

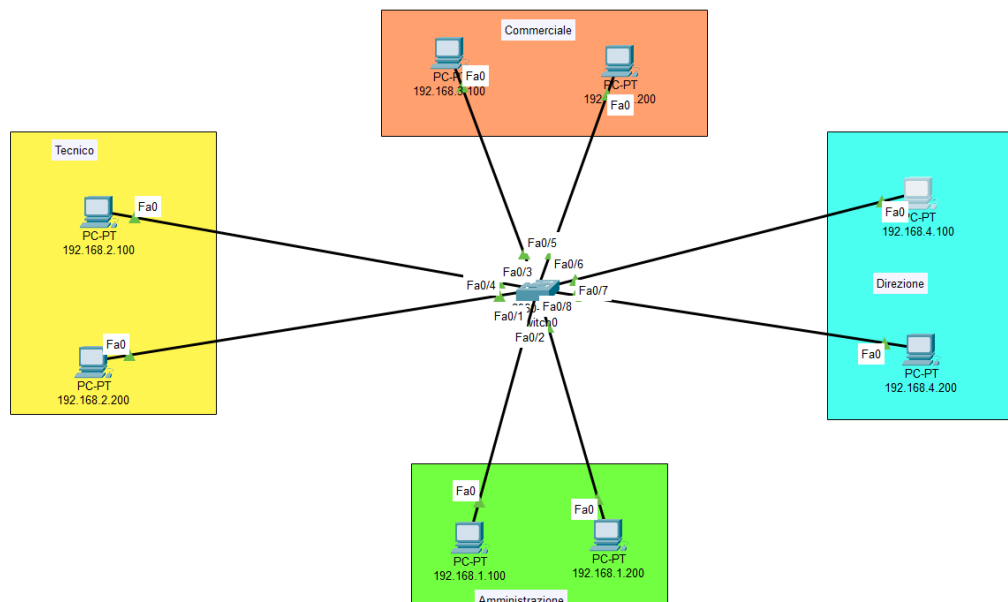
## PROGETTO S1 L5

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.

## RISPOSTA

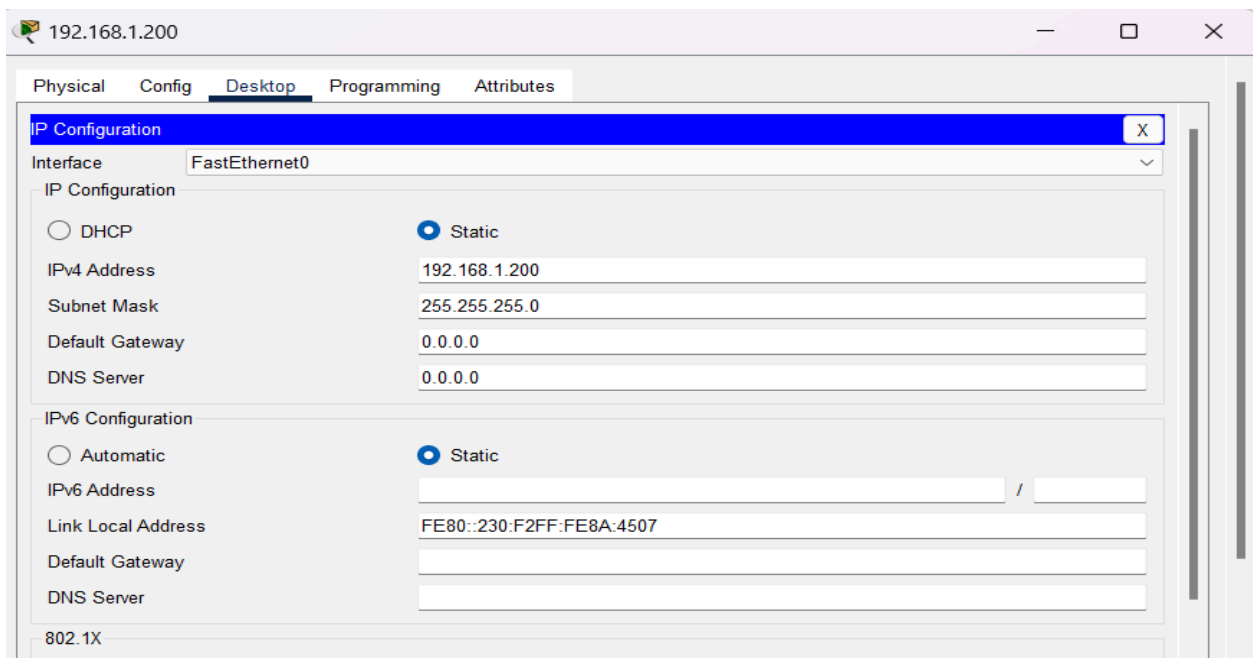
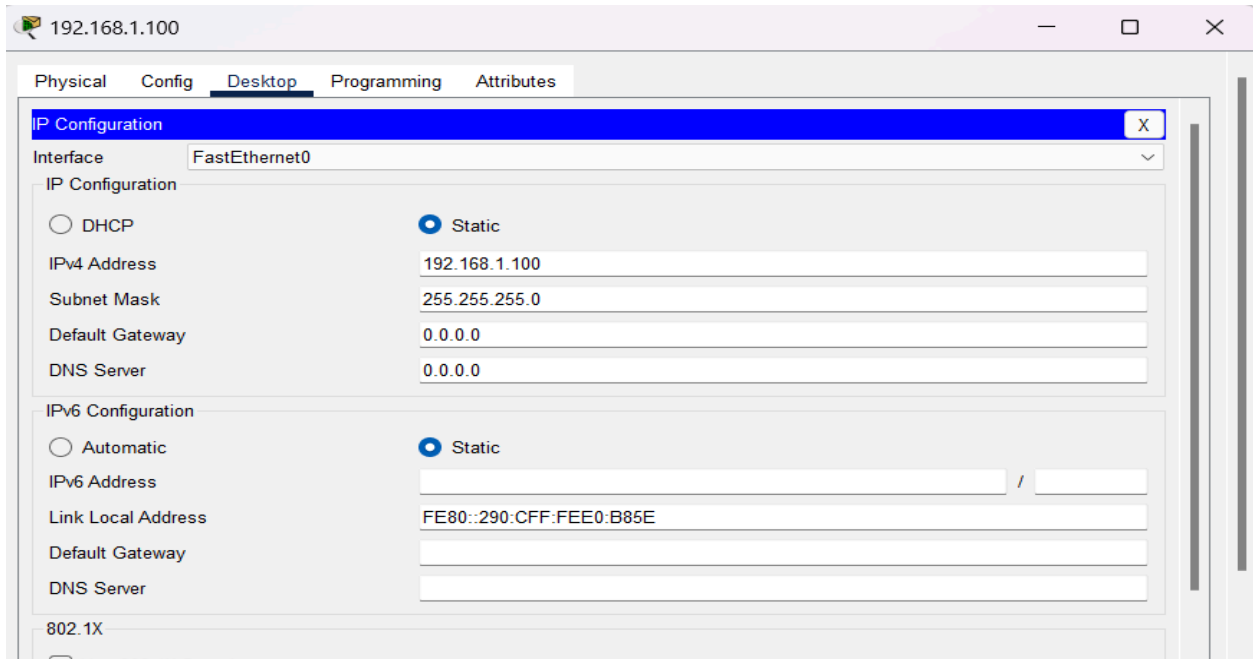
Per questo progetto ho immaginato un contesto aziendale suddiviso nei seguenti 4 reparti

- Amministrazione
- Tecnico
- Commerciale
- Direzione



Dopo aver creato i vari reparti assegno loro delle colorazioni per distinguerli meglio (Amministrazione in verde - Tecnico in giallo - Commerciale in rosa - Direzione in azzurro).

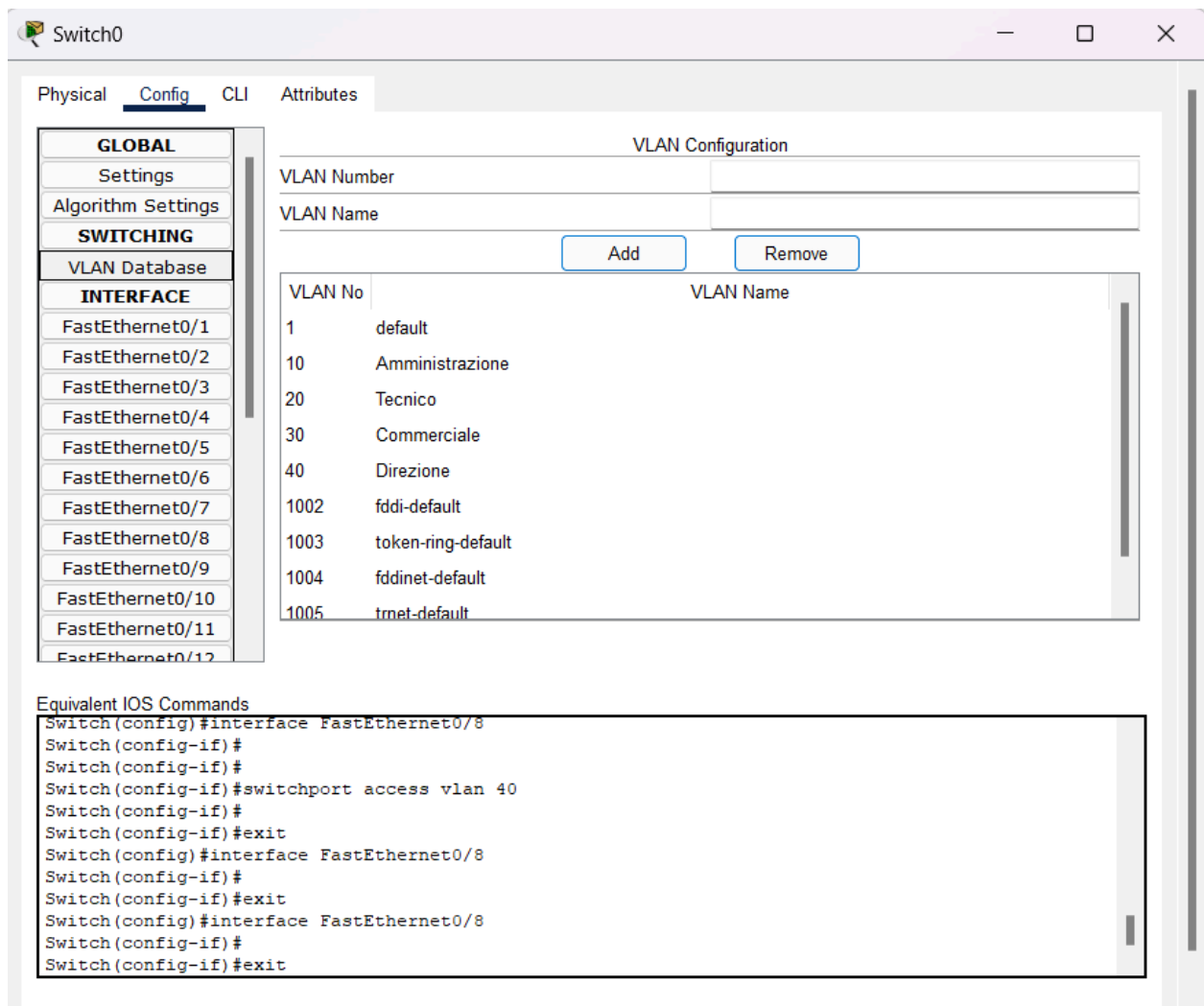
Ora comincio con l'assegnazione degli indirizzi IP e delle Subnet Mask per ciascun PC utilizzando la sezione Desktop > IP Config. Come da immagine sottostante.



In questo caso ho configurato gli Indirizzi IP di due dispositivi della stessa VLAN (Amministrazione) assegnando rispettivamente al PC0 l'IP 192.168.1.100 ed al PC1 l'IP 192.168.1.200 con subnet mask 255.255.255.0.

Ho ripetuto questo processo per tutti i dispositivi di ogni VLAN.

Ora passiamo allo Switch, dove andrò a configurare le VLAN e successivamente ad assegnare le porte alle VLAN.

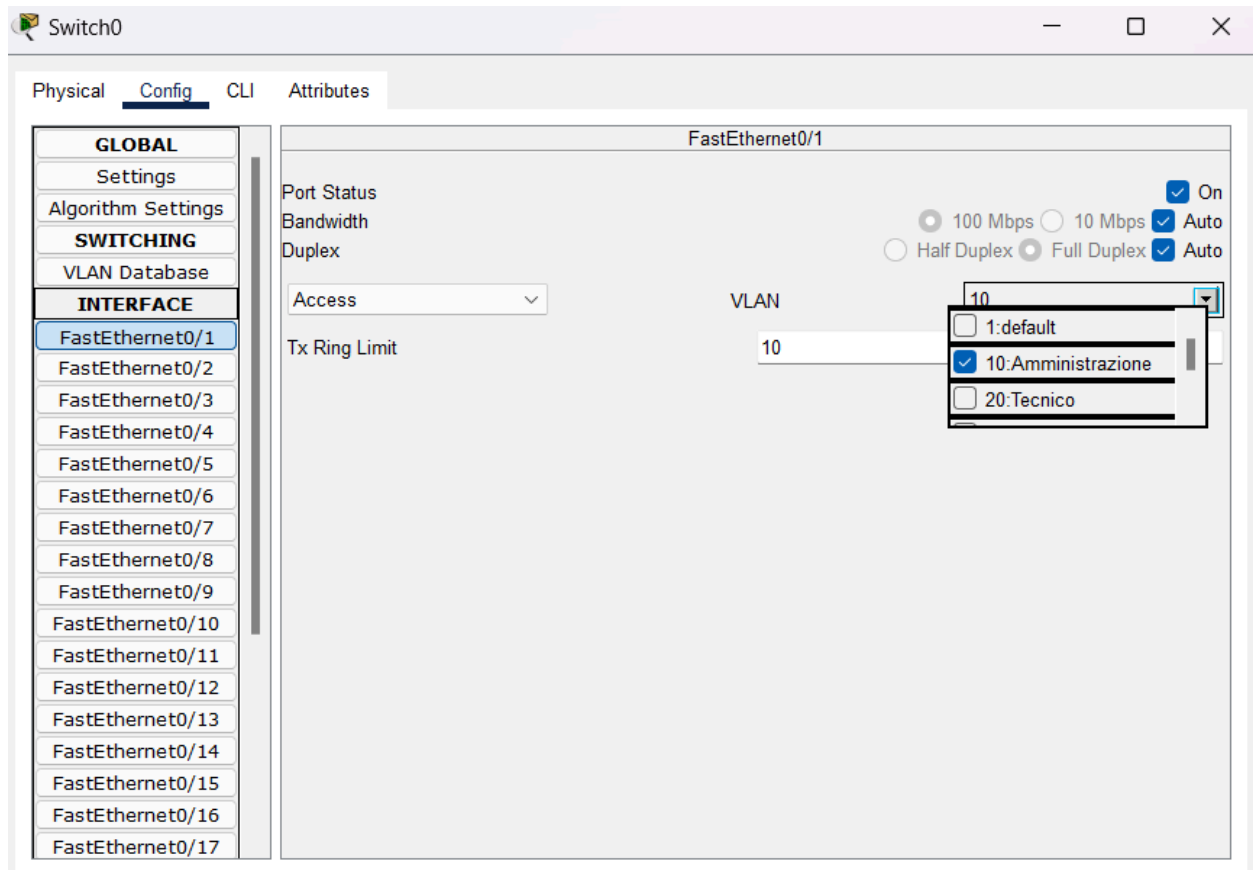


Come da immagine, andando sulla sezione VLAN Database vado a creare le 4 VLAN assegnando a ciascuna il proprio VLAN Number e VLAN Name, ottenendo

- 10 Amministrazione
- 20 Tecnico
- 30 Commerciale
- 40 Direzione

Il passo successivo è l'assegnazione delle porte alle VLAN nella sezione Config > Interface

- PC 192.168.1.100 e PC 192.168.1.200 su Fa0/1 e Fa0/2 >>> VLAN 10 Amministrazione

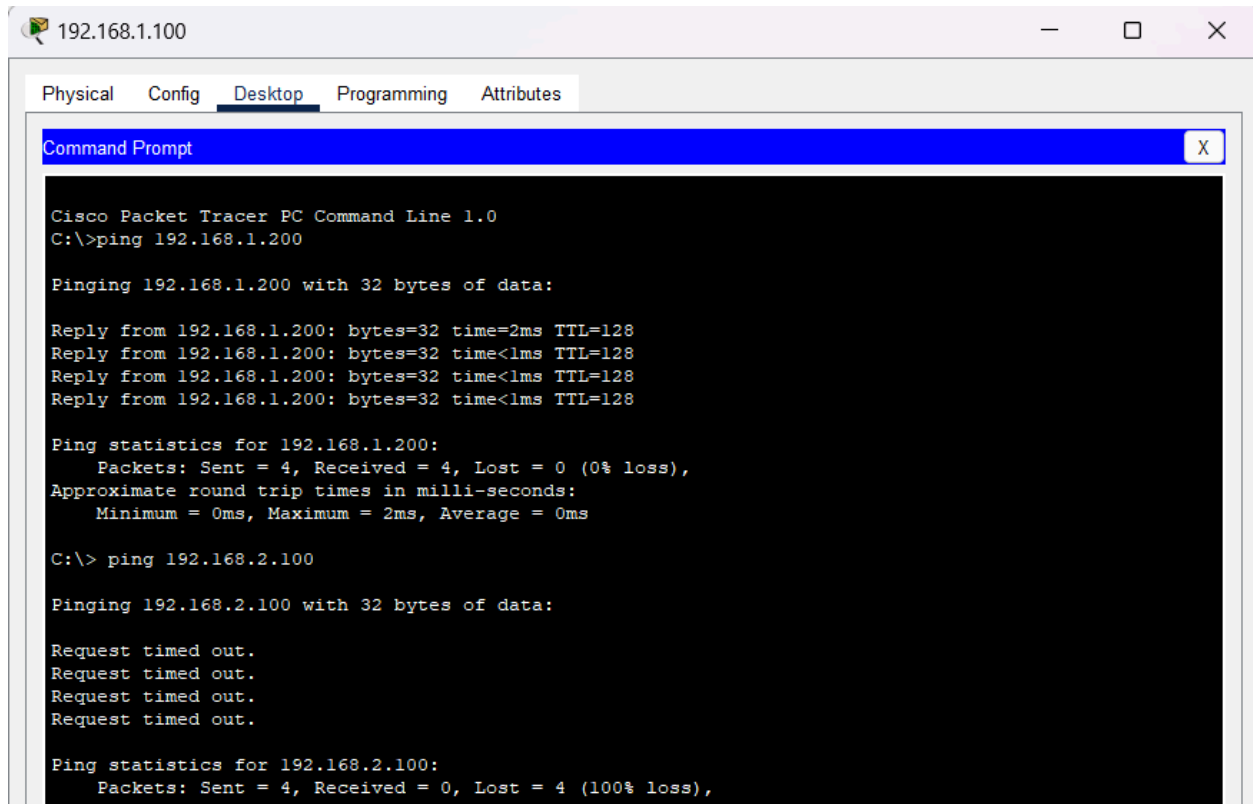


Ho ripetuto questo processo per gli altri dispositivi, ottenendo

- PC 192.168.2.100 e PC 192.168.2.200 su Fa0/3 e Fa0/4 >>> VLAN 20 Tecnico
- PC 192.168.3.100 e PC 192.168.3.200 su Fa0/5 e Fa0/6 >>> VLAN 30 Commerciale
- PC 192.168.4.100 e PC 192.168.4.200 su Fa0/7 e Fa0/8 >>> VLAN 40 Direzione

A questo punto procedo con i test di connettività, dimostrando per ciascuna VLAN che i dispositivi al loro interno comunicano tra loro e che siano isolate dalle altre VLAN non permettendo la comunicazione.

Procedo quindi con l'invio di un ping, utilizzando la sezione Desktop > Command Prompt, dal PC 192.168.1.100 al PC 192.168.1.200 (che si trovano nella stessa VLAN Amministrazione) per verificare che i dispositivi comunichino tra loro.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.200: bytes=32 time=2ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\> ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

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

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Notiamo che i dispositivi della stessa VLAN Amministrazione comunicano correttamente. Ora procedo con il testare che le VLAN siano isolate e non comunichino tra loro.

Utilizzo il comando ping da PC 192.168.1.100 ( Amministrazione) a PC 192.168.2.100 ( Tecnico) ed effettivamente il ping non avviene e da risposta “ Request Timed Out”, a dimostrazione che VLAN differenti in questo caso non comunicano tra loro.

## CONCLUSIONE

In questo scenario scegliamo di ricorrere alle VLAN perchè

- Isolano i vari dipartimenti/reparti anche se condividono lo stesso switch fisico
- Riducono il dominio di broadcast, avendo ogni VLAN un dominio separato, si ha meno traffico inutile
- Migliorano la sicurezza dato che i dispositivi di una VLAN non comunicano con altre VLAN

In conclusione, questa struttura logica rende la rete più efficiente e sicura.

