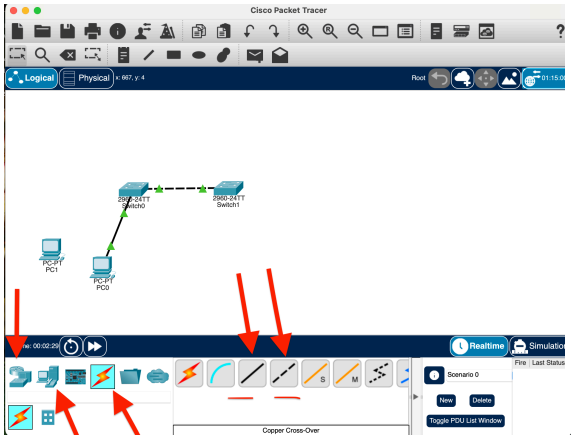
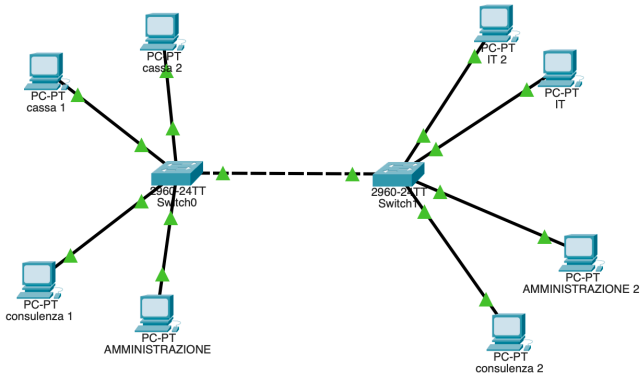
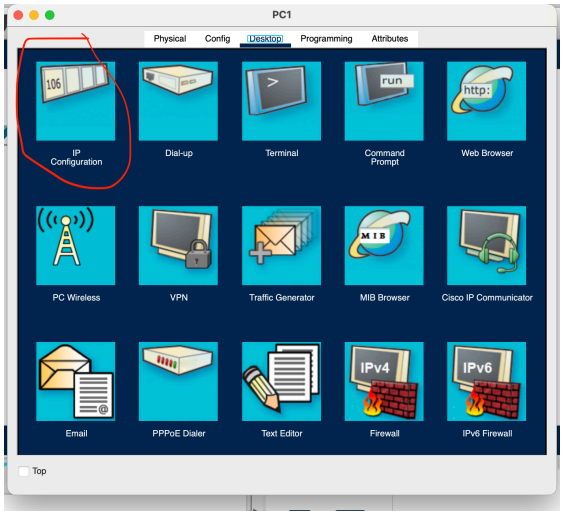
Creazione della rete e impostazioni iniziali

Ipotizzando di trovarci all'interno di una piccola filiale bancaria, creiamo una rete segmentata con quattro VLAN distinte, configurata in modo da evidenziare chiaramente l'utilità della segmentazione. Utilizziamo due switch, collegando i dispositivi in modo distribuito tra di essi.
Per prima cosa creiamo i nostri due switch con i rispettivi PC, per i collegamenti da a i pc useremo il cavo Copper Straight-Through (quello non tratteggiato) mentre per collegare i 2 switch il cavo Copper Cross-Over. Procediamo alla creazione del nostro scheletro, in cui ci saranno 2 Switch e 8 PC, 2 per ogni reparto (ovvero "cassa", "consulenza", "amministrazione" "IT") e andiamo a rinominarli. Successivamente imposteremo gli indirizzi IP (la maschera verrà applicata automaticamente). Attenzione, nella configurazione dei PC imposteremo anche il gateway, che sarà diverso per ogni gruppo IP.
Ecco come sarà il nostro scheletro:

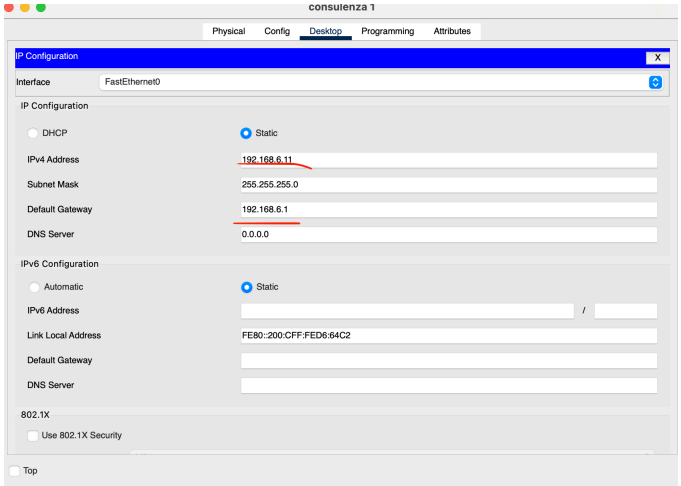


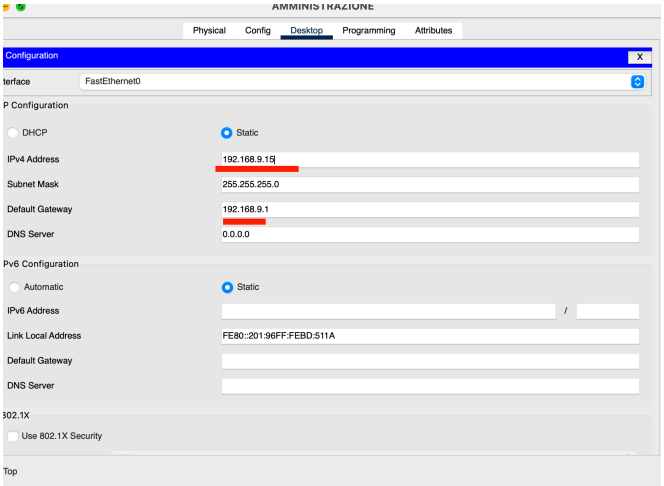




Configurazione degli indirizzi IP dei PC

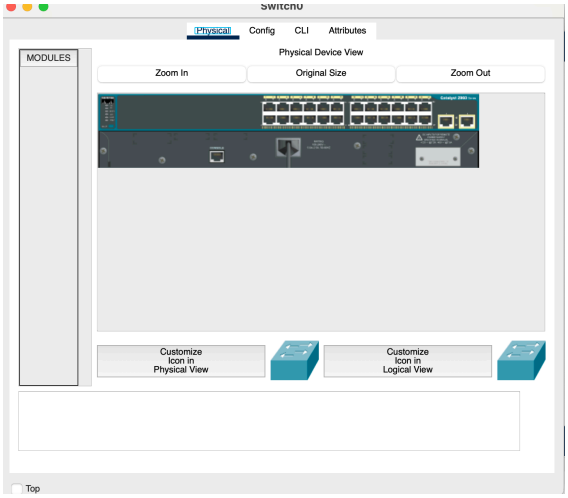
Una volta definito lo scheletro della rete, procediamo con la configurazione dei nostri PC. Selezioniamo il primo PC per applicare le impostazioni necessarie. Dal menu selezioniamo in alto Desktop → IP Configuration, impostiamo l'indirizzo IP e il gateway della rete. È importante che tali parametri siano identici per i PC appartenenti alla stessa VLAN, mentre devono differire per quelli appartenenti ad altri reparti, come mostrato nello screenshot. Facciamo l'operazione per ogni PC

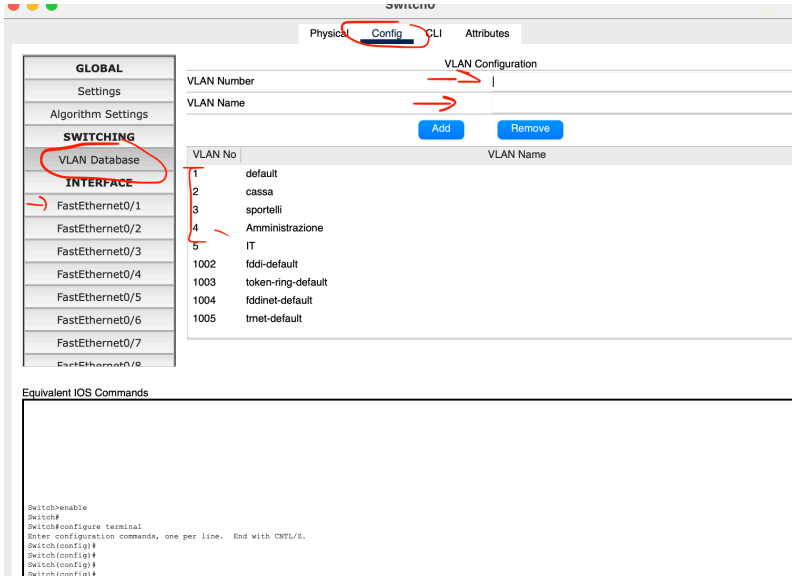




Configurazione delle VLAN sullo switch

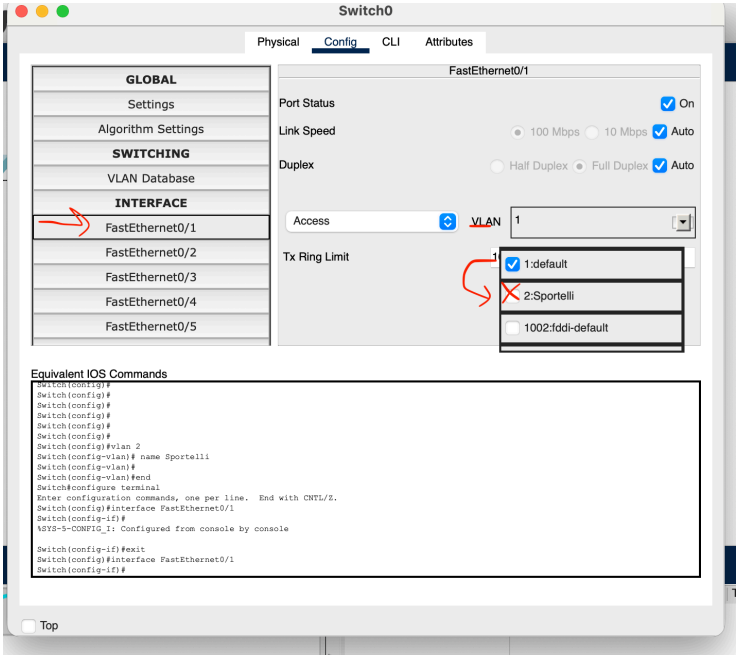
Ora andremo a configurare lo switch creando le VLAN necessarie. La prima VLAN da aggiungere sarà la VLAN 2, che rinomineremo *Cassa*, poiché la VLAN 1 è quella di default.
Per procedere, selezioniamo *Configuration → VLAN Database*: nella sezione indicata dalle frecce inseriamo il numero della VLAN e il relativo nome (senza spazi), quindi premiamo *Add*.
Dopo aver creato la VLAN *Cassa*, aggiungeremo anche le VLAN *Consulenza* e *Amministrazione* e *IT*.
Questa configurazione dovrà essere replicata su entrambi gli switch.





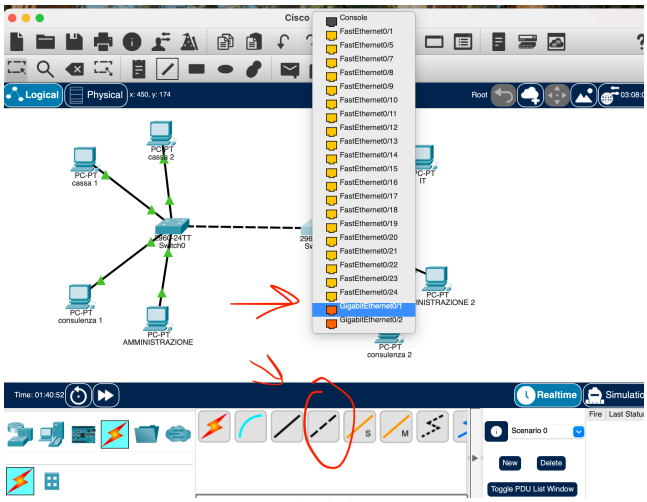
Assegnazione delle VLAN alle porte dello switch

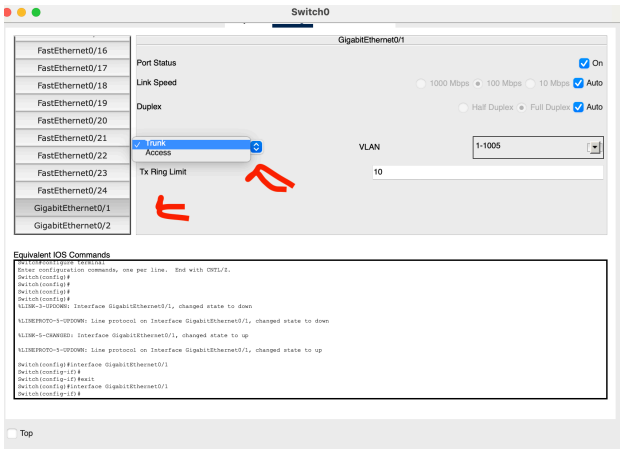
Una volta creata la VLAN, dobbiamo assegnarla alle porte dello switch. Per farlo, indichiamo la porta *FastEthernet 1* (o quella desiderata) che dovrà appartenere a quella specifica VLAN. In questo modo ogni porta servirà correttamente il gruppo di dispositivi associato.



Collegamento degli switch in modalità trunk

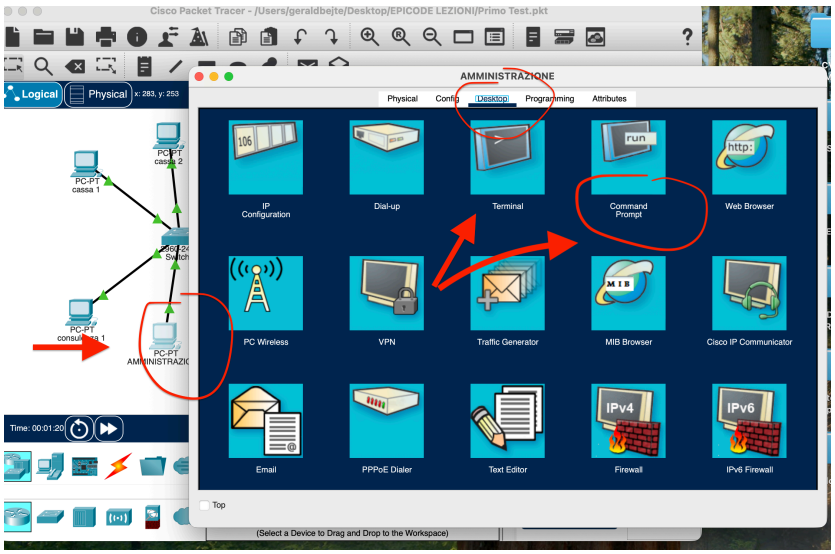
Una volta costruito lo schema, avendo almeno una VLAN con dispositivi distribuiti su switch diversi, e dopo aver assegnato a ciascuna VLAN il proprio nome e configurato su ogni PC l'indirizzo IP corrispondente, possiamo procedere al collegamento degli switch.
Per permettere la comunicazione tra tutte le VLAN presenti nella rete, colleghiamo gli switch utilizzando il cavo sulla porta Gigabit, configurata in modalità trunk. Questo collegamento consente il trasporto simultaneo di tutte le VLAN tra i due apparati.
Dopo aver stabilito il collegamento fisico, accediamo alla configurazione delle interfacce e impostiamo la porta come trunk, abilitando il passaggio di tutte le VLAN coinvolte nel progetto.
In questo modo le VLAN distribuite su entrambi gli switch possono comunicare correttamente e la rete risulta pienamente operativa.



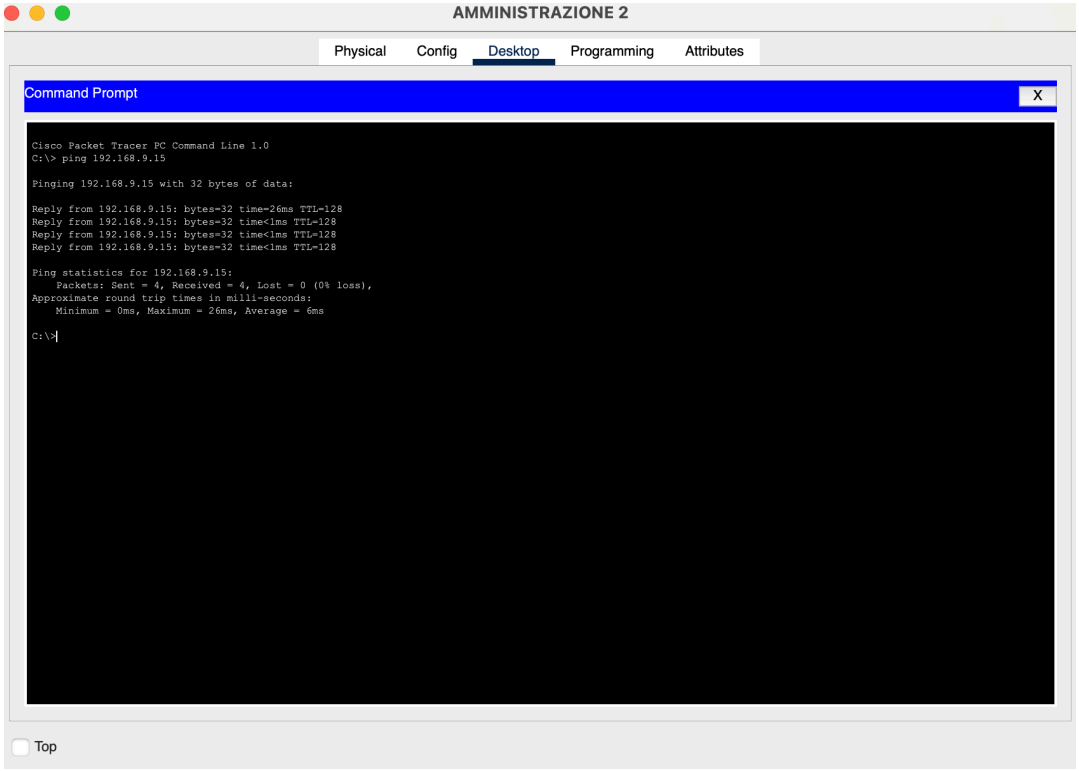


Verifica del funzionamento tramite ping

Per controllare che tutto funzioni correttamente, è necessario effettuare un test di comunicazione con il comando **ping**. Dal computer selezionato apriamo *Desktop → Command Prompt*, dove comparirà una schermata nera nella quale possiamo inserire i comandi di rete.
Il comando ping serve a verificare se un dispositivo è raggiungibile: basta digitare *ping* seguito dall'indirizzo IP del PC con cui vogliamo comunicare. Nel nostro esempio, il PC **Amministrazione 1** ha indirizzo **192.168.9.15** e vogliamo verificare la comunicazione con *Amministrazione 2* passando attraverso i due switch.
Se il comando è scritto correttamente e la configurazione è giusta, il terminale risponderà con la dicitura **Reply**, confermando che il dispositivo è raggiungibile. È importante fare attenzione a digitare correttamente l'indirizzo IP, perché anche un solo numero sbagliato impedirà il test.



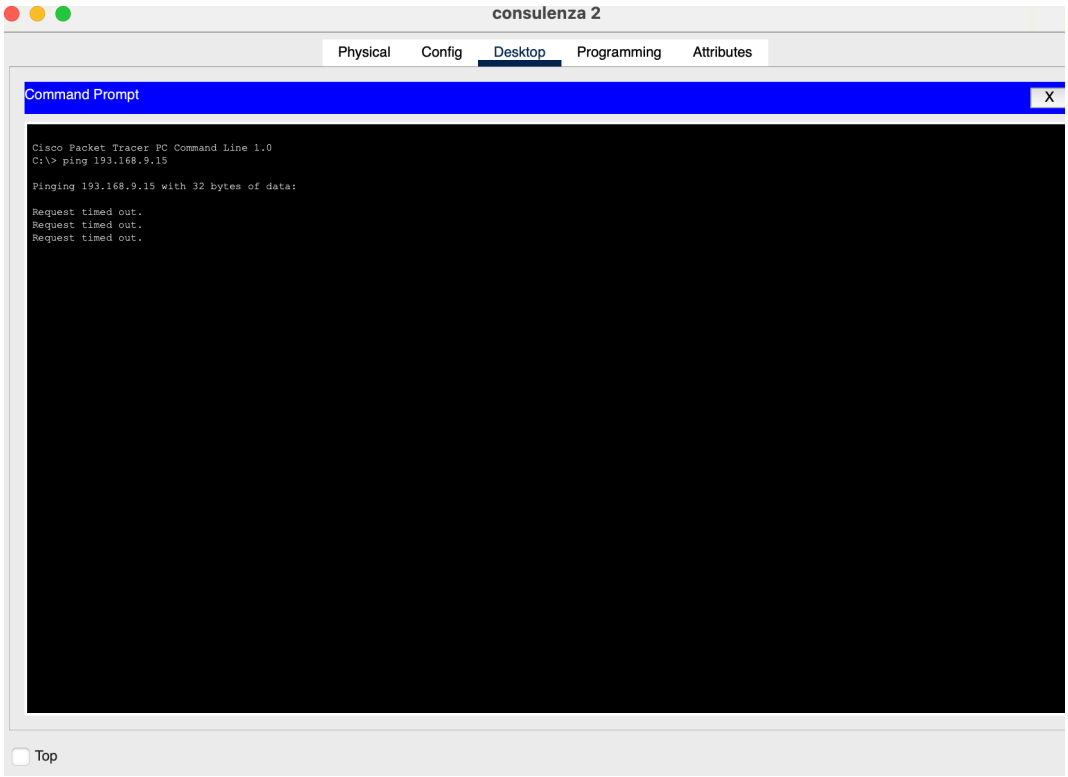
Come si vede dall'esempio del nostro caso il circuito di comunicazione funziona correttamente.



,

Verifica dell'isolamento tra VLAN diverse

Per fare la prova del nove e verificare che le VLAN siano realmente isolate tra loro, assegniamo lo stesso indirizzo IP a un altro computer collegato allo stesso switch, ma appartenente a una VLAN diversa e con un range di indirizzi differente.
Ora, eseguendo il test di comunicazione tramite *ping*, il risultato sarà **Request Time Out**, perché i dispositivi di VLAN diverse non possono comunicare tra loro senza un router o un'interfaccia Layer 3 che le instradi.
Nel nostro caso abbiamo effettuato il test su **Cassa 1**, confermando che la separazione tra le VLAN funziona correttamente.



Vantaggi e limiti dell'uso delle VLAN

Le VLAN vengono utilizzate per aumentare la sicurezza e l'organizzazione di una rete. Separando i computer in gruppi logici distinti, anche se collegati allo stesso apparato fisico, le VLAN permettono di isolarli tra loro: un dispositivo appartenente a una VLAN non può comunicare liberamente con quelli di un'altra, a meno che non si utilizzi un apparato di routing autorizzato. Questo isolamento riduce i rischi legati ad attacchi interni e limita la diffusione di eventuali problemi o malware all'interno della rete.

Oltre alla sicurezza, le VLAN migliorano anche le prestazioni complessive. Segmentando la rete, viene ridotto il dominio di broadcast e diminuisce il traffico generato da protocolli come ARP. Questo porta a una rete più ordinata, leggera e veloce, soprattutto in contesti dove i dispositivi sono numerosi e appartengono a reparti diversi. Un ulteriore vantaggio è la semplificazione della gestione: grazie alle VLAN è possibile organizzare o riorganizzare la rete senza dover spostare fisicamente i dispositivi, poiché la separazione avviene a livello logico.

Naturalmente esistono anche alcuni limiti. Le VLAN richiedono apparati compatibili e una configurazione più accurata rispetto a una rete non segmentata; un errore nell'assegnazione delle porte o nel collegamento trunk può impedire la comunicazione tra interi gruppi di dispositivi. Inoltre, se si desidera far comunicare le diverse VLAN è necessario introdurre un router o uno switch di livello superiore, aumentando così la complessità dell'infrastruttura.

A questi limiti si aggiungono ulteriori svantaggi pratici. Le VLAN dipendono fortemente dallo switch: un guasto dell'apparato può bloccare contemporaneamente più reti logiche, impattando l'intera organizzazione. La configurazione può risultare complessa, soprattutto in reti medio-grandi, e questa complessità introduce anche una certa rigidità nella gestione quotidiana. Infine, una VLAN configurata in modo scorretto può trasformarsi in un punto debole della rete, esponendo a vulnerabilità di sicurezza o a fughe di dati tra reparti separati.

Nel complesso, la creazione di una rete segmentata con quattro VLAN permette di ottenere un ambiente più sicuro, ordinato ed efficiente, adatto soprattutto in contesti organizzativi suddivisi per funzioni o reparti.