

VLAN

Mario Baldi

Politecnico di Torino
www.polito.it/~baldi

Pietro Nicoletti

Studio Reti
www.studioreti.it

Basato sul capitolo 5 di:

M. Baldi, P. Nicoletti, "Switched LAN", McGraw-Hill, 2002, ISBN 88-386-3426-2

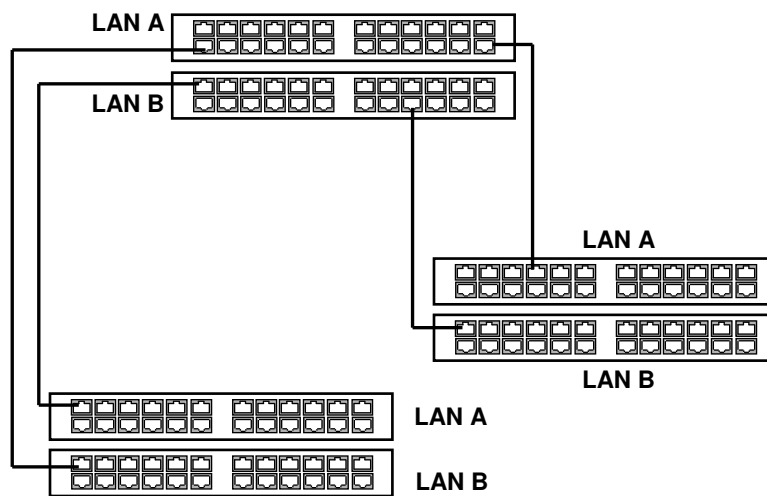
Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

Reti parallele indipendenti

- Esigenza di avere delle reti separate, per ragione di riservatezza o sicurezza, che si sviluppano per un intero edificio o comprensorio
 - nReti = nMezzi-trasmissivi + nApparati-di-rete per ogni punto di distribuzione
 - spreco di risorse
 - separazione massima

Esempio di reti parallele



LAN virtuali (VLAN)

- Le LAN estese, quando crescono troppo di dimensione, sono fonte di problemi
 - elevato traffico di multicast/broadcast
 - necessità di fare routing tra le sottoreti IP
 - problemi legati alla sicurezza
- Grazie al concetto di LAN virtuali
 - si evita di dover realizzare reti parallele
 - si può avere un'unica infrastruttura fisica
 - si possono definire più sottoreti logiche separate
- Le LAN virtuali possono coprire
 - un singolo switch
 - l'intera LAN estesa

Impiego delle VLAN

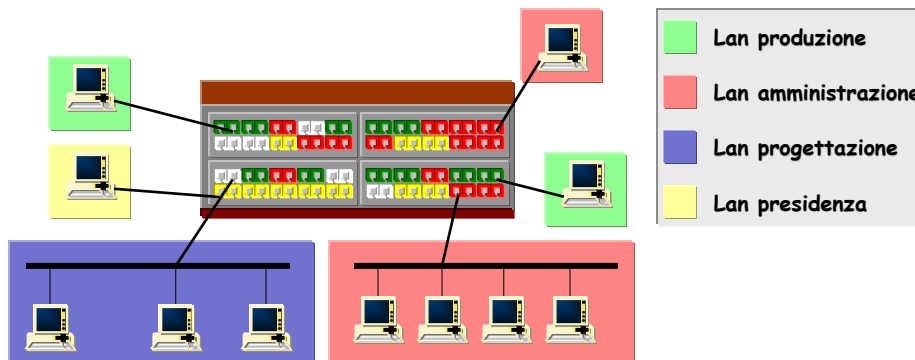
- Per ragioni di sicurezza
 - si possono mantenere completamente separate le reti tramite l'impiego delle VLAN
 - non c'è comunicazione tra le VLAN (separazione totale!)
 - si possono connettere le VLAN in modo più o meno sicuro tramite Access-List su router, Layer 3 Switch o Firewall
- Per risolvere conflitti di competenze tra enti diversi di una grande organizzazione
 - le VLAN vengono connesse tramite router, Layer 3 Switch
- Per limitare il traffico di broadcast
 - le VLAN vengono connesse tramite router, Layer 3 Switch

VLAN Intra-Switch e Inter-Switch

- Le prime soluzioni di VLAN di tipo Intra-Switch erano molto semplici ed erano applicabili solo in una rete costituita da Switch a centro stella e Hub in periferia
 - raggruppamento di porte dello switch in diversi domini di broadcast
- Oggi gli standard e i prodotti del mercato offrono soluzioni VLAN Inter-Switch applicabili sia a reti Full-Switched, sia a reti di tipo Segment-Switching

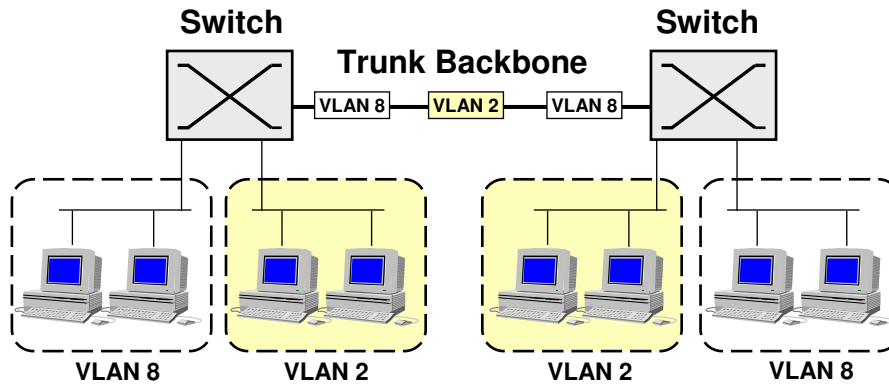
VLAN Intra-Switch

- Si possono raggruppare due o più porte dello switch in un dominio di broadcast



VLAN Inter-Switch

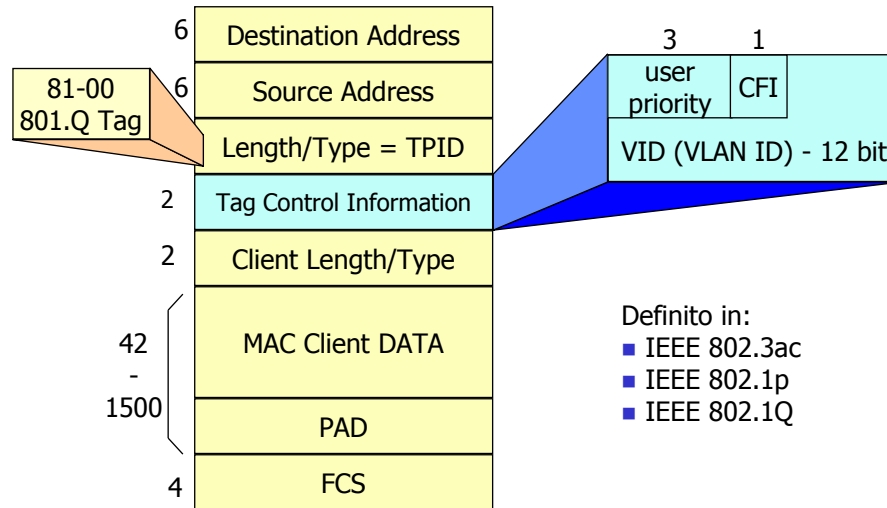
- Si creano delle LAN differenti sullo stesso mezzo trasmissivo in modo virtuale
 - occorre distinguere quali pacchetti sono destinati a quali VLAN



VLAN: marcatura dei pacchetti

- Frame Tagging
 - si utilizza la tecnica di incapsulamento
 - il pacchetto Ethernet, Token Ring o FDDI viene incapsulato in un pacchetto proprietario
 - soluzione Cisco con ISL
- Packet Tagging
 - si inserisce un header aggiuntivo (VLAN-ID) nella busta MAC; metodo previsto da 802.1Q

Codifica del tag: IEEE 802.1Q



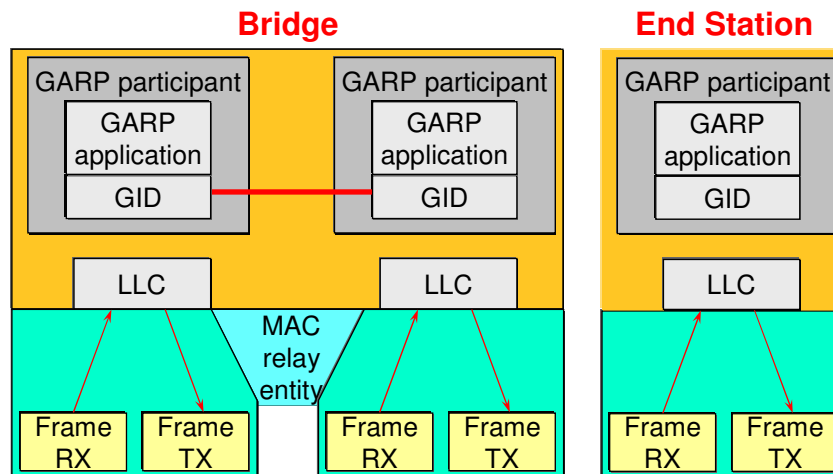
VLAN: gli standard coinvolti

- Lo standard IEEE 802.1Q, che definisce le funzioni e le specifiche inerenti le VLAN coinvolge altri standard IEEE:
 - 802.3ac per la definizione del nuovo formato di pacchetto Ethernet che richiede l'inserimento del campo TAG dove inserire l'informazione VLAN ID
 - 802.1p per due ragioni:
 - il campo TAG può contenere sia l'informazione di priorità associabile al pacchetto (problematica affrontata da 802.1p), sia il VLAN ID
 - il protocollo GVRP che serve per annunciare gli attributi inerenti le VLAN agli switch adiacenti si basa sulle specifiche più generiche contenute nel protocollo GARP definite in 802.1p
 - GARP = Generic Attribution Registration Protocol
 - GVRP = GARP VLAN Registration Protocol

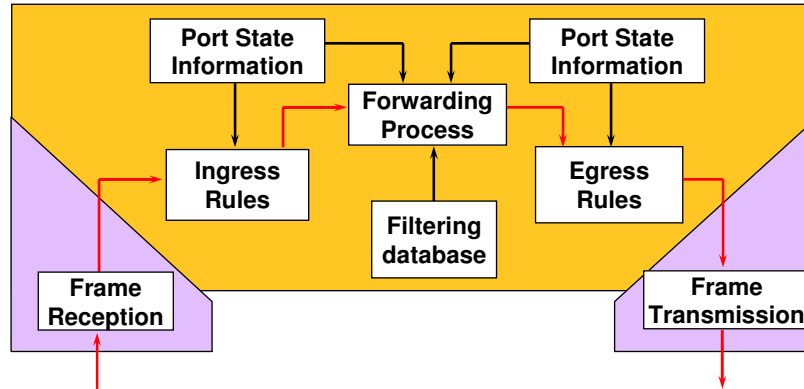
GARP: generalità

- Registra o cancella attributi di vario tipo in un entità interna all'apparato denominata **GID**
 - Il **GID** (GARP Information Distribution) è un insieme di macchine a stati che definisce lo stato corrente delle registrazioni e dichiarazioni per tutti i valori degli attributi
 - la registrazione o cancellazione di un attributo ha luogo soltanto sulla porta che riceve la GARP PDU contenente la dichiarazione
 - ra registrazione può aver luogo anche sulle porte che sono state poste in Blocking state dallo STP
- **GIP** (GARP Information Propagation)
 - Entità responsabile della propagazione delle informazioni tra i GARP Participant
 - internamente ad un singolo bridge
 - tra bridge diversi (basato su LLC di tipo 1)

GARP: entità e architettura



Funzione di inoltro del bridge 802.1Q

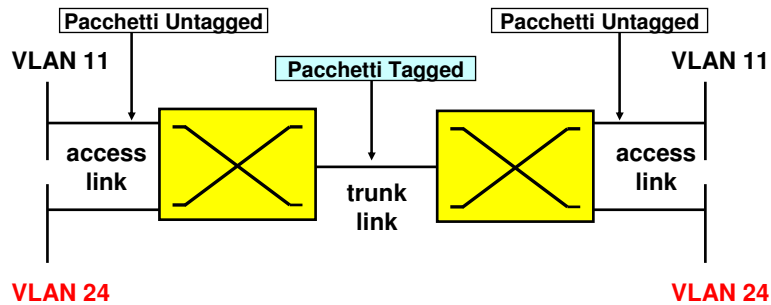


Caratteristiche di 802.1Q

- L'assegnazione di VLAN è per porta
 - prevede l'utilizzo di criteri diversi per l'assegnazione di VLAN ad una porta
- Prevede un unico spanning tree
- Prevede filtering database multipli identificati con il FID (Filtering Identifier)
 - il FID è assegnato dal bridge per identificare un set di VID (Virtual Lan Identifier)
 - può esistere una sola entry per ogni indirizzo MAC nel filtering database
 - un indirizzo MAC può essere presente in diversi filtering database

Port-based VLAN

- Viene assegnata una VLAN per porta
 - la porta può essere definita come access o trunk port



Tipi di apparati e di Link

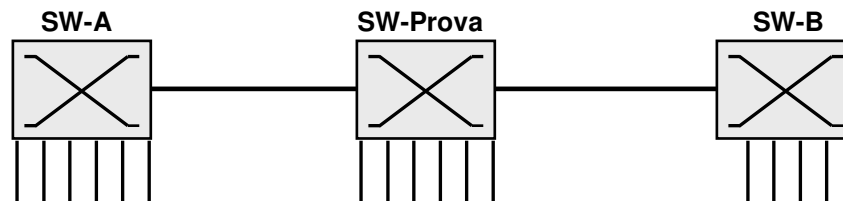
- Tipi di apparati:
 - VLAN-Aware trattano i pacchetti di tipo tagged e untagged e sono conformi a 802.1Q
 - VLAN-Unaware non trattano i pacchetti di tipo tagged
- Access link:
 - su porte che ricevono e trasmettono pacchetti Untagged impiegate per la connessione di interfacce di rete tradizionali (caso più comune e condizione di default sugli switch)
- Trunk link:
 - su porte che ricevono e trasmettono pacchetti Tagged impiegate per la connessione tra gli switch o tra switch e interfacce di rete che lavorano in modalità trunk 802.1Q

Configurazione di VLAN sugli switch

- Si può riassumere in tre fasi:
 - creazione delle VLAN necessarie su ogni switch;
 - associazione di porte a VLAN;
 - definizione delle porte Trunk
 - il default sugli switch è lo stato di Access

Esempio di configurazione VLAN

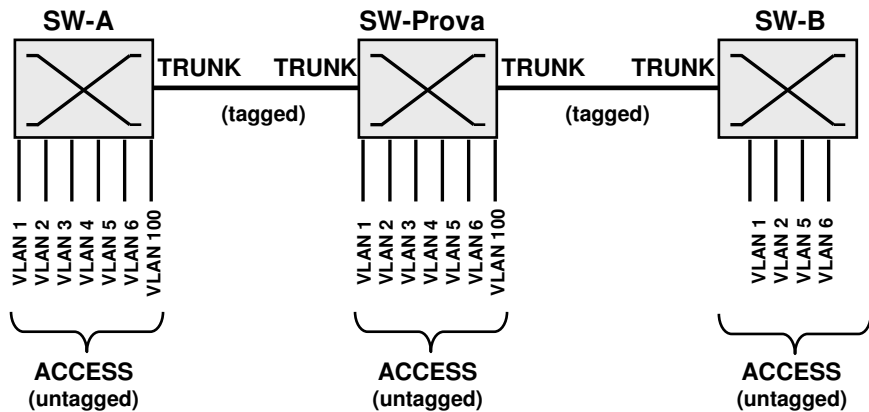
- Rete prima della configurazione delle VLAN



Stato delle porte prima della configurazione delle VLAN

```
SW-Prova#sho vlan brief
VLAN Name      Status      Ports
-----
1    default    active     Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                    Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                    Fa0/9, Fa0/10, Fa0/11, Fa0/12,
                    Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                    Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                    Fa0/21, Fa0/22, Fa0/23, Fa0/24,
                    Fa0/25, Fa0/26, Fa0/27, Fa0/28,
                    Fa0/29, Fa0/30, Fa0/31, Fa0/32,
                    Fa0/33, Fa0/34, Fa0/35, Fa0/36,
                    Fa0/37, Fa0/38, Fa0/39, Fa0/40,
                    Fa0/41, Fa0/42, Fa0/43, Fa0/44,
                    Fa0/45, Fa0/46, Fa0/47, Fa0/48,
                    Gi0/1, Gi0/2
```

VLAN che si vogliono creare



Creazione delle VLAN

```

SW-Prova#vlan database
Switch(vlan)#vlan 2 name Amministrazione
VLAN 2 added:
  Name: Amministrazione
Switch(vlan)#vlan 3 name Vendite
VLAN 3 added:
  Name: Vendite
Switch(vlan)#vlan 4 name prova-1
VLAN 4 added:
  Name: prova-1
Switch(vlan)#vlan 5 name prova-2
VLAN 5 added:
  Name: prova-2
Switch(vlan)#vlan 6 name prova-3
VLAN 6 added:
  Name: prova-3
Switch(vlan)#vlan 100 name Produzione
VLAN 100 added:
  Name: Produzione
SW-Prova(vlan)#exit
APPLY completed.
Exiting....
SW-Prova#

```

Associazione di porte a VLAN

```

SW-Prova(config)#int fastEthernet 0/12
SW-Prova(config-if)#switchport access vlan 100
Switch(config-if)#exit
.....
SW-Prova(config)#int fastEthernet 0/16
SW-Prova(config-if)#switchport access vlan 2
SW-Prova(config-if)#exit
.....
SW-Prova(config)#int fastEthernet 0/20
SW-Prova(config-if)#switchport access vlan 3
SW-Prova(config-if)#exit
.....
SW-Prova(config)#int fastEthernet 0/24
SW-Prova(config-if)#switchport access vlan 4
SW-Prova(config-if)#exit
.....
SW-Prova(config)#int fastEthernet 0/28
SW-Prova(config-if)#switchport access vlan 5
SW-Prova(config-if)#exit
.....
SW-Prova(config)#int fastEthernet 0/32
SW-Prova(config-if)#switchport access vlan 6
SW-Prova(config-if)#exit

```

Porte e VLAN sullo switch dopo la configurazione

```
SW-Prova#show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/36,
                                   Fa0/37, Fa0/38, Fa0/39, Fa0/40,
                                   Fa0/41, Fa0/42, Fa0/43, Fa0/44,
                                   Fa0/45, Fa0/46, Fa0/47, Fa0/48,
                                   Gi0/1, Gi0/2
2    Amministrazione        active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
3    Vendite                 active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
4    prova-1                 active    Fa0/24, Fa0/25, Fa0/26, Fa0/27
5    prova-2                 active    Fa0/28, Fa0/29, Fa0/30, Fa0/31
6    prova-3                 active    Fa0/32, Fa0/33, Fa0/34, Fa0/35
100  Produzione              active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
```

Definizione delle porte trunk

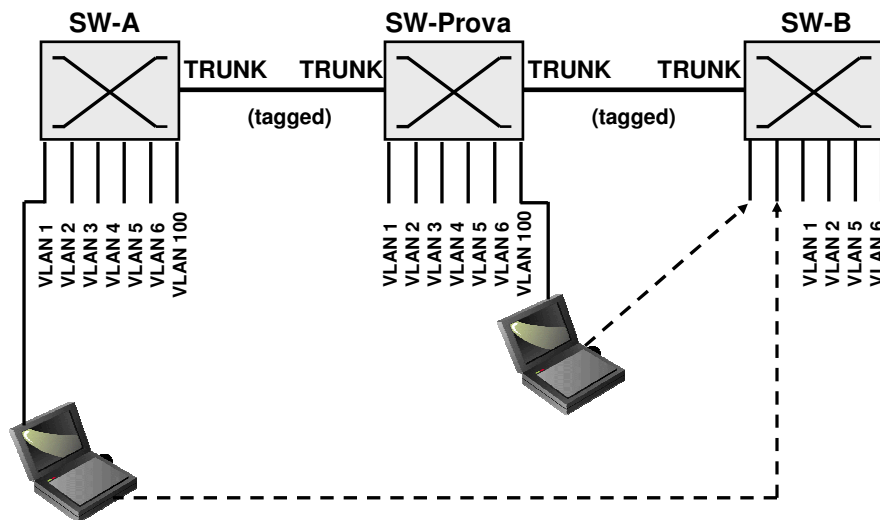
- Abilitazione statica di VLAN su porte trunk senza l'impiego di protocollo GVRP

```
SW-Prova(config)#interface GigabitEthernet 0/1
SW-Prova(config-if)#switchport mode trunk
SW-Prova(config-if)#switchport trunk allowed vlan add 1,2,5,6
SW-Prova(config-if)#exit
SW-Prova(config)#interface GigabitEthernet 0/2
SW-Prova(config-if)#switchport mode trunk
SW-Prova(config-if)#switchport trunk allowed vlan all
```

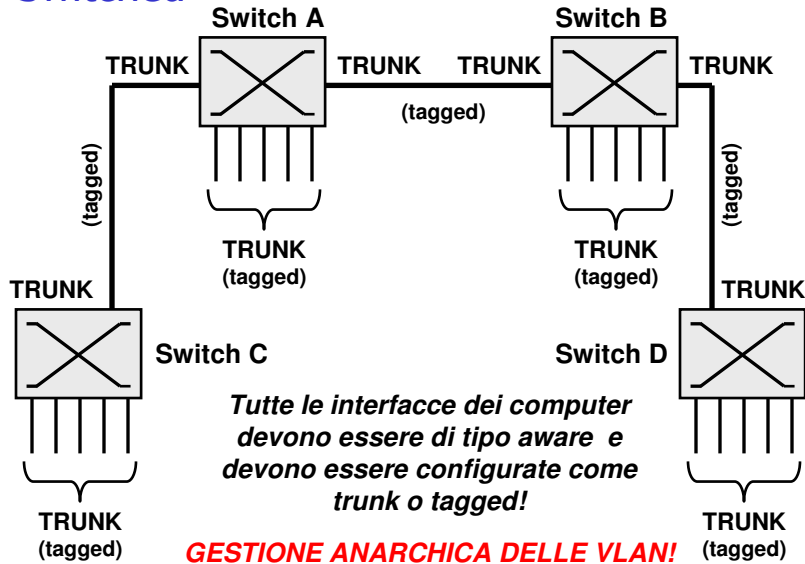
Il problema della mobilità

- L'assegnazione VLAN per porta su porte di tipo Access non permette la mobilità
 - ad utente connesso su una particolare porta di uno switch è assegnata una certa VLAN, se si lo sposta su un'altra porta o switch, non la mantiene automaticamente, ma è necessario l'intervento del gestore di rete
- Soluzioni possibili
 - gestione anarchica della rete tramite l'impiego di interfacce di rete che supportano l'imbustamento 802.1Q e vengono configurate come *Trunk*
 - applicabile su reti shared (basata solo su HUB) e switched
 - l'utente può definire l'appartenenza della propria macchina macchina ad una particolare VLAN
 - gestione mista con impiego di porte Access (elevato numero) e Trunk (poche) per connettere le stazioni

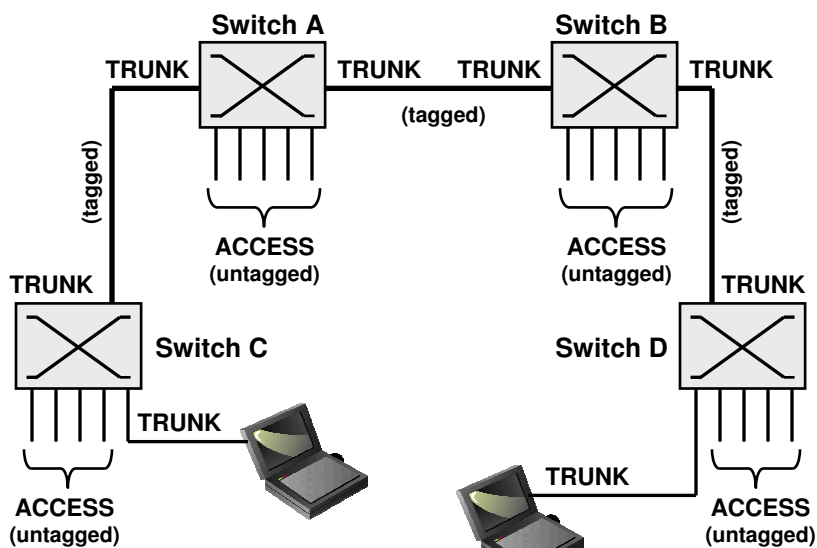
Esempio di mobilità degli utenti



Gestione anarchica delle VLAN su rete Switched

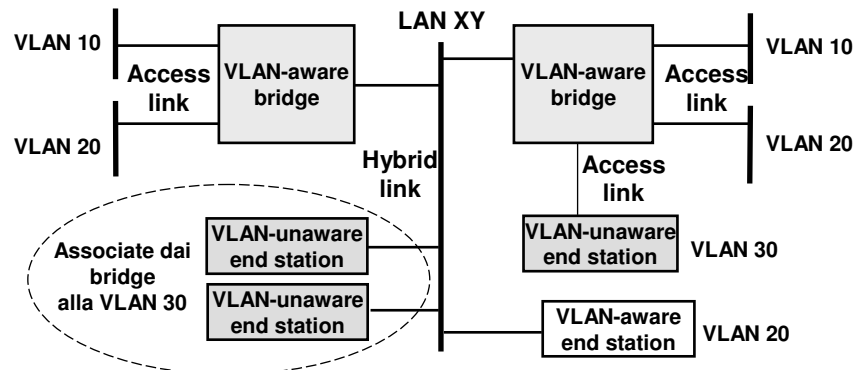


Gestione mista con porte Access e Trunk



Hybrid Link

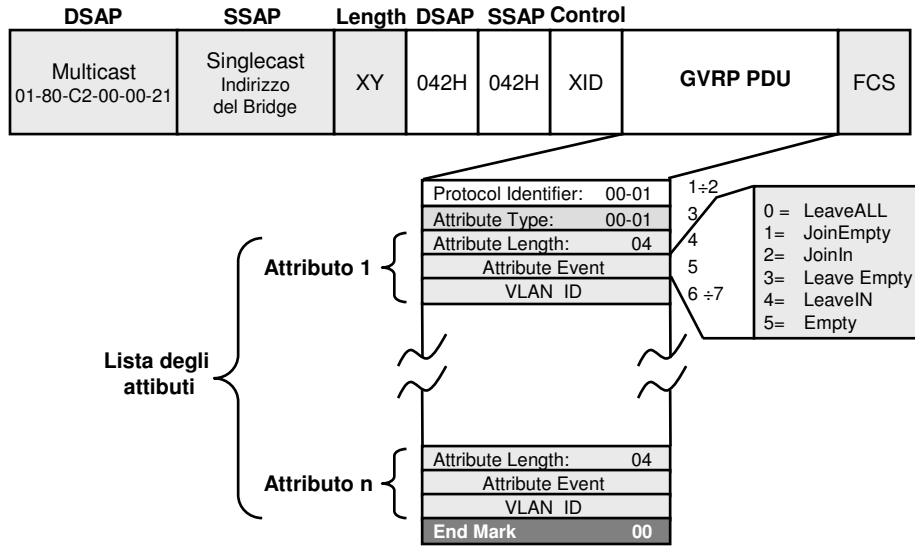
- Su questa connessione possono transitare pacchetti tagged e untagged



Il protocollo GVRP

- GARP VLAN Registration Protocol
 - serve per registrare o cancellare attributi riguardanti le VLAN
 - uno switch sulla base della presenza di determinate VLAN sullo switch adiacente, comunicategli da questo tramite il protocollo GVRP, può stabilire quali pacchetti convogliare sulla porta trunk
 - alternativa alla definizione statica delle VLAN da trasportare sui *Trunk Link*
 - gli switch che adottano il protocollo GVRP sono considerati GVRP-Aware

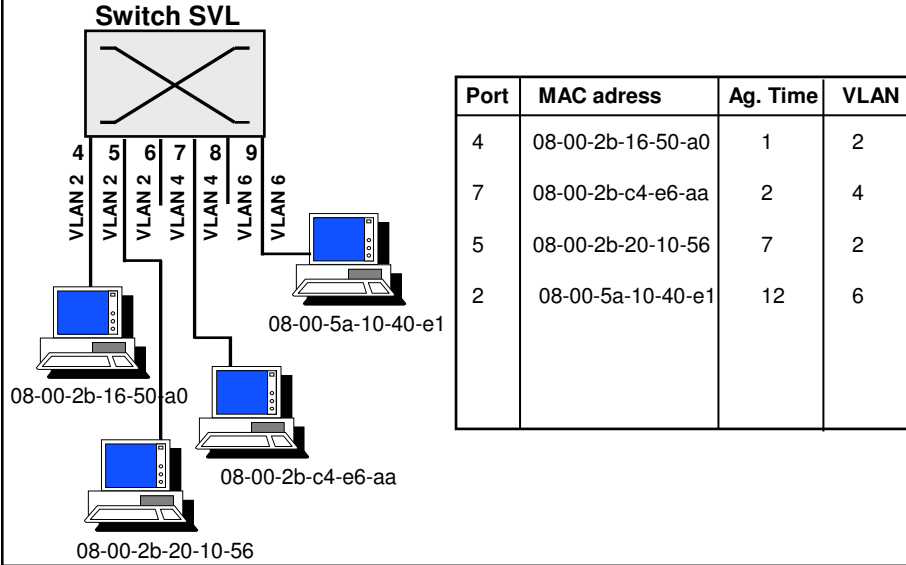
Il formato del pacchetto GVRP



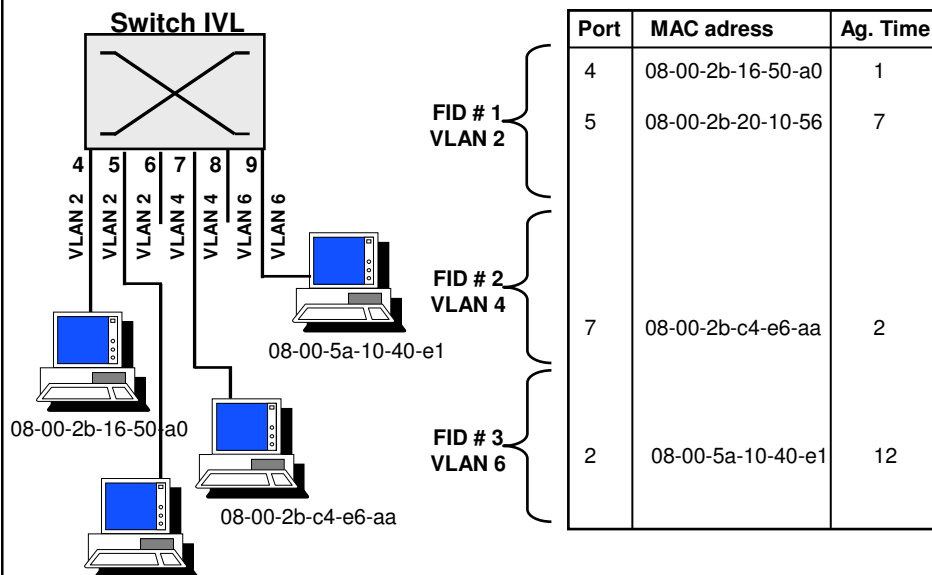
Bridge/Switch di tipo SVL e IVL

- Bridge SVL (*Shared VLAN*):
 - dispone di un'unica tabella d'inoltro (filtering database) che viene condivisa da tutte le VLAN
- Bridge IVL (*Independent VLAN*):
 - si crea una tabella di inoltro, identificata con un parametro denominato FID (Filtering Identifier), per ogni VLAN creata

Bridge/Switch di tipo SVL



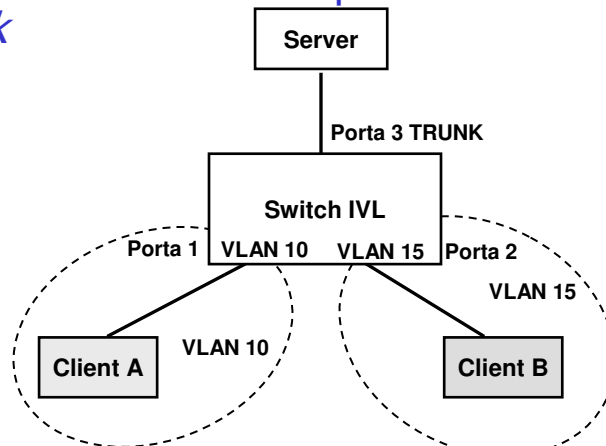
Bridge/Switch di tipo IVL



La condivisione di più VLAN da parte di un apparato di rete

- Condivisione su Switch di tipo IVL:
 - se sull'apparato (esempio un server) si dispone di un'interfaccia di rete che supporta il trunk 802.1q (VLAN-Aware)
 - si configurano l'interfaccia di rete e la porta dello switch in modalità Trunk
 - se l'interfaccia di rete non è di tipo VLAN-Aware nbel caso Cisco è possibile collegarla ad una porta dello switch che viene configurata di tipo *Multi VLAN*.
- Condivisione su Switch di tipo SVL:
 - interfaccia di rete di tipo Access sull'apparato che deve condividere più VLAN
 - necessita di una configurazione complessa sullo Switch in cui vengono associate VLAN e porte fisiche dello Switch

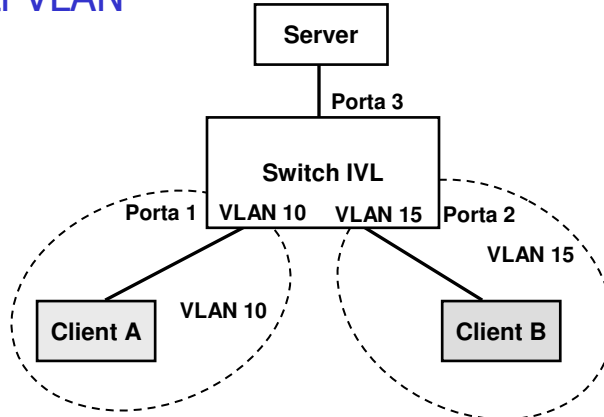
Server che condivide più VLAN su *Trunk Link*



```

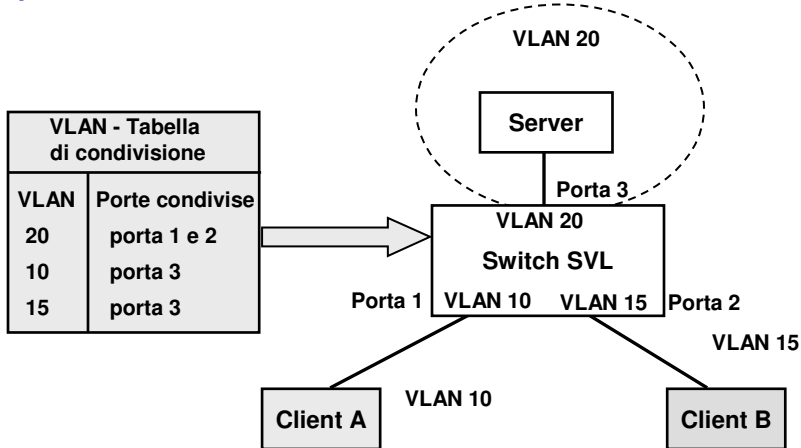
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,15
Switch(config-if)#end
    
```

Server che condivide più VLAN su porta Multi VLAN



```
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport mode multi
Switch(config-if)#switchport multi vlan add 10
Switch(config-if)#switchport multi vlan add 15
Switch(config-if)#end
```

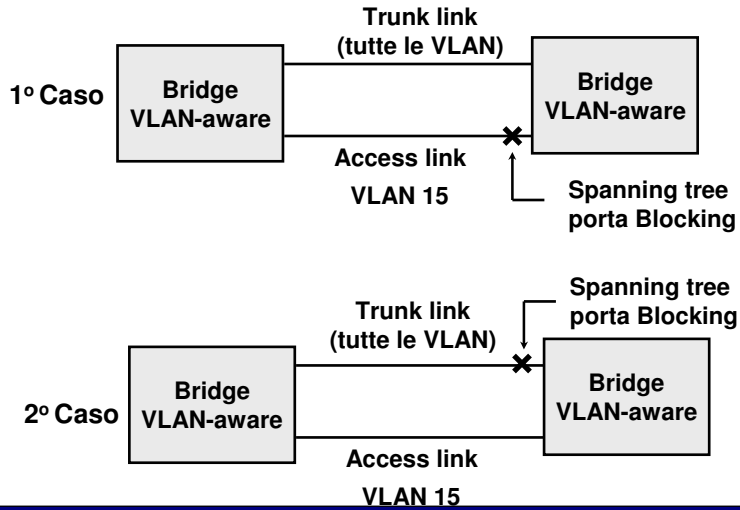
Server che condivide più VLAN su Switch di tipo SVL



VLAN - Tabella di condivisione	
VLAN	Porte condivise
20	porta 1 e 2
10	porta 3
15	porta 3

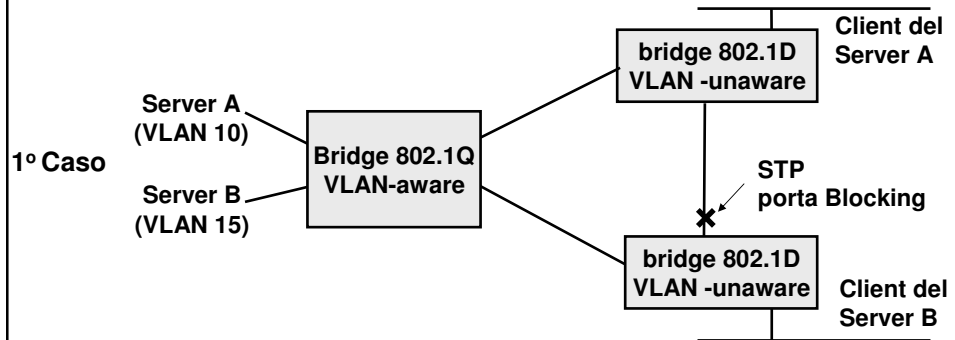
802.1Q problema di spanning tree

- Dipende dove STP effettua il blocco



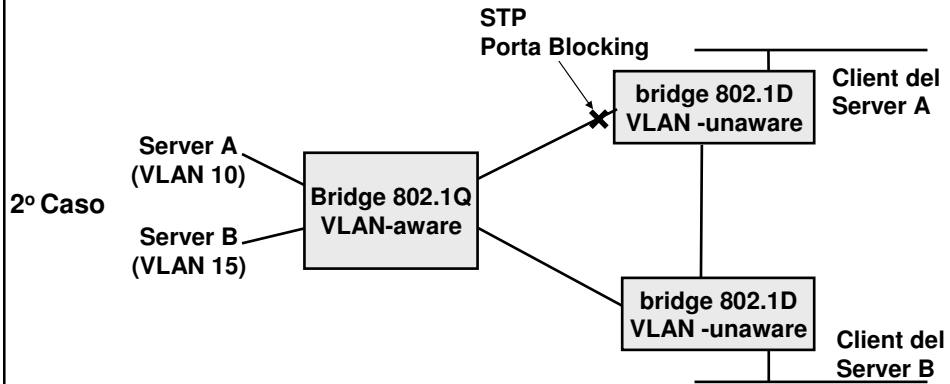
Convivenza tra bridge 802.1Q e 802.1D

- Dipende dove STP effettua il blocco



Convivenza tra bridge 802.1Q e 802.1D

- In questo caso il blocco non permette la connessione dei client del Server A



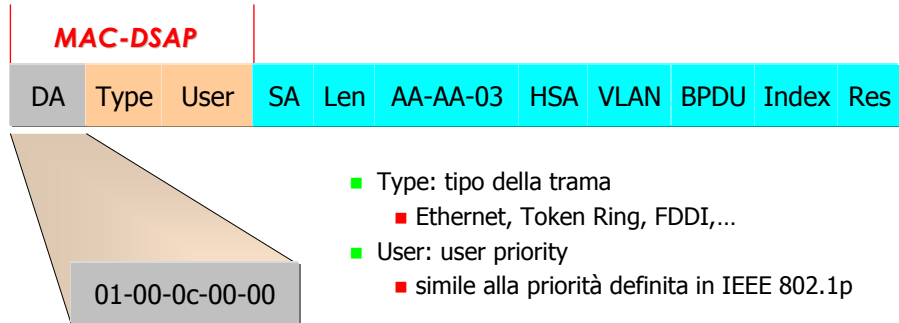
Inter Switch Link (ISL) di Cisco

- Il frame originale viene incapsulato con un header ISL ed una nuova FCS
 - Si tratta di un metodo di two level tagging
- Permette il supporto di 1024 VLAN
- Spanning multilpli (uno per VLAN)
- Realizzato in ASIC per garantire prestazioni wire speed



Formato dell'header ISL

- I primi 40 bit del MAC DA identificano un indirizzo di destinazione multicast
- Gli altri 8 bit sono usati come campo type e user



Spanning tree per VLAN su ISL

