

PROGETTO S1/L5 – CONFIGURAZIONE DI UNA RETE SEGMENTATA CON VLAN E COLLEGAMENTO TRUNK TRA SWITCH

1. INTRODUZIONE

L'attività svolta ha avuto come obiettivo la progettazione e configurazione, in Cisco Packet Tracer, di una rete locale segmentata mediante **4 VLAN distinte**, utilizzando almeno **due switch** interconnessi tramite **collegamento TRUNK**.

Come richiesto dal testo dell'esercizio, oltre al file di progetto sono stati prodotti uno schema della topologia, una descrizione dettagliata della configurazione, il subnetting applicato e uno o più test che dimostrano il corretto funzionamento delle VLAN e del collegamento trunk tra gli switch.

2. MOTIVAZIONI DELLA SCELTA DELLE VLAN

2.1 SCENARIO LOGICO

Per rendere l'esempio il più realistico possibile, la rete è stata suddivisa in **quattro domini logici**:

- **VLAN 10 – MANAGEMENT**
- **VLAN 20 – SECURITY**
- **VLAN 30 – OPERATIONS**
- **VLAN 40 – SERVICES**

Ogni gruppo ha esigenze diverse in termini di sicurezza e traffico, e la separazione logica tramite VLAN permette di riflettere questa suddivisione sulla rete fisica, pur utilizzando la stessa infrastruttura di switch.

2.2 VANTAGGI DELLE VLAN

L'utilizzo delle VLAN comporta diversi vantaggi tecnici, organizzativi ed economici:

- **Separazione del traffico**
Ogni VLAN isola il proprio broadcast domain, riducendo il traffico inutile e migliorando le prestazioni complessive della rete.
- **Maggiore sicurezza**
Gli host appartenenti a VLAN differenti non possono comunicare direttamente senza routing, limitando l'accesso non autorizzato tra reparti e contenendo la propagazione di eventuali minacce.
- **Flessibilità gestionale**
Permette di raggruppare logicamente utenti e dispositivi anche se distribuiti fisicamente su più piani, edifici o switch diversi, semplificando la gestione dell'infrastruttura.
- **Applicazione centralizzata delle policy**
È possibile applicare QoS, ACL o regole di filtraggio per singola VLAN anziché per singola porta, con una gestione più ordinata, scalabile ed efficiente.
- **Vantaggio economico su hardware e opere di cablaggio**
Le VLAN riducono significativamente i costi sia in fase di progettazione sia in fase di espansione della rete.
Poiché la segmentazione è logica e non fisica, non è necessario installare uno switch per ogni reparto né creare cablaggi separati per ogni gruppo di utenti. Questo comporta:
 - minore acquisto di switch e armadi aggiuntivi;
 - riduzione delle canalizzazioni, delle passerelle e delle opere murarie necessarie per nuovi passaggi cavo;
 - ottimizzazione dei percorsi: un unico link trunk può sostituire più cablaggi dedicati;
 - riduzione della manodopera di posa, installazione e manutenzione.

2.3 SVANTAGGI E CRITICITÀ DELLE VLAN

Nonostante i numerosi benefici, l'uso delle VLAN introduce anche alcuni aspetti critici da considerare in fase di progettazione e gestione:

- **Maggiore complessità di configurazione**

L'infrastruttura richiede una configurazione accurata di VLAN, porte access, trunk e, se necessario, del routing inter-VLAN.

Errori nella coerenza delle configurazioni tra switch possono causare interruzioni o segmentazioni involontarie della rete.

- **Dipendenza dal corretto funzionamento dei trunk**

Il collegamento trunk rappresenta il canale attraverso il quale transitano i frame appartenenti a tutte le VLAN.

VLAN non consentite, tag non riconosciuti o parametri errati possono impedire la comunicazione tra dispositivi che si trovano nella stessa rete logica ma su switch differenti.

- **Possibile collo di bottiglia sul link trunk**

Poiché il trunk trasporta simultaneamente il traffico di tutte le VLAN, esso diventa un punto di aggregazione critico.

In presenza di numerosi host distribuiti su più switch o in caso di elevato volume di traffico, il link può saturarsi, generando:

- congestione e latenza elevata;
- degradazione delle prestazioni per tutte le VLAN;
- potenziali perdite di pacchetti.

Per mitigare questo rischio, nelle reti reali si utilizzano tecniche come EtherChannel (aggregazione di link), trunk su porte ad alta capacità (10G/40G), oppure una distribuzione più equilibrata dei carichi tra diversi uplink.

- **Gestione del traffico inter-VLAN**

Se è necessaria comunicazione tra VLAN diverse, occorre introdurre dispositivi di livello 3 (router o switch Layer 3) e configurare opportunamente le interfacce logiche o le sub-interfacce.

Questo comporta ulteriori costi, complessità e potenziali punti di failure.

3. PROGETTAZIONE DELL'INDIRIZZAMENTO IP (SUBNETTING)

Per garantire l'isolamento anche a livello IP, a ciascuna VLAN è stata assegnata una **sottorete dedicata**. Lo schema utilizzato è il seguente:

VLAN 10 – MANAGEMENT

Rete: **192.168.10.0/24**

Gateway di riferimento: **192.168.10.1**

Host: **192.168.10.10 (PC0), 192.168.10.11 (PC1), 192.168.10.20 (PC8), 192.168.10.21 (PC9)**

Questa VLAN ospita dispositivi di gestione, amministrazione o controllo, che richiedono un dominio isolato e protetto.

VLAN 20 – SECURITY

Rete: **192.168.20.0/24**

Gateway di riferimento: **192.168.20.1**

Host: **192.168.20.10 (PC2), 192.168.20.11 (PC3), 192.168.20.20 (PC10), 192.168.20.21 (PC11)**

Viene utilizzata per dispositivi legati alla sicurezza della rete o da isolare per policy più restrittive.

VLAN 30 – OPERATIONS

Rete: **192.168.30.0/24**

Gateway di riferimento: **192.168.30.1**

Host: **192.168.30.10 (PC4), 192.168.30.11 (PC5), 192.168.30.20 (PC12), 192.168.30.21 (PC13)**

È il dominio operativo principale, dedicato alle postazioni di lavoro o ai client di produzione.

VLAN 40 – SERVICES

Rete: **192.168.40.0/24**

Gateway di riferimento: **192.168.40.1**

Host: **192.168.40.10 (PC6), 192.168.40.11 (PC7), 192.168.40.20 (PC14), 192.168.40.21 (PC15)**

Utilizzata per servizi interni o dispositivi che forniscono funzionalità applicative all'interno della rete.

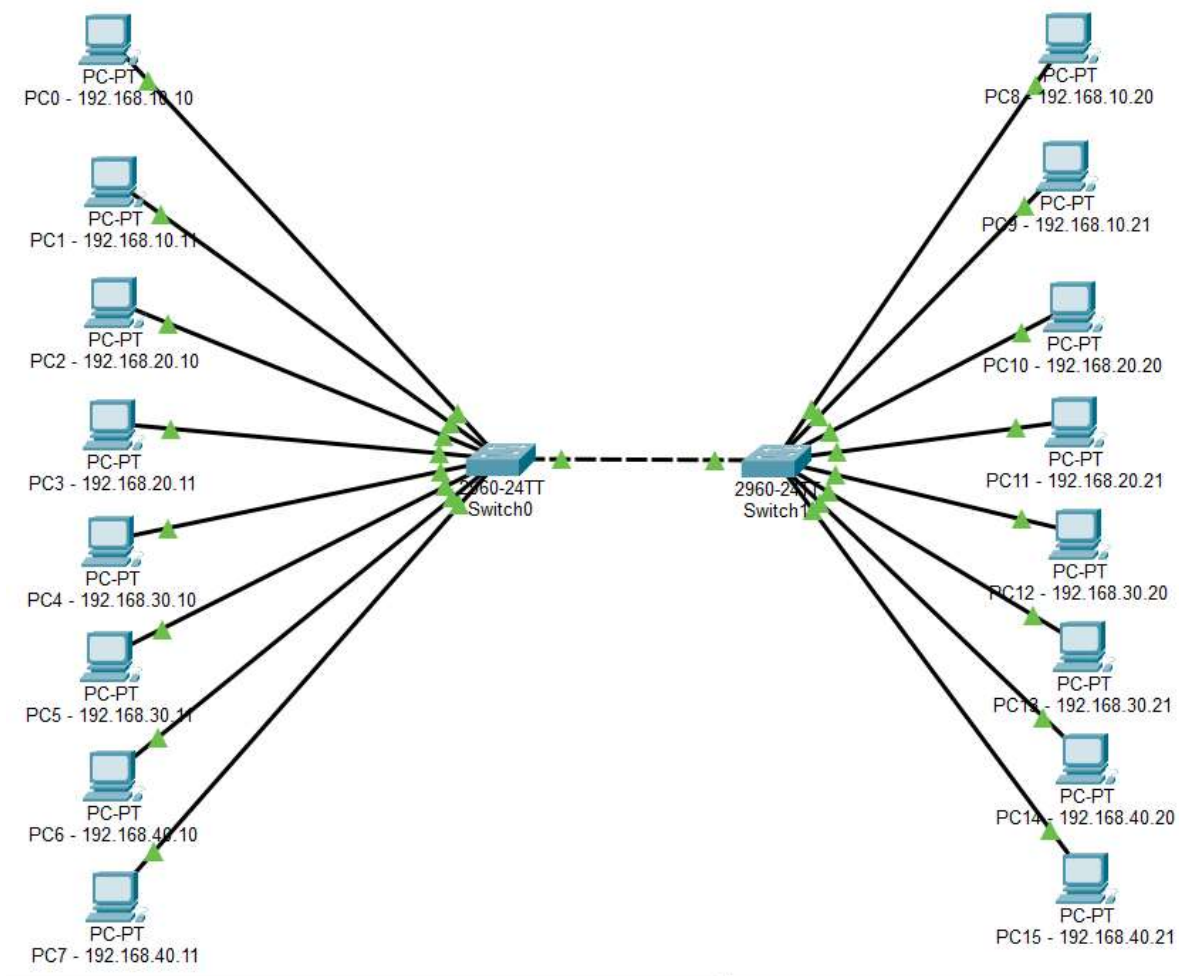
4. DESCRIZIONE DELLA CONFIGURAZIONE

4.1 TOPOLOGIA FISICA

La topologia si compone di:

- **2 switch** di livello 2 (**Switch0 e Switch1**)
- **Host collegati a ciascuno switch**, distribuiti sulle 4 VLAN (**PC0-PC15**)
- Un **collegamento tra gli switch** sulle porte GigabitEthernet configurate come trunk

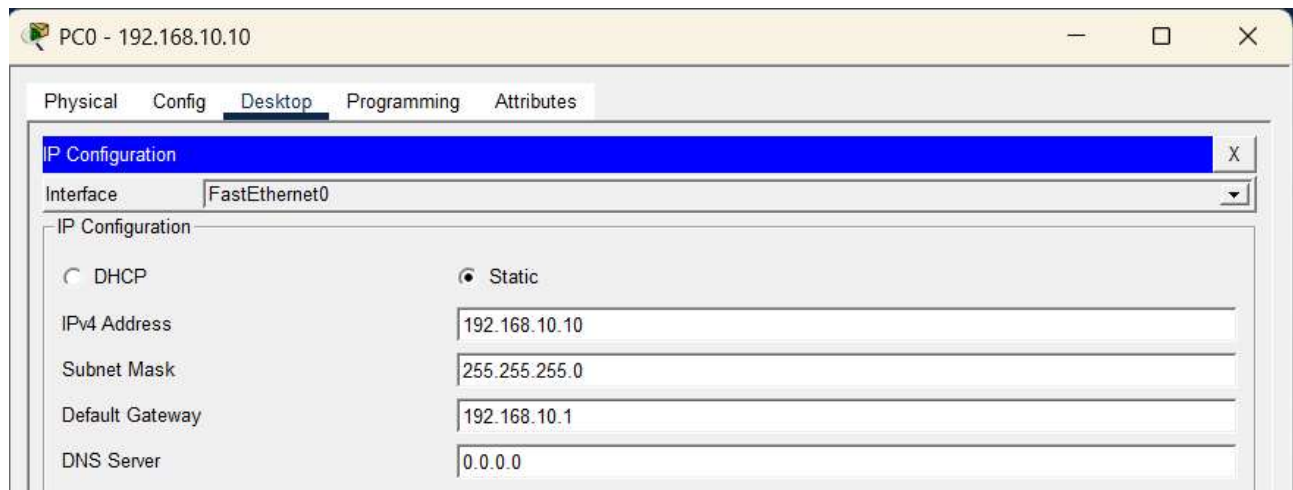
Gli host appartenenti alla stessa VLAN sono stati volutamente distribuiti su entrambi gli switch, in modo da dimostrare l'utilità del trunk.



4.2 CONFIGURAZIONE DEGLI HOST (PC0-PC15)

Per garantire il corretto funzionamento della segmentazione in VLAN e della comunicazione all'interno di ciascun dominio logico, a ogni PC è stato assegnato un indirizzo IP coerente con la subnet associata alla VLAN della porta a cui è collegato.

La configurazione è stata effettuata tramite il pannello Desktop → IP Configuration di ciascun host in Packet Tracer.



Configurazione del PC0 (192.168.10.10)

4.3 CREAZIONE DELLE VLAN SUGLI SWITCH

Su ciascuno switch sono state create le VLAN necessarie, assegnando un nome descrittivo:

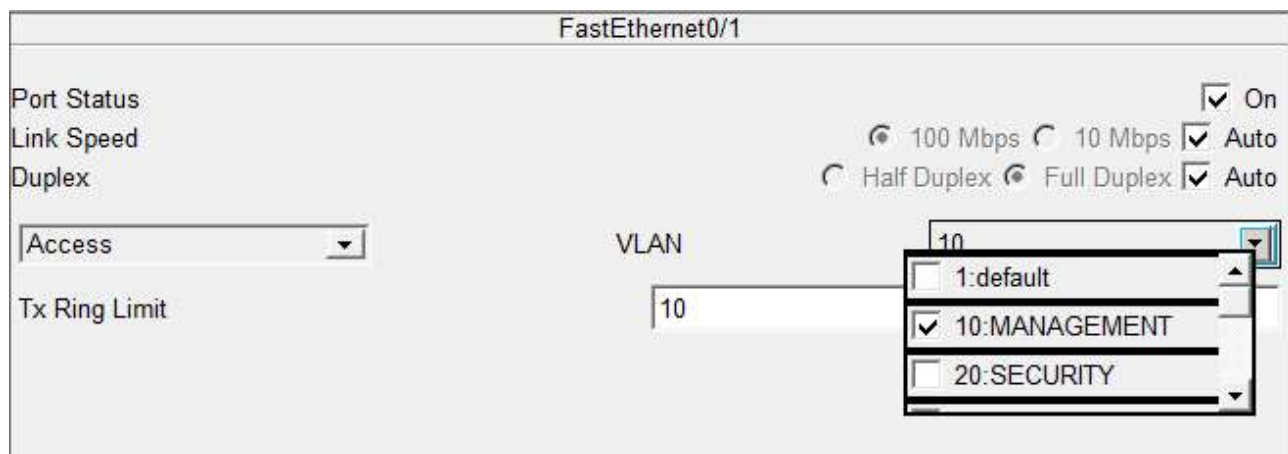
| VLAN No | VLAN Name |
|---------|--------------|
| 1 | default |
| 10 | MANAGEMENT |
| 20 | SECURITY |
| 30 | OPERATIONS |
| 40 | SERVICES |
| 1002 | fddi-default |

Questa configurazione è stata replicata su entrambi gli switch, in modo che la mappatura VLAN-ID sia identica su tutta la rete.

4.4 ASSEGNAZIONE DELLE PORTE ALLE VLAN

Le porte a cui sono collegati i PC sono state configurate in modalità access e assegnate alla VLAN corretta.

Esempio sull'interfaccia Fa/01 dello Switch0 sulla VLAN 10 (MANAGEMENT):



La stessa logica è stata applicata a tutte le porte, assegnandole alla VLAN dedicata in base al tipo di host collegato (MANAGEMENT, SECURITY, OPERATIONS, SERVICES).

Per verificare la corretta creazione delle VLAN e l'associazione delle porte a ciascun dominio logico, è stato utilizzato il comando seguente:

show vlan brief

Lo screenshot riportato sotto evidenzia la presenza delle quattro VLAN configurate (MANAGEMENT, SECURITY, OPERATIONS e SERVICES) e la corretta assegnazione delle porte a ciascuna di esse.

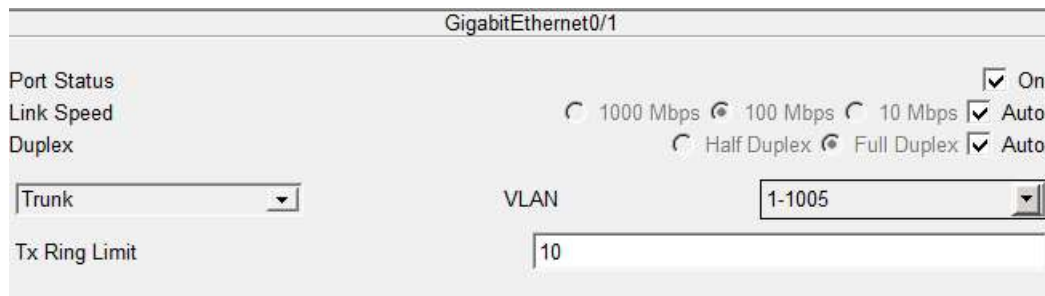
```
Switch#show vlan brief
```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|---|
| 1 | default | active | Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/2 |
| 10 | MANAGEMENT | active | Fa0/1, Fa0/2 |
| 20 | SECURITY | active | Fa0/3, Fa0/4 |
| 30 | OPERATIONS | active | Fa0/5, Fa0/6 |
| 40 | SERVICES | active | Fa0/7, Fa0/8 |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fddinet-default | active | |
| 1005 | trnet-default | active | |

```
Switch#
```

4.5 CONFIGURAZIONE DEL COLLEGAMENTO TRUNK TRA GLI SWITCH

Il collegamento tra Switch0 e Switch1 è stato configurato in modalità trunk, in modo da trasportare simultaneamente il traffico di tutte le VLAN:



GigabitEthernet0/1

Port Status ☒ On

Link Speed ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

Mode

VLAN

Tx Ring Limit

La stessa configurazione è stata effettuata sulla porta corrispondente dell'altro switch.

Il comando *show interfaces trunk* sulla CLI è stato utilizzato per verificare che il link risultasse correttamente in trunk e che le VLAN elencate fossero effettivamente consentite.

```
Switch#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Gig0/1    on        802.1q         trunking      1

Port      Vlans allowed on trunk
Gig0/1    1-1005

Port      Vlans allowed and active in management domain
Gig0/1    1,10,20,30,40

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    1,10,20,30,40

Switch#
```

5. TEST DI CONNETTIVITÀ E VERIFICA DEL FUNZIONAMENTO

Per dimostrare il corretto funzionamento della configurazione è stata eseguita una serie di **test ICMP** (ping) e di verifiche sulle ARP table.

5.1 TEST INTRA-VLAN SULLO STESSO SWITCH

Come primo controllo, è stata verificata la comunicazione tra due host appartenenti alla stessa VLAN e collegati allo stesso switch.

Risultato: il ping ha avuto esito positivo in tutti i casi, confermando la corretta configurazione delle porte in modalità access e l'assegnazione degli IP all'interno della stessa subnet.

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Test ICMP da PC0 (192.168.10.10) verso PC1 (192.168.10.11), entrambe sulla VLAN "MANAGEMENT" cablati su Switch0

5.2 TEST INTRA-VLAN SU SWITCH DIVERSI (VERIFICA DEL TRUNK)

Per evidenziare l'utilità del collegamento trunk, sono stati eseguiti ping tra host appartenenti alla stessa VLAN ma collegati a switch diversi.

Anche in questo caso **il ping ha avuto esito positivo**, dimostrando che:

- i frame Ethernet vengono taggati con l'ID VLAN sul collegamento trunk;
- lo switch di destinazione è in grado di ricostruire il frame nella VLAN corretta e di inoltrarlo verso la porta di access dell'host di destinazione.

```
C:\>ping 192.168.10.21

Pinging 192.168.10.21 with 32 bytes of data:

Reply from 192.168.10.21: bytes=32 time<1ms TTL=128
Reply from 192.168.10.21: bytes=32 time<1ms TTL=128
Reply from 192.168.10.21: bytes=32 time=3ms TTL=128
Reply from 192.168.10.21: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Test ICMP da PC0 (192.168.10.10) verso PC8 (192.168.10.21), entrambe su VLAN "MANAGEMENT" cablati su switch diversi

Durante il primo ping tra due host che non si erano mai comunicati, si è osservato inoltre il normale funzionamento del protocollo ARP:

- 1) L'host sorgente invia un ARP Request in broadcast all'interno della propria VLAN per ottenere il MAC dell'host di destinazione.
- 2) Solo l'host con l'indirizzo IP richiesto risponde con un ARP Reply unicast.
- 3) Una volta popolata la ARP table, il traffico successivo viene inviato direttamente all'indirizzo MAC corretto.

È importante sottolineare che, poiché gli host appartengono alla stessa rete IP, l'instradamento avviene solo a livello 2 (Ethernet) e quindi non è richiesto il passaggio attraverso un router o un dispositivo di livello 3. I pacchetti IP vengono incapsulati in frame Ethernet e inoltrati dagli switch sulla base degli indirizzi MAC.

7. CONSIDERAZIONI FINALI

La configurazione realizzata soddisfa tutti i requisiti dell'esercizio:

- la rete è stata segmentata in **4 VLAN distinte**;
- sono stati utilizzati **almeno due switch**, con host della stessa VLAN distribuiti su switch diversi;
- ogni VLAN è stata associata a una **sottorete IP dedicata**, con indirizzi assegnati coerentemente;
- il **collegamento tra gli switch** è stato configurato in modalità trunk, consentendo il trasporto del traffico di tutte le **VLAN**;
- i test di connettività (**ping**) hanno dimostrato il **corretto funzionamento delle VLAN e del trunk**, sia all'interno dello stesso switch sia tra switch differenti.