

Introduzione alle VLAN

Autore: Roberto Bandiera – 21 gennaio 2015

Definizione

Mentre una LAN è una rete locale costituita da un certo numero di pc connessi ad uno switch, una **VLAN** è una LAN VIRTUALE (**Virtual LAN**) e questo lascia immaginare una maggiore flessibilità rispetto ad una LAN.

Uso del concetto di VLAN per poter configurare uno switch da remoto

Si ricorda che lo switch opera al livello 2 Data Link dello stack ISO/OSI e che pertanto non ha niente a che vedere con gli indirizzi IP, che sono propri del livello 3 Network.

Tuttavia, per poter configurare uno switch si deve assegnare allo stesso un indirizzo IP. Pertanto, è lo switch nel suo complesso che viene visto come un dispositivo di rete, raggiungibile tramite *telnet* da un qualsiasi pc della stessa rete (o addirittura di Internet).

Per assegnare un indirizzo IP ad uno switch si considera l'interfaccia virtuale denominata VLAN 1 e le si assegna il desiderato indirizzo IP.

Con uno switch CISCO ci si collega tramite cavo rollover alla porta Console e tramite un programma di emulazione di terminale come Putty ci si collega e si danno i seguenti comandi:

```
switch> enable
switch# configure terminal
switch(config)# interface vlan 1
switch(config-if)# ip address 192.168.1.100 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
```

Tali comandi sono del tutto analoghi a quelli usati per configurare l'indirizzo IP delle interfacce di un router CISCO.

In questo modo da un qualsiasi pc collegato a una qualsiasi interfaccia dello switch sarà possibile dare il comando **telnet 192.168.1.100** per entrare nella modalità a comandi della configurazione dello switch.

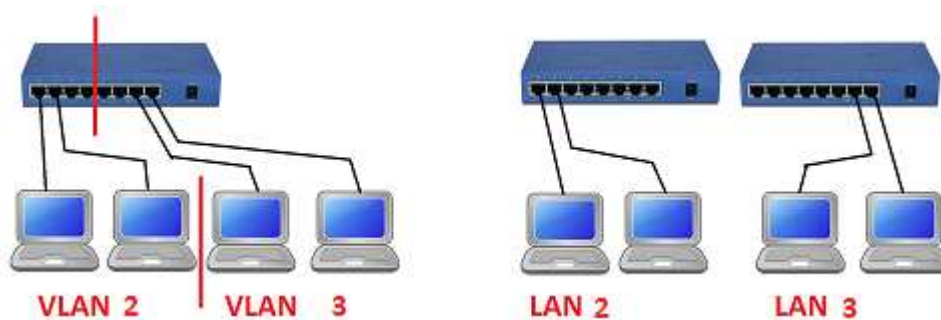
Questo funziona purchè i pc collegati allo switch siano anch'essi configurati con indirizzi IP appartenenti alla rete 192.168.1.0.

Si ribadisce che, anche volendo, non è possibile assegnare un indirizzo IP alle singole interfacce fisiche dello switch. L'interfaccia virtuale **VLAN 1** corrisponde all'insieme di tutte le interfacce fisiche dello switch.

VLAN come sottoinsieme di interfacce dello switch

Per capire meglio il significato di VLAN, conviene pensare a definire due VLAN nello stesso switch: si tratta di ripartire le interfacce dello switch in due sottoinsiemi.

In questo modo si ottiene uno switch VIRTUAMENTE diviso in due parti e del tutto equivalente ad avere 2 distinti switch.



Due VLAN equivalgono a due distinte LAN.

VLAN 2 = interfacce Fa1 Fa2 Fa3 Fa4 – VLAN 3 = interfacce Fa5 Fa6 Fa7 Fa8

Così facendo i pc collegati alle interfacce di una VLAN risulteranno del tutto isolati da quelli dell'altra VLAN.

Si ottengono quindi 2 LAN virtuali, mentre fisicamente appare una unica LAN.

In particolare si osserva che il traffico di broadcast originato da un pc della VLAN 2 raggiungerà solo i pc della medesima VLAN senza raggiungere i pc della VLAN 3.

La configurazione dello switch consiste nell'assegnare ciascuna interfaccia dello stesso alla VLAN desiderata.

Gli indirizzi IP dei pc collegati allo switch terranno conto del fatto che a tutti gli effetti si hanno due reti separate: ad esempio 192.168.2.0 per la VLAN 2 e 192.168.3.0 la VLAN 3. Si noti che per comodità si sono stabiliti indirizzi IP dove il terzo otteto coincide con il numero della VLAN.

Lo switch di livello 2 non effettua nessuna operazione di routing e pertanto non è possibile che due pc appartenenti alle due VLAN comunichino tra di loro.

La configurazione delle due VLAN

Per la configurazione dello switch si deve innanzitutto assegnare un indirizzo IP alla VLAN 1.

In questo modo da uno dei pc della VLAN 1 sarà possibile effettuare un collegamento telnet all'indirizzo dello switch per poterlo configurare. Innanzitutto si creano le due VLAN e poi si assegnano le interfacce desiderate alla VLAN 2.

Si ricorda che per default tutte le interfacce dello switch sono inizialmente assegnate alla VLAN 1.

Prima di assegnare le singole interfacce alla nuova VLAN si deve creare la VLAN:

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# exit
switch(config)# vlan 3
switch(config-vlan)# exit
```

I comandi per assegnare l'interfaccia Fa1 alla VLAN 2 sono i seguenti:

```
switch(config)# interface Fa1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
switch(config-if)# exit
```

E' anche possibile configurare in blocco un gruppo di interfacce dello switch. Ad esempio per configurare la gamma di interfacce dalla Fa1 alla Fa4 si danno i comandi:

```
switch(config)# interface range Fa1-4
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
switch(config-if)# exit
```

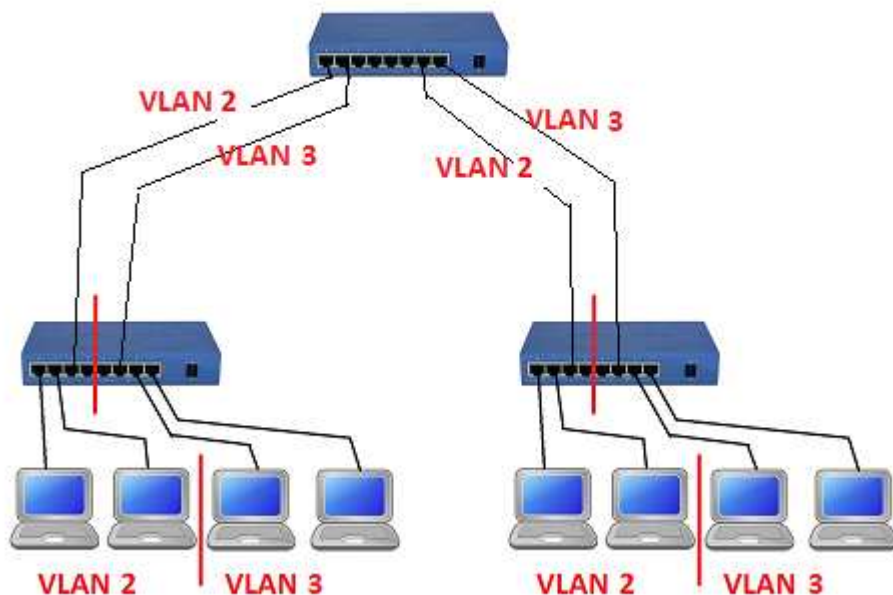
Si procede analogamente per le interfacce associate alla VLAN 3.

La flessibilità data dalle VLAN

Grazie alla definizione di VLAN diverse, è possibile **separare logicamente** i pc di una LAN scolastica in due VLAN assegnate rispettivamente ai professori e agli studenti, senza che sia possibile alcuna commistione di traffico.

La flessibilità della gestione delle VLAN consente di avere la stessa VLAN assegnata a pc situati in LAN diverse purché i rispettivi switch siano interconnessi tra di loro.

Ancora una volta i pc delle due VLAN non possono in nessun modo comunicare tra di loro.



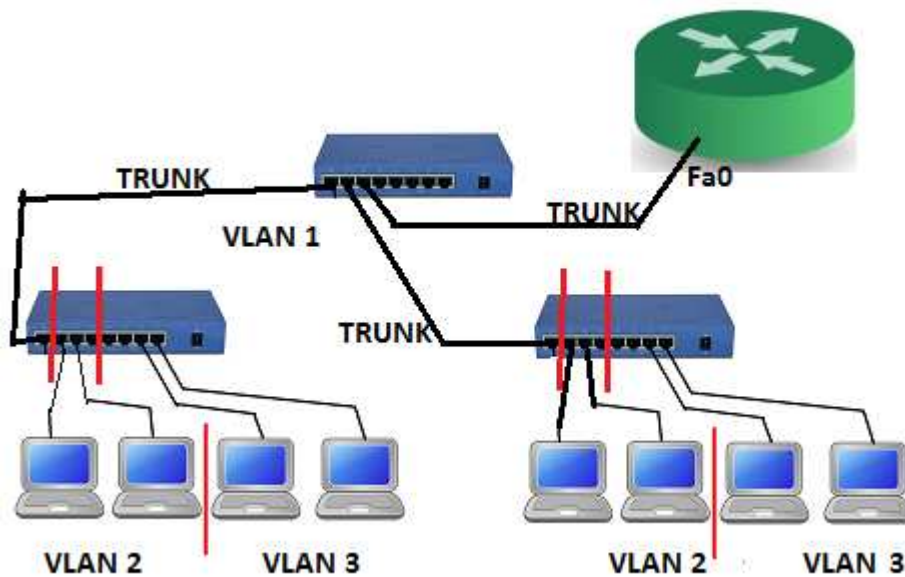
Due distinte VLAN con pc distribuiti fisicamente in zone diverse

Per maggiore flessibilità, e anche per risparmiare sui costi del cablaggio, è possibile utilizzare un singolo cavo tra gli switch e fare in modo che esso faccia passare il traffico delle due VLAN.

Per continuare a mantenere del tutto separato il traffico delle due VLAN, questo collegamento, che viene detto TRUNK, utilizza un protocollo speciale per i frame: il **protocollo 802.1Q** che in sostanza aggiunge una etichetta (tag) ai frame per identificare la VLAN alla quale essi appartengono.

Le interfacce che gestiscono questi collegamenti TRUNK sono solitamente associate alla VLAN 1 (VLAN Nativa) che funge anche da VLAN Amministrativa per la configurazione degli switch.

Nell'ambito dei collegamenti TRUNK, tale VLAN viene detta VLAN NATIVA in quanto il traffico da essa generato non viene "taggato" come invece accade per il traffico associato alle altre VLAN.



Uso di collegamenti TRUNK + Inter VLAN Routing

La configurazione delle interfacce di TRUNK avviene nel modo seguente:

```
switch(config)# interface Fa1
switch(config-if)# switchport mode trunk
switch(config-if)# exit
```

Negli switch più vecchi il protocollo utilizzato dai TRUNK era diverso, pertanto risulta necessario specificare il protocollo 802.1Q con il comando aggiuntivo:

```
switch(config-if)# switchport trunk encapsulation dot1q
```

Per default un collegamento TRUNK consente di far passare il traffico di tutte le VLAN. Tuttavia esso potrebbe essere programmato in modo più restrittivo specificando la lista delle VLAN ammesse:

```
switch(config-if)# switchport allowed vlan 2,3
```

Mettere in comunicazione le VLAN

Per mettere in comunicazione le VLAN occorre un dispositivo che faccia "routing". La figura precedente mostra come si possa collegare mediante un collegamento TRUNK uno switch con un Router

L'interfaccia del Router che ha il suddetto collegamento TRUNK viene vista come default gateway per le due VLAN i cui dispositivi appartengono a due diverse reti come ad esempio 192.168.2.0/24 e 192.168.3.0/24. Pertanto tale interfaccia dovrebbe avere due diversi indirizzi IP: uno per ciascuna rete.

Per consentire questo, si deve configurare l'interfaccia del Router come se fosse costituita da **due sottointerfacce**. Se l'interfaccia del Router si chiama Fa0, le due sottointerfacce vengono identificate aggiungendo un punto e il numero della VLAN: nel caso in esame esse saranno Fa0.2 e Fa0.3.

I comandi di configurazione devono anche prevedere l'utilizzo del protocollo 802.1Q per gestire il traffico che consiste di frame "taggati" con il numero della VLAN corrispondente:

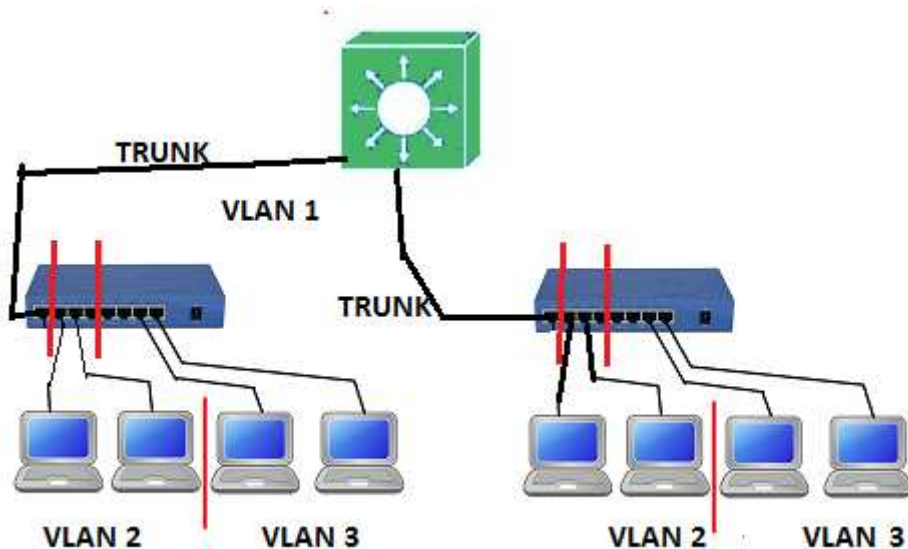
```
R(config)# interface Fa0.2
R(config-subif)# encapsulation dot1q 2
R(config-subif)# ip address 192.168.2.1 255.255.255.0
R(config-subif)# exit
R(config)# interface Fa0.3
R(config-subif)# encapsulation dot1q 3
R(config-subif)# ip address 192.168.3.1 255.255.255.0
R(config-subif)# exit
R(config)# interface Fa0
R(config-if)# no shutdown
R(config-if)# exit
```

Grazie al lavoro del Router ora è possibile che un pc della VLAN 2 comunichi con un pc della VLAN 3.

Il pacchetto indirizzato da un pc di una VLAN ad un pc dell'altra VLAN dovrà necessariamente transitare per il Router.

Il Router potrebbe anche essere programmato per filtrare in qualche modo il traffico indirizzato da una VLAN all'altra.

Per **maggior efficienza**, anziché un Router si potrebbe utilizzare uno **Switch Multilayer** che operando a livello 3 può effettuare il routing in modo molto efficiente tra le diverse VLAN.



Inter VLAN routing mediante Switch Multilayer

Per programmare lo switch multilayer si deve innanzitutto abilitarne la funzione di routing:

```
SwitchLayer3# configure terminal
SwitchLayer3(config)# ip routing
```

Poi si devono definire le VLAN tra cui deve effettuare il routing:

```
SwitchLayer3(config)# vlan 2
SwitchLayer3(config-vlan)# exit
SwitchLayer3(vlan)# vlan 3
SwitchLayer3(config-vlan)# exit
```

Poi si devono configurare le interfacce virtuali associate alle suddette VLAN:

```
SwitchLayer3(config)# interface vlan 2
SwitchLayer3(config-if)# ip address 192.168.2.1 255.255.255.0
SwitchLayer3(config-if)# no shutdown
SwitchLayer3(config-if)# exit
```

```
SwitchLayer3(config)# interface vlan 3
SwitchLayer3(config-if)# ip address 192.168.3.1 255.255.255.0
SwitchLayer3(config-if)# no shutdown
SwitchLayer3(config-if)# exit
```

Nella tabella di routing dello switch multilayer compariranno le seguenti route:

C 192.168.2.0/24 is directly connected, Vlan2

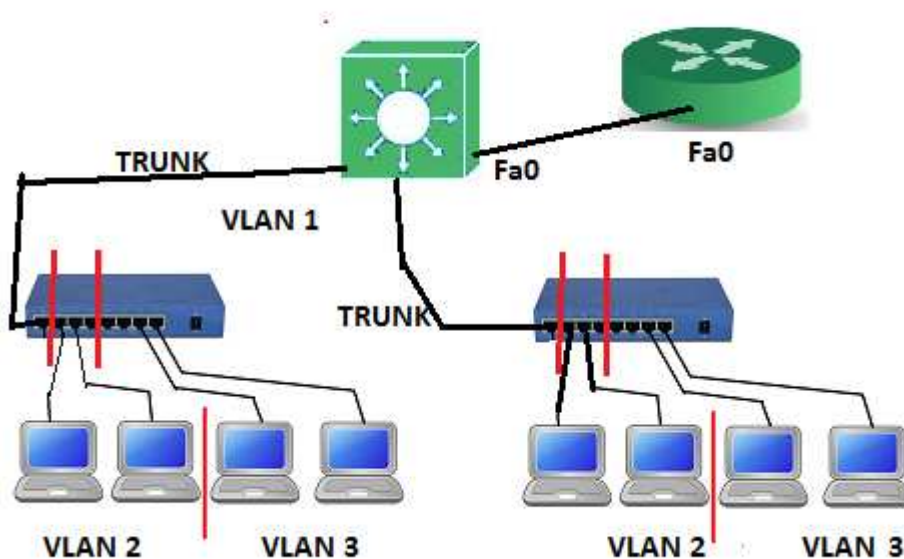
C 192.168.3.0/24 is directly connected Vlan3

si tratta di route direttamente connesse.

Anche lo switch multilayer può prevedere dei filtri per regolare il traffico dei pacchetti da una VLAN all'altra.

L'accesso a Internet

L'utilizzo di uno switch multilayer velocizza il routing interno tra le diverse VLAN aziendali, tuttavia, per consentire la connessione ad una rete geografica esterna ed in particolare per la connessione ad Internet, occorre connettere lo switch multilayer ad un Router.



Utilizzo di un router per l'accesso a Internet

L'interfaccia dello switch multilayer che viene utilizzata per la connessione al Router viene configurata non come una normale interfaccia dello switch (switchport) ma come se fosse a tutti gli effetti l'interfaccia di un router (**router port**); questo lo si ottiene con il comando `no switchport`.


```
SwitchLayer3(config)# interface Fa0
SwitchLayer3(config-if)# no switchport
SwitchLayer3(config-if)# ip address 192.168.0.2 255.255.255.0
SwitchLayer3(config-if)# exit
```

Per quanto riguarda l'interfaccia Fa0 del router, essa viene configurata con un singolo indirizzo IP:

```
R(config)# interface Fa0
R(config-if)# ip address 192.168.0.1 255.255.255.0
R(config-if)# no shutdown
```

A questo punto lo switch multilayer deve prevedere una route di default verso il router:

```
SwitchLayer3(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

In questo modo la tabella di routing dello switch multilayer conterrà anche una route statica di default verso l'interfaccia Fa0 del Router:

```
C 192.168.2.0/24 is directly connected, Vlan2
```

```
C 192.168.3.0/24 is directly connected Vlan3
```

```
S* 0.0.0.0/0 via 192.168.0.1
```

Per la configurazione dello switch multilayer, conviene lasciare una interfaccia associata alla VLAN 1 e assegnare un indirizzo IP all'interfaccia virtuale VLAN 1. In questo modo è possibile connettere allo switch un pc portatile e accedere tramite telnet a tutti gli switch della rete.