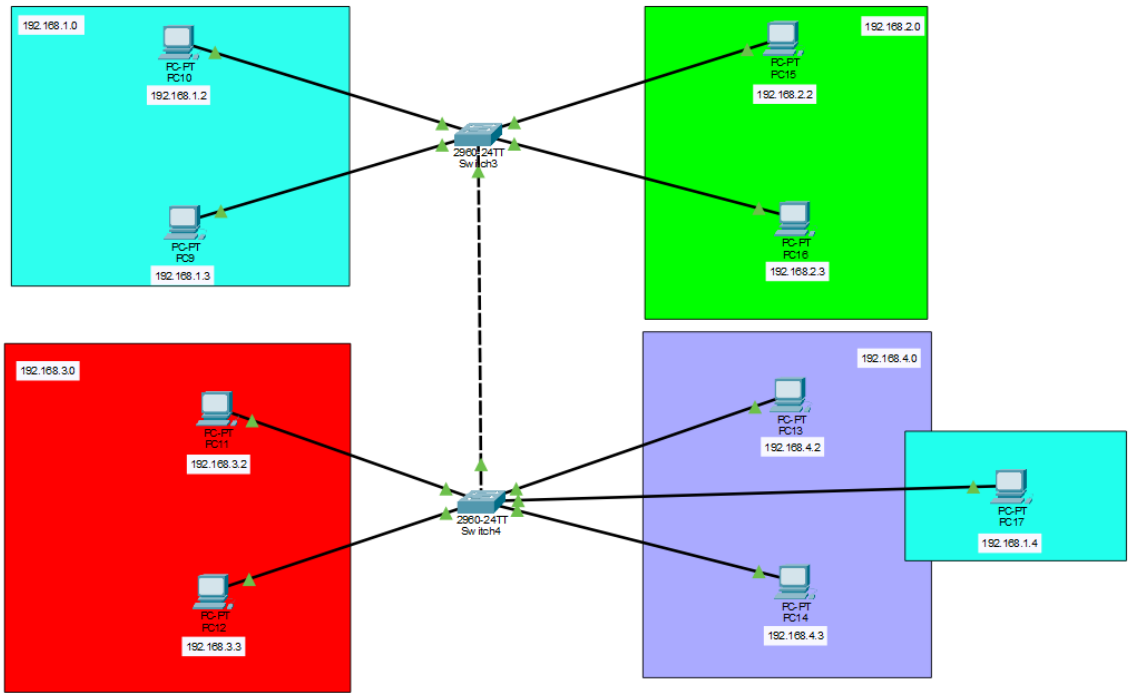
Relazione VLAN

L’obiettivo di questo progetto è quello di realizzare una rete segmentata tramite quattro VLAN distinte, distribuite su due switch. Oltre alla configurazione tecnica, è stato fondamentale comprendere le motivazioni che spingono all’utilizzo delle VLAN e dimostrare il funzionamento del collegamento trunk, necessario per permettere la comunicazione tra dispositivi appartenenti alla stessa VLAN ma collegati a switch differenti.

Fin da subito si è scelto di adottare almeno due switch proprio per mettere in risalto i vantaggi del trunking e della segmentazione logica della rete. In particolare, una delle VLAN contiene dispositivi collegati a entrambi gli switch, rendendo indispensabile configurare correttamente un collegamento trunk per trasportare il traffico VLAN-taggato.

Ogni VLAN è stata associata a una rete diversa attraverso il processo di subnetting: questa scelta permette di isolare il traffico, migliorare la sicurezza e gestire più facilmente l’indirizzamento IP.



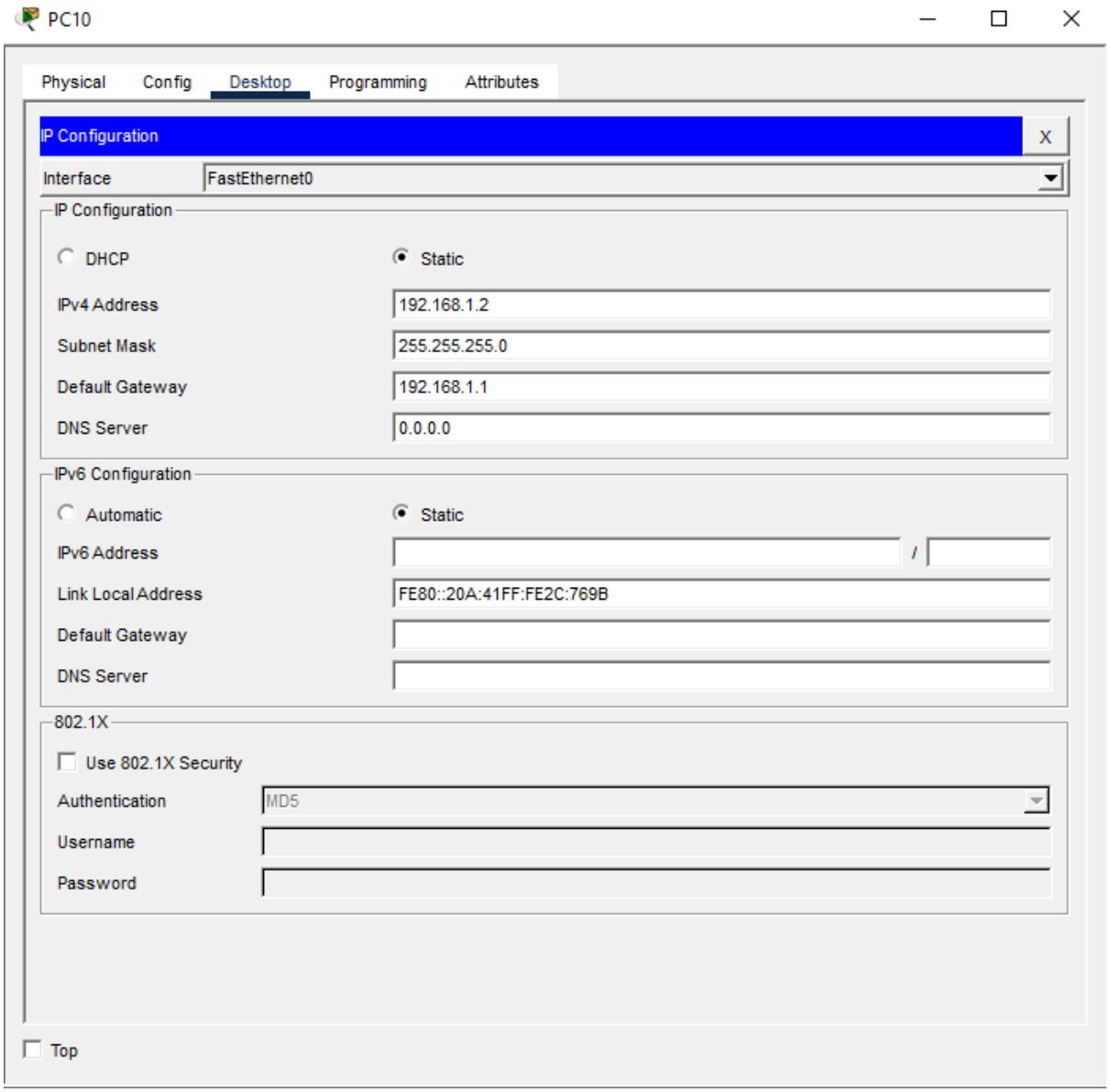
In questa immagine è riportata la struttura fisica della rete: due switch e i vari PC distribuiti nelle quattro VLAN. Ogni gruppo colorato rappresenta

una VLAN diversa, mentre alcune VLAN includono dispositivi collegati su switch differenti per mostrare l'utilità del trunk.
Il collegamento tra gli switch è quello su cui viene configurata la modalità trunk, necessaria a trasportare più VLAN sullo stesso cavo.

Motivazioni della scelta delle VLAN

Le VLAN sono state introdotte per separare logicamente domini di broadcast senza dipendere dalla posizione fisica dei dispositivi. Nel progetto ho scelto quattro VLAN distinte per replicare situazioni reali tipiche in azienda: amministrazione, sviluppo, programmatori, ospiti. Questa separazione permette di ridurre il traffico di broadcast in ogni dominio, aumentare la sicurezza (regole di accesso e firewall per VLAN), e semplificare la gestione e l'applicazione di policy. Ho voluto inoltre dimostrare che una singola VLAN può avere degli host collegati a switch diversi, questo è essenziale per ambienti distribuiti dove gli utenti della stessa funzione non sono concentrati su un unico switch.

Configurazione IP di un host



In questa schermata viene mostrata la configurazione IP dei dispositivi, assegnati a reti diverse in base alla VLAN di appartenenza.
La configurazione prevede:

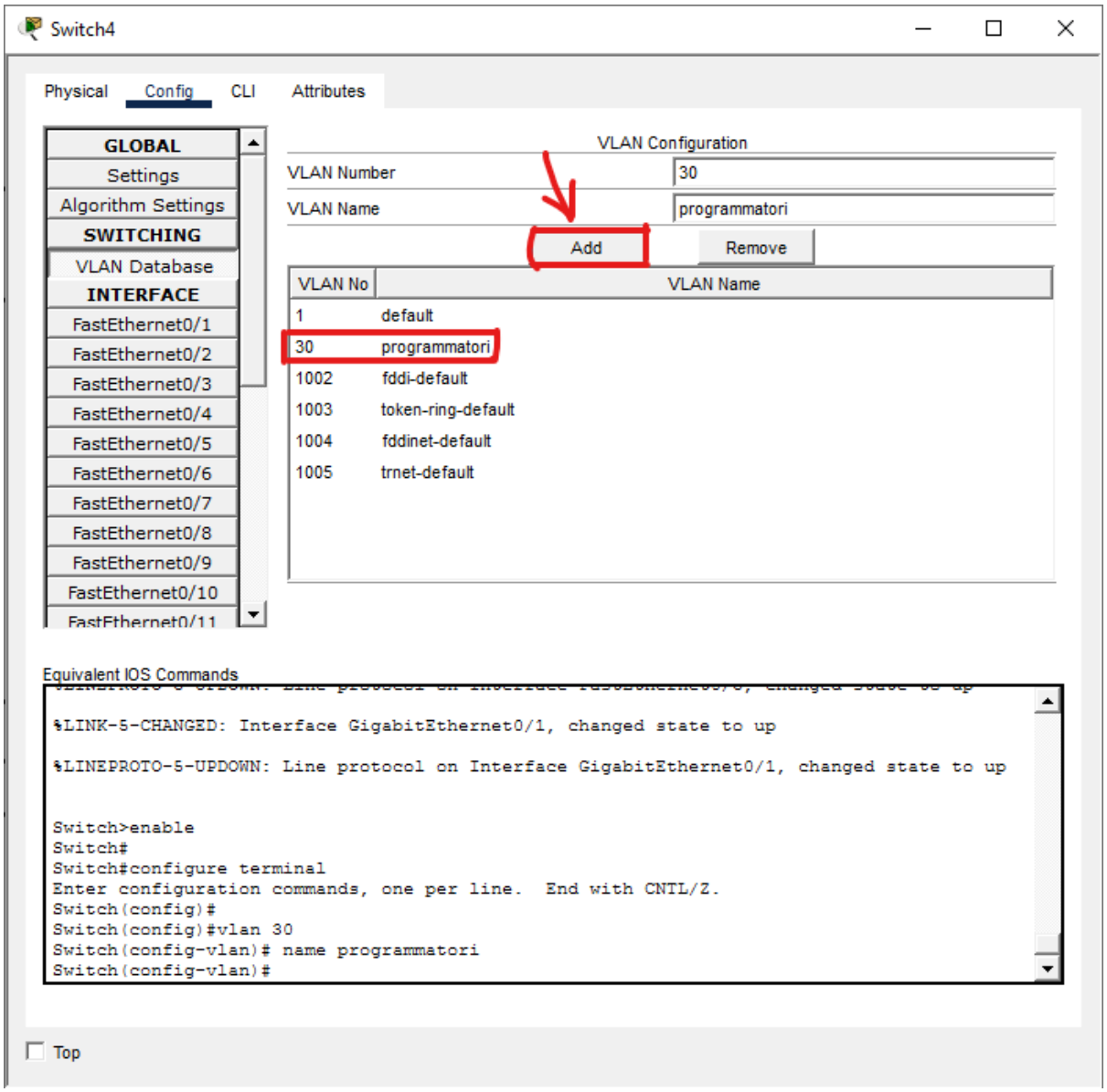
- indirizzo IP appartenente alla subnet dedicata alla VLAN
- maschera corretta in base al subnetting scelto
- gateway (se presente)

Questa fase è essenziale per garantire che gli host appartenenti alla stessa VLAN ma posizionati su switch diversi possano comunicare correttamente.

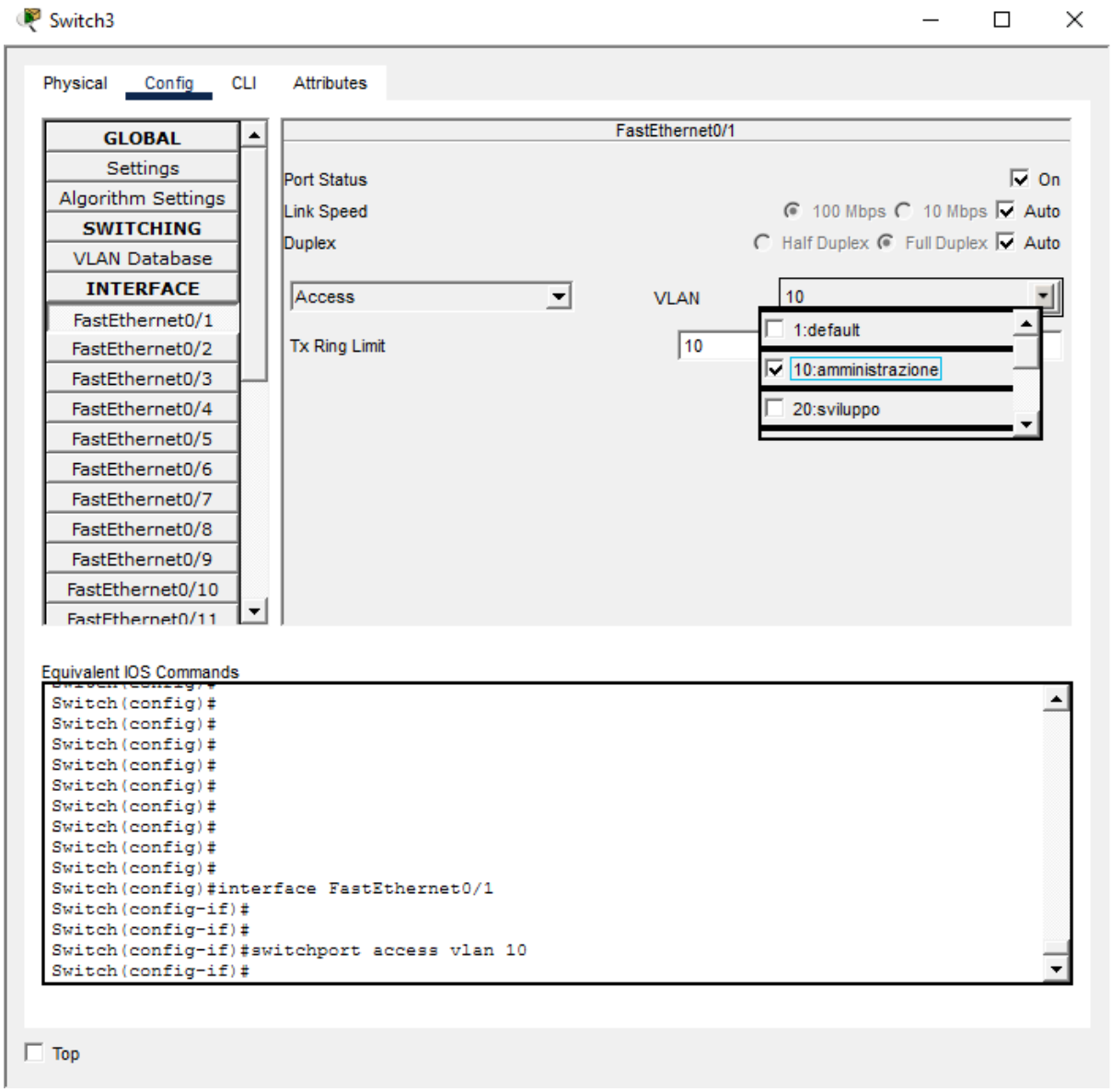
Configurazione delle VLAN sugli switch

Dopo aver configurato gli indirizzi IP bisogna creare le VLAN e collegarci le porte dei dispositivi appositi.

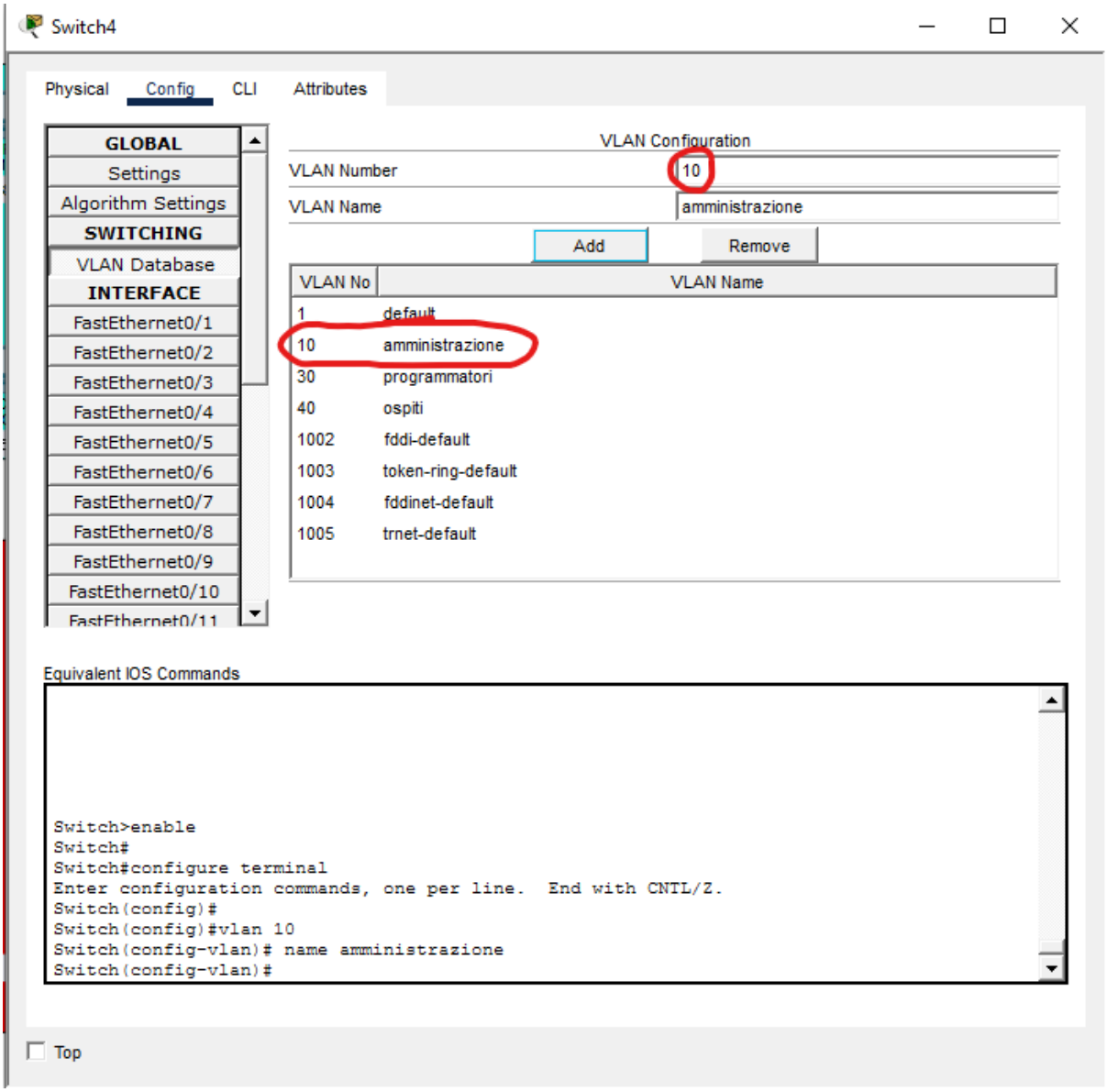
Per creare delle VLAN su Cisco Packet Tracer bisogna accedere allo switch e adare su “config “ e poi “VLAN Database”.



Creiamo le VLAN sull’interfaccia grafica dello switch come mostrato in figura. Ora per suddividere i dispositivi bisogna assegnare le loro porte alle VLAN corrette. Per farlo bisogna accedere di nuovo allo switch e andare sulla porta su cui è collegato il dispositivo interessato.



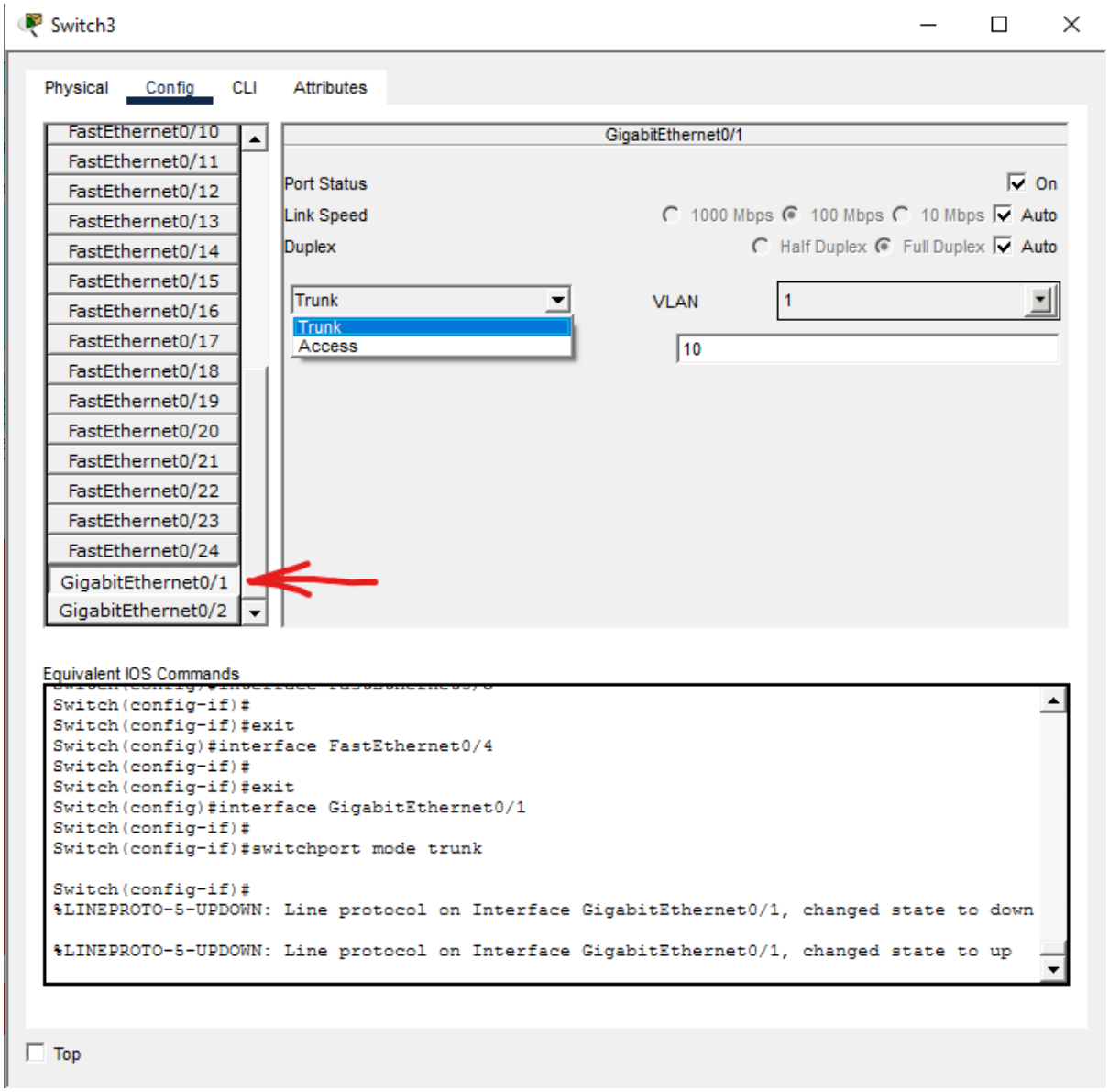
In questa figura assegniamo il dispositivo nella FA0/1 alla VLAN 10 degli amministratori, le porte access permettono allo switch di sapere esattamente a quale VLAN assegnare il traffico proveniente dal dispositivo connesso. Per fare in modo che due dispositivi della stessa VLAN collegati a due switch differenti comunichino bisogna andare sul secondo switch e creare una VLAN con lo stesso numero.



Il numerino cerchiato è il numero della VLAN che deve essere uguale a quello posto sull'altro switch.

Configurazione del TRUNK tra gli switch

Il trunk è il collegamento che permette allo switch di trasportare contemporaneamente più VLAN su un unico cavo.



Come funziona:

- Lo switch aggiunge un tag 802.1Q ai frame Ethernet che attraversano il trunk.
- Questo tag contiene il numero della VLAN.
- Lo switch destinatario riceve il frame, legge il tag e reindirizza il pacchetto alla VLAN corretta.

Se il trunk non fosse configurato:

- Le VLAN rimarrebbero “chiuse” dentro ogni singolo switch

- I dispositivi della stessa VLAN su switch diversi non potrebbero comunicare

Test di comunicazione (Ping) tra host della stessa VLAN

Questo è il test più importante perché dimostra:

- che la configurazione VLAN è corretta
- che gli IP sono stati assegnati correttamente
- che il trunk funziona
- che non ci sono errori sulle porte access

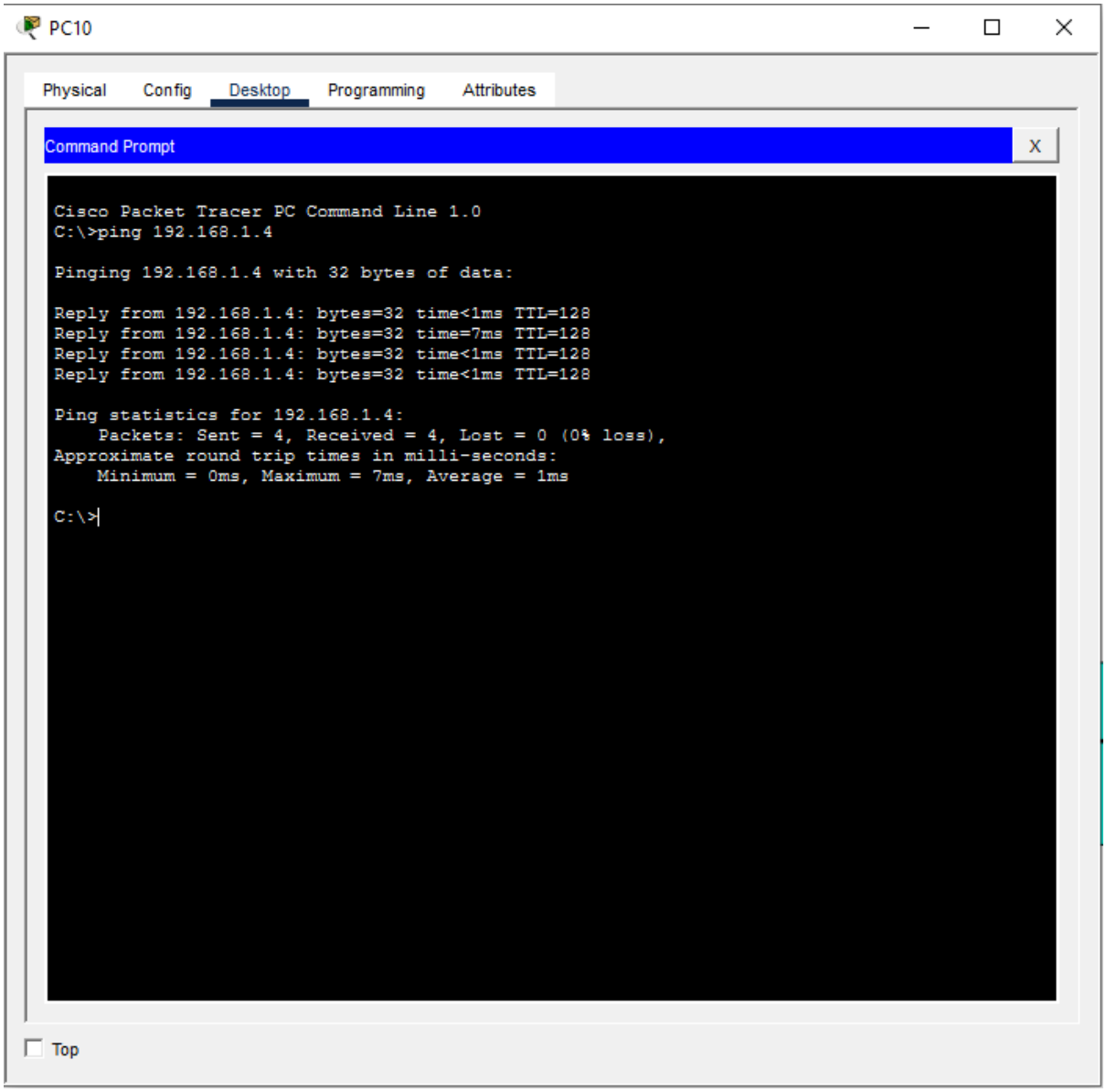
Perché è significativo?

Il ping viene fatto tra due PC

- nella stessa VLAN
- ma collegati a due switch diversi

Se il ping va a buon fine significa che

- il tag VLAN è aggiunto correttamente sul trunk
- gli switch gestiscono correttamente il traffico VLAN-tagged
- gli host sono assegnati alla VLAN corretta



Ho pingato l'indirizzo 192.168.1.4 che è il dispositivo situato sul secondo switch con il pc con indirizzo IP 192.168.1.2 che si trova sul primo switch.

Vantaggi delle VLAN

Maggiore sicurezza

Separare la rete in più VLAN permette di isolare i vari dipartimenti o gruppi di lavoro.

Esempio: un'azienda può isolare la VLAN dell'amministrazione da quella

dei dipendenti o degli ospiti, evitando che utenti non autorizzati accedano a dati sensibili.

Riduzione del traffico di rete

Le VLAN limitano il dominio di broadcast, migliorando le prestazioni complessive della rete.

Esempio: se un PC invia un broadcast ARP, questo rimarrà confinato all'interno della sua VLAN, evitando di danneggiare la rete con traffico inutile.

Maggiore flessibilità

Le VLAN permettono di raggruppare logicamente dispositivi anche se fisicamente lontani.

Esempio: due PC nello stesso reparto ma su piani diversi possono appartenere alla stessa VLAN senza essere collegati allo stesso switch.

Gestione più semplice

Organizzare la rete in VLAN facilita il controllo degli accessi e la manutenzione della rete.

Esempio: un amministratore di rete può facilmente spostare un dispositivo da una VLAN all'altra da remoto, senza dover cambiare la porta fisica dello switch.

Svantaggi delle VLAN

Configurazione più complessa

Richiedono conoscenze tecniche maggiori e una corretta configurazione dei trunk tra gli switch.

Esempio: se il trunk non è configurato correttamente, dispositivi della stessa VLAN ma su switch diversi non comunicano.

Possibili errori di sicurezza

Errori di configurazione possono portare al cosiddetto “VLAN hopping”, dove un dispositivo riesce a raggiungere una VLAN diversa dalla propria.

Esempio: una porta lasciata in modalità “dynamic desirable” può negoziare automaticamente un trunk non voluto.

Maggiore complessità nella diagnostica

Durante i problemi di rete bisogna verificare anche tag, trunk, modalità delle porte e ACL.

Esempio: un semplice errore di VLAN su una porta può far sembrare “guasto” un PC quando in realtà è solo isolato.