

CREAZIONE RETE SEGMENTATA CON VLAN

Di Tuccio Maicol

INTRODUZIONE

L'obiettivo del laboratorio di oggi è quello di creare un rete segmentata con 4 VLAN differenti.

In Particolare:

- Descrivere la configurazione e settaggi necessari;
- Scegliere una configurazione che metta in risalto l'utilità delle VLAN, usando minimo due switch con almeno la presenza di una VLAN con dispositivi collegati a switch diversi;
- Fare il subnetting della rete, assegnare ogni VLAN ad una rete diversa;
- Fare almeno un test che dimostri il corretto funzionamento del collegamento TRUNK tra switch;
- Spiegazione dei vantaggi e svantaggi delle VLAN;

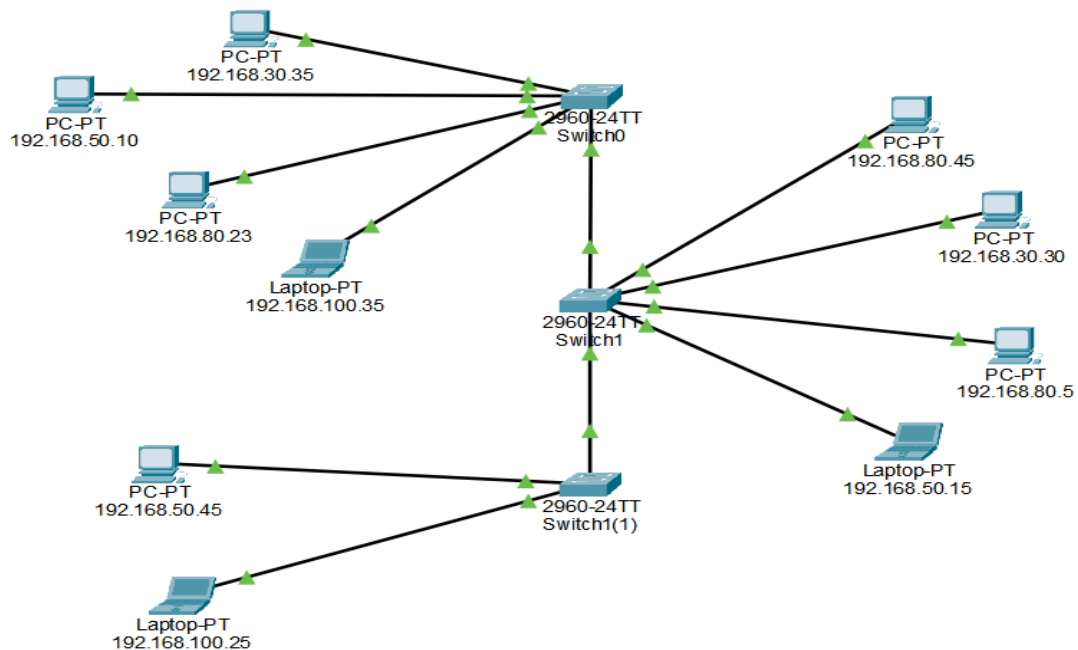
ESECUZIONE

Per realizzare questa rete segmentata con le **VLAN** si è preso come riferimento un'ipotetica rete di tipo aziendale. Lo schema impostato è il seguente:

ID VLAN	Nome VLAN	Rete
30	Logistica	192.168.30.0/24
50	Risorse Umane	192.168.50/24
80	Produzione	192.168.80.0/24
100	Guest	192.168.100.0/24

Per far comunicare tra loro gli addetti ad uno stesso reparto o dipartimento sono state utilizzate le **VLAN**, che permettono di creare delle reti logiche separate indipendentemente dalla posizione fisica che occupano i dispositivi. La comunicazione tra host dello stesso reparto, ovvero appartenenti alla stessa **VLAN** e quindi alla stessa sottorete **IP**, ma connessi a **Switch** diversi è possibile e si realizza tramite la configurazione di un link **Trunk** tra gli **Switch**.

Architettura di rete

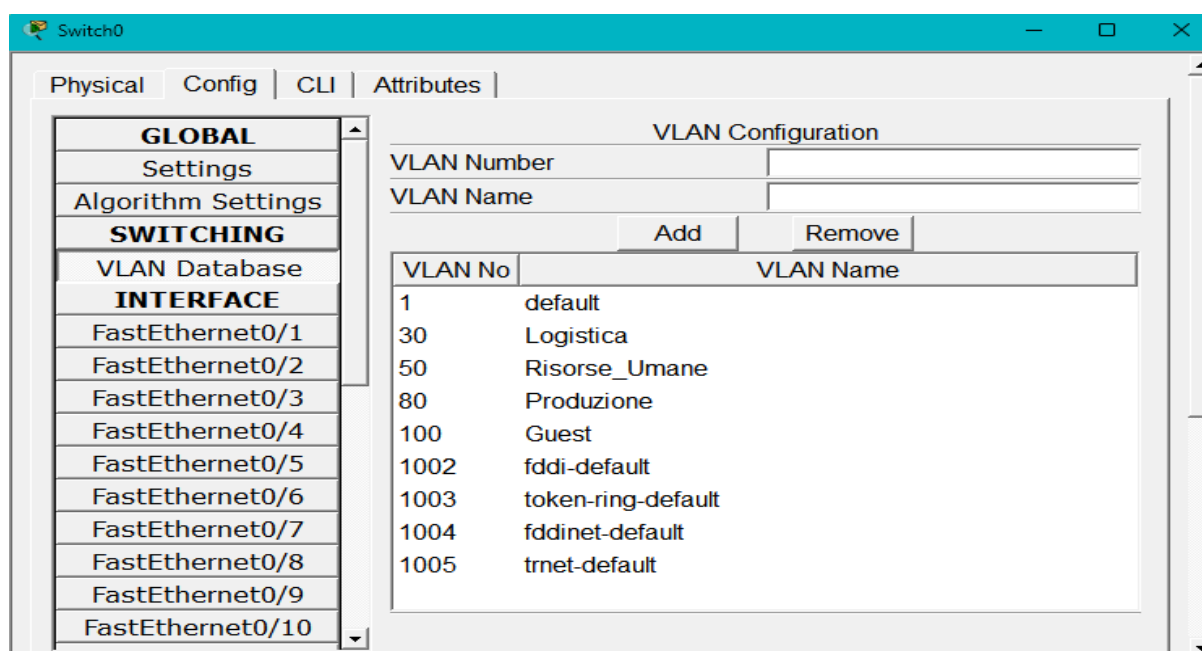


VLAN

VANTAGGI	SVANTAGGI
Maggiore sicurezza: le VLAN riesco ad isolare il traffico tra reparti diversi	Complessità di progettazione, configurazione e risoluzione dei problemi.
Riduzione dominio di broadcast: traffico broadcast non si propaga all'intera rete fisica, ma rimane confinato alla propria VLAN	Richiede la gestione degli Switch
Flessibilità e scalabilità: organizzano logicamente gli utenti indipendentemente dalla loro posizione fisica, possibilità di aggiungere nuove VLAN.	Richiede Trunking fra gli Switch: se non configurati bene le VLAN non comunicano
Evita i "colli di bottiglia"	

Grazie all'utilizzo delle **VLAN**, tutti gli host presenti sulla rete indipendentemente dalla loro posizione fisica hanno la possibilità di poter comunicare con dispositivi appartenenti alla stessa rete.

Creazione e configurazione VLAN negli Switch

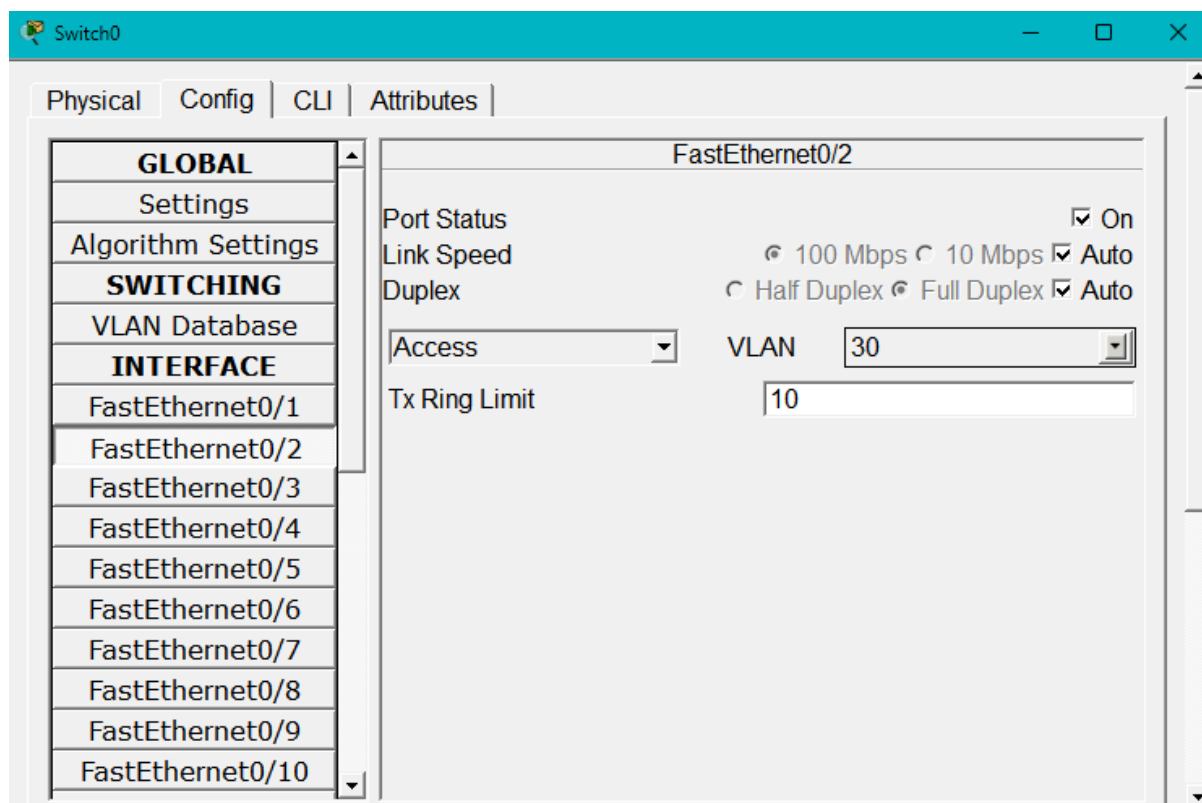


Dopo la creazione delle **VLAN** negli switch si passa all'assegnazione delle porte degli host alla loro specifica **VLAN**.

Per fare ciò si deve:

1. Entrare nella configurazione dello switch;
2. Si seleziona la porta a cui è collegato l'**host**;
3. Si imposta la **VLAN** specifica a cui appartiene l'**host**;

Esempio di assegnazione VLAN

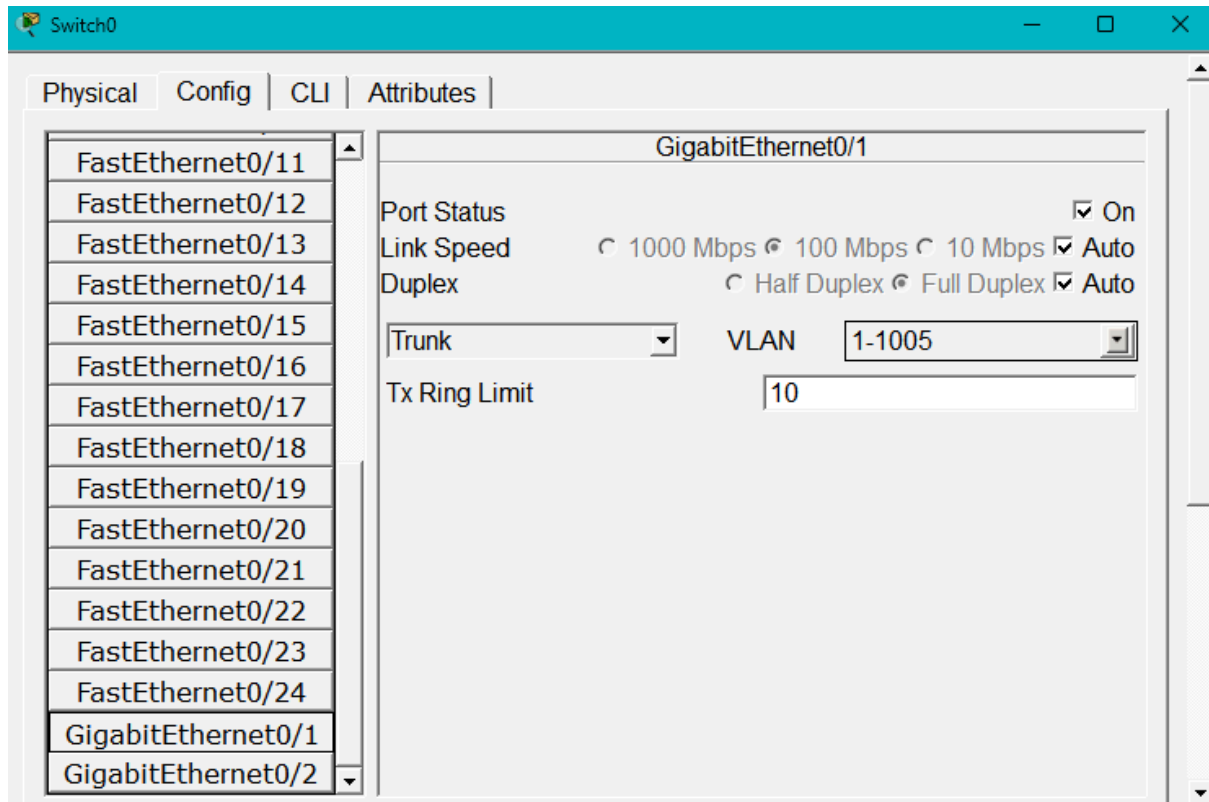


In questo caso specifico si evince che la porta **FastEthernet0/2** è assegnata alla **VLAN 30** (nel nostro caso reparto “**Logistica**”) in modalità **Access**.

Successivamente si passa alla configurazione in **TRUNK** tra gli switch.

Il **Trunk** è una connessione fisica che viene configurata per poter garantire il trasporto del traffico proveniente da più **VLAN** attraverso l'utilizzo di un singolo cavo. La porta utilizzata in questo caso è stata la porta **GigabitEthernet** per i collegamenti fra i vari **Switch**. Utilizzando questo tipo di porte si vanno ad eliminare i cosiddetti “**colli di bottiglia**” che si possono verificare se si utilizzano porte tradizionali **Fast Ethernet**.

Configurazione in Trunk



In questo caso la porta **GigabitEthernet0/1** è stata impostata in modalità trunk. Grazie a questo si ha:

- **Minor rischio di congestione;**
- **Minor latenza;**
- Utilizzare una porta **Gigabit** assicura che questo collegamento abbia la capacità adeguata per evitare che la segmentazione logica e la sicurezza offerta dalle **VLAN** siano vanificate da una **performance limitata** a livello fisico.

TEST DELLA RETE

Per poter testare che tutta la configurazione funzioni si procederà con un ping da un dispositivo connesso al primo **switch** ad un dispositivo connesso al secondo/terzo **Switch** appartenenti però alla stessa **VLAN**.

Nell'esempio riportato in basso abbiamo:

- Il PC con IP **192.168.50.10** (connesso al primo **Switch**, VLAN “ Risorse_Umane”) che esegue un ping verso il PC con IP **192.168.50.45** (connesso al secondo switch, VLAN “ Risorse_Umane “)

The screenshot displays a Cisco Packet Tracer simulation environment. The top window shows a Command Prompt for a PC with IP 192.168.50.10, executing a ping command to 192.168.50.45. The output shows successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 128. The ping statistics indicate 4 packets sent, 4 received, and 0% loss.

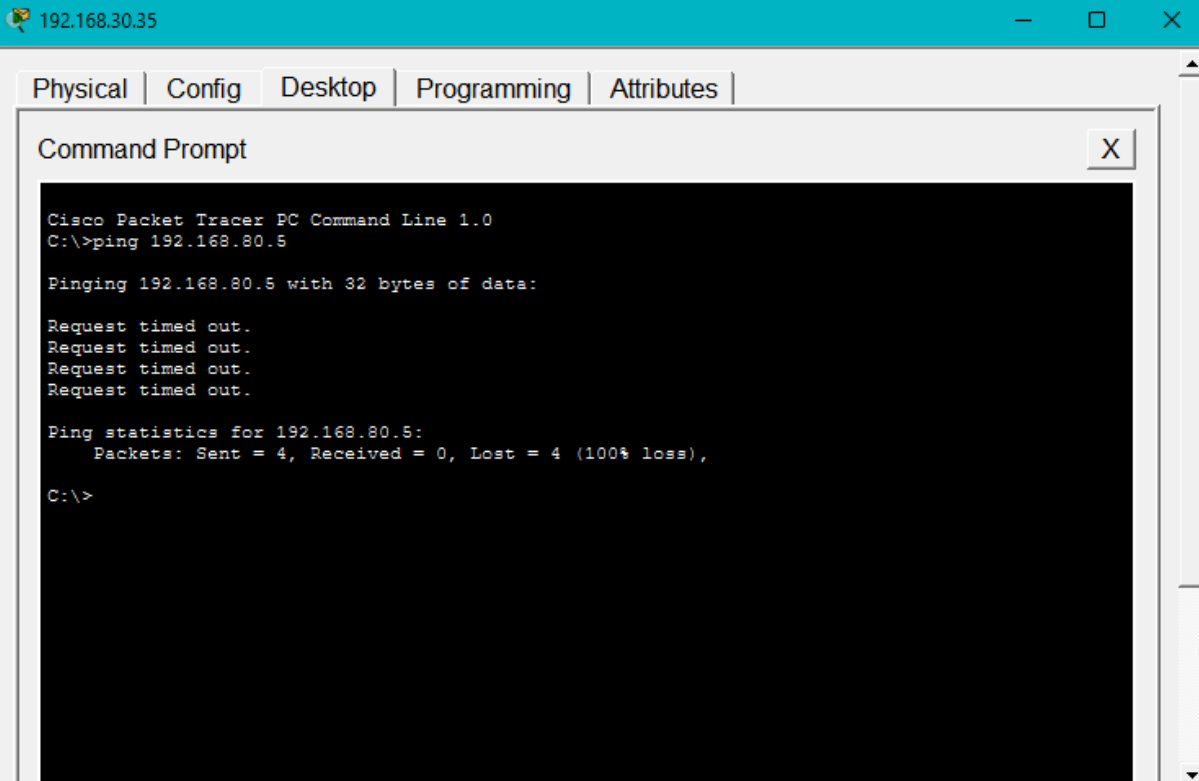
The bottom window shows the network topology. It consists of three switches (Switch0, Switch1, and Switch1(1)) connected in a triangle. Various devices are connected to these switches, including PCs and Laptops. The IP addresses of the devices are listed next to their icons.

The Simulation Panel on the right shows the Event List, which includes ARP and ICMP events. The Play Controls section shows the simulation running at 1.024 seconds.

Vis.	Time(sec)	Last Dev	At D	Type
	0.004	Switch1	S...	ARP
	0.004	Switch...	1...	ARP
	0.005	Switch...	1...	ARP
	0.006	192.16...	S...	ARP
	0.007	Switch...	S...	ARP
	0.008	Switch...	S...	ARP
	0.009	Switch0	1...	ARP
	0.009	-	1...	ICMP
	0.010	192.16...	S...	ICMP
	0.011	Switch0	S...	ICMP
	0.012	Switch1	S...	ICMP
	0.013	Switch...	1...	ICMP
	0.014	192.16...	S...	ICMP
	0.015	Switch...	S...	ICMP
	0.016	Switch1	S...	ICMP
	0.017	Switch0	1...	ICMP
	1.020	-	1...	ICMP
	1.021	192.16...	S...	ICMP
	1.022	Switch0	S...	ICMP
	1.023	Switch1	S...	ICMP
	1.024	Switch...	1...	ICMP

In questo tipo di configurazione quindi un **Pc** appartenente alla **VLAN “Logistica”** non potrà comunicare con un **Pc** di altri dipartimenti.

Esempio di “non” collegamento tra **Pc** con IP **192.168.30.35** (**VLAN “Logistica”**) e **Pc** con IP **192.168.80.5** (**VLAN “Produzione”**).



The screenshot shows a Cisco Packet Tracer PC Command Line window for a PC with IP 192.168.30.35. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Command Prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.80.5

Pinging 192.168.80.5 with 32 bytes of data:

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

Ping statistics for 192.168.80.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```