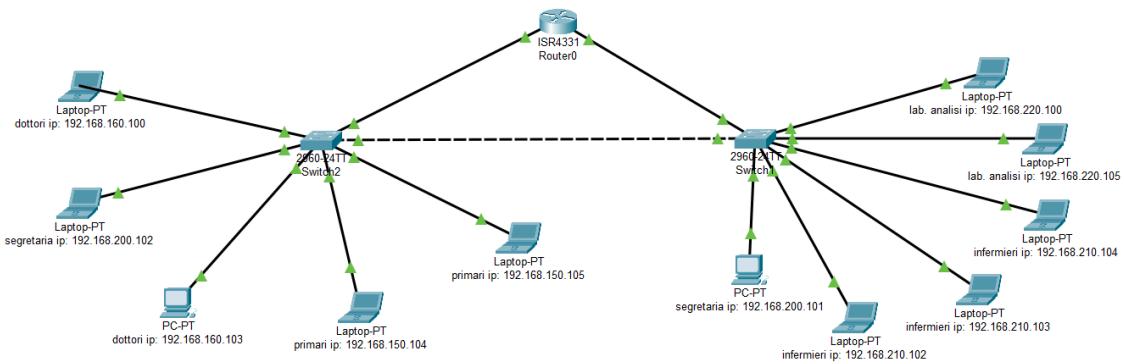


laboratorio

Creare una rete segmentata con 4 vlan diverse



configurazione e vantaggi - svantaggi delle VLAN

In questo progetto ho creato due reti locali separate e segmentate in due sottoreti ciascuna utilizzando la VLAN (virtual local area network) come metodo di isolamento dei dispositivi.

Le VLAN offrono vantaggi significativi in termini di sicurezza, prestazioni e gestione della rete.

- **sicurezza:** le VLAN isolano logicamente il traffico tra diversi gruppi di dispositivi o dipartimenti (es: segreteria, contabilità, server) impedendo l'accesso non autorizzato a dati sensibili e limitando la propagazione di malware o attacchi all'interno della rete.
- **Prestazioni:** riducono le dimensioni dei domini di broadcast e del traffico di rete migliorando le prestazioni complessive e l'utilizzo della larghezza di banda disponibile.
- **Riconfigurazione semplificata:** i dispositivi sono raggruppati in modo logico, il che permette di creare sottoreti anche con dispositivi fisicamente più distanti.

in caso di spostamento ad esempio da un piano all'altro basta riconfigurare il software delle porte senza bisogno di un nuovo cablaggio fisico.

- **Riduzione dei costi e scalabilità:** permettono di utilizzare un'unica infrastruttura di switch fisici per gestire più reti virtuali distinte, semplificando l'espansione della rete in base alle necessità.

Potenziali negativi

- **Configurazione tecnica:** implementare e gestire le reti VLAN richiede una conoscenza tecnica specifica, in caso di configurazioni errate possono insorgere problemi di connettività o in casi peggiori vulnerabilità di sicurezza.
- **Troubleshooting:** quando sorgono problemi di rete individuare l'origine in un ambiente virtualizzato può essere più difficile rispetto ad una rete fisica semplice.
- **Hardware compatibile:** per funzionare le VLAN richiedono switch e router gestibili e compatibili con lo standard 802.1q (protocollo di tagging vlan più comune)
- **Potenziali broadcast storm:** quando due o più switch di reti diverse sono collegati tra di loro si utilizza una configurazione detta "tree trunk" (tronco d'albero) il che consiste in un unico cavo che passa attraverso tutti gli switch rendendoli comunicanti tra di loro, nel caso ci fosse stato un errore di settaggio delle configurazioni VLAN nelle porte trunk può verificarsi un "loop" cioè una ridondanza di pacchetti broadcast che continuano a inondare la rete.

Configurazione e settaggio del laboratorio

Come prima cosa sono entrato nella configurazione ip di ogni computer dentro la quale ho impostato l'indirizzo ip privato , la maschera di rete e il gateway (router) di default per quella rete.

Interface

IP Configuration

DHCP Static

IPv4 Address
 Subnet Mask
 Default Gateway
 DNS Server

IPv6 Configuration

Automatic Static

IPv6 Address /
 Link Local Address
 Default Gateway
 DNS Server

802.1X

Use 802.1X Security

Authentication

Username
 Password

Successivamente dalle configurazioni ip del router ho assegnato a ogni porta gigabit ethernet corrispondente allo switch di rete il corretto indirizzo ip.

GLOBAL Settings Algorithm Settings ROUTING Static RIP SWITCHING VLAN Database INTERFACE GigabitEthernet0/0/0 GigabitEthernet0/0/1 GigabitEthernet0/0/2	<h3>GigabitEthernet0/0/0</h3> <p>Port Status <input checked="" type="checkbox"/> On Bandwidth <input checked="" type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto Duplex <input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto</p> <p>MAC Address <input type="text" value="0002.16A9.5001"/></p> <p>IP Configuration</p> <p>IPv4 Address <input type="text" value="192.168.100.1"/> Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Tx Ring Limit <input type="text" value="10"/></p>
---	--

Screenshot of a network configuration interface showing the configuration of GigabitEthernet0/0/1 port.

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

SWITCHING

- VLAN Database

INTERFACE

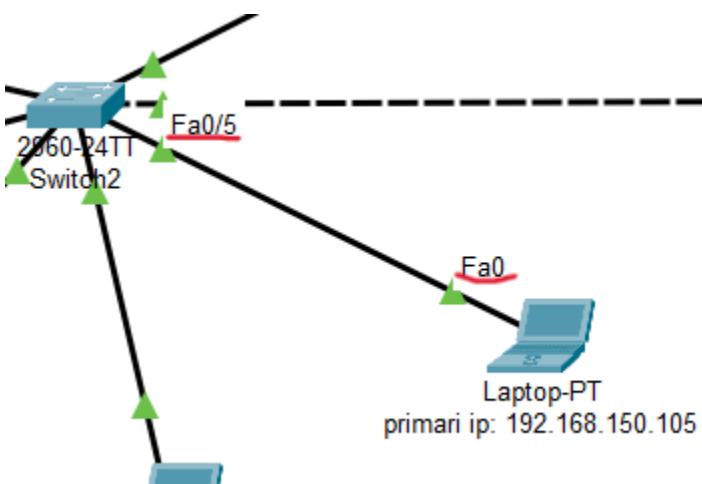
- GigabitEthernet0/0/0
- GigabitEthernet0/0/1** (Selected)
- GigabitEthernet0/0/2

Attributes

GigabitEthernet0/0/1

Port Status	1000 Mbps	100 Mbps	10 Mbps
Bandwidth	Half Duplex	Full Duplex	
Duplex			
MAC Address	0002.16A9.5002		
IP Configuration			
IPv4 Address	192.168.200.1		
Subnet Mask	255.255.255.0		
Tx Ring Limit	10		

In seguito per ogni porta ethernet connessa ai dispositivi sono entrato nelle impostazioni dello switch



E tramite il vlan database ho dato numero e nome alle connessioni vlan

GLOBAL

- Settings
- Algorithm Settings

SWITCHING

- VLAN Database** (Selected)

INTERFACE

- FastEthernet0/1

Attributes

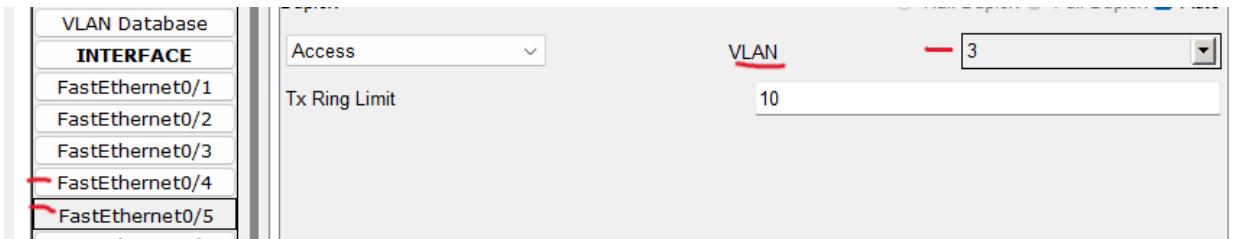
VLAN Configuration

VLAN Number	VLAN Name
-	-
Add	Remove

VLAN No	VLAN Name
1	default

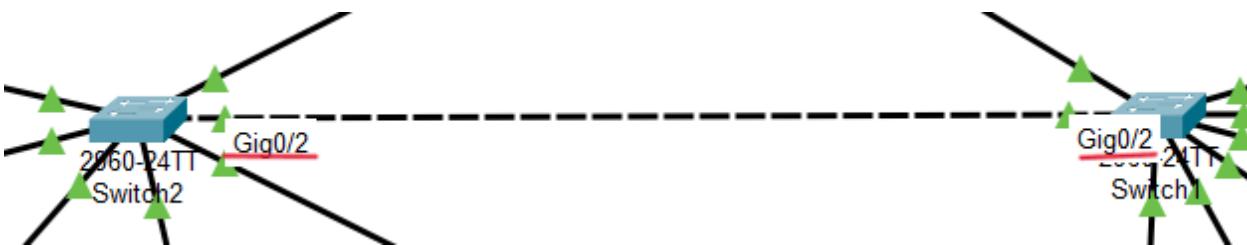
Che ora sono disponibili e assegnabili alle porte.

Essendo riportate in questo esempio le connessioni della porta 04 e 05, andando nelle impostazioni dello switch assegnerò alle porte una sottorete vlan a mia scelta che ho creato in precedenza.

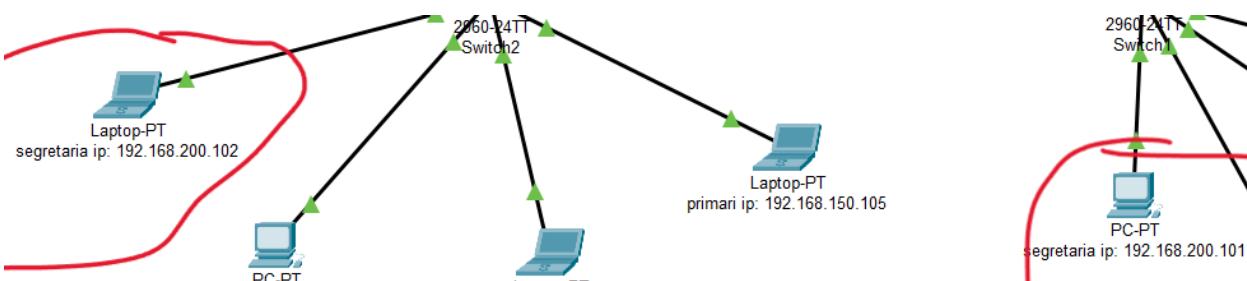


Ho ripetuto lo stesso processo per tutti i computer e le sottoreti che volevo assegnare.

Per connettere due dispositivi appartenenti alla stessa sottorete ma fisicamente collegati a due switch diversi ho connesso i due switch dalla porta gigabit ethernet 02 con un cavo copper crossover.



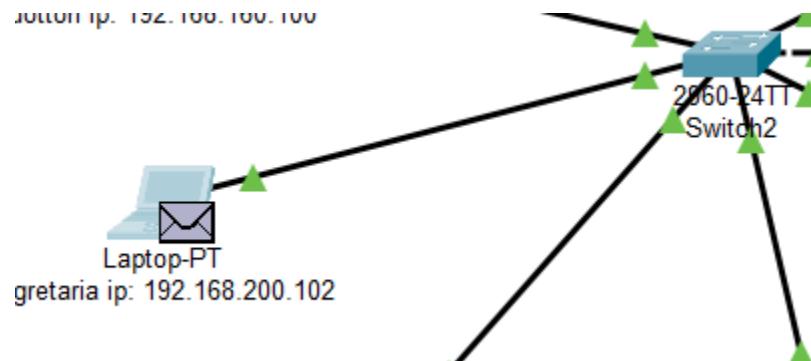
I due computer appartenenti alla stessa vlan (segretaria)



Questi due computer possono ora comunicare avendo assegnato alla porta di ogni switch corrispondente la vlan "segretaria" e avendo impostato lo stesso indirizzo di rete.

Dal terminale del laptop con ip: 192.168.200.102 inserisco il comando: ping
192.168.200.101

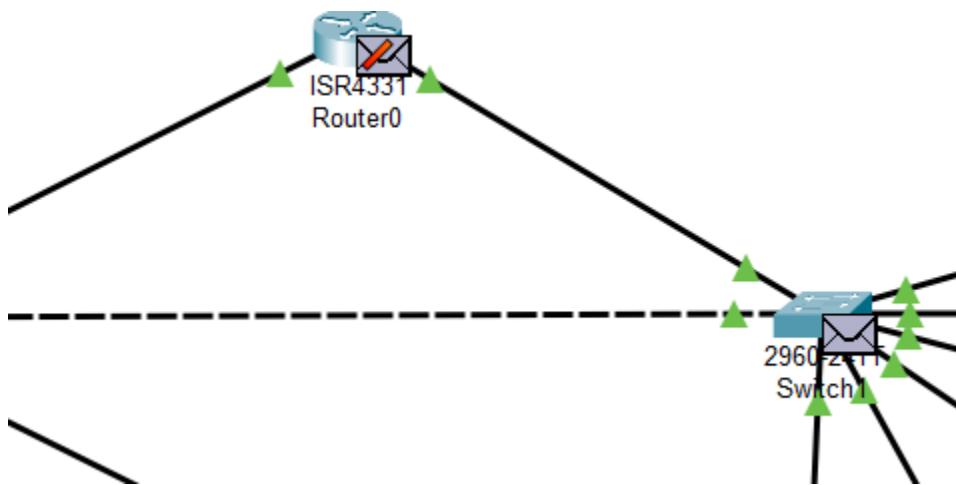
Il quale invierà una richiesta icmp al destinatario, Qui sotto possiamo vedere i movimenti del pacchetto attraverso la rete.



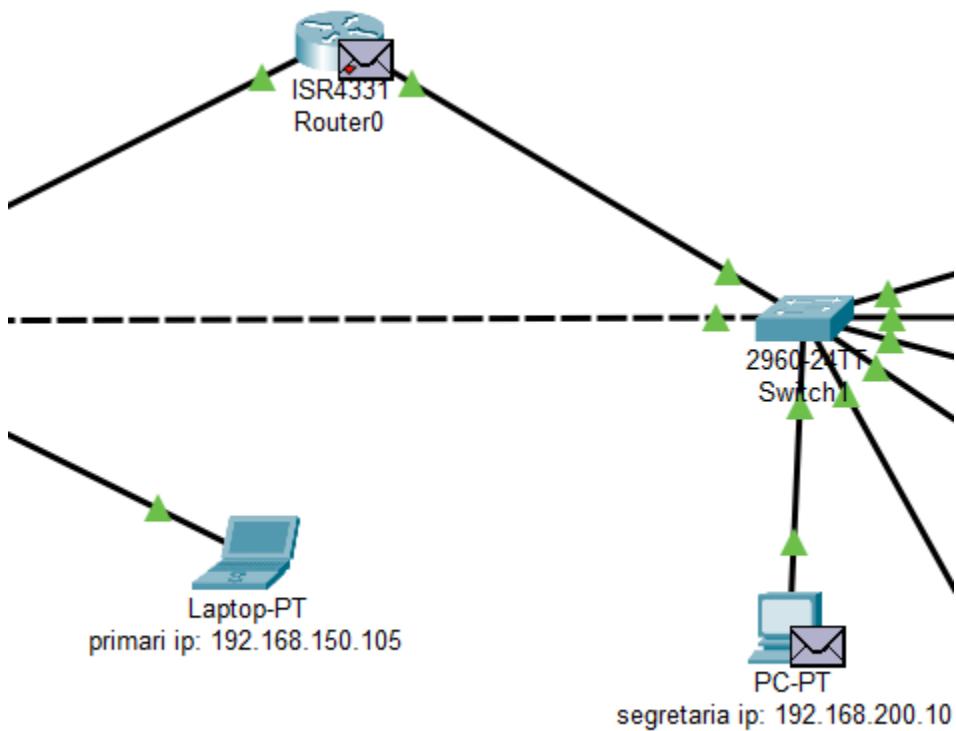
partendo dal primo laptop la richiesta arriva allo switch



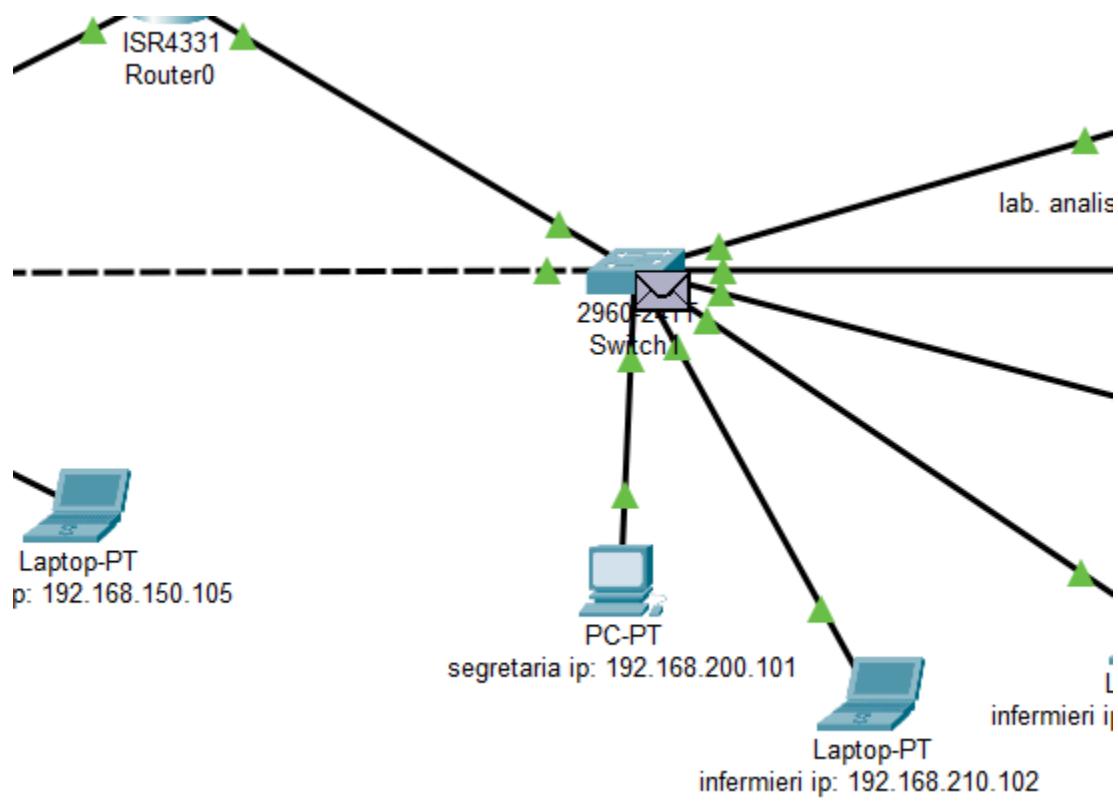
Che successivamente lo instraderà attraverso il trunk della porta gigabit 02 allo switch a cui è collegato il destinatario



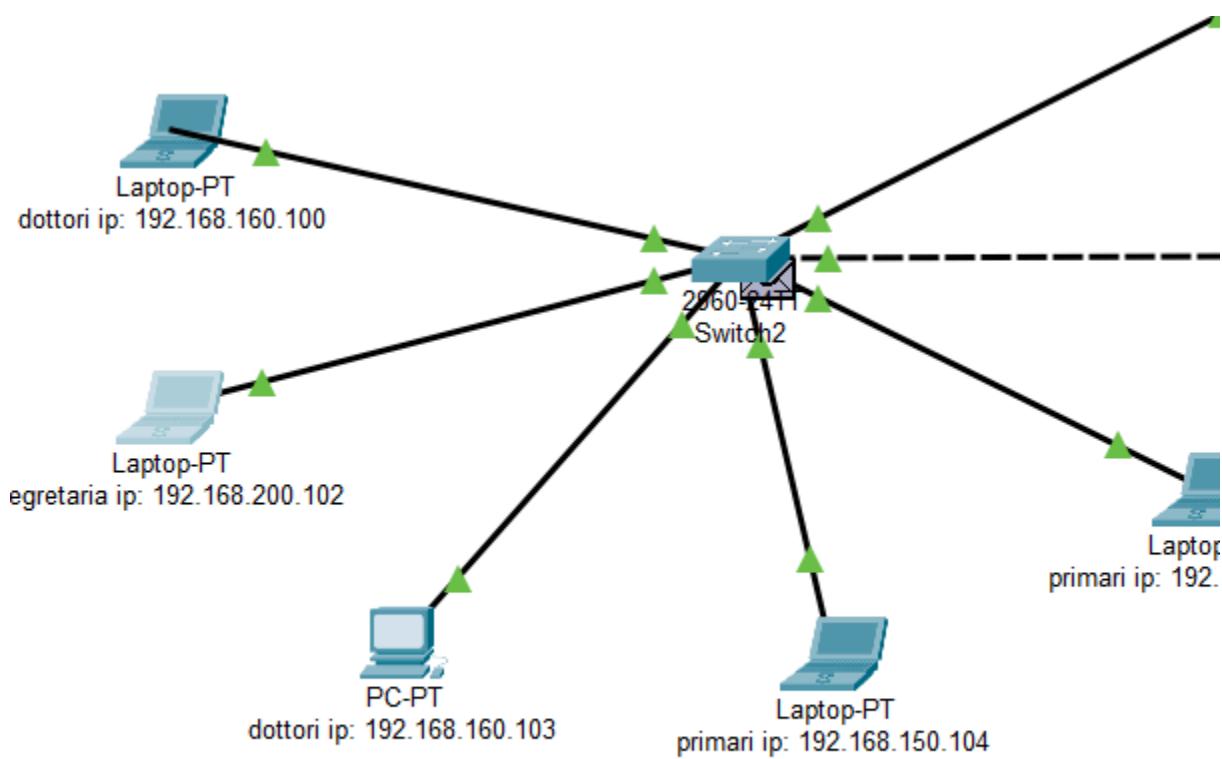
Una volta arrivato allo switch sarà inviato all'indirizzo ip corretto



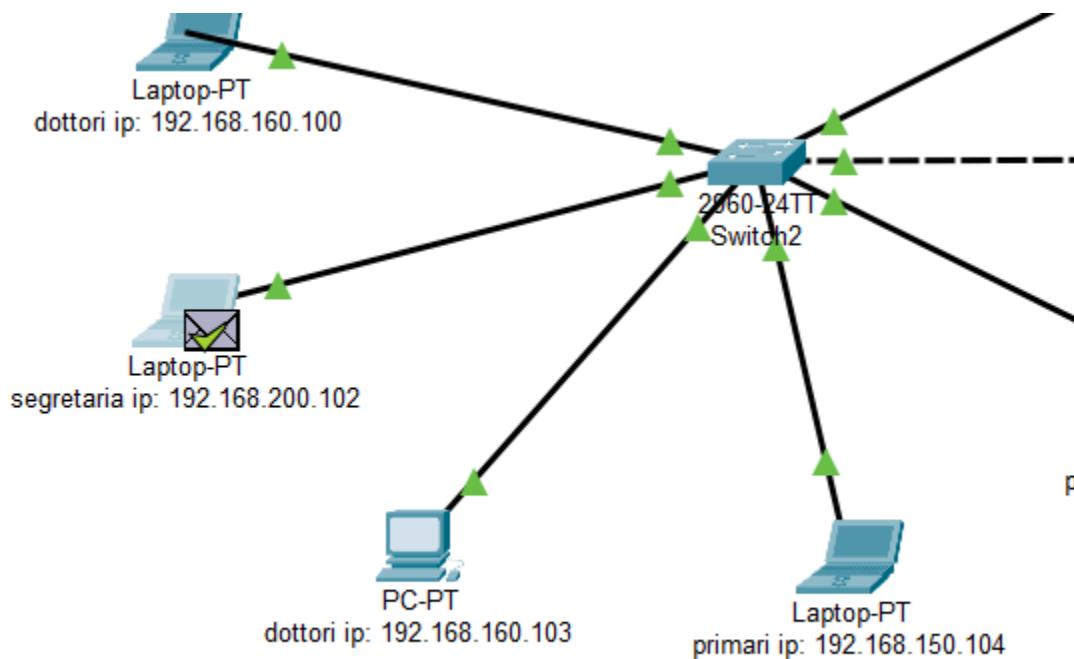
Che poi ritornerà la risposta allo switch



Il quale invierà la risposta al primo switch



Che infine riporterà il pacchetto al mittente.



Dal terminale si può vedere la corretta comunicazione tra i due dispositivi

```

Minimum = 6ms, Maximum = 13ms, Average = 7ms
C:\>ping 192.168.200.101

Pinging 192.168.200.101 with 32 bytes of data:

Reply from 192.168.200.101: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.200.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms

C:\>
  
```