



# Le VLAN nella gestione delle reti locali

Copyright 2006 - Damiano Verzulli

E' garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della "Licenza per Documentazione Libera GNU", Versione 1.1 o ogni versione successiva pubblicata dalla Free Software Foundation; senza Sezioni Non Modificabili, senza Testi Copertina e senza Testi di Retro Copertina.

Una copia della licenza è disponibile in:

<http://www.softwarelibero.it/gnudoc/fdl.it.html#SEC1>

---

**Dr. Damiano Verzulli**

**damiano@verzulli.it**

*Chieti, 24/11/2006*



# Chi vi parla...

---

*Questa diapositiva è stata proiettata alle 10.07*

- Damiano Verzulli, 35 anni, di Chieti, laureato con lode presso l'Università dell'Aquila nel 1995 in Scienze dell'Informazione;
- “Emigrato” a Bologna, per lavoro, dal maggio 1996 al febbraio 2003 prima in Cineca ([www.cineca.it](http://www.cineca.it) – il più grosso centro di calcolo italiano) e poi in Nextra ([www.nextra.it](http://www.nextra.it) ...attuale TiscaliBusiness, ai tempi uno dei principali ISP italiani);
- In Cineca (1996) scopre Linux ed il Software Libero. Sempre in Cineca viene circondato da persone che “vivono” di networking;
- Rientrato a Chieti nel 2003, da maggio 2004 si occupa della gestione dei principali servizi di rete dell'Ateneo “D'Annunzio”;
- Per (cercare di) risolvere alcuni dei problemi strutturali del network d'Ateneo ha introdotto, per primo, l'uso di VLAN



# Di cosa parleremo

---

*Questa diapositiva è stata proiettata alle 10.07*

- Obiettivo di questo incontro è quello di **presentare la tecnologia “Virtual-LAN”** (più comunemente **VLAN**) analizzandone qualche caso applicativo concreto (come, ad esempio, quello dei vostri laboratori)
- Accenneremo anche al protocollo che è alla base di tale tecnologia ed alle strette relazioni con il mondo “Ethernet”

## **Concetti preliminari alla base dei nostri discorsi:**

- **Networking Ethernet (reti CSMA/CD)**
- **Dominio di collisione**
- **Dominio di broadcast**

anche se ricordate tutto perfettamente... rinfreschiamoci la memoria ⇨



# Ethernet

Questa diapositiva è stata proiettata alle 10.07

- Le reti Ethernet funzionano secondo lo schema **CSMA/CD**:

– **Carrier Sense**: ogni postazione di rete, prima di trasmettere “sente” se la rete è libera (ossia se nessun altro sta trasmettendo);

– **Multiple Access**: l'accesso al mezzo trasmissivo è condiviso fra più postazioni. Ognuna di loro, se “sente” la rete libera, è perfettamente in grado di trasmettere;

– **Collision Detection**: è perfettamente possibile che due postazioni sentano entrambe la rete come “libera” ed inizino a trasmettere nello stesso istante  $T$  (o  $T+dT$ , con  $dT$  relativamente piccolo). In tal caso si genera una collisione, ossia un segnale elettrico anomalo. Segnale che deve essere opportunamente rilevato e gestito da tutte le postazioni che stavano trasmettendo



# Ethernet e indirizzamento (MAC)

*Questa diapositiva è stata proiettata alle 10.07*

- Affinchè “mittente” e “destinatario” siano in grado di comunicare:

– entrambi devono essere indirizzabili (ossia devono avere un “MAC address”);

– il MAC address deve essere univoco;

l'uno deve conoscere il MAC address dell'altro.

**Il MAC address è formato da 48 bit di cui i primi 24 sono assegnati univocamente ai vari produttori di schede ethernet che evidentemente utilizzeranno gli altri 24 in modo opportuno**

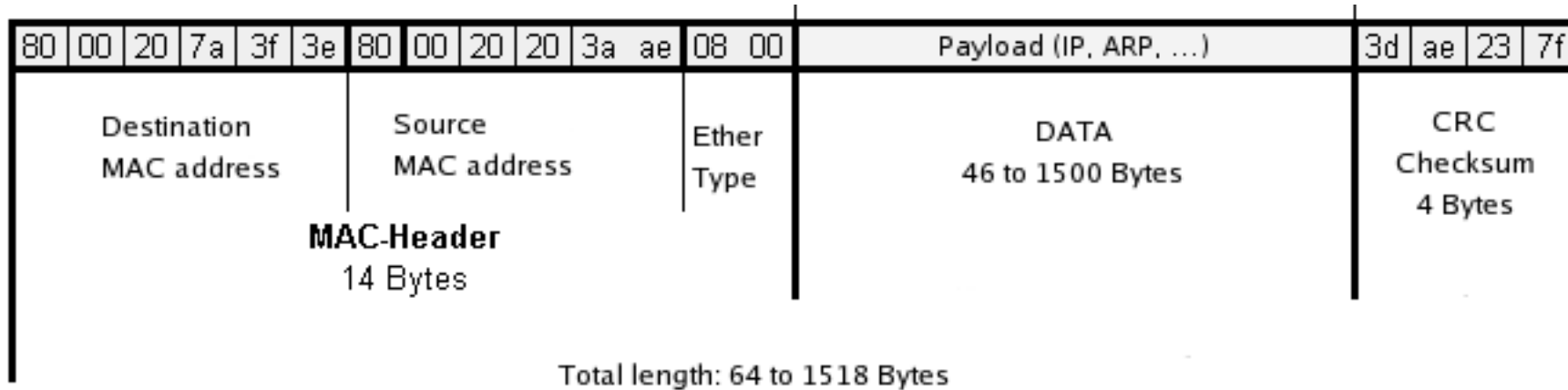
**Se è banale, per il destinatario, conoscere il MAC del mittente, per il contrario c'è bisogno di qualcosa di esplicito.**



# Un frame “ethernet”

Questa diapositiva è stata proiettata alle 10.07

- Un frame ethernet di esempio:



- si riconoscono:

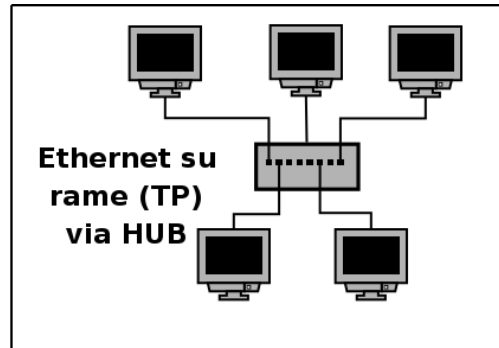
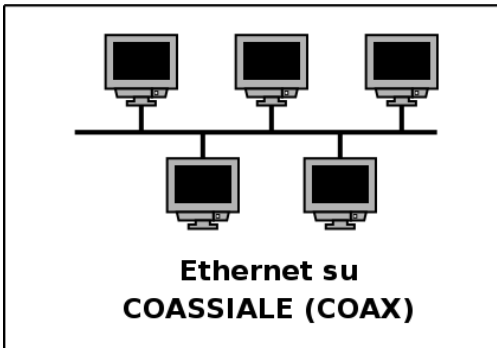
- Destination MAC (6 byte) ⇒ 80:00:20:7a:3f:3e
- Source MAC (6 byte) ⇒ 80:00:20:20:3a:ae
- Ether Type (2 byte) ⇒ 0x0800 (IP)
- Payload (fino a 1500 bytes)
- CRC (4 byte)



# Ethernet e gestione del traffico

Questa diapositiva è stata proiettata alle 10.07

- Considerando che:
  - La condivisione del mezzo trasmissivo (come da specifiche) è tale che il segnale emesso da una postazione raggiunge tutte le altre connesse allo stesso mezzo trasmissivo;
  - Per evitare problemi, ogni postazione si preoccupa di “filtrare” tutto il traffico in arrivo dal mezzo trasmissivo, per considerare solo quello a se destinato;
- ...è chiaro che il traffico complessivo veicolato da un segmento di rete cresce esponenzialmente con il numero di postazioni ad esso collegato.



***I mezzi trasmissivi “storici”  
come il cavo coassiale ed i  
successivi HUB, garantiscono  
esattamente questo aspetto***



# Ethernet e gestione del traffico

*Questa diapositiva è stata proiettata alle 10.07*

- Per limitare questo problema (crescita esponenziale del traffico rispetto al numero di postazioni connesse), si sono adottate via via varie soluzioni:
  - **ROUTING**: anziché avere una rete “grande”, si creano N reti più piccole interconnettendole attraverso un router
    - soluzione ideale per l'interconnessione attraverso reti geografiche (es.: CampusCH e CampusPE);
    - scomoda da applicare in contesti “solo-LAN” (non è facile trovare router con più di due o tre interfacce LAN)
    - soluzione “a massima efficienza”;
    - ...ma al tempo stesso... è la soluzione più costosa
  - **SWITCHING**: sostituzione degli (stupidi) HUB con oggetti più furbi in grado di forwardare il traffico solo alle porte interessate:
    - soluzione ideale per ambienti LAN
    - estremamente più economico rispetto al “routing”
    - ... “efficienza” buona... ma non ottima

# Ethernet “switchata”

Questa diapositiva è stata proiettata alle 10.07

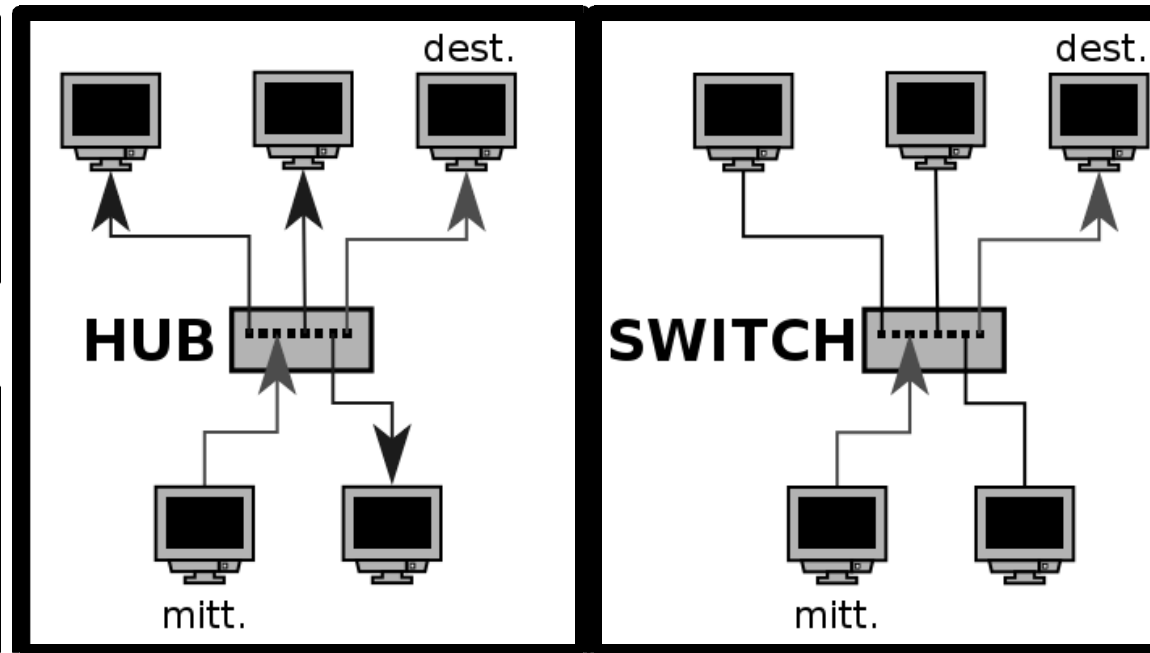
- A differenza di un HUB ch  va considerato come un semplice ripetitore di segnale, lo SWITCH:

–riconosce e memorizza i MAC address delle postazioni connesse alle sue porte

“Learning process”

–inoltra i “pacchetti” solo alla porta dov'  connesso il destinatario

“Forwarding process”



**Ma   sempre possibile?**



# Ethernet e “broadcast”

---

Questa diapositiva è stata proiettata alle 10.07

- Esistono delle condizioni nelle quali è necessario che un mittente contatti **deliberatamente** tutti i possibili destinatari. Ad esempio, quando deve scoprire qual'è il MAC del destinatario;
- **Esiste un indirizzo MAC speciale (ff:ff:ff:ff:ff:ff) che viene preso in esame da tutte le postazioni.** Questo indirizzo viene detto “indirizzo di broadcast”;
- E' evidente che se ad essere trasmesso è un pacchetto di broadcast, HUB e SWITCH si comportano allo stesso modo

**In una rete di grandi dimensioni  
(come CampusCH e CampusPE), il traffico di  
broadcast può essere molto elevato!**

***....e guardacaso, un'azienda che ha lungamente  
utilizzato il BROADCAST come “filosofia” è Microsoft,  
con il suo NETBIOS***



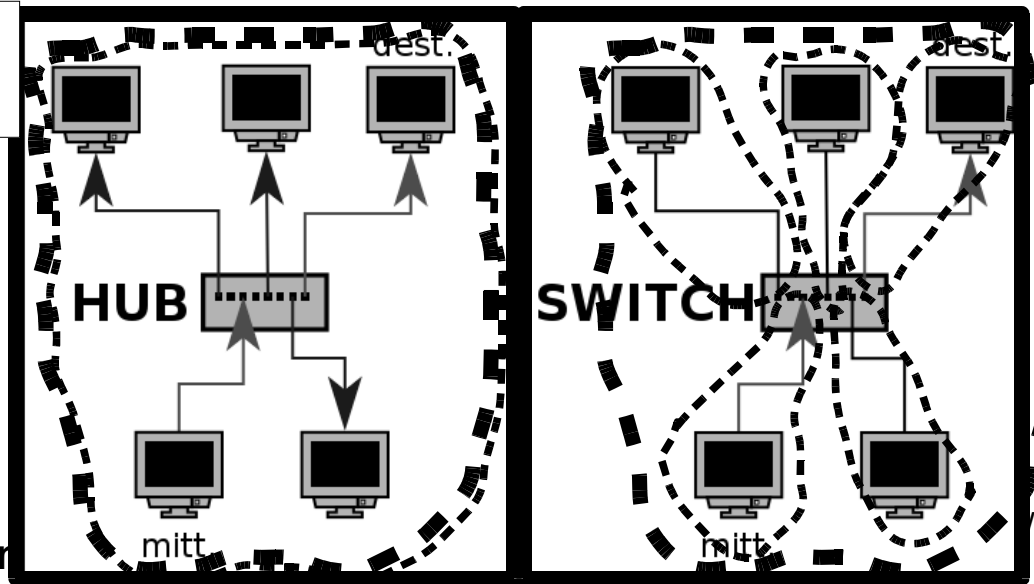
# Ethernet e “domini”

Questa diapositiva è stata progettata alle 10.07

- La differenza fra HUB e SWITCH si può formalizzare introducendo due nuovi concetti:
  - **Dominio di “collisione”**: è determinato dall'insieme di postazioni che possono risentire di una collisione generata da due postazioni arbitrarie;
  - **Dominio di “broadcast”**: è determinato dall'insieme di postazioni che ricevono i pacchetti di broadcast

----- dominio di broadcast  
- - - - - dominio di collisione

**Lo switch minimizza il “dominio di collisione” ma non cambia il “dominio di broadcast”**





# VLAN

---

*Questa diapositiva è stata proiettata alle 10.07*

- Le VLAN non sono altro che un livello di astrazione in grado:
  - di consentire a postazioni attestatae su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete (logica);
  - di separare postazioni attestatae sulla stessa rete (fisica) in più reti (logiche e distinte)
- Uno dei vantaggi fondamentali offerto dall'impiego estensivo di VLAN si riscontra in occasione della gestione delle postazioni di lavoro: laddove normalmente sarebbe necessario intervenire a livello di cablaggio (con costi e tempi non trascurabili), le VLAN offrono una soluzione che non comporta alcun intervento fisico/hardware.

**In termini di “domini”, le VLAN consentono la riduzione dei domini di broadcast**

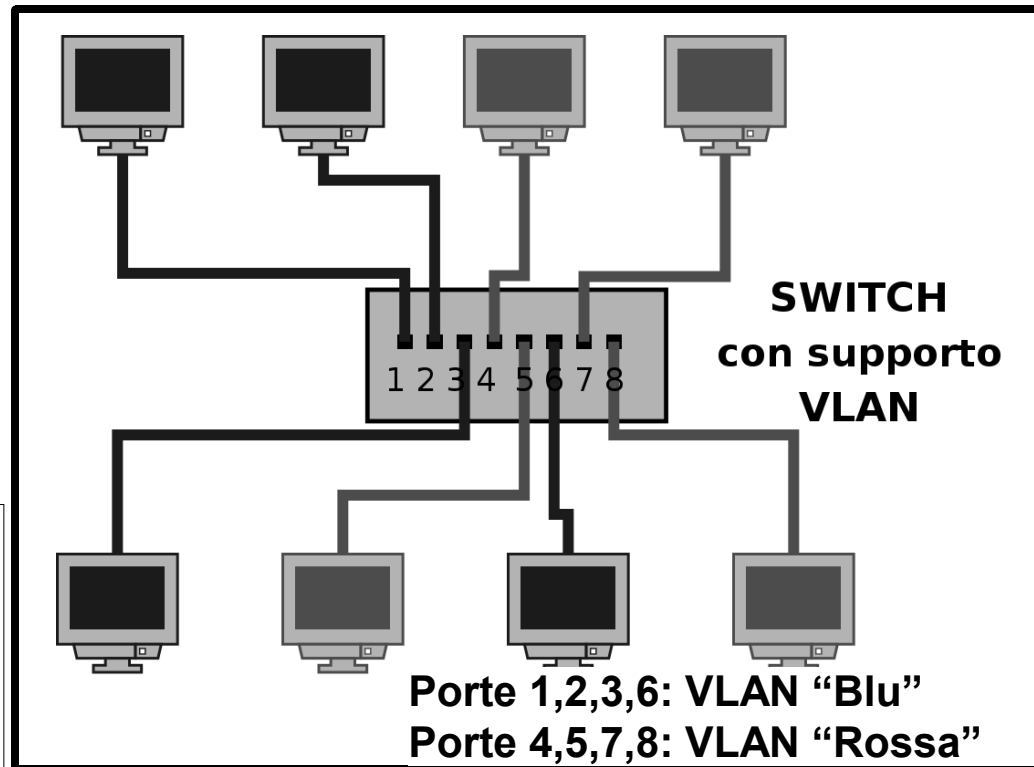


# VLAN – un primo esempio

Questa diapositiva è stata proiettata alle 10.07

- Una delle applicazioni più semplici di VLAN è quella del “taglio” di un unico switch fisico in due o più reti diverse

- Nell'esempio in figura, con un unico switch riusciamo a “separare” gli 8 PC in due gruppi (BLU, ROSSI). I PC “blu” vedranno solo i “blu”; i “rossi” solo i “rossi”



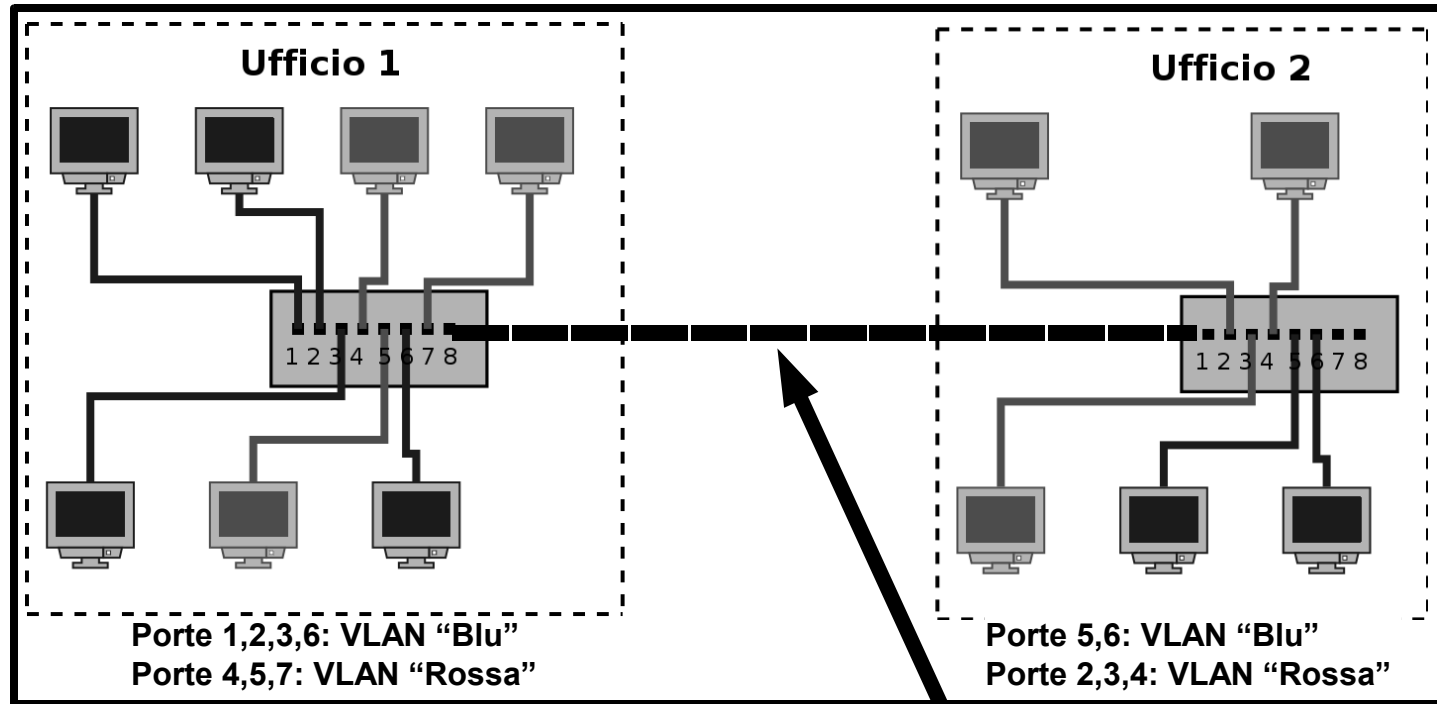
**Senza VLAN sarebbe necessario utilizzare DUE switch diversi (uno per ogni VLAN)**

# VLAN: un esempio più complesso

Questa diapositiva è stata proiettata alle 10.07

- L'utilità delle VLAN si manifesta chiaramente nello scenario seguente:

Come faccio a  
“collegare” i  
due gruppi  
“rossi” e “blu”  
senza fare  
pasticci?



Senza VLAN mi sarebbero serviti  
almeno 4 switch e, soprattutto,  
una quantità maggiore di  
metri di cavo

Inoltrando il traffico di entrambe  
le VLAN sulle porte 8 e 1  
(porte TRUNK)  
e lasciando agli switch il compito  
di “forwardarlo” opportunamente



# VLAN: tipologie

---

*Questa diapositiva è stata proiettata alle 10.07*

- Esistono diverse tipologie di VLAN (port-based, protocol-based, auth-based). Quelle attualmente utilizzate in UNICH sono le “Port-Based”
- In una VLAN Port-Based, le porte dello switch possono essere di tipo:
  - **UNTAGGED**: sono porte che vengono assegnate ad una determinata VLAN. Tutto il traffico di quella VLAN viene “inoltrato” su quella porta come normalissimo traffico ethernet
  - **TAGGED**: ad una porta “tagged” possono essere assegnate più VLAN. Ai frame ethernet in uscita viene “aggiunto” nell'header un campo (TAG) che indica, fra l'altro, il VLAN-ID del frame

**Lo standard 802.1q è quello che definisce le regole di “tagging” e che, quindi, assicura l'interoperabilità fra apparati di produttori diversi.**

**Linux, da tempo, supporta il protocollo 802.1q**



# 802.1q: la struttura

---

*Questa diapositiva è stata proiettata alle 10.07*

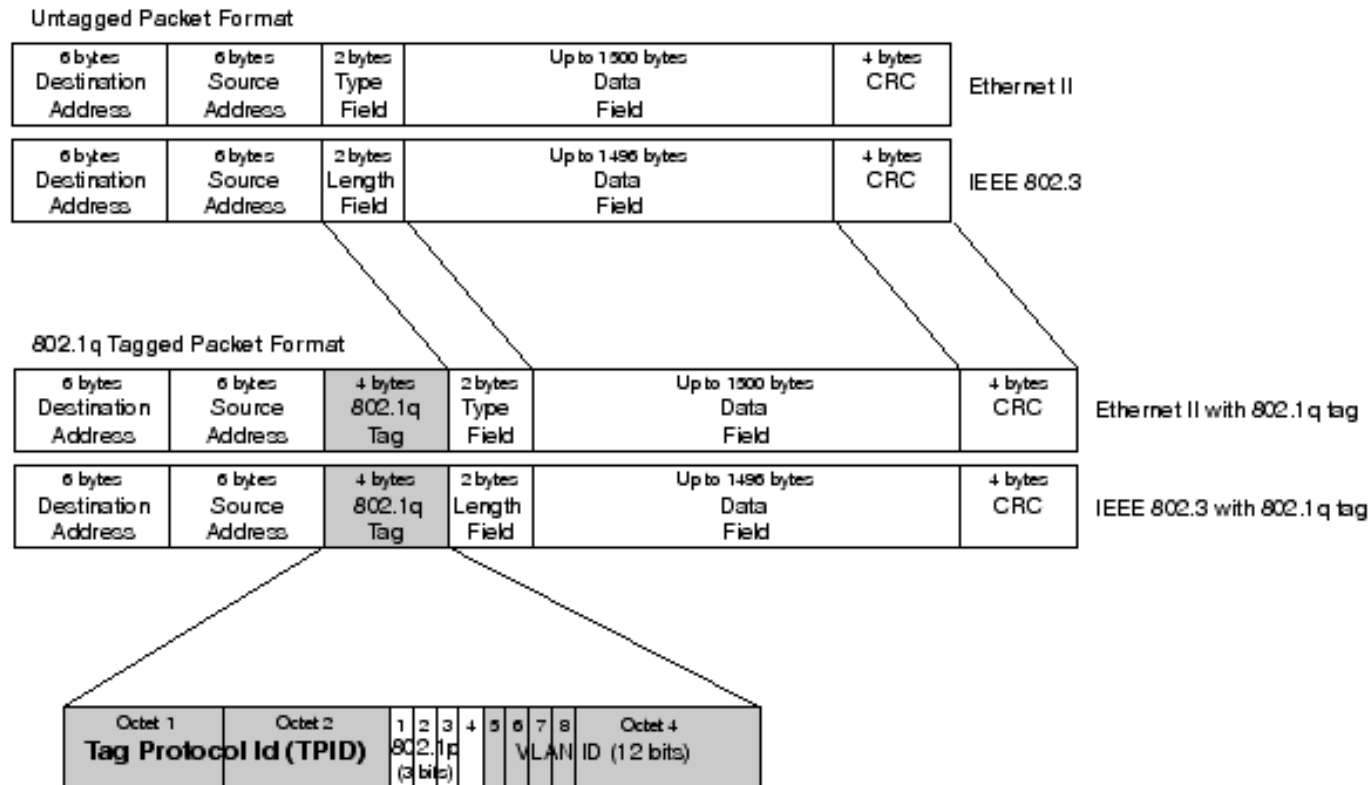
- L'802.1q non segue la logica dell'“incapsulamento” ma viene implementato aggiungendo 4 bytes nell'header Ethernet;
- Nei 4 bytes aggiunti troviamo:
  - un EtherType aggiuntivo (0x8100 – 2 byte) che identifica il frame;
  - user\_priority: 3 bit che possono essere utilizzati per prioritizzare il frame. Lo standard 802.1p disciplina tale prioritizzazione;
  - CFI (Canonica Format Indicator): 1 bit che indica la presenza, nel frame, di MAC address riportati in forma canonica;
  - VID: 12 bit che indicano il VLAN-ID di appartenenza (da 0 a 4096)

**L'aggiunta al frame comporta la necessità di ricalcolare il CRC/checksum di tutti i pacchetti “taggati”**



# 802.1q: la struttura

Questa diapositiva è stata proiettata alle 10.07





# 802.1q: altre considerazioni

---

*Questa diapositiva è stata proiettata alle 10.08*

- Uno switch VLAN-compliant, quando esce di fabbrica, è configurato con un'unica VLAN (VID=1) e con tutte le porte “UNTAGGED” su tale VLAN. In altri termini, si comporta in modo identico ad uno switch non-vlan-compliant;
- Delle 4096 VLAN possibili, le VLAN 0 e 4096 sono “riservate”;
- L'802.1q introduce (fra l'altro) due nuovi protocolli:
  - GVRP: Generic VLAN Registration Protocol – consente agli switch di negoziare dinamicamente quali VLAN gestire su un “trunk”;
  - MSTP: Multiple Spanning Tree Protocol – evoluzione dello STP adattata al contesto 802.1q

**Lo standard 802.1q ufficiale, pubblicato da IEEE (a pagamento), è un PDF da circa 300 pagine!**

***E' un classico esempio di formato “aperto” ma “non-libero”***

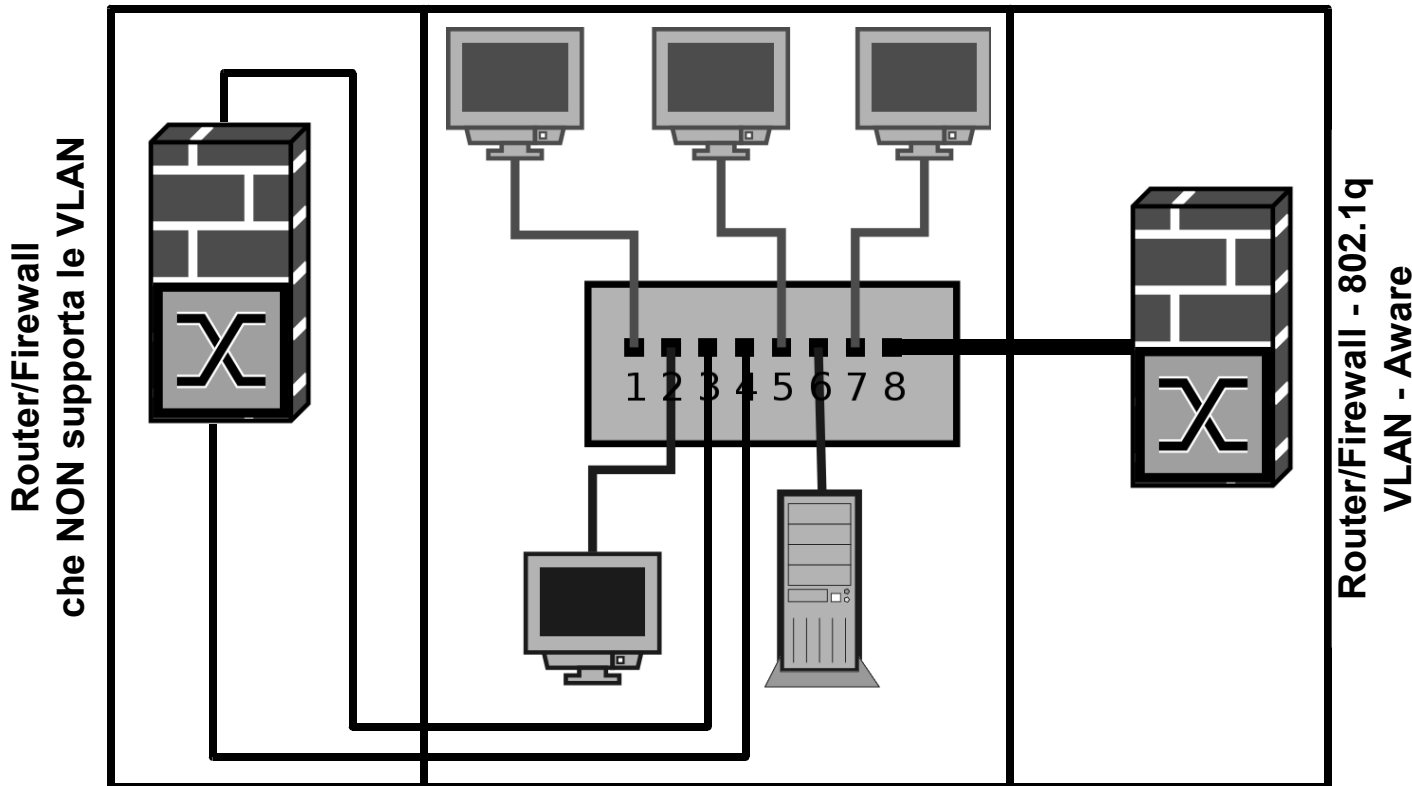
# 802.1q: altre considerazioni

Questa diapositiva è stata proiettata alle 10.08

- Se, dato uno switch, le VLAN risultano “isolate”, come si può ottenere la comunicazione fra i dispositivi attestati su tale VLAN?
- Semplice! Introducendo un router (o un firewall)

- Ma c'è una soluzione più elegante ;-)

**Ed ecco qui,  
un firewall  
(o un router)  
con UNA SOLA  
INTERFACCIA  
FISICA ;-)**



“Le VLAN nella gestione delle reti locali”

Pescara, 24/11/2006

Pag. 19 di 27



# VLAN: un (nuovo) trade-off da gestire

---

*Questa diapositiva è stata proiettata alle 10.08*

- Le VLAN vanno viste, da un network-engineer, come uno strumento che:
  - **SEMPLIFICA** enormemente la gestione di una rete, soprattutto a livello di “spostamenti” e “ottimizzazione del cablaggio”;
  - **COMPLICA** enormemente la gestione della rete, in termini di “configurazione”

**Se guardando uno switch “normale” si vedono  
24 o 48 porte.... e nulla più...**

**guardando uno switch VLANnizzato, si deve  
vedere.... qualcosa che può essere anche  
estremamente complesso da ricostruire.**



# Le VLAN c/o CampusCH

---

*Questa diapositiva è stata proiettata alle 10.08*

- **Campus Network:** VLAN che gestisce il traffico di streaming dei flussi audio/video di Campus Network Television (4 Mbps, H24, in multicast....);
- **Videosorveglianza:** VLAN che interconnette una decina di telecamere IP che inviano i flussi video ad un server centrale (da 1 a 2 Mbps, unicast, H24)
- un certo numero di VLAN “minori” introdotte per segmentare la rete principale (circa 800 client su un unico segmento)

**L'eventuale interconnessione fra queste VLAN ed il resto della rete d'Ateneo viene gestita da un server Linux opportunamente configurato (per le VLAN e per il Firewalling)**



# Il "mixer" di CampusCH

Questa diapositiva è stata proiettata alle 10.08

```
eth2      Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:460671688  errors:0  dropped:0  overruns:0  frame:
TX packets:416997252  errors:0  dropped:0  overruns:0  carrier
collisions:0  txqueuelen:1000
RX bytes:3455369631 (3295.2 Mb)  TX bytes:2258571906 (215
Base address:0x4100  Memory:cffc0000-cffe0000

eth2.2    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.12.254  Bcast:10.0.12.255  Mask:255.255.25
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:89998866  errors:0  dropped:0  overruns:0  frame:0
TX packets:90109244  errors:0  dropped:0  overruns:0  carrier
collisions:0  txqueuelen:0
RX bytes:1341127036 (1278.9 Mb)  TX bytes:368602030 (351.5 Mb)

[...]
eth2.3    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.10.254  Bcast:10.0.10.255  Mask:255.255.255.0

[...]
eth2.4    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.11.1  Bcast:10.0.11.255  Mask:255.255.255.0

[...]
eth2.5    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.18.1  Bcast:10.0.18.255  Mask:255.255.255.0

[...]
eth2.6    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.6.1  Bcast:10.0.6.255  Mask:255.255.255.0

[...]
eth2.8    Link encap:Ethernet  HWaddr 00:0E:0C:68:DB:78
inet addr:10.0.13.1  Bcast:10.0.13.255  Mask:255.255.255.0

[...]
```

```
[root@mixer ~]# cat /proc/net/vlan/config
VLAN Dev name | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
eth2.10      | 10 | eth2
eth2.11      | 11 | eth2
eth2.2       | 2  | eth2
eth2.3       | 3  | eth2
eth2.4       | 4  | eth2
eth2.5       | 5  | eth2
eth2.6       | 6  | eth2
eth2.8       | 8  | eth2
eth2.9       | 9  | eth2
```

**9 VLAN  
definite sulla  
interfaccia eth2  
(VID 2,3,4,5,6  
8,9,10,11)  
che si gestiscono  
con altrettante  
9 nuove  
eth2.<VID>**



# “mixer” visto dallo switch...

Questa dispositivo è stato proiettato alle 10:08

```
SB400_UNICH> sh conf dyn=vlan
#
# VLAN general configuration
#
create vlan="CNT" vid=2
create vlan="Sorveglianza" vid=3
create vlan="SEGR_PSICOLOGIA" vid=4
create vlan="WEB_AGENCY_WLAN" vid=5
create vlan="ProtezCivile" vid=6
create vlan="NetPublic" vid=7
create vlan="ADITEC" vid=8
create vlan="cesi_ospedale" vid=9
create vlan="segr-asilo" vid=10
create vlan="uffStip" vid=11
add vlan="2" port=6.45-6.48
add vlan="3" port=6.42
add vlan="5" port=6.31-6.34
add vlan="7" port=6.15
add vlan="8" port=6.35-6.36
add vlan="2" port=3.6,3.9,4.1-4.2,4.4,4.6,6.38 frame
add vlan="3" port=3.32,4.1-4.2,4.4-4.5,6.38,6.41 fr
add vlan="4" port=3.9,6.38 frame=tagged
add vlan="5" port=6.38 frame=tagged
add vlan="6" port=3.3,6.38 frame=tagged
add vlan="7" port=3.17,3.32,4.1,6.13,6.41 frame=tag
add vlan="8" port=6.38 frame=tagged
add vlan="9" port=3.17,6.13,6.38 frame=tagged
add vlan="10" port=4.6,6.38 frame=tagged
add vlan="11" port=6.5,6.38 frame=tagged
set vlan="1" port=3.3,3.9,4.2,4.5,6.38,6.41 frame=t
delete vlan="1" port=3.17,3.32,6.13
```

```
Manager SB400_UNICH> sh switch port=6.38
Switch Port Information
-----
Port ..... 6.38
Description ..... Uplink verso MIXER - varie VLAN
Status ..... ENABLED
Link State ..... Up
UpTime ..... 30 days, 01:44:27
Port Media Type ..... IS08802-3 CSMACD
Actual speed/duplex ..... 100 Mbps, full duplex
Acceptable Frames Type ..... Admit Only VLAN-tagged Frames
Intrusion action ..... Discard
Current learned, lock state ... 0, not locked
Relearn ..... OFF
Enabled flow control(s) ..... -
Port-based VLAN(s) ..... default (1)
                               CNT (2)
                               Sorveglianza (3)
                               SEGR_PSICOLOGIA (4)
                               WEB_AGENCY_WLAN (5)
                               ProtezCivile (6)
                               ADITEC (8)
                               cesi_ospedale (9)
                               segr-asilo (10)
                               uffStip (11)
Advanced Flow Control length .. -
Jumbo Packets ..... Off
Trunk Group ..... -
STP ..... disabled
-----
```



# Le VLAN sugli switch di periferia

Questa diapositiva è stata proiettata alle 10.08

```
***** Main Menu *****
1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Config Menu
6 - MAC Address Tables
7 - Ethernet Statistics
8 - Diagnostics
9 - Enhanced Stacking
C - Command Line Interface
Q - Quit

***** VLAN Menu *****
1 - VLANs Status ..... Enabled
2 - Ingress Filtering Status ..... Enabled
3 - VLANs Mode ..... User Configured VLANs
4 - Management VLAN ..... 1 (Default_VLAN)
5 - Configure VLANs
6 - Configure COS Priorities
7 - Show VLANs
8 - Show PVIDs & Priorities

***** Show VLANs *****
VID  VLAN Name          Mirror  Untagged (U) / Tagged (T)
-----
1    Default_VLAN          U: 2-20
                                T: 1, 25-26
2    CNT                   U: 21-24
                                T: 1, 25-26
```

**“Le VLAN nella gestione delle reti locali”**



# VLAN c/o CampusPE...

*Questa diapositiva è stata proiettata alle 10.08*

- Attualmente non sono definite VLAN. Da tempo si pensa di “separare” le tre scale (verde, gialla, azzurra – la rossa non ha rete), ma non si è mai proceduto a causa di vari fattori (switch, IP, etc.);
- E' imminente l'attivazione delle VLAN nella gestione dei vostri nuovi laboratori, con l'obiettivo di separare:
  - l'Aula 3-5;
  - l'Aula 7;
  - la futura Aula -2;
  - la sala GASL;
  - la rete dei server
  - le stampanti

**I vostro colleghi del gruppo GASL stanno iniziando a prendere in mano la questione**

**...visto che il venditore non è capace di farlo... e che qualcun altro... non vuole farlo gratis ;-)**

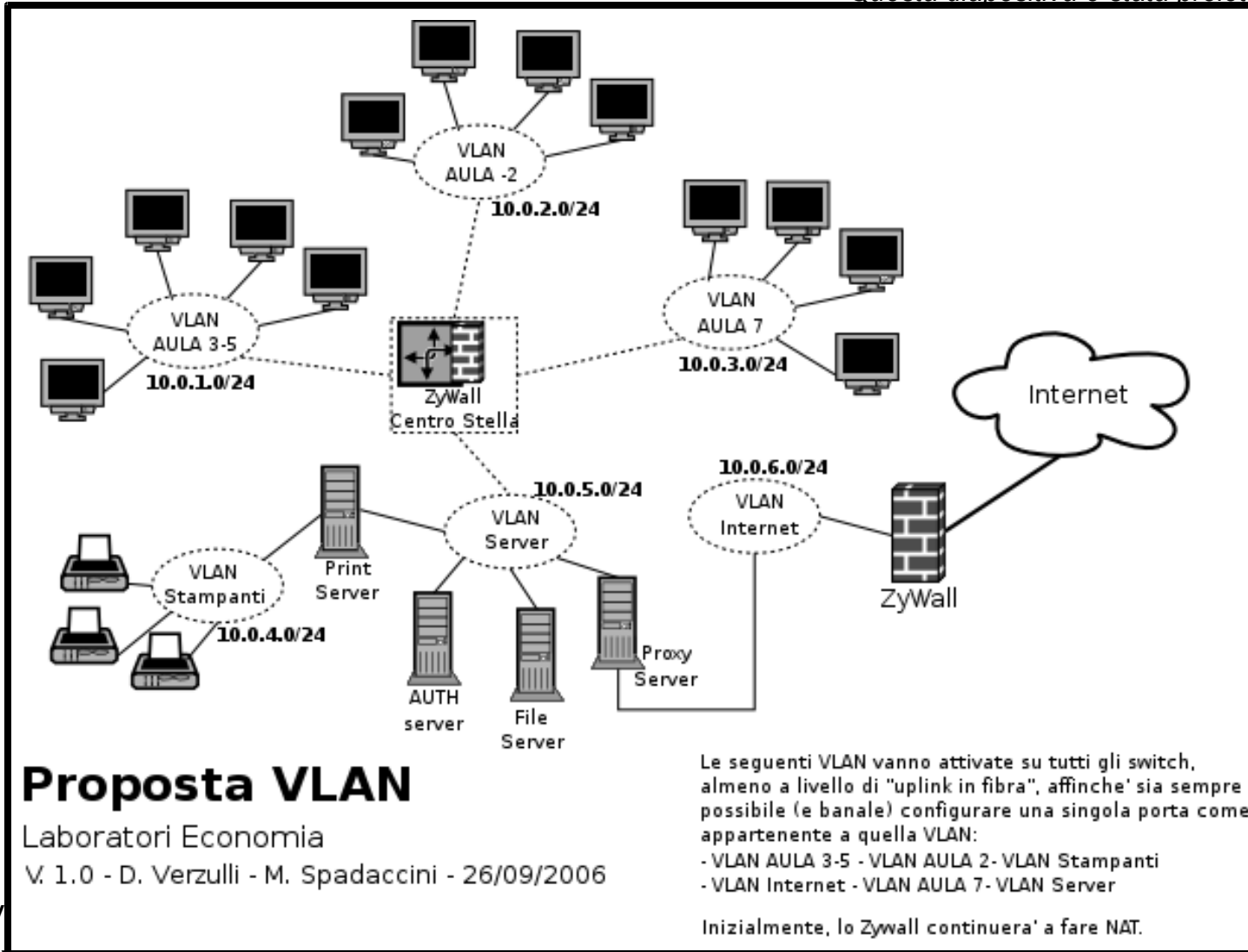
**“Le VLAN nella gestione delle reti locali”**

F. Escara, 24/11/2006

Pag. 25 di 27

# VLAN c/o Economia

Questa diapositiva è stata proiettata alle 10.08





# **E' tutto.**

---

*Questa diapositiva è stata proiettata alle 10.08*

**Per eventuali chiarimenti:**

***damiano@verzulli.it***

**Questo materiale è on-line all'indirizzo:**

**[http://www.verzulli.it/free\\_stuff/intro\\_vlan](http://www.verzulli.it/free_stuff/intro_vlan)**