

# Configurazione e analisi di una rete VLAN aziendale.

## Introduzione:

In questo report descriverò come ho creato, configurato ed implementato una rete di una piccola azienda in un edificio di due piani, con diversi uffici al suo interno.

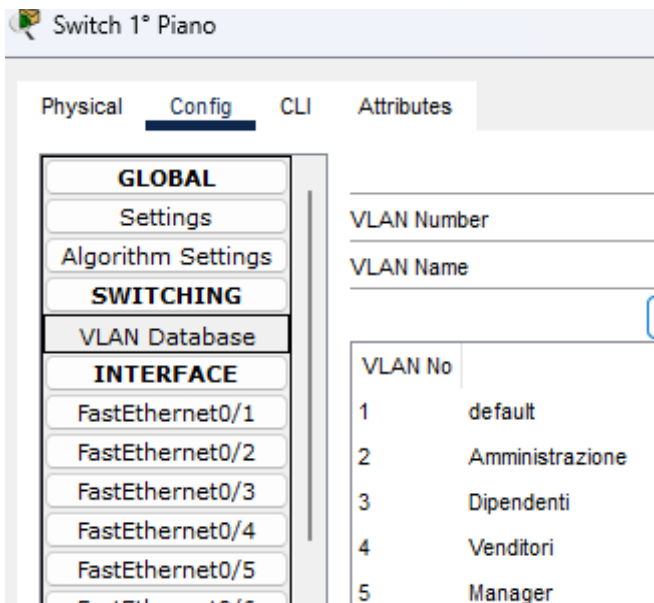
L'idea era quella di creare una rete con due switch interconnessi e suddivisi tramite VLAN per gestire la comunicazione tra diversi **dipartimenti**.

Il mio obiettivo finale per questa rete, era quello di dividere il traffico dei dati e di isolarlo dalle comunicazioni tra i diversi gruppi aziendali, permettendo però, l'invio di dati in modo diretto tra membri dello stesso dipartimento. Ogni VLAN è configurata in modo tale che tutti i dispositivi appartenenti allo stesso gruppo, possano comunicare tra loro anche se collegati a switch diversi.

La suddetta rete prevede:

- Due Switch Comunicanti tra loro (Layer 2)
- Quattro porte VLAN per switch.
- Quattro Host per switch.
- Subnet mask personalizzata.

Per prima cosa ho creato gli Switch, ed ho creato al loro interno, 4 VLAN dedicate ai vari Dipartimenti che fanno parte di questa rete.

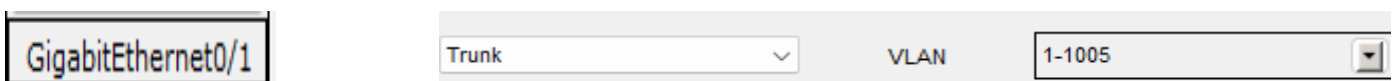


Come si evince dall'immagine a sinistra ho creato le varie categorie per lo switch del primo piano:

- Amministrazione 1 (FastEthernet/02)
- Dipendenti 1 (FastEthernet/03)
- Venditori 1 (FastEthernet/04)
- Manager (FastEthernet/05)

Per comodità ho lasciato la FastEthernet/01 in default in modo tale che seguisse il numero specifico del VLAN Number&Name che ho personalizzato alla porta corrispondente al numero che vi ho assegnato es: Amministrazione 2 – FastEthernet/2 (datosi che il Default non è modificabile), Dipendente 1 – FastEthernet/3 e così via dicendo.

A questo punto ho modificato la porta GigabitEthernet/01, dove andremo a connettervi il secondo switch, abilitando la modalità **Trunk** per consentire la comunicazione tra VLAN che si trovano su switch diversi (vedi sotto).



Una volta impostato lo Switch del 1° Piano, ho fatto la stessa identica cosa, con quello del secondo, facendo attenzione ai dettagli della configurazione fatta precedentemente e ripetendoli garantendo il corretto flusso di traffico di rete.

A questo punto, ho creato i vari Host che andranno a connettersi ai nostri Switch, dando loro IP tutti diversi e una Subnet Mask unica – 255.255.254.0.

Questo perché anche se l'azienda è piccola, è destinata a crescere in modo medio-moderato intensificando gli host connessi con la probabilità di raddoppiare il numero dei dispositivi.

Rimane comunque facile la gestione con 510 Host disponibili, da un IP base 192.169.0.1 a un massimo di 192.168.1.254, utili se ci sono più uffici e reparti in espansione nell'azienda.

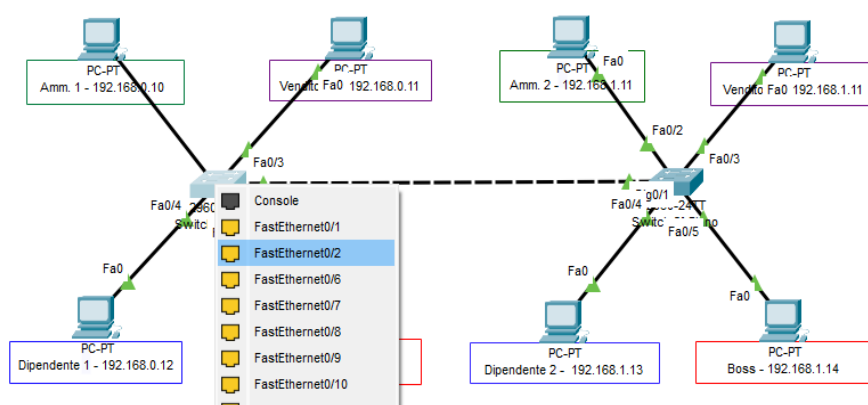
Questa Scelta l'ho fatta anche in termini di sicurezza, ovvero se dovessero esserci dispositivi infetti che riceve un malware in grado di propagarsi attraverso la rete, resta circoscritto in un unico dipartimento, evitando ulteriori danni alla rete nonché all'azienda. Altro vantaggio di questa scelta è la riduzione del traffico (Broadcast Domain) dandosi che il broadcast può rallentare tutto, separare le reti aiuta sicuramente a evitare rallentamenti o congestioni di rete.

Tornando alla configurazione, di seguito i vari IP scelti per i dipartimenti:

- Amministrazione 1 – IP: 192.168.0.10
- Amministrazione 2 – IP: 192.168.1.11
- Venditori 1 – IP 192.168.0.11
- Venditori 2 – IP 192.168.1.12
- Dipendente 1 – IP 192.168.0.12
- Dipendente 2 – IP 192.168.1.13
- Manager 1 – IP 192.168.0.13
- Boss – IP 192.168.1.14

Una volta impostati i vari IP e Subnet mask, non ci resta che fare i vari collegamenti via cavo.

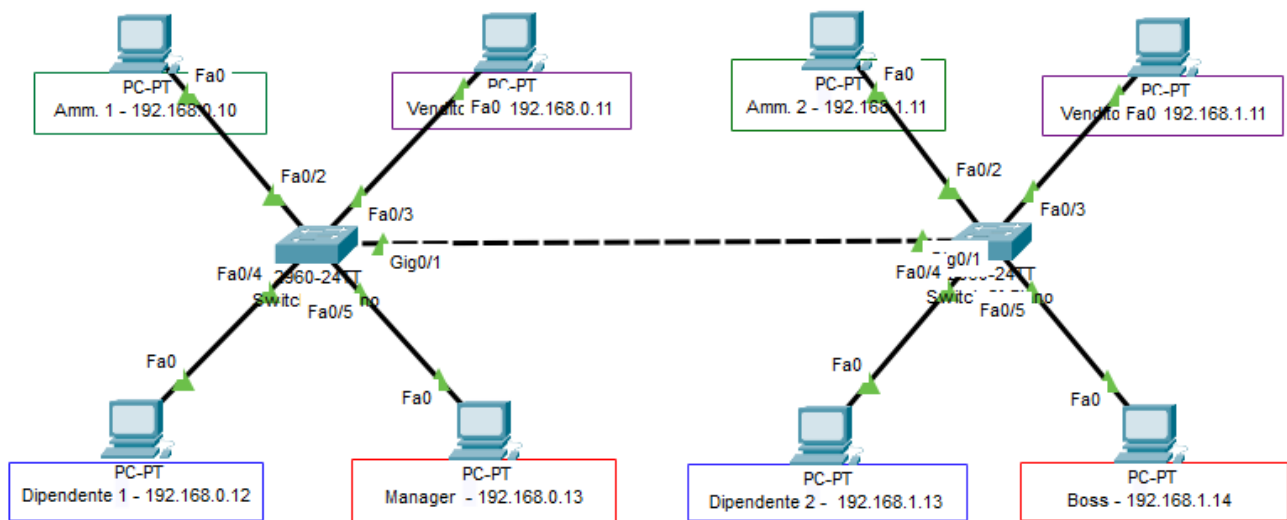
In questo passaggio ho fatto particolare attenzione a collegare ogni host, via cavo nella sua porta VLAN dedicata.



- Amministrazione 1 in FastEthernet/2
- Venditori 1 in FastEthernet/3
- Dipendenti 1 in FastEthernet/4
- Manager in FastEthernet/5.

A questo punto ho svolto la stessa identica azione per lo Switch del secondo piano. Facendo sempre attenzione ad inserire gli stessi identici parametri.

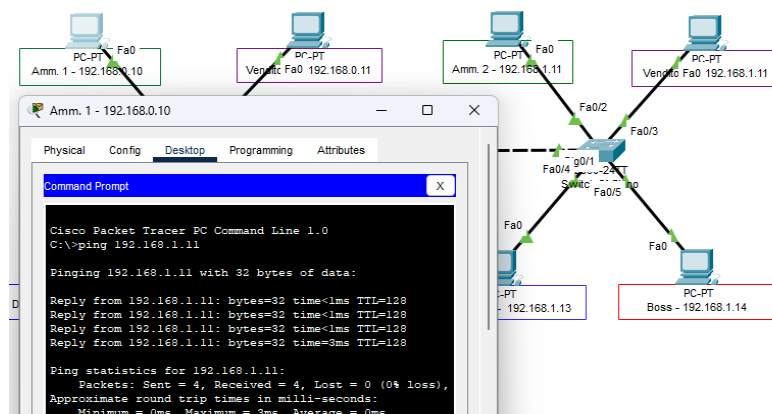
La rete al momento si presenta così:



Arrivati a questo punto non ci resta che verificare se effettivamente i nostri collegamenti siano tutti funzionanti.

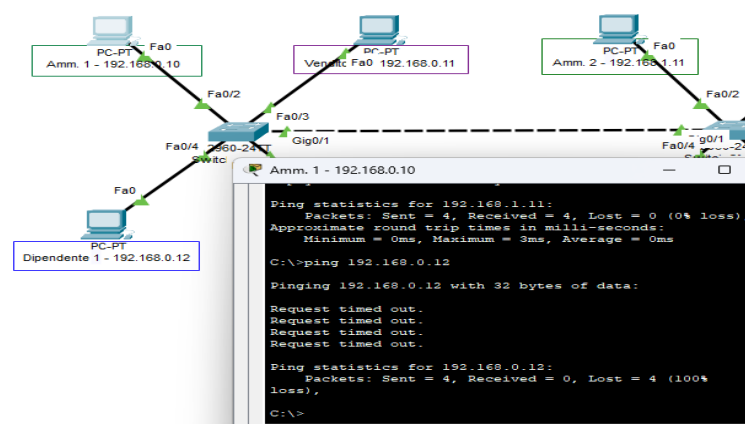
1. Cominciano innanzitutto con il ping Test dalla dashboard GUI di ogni Host.

Partendo appunto da Amministrazione 1.



Come possiamo denotare dal Reply, Amministrazione 1 è perfettamente comunicante con Amministrazione 2.

2. Proviamo in questo caso, sempre per verificare le connessioni, se Amministrazione 1 può comunicare col Dipendente 1 che fa parte della stessa rete e condividono lo stesso switch:



Amministrazione 1, da screen a sinistra, non riesce a comunicare con Dipendente 1, che fa parte della stessa rete e condividono lo stesso switch.

Questo perché i collegamenti stanno eseguendo le istruzioni date, tramite i comandi inseriti per la suddivisione delle VLAN.

3. A questo punto non ci resta che fare l'ultimo test inviando un ping via simple PDU:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Amm. 1 - 192.168.0.10	ICMP
	0.000	--	Amm. 1 - 192.168.0.10	ARP
	0.001	Amm. 1 - 192.168.0.10	Switch 1° Piano	ARP
	0.002	Switch 1° Piano	Switch 2° Piano	ARP
	0.003	Switch 2° Piano	Amm. 2 - 192.168.1.11	ARP
	0.004	Amm. 2 - 192.168.1.11	Switch 2° Piano	ARP
	0.005	Switch 2° Piano	Switch 1° Piano	ARP
	0.006	Switch 1° Piano	Amm. 1 - 192.168.0.10	ARP
	0.006	--	Amm. 1 - 192.168.0.10	ICMP
	0.007	Amm. 1 - 192.168.0.10	Switch 1° Piano	ICMP
	0.008	Switch 1° Piano	Switch 2° Piano	ICMP
	0.009	Switch 2° Piano	Amm. 2 - 192.168.1.11	ICMP
	0.010	Amm. 2 - 192.168.1.11	Switch 2° Piano	ICMP
	0.011	Switch 2° Piano	Switch 1° Piano	ICMP
	0.012	Switch 1° Piano	Amm. 1 - 192.168.0.10	ICMP

Da qui capiamo che giro ha fatto il nostro pacchetto e che Amministrazione 1 comunica in modo corretto con Amministrazione 2 al 2° piano.

4. Proviamo al contrario a fare un test simple PDU tra Venditori 1 e Dipendente 2:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Venditori 1 - 192.168.0.11	ICMP
	0.000	--	Venditori 1 - 192.168.0.11	ARP
	0.001	Venditori 1 - 192.168.0.11	Switch 1° Piano	ARP
	0.002	Switch 1° Piano	Switch 2° Piano	ARP
	0.003	Switch 2° Piano	Venditori 2 - 192.168.1.11	ARP
	0.008	--	Switch 2° Piano	STP
	0.009	Switch 2° Piano	Switch 1° Piano	STP
	0.009	Switch 2° Piano	Dipendente 2 - 192.168.1.13	STP
	0.010	Switch 1° Piano	Dipendente 1 - 192.168.0.12	STP
	0.027	--	Switch 2° Piano	STP
	0.028	Switch 2° Piano	Switch 1° Piano	STP
	0.028	Switch 2° Piano	Boss - 192.168.1.14	STP
	0.029	Switch 1° Piano	Manager - 192.168.0.13	STP

In questo caso vediamo che Venditori 1 cerca di mandare il pacchetto con le istruzioni date, ma all'infinito, e non riesce nello svolgere il comando.

Entrambi i test sono stati svolti su tutti i dispositivi connessi ai due switch e nessun dispositivo ha riportato errori.

## Conclusioni:

La configurazione scelta, permette un'ottima separazione dei dipartimenti aziendali, garantendo **Sicurezza** per via della suddivisione e dell'isolamento di quest'ultimi, gli uni dagli altri, e una buona organizzazione della gestione di rete.

L'uso delle VLAN riduce sicuramente il traffico di rete e gestisce meglio tutte le risorse disponibili. Questa topologia di rete potrebbe essere migliorata ulteriormente con l'aggiunta di un Router per consentire migliore comunicazione tra VLAN diverse.