Relazione Tecnica: Configurazione di Rete Segmentata con VLAN

1.0 Introduzione e Obiettivi del Progetto

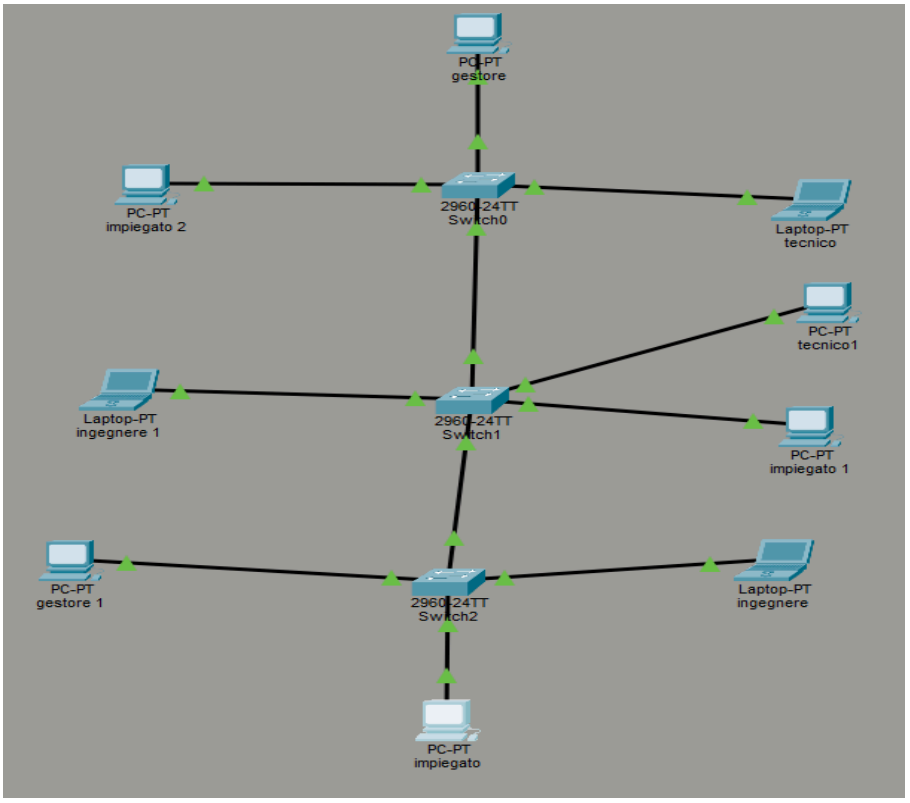
La presente relazione tecnica descrive la progettazione, la configurazione e la verifica di una rete aziendale segmentata logicamente tramite l'impiego di Virtual LAN (VLAN). L'obiettivo strategico di questa implementazione è migliorare in modo significativo la sicurezza, l'organizzazione e le prestazioni complessive dell'infrastruttura di rete. Attraverso l'isolamento dei domini di broadcast per differenti gruppi di utenti, si intende creare un ambiente di rete più efficiente, controllato e resiliente.

Gli obiettivi specifici del progetto, definiti in fase di pianificazione e raggiunti con successo, sono i seguenti:

- **Creazione di 4 VLAN distinte** per segmentare il traffico di rete in base ai ruoli aziendali (gestori, impiegati, tecnici, ingegneri).
- **Utilizzo di un'infrastruttura multi-switch** per dimostrare la scalabilità e la flessibilità della soluzione su più dispositivi fisici.
- **Assegnazione di sottoreti IP dedicate** a ciascuna VLAN per una gestione logica e ordinata dell'indirizzamento.
- **Configurazione di collegamenti Trunk** per garantire la comunicazione trasparente tra gli switch, permettendo l'estensione delle VLAN sull'intera infrastruttura.
- **Verifica della connettività e dell'isolamento** per validare il corretto funzionamento della segmentazione e il raggiungimento degli obiettivi di sicurezza.

Le sezioni successive analizzeranno in dettaglio l'architettura fisica e logica della rete implementata.

2.0 Architettura della Rete



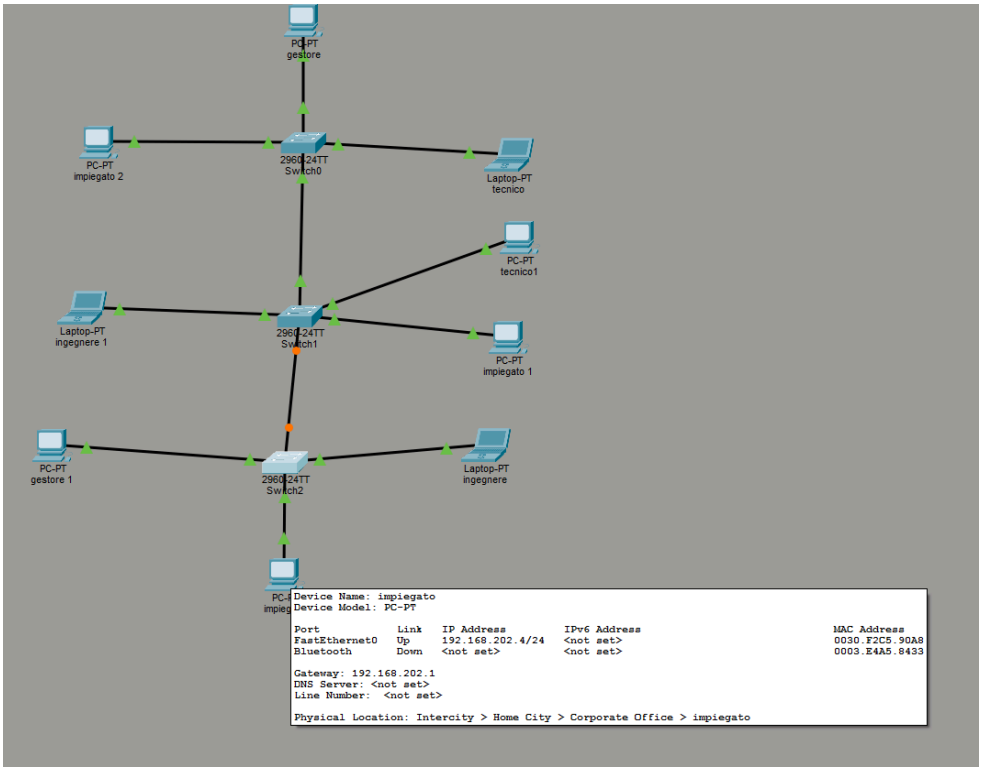
Per una comprensione completa dell'implementazione, è fondamentale distinguere tra l'architettura fisica e quella logica. L'architettura fisica descrive i componenti hardware (switch, cavi, dispositivi finali) e le loro interconnessioni fisiche. L'architettura logica, invece, definisce come la rete è organizzata virtualmente attraverso la segmentazione in VLAN e l'assegnazione di sottoreti IP. La topologia logica si sovrappone a quella fisica per creare gruppi di lavoro virtuali che operano in modo indipendente dall'ubicazione fisica dei dispositivi.

2.1 Componenti Fisici

L'infrastruttura di rete è basata su una topologia fisica a albero (o bus lineare), con `Switch1` che funge da punto di interconnessione centrale tra `Switch0` e `Switch2`. I componenti sono i seguenti:

- **Switch di Rete:** Sono stati utilizzati **tre switch modello 2960-24TT**, denominati `Switch0`, `Switch1` e `Switch2`. Gli switch sono interconnessi in serie per garantire la copertura dell'intera rete.
- **Dispositivi Terminali:** Alla rete sono connessi diversi dispositivi finali, tra cui PC e Laptop. I dispositivi sono stati nominati in modo descrittivo per riflettere il reparto di appartenenza, come ad esempio `gestore`, `impiegato`, `tecnico` e `ingegnere`, facilitando l'identificazione e la gestione.

2.2 Segmentazione Logica e Indirizzamento IP



La rete è stata segmentata logicamente in quattro VLAN distinte. Ogni VLAN raggruppa dispositivi con ruoli funzionali simili, indipendentemente dallo switch a cui sono fisicamente collegati. A ciascuna VLAN è stata assegnata una sottorete IP univoca, come illustrato nella tabella seguente:

Nome VLAN	Sottorete IP e Subnet Mask
Gestori	`192.168.200.0/24`
Tecnici	`192.168.201.0/24`
Impiegati	`192.168.202.0/24`
Ingegneri	`192.168.203.0/24`

Questa suddivisione logica è cruciale perché garantisce che il traffico di broadcast generato all'interno di una VLAN rimanga confinato ad essa. Ciò riduce il traffico non necessario sulle altre VLAN, ottimizzando le prestazioni generali della rete e rafforzando la sicurezza.

La sezione seguente entrerà nel merito delle configurazioni specifiche—le porte di accesso che assegnano i dispositivi come `impiegato` alla VLAN 202 e i collegamenti trunk che permettono a quella stessa VLAN di estendersi da `Switch2` a `Switch1`—per realizzare questa architettura.

3.0 Dettagli di Configurazione degli Switch

Il ruolo degli switch è cruciale per l'implementazione delle VLAN. La corretta configurazione delle loro porte è ciò che permette di applicare la segmentazione logica all'infrastruttura fisica. Questa sezione illustra le due modalità operative fondamentali utilizzate per le porte: la modalità `access`, per la connessione dei dispositivi finali, e la modalità `trunk`, per l'interconnessione tra gli switch.

3.1 Configurazione delle Porte di Accesso

Una porta di accesso (o "access port") è una porta dello switch configurata per appartenere a una singola e specifica VLAN. Tutto il traffico che transita su questa porta viene considerato parte di quella VLAN. Nel nostro progetto:

- Ogni porta a cui è collegato un dispositivo finale (PC o Laptop) è stata configurata in modalità `access`.
- A ciascuna di queste porte è stata assegnata la VLAN corrispondente al ruolo funzionale del dispositivo. Ad esempio, la porta a cui è collegato il PC `impiegato` è stata assegnata alla VLAN "Impiegati", mentre quella per il laptop `tecnico` è stata assegnata alla VLAN "Tecnici".

Questa configurazione garantisce che ogni dispositivo entri nella rete direttamente nel proprio segmento logico designato.

3.2 Configurazione dei Collegamenti Trunk

Un collegamento trunk (o "trunk link") è un canale punto-punto ad alta capacità tra due dispositivi di rete (tipicamente due switch) in grado di trasportare simultaneamente il traffico di più VLAN. Per permettere alle VLAN di estendersi attraverso l'intera infrastruttura fisica:

- I collegamenti fisici tra `Switch0` e `Switch1`, e tra `Switch1` e `Switch2`, sono stati configurati in modalità `trunk`.

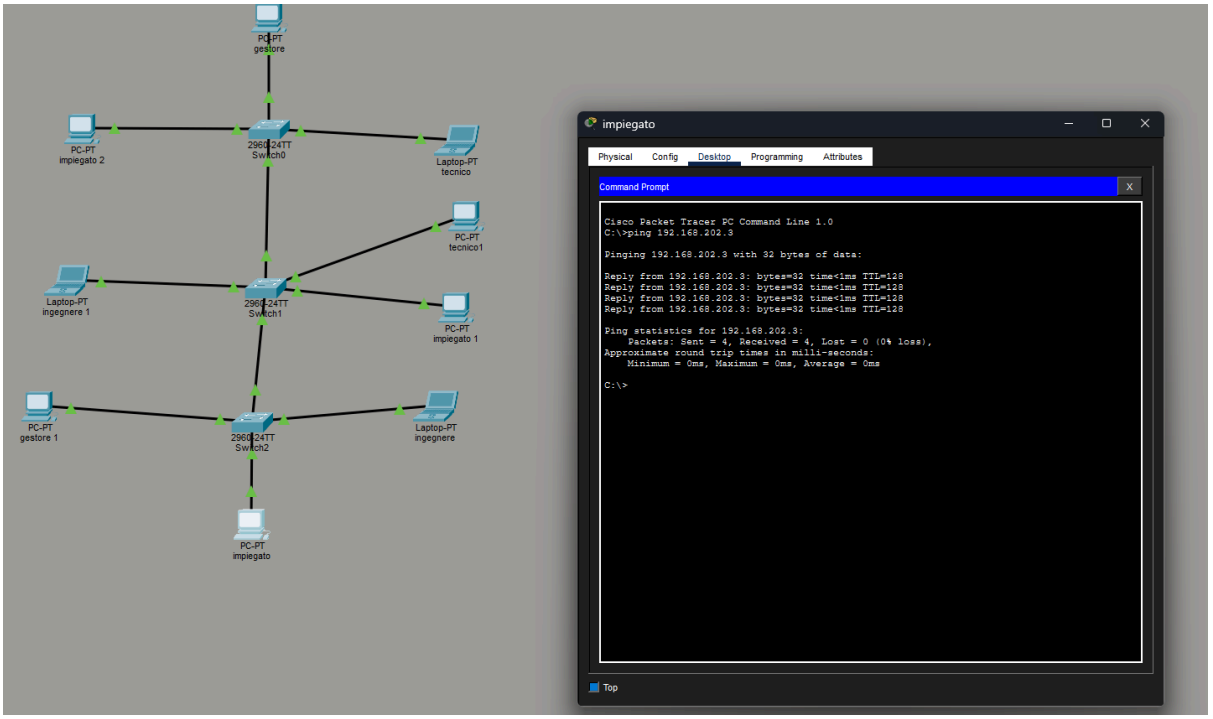
Questa configurazione è l'elemento chiave che permette, ad esempio, a un dispositivo della VLAN 'Impiegati' collegato a `Switch2` di comunicare con un altro dispositivo della stessa VLAN su `Switch0`, come verrà dimostrato nei test di connettività.

I risultati dei test eseguiti per validare la correttezza di queste configurazioni sono presentati nella sezione successiva.

4.0 Verifica del Funzionamento e Test di Connettività

Una volta completata la configurazione, è stata condotta una fase di verifica per assicurare che la rete si comportasse come previsto. Sono stati eseguiti test specifici utilizzando il comando `ping` per dimostrare due principi fondamentali: la corretta comunicazione all'interno di una stessa VLAN (connettività intra-VLAN) e il corretto isolamento tra VLAN diverse (isolamento inter-VLAN). Questi test confermano il raggiungimento degli obiettivi primari di sicurezza e segmentazione.

4.1 Test di Connettività Intra-VLAN (Comunicazione Abilitata)

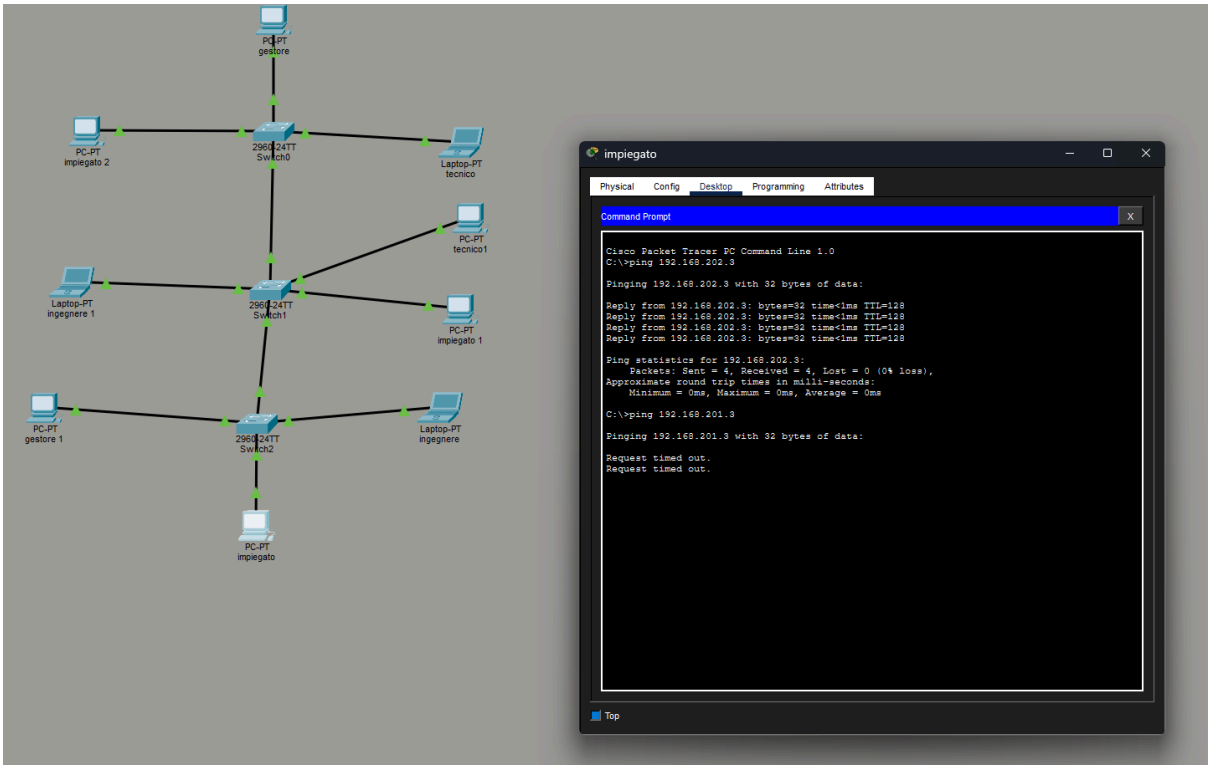


Per verificare che i dispositivi all'interno della stessa VLAN potessero comunicare, anche se collegati a switch diversi, è stato eseguito un test di `ping` tra due host della VLAN "Impiegati".

- **Azione:** Dal PC `impiegato`, con indirizzo IP `192.168.202.4`, è stato eseguito il comando `ping 192.168.202.3`.
- **Risultato:** Il test ha avuto esito positivo, come documentato dall'output della Command Line:
- **Analisi:** Il successo di questo test dimostra che la connettività all'interno della stessa VLAN è pienamente funzionante. Inoltre, poiché il dispositivo di origine `impiegato` (`192.168.202.4`) è connesso a `Switch2` e il dispositivo di destinazione si trova su uno switch diverso, questo risultato conferma in modo inequivocabile il corretto

funzionamento dei collegamenti trunk tra `Switch2` e `Switch1`, che trasportano il traffico della VLAN 'Impiegati' attraverso l'infrastruttura.

4.2 Test di Isolamento Inter-VLAN (Comunicazione Bloccata)



Il secondo test è stato progettato per confermare che le VLAN fossero isolate l'una dall'altra, impedendo comunicazioni dirette non autorizzate.

- **Azione:** Dallo stesso PC `impiegato` (`192.168.202.4`) è stato eseguito il comando `ping 192.168.201.3` verso un dispositivo appartenente a un'altra VLAN (VLAN "Tecnici").
- **Risultato:** Il test è fallito, come previsto. L'output restituito è stato il seguente:
- **Analisi:** Il fallimento del ping è il risultato atteso e desiderato in questa configurazione. Dimostra che il traffico di Livello 2 non può attraversare i confini della VLAN. Questo isolamento è il fondamento della sicurezza fornita dalla segmentazione, impedendo a un utente di una VLAN di accedere direttamente alle risorse di un'altra senza un dispositivo di routing intermedio.

I risultati di questi test validano la configurazione e ci permettono di passare a un'analisi più ampia dei vantaggi e delle considerazioni legate all'uso delle VLAN.

5.0 Analisi Generale delle VLAN: Vantaggi e Svantaggi

Sebbene l'implementazione descritta abbia avuto pieno successo, è fondamentale per un professionista di rete valutare in modo critico la tecnologia utilizzata. Le VLAN sono uno strumento estremamente potente, ma il loro impiego comporta una serie di benefici e

potenziali complessità. Questa sezione analizza i vantaggi intrinseci e le considerazioni pratiche associate all'uso delle VLAN in un ambiente di rete.

5.1 Vantaggi

Il progetto ha dimostrato concretamente i seguenti benefici chiave derivanti dall'uso delle VLAN:

1. **Sicurezza Migliorata** L'isolamento dei gruppi di utenti in segmenti di rete separati impedisce accessi non autorizzati tra reparti. Un utente malintenzionato o un malware che compromette un dispositivo in una VLAN avrà difficoltà a propagarsi ad altre VLAN, contenendo efficacemente la minaccia.
2. **Prestazioni Ottimizzate** La segmentazione della rete in domini di broadcast più piccoli riduce drasticamente il traffico di rete non necessario. I messaggi di broadcast (come le richieste ARP) vengono confinati all'interno della VLAN di origine, liberando banda preziosa e migliorando la reattività generale della rete per tutti gli utenti.
3. **Amministrazione Semplificata** Le VLAN offrono una notevole flessibilità gestionale. È possibile spostare fisicamente un utente da un ufficio all'altro senza dover riconfigurare il suo indirizzo IP o altre impostazioni di rete. Finché la nuova porta dello switch è assegnata alla stessa VLAN, il dispositivo manterrà la sua connettività e le sue policy di accesso, semplificando le operazioni di aggiunta, spostamento e modifica degli utenti.

5.2 Svantaggi e Considerazioni

Nonostante i chiari vantaggi, l'adozione delle VLAN introduce alcuni elementi di cui tenere conto:

1. **Complessità di Configurazione** Una rete segmentata con VLAN e trunk è intrinsecamente più complessa da progettare e gestire rispetto a una rete "piatta" tradizionale. La configurazione richiede una maggiore attenzione ai dettagli e una solida comprensione dei protocolli di rete per evitare errori che potrebbero causare problemi di connettività o di sicurezza.
2. **Necessità di Routing Inter-VLAN** Per impostazione predefinita, le VLAN sono completamente isolate. Sebbene questo sia un vantaggio per la sicurezza, spesso è necessario che alcuni utenti di una VLAN (es. un impiegato) accedano a risorse situate in un'altra (es. un server condiviso). Per consentire questa comunicazione controllata, è indispensabile un dispositivo di Livello 3, come un router o uno switch multi-livello, configurato per instradare il traffico tra le VLAN. Questo aggiunge un ulteriore livello di configurazione e gestione all'infrastruttura.

La valutazione di questi aspetti è fondamentale prima di procedere con l'implementazione in un ambiente di produzione.

6.0 Conclusioni

La presente relazione ha documentato la progettazione e l'implementazione di una rete aziendale segmentata tramite VLAN. L'implementazione non solo ha raggiunto gli obiettivi,

ma ne ha fornito prova tangibile: la connettività intra-VLAN è stata confermata da ping riusciti tra dispositivi su switch fisicamente distinti, validando i collegamenti trunk, mentre il fallimento mirato dei ping inter-VLAN ha dimostrato l'efficacia dell'isolamento a livello 2, fondamento della sicurezza della rete.

In conclusione, l'implementazione dimostra efficacemente come la tecnologia VLAN sia uno strumento potente e fondamentale per la creazione di reti moderne. Fornisce i meccanismi necessari per costruire infrastrutture non solo più performanti, ma anche intrinsecamente più sicure, flessibili e gestibili, rispondendo alle crescenti esigenze di sicurezza e organizzazione delle aziende contemporanee.

Studente
Caccamo Rocco Paolo

Data
28/11/2025