

Introduzione: Definizione e scopo di una VLAN

Una VLAN è una rete logica che permette di dividere una rete fisica in diverse sottoreti isolate tra loro, indipendentemente dalla configurazione fisica di switch e cavi, consentendo così una gestione del traffico di rete più flessibile e sicura.

Tra i vari vantaggi dell'implementazione di una VLAN, possiamo includere infatti una maggiore sicurezza e un miglioramento delle prestazioni di rete, dovuti alla riduzione del dominio di broadcast e alla separazione del traffico tra diversi gruppi di dispositivi. Una VLAN permette inoltre di modificare l'organizzazione della rete senza lo spostamento fisico dei dispositivi, garantendo notevole flessibilità.

Una VLAN viene configurata a livello di switch tramite la possibilità di assegnare ciascuna sua porta ad una VLAN specifica. Esistono principalmente due tipi di porte VLAN: la porta di accesso, attraverso cui si collegano i dispositivi che appartengono ad una singola VLAN, e le porte trunk, attraverso cui si collegano gli switch e che possono trasportare il traffico di più VLAN.

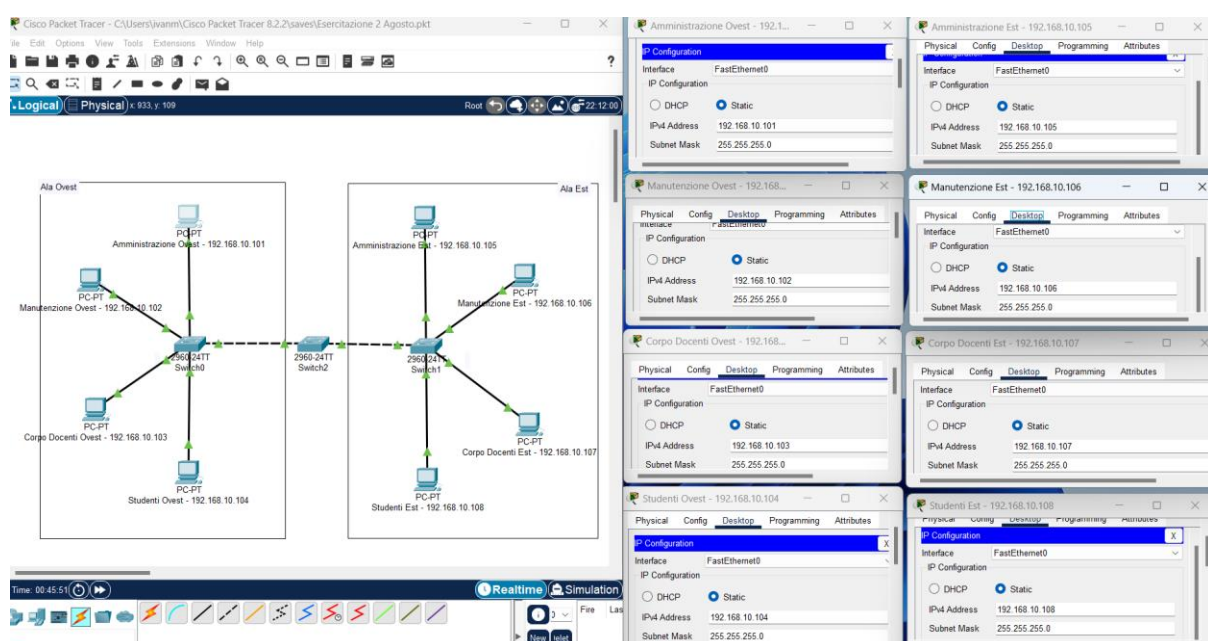
Caso Studio: creazione di una rete segmentata con quattro VLAN diverse

Prendiamo in esame l'esempio di una ipotetica rete di un campus universitario di piccolissime dimensioni che vogliamo segmentare in quattro diverse VLAN, così suddivise:

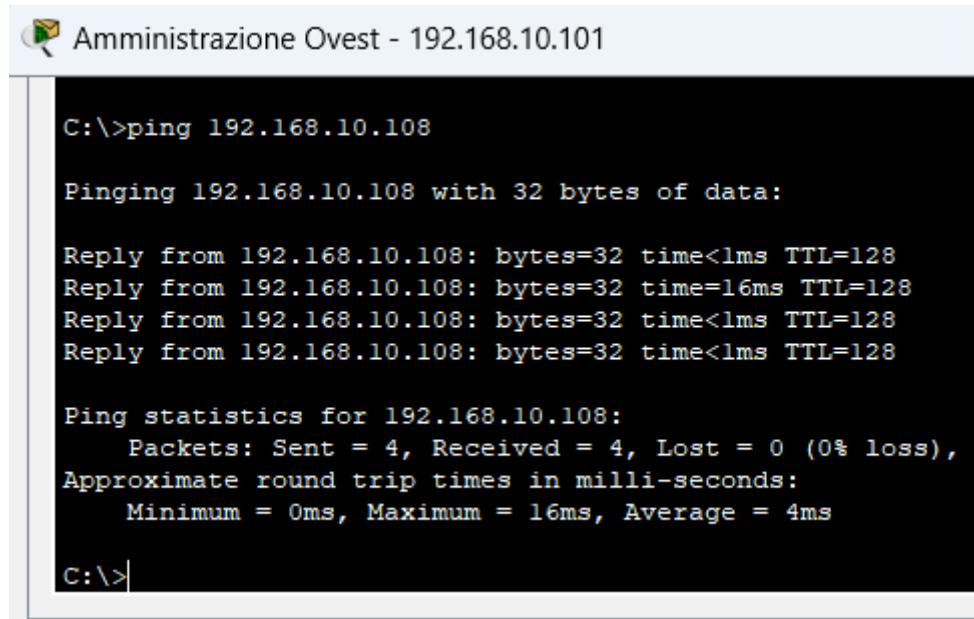
1. VLAN 10: Amministrazione
2. VLAN 20: Manutenzione
3. VLAN 30: Corpo Docenti
4. VLAN 40: Studenti

Lo scopo è quello di segmentare la rete in quattro sezioni isolate tra loro di modo da non solo diminuire il dominio di broadcast e quindi alleggerire il traffico, ma anche di aumentare la sicurezza e facilitare la risoluzione di eventuali problemi.

Per prima cosa andiamo ad inserire i vari dispositivi host, configurandone nome e IP, e collegandoli tra loro con degli switch. In questo esempio, immaginiamo una rete composta da otto dispositivi geograficamente distribuiti in due diverse aree e collegati da un numero totale di tre switch.



Per verificarne la connessione, eseguiamo un ping da PC Amministrazione Ovest (192.168.10.101) a PC Studenti Est (192.168.10.108) che al momento si trovano sulla stessa rete.



```
C:\>ping 192.168.10.108

Pinging 192.168.10.108 with 32 bytes of data:

Reply from 192.168.10.108: bytes=32 time<1ms TTL=128
Reply from 192.168.10.108: bytes=32 time=16ms TTL=128
Reply from 192.168.10.108: bytes=32 time<1ms TTL=128
Reply from 192.168.10.108: bytes=32 time<1ms TTL=128

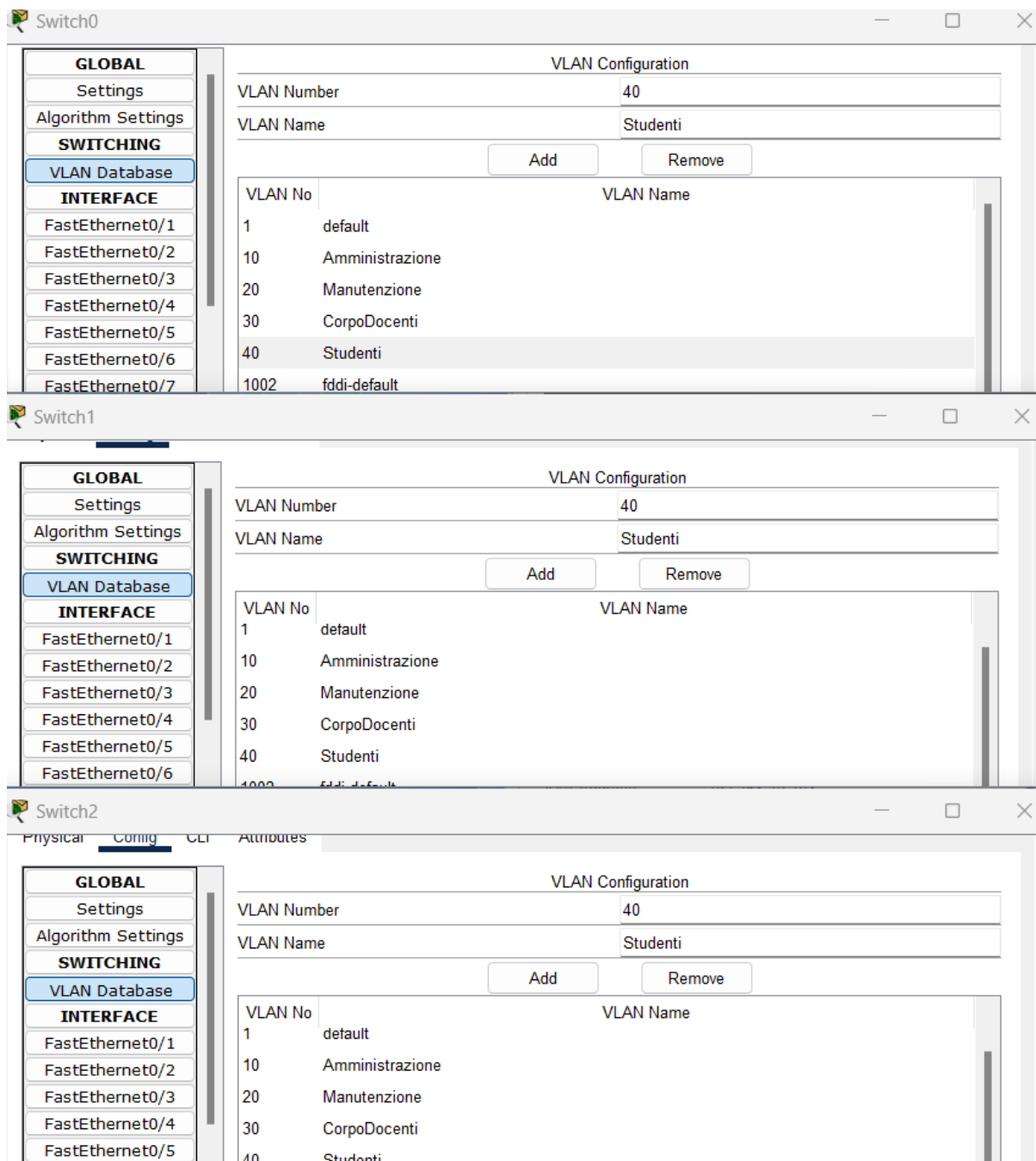
Ping statistics for 192.168.10.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>
```

Procediamo ora con la configurazione delle VLAN sugli switch.

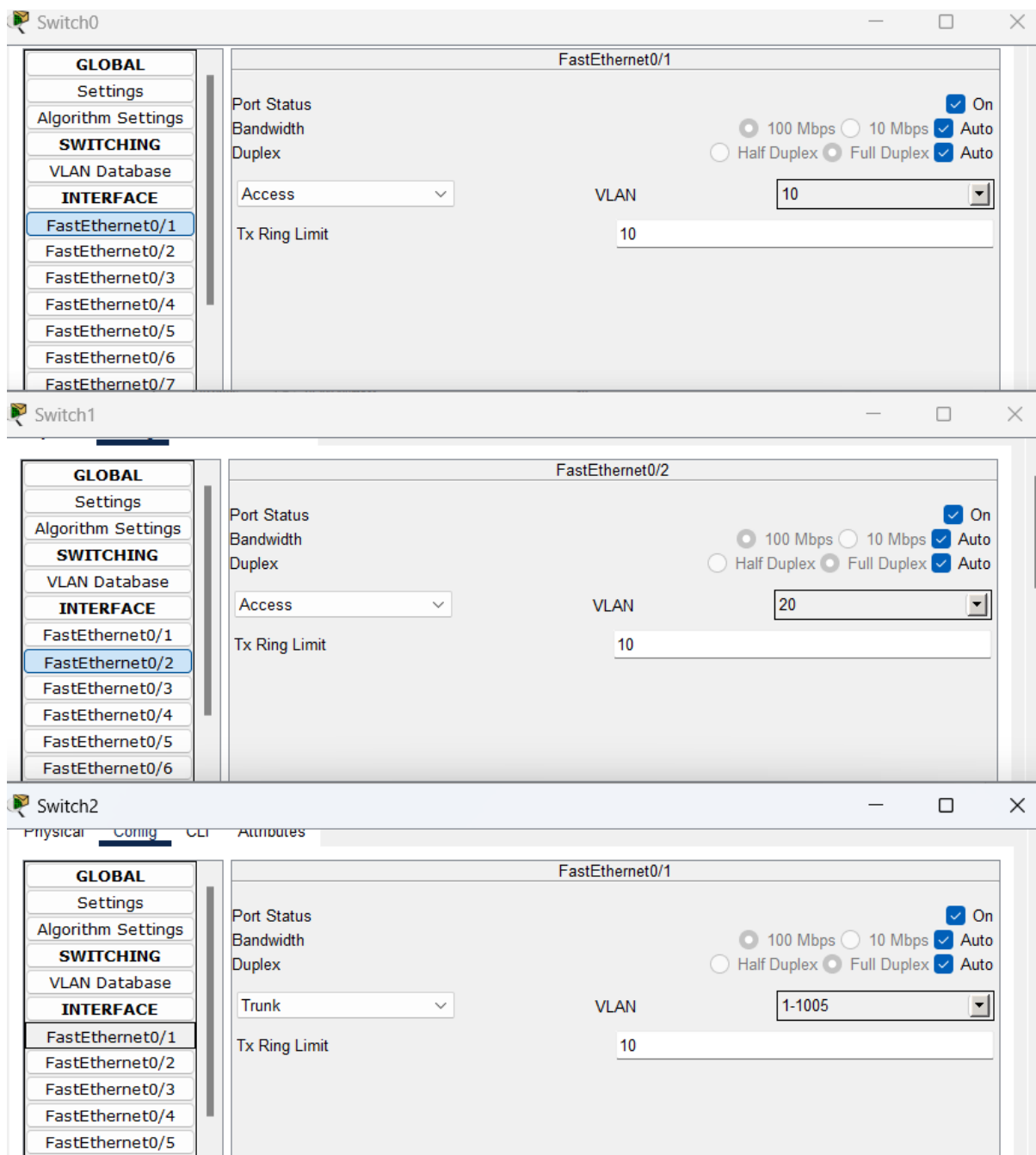
Per ogni switch inseriamo numeri ed etichetta corrispondenti alle VLAN che vogliamo creare, in questo caso:

1. VLAN 10: Amministrazione
2. VLAN 20: Manutenzione
3. VLAN 30: Corpo Docenti
4. VLAN 40: Studenti

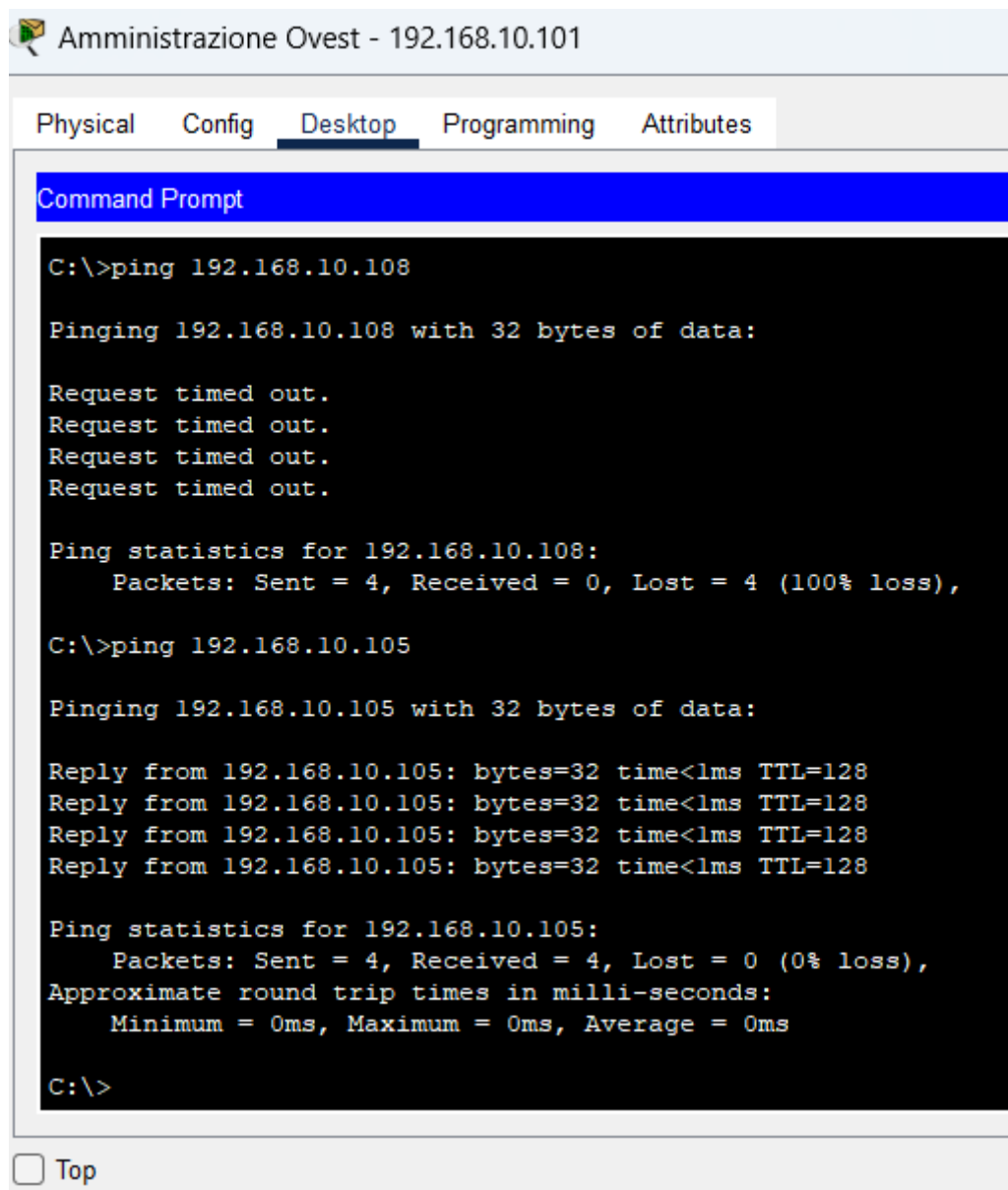


Dopodiché passiamo all'interfaccia di ciascuno switch e configuriamo ogni porta in collegamento con gli host al rispettivo VLAN come porta di accesso, mentre configuriamo la porta collegante gli switch come porta di trunk su tutti i dispositivi.

Alcuni esempi:



A questo punto possiamo verificare che dispositivi su VLAN diverse non comunicano più tra loro. Provando ad eseguire nuovamente un ping da PC Amministrazione Ovest (192.168.10.101) a PC Studenti Est (192.168.10.108) non risulta infatti nessuna comunicazione, mentre eseguire un ping dallo stesso dispositivo (PC Amministrazione Ovest - 192.168.10.101) verso un altro dispositivo sulla stessa VLAN (PC Amministrazione Est - 192.168.10.105) ritorna risultato positivo.



The screenshot shows a web-based network management interface titled "Amministrazione Ovest - 192.168.10.101". It has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows two ping commands being executed from the C:\ prompt. The first command is "ping 192.168.10.108", which results in four "Request timed out." messages and a summary showing 100% loss. The second command is "ping 192.168.10.105", which results in four successful replies with 0% loss and 0ms round trip times. At the bottom of the interface, there is a "Top" link with an unchecked checkbox.

```
C:\>ping 192.168.10.108

Pinging 192.168.10.108 with 32 bytes of data:

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

Ping statistics for 192.168.10.108:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.105

Pinging 192.168.10.105 with 32 bytes of data:

Reply from 192.168.10.105: bytes=32 time<1ms TTL=128
Reply from 192.168.10.105: bytes=32 time<1ms TTL=128
Reply from 192.168.10.105: bytes=32 time<1ms TTL=128
Reply from 192.168.10.105: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

☐ Top

Conclusioni

La suddivisione di una rete in diverse VLAN permette di mettere in comunicazione dispositivi sulla stessa rete virtuale isolandoli da dispositivi posti su reti virtuali diverse senza cambiarne la disposizione fisica. Questo viene fatto configurando gli switch con numeri ed etichette di VLAN, assegnando ad ogni porta del dispositivo in comunicazione con l'host la relativa etichetta in porta di accesso e la porta in comunicazione con altri switch in porta di trunk.