



L'Istituto Tecnico Euganeo  
di oggi è la tecnologia di  
domani

Obbligo scolastico (Biennio tecnologico)  
Automazione  
Elettronica  
Elettrotecnica  
Informatica  
Meccanica e Meccatronica  
Logistica  
Biotecnologie ambientali

Corso Serale Sirio  
Patente ECDL - Eucip IT ADMINISTRATOR

Titolo  
**HUB e SWITCH**

Autore  
**Prof. Nicola Ceccon**  
Classe  
**QUINTA INFORMATICA (5IA)**  
Anno scolastico  
**2010/2011**



**SIS  
02**

**PRA  
01**

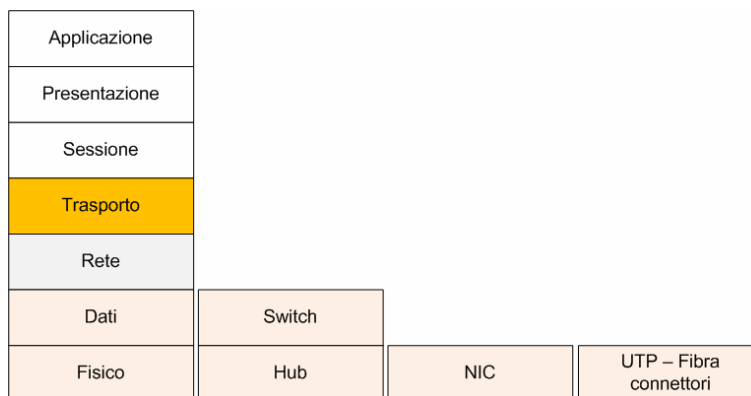
# HUB e SWITCH

## Dispositivi di rete: Hub e Switch

Esistono molti dispositivi hardware che servono per costruire reti, per ora i dispositivi di maggiore interesse, dal nostro punto di vista, sono l'**Hub** e lo **Switch**<sup>1</sup>.

Quindi, sono dispositivi che consentono di interconnettere tra loro due o più reti, permettendo: estensione della lunghezza della LAN; il passaggio dalla topologia fisica a bus a quella a stella; la connessione e la comunicazione tra host.

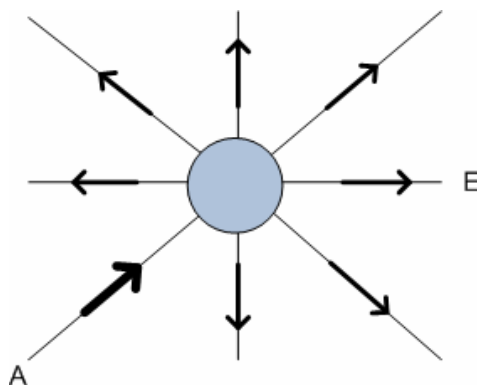
La figura che segue illustra il posizionamento dei dispositivi e degli elementi principali nella pila ISO/OSI.



### Hub

E' un **repeater multiporta di livello 1** che permette di collegare punto-punto ad ogni porta un nodo oppure un segmento<sup>2</sup> di rete trasmettendo i frame che riceve su una porta su tutte le altre porte (operazione di flooding).

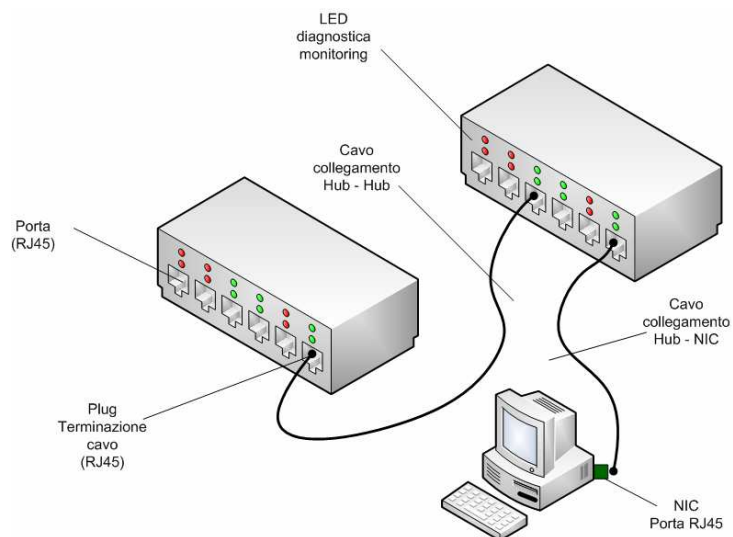
La figura illustra il funzionamento di un Hub nell'ipotesi di invio di un pacchetto dal mittente A al destinatario E.



La figura illustra il collegamento di un nodo ad un Hub e il collegamento di due Hub (collegamento di un segmento di rete ad un Hub).

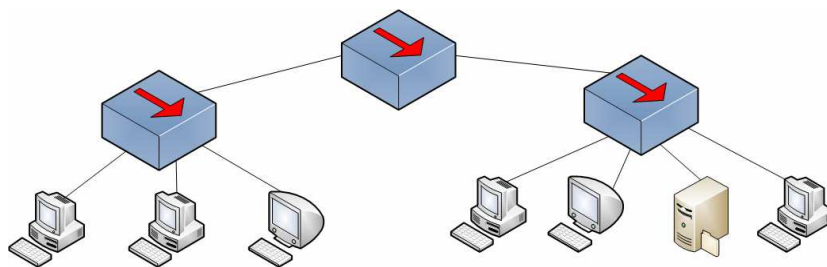
<sup>1</sup> Il bridge è qui considerato in modo semplificato come un subset dello switch.

<sup>2</sup> Qui inteso come parte della rete fisica.

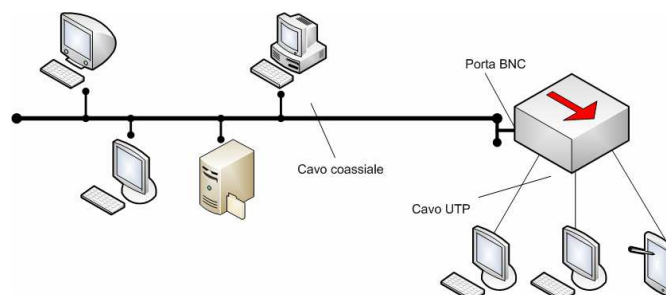


**Con l'utilizzo di un Hub<sup>3</sup> la topologia logica è a bus, ma quella fisica è a stella**, senza che quest'ultima introduca benefici in termini di capacità trasmissiva globale della rete, infatti, in tali casi l'Hub continua ad avere una capacità trasmissiva totale pari a quella del singolo cavo. **Inoltre, permane il fenomeno delle collisioni.**

Sono possibili molteplici combinazioni<sup>4</sup>, il problema è sempre quello del degrado della rete all'aumentare delle collisioni.



In alcune LAN legacy<sup>5</sup> è possibile trovare una topologia mista bus/stella realizzata con l'utilizzo di un Hub che dispone di una porta per il collegamento del cavo coassiale.



<sup>3</sup> Quindi l'Hub permette di effettuare una topologia logica a bus su di una topologia fisica a stella.

<sup>4</sup> Il numero di Hub in cascata è stabilito dagli standard.

<sup>5</sup> "Vecchie e ancora funzionanti".

## Switch (livello 2)

Uno Switch (identificato con la sigla **L2**), detto anche commutatore, è un dispositivo di rete multiporta ad alte prestazioni dotato di uno stack di comunicazione che comprende almeno il livello 2 di collegamento con funzionalità di **inoltro selettivo dei pacchetti**, sulla base degli indirizzi MAC.

Il dispositivo, a differenza dell'Hub, ha la capacità di leggere i campi contenenti gli indirizzi di destinazione e provenienza (MAC) del frame ethernet.

La funzione è di:

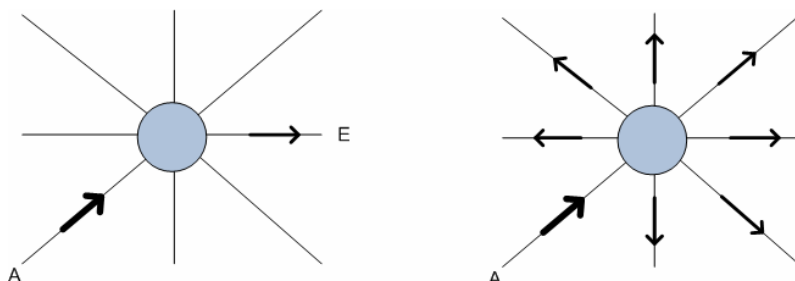
- inoltrare il pacchetto soltanto alla porta (detta di inoltro) a cui è indirizzato e non alle altre creando in tal modo un percorso univoco fra porta di entrata e di uscita;
- inoltrare il pacchetto a tutte le porte, caso di traffico di broadcast (indirizzo destinazione FF:FF:FF:FF:FF:FF, cioè tutti 1), perché destinato a tutti gli host della LAN collegati al dispositivo;
- inoltrare il pacchetto a tutte le porte quando non conosce la porta di inoltro.

Lo Switch è un dispositivo pluggable, cioè **apprende la topologia della LAN automaticamente**:

- rilevando su quali porte sono collocati i nodi (MAC) mediante l'ascolto delle trasmissioni dei pacchetti, è cioè in grado di imparare quali host (o meglio le NIC<sup>6</sup>) sono raggiungibili attraverso quali porte;
- inserendo gli indirizzi MAC in una tabella di livello 2 detta MAC table o filtering database o CAM table o tabella d'inoltro, che contiene l'elenco di tutte le destinazioni raggiungibili. La tabella viene aggiornata automaticamente man mano che arrivano i vari pacchetti (autoapprendimento) e viene anche reimpostata periodicamente, eliminando i valori presenti da più tempo.

La figura che segue illustra l'invio di un pacchetto:

- dal nodo mittente A al nodo destinazione E;
- di broadcast dal nodo mittente A.

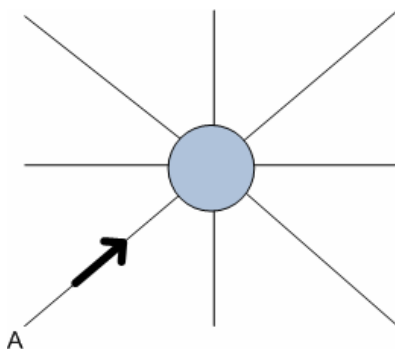


<sup>6</sup> Network Interface Card.

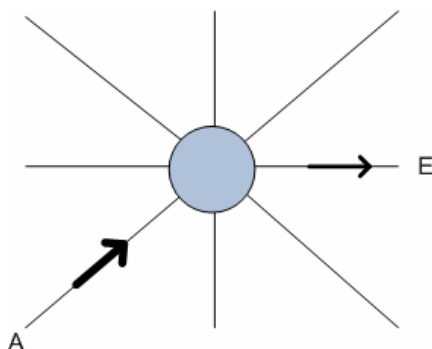
## Vediamo il funzionamento dello Switch.

Quando arriva un pacchetto ad una porta lo Switch controlla se l'indirizzo MAC del destinatario è presente nella MAC table:

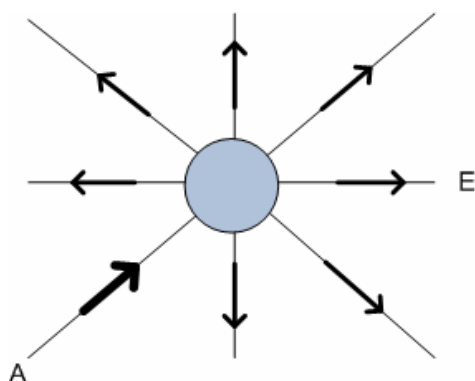
1. Se presente e la porta destinataria corrisponde a quella mittente, il pacchetto viene ignorato (operazione di Filtering), avviene ad esempio quando alla porta dello Switch è collegato un Hub.



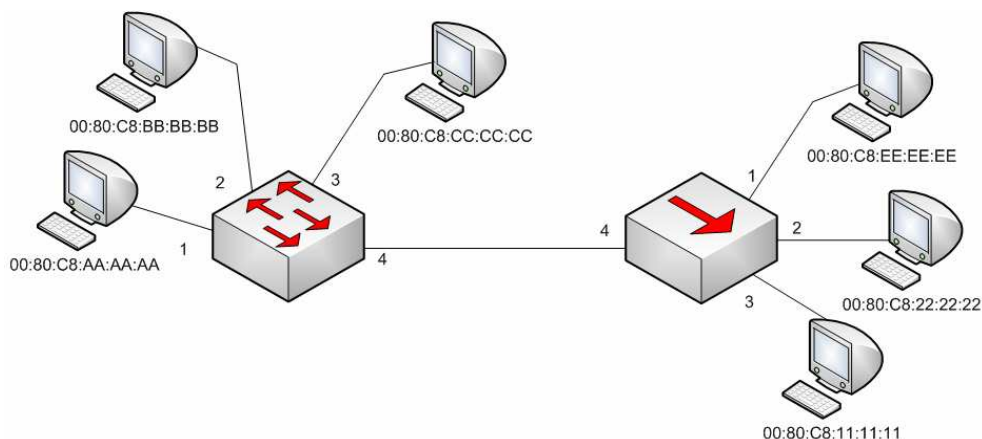
2. Se presente e la porta del destinatario è diversa da quella del mittente, si invia il pacchetto alla porta associata e solo a quella (operazione di Forwarding).



3. Se non presente, si invia il pacchetto a tutte le porte a parte quella del mittente (operazione di Flooding).



Analizziamo l'inoltro, cioè la gestione della tabella di instradamento, considerando la seguente rete di esempio nell'ipotesi che la MAC table sia vuota, cioè lo Switch sia appena stato acceso.



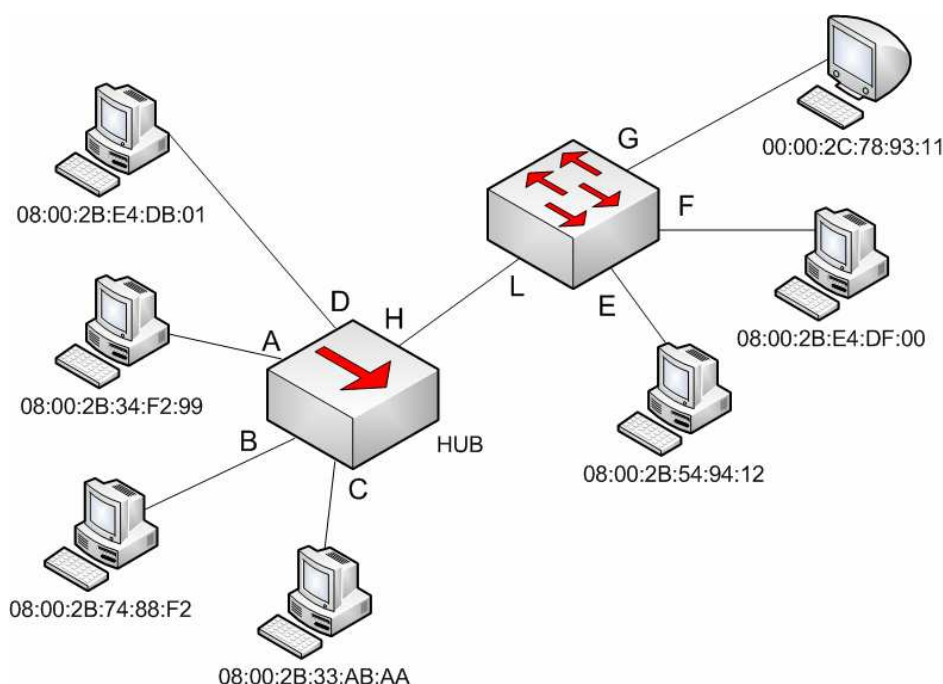
Si ipotizzi che l'host 00:80:C8:AA:AA:AA invii un frame all'host EE:EE:EE:EE:EE:EE e che l'host 00:80:C8:CC:CC:CC invii un frame all'host 00:80:C8:11:11:11 e successivamente all'host 00:80:C8:BB:BB:BB.

La MAC table dello Switch risulta essere:

Porta	MAC
1	00:80:C8:AA:AA:AA
2	00:80:C8:BB:BB:BB
3	00:80:C8:CC:CC:CC
4	00:80:C8:EE:EE:EE 00:80:C8:11:11:11

## Esercizio n.1

Si consideri la seguente LAN:



Si supponga che lo Switch sia appena stato acceso, e che i pacchetti transitati nella LAN, a partire da quel momento, siano stati:

1. mittente 08:00:2B:74:88:F2 con destinatario broadcast;
2. mittente 00:00:0C:78:93:11 con destinatario 08:00:2B:74:88:F2;
3. mittente 08:00:2B:54:94:12 con destinatario 00:00:0C:78:93:11;
4. mittente 08:00:2B:74:88:F2 con destinatario 00:00:0C:78:93:11;

a quale interfaccia dei dispositivi di rete (Hub e Switch) verrà inoltrato il pacchetto numero 4? Giustificare la risposta.

Risposta.

Il pacchetto numero 4 (mittente 08:00:2B:74:88:F2 con destinatario 00:00:0C:78:93:11) sarà inoltrato:

- alle porte A,C,D,H dell'Hub in quanto broadcast;
- alla porta G dello Switch in quanto esso ha appreso la posizione del destinatario dal pacchetto numero 2.

Infatti, lo stato della MAC table dello Switch è:

	porta E	porta F	porta G	porta L
pacchetto n.1				:88:F2
pacchetto n.2			:93:11	
pacchetto n.3	:94:12			
pacchetto n.4				



## Tecniche d'inoltro di uno Switch

---

Gli Switch implementano diverse tecniche di inoltro, cosa che ne determina una loro classificazione, tra le quali:

- **Store-and-Forward Switching:** lo Switch riceve l'intero frame in un buffer di memoria, ne controlla la presenza di errori e l'inoltra alla porta di destinazione solo se privo di errori.

Il principale vantaggio offerto da questa classe di Switch è rappresentato dal fatto che i frame contenenti errori non sono trasmessi e quindi non si ha un inutile speco di banda. Tuttavia, esso deve processare tutti i frame e quindi introducono un ritardo (detto ritardo o latenza del dispositivo o latency time) dovuto all'operazione.

E' questa la tecnica presente in tutti gli Switch e spesso anche l'unica utilizzata.

- **Cut-through Switching:** lo Switch inoltra il frame non appena legge l'indirizzo MAC di destinazione, quindi non verifica la correttezza dei frame ricevuti. Se l'operazione è di flooding lo Switch passa alla tecnica precedente. Il vantaggio principale nell'evitare uno store and forward dell'intero pacchetto risiede nella riduzione del tempo dell'operazione, la latenza di questo Switch è più bassa della latenza di uno Switch tradizionale. Lo svantaggio è quello di ritrasmettere eventuali pacchetti corrotti, quindi può sovraccaricare inutilmente la rete.
- **Fragment-free Switching:** si leggono i primi 64Byte, compreso l'header, e successivamente si effettua l'inoltro. E' un compromesso tra le due precedenti tecniche, poiché l'inoltro inizia prima che siano letti tutti i campi.

## Architettura dello Switch

---

In precedenza si è visto che lo Switch è un commutatore di porte:

- inoltra un pacchetto da una porta ad un'altra a seguito di un'operazione di decisione d'inoltro;
- effettua una ricerca su un database di indirizzi MAC e porte memorizzato permanentemente;
- quando riceve dal collegamento il pacchetto la porta è a tutti gli effetti una porta d'ingresso, quando invia ad una porta questa è a tutti gli effetti una porta d'uscita.

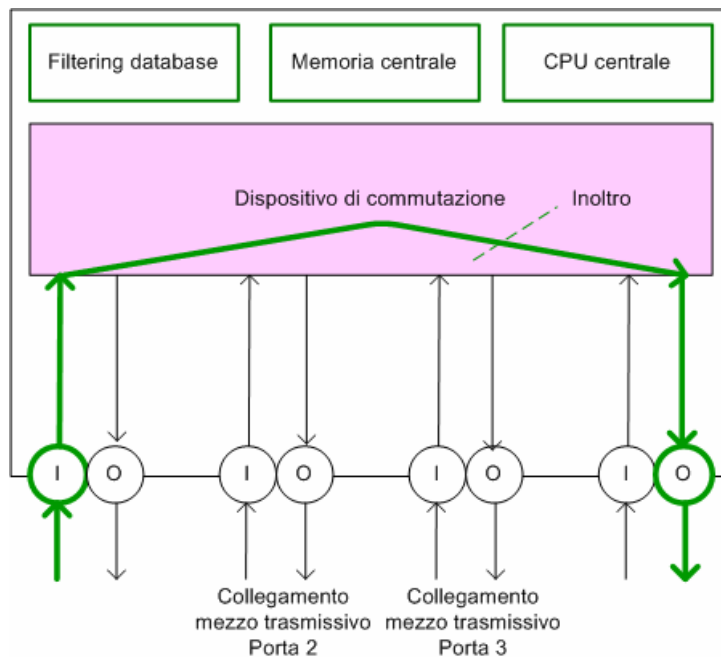
Compito delle porte di ingresso è di gestire le informazioni di controllo per trasferire il pacchetto all'uscita corretta.

Compito delle porte di uscita è di gestire la trasmissione del pacchetto attraverso il collegamento.

Dal punto di vista dell'architettura lo Switch si può considerare come un dispositivo dotato di porte (interfacce) d'ingresso, porte d'uscite e un dispositivo di commutazione (caratterizzato da un'architettura di commutazione) in grado di: ricevere il pacchetto dalla porta d'ingresso, memorizzando tutti i bit sino a completamento; prelevare il pacchetto dalla porta di ingresso; determinare la porta di uscita elaborando il pacchetto; trasferirlo alla giusta porta d'uscita; memorizzare tutti i bit sino a

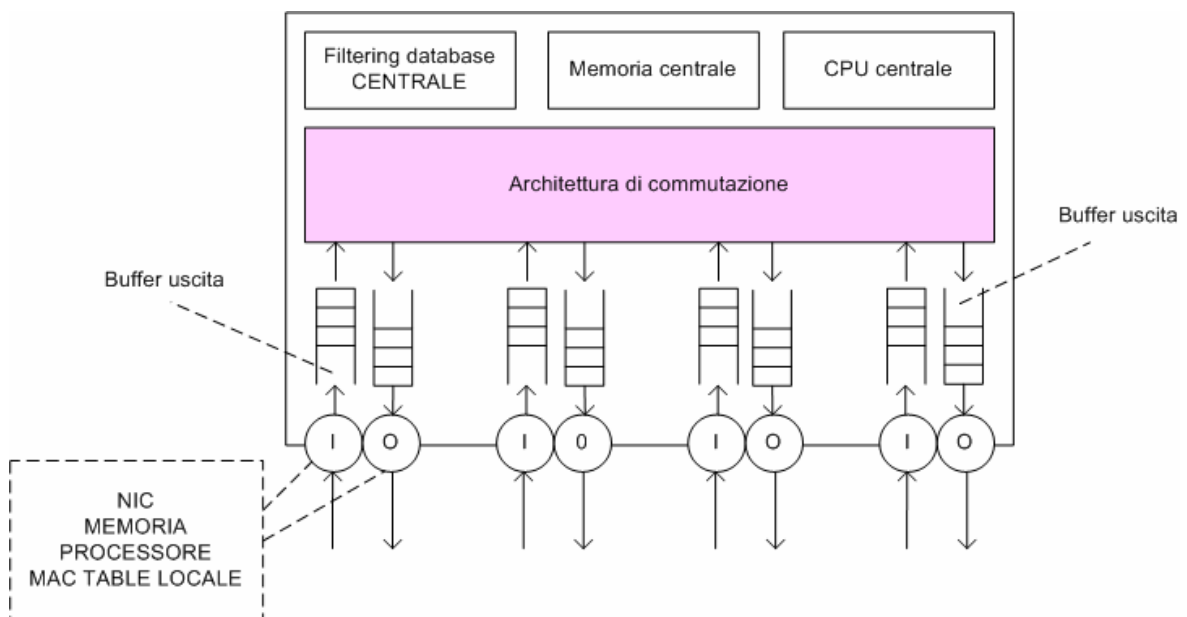
completamento del pacchetto; trasmettere il pacchetto attraverso il collegamento.

In figura lo schema logico (e didattico) di uno Switch a 4 porte.



Ogni interfaccia è dotata di memoria e processore e l'hardware localizzato sulle porte è specializzato nell'inoltro dei frame e costruito, solitamente con tecnologia ASIC (Application Specific Integrated Circuit).

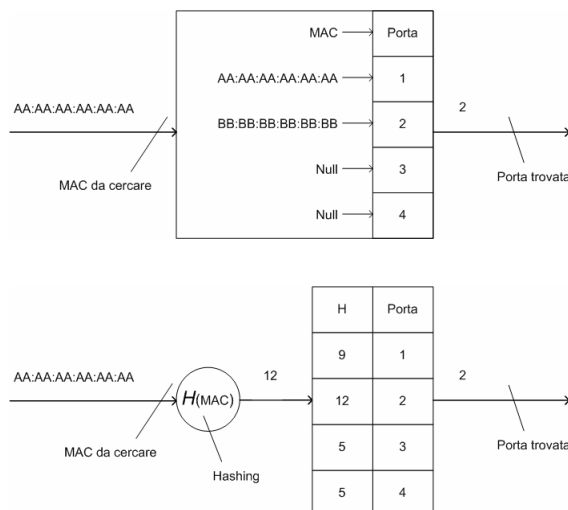
Inoltre, una funzione fondamentale dei commutatori a pacchetto è la memorizzazione dei pacchetti in buffer finiti di memoria che può essere realizzata nelle porte di ingresso e/o di uscita.



Gli elementi che ci interessa approfondire sono due:

1. La **MAC table (MAC, Porta, TTL<sup>7</sup>)** memorizzata in una memoria spesso di tipo associativo, la **Content-Addressable Memory (CAM)**, impostata come una tabella di mapping tale da fornire direttamente la porta associata ad un indirizzo MAC inserito senza usare algoritmi oppure in una **memoria veloce con l'utilizzo di algoritmi di recupero rapido (Hash)**.

Le figure che seguono illustrano la logica di una CAM table e di una Hashing table.



2. Il dispositivo di commutazione che permette il passaggio del pacchetto dall'interfaccia di ingresso a quella di uscita. E' caratterizzato da un sistema di collegamento tra interfacce in entrata e in uscita e una larghezza di banda di commutazione che è limitata dalla tecnologia di commutazione.

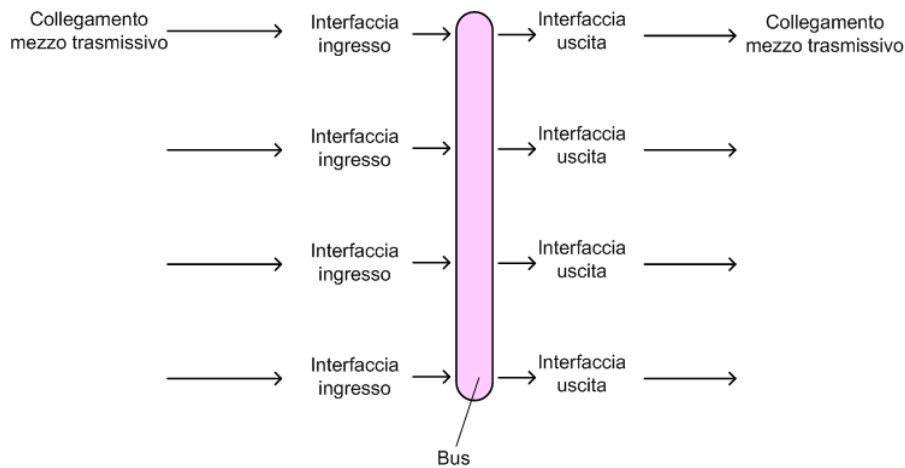
La tecnologia può essere di diversi tipi a seconda del tipo di commutazione implementata, o i due principali sono:

- a. la commutazione a Bus;
- b. la commutazione Crossbar (matrice di commutazione o Switching fabric).

## Dispositivo di commutazione a Bus

Nel caso dell'architettura a bus si utilizza un bus condiviso di collegamento tra le interfacce, e l'interfaccia d'ingresso trasferisce un pacchetto direttamente all'interfaccia d'uscita, senza coinvolgere un processore d'oltro.

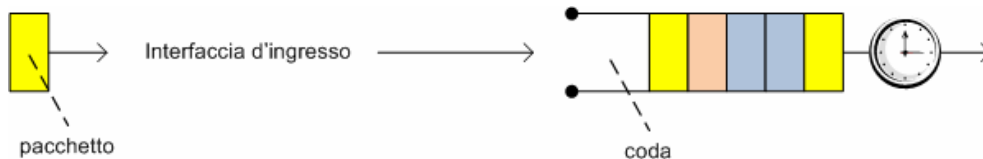
<sup>7</sup> Tempo di registrazione che serve per eliminare gli indirizzi dopo una scadenza, impostato ad alcuni secondi.



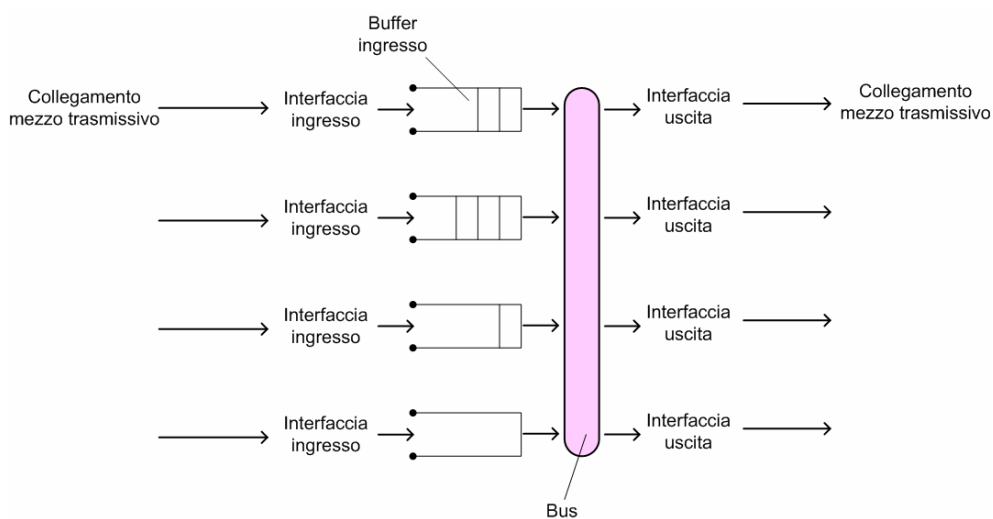
Il problema è che sul bus può comunque essere trasferito un solo pacchetto alla volta.

Se una porta di ingresso una volta determinata la porta d'uscita trova il bus occupato, perché c'è un altro pacchetto proveniente da un'altra porta, allora il pacchetto per non essere perso deve essere memorizzato in un **buffer di memorizzazione ad ampiezza finita d'ingresso** associato alla porta per essere servito dal dispositivo di commutazione successivamente.

I pacchetti nel buffer sono gestiti con una coda logica, cioè il buffer è matematicamente un sistema a coda, in cui quando un nuovo pacchetto viene memorizzato nel buffer è accodato alla coda e attende che il dispositivo sia libero.



E' importante sottolineare che in uno Switch a N porte le memorie devono avere velocità fino a N volte superiore a quella dei collegamenti d'ingresso.



L'accodamento in ingresso si evita aumentando la banda del bus.

Si usa la tecnica dello **speedup** che consiste nell'utilizzare una capacità di trasferimento del bus più alta della capacità delle interfacce, tipicamente si utilizza una banda che è almeno uguale alla capacità aggregata delle interfacce: con  $B_{max}$  la velocità della porta e  $N$  le porte la velocità del Bus è pari almeno a  $NB_{max}$  (per esempio nel caso di 24 interfacce ad 1 Gbps si ha un bus a 24 Gbps).

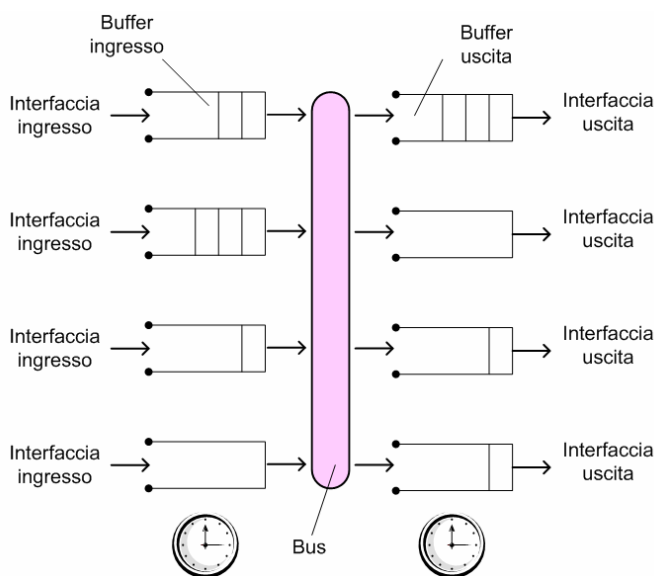
Nasce, però, un problema.

La maggiore velocità del Bus causa un problema nelle interfacce d'uscita che si contendono la trasmissione (stessa uscita contemporaneamente): la porta d'uscita trasferisce quando il collegamento è libero, cioè quando l'ultimo bit del pacchetto inviato è ricevuto dalla porta d'ingresso del dispositivo successivo (Switch, router o NIC) ed è quindi probabile che il collegamento di uscita non sia in grado di assorbire tutto il traffico.

Si pensi per esempio al caso di un dispositivo con  $N$  porte: potrebbe accadere il caso peggiore in cui tutti i  $N-1$  pacchetti devono uscire dalla stessa porta di uscita.

Anche in questo caso la soluzione è il ricorso ad un buffer di memoria finito per ogni porta d'uscita che consente di assorbire i tempi di attesa nello smaltimento del traffico.

La figura che segue illustra lo schema di un dispositivo di commutazione a Bus con buffer in ingresso e in uscita.



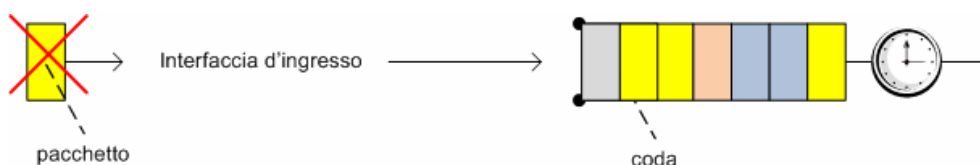
**L'adozione di buffer d'uscita ha una conseguenza molto importante: la possibilità dello scarto di pacchetti legato al verificarsi del buffer overflow.**

Riprendendo l'esempio precedente se alla porta d'uscita dovessero arrivarne altri  $N-1$  pacchetti nel tempo successivo e sempre alla stessa porta di uscita si potrebbe arrivare presto all'esaurimento spazio dello spazio nel buffer.

La perdita dipende da diversi fattori: dal traffico, dalla velocità del dispositivo di commutazione e dalla velocità del collegamento.

Una soluzione, ovvia, del fenomeno della perdita di pacchetti per buffer overflow si allieva con buffer sufficientemente grandi.

La figura che segue illustra il buffer overflow e l'azione di perdita del pacchetto.



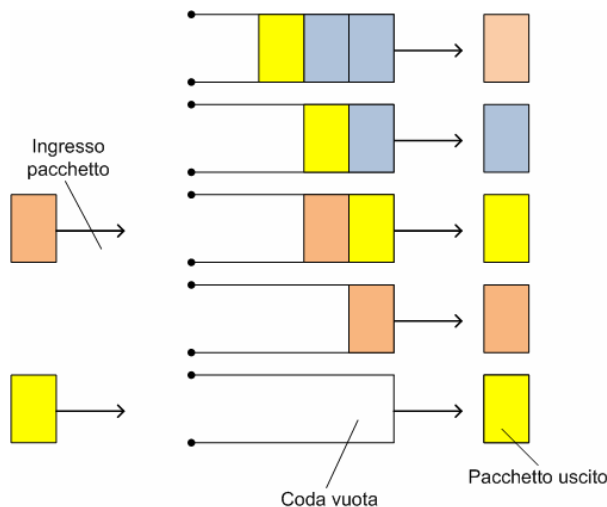
## Scheduling delle code

L'utilizzo di buffer d'ingresso e d'uscita comporta la necessità dello scheduler di pacchetto, è cioè necessario scegliere fra quelli accodati quale fare uscire per primo (è una logica di arbitraggio).

Esistono diversi algoritmi di arbitraggio, come: l'algoritmo **FIFO** (First In First Out) oppure l'algoritmo **RR** (Round Robin).

L'algoritmo solitamente implementato è l'algoritmo FIFO, quindi il pacchetto che si seleziona e quindi si invia attraverso il collegamento è il primo che è entrato nella coda.

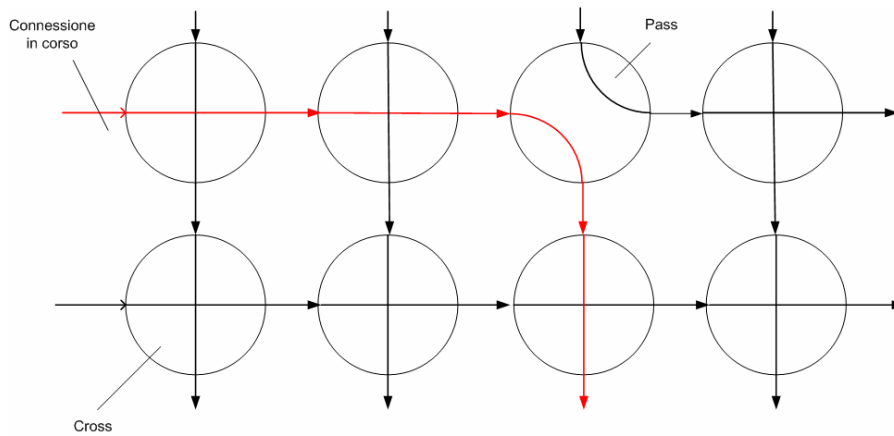
La figura illustra l'algoritmo FIFO nel caso di quattro pacchetti in coda (attesa) e l'accodamento di due pacchetti, di cui l'ultimo trova la situazione più favorevole di coda vuota.



## Crossbar

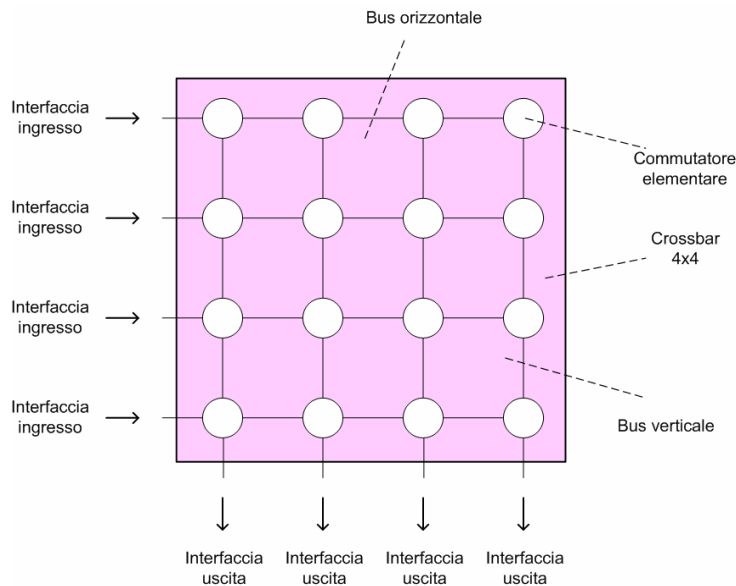
Una possibile alternativa per superare le limitazioni introdotte dallo Switching a Bus condiviso è usare una rete di interconnessione, come quella usata nell'architettura dei computer multiprocessori, che implementa una capacità di trasferimenti multipli sulla Switching fabric grazie alla distribuzione dei pacchetti da trasferire su percorsi diversi.

Dal punto di vista logico (e didattico) la Crossbar è costituita da commutatori elementari collegati da bus di comunicazione, che per una prefissata coppia ingresso-uscita presenta una pluralità di connessioni possibili.



Nell'ipotesi di un commutatore a **N porte**, cioè con N ingressi con N uscite, si hanno  **$N^2$  commutatori** e  **$2N$  bus** e le possibili connessioni sono  **$N^N$** , ma **solo N connessioni possono essere simultaneamente attive**.

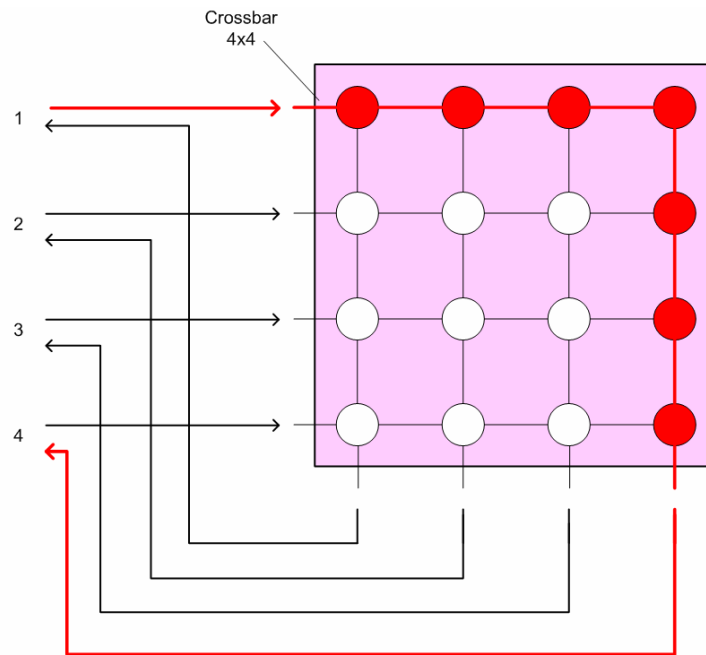
La figura che segue illustra lo schema logico (e didattico) di uno Switch a 4 porte ad architettura Crossbar.



La chiusura di un punto di incrocio permette la connessione tra un'interfaccia di ingresso e una di uscita: un pacchetto che arriva a una porta di ingresso si muove sul bus orizzontale corrispondente sino a incrociare il bus verticale della porta di uscita desiderata.

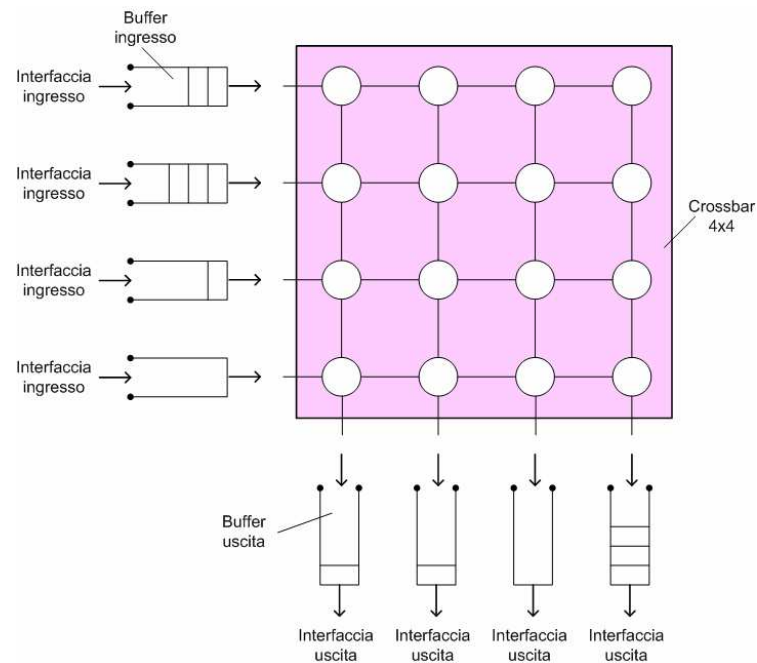
La Crossbar è cioè in grado di trasferire i pacchetti ricevuti su ogni interfaccia di ingresso sulla rispettiva interfaccia di uscita se non occupata in un trasferimento, cioè in ogni istante può collegare qualsiasi ingresso a qualsiasi uscita non occupata.

La figura che segue illustra lo stato della matrice di commutazione dello Switch nell'ipotesi d'inoltro di un pacchetto dalla porta 1 alla porta 4.



Anche nel caso della tecnologia Crossbar se il bus della porta di uscita è occupato, il pacchetto viene bloccato e accodato alla porta di uscita in un buffer finito, se invece il dispositivo di commutazione non è tanto veloce da trasferire i pacchetti in arrivo allora si ha un accodamento anche alle porte di ingresso in appositi buffer finiti d'ingresso.

La figura che segue illustra lo schema di un dispositivo di commutazione a Crossbar con buffer in ingresso e uscita.



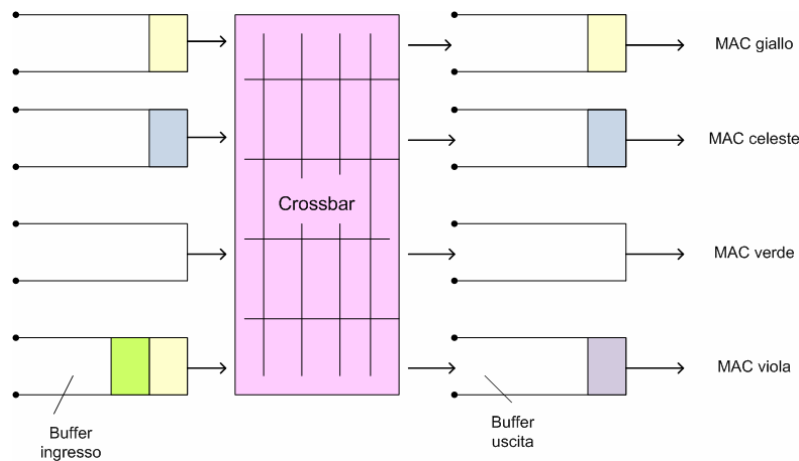
Come per l'architettura a Bus se la velocità è almeno uguale alla capacità aggregata delle interfacce,  $NB_{max}$ , non c'è accodamento alle porte di ingresso e code alle porte di uscita.



Se la velocità dell'architettura è pari alla velocità del collegamento, cioè non dipende dal numero delle porte (speedup pari a 1) c'è accodamento alle porte di ingresso e assenza di code alle porte di uscita.

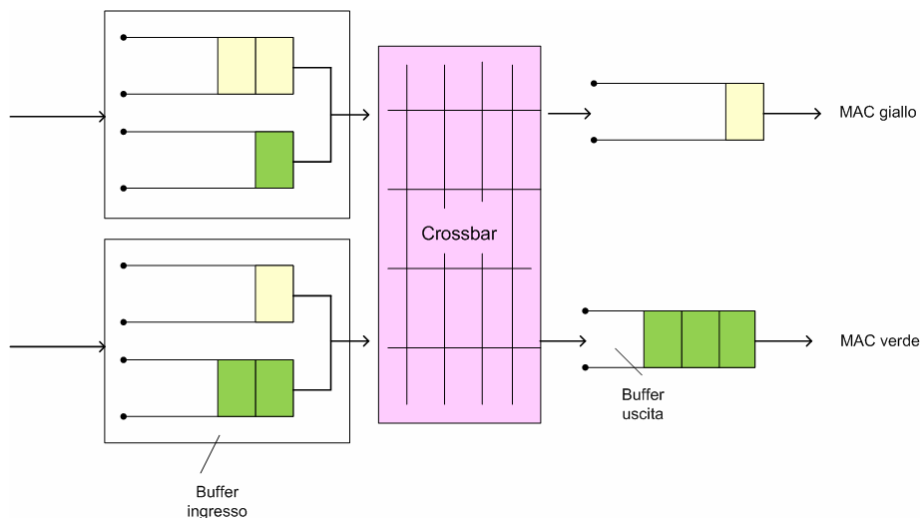
L'accodamento alle porte di ingresso comporta che ci possa essere attesa in coda anche per i pacchetti che potrebbero essere trasferiti perché pur essendo la porta di uscita libera sono bloccati dal pacchetto in cima alla coda (fenomeno conosciuto come **blocco HOL**, Head Of Line Blocking).

Nella figura che segue si illustra il blocco HOL: il pacchetto verde non può essere trasmesso, anche se la porta verde è libera, perché il pacchetto giallo che lo precede è bloccato.



In questo caso è necessario un sistema di decisione di quale dei pacchetti gialli ha diritto ad essere trasmesso, come per esempio: random (necessario un random engine); round-robin (necessario un puntatore all'ultima uscita servita); coda più lunga (necessario indicatori di occupazione),...

Un'altra soluzione consiste nella **Virtual output queuing WOQ** che consiste nel definire su ogni buffer di memoria d'ingresso un numero di code logiche pari al numero di porte di uscita in cui ciascuna coda logica contiene i pacchetti diretti ad un'uscita. Si nota che il collo di bottiglia del sistema è lo scheduler che deve gestire  $N^2$  code contemporaneamente.



Un'altra situazione di accodamento, in ingresso, è quella che si verifica quando più porte in ingresso vogliono trasferire sulla stessa porta in uscita e la Crossbar è libera, cioè pronta a trasferire: un pacchetto viene trasferito e gli altri accodati... la soluzione consiste nell'aumentare la velocità di trasferimento eliminando le code d'ingresso.

E' evidente che la velocità interna del dispositivo per non costituire un collo di bottiglia deve essere superiore alla velocità della singola porta per permettere più trasmissioni in contemporanea e che questa banda interna aumenta, anche, la banda utile per ogni host.

Se, per esempio, lo Switch ha una capacità trasmissiva di 160 Mbps e il numero di host collegati è 32 allora i 10 Mbps di ethernet diventano effettivamente disponibili per ciascuna singola stazione: 10 Mbps per ognuna delle 16 possibili coppie.

## Bloccante e non bloccante

---

Introduciamo il concetto di dispositivo di commutazione **bloccante** e **non bloccante**.

In un dispositivo bloccante, come il Bus, la possibilità di instaurare una connessione tra due porte libere è condizionata dallo stato interno del dispositivo: se il dispositivo è in stato di blocco non è possibile la connessione.

In un dispositivo bloccante la probabilità di blocco è diversa da zero.

In un dispositivo non bloccante, come il Crossbar, è sempre possibile instaurare un percorso tra due porte libere qualunque: il dispositivo non ammette stati di blocco, in altri termini un commutatore si dice non bloccante se in qualunque condizione di traffico è sempre possibile collegare qualunque ingresso con qualunque uscita. In realtà il concetto è in senso lato, cioè gli stati bloccanti possono essere evitati con opportuna strategia di assegnamento dei percorsi.

In un dispositivo non bloccante la probabilità di blocco è uguale a zero.

Sebbene possa sembrare conveniente utilizzare dispositivi non bloccanti in modo tale da avere una garanzia di connessione, è da osservare che la complessità e il costo di tali dispositivi rende in molti casi più interessante la scelta bloccante: un'attenta analisi statistica della probabilità di blocco in funzione del traffico da gestire permette di verificare le perdite di prestazioni introdotte e giustificare o meno la scelta.

## Banda passante aggregata

---

Introduciamo il concetto di **banda passante aggregata**.

La banda passante aggregata di un nodo di rete (Switch) è il massimo traffico possibile gestibile dal nodo, che è uguale alla somma della banda passante di tutti collegamenti contemporaneamente in funzione in un dato momento.

Quindi, un nodo con  $N$  porte con banda massima uguale per ogni porta di  $B_{max}$  con trasferimento full-duplex è pari  $N \times B_{max}$ .

Infatti, se tutti i collegamenti inviano contemporaneamente dati alla velocità  $B_{max}$  il massimo traffico sarà rappresentato da  $N/2$  porte a  $2B_{max}$

che conversano con le altre  $N/2$  porte alla stessa velocità, quindi  $N/2 \times 2B_{\max}$  pari a  $N \times B_{\max}$ .

Ad esempio, nel caso di uno Switch con 24 porte 10/100/1000 Mbps, il massimo traffico sarà rappresentato da 12 porte a 1000 Mbps che conversano con le altre 12 porte alla stessa velocità, con la modalità a più alte prestazioni (full-duplex), dando origine ad un traffico di 24 Gbps. La banda passante effettiva dello Switch, per riuscire a gestire il traffico richiesto, dovrà quindi essere uguale a 24 Gbps.

## Classificazione delle architetture di commutazione

Come si è visto le architetture di commutazione prevedono l'utilizzo di code in ingresso, code in uscita oppure code distribuite (ingresso/uscita).

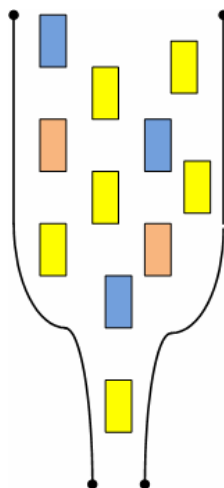
La presenza di una tipologia di coda determina la tipologia dell'architettura di commutazione, riassumendo:

- Architettura a coda d'uscita, richiede un'architettura ad alta velocità (alto speedup) e si utilizza solitamente con il Bus.
- Architettura a coda d'ingresso, necessita di un controllo per la gestione del blocco HOL e si utilizza solitamente con dispositivi non bloccanti.
- Architettura distribuita, molto complessa da implementare.

## Switch collo di bottiglia (bottleneck)

**Un problema che si evidenzia nelle LAN riguarda la capacità dei nodi, posizionati nelle aree ad elevato traffico, di discriminare e instradare il traffico con la velocità richiesta.**

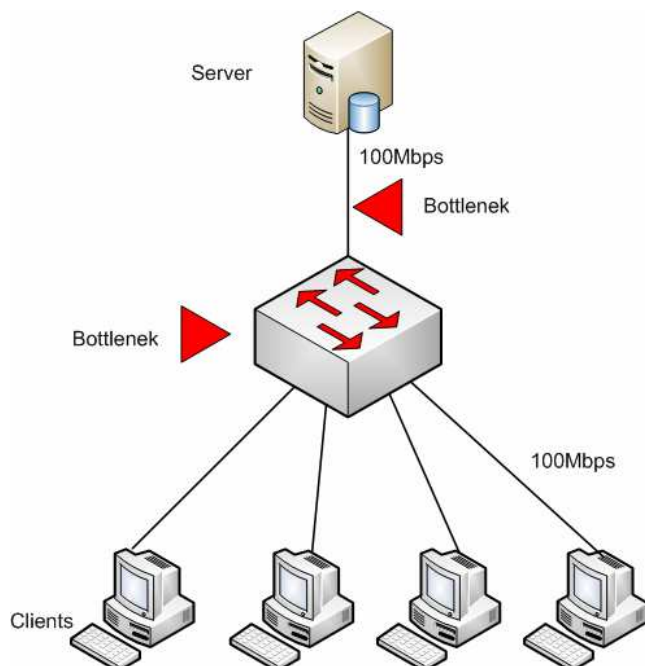
**In caso contrario i dispositivi costituiscono dei colli di bottiglia per il traffico, cioè i punti in cui la LAN ha le minori prestazioni.**



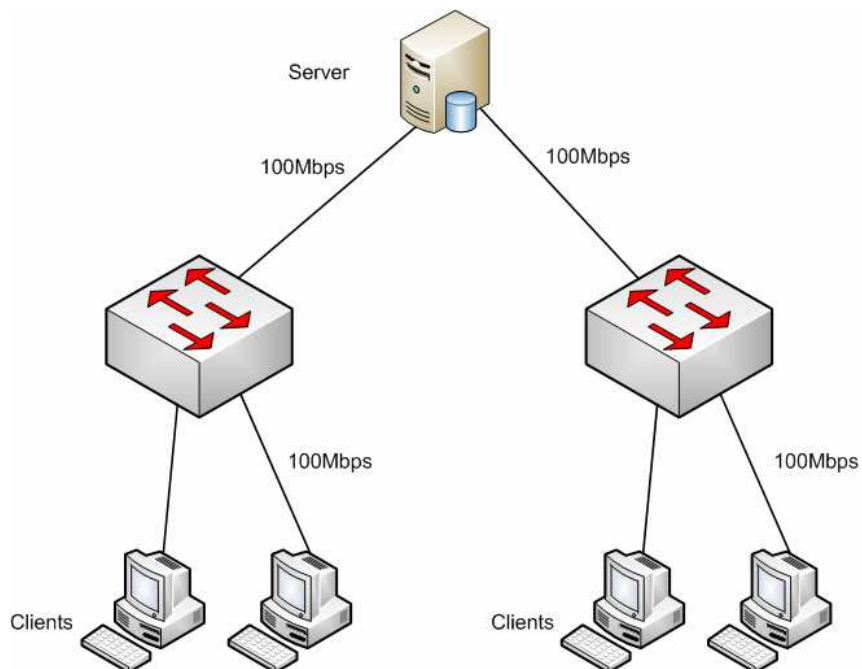
Per esempio in una LAN con 200 host se il 25% delle 200 postazioni opera con una velocità di 100 Mbps, avremo un traffico complessivo nell'area ad elevato traffico uguale a 5 Gbps e quindi è necessario che i dispositivi attivi siano in grado di processare dati a quella velocità.

Le aree ad elevato traffico sono tipicamente quelle dove vi sono servizi condivisi e i nodi/collegamenti che accedono a questi (dorsali della rete), per esempio i server oppure l'accesso ad Internet.

Nella figura che segue si evidenziano i possibili colli di bottiglia.



Risulta intuitivo che un possibile miglioramento delle prestazioni della rete si ha con la seguente soluzione:



## Throughput

E' tipicamente espresso in numero di pacchetti per secondo **PPS** calcolati nel caso peggiore di pacchetto da trasferiti dal commutatore ed è limitato per ragioni tecnologiche e di traffico (contesa per risorse interne e sulle uscite).

## Dominio di collisione e broadcast

Nelle reti "Ethernet" rilevanti sono il concetto di dominio di collisione e di broadcast.

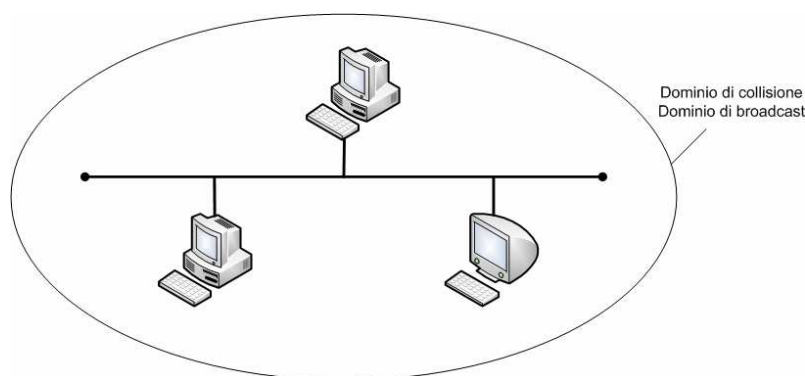
Il **dominio di collisione** è la parte di una LAN per cui se due nodi trasmettono contemporaneamente si ha una collisione, cioè è un segmento di rete in cui c'è contesa del mezzo trasmissivo.

E' un concetto molto importante perché se la rete è suddivisibile in domini di collisione separati, partizionati, allora più host possono accedere contemporaneamente al mezzo.

Il **dominio di broadcast** è la parte della rete raggiunta da un pacchetto con indirizzo di broadcast ed è costituito dai nodi che appartengono alla medesima rete di livello 2, per questo il dominio è anche detto segmento data-link, in altri termini un dominio broadcast è un insieme di domini di collisione connessi tra loro con dispositivi di livello 2 e delimitato da dispositivi di livello 3.

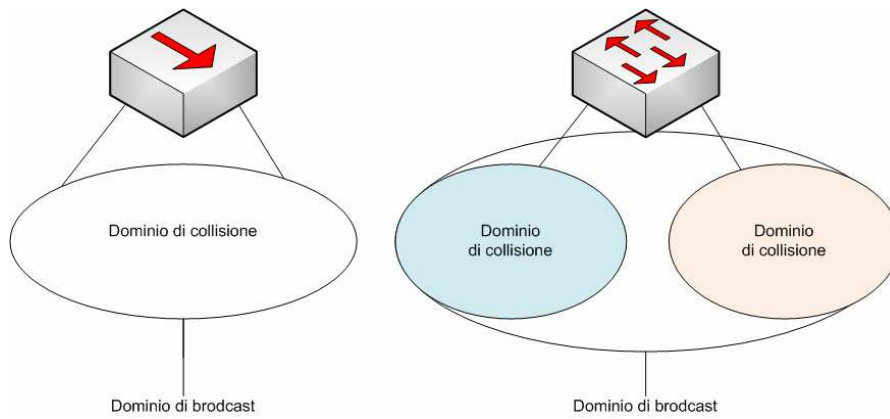
Quindi, la dimensione del dominio di broadcast è ricavabile dai domini di collisione che processano il frame di broadcast.

I due domini coincidono nella topologia a bus e possono essere diversi nella topologia a stella a seconda del dispositivo utilizzato per implementare il centro stella.



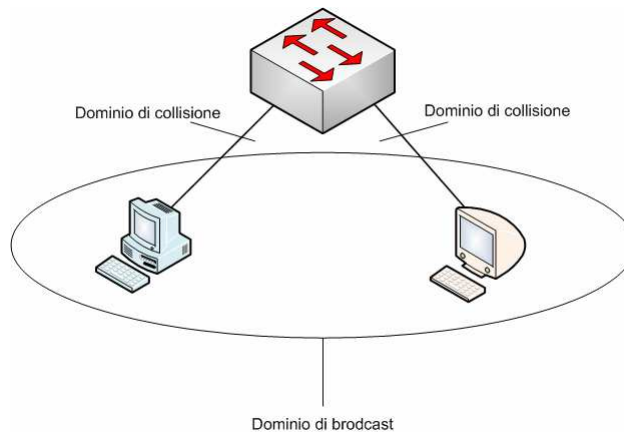
In particolare nelle topologie a stella l'Hub non modifica il dominio di collisione, mentre lo Switch lo partiziona in sottodomini, detti anche segmenti, pari al numero delle porte del dispositivo.

La capacità dello Switch di partizionare il dominio di collisione è di fondamentale importanza per le prestazioni della rete: il fenomeno delle collisioni è confinato all'interno di ogni singolo dominio e non vi è propagazione negli altri domini, quindi le prestazioni di una rete a stella sono notevolmente superiori nel caso di centri stella con Switch e con Hub rispetto a centri stella con soli Hub.



Nel caso di utilizzo di soli Switch?

In questo caso la rete è costituita da soli canali punto-punto: i collegamenti dominio di collisione sul mezzo condiviso (micro-segmento) costituito da 2 nodi.



Con l'utilizzo dello Switch il canale punto-punto è conteso da due soli contendenti se questo è half-duplex, mentre non lo è se full-duplex.

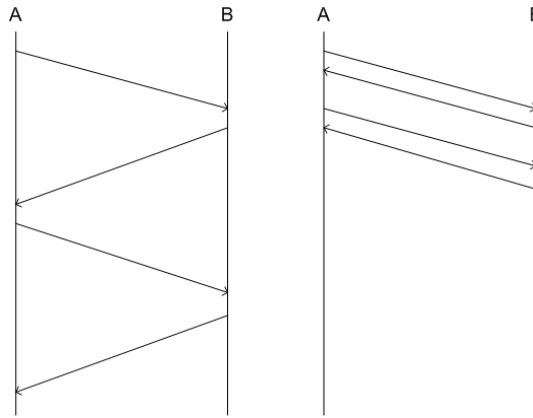
### Half-duplex e full-duplex

I collegamenti half-duplex, un esempio è il walkie-talkie, non sono in grado di consentire la trasmissione contemporanea nelle due direzioni. In tali collegamenti le collisioni si possono verificare solo tra l'host e lo Switch e servono appunto a gestire la natura half-duplex del collegamento.

I collegamenti full-duplex<sup>8</sup>, un esempio la telefonia, costituiscono un canale dedicato e la trasmissione è contemporanea nelle due direzioni, cosa che raddoppia la banda teorica del canale. Questi sono dei canali molto particolari in quanto non esiste rivalità sul mezzo (media contention) e di conseguenza non soggetti a collisione (in ogni direzione c'è un solo nodo che può trasmettere e quindi per definizione non può collidere con nessun'altro) e non esiste l'arbitraggio CSMA/CD. Inoltre i limiti di distanza non sono più dettati dal livello MAC, ma solo dal livello fisico.

La figura che segue illustra le due tipologie di canale: half-duplex e full-duplex nella comunicazione tra due nodi A e B.

<sup>8</sup> Cosa ottenibile anche con due collegamenti half-duplex in parallelo.



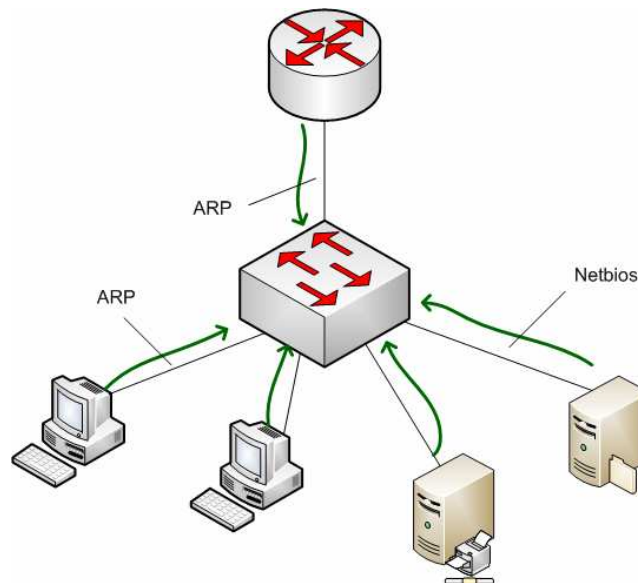
La comunicazione full-duplex implica l'adozione di tecnologie full-duplex in tutti i livelli, e in particolare l'adozione di un cablaggio idoneo a questa comunicazione come il cavo UTP di categoria 5 con 4 coppie in cui una coppia si usa per trasmettere e una per ricevere simultaneamente oppure il cavo bifibra per la fibra ottica.

### Router e dominio di broadcast e collisione

Il dominio di broadcast rimane sempre lo stesso con Hub e Switch.

Sorgenti possibili di broadcast (e multicast) in IP sono host (richieste ARP, annunci dei server), router, applicazioni multicast e protocolli (Netbios).

E' utile rilevare che spesso non vi sono benefici nel traffico broadcast: le informazioni propagate non interessano gli host oppure ne sono già a conoscenza.

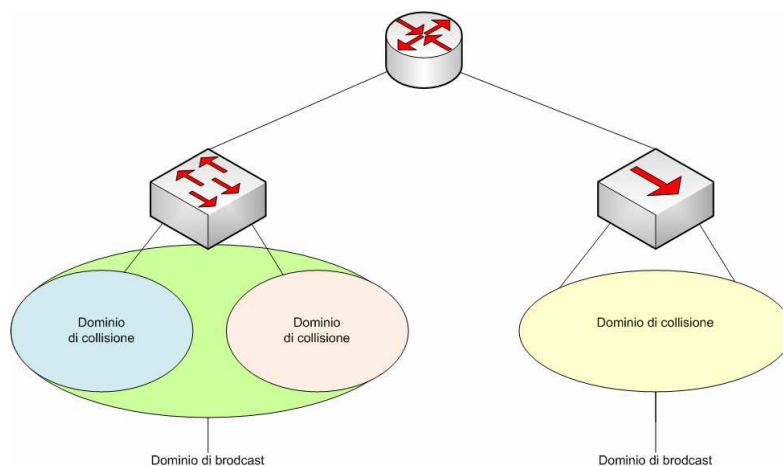


La separazione del broadcast (e multicast) necessita di dispositivi di livello 3 come il Router che blocca l'indirizzo di broadcast, cioè lo confina alla rete attestata nella propria interfaccia.

**Il Router è un dispositivo di livello 3 che assume decisioni d'inoltro sulla base dell'indirizzo di livello 3 e non sull'indirizzo di livello 2 MAC.**

Per questo: non propagano le collisioni, spezzano il dominio di collisione in sottodomini e soprattutto e diversamente dai dispositivi di livello 2, separano anche il dominio di broadcast in più domini.

La figura che segue illustra i domini nel caso di una rete costituita da due reti interconnesse da Router, con una basata su Switch e l'altra su Hub.



Questa capacità di separazione del broadcast è importante per le prestazioni di una LAN anche alla luce del fenomeno del broadcast radiation (propagazione).

Il broadcast radiation è l'accumulo totale del traffico broadcast (e multicast) dei nodi che può raggiungere lo stato del broadcast storm<sup>9</sup> (tempesta) che si ha quando la circolazione del traffico broadcast arriva a saturare la banda, inibendo o interrompendo le connessioni di rete esistenti.

---

<sup>9</sup> La probabilità di avere tempeste broadcast è proporzionale al numero di Switch.



## Cavi di collegamento

Nell'utilizzo delle topologie a stella particolare attenzione deve essere rivolta al cavo utilizzato per il collegamento tra nodi e dispositivi di rete e tra dispositivi di rete.

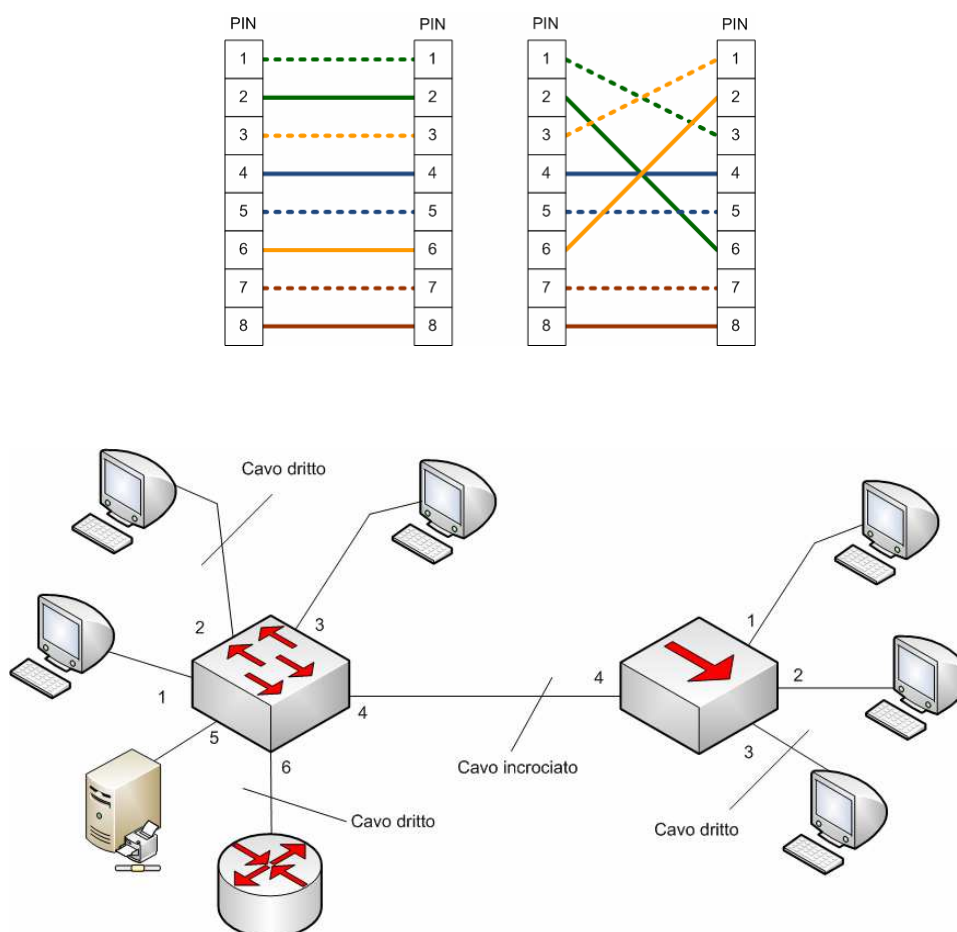
Gli standards Ethernet **10Base-T** e **100BASE-TX** usano due coppie per la trasmissione in ciascuna direzione in cui la coppia che trasmette di ciascun dispositivo deve essere connessa alla coppia ricevente del dispositivo dall'altra parte.

Quando un nodo è connesso ad uno Switch o Hub, questo incrocio è fatto internamente nell'apparato e per questo il cavo deve essere dritto (straight-through), cioè ciascun piedino del connettore da una parte è connesso al corrispondente piedino sull'altro connettore.

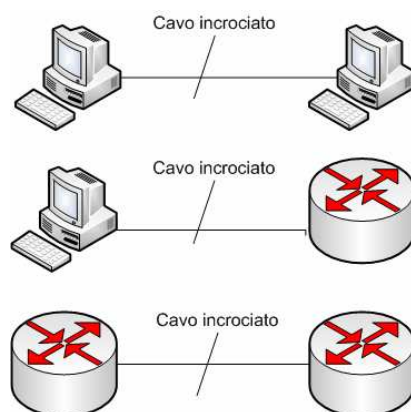
Quando un nodo è connesso ad un altro nodo oppure si connettono due dispositivi che effettuano l'incrocio internamente, come Hub e Switch, deve essere utilizzato un cavo incrociato (o crossover) in modo che gli incroci interni si annullino a vicenda.

Nel caso di connessione ad un router, a differenza di Hub e Switch, il cavo utilizzato deve essere quello dritto.

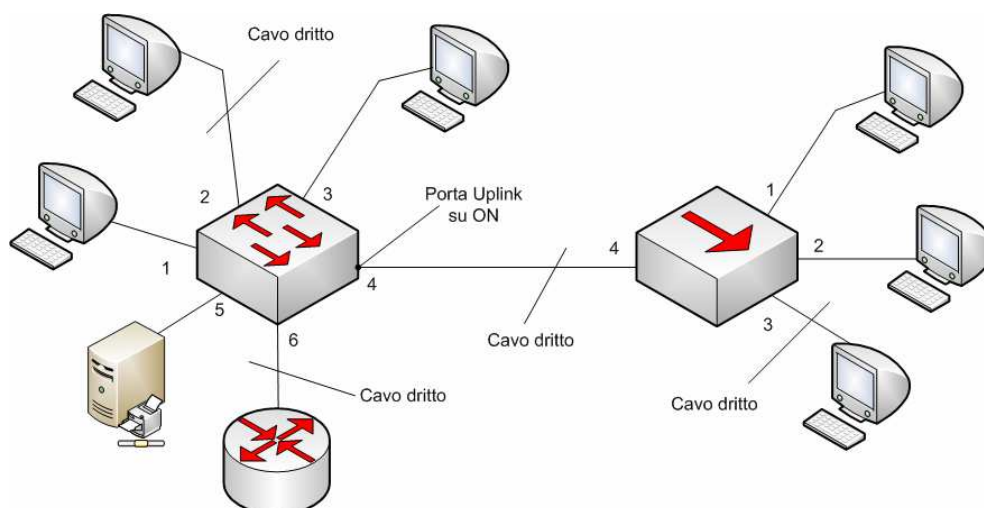
Le figure che seguono illustrano le due tipologie di cavo (dritto e incrociato) e il loro utilizzo in una rete con Hub, Switch e Router.



La seguente figura illustra il caso di collegamento tra due host, tra un host e un router e tra due router.



Gli Hub e gli Switch allo scopo di utilizzare il cavo dritto, e quindi eliminare eventuali errori di installazione, permettono di configurare meccanicamente (con un pulsante) una porta, detta solitamente di Uplink o MDI/MDIX<sup>10</sup>, come porta da usare per il collegamento di altri dispositivi.



E' importante sottolineare che oggi quasi tutte le schede di rete e i dispositivi di rete applicano automaticamente un incrocio interno quando necessario, rendendo non necessario l'utilizzo dei cavi incrociati e rende obsoleta le porte uplink, oggi non più fornite. Questa caratteristica è conosciuta con vari termini specifici dei rivenditori, comunemente Auto-MDI/MDIX o auto sensing.

Nello **standard 1000BASE-T** la capacità MDI/MDIX automatica è specificata nello standard e al contrario dei cavi incrociati descritti sopra, con solo 2 coppie invertite, un cavo incrociato 1000BASE-T ha tutte le coppie.

<sup>10</sup> Medium dependent interface crossover.

**Titolo**

Hub e Switch

**Autore**

Prof. Nicola Ceccon

**Email**

nicola.ceccon@istruzione.it

**Classe**

QUINTA INFORMATICA (5IA)

**Anno scolastico**

2010/2011

**Scuola**

Itis Euganeo

Via Borgofuro 6 - 35042 Este (PD) - Italy

Telefono 0429.21.16 - 0429.34.72

Fax 0429.41.86

<http://www.itiseuganeo.it>

[segreteria@itiseuganeo.it](mailto:segreteria@itiseuganeo.it)

---

**Note legali**

Diffusione consentita con obbligo di citarne le fonti

---

**Informazioni**

[siteditor@itiseuganeo.it](mailto:siteditor@itiseuganeo.it)

[dispense.itiseuganeo.it](http://dispense.itiseuganeo.it)

---