Sommario

1. Progetto

La richiesta del cliente consiste nella creazione di una rete segmentata con 4 VLAN diverse.

1.1 Contesto

Il progetto si propone di implementare una rete segmentata all'interno di un negozio di arredamento su tre livelli, per migliorare l'efficienza della rete, la sicurezza e l'organizzazione. Utilizzando la suddivisione in 4 VLAN, si intende ottimizzare la gestione del traffico di rete e proteggere i dati sensibili dei clienti.

I 3 livelli del negozio saranno individuati successivamente con le diverse nomenclature, piano terra (PT), piano primo (P1), piano 2 (P2).

Di seguito, si descriverà la divisione funzionale dei diversi livelli considerando la presenza dello showroom sui primi due piani.

PT:

- Magazzini per lo stoccaggio dei prodotti e materiali;
- Segreteria con funzione di info-point e smistamento della clientela;
- Reparto progettazione per accompagnamento alla clientela nelle diverse fasi dell'acquisto.

P1:

- Magazzino a supporto di quello al PT;
- Reparto progettazione a supporto di quello al PT;
- Segreteria a supporto di quella a PT;
- Reparto amministrativo/contabile a supporto di quello al P2, con lo scopo di seguire il cliente in fase d'acquisto.

P2:

- Reparto progettazione per fase definitiva di acquisto e progetto esecutivo;
- Reparto amministrativo/contabile.

2. Proposta

Si è deciso di attuare una suddivisione logistica delle VLAN in base alle diverse funzioni presenti nel punto vendita (*fig.1*), inserendo uno switch per ogni piano. Questa soluzione permette di ridurre i costi del cablaggio fisico tra gli end device e di garantire un'organizzazione più flessibile delle postazioni di lavoro.

Vediamo nel dettaglio la suddivisione delle 4 VLAN, considerando la VLAN 1 come quella di default:

- VLAN 2 dedicata ai magazzini, per tenere sempre traccia dei materiali e prodotti presenti, nonché l'organizzazione delle consegne;
- VLAN 3 dedicata al reparto progettazione, per consentire il passaggio di informazioni e progetti relativi al singolo cliente;
- VLAN 4 dedicata alla segreteria, per l'organizzazione di appuntamenti e gestione delle risorse;
- VLAN 5 dedicata all'area amministrativa/contabile, per separare e proteggere i dati sensibili dei clienti che hanno effettivamente effettuato l'acquisto di prodotti e dei loro metodi di pagamento.

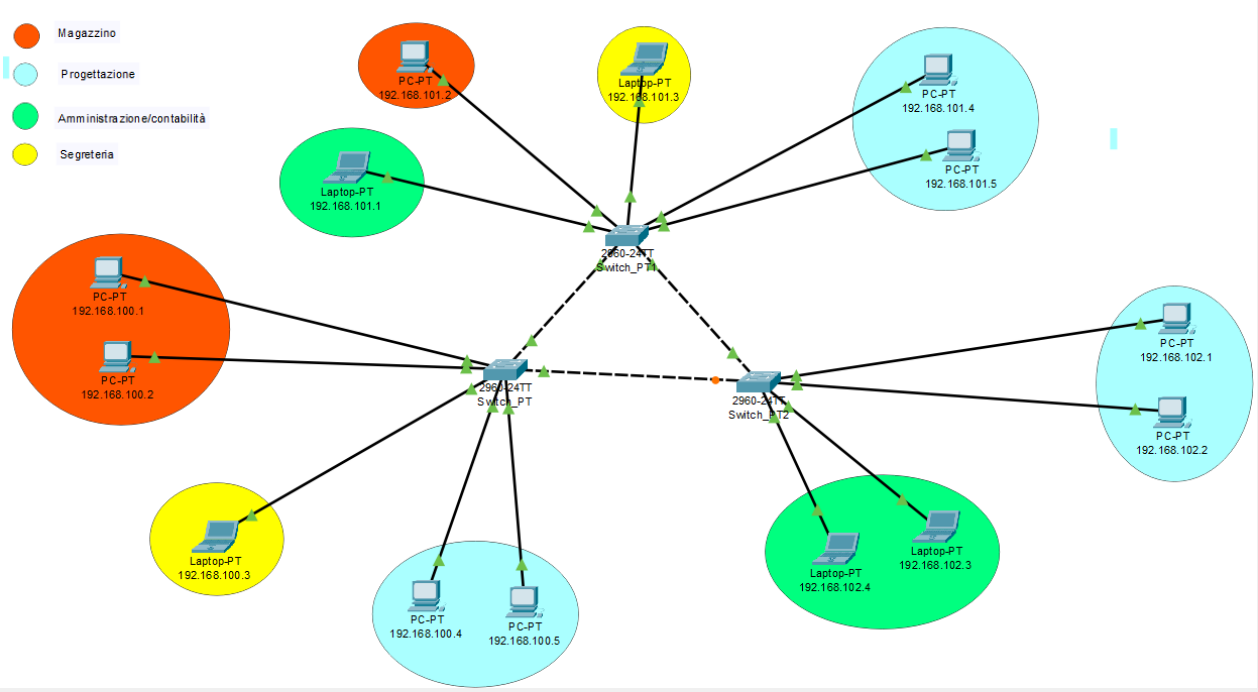

Fig. 1 – Configurazione della rete con Cisco Packet Tracer

2.1 Configurazioni degli Switch

Su Cisco Packet Tracer, cliccando sullo switch di interesse possiamo impostare le VLAN (*fig.2*). Tale impostazione viene ripetuta per tutti e tre gli switch.

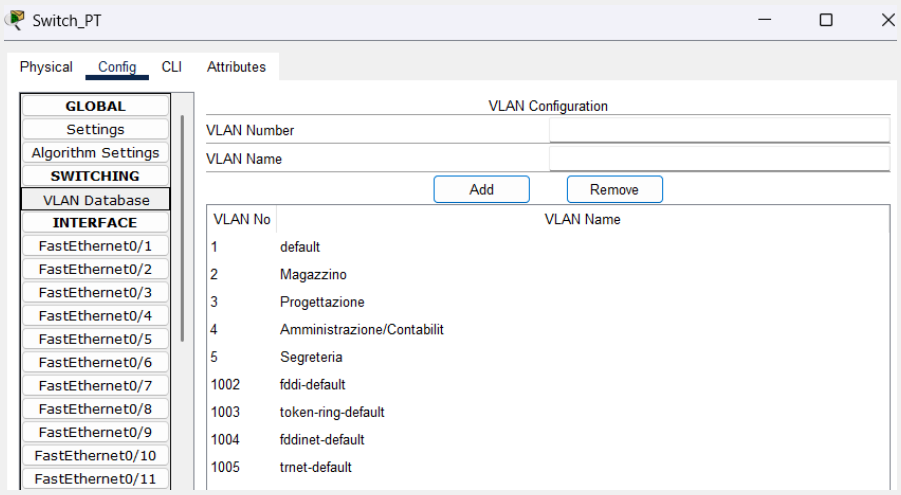

Fig. 2 - Inserimento delle 4 VLAN sullo switch del PT

Vengono inoltre configurate le interfacce occupate dai diversi dispositivi con le VLAN corrispondenti alla funzione individuate.

Ad esempio, il PC con IP 192.168.100.1 è collegato all'interfaccia FastEthernet0/1 dello switch, quindi configuriamo tale interfaccia per appartenere alla VLAN 2, dedicata al magazzino (*fig.3*).

Anche tale impostazione va ripetuta per tutte le interfacce occupate dagli end device.

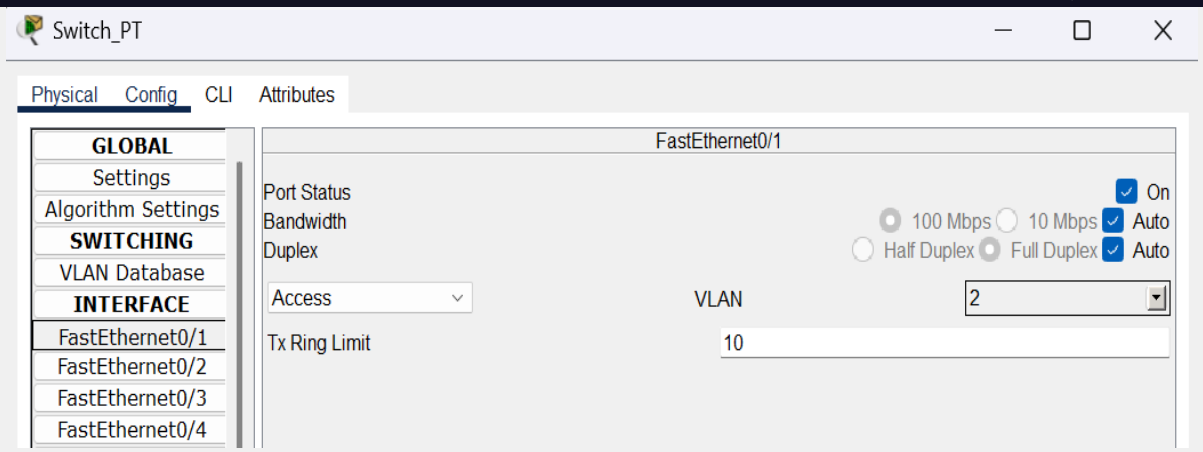

Fig. 3 – Configurazione della porta FastEthernet0/1 dello switch PT0.

Inoltre, bisogna impostare la porta occupata dal collegamento con gli altri switch su *Trunk (fig. 4)*. Tale impostazione va ripetuta per tutte le porte degli switch occupate dagli altri switch e consente il trasporto sul collegamento del traffico di più VLAN, a differenza dell'impostazione *Access* che permette il trasporto di traffico appartenente ad una sola VLAN.

Ad esempio, lo switch PT0 è collegato a PT1 tramite la porta GigabitEthernet0/1, che verrà configurata come Trunk per consentire il trasporto del traffico di più VLAN.

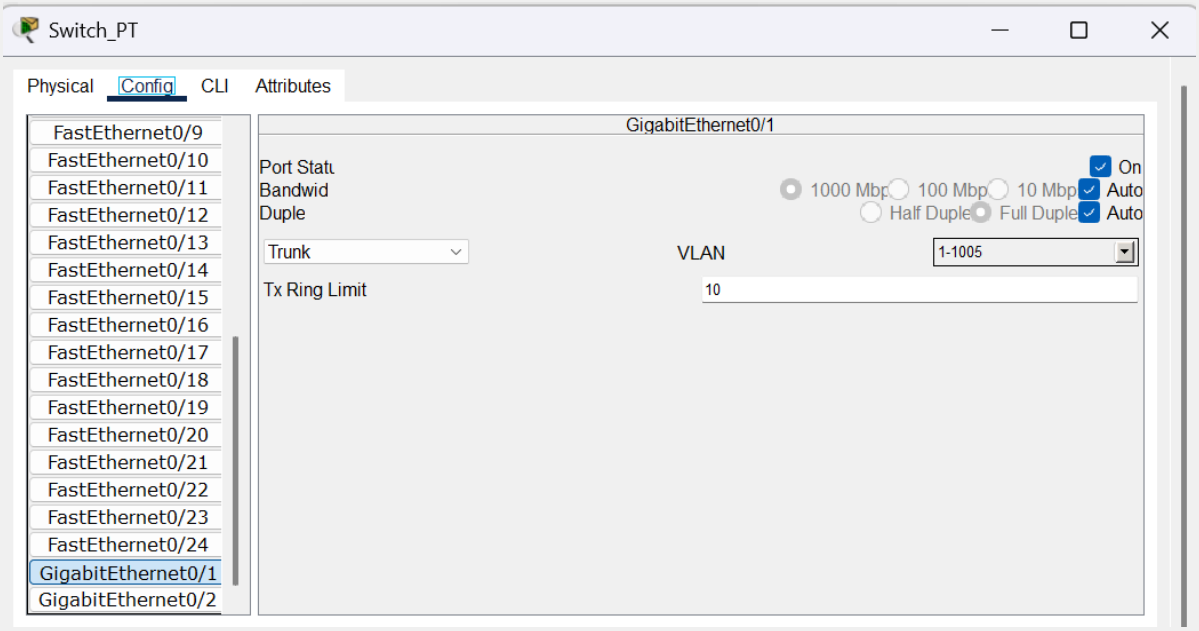

Fig. 4 – Configurazione della porta GigabitEthernet0/1 dello switch PT0 occupata dallo switch PT1

Gli switch risultano così collegati correttamente.

2.2 Configurazioni end device

La rete in oggetto ha IP 192.168.0.0/16, quindi impostiamo gli IP dei diversi end device.

Per semplicità ad ogni piano viene dato un numero progressivo al terzo ottetto in relazione al piano (PT: 192.168.100.0, P1: 192.168.101.0, P2: 192.168.0.0) e numero progressivo al quarto ottetto per ogni device (esempio: 192.168.100.1 per un device al primo piano (*fig. 5*), 192.168.101.1 per un device del secondo, 192.168.102.1 per un device al terzo piano).

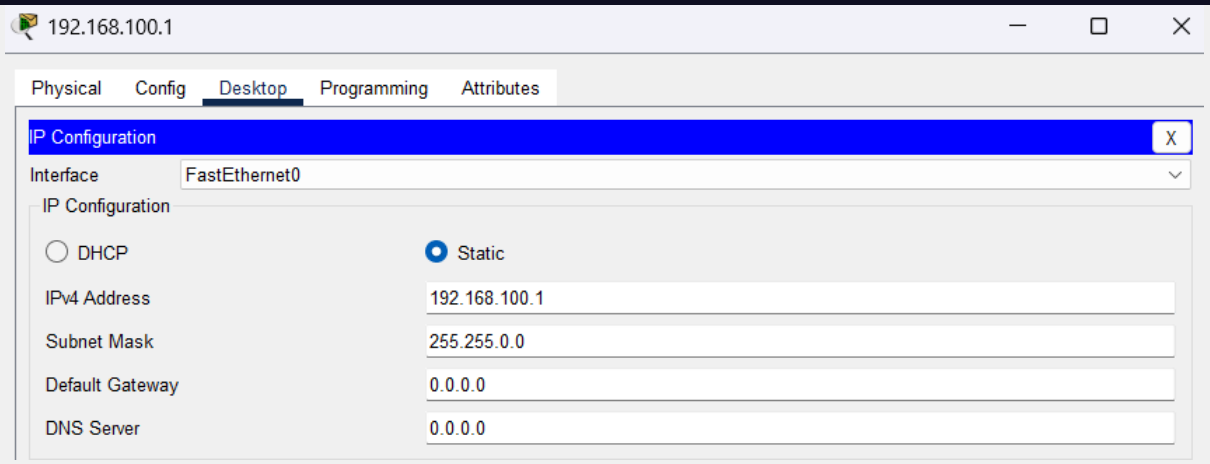

Fig. 5 – Configurazione di un end device al PT

A questo punto tutti i dispositivi presenti nella rete risultano configurati correttamente. Si passerà ora alla fase di testing.

3. Verifica della configurazione

Si effettueranno *ping test* tra dispositivi nella stessa VLAN e *ping test* diversi, i primi serviranno a confermare che la comunicazione avviene correttamente tra dispositivi nella stessa VLAN, gli altri a confermare che due VLAN diverse risultano isolate tra loro.

3.1 *Ping test* tra dispositivi nella stessa VLAN

Testiamo la connessione tra PC con IP 192.168.100.4 connesso allo switch PT0 e il pc con IP 192.168.102.1 connesso allo switch PT2, entrambi appartenenti al VLAN 3 *'Progettazione' (fig. 6).*

Entrambi i PC appartengono alla stessa rete, ma il PC mittente non conosce ancora il MAC del destinatario, trattandosi del primo contatto. Per questo motivo, invierà un'ARP Request in modalità broadcast (indirizzo MAC di destinazione: **FF:FF:FF:FF:FF:FF**) a tutti i dispositivi della rete, richiedendo l'indirizzo MAC corrispondente all'IP 192.168.102.1 (*fig. 7*). Lo switch a sua volta, inoltrerà la richiesta a tutti i suoi dispositivi connessi, compresi gli switch che ripeteranno tale processo per i dispositivi a loro connessi (*fig.* 8). Solo il PC con IP 192.168.102.1 invierà una ARP Response al PC richiedente. A quel punto, gli end device registreranno nella loro ARP table gli indirizzi IP e il MAC associato per un periodo di tempo limitato, mentre gli switch registreranno il MAC dei device collegati nella MAC Table (*fig.9)*.

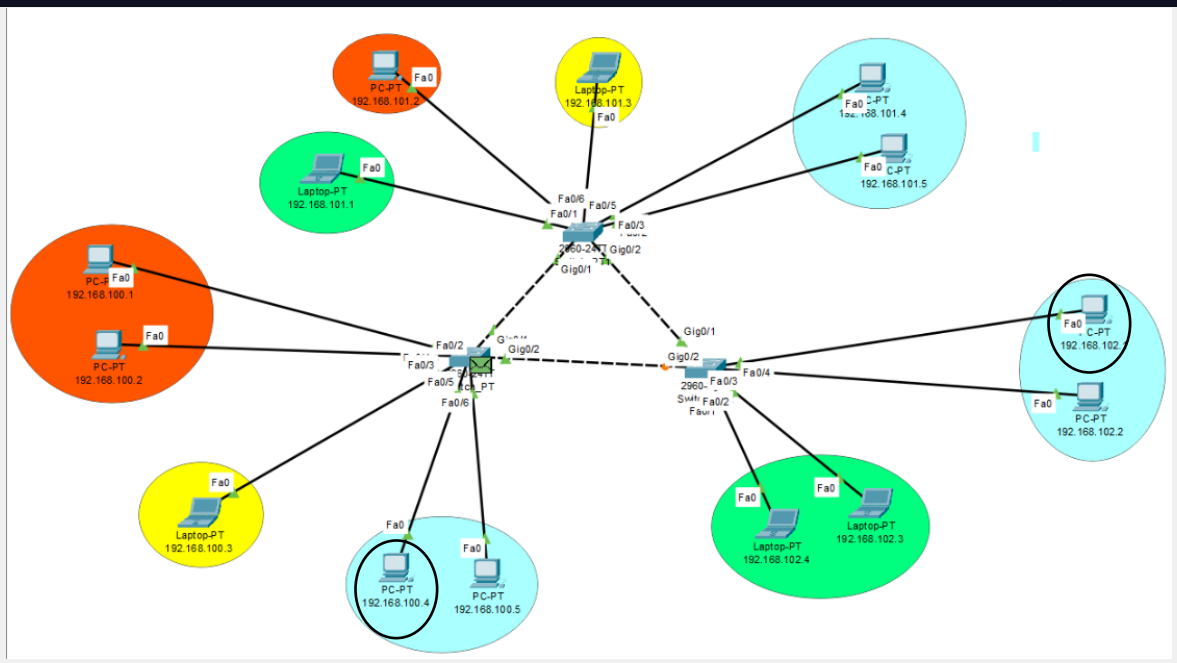

Fig. 6 – Individuazione dei PC che si vuol far comunicare

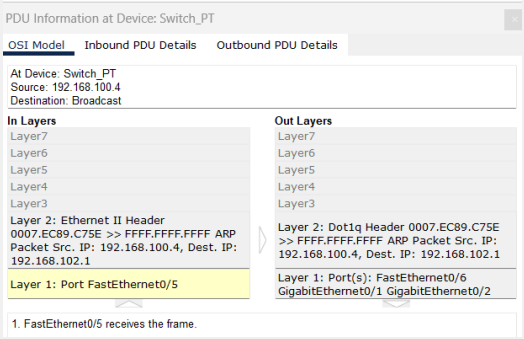

Fig. 7 – ARP Request da PC 192.168.100.4

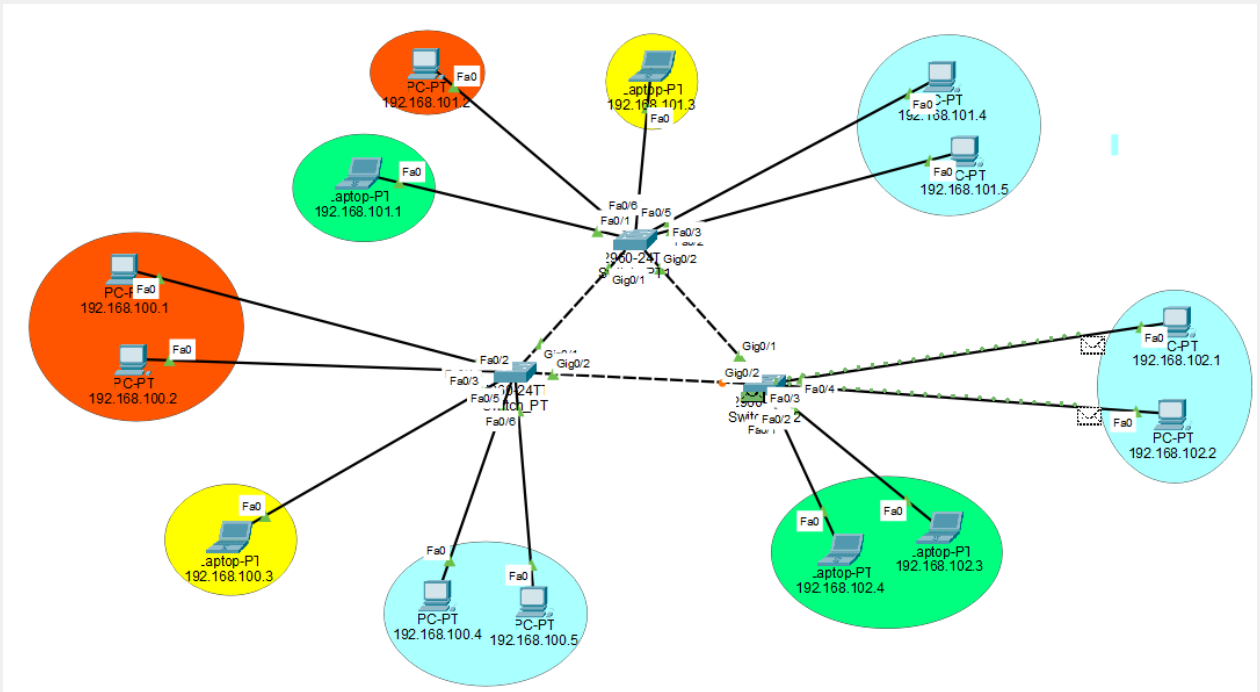

Fig. 8 – Inoltro dell'ARP Request da parte degli switch collegati allo switch PT0.

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	192.168.100.4	ICMP
	0.000	--	192.168.100.4	ARP
	0.001	192.168.100.4	Switch_PT	ARP
	0.002	Switch_PT	192.168.100.5	ARP
	0.002	Switch_PT	Switch_PT1	ARP
	0.002	Switch_PT	Switch_PT2	ARP
	0.003	Switch_PT1	192.168.101.5	ARP
	0.003	Switch_PT1	192.168.101.4	ARP
	0.003	Switch_PT2	192.168.102.2	ARP
	0.003	Switch_PT2	192.168.102.1	ARP
	0.003	Switch_PT2	Switch_PT1	ARP
	0.004	192.168.102.1	Switch_PT2	ARP
	0.005	Switch_PT2	Switch_PT	ARP
	0.006	Switch_PT	192.168.100.4	ARP
	0.006	--	192.168.100.4	ICMP
	0.007	192.168.100.4	Switch_PT	ICMP

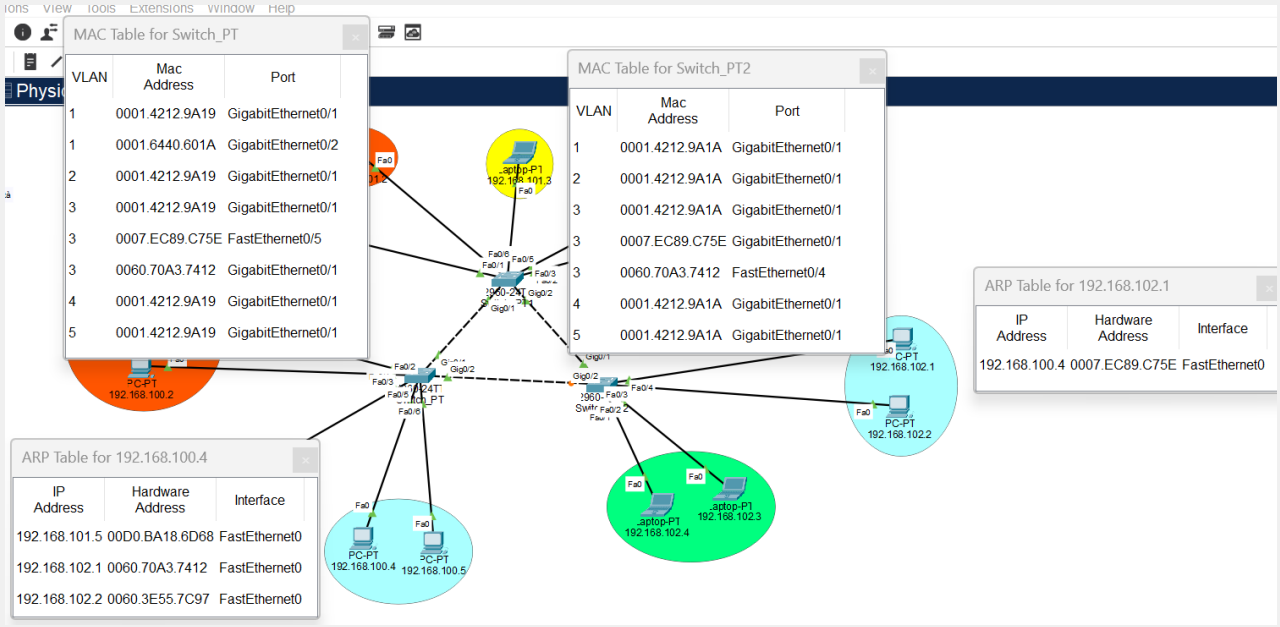

Fig. 9 – L'immagine sopra descrive i diversi passaggi dell'ARP Request tra i dispositivi. L'immagine sottostante mostra la compilazione automatica dell'ARP Table dei device e del MAC Table degli switch.

3.2 Ping test tra dispositivi in una diversa VLAN

Testiamo la connessione tra PC con IP 192.168.100.3 connesso allo switch PT0 e il laptop con IP 192.168.101.1 connesso allo switch PT1, il primo appartenente alla VLAN 5 *'Segreteria'* e il secondo appartenente alla VLAN 4 *'Amministrazione/Contabilità' (fig. 10).*

Questo conferma che la segmentazione in VLAN sta funzionando correttamente, isolando il traffico tra le diverse funzioni aziendali come previsto (*fig. 11*).

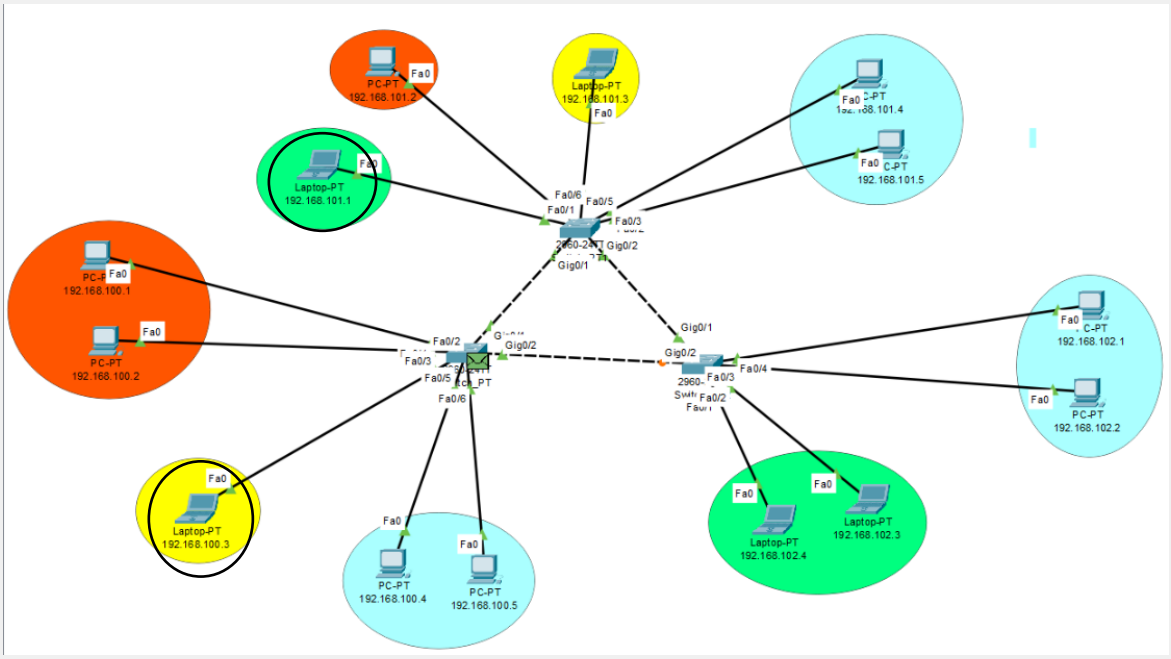

Fig. 10 – Individuazione dei PC che si vuol far comunicare.

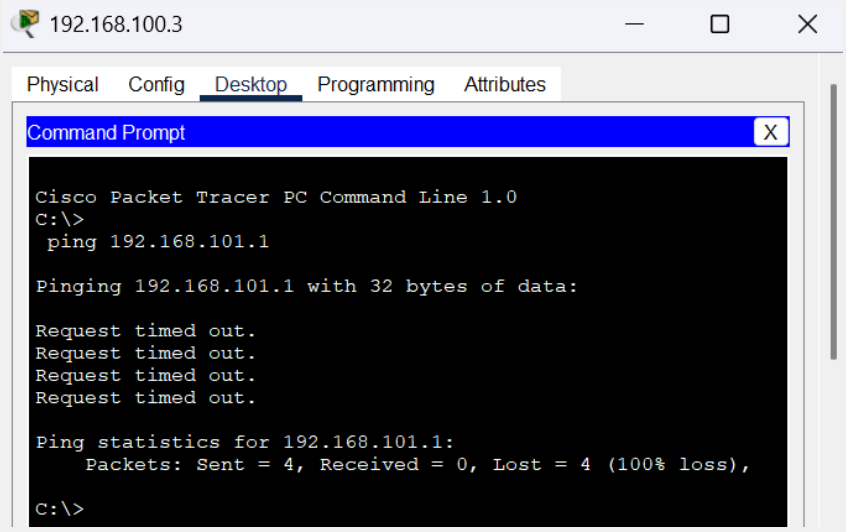

Fig. 11 – Ping tra i due dispositivi che dimostra che i due PC in due VLAN diverse non comunicano tra loro.

4. Conclusione

La suddivisione in VLAN ha portato a un significativo miglioramento delle prestazioni, grazie alla riduzione del traffico e del dominio di broadcast. Inoltre, l'isolamento dei dati sensibili garantisce una maggiore sicurezza, mentre l'organizzazione delle postazioni di lavoro su più livelli risulta più efficiente e flessibile.

Questa configurazione non solo garantisce prestazioni ottimali e sicurezza dei dati, ma permette anche una facile scalabilità della rete in caso di espansione dell'attività. Inoltre, la gestione centralizzata delle VLAN semplifica la manutenzione, ottimizzando i tempi di intervento e riducendo i costi operativi. In futuro, sarà possibile integrare ulteriori miglioramenti, come l'implementazione di un server DHCP.