

PROGETTO S1/L4

L'esercizio di oggi ha come obiettivo la creazione di una rete segmentata utilizzando 4 VLAN (Virtual Local Area Network) diverse.

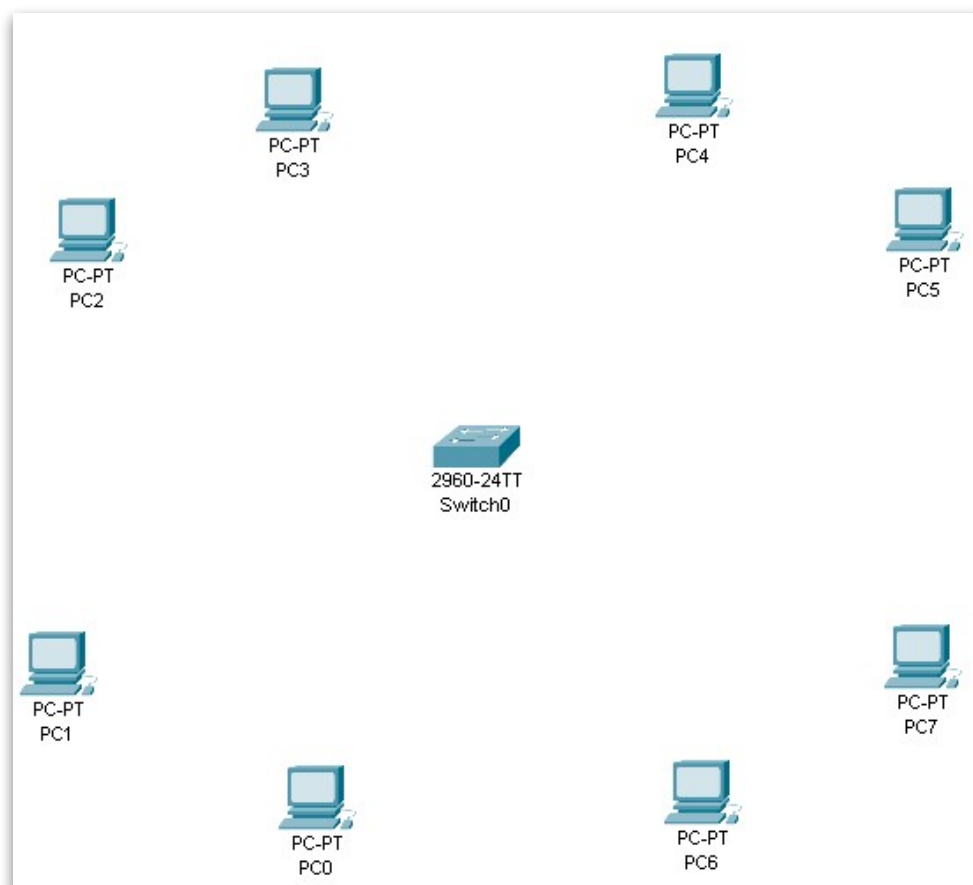
INTRODUZIONE

L'uso delle VLAN consente di segmentare la rete in domini di broadcast separati, migliorando sicurezza, efficienza e gestione del traffico di rete. Le VLAN in questione non possono comunicare tra loro.

PROCEDIMENTO

1. STRUTTURA DELLA RETE

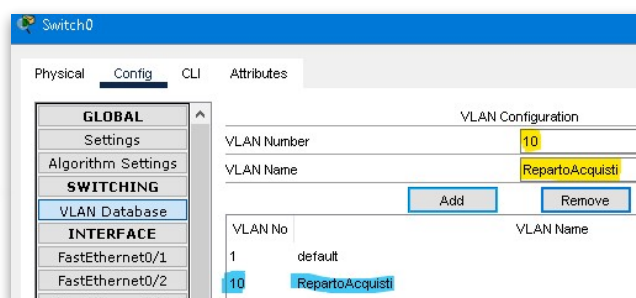
Per prima cosa dispongo nello spazio 1 Switch e 8 PC in totale in modo da avere poi 2PC per ogni VLAN. Non effettuo subito i collegamenti perché voglio prima configurare le porte dello switch.



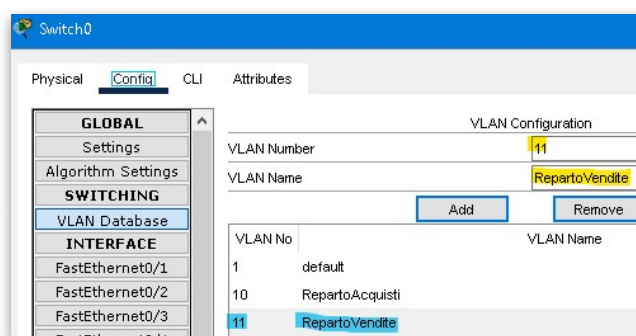
2. CONFIGURAZIONE DELLO SWITCH

A questo punto apro la configurazione dello switch e alla voce **"VLAN Database"** inizio a configurare le mie VLAN dandole numero e nome:

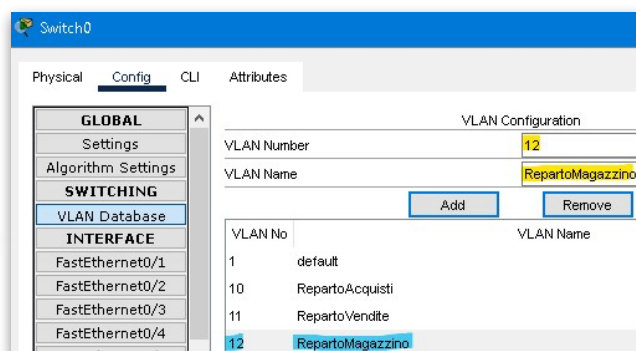
VLAN 10 - Reparto Acquisti →



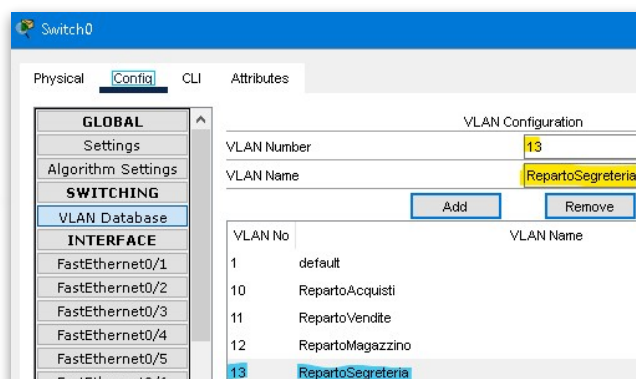
VLAN 11 - Reparto Vendite. →



VLAN 12 - Reparto Magazz. →



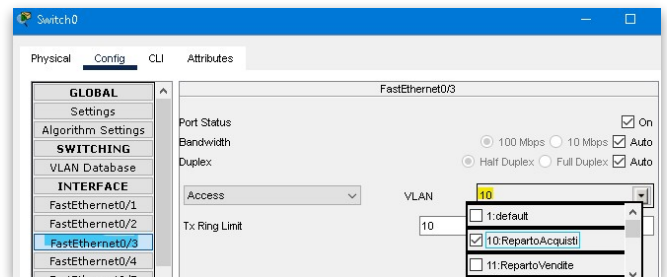
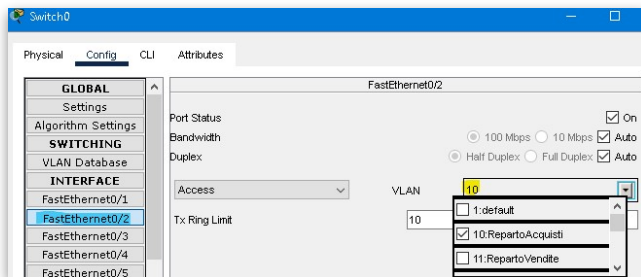
VLAN 13 - Reparto Segret. →



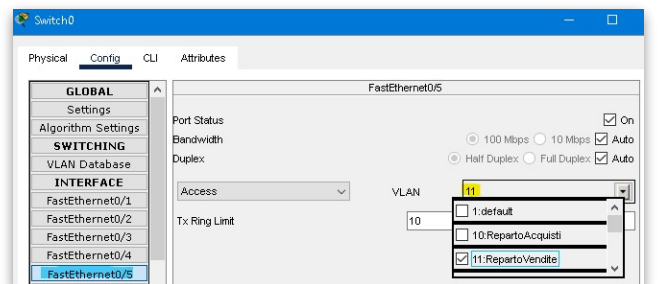
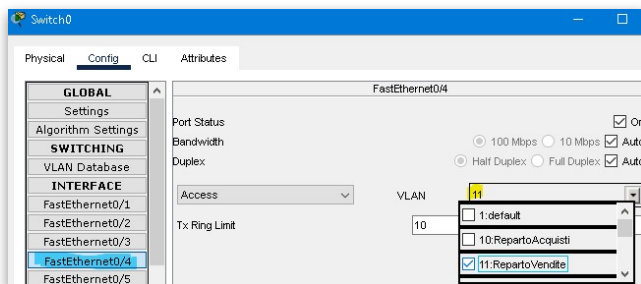
3. ASSEGNAZIONE DELLE PORTE E COLLEGAMENTI

Adesso procedo con l'assegnare alle varie porte dello Switch le VLAN appena create in modo da dividere i PC in 2 per ogni VLAN.

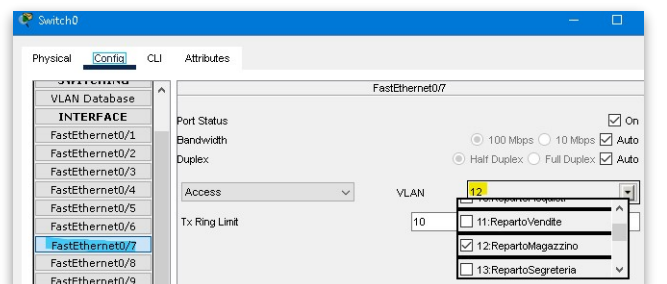
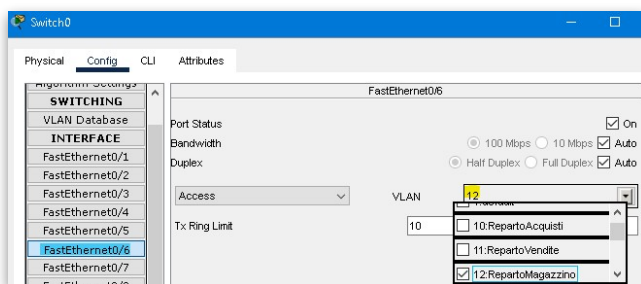
- Assegno la VLAN 10 alle porte FastEthernet0/2 e FastEthernet0/3:



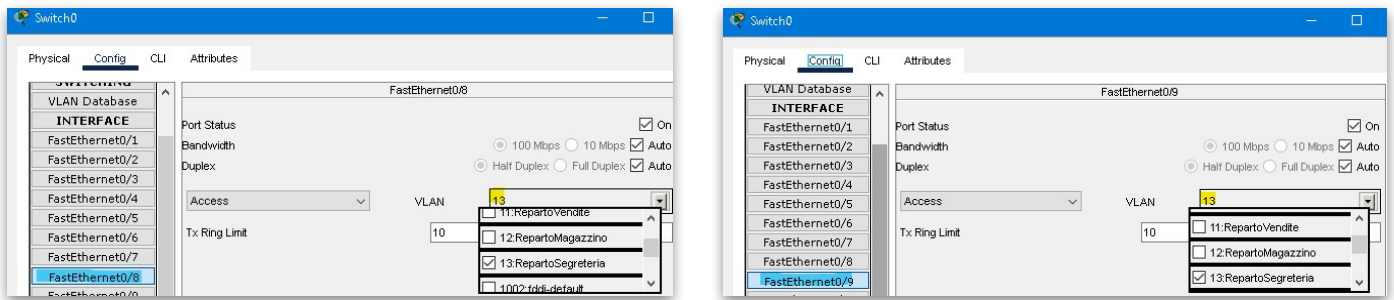
- Assegno la VLAN 11 alle porte FastEthernet0/4 e FastEthernet0/5:



- Assegno la VLAN 12 alle porte FastEthernet0/6 e FastEthernet0/7:

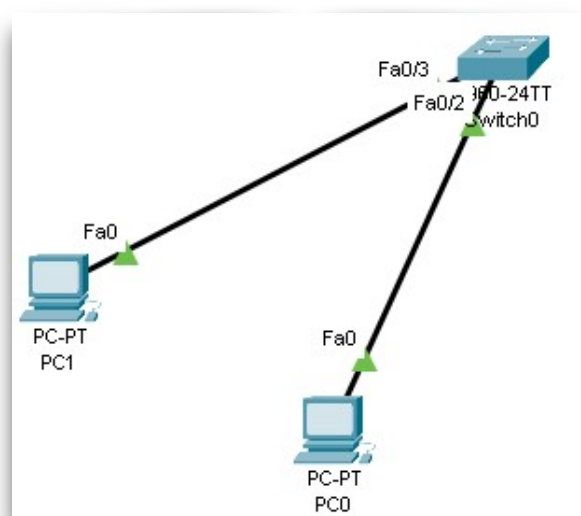


- Assegno la VLAN 13 alle porte FastEthernet0/8 e FastEthernet0/9:

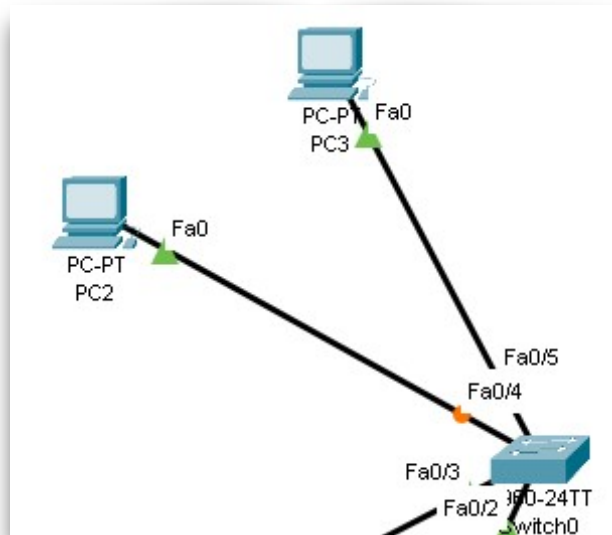


Assegnate le VLAN alle porte posso procedere con i collegamenti, che eseguo tutti con cavo **Copper Straight-Through**, stando attento ad assegnare correttamente i dispositivi alle porte dello Switch:

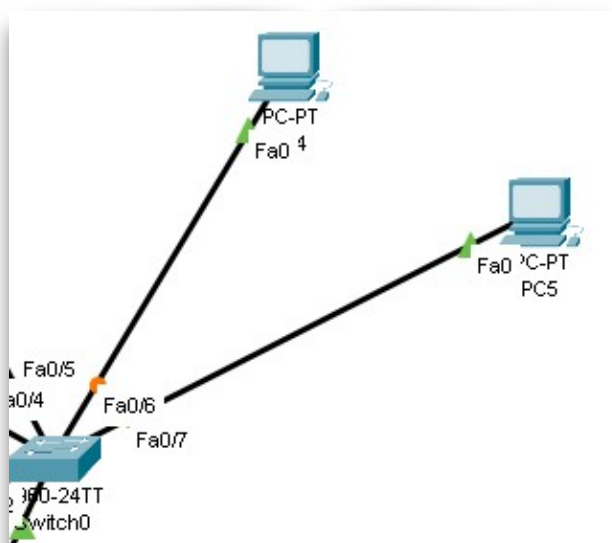
- A PC(0) e PC(1) assegno la VLAN 10, quindi li collego alle porte FastEthernet 0/2 e 0/3.



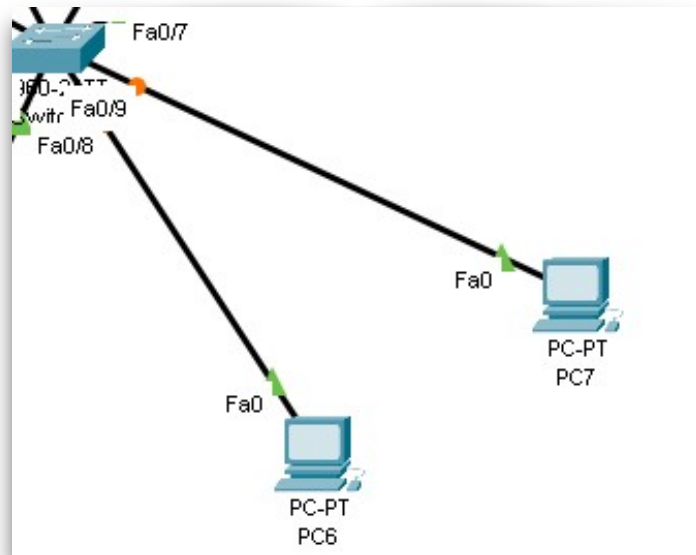
- A PC(2) e PC(3) assegno la VLAN 11, quindi li collego alle porte FastEthernet 0/4 e 0/5.



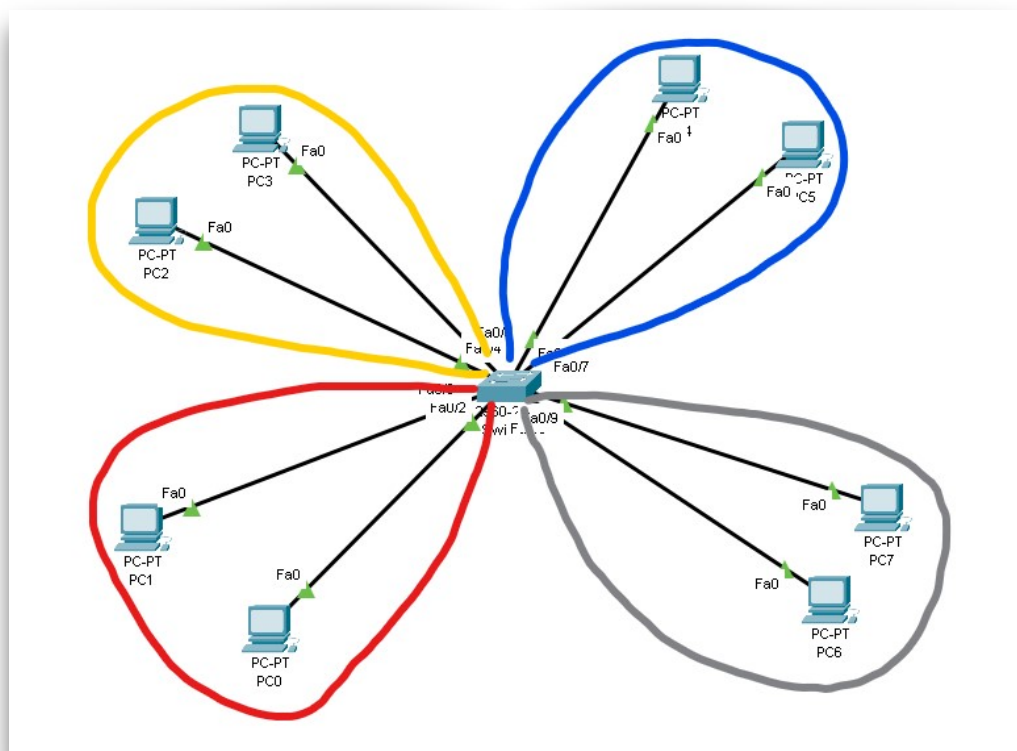
- A PC(4) e PC(5) assegno la VLAN 12, quindi li collego alle porte FastEthernet 0/6 e 0/7.



- A PC(6) e PC(7) assegno la VLAN 13, quindi li collego alle porte FastEthernet 0/8 e 0/9.



A questo punto immaginiamo la divisione delle VLAN in questo modo:



4. ASSEGNAZIONE DEGLI INDIRIZZI IP AI DISPOSITIVI

Assegno un indirizzo IP inventato ad ogni dispositivo, che rispetti però la divisione delle sottoreti, per farlo assegno prima un IP di RETE a ogni VLAN; quindi mi aspetto di avere 8 IP diversi, che a coppie di 2 appartengano alla stessa VLAN.

Quindi assegno:

VLAN10 = 192.168.10.0/24

PC(0) = 192.168.10.2/24

PC(1) = 192.168.10.3/24

VLAN11 = 192.168.11.0/24

PC(2) = 192.168.11.2/24

PC(3) = 192.168.11.3/24

VLAN12 = 192.168.12.0/24

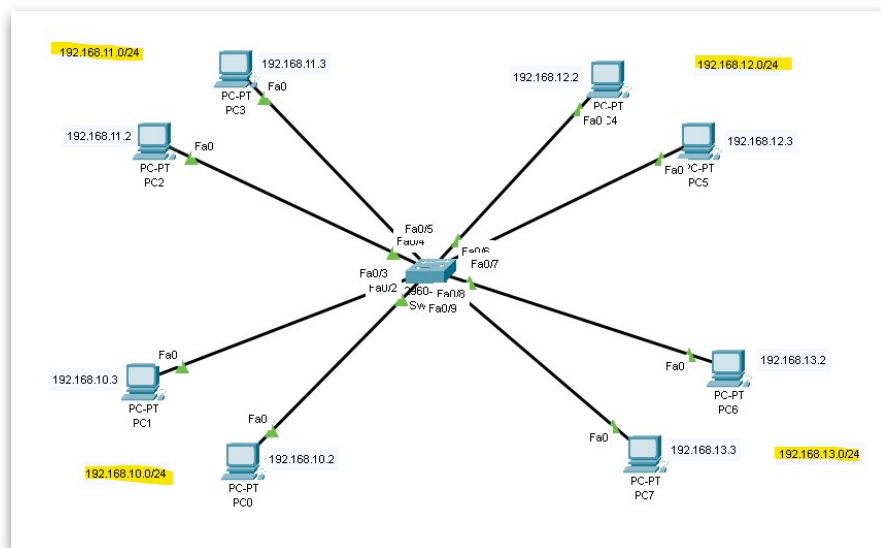
PC(4) = 192.168.12.2/24

PC(5) = 192.168.12.3/24

VLAN13 = 192.168.13.0/24

PC(6) = 192.168.13.2/24

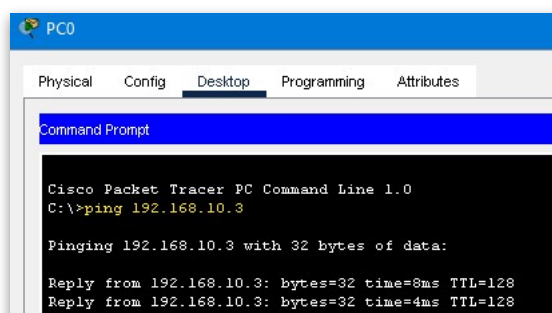
PC(7) = 192.168.13.3/24



5. VERIFICA DELLE COMUNICAZIONI

Per verificare che ci sia comunicazione all'interno delle VLAN eseguo un comando di **ping** tra i dispositivi interni alle singole VLAN attraverso il Comand Prompt:

- VLAN10 - ping PC(0) —> PC(1):



32.530	--	PC0	ARP
32.531	PC0	Switch0	ARP
32.532	Switch0	PC1	ARP
32.533	PC1	Switch0	ARP
32.534	Switch0	PC0	ARP

- VLAN11 - ping PC(2)→ PC(3):

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=8ms TTL=128
Reply from 192.168.11.3: bytes=32 time=4ms TTL=128
  
```

34.528	PC2	Switch0	ARP
34.529	Switch0	PC3	ARP
34.530	PC3	Switch0	ARP
34.531	Switch0	PC2	ARP

- VLAN12 - ping PC(4)→ PC(5):

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Reply from 192.168.12.3: bytes=32 time=8ms TTL=128
Reply from 192.168.12.3: bytes=32 time=4ms TTL=128
  
```

--	PC4	ARP
PC4	Switch0	ARP
Switch0	PC5	ARP
PC5	Switch0	ARP
Switch0	PC4	ARP

- VLAN13 - ping PC(7)→ PC(6):

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.13.2

Pinging 192.168.13.2 with 32 bytes of data:

Reply from 192.168.13.2: bytes=32 time=4ms TTL=128
  
```

PC7	Switch0	ICMP
Switch0	PC6	ICMP
Switch0	PC6	ICMP
PC6	Switch0	ICMP
Switch0	PC7	ICMP

Ora non mi resta che verificare che effettivamente le VLAN non siano in comunicazione tra loro, per farlo eseguo dei comandi di **ping** incrociati tra macchine che non si trovano nella stessa VLAN:

Ping PC(0) → PC(3)



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=8ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Request timed out.
```

Ping PC(2) → PC(4)



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=8ms TTL=128
Reply from 192.168.11.3: bytes=32 time=4ms TTL=128
Reply from 192.168.11.3: bytes=32 time=4ms TTL=128
Reply from 192.168.11.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.11.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ping 192.168.12.2

Pinging 192.168.12.2 with 32 bytes of data:

Request timed out.
```

Ping PC(7) → PC(5)



```
PC7
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.13.2

Pinging 192.168.13.2 with 32 bytes of data:

Reply from 192.168.13.2: bytes=32 time=4ms TTL=128
Reply from 192.168.13.2: bytes=32 time=4ms TTL=128
Reply from 192.168.13.2: bytes=32 time=4ms TTL=128
Reply from 192.168.13.2: bytes=32 time=4ms TTL=128

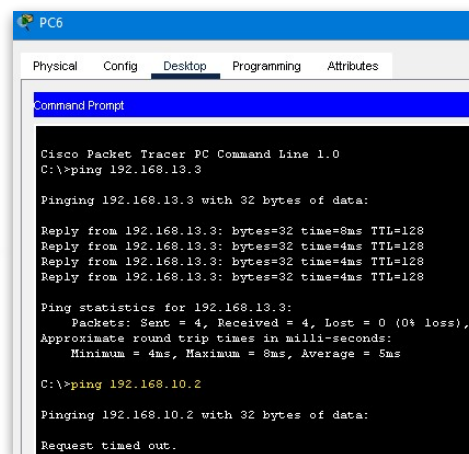
Ping statistics for 192.168.13.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Request timed out.
```

Ping PC(6) —> PC(0) —————→



```
PC6
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.13.3

Pinging 192.168.13.3 with 32 bytes of data:

Reply from 192.168.13.3: bytes=32 time=8ms TTL=128
Reply from 192.168.13.3: bytes=32 time=4ms TTL=128
Reply from 192.168.13.3: bytes=32 time=4ms TTL=128
Reply from 192.168.13.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.13.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
```



In questo modo ho dimostrato che le comunicazioni avvengono tra dispositivi appartenenti alla stessa VLAN, ma non avvengono tra dispositivi appartenenti a VLAN diverse.

6. MOTIVI PER L'USO DELLE VLAN

La scelta di ricorrere ad una VLAN ha diversi vantaggi.

Nel progetto ho cercato di rendere l'idea assegnando alle VLAN un nome che sia quanto più verosimile per un'area dell'azienda.

Tralasciando il fatto che nel progetto troviamo pochi dispositivi per ogni VLAN, nella realtà questi possono essere molti di più e quindi sicuramente la divisione in aree separate può offrire una gestione migliore della rete e dei dati, una sicurezza maggiore e un'efficienza maggiore.

*Faccio degli esempi: Con la **segmentazione della rete** il traffico di broadcast viene notevolmente ridotto e ne consegue un miglioramento significativo delle prestazioni.*

*Per quanto riguarda la **sicurezza**, la VLAN separa dalle altre aree della rete e quindi sarà più difficile per un malintenzionato ad esempio raggiungere dati sensibili.*

*In più le VLAN hanno una **gestione semplificata** essendo virtuali e una **flessibilità nella configurazione** che permette di riorganizzarla facilmente. Sono solo alcuni dei vantaggi delle VLAN che ho capito essere essenziali per sicurezza, gestione, prestazioni e tanto altro.*

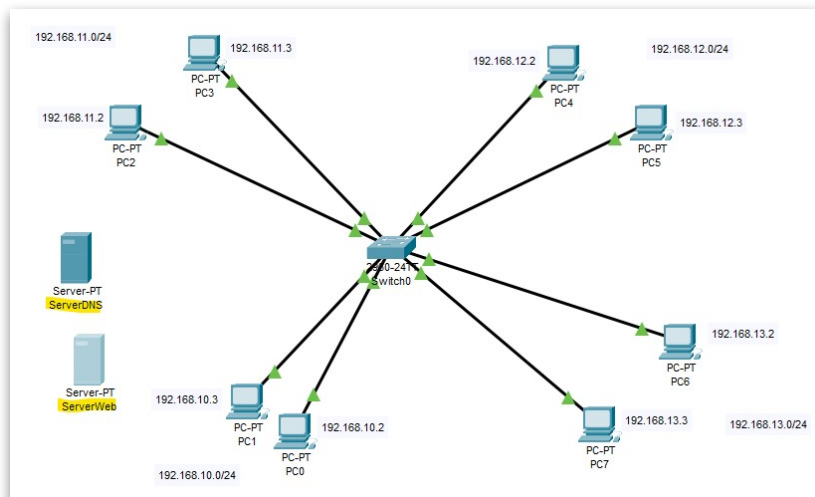
ESERCIZIO BONUS

Nell'esercizio bonus, viene richiesto di inserire un Server DNS e un Server Web, in modo che da un PC si possa raggiungere la pagina web "helloworld.html".

1. POSIZIONAMENTO DEI SERVER

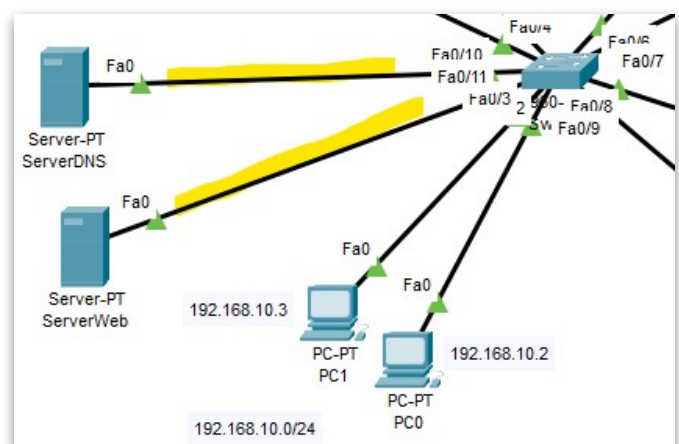
Scelgo di lavorare sulla prima rete VLAN individuata nell'esercizio precedente quindi la VLAN 10 e di effettuare il test tramite il PC(0), appartenente anch'esso alla suddetta VLAN.

Posiziono i server nella rete selezionandoli dalla barra degli strumenti e per ordine mentale e visivo li rinominerò Server DNS e Server Web:

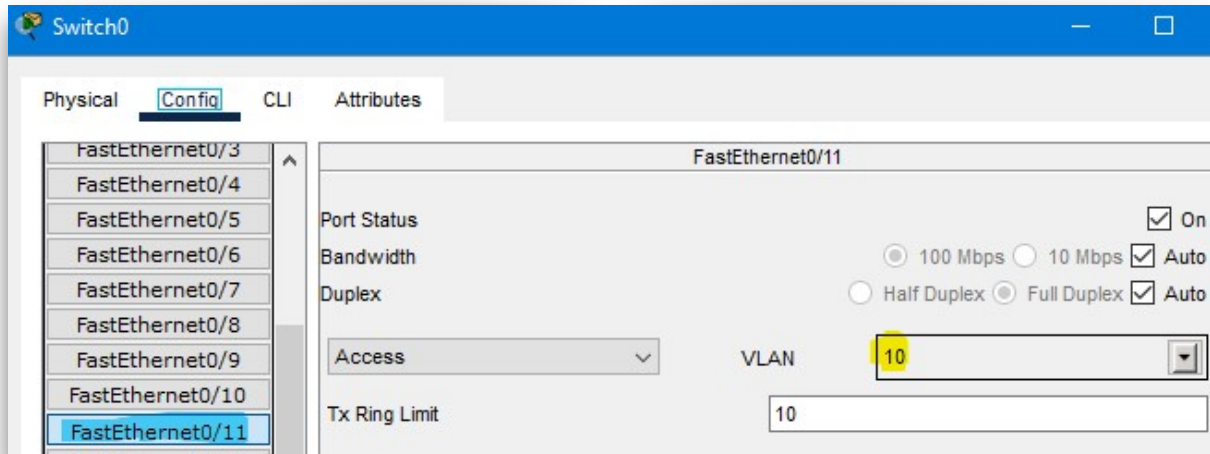
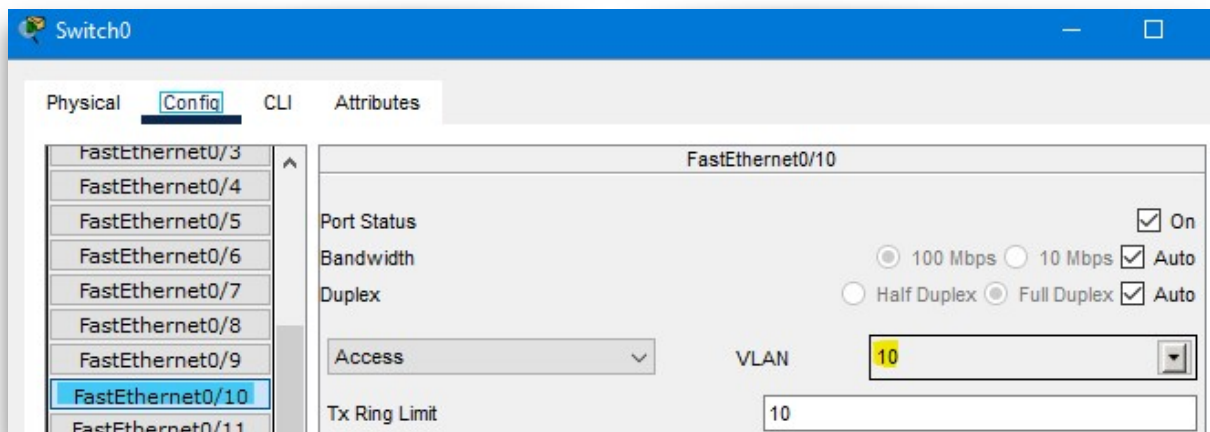


2. COLLEGAMENTO DEI SERVER CON LO SWITCH

A questo punto collego entrambi i server allo Switch con un cavo Copper Straight-Through, facendo attenzione poi ad assegnare la giusta VLAN alle porte sullo Switch:

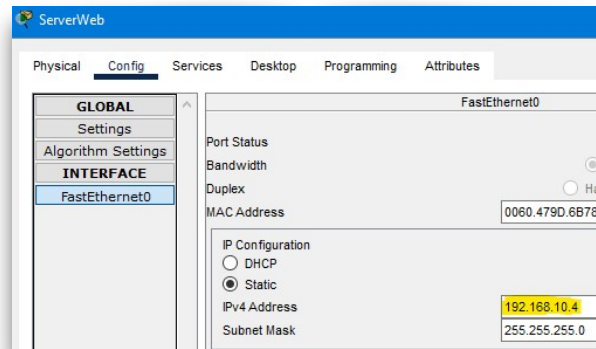


Ora come detto devo assegnare alle porte sullo Switch la VLAN 10. Avendo collegato il **Server DNS** alla porta **FastEthernet0/10** e il **Server Web** alla porta **FastEthernet0/11**, nella configurazione dello Switch imposterò queste due porte alla VLAN 10:

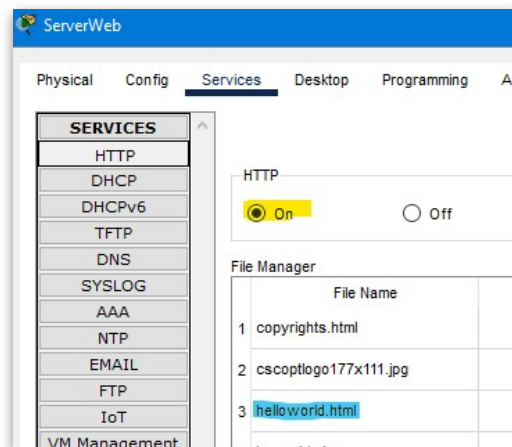


3. CONFIGURAZIONE SERVER WEB

Devo assegnare un indirizzo IP al Server Web che sia compreso nella sottorete interessata quindi metto ad esempio 192.168.10.4:

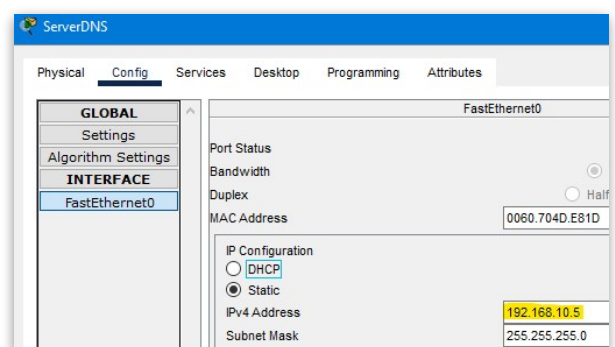


Poi abilito il servizio HTTP sul server, per permettere l'accesso alla pagina helloworld.html, andando nelle impostazioni dei servizi, più precisamente nella sezione HTTP:

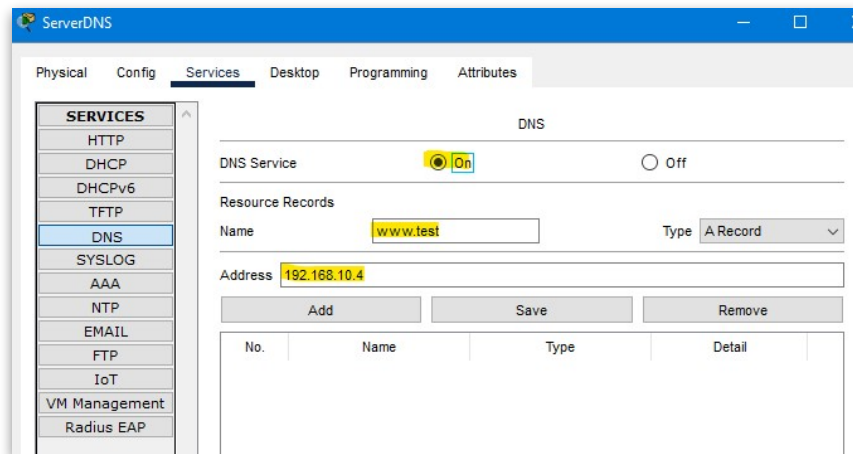


4. CONFIGURAZIONE SERVER DNS

Anche in questo caso assegno un indirizzo IP che appartenga a questa VLAN come 192.168.10.5:



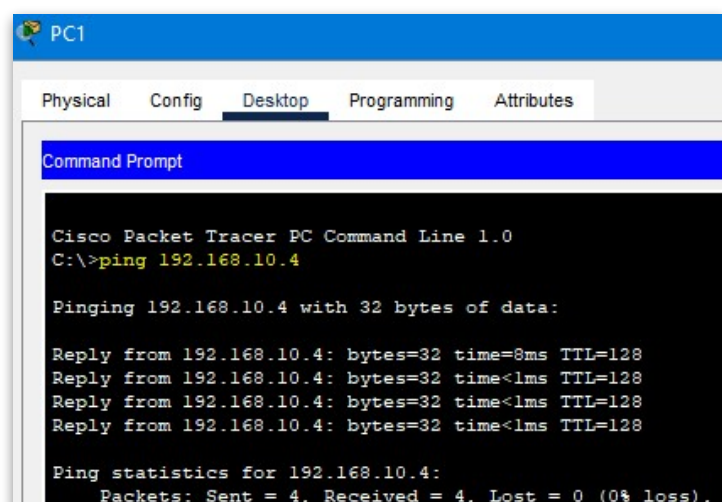
Poi nella sezione Servizi, alla voce DNS, dopo aver impostato il DNS Service su ON, imposto un record con nome www.test e con Address l'indirizzo IP del Server Web e faccio aggiungi:



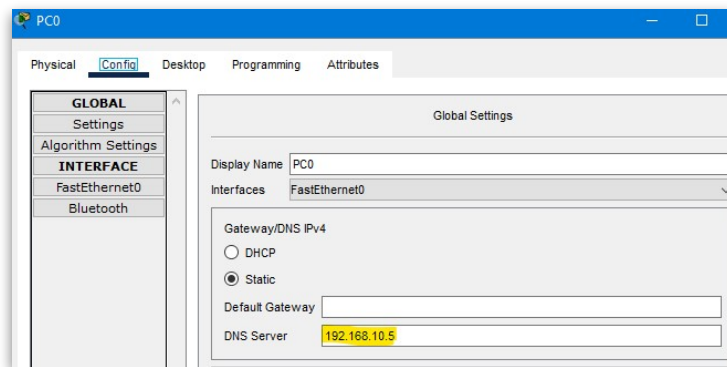
No.	Name	Type	Detail
0	www.test	A Record	192.168.10.4

5. COMUNICAZIONE TRA LE MACCHINE

Eseguo un semplice ping dal PC(1) al server Web per controllare che la comunicazione sia attiva:



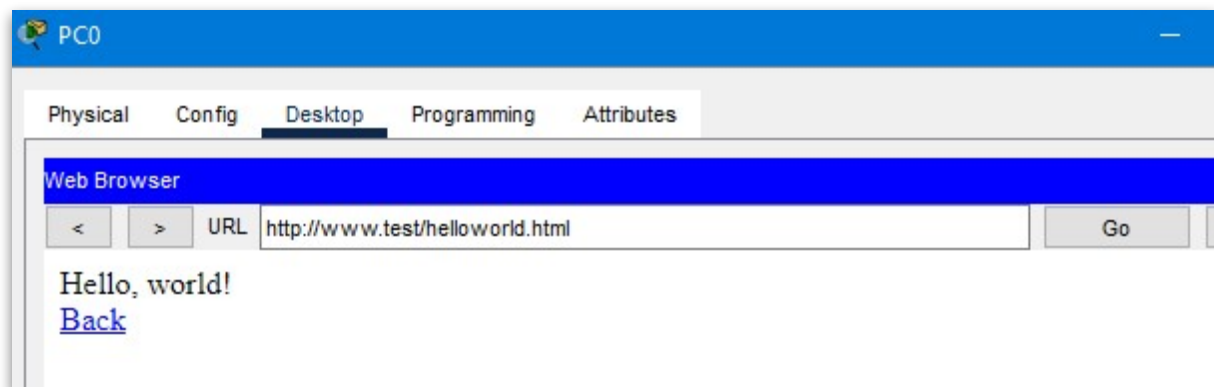
6. CONFIGURAZIONE DEL PC(0)



Per permettere al PC(0) di raggiungere il Server DNS devo assegnare l'IP nella configurazione in questo modo:

7. ACCESSO ALLA PAGINA WEB

Non resta che testare la possibilità di accedere alla pagina web, per farlo uso il PC(0) e dal desktop vado nel Web Browser ed eseguo la ricerca:



Come si vede dall'immagine il PC(0) riesce a raggiungere correttamente la pagina e volendo si potrebbe fare lo stesso con il PC(1):



Anche il PC(1) raggiunge correttamente la pagina!