UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria Informatica e dell'Automazione

TESI DI LAUREA

Progettazione e ottimizzazione di reti dinamiche: Sfide, Soluzioni e Analisi dati

Dynamic Network Design and Optimization: Challenges, Solutions and Data Analysis

Relatore

Prof. Ennio Gambi

Correlatore

Ing. Adelmo De Santis

Candidato

Danilo La Palombara

ANNO ACCADEMICO 2022-2023

“Un tempo esistevano domande per le quali non c'erano risposte. Oggi, all'epoca dei computer, ci sono molte risposte per le quali non abbiamo ancora pensato alle domande.”

Peter Ustinov

INDICE

INTRODUZIONE

Nell'era moderna del digitale, le reti di comunicazione giocano un ruolo fondamentale nel connettere dispositivi e trasmettere dati efficacemente. Queste reti sono infrastrutture essenziali che collegano individui, aziende e istituzioni in tutto il mondo. La loro progettazione e implementazione possono variare da semplici configurazioni domestiche a complesse architetture di reti aziendali o di provider di servizi internet, diventando elementi chiave per assicurare connettività affidabile e condivisione di risorse.

La creazione di una topologia di rete complessa, che può includere numerosi dispositivi, collegamenti e nodi, richiede una pianificazione meticolosa. Gli esperti di rete devono tenere in considerazione diversi aspetti come la scalabilità, l'affidabilità, la sicurezza e le specifiche esigenze degli utenti o dell'organizzazione. Progettare reti complesse è spesso una sfida che necessita di avanzate competenze tecniche e una profonda comprensione dei protocolli di rete, dell'architettura e delle necessità degli utenti finali.

Una volta implementata, il monitoraggio dinamico di una rete complessa diventa un elemento critico. L'analisi delle prestazioni, la sicurezza e l'ottimizzazione sono processi continui che assicurano un funzionamento corretto ed efficiente della rete, permettendo una rapida identificazione e risoluzione delle problematiche. Questo monitoraggio implica l'uso di strumenti e tecnologie specializzati per raccogliere dati in tempo reale sulla rete, analizzarli e prendere misure correttive se necessario.

Nel campo delle telecomunicazioni e delle tecnologie dell'informazione, la progettazione e il monitoraggio delle reti sono cruciali per offrire servizi di qualità e supportare l'aumento delle esigenze di connettività. L'evoluzione continua delle tecnologie di rete e l'aumento delle minacce alla sicurezza informatica rendono questo settore un terreno fertile per innovazioni e progressi costanti.

Nel contesto di questo progetto, la topologia di rete è stata inizialmente creata collegando fisicamente cavi di rete tra cinque router e due switch prodotti da Huawei. È importante sottolineare che l'interconnessione di dispositivi fisici è solo il primo passo nella creazione di una rete funzionante. L'elemento critico di questa implementazione è la configurazione avanzata dei dispositivi, che permette di realizzare la topologia logica

desiderata. In questo capitolo, esploriamo in dettaglio la progettazione di questa topologia complessa, mettendo in luce le sfide tecniche incontrate e le decisioni fondamentali prese durante il processo di implementazione. Verrà anche esaminato il software di gestione dinamica utilizzato per monitorare e ottimizzare la rete, un aspetto vitale per garantire efficienza e sicurezza in un ambiente di rete sempre più complesso e interconnesso. Questa attenta gestione e configurazione rappresentano la chiave per il successo di una rete moderna, efficiente e sicura.

ANALISI DEL PROGETTO

1.1 Obiettivo della tesi

L'obiettivo principale di questa tesi è descrivere il processo di progettazione, configurazione e monitoraggio della rete che ha portato alla realizzazione di una topologia in grado di adattarsi dinamicamente alle condizioni di traffico, mettendo in luce le sfide tecniche affrontate e le decisioni prese durante il percorso di implementazione. Inoltre, verrà valutata l'efficacia di questa topologia di rete nell'ottenere gli obiettivi prestabiliti in termini di prestazioni, affidabilità e sicurezza delle comunicazioni.

Un aspetto fondamentale che sarà trattato riguarda le problematiche incontrate, fornendo un'analisi dettagliata dei vari ostacoli e delle soluzioni adottate. In aggiunta, la tesi si dedicherà anche allo studio del Data collecting, esaminando come la raccolta e l'analisi dei dati siano state gestite per ottimizzare la performance della rete e per garantire una risposta efficace ai diversi scenari operativi. Questa sezione mira a fornire una visione completa di come le tecniche di raccolta dati influenzino direttamente la gestione e l'efficienza di una rete in un contesto dinamico e in continuo cambiamento.

1.1.1 Software di gestione dinamica

Per migliorare le prestazioni della rete, è stato sviluppato un software di visualizzazione utilizzando il linguaggio di programmazione Python. Questo software è specificamente progettato per monitorare le interfacce dei router Huawei considerati nel progetto. È in

grado di interagire con i dispositivi di rete e, all'occorrenza, di ottimizzare la distribuzione del traffico di rete tra le diverse interfacce o porte dei router.

La tesi sarà suddivisa in varie sezioni, ciascuna dedicata all'esplorazione di aspetti particolari legati alla progettazione, all'implementazione della rete e allo sviluppo del software di gestione dinamica. Si effettuerà un'analisi approfondita dei protocolli di comunicazione impiegati, nonché delle procedure di monitoraggio e manutenzione indispensabili per assicurare una performance ottimale della rete.

In aggiunta, un aspetto di grande rilievo che verrà esaminato in maniera dettagliata è rappresentato dalle problematiche incontrate nel corso del progetto. Questa analisi includerà le sfide tecniche, le limitazioni dei dispositivi e del software utilizzato, e come queste difficoltà siano state affrontate e superate. L'intento è fornire una visione completa e realistica del processo di sviluppo, evidenziando non solo i successi, ma anche gli ostacoli che sono stati parte integrante del percorso di realizzazione della rete. Questo approccio mira a offrire un quadro chiaro delle dinamiche di lavoro e delle soluzioni ingegneristiche adottate per raggiungere gli obiettivi prefissati.

1.2 Progetto

In questa sezione, verrà presentato il progetto di implementazione della topologia di rete complessa e del software di gestione dinamica. Saranno discussi gli obiettivi specifici del progetto, le fasi di sviluppo, e le tecnologie utilizzate.

1.2.1 Fasi di sviluppo

Il progetto è stato suddiviso in diverse fasi, tra cui:

1. Progettazione della topologia di rete fisica, inclusa la scelta dei dispositivi Huawei.

2. Configurazione iniziale dei dispositivi e interconnessione fisica.

3. Implementazione delle regole di routing e delle politiche di sicurezza.

4. Sviluppo del software di gestione dinamica.

5. Test e validazione delle funzionalità di monitoraggio e ottimizzazione.

6. Analisi dei dati raccolti e valutazione delle prestazioni.

Queste fasi di sviluppo rappresentano effettivamente anche quali sono gli obiettivi del progetto.

1.2.2 Configurazione fisica

Nella fase iniziale del progetto, è stata implementata la configurazione fisica della rete utilizzando il simulatore di dispositivi Huawei eNSP. Nella figura 3.5 è mostrata la topologia fisica dei dispositivi di rete:

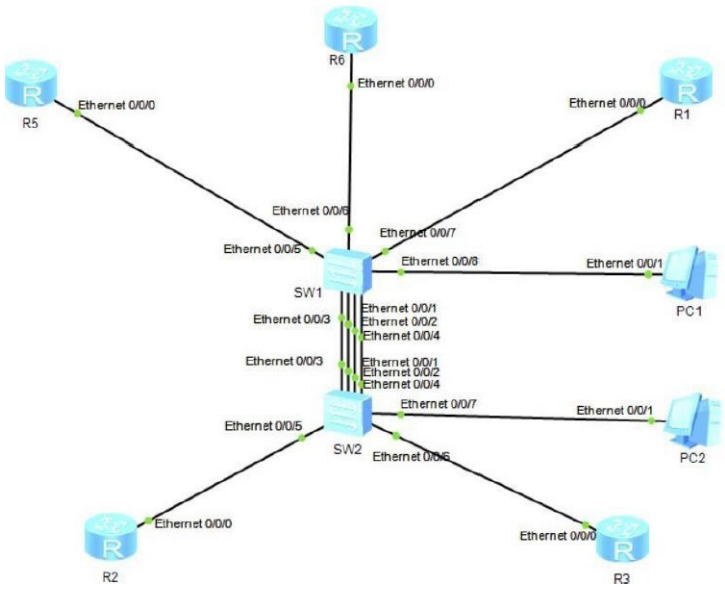

Figura 1.1: Configurazione fisica della rete

Come illustrato nella figura 1.1, i router R1, R5 e R6 sono connessi allo switch SW1, mentre i router R2 e R3 sono connessi allo switch SW2. Questa configurazione fisica costituisce la base sulla quale è stata implementata la topologia logica desiderata.

1.2.3 Configurazione logica

La topologia logica in figura1.2 è stata ottenuta attraverso la configurazione di apparati di rete, utilizzando una serie di tecniche, proprie di un approccio enterprise:

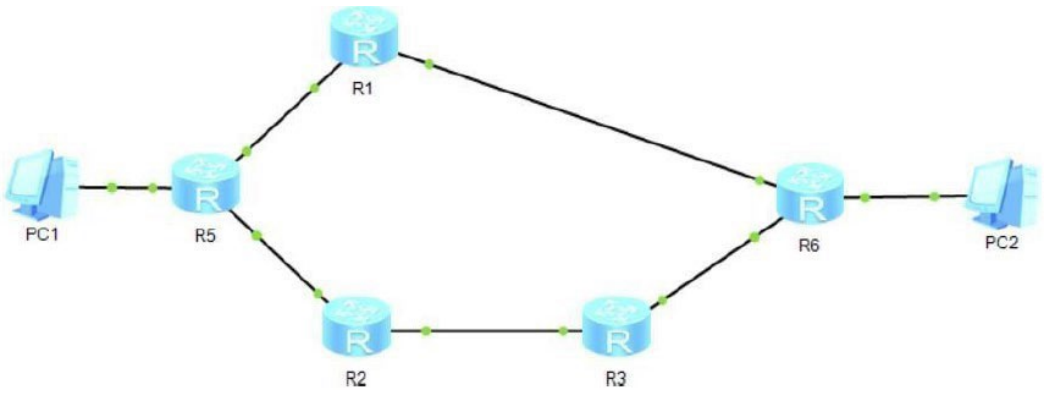

Figura 1.2: Configurazione logica desiderata della rete

1.2.4 Implementazione software

In questa parte della tesi, si approfondirà la parte relativa all'implementazione del software progettato per gestire e ottimizzare il flusso di traffico sui router R5 e R6, nonché per monitorare altri dispositivi come R1, R2 ed R3. Il software si distingue per la sua interfaccia grafica intuitiva, che rende facile per gli utenti selezionare e controllare il router di loro interesse. Qui forniremo una panoramica delle caratteristiche principali e delle funzionalità offerte dal software.

La comunicazione tra il software, sviluppato in Python, ed i dispositivi di rete avviene attraverso il protocollo SSH (Secure Shell). In questa configurazione, tutti i router agiscono come server SSH, permettendo al software di instaurare connessioni sicure con

questi dispositivi. Il PC dell'utente opera come client SSH e interagisce con i router tramite una connessione wireless, rendendo superfluo l'uso di cavi di rete fisici.

Per quanto riguarda l'interfaccia grafica, il software è equipaggiato con una GUI (Graphical User Interface) user-friendly. Tramite questa interfaccia, gli utenti possono decidere se vogliono gestire il traffico su R5 o R6.

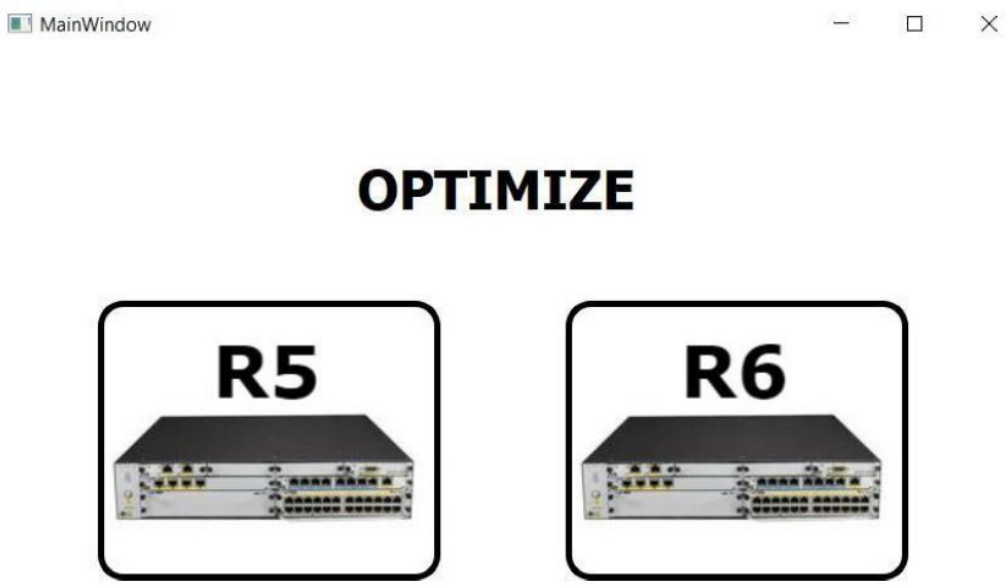

Figura 1.3: Interfaccia introduttiva del software

La gestione avanzata del traffico del software progettato permette di supervisionare e regolare il flusso di traffico nelle interfacce specifiche dei router R5 e R6. Questa funzione opera attraverso verifiche regolari, effettuate a intervalli prestabiliti, focalizzandosi sulle interfacce 0/0/0 e 0/0/1. Qualora il software rilevi che l'uso di una di queste interfacce superi una determinata soglia critica, viene attivato un meccanismo automatico. Tale meccanismo lancia uno script che reindirizza il traffico in arrivo verso un percorso alternativo, utilizzando rotte statiche. Questo processo assicura una distribuzione più efficiente del carico di rete, evitando sovraccarichi e congestioni.

Il monitoraggio dello stato delle interfacce è un altro aspetto chiave del software e la sua funzionalità permette agli utenti di osservare in tempo reale lo stato operativo delle interfacce di tutti i router coinvolti. Attraverso questa funzione, è possibile identificare immediatamente eventuali anomalie, interruzioni o problemi di connessione che possono influenzare la performance della rete. Questo monitoraggio continuo è essenziale per mantenere l'integrità e l'efficienza della rete.

CAPITOLO 2

TECNOLOGIE UTILIZZATE

In questo capitolo, esporremo le tecnologie chiave che hanno supportato il nostro progetto, organizzando la discussione in tre sezioni ben distinte per una maggiore chiarezza.

1. Hardware: La prima sezione si concentrerà sull'hardware. Discuteremo i dispositivi come router e switch, esplorando le loro specifiche tecniche e il ruolo che hanno avuto nella costruzione della nostra rete. Questo ci permetterà di capire come la scelta dell'hardware influenzi direttamente le prestazioni e l'efficienza della rete.

2. Sviluppo della Topologia di Rete: Nella seconda sezione, passeremo alle tecnologie utilizzate per sviluppare la topologia della rete. Analizzeremo i software e i protocolli impiegati, mostrando come questi abbiano contribuito a progettare e configurare la rete in modo efficace.

3. Software di Gestione: Infine, la terza sezione tratterà le tecnologie impiegate nello sviluppo del software di gestione. Questa parte si concentrerà sugli strumenti di programmazione e le librerie utilizzate, spiegando come queste scelte abbiano facilitato il monitoraggio e la gestione della rete.

Ogni sezione fornirà un'analisi approfondita, permettendo di comprendere come le diverse componenti tecnologiche siano state integrate per realizzare il progetto.

2.1 Hardware

2.1.1 Router

Nella topologia di rete progettata, sono stati selezionati router specifici in base alle loro funzionalità e prestazioni per ottimizzare la gestione del traffico. I router AR1220 sono stati implementati per i nodi 1, 2 e 3, mentre per i nodi più critici, i router 5 e 6, si è optato per i modelli AR2220.

I router AR1220, scelti per i primi tre nodi, sono noti per la loro affidabilità e per le prestazioni adeguate a scenari di rete di medie dimensioni. Questi dispositivi offrono una varietà di funzionalità di rete, inclusa la capacità di gestire connessioni VPN, QoS avanzata (Quality of Service) per la priorizzazione del traffico, e supporto per molteplici protocolli di routing.Per i router 5 e 6, critici per la topologia data la loro posizione e il ruolo nel network, si è scelto di adottare i modelli AR2220. Questi router offrono capacità superiori rispetto agli AR1220, con prestazioni migliorate, maggior capacità di throughput e opzioni di configurazione più avanzate. Questi aspetti li rendono particolarmente adatti per gestire volumi di traffico più elevati e per fornire servizi di rete più complessi, come la virtualizzazione e servizi integrati di sicurezza.

L'adozione di questi due tipi di router nella topologia ha permesso di creare una rete bilanciata, dove i dispositivi sono stati scelti e posizionati strategicamente per massimizzare l'efficienza operativa e la resilienza della rete, assicurando al contempo una gestione ottimale del traffico e delle risorse.

2.1.2 Switch

Nella configurazione della rete del progetto, sono stati utilizzati due switch Huawei S5700. Questi switch hanno avuto un ruolo fondamentale nell'organizzazione del traffico e nella gestione delle VLAN, assicurando una comunicazione fluida tra i diversi segmenti di rete. Le principali configurazioni degli switch S5700 hanno incluso l'assegnazione di porte specifiche a determinate VLAN, l'implementazione di porte trunk per il traffico multiplo di VLAN, e la configurazione del Quality of Service (QoS) per prioritizzare il traffico critico. Inoltre, sono state adottate misure di sicurezza come gli elenchi di controllo di accesso (ACL) per proteggere la rete.

2.2 Tecnologie di rete

2.2.1 eNSP

Una tecnologia fondamentale per la progettazione e l'implementazione della topologia di rete è stata l'impiego di eNSP, acronimo di "Emulated Network Simulation Platform". Questo simulatore di dispositivi Huawei ha permesso la creazione e il test della topologia di rete in un ambiente virtuale prima della sua effettiva implementazione fisica. Grazie a eNSP, è stato possibile:

- Realizzare una rappresentazione virtuale dei dispositivi Huawei, come router e switch, che sarebbero stati impiegati nella rete reale.

- Simulare l'interconnessione di questi dispositivi mediante cavi di rete virtuali, agevolando la pianificazione e la configurazione della topologia fisica.

eNSP si è rivelato uno strumento estremamente utile nel processo di progettazione, consentendo l'esplorazione di diverse configurazioni e la valutazione preliminare del funzionamento della topologia. La sua capacità di simulare scenari realistici ha facilitato l'affinamento della progettazione, assicurando che la topologia finale rispondesse efficacemente agli obiettivi di prestazioni e affidabilità.

2.2.2 OSPF

Nella topologia di rete elaborata, è stato adottato OSPF, acronimo di “Open Shortest Path First”, come protocollo di routing principale. La scelta di OSPF è stata motivata dalla sua efficacia nel gestire le tabelle di routing in modo dinamico, permettendo di ottimizzare il routing dei pacchetti dati attraverso la sua specifica metrica. Grazie a OSPF, è stato possibile configurare i router per scambiarsi informazioni sulle rotte di rete e determinare il percorso più efficiente per il trasferimento dei dati.

2.2.3 VLAN

Le VLAN, abbreviazione di "Virtual LAN", sono state impiegate per segmentare e isolare il traffico di rete in più sottoinsiemi logici. Questo approccio ha permesso di dividere una singola rete fisica in più gruppi logici. Una caratteristica importante delle VLAN è l'uso dei tag VLAN, che sono etichette assegnate ai pacchetti di dati per identificare a quale VLAN appartengono. Questi tag consentono ai switch di rete di dirigere il traffico in modo appropriato, assicurando che i dati vengano trasmessi solo all'interno del loro segmento VLAN specifico, migliorando così la sicurezza e l'efficienza della rete.

2.2.4 Sub-Interface

Nella configurazione di reti avanzate, in particolare quelle che impiegano diverse VLAN (Virtual LAN), le sub-interface svolgono un ruolo fondamentale. Queste permettono di suddividere le interfacce fisiche dei router in più sotto-interfacce virtuali, ciascuna con una configurazione di rete distinta, inclusi indirizzo IP e netmask. L'utilizzo strategico delle sotto-interfacce è cruciale per convertire una struttura fisica di rete in una configurazione logica e per gestire efficacemente il traffico VLAN.

2.2.5 DHCP

Per facilitare la gestione degli indirizzi IP nella rete, è stato adottato il protocollo DHCP, acronimo di “Dynamic Host Configuration Protocol”. Questo protocollo permette a un dispositivo designato come "dhcp server" di distribuire automaticamente indirizzi IP ai client che ne fanno richiesta. Tale approccio migliora l'efficienza nell'utilizzo degli indirizzi IP e contribuisce a prevenire conflitti di indirizzamento.

2.2.6 Link Aggregation

Il Link Aggregation consente l'unione di più collegamenti fisici di rete in un singolo link logico. Questo approccio non solo aumenta la capacità di banda complessiva tra i dispositivi, come router e switch, ma contribuisce anche a un più efficace bilanciamento

del carico. Distribuendo il traffico su più collegamenti, il sistema minimizza il rischio di congestione, garantendo prestazioni di rete ottimali. Un altro aspetto cruciale del Link Aggregation è il miglioramento della ridondanza. In caso di guasto di un collegamento fisico, il traffico viene automaticamente reindirizzato su un altro collegamento all'interno del gruppo aggregato, mantenendo così la continuità delle operazioni di rete senza interruzioni per l'utente finale.

2.3 Software di gestione della rete

2.3.1 Python

Python si afferma come linguaggio di programmazione di primaria importanza, caratterizzato da un'ampia popolarità ed una notevole versatilità, che ne hanno favorito l'adozione in un vasto spettro di applicazioni software, tra cui spicca la gestione del traffico di rete. La predilezione per Python in contesti di networking si radica in molteplici fattori distintivi:

- Leggibilità e Semplicità Sintattica: La sintassi di Python, notoriamente intuitiva e di facile comprensione, facilita la scrittura di codice trasparente e facilmente interpretabile, aspetto di cruciale importanza nello sviluppo di sistemi per la gestione di reti, dove la precisione e la chiarezza sono essenziali per prevenire disfunzioni e malfunzionamenti onerosi.

- Ricchezza dell'Ecosistema e Supporto Comunitario: La vasta comunità di sviluppatori che circonda Python contribuisce a un ecosistema dinamico di librerie e framework, in particolare per il networking, arricchendo le risorse disponibili per l'elaborazione di soluzioni avanzate nella gestione del traffico di rete.

- Portabilità Interpiattaforma: La natura multipiattaforma di Python garantisce l'esecuzione di applicazioni su svariati sistemi operativi senza necessità di modifiche sostanziali, vantaggio non trascurabile nella gestione di infrastrutture di rete eterogenee.

- Efficienza nello Sviluppo: Python è rinomato per la sua capacità di facilitare uno sviluppo agile e veloce, consentendo agli sviluppatori di redigere, testare e perfezionare

il codice con celerità, accelerando così l'implementazione di nuove funzionalità e la risoluzione di problematiche.

- Prevalenza nell'Automazione di Rete: Python trova vasta applicazione nell'automazione di rete, avvalendosi di librerie specializzate quali Paramiko, Netmiko e Scapy, che agevolano la gestione e la configurazione di dispositivi di rete, oltre alla manipolazione di flussi di traffico.

- Librerie Specializzate per il Networking: Il linguaggio mette a disposizione un insieme di librerie dedicate al networking, come Scapy, NetworkX e Twisted, che abilitano un'analisi e una gestione efficaci del traffico di rete.

L'impiego di Python come strumento predominante nella programmazione di software dedicato all'ottimizzazione del traffico di rete ha reso possibile l'exploit di queste peculiarità, facilitando l'implementazione di meccanismi sofisticati per il monitoraggio e l'ottimizzazione dinamica del traffico di rete, grazie alla flessibilità offerta dal linguaggio e all'ampio ventaglio di risorse specialistiche nel campo del networking.

2.3.2 Netmiko

La libreria Netmiko, sviluppata in Python per facilitare la comunicazione con dispositivi di rete mediante protocollo SSH, ha svolto un ruolo determinante. La sua implementazione ha consentito l'instaurazione di connessioni sicure con i dispositivi router R5 e R6, risultando indispensabile per le operazioni di monitoraggio e ottimizzazione del flusso di traffico di rete. Netmiko si è distinta per la sua capacità di offrire un'interfaccia semplificata per l'esecuzione di compiti quali l'autenticazione, la gestione delle sessioni SSH, la configurazione dei dispositivi e l'acquisizione di dati di rete, evidenziando la sua compatibilità con una vasta gamma di dispositivi di rete, tra cui i router Huawei integrati nell'infrastruttura del progetto.

La funzionalità di automazione fornita da Netmiko ha permesso di effettuare invii di comandi e raccolte di dati in tempo reale, facilitando l'analisi delle prestazioni di rete e l'identificazione di potenziali miglioramenti nelle strategie di routing e sicurezza. In conclusione, l'adozione di Netmiko ha rappresentato un elemento cardine per la

realizzazione di una gestione efficace e sicura dei dispositivi di rete, contribuendo in maniera significativa agli obiettivi di ottimizzazione del traffico delineati in questo studio.

2.3.3 Qt Designer

Nel corso dello sviluppo del presente progetto, si è fatto ricorso a Qt Designer, un'applicazione avanzata per la progettazione di interfacce utente (UI), integrata nel framework Qt. Quest'ultimo, noto per la sua capacità di supportare lo sviluppo di applicazioni cross-platform sia desktop che mobile e embedded, ha offerto una base solida per la realizzazione del software in questione. Qt Designer si è distinto per la sua interfaccia visuale intuitiva, che ha permesso la creazione di UI complesse senza la necessità di codifica manuale. Attraverso un approccio "drag-and-drop" per l'inserimento e la configurazione di elementi UI come pulsanti, caselle di testo e menu, ha semplificato notevolmente il processo di design, rendendo l'interfaccia utente del software non solo funzionale ma anche esteticamente gradevole.

L'impiego di Qt Designer ha avuto un ruolo cruciale nella progettazione di un'interfaccia grafica che rispondesse alle esigenze di usabilità e accessibilità, fondamentali per l'efficacia del software. La UI risultante ha garantito agli utenti finali un'interazione chiara e diretta con le funzionalità del software, specialmente per quanto riguarda le operazioni di monitoraggio e ottimizzazione del traffico di rete, senza richiedere competenze tecniche avanzate.

2.3.4 Iperf

Iperf è uno strumento avanzato per l'analisi delle prestazioni di rete che ha rivestito un ruolo centrale nello sviluppo del software di ottimizzazione del traffico. Funzionando in modalità client/server, Iperf ha abilitato la generazione mirata di traffico di rete, facilitando l'analisi dettagliata delle prestazioni sotto vari scenari di carico. Questo strumento si distingue per la sua versatilità, permettendo agli utenti di scegliere tra protocolli quali TCP e UDP per adattarsi alle specifiche esigenze di test. La precisione nelle misurazioni di parametri critici come larghezza di banda, latenza e perdita di

pacchetti ha reso Iperf indispensabile per valutare l'effetto delle strategie di ottimizzazione adottate.

L'impiego di Iperf ha consentito una valutazione quantitativa dell'efficacia delle ottimizzazioni, oltre a identificare aree di potenziale miglioramento. La capacità di configurare dettagliatamente i test ha garantito la simulazione di condizioni di traffico reali, migliorando la comprensione del comportamento della rete sotto diverse condizioni operative. La semplicità d'uso di Iperf, unita alla sua potente configurabilità, ne ha fatto uno strumento fondamentale nella fase di testing. Questa combinazione ha permesso una rapida adattabilità dei test alle specifiche esigenze, rendendo Iperf un pilastro nella valutazione delle prestazioni della rete e nella simulazione di una vasta gamma di scenari di traffico. Grazie a Iperf, le soluzioni implementate sono state rigorosamente testate, assicurando robustezza e affidabilità nel contesto dinamico della gestione del traffico di rete.

SVILUPPO DEL PROGETTO

In questa sezione, si esploreranno le varie tappe e le operazioni intraprese nella realizzazione della struttura di rete e del sistema software per la gestione attiva del traffico. La discussione si articolerà attorno alle metodologie adottate e alle sequenze operative impiegate per configurare l'architettura di rete e sviluppare il software correlato.

3.1 Topologia

La realizzazione della rete di comunicazione ha richiesto l'adozione di una metodologia di progettazione sofisticata, iniziando con uno studio dettagliato della struttura topologica fisica.

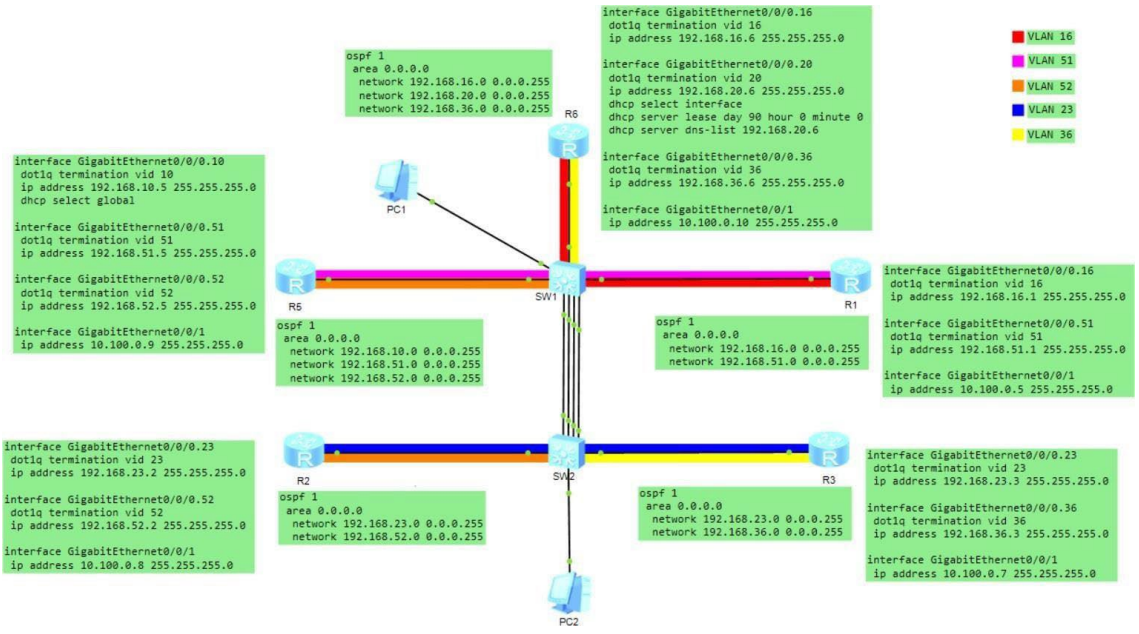

Figura 3.1: Configurazione fisica della rete ottenuta con eNSP

Nella fase introduttiva del progetto, ho elaborato un concetto di base per il funzionamento della rete, esplorando le possibili tecnologie e strumenti per realizzare gli obiettivi stabiliti. Questo primo passo ha comportato l'analisi delle richieste di rete e la creazione

di una topologia che potesse rispondere efficacemente a tali requisiti. Da lì, ho proceduto a tradurre questa idea iniziale in un'implementazione tangibile, occupandomi direttamente della configurazione dei dispositivi di rete.

Il passaggio dal concettuale al pratico ha coinvolto la messa in atto delle configurazioni previste sui dispositivi e l'introduzione delle tecnologie selezionate. Questo percorso ha necessitato una conoscenza approfondita delle soluzioni di rete e del loro impiego strategico, insieme a una pianificazione e configurazione accurate per assicurare che la topologia di rete funzionasse secondo le aspettative.

3.1.1 Configurazione VLAN e Sub-Interfaces

L'analisi della topologia di rete ha rivelato la definizione di cinque VLAN distinte (VLAN 16, 36, 52, 51 e 23), implementate per facilitare la connettività diretta tra router specifici. Ogni VLAN è stata configurata su una sub-interface distinta dell'interfaccia 0/0/0 su ciascun router, come illustrato nella Tabella 3.1, che dettaglia l'assegnazione delle sub-interfaces ai rispettivi router: R6 con le sub-interfaces 0/0/0.16 e 0/0/0.36, R5 con le sub-interfaces 0/0/0.51 e 0/0/0.52, e così via per R1, R2 e R3.

Router	Sub-Interface 1	Sub-Interface 2
R6	0/0/0.16	0/0/0.36
R5	0/0/0.51	0/0/0.52
R1	0/0/0.16	0/0/0.51
R2	0/0/0.23	0/0/0.52
R3	0/0/0.23	0/0/0.36

Figura 3.2: Assegnazione sub-interface ai router

Questa divisione assicura che ogni router stabilisca comunicazioni selettive con altri router, tramite il trasferimento di frame taggati, garantendo così la segregazione e l'efficienza del traffico di rete. In aggiunta, sono state configurate due ulteriori VLAN, la 20 e la 10, con lo scopo di simulare connessioni dirette tra i PC e i router. Questa configurazione si basa su collegamenti fisici dei PC agli switch 1 e 2, rappresentando la

loro posizione logica esterna nella topologia di rete. Di conseguenza, il PC1 è logicamente connesso al router 5, mentre il PC2 al router 6, permettendo la comunicazione tra i due PC attraverso due percorsi distinti. Per il PC1, il percorso superiore transita esclusivamente attraverso il router 1, dove il frame proveniente dal PC1 viene incapsulato e taggato nella VLAN 10 mediante la terminazione dot1q sulla sub-interface del router 5, agendo come pvid, per poi essere inoltrato allo switch e successivamente al router 1, che lo dirige verso il router 6 destinato al PC2. In alternativa, il percorso inferiore prevede che i pacchetti vengano inoltrati prima al router 2, poi al router 3, e infine al router 6 per il routing finale verso il PC2. Questa dinamica è applicabile indipendentemente dalla direzione del traffico, sia che i pacchetti provengano dal PC1 che dal PC2.

3.1.2 Configurazione Switch

La configurazione degli switch rappresenta un aspetto fondamentale della struttura della rete, essendo questi dispositivi incaricati di interconnettere router e VLAN in maniera efficiente. Al fine di garantire una gestione ottimale del traffico di rete, sono state adottate due configurazioni principali per gli switch:

1. Modalità Access: Impiegata per assegnare i dispositivi collegati a una specifica VLAN. Le porte che collegano i router ai PC, ad esempio, sono state impostate in modalità access per assicurare che i pacchetti trasmessi e ricevuti su queste porte siano associati a un determinato tag VLAN.

2. Modalità Trunk: Utilizzata per abilitare il flusso di dati attraverso multiple VLAN. Le connessioni tra gli switch e i router sono state configurate in modalità trunk, permettendo così il transito di frame appartenenti a diverse VLAN.

```
interface GigabitEthernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 51 to 52
#
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk allow-pass vlan 16 36
#
interface GigabitEthernet0/0/7
 port link-type trunk
 port trunk allow-pass vlan 16 51
#
interface GigabitEthernet0/0/8
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10
#
```

Figura 3.3: Configurazione switch 1

```
interface GigabitEthernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 23 52
#
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk allow-pass vlan 23 36
#
interface GigabitEthernet0/0/7
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/8
 port link-type trunk
 port trunk pvid vlan 20
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 3.4: Configurazione switch 2

Le porte GigabitEthernet che collegano i PC sono state configurate come porte access, con lo scopo di consentire esclusivamente il transito di pacchetti marcati con i tag VLAN 10 e 20. È interessante notare come le prime quattro porte di ciascuno switch siano state impostate in modalità eth-trunk, facendo leva sulla tecnologia di link aggregation. Quest'ultima, migliora l'efficacia della rete combinando più connessioni fisiche in un

unico canale logico, incrementando così la larghezza di banda complessiva e la ridondanza della rete.

```
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 1
#
interface GigabitEthernet0/0/4
 eth-trunk 1
#
```

Figura 3.5: Configurazione link-aggregation

```
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 load-balance dst-ip
#
```

Figura 3.6: Configurazione porte Eth-Trunk

Per il progetto in questione, sono stati attivati tre dei quattro collegamenti tra gli switch 1 e 2, mantenendo il quarto come riserva per eventuali guasti. Questa strategia incrementa la robustezza della connessione tra gli switch, assicurando la continuità operativa della rete anche in presenza di guasti su uno dei canali primari. Inoltre, è stato implementato un meccanismo di load balancing sugli switch Huawei per distribuire equamente il traffico di rete tra le porte, ottimizzando così la gestione del carico e prevenendo congestioni in situazioni di elevato traffico.

3.1.3 Configurazione Router

Il protocollo OSPF è stato selezionato per orchestrare la gestione dinamica delle rotte all'interno della rete, consentendo un aggiustamento flessibile e tempestivo del percorso dei dati in risposta a variazioni delle condizioni di rete. Le configurazioni OSPF implementate sui router sono descritte di seguito:

```
R1:
ospf 1
area 0.0.0.0
network 192.168.16.0 0.0.0.255
network 192.168.20.0 0.0.0.255
network 192.168.36.0 0.0.0.255

R2:
ospf 1
area 0.0.0.0
network 192.168.23.0 0.0.0.255
network 192.168.36.0 0.0.0.255

R3:
ospf 1
area 0.0.0.0
network 192.168.23.0 0.0.0.255
network 192.168.36.0 0.0.0.255

R5:
ospf 1
area 0.0.0.0
network 192.168.23.0 0.0.0.255
network 192.168.52.0 0.0.0.255

R6:
ospf 1
area 0.0.0.0
network 192.168.10.0 0.0.0.255
network 192.168.51.0 0.0.0.255
network 192.168.52.0 0.0.0.255
```

Ciascuna sezione dettaglia la configurazione OSPF relativa a un determinato router, evidenziando le reti e le aree OSPF implicate. In questa struttura, ogni router è impostato

per operare nell'area OSPF 0.0.0.0, nota come area backbone. Quest'ultima riveste un ruolo fondamentale all'interno dell'architettura OSPF, poiché assicura la comunicazione tra le varie aree, fungendo da punto centrale per lo scambio di informazioni di routing tra router appartenenti ad aree differenti. La scelta di adottare un'unica area backbone per tutti i router mira a razionalizzare la configurazione e a conferire maggiore coerenza all'intera infrastruttura di rete, facilitando la gestione delle rotte e rendendo l'implementazione di OSPF più intuitiva e gestibile.

3.1.4 Comunicazione tra Router

La connettività tra i router rappresenta un pilastro della nostra architettura di rete, articolandosi in due scenari distinti, ciascuno con le proprie caratteristiche e meccanismi:

1. Connessione Diretta: Quando due router sono fisicamente connessi, la metrica di routing è impostata a zero, indicando questa via come la più affidabile. La trasmissione di dati tra questi dispositivi avviene in maniera diretta, senza necessità di protocolli di routing intermedi.

2. OSPF: Nei casi in cui i router non siano connessi direttamente, intervengono i meccanismi del protocollo OSPF. Questo protocollo di routing dinamico facilita lo scambio di informazioni sullo stato delle connessioni e calcola il percorso più efficiente per il traffico di rete. Grazie a OSPF, le tabelle di routing di ciascun router vengono popolate con le rotte ottimali, consentendo ai dispositivi di individuare il miglior percorso verso ogni destinazione.

Per analizzare in dettaglio l'interazione tra OSPF e le connessioni dirette, è utile esaminare le tabelle di routing dei router coinvolti. Di seguito, le tabelle di routing relative al Router 5 e al Router 6 per illustrare come questi dispositivi gestiscono la comunicazione interna alla rete:

```
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 20        Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.100.0.0/24  Direct  0    0           D   10.100.0.9      GigabitEthernet0/0/2
     10.100.0.9/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
   10.100.0.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  Direct  0    0           D   192.168.10.5    GigabitEthernet0/0/2.10
   192.168.10.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2.10
 192.168.10.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2.10
   192.168.16.0/24  OSPF    10   2           D   192.168.51.1    GigabitEthernet0/0/0
   192.168.20.0/24  OSPF    10   3           D   192.168.51.1    GigabitEthernet0/0/0
   192.168.23.0/24  OSPF    10   2           D   192.168.52.2    GigabitEthernet0/0/1
   192.168.36.0/24  OSPF    10   3           D   192.168.52.2    GigabitEthernet0/0/1
                    OSPF    10   3           D   192.168.51.1    GigabitEthernet0/0/0
   192.168.51.0/24  Direct  0    0           D   192.168.51.5    GigabitEthernet0/0/0
   192.168.51.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
 192.168.51.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
   192.168.52.0/24  Direct  0    0           D   192.168.52.5    GigabitEthernet0/0/1
   192.168.52.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
 192.168.52.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 3.7: Tabella di routing del Router 5

```
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 20        Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.100.0.0/24  Direct  0    0           D   10.100.0.10     GigabitEthernet0/0/2
    10.100.0.10/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
   10.100.0.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  OSPF    10   3           D   192.168.16.1    GigabitEthernet0/0/0
   192.168.16.0/24  Direct  0    0           D   192.168.16.6    GigabitEthernet0/0/0
   192.168.16.6/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
 192.168.16.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
   192.168.20.0/24  Direct  0    0           D   192.168.20.6    GigabitEthernet0/0/2.20
   192.168.20.6/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2.20
 192.168.20.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2.20
   192.168.23.0/24  OSPF    10   2           D   192.168.36.3    GigabitEthernet0/0/1
   192.168.36.0/24  Direct  0    0           D   192.168.36.6    GigabitEthernet0/0/1
   192.168.36.6/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
 192.168.36.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
   192.168.51.0/24  OSPF    10   2           D   192.168.16.1    GigabitEthernet0/0/0
   192.168.52.0/24  OSPF    10   3           D   192.168.36.3    GigabitEthernet0/0/1
                    OSPF    10   3           D   192.168.16.1    GigabitEthernet0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 3.8: Tabella di routing del Router 6

Le tabelle di routing rappresentano elementi chiave per interpretare le decisioni dei router riguardo al percorso più efficiente per il trasferimento dei dati attraverso le reti. L'analisi di queste tabelle fornisce una visione chiara dell'importanza di OSPF nel determinare le rotte e dell'impatto delle connessioni dirette sulle scelte di routing. Nel caso specifico del

Router 5, le reti con indirizzi 192.168.16.0/24, 192.168.20.0/24, 192.168.23.0/24 e 192.168.36.0/24 sono accessibili tramite le rotte stabilite da OSPF. D'altro canto, il Router 6 gestisce le rotte OSPF per accedere alle reti 192.168.10.0/24, 192.168.23.0/24, 192.168.51.0/24 e 192.168.52.0/24. Le rotte rimanenti, caratterizzate da un costo nullo, si basano su collegamenti diretti, riflettendo la natura immediata e senza intermediari di queste connessioni.

3.1.5 Configurazione DHCP

L'implementazione del DHCP è stata adottata per facilitare l'assegnazione e la gestione degli indirizzi IP nella rete, ricorrendo a due approcci distinti per i router R5 e R6. Le configurazioni DHCP adottate per questi dispositivi sono dettagliate di seguito:

```
R5:
ip pool poolR5
gateway-list 192.168.10.5
network 192.168.10.0 mask 255.255.255.0
lease day 90 hour 0 minute 0
dns-list 192.168.10.5
interface GigabitEthernet0/0/0.10
dot1q termination vid 10
ip address 192.168.10.5 255.255.255.0
dhcp select global
```

```
R6:
interface GigabitEthernet0/0/0.20
dot1q termination vid 20
ip address 192.168.20.6 255.255.255.0
dhcp select interface
dhcp server lease day 90 hour 0 minute 0
dhcp server dns-list 192.168.20.6
```

È rilevante sottolineare che il router R5 adotta la strategia 'dhcp select global', configurando così un servizio DHCP unificato per l'intero dispositivo, che distribuisce indirizzi IP da un unico insieme globale. In contrasto, R6 impiega il metodo 'dhcp select interface', dove ciascuna interfaccia DHCP si occupa autonomamente di assegnare indirizzi IP ai dispositivi connessi direttamente ad essa. La decisione su quale delle due

opzioni utilizzare si basa sulle necessità specifiche dell'infrastruttura di rete e sulla politica di gestione degli indirizzi IP adottata.

3.1.6 Configurazione logica

Grazie all'architettura definita e alle soluzioni tecnologiche adottate, la rete opera seguendo principi logici e coerenti, che includono gli aspetti fondamentali precedentemente discussi. In particolare, la comunicazione tra il Router 5 e il Router 6 può avvenire attraverso due percorsi distinti. Il percorso superiore, come già anticipato, è generalmente preferito per il suo minor costo, permettendo ai pacchetti di passare attraverso un solo router e minimizzando così la latenza, il che si traduce in un incremento dell'efficienza. Al contrario, il percorso inferiore prevede il passaggio attraverso due router, risultando in un costo più elevato e in una latenza leggermente maggiore.

La figura sottostante illustra la struttura logica della rete, evidenziando le scelte di routing effettuate dai router in base alle rotte a loro disposizione:

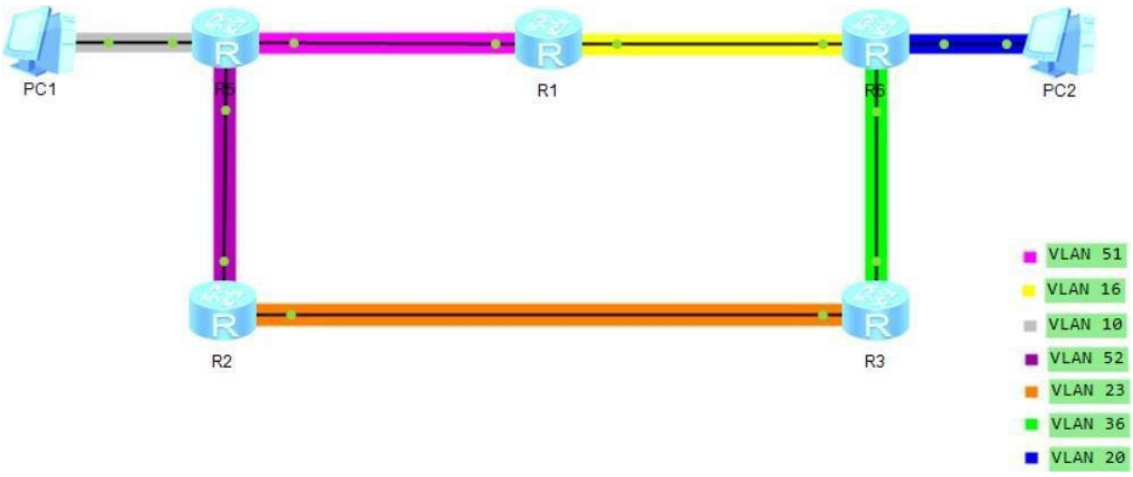

Figura 3.9: Configurazione logica

La visualizzazione grafica della struttura logica della rete fornisce un quadro dettagliato del processo di instradamento del traffico tra i router e le varie reti. La capacità di selezionare tra itinerari alternativi, come i percorsi superiore e inferiore tra il Router 5 e

il Router 6, sottolinea il ruolo cruciale delle strategie di routing nel migliorare le prestazioni della rete. È essenziale riconoscere che la configurazione logica incarna l'interazione complessa tra i protocolli di routing, le connessioni dirette e la disposizione fisica della rete, creando un'infrastruttura capace di gestire le richieste di comunicazione in modo efficiente e affidabile. La presenza di molteplici percorsi aggiunge un livello di flessibilità, permettendo alla rete di adattarsi a cambiamenti o a potenziali guasti, assicurando così la continuità operativa.

Al centro del software di monitoraggio e gestione della rete che ho sviluppato vi è il principio della doppia rotta. Questo applicativo consente di utilizzare entrambi i percorsi disponibili per dirigere il traffico attraverso la struttura di rete, offrendo agli amministratori la possibilità di ottimizzare le comunicazioni adattando dinamicamente la scelta delle rotte alle necessità momentanee. Ad esempio, in situazioni di congestione su un percorso, il software può reindirizzare il traffico lungo un'alternativa, mantenendo così un flusso di dati costante e senza interruzioni. Questa capacità di manovra fornisce un controllo avanzato sulle rotte OSPF, consentendo un'affinata ottimizzazione del traffico in funzione delle condizioni di rete e delle specifiche esigenze operative.

3.2 Sviluppo Software

Il software integra una serie di requisiti funzionali chiave, tra cui la selezione di specifici router per l'esame delle statistiche di utilizzo e la visualizzazione dello stato delle interfacce lungo i determinati percorsi di instradamento. Questi requisiti sono stati definiti per garantire che gli utenti possano accedere facilmente ad informazioni critiche e gestire in modo proattivo le configurazioni di rete. La figura sottostante illustra il layout e la disposizione degli elementi in questa schermata:

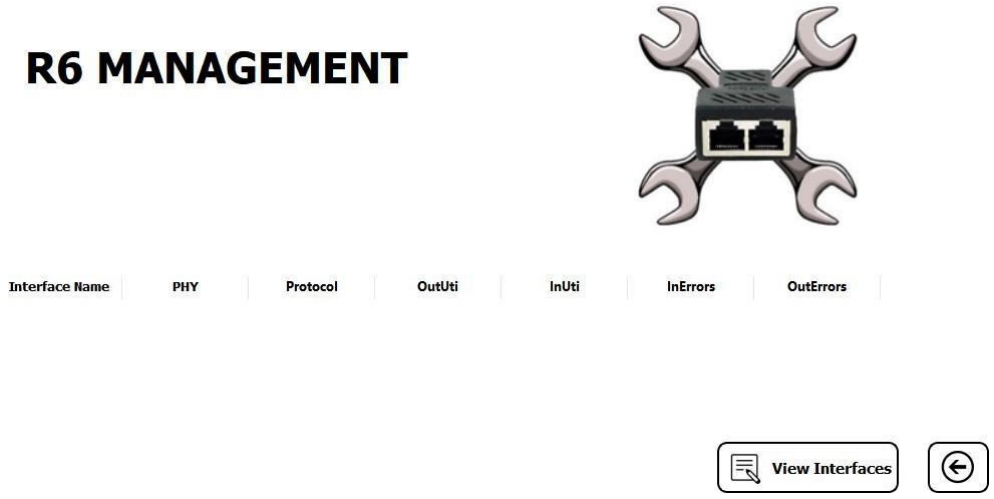

Figura 3.10: Schermata di controllo del router R6

Gli elementi principali dell'interfaccia includono:

1. Etichetta Router Management: una QLabel che varia dinamicamente per riflettere il router selezionato dall'utente, visualizzando "R6 Management" o "R5 Management". Questo fornisce un feedback immediato sull'oggetto della gestione corrente.

2. Immagine del Router: integrata in un QFrame, questa immagine statica arricchisce l'interfaccia utente, rendendo la schermata più accattivante e fornendo un contesto visuale.

3. Tabella delle Statistiche (QTableWidget): questo componente centrale esibisce dettagliatamente le statistiche operative delle interfacce del router selezionato, attraverso colonne dedicate come:

- Interface Name: Mostra l'identificativo dell'interfaccia, es. 0/0/0 o 0/0/1.
- PHY: Indica lo stato fisico dell'interfaccia, che può essere "up" o "down".
- Protocol: Riflette lo stato del protocollo a livello di collegamento dell'interfaccia.
- OutUti e InUti: Presentano l'utilizzo medio della larghezza di banda in uscita e in entrata, rispettivamente.
- InErrors e OutErrors: Conteggiano i pacchetti di errore ricevuti e inviati dall'interfaccia.

4. Bottoni di Navigazione: posizionati strategicamente, questi bottoni consentono all'utente di navigare facilmente all'interno dell'applicazione, sia per ritornare alla vista precedente sia per avanzare verso la schermata di dettaglio delle interfacce di altri router come R1, R2, R3.

Dal punto di vista tecnico, il software sfrutta requisiti non funzionali come la connessione via protocollo SSH per l'acquisizione di dati di rete, e la capacità di adattare le rotte di traffico in base all'analisi delle condizioni di utilizzo delle interfacce. Queste caratteristiche sottolineano l'approccio flessibile e orientato alla performance adottato nello sviluppo dell'applicazione.

L'architettura del software si basa sul modello Model-View-Controller (MVC), che facilita una chiara separazione delle responsabilità tra la gestione dei dati di rete (Model), la presentazione delle informazioni all'utente (View) e il controllo delle interazioni e delle operazioni (Controller). Attraverso l'utilizzo di classi specifiche come InterfaceObj per la rappresentazione delle interfacce di rete e ConnectionSSH per le connessioni sicure ai dispositivi di rete, il software assicura un'interazione efficiente con l'infrastruttura di rete, contribuendo significativamente alla gestione ottimale delle risorse di rete e alla risoluzione di eventuali criticità operative.

CAPITOLO 4

PROBLEMATICHE DI CONFIGURAZIONE

In questo capitolo, esploreremo le principali criticità incontrate nella realizzazione della topologia di rete e le strategie adottate per superarle. Questa sezione mira a fornire un insight sul processo decisionale e sulla risoluzione creativa dei problemi, sottolineando l'importanza dell'innovazione e dell'adattabilità nel campo del networking.

4.1 Il problema delle sub-interfaces

La struttura originaria della rete, basata sull'uso di sub-interfaces per l'amministrazione delle varie VLAN, ha introdotto una problematica non trascurabile: la difficoltà nel rilevare ed analizzare le percentuali di utilizzo specifiche di tali sub-interfaces. Contrariamente alle aspettative, i router impiegati offrivano dati relativi unicamente alle porte fisiche, escludendo di fatto le interfacce virtuali create per la gestione delle VLAN.

Questa limitazione si è rivelata particolarmente critica, poiché la capacità di monitorare dettagliatamente l'utilizzo delle interfacce è fondamentale per una gestione efficace e per l'ottimizzazione delle prestazioni di rete. Di fronte a questo ostacolo, si è reso indispensabile ricercare una soluzione per ovviare a tale mancanza.

4.1.1 Il primo approccio: SNMP

Una soluzione inizialmente considerata per superare questo ostacolo è stata l'implementazione del protocollo Simple Network Management Protocol (SNMP), nelle sue versioni v2 e v3, affiancato dall'utilizzo di FrameFlow SNMP Browser per una gestione semplificata e un'analisi approfondita dei dati. Le versioni v2 e v3 di SNMP sono state scelte per le loro capacità di raccolta dati migliorata e per le funzionalità di sicurezza avanzate, rispettivamente. Queste versioni del protocollo erano intese a fornire un accesso dettagliato e sicuro alle informazioni di rete, permettendo di monitorare vari parametri, tra cui lo stato delle interfacce e l'utilizzo della banda. FrameFlow SNMP Browser, d'altra parte, è stato impiegato come strumento di visualizzazione e analisi, progettato per facilitare l'interrogazione dei dispositivi di rete e l'interpretazione dei dati raccolti tramite

SNMP. Nonostante l'integrazione di queste tecnologie avanzate, la soluzione non ha portato ai risultati attesi. La principale difficoltà riscontrata è stata l'incapacità di ottenere le percentuali di utilizzo specifiche per le sub-interfaces attraverso SNMP. Sebbene il protocollo e il software di analisi forniscano una vasta gamma di informazioni sulle prestazioni della rete e sullo stato delle interfacce, le metriche raccolte non includevano dettagli granulari sulle percentuali di utilizzo delle sub-interfaces, essenziali per un monitoraggio efficace e per l'ottimizzazione delle prestazioni di rete in relazione alle VLAN. Questa limitazione ha evidenziato le restrizioni intrinseche nell'uso di SNMP per il monitoraggio di strutture di rete complesse, in cui le sub-interfacce svolgono un ruolo cruciale. Nonostante le potenzialità offerte da SNMP e FrameFlow SNMP Browser nel fornire una visione d'insieme della rete e nel facilitare l'analisi dei dati, la specifica esigenza di monitorare le percentuali di utilizzo delle sub-interfaces non è stata soddisfatta. Di conseguenza, si è reso necessario valutare ulteriori approcci e soluzioni alternative per affrontare efficacemente questa sfida e garantire una gestione ottimale delle prestazioni e delle risorse di rete.

4.1.2 Soluzione adottata

Di fronte alla problematica di non poter ottenere le percentuali di utilizzo specifiche per le sub-interfaces tramite SNMP, è stato necessario intraprendere un percorso alternativo per garantire un monitoraggio efficace delle prestazioni della rete. La soluzione finale ha comportato una revisione sostanziale della topologia di rete, focalizzandosi sui router R6 e R5, per i quali è stata adottata una strategia innovativa che prevedeva l'uso di tre interfacce fisiche separate, ognuna assegnata esclusivamente a una VLAN distinta. Questa modifica ha introdotto una riconfigurazione degli switch adiacenti per assicurare l'adeguato instradamento dei frame all'interno delle VLAN designate. Tale riconfigurazione ha implicato non solo un aggiustamento delle impostazioni degli switch ma anche una riallocazione delle risorse di rete, per accomodare l'incremento di porte fisiche necessarie a supportare le nuove interfacce dedicate. L'introduzione di interfacce separate per VLAN ha risolto il problema di monitoraggio, permettendo di osservare direttamente l'utilizzo delle porte fisiche associate a ciascuna VLAN, bypassando così le restrizioni legate al monitoraggio delle sub-interfaces. Questa soluzione ha garantito un controllo più diretto e accurato sulle prestazioni della rete, facilitando l'identificazione di

eventuali colli di bottiglia o inefficienze e consentendo una gestione più mirata delle prestazioni. Nonostante le sfide tecniche e logistiche incontrate nella riconfigurazione della topologia e nell'adattamento delle risorse di rete, le modifiche apportate hanno significativamente migliorato la robustezza e la flessibilità della configurazione di rete. Questo adattamento ha non solo soddisfatto le esigenze specifiche del progetto ma ha anche fornito una base più solida per la gestione delle VLAN e delle rotte di traffico, contribuendo a una maggiore stabilità e affidabilità dell'infrastruttura di rete nel suo complesso.

4.2 Configurazione del DHCP

Un'altra sfida significativa incontrata durante l'implementazione della topologia di rete ha riguardato la configurazione del DHCP sui router 5 e 6. La problematica principale è emersa quando si è tentato di assegnare automaticamente gli indirizzi IP ai dispositivi connessi tramite DHCP. Nonostante la configurazione iniziale sembrasse corretta, si è riscontrato che i dispositivi non ricevevano gli indirizzi IP previsti, compromettendo la connettività e la comunicazione all'interno della rete. L'analisi del problema ha rivelato che le pool DHCP configurate sui router 5 e 6 presentavano delle incongruenze che impedivano il corretto funzionamento del servizio. Le pool DHCP sono fondamentali in una rete, poiché definiscono gli intervalli di indirizzi IP che possono essere assegnati dinamicamente ai dispositivi client che ne fanno richiesta. Ogni pool è associata a una specifica VLAN o a un segmento di rete, e deve essere configurata con parametri accurati, come il range di indirizzi IP disponibili, il gateway predefinito, i server DNS e altri parametri di rete.

4.2.1 Soluzione adottata

Per risolvere il problema, è stato necessario eseguire una revisione dettagliata delle configurazioni DHCP sui router interessati. Questo ha comportato la verifica delle associazioni tra le pool DHCP e le relative VLAN, l'analisi dei range di indirizzi IP definiti e la correzione di eventuali errori nelle impostazioni di gateway predefinito o di altre opzioni di rete. In alcuni casi, è stato necessario eliminare e ricreare le pool DHCP

per assicurare che tutti i parametri fossero configurati correttamente. Una volta apportate le modifiche necessarie e verificata l'integrità delle configurazioni DHCP, si è proceduto con una serie di test per garantire che i dispositivi client ricevessero correttamente gli indirizzi IP assegnati dalle pool DHCP riconfigurate. Questi test hanno incluso la verifica della connettività, del rilascio e del rinnovo degli indirizzi IP e della corretta comunicazione tra i dispositivi all'interno delle VLAN. La soluzione di questa problematica ha richiesto un'attenzione particolare ai dettagli e una comprensione approfondita del funzionamento del DHCP in contesti di rete complessi.

4.3 Utilizzo di Iperf3

Durante la fase di testing della rete, utilizzando il software Iperf3 per misurare le prestazioni di banda tra i nodi, è emerso un ulteriore ostacolo legato alla sicurezza informatica: il firewall di Windows sui dispositivi di test interferiva con il corretto funzionamento di iperf3, impedendo la visualizzazione dei dati sui pacchetti inviati e ricevuti. Questa problematica ha evidenziato l'importanza di considerare gli aspetti di sicurezza e le configurazioni di sistema quando si conducono test di rete in ambienti controllati. Il firewall di Windows, progettato per proteggere il sistema da accessi non autorizzati e da traffico di rete potenzialmente dannoso, può talvolta entrare in conflitto con strumenti di testing di rete come iperf3. Nel caso specifico, le regole del firewall impedivano le connessioni in entrata e in uscita necessarie per il corretto funzionamento di iperf3, bloccando di fatto la trasmissione dei pacchetti di test e la raccolta dei dati relativi alla velocità e alla qualità della connessione.

4.3.1 Soluzione adottata

Dopo aver identificato il firewall come causa del problema, la soluzione adottata è stata la disattivazione temporanea del firewall sui dispositivi utilizzati per i test. Questo approccio, sebbene efficace nel risolvere immediatamente la problematica, richiede un'attenzione particolare alla sicurezza, poiché disabilitare il firewall espone il sistema a potenziali rischi. Pertanto, questa operazione è stata eseguita in un ambiente di test controllato e per un periodo di tempo limitato, strettamente necessario per completare le

misurazioni con iperf3. La disattivazione del firewall ha permesso a iperf3 di funzionare senza intoppi, facilitando la trasmissione dei pacchetti di test e consentendo la raccolta di dati accurati sulle prestazioni di rete.

4.4 Utilizzo dello switch

Un problema significativo emerso durante l'implementazione della topologia di rete ha riguardato uno degli switch principali, identificato come "Switch 2". Durante le fasi iniziali di testing e monitoraggio, è stata osservata una consistente degradazione delle prestazioni di rete, con sintomi quali latenza elevata, perdita di pacchetti e throughput inferiore alle aspettative, particolarmente evidenti nelle comunicazioni attraverso Switch 2. Analisi approfondite hanno rivelato che Switch 2 soffriva di una serie di malfunzionamenti hardware, inclusi problemi ai moduli delle porte Ethernet, che compromettevano la capacità di gestire efficacemente il traffico di rete ad alta velocità.

4.4.1 Soluzione adottata

La decisione di sostituire Switch 2 è stata presa dopo aver valutato che le riparazioni hardware e gli aggiornamenti del firmware non avrebbero risolto in modo definitivo i problemi relativi alle prestazioni. La sostituzione è stata vista come un investimento necessario per assicurare la stabilità, l'affidabilità e l'espandibilità a lungo termine della rete. La scelta del nuovo switch, denominato "Switch 3", è stata guidata da criteri rigorosi, tra cui la piena compatibilità con gli standard di rete impiegati, elevate prestazioni garantite anche sotto carico intenso, supporto nativo per QoS avanzato e protocolli di routing dinamico, nonché la capacità di integrarsi senza soluzione di continuità con l'infrastruttura di rete esistente. La transizione a Switch 3 ha comportato una pianificazione accurata per minimizzare i tempi di inattività e garantire una migrazione dei dati senza interruzioni. Una volta completata l'installazione e la configurazione di Switch 3, si è osservata un marcato miglioramento delle prestazioni di rete, con una riduzione significativa della latenza, l'eliminazione della perdita di pacchetti e un throughput generale in linea con le aspettative del progetto.

CAPITOLO 5

DATA COLLECTING

In questo capitolo, affronteremo nell'analisi delle prestazioni della rete attraverso una serie di test mirati. L'intento è di offrire una panoramica dettagliata dei metodi di test impiegati, della raccolta dati e delle successive fasi di analisi, per trarre conclusioni significative sul comportamento della rete. Le informazioni raccolte da questi test saranno cruciali per identificare le aree di efficacia della configurazione attuale e per evidenziare potenziali margini di ottimizzazione.

5.1 Introduzione ai test: Iperf3

Iperf3 è uno strumento di benchmarking di rete open source, ampiamente riconosciuto per la sua affidabilità e precisione nel misurare la larghezza di banda disponibile tra host nella rete. Il software funziona generando traffico di dati che può essere configurato per simulare vari tipi di comunicazione di rete e carichi di lavoro, consentendo così di valutare le prestazioni di throughput, la latenza e la perdita di pacchetti. Attraverso i test con iperf3, si esploreranno vari scenari di traffico, dalla trasmissione di dati su singoli flussi TCP/UDP fino a test più complessi che coinvolgono multipli flussi paralleli, per valutare l'impatto di diverse configurazioni di rete e l'efficienza del routing. Questi test offriranno una visione dettagliata della capacità di rete, della sua efficienza nel gestire il traffico e della robustezza delle sue configurazioni sotto diverse condizioni operative.

5.2 Configurazione test

Per la configurazione dei test di prestazione della rete, l'ambiente di test è stato strutturato in tre fasi distinte per valutare in modo approfondito la reattività e la capacità della topologia di rete sotto diversi scenari di traffico:

1. Test bidirezionali. Utilizzando due dispositivi terminali connessi alla configurazione.

2. Test bidirezionali con flussi paralleli. Utilizzando due dispositivi terminali connessi alla configurazione.

3. Test con multipli flussi di dati. Utilizzando quattro dispositivi terminali connessi alla configurazione.

5.2.1 Fase 1: Test bidirezionali

Nella prima fase dell'ambiente di test, sono stati impiegati due dispositivi terminali, uno collegato al router R5 e l'altro al router R6, per valutare il flusso di dati tra questi due nodi cruciali della rete. L'intento era di analizzare in dettaglio le prestazioni di trasferimento dati, concentrandosi sul throughput, sulla latenza e sulla perdita di pacchetti in un flusso unidirezionale. Questo setup ha avuto l'obiettivo di investigare come la topologia progettata fosse in grado di gestire il traffico dati in scenari di comunicazione diretta tra i router.

Si è adottato un approccio flessibile riguardo alla grandezza dei pacchetti. Invece di limitarsi a una dimensione fissa, sono state testate diverse grandezze, variando da pacchetti piccoli a pacchetti grandi, per simulare una gamma più ampia di condizioni di traffico e tipologie di dati. Questa variazione nelle dimensioni dei pacchetti ha permesso di ottenere una visione più comprensiva dell'efficienza della rete, evidenziando come differenti tipi di carichi influenzassero le prestazioni. La durata di ogni sessione di test è stata attentamente calibrata per raccogliere un set di dati significativo, consentendo una valutazione dettagliata delle prestazioni della rete sotto vari profili di traffico.

5.2.2 Fase 2: Test bidirezionali con flussi paralleli

Nella fase successiva dei test, si è proceduto con una configurazione che prevedeva l'esecuzione di test bidirezionali paralleli, mantenendo la stessa disposizione di base dei dispositivi terminali connessi ai router R5 e R6. La novità di questa fase risiedeva nell'impostazione del client di iperf in modo tale da simulare più flussi paralleli di dati. Questo approccio è stato adottato per valutare la capacità della topologia di rete di gestire simultaneamente più sessioni di comunicazione, un aspetto critico per comprendere la resilienza e l'efficienza della rete sotto carichi di traffico più intensi e complessi.

5.2.3 Fase 3: test con multipli flussi di dati

Proseguendo nella fase di sperimentazione, l'attenzione si è spostata verso test avanzati con flussi multipli di dati, impiegando quattro terminali per esaminare la capacità della topologia di rete di gestire e distribuire efficacemente il traffico. Due terminali erano connessi al router R5 e gli altri due al router R6, creando un ambiente di test che simulava un utilizzo di rete intensificato e diversificato, tipico di scenari operativi reali. L'obiettivo principale di questi test era di verificare se la topologia progettata fosse in grado di riconoscere la saturazione di un percorso primario e, di conseguenza, di reindirizzare il traffico in eccesso verso un percorso secondario disponibile, mantenendo così le prestazioni ottimali della rete. Questa funzionalità è fondamentale per garantire la resilienza e l'affidabilità della rete, soprattutto in presenza di carichi di traffico elevati o di potenziali guasti in uno dei percorsi principali.

Per realizzare questi test, i terminali sono stati configurati per generare simultaneamente flussi di dati diretti sia verso il router R5 che verso il router R6, creando così una situazione di traffico bilanciato ma intensivo. L'utilizzo di iperf su ciascun terminale ha permesso di generare traffico in modo controllato e misurabile, offrendo la possibilità di monitorare con precisione come la rete gestisse i flussi multipli e distribuisse il carico tra i percorsi disponibili.

5.3 Analisi dei dati

L'analisi dei dati raccolti nelle tre distinte fasi di test offre una panoramica completa delle prestazioni della topologia di rete sotto vari scenari di traffico. Questa sezione si propone di esaminare i risultati ottenuti, confrontandoli con gli obiettivi prestazionali prefissati e valutando l'efficacia della rete nel gestire diversi carichi di traffico.

5.3.1 Analisi dei test bidirezionali

L'analisi ha permesso di stabilire un benchmark delle prestazioni della rete in condizioni ideali, evidenziando la capacità massima di trasferimento dati e fornendo un punto di riferimento per i test successivi.

5.3.2 Analisi dei test bidirezionali con flussi paralleli

L'analisi di questi test ha permesso di osservare come la rete distribuisse il traffico e gestisse il carico tra i percorsi disponibili, mettendo in luce l'efficienza del sistema di routing e del bilanciamento del carico. Particolare attenzione è stata rivolta alla capacità della rete di mantenere prestazioni ottimali anche con l'aumentare dei flussi di dati.

5.3.3 Analisi dei test con multipli flussi di dati

L'obiettivo era di valutare la capacità della rete di reindirizzare il traffico verso un percorso secondario in caso di saturazione delle interfacce principali. I dati raccolti hanno offerto spunti preziosi sulla resilienza della rete e sulla sua capacità di adattarsi dinamicamente a scenari operativi complessi, evidenziando eventuali limiti nella gestione del traffico e nel meccanismo di failover.

5.3.4 Sintesi dell’analisi

La sintesi dei dati raccolti dalle tre fasi di test evidenzia la complessità e la dinamicità delle prestazioni della rete. Attraverso un'analisi approfondita, è stato possibile identificare punti di forza e aree di miglioramento della topologia. Questi risultati non solo confermano l'adeguatezza della configurazione di rete rispetto agli obiettivi prefissati ma forniscono anche una base solida per future ottimizzazioni. L'approccio metodico ai test e all'analisi dei dati sottolinea l'importanza di una verifica empirica delle prestazioni di rete, essenziale per garantire la realizzazione di infrastrutture di rete affidabili, efficienti e scalabili.

5.4 Osservazioni chiave e implicazioni

1. Reindirizzamento del Traffico: Contrariamente alle aspettative, il reindirizzamento automatico del traffico verso il percorso secondario non è stato immediato, evidenziando una latenza nella risposta della rete alla saturazione delle interfacce. Questo ritardo ha causato temporanei rallentamenti e una lieve perdita di pacchetti, sottolineando la necessità di ottimizzare il meccanismo di failover.

2. Capacità di Bilanciamento del Carico: Nonostante il problema iniziale, una volta attivato, il sistema di bilanciamento del carico ha funzionato efficacemente, distribuendo il traffico in maniera equa tra i percorsi disponibili e ripristinando le prestazioni ottimali della rete.

3. Scalabilità della Rete: Il test ha confermato la scalabilità della topologia di rete, dimostrando che, nonostante le sfide iniziali, la rete è in grado di adattarsi a un aumento significativo del carico di traffico mantenendo livelli accettabili di prestazione.

Le osservazioni chiave derivanti dai test evidenziano l'importanza di:

1. Monitorare e Testare Continuamente: La necessità di monitorare costantemente le prestazioni di rete e di condurre test regolari per identificare e risolvere proattivamente potenziali punti deboli nella configurazione di rete.

2. Ottimizzare i Meccanismi di Failover: L'importanza di ottimizzare i meccanismi di failover per garantire una transizione fluida e tempestiva del traffico in scenari di saturazione delle interfacce.

3. Investire in Scalabilità: La conferma che investire nella scalabilità della rete è fondamentale per supportare efficacemente l'evoluzione delle esigenze di traffico.

CAPITOLO 6

CONCLUSIONI

Questo progetto ha esplorato in profondità la creazione e gestione di una topologia di rete avanzata, con un focus specifico sulle strategie di monitoraggio e ottimizzazione delle prestazioni di rete attraverso una serie di test approfonditi. L'obiettivo era di sviluppare una topologia di rete che non solo rispondesse alle esigenze operative ma che fosse anche capace di adattarsi dinamicamente alle variazioni del traffico e alle esigenze di performance. L'implementazione della topologia di rete ha rappresentato un elemento chiave per simulare un ambiente reale e testare la resilienza e l'efficienza della rete. Gli esperimenti condotti, in particolare quelli che utilizzavano iperf3 per simulare flussi di dati multipli, hanno permesso di valutare la capacità della rete di gestire carichi di traffico intensi e di reindirizzare il traffico in maniera efficiente quando necessario. Durante il progetto, è emersa l'importanza cruciale dell'ottimizzazione della rete, specialmente in termini di bilanciamento del carico e gestione delle risorse, per mantenere prestazioni ottimali sotto vari scenari di utilizzo. Questo ha implicato non solo un'attenta pianificazione della topologia, ma anche un monitoraggio costante e un'adattabilità della configurazione di rete per rispondere alle esigenze dinamiche. Sebbene i risultati ottenuti abbiano confermato l'efficacia della topologia di rete proposta e delle strategie di monitoraggio adottate, vi è sempre spazio per ulteriori miglioramenti. Potenziali aree di sviluppo futuro includono l'espansione delle capacità di monitoraggio per coprire una gamma più ampia di metriche di prestazione, l'ottimizzazione delle strategie di failover per garantire una maggiore resilienza della rete, e l'integrazione di sistemi di allerta e diagnostica più avanzati per facilitare la gestione proattiva della rete.

In sintesi, il progetto ha stabilito una solida base per la gestione avanzata della rete, offrendo preziose intuizioni su come ottimizzare e monitorare le infrastrutture di rete per supportare le esigenze attuali e future. Continuando su questa traiettoria, con ulteriori raffinamenti e integrazioni, la soluzione proposta potrà evolversi in uno strumento ancora più potente e versatile per gli amministratori di rete, assicurando prestazioni di rete elevate e affidabili.

BIBLIOGRAFIA E SITOGRAFIA

Bibliografia

ALADHAMI MAHMOOD MAZIN, M. K. A. R. M., RUHANI AB RAHMAN (2021), «Performance Analysis on Network Automation Interaction with Network Devices Using Python».

DONAHUE, G. A. (2007), «Network Warrior».

E ETHAN BANKS, R. W. (2017), «Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient, Modern Networks».

EDELMAN, J. (2018), «Network Programmability and Automation: Skills for theNext-Generation Network Engineer».

JIA, B. (2010), «Research of Physical Topology Discovery in Heterogeneous IP Networks with VLAN».

KUMAR, B. K. (2019), «Fixing Network Security Vulnerabilities in Local Area Network».

KUROSE, J. (2022), «Reti di calcolatori e internet. Un approccio top-down».

N., P. (2016), «Software-Defined Networking: Reconfigurable Network Systems in LAN Topology».

OLENA STARKOVA, K. N. O. Z. A. B. N. S., KOSTIANTYN HERASYMENKO (2022), «Virtualization and Programmability in Modern Networks in the Context of SDN Concept».

PAUL MIHA ˇ ILA ˇ , R. C. F. S., TITUS BA ˇ LAN (2017), «Network Automation and Abstraction using Python Programming Methods».

STEVEN S. W. LEE, K.-Y. L. (2013), «Study of Dynamic Topology Change for Total Energy Consumption in Green IP Networks».

TANENBAUM, A. S. (2003), «Reti di calcolatori».

Sitografia

• Huawei – https://e.huawei.com/it/solutions/enterprise-network

• Huawei ICS

• Paramiko – https://www.paramiko.org/

• Programmazione Python – https://docs.python.it/html/lib/module-threading

• Visure – https://visuresolutions.com/it/

• Visure – https://visuresolutions.com/it/blog/functional-requirements/

• Wikipedia – www.wikipedia.org

• Vega Training – https://www.vegatraining.eu/

• Huawei- https://support.huawei.com/enterprise/it/doc/EDOC1100008295/a867611a/vlan-configuration/

• Manage Engine – https://www.manageengine.com/it/network-monitoring/what-is-snmp.html

• HTML.it – https://www.html.it/guide/guida-ad-ssh-il-protocollo-di-rete/

• Trovalost – https://trovalost.it/putty/

• HTML.it – https://www.html.it/disegnare-interfacce-con-qt-designer/

• Programmazione Python – https://www.python.it/wiki/show/qttutorial/

• IPERIUS – https://www.iperiusbackup.net/

• Iperf https://iperf.fr/

• Netmiko – https://pynet.twb-tech.com/blog/netmiko-python-library.

• Librerie Python per l'automazione https://datascience.eu/it/programmazione/le-migliori-librerie-di-python-per-lapprendimento-automatico/

RINGRAZIAMENTI

Desidero rivolgere un sentito ringraziamento all'Ing. Adelmo De Santis, correlatore di questa tesi, la cui guida esperta ed immensa disponibilità sono stati indispensabili e fondamentali nel mio viaggio di ricerca. Un ringraziamento particolare va anche al Prof. Ennio Gambi, relatore di questa tesi, per il suo contributo inestimabile e la sua disponibilità a condividere le sue conoscenze.

Desidero esprimere la mia più profonda gratitudine alla mia famiglia, il pilastro fondamentale della mia vita. Un ringraziamento speciale va a mia mamma e al mio papà, per il loro amore incondizionato, il sostegno incessante ed i numerosi sacrifici fatti per me. La loro presenza costante ha illuminato il mio cammino in ogni momento.

Un caloroso ringraziamento va a mia sorella Selena, che è stata per me un modello da seguire in tutti questi anni. La sua forza, il suo esempio e il suo incoraggiamento hanno lasciato un segno indelebile nel mio cuore.

Un grazie infinito va ai miei amati nonni: Nonna Nina e Nonno Antonio, Nonno Saverio e Nonna Rosa. Le vostre storie, i vostri sorrisi ed i vostri insegnamenti sono il tesoro più prezioso che porto nel cuore. Avete nutrito la mia infanzia non solo di cibo, ma anche di racconti e valori. In ogni passo che compio, sento il sostegno della vostra saggezza e la forza del vostro amore. Siete stati i maestri della mia vita.

Desidero ringraziare Michele, che più di un amico è per me un fratello maggiore, sempre presente e pronto a offrire il suo sostegno e la sua saggezza nei momenti di bisogno.

Un grazie speciale va a Mattia, la cui amicizia, seppur nata in circostanze inaspettate, si è rivelata una delle più preziose nel corso degli anni. La sua lealtà e la sua presenza costante sono state una fonte di conforto e gioia nei momenti difficili.

Non posso dimenticare di ringraziare Nicolò, mio coinquilino e compagno di innumerevoli avventure. Abbiamo condiviso così tanto in questi anni che è impossibile immaginare i miei giorni senza la sua amicizia.

Un sentito ringraziamento va anche alle nuove amicizie del Circolo Fazioli 14, Antonio Espansione e Marco Dipi, che in poco tempo sono diventati cari amici, portando allegria e leggerezza nei giorni più pesanti, ma soprattutto per avermi riempito di cornetti alla marmellata in questi ultimi mesi.

Desidero ringraziare Dionigi e Gianmarco, per avermi fatto ridere a crepapelle durante la nostra convivenza e per tutti i momenti felici condivisi; un ROAR speciale per Gianmarco.

Un grazie va a Simone, il mio primo amico in questa avventura, che mi ha aperto le porte a un mondo di nuove amicizie e esperienze indimenticabili.

Non posso non menzionare Matteo, detto Coppols, perché... è semplicemente Coppola. La sua unicità e la sua presenza hanno arricchito la mia vita in modi inimmaginabili.

Infine, un ringraziamento va a tutti gli amici e le persone che mi hanno accompagnato in questi anni, condividendo con me momenti belli e brutti. Ognuno di voi ha contribuito a rendere questo viaggio indimenticabile. Grazie di cuore a tutti voi per aver camminato al mio fianco in questo capitolo della mia vita.