LEZIONE 1

Le Virtual LAN (VLAN)

In questa lezione impareremo...

- le caratteristiche delle VLAN
- la differenza tra VLAN port based e tagged

Virtual LAN

Una Virtual LAN, meglio conosciuta come ◀ VLAN ▶, è una LAN realizzata *logicamente* grazie allo standard 802.1Q che definisce le specifiche che permettono di definire più reti locali virtuali (VLAN) distinte, utilizzando e condividendo una stessa infrastruttura fisica.

◀ Anche chiamata dominio di broadcast, è un segmento della rete all'interno del quale diversi host appartenenti a una stessa subnet comunicano tra di loro senza dover necessariamente passare da un router, appartenendo alla stessa VLAN. Prima della diffusione degli switch veniva utilizzato anche il termine dominio di collisione, tuttavia dato che lo switch elimina le collisioni, l'attenzione si è spostata sul traffico broadcast. ▶

Ciascuna VLAN si comporta come se fosse una rete locale separata dalle altre dove i pacchetti broadcast sono confinati all'interno di essa.

Possiamo affermare che la comunicazione a livello 2 è confinata all'interno della VLAN e la connettività tra diverse VLAN può essere realizzata solo a livello 3, attraverso il routing.

Le VLAN riguardano il livello 2 mentre le subnet interessano il livello 3: generalmente c'è una corrispondenza biunivoca tra VLAN e sottorete che viene definita con l'assegnazione delle porte dello switch, dato che la maggior parte degli switch moderni con un adeguato numero di porte sono in grado di gestire le VLAN.

In generale le VLAN consentono una maggiore agilità di manutenzione e modifica delle infrastrutture di rete, consentono di aggiungere dispositivi senza dover spostare cavi, riposizionare apparati di rete, semplicemente tramite strumenti software, inoltre riducono il traffico, isolando il broadcast. Vediamo i principali vantaggi delle VLAN.

- Economicità: attraverso uno switch di livello 3, è possibile effettuare routing tra le diverse VLAN.
- Scalabilità: l'espansione della rete diventa semplice ed economica, le VLAN si possono estendere su diversi switch, spostando semplicemente una porta o un cavo patch.
- Ottimizzazione dell'uso delle infrastrutture: per isolare una subnet non è necessario aggiungere uno switch e/o un router, ma riassegnare alcune porte.
- Possibilità di estensione oltre i limiti fisici di un singolo switch: una LAN può venire estesa, ad esempio su piani diversi, utilizzando un'unica dorsale di collegamento.

Usare una VLAN per isolare ad esempio il DMZ dalla Trusted LAN, potrebbe essere vulnerabile a un attacco di tipo Spoofing. Esistono diversi tipi di attacco a questo livello, sostanzialmente però tutti tendono a catturare i dati che passano su VLAN diverse, sfruttando eventuali configurazioni errate presenti sulle porte di trunk. Le porte di trunk, come vedremo, hanno accesso ai dati di tutte le VLAN. Per isolare le zone di una LAN è preferibile utilizzare, come vedremo in seguito, un firewall.

Realizziamo una VLAN

Per realizzare una VLAN è necessario che gli switch della infrastruttura di rete siano capaci di distinguere le diverse VLAN esistenti: questo avviene per mezzo dello standard 802.1Q.

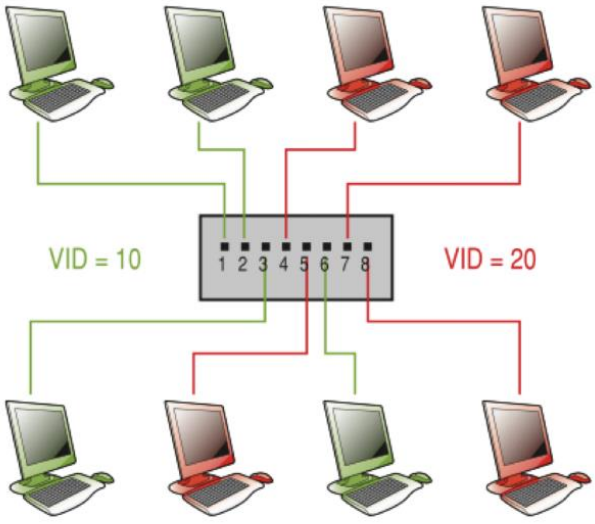
La realizzazione di VLAN può avvenire secondo due modalità:

- VLAN port based (untagged LAN o private VLAN);
- VLAN tagged (802.1Q).

Le VLAN vengono distinte, le une dalle altre, attraverso un nome, un numero identificativo chiamato VID (Virtual Identificator), compreso tra 1-4094 e un proprio blocco di indirizzi IP.

Una delle applicazioni più semplici realizzate tramite una VLAN è quella di "tagliare" un unico switch fisico in due o più reti diverse.
La figura seguente mostra due reti isolate attraverso l'utilizzo di un unico switch:

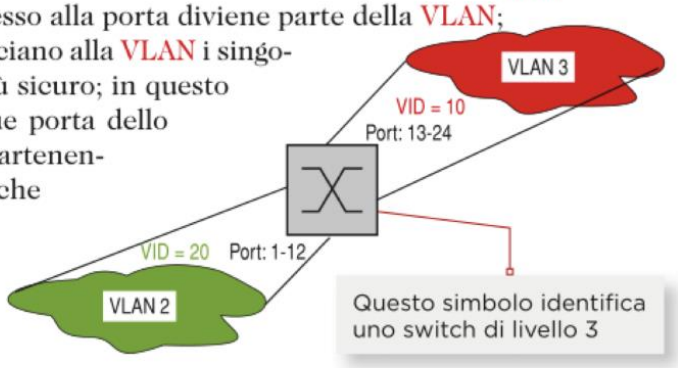
Ⓐ la rete rossa è una VLAN con VID 20 e collega i 4 host (porta 4,5,7,8);
Ⓑ la rete verde è una VLAN con VID 10 e collega i 4 host (porta 1,2,3,6).



Gli host di colore verde "vedono" soltanto gli host di colore verde, così come gli host rossi "vedono" solo quelli rossi. Senza la presenza di una VLAN sarebbe necessario utilizzare due switch diversi, uno per ogni VLAN.

Una volta definita una VLAN, ci sono sostanzialmente due tecniche per associarvi degli host:

- usando i numeri di porta dello switch: potremmo decidere che la prima metà delle porte è riservata agli host della VLAN 20 e le rimanenti per quelli della VLAN 10; questo è il sistema più semplice ma ha grossi limiti di sicurezza in quanto il concentratore associa una sua porta alla VLAN e non a un host: qualunque "dispositivo" venga connesso alla porta diviene parte della VLAN;
- usando gli indirizzi di rete degli host: se si associano alla VLAN i singoli indirizzi degli host si realizza un sistema più sicuro; in questo caso un host viene collegato a una qualunque porta dello switch dato che viene riconosciuta la sua appartenenza alla VLAN o per mezzo del suo indirizzo IP, che sappiamo però poter essere modificabile in qualsiasi momento, oppure l'indirizzo MAC, che è unico e immutabile per ogni interfaccia.



ESEMPIO

Switch a 48 porte

Se abbiamo a disposizione uno switch a 48 porte potremmo assegnare le porte nel modo seguente:

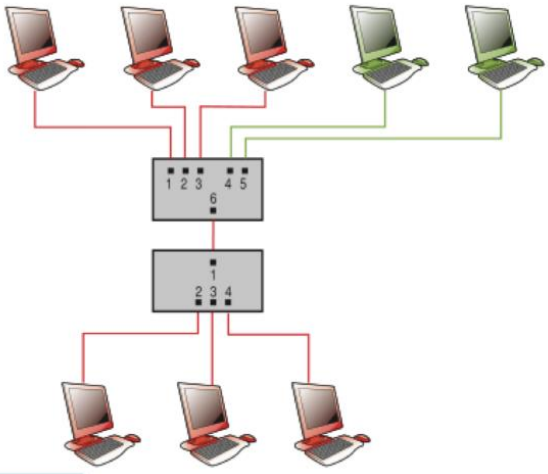
- le porte da 1 a 30 per la VLAN principale, con i client e i server di dominio (ad esempio rete alunni);
- le porte da 31 a 35 per una VLAN di stampanti con routing verso la LAN;
- sulle porte restanti si potrebbe definire una VLAN completamente separata per ospitare una rete riservata ai docenti e/o alla segreteria, che non si vuole condividere con il resto della popolazione scolastica.

Port based VLAN (untagged)

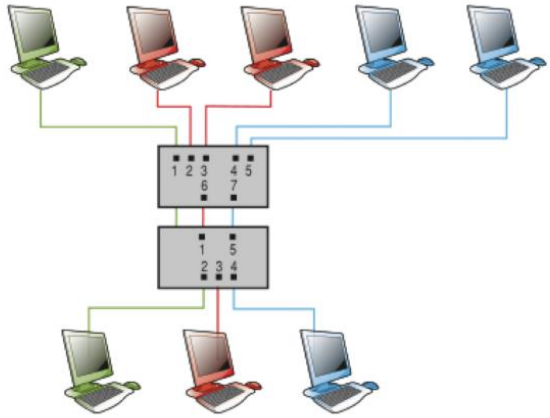
Questo metodo utilizza i numeri delle porte dello switch per realizzare VLAN differenti. Ciascuna porta prende anche il nome di Access port.

ESEMPIO

In questo esempio abbiamo due VLAN, una delle quali è limitata a un singolo switch.



In questo secondo esempio abbiamo tre VLAN e ciascuna crea una connessione "virtuale" tra i due switch.



Le operazioni che devono svolgere gli switch sono particolarmente semplici:

- ingress: un frame in ingresso appartiene alla VLAN a cui è assegnata la porta, quindi non è richiesto nessun altro "meccanismo "di riconoscimento di appartenenza sul frame;
- forwarding: il frame può essere inoltrato solo verso porte appartenenti alla stessa VLAN a cui appartiene la porta di ingresso che è mappato in un forwarding database, distinto per ogni VLAN;
- egress: una volta determinata la porta (o le porte) attraverso cui deve essere trasmesso il frame, questo può essere trasmesso così come è stato ricevuto, senza che venga modificato.

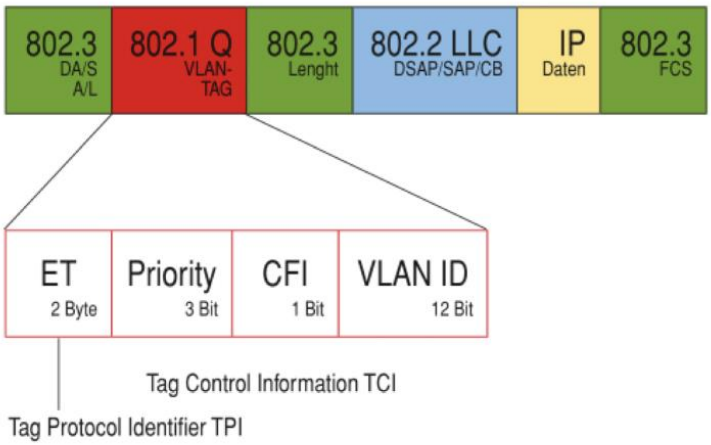
VLAN 802.1Q (tagged VLAN)

La tecnologia che permette di far condividere una VLAN a due o più switch mediante una modifica del formato del frame ethernet è quella che utilizza lo standard 802.1Q, la quale aggiunge 4 byte (TAG) che trasportano le informazioni sulla VLAN e altre aggiuntive. Ciascuna porta tagged prende anche il nome di porta di Trunk.

> Quando un pacchetto con tag VLAN n entra in una porta tagged se quella porta è tagged VLAN n, viene fatto passare, altrimenti viene scartato. Una volta che il pacchetto entra su una porta tagged può essere indirizzato solo sulle porte tagged e untagged della stessa VLAN n; se il pacchetto esce da una porta tagged sarà taggato come VLAN n, se invece esce da una porta untagged sarà privato del VLAN tag.

I primi 2 byte sono chiamati Tag Protocol Identifier (TPI) e contengono il tag EtherType (valore 0x8100), numero che evidenzia il nuovo formato del frame. I successivi 2 byte sono chiamati Tag Control Information TCI (o VLAN Tag), così strutturati:

- user_priority: campo a 3 bit che può essere utilizzato per indicare un livello di priorità per il frame;
- CFI: campo di 1 bit che indica se i MAC address nel frame sono in forma canonica;
- VID: campo di 12 bit che indica l'ID delle VLAN; con 12 bit possono essere definite 4096 VLAN: la prima (VLAN 0) e l'ultima (VLAN 4095) sono riservate, quindi gli ID realmente usabili sono 4094.

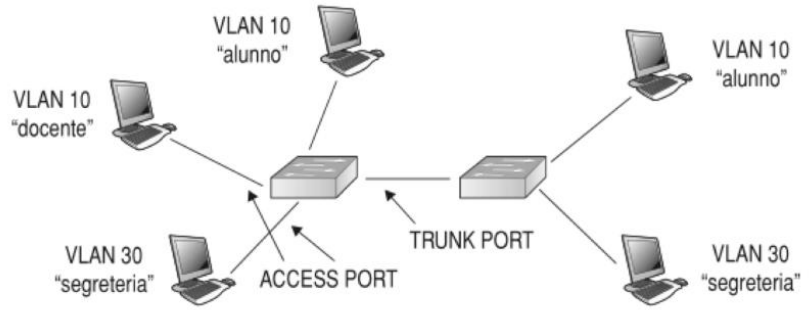


> Con queste "aggiunte" è possibile che il frame possa superare la lunghezza di 1518 byte, limite massimo dello standard Ethernet: gli switch che ammettono standard 802.1Q devono poter accettare frame con 2 byte in più.

I pacchetti con questo formato non possono arrivare su qualsiasi porta dello switch in quanto questo deve essere in grado di interpretarli: è necessario avere una classificazione anche delle porte, che possono essere distinte in porte trunk/tagged e porte untagged:

- se la porta è associata a una VLAN "port based" (untagged) i frame ricevuti da quella porta non necessitano (e non trasportano) tag TPI e TCI, né dovranno trasportarla i frame in uscita; queste porte sono chiamate porte d'accesso (access port) e il link attestato su tali porte si dice access link;
- se la porta è associata a una o più VLAN in modalità tagged, i frame trasporteranno le informazioni di TAG e la VLAN di appartenenza del frame è definita dal valore inserito nel TAG: queste porte sono chiamate porte Trunk e il link associato a tali porte si dice trunk link.

Osservando la rete rappresentata nella figura possiamo sicuramente affermare che le porte che connettono i due switch devono essere trunk in quanto in esse circoleranno frame di più VLAN.



Porte ibride

Lo standard VLAN 802.1Q richiede che una porta deve poter essere utilizzata in entrambe le modalità cioè deve poter essere associata a una VLAN in modalità untagged oppure ad altre VLAN in modalità tagged: in questo caso si parla di hybrid port.
Questa porta, come primo passo, riconosce se nel frame vi sono i tag TGI e TCI: se questi non sono presenti, il frame è del tipo untagged e quindi la porta funzionerà in tale modalità, se invece sono presenti, questi vengono analizzati e la VLAN di appartenenza viene individuata dal valore del VID.

> La VLAN a cui la porta è associata in modalità untagged viene anche detta PVID (Private Vlan ID).

Le operazioni che devono svolgere gli switch in questi casi sono diverse da quelle descritte per le VLAN untagged:

- ingress: per prima cosa lo switch deve riconoscere il tipo di frame e identificare la VLAN di appartenenza e quindi:
  - se il frame è untagged, la VLAN di appartenenza è identificata con la VLAN a cui la porta è associata in modalità untagged;
  - se il frame è tagged, la VLAN di appartenenza viene identificata dai TAG;
- forwarding: una volta identificata la VLAN di appartenenza vengono applicate le regole di forwarding e viene identificata la porta di uscita:
- egress: in questo caso può essere necessario effettuare l'inserimento e la rimozione dei TAG:
  - se il frame in ingresso è di tipo 802.1Q e la porta in uscita è associata alla VLAN di appartenenza in modalità tagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è untagged e la porta in uscita è associata alla VLAN di appartenenza in modalità untagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è di tipo 802.1Q e la porta di uscita è in modalità untagged è necessario rimuovere la TPI e TCI prima di effettuare l'inoltro;
  - se il frame in ingresso è di tipo 802.3 e la porta di uscita è associata alla VLAN di appartenenza in modalità tagged è necessario inserire TPI e TCI prima di effettuare l'inoltro.

> Negli ultimi due casi lo switch deve ricalcolare il valore del CRC del frame prima di ritrasmetterlo.

Naturalmente in una rete possono coesistere apparati che non supportano il protocollo 802.1Q: questi saranno connessi su porte dello switch associate esclusivamente a una VLAN in modalità untagged in modo che ogni frame ricevuto sarà associato a una VLAN e nessun frame di tipo 802.1Q sarà inoltrato verso l'apparato a valle, in quanto prima di arrivare al frame vengono rimossi i TAG.
In questo modo non è necessario sostituire tutto l'hardware esistente nel caso si voglia realizzare una VLAN: basta inserire in modo opportuno solo alcuni apparati 802.1Q e integrarli con l'hardware esistente, senza doverlo sostituire.
Anche le schede di rete presenti sugli host devono essere compatibili, e generalmente non lo sono: deve inoltre essere installato l'apposito driver e, infine, è necessario che il sistema operativo fornisca la possibilità di utilizzare le VLAN.

> È buona norma non utilizzare le VLAN per isolare le diverse zone della rete, ad esempio per ospitare una DMZ, perché il traffico tra le VLAN è spoofabile, cioè facilmente falsificabile: è quindi sempre meglio affidarsi a un firewall per isolare le zone tra le quali la sicurezza del traffico è un fattore critico.