

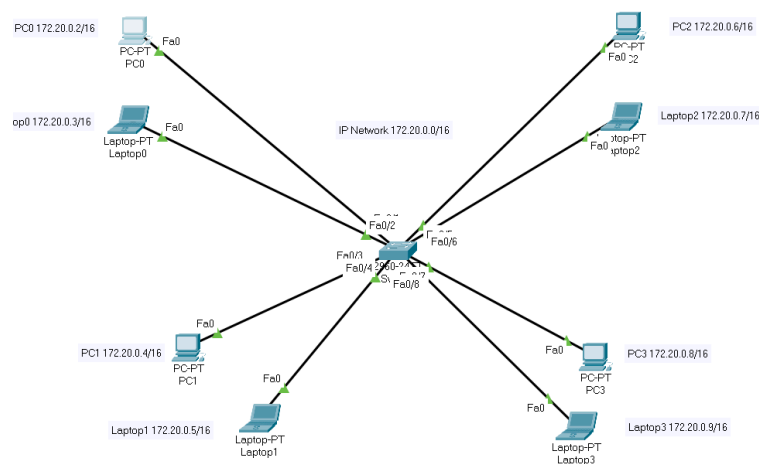
PROGETTO S1-E5: RETI VLAN

Testo dell'esercizio: realizzazione di una rete segmentata con 4 VLAN diverse.

Per lo svolgimento di questo esercizio, prima di ogni cosa ho utilizzato il software Cisco Packet Tracer per realizzare una rete composta da:

- 1 Switch
- 8 Host

Di seguito l'immagine di come apparirà la rete:



Ho scelto, in maniera casuale, un IP network tra quelli privati: 172.20.0.0/16.

Ho configurato i vari dispositivi assegnando un IP per ciascuno e verificato che, appartenendo alla stessa rete, tra di loro comunicassero correttamente. Qui di seguito un' immagine del ping effettuato tra i dispositivi PC0 e Laptop3:

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.20.0.9

Pinging 172.20.0.9 with 32 bytes of data:

Reply from 172.20.0.9: bytes=32 time<1ms TTL=128
Reply from 172.20.0.9: bytes=32 time<1ms TTL=128
Reply from 172.20.0.9: bytes=32 time<1ms TTL=128
Reply from 172.20.0.9: bytes=32 time<1ms TTL=128

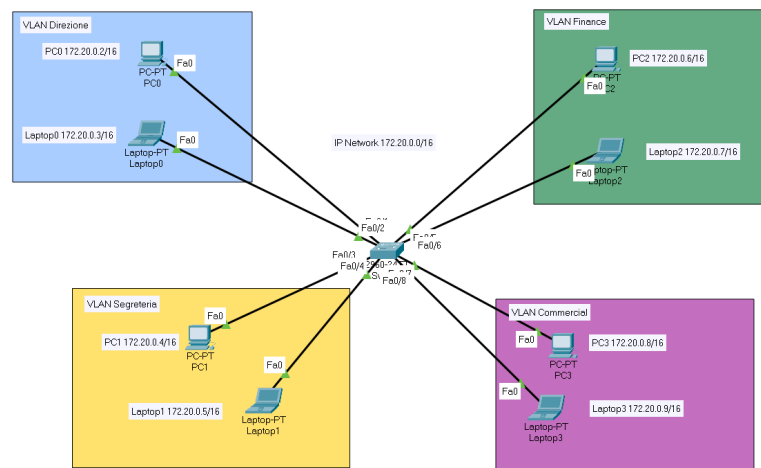
Ping statistics for 172.20.0.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Una volta realizzata la rete e verificato il corretto funzionamento, ho suddiviso la rete in 4 diverse VLAN, configurando lo Switch e le porte che lo collegano ad ogni Host:

- VLAN Direzione: PC0, Laptop0;
- VLAN Segreteria: PC1, Laptop1;
- VLAN Finance: PC2, Laptop2;
- VLAN Commercial: PC3, Laptop3.

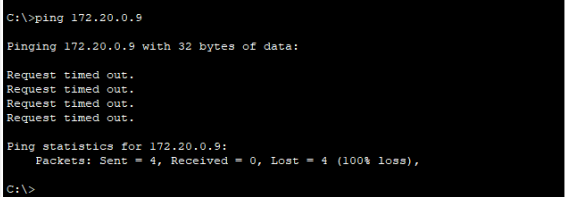
Nell'immagine seguente andremo a vedere la loro suddivisione a livello grafico, rappresentata da riquadri con colori diversi per ciascuna VLAN:



Una volta segmentata la rete grazie alla realizzazione delle VLAN, andremo ad effettuare il ping tra due dispositivi appartenenti alla stessa VLAN, qui di seguito avremo il ping effettuato tra PC0 e Laptop 0, appartenenti alla VLAN Direzione, il risultato sarà che comunicano correttamente:

```
Ping statistics for 172.20.0.9:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 172.20.0.3  
  
Pinging 172.20.0.3 with 32 bytes of data:  
  
Reply from 172.20.0.3: bytes=32 time<1ms TTL=128  
Reply from 172.20.0.3: bytes=32 time<1ms TTL=128  
Reply from 172.20.0.3: bytes=32 time<1ms TTL=128  
Reply from 172.20.0.3: bytes=32 time<1ms TTL=128  
  
Ping statistics for 172.20.0.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>
```

La seconda verifica che andremo a fare sarà il ping tra due dispositivi appartenenti a VLAN differenti, nello specifico PC0, appartenente alla VLAN Direzione, e Laptop3, appartenente alla VLAN Commercial, se la configurazione è avvenuta correttamente, i dispositivi non potranno comunicare, come vedremo nella prossima immagine:



```
C:\>ping 172.20.0.9

Pinging 172.20.0.9 with 32 bytes of data:

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

Ping statistics for 172.20.0.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

Le VLAN sono delle reti virtuali, vengono utilizzate per segmentare una rete unica in più parti allo scopo di renderla più sicura da eventuali attacchi esterni.

Il concetto di base è simile a quello del Subnetting, il quale è nato negli anni '80 per colmare la carenza di indirizzi IP disponibili, la differenza delle VLAN con quest'ultimo è che le VLAN sono state create con l'esatto scopo di segmentare le reti senza crearne di nuove, e rendere la rete più sicura da attacchi informatici.

Analogamente al Subnetting, le VLAN non possono comunicare tra di loro, come se appartenessero a reti differenti, a meno che non si utilizzi un Router Gateway correttamente configurato o uno Switch Layer 3, i quali consentono il trasferimento di pacchetti di dati (vedi modello ISO/OSI) senza invalidare la segmentazione della rete.