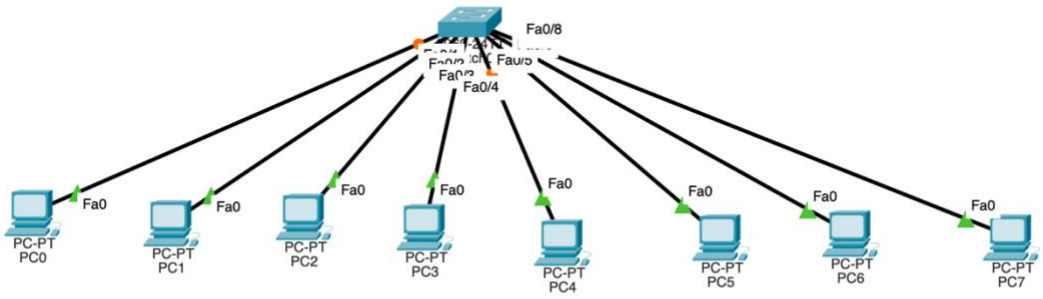
L'esercizio di oggi riguarderà la creazione di una rete segmentata con 4 VLAN diverse. Oltre agli screenshot del progetto, spiegherete le motivazioni per cui si è scelto di ricorrere alle VLAN.

Passaggi:

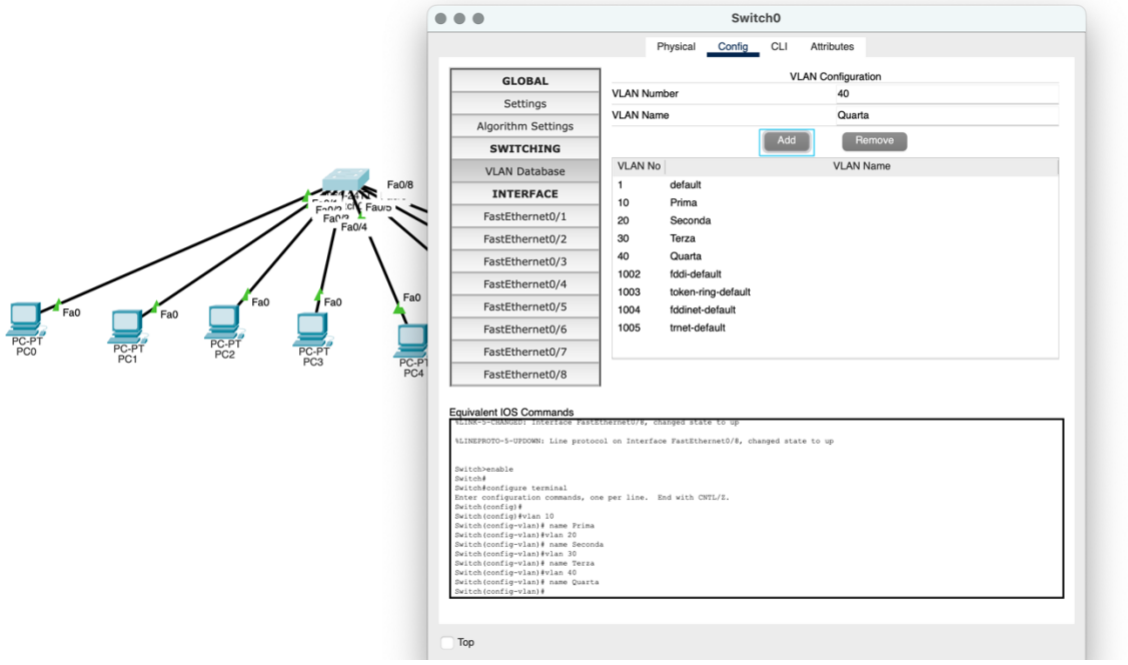
-Creare la topologia di rete:

1. Aggiungere i dispositivi:
    - Aggiungi uno Switch (Cisco 2960 o simile).
    - Aggiungi 8 PC.
    - Collegare i PC allo switch. Puoi usare i cavi copper straight-through per connettere ciascun PC a una porta dello switch.
2. Aggiungere un router (opzionale):
    - Se vuoi che le VLAN comunichino tra loro, avrai bisogno di un router. In caso contrario, puoi limitare la comunicazione all'interno delle VLAN. Per fare in modo che comunichino è necessario collegare il router allo switch tramite una porta trunk.



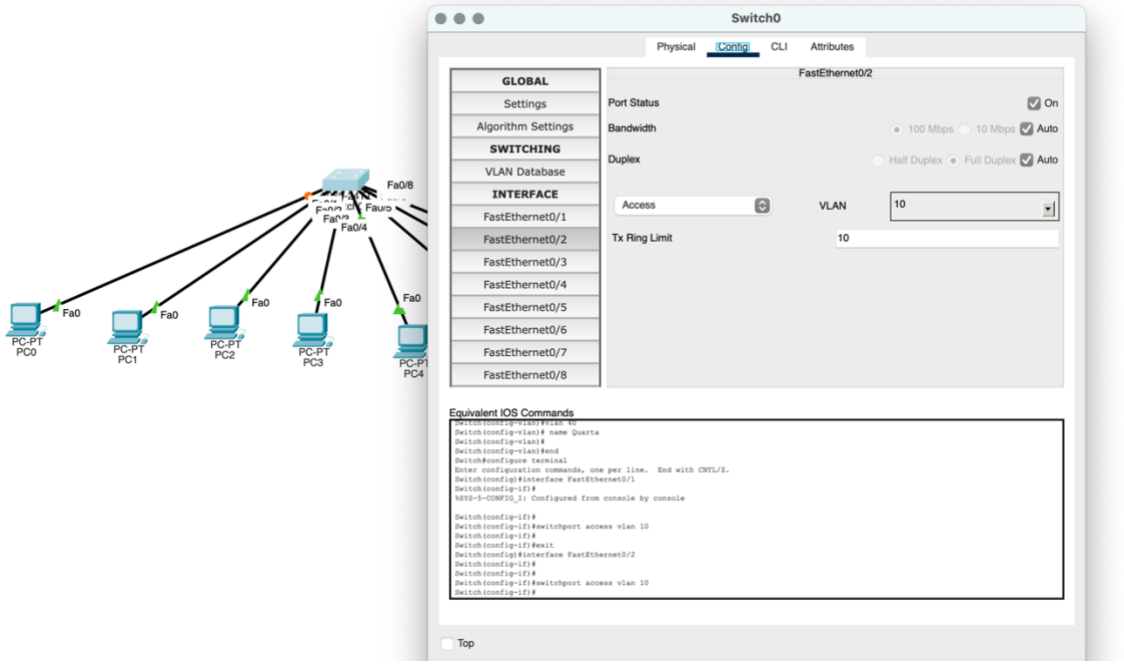
-Creare e configurare le 4 VLAN

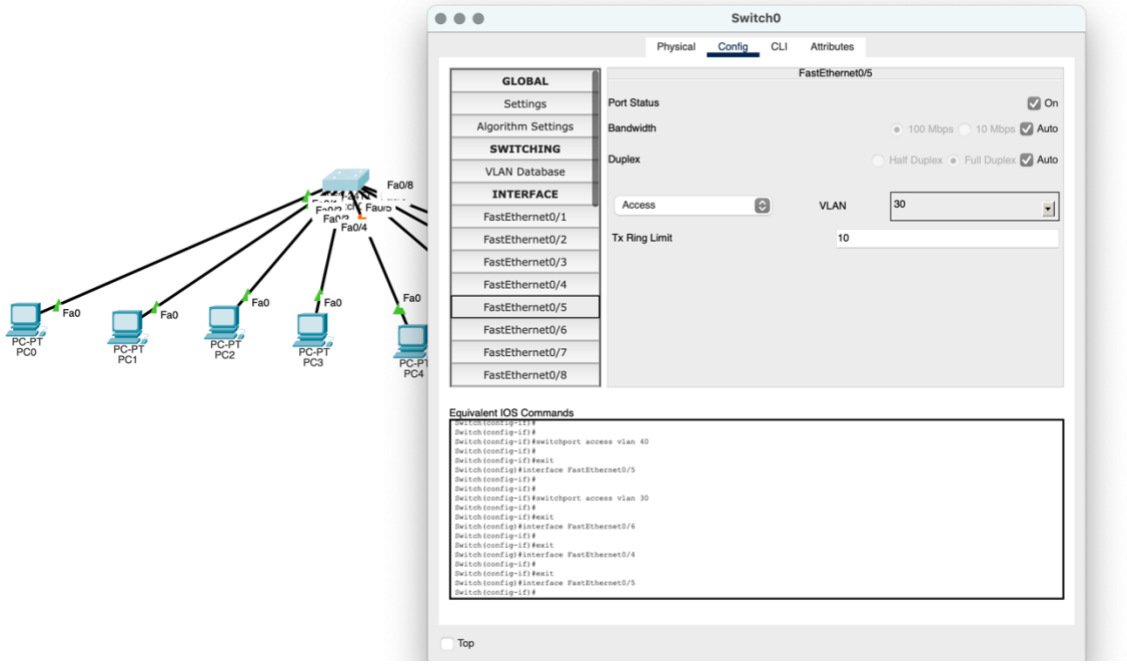
1. Accedere alla configurazione dello switch:
    - Clicca sullo Switch per aprire la finestra di configurazione.
    - Vai alla scheda "Config".
2. Creare le VLAN:
    - Nella sezione VLAN Database (sul lato sinistro), clicca su Add VLAN.
    - Crea la VLAN 10:
        - Inserisci VLAN Number :10 e il nome "Prima".
        - Clicca su OK per aggiungere la VLAN.
    - Ripeti per le altre VLAN:
        - VLAN 20 con nome "Seconda".
        - VLAN 30 con nome "Terza".
        - VLAN 40 con nome "Quarta".
3. Verifica la creazione delle VLAN:
    - Dopo aver creato tutte le VLAN, dovresti vederle elencate nel VLAN Database.



-Assegnare le porte dello switch alle VLAN:

1. Assegnare le porte:
    - Nella finestra di configurazione dello switch, vai alla sezione "Ports".
    - Ora assegna le porte ai rispettivi VLAN:
        - Porta FastEthernet 0/1 e 0/2: Assegna alla VLAN 10 (Prima).
        - Porta FastEthernet 0/3 e 0/4: Assegna alla VLAN 20 (Seconda).
        - Porta FastEthernet 0/5 e 0/6: Assegna alla VLAN 30 (Terza).
        - Porta FastEthernet 0/7 e 0/8: Assegna alla VLAN 40 (Quarta).
2. Configurare la modalità delle porte:
    - Le porte dovrebbero essere configurate come "Access" per ciascuna VLAN.

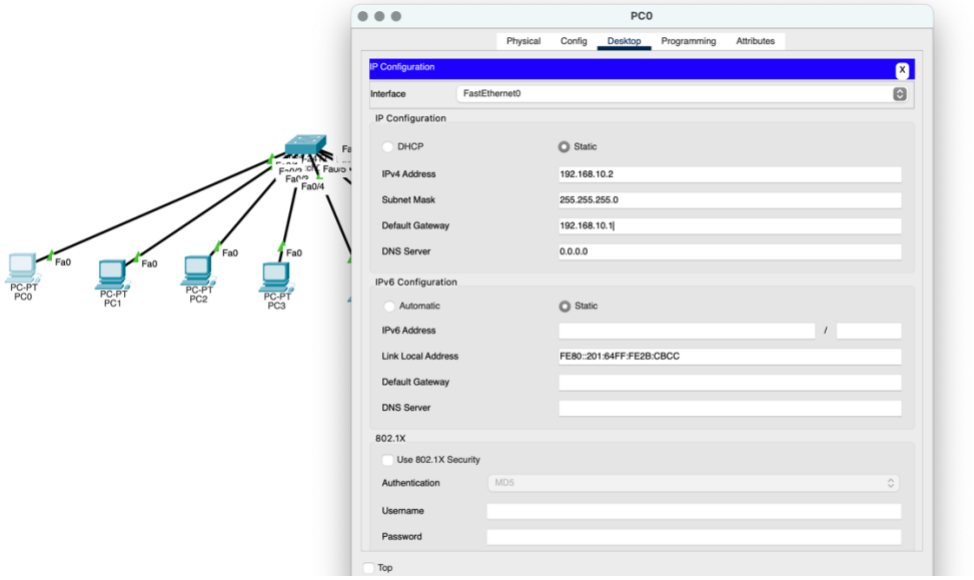


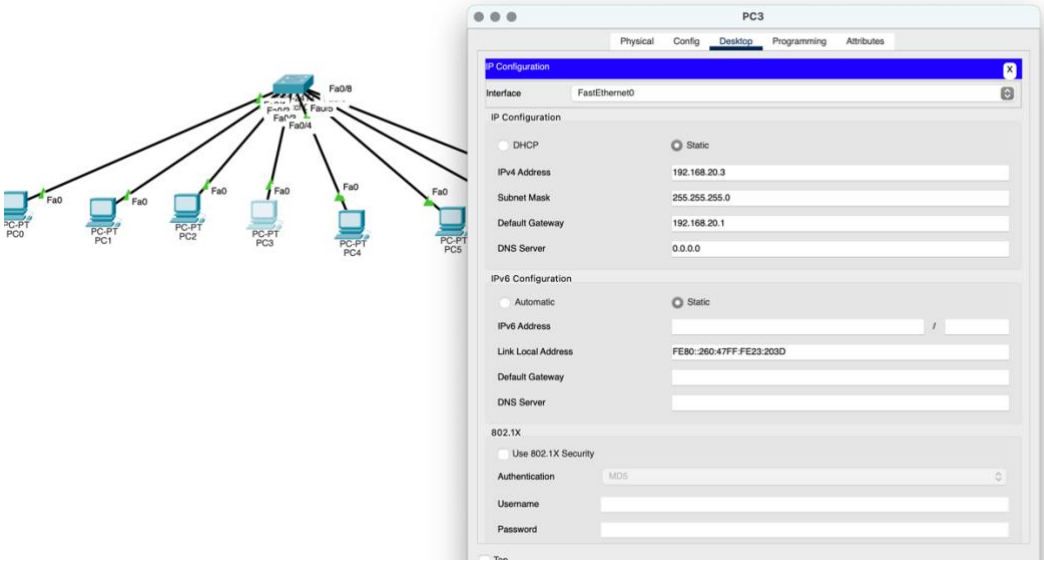


-Configurare gli indirizzi IP sui PC
Ogni PC deve appartenere a una VLAN, quindi assegna a ciascun PC un indirizzo IP nella stessa sottorete della VLAN a cui appartiene:

- VLAN 10 (Prima):
  - PC0: IP = 192.168.10.2, Subnet Mask = 255.255.255.0, Gateway = 192.168.10.1.
  - PC1: IP = 192.168.10.3, Subnet Mask = 255.255.255.0, Gateway = 192.168.10.1.
- VLAN 20 (Seconda):
  - PC2: IP = 192.168.20.2, Subnet Mask = 255.255.255.0, Gateway = 192.168.20.1.
  - PC3: IP = 192.168.20.3, Subnet Mask = 255.255.255.0, Gateway = 192.168.20.1.
- VLAN 30 (Terza):
  - PC4: IP = 192.168.30.2, Subnet Mask = 255.255.255.0, Gateway = 192.168.30.1.

    - PC5: IP = 192.168.30.3, Subnet Mask = 255.255.255.0, Gateway = 192.168.30.1.
- VLAN 40 (Quarta):
    - PC6: IP = 192.168.40.2, Subnet Mask = 255.255.255.0, Gateway = 192.168.40.1.
    - PC7: IP = 192.168.40.3, Subnet Mask = 255.255.255.0, Gateway = 192.168.40.1.

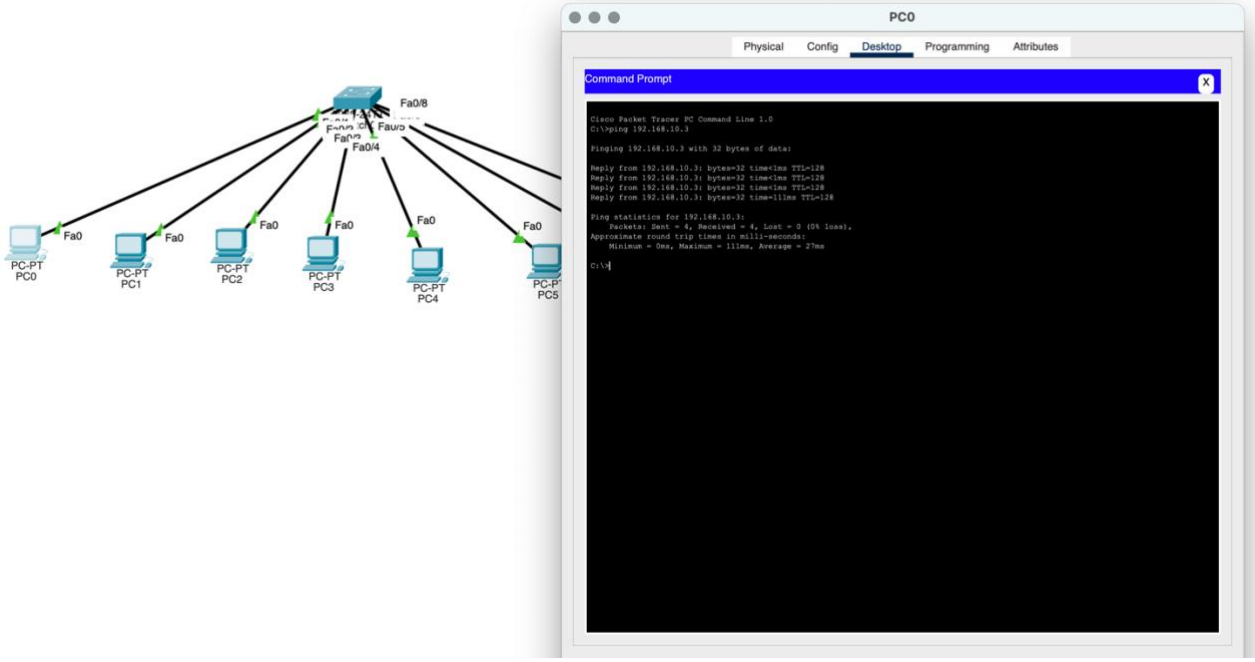


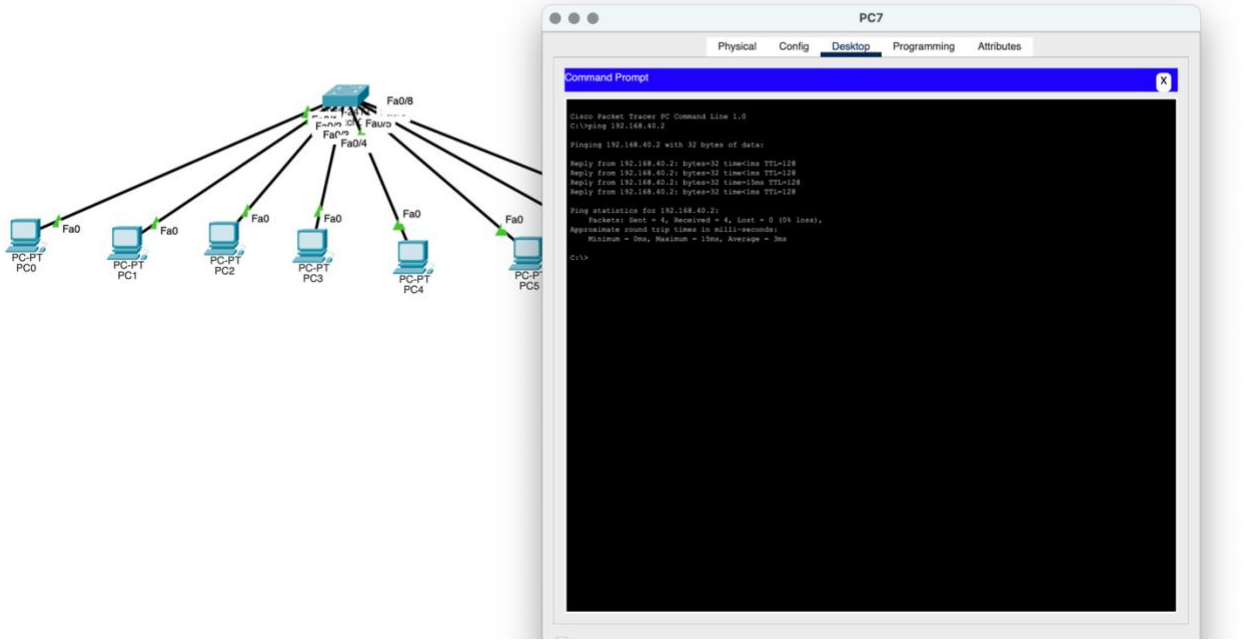


-Verifica la configurazione:

1. Ping tra PC nella stessa VLAN:
    - Prova a fare un ping tra i PC della stessa VLAN per verificare che siano in grado di comunicare correttamente.

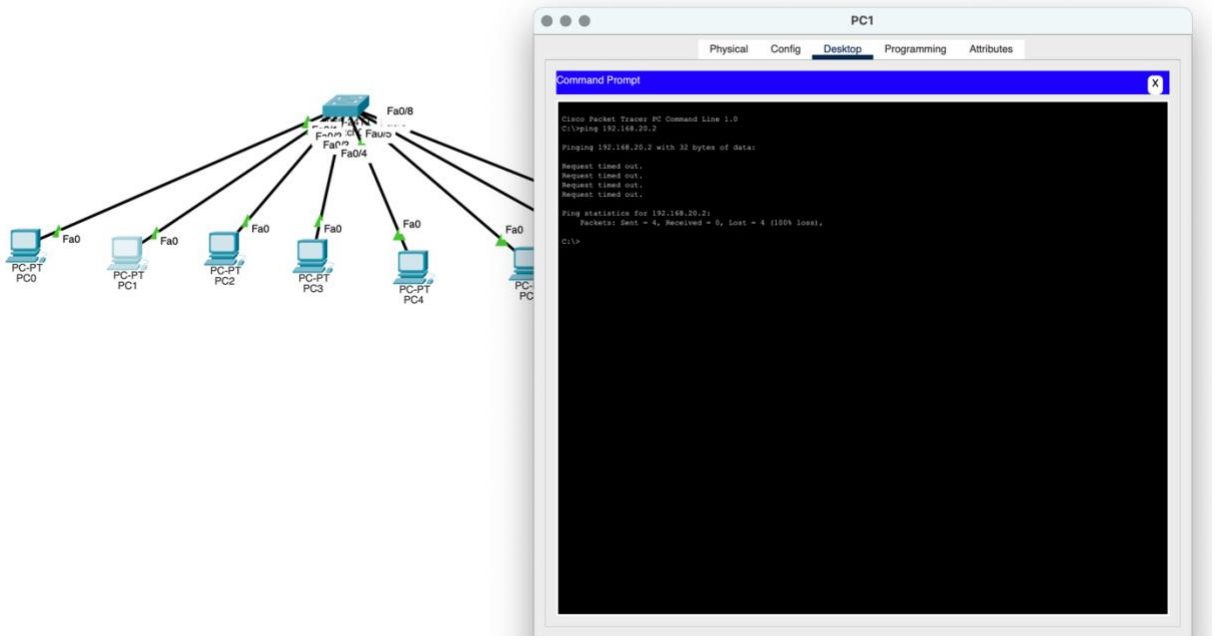
Dalle seguenti immagini si evince che i PC appartenenti alle stesse VLAN sono in grado di comunicare correttamente.





2. Verifica l'isolamento tra VLAN:
    - I PC che appartengono a VLAN diverse non dovrebbero potersi pingare direttamente tra loro. Questo è l'isolamento offerto dalle VLAN.

Nella seguente immagine ho provato a fare ping da PC1 a PC2 appartenenti a VLAN diverse e non ha funzionato in quanto le due VLAN sono isolate.



Motivazioni per l'uso delle VLAN:
Le VLAN (Virtual Local Area Network) sono utilizzate per segmentare una rete fisica in più reti logiche, con vantaggi significativi:

1. Sicurezza:
    - Le VLAN isolano i traffici delle diverse sezioni della rete. Ad esempio, i PC della VLAN “Prima” non possono accedere ai PC della VLAN “Seconda” senza passare attraverso il router, aumentando la sicurezza.
2. Gestione del traffico:
    - Ogni VLAN può avere il proprio dominio di broadcast, riducendo la congestione causata da traffico broadcast non necessario in altre aree della rete.
3. Organizzazione e separazione dei compiti:
    - Le VLAN permettono di separare facilmente i dispositivi in base al reparto o alla funzione, migliorando l'efficienza della gestione della rete.
4. Scalabilità:
    - Le VLAN possono essere facilmente aggiunte o modificate senza la necessità di cambiare la struttura fisica della rete.
5. Ottimizzazione delle risorse:
    - Separando i traffici delle diverse VLAN, è possibile ottimizzare le risorse della rete (come la larghezza di banda), riducendo i conflitti e migliorando le prestazioni generali.

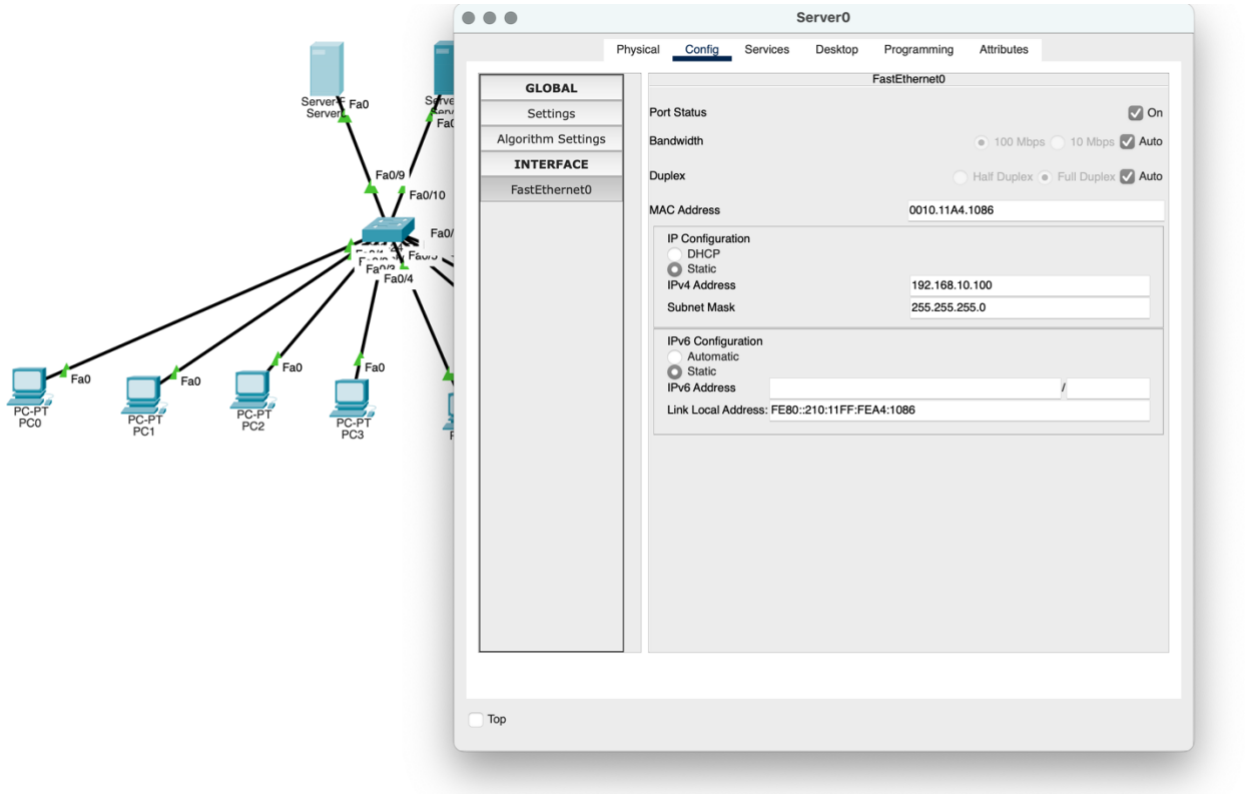
-Esercizio bonus:
Nella rete inserite un server dns e un server web, separati in modo che da un pc sia possibile andare sulla pagina web helloworld.html.

Aggiungiamo due server alla rete, uno per il DNS e un per il web:
Ora, aggiungiamo due server alla rete, uno per il DNS e uno per il web.

1. Server DNS:
    - Trascina un server nella topologia di rete.
    - Collegalo allo switch.
    - Vai nella scheda Config del server DNS e assegna un indirizzo IP (ad esempio 192.168.10.100 per la VLAN 10.

2. Server Web:
    - Trascina un altro server nella rete, collegalo allo switch.
    - Vai nella scheda Config del server web e assegna un indirizzo IP (ad esempio 192.168.10.200 nella VLAN 10).

Vai alla scheda HTTP e abilita il servizio HTTP (selezionando "On").



Da adesso in poi non sono riuscito ad andare avanti, ho provato a fare ping da PC0 o PC1 verso il server DNS ma risultava sempre errore, mentre il ping tra i due PC andava a buon fine.