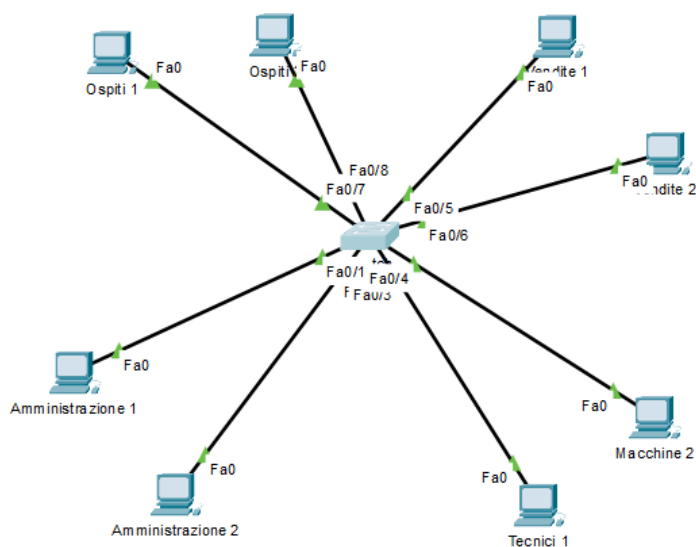


CREAZIONE DI UNA RETE SEGMENTATA CON 4 VLAN DIVERSE



Nella vita di tutti i giorni, sia essa a casa o nella propria azienda, può presentarsi la necessità di avere più reti distinte, per ridurre il traffico e aumentare la sicurezza, ma senza avere troppi dispositivi dedicati.

Per fare ciò si possono intraprendere 2 strade, che sono:

- utilizzo di Sottoreti;
- utilizzo di VLAN;

Entrambi i casi possono essere classificati come Reti di Livello 2 del modello **ISO-OSI** (Open Systems Interconnection). Il Modello ISO-OSI è uno schema di riferimento che descrive come i dati viaggiano in una rete. Il Livello 2 è chiamato Livello di Collegamento Dati (*Data Link Layer*). Questo livello si occupa di trasferire i dati tra dispositivi collegati alla stessa rete locale (LAN).

La creazione di **Sottoreti** (anche detta **Subnetting**) serve a suddividere una rete più grande in due o più reti più piccole. Questo è utile per organizzare, ottimizzare e proteggere il traffico di rete in un'azienda.

Con la suddivisione di una rete in 4 sottoreti però viene limitato il numero dei dispositivi collegabili ad esso. Prendendo ad esempio una rete domestica o di una piccola impresa darà la possibilità di collegare 64 dispositivi rispetto ai 256 della rete originale. Inoltre le sottoreti richiedono una maggiore competenza informatica e un maggior tempo per la configurazione e la gestione.

L'alternativa al subnetting è la creazione di **VLAN (Virtual Local Area Network)** per separare i dispositivi in gruppi distinti, anche se tutti sono collegati allo stesso **switch**.

Si deve considerare ogni VLAN è come una rete separata dalle altre, infatti i computer collegati ad una VLAN non possono comunicare con quelli di un'altra VLAN.

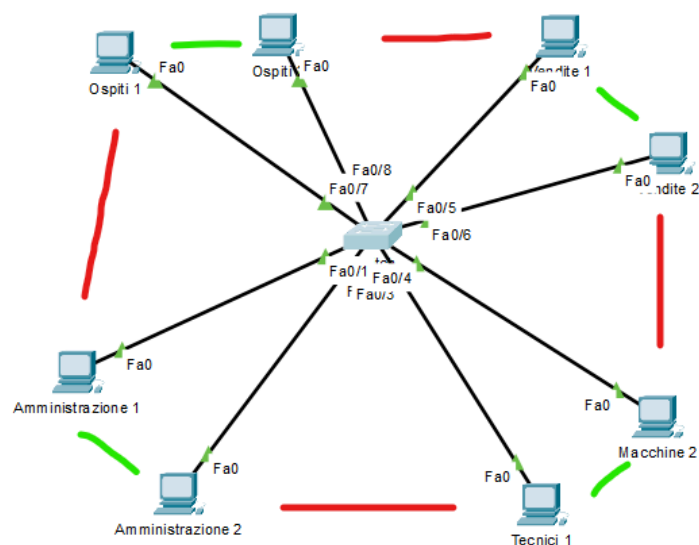
Con una **VLAN**, i dispositivi sono fisicamente separati a livello di switch, impedendo accessi non autorizzati. Le VLAN riducono il traffico **broadcast** (un tipo di comunicazione in cui un messaggio viene inviato a tutti i dispositivi all'interno di una rete) perché ognuna di esse è "isolata", mentre con solo le sottoreti, il traffico potrebbe diffondersi in tutta la rete andandola a rallentare.

Con le VLAN si possono separare dispositivi senza cambiare i cavi, mentre con le sottoreti, si deve riorganizzare fisicamente la rete e cambiare configurazioni IP.

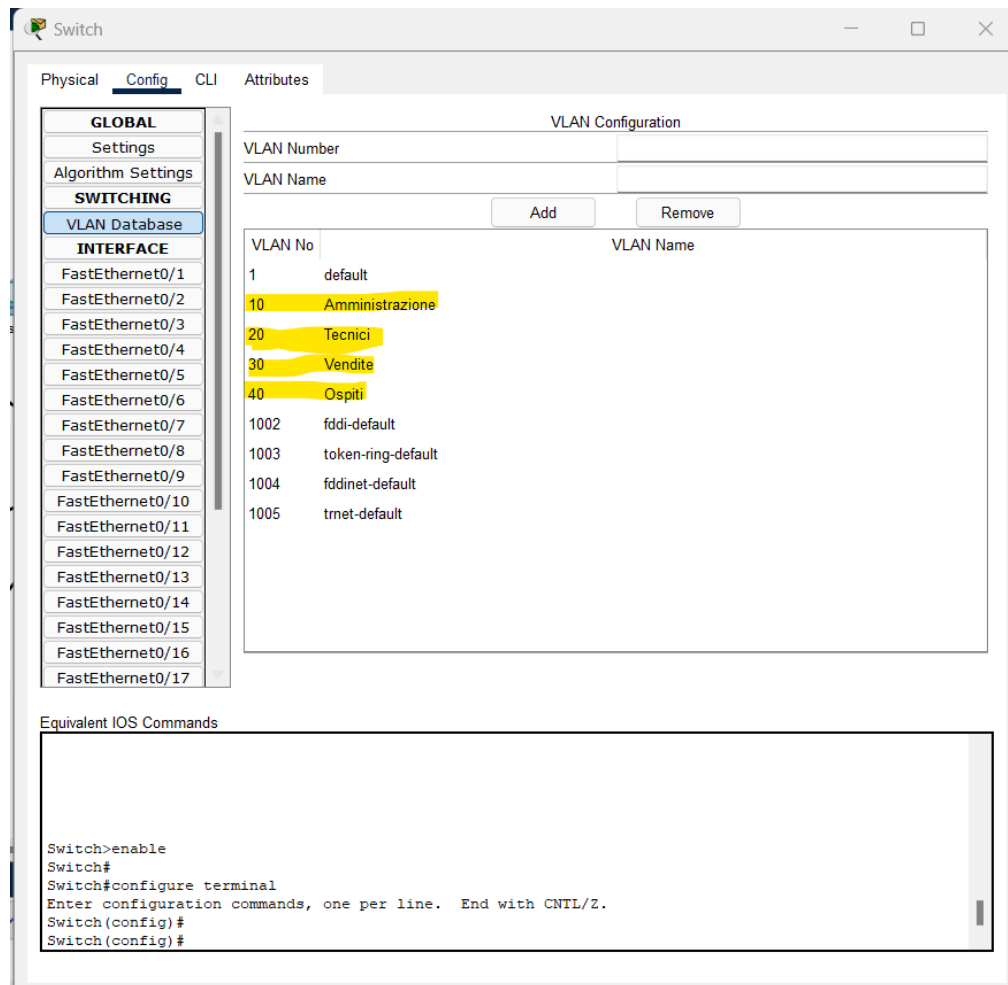
Come abbiamo già detto la creazione di 4 VLAN distinte può essere effettuato con un solo switch e con pochi passaggi.

Ma come si può fare?

Riprendendo l'immagine di apertura, si immagini un'Azienda con quattro diversi reparti a cui sono stati assegnati 2 PC ciascuno. Ovviamente ogni reparto non ha la necessità di comunicare con un altro, però i dispositivi di un determinato reparto devono comunicare tra loro. Quindi il PC denominato "Ospiti 1" dovrà comunicare col PC "Ospiti 2" ma non con il PC "Vendite 1" e gli altri.



Per creare 4 VLAN differenti ed indipendenti tra loro bisogna accedere alle impostazioni dello switch e creare una VLAN per ogni reparto, assegnando un numero ed un nome



Dopo di che, bisogna configurare ogni porta dello switch in modalità **Access** e assegnarla a una VLAN. In questo caso si dovranno configurare 4 porte

Switch

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

SWITCHING

- VLAN Database

INTERFACE

- FastEthernet0/1**
- FastEthernet0/2
- FastEthernet0/3
- FastEthernet0/4
- FastEthernet0/5
- FastEthernet0/6
- FastEthernet0/7
- FastEthernet0/8
- FastEthernet0/9
- FastEthernet0/10
- FastEthernet0/11
- FastEthernet0/12
- FastEthernet0/13
- FastEthernet0/14
- FastEthernet0/15
- FastEthernet0/16
- FastEthernet0/17

FastEthernet0/1

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

Access VLAN 10

Tx Ring Limit 10

Equivalent IOS Commands

```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
```

☐ Top

Ora bisogna configurare gli 8 PC. Per fare ciò si deve accedere alle impostazioni di rete del PC ed impostare un **indirizzo IP statico** appartenente alla sottorete corretta, per esempio per i PC dell'Amministrazione è stata creata la VLAN 10, si dovrà perciò inserire l'IP 192.168.10.x, dove la terza cifra (in gergo informatico ottetto) identifica la rete a cui collegarsi; si avrà perciò una situazione come riportata nello schema:

PC	IP
Amministrazione 1	192.168.10.2
Amministrazione 2	192.168.10.3
Tecnici 1	192.168.20.2
Tecnici 2	192.168.20.3
Vendite 1	192.168.30.2
Vendite 2	192.168.30.3
Ospiti 1	192.168.40.2
Ospiti 2	192.168.40.3

Durante la configurazione noteremo che il **subnet mask** prende in automatico l'indirizzo **255.255.255.0**. Tale indirizzo è standard per le reti di **Classe C**, che sono comunemente usate nelle reti aziendali e domestiche. Questo permette di avere all'interno della rete **256 indirizzi IP totali**, di cui **254 utilizzabili** per dispositivi (escludendo l'indirizzo di rete 192.168.x.0 e il broadcast 192.168.x.255).

Amministratore 1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.10.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::250:FFF:FE9D:731A

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

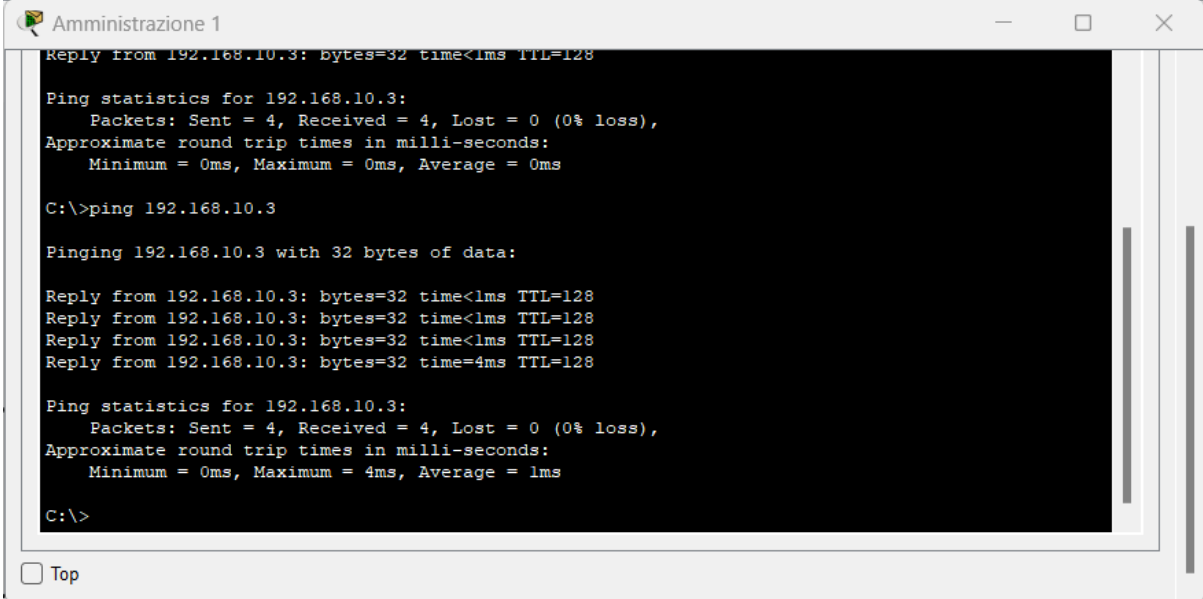
Authentication: MD5

Username:

Password:

☐ Top

Configurati i PC, si può procedere al test tramite il prompt dei comandi utilizzando il comando *ping*. Dal PC Amministrazione 1 cercheremo di contattare il PC Amministrazione 2 (indirizzo IP 192.168.10.3), appartenenti alla VLAN 10 e ci dovrà essere un invio e ricezione dei dati



```
Amministrazione 1
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

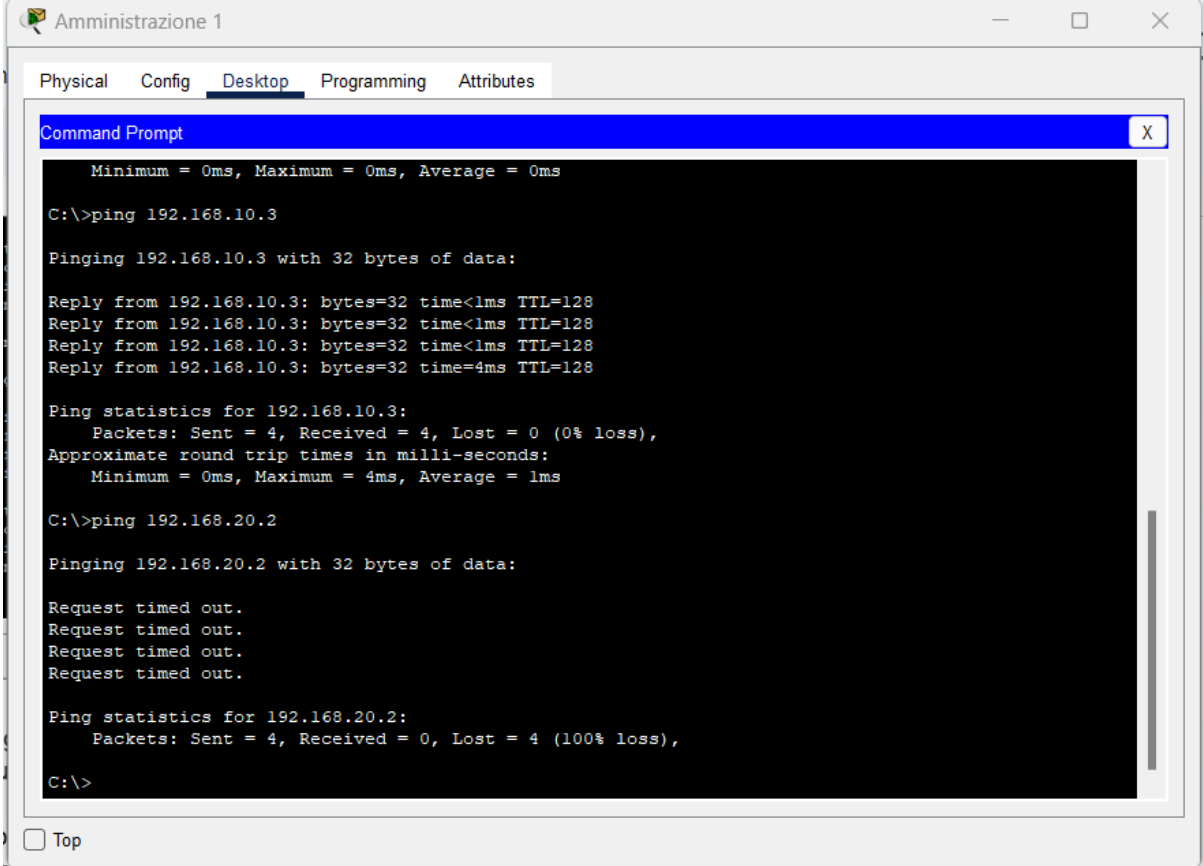
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Se si legge attentamente si noterà che sono stati inviati 4 pacchetti (Sent = 4) e l'altro PC li ha ricevuti tutti (Received = 4)

Andando invece a contattare il PC Tecnici 1 (a cui è stato assegnato l'IP 192.168.20.2) non dovranno essere recapitati pacchetti



```
Amministrazione 1
Physical Config Desktop Programming Attributes

Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

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

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Si noterà che sono stati inviati 4 pacchetti (Sent = 4), non ne è stato ricevuto nessuno (Received = 0) perchè sono tutti andati persi (Lost = 4).

Ciò vuol dire che la VLAN 10 dedicata all'Amministrazione non può contattare ne essere contattata dalle altre VLAN.

Concludendo le VLAN permettono di dividere una rete fisica in più reti virtuali, offrendo diversi vantaggi, tra cui una maggiore sicurezza (i dispositivi di una VLAN non possono comunicare con quelli di un'altra, proteggendo così dati sensibili), si avrà meno traffico di rete e migliori prestazioni riducendo il numero di messaggi broadcast che rallentano la rete ed evitando congestioni e migliora la velocità di comunicazione, si avrà una maggiore flessibilità e gestione semplificata, ed una ottimizzazione della rete aziendale creando reti su misura per ogni settore dell'azienda.