UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI INGEGNERIA

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Ingegneria Elettronica

TESI DI LAUREA

Studio di topologia per PoC in ambito Network Programmability

Topology study for PoC in the Network Programmability field

Relatore

Prof. Ennio Gambi

Correlatore

Ing. Adelmo De Santis

Candidato

Maria Chiara Melograna

ANNO ACCADEMICO 2022-2023

Sommario

Introduzione

In una società sempre più immersa nella tecnologia quale è la nostra, l'importanza delle reti di comunicazione è quantomai evidente. Ogni individuo, dal più giovane al più anziano, usufruisce quotidianamente di tanti degli innumerevoli servizi in ambito ICT disponibili, motivo per cui "navigare in rete" è passata da essere una comodità ad una necessità per chiunque.

L'idea del presente progetto di tesi è nata durante il corso di formazione per la certificazione Huawei HCIA Datacom, un contesto stimolante che, nel presentare i concetti e le tendenze attuali nel settore delle telecomunicazioni e delle reti informatiche, ha suscitato l'interesse e la fantasia necessari allo sviluppo di una Proof of Concept (PoC) nell'ambito della Network Programmability.

Il lavoro consiste nella realizzazione di una topologia di rete che sia conforme a precise specifiche, successivamente programmata in modo da ottimizzare le proprie prestazioni, specialmente l'instradamento dei pacchetti, sulla base di un monitoraggio continuo delle condizioni di traffico nella rete. Attraverso l'implementazione di un meccanismo di network è stata implementata una rete intelligente in grado di prendere decisioni istantanee per indirizzare il traffico attraverso il percorso più vantaggioso in tempo reale.

L'approccio dinamico adottato, grazie alla sua capacità di ottimizzare l'efficienza di trasmissione, risulta essere una valida soluzione all'attualissima sfida del miglioramento della qualità del servizio nelle reti moderne.

1. Panoramica del Progetto

Grazie alla richiesta sempre crescente in termini di trasferimento dati, il presente progetto si inserisce in un contesto fertile e in continua evoluzione: le reti informatiche.

L'obiettivo finale è quello di progettare e implementare una rete composta da cinque router, in grado di effettuare la commutazione automatica fra due percorsi alternativi in base al traffico dati.

Con questo lavoro si intende approfondire lo sviluppo dell'architettura di rete alla base del progetto, garantendo non solo un funzionamento corretto, ma anche il rispetto rigoroso delle specifiche relative alle dinamiche operative della rete. Di particolare interesse è il fatto che queste ultime non sono determinate esclusivamente dai collegamenti fisici, come potrebbe suggerire l'intuizione comune, esse sono invece il risultato di un'attenta e ponderata selezione e applicazione delle tecnologie e dei protocolli di livello 2 e 3 del modello ISO-OSI. Questo sottolinea l'importanza di valutazioni approfondite durante la progettazione e l'implementazione delle reti, poiché le scelte effettuate in queste fasi influenzano direttamente il comportamento e le prestazioni del sistema nel suo complesso.

1.1 Obiettivi progettuali

Questa sezione delinea gli obiettivi progettuali sviluppati e affrontati in sequenza durante l'organizzazione del lavoro. In particolare, si sono strutturati in due fasi distinte: il rispetto di una topologia logica ben precisa e l'implementazione della parte di network automation.

- **Rispetto della topologia logica**

La prima fase si concentra sul mantenimento e il rispetto della topologia logica in *figura 1*.

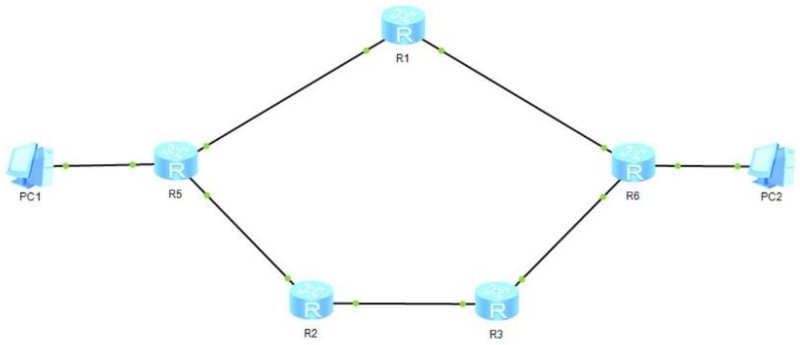

Figura 1 - Topologia logica

Come si può notare è composta da cinque router disposti in modo tale che il traffico da PC1 a PC2 possa seguire due possibili percorsi di routing: il primo attraverso i router R5, R1 ed R6, e il secondo attraverso i router R5, R4, R3, R6. È rilevante sottolineare che i router R5 e R6 rivestono un ruolo cruciale in quanto rappresentano i nodi in cui convergono entrambi i percorsi di routing, grazie ai loro collegamenti diretti con PC1 e PC2, rispettivamente. Pertanto, sono tali router che gestiscono l'instradamento del traffico dati lungo uno dei due percorsi. Il rispetto di questa specifica influenza la progettazione e realizzazione di quella fisica, che potrà rispettarla grazie ad un'accurata scelta dei collegamenti hardware e ad un adeguato uso dei protocolli di livello 2 e 3.

- **Network automation**

La seconda fase consiste nella realizzazione di un software che effettui il monitoraggio del traffico dati della rete e stabilisca delle soglie il cui superamento metta in atto delle modifiche tali per cui il percorso di routing venga deviato sul percorso inutilizzato. Il software in questione sarà in grado di comunicare con i dispositivi di rete tramite una connessione wireless e consentirà all'utente di visualizzare il traffico e apprezzare il meccanismo di netwok automation tramite un'apposita interfaccia grafica. In altre parole, il software, in caso di traffico intenso, effettuerà una vera e propria modifica della topologia rendendo effettivi dei comandi preparati appositamente per la gestione del routing in tali condizioni.

2. Tecnologie utilizzate

Al fine di agevolare la comprensione del capitolo successivo relativo allo sviluppo del progetto, il presente capitolo mira a fornire un quadro generale delle tecnologie considerate durante la fase di progettazione. L'obiettivo è illustrare e giustificare le scelte relative sia all'hardware che al software impiegati, oltre a delineare i concetti e i protocolli che hanno sostenuto lo sviluppo del progetto, specialmente durante la prima fase. Ognuno di essi ha contribuito in modo significativo, e in questa sede si intende chiarirne il ruolo e l'utilità.

2.1 Hardware e software: Huawei

L'hardware necessario alla realizzazione della topologia fisica consiste sostanzialmente in cinque router e, in questo specifico contesto, due switch. La decisione di optare per due switch è stata motivata dalla disponibilità di più apparati di questo tipo nel laboratorio. Tale scelta ha consentito di distribuire il carico di lavoro su due dispositivi anziché uno, migliorando le prestazioni complessive della rete. La gestione di un volume inferiore di traffico da parte di ciascuno switch ha permesso di ridurre le congestioni e di migliorare i tempi di risposta complessivi dei dispositivi di rete.

Di seguito sono riportati gli apparati utilizzati.

Dispositivo di rete	**Azienda produttrice**	**Serie**
R1 R2 R3	Huawei	AR1220
R5 R6	Huawei	AR2220
SW1 SW2	Huawei	S5700
SW3	Huawei	S3700

Il ruolo e l'utilizzo di SW3 saranno chiariti nel capitolo 3.

Per quanto riguarda la parte relativa al software, un valido strumento è stato eNSP. Enterprise Network Simulation Platform (eNSP) è una piattaforma di simulazione di rete grafica sviluppata da Huawei che si è rivelata particolarmente utile in fase di progettazione. Grazie alla possibilità di selezionare e quindi simulare il funzionamento di gran parte dei dispositivi di rete prodotti di Huawei, ha consentito di eseguire test realistici contribuendo in modo significativo allo sviluppo complessivo del progetto.

2.2 VLAN

L'impiego delle Virtual LAN si è dimostrato estremamente vantaggioso poiché ha permesso la suddivisione della rete fisica in segmenti logici distinti. Questa suddivisione ha consentito a router appartenenti allo stesso dominio di broadcast di comunicare in modo efficiente e sicuro. In buona sostanza, l'implementazione delle VLAN è stata cruciale affinché la topologia fisica rispecchiasse quella logica.

2.3 Sub-Interface

Questa tecnologia, in una prima fase, è stata utilizzata per ottimizzare i collegamenti fisici dei router, consentendo il trasporto del traffico di più VLAN attraverso una singola connessione fisica, pur mantenendo l'isolamento dei dati tra le VLAN.
In una seconda fase è stata sfruttata per la capacità di contrassegnare i frame con la VLAN specificata nel PVID mediante un tag.

2.4 OSPF

OSPFv2, acronimo di Open Shortest Path First, è il protocollo di routing utilizzato nella configurazione. Effettivamente, ha consentito il riempimento e l’aggiornamento continuo delle tabelle di routing grazie allo scambio di informazioni di stato dei collegamenti con gli altri router presenti nella rete. Grazie a OSPF, ogni router mantiene un database di stato dei collegamenti che indica i router adiacenti e le metriche associate ai collegamenti in modo da poter instradare il traffico attraverso il percorso più breve.

2.5 LAG

Il link aggregation fra due switch, anche noto come LAG (Link Aggregation Group), permette di combinare più collegamenti fisici tra due dispositivi di rete in un unico collegamento logico ad alta velocità. È stato sfruttato per massimizzare quanto più possibile e prestazioni del collegamento fra SW1 e SW2.

2.6 DHCP

Il DHCP (Dynamic Host Configuration Protocol) è un protocollo di rete utilizzato per assegnare automaticamente indirizzi IP ai dispositivi client all'interno di una rete locale. In particolare, è stato sfruttato per consentire a PC1 e PC2 di ottenere degli IP address relativi allo spazio di indirizzi della VLAN 10 e 20 rispettivamente.

2.7 ICMP

ICMP, o Internet Control Message Protocol, è un protocollo utilizzato per inviare messaggi di controllo e diagnostica tra dispositivi di rete, come router e computer. Tra le varie funzionalità di controllo e diagnostica (come l'invio di messaggi d'errore) che fornisce, ciò che è risultato particolarmente utile è il messaggio di "echo request" utilizzato per testare la connettività di rete, richiesto tramite il comando "ping".

2.8 Altre tecnologie utilizzate

SSH (Secure Shell) è il protocollo che si è preferito utilizzare per effettuare l'accesso remoto ai dispositivi di rete durante la seconda fase del progetto. Grazie ad una forte autenticazione e alla garanzia della crittografia dei dati durante le comunicazioni, si è potuta stabilire una connessione remota sicura e affidabile.

Questa fase ha visto anche l'uso del protocollo SNMP per quanto riguarda il monitoraggio e la gestione dei dispositivi di rete. Nello specifico, ha consentito di raccogliere informazioni sullo stato e le prestazioni della rete (data collecting), nonché di configurarli e controllarli in remoto. iPerf, invece, è lo strumento che ha consentito di generare flussi di dati tra PC1 e PC2 in fase di test e di misurare le prestazioni della connessione in termini di velocità di trasferimento dati. Infine, è

doveroso menzionare Python, il linguaggio di programmazione che, grazie alla sua semplicità e versatilità ma anche soprattutto alla disponibilità di particolari librerie con Paramiko e Netmiko, è stato utilizzato nello sviluppo del software di monitoraggio e ottimizzazione dinamica del traffico.

3. Sviluppo del progetto

In questa sezione sono descritte tutte le fasi progettuali nell'ordine in cui sono state effettivamente seguite in fase di sviluppo, entrando nel dettaglio di ognuna. Dopo la scelta dei dispositivi, si è provveduto ad abbozzare prima su carta e poi sul simulatore la topologia di rete fisica. In questo contesto, quindi ancor prima di mettere le mani sugli apparati, sono state effettuate le scelte progettuali riguardanti l'organizzazione della configurazione dei dispositivi in modo che la rete potesse avere delle dinamiche operative che rispettassero il comportamento logico desiderato. Avere uno schema chiaro e dettagliato della rete con le componenti logico-fisiche previste è stato molto utile e ha permesso di procedere alla realizzazione della configurazione dei router e degli switch in maniera organizzata e celere. Di seguito saranno approfondite le motivazioni delle scelte relative al primo obiettivo progettuale, la loro implementazione e i test che ne hanno confermato il funzionamento.

3.1 Configurazione provvisoria della topologia

3.1.1 Topologia fisica

La topologia fisica (*figura 2*) è stata attentamente progettata tenendo in considerazione l'architettura logica desiderata (*figura 3*).

Come mostrato in *figura 2*, essa si compone di cinque router interconnessi tra loro e con gli host (PC1 e PC2) tramite due switch. Nello specifico, i router R1, R5, e R6, insieme a PC1, sono collegati a SW1, mentre R2, R3, e PC2 sono connessi a SW2. Per quanto riguarda il cablaggio, si è deciso di ottimizzare i collegamenti fisici fra router e switch, limitandoli ad un solo link ciascuno prevedendo l'utilizzo di sub-interface per distinguere il traffico fra VLAN. In questo modo è stato inoltre possibile di sfruttare la disponibilità delle porte restanti per potenziare il collegamento fra i due switch, che potranno contare su quattro collegamenti fisici.

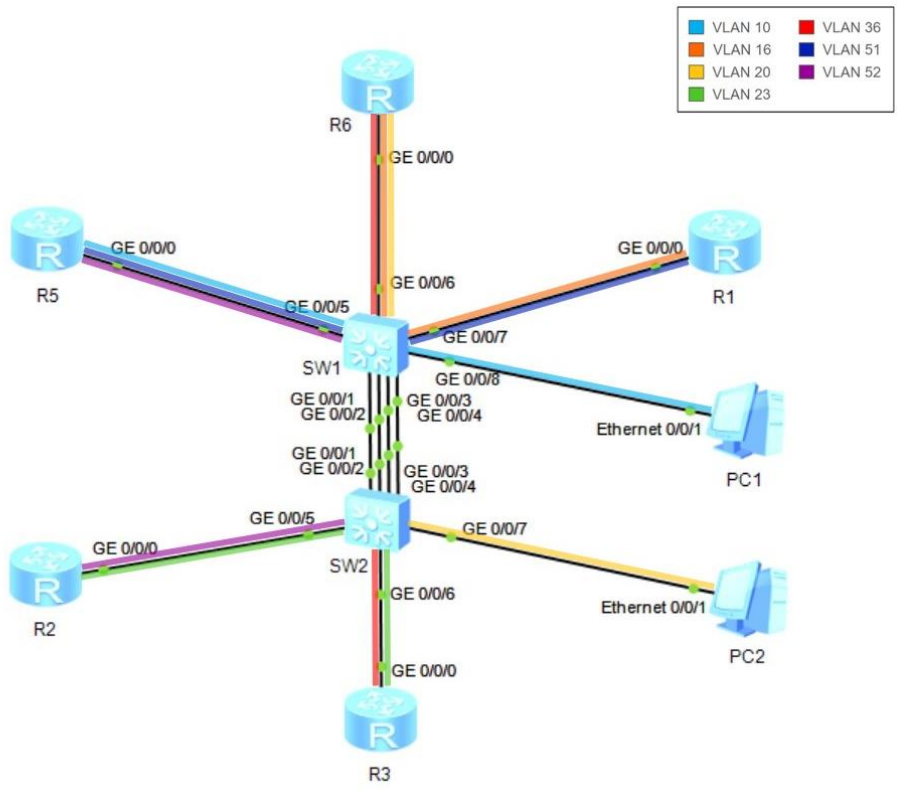

Figura 2 - Topologia fisica

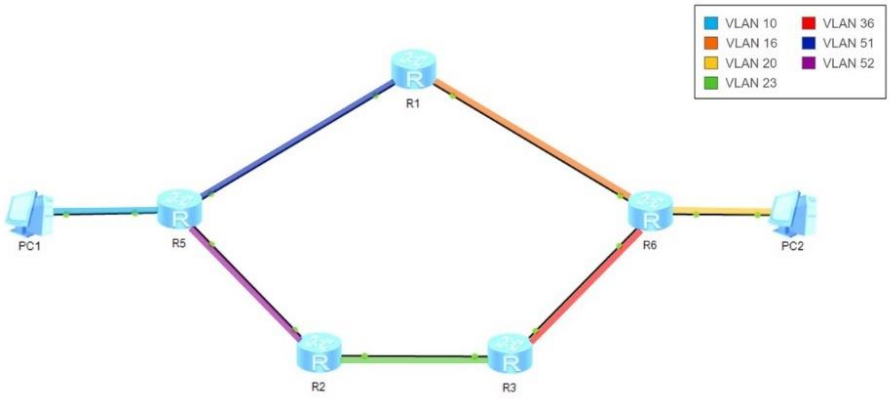

Figura 3 - Topologia logica con VLAN

3.1.2 Topologia logica

L'immagine consente di apprezzare, oltre alla topologia fisica, anche il percorso dei dati all'interno di ogni VLAN. Come evidenziato nel capitolo precedente, l'utilizzo di

questa tecnologia ha permesso alla rete fisica di rispecchiare il modello logico desiderato. Infatti, le specifiche riguardanti la topologia di livello 2 impongono dei collegamenti fra router che possono facilmente essere creati circoscrivendo opportunamente i domini di broadcast. Le VLAN, di fatto, creano dei sottogruppi logici all'interno della rete locale che comunicano come se fossero collegati allo stesso segmento di rete nonostante si trovino fisicamente su segmenti diversi. Affinché venga rispettato il collegamento logico fra due router indicato in figura, è sufficiente che essi appartengano allo stesso dominio di broadcast, ossia alla stessa VLAN. Pertanto, si è deciso di introdurre sette VLAN, ciascuna corrispondente a un segmento logico.

Scelta delle VLAN e assegnazione indirizzi IP sui router

L'attribuzione dei nomi delle singole VLAN, per quanto possa risultare una scelta assolutamente marginale, ha consentito di semplificare notevolmente il riconoscimento sia del segmento di rete sia dello spazio di indirizzi ad esso associato.

Il criterio per la denominazione delle varie VLAN è stato il seguente:

- La prima cifra identifica il router di partenza.
- La seconda cifra identifica il router di destinazione.

Si tenga presente che la convenzione adottata in questo contesto assume che il router di "partenza" sia, fra i due, quello più prossimo a PC1, mentre il router di "destinazione" sia quello più vicino a PC2.

Tuttavia, fanno eccezione le VLAN che collegano gli host ai router R5 ed R6. Per quanto riguarda il collegamento fra PC1 e R5 si è preferito utilizzare la VLAN 10, mentre per il collegamento fra PC2 e R6 la VLAN 20.

La tabella sottostante riepiloga le scelte relative alle VLAN e mostra gli spazi di indirizzi IPv4 associati ad ognuna.

VLAN	Spazio di indirizzi associato
10	192.168.10.0/24
16	192.168.16.0/24
20	192.168.20.0/24
23	192.168.23.0/24
36	192.168.36.0/24
51	192.168.51.0/24
52	192.168.52.0/24

Sub-interfaces

Come anticipato in precedenza, l'utilizzo delle sub-interface è stato introdotto e sfruttato allo scopo di ottimizzare i collegamenti fisici fra router e switch. Grazie a questa tecnologia, è stato possibile suddividere l'interfaccia fisica di ogni router in almeno due interfacce di livello logico in modo che ognuna, dopo essere stata accuratamente configurata, potesse occuparsi di inoltrare il traffico mantenendo l'isolamento dei dati tra le VLAN.

I router della serie 1220, quindi R1, R2 ed R3, erano coinvolti ognuno in sole due VLAN, per cui si è messa in conto la creazione di due sub-interface per collegamento; mentre per i router della serie 2220, R5 ed R6, coinvolti in tre VLAN, si è prevista la creazione di tre sub-interface.

A ciascuna sub-interface è stato associato un indirizzo IP e un VID, coerentemente con la VLAN corrispondente. Mentre l'importanza dell'indirizzo IP nel contesto del routing tra VLAN è evidente, il ruolo del VID (VLAN IDentifier) è meno banale: esso viene assegnato alla sub-interface per indicare a quale VLAN appartiene il traffico instradato attraverso di essa. In altre parole, il VID è un meccanismo che consente ai dispositivi di rete di distinguere e gestire il traffico appartenente a diverse VLAN all'interno di una singola interfaccia fisica.

Per l'implementazione della configurazione è stata presa come riferimento la seguente tabella riassuntiva.

Router	VLAN consentite	Interfaccia	Indirizzo IP	VID
R1	16 51	0/0/0.16	192.168.16.1	16
		0/0/0.51	192.168.51.1	51
R2	23 52	0/0/0.23	192.168.23.2	23
		0/0/0.52	193.168.52.2	52
R3	23 36	0/0/0.23	192.168.23.3	23
		0/0/0.36	192.168.36.3	36
R5	10 51 52	0/0/0.51	192.168.51.5	51
		0/0/0.52	192.168.52.5	52
		0/0/0.10	192.168.10.5	10
R6	16 20 36	0/0/0.16	192.168.16.6	16
		0/0/0.36	192.168.36.6	36
		0/0/0.20	192.168.20.6	20

Ulteriori considerazioni hanno riguardato il fatto che ai fini della trasmissione fra VLAN gli host necessitano di un indirizzo IP appartenente allo spazio di indirizzi della VLAN 10 o 20. In particolare, è essenziale che PC1 appartenga alla VLAN 10 e PC2 alla VLAN 20. Per questo motivo si è previsto di configurare R5 ed R6 come DHCP server in modo che gli host, agendo come client, possano ricevere un indirizzo IP appropriato.

Per quanto riguarda gli switch, le scelte hanno riguardato due aspetti principali: l'assegnazione delle VLAN e l'aggregazione del link fra i due switch.

Assegnazione delle VLAN sugli switch

Il metodo di assegnazione VLAN scelto è basato su interfaccia, per cui le scelte riguardanti la configurazione si sono concentrate sul tipo di interfaccia e sulle VLAN consentite da ognuna.

La selezione dei vari tipi di interfaccia è stata determinata da considerazioni legate alla funzionalità e al flusso del traffico nella rete. Si è ritenuto appropriato configurare le interfacce coinvolte nel collegamento tra gli switch e i terminali come access interface, poiché queste interfacce sono destinate a dispositivi finali che non richiedono il supporto di VLAN multiple e devono invece essere assegnati a una singola VLAN.

Per quanto riguarda le interfacce coinvolte nel collegamento tra i due switch, è stato scelto l'utilizzo di trunk interface. Questo tipo di interfaccia è stato preferito in quanto consente il trasporto di più VLAN su un singolo collegamento, agevolando la gestione del traffico e garantendo una maggiore flessibilità nella distribuzione delle VLAN attraverso la rete.

Analogamente, è stata configurata l'interfaccia trunk tra gli switch e i router per consentire il passaggio esclusivo del traffico VLAN desiderato. Questa scelta è stata motivata dalla necessità di permettere ai router di interagire con più VLAN e svolgere funzioni di routing tra di esse, garantendo il controllo sul traffico VLAN.

Di seguito si riportano le tabelle riassuntive che hanno agevolato e velocizzato la configurazione dei dispositivi.

SW1		
Interfaccia	**Tipo**	**VLAN consentite**
0/0/1	Trunk	tutte
0/0/2	Trunk	tutte
0/0/3	Trunk	tutte
0/0/4	Trunk	tutte
0/0/5	Trunk	10 51 52
0/0/6	Trunk	16 20 36
0/0/7	Trunk	16 51
0/0/8	Access	10

SW2		
Interfaccia	**Tipo**	**VLAN consentite**
0/0/1	Trunk	tutte
0/0/2	Trunk	tutte
0/0/3	Trunk	tutte
0/0/4	Trunk	tutte
0/0/5	Trunk	23 52
0/0/6	Trunk	23 36
0/0/7	Access	20

Link Aggregation Group

Come anticipato nel precedente capitolo, la tecnologia LAG è stata sfruttata per ottimizzare le prestazioni della rete. Integrando più collegamenti fisici in un singolo collegamento logico, infatti, si ottiene un aumento della larghezza di banda

disponibile e si garantisce la stabilità dei collegamenti tra gli switch. Questo incremento della larghezza di banda deriva dalla distribuzione del traffico su più collegamenti fisici, ciascuno con la propria capacità di trasmissione. L'affidabilità dei collegamenti tra gli switch è stata ulteriormente potenziata mediante l'implementazione del load balancing, che ha consentito di riservare uno dei quattro collegamenti fisici disponibili in caso di malfunzionamento, incrementando così la ridondanza complessiva della rete.

3.1.3 Configurazione dei router

Dopo aver organizzato il lavoro si è potuto procedere alla vera e propria configurazione dei dispositivi, attraverso un dispositivo che funge da "terminal server" e rende disponibile la porta "console" (seriale RS-232) attraverso una connessione in Telnet. Nel presente paragrafo si intende descrivere dettagliatamente la configurazione dei router.

Innanzitutto, su ogni router sono state definite le relative VLAN, generate le sub-interface e ad ognuna è stato assegnato l'indirizzo IP e il VID. Di seguito sono riportati i comandi riservati a R1. Per quanto riguarda gli altri router, sono stati eseguiti sostanzialmente gli stessi comandi, ma riferiti alle VLAN in cui ognuno è coinvolto (si tenga presente la tabella precedentemente illustrata).

```
<R1>system-view
[R1]interface GigabitEthernet 0/0/0.16
[R1-GigabitEthernet0/0/0.16]ip address 192.168.16.1 24
[R1-GigabitEthernet0/0/0.16]dot1q termination vid 16
[R1-GigabitEthernet0/0/0.16]interface GigabitEthernet 0/0/0.51
[R1-GigabitEthernet0/0/0.51]ip address 192.168.51.1 24
[R1-GigabitEthernet0/0/0.51]dot1q termination vid 51
[R1-GigabitEthernet0/0/0.51]quit
```

Successivamente, è stato abilitato il protocollo di routing OSPF su ogni router, tenendo chiaramente presente le VLAN e quindi gli spazi di indirizzi di pertinenza di ogni router.

```
[R1]ospf 1 router-id 1.1.1.1
[R1-ospf-1]area 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 192.168.16.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 192.168.51.0 0.0.0.255

[R2]ospf 1 router-id 2.2.2.2
[R2-ospf-1]area 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 192.168.23.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.52.0 0.0.0.255

[R3]ospf 1 router-id 3.3.3.3
[R3-ospf-1]area 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 192.168.23.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 192.168.36.0 0.0.0.255

[R5]ospf 1 router-id 5.5.5.5
[R5-ospf-1]area 0.0.0.0
[R5-ospf-1-area-0.0.0.0]network 192.168.10.0 0.0.0.255
[R5-ospf-1-area-0.0.0.0]network 192.168.51.0 0.0.0.255
[R5-ospf-1-area-0.0.0.0]network 192.168.52.0 0.0.0.255
[R5-ospf-1-area-0.0.0.0]quit

[R6]ospf 1 router-id 6.6.6.6
[R6-ospf-1]area 0.0.0.0
[R6-ospf-1-area-0.0.0.0]network 192.168.16.0 0.0.0.255
[R6-ospf-1-area-0.0.0.0]network 192.168.20.0 0.0.0.255
```

```
[R6-ospf-1-area-0.0.0.0]network 192.168.36.0 0.0.0.255
```

Si è provveduto poi ad abilitare il protocollo DHCP su R5 ed R6. Esistono due possibilità per la configurazione di un DHCP server: la modalità global e su singola interfaccia. La modalità global prevede la creazione di un pool di indirizzi IP assegnabili e altre informazioni di configurazione come l'indirizzo IP del gateway e del DNS. Caratteristica di questa modalità di configurazione è che è accessibile a tutta la rete, per cui viene definita una volta e abilitata sulle interfacce del router cui gli host si agganceranno. D'altra parte, quando il DHCP è configurato direttamente su una singola interfaccia, le sue informazioni di configurazione sono limitate solo ai dispositivi che si connettono tramite quella specifica interfaccia.
Si è optato per l'utilizzo della modalità global su R5 e su singola interfaccia su R6. Di seguito sono riportati i comandi inseriti su ogni router.

```
[R5]dhcp enable
[R5]ip pool poolR5
[R5-ip-pool-poolR5]network 192.168.10.0 mask 255.255.255.0
[R5-ip-pool-poolR5]gateway-list 192.168.10.5
[R5-ip-pool-poolR5]dns-list 192.168.10.5
[R5-ip-pool-poolR5]lease day 90 hour 0 minute 0
[R5-ip-pool-poolR5]quit
[R5]interface GigabitEthernet 0/0/0.10
[R5-GigabitEthernet0/0/0.10]dhcp select global
```

```
[R6]dhcp enable
[R6]interface GigabitEthernet 0/0/0.20
[R6-GigabitEthernet0/0/0.20]dhcp select interface
[R6-GigabitEthernet0/0/0.20]dhcp server dns-list 192.168.20.6
[R6-GigabitEthernet0/0/0.20]dhcp server lease day 5 hour 0
minute 0
```

3.1.4 Configurazione degli switch

A differenza dei router, negli switch sono state create tutte le VLAN esistenti nella rete, poiché il traffico VLAN, nel raggiungere i diversi router, deve necessariamente passare per gli switch. Dopo questa operazione, è stato realizzato il link aggregation fra i quattro link fisici che collegano SW1 e SW2. È stata dunque creata e configurata un'interfaccia Eth-Trunk e aggiunte le 4 interfacce relative ai collegamenti in questione.

```
[SW1]VLAN batch 10 16 20 23 36 51 52
[SW1]interface Eth-Trunk1
[SW1-Eth-Trunk1]mode manual load-balance
[SW1-Eth-Trunk1]trunkport GigabitEthernet 0/0/1 to 0/0/4
[SW1-Eth-Trunk1]port link-type trunk
[SW1-Eth-Trunk1]port trunk allow-pass VLAN all
[SW1-Eth-Trunk1]load-balance dst-ip
```

Successivamente, tenendo presente lo schema di riferimento, ci si è occupati della configurazione delle interfacce restanti:

```
[SW1-GigabitEthernet0/0/5]port link-type trunk
[SW1-GigabitEthernet0/0/5]port trunk allow-pass VLAN 1 10 51 52

[SW1-GigabitEthernet0/0/6]port link-type trunk
[SW1-GigabitEthernet0/0/6]port trunk allow-pass VLAN 1 16 20 36

[SW1-GigabitEthernet0/0/7]port link-type trunk
[SW1-GigabitEthernet0/0/7]port trunk allow-pass VLAN 1 16 51

[SW1-GigabitEthernet0/0/8]port link-type access
[SW1-GigabitEthernet0/0/8]port default VLAN 10
```

La configurazione di SW2 non viene riportata in quanto analoga a quella di SW1.

3.1.5 Test

Durante la fase di test della rete, è stato eseguito un controllo approfondito per verificare l'efficacia delle configurazioni implementate sui dispositivi di rete. Questi test si sono concentrati principalmente sulla verifica delle tabelle di routing dei router al fine di garantire la corretta presenza delle rotte OSPF e delle relative metriche per raggiungere punti specifici della rete. Inoltre, è stato esaminato il comando "display current configuration" per confermare l'effettività delle configurazioni inserite negli apparati. Questa analisi dettagliata è stata fondamentale per assicurare che le impostazioni di rete fossero state applicate correttamente e che rispecchiassero le necessità progettuali. Infine, è stato eseguito il comando *ping* per testare la connettività tra i diversi dispositivi di rete e verificare il corretto funzionamento delle comunicazioni all'interno della rete. Mediante questi metodi di test, è stato possibile identificare e risolvere eventuali problemi di configurazione o di connettività, assicurando il corretto funzionamento e la stabilità della rete.

3.2 Revisione della Topologia di Rete

3.2.1 Descrizione delle modifiche

Una volta realizzata la rete nel rispetto della topologia logica, si è reso necessario passare al secondo obiettivo principale del progetto, ovvero lo sviluppo di un software in grado di monitorare il traffico dati della rete e di stabilire una rotta statica che lo indirizzasse su un percorso di routing alternativo.

Sebbene la configurazione di questo software non sia descritta in dettaglio nella presente trattazione, poiché il focus della tesi è sull'adeguamento della rete alla topologia logica fornita, è opportuno menzionare brevemente i passaggi preliminari necessari al suo sviluppo in quanto i problemi riscontrati durante questa fase hanno richiesto una revisione completa dell'intera topologia di rete.

Per consentire al software, e quindi al terminale da cui viene eseguito, di accedere alla configurazione di rete, è stata inizialmente implementata una connessione ritenuta appropriata per il contesto. La scelta è ricaduta sull'utilizzo della connessione SSH, per le sue caratteristiche di sicurezza e affidabilità nel garantire l'accesso remoto ai dispositivi di rete. Successivamente, è stato impiegato il protocollo SNMP (Simple Network Management Protocol) per effettuare interrogazioni sulla rete e acquisire le informazioni di traffico necessarie per il monitoraggio. La capacità di SNMP di estrarre dati in tempo reale è stata rilevante; tuttavia, durante l'analisi dei dati, è emerso un problema cruciale: sui router di interesse, ovvero R5 ed R6, non era possibile distinguere il traffico delle interfacce logiche (sub-interface) da quello delle interfacce fisiche. Questa distinzione, essenziale per impostare le soglie di monitoraggio in modo appropriato, ha comportato modifiche significative all'architettura di rete.

Il dilemma relativo al monitoraggio del traffico VLAN e all'accesso alle interfacce logiche è stato risolto fondamentalmente mediante l'introduzione di nuove connessioni fisiche e l'evitamento, ove problematico, dell'utilizzo delle sub-interface. Partendo dall'analisi di *figura 4*, che offre una panoramica generale della nuova topologia, si procede all'enumerazione e alla dettagliata descrizione delle modifiche apportate, le quali hanno determinato la configurazione finale.

Per quanto riguarda il livello fisico, innanzitutto, è stato introdotto lo switch SW3, che svolge il ruolo di punto di convergenza di tutti i router, nonché di PC1 e PC2. Il cablaggio che ne è conseguito riguarda dunque tutti i router: ognuno ha riservato un'interfaccia fisica per il collegamento in questione. In particolare, i router R1, R2 ed R3 hanno impegnato per lo scopo l'interfaccia GigabitEthernet 0/0/1, mentre i router R5 ed R6 hanno utilizzato l'interfaccia GigabitEthernet 0/0/2. Poiché R5 e R6 sono responsabili del monitoraggio del traffico, è stato necessario dotarli di un'interfaccia fisica dedicata alle VLAN. Di conseguenza, oltre al link fisico preesistente tramite l'interfaccia 0/0/0, è stato aggiunto per ciascuno un collegamento supplementare attraverso le interfacce 0/0/1.

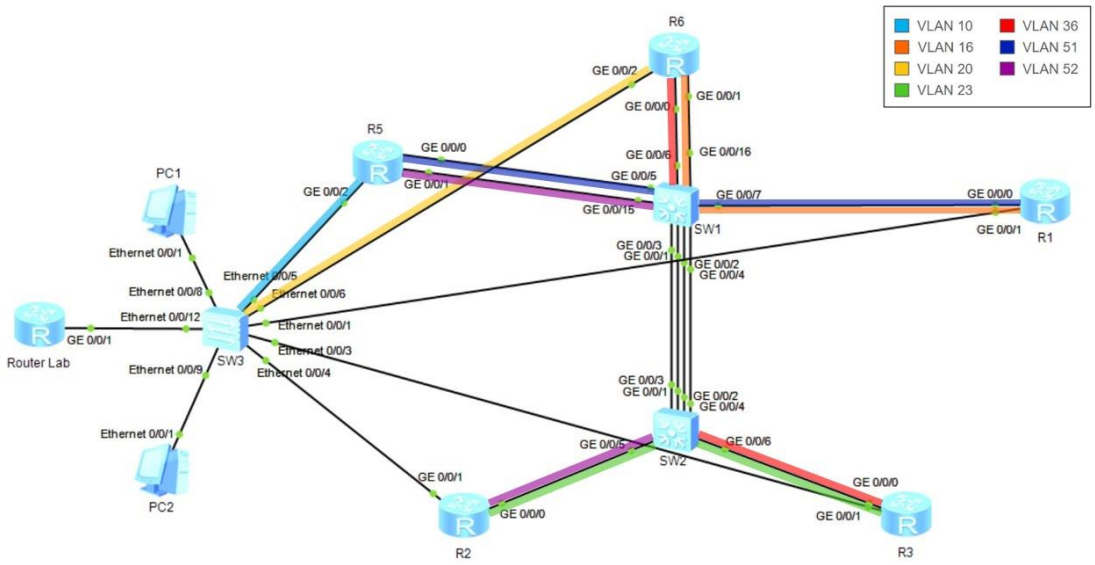

Figura 4 - Topologia fisica definitiva

Le modifiche apportate a livello fisico hanno richiesto delle correzioni nella configurazione della rete. Come precedentemente indicato, il traffico VLAN sui router R5 e R6 è stato suddiviso a livello fisico. Questa modifica ha comportato non solo la rimozione delle sub-interface dalle interfacce GigabitEthernet 0/0/0, ma anche la loro riconfigurazione per integrare le interfacce 0/0/1 aggiuntive. Sia le interfacce 0/0/0 che le 0/0/1 di R5 e R6 sono state configurate come interfacce di tipo trunk con VLAN ID relativo al collegamento corrispondente, come illustrato nell'immagine di riferimento. Inoltre, le interfacce 0/0/2 dei suddetti router sono state configurate come sub-interface, in modo tale che il traffico da esse attraversato venga etichettato con VID 10 per R5 e 20 per R6, come illustrato nell'immagine di riferimento. Anche la configurazione di SW1 è stata soggetta ad adeguamenti significativi. Precisamente, la VLAN 52 è stata rimossa dall'elenco delle VLAN consentite sull'interfaccia trunk 0/0/5 e aggiunta alla nuova interfaccia 0/0/15, anch'essa configurata di tipo trunk. Analogamente, la VLAN 36 è stata esclusa dall'interfaccia trunk 0/0/6 e inserita nella nuova interfaccia 0/0/16, che è stata configurata allo stesso modo.

Infine, per SW3 è stato sufficiente configurare le interfacce 0/0/5 e 0/0/6 come interfacce di tipo trunk, limitando l'accesso alla sola VLAN 10 per la prima e alla VLAN 20 per la seconda. Le interfacce destinate ai terminali sono state configurate come interfacce di tipo access.

Attraverso le suddette modifiche, è stato assicurato il coerente funzionamento logico della topologia di rete, risolvendo con successo il problema relativo all'inaccessibilità dei dati relativi al traffico sulle interfacce logiche (sub-interface), circostanza fondamentale ai fini del progetto. Un punto chiave di distinzione rispetto alla configurazione di rete precedente risiede nell'allocazione del traffico VLAN su molteplici collegamenti fisici per i router R5 ed R6, ciascuno corrispondente a una specifica VLAN.

3.2.1 Configurazioni

A completezza e riepilogo di quanto appena esposto riguardo alla nuova configurazione, di seguito sono riportate le voci relative alle interfacce aggiunte e modificate in ciascun router e switch, restituite dal comando 'display current configuration'.

R1:

```
interface GigabitEthernet0/0/1
 ip address 10.100.0.5 255.255.255.0
```

R2:

```
interface GigabitEthernet0/0/1
 ip address 10.100.0.8 255.255.255.0
```

R3:

```
interface GigabitEthernet0/0/1
 ip address 10.100.0.5 255.255.255.0
```

R5:

```
interface GigabitEthernet0/0/0
```

```
 ip address 192.168.51.5 255.255.255.0
 ospf dr-priority 20
interface GigabitEthernet0/0/1
 ip address 192.168.52.5 255.255.255.0
interface GigabitEthernet0/0/2
 ip address 10.100.0.9 255.255.255.0
interface GigabitEthernet0/0/2.10
 dot1q termination vid 10
 ip address 192.168.10.5 255.255.255.0
 dhcp select global
```

R6:

```
interface GigabitEthernet0/0/0
 ip address 192.168.16.6 255.255.255.0
interface GigabitEthernet0/0/1
 ip address 192.168.36.6 255.255.255.0
interface GigabitEthernet0/0/2
 ip address 10.100.0.10 255.255.255.0
interface GigabitEthernet0/0/2.20
 dot1q termination vid 20
 ip address 192.168.20.6 255.255.255.0
 dhcp select interface
 dhcp server lease day 5 hour 0 minute 0
 dhcp server dns-list 192.168.20.6
```

SW1:

```
interface GigabitEthernet0/0/5
 port link-type trunk
```

```
 port trunk pvid vlan 51
 port trunk allow-pass vlan 51
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk pvid vlan 16
 port trunk allow-pass vlan 16
interface GigabitEthernet0/0/15
 port link-type trunk
 port trunk pvid vlan 52
 port trunk allow-pass vlan 52
interface GigabitEthernet0/0/16
 port link-type trunk
 port trunk pvid vlan 36
 port trunk allow-pass vlan 36
```

SW3:

```
interface GigabitEthernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 10
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk allow-pass vlan 20
interface GigabitEthernet0/0/8
 port link-type access
 port default vlan 10
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 20
```

3.3 Sviluppo del software per l'ottimizzazione del traffico di rete

Questo capitolo si propone di fornire una breve panoramica del software sviluppato per consentire alla rete di operare in modo intelligente. Il linguaggio di programmazione scelto per l'implementazione è stato Python, mentre l'interfaccia grafica è stata realizzata tramite QT Designer.

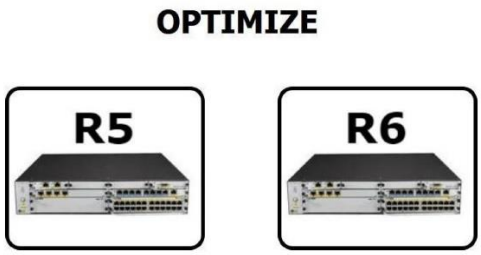

Figura 5 - Interfaccia utente iniziale

L'applicazione, una volta avviata, presenta all'utente una schermata iniziale dalla quale è possibile selezionare il router di interesse tra R5 e R6 per visualizzare le statistiche relative all'utilizzo delle interfacce. Tuttavia, il sistema non si limita alla mera visualizzazione dello stato delle interfacce e del percorso dei pacchetti da R5 a R6, ma implementa un'effettiva gestione del traffico. In particolare, monitora costantemente la percentuale di utilizzo delle interfacce del router selezionato e, se questa supera una determinata soglia, attiva una rotta statica con una priorità più elevata, deviando il percorso dei pacchetti su un percorso fisico alternativo.

La struttura del codice Python che realizza questa funzionalità è organizzata in moduli e package, seguendo i principi della programmazione orientata agli oggetti. All'interno di questi, ciascun metodo svolge un ruolo specifico. Particolarmente significativo è il metodo '`switchTraffic`', responsabile dell'ottimizzazione della rete e dell'esecuzione della commutazione del traffico. Questo metodo utilizza il metodo '`splitOutput`' per ottenere le percentuali di utilizzo in ingresso e in uscita delle interfacce dei router R5 e R6. Successivamente, se una delle percentuali supera la soglia superiore definita, viene impostata una rotta statica. Nel caso in cui

tutte le percentuali scendano al di sotto della soglia inferiore definita, la rotta statica viene rimossa. Altri metodi e moduli gestiscono altri aspetti del software, inclusa l'interfaccia grafica.

In conclusione, anche dal punto di vista del software, l'obiettivo di ottimizzare le prestazioni della rete è stato pienamente raggiunto. La soluzione implementata consente una gestione dinamica e automatizzata del traffico di rete, migliorando l'efficienza complessiva dell'infrastruttura.

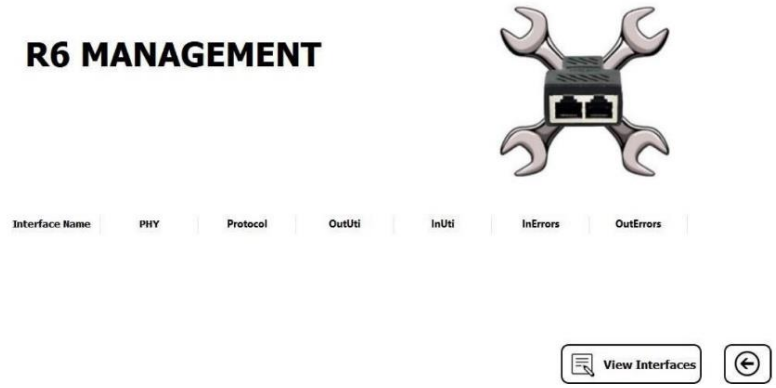

Figura 6 - Interfaccia per il riepilogo dei dati di R6

4. Verifica finale

Dopo il completamento delle configurazioni della topologia di rete e del software applicativo, è stata avviata la fase di test. Le verifiche riguardanti l'integrità della configurazione di rete sono state condotte principalmente utilizzando le stesse metodologie precedentemente impiegate, che includono un'attenta analisi delle tabelle di routing (si vedano le figure 7 e 8) e delle configurazioni dei singoli dispositivi di rete tramite il comando 'display current configuration' e la verifica della raggiungibilità della rete tramite l'implementazione di vari comandi 'ping' opportunamente indirizzati.

```
<R5> dis ip rou
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
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 7 - Tabella di routing di R5

```
<R6> dis ip rou
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
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       InLoopBack0S
   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 8 - Tabella di routing di R6

I test di verifica del software sono stati condotti utilizzando iPerf, un'applicazione che opera su un modello client-server. Questo strumento ha permesso di generare traffico dati per valutare le prestazioni della rete. Nel dettaglio, il client ha inviato dati al server tramite la rete, mentre il server ha misurato le performance della connessione. La flessibilità di iPerf ha consentito di definire il numero e le dimensioni dei pacchetti inviati, consentendo di stressare il sistema e valutare la sua capacità di superare le soglie prestabilite. Un elemento significativo è stato il monitoraggio delle percentuali di traffico sulle interfacce, che ha evidenziato l'effettiva commutazione del traffico avvenuta grazie al software.

In conclusione, i test condotti mediante l'utilizzo di iPerf hanno fornito una valutazione esaustiva delle prestazioni del software implementato, confermando la correttezza delle configurazioni adottate e il conseguimento degli obiettivi di progetto.

5. Conclusioni e proposte di sviluppo

Grazie alla conferma degli esiti dei test, le conclusioni di questa tesi riflettono il successo nel raggiungimento degli obiettivi prefissati nell'ambito della network programmability.

Il presente lavoro ha voluto approfondire la progettazione e realizzazione della complessa architettura di rete alla base dell'utilizzo del software di gestione dinamica sviluppato. Lo studio ha evidenziato l'importanza di un funzionamento corretto e perfettamente compatibile con le specifiche relative alle dinamiche operative della rete, che vanno oltre la semplice configurazione dei collegamenti fisici.

Il progetto si è concluso con la consapevolezza che vi è ampio margine di miglioramento. Un primo aspetto riguarda la sicurezza, che potrebbe beneficiare di una configurazione più robusta dei firewall e della NAT. Altre possibilità di miglioramento riguardano un'ulteriore ottimizzazione del software, ad esempio riducendo i tempi di monitoraggio e introducendo criteri avanzati per la commutazione del traffico. Inoltre, potrebbe essere interessante esplorare modi per acquisire i dati relativi al traffico delle interfacce logiche, in modo da poter sfruttare la configurazione iniziale ed evitare l'impiego di dispositivi di rete aggiuntivi.

Questo, insieme ai numerosi studi pubblicati di recente sulle reti con topologie dinamiche definite tramite software, dimostra l'ampia attenzione e lo sviluppo in corso in tutto il mondo riguardo agli argomenti trattati. Tale interesse è alimentato dalle crescenti esigenze in ambito tecnologico, sempre più indispensabili.

Bibliografia e sitografia

Huawei Technologies Co., Ltd., “Data Communications and Network Technologies,” Springer, 2021.

M. Marconi, “Networking in ambito industriale applicato all’ottimizzazione delle prestazioni di rete”, Tesi di laurea, Università Politecnica delle Marche, 2023.

S. S. W. Lee and K. -Y. Li, "Study of Dynamic Topology Change for Total Energy Consumption in Green IP Networks," *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, 2013.

A. M. Mazin, R. A. Rahman, M. Kassim and A. R. Mahmud, "Performance Analysis on Network Automation Interaction with Network Devices Using Python," *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2021.

Praveen N and K. Kumar, "Software-defined networking: Reconfigurable network systems in LAN topology," *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2016.

G. Milios, “Network automation using Python,” report, 2021.

Mihăilă, Paul et al. "Network Automation and Abstraction using Python Programming Methods." *MACRo 2015* vol. 2,1 (2017).

Huawei - https://e.huawei.com/en/talent/outPage/#/sxz-course/home?courseId=tpDnx8BSoUVoUNyOKHI5UTQi-oc

ICS Lite - http://127.0.0.1:51299/icslite/#hash=onlinesearch

RFC Editor – https://www.rfc-editor.org/

iPerf – https://iperf.fr/iperf-doc.php

Paramiko – https://www.paramiko.org/