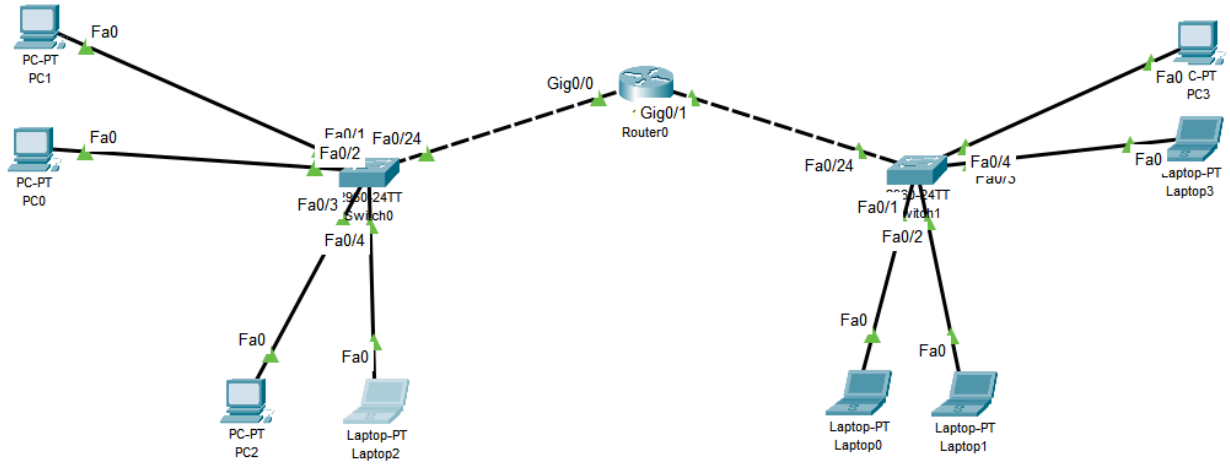
Consegna Progetto S1 L5

Richiesta

L'esercizio di oggi riguarderà la creazione di una rete segmentata con 4 VLAN diverse. Oltre agli screenshot del progetto, spiegherete le motivazioni per cui si è scelto di ricorrere alle VLAN.

Consegna

Iniziamo il nostro progetto creando il setup su Cisco Packet Tracer



La rete di partenza è 192.168.1.0/24. Ho deciso poi di suddividerla in 4 sottoreti con una subnet mask /26. quindi ogni sottorete avrà 62 indirizzi disponibili per i dispositivi.
(Ci tengo a precisare che ho effettuato la divisione in sottoreti nonostante non fosse necessario come esercitazione e in quanto si trattava di pochi dispositivi)

le sottoreti che andremo ad ottenere saranno divise nel seguente modo:

VLAN10 (192.168.1.0/26) con indirizzi che andranno da 192.168.1.1 a 192.168.1.62
VLAN20 (192.168.1.64/26) con indirizzi che andranno da 192.168.1.65 a 192.168.1.126
VLAN30 (192.168.1.128/26) con indirizzi che andranno da 192.168.1.129 a 192.168.1.190
VLAN40 (192.168.1.192/26) con indirizzi che andranno da 192.168.1.193 a 192.168.1.254

Ogni sottorete ha un Gateway, ma visto che per ora non abiliteremo il routing tra VLAN, i dispositivi non potranno comunicare tra di loro attraverso il router.

Il prossimo passo sarà configurare delle vlan sugli switch, nel nostro caso andremo a creare due VLAN sullo switch1 (VLAN 10, VLAN 20) e assegneremo le porte 1 e 2 per la VLAN 10 mentre le porte 3 e 4 saranno assegnate alla VLAN 20.

Per procedere abbiamo due possibilità o cliccando sullo switch selezionando config e impostandolo con i pulsanti predisposti oppure possiamo andare a scrive nella CLI.

```
Switch#
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name "VLAN10"
Switch(config-vlan)#exit
Switch(config)# vlan 20
Switch(config-vlan)#name "VLAN20"
Switch(config-vlan)#exit
Switch(config)#
```

Lo stesso procedimento verrà applicato sullo switch2 per le VLAN 30 e VLAN 40 assegnando le porte 1 e 2 a VLAN 30 e le porte 3 e 4 a VLAN 40.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 30
Switch(config-vlan)#name "VLAN30"
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name "VLAN40"
Switch(config-vlan)#exit
Switch(config)#
```

Dopo la creazione delle VLAN non ci resta che assegnare le porte alle VLAN 10 e 20 su Switch1.

```
Switch(config)#interface range fa0/1 - fa0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/3 - fa0/4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#
```

e le porte alle VLAN 30 e 40 su Switch2:

```
Switch(config)#interface range fa0/1 - fa0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fa0/3 - fa0/4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#
```

Per collegare gli switch al router configuriamo una connessione trunk sulla porta fa0/24 di entrambi gli switch tramite i comandi:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Andremo a configurare i computer nel seguente modo:

VLAN10-SWITCH1:

PC1

IP: 192.168.1.2

Subnet Mask: 255.255.255.192

Gateway: 192.168.1.1

PC2

IP: 192.168.1.3

VLAN20-SWITCH1:

PC3

IP: 192.168.1.66

Subnet Mask: 255.255.255.192

Gateway: 192.168.1.65

PC4

IP: 192.168.1.67

VLAN30-SWITCH2:

PC5

IP: 192.168.1.130

Subnet Mask: 255.255.255.192

Gateway: 192.168.1.129

PC6

IP: 192.168.1.131

VLAN40-SWITCH2:

PC7

IP: 192.168.1.194

Subnet Mask: 255.255.255.192

Gateway: 192.168.1.193

PC8

IP: 192.168.1.195

Andiamo a testare il corretto funzionamento della connessione tra i dispositivi nella rete.

La prima prova che andremo a fare è da un pc verso un altro pc nella stessa VLAN.

```
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Come possiamo osservare eseguendo un ping dal PC1 verso il PC2 all'interno della VLAN10, i pacchetti giungono a destinazione.

La seconda prova viene eseguita tra il PC1 e il PC3 (situato nella VLAN20 e collegato allo stesso switch)

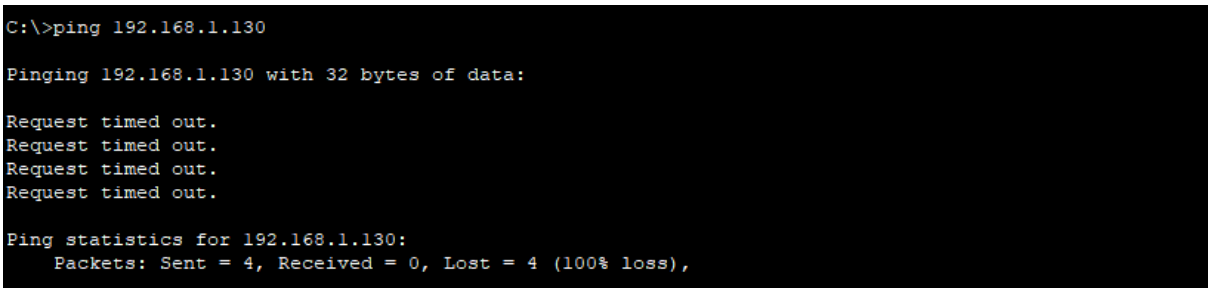
```
Pinging 192.168.1.66 with 32 bytes of data:

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

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Come ci aspettavamo i pacchetti vengono droppati in quanto non giungono a destinazione.

La terza ed ultima prova che andremo a fare è tra il PC1 e il PC5 (situato nella VLAN30 collegato allo switch2)



Anche in questo caso i pacchetti vengono droppati confermando la corretta impostazione delle VLAN le quali permettono il traffico tra dispositivi collegati al medesimo switch.

Si è deciso di utilizzare le VLAN in quanto, immaginando uno scenario reale in una rete aziendale, questa soluzione offre numerosi vantaggi. Prima di tutto, consente una maggiore sicurezza e una gestione ottimizzata del traffico. Segmentando e isolando il traffico, infatti, si migliora sia l'efficienza che la sicurezza della rete. Inoltre, le VLAN offrono flessibilità, permettendo di espandere o modificare la rete senza dover intervenire sulla struttura fisica. Ad esempio, è possibile aggiungere nuovi dispositivi a una VLAN senza alterare il cablaggio o l'infrastruttura esistente. Un altro vantaggio significativo delle VLAN è la possibilità di segmentare la rete per gruppi di lavoro aziendali. Si può, ad esempio, separare il reparto vendite dalle risorse umane, facilitando la gestione e la sicurezza. Infine, le VLAN permettono che, in caso di guasti o malfunzionamenti, le altre VLAN non vengano influenzate, consentendo una risoluzione dei problemi più rapida e senza compromettere l'intera rete.

Il report sarebbe giunto alla sua conclusione ma ho deciso anche di implementare il routing intra-VLAN, in modo che dispositivi di VLAN diverse possano comunicare tra loro.

Il primo passo è quello di andare ad operare nella CLI del Router, il supporto della VLAN sulla sub-interfaccia va abilitato utilizzando il comando encapsulation dot1Q.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.192
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Questa configurazione andrà ripetuta per le altre VLAN.

Una volta configurate tutte le VLAN andremo a compiere una verifica della corretta configurazione con il comando “show ip interface brief”.

```
enable
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.1.1     YES manual up                    up
GigabitEthernet0/0.20  192.168.1.65    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/1.30  192.168.1.129   YES manual up                    up
GigabitEthernet0/1.40  192.168.1.193   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Come possiamo vedere tutto è settato correttamente, non ci resta che verificare con il ping se PC1 può comunicare con PC8 nela VLAN40 dello switch2.

```
C:\>ping 192.168.1.195

Pinging 192.168.1.195 with 32 bytes of data:

Reply from 192.168.1.195: bytes=32 time<1ms TTL=127
Reply from 192.168.1.195: bytes=32 time<1ms TTL=127
Reply from 192.168.1.195: bytes=32 time<1ms TTL=127
Reply from 192.168.1.195: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In questo caso il pacchetto viene inviato verso il router, il quale lo instrada verso l’ip di destinazione sulla diversa VLAN.

```
C:\>tracert 192.168.1.195

Tracing route to 192.168.1.195 over a maximum of 30 hops:

  1    2 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      192.168.1.195

Trace complete.
```