

Creazione di una rete segmentata con 4 VLAN

Catalin Ardelean Pop

Obiettivo dell'esercizio

Progettare e implementare una rete aziendale distribuita su 4 piani utilizzando 4 VLAN distinte. Consegnare report con screenshot, il file .pkt di Packet Tracer e dimostrare tramite test il corretto funzionamento dei trunk 802.1Q, l'assegnazione delle subnet e la separazione logica tra reparti.

Sommario

La rete simulata rappresenta una società di consulenza IT su 4 piani. Per ogni piano è presente uno switch access e i dispositivi sono raggruppati per reparto: Programmatori, Marketing, HR e PM. Le VLAN isolano il traffico di ciascun reparto; almeno una VLAN (Programmatori) ha host distribuiti su switch diversi per dimostrare il ruolo del trunk. Nel report sono riportati indirizzi, comandi principali, test eseguiti e vantaggi/svantaggi.

1 Requisiti e vincoli

- Minimo 2 switch (qui impiegati 4, uno per piano). - Almeno una VLAN con host su switch diversi (VLAN Programmatori). - Ogni VLAN associata a una rete IP distinta. - Test che dimostri il funzionamento del trunk 802.1Q. - Consegna: PDF con screenshot + .pkt Packet Tracer + file di configurazione.

2 Topologia implementata

La topologia è composta da quattro switch verticalmente collegati con trunk gigabit (uno per piano). Su ciascun switch sono connessi PC e laptop appartenenti ai quattro reparti. L'immagine allegata mostra la distribuzione fisica: Switch al piano 1 (in basso) fino al piano 4 (in alto) con i relativi host.

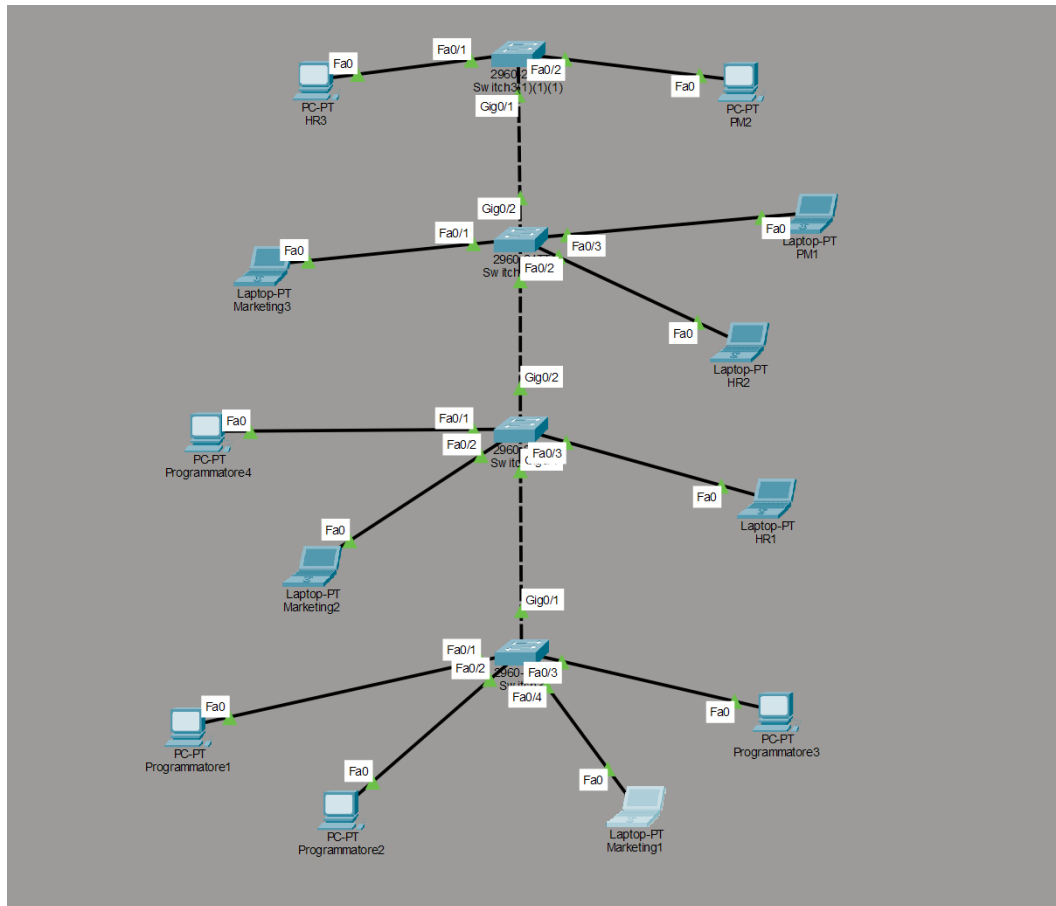


Figura 1: 4 switch interconnessi via trunk; host distribuiti su più piani.

3 Configurazioni

3.1 Configurazione Switch - Creazione VLAN

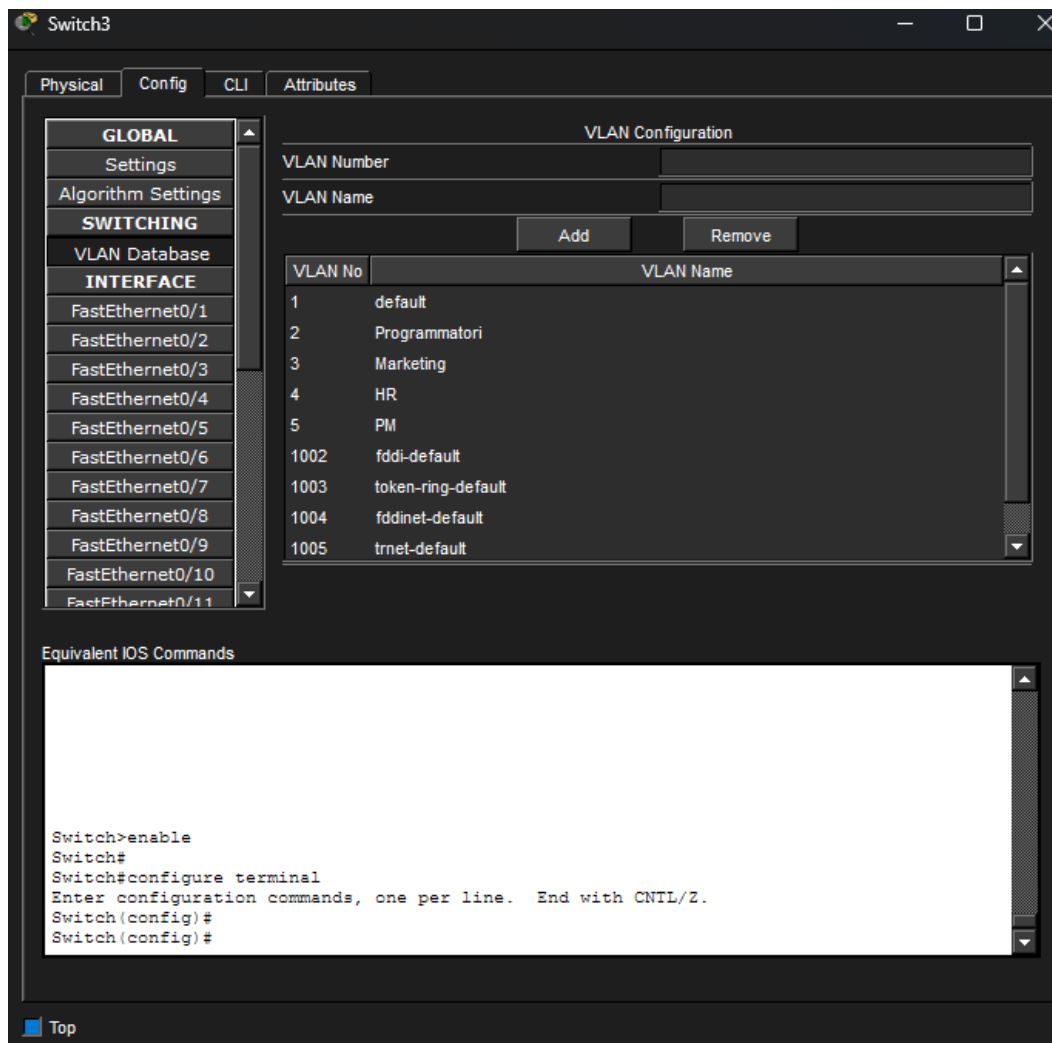


Figura 2: Schermata della configurazione dello switch che mostra le VLAN configurate.

```

1 Switch(config)# vlan 2
2 Switch(config-vlan)# name Programmatori
3 Switch(config)# vlan 3
4 Switch(config-vlan)# name Marketing
5 Switch(config)# vlan 4
6 Switch(config-vlan)# name HR
7 Switch(config)# vlan 5
8 Switch(config-vlan)# name PM

```

4 Configurazione host - Creazione Subnet e assegnazione IP

Di seguito un esempio di configurazione degli indirizzi IP e della subnet mask usati nei PC/laptop della simulazione.

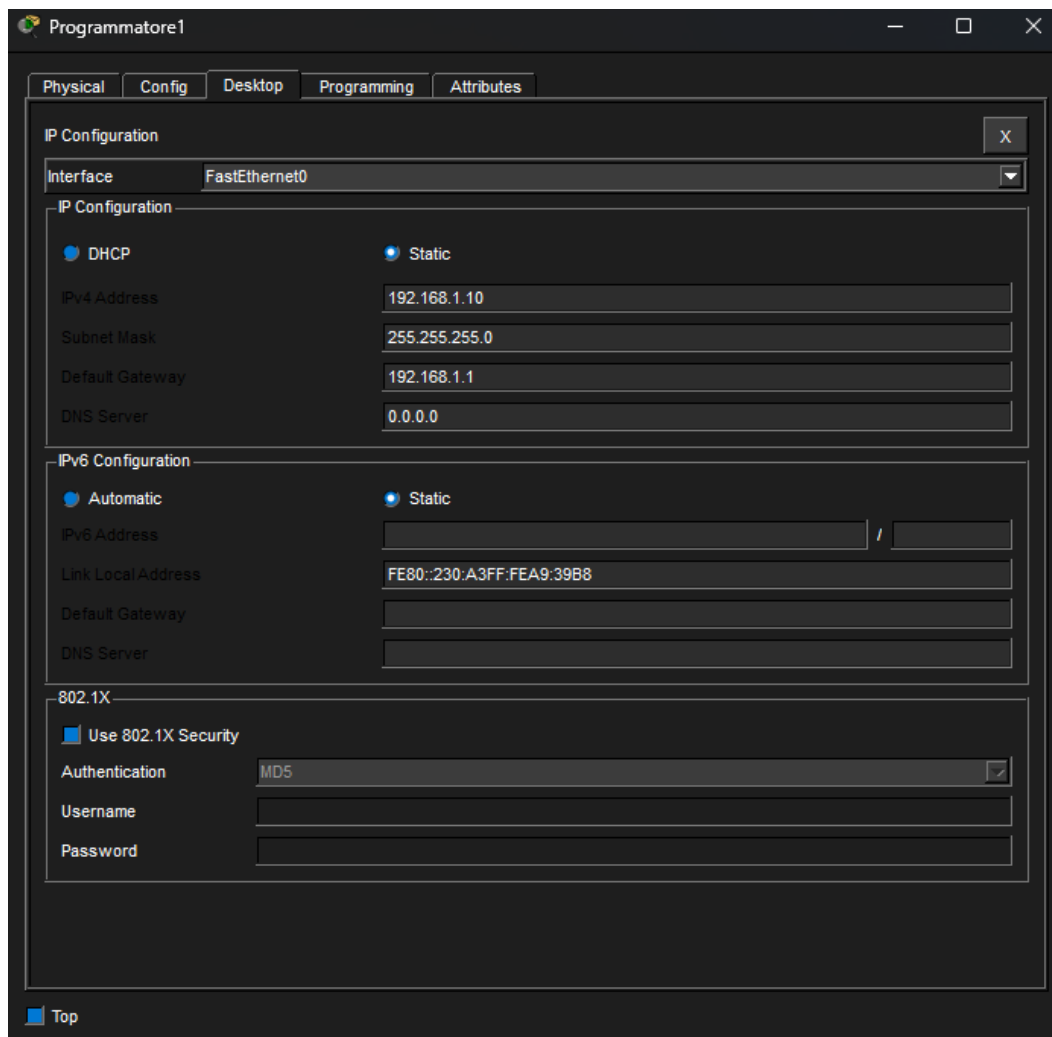


Figura 3: Screenshot della configurazione effettuata.

5 Mappatura VLAN e subnet

VLAN	Reparto	Indirizzi IP host
2	Programmatori	192.168.1.10 - 192.168.1.13
3	Marketing	192.168.2.10 - 192.168.2.12
4	HR	192.168.3.10 - 192.168.3.12
5	PM	192.168.4.10 - 192.168.4.11

Tabella 1: Nota: IP statici usati per chiarezza; in produzione si consiglia DHCP.

6 Test eseguiti e risultati

- Ping intra-VLAN su switch diversi: Programmatore1 → Programmatore4: reply continuo.
- Ping Marketing1 → Marketing3: reply continuo.
- Isolamento VLAN senza routing: ping tra VLAN diverse → nessuna risposta.

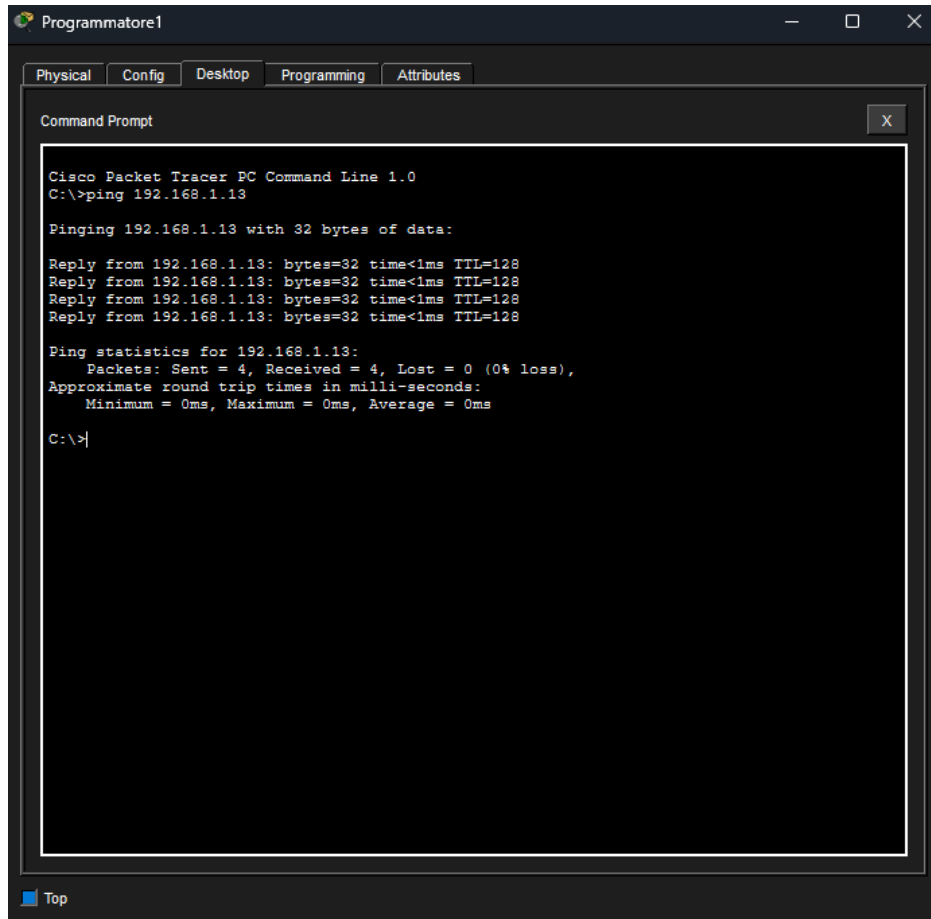


Figura 4: Ping tra Programmatore1 (piano 1) e Programmatore4 (piano 2) su VLAN 2 tramite trunk.

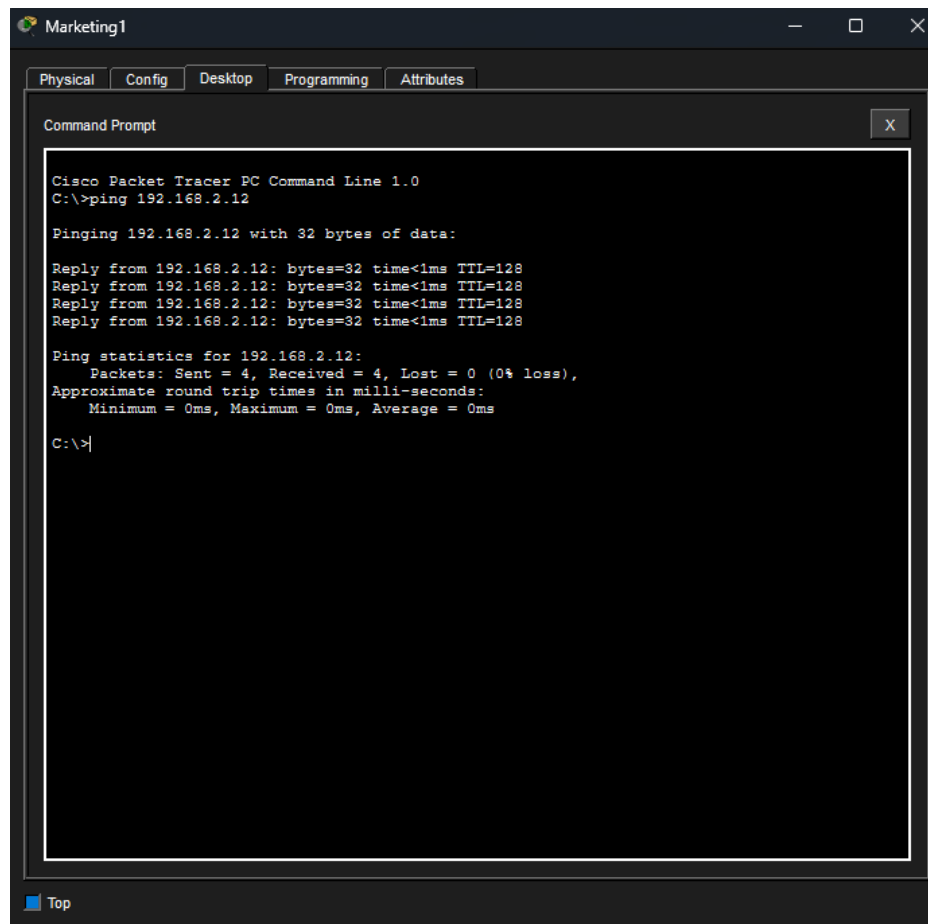


Figura 5: Ping tra Marketing1 (piano 1) e Marketing3 (piano 3) su VLAN 3 tramite trunk.

7 Motivazioni, vantaggi e limiti

Motivazioni

Separare i reparti tramite VLAN offre isolamento logico, facilita l'applicazione di policy di sicurezza e semplifica la gestione (es. backup, monitoraggio, segmentazione dei servizi). Inoltre permette di utilizzare lo stesso cablaggio fisico per più domini logici e di scalare la rete in modo più ordinato.

Vantaggi

- Isolamento del traffico: le VLAN limitano il dominio broadcast e riducono il rumore di rete, migliorando le prestazioni percepite dai singoli reparti.
- Gestione centralizzata delle policy: è più semplice applicare ACL, QoS o politiche di sicurezza a insiemi logici di host anziché porta per porta.
- Flessibilità e mobilità: spostando un utente su un altro switch non è necessario cambiare l'indirizzo IP o il cablaggio se rimane nella stessa VLAN.
- Scalabilità: aggiungere nuovi host o reparti è più veloce, mantenendo ordine e separazione logica.

Svantaggi e rischi operativi

- Complessità di gestione: senza buona documentazione e naming convention, le VLAN e i trunk possono diventare difficili da mantenere.
- Errori di configurazione: mismatch di trunk, native VLAN non allineate o impostazioni STP inappropriate possono causare interruzioni o loop.
- Necessità di routing inter-VLAN: per comunicazioni tra VLAN è necessario un router o un L3 switch; questo introduce costi e possibili punti di congestione.
- Monitoraggio e troubleshooting più complessi: occorrono strumenti (SNMP, syslog, sFlow) e procedure per rilevare rapidamente problemi su trunk e LACP.

Collo di bottiglia sugli uplink fra switch

Il collegamento fisico che unisce gli switch (l'uplink/trunk) trasporta tutto il traffico delle VLAN attraversanti; se questo link ha capacità inferiore rispetto alla somma del traffico generato dagli host collegati agli switch, si crea un collo di bottiglia. Esempi e conseguenze:

- Se gli host hanno porte gigabit ma l'uplink tra switch è 100 Mbps, anche pochi flussi contemporanei possono saturare il link e causare latenze, ritrasmissioni e degrado delle applicazioni.
- Sintomi tipici: ping elevati, throughput ridotto, perdita di pacchetti durante peak, degradazione di VoIP o applicazioni realtime.
- Valutazione rapida: sommare il traffico medio/di picco previsto per gli host su uno switch; se il totale può superare la capacità dell'uplink, è necessario intervenire.

Mitigazioni pratiche:

- Usare link fisici più veloci (Gigabit, 10 Gbps) per gli uplink fra switch.
- Aggregazione di link (Link Aggregation / LACP) per aumentare la banda e fornire ridondanza: creare un Port-Channel su più porte fisiche.
- Bilanciamento del traffico e redistribuzione delle VLAN su più uplink per non concentrare tutto su un singolo link.
- Applicare QoS per dare priorità al traffico critico (VoIP, management) e limitare bulk transfers.
- Monitorare costantemente utilizzo uplink (SNMP, NetFlow/sFlow) per pianificare upgrade prima che si manifesti degrado.

In sintesi: le VLAN migliorano isolamento e gestione, ma la capacità e la ridondanza degli uplink sono critiche per evitare colli di bottiglia; usare uplink adeguati o tecniche di aggregazione è essenziale in reti con host ad alta domanda di banda.