

Simulazione rete complessa S1/L5

A cura di Iris Canole

Prefazione

L'obiettivo dell'esercizio di oggi è la creazione di una rete segmentata con 4 VLAN diverse. Bisognerà spiegare le motivazioni per cui si è scelto di ricorrere alla VLAN.

Nello specifico:

- Consegnare un report che descriva la configurazione, i settari necessari e parli di vantaggi e svantaggi della VLAN;
- Consegnare anche il file .pkt di packet tracer;
- Scegliere una configurazione che metta in risalto l'utilità delle VLAN, quindi:
 - usare minimo due switch;
 - ci deve essere almeno una VLAN con dispositivi collegati a switch diversi;
- Fare il subnetting della rete, o comunque assegnare ogni VLAN ad una rete diversa;
- Fare almeno un test che dimostri il corretto funzionamento del collegamento TRUNK tra gli switch.

Svolgimento dell'esercizio e configurazioni

Dato l'obiettivo dell'esercitazione, imposto la relazione scritta come una serie di passaggi eseguiti per la realizzazione del progetto, in tal modo da non perdere niente per strada.

Primo passaggio

Per la realizzazione di questo progetto, ho usato Cisco Packet Tracer, un applicativo che permette di creare delle simulazioni di rete, sviluppato, per l'appunto, da Cisco.

Come prima cosa, configureremo due switch (2960), in quanto lo chiede la consegna.

Note

In questo progetto, non ci interessa far comunicare le VLAN, quindi basta implementare anche solo due switch.

Ho pensato di creare 4 VLAN differenti pensando a un ambiente scolastico/universitario, usando come Nome dei possibili incarichi all'interno di un istituto. Lo schema è il seguente:

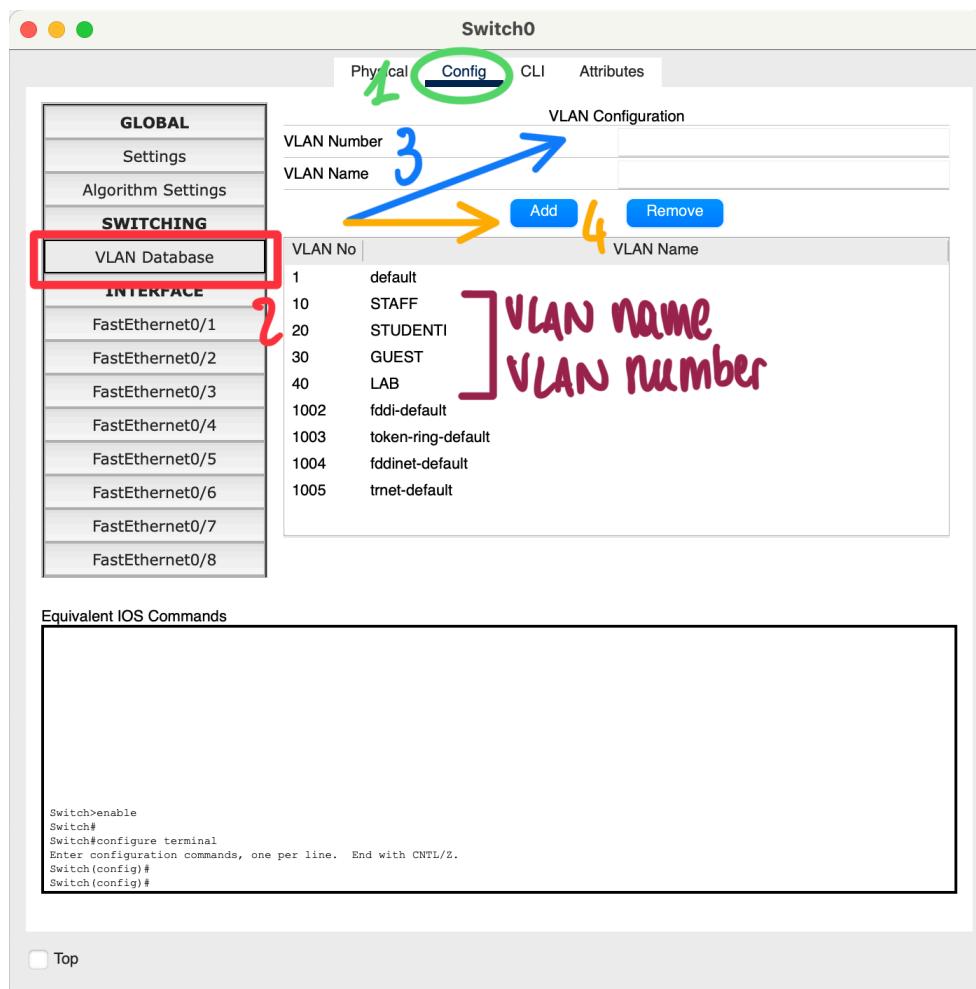
VLAN	Nome	Rete
10	STAFF	192.168.10.0/24
20	STUDENTI	192.168.20.0/24
30	GUEST	192.168.30.0/24
40	LAB	192.168.40.0/24

Per mettere in risalto l'utileità del TRUNK, ho voluto fare i seguenti assegnamenti:

- VLAN10 (STAFF) > un PC/laptop sullo Switch0 e uno sullo Switch1
- VLAN20 (STUDENTI) > uno sullo Switch0 e uno sullo Switch1
- VLAN30 (GUEST) > uno sullo Switch0 e uno sullo Switch1
- VLAN40 (LAB) > uno su Switch0 e uno su Switch1

In questo modo tutte le VLAN sono distribuite su entrambi gli Switch.

Di seguito qualche screenshot che mostra i passaggi:



Note

Qui ho preso lo screenshot dello Switch0 come esempio, ma è chiaro che gli stessi passaggi devono essere effettuati anche per Switch1, nella medesima maniera.

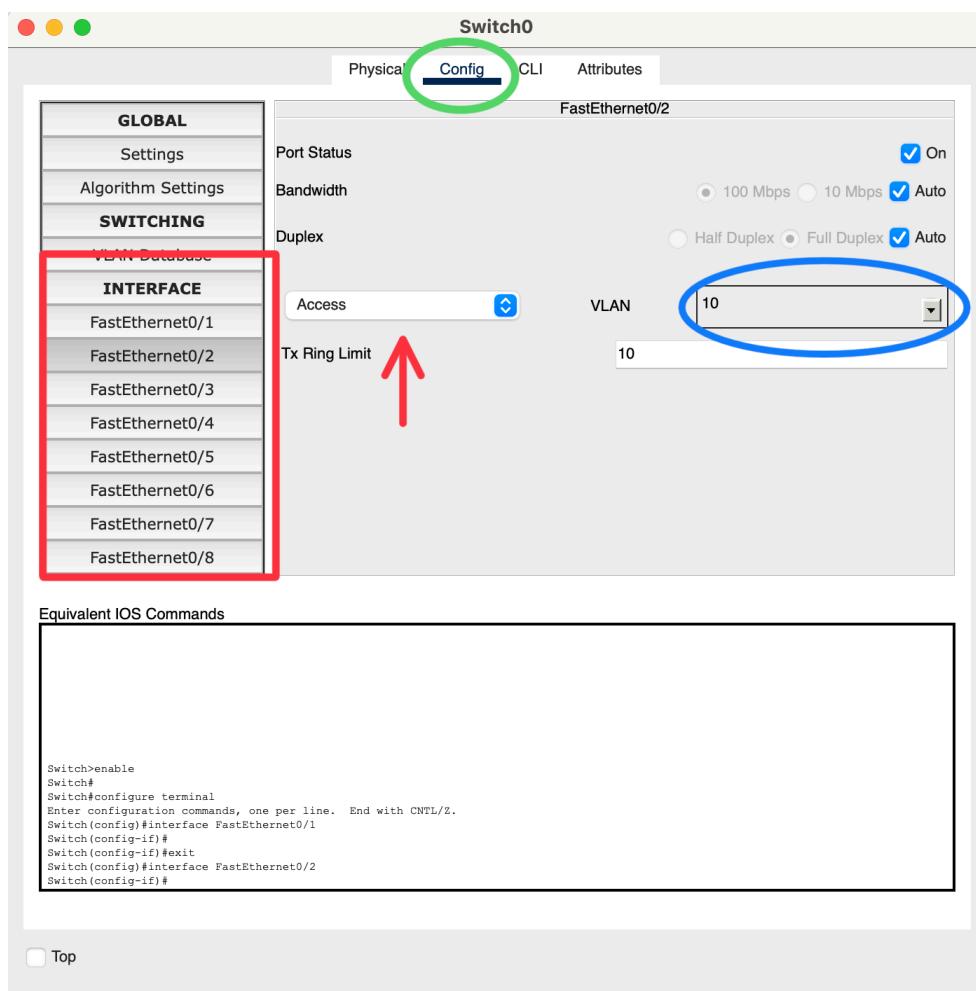
Secondo passaggio

Una volta create le VLAN sugli Switch, non ci resta che assegnare le porte degli host alle VLAN.

Come si effettua questo passaggio?

- Sempre nello switch si va in "Config" > "FastEthernet"
- Da qui si seleziona la porta dove è collegato l'host
- A questo punto si imposta:
 - Port Mode > Access
 - Access VLAN > numero della VLAN corretta

La seguente immagine mostra i passaggi:



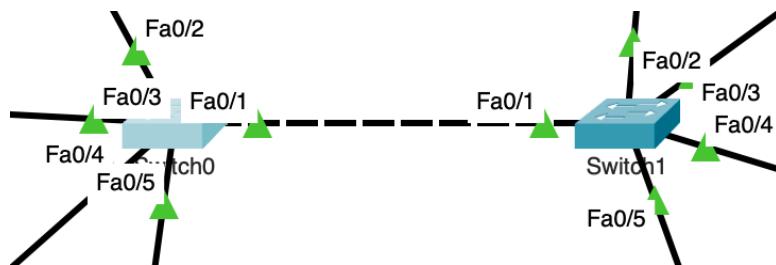
Note

Come prima, stessa cosa si effettua anche sullo Switch1. Importante qui è controllare la VLAN.

Terzo passaggio

In questo passaggio configuro il TRUNK tra gli Switch. Ma esattamente, cos'è un TRUNK?

Un TRUNK è un collegamento tra switch che trasporta più VLAN insieme, aggiungendo una sorta di etichetta ai pacchetti per dire "io appartengo alla VLAN X". Senza il TRUNK, il collegamento tra switch porterebbe solo a una VLAN, e quindi gli host delle stesse VLAN ma su switch diversi, non riuscirebbero a comunicare.



Come faccio a configurare tutto ciò?

1. Identifico la porta del collegamento
 2. Configuro il trunk su entrambi gli switch
 3. Test. Funziona tutto?

Considerando che in questo caso, la porta usata da entrambi gli switch per il collegamento è la `Fa0/1`, le operazioni da seguire saranno le seguenti (UI level):

Note

| Stessa configurazione da eseguire anche per Switch1

Quarto passaggio

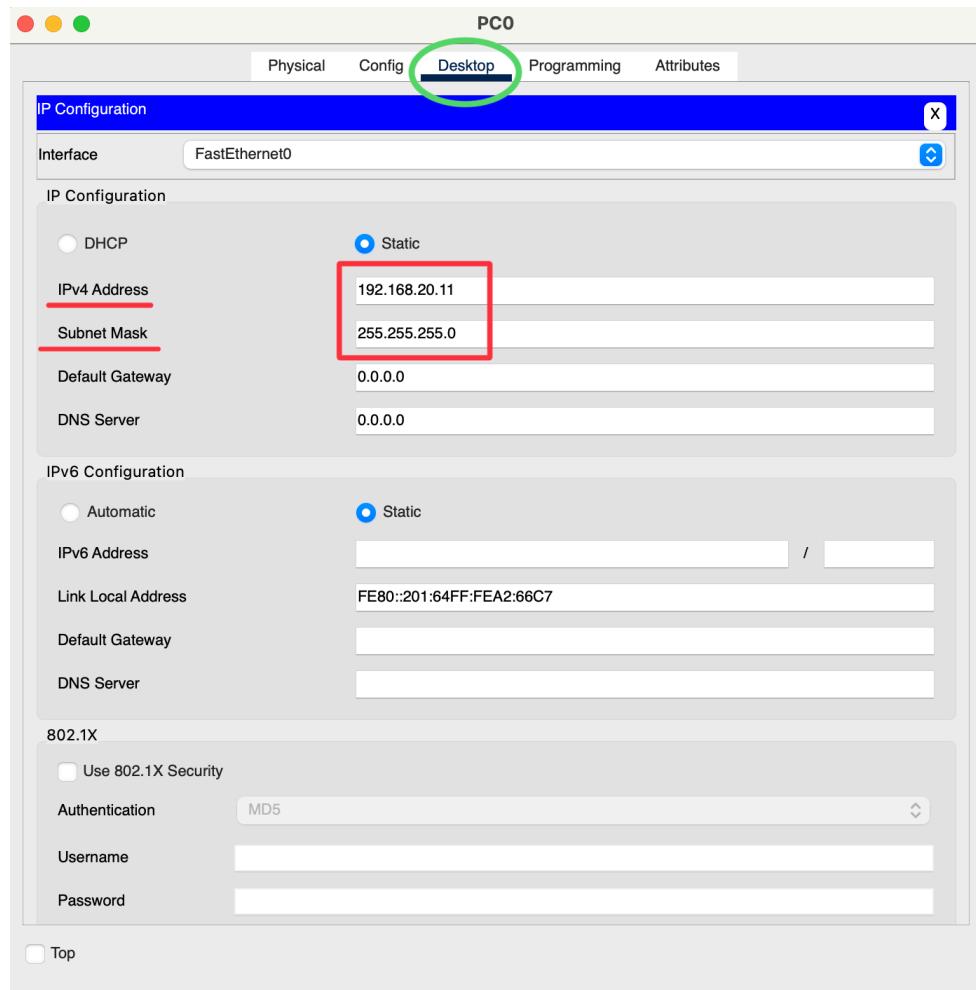
A questo punto si vogliono dare degli indirizzi IP ai vari PC/laptop. Procediamo prendendo singolarmente ciascun host e apriamo la sua pagina di configurazione: [Desktop > IP Configuration](#).

Cominciamo a inserire degli indirizzi IP coerenti con la VLAN. In questo caso il gateway va lasciato vuoto o comunque in valore di default, in quanto non stiamo utilizzando un router.

⚠ Caution

Non dimenticarsi di inserire la subnet mask (basta cliccare sul blank apposito e viene inserita in automatico).

Esempio visivo:



Quinto passo

Una volta settato tutto, non ci resta che rivelare la struttura completa della rete e di testare il tutto.

Per testare la rete:

- Si va, per esempio, su un PC o Laptop di VLAN10 (ex - Laptop0 su Switch0);

- Pingo l'altro host della VLAN10 (Laptop3 su Switch1) - in questo caso deve funzionare ✓
- Se provo a pingare un host di VLAN diversa (esempio Laptop0 - PC0) non funziona ✗

Note

Ripeto questo procedimento per tutte le altre VLAN.

Esempio di ping andato a buon fine:

```
C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=17ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 4ms
```

Esempio di ping non andato a buon fine:

```
C:\>ping 192.168.20.11

Pinging 192.168.20.11 with 32 bytes of data:

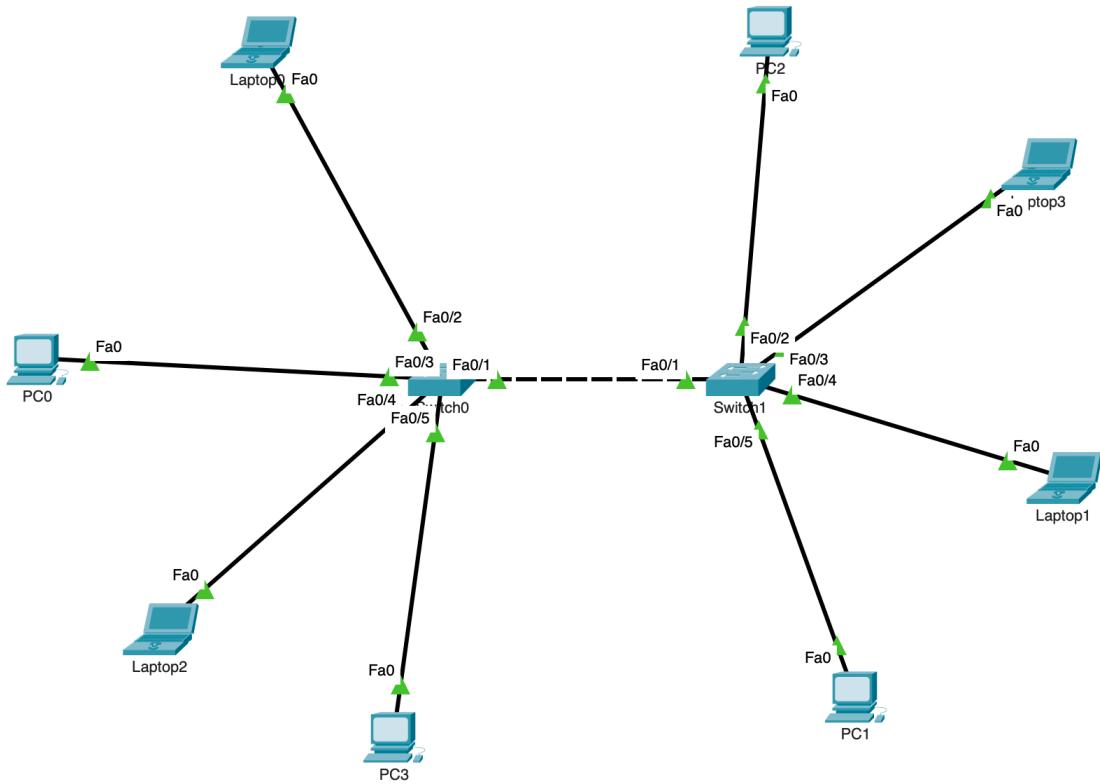
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Se tutto va bene si dimostra che:

- Il TRUNK funziona perché gli host sulla stessa VLAN ma su switch diversi comunicano;
- Le VLAN sono separate.

Di seguito lo schema completo della rete:



Conclusioni e considerazioni

L'esercizio è concluso e completo in tutte le sue parti. Più avanti ho intenzione di aggiungere un multilayer switch per la comunicazione delle VLAN.

Considerazione 1

Perché si è scelto di usare la VLAN per questo progetto? Suddividiamo due case study:

- **Cosa sarebbe successo se non avessi usato la VLAN?**
 - Tutti i PC riceverebbero i pacchetti di tutti, in quanto esiste un unico dominio d broadcast. Questo comporta ad avere una rete più lenta e meno sicura.
 - Ci sarebbe una "lack of logic separation", ovvero una mancanza di separazione logica.
- **Cosa abbiamo ottenuto usando le VLAN?**
 - Segmentazione logica della rete: con soli due Switch, ho creato quattro reti virtuali indipendenti.
 - Gli host di una VLAN non vedono quelli delle altre VLAN.
 - Sicurezza: si riduce il rischio che gli utenti non autorizzati accedano a risorse interne.
 - Flessibilità grazie alla presenza del TRUNK.

Quindi alla domanda iniziale la risposta è: si è scelto di utilizzare le VLAN perché permettono di segmentare logicamente la rete, migliorando sicurezza, efficienza e gestione.

Considerazione 2

PRO e CONTRO delle VLAN

Per descrivere i pro e i contro delle VLAN userò la seguente tabella:

VANTAGGI	SVANTAGGI
Segmentazione logica della rete	Configurazione più complessa rispetto a una LAN piatta
Maggiore sicurezza - VLAN isolano il traffico tra reparti diversi	Richiedono trunking tra gli switch, se non configurato bene le VLAN non comunicano
Riduzione del traffico di broadcast - maggiore efficienza	Per la comunicazione tra VLAN serve un router oppure uno switch multilayer
Flessibilità: se voglio spostare un host in un'altra VLAN lo posso fare	Rischio errori se le port vengono assegnate alla VLAN sbagliata
Scalabilità: posso aggiungere nuove VLAN	
Migliore prestazione: la separazione del traffico evita il "collo di bottiglia"	

Le VLAN convengono quando la rete deve essere organizzata in più gruppi logici che richiedono isolamento, sicurezza e gestione semplice. Sono particolarmente utili in reti medio-grandi, dove il traffico broadcast può diventare un problema e la sicurezza è quello che ci interessa maggiormente.

Nelle reti molto piccole, invece, l'uso della VLAN potrebbe risultare esagerato.