

Corso di Laurea in Ingegneria Informatica



**Corso di Reti di Calcolatori
(a.a. 2011/12)**

**Roberto Canonico (roberto.canonico@unina.it)
Giorgio Ventre (giorgio.ventre@unina.it)**

**Interconnessione di LAN
Hub, bridge e switch**

2 dicembre 2011

**I lucidi presentati al corso sono uno strumento didattico
che NON sostituisce i testi indicati nel programma del corso**

Nota di copyright per le slide COMICS



Nota di Copyright

Questo insieme di trasparenze è stato ideato e realizzato dai ricercatori del Gruppo di Ricerca COMICS del Dipartimento di Informatica e Sistemistica dell'Università di Napoli Federico II. Esse possono essere impiegate liberamente per fini didattici esclusivamente senza fini di lucro, a meno di un esplicito consenso scritto degli Autori. Nell'uso dovranno essere esplicitamente riportati la fonte e gli Autori. Gli Autori non sono responsabili per eventuali imprecisioni contenute in tali trasparenze né per eventuali problemi, danni o malfunzionamenti derivanti dal loro uso o applicazione.

Autori:
Simon Pietro Romano, Antonio Pescapè, Stefano Avallone,
Marcello Esposito, Roberto Canonico, Giorgio Ventre

Token Passing: standard IEEE 802.5

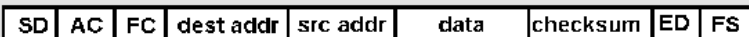
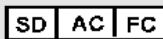


- 4 Mbps
- max token holding time: 10 ms (limita la massima lunghezza del frame)



- **SD, ED** rappresentano inizio e fine del frame
- **AC**: access control byte:
 - **token bit**: valore 0 significa che il token può essere preso, valore 1 indica che dei dati seguono il FC
 - **priority bits**: priorità della frame
 - **reservation bits**: una stazione può configurare questi bit per evitare che le stazioni con una priorità più bassa possano impossessarsi del token quando quest'ultimo diventa libero

Token Passing: standard IEEE 802.5



- **FC**: frame control utilizzato per effettuare monitoraggio e gestione della rete
- **source, destination address**: 48 bit per gli indirizzi fisici, così come in Ethernet
- **data**: pacchetto proveniente dal livello rete
- **checksum**: CRC
- **FS**: frame status: impostato dal **receiver** e letto dal **sender**
 - set per indicare che il ricevente è attivo, e che il frame è stato prelevato dall'anello
 - ACK di livello DLC

Interconnettere più LAN



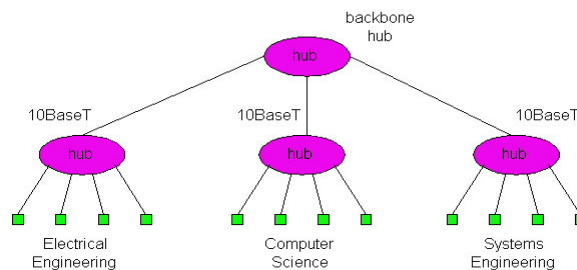
D: Perché non creare un'unica grande LAN?

- Limitata quantità di banda disponibile, considerato che su una singola LAN tante stazioni dovrebbero condividere la banda
- Estensione limitata: ad esempio, 802.3 specifica la massima lunghezza del cavo
- “Dominio di collisione” troppo ampio (una trasmissione può collidere con molte altre)
- Numero limitato di stazioni: ad esempio, 802.5 introduce un ritardo in ogni stazione dovuto al passaggio del token

Hub



- Dispositivi di Livello Fisico:
 - sostanzialmente si tratta di ripetitori di bit
 - riproducono i bit in ingresso ad un'interfaccia su tutte le altre interfacce
- Gli hub possono essere organizzati in una gerarchia (o architettura multi-livello), con un backbone hub al livello più alto



Hub: caratteristiche



- Ogni LAN collegata è considerata come un **segmento di LAN**
- Gli hub **non isolano** i domini di collisione:
 - le stazioni possono subire una collisione per una trasmissione simultanea con qualunque stazione presente su qualunque segmento
- Vantaggi degli hub:
 - Sono dispositivi semplici e poco costosi
 - L'organizzazione Multi-livello garantisce una parziale tolleranza ai guasti: porzioni di LAN continuano a funzionare in caso di guasto ad uno o più hub
 - Estende la massima distanza esistente tra i nodi (100m per ogni Hub)

Limiti degli hub



- La creazione di un singolo dominio di collisione non comporta alcun aumento del throughput massimo
 - Il throughput complessivo in una rete multi-livello è lo stesso di una rete con un unico segmento
- La realizzazione di un'unica LAN impone un limite al numero massimo di stazioni che è possibile collegare, nonché all'estensione geografica che è possibile raggiungere
- Solo una tipologia di Ethernet (per esempio, 10BaseT e 100baseT)

Bridge (1/2)



- **Dispositivi di livello 2:** in grado di leggere le intestazioni di frame Ethernet, ne esaminano il contenuto, e selezionano il link d'uscita sulla base dell'indirizzo destinazione
- I bridge **isolano** i domini di collisione, grazie alla loro capacità di porre le frame in un buffer (dispositivi store & forward)
- Non appena una frame può essere inoltrata su un link d'uscita, un bridge usa il protocollo CSMA/CD sul segmento LAN d'uscita prima di trasmettere

Bridges (2/2)



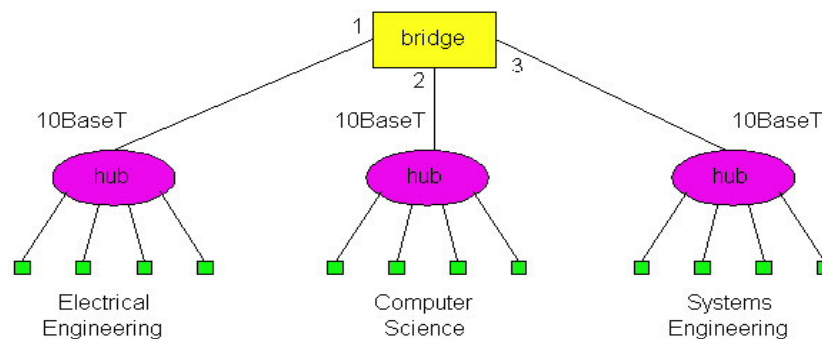
- Vantaggi dei bridge:
 - Isolano i domini di collisione, determinando un aumento complessivo del throughput massimo
 - Non introducono limitazioni sul numero massimo delle stazioni, né sull'estensione geografica
 - Possono collegare differenti tecnologie, dal momento che sono dispositivi di tipo store & forward
 - Trasparenti: non richiedono alcuna modifica negli adattatori dei computer

Bridge: frame filtering & forwarding

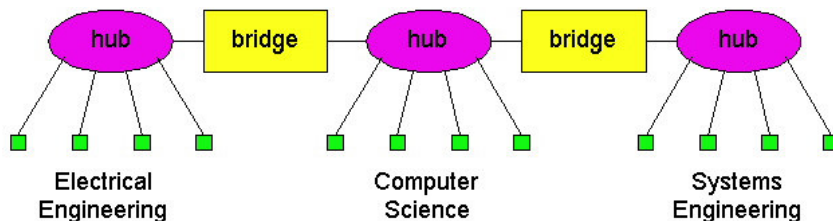


- Forwarding:
 - Come fare a sapere su quale segmento una frame deve essere inoltrata?
 - Analogia con i problemi di routing (anche se su scala meno ampia!)
- I bridge filtrano i pacchetti
 - Stesso segmento di LAN:
 - le frame non sono inoltrate su altri segmenti di LAN

Backbone Bridge



Interconnessione senza backbone



- Soluzione non consigliata a causa di due motivi:
 - esiste un punto critico presso l'hub di Computer Science, in caso di rottura dello stesso
 - il traffico tra EE e SE deve necessariamente attraversare il segmento CS

Bridge Filtering



- I bridge eseguono un algoritmo di *auto apprendimento* per scoprire a quali interfacce sono collegati gli host:
 - Tali informazioni sono salvate in delle “filtering tables”
 - Quando una frame è ricevuta, il bridge “prende nota” del segmento di LAN di provenienza
 - L’interfaccia di provenienza è memorizzata in una filtering table
 - filtering table entry:
 - » (Node LAN Address, Bridge Interface, Time Stamp)
 - » dati della Filtering Table obsoleti vengono cancellati (TTL tipicamente pari a 60 minuti)

Bridge Filtering

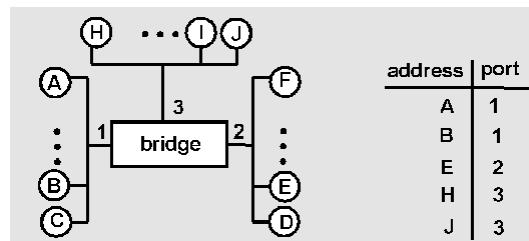


- filtering procedure:
 - if** destination is on LAN on which frame was received
 - then** drop the frame
 - else {** lookup filtering table
 - if** entry found for destination
 - then** forward the frame on interface indicated;
 - else** flood; */* forward on all but the interface on which the frame arrived*/*
 - }**

Bridge Learning: esempio (1/2)

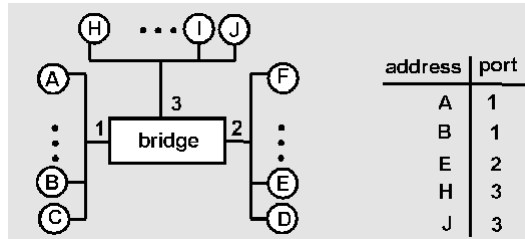


Supponendo che C invii una frame a D e che D risponda con una frame a C



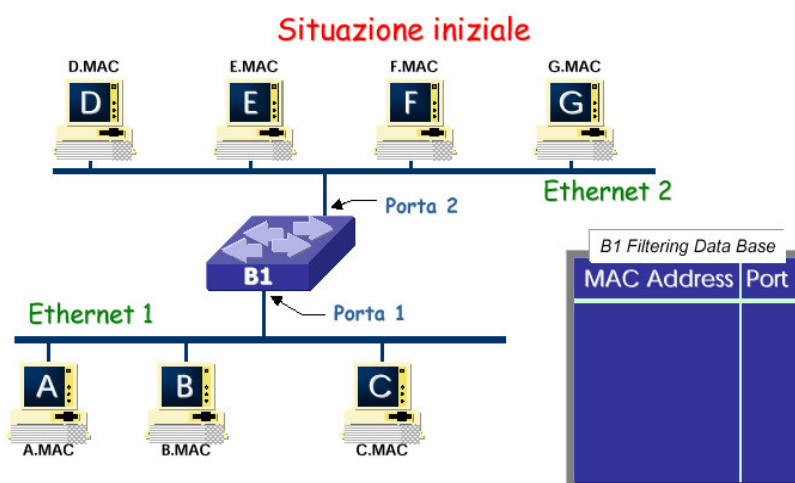
- C invia la frame, il bridge non ha alcuna informazione circa D, pertanto invia in flooding
 - Il bridge annota C sul porto 1
 - La frame è ignorata nella LAN in alto
 - La frame viene ricevuta da D

Bridge Learning: esempio (2/2)

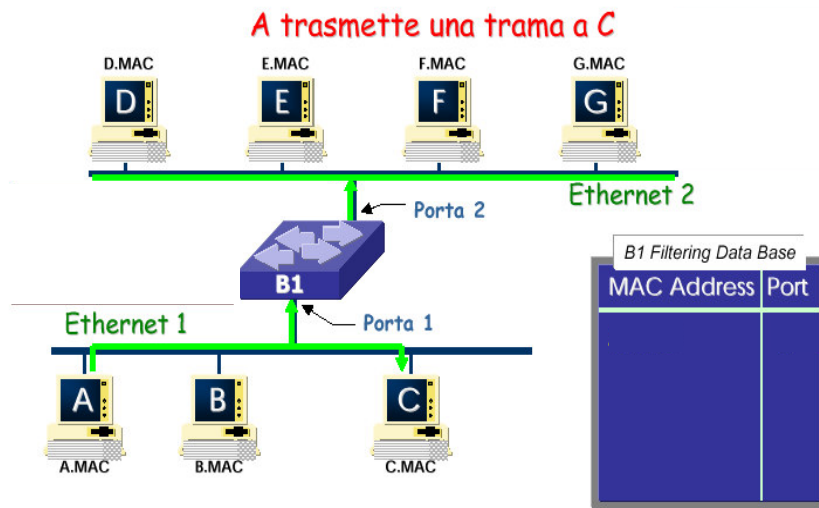


- D genera una risposta destinata a C e la invia
 - Il bridge vede la frame proveniente da D
 - Il bridge annota D sul porto 2
 - Il bridge sa che C è sul porto 1, quindi invia *esclusivamente* la frame sul porto 1

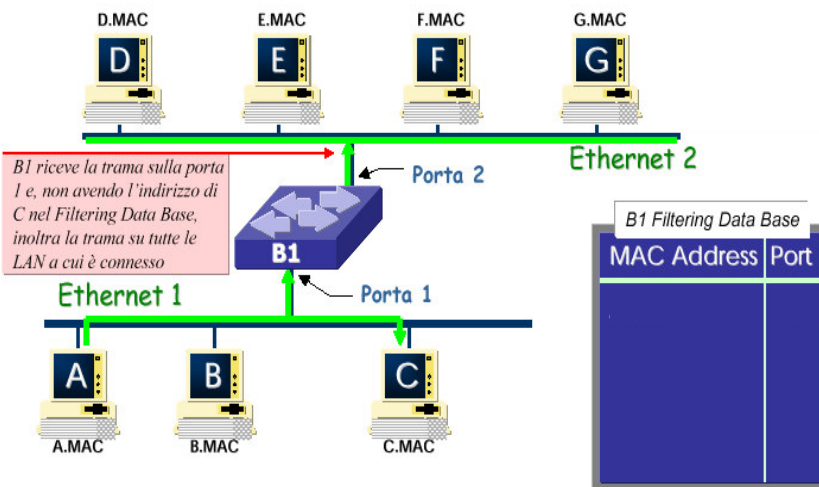
Bridge Learning: esempio (1/5)



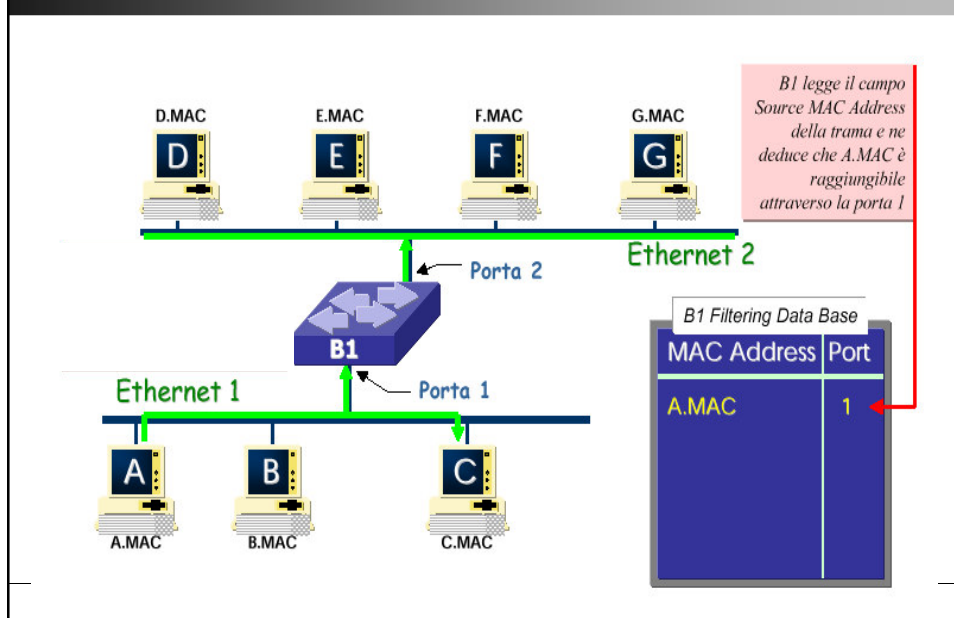
Bridge Learning: esempio (2/5)



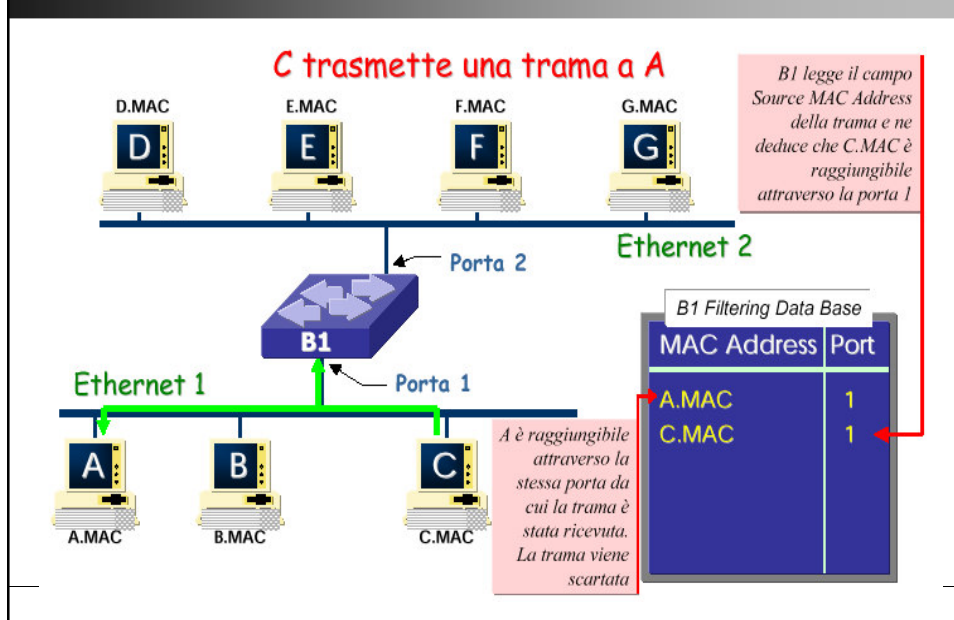
Bridge Learning: esempio (3/5)



Bridge Learning: esempio (4/5)



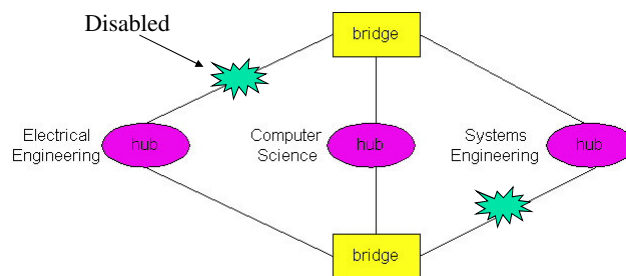
Bridge Learning: esempio (5/5)



Bridge Spanning Tree



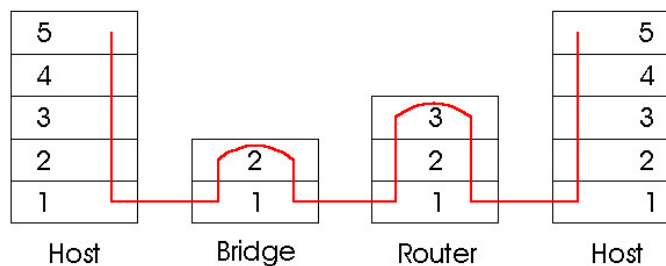
- Per incrementare l'affidabilità, può essere utile introdurre un certo grado di ridondanza:
 - percorsi alternativi
- In presenza di percorsi alternativi simultanei, vengono create copie molteplici delle frame (loop)
- SOLUZIONE: organizzare i bridge mediante uno spanning tree, disabilitando alcune interfacce



Bridge vs Router



- Sono entrambi dispositivi di tipo store-and-forward
 - router: dispositivi di livello rete (esaminano il contenuto dell'header di livello 3)
 - Bridge: sono dispositivi di livello Data Link
- I router si basano sulle *routing table* ed implementano algoritmi di routing
- I bridge si basano sulle *filtering table* ed implementano algoritmi di filtering, learning e spanning tree



Router vs Bridge



Bridge: pro (+) e contro (-)

- + Le operazioni nei bridge sono più semplici
- + I bridge processano meno richieste
- Le topologie sono limitate: è necessario uno spanning tree per prevenire i cicli
- I bridge non offrono alcuna protezione contro le tempeste broadcast (il broadcast ininterrotto generato da un host è normalmente inoltrato da un bridge)

Router vs Bridge



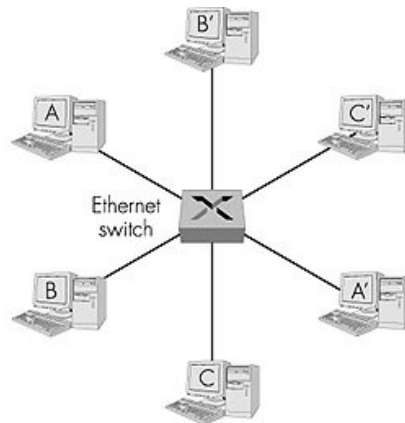
Router: pro (+) e contro (-)

- + possono essere realizzate differenti topologie, i loop sono limitati grazie al contatore TTL (ed all'impiego di buoni protocolli di routing)
- + forniscono una naturale protezione contro le tempeste broadcast
- richiedono configurazione al livello IP (non sono *plug and play*)
- richiedono capacità adeguata per processare una grande quantità di pacchetti
- I bridge sono maggiormente utili in caso di reti piccole (con poche centinaia di host) mentre i router sono usati nelle grandi reti (migliaia di hosts)

Switch Ethernet 1/3



- Effettuano l'inoltro di frame a livello 2
 - filtraggio mediante l'uso di indirizzi LAN
- **Switching**: da A a B e da A' a B' simultaneamente:
 - non ci sono collisioni
- Alto numero di interfacce
- spesso: host singoli, topologia a stella con collegamento ad uno switch:
 - È Ethernet, ma senza collisioni!



Switch Ethernet 2/3



- **Cut-through switching**:
- Pro
 - frame inoltrate dall'ingresso all'uscita senza attendere l'assemblamento dell'intera frame
 - Leggera diminuzione della latenza
 - Consentono la combinazione di interfacce condivise/dedicate, a 10/100/1000 Mbps
- Contro
 - E le frame affette da errore ?

Switch Ethernet 3/3

