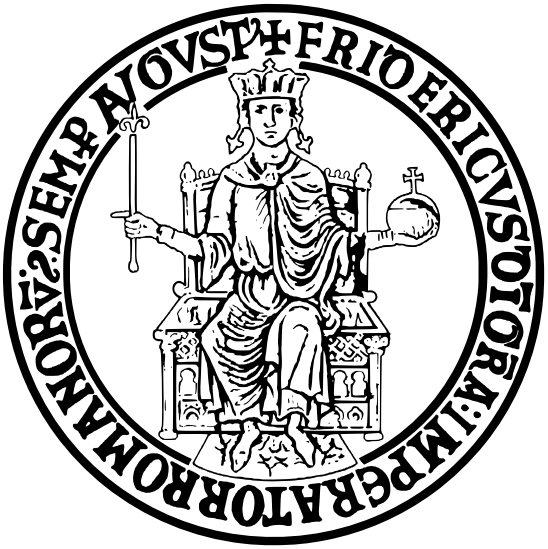
VLAN - Virtual Local Area Network

Ivan De Marino
566/2145



4 febbraio 2006

Indice

Capitolo 1

Introduzione alle VLAN

1.1 Una prima definizione di VLAN

Una Virtual LAN, meglio conosciuta come VLAN, é una LAN realizzata *logicamente*: la sua struttura fisica non é quella di una normale rete di computer locale (in inglese, *Local Area Network - LAN*) ma una astrazione (realizzata in hardware o in software, vedremo poi bene come) che permette a computer, anche collocati in luoghi non vicini fisicamente, di comunicare come se fossero sulla stesso *dominio di collisione*.

1.2 Background

Per parlare di VLAN é necessaria la conoscenza di cosa sia una *LAN*, dei problemi legati ai *Domini di Collisione*, del modo di funzionare del *CSMA/CD*: l'appendice A contiene documentazione sufficiente a tale scopo.

1.3 Cos'é una VLAN?

Una VLAN é una rete di computer che si comportano come se fossero connessi allo stesso cavo, malgrado essi siano connessi a diversi segmenti di LAN (quindi, su differenti **Domini di Collisione** (vedi A.2)). Il Network Administrator può configurare VLAN sia tramite software, sia tramite hardware, che le rende estremamente flessibili (vedi anche 1.5). Uno dei più grossi vantaggi delle VLAN emerge quando un computer viene fisicamente cambiato di locazione: esso rimane comunque collegato alla stessa VLAN senza alcuna riconfigurazione dell'hardware.

Il mondo delle VLAN é attualmente dominato dall'**IEEE 802.1Q** *tagging protocol* (vedi 2.1). Prima di esso esistevano già altri protocolli proprietari, come l'**ISL di Cisco** (*Inter-Switch Link*, una variante dell'IEEE 802.10) (vedi 2.2) e il **VLT di 3Com** (*Virtual LAN Trunk*). Attualmente si tende ad abbandonare i protocolli proprietari in favore dell'802.1Q.

Inizialmente i progettisti di rete configuravano le VLAN con lo scopo di ridurre le dimensioni del Dominio di Collisione in un ampio segmento Ethernet, aumentando di conseguenza le performance globali. Quando però gli Switch fecerò scomparire questo problema poiché, in pratica, il Dominio di Collisione era simulato e non più reale, l'attenzione fu rivolta a ridurre le dimenzioni del **Dominio di Broadcast** (vedi **A.2.1)** al livello MAC.

Le VLAN possono essere utili anche allo scopo di *restringere* l'accesso a delle risorse, senza bisogno di modificare la topologia fisica della rete[1].

Le VLAN operano al livello 2 (il Data Link Layer) dello **Stack ISO/OSI**[2][4]. E' possibile però configurare delle VLAN costruite mappando direttamente gli indirizzi IP, o delle sottoreti intere, coinvolgendo, di fatto, anche il livello 3 (il Network Layer).

Nel contesto delle VLAN, il termine "**trunk**[3]" denota un collegamento della rete che trasposta VLAN multiple, identificate tramite etichette (dette "`tag`") inserite nei loro pacchetti (vedi 2.1 per maggiori dettagli). Ogni "trunk" deve passare attraverso le "`tagged-port`" di una device abilitata alle VLAN: spesso si tratta collegamenti Switch-Switch o Switch-Router.

[1] L'efficacia di questo metodo é buona ma non impossibile da aggirare: basta citare un esempio di attacco basato su una ***tecnica di IP Spoofing.***

[2] Il modello di riferimento Open Systems Interconnection (anche detto Modello di Riferimento OSI) é una descrizione stratificata astratta per protocolli di comunicazione sulle reti. E' anche detto Modello OSI a sette livelli.

[3] Erroneamente, il termine "trunk" é usato per indicare quello che Cisco definisce "channels".

1.4 Come funziona una VLAN

In pratica una VLAN viene realizzata simulando un *unico Dominio di Broadcast*: data una VLAN (che chiameremo VLAN A), i pacchetti che partono da macchine che appartengono ad A sono diretti a tutte e sole le macchine di A.

Il suo funzionamento é **semplice** e, al contempo, **potente**.

1.5 Tipi di VLAN

Possibili configurazioni Gli amminstratori di rete possono configurare VLAN in vari modi:

- a livello protocollo, usando IP, IPX, LAT, ecc.: lo Switch analizza il frame di livello 2 ed il relativo campo "`protocol`" e dirige il traffico verso la rispettiva VLAN - *coinvolti i livelli 2/3*;
- basandosi sul MAC address delle macchine: lo Switch é configurato con tabelle che raggruppano i MAC address in VLAN e dirige il traffico in base ad esse - *coinvolto il livello 2*;
- basandosi sulle subnet IP: simile alla tecnica basata su MAC, tranne appunto che si usa l'indirizzo IP - *coinvolto il livello 3*;
- basandosi sulle porte degli Switch che devono gestire la VLAN - *coinvolto il livello 1*;

Metodi di identificazione su VLAN Quando uno Switch é configurato per supportare più VLAN basate su livelli superiori al primo, esiste la necessità di identificare ogni singolo pacchetto (di livello 2 o 3, a seconda delle esigenze) per poterlo "dirigere" da e verso la propria VLAN. Per astrazione si possono indicare 2 metodologie per identificare una VLAN: il `Frame-Tagging` e il `Frame-Filtering`:

1. il `Frame-Tagging` si basa sulla modifica delle informazioni del frame di livello 2, così che lo Switch possa dirigere il traffico verso la VLAN corretta, dopo aver riportato il frame in condizioni normali - *necessità di modifica dei frame*;
2. il `Frame-Filtering` fa si che lo Switch analizzi i pacchetti di livello 2 in base ad un particolare criterio e diriga il traffico di conseguenza - *nessuna necessità di modifica dei frame*;

Capitolo 2

VLAN standard e VLAN proprietarie

2.1 Standard IEEE 802.1Q

L'IEEE 802.1Q é un progetto che appartiene alla famiglia di standard IEEE 802: il suo scopo é sviluppare un meccanismo per permettere a più reti collegate tramite Bridge/Switch di condividere *trasparentemente* lo stesso collegamento fisico di rete, senza la fuoriuscita di informazioni. IEEE 802.1Q é anche il nome del ***protocollo di incapsulamento***[1] usato per implementare questo meccanismo su reti Ethernet.

IEEE 802.1Q definisce il significato di VLAN rispetto al modello concettuale basato sul livello MAC e il protocollo IEEE 802.1D Spanning Tree[8, 9]. La documentazione ufficiale é al [10] della Bibliografia.

Questo protocollo permette anche l'intercomunicazione tra varie VLAN attraverso l'uso di dispositivi di livello 3 (come Switch Layer 3 e Router).

2.1.1 Formato dei Frame

802.1Q non incapsula il frame originale: i dispositivi che lo implementano aggiungono un header di 2 byte all'originale pacchetto Ethernet. Il campo "`EtherType`" (vedi A.3) é modificato a `0x8100`, denotando il nuovo formato del frame.

Confrontandolo con i metodi di identificazione al paragrafo 1.5, deduciamo che 802.1Q é un protocollo basato su `Frame-Tagging`.

L'header contiene i seguenti campi:

[1] Per "protocollo di incapsulamento" si intende un protocollo per le reti che si occupa di far viaggiare un protocollo (incapsulato) in un sistema incompatibile con quest'ultimo: ad esempio, il protocollo di livello 2 dell'OSI fa da incapsulamento per il livello 3.

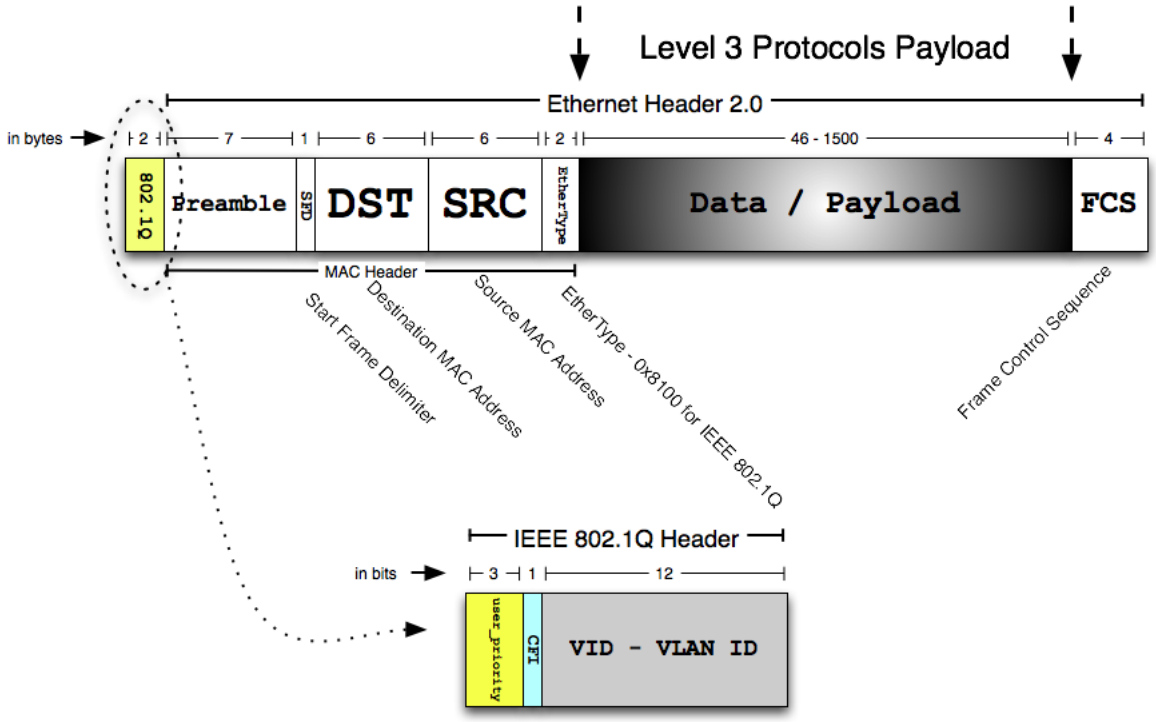


Figura 2.1: Frame 802.1Q

- **`user_priority`**: campo di 3 bit che può essere usato per indicare il livello di priorità del frame. L'uso di questo campo é definito dallo standard IEEE 802.1P;
- **`CFI - Canonical Format Indicator`**: flag da 1 bit che indica se il MAC address é in formato canonico;
- **`VID - VLAN ID`**: campo di 12 bit che identifica la VLAN. Si possono quindi indirizzare fino a $2^{12} = 4096$ VLAN.

L'aggiunta di questo header al frame Ethernet richiede ovviamente il ricalcolo del valore `CRC`[2] nel capo `FCS`[3].

2.1.2 Native VLAN

Il punto 9 dello standard definisce il protocollo usato per il multiplexing di più VLAN su un singolo collegamento, ed introduce il concetto di ***Native VLAN***. I frame che appartengono alla Native VLAN non vengono modificate quando inviati sul "trunk" della VLAN.

Esempio Immaginiamo di avere una porta .1Q[4] (chiamiamola *porta A*) con VLAN 2, 3 e 4 assegnate ad essa. Ipotiziamo che la VLAN 2 sia quella Native: i pacchetti della VLAN 2 che arrivano sulla porta A non vengono modificati con l'header .1Q, bensi restano dei frame Ethernet standard; i pacchetti che entrano nella porta A che non sono dotati di header .1Q vengono automaticamente diretti verso la VLAN 2.

Questo esempio ci fa capire che 1) la Native VLAN é, sostanzialmente, la "VLAN di default" e 2) che per ogni porta può esserci al **massimo una sola Native VLAN**.

2.1.3 GVRP - Generic VLAN Registration Protocol

IEEE 802.1Q definisce il GVRP, una applicazione del GARP (Generic Attribute Registration Protocol), che permette agli Switch di *negoziare automaticamente* l'insieme delle VLAN che devono essere create su uno specifico link.

GVRP é un protocollo di livello 2 molto utile per gli amministratori di rete: ogni volta che una VLAN viene configurata su uno Switch, il protocollo GVRP diffonde l'informazione agli altri apparati coinvolti nelle VLAN. Questo vuol dire che é sufficiente, per ogni modifica alla configurazione delle VLAN, operare su un unico Switch.

[2] "Cyclical Redundancy Check".
[3] "Frame Control Sequence".
[4] Abbreviazione di "IEEE 802.**1Q**".

Lo standard IEEE 802.1D[8] menziona l'idea di sviluppare un *protocollo per la registrazione automatica di "group membership"* attraverso dispositivi come Switch o Bridge. Attualmente, quasi tutti i dispositivi che ricoprono i livelli 2 e 3 dell'OSI implementano GVRP.

2.1.4 MSTP - Multiple spanning-tree protocol

La revisione del 2003 dello standard 802.1Q ha introdotto l'MSTP, inizialmente definito nell'IEEE 802.1S.

Il protocollo/algoritmo MSTP permette di costruire VLAN dalla topologia ad albero (quindi senza loop) anche in caso di VLAN multiple.

Se esiste una unica VLAN (ad esempio, quella Native (vedi 2.1.2)), il tradizionale STP[5] funziona in maniera appropriata. In caso di più VLAN, la rete logica configurata da un singolo STP non é più sufficiente, poiché l'algoritmo non tiene conto di tutti i possibili Spanning Tree[6][12] (d'ora in avanti "ST") ma solo di quello corrente. L'MSTP configura uno ST separato per ogni VLAN e blocca i link ridondanti all'interno di ogni ST. Per connettere i vari ST delle VLAN, costruisce un ST gerarchicamente superiore chiamato "Common ST".

2.2 Cisco ISL - Inter-Switch Link

Cisco ISL é un protocollo proprietario di Cisco che gestisce informazioni sulle VLAN come flussi di traffico tra Switch e Router.

ISL si basa sul metodo di "tagging" di Cisco ed é supportato solo da apparati attivi Cisco come Fast/Giga Ethernet Switch/Router. La dimensione del frame ISL può variare tra i 94 e i 1548 byte a causa dell'overhead del protocollo stesso.

Un protocollo sviluppato usando l'ISL é il Dynamic ISL: esso semplifica la creazione di trunk ISL tra 2 apparati Cisco Fast Ethernet connessi. In sostanza, é possibile creare un trunk VLAN basato su ISL semplicemente configurando uno solo degli estremi del canale Ethernet: DISL si occuperà di configurare da remoto l'altro apparato.

Cisco ISL ha contribuito sostanzialmente per lo sviluppo dello standard IEEE 802.1Q (vedi 2.1).

2.2.1 Cisco VTP - VLAN Trunking Protocol

Il protocollo VTP[6] é usato per configurare e gestire VLAN su apparati Cisco. VTP può essere configurato su Switch Cisco in tre modalità:

- Client
- Server
- Transparent

L'amministratore di rete può modificare la configurazione delle VLAN solo sugli Switch in modalità "Server". Dopo che le modifiche sono state applicate, esse vengono automaticamente distribuite a a tutti gli Switch del trunk VLAN: gli apparati in modalità "Transparent" reinviano le modifiche a tutti gli altri apparati ad esso collegati, scartando però la configurazione per se stessi; gli apparati in modalità "Client", invece, applicano la modifica a se stessi e la reinviano.

L'informazione viene propagato in base a mappe di raggiungibilità ST costruite dagli stessi apparati in maniera automatica (molto simile ad MSTP (vedi 2.1.4)).

Per monitorare la configurazione sui trunk VLAN si usano i "*version number*", così che un apparato in modalità "Client" applica la modifica a se stesso solo se risulta avere un version number maggiore di quello attuale. Per evitare conflitti, i version number vengono resettati quando si aggiunge un nuovo componente al trunk VLAN.

2.2.1.1 VLAN Pruning

VTP, usando le mappe di raggiungibilità ST, abilita il traffico diretto solo a quegli Switch che si conosce dotati di porte per la VLAN puntata: questo permette una migliore gestione del bandwidth sul trunk, migliorando le prestazioni.

[5] "Spanning Tree Protocol".
[6] "Spanning Tree" si traduce "Albero di Copertura".

2.2.1.2 VTP e Sicurezza

VTP può operare in modalità non autenticata: ne consegue che un attacker abbastanza esperto può inviare uno pacchetto VTP malevolo per modificare la configurazione delle VLAN o, peggio, dannegiarle. VTP é però anche dotato di una modalità che usa password cifrate con MD5[7] per l'autenticazione.

E' comunque chiaro che l'uso di VTP su reti ad alto rischio é sconsigliabile, malgrado la sua indubbia utilità.

[7] Una ottima documentazione sull'MD5 e sulle funzioni di Hash in generale é disponibile su Wikipedia: `http://en.wikipedia.org/wiki/Hash_function`.

Capitolo 3

Esempio d'uso delle VLAN

Analiziamo adesso una possibile situazione in cui l'uso delle VLAN può rivelarsi davvero utile: partiremo dalla descrizione di un proggetto di base in cui non rientrano le VLAN e procederemo evolvendo e migliorando l'infrastruttura logica (e fisica) della rete, concentrandoci sull'introduzione delle VLAN nel progetto.

3.1 Lo scenario

Campus universitario, una rete distribuita su quattro edifici che contengono:

- uffici di diversi dipartimenti
- gruppi di ricerca
- laboratori informatizzati
- Centri di Calcolo

Vediamo una prima soluzione basata solo su un uso "elementare" di Router e Switch.

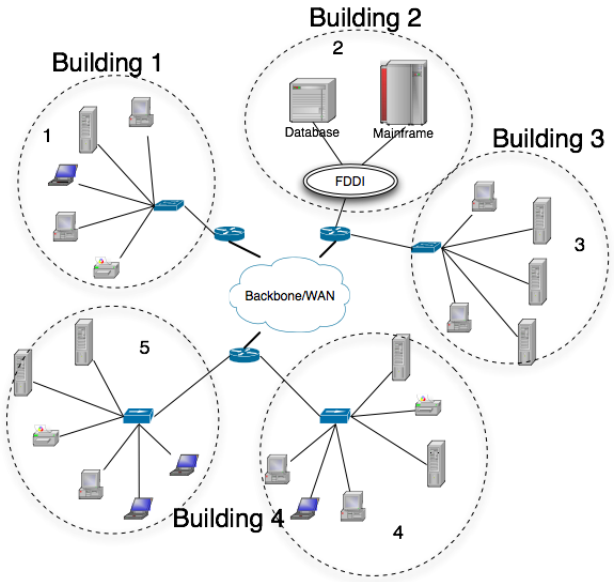


Figura 3.1: Rete basata su Router

Ogni LAN (figura 3.1) risulta separata dalle altre tramite un Router e rappresenta un Dominio di Broadcast (vedi A.2.1) a se stante. Questo comporta che, in caso di necessità di espansione della rete al fine di aumentare il numero di **End-System**[1], sarà necessario acquistare anche ulteriori Router per evitare di far crescere eccessivamente i Domini di Broadcast.

[1] E' una termine nato nell'ambito di Internet e sta ad indicare, sostanzialmente, la "macchina utente" finale in una rete. E' sinonimo di **Host**.

E' importante però sottolineare che **l'aumento del numero dei Router riduce sensibilmente le prestazioni della rete**, dati i non trascurabili tempi di latenza (*latency*) di cui soffrono questi apparati[2], soprattutto se confrontato con uno Switch della stessa fascia.

3.2 Evoluzione

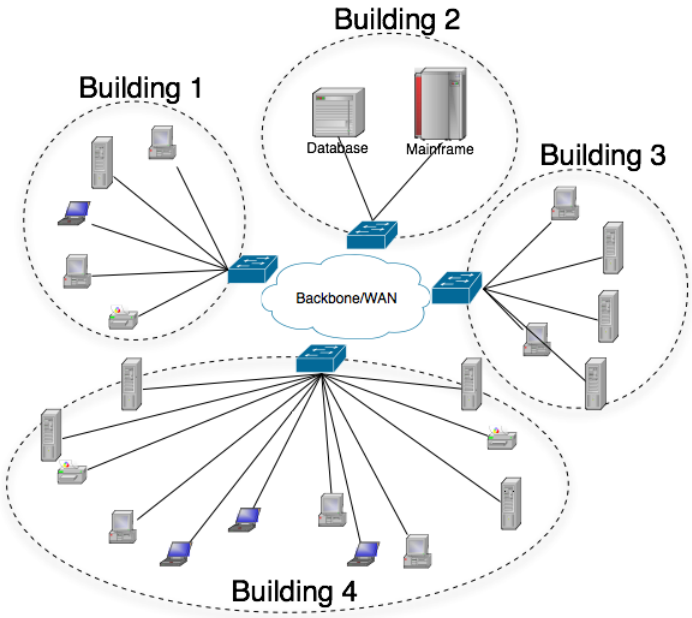


Figura 3.2: Rete basata su Switch

In questa ristrutturazione (figura 3.2) gli End-System collegati sono i medesimi e la velocità di connessione tra le sedi é aumentata grazie alle elevate capacità di una rete Full-Switched. Restano però i problemi dei Domini di Broadcast con cui non si può non fare i conti: basti pensare a tutte quelle device che fanno uso di *Broadcast* per segnalare la propria presenza (come le Stampanti di rete).

E' necessario (e desiderabile) ridurre al minimo questo problema, e, magari, aumentare la flessibilità della nostra rete che, così com'é ora, é intimamente legata alla sua struttura fisica.

[2] Il Routing é un processo che ha un suo peso nell'economia di una rete.

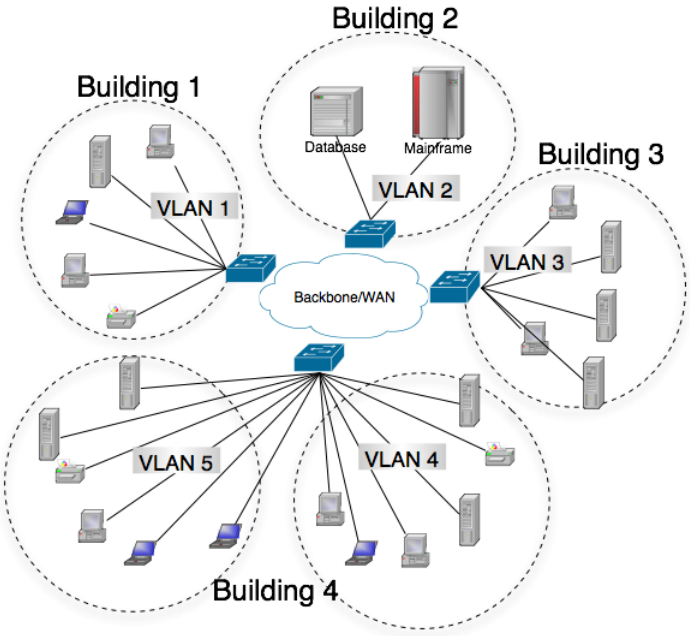


Figura 3.3: Rete basata su Switch e VLAN

Introducendo le VLAN (figura 3.3) abbiamo ripristinato la stessa topologia che si trova in figura 3.1. E' però importante notare che, in base alla marca dei prodotti scelti per realizzare le VLAN (vedi 2), cambia la modalità con cui queste VLAN possono comunicare tra di loro. Per i modelli più evoluti, é possibile passare da un dominio all'altro usanto gli Switch come dei gateway, per altri modelli può esse necessario l'utilizzo di un Router supplementare che faccia da "*bridge*" tra le varie VLAN.

3.3 Risultato

Fin'ora però il risultato ottenuto é qualcosa che, a parte la velocità, risulta essere equivalente alla soluzione iniziale: le VLAN però sono "physical-location-indipendent". Sfruttiamole quindi per migliorare sensibilmente il progetto.

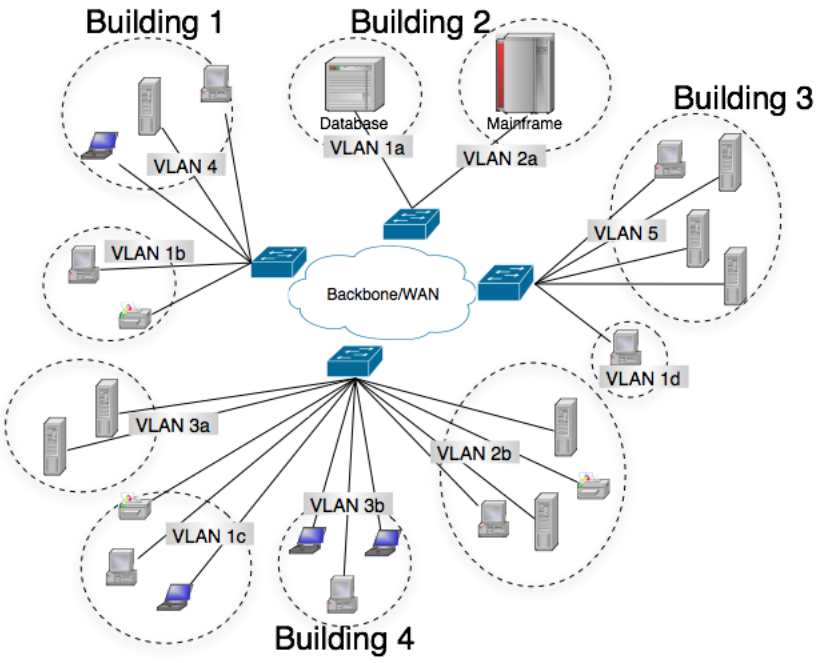


Figura 3.4: Rete basata su Switch e VLAN "logiche"

La topologia finale (figura 3.4) ha queste caratteristiche:

- *Sono disponibili 5 VLAN*:
  1. Gruppo di utenti che deve accedere al Database
  2. Gruppo di utenti che deve accedere al Mainframe
  3. Uffici di un dipartimento distribuiti su più piani o anche in edifici differenti
  4. Altro dipartimento
  5. Altro dipartimento
- *Domini di Broadcast ridotti al minimo*
- *Velocità di trasmissione é elevata*: la rete é Full-Switched
- *Sicurezza/Discrezionalità aumentata*: si possono strutturare VLAN in base agli indirizzi MAC, così da ridurre al minimo i rischi nei segmenti sensibili della rete
- *Topologia logica indipendente da quella fisica*: cambiare di posizione o aggiungere un computer non richiede riconfigurazione delle VLAN
- *Gestione e manutezione semplificata*: esistono svariati protocolli (proprietari e non) per la gestione da remoto delle VLAN
- *Costi contenuti*

3.3.1 Connettività tra le sedi

E' importante sottolineare che **la connettività tra le sedi può essere realizzata in vari modi** (Fibra Ottica, Giga Ethernet, ATM con LANE[3]), tutte dipendenti dalle esigenze e dai tipi di Switch utilizzati. Inoltre, sempre in base a questo, si può fornire connettività verso WAN pubbliche come Internet.

Evitiamo di scendere nei particolari perché questo esula dai nostri scopi.

[3]LANE[13] é un software che permette di simulare una LAN su un mezzo fisico differente come l'ATM.

Appendice A

Concetti utili

A.1 LAN

Nel campo dell'informatica LAN è l'acronimo per il termine inglese **Local Area Network**, in italiano ***rete locale***. Identifica una rete costituita da computer collegati tra loro (comprese le interconnessioni e le periferiche condivise) all'interno di un ambito fisico delimitato (ad esempio in una stanza o in un edificio (LAN casalinga o LAN ufficio), o anche in piú edifici vicini tra di loro (LAN di Campus)) che non superi la distanza di qualche chilometro. Le LAN hanno dimensioni contenute, il che favorisce il tempo di trasmissione[1], che è noto in base al tipo di rete. Le LAN tradizionali lavorano tra 10 Mb/s (*10Base-T*) e 100 Mb/s (*100Base-T*), hanno **bassi ritardi** e **pochissimi errori**. Le LAN piú recenti operano fino all'ordine dei Gb/s (*1000Base-T*), ma sono utilizzate solo in *ambienti server* e/o *storage di grosse dimensioni* (**SAN**[2]).

A.1.1 LAN basate su Standard Base-T

10/100/1000Base-T sono implementazioni dello standard **Ethernet IEEE 802.3**[3]. Usano cavi **twisted-pair**[3][4] con lunghezza massima che varia in base alla categoria del cavo (ormai quasi sempre *CAT-5E* o *CAT-6* o *CAT-7*[5]). I cavi sono più piccoli e più flessibili dei cavi coassiali[6] su cui si basano gli standard 10Base-2 e 10Base-5. I cavi degli standard Base-T usano **connettori di tipo RJ-45**.

A.2 Dominio di Collisione

Si parla di "Dominio di Collisione" nelle reti che si basano sulla **condivisione dinamica del mezzo trasmissivo**: l'espressione "dominio di collisione" si riferisce ad una parte di una rete nella quale, se due apparecchiature tentassero di trasmettere contemporaneamente, avverrebbe una collisione. Per regolamentare e ridurre le collisioni l'Ethernet usa il protocollo **CSMA/CD** (vedere **A.2.2 a pagina 14**).

La condivisione del mezzo trasmissimo tra più macchine é realizzata nelle reti con **topologia a Bus**: un solo cavo da cui "ascoltano" ed in cui "parlano" tutte le macchine della stessa rete.

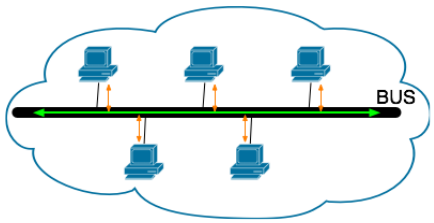


Figura A.1: Schema topologia a bus

[1] Il "tempo di trasmissione" é un **fattore fondamentale** per le reti che si basano su *condivisione dinamica a contesa del mezzo* come le reti ***Ethernet***, a loro volta basate su ***CSMA/CD.***

[2] Storage Area Network (SAN) é una rete progettata per collegare periferiche di storage come *disk array controllers*, *sistemi di registrazione su nastro*, *ampie batterie di dischi SCSI in RAID* ad uno o piú *server di produzione*. A livello Enterprise (grandi aziende e/o grandi enti) le SAN sono utilizzatissime (un esempio possono essere le Web-Farm delle società che offrono Hosting Web).

[3] Letteralmente "a coppie-ritorte".

[4] "T" sta per "twisted".

[5] "CAT" sta per "categoria".

[6] I cavi coassiali sono strutturalmente identici al cavo usato per il segnale della TV.

Nelle reti più vecchie la topologia a BUS era realizzata fisicamente; nelle reti moderne si usa la **topologia fisica a Stella ma logica a BUS**: un unico apparato accentratore, che sarà il centro della stella, ha il compito di ricevere in ingresso il segnale da tutte le macchine della rete e ritrasmetterlo.

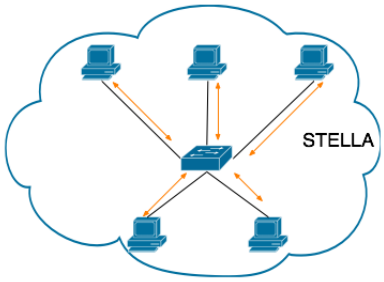


Figura A.2: Schema topologia fisica a stella e logica a bus

Il più famoso, ma ormai in disuso, apparato accentratore é l'**Hub**. Tutte le porte di un hub si trovano nello stesso dominio di collisione: esso si limita a ripetere l'informazione (anche detta **frame**[7]) che riceve a tutte le porte che possiede, indipendentemente dal fatto che il traffico sia *Unicast*, *Multicast* o *Broadcast*[8]. E' per questo che l'Hub é definito anche "*apparato passivo*": opera al *livello 1* dello Stack ISO/OSI e quindi non é dotato di "intelligenza"[9].

Oggi, come noto, esistono gli **Switch** che sono capaci di ridurre sensibilmente le collisioni, **differenziando e partizionando il traffico** in base alla destinazione, operando funzioni di **buffering** e, in generale, migliorando sensibilmente le prestazioni rispetto agli Hub. Lo Switch rientra nella categoria degli "*apparati attivi*" di rete: ci sono svariati modelli di Switch che operano tra i *livelli 2 e 3* dello Stack OSI (ma ci sono anche di quelli che arrivano ai *livelli 4-7*).

A.2.1 Segmentazione: il problema del Dominio di Broadcast

La separazione di un dominio di collisione in 2 o più domini di dimensioni ridotte prende il nome di ***segmentazione***. Si realizza utilizzando dispositivi di livello Data Link e/o Network (liv. 2 e/o 3): Bridge e Switch. Tralasciando l'approfondimento su come lavorano questi device cerchiamo di capire perchè, una volta separati i domini di collisione, possiamo ancora utilizzare le VLAN per aumentare l'efficienza della nostra rete.

Se è vero che le *reti switched* "ammorbidiscono" il problema delle collisioni riducendolo talvolta al minimo (i frame sono inoltrati **solo** sui segmenti che contengono il *destination address* del frame), rimane un altro problema da affrontare: i *domini di broadcast*. Il termine dominio di broadcast si riferisce a quella parte di una rete dove un singolo pacchetto broadcast viene trasmesso dallo switch a tutti i segmenti di rete ad esso connessi (ad es: `ARP Request`, `NetBIOS name request`, `HP-IP Print`, ...). Questo tipo di traffico broadcast colpisce l'intera rete poichè **ciascun device che riceve un frame broadcast è costretto ad analizzarlo**. E se il traffico broadcast cresce, la banda disponibile comincia a diminuire sensibilmente fino a consumarsi (dicesi *broadcast storming*). Per localizzare (o circoscrivere) il traffico broadcast si possono adottare 2 soluzioni:

[7] Un frame é un **pacchetto** di informazione che viene codificato/decodificato per viaggiare su un link.

[8] Il termine **Broadcast** si riferisce alla trasmissione di un pacchetto di informazione verso tutte le device collegate alla rete. Il broadcast é limitato ad un Dominio di Broadcast.
Unicast é, per contrapposizione a Broadcast, la trasmissione di un pacchetto verso una sola device sulla rete.
Multicast é la trasmissione verso un sottoinsieme di tutte le device collegate alla rete.

[9] Per "intelligenza" si intendono algoritmi/funzioni di ottimizzazione/miglioramento inseriti nell'hardware o nel software dell'apparato.

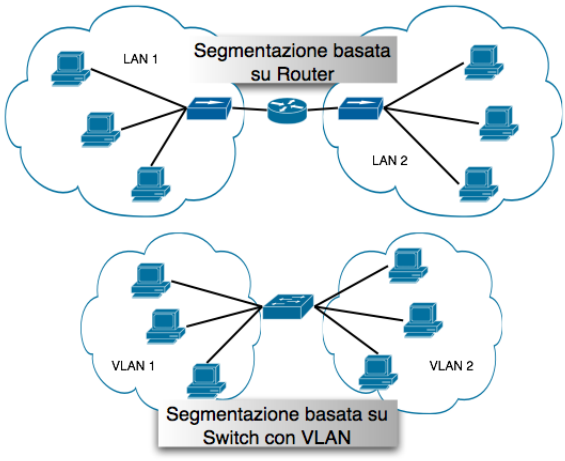


Figura A.3: Confronto segmentazione con Router e segmentazione con VLAN

1. Utilizzare dei **Router**: i Router non propagano traffico broadcast.
2. Utilizzare le VLAN: esse contengono il traffico broadcast.

La seconda soluzione é migliore sia in termine di numero di componenti necessarie, sia in termini economici.

A.2.2 Cos'é e come funziona il CSMA/CD

CSMA/CD è l'acronimo inglese di **Carrier Sense Multiple Access with Collision Detection**, ovvero *accesso multiplo tramite rilevamento della portante con rilevamento delle collisioni*. È un'evoluzione del protocollo MAC del CSMA.
È nato per la risoluzione del conflitti di trasmissione dovuti al CSMA puro.

Algorithm 1 Algoritmo del CSMA/CD

1. `L'adattatore sistema il frame in un buffer;`
2. `Se il canale è inattivo si procede alla trasmissione, se è occupato si attende prima di ritrasmettere;`
3. `Mentre si trasmette l'adattatore monitora la rete (è questo il vero e proprio Collision Detection): se non riceve segnali da altri adattatori considera il frame spedito, tale segnale si ricava confrontandolo con quello che trasmette, se i due differiscono è avvenuta una collisione, quindi va interrotta la trasmissione;`
4. `Se l'adattatore riceve, durante una trasmissione, un segnale da un altro adattatore, arresta la trasmissione e trasmette un segnale di disturbo (jam);`
5. `Dopo aver abortito la trasmissione attende in maniera esponenziale (backoff esponenziale);`
6. `Alla fine del backoff, riprende dal punto 1 o 2 (a seconda dello stato del buffer).`

L'***attesa esponenziale*** funziona in questo modo: gli adattatori aspettano un tempo casuale entro un valore massimo *d* (il protocollo che usa il CSMA/CD, ad esempio Ethernet, fissa tale valore). Se viene generata nuovamente una collisione il valore *d* viene raddoppiato, così fino a che questo è sufficientemente grande. Questa tecnica viene chiamata *recessione binaria esponenziale*. Avviene perché se altri adattatori sono contemporaneamente in attesa, tutti simultaneamente tenteranno di trasmettere provocando altre collisioni. Il segnale di disturbo (il *jam*) viene inviato per avvertire tutti gli adattatori che è avvenuta una collisione.

A.3 EtherType

`EtherType`[14] é un campo del frame Ethernet standard. E' utilizzato per indicare che protocollo é trasportato (incapsulato) nel frame Ethernet.
Una vecchia specifica Ethernet (probabilmente di Xerox) aveva un campo da 16 bit chiamato `Length`, usato per indicare la lunghezza del campo `Data`, benché la massima lunghezza del pacchetto fosse di 1500 byte. Le versioni 1.0 e 2.0 della specifica Ethernet di Digital/Intel/Xerox[10] ha anch'essa un campo di 16 bit chiamato EtherType, con la convenzione che:

[10] Questa specifica Ethernet é anche nota come **DIX**, acronimo delle 3 compagnie che l'hanno ideata.

- i valori tra 0 e 1500 indicano l'uso del formato Ethernet originale con un campo che indica la lunghezza
- i valori da 1536 in poi (0x0600 in esadecimale) (vedi tabella A.1) indicano l'uso di un nuovo formato del frame con un identificativo di sotto-protocollo EtherType

Con l'avvento della suite di standard **IEEE 802[1, 2]**, l'header SNAP[11], é usato per trasmettere l'EtherType del pacchetto per reti IEEE 802 diverse dalle Ethernet, ed anche per le reti non IEEE che usano l'header IEEE 802.2 LLC, come lo standard FDDI.
Attualmente, su reti Ethernet é utilizzata la specifica Ethernet 2.0.

EtherType[12]	***Protocollo***
0x0800	Internet Protocol, Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	**IEEE 802.1Q-tagged frame**
0x8137	Novell IPX (alt)
0x8138	Novell
0x86DD	Internet Protocol, Version 6 (IPv6)
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage

Tabella A.1: L'EtherType dei protocolli più comuni

[11] Il "**SubNetwork Access Protocol**" é un meccanismo per il *multiplexing di più protocolli*, distinguendo grazie agli 8 bit dell'IEEE 802.2 Service Access Point (SAP): é necessario quindi che i protocolli usino IEEE 802.2 LLC.

Appendice B

Licenza

Attribution-NonCommercial 2.0 Italy[15]

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works

Under the following conditions:

Attribution. You must give the original author credit.

Non-Commercial. You may not use this work for commercial purposes.

- For any reuse or distribution, you must make clear to others the licence terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.
Complete version of the Licenses here: [15].

Bibliografia

[1] IEEE 802 suite official website: http://www.ieee802.org/.

[2] IEEE 802 suite su Wikipedia: http://en.wikipedia.org/wiki/IEEE_802.

[3] The IEEE 802.3 Working Group for CSMA/CD (Ethernet) based LANs: http://www.ieee802.org/3/.

[4] Documentazione esaustiva sullo Stack ISO/OSI su Wikipedia: http://en.wikipedia.org/wiki/OSI_reference_model.

[5] Cisco Doc. - Configuring ISL Trunks on Cisco Routers: http://www.cisco.com/warp/public/473/24.shtml.

[6] Cisco Doc. - Configuring VTP and Virtual LANs: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/vlans.htm.

[7] 3Com Superstack 3 Switch 4500: http://support.3com.com/infodeli/tools/switches/4500/DUA1756-1BAA01.pdf.

[8] 802.1D MAC Bridges Standard: http://www.ieee802.org/1/pages/802.1D-2003.html.

[9] Documentazione sull'IEEE 802.1D su Wikipedia: http://en.wikipedia.org/wiki/IEEE_802.1D.

[10] IEEE 802.1Q-2003 standard: http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf. ISBN: 0-7381-3662-X.

[11] Understanding Multiple Spanning Tree Protocol (Cisco Systems): http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml.

[12] Documentazione esaustiva sullo Spanning Tree su Wikipedia: http://en.wikipedia.org/wiki/Spanning_Tree_Protocol.

[13] Cisco Documentation on LANE - LAN Emulation: http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcovlane.htm.

[14] IEEE EtherType Registration Authority: http://standards.ieee.org/regauth/ethertype.

[15] CC Licenses used for this document: http://creativecommons.org/licenses/by-nc/2.0/it/deed.en_GB.