Sistemi e Tecnologie della Comunicazione

Le Virtual LAN

1

Le virtual LAN

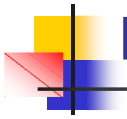
- Lo standard 802.1Q (2003) definisce le specifiche che permettono di definire piu' reti locali virtuali (VLAN) distinte, utilizzando una stessa infrastruttura fisica
- Ciascuna VLAN si comporta come se fosse una rete locale separata dalle altre
  - i pacchetti broadcast sono confinati all'interno della VLAN
  - la comunicazione a livello 2 e' confinata all'interno della VLAN
  - la connettivita' tra diverse VLAN puo' essere realizzata solo a livello 3, attraverso routing
- Lo standard e' definito nell'ambito del protocollo 802.1D (bridging) che in generale riguarda la comunicazione tra diversi standard 802 attraverso bridge
  - gli switch ethernet sono sostanzialmente bridge monoprotocollo

2

Scopo delle VLAN

- L'utilizzo delle Virtual LAN permette di realizzare
  - risparmio: non e' necessario realizzare una nuova infrastruttura di rete locale con apparati e linee dedicate per creare una nuova LAN parallela entro lo stesso ambiente della LAN preesistente
  - aumento di prestazioni: il confinamento del traffico broadcast permette di evitare la propagazione di frame verso destinazioni che non hanno necessita' di riceverlo
  - aumento della sicurezza: una utenza connessa ad una VLAN non ha modo di vedere il traffico interno alle altre VLAN
  - flessibilita': lo spostamento fisico di una utenza all'interno dei locali raggiunti dalla infrastruttura di rete puo' essere realizzato senza modifiche della topologia fisica, ma logicamente attraverso la opportuna riconfigurazione degli apparati di rete (switch o bridge)

3



Requisiti sui bridge

- Per realizzare VLAN e' necessario che gli switch ed i bridge della infrastruttura di rete siano capaci di distinguere le diverse VLAN
- Gli apparati devono quindi osservare lo standard 802.1Q
- Vi sono diversi modi per realizzare VLAN
  - VLAN port based (o private VLAN)
  - VLAN tagged (802.1Q)
- In ogni caso entro il bridge devono essere definite le VLAN, con nome e numero identificativo per distinguerle una dall'altra

4

Funzioni del bridge in 802.1Q

- Sostanzialmente esistono tre funzioni che i bridge devono saper svolgere per poter gestire piu' reti virtuali
  - ingress: il bridge deve essere in grado di capire a quale VLAN appartienga un frame in ingresso da una porta
  - forwarding: il bridge deve conoscere verso quale porta deve essere inoltrato il frame verso destinazione, in funzione della VLAN di appartenenza
  - egress: il bridge deve poter trasmettere il frame in uscita in modo che la sua appartenenza alla VLAN venga correttamente interpretata da altri bridge a valle

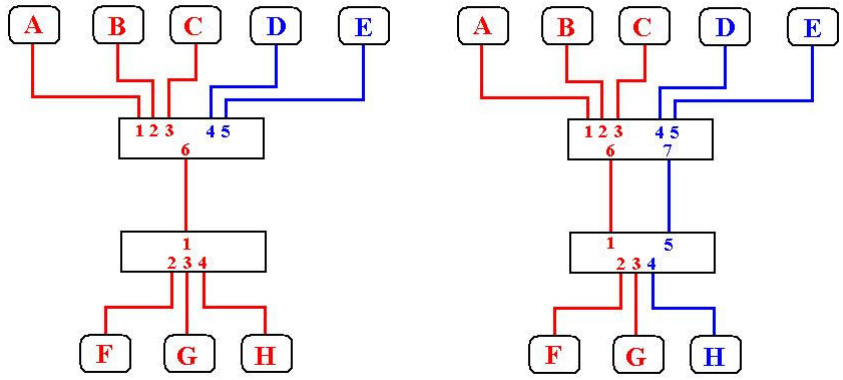
5

Port based VLAN (untagged)

- Questa tecnica prevede l'assegnazione statica di ciascuna porta del bridge ad una VLAN (definita sul bridge)
  - porte diverse possono essere assegnate a VLAN differenti
- Di fatto in questo modo si realizza un partizionamento del bridge in due o piu' bridge logici
- In questa configurazione le funzioni del bridge sono semplici:
  - ingress: un frame in ingresso appartiene alla VLAN a cui e' assegnata la porta
    - non c'e' bisogno di utilizzare indicatori di appartenenza sul frame
  - forwarding: il frame potra' essere inoltrato solo verso porte appartenenti alla stessa VLAN a cui appartiene la porta di ingresso
    - il bridge mantiene un forwarding database distinto per ogni VLAN: nessuna stazione appartenente ad una VLAN potra' essere vista attraverso una porta assegnata ad una VLAN differente
  - egress: una volta determinata la porta (o le porte) attraverso cui deve essere trasmesso il frame, questo puo' essere trasmesso cosi' com'e'
- Le VLAN untagged (dette anche private) non richiedono l'osservanza dello standard 802.1Q, ma solo che lo switch ne supporti la configurabilita'

6

Esempi di VLAN port based



7

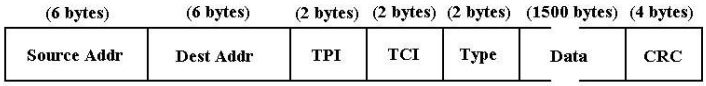
VLAN 802.1Q (tagged VLAN)

- Lo standard 802.1Q viene utilizzato per poter condividere lo stesso link fisico tra VLAN differenti
- Per poter fare cio' il bridge deve poter distinguere la VLAN di appartenenza del frame in arrivo
- Lo standard definisce una modifica del formato del frame ethernet aggiungendo 4 byte che trasportano le informazioni sulla VLAN (ed altro)
- Poiche' tutti i bridge devono concordare sulla VLAN di appartenenza di un frame, l'identificativo (VLAN tag) della VLAN deve essere uguale per tutti i bridge

8

Frame (Ethernet) 802.1Q

- Il formato del frame Ethernet secondo lo standard 802.1Q continene i campi aggiuntivi:
  - TPI (Tag Protocol Identifier): due bytes di valore 81 00 che identificano il frame come frame 802.1Q
  - TCI (Tag Control Information): due bytes che trasportano le informazioni sulla tag
    - i primi tre bit (user priority) indicano l'eventuale livello di priorita' del frame
    - il quarto bit (CFI) vale 1 se il frame proviene da una LAN token ring
    - i restanti 12 bit (VID) trasportano la VLAN tag (da 0 a 4095)
      - i valori 0 e 4095 sono riservati e non vanno utilizzati come VLAN ID



9

Considerazioni sul frame

- Il frame cosi' costituito rappresenta una violazione dello standard Ethernet, in quanto puo' eccedere la dimensione massima di 1518 bytes
  - tutti i bridge che osservano lo standard devono poter accettare frame con 2 byte in piu'
- Il campo TPI ha un valore che non e' utilizzato come "protocol type" nei frame Ethernet ordinari
  - questo permette di identificare immediatamente se un frame e' di tipo 802.1Q
  - una scheda Ethernet non conforme allo standard 802.1Q scarterebbe il frame

10

Porte tagged ed untagged

- In un bridge 802.1Q tutte le porte devono essere associate ad una o piu' VLAN
  - se la porta e' associata ad una VLAN "port based" (untagged) i frame ricevuti da quella porta non trasporteranno TAG, ne' dovranno trasportarla i frame in uscita
    - il link attestato su tali porte si dice *access link*
  - in caso contrario la porta sara' associata ad una o piu' VLAN in modalita' tagged, ed i frame trasporteranno le informazioni di tag
    - il link associato a tali porte si dice *trunk link*
    - la VLAN di appartenenza del frame e' definito dal valore inserito nella TAG

11

Porte ibride

- Lo standard richiede che una porta possa essere associata ad una VLAN in modalita' untagged, e ad altre VLAN in modalita' tagged
  - il link attestato su tali porte si dice *hybrid link*
  - l'appartenenza del frame ricevuto ad una VLAN e' definito univocamente
    - se non ha la TAG, il frame appartiene alla VLAN a cui la porta e' associata in modalita' untagged
    - se ha la TAG, la VLAN di appartenenza e' definita dal valore trasportato dalla TAG
  - la VLAN a cui la porta e' associata in modalita' untagged viene anche detta PVID (Private Vlan ID)

12

Funzioni ingress e forwarding in 802.1Q

- ingress: quando viene ricevuto un frame il bridge deve identificare la VLAN di appartenenza
  - se il frame e' untagged, la VLAN di appartenenza e' identificata con la VLAN a cui la porta e' associata in modalita' untagged
    - se il link e' di tipo trunk, il frame viene scartato
  - se il frame e' tagged, la VLAN di appartenenza viene identificata dalla TAG
    - se il link e' di tipo access, o la porta non e' associata in modalita' tagged alla VLAN indicata nella TAG, il frame viene scartato
- forwarding: una volta identificala la VLAN di appartenenza vengono applicate le regole di forwarding e viene identificata la porta di uscita
  - la o le porte in uscita devono essere associate alla VLAN di appartenenza del frame

13

egress: inserimento e rimozione della TAG

- La funzione egress puo' richiedere la modifica del frame ricevuto:
  - se il frame in ingresso e' di tipo 802.1Q e la porta in uscita e' associata alla VLAN di appartenenza in modalita' tagged, il frame viene inoltrato senza modifiche
  - se il frame in ingrsso e' untagged e la porta in uscita e' associata alla VLAN di appartenenza in modalita' untagged, il frame viene inoltrato senza modifiche
  - se il frame in ingresso e' di tipo 802.1Q e la porta di uscita e' in modalita' untagged, la TAG deve essere rimossa
  - se il frame in ingresso e' di tipo 802.3 e la porta di uscita e' associata alla VLAN di appartenenza in modalita' tagged, deve essere inserita la TAG
  - negli ultimi due casi, il bridge deve ricalcolare il valore del CRC

14

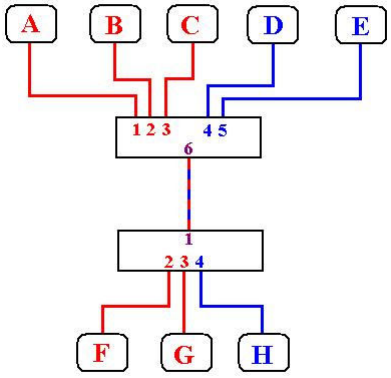
Coesistenza con apparati non 802.1Q

- Gli apparati che non osservano lo standard 802.1Q saranno connessi su porte del bridge associate esclusivamente ad una VLAN in modalita' untagged
  - questo garantisce che
    - ogni frame ricevuto sara' associato ad una VLAN
    - nessun frame di tipo 802.1Q sara' inoltrato verso l'apparato a valle, in quanto la TAG deve essere rimossa
- Questo permette di inserire in una rete locale apparati 802.1Q senza dover sostituire l'hardware preesistente
- Solitamente le interfacce di rete degli host connessi alla LAN non sono compatibili con lo standard 802.1Q
  - la possibilita' di utilizzare 802.1Q su una interfaccia di rete dipende sia dalla scheda che dal driver del sistema operativo
  - tutte le schede moderne installate sui server possono lavorare in modalita' 802.1Q
  - tutte le recenti versioni di linux hanno driver che permettono di utilizzare 802.1Q sulle schede che possono farlo
  - su Windows non sempre e' possibile (sempre sulle versioni Server)

15

Esempio di topologia 802.1Q

- Nell'esempio il link tra i due switch e' di tipo trunk e trasporta frame di entrambe le VLAN
- I frame ricevuti dalle stazioni entrano privi di tag
- I bridge devono inserire la tag per trasmettere i frame verso l'altro bridge
- I bridge dovranno rimuovere la tag prima di inoltrare i frame verso la stazione di destinazione
- Nessun frame appartenente ad una VLAN puo' raggiungere stazioni connesse su porte associate ad un'altra VLAN
  - per realizzare una comunicazione tra stazioni appartenenti a VLAN differenti i dati devono essere inoltrati a livello di rete da un router



16

Protocol based VLAN

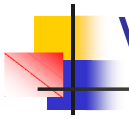
- L'assegnazione di un frame ad una VLAN puo' essere effettuata dinamicamente, in funzione di diversi parametri
  - le regole di assegnazione devono essere configurate nei bridge opportunamente
  - non tutti i bridge 802.1Q sono in grado di effettuare l'assegnazione dinamica, anche se osservano lo standard 802.1Q
  - l'applicazione di queste regole viene definita packet filtering
- I parametri possono essere
  - indirizzo IP del mittente (se il frame trasporta un pacchetto IP)
  - protocol type del frame Ethernet (IP, NETBios, AppleTalk, ...)
  - indirizzo Ethernet della stazione mittente
- Queste regole di assegnazione possono anche convivere con una assegnazione statica, che avra' priorita' maggiore
  - se pero' il frame ha gia' una tag, questa ha la precedenza sulle altre regole
- Alcuni bridge o switch supportano protocolli proprietari che permettono di configurare le regole di assegnazione dinamica centralmente, su uno o piu' server dai quali lo switch importa le configurazioni
- Un esempio tipico e' la assegnazione definita dal MAC address: nessuna stazione puo' accedere ad una VLAN se il suo MAC address non e' registrato opportunamente dall'amministratore della rete, indipendentemente dalla porta a cui si connette

17

Default VLAN

- Gli switch 802.1Q vengono venduti con una VLAN predefinita, detta default VLAN,
  - questa configurazione permette di inserire lo switch in una LAN che non utilizza 802.1Q in modo trasparente
- Alla default VLAN e' assegnata la TAG 1
- Tutte le porte appartengono alla default VLAN in modalita' untagged (PVID = 1)
- Vi sono configurazioni che non tutti gli switch supportano
  - non sempre e' possibile cambiare la TAG della default VLAN (puo' dipendere dalla release del firmware)
  - non sempre e' possibile assegnare una porta alla default VLAN in modalita' tagged e ad un'altra VLAN in modalita' untagged
- Poiche' una porta non puo' essere associata a piu' di una VLAN in modalita' untagged, per modificare il PVID di una porta si deve prima rimuovere l'associazione della porta in modalita' untagged preesistente

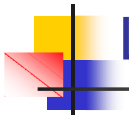
18



VLAN di management

- Tutti gli switch 802.1Q sono gestibili in remoto via TCP/IP
  - l'indirizzo IP viene assegnato ad una VLAN, e lo switch sara' raggiungibile via TCP/IP solo all'interno della VLAN a cui e' assegnato l'indirizzo IP (o via routing)
  - gli switch layer 2 hanno generalmente la possibilita' di avere un solo indirizzo IP
  - gli switch layer 3 possono avere piu' indirizzi IP assegnati a VLAN differenti, ed eventualmente possono fare routing tra le VLAN
    - spesso sono supportati anche i protocolli di routing RIP ed OSPF
- E' consigliabile per motivi di sicurezza creare una VLAN dedicata al management degli apparati di rete
  - gli indirizzi IP saranno assegnati a questa VLAN
  - per maggiore sicurezza non dovrebbe essere abilitato il routing verso questa VLAN: in questo modo lo switch sara' raggiungibile (via TCP/IP) solo da una macchina connessa alla VLAN di management (questo potrebbe costituire un limite alla flessibilita' del management)

19



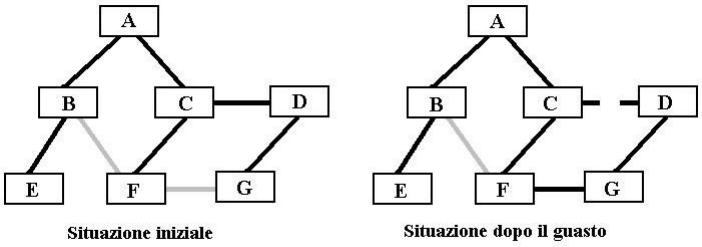
Lo spanning tree

- Lo standard 802.1D definisce un protocollo attraverso il quale e' possibile realizzare una topologia ridondante per una LAN di tipo 802.*
  - gli switch comunicano tramite un protocollo definito dallo standard 802.1D ed eleggono un nodo con funzioni di controllo
  - il nodo master raccoglie dati dagli altri switch e ricostruisce la topologia della rete
  - in base alla topologia vengono identificati (tramite un algoritmo detto spanning tree) e dinamicamente disabilitati uno o piu' link della LAN al fine di rimuovere percorsi circolari
  - i link disabilitati possono essere automaticamente riabilitati in occasione di problemi che generano una partizione della rete, in modo da riottenere la connettivita'
- Il protocollo che realizza questa funzionalita' si chiama STP (Spanning Tree Protocol)
- Un bridge osserva lo standard 802.1D se e' capace di gestire questo protocollo, comunicando con gli altri bridge ed attivando o disattivando i link all'occorrenza
  - tutti gli switch di medio livello sono oggi compatibili con lo standard 802.1D

20

Esempio di spanning tree

- Inizialmente lo spanning tree protocol disattiva i link tra gli switch B-F e F-G
- Il guasto del link C-D rende D e G irraggiungibili
- L'attivazione del link F-G ripristina la connettivita' verso entrambi gli switch senza introdurre percorsi circolari



Situazione iniziale

Situazione dopo il guasto

21

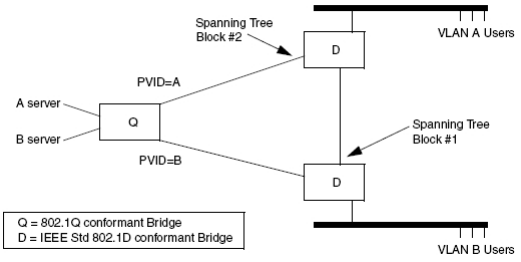
STP e 802.1Q

- Poiche' ogni VLAN costituisce una LAN logicamente separata dalle altre, il protocollo STP deve operare distintamente sulle diverse VLAN
  - un link di tipo trunk puo' risultare attivo per una VLAN e disattivo per un'altra VLAN
- La topologia fisica deve tenere in considerazione attentamente la configurazione delle VLAN, per offrire ridondanza su tutte le VLAN desiderate

22

Problemi con bridge 802.1Q e 802.1D

- L'utilizzo contemporaneo di bridge 802.1Q e 802.1D (non 802.1Q) puo' portare problemi di configurazione nascosti
- Nell'esempio, se l'STP disabilita il link tra i due bridge 802.1D tutto funziona, ma se viene disabilitato uno degli altri link, gli user di una VLAN perdono connettivita' verso i loro server



23