Le Virtual LAN (VLAN)
Teoria, funzionamento e applicazioni

Prof. Fedeli Massimo

Indice

1 Cos'è una VLAN

Una **Virtual LAN (VLAN)** è una rete locale creata in modo **logico** e non fisico. Attraverso le VLAN è possibile suddividere un'unica infrastruttura di rete (switch, cavi, apparati) in più reti separate tra loro, come se esistessero switch distinti, pur utilizzando lo stesso hardware.

Lo standard tecnico che permette questa suddivisione è lo **IEEE 802.1Q**.

L'idea fondamentale è semplice:

> *Host collegati allo stesso switch possono appartenere a reti diverse, anche se fisicamente connessi allo stesso dispositivo.*

Ogni VLAN si comporta come una LAN indipendente:

- il traffico broadcast resta confinato all'interno della VLAN
- i dispositivi di VLAN diverse non possono comunicare direttamente a livello 2

2 VLAN e modello ISO/OSI

Le VLAN operano a **Livello 2 (Data Link)** del modello ISO/OSI. Questo significa che la separazione avviene a livello di frame Ethernet, non a livello IP.

La comunicazione tra dispositivi appartenenti a VLAN diverse richiede quindi un dispositivo di **Livello 3**, cioè:

- un router
- oppure uno switch Layer 3

Per questo motivo, nella progettazione delle reti si crea spesso una corrispondenza:

$$\textbf{1 VLAN} \longleftrightarrow \textbf{1 sottorete IP}$$

3 Perché usare le VLAN

L'introduzione delle VLAN risponde a tre esigenze fondamentali:

3.1 Riduzione del traffico

Limitando il dominio di broadcast si evita che tutti i dispositivi ricevano traffico non necessario, migliorando le prestazioni.

3.2 Maggiore sicurezza

Le VLAN permettono di isolare gruppi di utenti o servizi (ad esempio studenti, segreteria, server), riducendo il rischio di accessi indesiderati.

3.3 Flessibilità e gestione

Spostare un utente da una rete a un'altra non richiede di cambiare cablaggio: basta modificare la configurazione della porta dello switch.

4 Identificazione delle VLAN

Ogni VLAN è identificata da:

- un **nome descrittivo** (es. VLAN_DOCENTI)
- un **VID (VLAN Identifier)**

Il VID è un numero a 12 bit:

$$VID \in [1, 4094]$$

I valori 0 e 4095 sono riservati dallo standard.

5 Modalità di realizzazione delle VLAN

5.1 VLAN Port-Based (Access o Untagged)

È la modalità più semplice. Ogni porta dello switch viene assegnata manualmente a una VLAN.

Caratteristiche principali:

- una porta appartiene a una sola VLAN
- i frame Ethernet non contengono informazioni aggiuntive (nessun tag)
- i dispositivi collegati non devono conoscere l'esistenza delle VLAN

Limite: l'appartenenza alla VLAN dipende solo dalla porta fisica, quindi chiunque si colleghi a quella porta entra automaticamente nella VLAN.

5.2 VLAN Tagged (802.1Q)

Questa modalità consente di trasportare traffico di **più VLAN sullo stesso collegamento fisico**. Per farlo, i frame Ethernet vengono modificati inserendo un **tag VLAN**.

Le porte si distinguono in:

- **Access Port**: traffico di una sola VLAN, frame senza tag
- **Trunk Port**: traffico di più VLAN, frame con tag 802.1Q

6 Il Tag 802.1Q

Quando un frame attraversa una porta trunk, lo switch inserisce un campo aggiuntivo di 4 byte nel frame Ethernet.

Questo campo contiene:

- **TPID (Tag Protocol Identifier)** = 0x8100
- **TCI (Tag Control Information)**, che include:
  - Priorità del traffico (QoS)
  - CFI (compatibilità formato MAC)
  - VID (identificatore VLAN)

Grazie al VID, gli switch lungo il percorso sanno a quale VLAN appartiene ogni frame.

7 VLAN Nativa

Su un collegamento trunk esiste una VLAN speciale chiamata **VLAN nativa**.
I frame appartenenti alla VLAN nativa:

- viaggiano sul trunk **senza tag**
- per default corrispondono alla VLAN 1

Per motivi di sicurezza è consigliato:

- non usare la VLAN 1 come VLAN nativa
- scegliere una VLAN dedicata non utilizzata per utenti

8 Porte Ibride

Una **porta ibrida** può gestire sia traffico tagged sia untagged.
Funzionamento:

- se arriva un frame senza tag, viene associato alla VLAN PVID della porta
- se arriva un frame con tag, viene associato alla VLAN indicata nel VID

Questa modalità è utile quando convivono dispositivi moderni e dispositivi che non supportano il tagging VLAN.

9 Operazioni svolte dallo switch

Quando un frame entra in uno switch, avvengono tre fasi:

Ingress

Lo switch identifica la VLAN di appartenenza del frame (tramite porta o tag).

Forwarding

Il frame viene inoltrato solo verso porte appartenenti alla stessa VLAN, usando una tabella MAC separata per ogni VLAN.

Egress

Se necessario, lo switch:

- aggiunge il tag VLAN (verso trunk)
- rimuove il tag VLAN (verso access port)

10 VLAN estese su più switch

Le VLAN possono estendersi su più switch grazie ai collegamenti **trunk**. Un trunk è un collegamento punto-punto tra due switch che trasporta traffico di più VLAN mediante tagging 802.1Q.

11 Protocollo VTP (Cisco)

Il **VLAN Trunking Protocol** è un protocollo proprietario Cisco che consente di distribuire automaticamente la configurazione VLAN tra più switch.

Modalità operative:

- Server (crea e modifica VLAN)
- Client (riceve configurazioni)
- Transparent (propaga ma non modifica)

12 Inter-VLAN Routing

Poiché le VLAN sono isolate a livello 2, per permettere la comunicazione tra di esse è necessario il routing.

Le principali soluzioni sono:

- Router tradizionale con più interfacce fisiche
- Router-on-a-stick (una sola interfaccia trunk)
- Switch Layer 3

13 Conclusione

Le VLAN rappresentano uno strumento fondamentale per la progettazione delle reti moderne. Consentono segmentazione logica, migliore controllo del traffico, maggiore sicurezza e una gestione molto più flessibile dell'infrastruttura.

Comprendere il funzionamento del tagging 802.1Q, delle porte access e trunk e del routing tra VLAN è essenziale per chiunque si occupi di reti.