VLAN

Virtual Local Area Network

Il termine VLAN (Virtual LAN) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale (tipicamente IEEE 802.3) basata su switch, in più reti non comunicanti tra loro.
Le applicazioni di questa tecnologia sono tipicamente legate ad esigenze di separare il traffico di gruppi di lavoro o dipartimenti di una azienda, per applicare diverse politiche di sicurezza informatica.
Le prime versioni proprietarie permettevano di realizzare su un singolo switch diverse reti "virtuali" (VLAN), assegnando ciascuna porta ad una di queste reti.
Gli host collegati ad una rete potevano comunicare solo tra di loro e non con quelli collegati alle altre reti, se non per mezzo di un router connesso ad entrambe le VLAN.
Ad esempio, ipotizziamo di avere un solo switch, e di avere la necessità di incrementare la sicurezza affinché utenti di un gruppo di lavoro non interagiscano con utenti di un altro gruppo.
Attivando, via software, la gestione delle VLAN sullo switch, si può impostare che su 24 porte ethernet disponibili, le prime 12 facciano parte del gruppo 1 e le ultime 12 facciano invece parte del gruppo 2.
Il risultato è lo stesso che si otterrebbe utilizzando un diverso switch "tradizionale" per ciascuna rete, ma con alcuni vantaggi:

- costi e ingombri: invece di diversi switch, è possibile utilizzare un solo switch con molte porte, risparmiando in costi di acquisizione e manutenzione, spazio occupato, prese di alimentazione elettrica, indirizzi IP per la gestione remota;
- flessibilità: le porte dello switch possono essere spostate da una VLAN ad un'altra per mezzo di semplici operazioni di riconfigurazione software, spesso effettuabili da remoto. Altre VLAN possono essere aggiunte utilizzando le porte esistenti, e quindi a costo nullo.

In seguito la tecnologia è stata sviluppata, aggiungendo la possibilità di collegare tra loro due switch unendo le VLAN presenti su di essi (VLAN trunking).
Questo permette di realizzare VLAN che si estendono nelle diverse parti di una rete aziendale, anche su scala geografica.
Questa tecnologia è poi stata standardizzata come IEEE 802.1q, in modo che apparati di rete di diversi fornitori possano essere collegati.