

2 LE RETI LOCALI VIRTUALI (VLAN)

2.1 Dominio di broadcast

Nella Lezione precedente si è visto come l'impiego di switch in una LAN consenta di segmentare la rete in domini di collisione separati. Oltre a ciò, è utile avere anche domini di broadcast separati, in modo da poter implementare tra i diversi segmenti di rete funzioni tipiche del livello Network, come la sicurezza o la qualità del servizio.

Il **dominio di broadcast** di una rete è un insieme di computer che riceve un messaggio di broadcast trasmesso da uno di essi.

La **TABELLA 1** mostra come l'impiego di apparati di rete diversi (hub, switch o router) comporti un diverso rapporto con i domini di collisione e di broadcast.

apparato di rete	dominio di collisione	dominio di broadcast
hub	uno per tutte le porte	uno per tutte le porte
switch	uno per ogni porta	uno per tutte le porte
router	uno per ogni porta	uno per ogni porta

TABELLA 1 Descrizione dei domini per tipo di apparato

La tipica configurazione di uno switch prevede quindi che tutti gli host collegati a esso siano parte dello stesso dominio di broadcast, mentre vi possono essere molti domini di collisione. Infatti una coppia di host che comunica tramite lo switch forma un singolo dominio di collisione, di conseguenza con gli switch non si eliminano del tutto le collisioni (se due host vogliono inviare l'uno all'altro un messaggio esattamente nel medesimo istante, si avrà ancora una collisione).

Se quindi le collisioni non sono più un problema nelle reti che usano switch, il fatto che questi inoltrino su tutte le porte un messaggio di broadcast può generare molto traffico su reti con centinaia di host.

Per ovviare a questo problema, gli switch attuali offrono due diverse tecnologie:

- 1. Virtual LAN (VLAN):** si creano delle sottoreti nella rete locale che, in realtà, esistono solo sugli switch. La rete rimane configurata con la stessa topologia fisica, mentre cambia la topologia logica; quando un computer su una data sottorete invia un messaggio broadcast, esso verrà trasmesso solo ai computer appartenenti a quella sottorete e non a tutta la rete locale;
- 2. Layer 3 switching:** quando un host su una VLAN deve comunicare con un host su un'altra VLAN, è necessaria la presenza di un router che interconnette le due VLAN, dopo di che intervengono i rispettivi switch (questo processo viene anche detto: *route once, switch many*). Se invece si usano switch con funzionalità di routing, detti **switch Layer-3** (il riferimento è al livello 3 del modello OSI che si occupa dell'instradamento dei pacchetti), non è più necessario avere un router, in quanto questi switch sono in grado di leggere l'indirizzo di rete contenuto nel pacchetto e individuare verso quale switch inviare i pacchetti. In questo modo viene minimizzata l'attività di routing tra VLAN, effettuandola solo quando è assolutamente necessario.

2.2 Vantaggi e svantaggi delle VLAN

La segmentazione e l'isolamento del traffico che si realizzano con le VLAN consentono di ridurre il traffico non necessario, migliorando notevolmente le prestazioni di rete. Questo importante vantaggio compensa la difficoltà nel configurare le VLAN, attività che richiede un notevole lavoro di pianificazione e realizzazione.

Con le VLAN, infatti:

- è semplice aggiungere, cambiare o spostare gli host sulla rete;
- si definiscono più domini di broadcast, di dimensioni ridotte, all'interno di una stessa rete locale switched, e questo implica un miglioramento delle prestazioni della rete;
- migliora la sicurezza della rete;
- riduce i costi relativi agli apparati di rete impiegati.

Le VLAN non sono da considerarsi una soluzione alternativa alle reti con router per realizzare la comunicazione tra reti differenti (internetworking).

2.3 Creazione di una VLAN

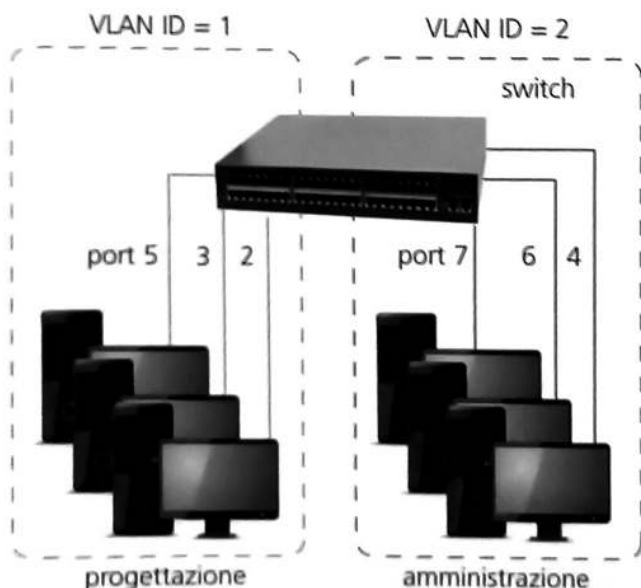
#prendinota

Quando si configura una VLAN, la topologia logica è indipendente da quella fisica.

Una **Virtual Local Area Network** (VLAN) è un insieme di computer, stampanti, server o altri device di rete che sono trattati come se fossero collegati a una singola rete, mentre, in realtà, si trovano su LAN fisiche diverse.

La tecnica di realizzazione delle VLAN permette di raggruppare, per esempio, una o più porte di uno switch in modo da considerarle parte di una stessa rete virtuale alla quale possono essere aggiunte porte di altri switch.

A ogni host della LAN può essere assegnato un numero identificativo (**VLAN ID**) per identificare la VLAN di appartenenza (FIGURA 5). Host con lo stesso VLAN ID si comportano come se si trovassero nella stessa rete fisica.



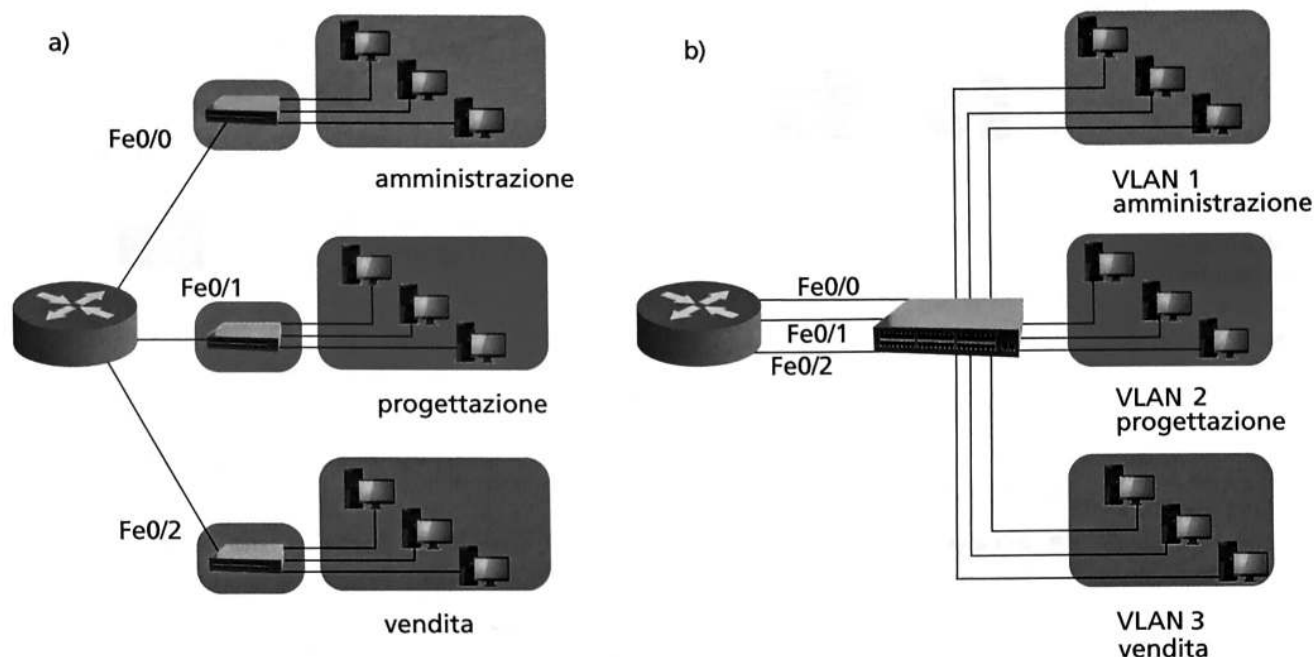
Una VLAN può essere creata in più modi:

- per **gruppi di porte**, a questo scopo si utilizza l'identificativo della porta; è la modalità più comune ed è tipica delle LAN che utilizzano un indirizzamento dinamico a livello Network (per esempio tramite il protocollo DHCP, Dynamic Host Configuration Protocol, per l'assegnazione degli indirizzi IP);
- per **utenti**, tramite l'indirizzo fisico (MAC) dell'host; questa modalità è poco usata in quanto più difficile da gestire;
- per **protocolli**, la modalità è simile alla precedente, ma invece di indirizzi fisici usa indirizzi logici (per esempio l'indirizzo IP); da quando si è diffuso l'uso del DHCP per assegnare gli indirizzi IP non è più comunemente usata.

Vediamo con un esempio cosa significa che le VLAN permettono di raggruppare dispositivi indipendentemente dalla loro locazione fisica.

Supponiamo di dover suddividere una rete LAN in 3 aree distinte che corrispondono a 3 diversi gruppi di utenti: gli amministrativi, i progettisti e i venditori.

La FIGURA 6 mostra due diverse soluzioni per realizzare la segmentazione di rete richiesta da questo scenario:



- a) la LAN è divisa in 3 segmenti di rete realizzati tramite l'impiego di 3 switch;
 b) la LAN è divisa in 3 segmenti di rete realizzati tramite la configurazione software di 3 VLAN.

Si noti che affinché un membro del personale di vendita della VLAN 3 possa condividere delle risorse con il dipartimento della progettazione della VLAN 2, è necessario introdurre un router o scegliere uno switch Layer-3.

Tra router e switch occorrono, però, tante linee quante sono le VLAN definite, quindi sul router deve essere configurata un'interfaccia per ogni VLAN. In questa modalità, il traffico fluisce attraverso il router come se si usassero LAN fisiche e non virtuali. Dal momento che un router deve effettuare maggiori elaborazioni sui pacchetti rispetto a uno switch, le prestazioni che offre questa realizzazione dipendono da quanto traffico rimane all'interno di una singola VLAN e quanto deve essere instradato verso altre VLAN.

Inoltre, dedicare un'interfaccia per ogni VLAN realizzata richiede di riservare un certo numero di porte sia sullo switch che sul router; spesso però i router di fascia bassa non hanno un elevato numero di porte Ethernet, quindi si dovrebbe scegliere un router più costoso.

Un'alternativa a questa realizzazione è quella di usare un trunk.

2.4 VLAN Trunking

Un metodo per permettere la comunicazione tra host collocati in VLAN diverse è di realizzare tra switch e router, oppure tra switch e switch, un canale comune, detto **trunk**, sul quale far transitare le comunicazioni tra VLAN diverse (FIGURA 7).

Di norma per realizzare questo collegamento si sceglie la porta più veloce disponibile sull'apparato di rete, in quanto sarà usato per trasportare grossi volumi di traffico.

FIGURA 6 (a) Rete locale segmentata con 3 switch;
 (b) rete locale con uno switch e 3 VLAN

#prendinota

Il concetto di **trunk** ha origine nella tecnologia radio, dove rappresenta una linea di comunicazione che trasporta più canali con segnali radio.

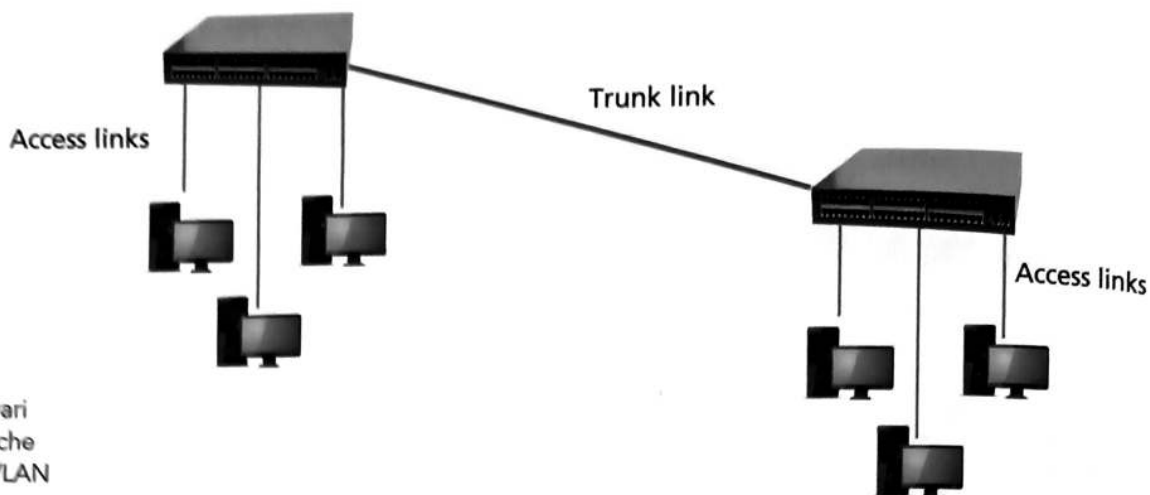


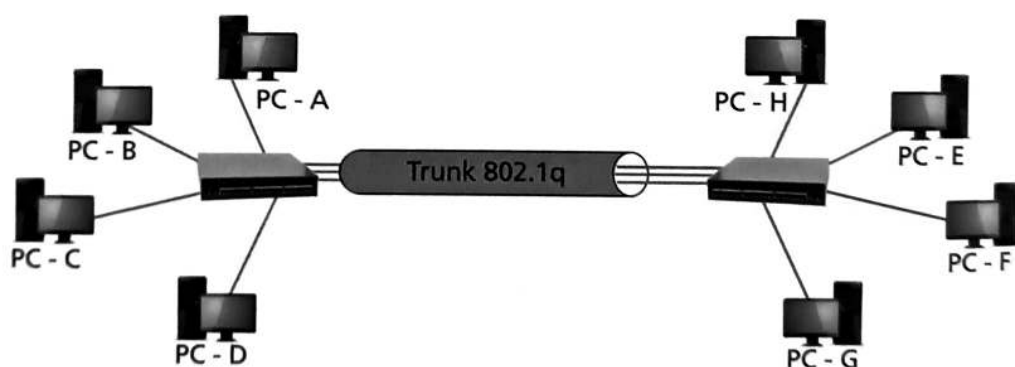
FIGURA 7 Le VLAN si possono estendere tra vari switch utilizzando trunk che convogliano traffico di VLAN diverse

Nella Figura 7 vengono evidenziati i due tipi di collegamento presenti nelle reti VLAN:

- **access link:** si tratta di un collegamento che fa parte di una sola VLAN; un computer collegato tramite questo tipo di link diventa parte di un dominio di broadcast e può comunicare solo con gli altri computer di questo dominio, a meno che il pacchetto da trasmettere sia inoltrato verso un router; il computer non è consapevole di appartenere a una VLAN, in quanto lo switch rimuove ogni informazione a essa relativa prima di inviargli il pacchetto;
- **trunk link:** è un collegamento punto-punto sul quale transita il traffico appartenente a VLAN diverse (fino a 4096); può essere usato tra due switch, tra uno switch e un server o anche tra uno switch e un router.

La FIGURA 8 visualizza un trunk attraverso il quale transitano le comunicazioni relative a 3 diverse VLAN.

FIGURA 8 Rappresentazione di un trunk usato per mettere in comunicazione 3 diverse VLAN



#preindinota

Affinché uno switch possa inoltrare il messaggio al destinatario tramite un trunk, esso deve contenere un riferimento alla VLAN di appartenenza del computer di destinazione; la tecnica usata prevede l'uso di un **tag** e viene detta **VLAN tagging**.

Il frame Ethernet non prevede un campo per effettuare il **tagging delle VLAN** (le VLAN sono state inventate successivamente), esistono quindi vari metodi per associare un tag ai messaggi (frame) inviati sul trunk; per esempio, Cisco ha definito, per alcuni suoi switch, il protocollo Inter-Switch Link (ISL) e 3COM il protocollo Virtual LAN Trunk (VLT).

Attualmente, però, si tende ad abbandonare i protocolli proprietari, preferendo a questi degli standard internazionali.

Lo standard definito a livello internazionale, quindi protocollo non proprietario, è: **IEEE 802.1q**.

IEEE 802.1Q

Questo standard prevede di inserire un campo di 4 byte per la gestione del tag (FIGURA 9), suddiviso come di seguito indicato.

- **Tag Protocol ID (TPID)**, 2 byte, usato per identificare il frame come un frame IEEE 802.1q (il valore è 0x8100).
- **Tag Control Information (TCI)**, 2 byte, così suddiviso:
 - **User Priority**, 3 bit, indica il livello di priorità del frame; va da 1, bassa priorità, a 7, alta priorità. Lo zero indica nessuna priorità (best effort).
 - **Canonical Format Indicator (CFI)**, 1 bit, usato in passato per indicare se gli indirizzi nel frame erano in forma canonica, ora è chiamato **Drop Eligible Indicator (DEI)** e, usato insieme a User Priority, segnala i frame da scartare (drop) in caso di congestione in rete;
 - **VLAN ID**, 12 bit, indica a quale VLAN appartiene il frame (ID = 0 e ID = 4096 sono riservati).

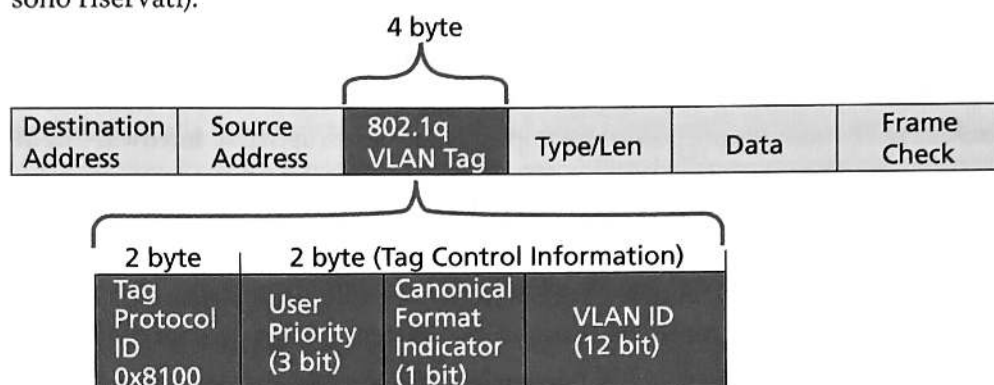


FIGURA 9 Frame Ethernet modificato con l'inserimento del campo per il tagging delle VLAN

VLAN TRUNKING PROTOCOL (VTP)

In reti complesse, la gestione delle VLAN richiede molto tempo e si possono commettere facilmente errori. Una soluzione a questo problema è l'utilizzo del protocollo **VTP** (VLAN Trunking Protocol), proprietario Cisco, che permette di gestire centralmente su uno switch i nomi e i membri di una VLAN e poi distribuire in automatico la configurazione sugli altri switch.

Dal punto di vista del protocollo VTP, gli switch si suddividono in:

- **VTP server**: switch sui quali si effettuano le modifiche di configurazione delle VLAN;
- **VTP client**: switch ai quali sono propagati i cambiamenti effettuati sui VTP server;
- **VTP transparent**: switch che ricevono e inoltrano gli aggiornamenti, ma non li applicano alla propria configurazione; eventuali modifiche su questi switch dovranno essere fatte manualmente.

Nella Lezione 7 vedremo come realizzare delle VLAN con trunk e come STP risolva i loop mediante un'esercitazione con Cisco Packet Tracer.

FISSA LE CONOSCENZE

- Che cos'è una VLAN?
- In quale standard si trovano le specifiche per le VLAN?
- In che modo è possibile comunicare tra VLAN?
- Spiega l'uso di trunk con le VLAN.



Case study
Progettazione di una rete con 3 VLAN