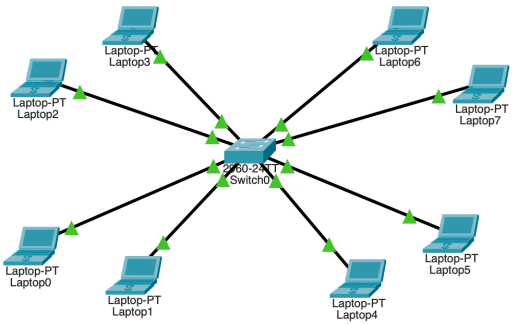
REPORT TECNICO: IMPLEMENTAZIONE DI UNA RETE SEGMENTATA CON VLAN

INTRODUZIONE

Il presente report descrive l'implementazione di una rete locale segmentata utilizzando la tecnologia VLAN (Virtual Local Area Network) per separare logicamente quattro diversi settori aziendali: Amministrazione, Vendite, Sviluppo e area Guest. L'implementazione è stata realizzata utilizzando Cisco Packet Tracer come ambiente di simulazione.

ARCHITETTURA DELLA RETE

La rete è stata strutturata utilizzando:
- 1 Switch Layer 2 Cisco 2960
- 8 PC Client (2 per ogni VLAN)
- 4 VLAN distinte



SEGMENTAZIONE VLAN

- VLAN 10: Rete1
  * Porte Switch: Fa0/1-2
  * Range IP: 172.16.10.0

- VLAN 20: Rete2
  * Porte Switch: Fa0/3-4
  * Range IP: 172.16.20.0

- VLAN 30: Rete3
  * Porte Switch: Fa0/5-6
  * Range IP: 172.16.30.0

- VLAN 40: Rete4
  * Porte Switch: Fa0/7-8
  * Range IP: 172.16.40.0

BENEFICI IMPLEMENTATIVI

L'implementazione delle VLAN ha portato i seguenti vantaggi:

1. Sicurezza Migliorata
   - Isolamento del traffico tra dipartimenti
   - Protezione dei dati sensibili dell'amministrazione
   - Segregazione della rete guest dal resto dell'infrastruttura

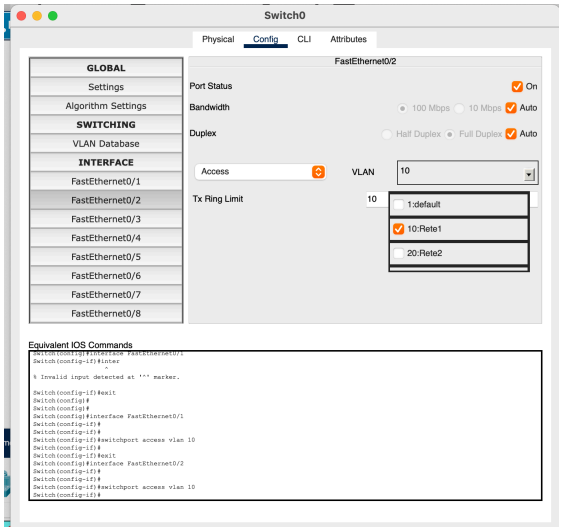
2. Ottimizzazione delle Prestazioni
   - Riduzione dei domini di broadcast
   - Diminuzione del traffico di rete non necessario
   - Miglior gestione della banda disponibile

3. Flessibilità Organizzativa
   - Raggruppamento logico degli utenti indipendente dalla posizione fisica
   - Facilità di spostamento delle postazioni di lavoro
   - Gestione semplificata delle modifiche alla rete

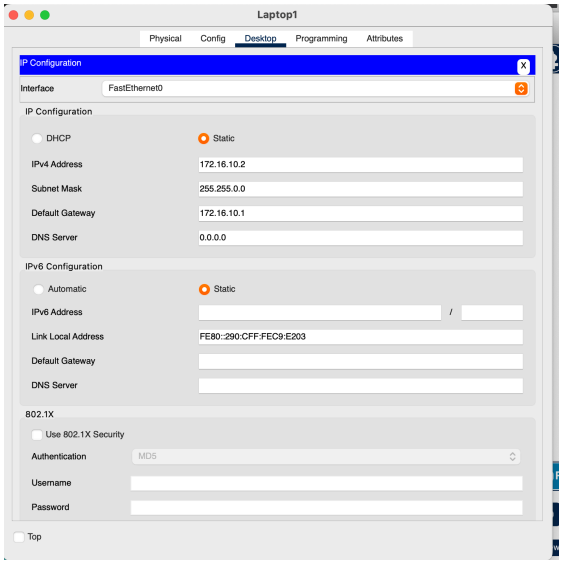
CONFIGURAZIONE TECNICA

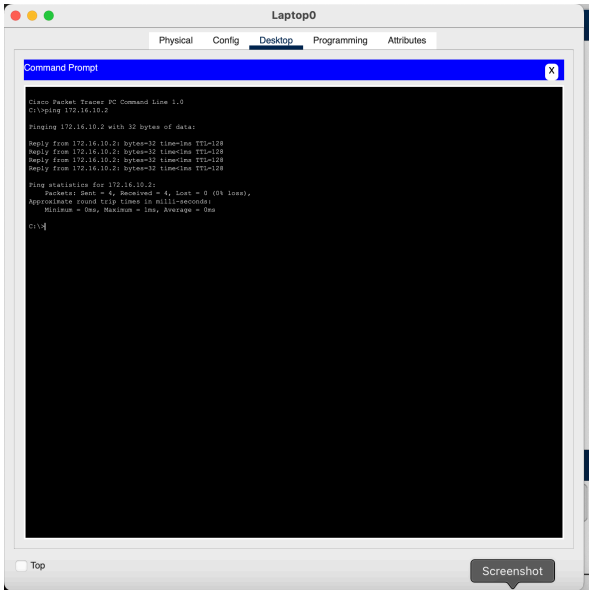
La configurazione dello switch ha richiesto i seguenti passaggi:

1. Creazione delle VLAN:
   - Definizione degli ID VLAN (10, 20, 30, 40)
   - Assegnazione dei nomi descrittivi
   - Configurazione delle porte in modalità access



2. Assegnazione IP:
   - Subnet distinte per ogni VLAN
   - Configurazione degli endpoint con indirizzi IP appropriati
   - Implementazione delle subnet mask corrette (255.255.255.0)





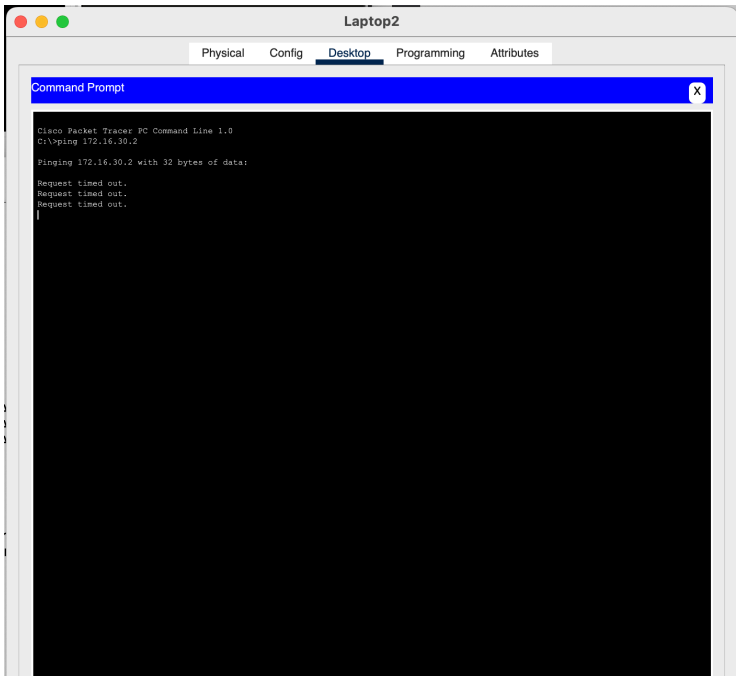
TEST DI CONNETTIVITÀ

Sono stati effettuati test di ping per verificare l'isolamento delle VLAN:

1. Test intra-VLAN (stesso segmento):
   - VLAN 10: Ping da PC1 (172.16.10.2) a PC2 (172.16.10.3) - SUCCESSO
   - VLAN 20: Ping da PC3 (172.16.20.2) a PC4 (172.16.20.3) - SUCCESSO
   - VLAN 30: Ping da PC5 (172.16.30.2) a PC6 (172.16.30.3) - SUCCESSO

- VLAN 40: Ping da PC7 (172.16.40.2) a PC8 (172.16.40.3) - SUCCESSO

2. Test inter-VLAN (segmenti diversi):
   - Da VLAN 10 a VLAN 20: Ping da PC1 (172.16.10.2) a PC3 (172.16.20.2) - FALLITO
   - Da VLAN 20 a VLAN 30: Ping da PC3 (172.16.20.2) a PC5 (172.16.30.2) - FALLITO
   - Da VLAN 30 a VLAN 40: Ping da PC5 (172.16.30.2) a PC7 (172.16.40.2) - FALLITO



I risultati dei test confermano che:

- I dispositivi all'interno della stessa VLAN possono comunicare tra loro
- I dispositivi in VLAN diverse sono correttamente isolati
- La segmentazione della rete funziona come previsto

Questi test dimostrano l'efficacia dell'implementazione delle VLAN nel creare segmenti di rete isolati. Per permettere la comunicazione tra VLAN diverse sarebbe necessario implementare il routing inter-VLAN tramite un router Layer 3.

CONSIDERAZIONI SULLA SICUREZZA

La segmentazione implementata garantisce:
- Isolamento del traffico di rete tra i vari dipartimenti
- Protezione dei dati sensibili dell'amministrazione
- Separazione della rete guest dalle risorse aziendali
- Controllo granulare degli accessi alle risorse

CONCLUSIONI

L'implementazione delle VLAN ha permesso di creare una struttura di rete moderna ed efficiente, che soddisfa le esigenze di sicurezza e prestazioni dell'organizzazione. La soluzione adottata offre

la flessibilità necessaria per future espansioni e modifiche, garantendo al contempo un elevato livello di sicurezza e prestazioni ottimali.

RACCOMANDAZIONI FUTURE

Per migliorare ulteriormente l'infrastruttura, si suggerisce di:
1. Implementare il routing inter-VLAN per la comunicazione tra segmenti
2. Configurare policy di sicurezza specifiche per ogni VLAN
3. Implementare un sistema di monitoraggio del traffico
4. Documentare tutte le modifiche future alla configurazione