

Corso di Laurea in Ingegneria Informatica



Corso di Reti di Calcolatori I

Roberto Canonico (roberto.canonico@unina.it)

Giorgio Ventre (giorgio.ventre@unina.it)

**Interconnessione di LAN:
hub e bridge**

**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

Interconnessione di LAN

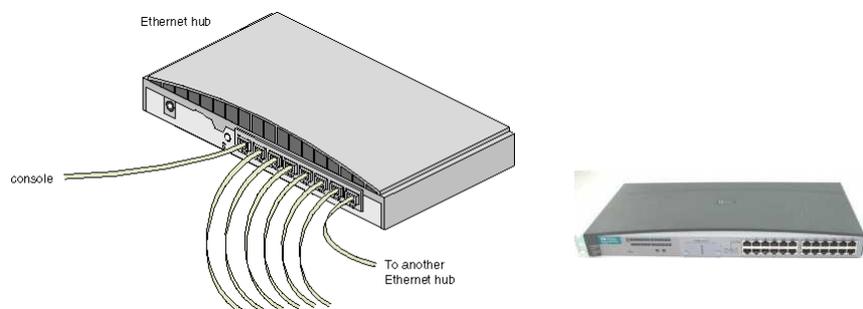


- Esigenza: Dovendo collegare i computer di diversi uffici collocati nello stesso edificio (o comprensorio) perché non creare un'unica grande LAN?
- Soluzione 1: interconnessione mediante hub
- Soluzione 2: interconnessione mediante bridge/switch

Hub Ethernet



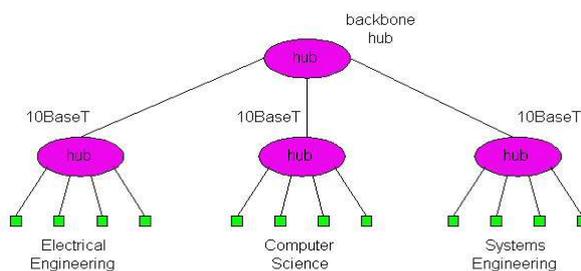
- Gli hub sono dispositivi di Livello Fisico, sostanzialmente si tratta di ripetitori di bit
 - riproducono i bit in ingresso ad un'interfaccia su tutte le altre interfacce
 - sono dispositivi semplici e poco costosi



Interconnessione di LAN con hub



- Hub organizzati in una **gerarchia multi-livello**, con un *backbone hub* al livello più alto
- Ogni LAN collegata è detta un **segmento di LAN**



Interconnessione con hub: pro e contro



- **Vantaggi:**
 - 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
 - Si estende la massima distanza tra i nodi
 - 100m per ogni hub
- **Svantaggi:**
 - Gli hub **non isolano** i domini di collisione: le stazioni di un segmento possono subire una collisione per una trasmissione simultanea da parte di una qualunque stazione presente su un qualunque altro segmento
 - 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

Bridge Ethernet

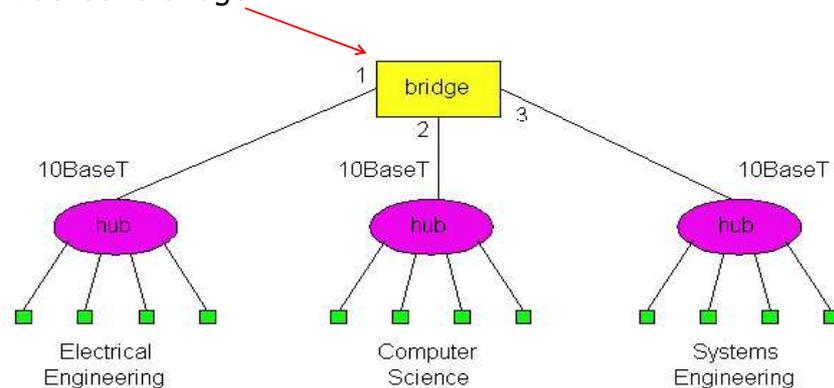


- I bridge sono **dispositivi di livello 2**: in grado di leggere le intestazioni di frame Ethernet, ne esaminano il contenuto, e selezionano il link d'uscita sulla base dell'indirizzo destinazione
- I bridge **isolano** i domini di collisione, grazie alla loro capacità di porre le frame in un buffer (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

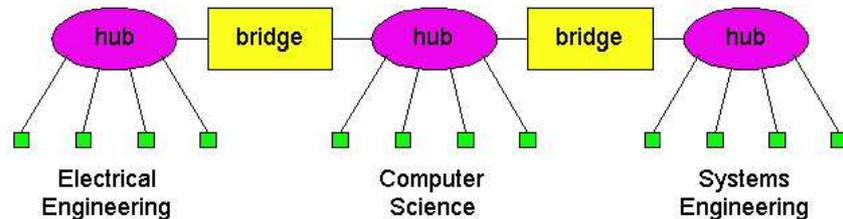
Interconnessione di LAN con bridge (1/2)



Backbone bridge



Interconnessione di LAN con bridge (2/2)



- 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

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*
- Sono **trasparenti**: non richiedono alcuna modifica negli adattatori dei computer né configurazione da parte di un amministratore (*plug & play*)

Bridge: frame filtering & forwarding



- I bridge filtrano i pacchetti
 - Destinazione sullo stesso segmento di LAN del mittente:
 - Nessuna azione da parte del bridge
 - Destinazione su un segmento di LAN differente da quello del mittente:
 - Il bridge inoltra la frame sul segmento di LAN del destinatario
- Come fare a sapere su quale segmento una frame deve essere inoltrata?

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

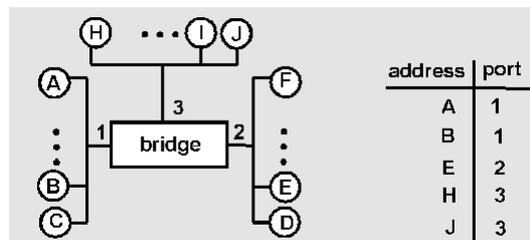


- filtering procedure:
 - if** destination is on LAN on which frame was received
 - then** drop the frame
 - else** { lookup filtering table
 - if** entry found for destination
 - then** forward the frame on interface indicated;
 - else** flood; */* forward on all but the interface on which the frame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

Bridge Learning: esempio (1/2)

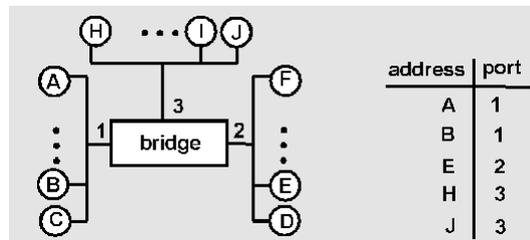


Supponendo che C invii una frame a D e che D risponda con una frame a C



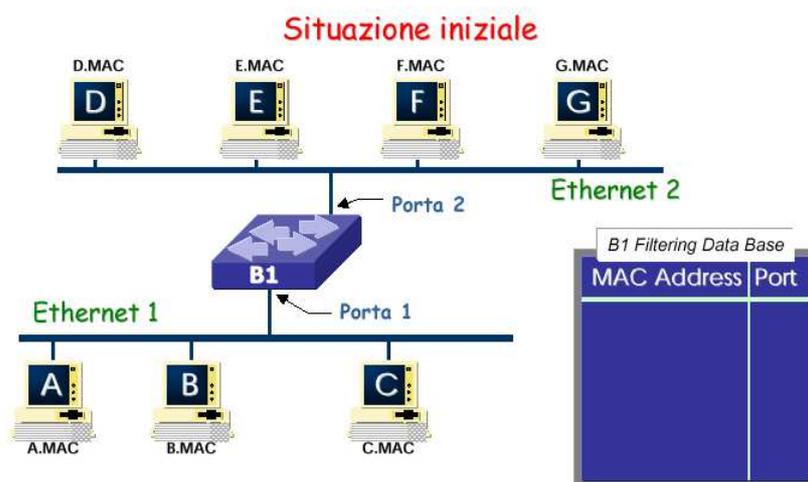
- C invia la frame, il bridge non ha alcuna informazione circa D, pertanto invia in flooding
 - Il bridge annota C sul porto 1
 - La frame è ignorata nella LAN in alto
 - La frame viene ricevuta da D

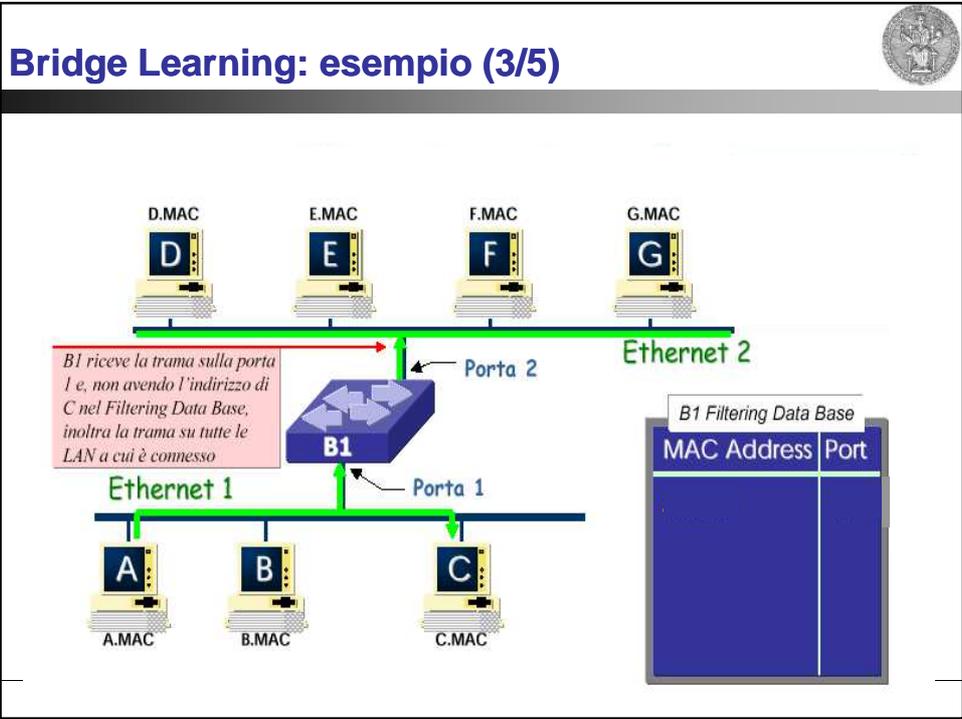
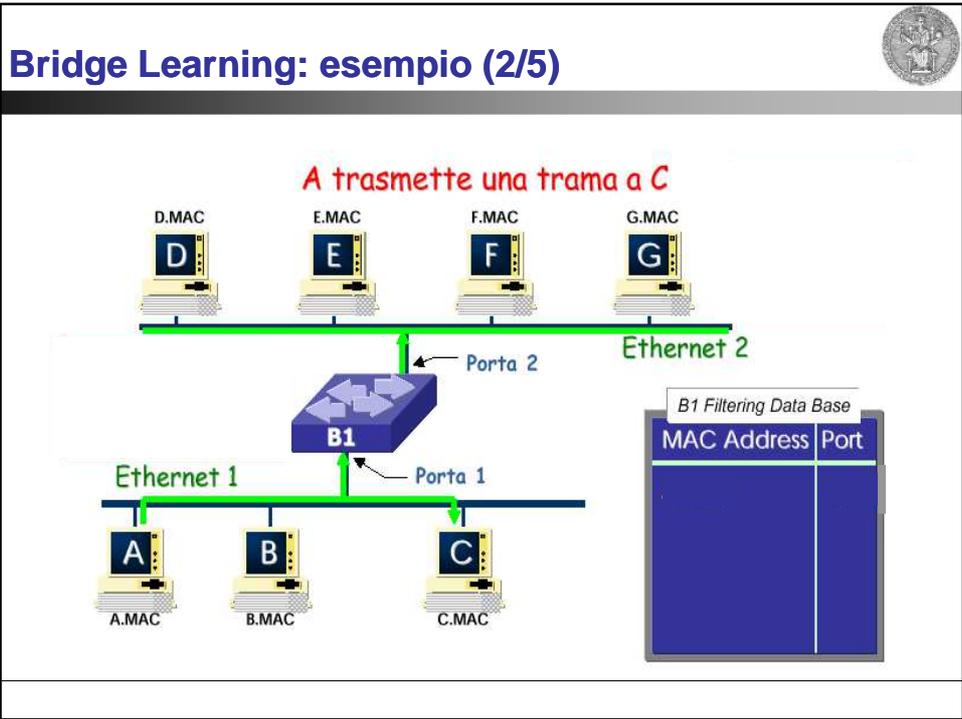
Bridge Learning: esempio (2/2)

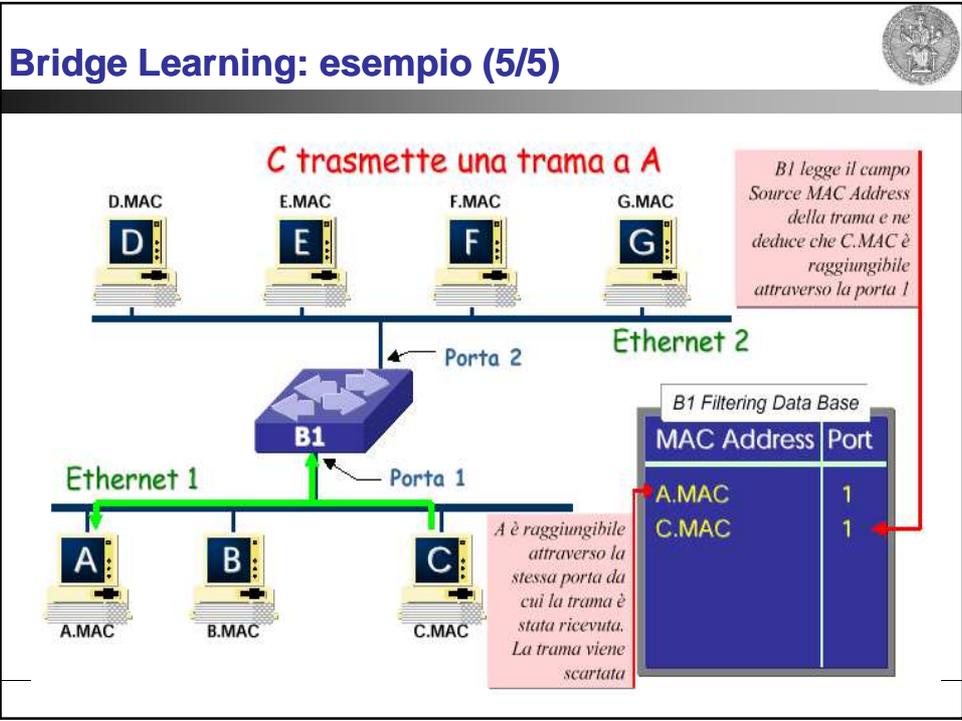
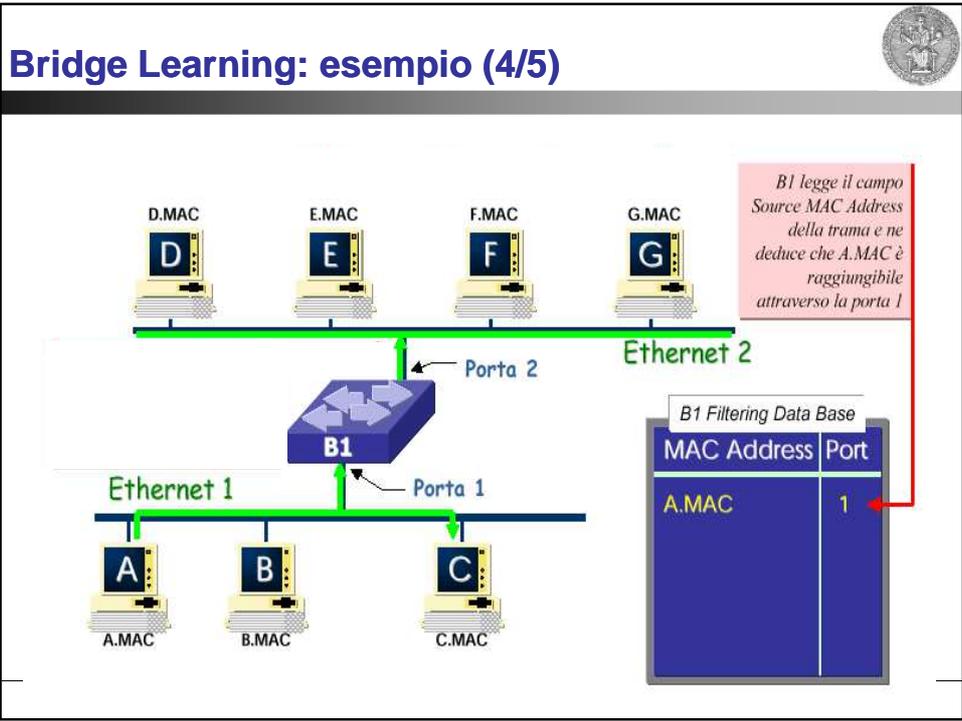


- D genera una risposta destinata a C e la invia
 - Il bridge vede la frame proveniente da D
 - Il bridge annota D sul porto 2
 - Il bridge sa che C è sul porto 1, quindi invia *esclusivamente* la frame sul porto 1

Bridge Learning: esempio (1/5)



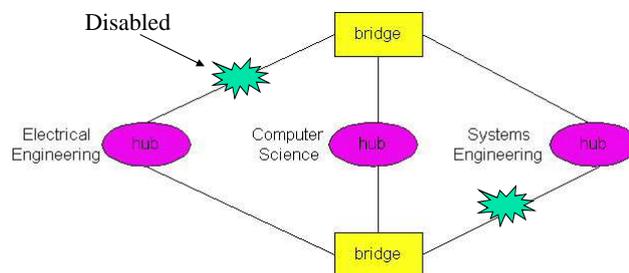




Bridge Spanning Tree



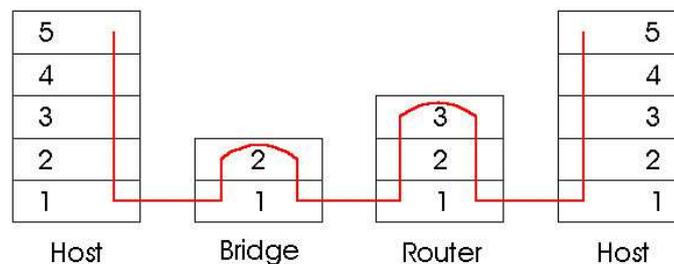
- Per incrementare l'affidabilità, può essere utile introdurre un certo grado di ridondanza:
 - percorsi alternativi
- In presenza di percorsi alternativi simultanei, vengono create copie molteplici delle frame (loop)
- **SOLUZIONE:** organizzare i bridge mediante uno spanning tree, disabilitando alcune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