



Federico  
Cuccu

# Rete segmentata con 4 VLAN

Progetto S1/L5

# Progetto della rete

Sottorete	IP Network	IP Broadcast	Host	IP Host
VLAN 10 DIREZIONE	192.168.1.0/24	192.168.1.255/24	PC0	192.168.1.2/24
			PC1	192.168.1.3/24
VLAN 20 SEGRETERIA			PC2	192.168.1.4/24
			PC3	192.168.1.5/24

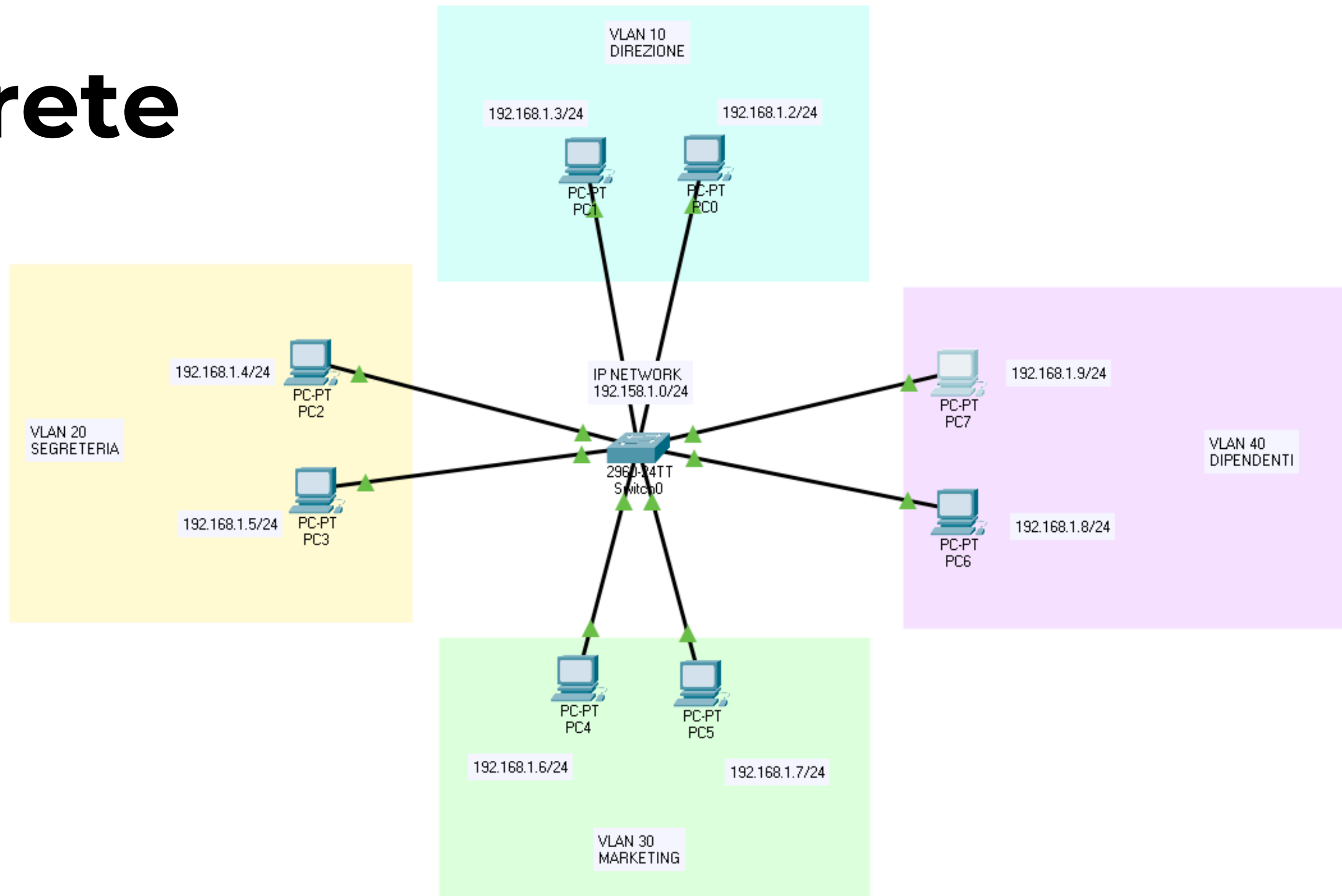
# Progetto della rete

Sottorete	IP Network	IP Broadcast	Host	IP Host
VLAN 30 MARKETING	192.168.1.0/24	192.168.1.255/24	PC4	192.168.1.6/24
			PC5	192.168.1.7/24
VLAN 40 DIPENDENTI			PC6	192.168.1.8/24
			PC7	192.168.1.9/24

# Progetto della rete

Switch	IP Network	IP Broadcast	Interfaccia	ID VLAN
Switch0	192.168.1.0/24	192.168.1.255/24	Ethernet0/1, Ethernet0/2	VLAN 10 DIREZIONE
			Ethernet0/3, Ethernet0/4	VLAN 20 SEGRETERIA
			Ethernet0/5, Ethernet0/6	VLAN 30 MARKETING
			Ethernet0/7, Ethernet0/8	VLAN 40 DIPENDENTI

# La rete



# Prima della segmentazione

Prendiamo come esempio:

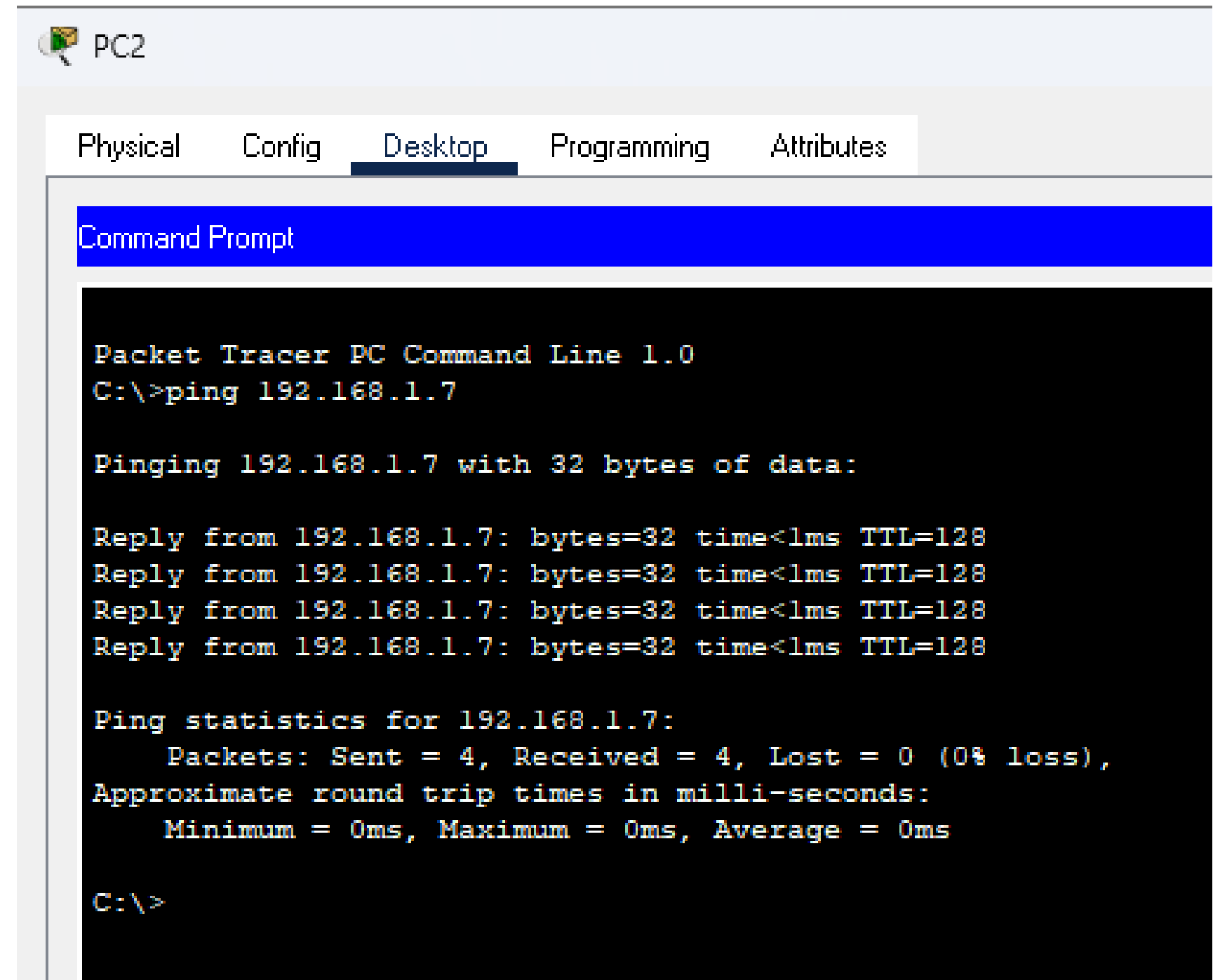
Host mittente: PC2, che ha indirizzo 192.168.1.4/24.

Host destinatario: PC5, con indirizzo 192.168.1.7/24

L'host mittente fa parte della segreteria, mentre l'host destinatario fa parte del reparto marketing, ma solo fisicamente.

La rete ancora **non è stata segmentata** con le VLAN, di conseguenza tutti gli host di questa rete potranno comunicare tra di loro liberamente.

Infatti se proviamo a fare un ping da PC2 a PC5, possiamo notare che tutti e 4 i pacchetti vengono inviati e ricevuti con successo.



The screenshot shows the Packet Tracer interface for PC2. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command from PC2 to PC5 (192.168.1.7). The output indicates that all four packets were successfully received with 0% loss.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

# Dopo la segmentazione

Prendiamo come esempio:

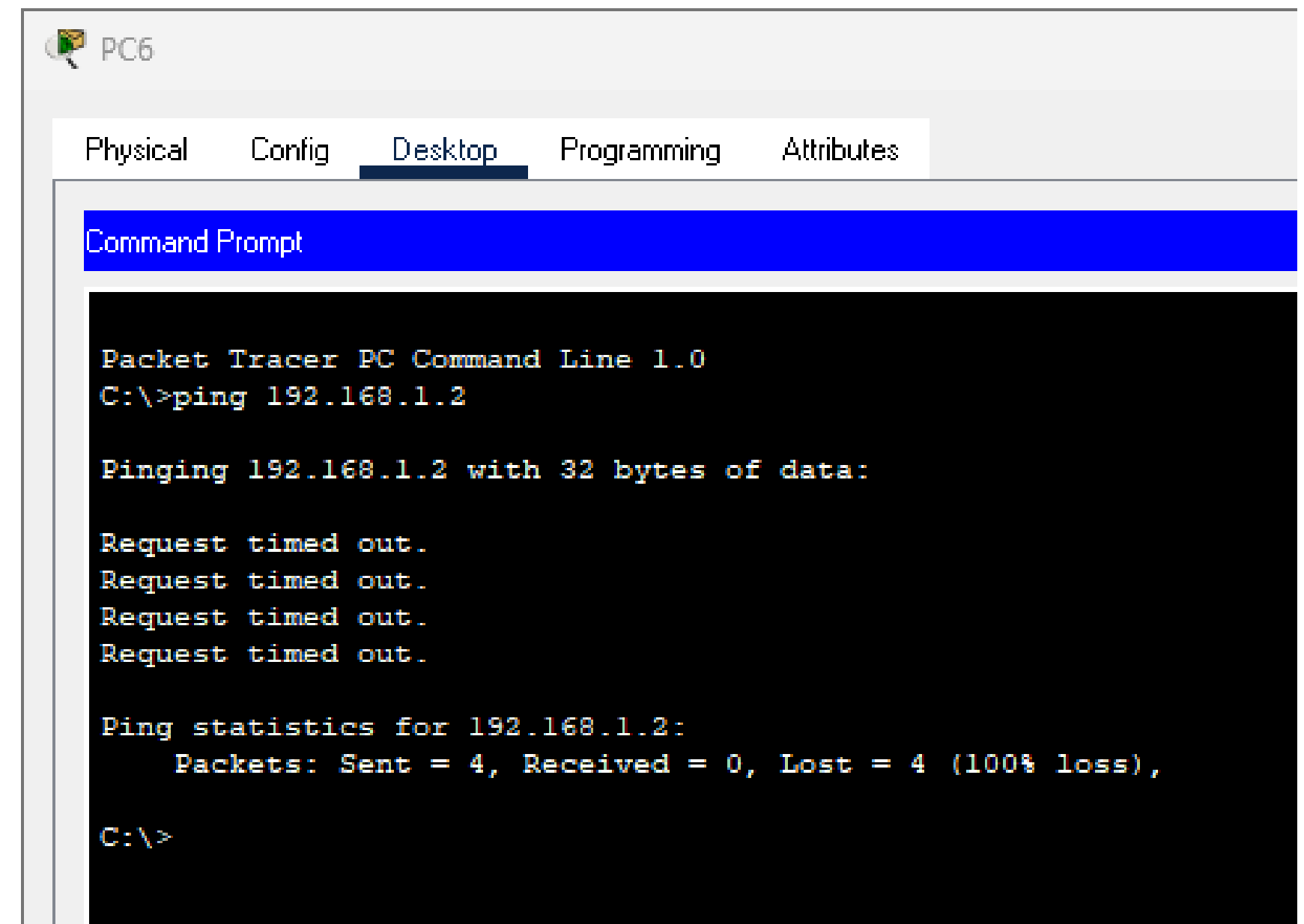
Host mittente: PC6, che ha indirizzo 192.168.1.8/24.

Host destinatario: PC0, con indirizzo 192.168.1.2/24

Ora la rete **è segmentata**: PC6 fa parte della VLAN 40 (Dipendenti) e PC0 fa parte della VLAN 10 (Direzione).

Se proviamo a fare un ping da PC6 a PC0, possiamo notare che tutti e 4 i pacchetti vengono persi.

Da questo momento in poi, gli host non potranno comunicare con host di altre VLAN, bensì potranno comunicare solo con gli host della **stessa VLAN**.



The screenshot shows the Packet Tracer interface for PC6. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command from PC6 to PC0 (192.168.1.2). The output indicates that all four ping requests timed out, resulting in a 100% loss of packets. This demonstrates the failure of communication between hosts in different VLANs after network segmentation.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

# Dopo la segmentazione

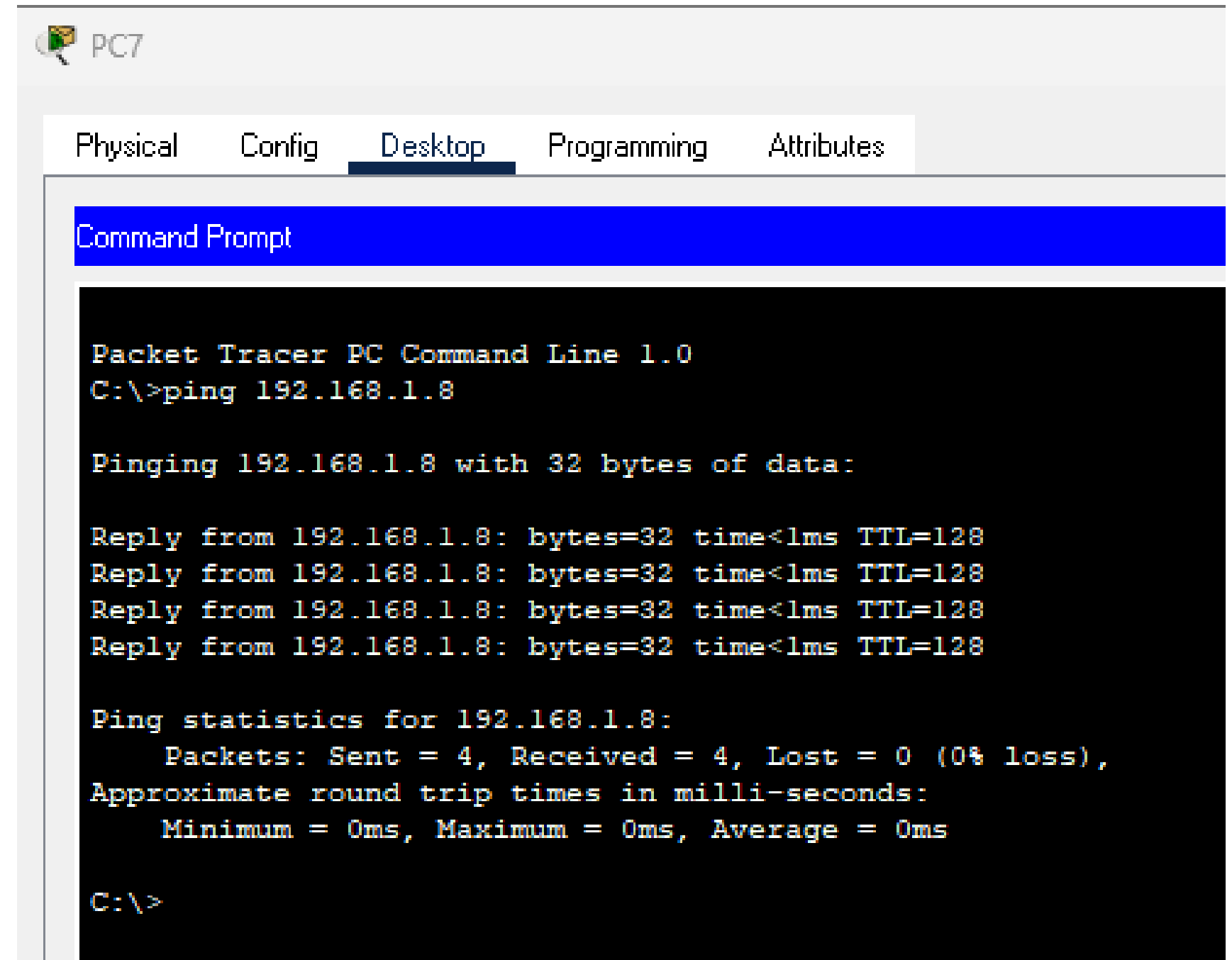
Prendiamo come esempio:

Host mittente: PC7, che ha indirizzo 192.168.1.9/24.

Host destinatario: PC6, con indirizzo 192.168.1.8/24

Entrambi gli host fanno parte della **stessa VLAN** 40  
Dipendenti.

Se proviamo a fare un ping da PC7 a PC6, questi  
possono comunicare tra loro normalmente.



The screenshot shows the Packet Tracer interface for PC7. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command from 192.168.1.9 to 192.168.1.8. The output indicates that all four packets were received successfully with 0% loss and 0ms round trip times.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



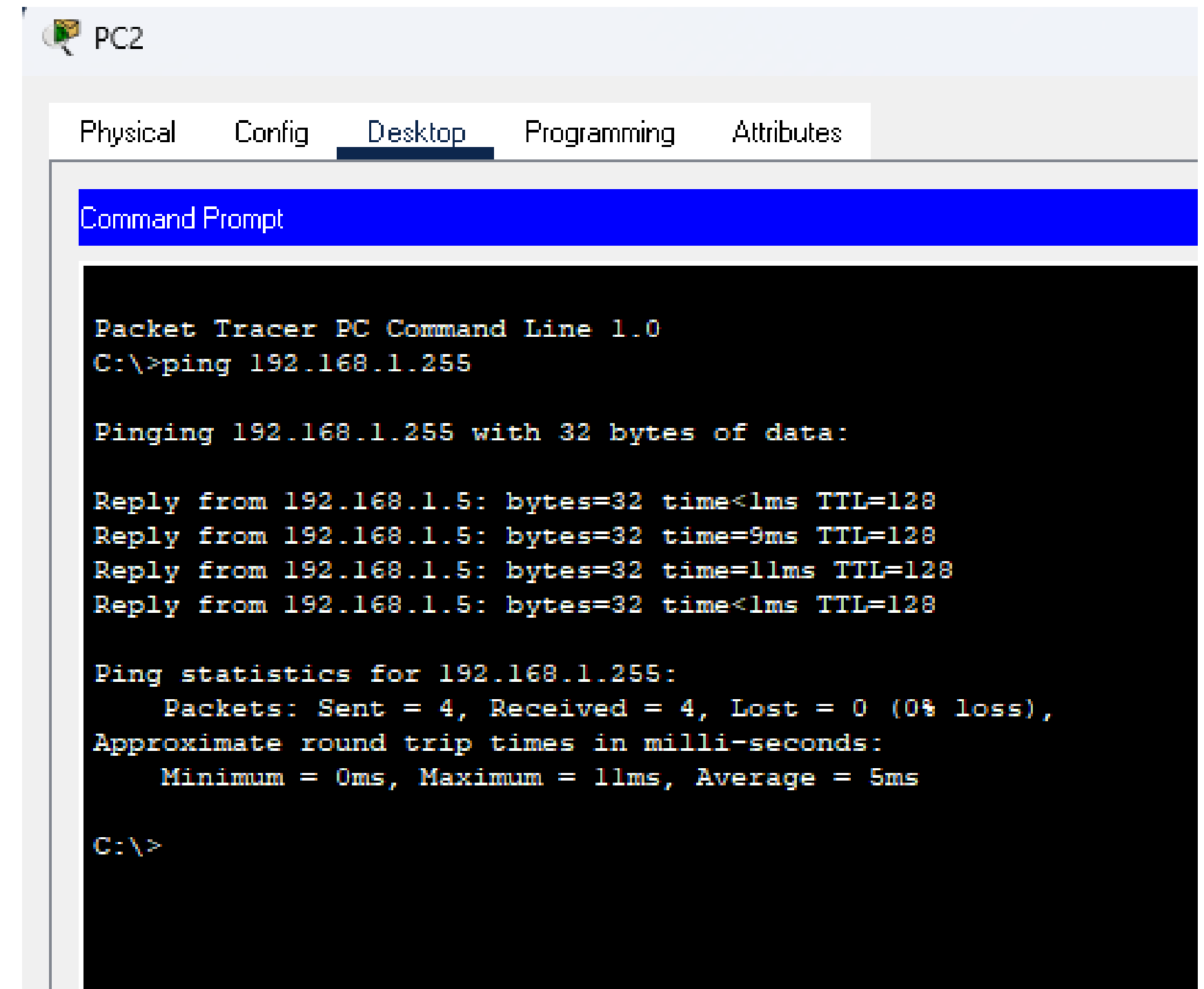
# Dopo la segmentazione

Un'ulteriore prova che dimostra la segmentazione della rete è provare il ping verso l'indirizzo di broadcast, ovvero 192.168.1.255/24.

Provando il ping da uno qualsiasi degli host, si noterà subito che a rispondere saranno solamente gli altri host presenti all'interno della **stessa VLAN**.

Ad esempio: il ping parte da PC2, con indirizzo 192.168.1.4/24, VLAN 20 Segreteria.

Risponderà solamente PC3, con indirizzo 192.168.1.5/24, che fa parte della stessa VLAN.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=9ms TTL=128
Reply from 192.168.1.5: bytes=32 time=11ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>
```

# Perché le VLAN

Con le VLAN si può segmentare la rete senza cambiare la configurazione fisica degli switch e dei cavi.

È sufficiente una semplice **configurazione software** degli switch:

- Si creano le VLAN all'interno del VLAN database
- Ad ogni interfaccia Ethernet, si assegna la VLAN corrispondente

Ad esempio, PC0 e PC1 sono gli host della sala Direzione. Sono collegati allo switch tramite le interfacce Ethernet 0/1 ed Ethernet 0/2.

Nello switch, si assegnano le interfacce Ethernet 0/1 e 0/2 alla VLAN 10 Direzione e il gioco è fatto. La sala Direzione risulterà isolata a livello di rete.

# Perché le VLAN

Oltre ad essere molto semplice creare e gestire le VLAN, queste aumentano:

- **Sicurezza:** si evitano accessi non autorizzati da parte di soggetti non autorizzati ad host della rete contenenti informazioni confidenziali. Inoltre, un attaccante dall'esterno non sarebbe in grado di accedere a tutta la rete, complicando la vita al malintenzionato.
- **Prestazioni:** in ogni sottorete circoleranno solo i pacchetti necessari, riducendo il traffico di pacchetti inutili e diminuendo il carico di traffico nella rete
- **Flessibilità:** si può sempre riorganizzare la rete includendo nuovi host e nuove policy in qualsiasi momento, senza riposizionare fisicamente i dispositivi

# Note

- Non inseriamo l'indirizzo IP gateway e non inseriamo un router gateway nella rete in quanto le sottoreti non devono comunicare tra loro.
- Normalmente i nomi delle VLAN dovrebbero avere nomi in codice, ma in questo caso li scriviamo "in chiaro". Se un attaccante riesce ad entrare nella rete dall'esterno, con i nomi in chiaro saprebbe subito dove si trova all'interno della rete. Utilizzando i nomi in codice, invece, non saprà dove si trova e dovrà andare alla cieca.