ROMA TRE
UNIVERSITÀ DEGLI STUDI

INGEGNERIA
CIVILE, INFORMATICA E DELLE TECNOLOGIE AERONAUTICHE

Internet and Data Centers

Virtual LAN (VLAN)
e lo standard IEEE 802.1Q

G. Barbagallo, G. Di Battista, M. Patrignani

copyright notice

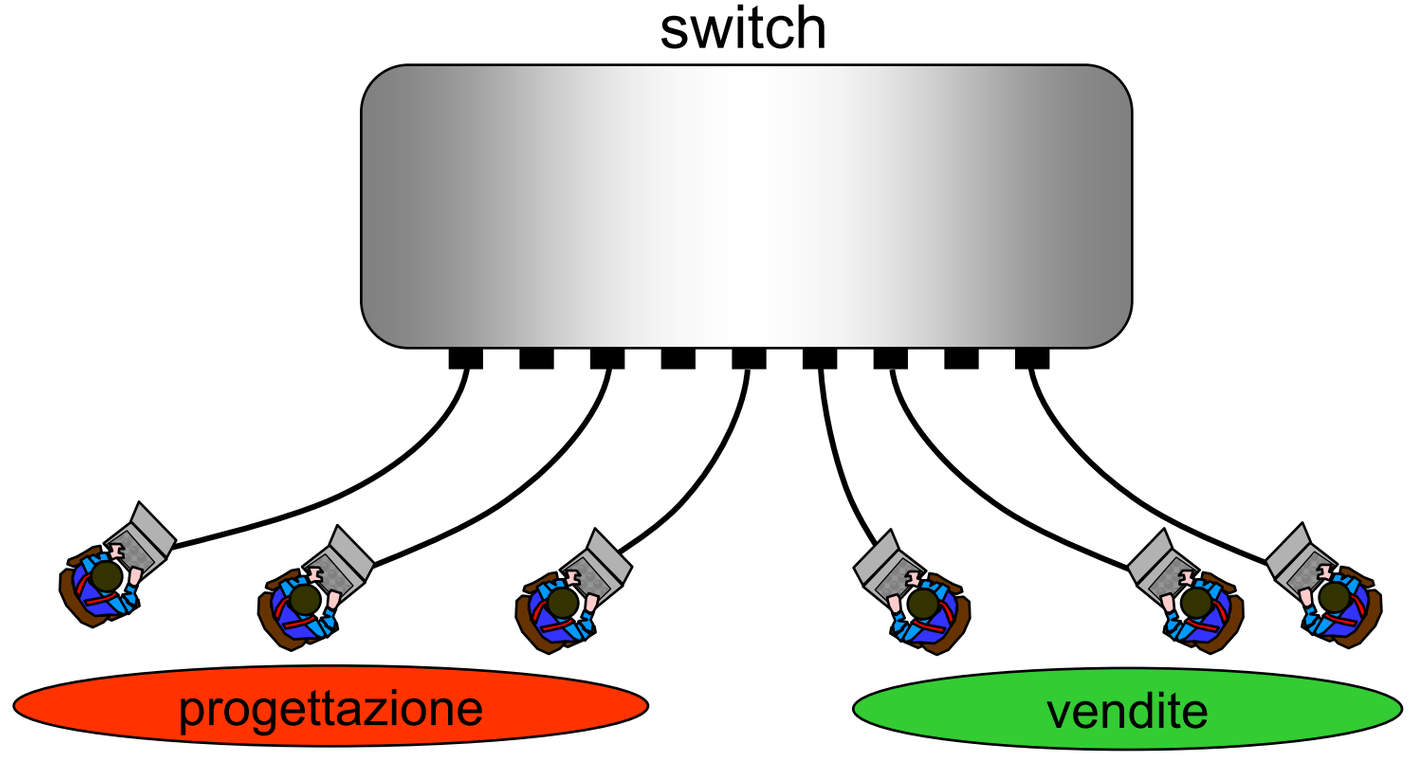
- all the pages/slides in this presentation, including but not limited to, images, photos, animations, videos, sounds, music, and text (hereby referred to as “material”) are protected by copyright
- this material, with the exception of some multimedia elements licensed by other organizations, is property of the authors and/or organizations appearing in the first slide
- this material, or its parts, can be reproduced and used for didactical purposes within universities and schools, provided that this happens for non-profit purposes
- any other use is prohibited, unless explicitly authorized by the authors on the basis of an explicit agreement
- this copyright notice must always be redistributed together with the material, or its portions

motivazioni

la virtualizzazione nelle LAN può rivelarsi utile e talvolta indispensabile: es. nelle LAN degli uffici e in quelle dei data center

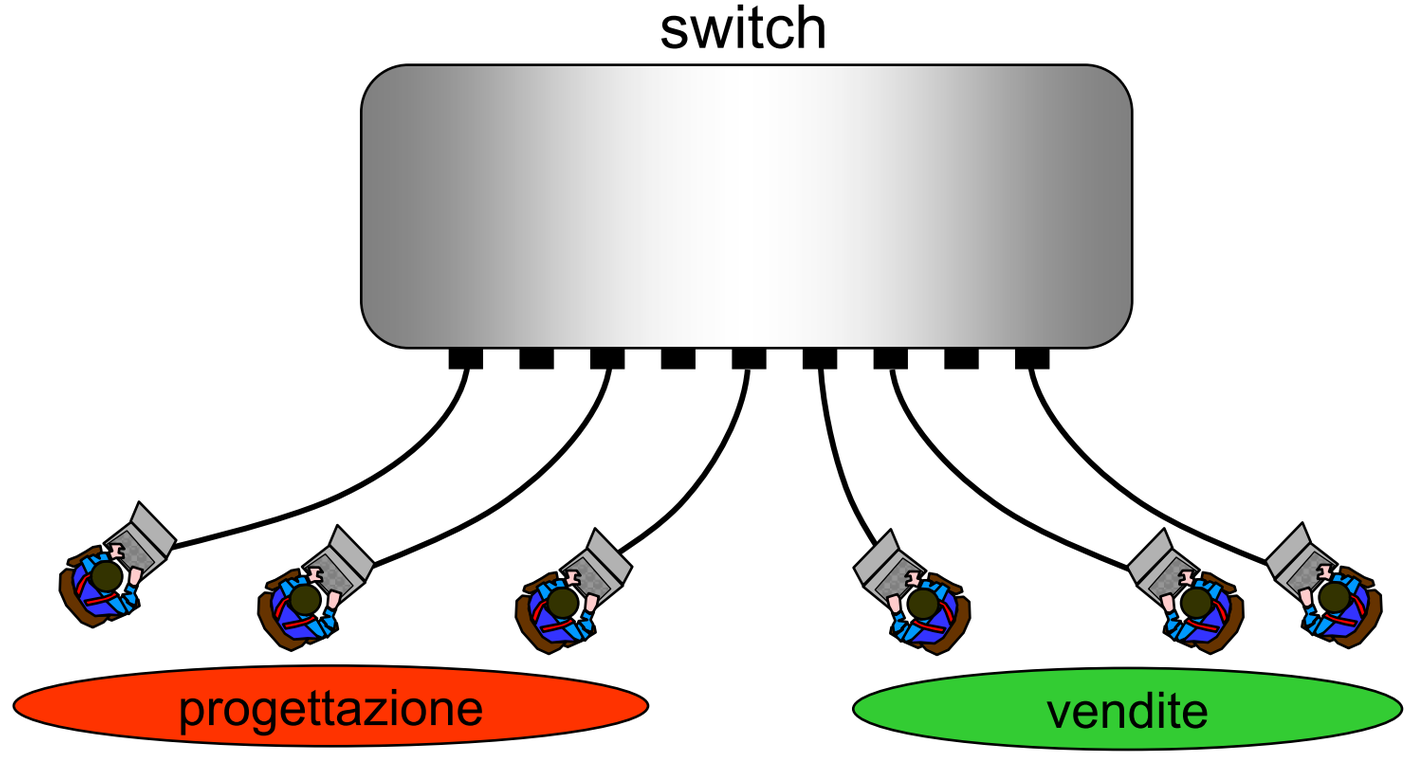
un esempio semplice

- il data center di un'azienda ha una LAN, con un singolo switch, a cui sono connessi vari calcolatori di due diversi uffici



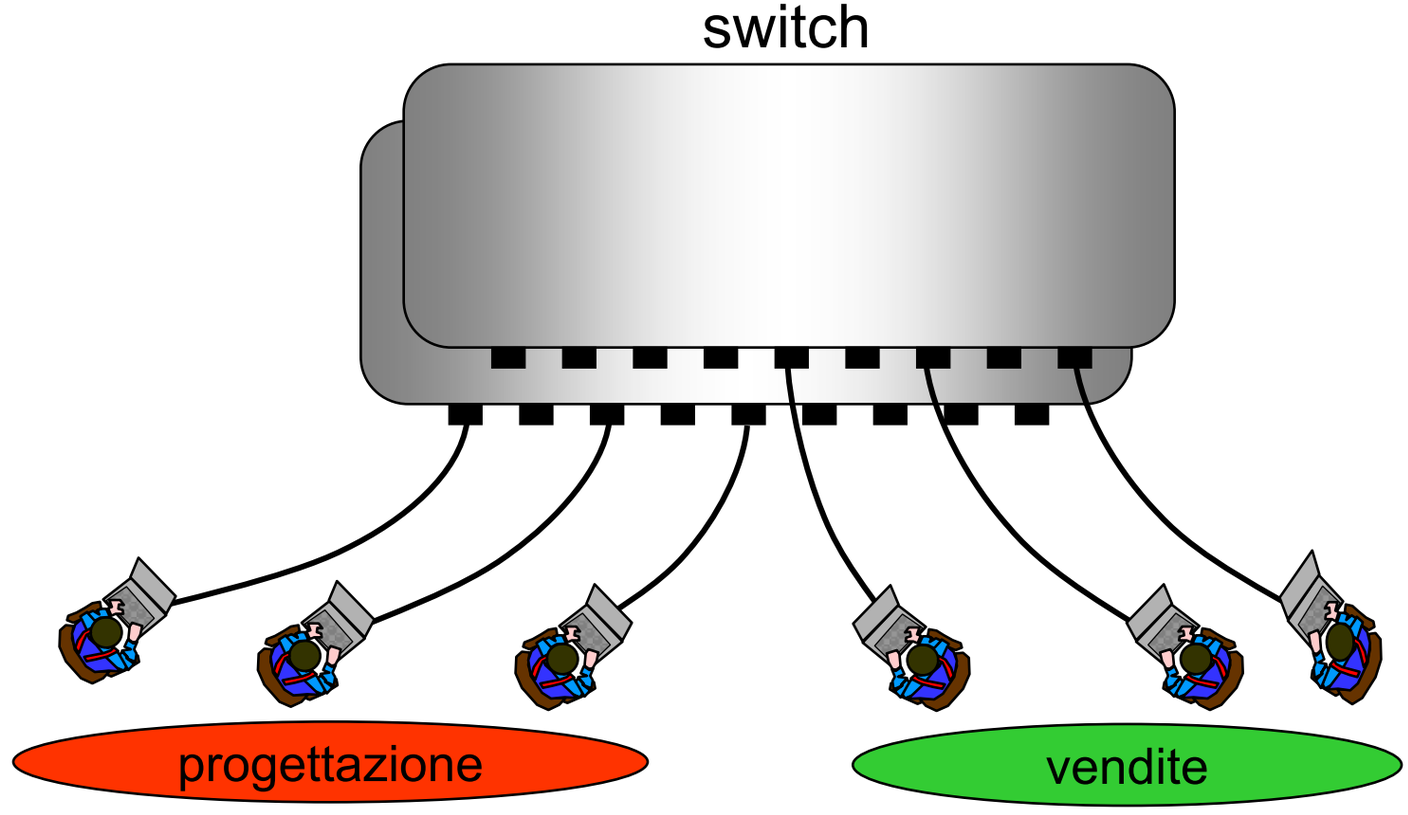
un esempio semplice

- l'azienda vuole suddividere i calcolatori in due LAN separate, per motivi di sicurezza o anche solo per dividere il traffico broadcast



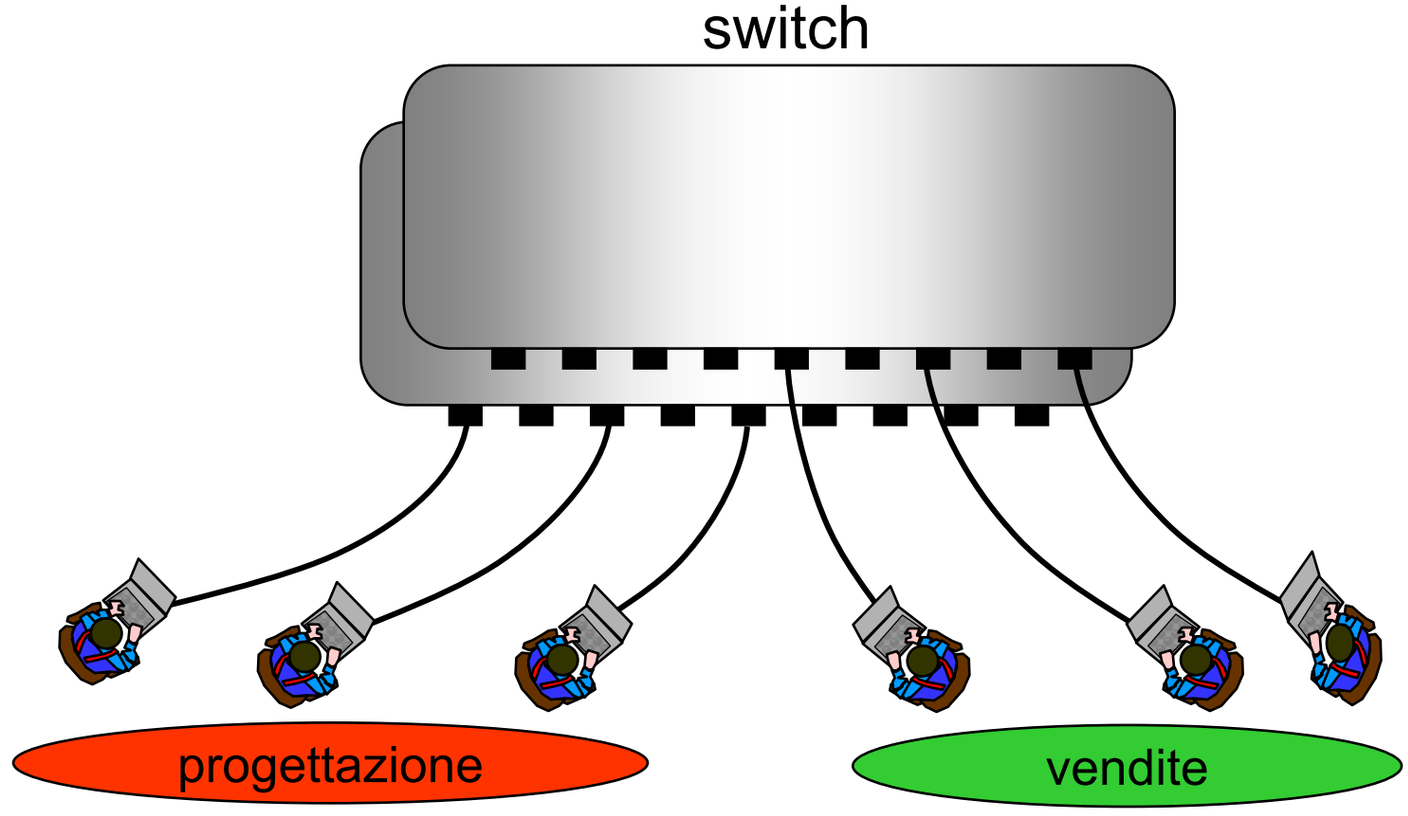
un esempio semplice

- una possibile soluzione : acquistare un nuovo switch e distribuire i calcolatori sui due switch



un esempio semplice

- limitazioni: soluzione poco flessibile, poco adattabile ai cambiamenti, poco economica

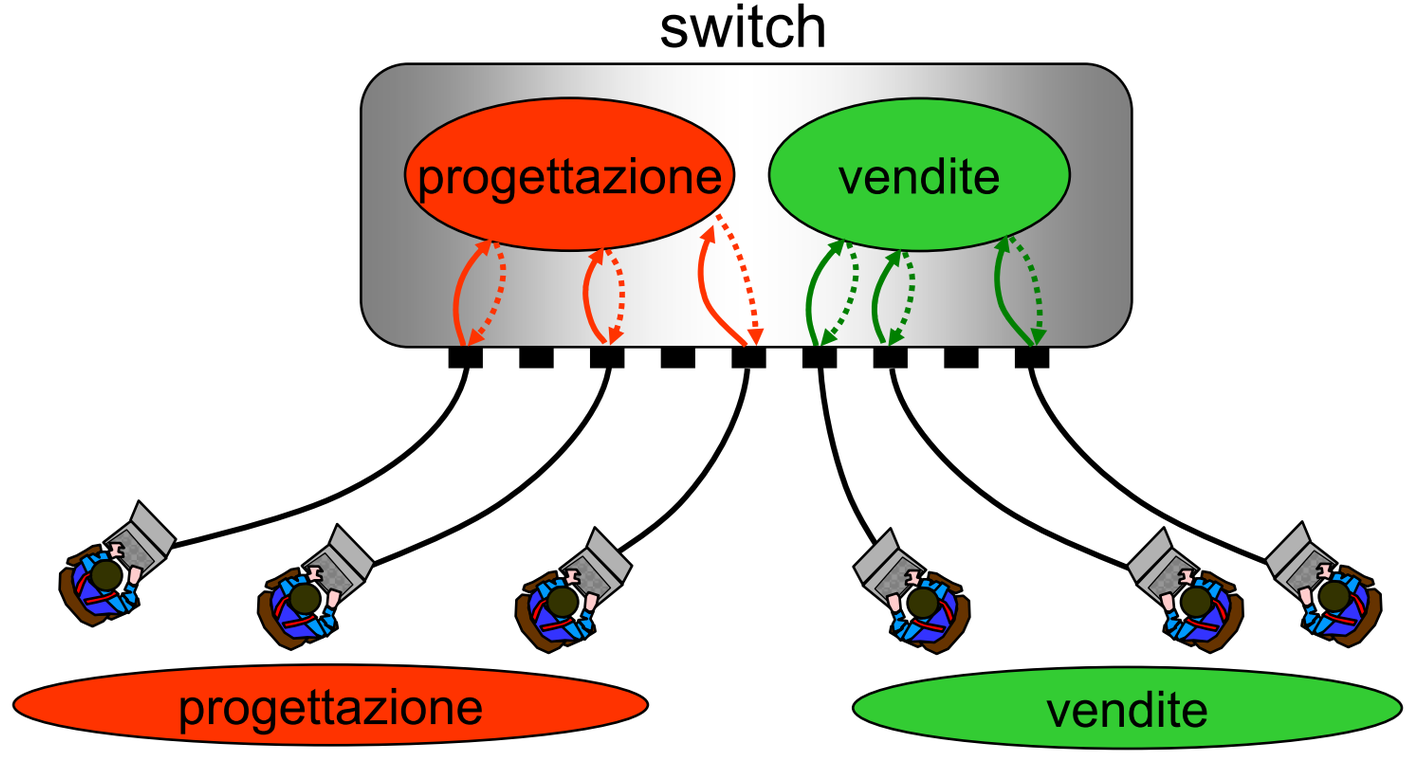


VLAN su un solo switch

come realizzare vari switch virtuali avendo a disposizione un singolo switch

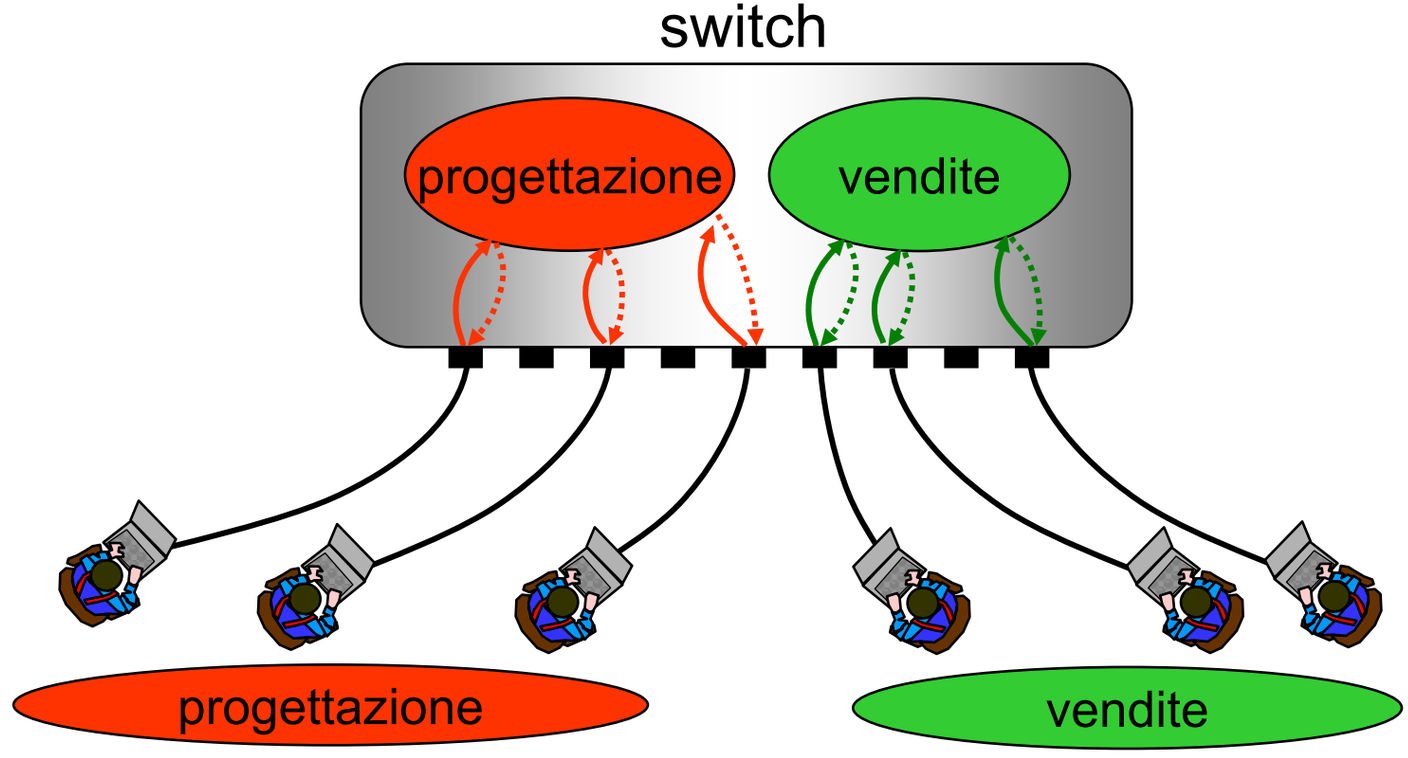
l'idea di VLAN

- definizione di una topologia logica indipendente da quella fisica; diverse lan virtuali sono realizzate sullo stesso switch



l'idea di VLAN

- il traffico di una VLAN è tenuto completamente separato ("segregato") da quello delle altre VLAN



l'idea di VLAN

- le VLAN sono configurate dall'amministratore della rete
- situazione semplice
  - VLAN definite in funzione della porta
    - es: le porte 1, 3, 4 e 7 appartengono alla VLAN rossa; le porte 2, 5 e 6 alla VLAN blu e le porte 8 e 9 alla VLAN arancione
- situazione più complessa
  - VLAN definite in funzione della porta e del contenuto del pacchetto
    - es: MAC address, protocollo di livello 3, ecc.

una semantica per le VLAN

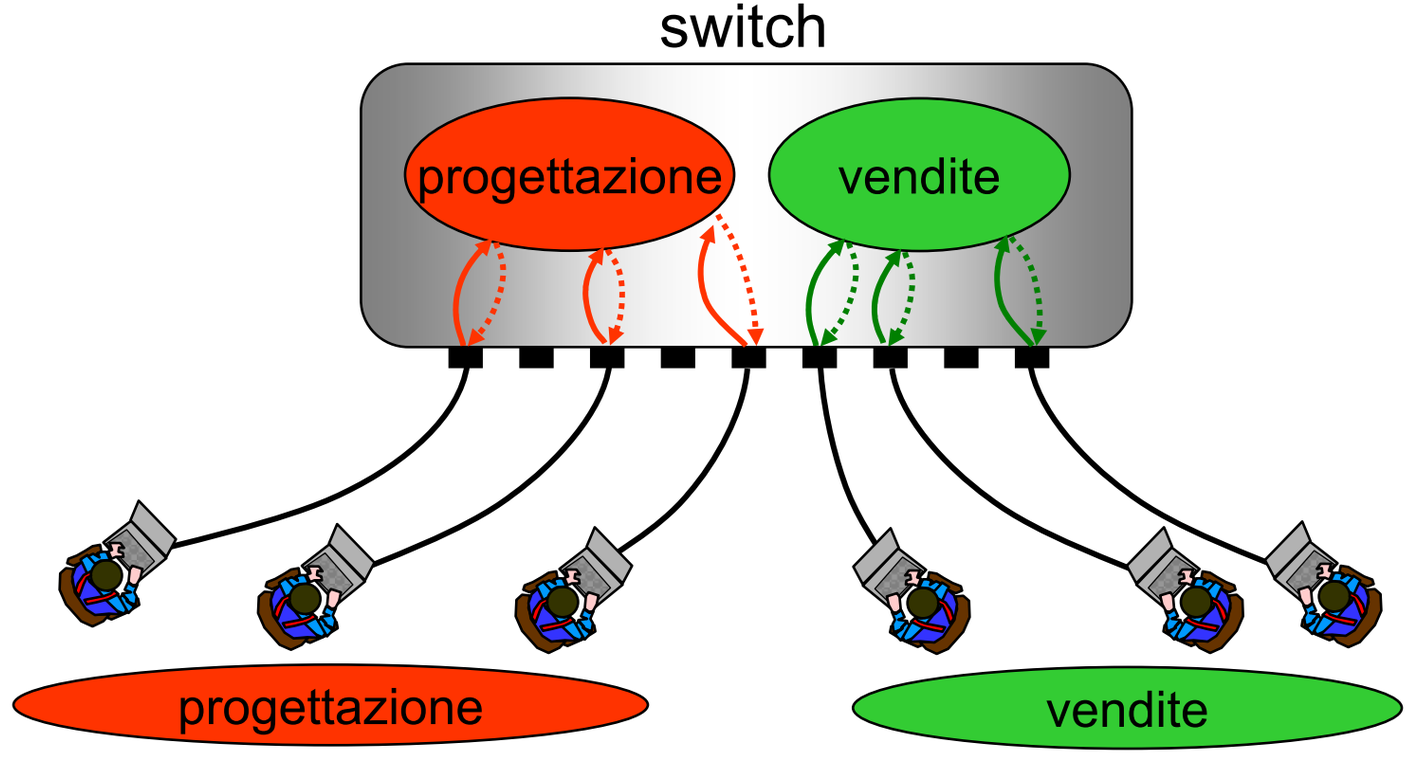
- una VLAN denota un insieme di pacchetti in transito per uno switch
  - es, VLAN rossa: tutti i pacchetti che entrano dalla porta 1, dalla porta 3, dalla porta 4 o dalla porta 7
- un pacchetto può appartenere ad una sola VLAN
  - le regole che descrivono le VLAN (specificabili con un linguaggio che dipende dal costruttore dello switch) attribuiscono ciascun pacchetto ad una VLAN
  - l'insieme dei pacchetti che entrano in uno switch è quindi partizionato in VLAN
  - talvolta per uno switch l'amministratore non definisce nessuna VLAN: in questo caso tutti i pacchetti sono attribuiti ad una VLAN di default

una semantica per le VLAN

- configurazione di una VLAN
  - considera i pacchetti che arrivano allo switch da un certo insieme di porte (*ingress port*)
  - di questi pacchetti, fanno parte della VLAN solo quelli con certe caratteristiche
    - per esempio tutti, o solo quelli con certi MAC address, o solo quelli che portano a bordo il protocollo IP, o…
  - i pacchetti che fanno parte della VLAN possono uscire dallo switch solo attraverso un certo insieme di porte (*egress port*)

una semantica per le VLAN

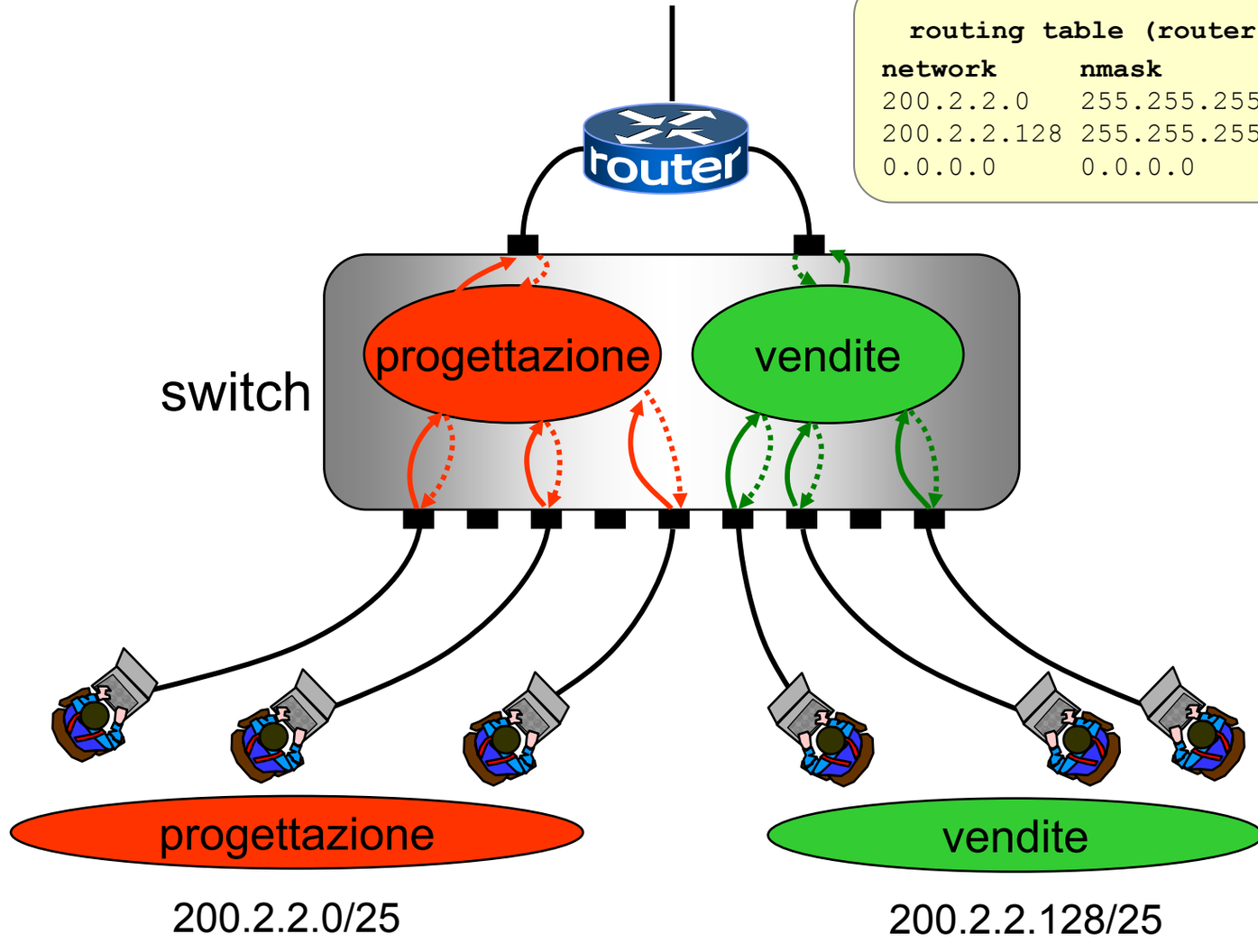
- nell'esempio iniziale (vedi sotto) tutte le ingress port sono anche egress port e tutti i pacchetti ricevuti su un certo insieme di porte partecipano alla VLAN; vedremo esempi più complessi



una semantica per le VLAN

- associazione di un pacchetto ad una VLAN
  - un pacchetto è associato ad una VLAN nell'istante in cui entra nello switch
- ad ogni VLAN è associato un intero (VLAN id) tra 1 e 4094, che la identifica
  - la VLAN di default ha VLAN id = 1
- ad una VLAN è spesso possibile anche dare un nome di 32 caratteri alfanumerici, più facile da ricordare

VLAN e livello 3: un primo esempio



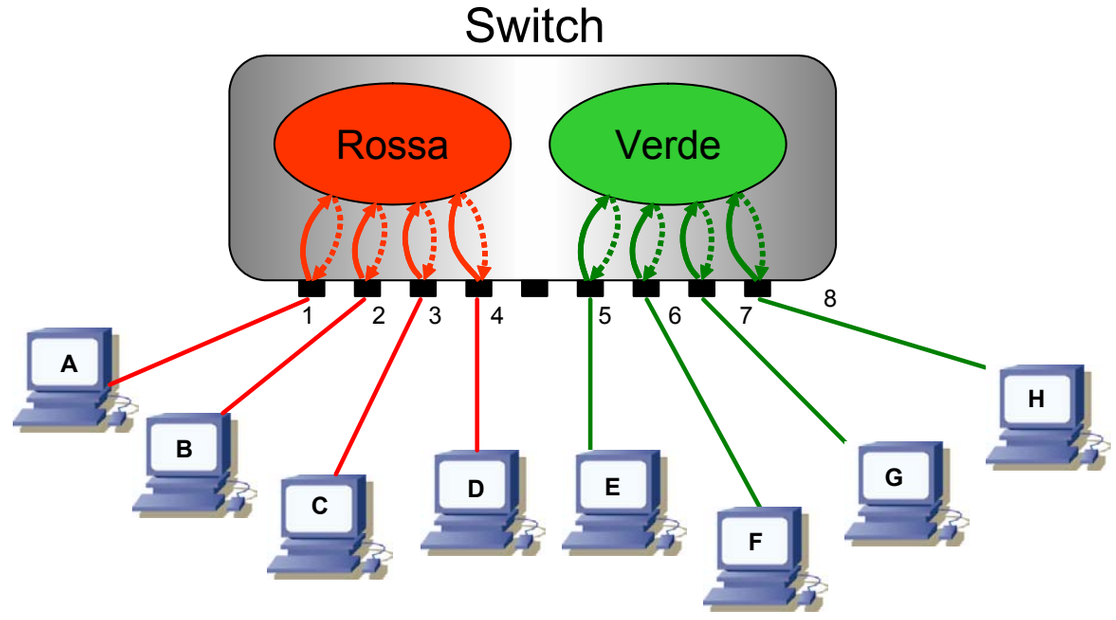
inoltro di un pacchetto

- quando uno switch riceve un pacchetto (in presenza di VLAN):
  - associa il pacchetto ricevuto alla giusta VLAN
    - usando le regole di configurazione
  - individua la porta dello switch da utilizzare per poter trasmettere il pacchetto
    - accedendo al filtering database
  - trasmette (eventualmente) il pacchetto

filtering database

- gli switch possono operare in due modalità alternative
  - IVL, Independent VLAN Learning
    - un filtering database separato per ogni VLAN
  - SVL, Shared VLAN Learning
    - un solo filtering database condiviso tra tutte le VLAN
- alcuni switch possono operare solo in modalità SVL

filtering database: IVL vs SVL



modalità SVL

Porta	Mac	VLAN
1	A	Rossa
2	B	Rossa
3	C	Rossa
4	D	Rossa
5	E	Verde
6	F	Verde
7	G	Verde
8	H	Verde

modalità IVL

Porta	Mac
1	A
2	B
3	C
4	D

DB VLAN rossa

Porta	Mac
5	E
6	F
7	G
8	H

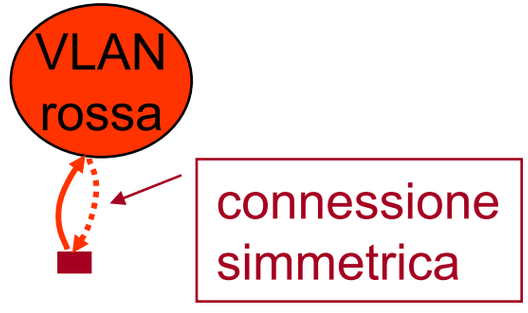
DB VLAN verde

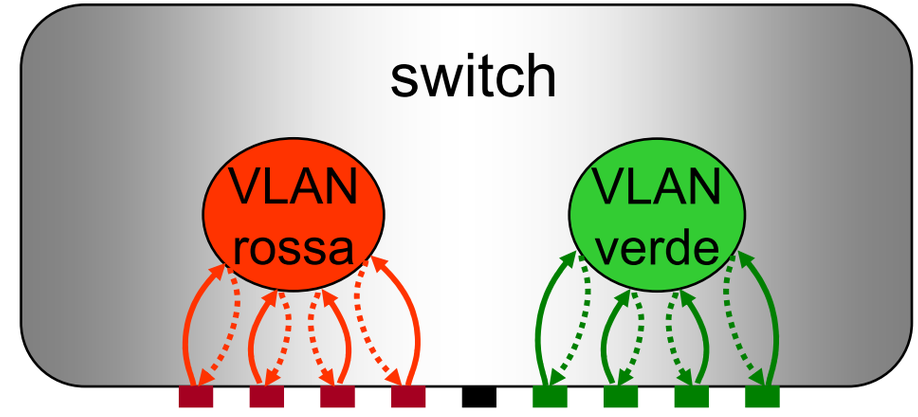
eventuale trasmissione del pacchetto

- due possibilità:
  - la ricerca nel filtering database non è andata a buon fine ovvero non è stata individuata nessuna porta
    - lo switch trasmette il pacchetto in broadcast su tutte le egress port associate alla VLAN di appartenenza del pacchetto
  - la ricerca nel filtering database ha individuato una porta
    - lo switch, prima di trasmettere il pacchetto, controlla che la porta individuata sia stata configurata come egress port per la VLAN del pacchetto
    - in caso affermativo il pacchetto viene trasmesso, altrimenti viene scartato

VLAN simmetriche

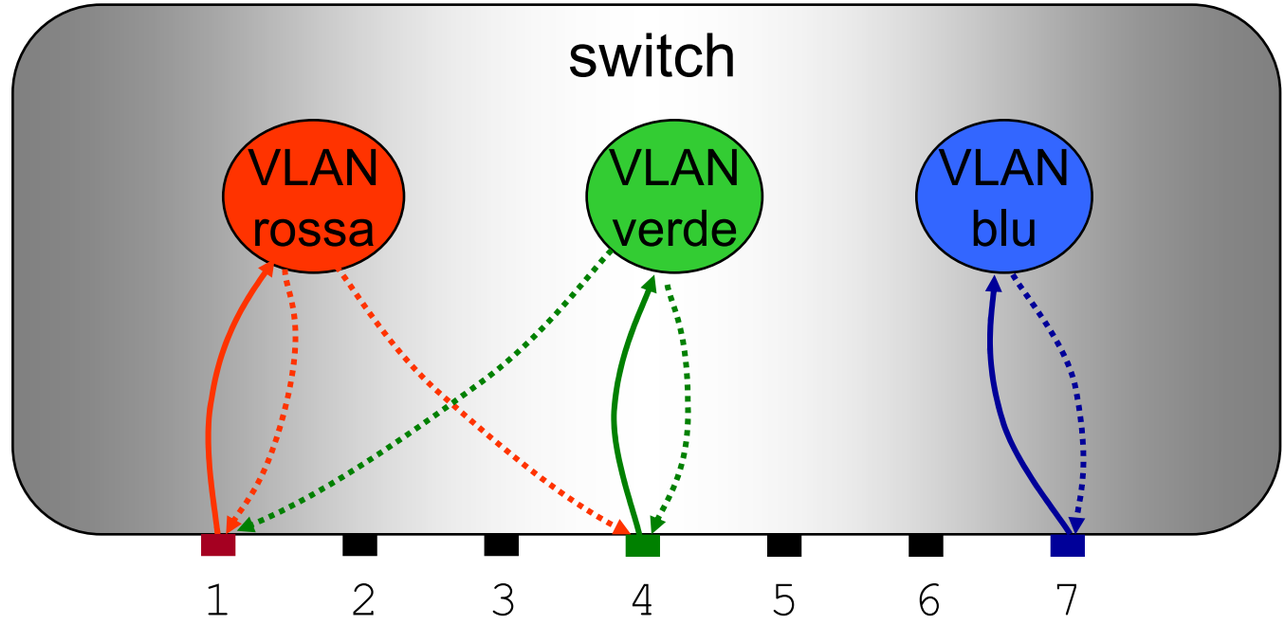
- finora abbiamo fatto solo esempi di VLAN simmetriche
  - *VLAN simmetriche*: ogni volta che una porta è ingress per una VLAN è anche egress per la stessa VLAN e viceversa





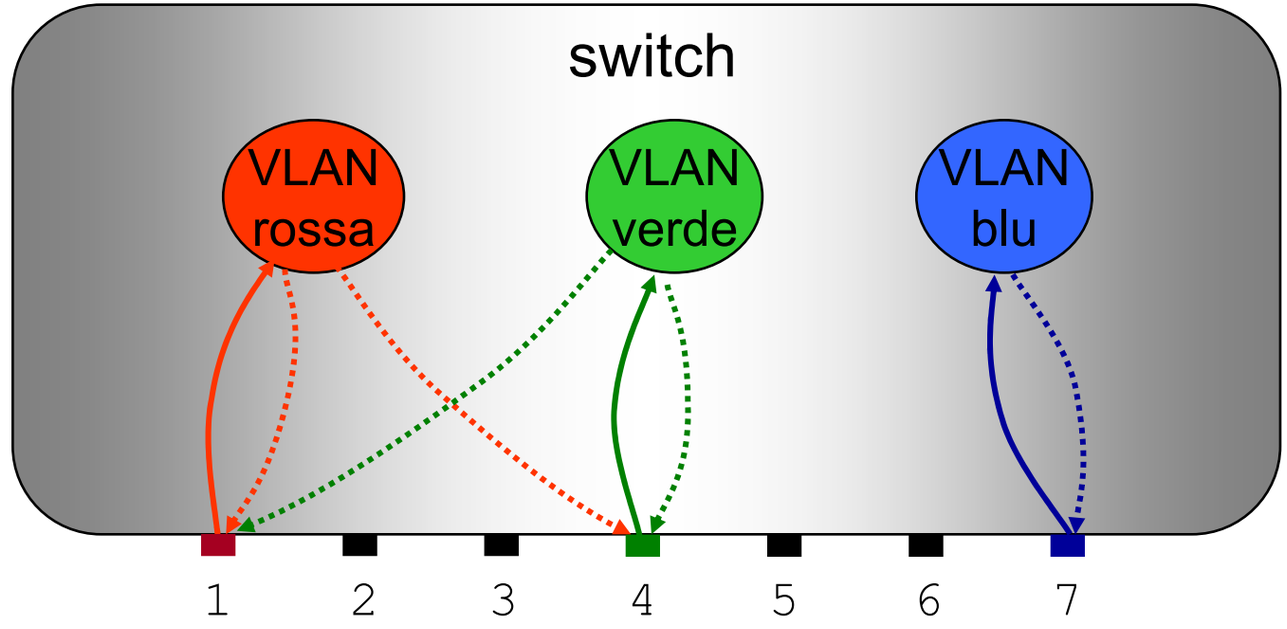
VLAN asimmetriche

- più in generale: l'insieme delle egress port di una VLAN può essere diverso da quello delle ingress port



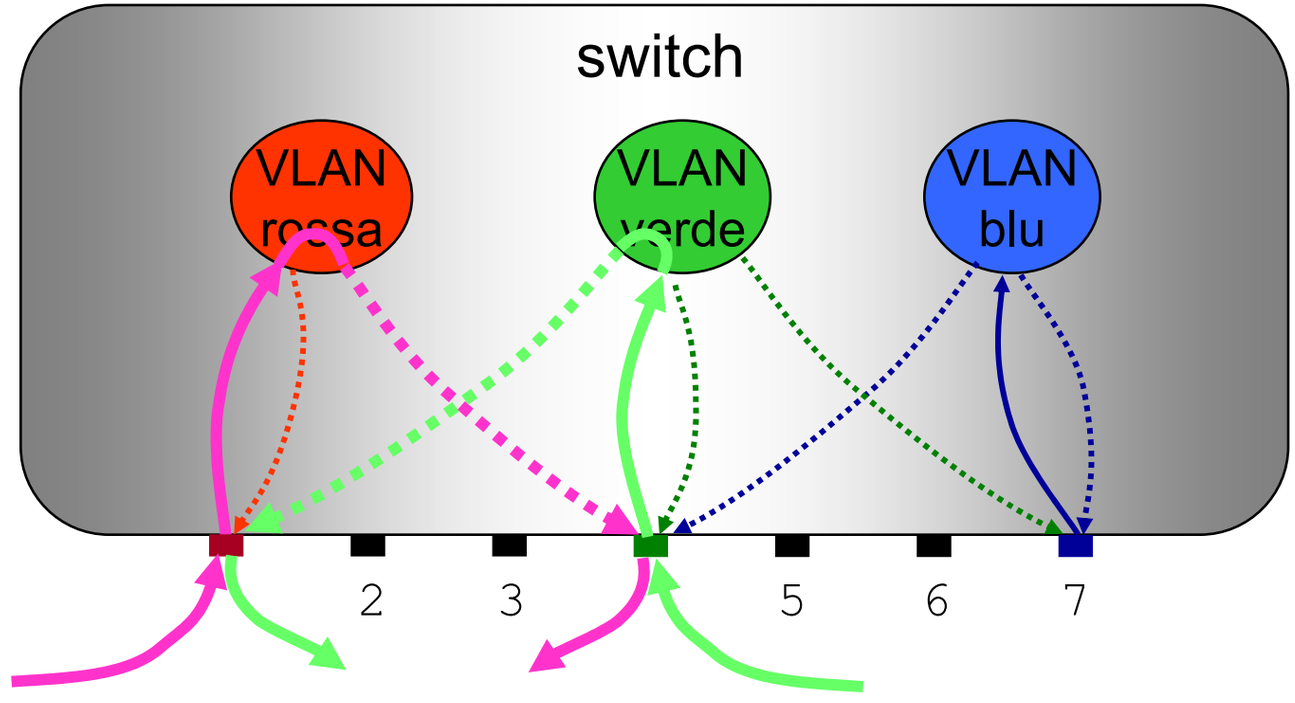
connessioni virtuali asimmetriche

- un esempio



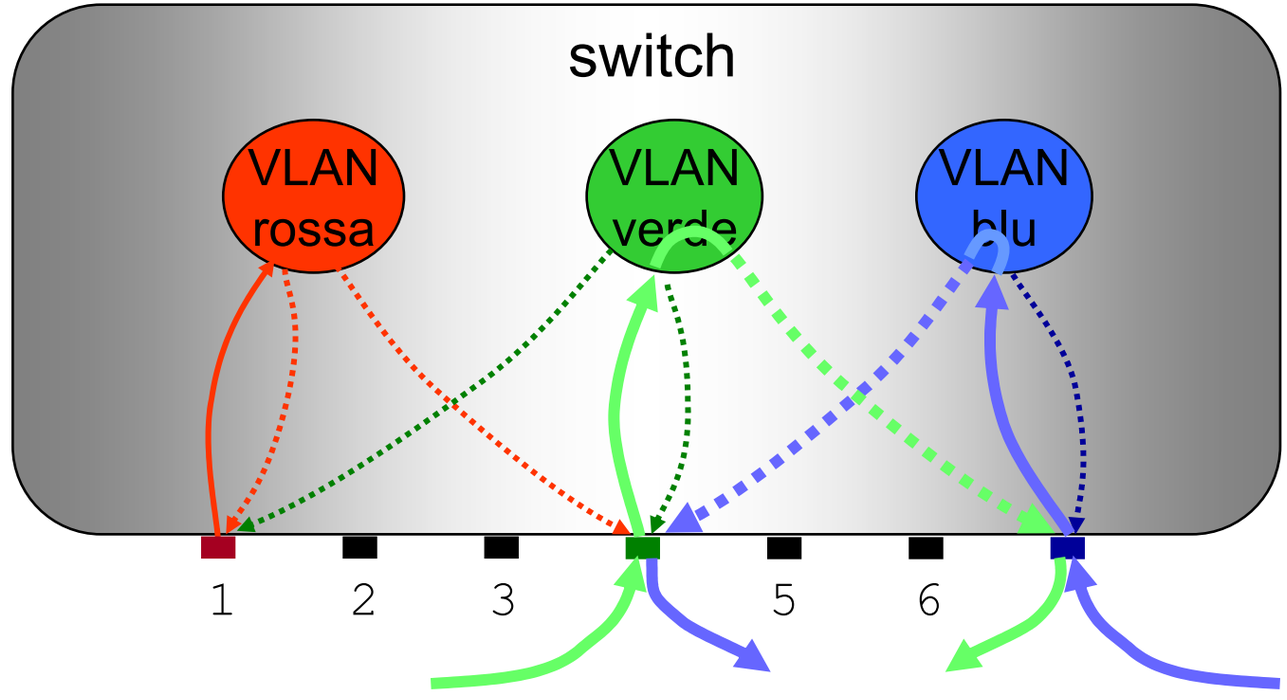
connessioni virtuali asimmetriche

- nell'esempio: un computer di una porta rossa può spedire un pacchetto ad un computer di una porta verde e viceversa



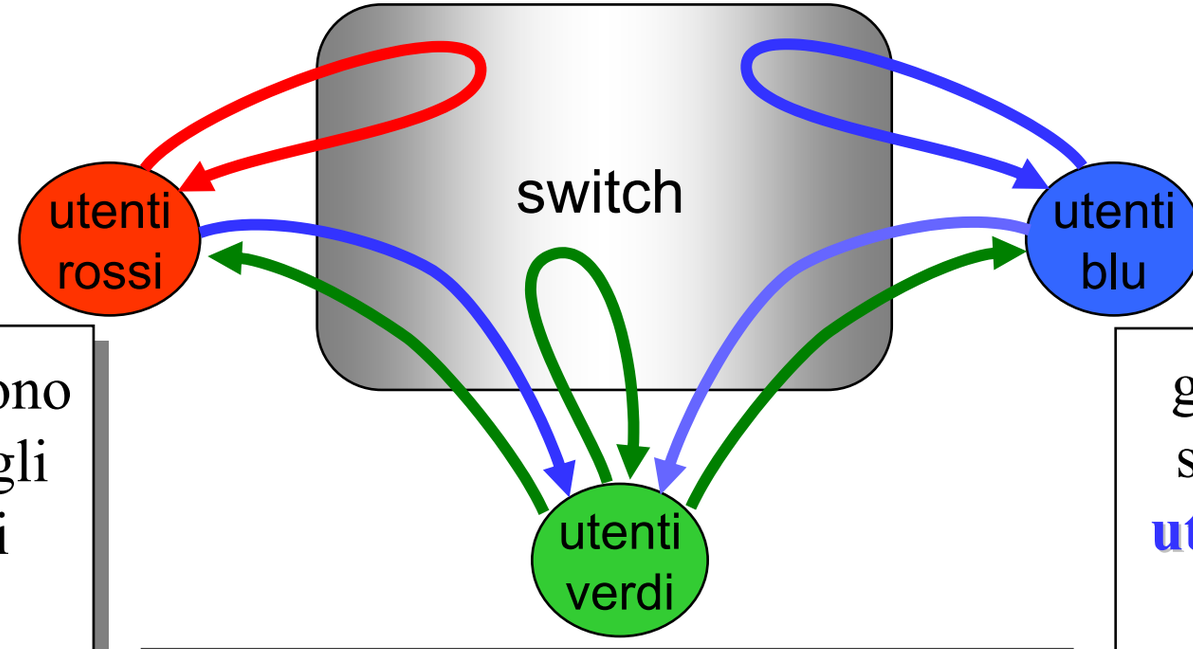
connessioni virtuali asimmetriche

- nell'esempio: un computer di una porta blu può spedire un pacchetto ad un computer di una porta verde e viceversa



connessioni virtuali asimmetriche

- situazione complessiva dell'esempio



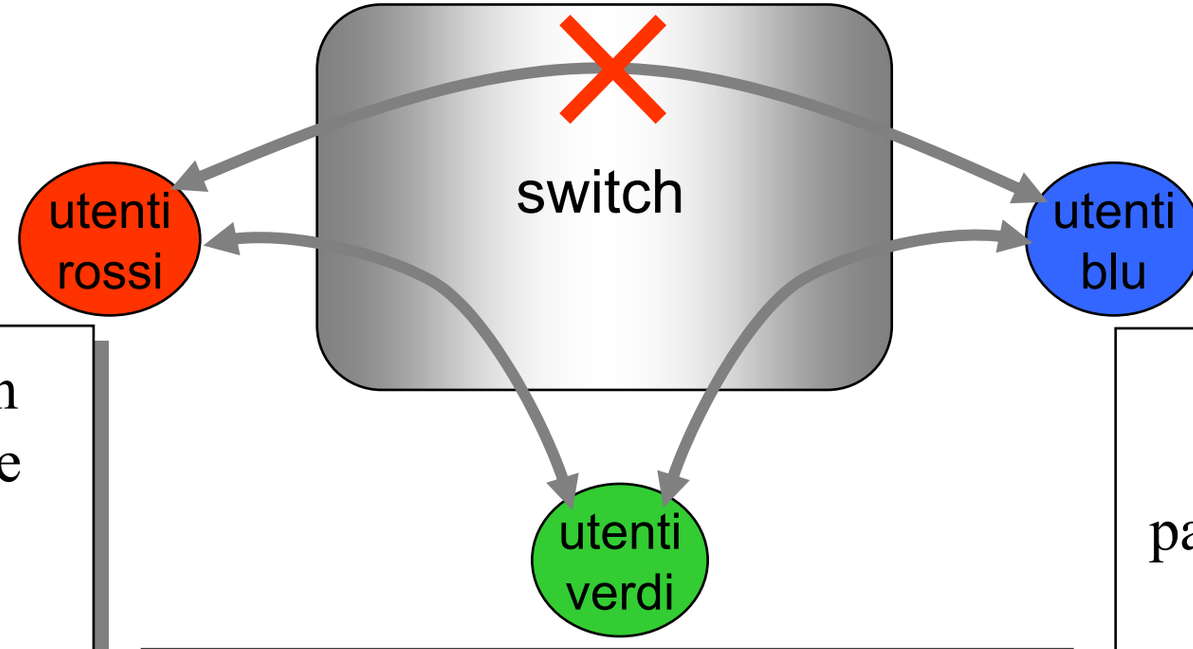
gli utenti rossi possono spedire pacchetti agli **utenti rossi** e agli **utenti verdi**

gli utenti blu possono spedire pacchetti agli **utenti blu** e agli **utenti verdi**

gli utenti verdi possono spedire pacchetti agli **utenti verdi**, **utenti rossi**, e **utenti blu**

connessioni virtuali asimmetriche

- situazione complessiva dell'esempio



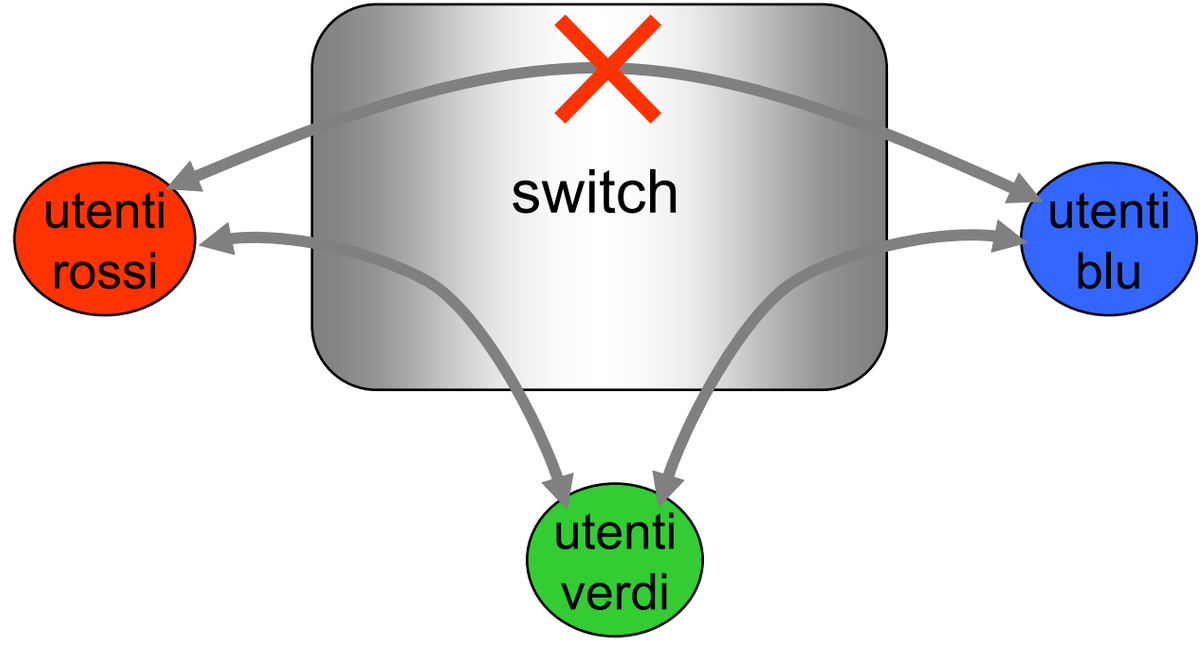
gli utenti rossi non possono scambiare pacchetti con gli **utenti blu**

gli utenti blu non possono scambiare pacchetti con gli **utenti rossi**

gli utenti verdi possono scambiare pacchetti con tutti

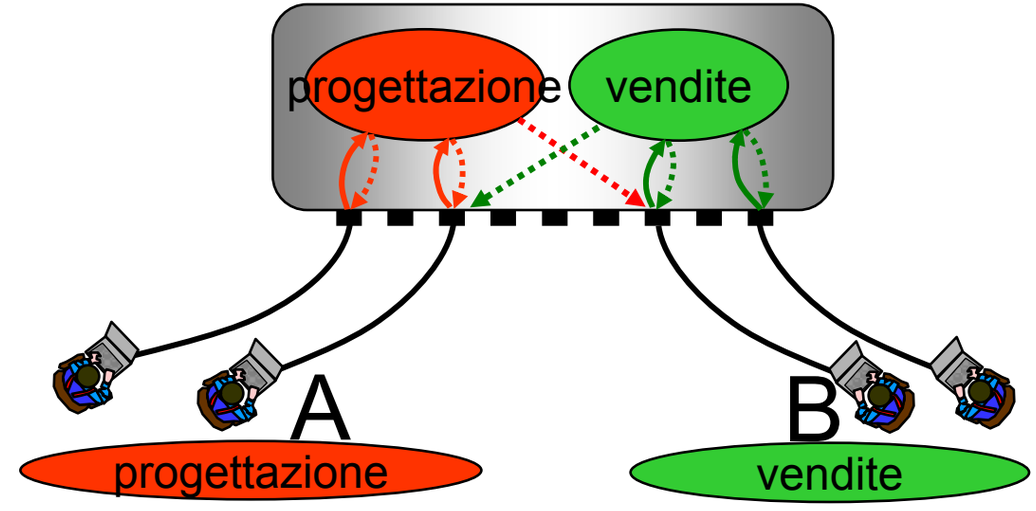
connessioni virtuali asimmetriche

- nell'esempio: la lan verde potrebbe essere quella dei server aziendali e del router; le altre lan quelle dei vari dipartimenti



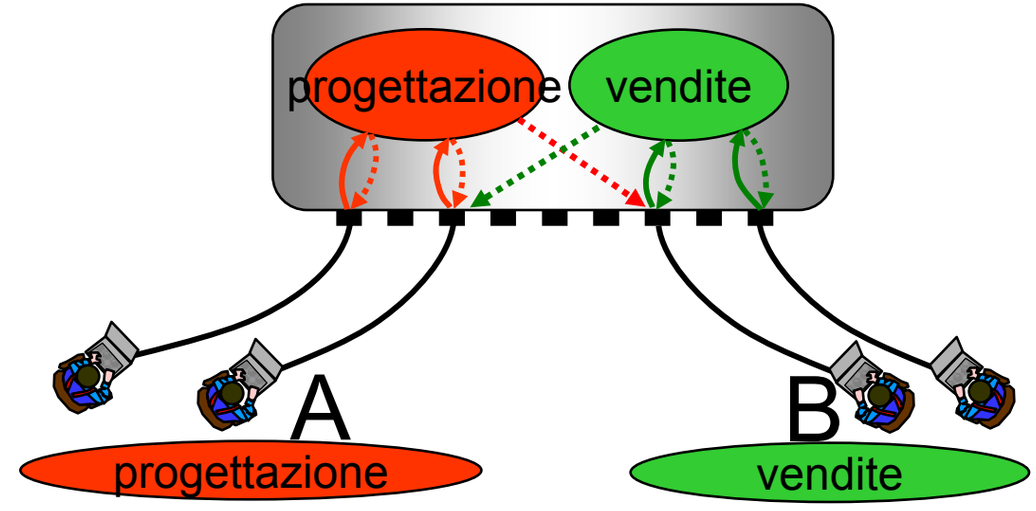
VLAN asimmetriche e filtering database

- in presenza di VLAN asimmetriche è preferibile utilizzare switch in modalità SVL
- consideriamo l'esempio qui accanto
- lo switch è configurato in modo che A ed B riescano a parlare tra loro
- quando A invia un pacchetto destinato a B, questo viene classificato come appartenente alla VLAN rossa



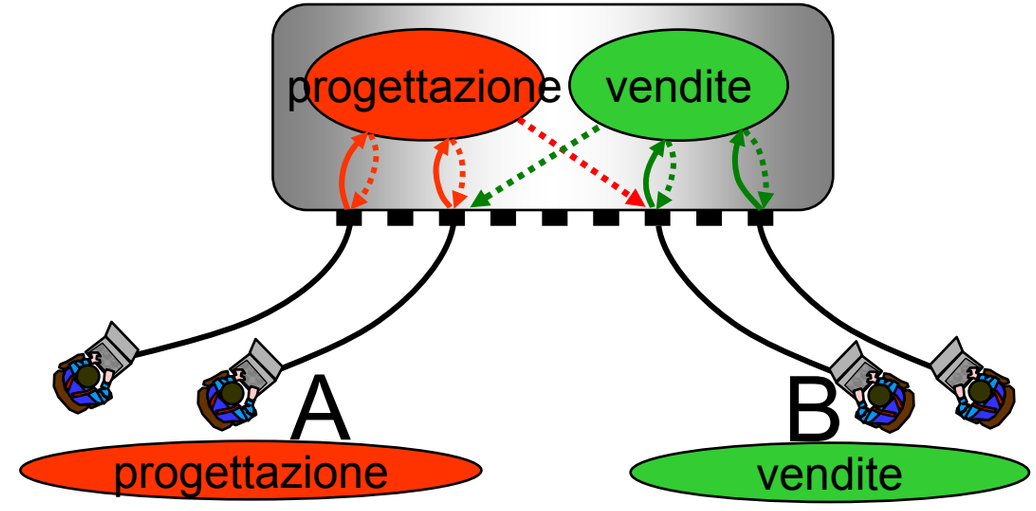
VLAN asimmetriche e filtering database

- se lo switch opera in modalità IVL, allora:
  - Il mac di B non viene trovato nel filtering database associato alla VLAN rossa e viene inviato su tutte le porte egress della VLAN rossa
  - i pacchetti arriveranno oltre che a B anche a tutte le macchine della VLAN rossa (degrado delle prestazioni)



VLAN asimmetriche e filtering database

- se lo switch invece opera in modalità SVL, allora:
  - il MAC address di B viene individuato (o meglio viene individuata la porta ad esso associata)
  - i pacchetti vengono inviati solamente a B



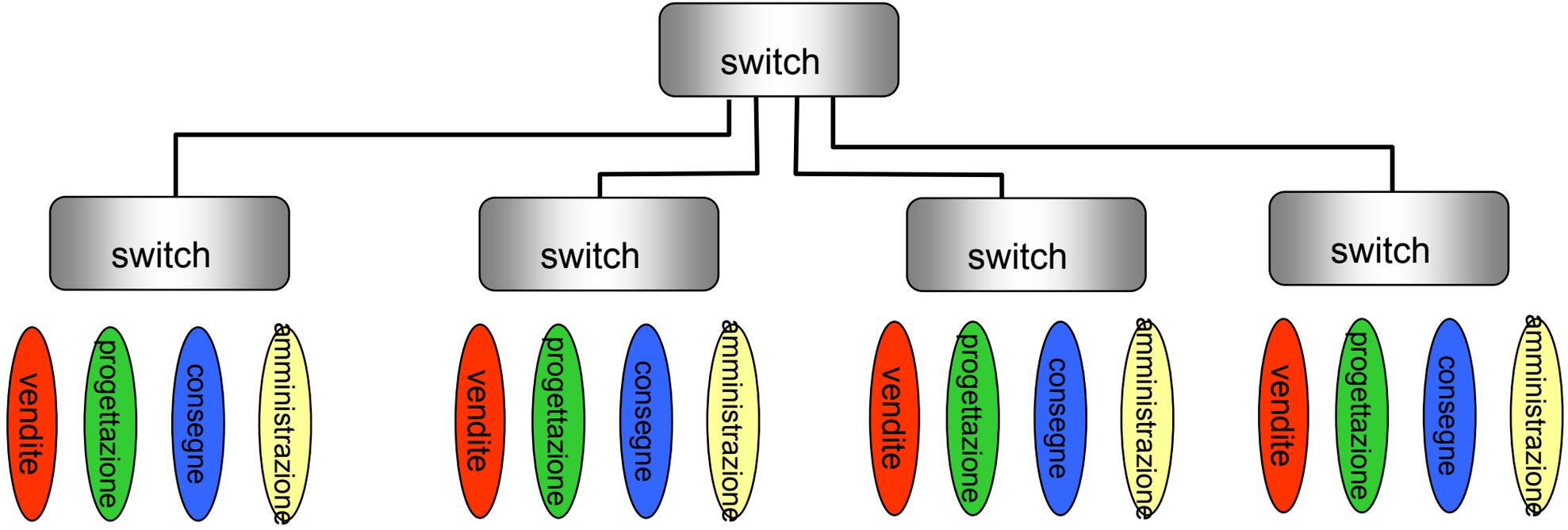
VLAN in reti con più switch

VLAN in reti con più switch

- in quanto detto finora abbiamo fatto riferimento ad una LAN con un unico switch
- in realtà le LAN sono composte quasi sempre da più switch
- è fondamentale poter definire le VLAN anche in questo caso più complesso
  - per realizzare un insieme di LAN logiche “sopra” una infrastruttura LAN fisica

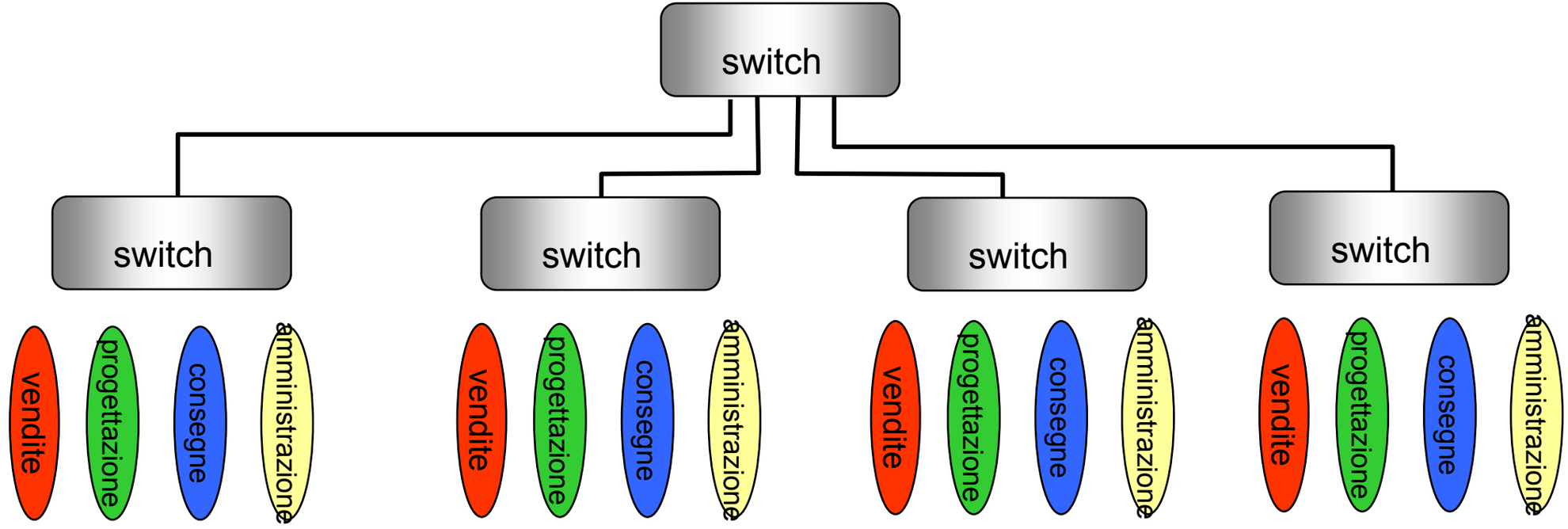
VLAN in reti con più switch

- come realizzare le VLAN in presenza di più switch?



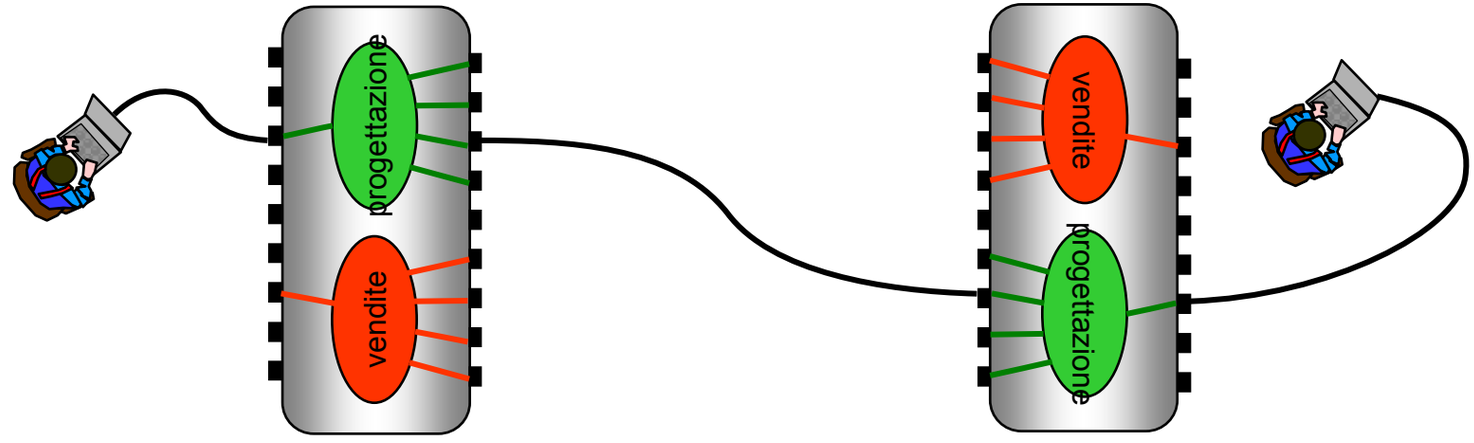
VLAN in reti con più switch

- in questo esempio potrebbe essere utile avere 4 VLAN: vendite, progettazione, consegne, amministrazione



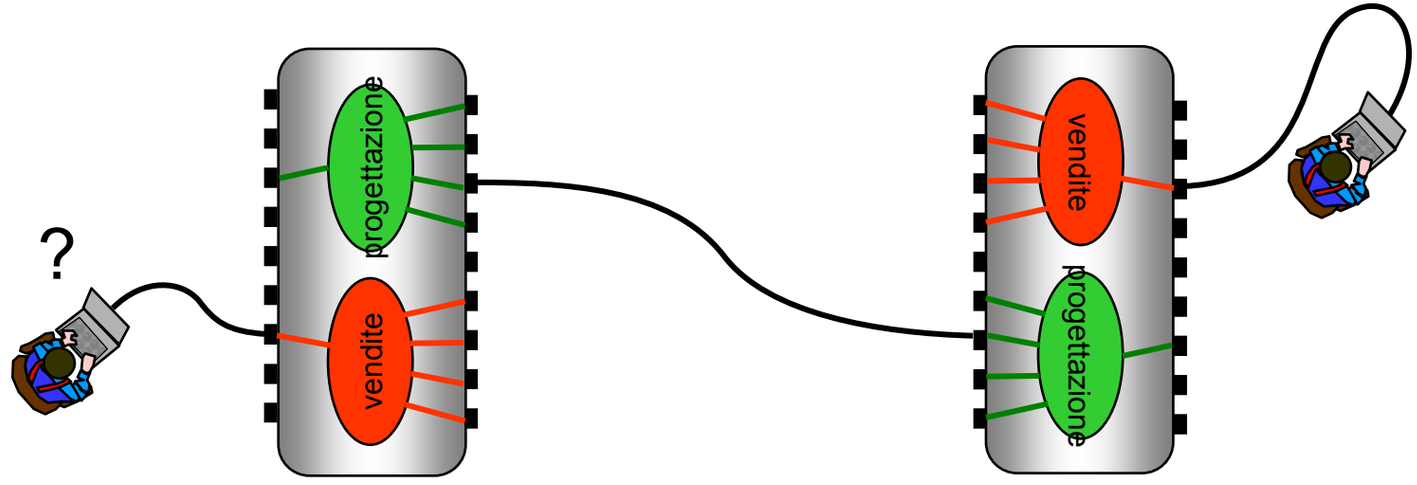
una possibile soluzione?

- caso di 2 switch: connettere due porte verdi dei due switch
  - problema: questa soluzione interconnette una sola VLAN



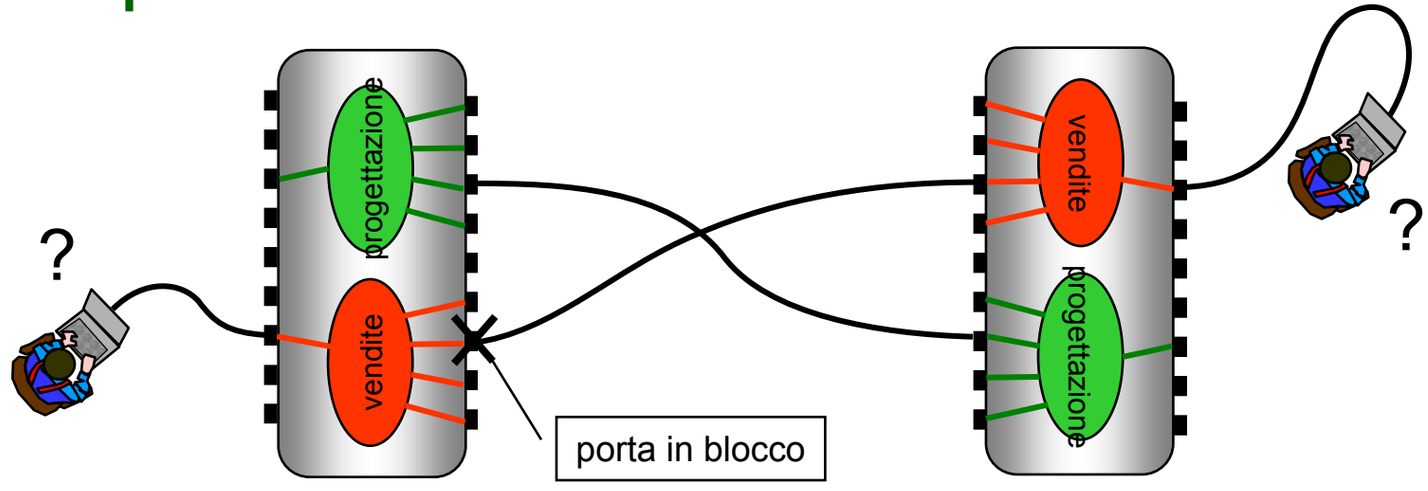
una possibile soluzione?

- caso di 2 switch: connettere due porte verdi dei due switch
  - problema: le due VLAN del dipartimento vendite, create sui due switch, rimangono non connesse



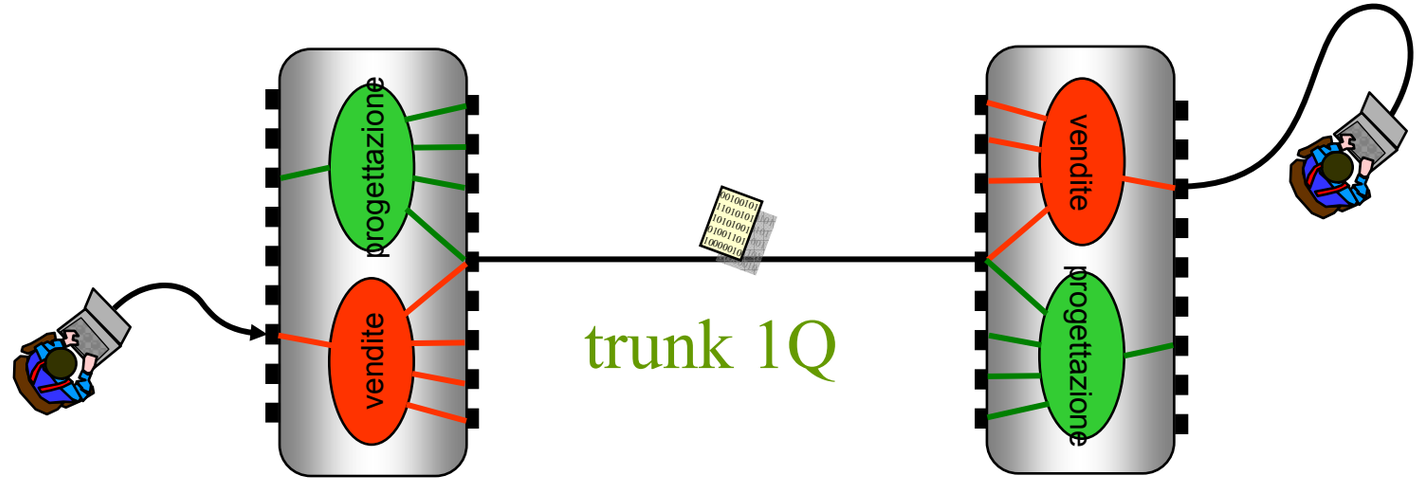
interconnessione doppia?

- attenzione: interconnettere entrambe le VLAN origina un ciclo
  - per risolvere il problema l'algoritmo per il calcolo dello spanning tree (IEEE 802.1D) blocca una delle quattro porte



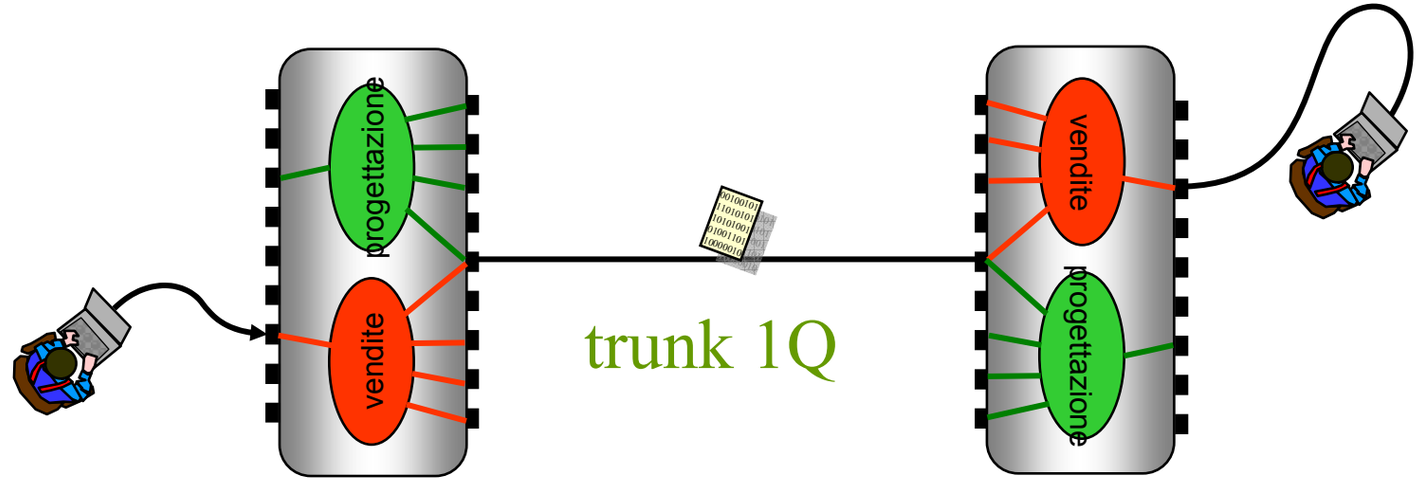
trunk IEEE 802.1Q

- lo standard prevede che un link tra 2 switch possa essere dichiarato *trunk 1Q*
- in un trunk 1Q possono transitare pacchetti di varie VLAN



trunk IEEE 802.1Q

- i pacchetti che attraversano un trunk 1Q sono *tagged* (etichettati) dallo switch trasmittente con l'identificatore della VLAN a cui appartengono
- il *tag* (etichetta) è un campo addizionale della pdu di livello 2



trunk IEEE 802.1Q

- lo switch che riceve da un trunk 1Q un pacchetto tagged lo attribuisce alla VLAN a cui appartiene
- il tag viene rimosso dallo switch e non arriverà agli utenti
- una porta trunk 1Q partecipa per default a tutte le VLAN come egress port

una semantica per i trunk 1Q

- quando una porta è indicata come egress port per una VLAN si può specificare se i pacchetti in uscita devono essere tagged come appartenenti alla VLAN
- quando una porta riceve un pacchetto
  - se è tagged con una VLAN viene attribuito a quella VLAN
  - se non è tagged viene attribuito ad una VLAN secondo le regole definite per quella porta
- è tipicamente possibile configurare una porta in modo tale che i pacchetti in ingresso non tagged (o quelli tagged) siano scartati

una semantica per i trunk 1Q

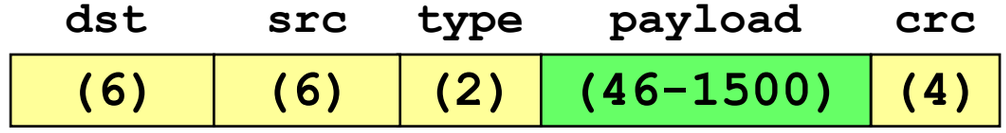
- coerentemente con le definizioni precedenti una porta può essere:
  - access
    - riceve ed invia solo pacchetti non tagged
  - trunk
    - riceve ed invia solo pacchetti tagged
  - ibrida
    - riceve e/o invia pacchetti tagged e/o non tagged

tag IEEE 802.1Q

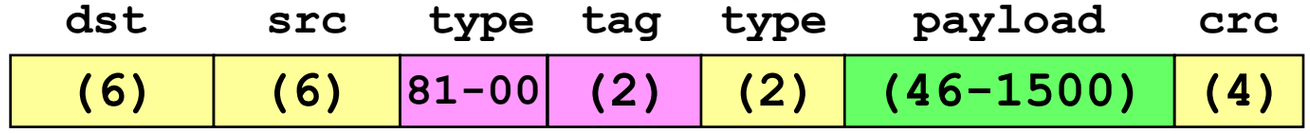
- la specifica si trova nello standard IEEE 802.3ac
- il campo di 2 byte length/type (IEEE 802.3/ethernet 2.0) assume il valore 81-00
- è seguito da 2 byte di tag
  - contiene anche informazioni di priorità IEEE 802.1p
- quindi segue un altro campo length/type usato in modo tradizionale
- conseguenza: il maximum packet size passa da 1518 byte a 1522 byte

tag IEEE 802.1Q

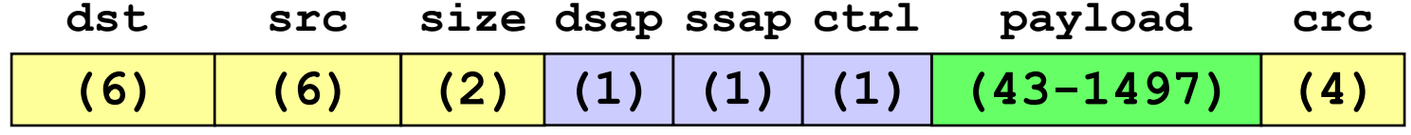
pacchetto ethernet 2.0



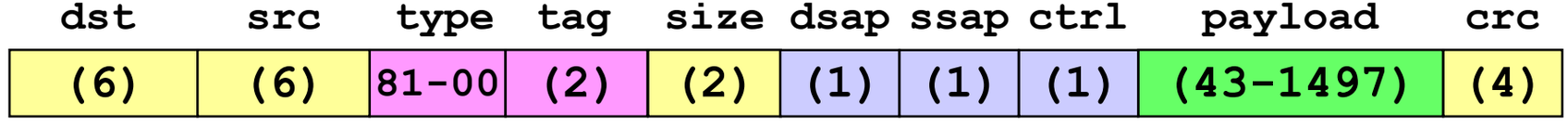
pacchetto ethernet 2.0 (con tag 802.3ac)



pacchetto IEEE 802.3 + IEEE 802.2



pacchetto IEEE 802.3 + IEEE 802.2 (con tag 802.3ac)



tag IEEE 802.1Q

- lo standard IEEE 802.1ad ha introdotto l'idea di *double tagging*
  - nel pacchetto si possono usare due tag consecutive
- molto usato dagli Internet Service Provider
  - è possibile sovrapporre tag associate ai customer (C-TAG) a tag associate al servizio (S-TAG)

esempio: la LAN di un edificio