Il Lego dell'inter-VLAN routing

by MP, feb 2016

Cerchiamo di spiegare con **un paragone ludico-grafico** i vari elementi coinvolti nell'instradamento del traffico tra diverse **VLAN**-Virtual LAN, la "replica a livello 2" delle **subnet**, definite invece a livello 3 in base agli indirizzi IP. Come sappiamo, VLAN e subnet si dicono "**coestensive**", perché i due tipi di raggruppamento devono normalmente comprendere gli stessi apparati.

L'esistenza delle VLAN mantiene **separato il traffico** tra i gruppi anche sugli **Switch layer 2**, evitando che un utente possa **cambiare gruppo**, e accedere direttamente a risorse che non gli competono, semplicemente assegnandosi l'IP di una **subnet diversa** dalla propria.

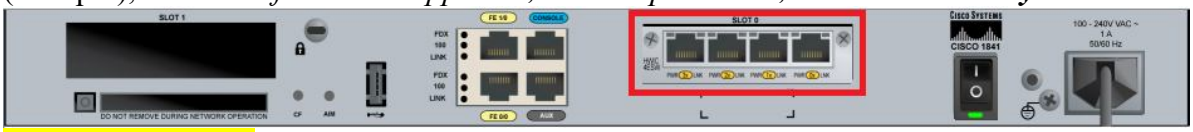
Mentre le **subnet** possono essere definite su segmenti di rete di qualunque tipo (Ethernet e seriali, quindi **LAN** e **WAN**), le **VLAN** sono definite **solo nelle LAN**, sugli **Switch**. Quindi parleremo solo delle **reti Ethernet**, dove hanno senso entrambi i termini.

Due host appartenenti a **subnet/VLAN diverse** possono colloquiare solo attraverso un apparato di **livello 3**, che faccia **routing** tra loro; è così possibile applicare dei **controlli** tra le diverse subnet, tramite opportune **ACL**-Access Control List, per consentire solo il traffico desiderato.

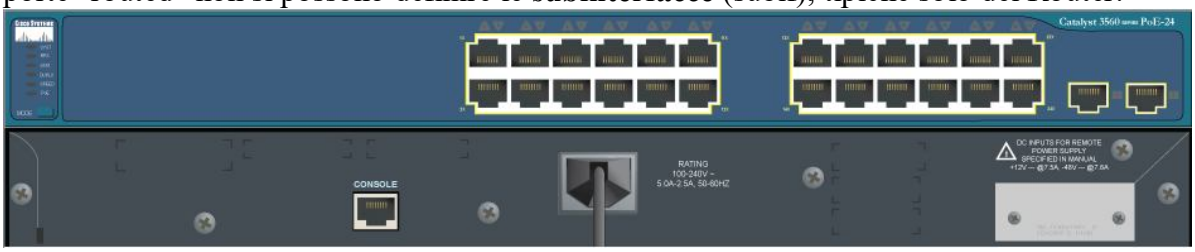
Gli **apparati** possibili per questo **instradamento** sono quindi di solito:

- un **Router normale**, che ha solo interfacce "**routed**" (cioè operanti a **livello 3**, con **IP**):

- un **Router ISR**-Integrated Services Router, che accetta espansioni **HWIC-4ESW**; queste schede inseriscono nel Router un piccolo **Switch a 4 porte**, con tutte le funzionalità di un normale **Switch Layer 2**: porte di accesso o di trunk, protocollo DTP, port-security, SVI (vedi poi), ecc. *e trasformano l'apparato, come ci piace dire, in un…* ***Router layer 2***:



- uno **Switch layer 3**, come i **3560** o superiori, in cui alcune porte possono essere configurate da "**switched**" a "**routed**", col comando: SL3(config-if)#**no switchport**. Dopo tale comando lo Switch L3 diventa praticamente un **Router ISR**, con la piccola differenza che sulle sue porte "routed" non si possono definire le **subinterfacce** (subif), tipiche solo dei Router:

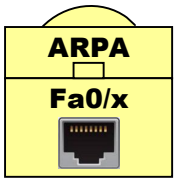


Il traffico degli host da instradare può arrivare, alle interfacce degli apparati L3 che fanno il routing, **direttamente** dai singoli host, o tramite altri **apparati di accesso**, tipicamente **Switch L2** o **Access Point** wireless, che lo raccolgono e lo convogliano verso gli apparati L3 tramite **trunk L2**.

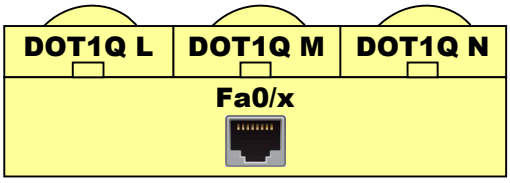
L'**indirizzo IP** dell'apparato L3, che ogni subnet può così raggiungere, funge per essa da **Default Gateway**; tramite tale IP gli host possono dialogare con **altre subnet**, e spesso anche con **Internet**.

I "**mattoni**" del nostro **Lego** per fare **Inter-VLAN routing** su tali apparati sono sono quindi:

1) le porte "**switched**" di modo "**access**"; fisicamente, stanno a **livello 1**, e sono associate a **una sola VLAN** (per default, la **1**); ricevono e trasmettono Trame **Ethernet** (ARPA); come i "trunk", ci sono solo su Router ISR e Switch L3, oltre ovviamente sugli Switch L2, ma mancano sui Router "puri" o normali:

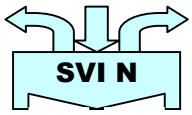


2) le porte "**switched**" di modo "**trunk**"; fisicamente, sono anch'esse a **livello 1**, ma sono associate per default a **tutte le VLAN** del dominio (in figura, 3); ricevono e trasmettono Trame **802.1Q**, ossia Trame Ethernet con l'aggiunta del **TAG** (n.) della VLAN:

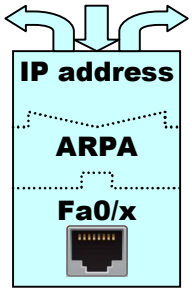


3) le **VLAN**, che sono i **gruppi** creati a **livello 2** col comando: S(config)#**vlan N** oppure automaticamente dall'IOS, assegnando una porta a una nuova VLAN, col comando: S(config-if)#**switchport access vlan N** (nome = VLAN000N):

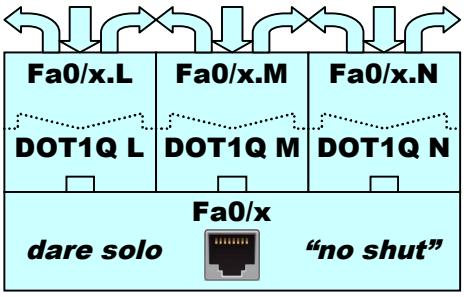
4) le porte virtuali "**routed**" o **SVI**-Switch Virtual Interface dei Router ISR e degli Switch L3, create col comando: SL3(config)#**interface vlan N**, che ricevono un **indirizzo IP** e operano a **livello 3** (le frecce indicano il **routing**); **più porte** di accesso e trunk possono portare traffico alle VLAN e alle SVI:



5) le porte fisiche "**routed**" di **tutti** gli apparati L3, che ricevono un **indirizzo IP** e operano nativamente a **livello 3**; queste interfacce gestiscono al loro interno anche un **livello 2 Ethernet** (encapsulation **ARPA**) e un livello **fisico**, che risultano però quasi "**trasparenti**" all'utente, che vede l'interfaccia ricevere direttamente un indirizzo IP:



6) le porte logiche "**routed**" di tipo **subinterface** (subif), con cui i **Router** normali e ISR gestisono i **trunk L2** connessi a una porta "routed"; le subif sono create col comando: R(config)#**interface Fa0/x.N**, cui segue il prompt R(config-subif)# ; prima di poter ottenere un **indirizzo IP** e operare a **livello 3**, devono ricevere il comando: R(config-subif)#**encapsulation dot1q N** che le associa alla rispettiva VLAN **N**; le subif sono già **up** e gestiscono al loro interno anche un **livello 2** per l'encapsulation **DOT1Q** del trunk, e un **livello fisico**, che dev'essere almeno da **100 Mbps** e va **acceso**:

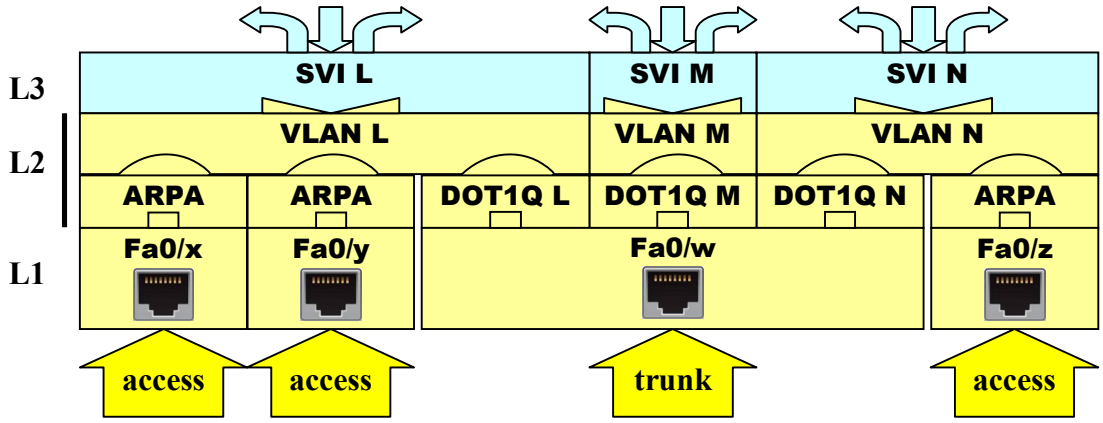


Esistono anche **altri tipi** di porte **LAN** operanti a **L2** ed **L3**, quali ad esempio i **port-channel**, che si ottengono con l'aggregazione di più porte fisiche, fino a 8, per aumentare la **banda** e l'**affidabilità** del collegamenti, coi protocolli **PAgP** ed **LACP**. Una volta creati, questi port-channel vengono configurati al posto delle singole porte fisiche, e possono essere "**switched**" (L2) o "**routed**" (L3). Non li esaminiamo per mantenere abbastanza **semplice** la trattazione.

Gli **indirizzi IP** delle porte "**routed**" o delle **SVI**, oltre che per il **passaggio** del traffico tra le **diverse subnet** e verso **Internet**, possono anche servire per la **gestione** degli apparati, che su tali indirizzi vengono raggiunti con PING, Telnet, SSH, HTTP, ecc. Perché un apparato possa **rispondere** a tale traffico, se provenente da **reti diverse** dalla propria, deve essere dotato dell'IP di un **Default Gateway** o, nel caso dei **Router**, da un'**apposita rotta** o da una **default route**.

Il **routing** fatto con le **porte virtuali "routed"** di tipo **SVI**-Switch Virtual Interface, tramite le porte "**switched**" dei **Router ISR** e degli **Switch L3**, viene quindi costruito con questi **mattoni**:

- delle porte "**switched**" di modo "**access**" o "**trunk**" portano all'apparato L3 il traffico da instradare (Pacchetti IP); le prime in Trame **Ethernet/ARPA**, le seconde in Trame **802.1Q**
- il traffico viene **associato** alla rispettiva **VLAN** di **livello 2**; nelle porte di **accesso** ciò avviene esaminando la **VLAN assegnata** alla porta (per default la **n. 1**), mentre sui **trunk** il numero della VLAN è **già presente** all'interno delle Trame **802.1Q**
- se il destination **MAC** della Trama è quello del D.G., l'apparato invia il Pacchetto alla **SVI** con lo **stesso numero** della **VLAN** e questa, che funge da **Default Gateway** della **subnet** corrispondente, fa gli eventuali **controlli** (ACL), e il **routing** richiesto dal destination **IP**.

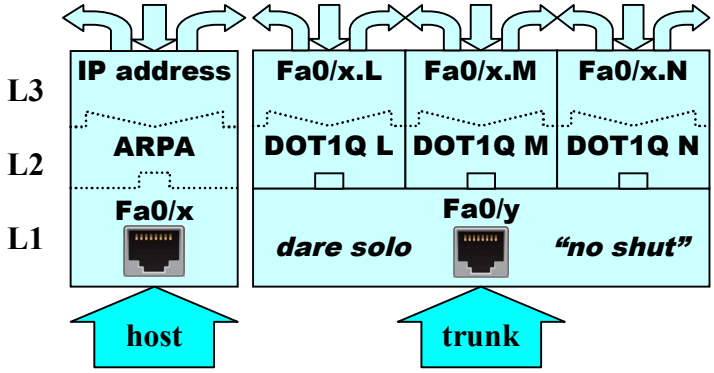


Si noti l'**assoluta necessità** della **presenza delle VLAN** di **livello 2**, definite nel **VLAN database** dello Switch, perché la comunicazione tra le **interfacce** e le **SVI** abbia luogo con successo.

Ciò è abbastanza **garantito** dalle porte di **accesso**, ove la VLAN L2 viene **creata** quando la porta viene associata a una **VLAN inesistente**, col comando: S(config-if)#**switchport access vlan L**. Altrettanto non si può dire invece se il traffico arriva allo Switch solo su porte di **trunk**; infatti su queste porte transitano tutte le **VLAN esistenti**, ma la loro **creazione** è lasciata all'utente, tramite il comando (nell'esempio): S(config)#**vlan M**, seguito dall'eventuale comando: **name**. *Sui **Router ISR**, in PT, le VLAN si creano solo nel "modo deprecato": R#**vlan database** → R(vlan)#**vlan N** …*

In **alternativa**, il **database** delle VLAN (file **vlan.dat** in flash) può essere gestito dal protocollo **VTP**-VLAN Trunking Protocol, che lo aggiorna in base ai messaggi ricevuti dagli Switch della rete con ruolo di **VTP Server**, associati allo stesso "**VTP domain**".

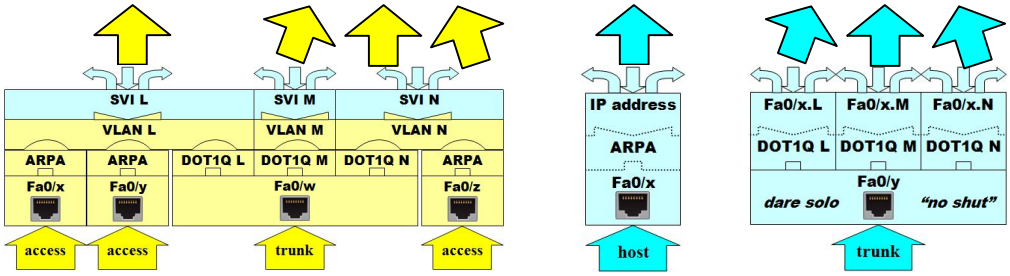
Il **routing** fatto con le porte **fisiche** "**routed**" o con le **subif**, su tutti i tipi di **Router**, e sulle porte "**routed**" degli **Switch L3**, si basa invece su questi **mattoni** del nostro **Lego**. Qui non è necessario definire il database delle VLAN, ma nelle **subif** va usato il comando: **encapsulation dot1q N**:



È evidente come le **due soluzioni** possono essere **combinate** sui **Router ISR** e sugli **Switch L3** →

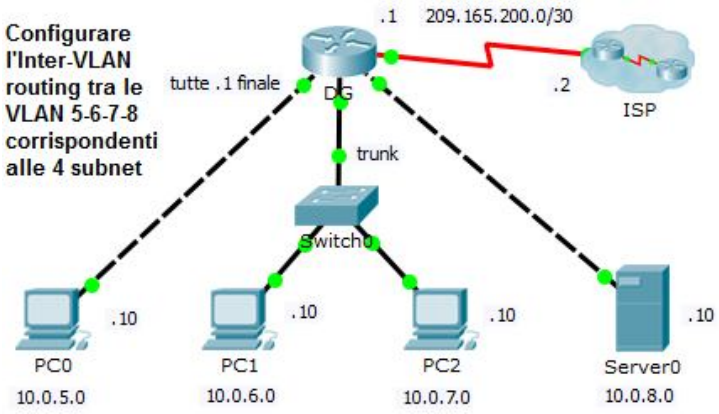
Tabella sulle possibilità di fare **Inter-VLAN routing** sui tre tipi di apparati L3 citati:

Interfacce / Apparati	una SVI su p. switched access	varie SVI su p. switched trunk	Interfaccia fisica routed	Subinterfacce logiche routed
Router normale			X	X
Router ISR	X	X	X	X
Switch L3 *	X	X	X	



* Gli **Switch L3** sono gli unici le cui interfacce possono essere trasformate da **switched** a **routed**.

Esempi di configurazione di Inter-VLAN routing basato su **Router ISR** (il più flessibile→tabella):



Estratti da **sh run** e **sh vlan** dello **Switch**:

```
interface FastEthernet0/1
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/24
 switchport mode trunk
```

```
Switch>sh vlan bri
VLAN Name       Status    Ports
---- ---------- --------- -----------------
1    default    active    Fa0/3, Fa0/4, ...
6    SEI        active    Fa0/1  (Fa0/24 non
7    SETTE      active    Fa0/2   c'è = è trunk)
```

Inoltre è stata creata la DG(vlan)#**vlan 5**. Nell'esempio, sul Router ISR non si usa l'opzione "porta **switched di trunk**" con **SVI**, preferendo quella delle due "**subif**" **.6** e **.7** sulla porta **routed** built-in Fa0/0.

Estratti dallo **show run** del **Router ISR 1841**:

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto                          ← solo "no shut"
!
interface FastEthernet0/0.6          ← subif 6
 encapsulation dot1Q 6
 ip address 10.0.6.1 255.255.255.0
!
interface FastEthernet0/0.7          ← subif 7
 encapsulation dot1Q 7
 ip address 10.0.7.1 255.255.255.0
!
interface FastEthernet0/1            ← IF fisica
 ip address 10.0.8.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/0/0          ← porta switched
 switchport access vlan 5
 switchport mode access
!
interface Vlan5                      ← SVI 5
 ip address 10.0.5.1 255.255.255.0
```