

RELAZIONE TECNICA– Segmentazione di Rete con VLAN in Ambiente Ospedaliero

1. Introduzione

L’obiettivo dell’esercitazione è la progettazione e simulazione, tramite Cisco Packet Tracer, di una rete ospedaliera segmentata mediante Virtual LAN (VLAN).

La segmentazione tramite VLAN rappresenta una delle tecniche fondamentali nel networking moderno per garantire sicurezza, isolamento dei domini di broadcast, scalabilità e migliore gestione del traffico di rete.

Nel contesto di un ospedale — dove coesistono reparti con esigenze diverse, livelli di accesso differenziati e dispositivi critici — l’uso delle VLAN permette di suddividere logicamente la rete in gruppi distinti pur condividendo la stessa infrastruttura fisica.

2. Obiettivi del Progetto

- Creare una rete suddivisa in **4 VLAN** rappresentanti i reparti ospedalieri.
 - Utilizzare **almeno 2 switch** interconnessi tramite collegamento **trunk**.
 - Assegnare indirizzi IP statici ai dispositivi di ciascuna VLAN.
 - Effettuare il **subnetting** e associare ogni VLAN a una rete IP distinta.
 - Verificare la corretta configurazione tramite ping e analisi delle tabelle di switch.
 - Analizzare vantaggi e svantaggi dell’uso delle VLAN.
-

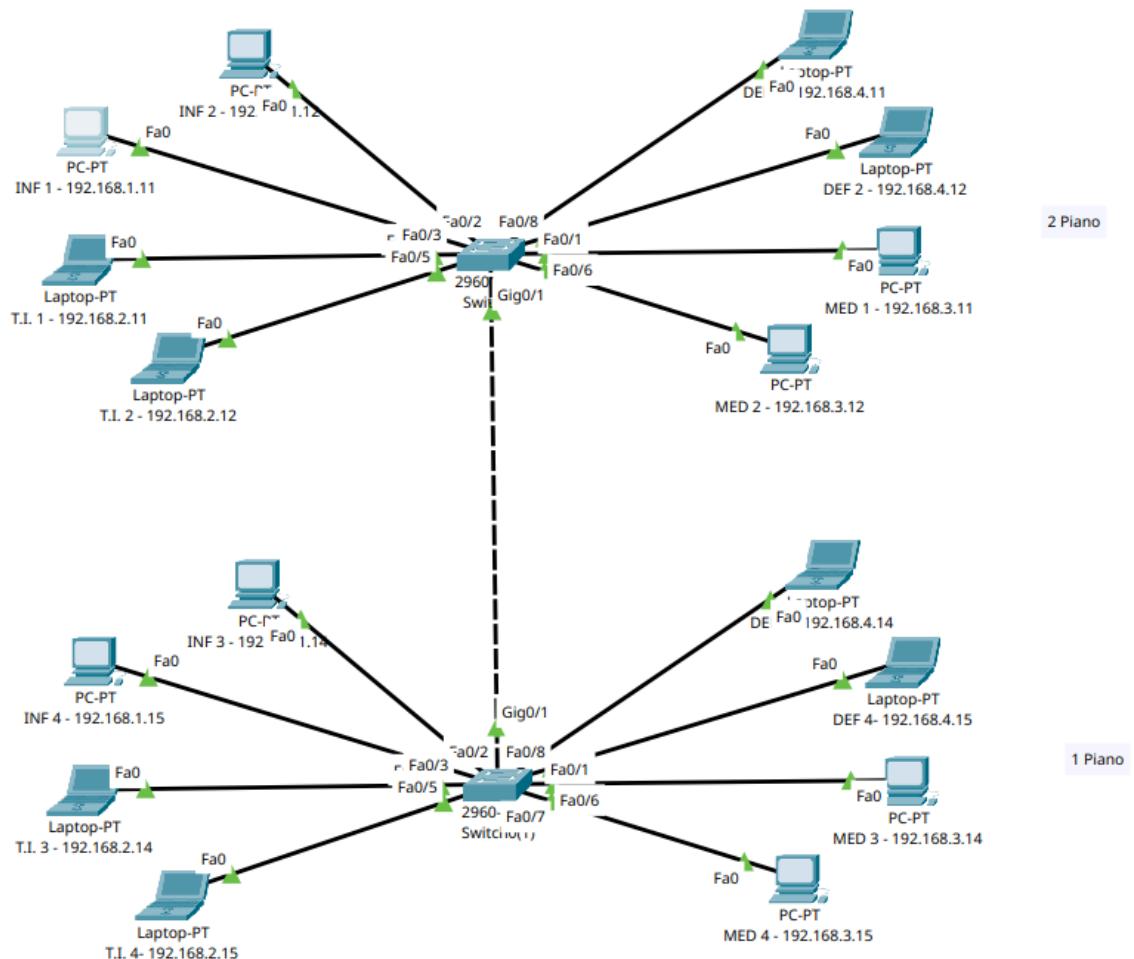
3. Architettura della Rete

La rete è composta da:

- **2 Switch Cisco 2960**
- **16 dispositivi** (PC e Laptop) distribuiti in quattro VLAN
- Collegamento trunk tra i due switch
- Configurazioni di porte Access per i dispositivi finali

Topologia generale

- Riferimento immagine: **Figura 1 – Topologia della rete**



La figura mostra l'organizzazione spaziale dei dispositivi e dei due switch. Ogni gruppo di host è collegato a porte configurate come Access per la rispettiva VLAN, mentre gli switch sono collegati tra loro tramite Gi0/1 in modalità Trunk.

4. Tabella delle VLAN e delle Sottoreti

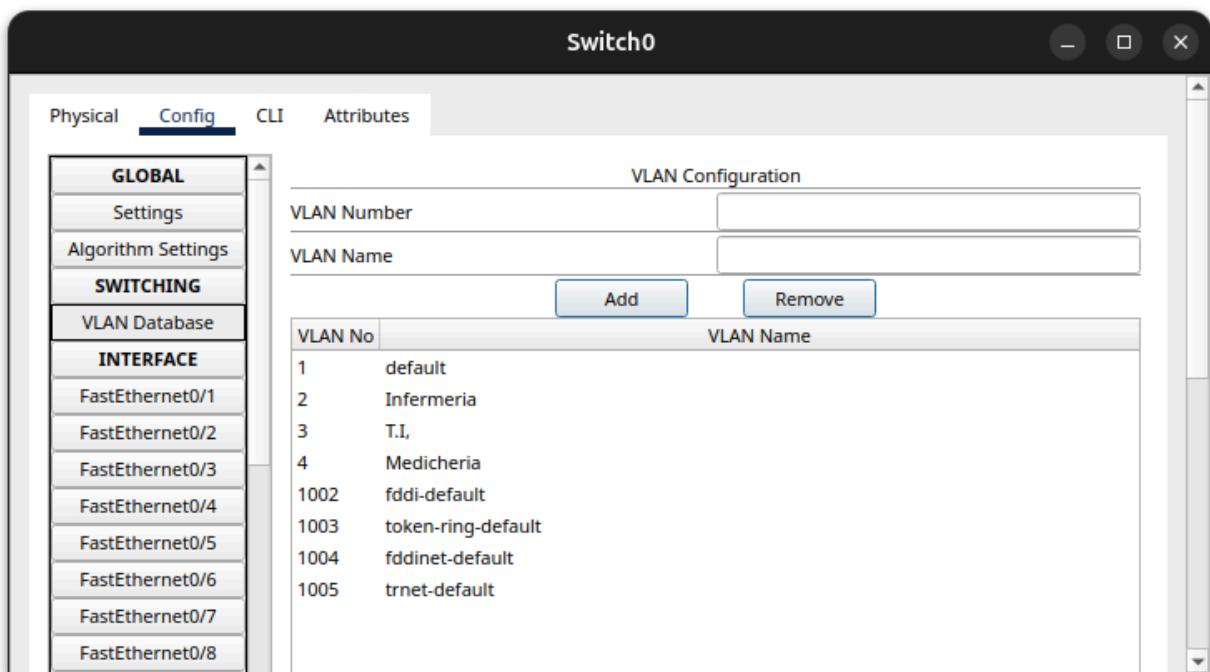
VLAN	Nome Reparto	Subnet	Range Host	Note
VLAN 1	Desk / Reception	192.168.1.0/24	192.168.1.1–254	Area accoglienza
VLAN 2	Infermeria	192.168.2.0/24	192.168.2.1–254	Supporto medico
VLAN 3	Intensive Care	192.168.3.0/24	192.168.3.1–254	Dispositivi critici
VLAN 4	Medicheria	192.168.4.0/24	192.168.4.1–254	Farmaci e attrezzature

Il subnetting è stato realizzato utilizzando una classica maschera /24, garantendo fino a 254 host disponibili per ciascuna VLAN, più che sufficienti per la dimensione dell'infrastruttura simulata.

5. Configurazione delle VLAN sugli Switch

5.1 VLAN Database

- Riferimento immagine: **Figura 2 – VLAN Database sullo switch**



Nella figura sono visibili le VLAN create manualmente:

- VLAN 2 – Infermeria
- VLAN 3 – T.I. (Terapia Intensiva)
- VLAN 4 – Medicheria

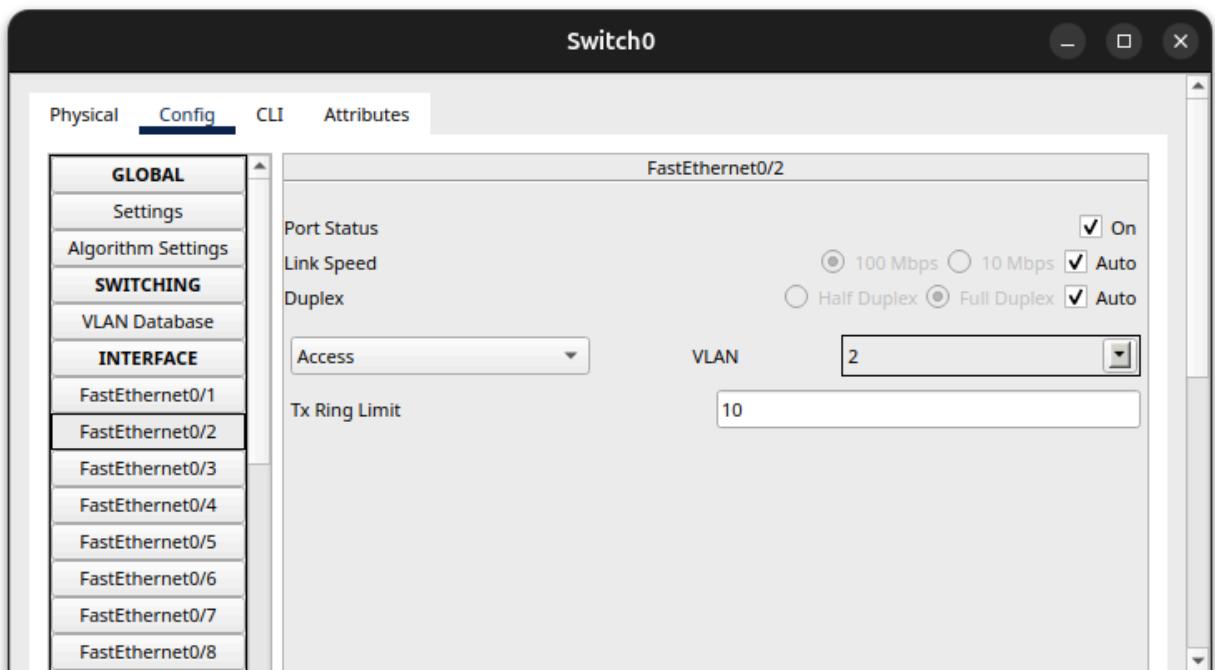
La VLAN 1 rimane quella di default.

6. Configurazione delle Porte

6.1 Porte Access

- Riferimento immagine:

Figura 3 – Configurazione porta Access Fa0/2



La figura mostra l'impostazione di una porta in modalità Access sulla VLAN 2, con:

- Modalità: Access
- VLAN assegnata: 2 *Infermeria*

Tutte le porte collegate a host sono state configurate in modo analogo, assegnandole alla VLAN corretta.

6.2 Elenco completo porte

- Riferimento immagine:

Figura 4 – Tabella porte dello switch

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	0060.47C4.E001
FastEthernet0/2	Up	2	--	0060.47C4.E002
FastEthernet0/3	Up	2	--	0060.47C4.E003
FastEthernet0/4	Up	3	--	0060.47C4.E004
FastEthernet0/5	Up	3	--	0060.47C4.E005
FastEthernet0/6	Up	4	--	0060.47C4.E006
FastEthernet0/7	Up	4	--	0060.47C4.E007
FastEthernet0/8	Up	1	--	0060.47C4.E008
FastEthernet0/9	Down	1	--	0060.47C4.E009
FastEthernet0/10	Down	1	--	0060.47C4.E00A
FastEthernet0/11	Down	1	--	0060.47C4.E00B
FastEthernet0/12	Down	1	--	0060.47C4.E00C
FastEthernet0/13	Down	1	--	0060.47C4.E00D
FastEthernet0/14	Down	1	--	0060.47C4.E00E
FastEthernet0/15	Down	1	--	0060.47C4.E00F
FastEthernet0/16	Down	1	--	0060.47C4.E010
FastEthernet0/17	Down	1	--	0060.47C4.E011
FastEthernet0/18	Down	1	--	0060.47C4.E012
FastEthernet0/19	Down	1	--	0060.47C4.E013
FastEthernet0/20	Down	1	--	0060.47C4.E014
FastEthernet0/21	Down	1	--	0060.47C4.E015
FastEthernet0/22	Down	1	--	0060.47C4.E016
FastEthernet0/23	Down	1	--	0060.47C4.E017
FastEthernet0/24	Down	1	--	0060.47C4.E018
GigabitEthernet0/1	Up	--	--	0060.47C4.E019
GigabitEthernet0/2	Down	1	--	0060.47C4.E01A
Vlan1	Down	1	<not set>	0010.11A8.9D57

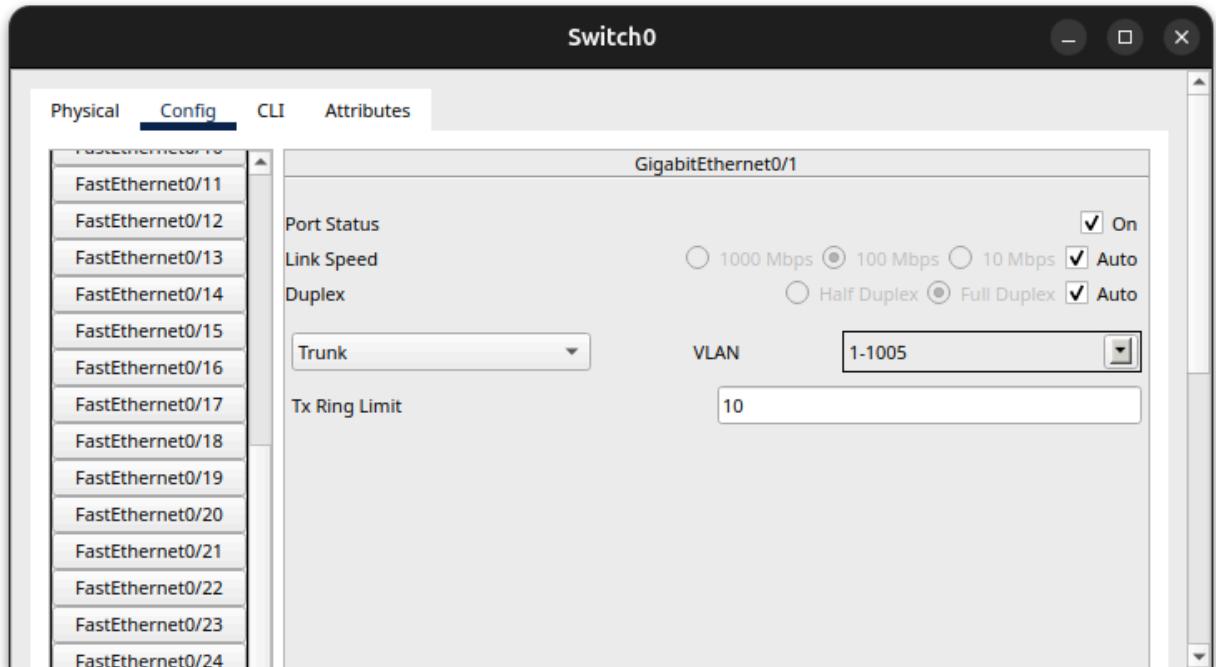
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0

- Questo screenshot riepiloga lo stato delle porte, ciascuna assegnata alla VLAN prevista.

7. Collegamento tra gli Switch (Trunk)

- Riferimento immagine:

Figura 5 – Configurazione Trunk Gi0/1



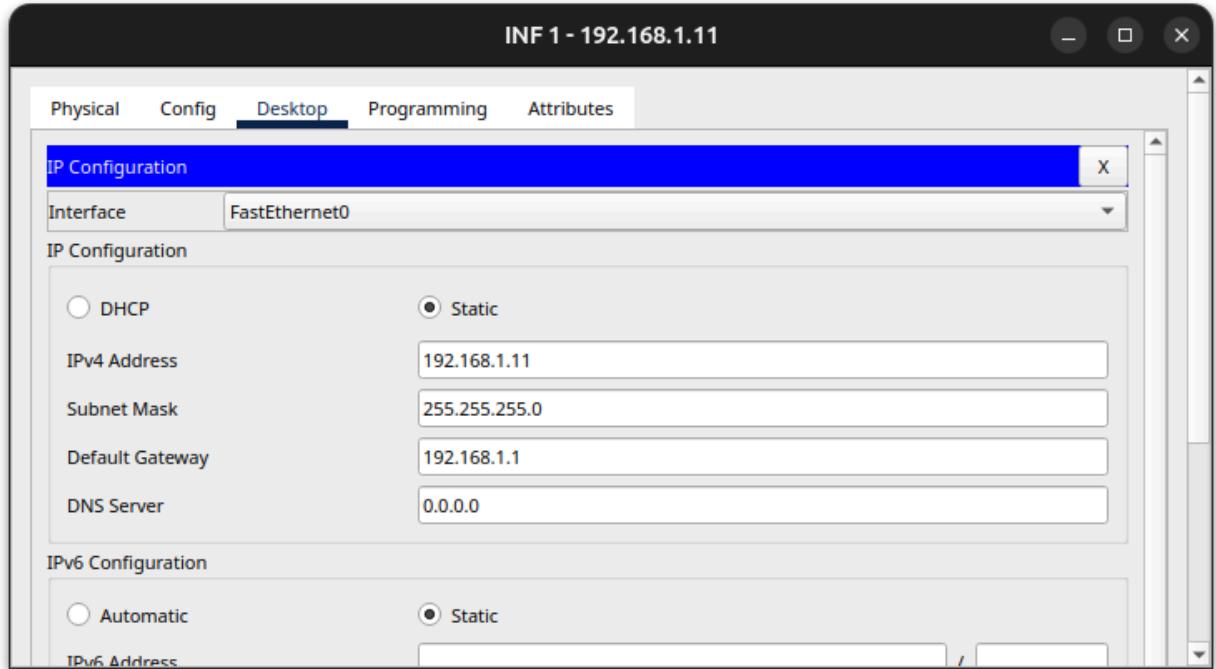
La porta Gi0/1 di entrambi gli switch è configurata in modalità **Trunk**, permettendo il trasporto simultaneo di tutte le VLAN (1–1005).

La modalità trunk consente agli switch di condividere più VLAN sullo stesso collegamento, mantenendo separato il traffico tramite tagging.

8. Configurazione dei Client (Host)

- Riferimento immagine:

Figura 6 – Configurazione IP statica dell'host INF1



Ogni dispositivo ha ricevuto un indirizzo coerente con la propria VLAN.
Esempio (VLAN 2 – Infermeria):

- IP: 192.168.2.11
- Mask: 255.255.255.0
- Gateway (facoltativo nel lab): 192.168.2.1

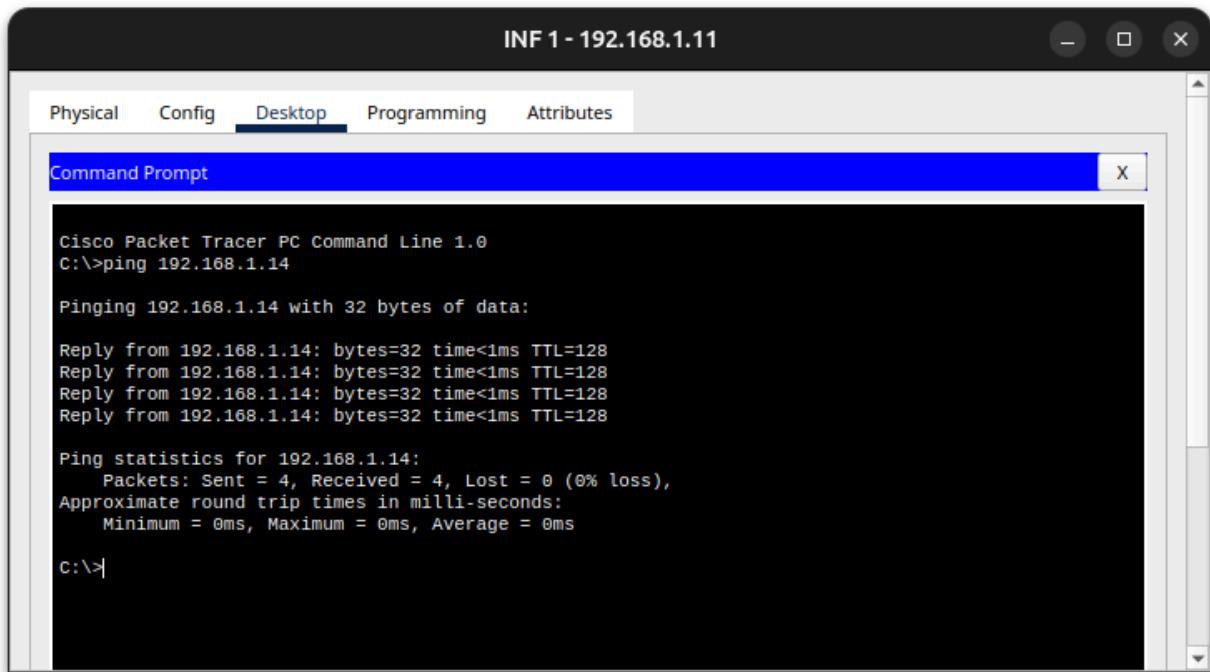
Il set IP è coerente con la tabella delle subnet.

9. Test di Connessione

9.1 Ping intra-VLAN

- Riferimento immagine:

Figura 7 – Test ping INF1 → INF3



The screenshot shows a Cisco Packet Tracer window titled "INF 1 - 192.168.1.11". The "Desktop" tab is selected. A command prompt window titled "Command Prompt" is open, displaying the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.14

Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

La figura mostra un ping riuscito tra due host appartenenti alla stessa VLAN (Infermeria).

Il successo del test dimostra:

- corretta configurazione delle porte Access,
- corretta appartenenza alla stessa VLAN,
- corretta propagazione della VLAN tra gli switch tramite il Trunk.

9.2 Connessione inter-VLAN

Non viene effettuato routing inter-VLAN in questo esercizio, poiché non è richiesto un router o uno switch Layer 3.

Pertanto, **host di VLAN diverse non devono potersi pingare**, condizione che rientra nel comportamento atteso.

10. Vantaggi e svantaggi delle VLAN

10.1 Vantaggi

1. **Riduzione del broadcast:** ogni VLAN è un dominio di broadcast separato → meno traffico inutile.
 2. **Aumento della sicurezza:** dispositivi in VLAN diverse non comunicano senza routing → isolamento dei gruppi.
 3. **Maggiore organizzazione:** permette di raggruppare utenti e dispositivi per funzione senza cambiare cablaggi.
 4. **Flessibilità:** spostare un host da una VLAN all'altra richiede solo una modifica software.
 5. **Scalabilità:** facilita l'espansione della rete mantenendo il controllo sul traffico.
 6. **Ottimizzazione del traffico:** segmentazione logica che migliora prestazioni e gestione.
-

10.2 Svantaggi

1. **Configurazione più complessa:** richiede corretta impostazione di Access, Trunk e sincronizzazione tra switch.
2. **Richiede competenze specifiche:** gestione e troubleshooting non sono adatti a personale inesperto.
3. **Dipendenza dal routing inter-VLAN:** comunicazioni tra VLAN richiedono router o switch Layer 3.
4. **Rischi di misconfigurazione:** errori possono interrompere la connettività o aprire falle di sicurezza.