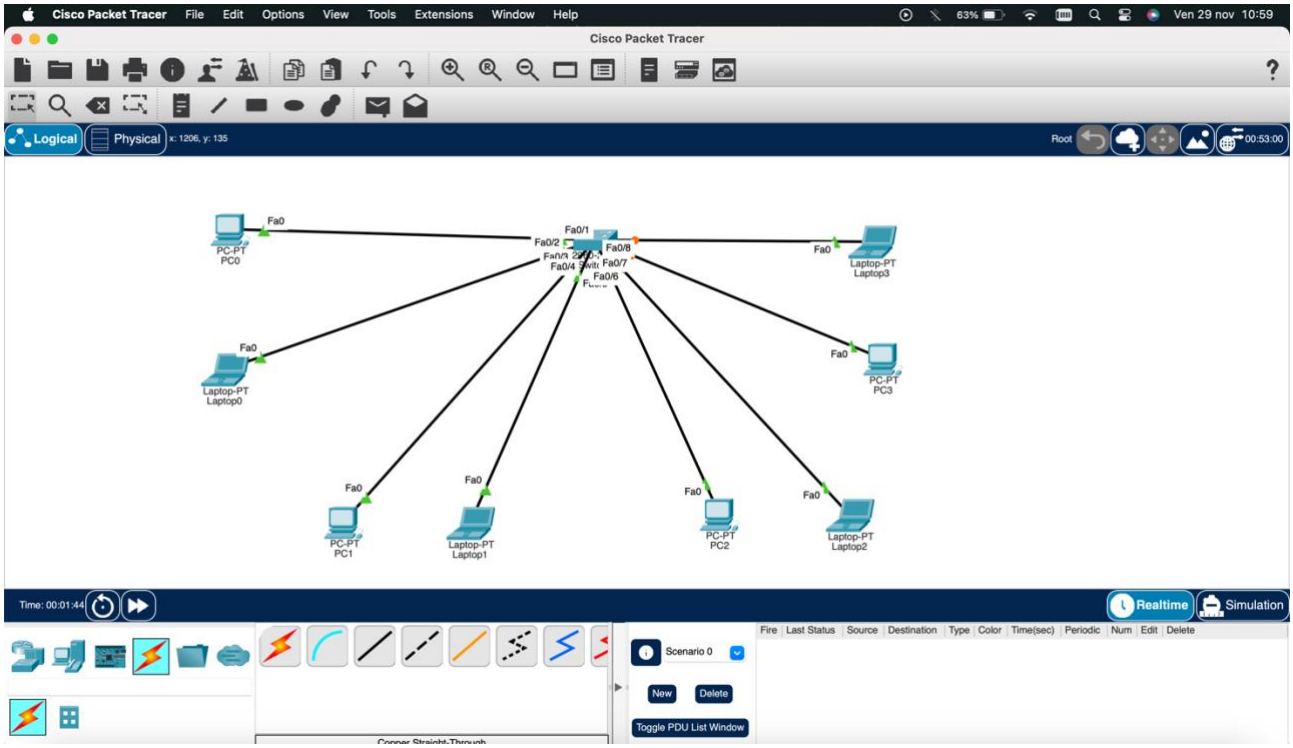
REPORT PROGETTO S1/L5 PACKET TRACER- VLAN

Esercizio: L'esercizio di oggi riguarderà la creazione di una rete segmentata con 4 VLAN diverse. Oltre agli screenshot del progetto, spiegherete le motivazioni per cui si è scelto di ricorrere alle VLAN.

Per procedere con la realizzazione di questo progetto, avremo bisogno di uno switch e almeno un host per ogni VLAN che vogliamo configurare. Nel mio caso, ho inserito 2 host per ogni VLAN, collegandoli allo switch tramite i cavi straight-through.
Ecco lo schema iniziale:



E’ importante ricordare a quale porta è assegnato ogni host poiché ci servirà nella configurazione delle VLAN nello switch.

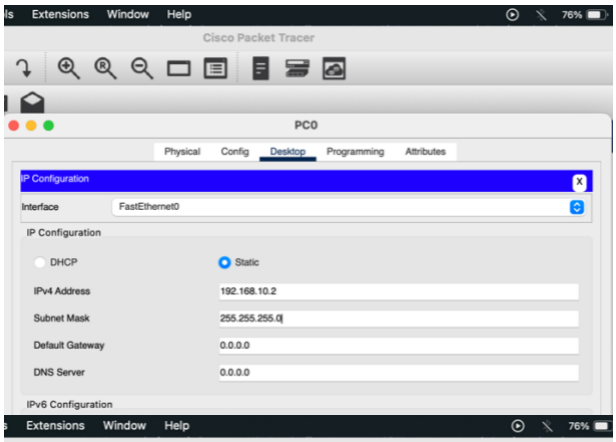
Assegniamo adesso un indirizzo IP per ogni host presente all’interno di questa rete.
Gli indirizzi che ho utilizzato sono:

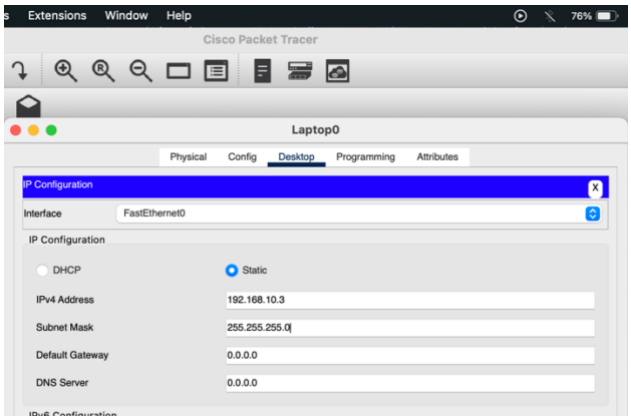
PC0: 192.168.10.2
LAPTOP0: 192.168.10.3

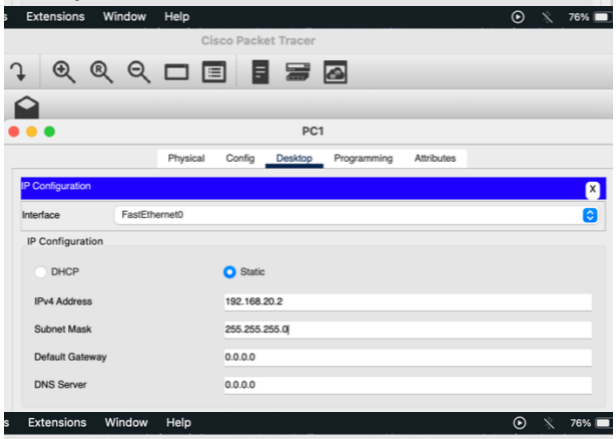
PC1: 192.168.20.2
LAPTOP1: 192.168.20.3

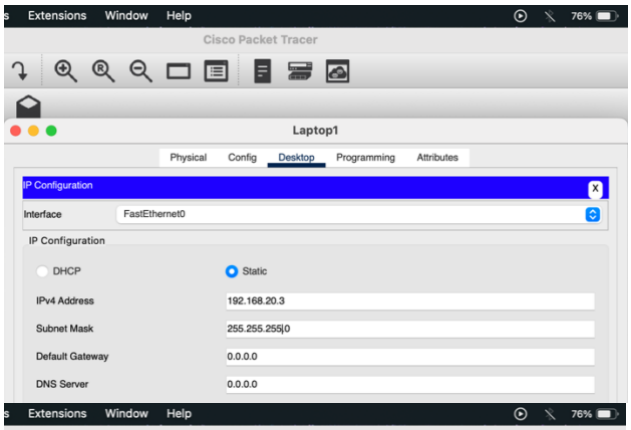
PC2: 192.168.30.2
LAPTOP2: 192.168.30.3

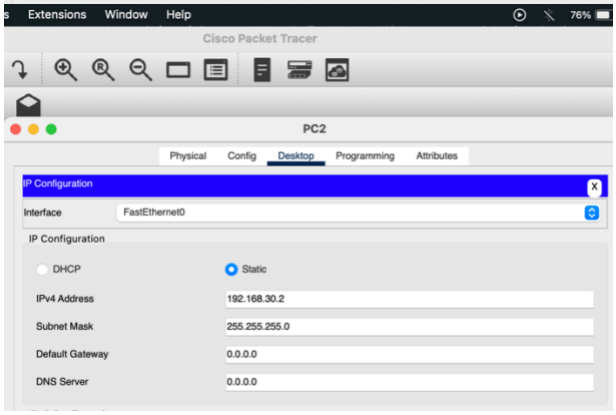
PC3: 192.168.40.2
LAPTOP3: 192.168.40.3

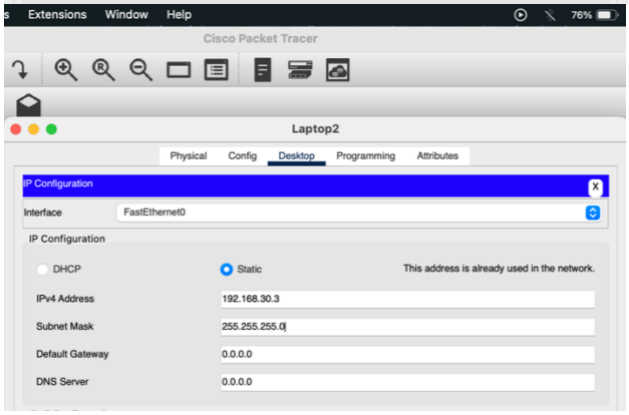


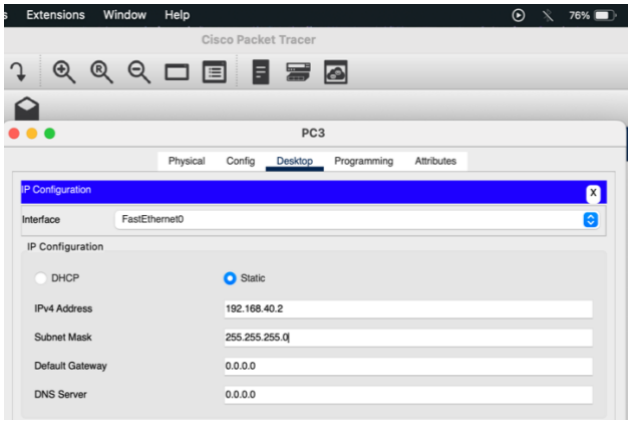


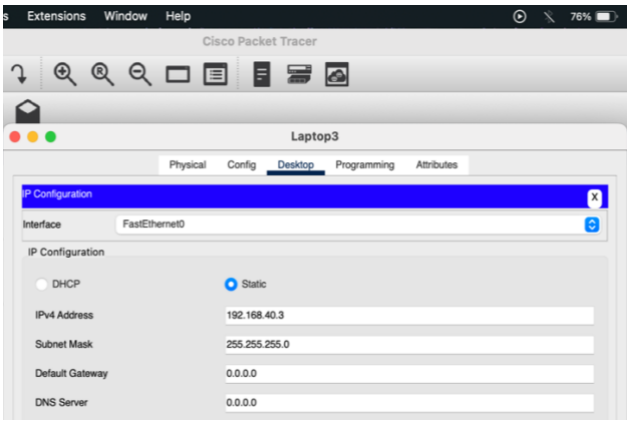




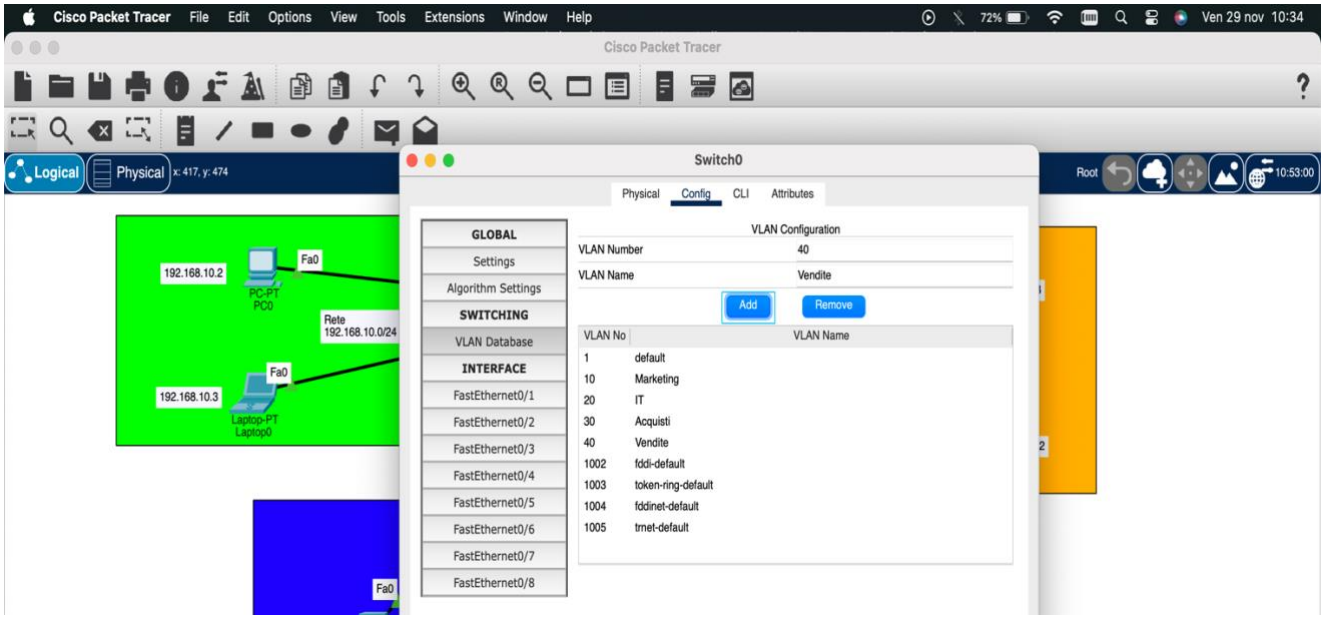






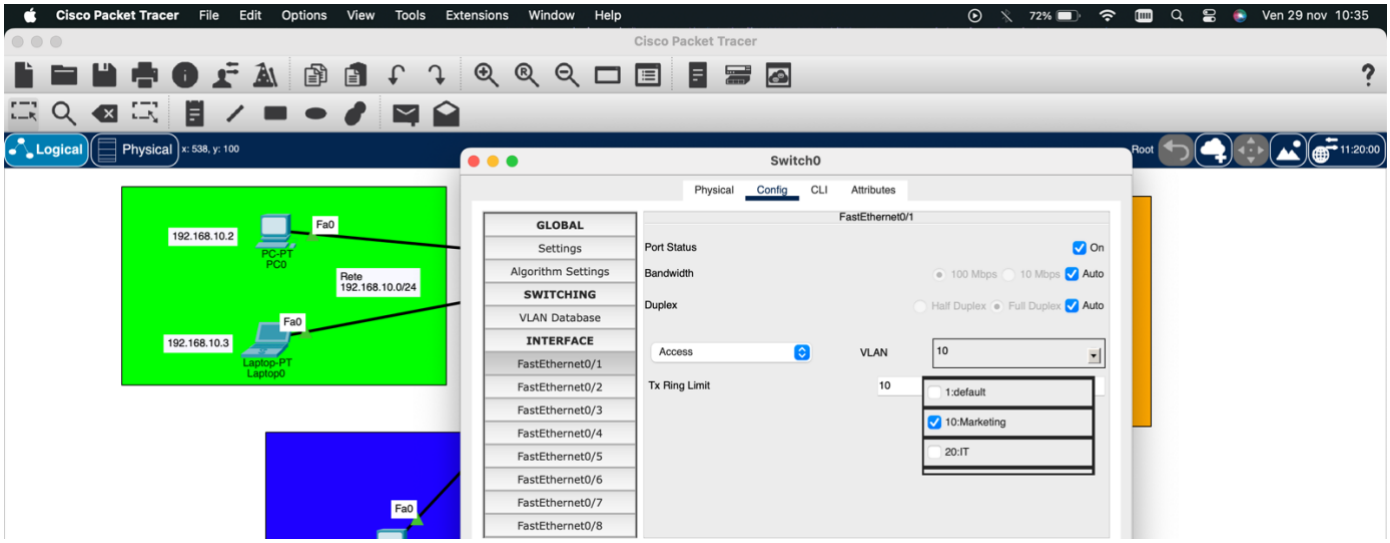


Il passo successivo è quello più importante, dopo aver configurato i vari host, dobbiamo configurare lo switch. Per prima cosa, aggiungo le varie VLAN assegnando un nome ed un numero ad ognuna di esse:

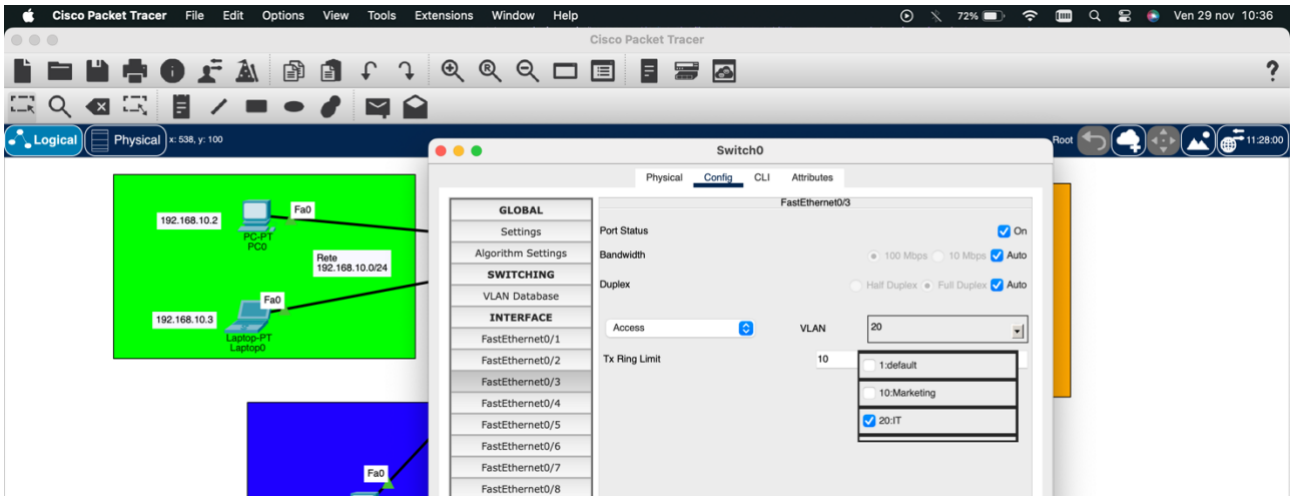


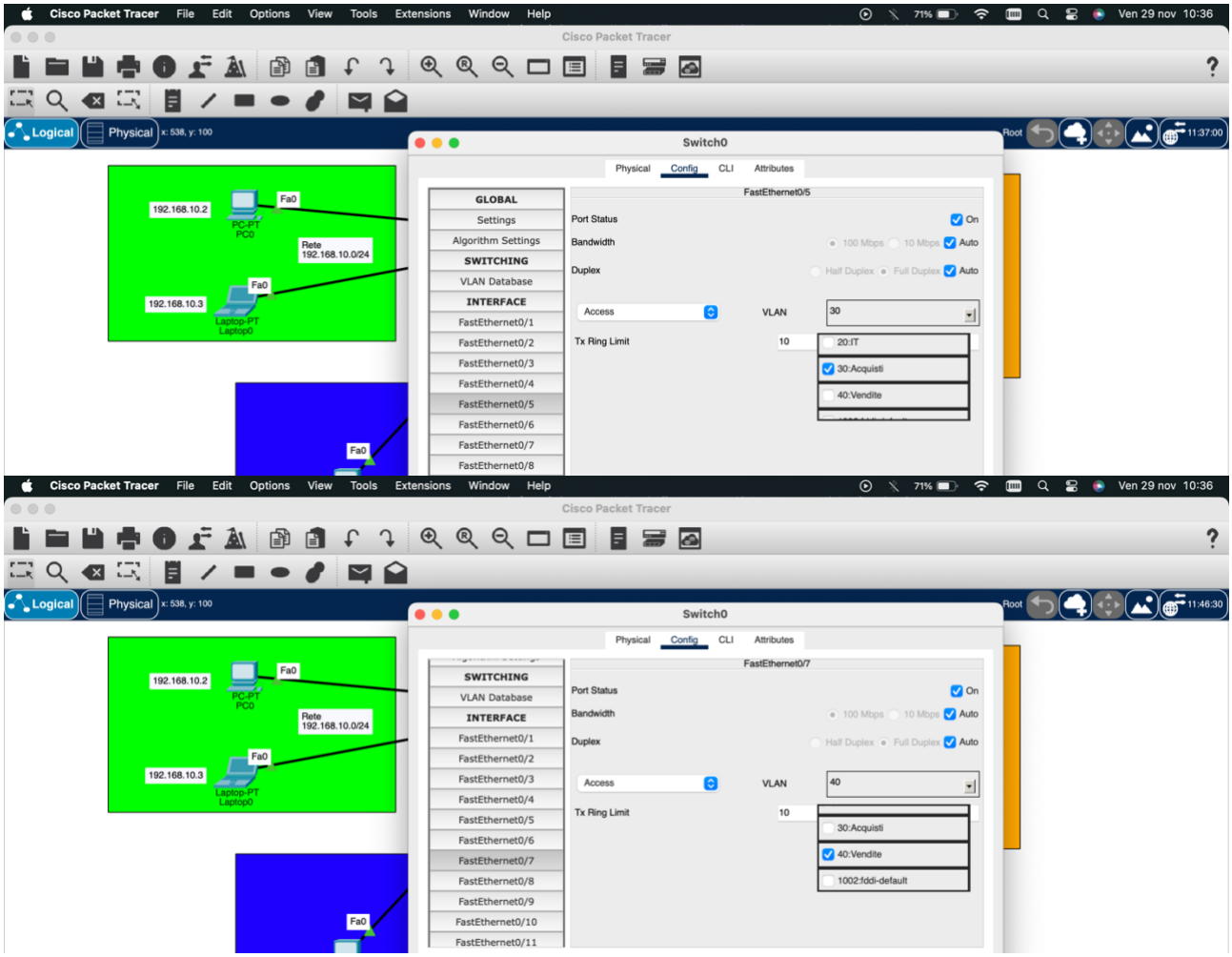
Successivamente, andiamo ad assegnare le nostre 4 VLAN a 4 differenti porte dello switch, ovviamente utilizzeremo quelle precedentemente utilizzare per collegare i vari host allo switch.

Sapendo che i primi due host sono connessi alla FastEthernet0/1 e 0/2, andrò ad assegnare quelle porte alla VLAN 10 nominandola “Marketing”.



Così facendo creerò la mia prima VLAN alla quale saranno collegati gli Host PC0 e LAPTOP0.
Utilizzando la stessa procedura con differenti porte dello switch configurerò anche le altre 3 VLAN:



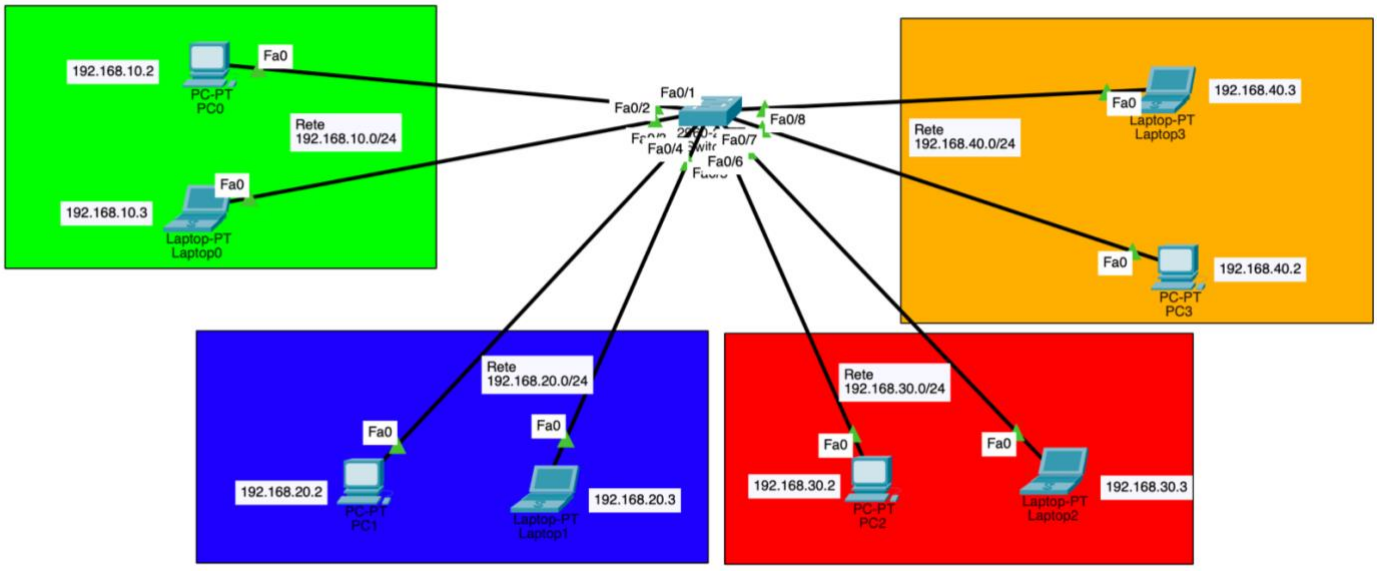


PROVA PACCHETTI: Per verificare il funzionamento delle VLAN, ho effettuato una prova di invio pacchetti:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Laptop0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC0	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	Laptop1	ICMP		0.000	N	2	(edit)	(delete)
	Failed	PC1	PC2	ICMP		0.000	N	3	(edit)	(delete)

Come possiamo vedere, la comunicazione avviene correttamente tra gli host facenti parte della stessa VLAN, mentre non avviene la comunicazione tra gli host che fanno parte di VLAN differenti.

Lo schema finale del progetto è il seguente:



PERCHE' SI RICORRE ALLE VLAN?
CONSIDERAZIONI FINALI:

L'uso delle VLAN è utile per garantire sicurezza, gestione del traffico e per separare i gruppi di lavoro all'interno di una stessa infrastruttura fisica.

Le VLAN permettono di suddividere una rete fisica in più reti logiche. Questo significa che, pur essendo connessi allo stesso switch fisico, i dispositivi appartenenti a VLAN diverse non potranno comunicare tra loro senza un dispositivo di routing.
Questo è utile per isolare gruppi di utenti, evitando che il traffico non necessario o pericoloso circoli tra diversi dipartimenti o aree della rete.
Separare il traffico tra diverse VLAN aumenta la sicurezza della rete. Per esempio, se una VLAN è utilizzata per i terminali amministrativi e un'altra per i computer degli utenti, è possibile impedire che un attacco o una violazione su una VLAN si propaghi ad altre aree della rete.
Le VLAN riducono il traffico di broadcast, poiché i pacchetti broadcast vengono limitati ai dispositivi appartenenti alla stessa VLAN. Questo

migliora le prestazioni della rete, poiché i pacchetti di broadcast non devono essere inoltrati a tutti i dispositivi della rete fisica, ma solo a quelli della stessa VLAN.

Le VLAN permettono una maggiore flessibilità nella progettazione della rete. Non è necessario cablare fisicamente nuove linee o cambiare l'infrastruttura ogni volta che si desidera separare nuovi gruppi di lavoro. Basta configurare le VLAN sui dispositivi di rete esistenti, risparmiando tempo e risorse.