Vlan Tagged e UntAgged

Cos’è una Vlan?

Le Vlan(Virtual Lan) sono un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale basata su switch, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.

Le versioni iniziali

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 VLAN potevano comunicare solo tra di loro e non con quelli collegati alle altre reti VLAN, se non per mezzo di un router connesso ad entrambe le VLAN cioè tramite un indirizzamento a livello 3 di *internetworking*.

Come si identificano le Vlan

Ciascuna VLAN è identificata da un numero, detto VID (**V**lan **ID**), che va da 1 a 4094 (0 e 4095 sono riservati).

Per fare questo, nel frame ethernet IEEE 802.3 viene aggiunto un campo di 4 byte posto tra il destination address e il campo type/length, questo tag detto **VLAN TAG** oppure DOT1Q TAG,

Lo switch che riceve questo pacchetto deve quindi sapere che deve interpretare questi 4 byte come VLAN TAG, ed il resto del pacchetto come un normale pacchetto 802.3.

Criteri di appartenenza di un host a una Vlan

Una porta di uno switch su cui viaggiano pacchetti con il VLAN TAG è detta tagged o trunk port. Viceversa, una su cui viaggiano pacchetti senza VLAN TAG è detta access port. Alcuni switch accettano anche un traffico misto di pacchetti tagged e non tagged, e una porta configurata in questo modo è detta hybrid port.

Più in generale l'appartenenza di un host ad una VLAN può essere definita secondo diversi criteri:

- porte: come nell'esempio sopra descritto, ciascuna porta di uno switch è configurata per appartenere ad una data VLAN. Tutti i pacchetti provenienti da quella porta saranno "taggati" con l'ID della sua VLAN, e su questa porta verranno inviati solo pacchetti provenienti dalla sua VLAN. Questo è il metodo più diffuso e più semplice da implementare, in quanto lo switch deve guardare solo da quale porta viene un pacchetto per attribuirgli un VID.
- Autenticazione: i diversi apparati possono essere assegnati automaticamente a determinate VLAN sulla base di credenziali di autenticazione dell'utente o dell'apparato stesso tramite l'impiego del protocollo 802.1x.

- ***protocollo***: l'appartenenza ad una VLAN è dettata dal protocollo incapsulato in 802.3. Ad esempio, i pacchetti IP possono appartenere ad una VLAN, diversa da quella usata dai pacchetti IPX.
- ***MAC Address o indirizzo IP:*** i pacchetti vengono attribuiti ad una VLAN sulla base dell'indirizzo MAC o IP dell'host da cui provengono. In questo modo, ad una porta di uno switch possono essere collegati diversi host, che però appartengono a VLAN diverse.
- **analisi del pacchetto**: lo switch che riceve il pacchetto lo esamina in dettaglio, possibilmente fino al livello applicazioni, e sulla base dei risultati decide a quale VLAN attribuirlo sulla base del suo contenuto.

Vlan tagged e Untagged

Per quanto riguarda gli switch, le porte possono essere **untagged** member o **tagged** member di una VLA. NIn base al tipo di switch, è possibile configurare le porte in una delle modalità seguenti:

- **General** - l'interfaccia supporta tutte le funzioni definite nelle specifiche IEEE 802.1q e può essere tagged o untagged member di una o più VLAN.
- **Access o untagged** - in questa modalità l'interfacciapuò essere untagged member di una sola VLAN. Access Port o Untagged Port sono definizioni equivalenti. I pacchetti che attraversano una porta untagged (o access) sono privi del tag VLAN. Infatti sulle porte untagged sono collegati PC e dispositivi che nulla sanno delle VLAN.
- **Trunk o tagged** - l'interfaccia è tagged member di una o più VLAN. Una porta tagged è in grado di ricevere pacchetti "taggati", e su queste porte possono essere collegati solo dispositivi in grado di interpretare i VLAN tag, come switch, router e firewall compatibili con il protocollo 802.1q.

Esempio

Abbiamo detto che le VLAN servono a segmentare una rete e questo nella pratica significa che fisicamente andiamo a dire ad uno switch che le porte 1 – 2 – 3 appartengono alla VLAN 2 mentre tutte le altre rimangono come di default nella VLAN 1. Gli apparati che collegheremo sulle porte 1 – 2 – 3 potranno parlare solo fra di loro e non vedranno in nessun caso altri dispositivi connessi sullo stesso switch o su altri. Viceversa vale la stessa teoria, un pc connesso alla porta 7 dello switch non saprà dell'esistenza di un server che è connesso sulla 2 perché appartenenti a due VLAN diverse.

In questo caso si dice che stiamo TAGGANDO staticamente le porte di uno switch ed in pratica la parte intelligente e di gestione è tutta centralizzata sul nostro apparato di rete.