attiva della BLAN.

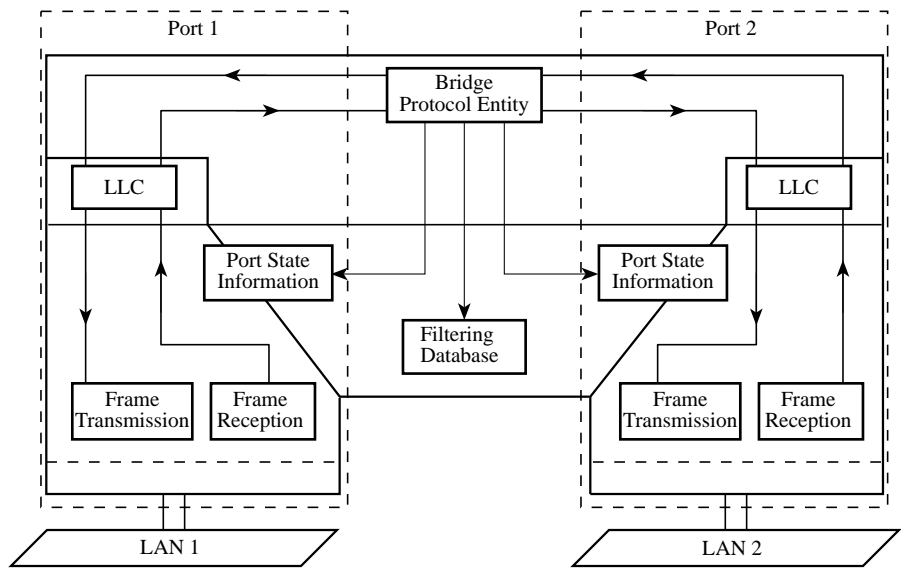


Fig. 10.10 - Entità di protocollo.

10.14 ENTITÀ DI MANAGEMENT DEI BRIDGE

Le entità di management dei bridge (*bridge management entities*) trasmettono e ricevono pacchetti di management, usando il servizio fornito dalle entità LLC associate alle porte. Lo standard IEEE 802.1D specifica l'indirizzo di multicast denominato *all LANs bridge management group address* (tabella 10.3). Tale indirizzo serve a raccogliere tutte le richieste delle entità di bridge management associate a tutte le porte dei bridge connesse alla BLAN.

Assignment	Value
All LANs bridge management group address	01-80-C2-00-00-10

Tab. 10.3 - Indirizzo riservato per il management dei bridge.

10.15 SUPPORTO DEL SERVIZIO MAC

I bridge realizzano le primitive `MA_UNIDATA.request` e `MA_UNIDATA.indication` di un servizio non connesso e non confermato (*unacknowledged connectionless service*).

Questo implica che quando un sistema trasmette un pacchetto indirizzato ad un altro sistema che si trova su un'altra LAN, il bridge non conferma alla stazione trasmittente l'avvenuta ritrasmissione del pacchetto. L'uso di servizi di tipo confermato non è ammesso.

Il servizio offerto da una BLAN è simile a quello di una singola LAN, di conseguenza un bridge non è direttamente indirizzato dai sistemi comunicanti, eccetto che per scopi di management del bridge stesso.

La presenza di bridge non deve porre restrizioni sulla posizione dei sistemi nella BLAN che deve poter variare dinamicamente (ad esempio, un PC portatile deve poter essere connesso prima a una LAN o poi ad una seconda LAN e i bridge devono adattare le loro tabelle di instradamento al cambiamento di posizione).

10.16 QUALITÀ DEL SERVIZIO

La qualità del servizio MAC offerto da una BLAN non deve essere significativamente inferiore a quella fornita da una singola LAN. I parametri da considerare in relazione alla qualità del servizio sono descritti nei seguenti sottoparagrafi.

10.16.1 Disponibilità del servizio

La disponibilità del servizio è misurata come la percentuale di tempo durante il quale il servizio è fornito. La presenza di un bridge può aumentare o ridurre la disponibilità del servizio.

La disponibilità del servizio può essere aumentata tramite la possibilità di riconfigurare automaticamente la BLAN, nel caso in cui uno dei percorsi non sia più disponibile a seguito di un guasto ad uno dei componenti (repeater, cavi, connettori).

La disponibilità del servizio può essere ridotta a seguito del guasto di un bridge o durante le operazioni di riconfigurazione della topologia di rete. Infatti, un bridge può bloccare il servizio e scartare i pacchetti, per preservare altri aspetti importanti del servizio MAC, quando avviene una riconfigurazione automatica, ad esempio per evitare la creazione di loop.

10.16.2 Pacchetti persi o fuori sequenza

Il servizio non connesso fornito dal sottolivello MAC non garantisce il recapito dei pacchetti. I pacchetti trasmessi dalla stazione sorgente hanno tuttavia

elevate probabilità di arrivare integri alla stazione destinataria. La presenza di un bridge incrementa leggermente la probabilità di perdita di pacchetti nei seguenti casi:

- il bridge non è in grado di trasmettere il pacchetto entro un certo tempo massimo (*maximum bridge transit delay*), quindi deve scartarlo;
- il bridge non è in grado di immagazzinare altri pacchetti a causa della saturazione del buffer interno, in quanto i pacchetti continuano ad arrivare ad una velocità superiore a quella di inoltro;
- la dimensione del pacchetto eccede quella massima ammessa dal MAC della LAN di destinazione;
- durante un cambiamento di topologia il bridge deve scartare i pacchetti per un limitato periodo di tempo, in modo da garantire altri aspetti della qualità del servizio.

Il servizio fornito dai bridge garantisce una trasmissione ordinata dei pacchetti tra mittente e destinatario.

10.16.3 Duplicazione di pacchetti

I bridge non devono introdurre la duplicazione dei pacchetti. Questa, tuttavia, può essere causata da una trasmissione attraverso più bridge facenti parte di percorsi alternativi (figura 10.11). Questo potenziale problema viene risolto dall'algoritmo di spanning tree.

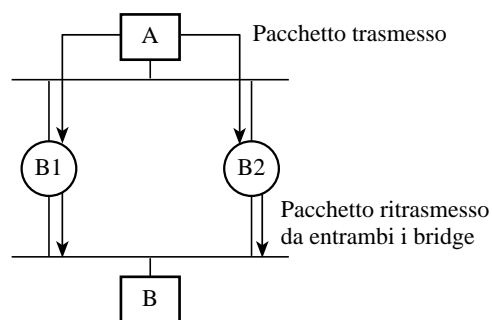


Fig. 10.11 - Duplicazione di pacchetti.

10.16.4 Ritardo di transito

Un bridge introduce un ritardo di transito addizionale poiché esso deve svolgere le seguenti funzioni prima di ritrasmettere il pacchetto ricevuto:

- aspettare di aver ricevuto completamente il pacchetto;
- verificare la FCS ed eventualmente scartare il pacchetto corrotto;
- controllare la tabella di instradamento per decidere se e dove inoltrare il pacchetto.

10.16.5 Dimensione massima della Service Data Unit

La dimensione massima della Service Data Unit (campo dati del pacchetto) ammessa da una LAN IEEE 802 varia in funzione del MAC e di altri parametri ad esso associati (ad esempio, la velocità).

La dimensione massima di pacchetto ammessa da un bridge che interconnette due LAN è quella inferiore ammessa dalle LAN. Ad esempio, se un bridge interconnette una LAN 802.3 e una LAN FDDI, userà come massima dimensione della Service Data Unit quella di 802.3 e cioè 1500 byte, invece di usare quella di FDDI che è di 4478 byte.

10.16.6 Throughput

Il throughput totale ammesso da una BLAN può essere significativamente maggiore di quello ammesso da una singola LAN. Ad esempio, il throughput globale della BLAN di figura 10.12 (cinque LAN 802.3, interconnesse da bridge full-speed) è di 50 Mb/s (10 Mb/s per 5 LAN).

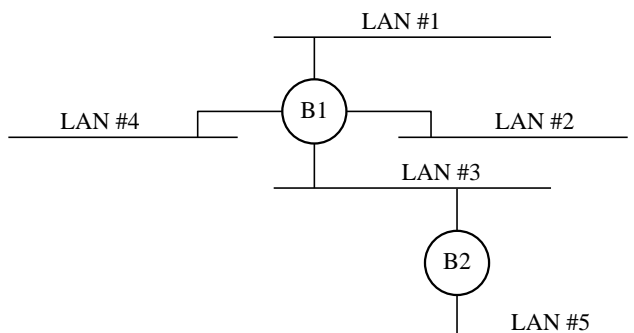


Fig. 10.12 - Throughput di una BLAN.

In figura 10.13 è riportato un esempio riferito ad una BLAN nella quale, a causa del bridge B che non è full-speed, e che ha quindi un inter frame spacing elevato, si ha una perdita di pacchetti quando la stazione A trasmette in continuazione pacchetti alla stazione E. In questo esempio, che rappresenta un caso limite, si ha una perdita del 50% dei pacchetti.

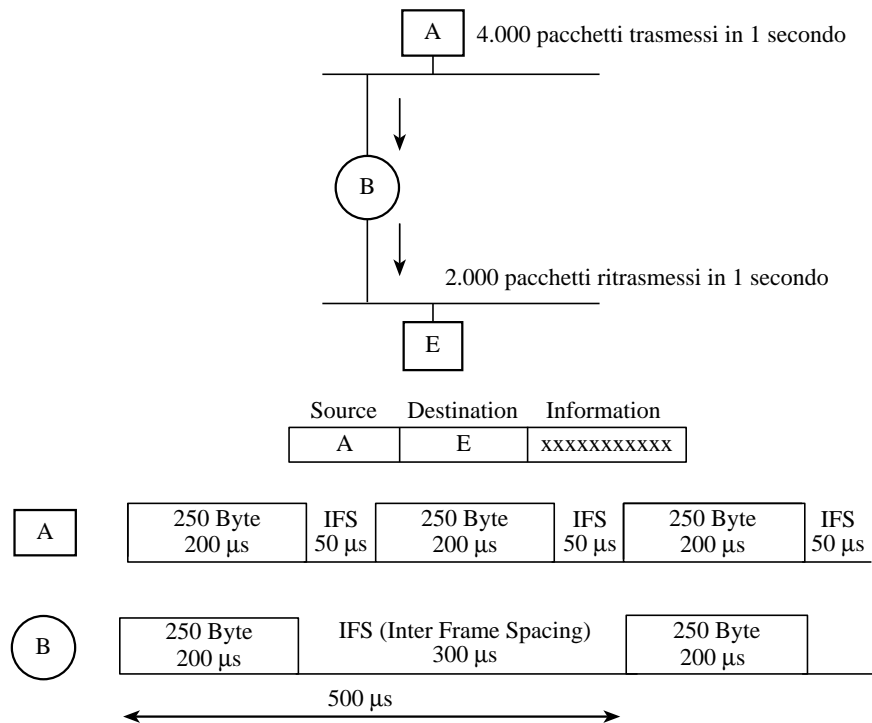


Fig. 10.13 - LAN interconnesse da bridge non full-speed.

10.17 SPANNING TREE

L'algoritmo di spanning tree riconfigura una topologia magliata di una BLAN in una topologia ad albero, eliminando i loop nel caso in cui ci siano più percorsi alternativi. In caso di guasto sul percorso primario, lo spanning tree deve riconfigurare automaticamente la topologia della BLAN, senza la formazione di loop nel transitorio. L'algoritmo di spanning tree opera attraverso un protocollo di spanning tree che genera BPDU (Bridge PDU).

Le caratteristiche desiderate dell'algoritmo di spanning tree sono:

- stabilizzare in breve tempo la topologia riconfigurata di una BLAN per ridurre il disservizio della rete;
- garantire che i percorsi tra sistemi siano prevedibili, riproducibili e configurabili tramite opportuni parametri;
- avere un limitato consumo di banda per le BPDU che i bridge si devono scambiare;
- ammettere che un bridge venga aggiunto alla BLAN senza che siano indispensabili operazioni di configurazione.

Per gestire la configurazione della topologia attiva l'algoritmo di spanning tree prevede l'assegnazione di una priorità ai bridge e alle porte di ciascun bridge. Tutti i bridge devono inoltre avere un identificatore univoco. A tal fine si definisce il *bridge ID* come la concatenazione della *priorità del bridge* definita da management (2 byte) e dell'indirizzo MAC del bridge (6 byte). Anche la *priorità della porta* (1 byte) è definita da management. I valori numerici più bassi indicano priorità maggiore.

La configurazione di una topologia attiva (albero) partendo da una topologia arbitraria (maglia) avviene ponendo alcune porte di alcuni bridge in blocking state. Infatti un bridge inoltra i pacchetti solo sulle porte che si trovano in forwarding state. Le porte che sono in blocking state non partecipano alla topologia attiva, ma sono pronte ad entrare a farne parte in caso di guasto di qualche componente della BLAN.

La figura 10.14 mostra un esempio di una BLAN configurata in modo magliato.

La figura 10.15 mostra una possibile topologia attiva della stessa BLAN.

10.17.1 L'algoritmo di spanning tree

L'algoritmo di spanning tree opera nei seguenti passi:

- *elezione del root bridge*: poiché si vuole identificare un albero, il primo passo consiste nell'identificare la radice dell'albero, cioè il *root bridge*. Il root bridge è per definizione il bridge che ha bridge ID minore;
- *selezione della root port*: per ogni bridge si identifica la porta più "conveniente" per interconnettere il bridge verso il root bridge. Tale porta è detta *root port*;

- *selezione del designated bridge*: per ogni LAN si sceglie quale bridge è designato a interconnettere la LAN con il root bridge. Questo passo è particolarmente importante quando esistono più cammini tra la LAN e il root bridge. Ogni LAN ha quindi un solo designated bridge che è il bridge "più vicino" al root bridge e che si incaricherà di trasmettere i pacchetti verso il root bridge. La porta del designated bridge che interconnette la LAN è detta *designated port*. Il root bridge è l'unico bridge che ha tutte *designated port*.

Al termine di questi tre passi si può procedere alla messa in stato di blocking delle porte che non sono né root né designated.

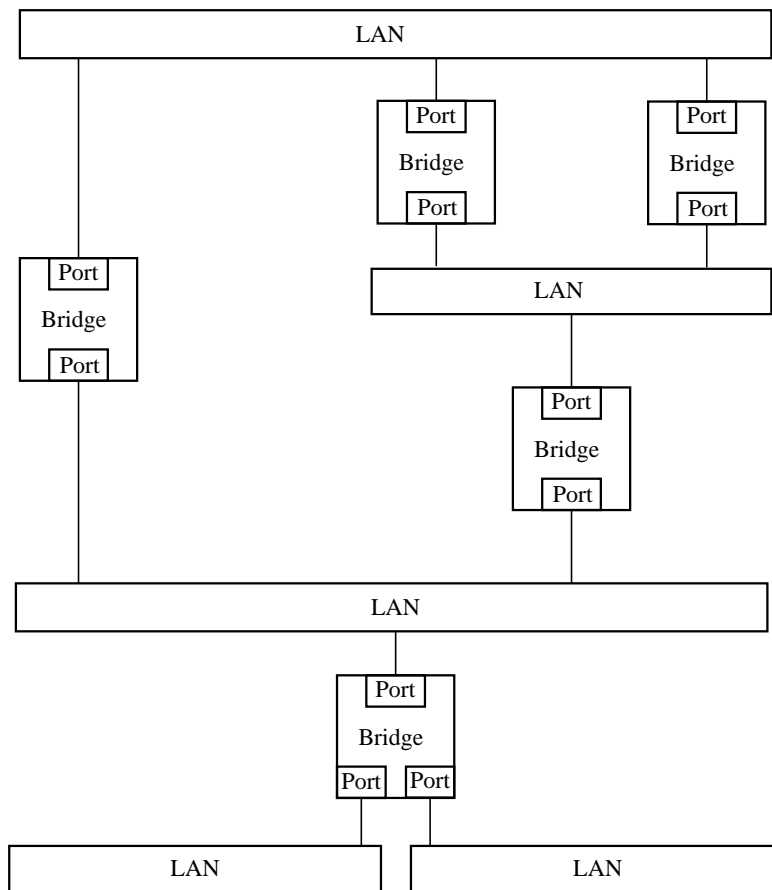


Fig. 10.14 - Una BLAN magliata.

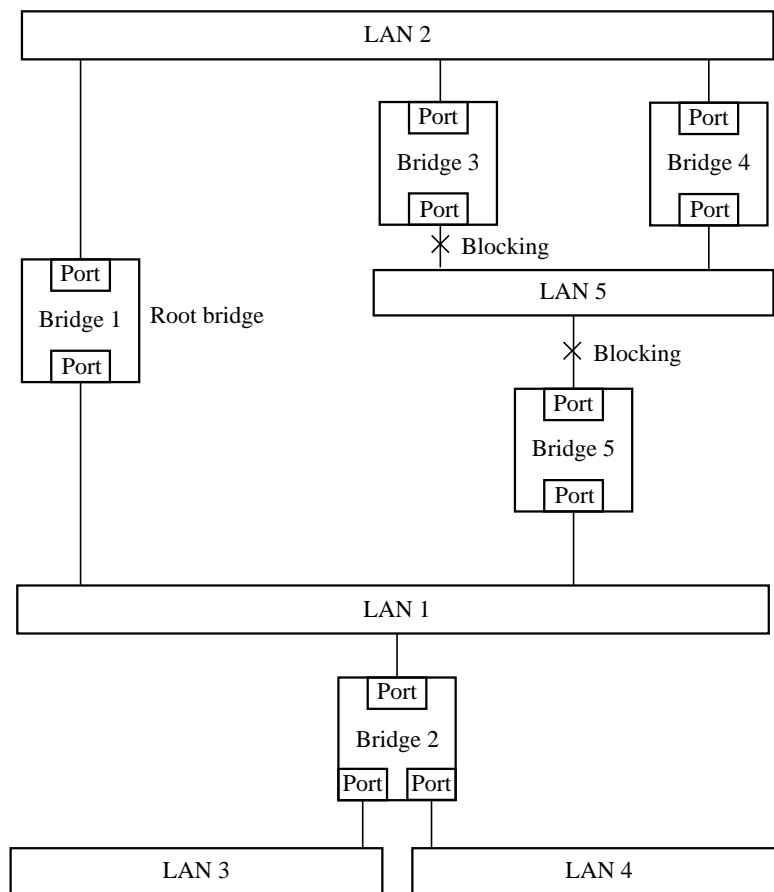


Fig. 10.15 - Topologia attiva ad albero.

In figura 10.15 il bridge 1 è stato eletto come root bridge ed è quindi il designated bridge per la LAN 1 e la LAN 2, il bridge 2 è il designated bridge per la LAN 3 e la LAN 4 e il bridge 4 è il designated bridge per la LAN 5. Le porte del bridge 3 e del bridge 5 collegate alla LAN 5 sono state messe in stato di blocking.

La figura 10.16 mostra lo spanning tree di questa configurazione attiva della BLAN.

Ogni porta ha un path cost che può essere configurato da management e che indica il costo di attraversamento di quella porta. Per ogni bridge e per ogni porta del bridge si definisce inoltre il *root path cost* come il costo totale di percorso per raggiungere il root bridge.

Il root path cost delle porte serve a due scopi:

- all'interno di un bridge, per scegliere quale sia la root port (quella che ha root path cost minore);
- tra le non root port dei bridge che si collegano su una LAN, per scegliere la designated port (quella che ha root path cost minore).

Il gestore della VLAN può controllare la formazione delle topologie attive intervenendo sui parametri bridge ID, port priority e path cost.

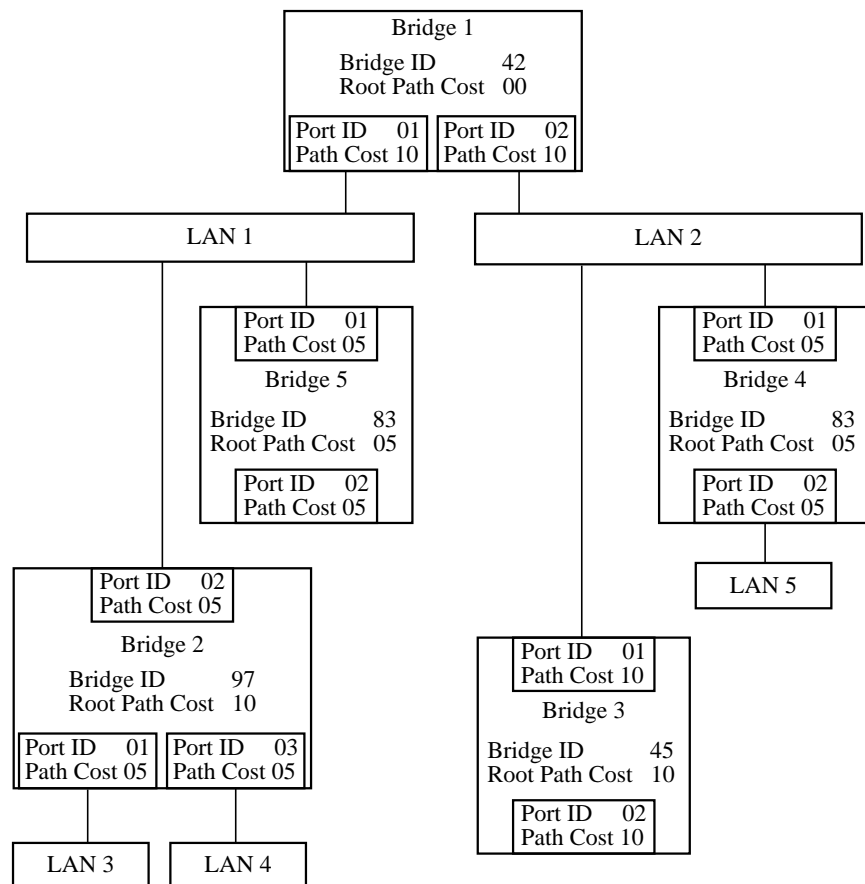


Fig. 10.16 - Esempio di spanning tree.

10.17.2 Bridge PDU e loro utilizzo nell'algoritmo di spanning tree

Le BPDU sono i pacchetti del protocollo 802.1D spanning tree che servono a realizzare il protocollo stesso.

Il root bridge genera periodicamente delle configuration BPDU (figura 10.17) che vengono trasmesse in multicast a tutti i bridge della BLAN. Gli altri bridge, quando ricevono una BPDU, ne aggiornano alcuni campi e la ritrasmettono sulle designated port.

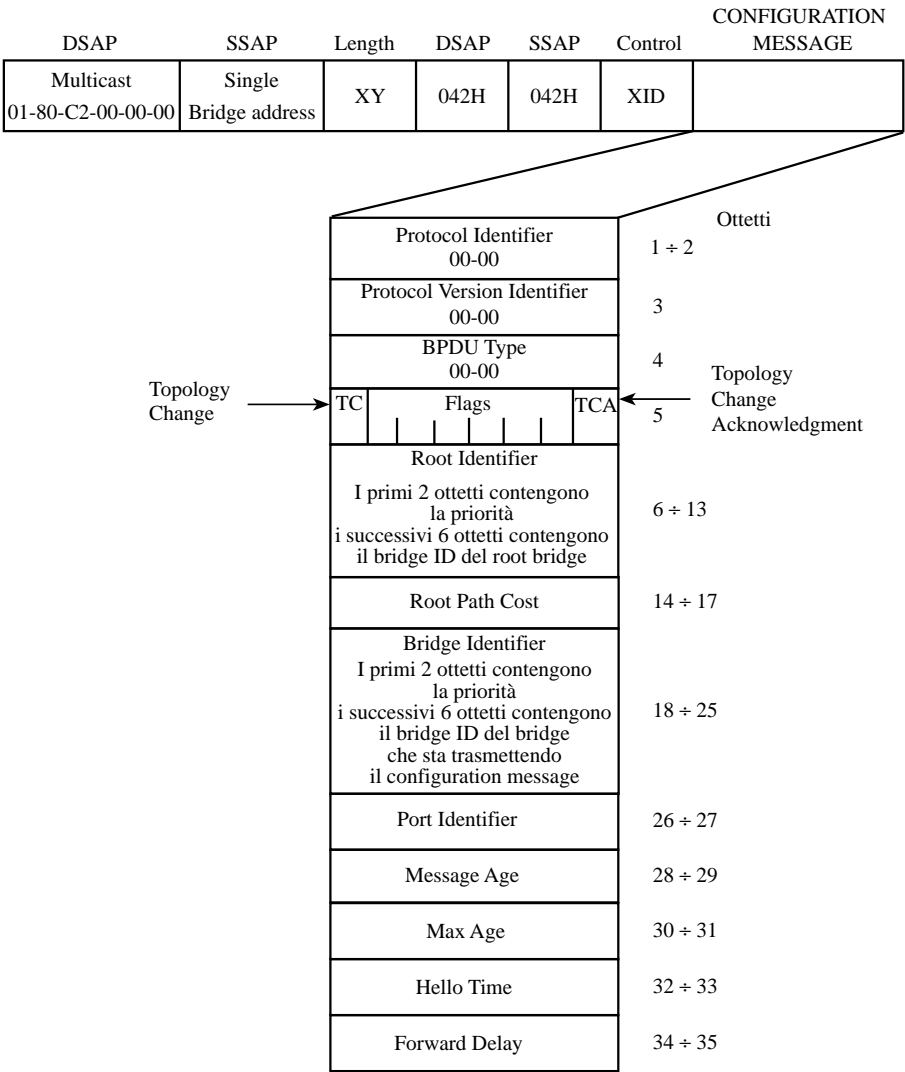


Fig. 10.17 - Configuration Bridge PDU.

I campi presenti in una configuration BPDU sono:

- *root identifier*: è l'identificatore del root bridge. Esso è composto da una prima parte di due ottetti, che è la priorità, e da una seconda parte di 6 ottetti, che è l'indirizzo MAC del root bridge;
- *root path cost*: è il costo totale di percorso per raggiungere il root bridge; questo valore è aggiornato ad ogni attraversamento di un bridge;
- *bridge identifier*: è l'identificatore del bridge che ha ritrasmesso il messaggio di configurazione. Esso è composto da una prima parte di due ottetti, che è la priorità, e da una seconda parte di 6 ottetti, che è l'indirizzo MAC del bridge;
- *port identifier*: è l'identificatore della porta da cui è stata trasmessa la BPDU. Esso è composto da una prima parte (primo ottetto) che è la priorità e da una seconda parte (secondo ottetto) che è il numero identificativo della porta (il valore zero non è ammesso);
- *message age*: è il tempo stimato (in multipli di 4 millisecondi) trascorso da quando il root bridge ha generato la configuration BPDU;
- *max age*: è il valore massimo di tempo (in multipli di 4 millisecondi) trascorso il quale la configuration BPDU deve essere scartata;
- *hello time*: è l'intervallo di tempo che intercorre tra la generazione di due configuration BPDU successive;
- *forward delay*: indica il tempo di permanenza nello stato di listening prima di passare allo stato di learning e nello stato di learning prima di passare a quello di forwarding;
- *Topology Change (TC)*: è un flag che viene impostato dal root bridge in tutti i pacchetti di configuration BPDU trasmessi a seguito della ricezione di un pacchetto di topology change notification BPDU o del rilevamento di un cambiamento di topologia;
- *Topology Change Acknowledgment (TCA)*: è un flag che viene messo a uno in una configuration BPDU dal designated bridge di una LAN, in risposta ad un pacchetto di topology change notification BPDU.

Per comprendere il ruolo delle configuration BPDU assumiamo di trovarci in un istante iniziale in cui tutti i bridge vengono accesi contemporaneamente. Si verificano i seguenti fatti:

- ogni bridge crede di essere il root bridge (fino a quando non ha un diverso riscontro) e origina le configuration BPDU su tutte le LAN ad esso connesse ad intervalli regolari specificando come root bridge il suo bridge ID e come root path cost zero;

- quando un bridge riceve da un altro bridge una configuration BPDU confronta il bridge ID del bridge che ha generato la PDU con il suo bridge ID: se è minore esso smette di considerarsi un root bridge e quindi di generare le configuration BPDU.

Questo porta rapidamente all'elezione del root bridge, che diventa l'unico bridge che genera le configuration BPDU. Eletto il root bridge si procede nel seguente modo:

- ogni bridge riceve le configuration BPDU da tutte le porte ed autonomamente decide che la sua root port sia quella con il minor valore di root path cost. Nel caso in cui due o più porte presentino un root path cost uguale, verranno presi in considerazione i parametri di bridge identifier della BPDU e port identifier per selezionare la root port;
- un bridge che riceve una configuration BPDU "minore" (cioè che, paragonata ai parametri associati alla porta ricevente quali root path cost, bridge identifier e port identifier, risulti prioritaria) su una porta che esso considera essere una designated port per la LAN a cui è connessa, smette di considerare tale porta designated e la pone in blocking state in quanto la BPDU "minore" evidenzia l'esistenza di un cammino più conveniente verso il root bridge;
- le root port e le designated port sono messe in stato di forwarding, le altre in stato di blocking.

10.17.3 Notifica del cambiamento di topologia

Un bridge, durante la sua normale operatività, può accorgersi che la topologia attiva è stata riconfigurata senza che questo diventi evidente a tutti gli altri bridge. Questo può causare delle inconsistenze nelle tabelle di instradamento dei bridge che sono estremamente pericolose in quanto possono generare loop.

I loop nei bridge sono particolarmente temuti in quanto nelle MAC-PDU non c'è un contatore (*hop count*) che consenta di scartare un pacchetto che continua a girare su di un loop ed inoltre tali pacchetti possono facilmente moltiplicarsi se ritrasmessi da più di un bridge collegato alla stessa LAN.

Per questo motivo, non appena un bridge verifica un cambiamento di topologia, lo comunica al root bridge trasmettendo una *topology notification change BPDU* (figura 10.18). Tale PDU viene trasmessa sulla root port e il bridge che la riceve la ritrasmette sulla sua root port sino a quando la PDU arriva al root bridge. Il root bridge comunica tale cambiamento ponendo a 1 il *Topology Change flag (TC)* nella

configuration BPDU (figura 10.17). Il pacchetto di topology notification change viene ritrasmesso più volte dal bridge che l'ha generato fino a quando questo non riceve una risposta di acquisizione dal designated bridge della LAN su cui il pacchetto è stato trasmesso.

La conferma di acknowledgment (TCA) è contenuta nella configuration BPDU (figura 10.17).

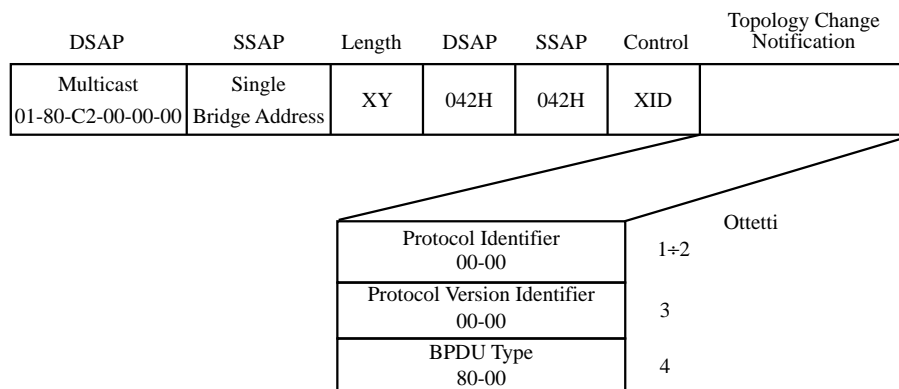


Fig. 10.18 - Topology Change Notification BPDU.

10.17.4 Cambio di stato delle porte

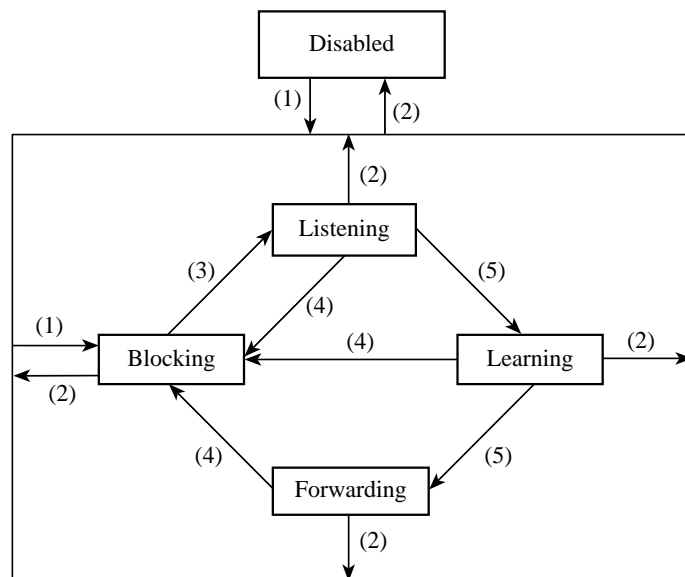
Il cambio di stato delle porte avviene seguendo precise sequenze, come viene rappresentato in figura 10.19. Esso può essere determinato sia dall'algoritmo di spanning tree, sia dal management.

Una porta *disabled* non partecipa alla topologia attiva della LAN, mentre una porta *enabled* può partecipare alla topologia attiva della LAN in funzione dello stato in cui si trova.

La transizione enabled-disabled e quella disabled-enabled sono controllate esclusivamente dal management o eventualmente in seguito all'insorgere di un guasto. Le porte enabled si possono trovare in uno degli stati sotto elencati.

- *Listening*. La porta si prepara a partecipare alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti. Il processo di learning non aggiunge nuove informazioni alla tabella di instradamento. La porta abbandona questo stato allo scadere del forward delay time per passare in stato di learning.

- *Learning*. La porta si prepara a partecipare alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti, ma il processo di learning aggiunge le informazioni ricevute alla tabella di instradamento. La porta abbandona questo stato allo scadere del forward delay time per passare in stato di forwarding.
- *Forwarding*. La porta partecipa alla ritrasmissione dei pacchetti. Il processo di forwarding può inoltrare i pacchetti ricevuti. Il processo di learning aggiunge le informazioni ricevute alla tabella di instradamento.
- *Blocking*. La porta non partecipa alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti. Una porta entra in stato di blocking perché ha ricevuto l'informazione che un'altra porta, facente parte del medesimo o di un altro bridge, è la designated port per la LAN a cui è connessa.



- (1) Porta abilitata dal management o dall'inizializzazione
- (2) Porta disabilitata dal management o da un guasto
- (3) L'algoritmo seleziona la porta come una designated o root port
- (4) L'algoritmo seleziona la porta come una "non designated port" o "non root port"
- (5) Il forward delay timer è scaduto

Fig. 10.19 - Diagramma di stato delle porte.

10.17.5 Parametri raccomandati

Lo standard 802.1D raccomanda che non ci siano più di sette bridge in cascata e che vengano rispettati i parametri della tabelle 10.4, 10.5, 10.6 e 10.7.

Parameter	Recommended Value	Absolute Maximum
Maximum Bridge transit delay	1	4
Maximum BPDU transmission delay	1	4
Maximum Message Age increment overestimate	1	4

Tutti i tempi sono espressi in secondi

Tab. 10.4 - Ritardi di transito e trasmissione.

Parameter	Recommended or Default Value	Fixed Value	Range
Bridge Hello Time	2	-	1 ÷ 10
Bridge Max Age	20	-	6 ÷ 40
Bridge Forward Delay Timer	15	-	4 ÷ 30
Hold Time	-	1	-

Tutti i tempi sono espressi in secondi

Tab. 10.5 - Algoritmo di spanning tree - tempi consigliati.

Parameter	Recommended or Default Value	Range
Bridge Priority	32768	0 ÷ 65535
Port Priority	128	0 ÷ 255

Tab. 10.6 - Priorità dei bridge e delle porte - valori consigliati.

Parameter	Recommended Value	Absolute Minimum	Range
Path Cost	$\text{Path Cost} = \frac{1000}{\text{Attached LAN speed in Mb/s}}$	1	0 ÷ 65535

Tab. 10.7 - Parametro path cost - valore consigliato.

10.18 SOURCE ROUTING

Come già accennato nell'introduzione a questo capitolo, esistono anche dei bridge, progettati prima dello standard 802.1D, che usano una modalità detta *source routing*. Tali bridge sono stati concepiti per interconnettere esclusivamente LAN IEEE 802.5, e hanno avuto per un lungo periodo di tempo uno sviluppo parallelo a quello dei transparent bridge.

La necessità di interconnettere LAN 802.5 con LAN 802.3 fece nascere dei bridge denominati *source routing to transparent bridging* (SR-TB) che avrebbero dovuto risolvere il problema. Tali bridge risultarono molto complessi e si decise di abbandonarli.

Lo stato attuale degli standard prevede che i bridge standard siano transparent bridge e che la possibilità di effettuare source routing sia una prestazione addizionale. Un bridge in grado di realizzare source routing oltre al transparent bridging è detto *Source-Routing Transparent* (SRT) bridge.

Per semplicità di esposizione verranno illustrati prima i bridge puramente source routing e poi gli SRT.

10.19 BRIDGE PURAMENTE SOURCE ROUTING

I bridge source routing sono stati sviluppati per operare tra reti Token Ring in uno scenario simile a quello di figura 10.20. Essi sono esplicitamente indirizzati dalle stazioni che necessitano di inviare un messaggio sulla BLAN.

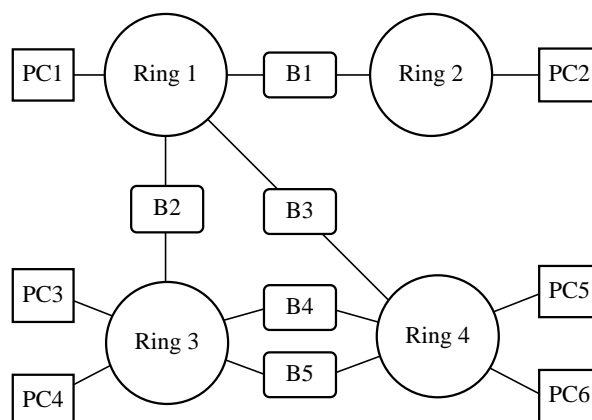


Fig. 10.20 - Una rete locale estesa Token Ring.

Se un pacchetto non ha un campo RI è un pacchetto destinato a un sistema connesso alla stessa LAN su cui è stato generato e viene quindi ignorato dai bridge.

Ogni bridge che inoltra un pacchetto multicast di route discovery ARE aggiunge al campo RI il suo identificativo e la massima dimensione ammissibile del pacchetto. In questo modo l'informazione d'instradamento viene costruita dai bridge al momento in cui il pacchetto di explorer viene inoltrato da un segmento di LAN ad un altro. Quando il pacchetto di explorer raggiunge la stazione di destinazione, esso contiene nel campo di RI tutte le informazioni di percorso e di massima dimensione del pacchetto ammissibile lungo l'intero percorso. La stazione di destinazione ritrasmette il pacchetto di explorer alla stazione mittente, che lo usa per calcolare la entry corrispondente nella tabella di instradamento. La stazione di destinazione riceve più copie del pacchetto di ARE, ma considera solo la prima in quanto ritenuta la più conveniente.

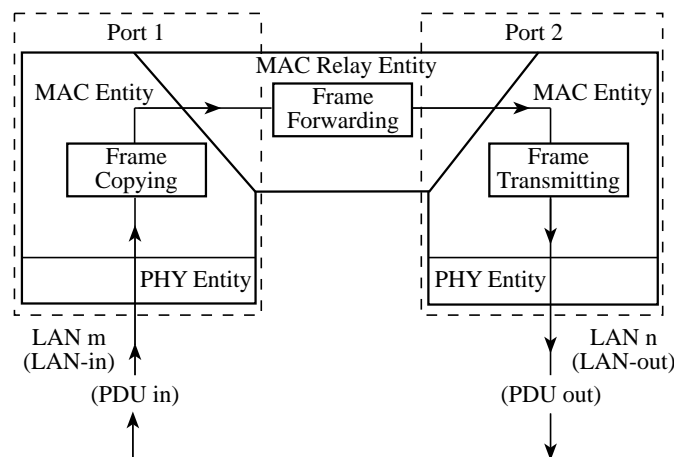


Fig. 10.21 - Elementi di un bridge source routing.

La figura 10.21 rappresenta gli elementi di un bridge source routing.

Poiché il campo RI non è presente in tutti i pacchetti token-ring, quando c'è è necessario indicarne la presenza. Per fare ciò, si utilizza il bit I/G (Individual/Global) dell'indirizzo MAC-SSAP (di mittente) che non serve non potendo valere altro che zero, essendo l'indirizzo di mittente sempre di un indirizzo singolo (figura 5.5). Tale bit viene ribattezzato RII e vale 0 in assenza di routing information e 1 in presenza di esse (figura 10.22).

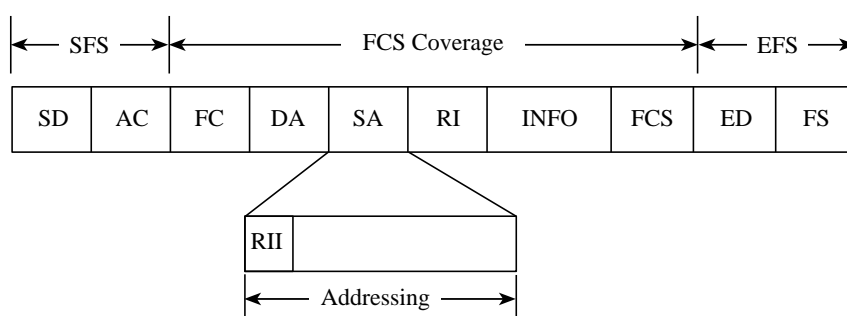


Fig. 10.22 - Formato del pacchetto 802.5.

10.20 SOURCE ROUTING TRANSPARENT BRIDGE

Un *Source-Routing Transparent (SRT) bridge* utilizza il metodo di source routing quando i pacchetti ricevuti contengono le informazioni di instradamento (RII = 1), ed utilizza il metodo transparent bridging quando i pacchetti ricevuti non contengono le informazioni di instradamento (RII = 0).

Il SRT bridge è l'unico bridge source routing riconosciuto a livello di standard. Nella modalità source-routing esso opera nel seguente modo:

- il sistema mittente determina a priori l'instradamento del messaggio includendolo in ogni pacchetto;
- l'instradamento è espresso come una serie di identificatori (anello, bridge);
- i bridge non hanno tabelle di instradamento in quanto queste sono mantenute ed utilizzate dai sistemi mittenti;
- quando un sistema vuole imparare l'instradamento verso un altro sistema, invia un pacchetto di route explorer a cui il destinatario risponde;
- il meccanismo ammette fino a otto bridge in cascata.

Nella modalità transparent bridging, un SRT bridge opera esattamente come descritto nei precedenti paragrafi sui transparent bridge e quindi utilizza una tabella di instradamento locale, costruita come spiegato nel paragrafo 10.6.

Quindi per ogni pacchetto la decisione di inoltrare è presa in base all'osservazione del campo RII dell'indirizzo MAC-SSAP: se è a 1, si utilizza l'informazione di instradamento contenuta nel campo RI, altrimenti la decisione di inoltrare viene presa in base alla tabella di instradamento locale al bridge e all'indirizzo di destinazione (secondo la logica del transparent bridging). La figura 10.23 illustra l'architettura logica di un bridge SRT.

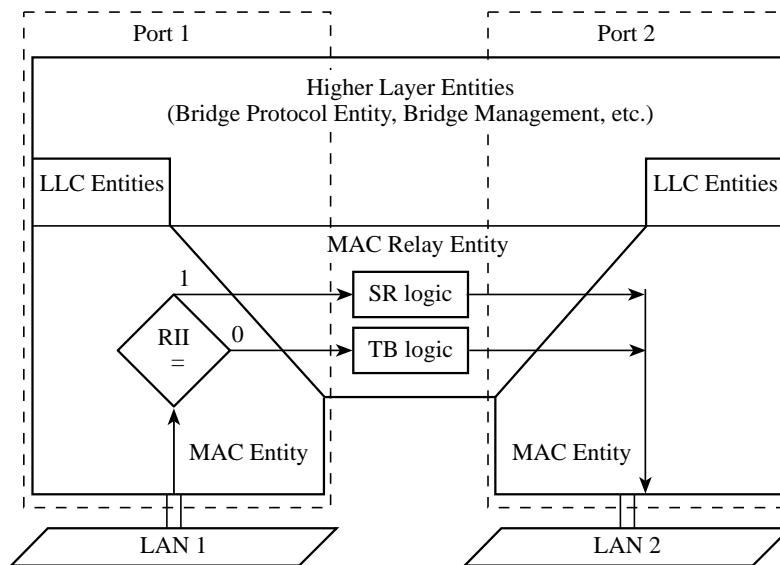


Fig. 10.23 - Schema logico di un bridge SRT.

10.20.1 Campo RI

Il campo di routing information è composto da due parti: il campo *routing control* (2 ottetti) e i campi *route descriptor* (da 2 ottetti ciascuno). La figura 10.24 illustra l'organizzazione del campo routing information.

I route descriptor contenuti nel campo RI possono essere al massimo 14 e quindi la lunghezza massima del campo RI è di 30 byte. La figura 10.25 illustra con maggiore dettaglio il campo routing information.

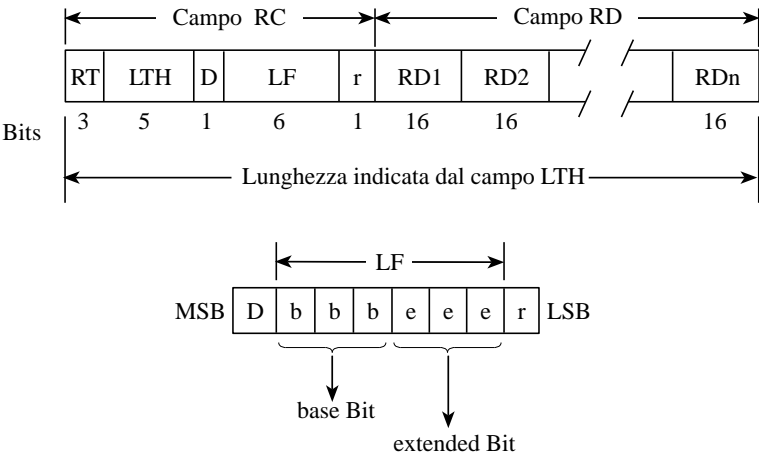


Fig. 10.24 - Campo RI.

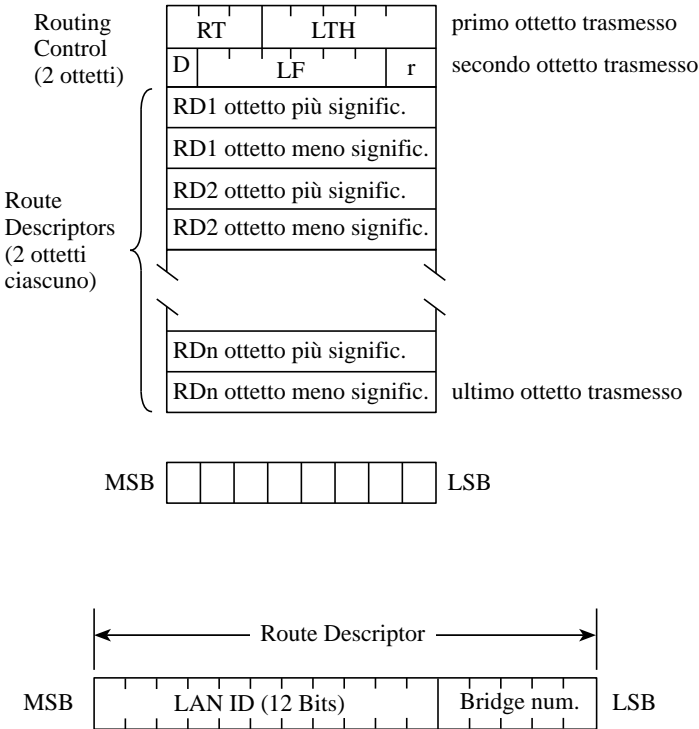


Fig. 10.25 - Dettaglio del campo RI.

10.20.2 Campo Routing Type (RT)

Questo campo indica se il pacchetto deve essere inoltrato attraverso la rete lungo un singolo percorso o lungo percorsi multipli. I routing type ammessi sono i seguenti:

- SRF (*Specifically Routed Frame*) (RT = 0XX). In questo tipo di pacchetto i campi RD (Route Descriptors) indicano un percorso specifico attraverso la rete;
- ARE (*All Routes Explorer frame*) (RT = 10X). Questo tipo di pacchetto viene instradato lungo tutti i percorsi della rete. Esso è originato da un sistema senza i route designators, che vengono aggiunti al pacchetto dai bridge SRT durante la fase di inoltro del pacchetto. Il sistema destinatario riceverà più pacchetti ARE i quali proporranno percorsi diversi;
- STE (*Spanning Tree Explorer frame*) (RT = 11X). Questo tipo di pacchetto può essere ritrasmesso da una LAN ad un'altra, solamente da una porta in *transparent bridging forwarding state*, con il risultato che il pacchetto verrà inoltrato a tutte le LAN appartenenti alla BLAN seguendo lo spanning tree, e raggiungerà ogni LAN una e una sola volta. L'utilizzo ovvio di questo tipo di pacchetto è per la trasmissione di pacchetti multicast.

10.20.3 Campo Length (LTH)

I cinque bit del campo indicano la lunghezza del campo RI in ottetti. La dimensione del campo RI è compresa tra due e trenta ottetti.

10.20.4 Campi LAN ID e bridge number

LAN ID è un identificativo univoco per ogni LAN assegnato dal gestore della BLAN. Poiché la tecnica SRT permette di avere percorsi multipli tra due LAN (tramite bridge collegati in parallelo), viene assegnato anche un numero di bridge (*bridge number*) ad ogni bridge. Tale bridge number non deve essere univoco su tutta la BLAN, ma solo nell'ambito dei bridge collegati in parallelo. Quindi un percorso tra due LAN è identificato da una serie di coppie {LAN ID, bridge number}.

10.20.5 Campo Direction (D)

Questo campo indica la direzione in cui il pacchetto attraversa la rete. Essa è indicata dal valore del bit D:

- se il bit D = 0, la direzione sarà quella specificata nel campo di Routing Information (da RD1 a RD2 ... a RDn);
- se il bit D = 1, la direzione sarà inversa a quella specificata dal campo di Routing Information (da RDn a ... RD2 a RD1).

Nei pacchetti STE e ARE il bit D è impostato a zero.

10.20.6 Campo di Largest Frame (LF)

I bit del campo indicano la dimensione massima del MAC Service Data Unit (parte INFO del pacchetto) che può essere trasmessa tra due stazioni comunicanti su uno specifico percorso (route). I bit del campo LF hanno significato solo per i pacchetti STE e ARE, mentre essi vengono ignorati dai pacchetti SRF. Una stazione che origina un pacchetto di explorer imposta i bit del LF alla massima dimensione che può trattare, i bridge che inoltrano il pacchetto potranno ridurre il valore contenuto in LF che non dovrà eccedere:

- il valore indicato dai bit LF ricevuti;
- la dimensione massima della MAC SDU ammessa dal bridge;
- la dimensione massima della MAC SDU ammessa dalla porta ricevente;
- la dimensione massima della MAC SDU ammessa dalla porta trasmittente.

La figura 10.24 illustra il campo LF e le tabelle 10.8, 10.9 e 10.10 illustrano i valori massimi di LF impostabili.

000:	516	ottetti (ISO 8473 più LLC)
001:	1.470	ottetti (ISO/IEC 8802.3, CSMA/CD)
010:	2.052	ottetti (matrice caratteri dello schermo 80x24)
011:	4.399	ottetti (ISO/IEC 8802.5, FDDI, 4 Mb/s Token Ring, ISO 9314-3)
100:	8.130	ottetti (ISO/IEC 8802.4 Token Bus)
101:	11.407	ottetti (ISO/IEC 8802.5 4-bit burst error unprotected)
110:	17.749	ottetti (ISO/IEC 8802.5 16 Mb/s Token Ring)
111:	41.600	ottetti (base per estendere fino a 65.535 ottetti)

Tab. 10.8 - Origine dei valori LF.

Base	Valore in ottetti	Base	Valore in ottetti
000	516	100	8.130
001	1.470	101	11.407
010	2.052	110	17.749
011	4.399	111	>17.749

Tab. 10.9 - Valori di Largest Frame base.

		EXTENSION							
B A S E		000	001	010	011	100	101	110	111
	000	516	635	754	873	993	1.112	1.231	1.350
	001	1.470	1.542	1.615	1.688	1.761	1.833	1.906	1.979
	010	2.052	2.345	2.638	2.932	3.225	3.518	3.812	4.105
	011	4.399	4.865	5.331	5.798	6.264	6.730	7.197	7.663
	100	8.130	8.539	8.949	9.358	9.768	10.178	10.587	10.997
	101	11.407	12.199	12.992	13.785	14.578	15.370	16.163	16.956
	110	17.749	20.730	23.711	26.693	29.674	32.655	35.637	38.618
	111	41.600	44.591	47.583	50.575	53.567	56.559	59.551	>59.551

Tab. 10.10 - Valori di Largest Frame estesi.

BIBLIOGRAFIA

- [1] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.
- [2] R. Perlman, "Interconnections: Bridges and Routers", Addison Wesley, Reading MA (USA), 1992.
- [3] Special Issue on Bridges, IEEE Network, Vol.2, No.1, January 1988.
- [4] R.P. Davidson, N.J. Muller, "Internetworking LANs: Operation, Design and Management", Artech House, London (UK), 1992.
- [5] IEEE Std 802, "Overview and Architecture", Piscataway N.J. (USA).
- [6] ISO/IEC 10038 [ANSI/IEEE Std 802.1D] MAC Bridging, 1993.
- [7] ISO/IEC 8802-5 [IEEE Std 802.5], "Token ring access method and physical layer specifications", 1992.