



UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea in Ingegneria Informatica e dell'Automazione

Tesi di Laurea

TECNOLOGIE DI NETWORKING IN AMBITO ENTERPRISE

ENTERPRISE NETWORKING TECHNOLOGIES

Relatore:

Prof. Ennio Gambi

Tesi di Laurea di:

Daniele Gjeka

Correlatore:

Prof. Adelmo De Santis

A.A. 2020/2021

Sommario

1.0 Introduzione	3
2.0 Strumenti	6
2.1 eNSP	6
2.2 Wireshark	7
3.0 Assegnazione spazio di indirizzi	9
3.1 Configurazione degli spazi di indirizzi	10
4.0 Link Aggregation	14
4.1 Configurazione Link Aggregation	15
5.0 Vlan	19
5.1 Configurazione VLAN	21
5.2 VLAN Routing	25
5.2.1 Configurazione VLAN Routing	26
6.0 STP	31
6.1 RSTP	38
6.1.1 Configurazione RSTP	38
7.0 OSPF	41
7.1 Configurazione OSPF	43
8.0 ACL	46
9.0 NAT	48
9.1 Configurazione NAT	50
10.0 DMZ	55
10.1 Configurazione DMZ	55
11.0 Conclusioni	62
12.0 Bibliografia	62

1.0 Introduzione

Il presente elaborato di tesi presenta l'analisi che ha portato allo sviluppo e alla risoluzione della topologia di rete assegnatami dal correlatore Prof. Adelmo De Santis.

Una parte importante del periodo di tirocinio è stata caratterizzata dallo studio dei contenuti del corso HCIA Routing e Switching della multinazionale Huawei, con il fine di apprendere al meglio i concetti teorici che rappresentano le fondamenta delle tecnologie necessarie per la corretta configurazione della topologia di rete, ma, in generale, adoperate in tutto il mondo del network; questa fase di preparazione e apprendimento si è conclusa con il conseguimento di una certificazione Huawei.

In ogni azienda, ufficio o casa, è facile imbattersi in una rete privata. Grazie al costante sviluppo delle tecnologie di networking, inoltre, è aumentata l'efficienza con cui gli utenti di un'azienda riescono a comunicare e scambiarsi informazioni in modo rapido, senza la necessità di trovarsi fisicamente nello stesso luogo.

Risulta evidente che, in ambito aziendale, un'adeguata gestione dei calcolatori è fondamentale: permette un'ottimizzazione dei costi e della gestione delle risorse, l'incremento della produttività e della sicurezza.

Una delle principali caratteristiche che stanno alla base dell'architettura delle "Enterprise Network" è la ridondanza: collegamenti ridondanti consentono infatti di aumentare la robustezza della rete e sono di fondamentale aiuto per fare in modo che il guasto di un collegamento o di una macchina non comprometta il funzionamento dell'intera rete, poiché il segnale ha a disposizione più percorsi per arrivare a destinazione.

Un altro strumento fondamentale per l'attività aziendale è, ovviamente, Internet. Al giorno d'oggi, infatti, molte imprese fondano il proprio business sulla fornitura di servizi, come ad esempio siti web, agli utenti pubblici. Tali servizi sono tendenzialmente risiedenti all'interno di un server, quindi un software o un dispositivo hardware, all'interno del quale sono allocate le risorse e messe poi a disposizione di coloro che ne fanno richiesta.

Per l'azienda è dunque di primaria importanza immagazzinare queste informazioni all'interno di adeguati supporti informatici, i quali devono garantire sicurezza e difesa dei dati.

In particolare, la topologia di rete conferitami è stata progettata ad hoc per trattare la maggior parte delle tecnologie necessarie alla realizzazione di un sistema efficiente ed allo stesso tempo sicuro, simulando quella che può essere la struttura di una rete in ambito enterprise.

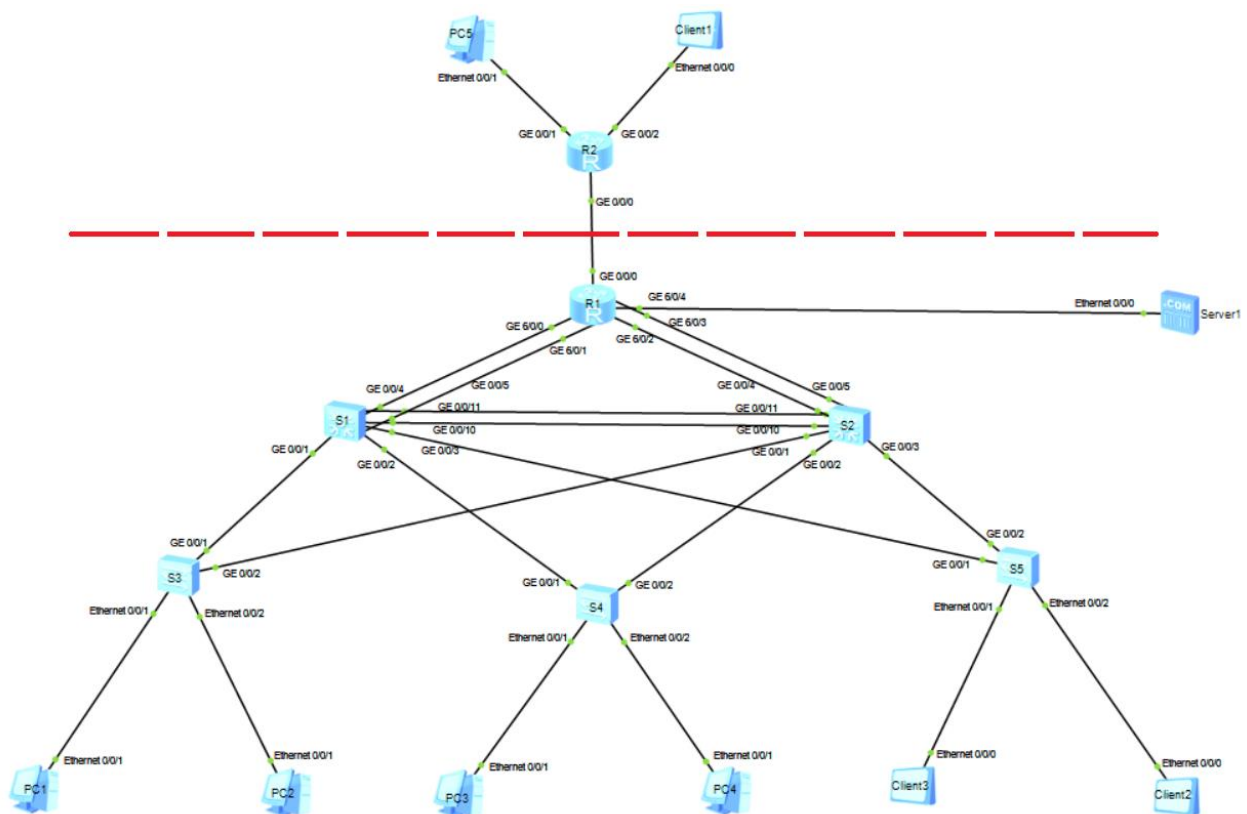


Figura 1 - Topologia di rete

Osservando nel complesso la figura 1, è possibile notare come la topologia di rete possieda una struttura che può essere considerata la simulazione di una rete standard adoperata in ambito enterprise, nella quale la parte sottostante al router R1 rappresenta la rete privata aziendale, mentre la sezione soprastante rappresenta Internet, ipotizzando quindi che R2 sia un router dell'ISP (Internet Service Provider).

In particolare, sulla base delle nozioni teoriche precedentemente apprese durante il corso HCIA, l'obiettivo è stato quello di studiare una soluzione che venisse poi configurata manualmente e che portasse al corretto funzionamento della topologia di rete in tutte le sue funzionalità, tenendo conto di una serie di requisiti di progetto:

- ✓ Assegnare uno spazio di indirizzi alle reti presenti.
- ✓ Configurare tre VLAN all'interno della rete privata. In particolare, gli host PC1, PC4 e Client3 appartenenti alla VLAN 10, gli host PC2, PC3 e Client2 appartenenti alla VLAN 20 ed il Server 1 appartenente alla VLAN 30.
- ✓ Configurare NAT per la VLAN 10 e verificarne il funzionamento.
- ✓ Configurare RSTP.

- ✓ Considerare il Server1 appartenente ad una DMZ, dove:
 - I. La porta 80 deve essere raggiungibile dall'esterno (PC5 - Client1)
 - II. Non deve essere raggiungibile dalla VLAN 20
- ✓ I nodi di tutte le VLAN devono potere comunicare tra loro.

2.0 Strumenti

2.1 eNSP

Il progetto è stato sviluppato utilizzando il software eNSP (Enterprise Network Simulation Platform). Si tratta di uno strumento molto potente che supporta la simulazione di una rete su larga scala in tutti i minimi dettagli. L'interfaccia grafica di eNSP si presenta così:

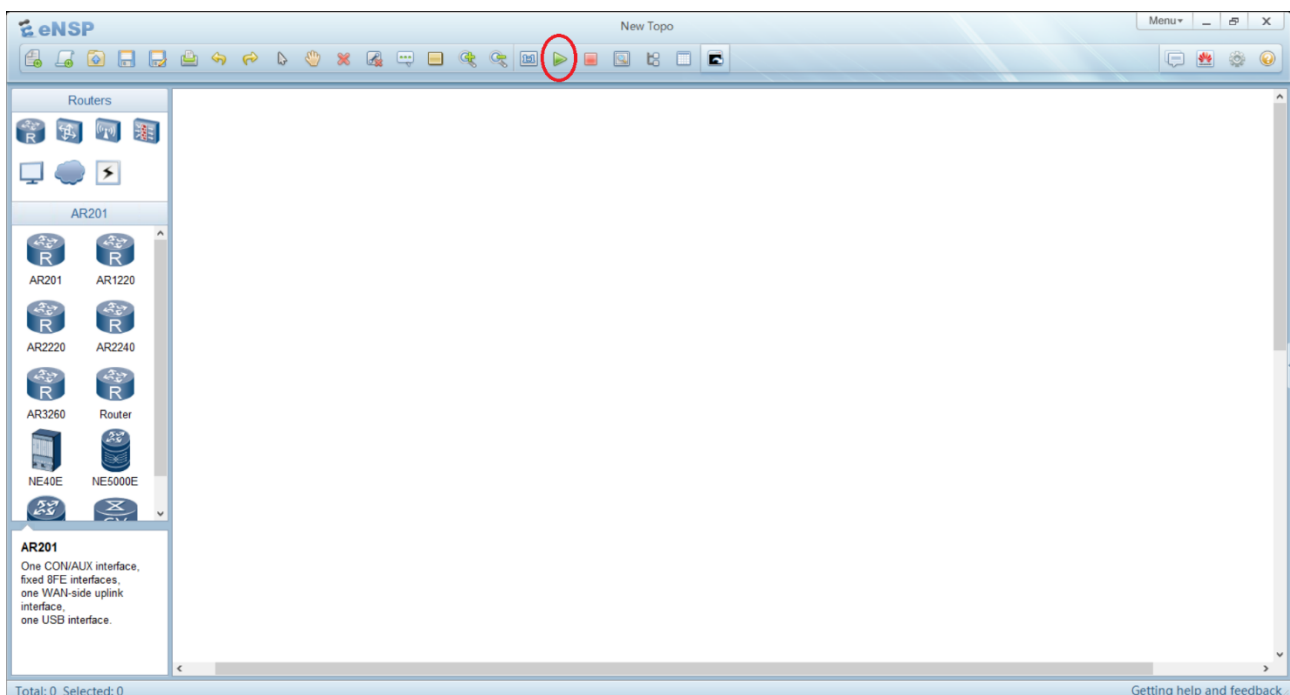


Figura 2 - Interfaccia grafica eNSP

Nella sezione a sinistra è presente un menù composto da una serie di icone relative a diverse componenti hardware e software ordinariamente utilizzate per la creazione di topologie di rete, più o meno complesse.

Dopo aver costruito la topologia di rete di nostro interesse trascinando i dispositivi nella zona bianca, è possibile avviarli effettuando un click sul triangolo verde cerchiato di colore rosso, visualizzabile nella figura 2.

Successivamente, effettuando un doppio click su qualsiasi icona, verrà visualizzata immediatamente l'interfaccia terminale, la quale permette l'effettiva configurazione del dispositivo in base alle proprie necessità.

Esiste una struttura gerarchica dei comandi assegnabili all'interno del terminale di ciascun dispositivo.

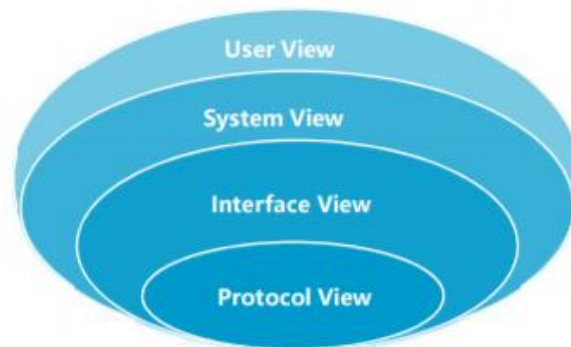


Figura 3 - Gerarchia view in eNSP

Ciascuno strato della figura 3 corrisponde ad una view, ognuna delle quali abilita all'esecuzione di determinati comandi. La prima view che si visualizza all'apertura di un qualsiasi dispositivo è chiamata user-view, la quale consente di osservare delle statistiche generali ed eseguire semplici comandi.

La view successiva, chiamata system-view, consente all'utente di configurare i parametri di sistema in base alle proprie esigenze ed è accessibile eseguendo il comando *system-view* a partire dalla user-view iniziale.

Di seguito sono presenti la interface-view e la protocol-view, all'interno delle quali è possibile configurare rispettivamente i parametri delle interfacce e dei protocolli adoperati nella topologia di rete.

2.2 Wireshark

Un ulteriore strumento software largamente adoperato è Wireshark. Esso consiste in un software versatile attraverso il quale si ha la possibilità di analizzare e tracciare nel dettaglio i pacchetti che transitano su ciascuna interfaccia dei dispositivi presenti nella topologia di rete.

Wireshark, a seguito del download, verrà automaticamente incluso all'interno di eNSP, poiché si tratta di una delle funzionalità di default. Effettuando un click con il tasto destro su un qualsiasi dispositivo, e proseguendo nella voce 'CaptureData', verrà visualizzato un menu contenente tutte le interfacce attive in quel dato momento sul dispositivo.

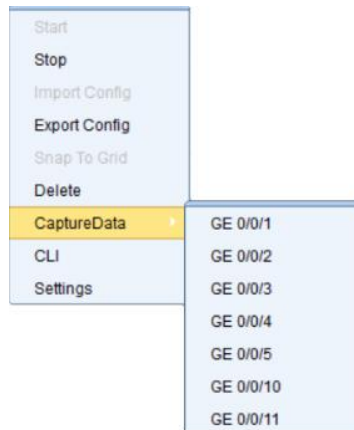


Figura 4 - Menu con interfacce ispezionabili

Dopo aver selezionato le interfacce che verranno poi ispezionate, apparirà la schermata di Wireshark, contenente un elenco di informazioni dettagliate che possono risultare fondamentali nella risoluzione di molteplici problematiche.

No.	Time	Source	Destination	Protocol	Length	Info
36	46.672000	HuaweiTe_fb:6d:0e	Broadcast	ARP	64	who has 192.168.10.4? Tell 192.168.10.1
37	46.735000	HuaweiTe_72:1e:8e	HuaweiTe_fb:6d:0e	ARP	64	192.168.10.4 is at 54:89:98:72:1e:8e
38	46.766000	192.168.10.1	192.168.10.4	ICMP	78	Echo (ping) request id=0xd3f5, seq=1/256, ttl=128 (reply in 39)
39	46.813000	192.168.10.4	192.168.10.1	ICMP	78	Echo (ping) reply id=0xd3f5, seq=1/256, ttl=128 (request in 38)
40	47.829000	192.168.10.1	192.168.10.4	ICMP	78	Echo (ping) request id=0xd4f5, seq=2/512, ttl=128 (reply in 41)
41	47.860000	192.168.10.4	192.168.10.1	ICMP	78	Echo (ping) reply id=0xd4f5, seq=2/512, ttl=128 (request in 40)
42	48.313000	192.168.20.254	224.0.0.5	OSPF	78	Hello Packet
43	48.563000	HuaweiTe_45:5e:f7	Spanning-tree-(for-...	STP	60	RST. Root = 4096/0/00:e0:fc:0b:49:fd Cost = 10000 Port = 0x8003
44	48.891000	192.168.10.1	192.168.10.4	ICMP	78	Echo (ping) request id=0xd5f5, seq=3/768, ttl=128 (reply in 45)
45	48.938000	192.168.10.4	192.168.10.1	ICMP	78	Echo (ping) reply id=0xd5f5, seq=3/768, ttl=128 (request in 44)
46	49.969000	192.168.10.1	192.168.10.4	ICMP	78	Echo (ping) request id=0xd6f5, seq=4/1024, ttl=128 (reply in 47)
47	50.032000	192.168.10.4	192.168.10.1	ICMP	78	Echo (ping) reply id=0xd6f5, seq=4/1024, ttl=128 (request in 46)
48	50.844000	HuaweiTe_45:5e:f7	Spanning-tree-(for-...	STP	60	RST. Root = 4096/0/00:e0:fc:0b:49:fd Cost = 10000 Port = 0x8003
49	51.047000	192.168.10.1	192.168.10.4	ICMP	78	Echo (ping) request id=0xd7f5, seq=5/1280, ttl=128 (reply in 50)

```

> Frame 38: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface -, id 0
▼ Ethernet II, Src: HuaweiTe_fb:6d:0e (54:89:98:fb:6d:0e), Dst: HuaweiTe_72:1e:8e (54:89:98:72:1e:8e)
  > Destination: HuaweiTe_72:1e:8e (54:89:98:72:1e:8e)
  > Source: HuaweiTe_fb:6d:0e (54:89:98:fb:6d:0e)
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
▼ Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf5d2 (62930)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x6f98 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.1
    Destination: 192.168.10.4
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xb287 [correct]

```

Figura 5 - Risultato Wireshark

3.0 Assegnazione spazio di indirizzi

Gli indirizzi IP sono composti da 32 bit (4 byte) suddivisi in 4 gruppi da 8 bit (1 byte), separati ciascuno da un punto e servono per identificare le reti e gli host che ne fanno parte.

Gli indirizzi IP si compongono di due sezioni: la sezione rete (network) è utilizzata per l'instradamento a livello geografico mentre la sezione host consente di identificare il nodo al quale sono destinati i dati del pacchetto.

Altro parametro fondamentale è la subnet mask (maschera di sottorete), che definisce la dimensione, intesa come intervallo di indirizzi, della sottorete IP, chiamata anche *subnet*, a cui appartiene un host.

La subnet mask consiste in un valore binario di 32 bit che determina quali bit, attraverso una serie di 1 consecutivi, rappresentano la sezione rete dell'indirizzo IP sulla quale viene applicata; i restanti bit rappresentano la sezione host e sono una serie di 0 consecutivi.

Utilizzando la notazione *Prefix Length* è possibile identificare più velocemente la subnet mask di un qualsiasi indirizzo IP come $/[numero\ di\ bit\ a\ 1]$. Ciò significa che una subnet mask $/24$ corrisponde alla notazione binaria 11111111.11111111.11111111.00000000 ed alla notazione decimale 255.255.255.0.

Quindi, in particolare, la sezione rete consente di individuare il massimo numero di sottoreti istanziabili con quel determinato indirizzo IP, mentre la sezione host specifica il massimo numero di host supportati per ciascuna sottorete stessa.

Esistono tre classi di range di indirizzi IP privati assegnabili: classe A, B e C.

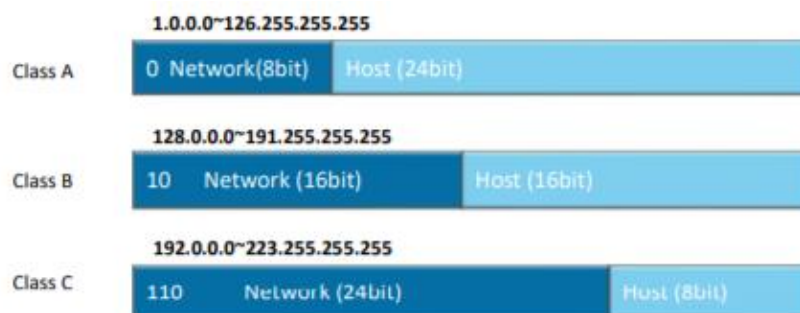


Figura 6 - Classi degli indirizzi IP assegnabili

Le reti Ethernet si caratterizzano per la poca scalabilità, ovvero perdono di efficienza e prestazioni all'aumentare dal numero di host che le compongono.

Gli indirizzi IP di classe C rappresentano la soluzione più equilibrata tenendo conto della problematica appena descritta, poiché permettono di istanziare potenzialmente oltre due milioni di sottoreti (2^{21}) ciascuna delle quali è capace di supportare 2^8-2 host, per un totale di 254 [1].

Osservando la figura 6 si può dedurre che, nel caso di un indirizzo di classe A, la corrispondente notazione *Prefix Length* sarà /8, per gli indirizzi di classe B sarà /16 mentre per quelli di classe C sarà /24, trattandosi del numero di bit a 1 dell'identificatore di rete.

Relativamente alla topologia di rete oggetto di studio, si suppone che si tratta della simulazione di una realtà potenzialmente in crescita, nella quale non saranno presenti solamente i pochi host che troviamo in figura 1, bensì vi può essere la necessità di aumentare il numero di sottoreti in un futuro prossimo.

Per questo motivo, sono stati assegnati spazi di indirizzi di classe C (quindi con subnet mask /24) a tutti i segmenti di rete, ad eccezione di quello che collega i due router R1 e R2. Infatti, essendo necessari al massimo due indirizzi IP da associare alle singole interfacce GigabitEthernet 0/0/0 di ciascun router (che d'ora in poi verranno citate come GE), è stata creata un'apposita rete con subnet mask pari a 255.255.255.252 (/30). In questo modo si ottengono esattamente 2 indirizzi assegnabili, poiché i bit appartenenti all'identificatore di host sono solo gli ultimi 2 dei 32 totali, per un totale di 2^2-2 indirizzi, con lo scopo di risparmiare indirizzi IP che sarebbero rimasti inutilizzati.

3.1 Configurazione degli spazi di indirizzi

Ad un maggior livello di dettaglio, accedendo al terminale dei router R1 e R2, il comando da utilizzare per assegnare un indirizzo IP e relativa subnet mask ad una determinata interfaccia fisica o logica è *ip address [ip address] [subnet mask]*; si fa riferimento esclusivamente ai router R1 e R2 poiché si tratta degli unici dispositivi di livello 3 e quindi capaci di lavorare con gli indirizzi IP, in relazione al modello ISO/OSI, della topologia di rete.

Nel router R1 sono stati assegnati gli indirizzi IP che si comportano da default gateway per ciascuna delle tre VLAN, i quali verranno trattati più dettagliatamente nei capitoli successivi. Quindi, ad esempio, dopo aver stabilito lo spazio di indirizzi della VLAN 10 come 192.168.10.0/24, è stato configurato il default gateway per tutti gli host appartenenti alla VLAN 10 pari a 192.168.10.254 con medesima subnet mask /24, per cui 255.255.255.0, applicando il seguente comando in interface-view:

```
ip address 192.168.10.254 255.255.255.0
```

Figura 7 - Comando default gateway VLAN 10

Analogo discorso vale per le VLAN 20 e VLAN 30, alle quali sono stati assegnati rispettivamente gli spazi di indirizzi 192.168.20.0/24 e 192.168.30.0/24. Per questo motivo, sono stati utilizzati i seguenti comandi:

```
ip address 192.168.20.254 255.255.255.0
```

```
ip address 192.168.30.254 255.255.255.0
```

Figura 8 - Comandi default gateway VLAN 20 e VLAN 30

Relativamente allo spazio di indirizzi impiegato nel collegamento che unisce i router R1 e R2, è stata istanziata la rete 100.0.0.0/30 e ne sono stati assegnati gli unici due indirizzi, ovvero 100.0.0.1 e 100.0.0.2, con corrispondente subnet mask pari a 255.255.255.252 (/30).

Quindi, all'interno del terminale del router R1, dopo essere entrati in interface-view attraverso il comando *interface GigabitEthernet 0/0/0*, è stato assegnato il seguente comando:

```
ip address 100.0.0.2 255.255.255.252
```

Figura 9 - Indirizzo interfaccia GE 0/0/0 di R1

Allo stesso modo, all'interno del router R2, sempre dopo essere entrati in interface-view attraverso il comando *interface GigabitEthernet 0/0/0*, il comando configurato è analogo utilizzando il restante indirizzo IP:

```
ip address 100.0.0.1 255.255.255.252
```

Figura 10 - Indirizzo interfaccia GE 0/0/0 di R2

PC5 e Client2, che simulano dei nodi in “Global Internet”, sono stati associati a due spazi di indirizzi /24, in modo da renderli raggiungibili dal resto della rete. In particolare, è stato stabilito lo spazio 150.0.0.0/24 per la sottorete che possiede l'host PC5 e 160.0.0.0/24 per la sottorete che possiede l'host Client2.

Analogamente a quanto configurato nel router R1, all'interno del router R2 sono stati assegnati gli indirizzi che agiscono da default gateway per gli host PC5 e Client2.

Nel primo caso, entrando in interface-view nell'interfaccia del router R2 che si collega al PC5 attraverso il comando *interface GigabitEthernet 0/0/1*, è stato applicato il seguente comando:

```
ip address 150.0.0.254 255.255.255.0
```

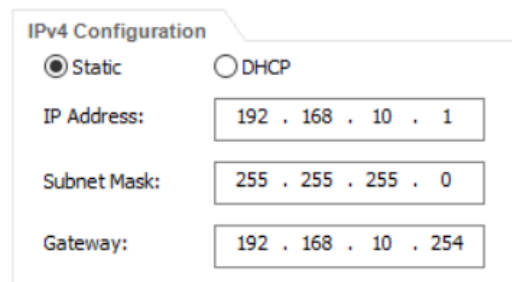
Figura 11 - Comando default gateway rete 150.0.0.0/24

Allo stesso modo, è stata configurato anche il default gateway per la rete 160.0.0.0/24, entrando prima in interface-view con il comando *interface GigabitEthernet 0/0/2* ed applicando successivamente il seguente comando:

```
ip address 160.0.0.254 255.255.255.0
```

Figura 12 - Comando default gateway rete 160.0.0.0/24

Infine, per quel che riguarda tutti gli host presenti nella topologia di rete, è possibile velocizzare il processo configurando l'indirizzo IP e la subnet mask dell'host tramite la compilazione dell'apposita form di configurazione. In figura 13 è riportata la form di configurazione dell'host PC1 compilata adeguatamente con gli indirizzi corrispondenti ai campi: IP address (indirizzo IP), subnet mask e default gateway.



IPv4 Configuration	
<input checked="" type="radio"/> Static	<input type="radio"/> DHCP
IP Address:	192 . 168 . 10 . 1
Subnet Mask:	255 . 255 . 255 . 0
Gateway:	192 . 168 . 10 . 254

Figura 13 - Form di configurazione degli host

Di seguito è mostrata la tabella riepilogativa degli indirizzi assegnati a ciascun host appartenente alla topologia di rete.

	IP Address	Subnet Mask	Default Gateway
PC1	192.168.10.1	255.255.255.0	192.168.10.254
PC2	192.168.20.2	255.255.255.0	192.168.20.254
PC3	192.168.20.3	255.255.255.0	192.168.20.254
PC4	192.168.10.4	255.255.255.0	192.168.10.254
Client3	192.168.10.3	255.255.255.0	192.168.10.254
Client2	192.168.20.22	255.255.255.0	192.168.20.254
PC5	150.0.0.5	255.255.255.0	150.0.0.254
Client1	160.0.0.1	255.255.255.0	160.0.0.254
Server1	192.168.30.1	255.255.255.0	192.168.30.254

4.0 Link Aggregation

Il Link Aggregation è una tecnica che permette di aggregare molteplici interfacce fisiche in un unico collegamento Ethernet-trunk, creando così un'associazione che consente a queste interfacce di operare come un singolo collegamento logico.

I principali vantaggi nell'adottare questa tecnologia sono:

- Maggior affidabilità e sicurezza, poiché nel caso in cui una generica interfaccia subisca un guasto, è possibile trasferire il traffico da un collegamento all'altro.
- Aumento della larghezza di banda, la quale risulta essere pari alla somma della larghezza di banda di ciascuna interfaccia appartenente all'Ethernet-trunk, portando automaticamente ad un aumento delle prestazioni di inoltro del traffico.
- Miglior bilanciamento del carico, in quanto essendo composto da più d'una interfaccia fisica, può dividere il traffico tra esse, riducendo al minimo la probabilità di congestione della rete e i conseguenti ritardi nelle trasmissioni.

Esistono due metodi per implementare il Link Aggregation:

- Load balancing mode, in cui le interfacce interessate vengono inserite manualmente all'interno di un link aggregation group (LAG).
- Static LACP mode, in cui i due endpoint del link Ethernet-trunk negoziano i parametri di aggregazione per le interfacce utilizzando il protocollo LACP. Questo consente, ai due endpoint, di negoziare il numero delle interfacce attive, in quanto, a partire da un pool di interfacce, solo alcune vengono scelte come attive, aumentando in questo modo la robustezza del collegamento, poiché le interfacce inizialmente inattive entreranno in azione solo nel momento in cui una o più interfacce attive dovessero subire un guasto.

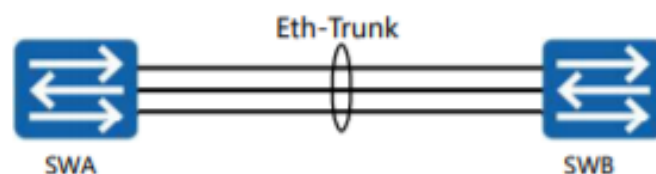


Figura 14 - Esempio di collegamento logico Ethernet-trunk

In figura 14 è possibile osservare in maniera simbolica il concetto precedentemente descritto, in cui vengono aggregati logicamente due o più collegamenti fisici. In questo caso, con il termine endpoint si fa riferimento ai due switch SWA e SWB, i quali rappresentano le due estremità del collegamento Ethernet-trunk.

Tuttavia, questa soluzione presenta alcuni limiti. In primo luogo, il fatto che un collegamento Ethernet-trunk può incorporare al massimo otto interfacce fisiche, in seconda istanza la necessità di dover far in modo che i due endpoint appartenenti al sistema di aggregazione lavorino sempre in modalità coerente, ovvero che le rispettive interfacce debbono essere omogenee, quindi dello stesso tipo, e operare con la medesima modalità di trasmissione e ricezione delle informazioni, chiamata anche duplex mode [2]; ciò comporta che un'interfaccia Ethernet ed una GigabitEthernet non possono essere aggiunte allo stesso Ethernet-trunk.

Inoltre, è preferibile che le interfacce membro abbiano medesima velocità, poiché nel caso in cui si utilizzino interfacce con velocità di trasmissione discordi è altamente probabile che il collegamento più lento possa congestionare e portare alla perdita di pacchetti.

Osservando la topologia di rete oggetto di studio, si può osservare che sono presenti tre potenziali collegamenti Ethernet-trunk, che uniscono i dispositivi R1, S1 e S2.

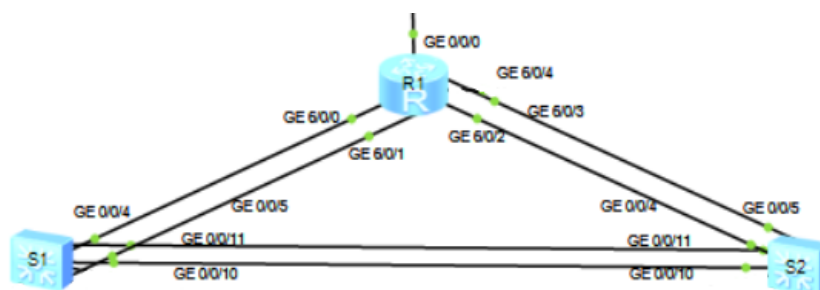


Figura 15 - Collegamenti Ethernet-trunk della topologia di rete

4.1 Configurazione Link Aggregation

Passando ora ad esaminare la configurazione dal lato pratico, è stata effettuata una scelta progettuale tale per cui i collegamenti Ethernet-trunk che congiungono le coppie di dispositivi S1-R1 e S2-R1, rispettivamente nominati Ethernet-trunk 2 ed Ethernet-trunk 3, sono implementati utilizzando la modalità Load balancing. Il motivo di tale decisione consiste nel fatto che, a livello hardware, il router è un dispositivo dotato di un numero di interfacce di rete contenuto ed automaticamente limitate sono

le possibili interfacce fisiche allegabili all'Ethernet-trunk, tenendo pur sempre conto che il massimo numero di interfacce fisiche istanziabili è pari a 8.

Perciò, l'amministrazione manuale delle interfacce fisiche, nell'ipotesi in cui se ne debbano gestire indicativamente al massimo 4, è facilmente mantenibile dall'amministratore di rete, senza eccessive complicazioni.

Relativamente all'implementazione concreta, è innanzitutto necessario istanziare l'interfaccia logica Ethernet-trunk attraverso il comando `interface Eth-Trunk <trunk-id>`, con valore del `trunk-id` appartenente al range 0-63. In questo caso, è stato scelto di configurare un valore del `trunk-id` pari a 2 nel caso del collegamento S1-R1 e pari a 3 nel caso del collegamento S2-R1. Successivamente, sono state incluse le interfacce fisiche all'interfaccia logica Ethernet-trunk appena creata attraverso il comando `trunkport <interface>`.

Quindi, prendendo come esempio di riferimento il collegamento S1-R1, i comandi assegnati all'interno del terminale dello switch S1 sono:

```
interface Eth-Trunk 2
trunkport GigabitEthernet 0/0/4
trunkport GigabitEthernet 0/0/5
```

Figura 16 - Ethernet-trunk S1-R1 in S1

In effetti, osservando la figura 15 è possibile notare come le interfacce GE 0/0/4 e GE 0/0/5 corrispondano esattamente a quelle relative allo switch S1.

Allo stesso modo, i comandi configurati all'interno del router R1 sono

```
interface Eth-Trunk 2
trunkport GigabitEthernet 6/0/0
trunkport GigabitEthernet 6/0/1
```

Figura 17 - Ethernet-trunk S1-R1 in R1

poiché GE 6/0/0 e GE 6/0/1 sono le interfacce L2 del router R1 da includere nel collegamento Ethernet-trunk.

Per verificare l'avvenuta configurazione del collegamento Ethernet-trunk, in questo caso quella relativa al collegamento S1-R1 con `trunk-id` pari a 2, è possibile utilizzare il comando `display Eth-Trunk <trunk-id>` all'interno del terminale di uno dei due dispositivi interessati, ovvero S1 oppure R1.

```

[S1]display interface Eth-Trunk 2
Eth-Trunk2 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID : 20, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-ccb2-7281
Current system time: 2021-05-21 20:00:57-08:00
  Input bandwidth utilization : 0%
  Output bandwidth utilization : 0%
-----
PortName                Status    Weight
-----
GigabitEthernet0/0/4    UP        1
GigabitEthernet0/0/5    UP        1
-----
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2

```

Figura 18 - risultato del comando eseguito nel terminale dello switch S1

Come si può osservare in figura 18, lo stato dell'Ethernet-trunk è UP, per cui attivo. Inoltre, dalla voce “*The number of ports in trunk is*”, vi è la possibilità di convalidare la corretta inclusione delle interfacce fisiche all'interno del collegamento logico, infatti il suo valore è pari a 2 e le interfacce fisiche che l'Ethernet-trunk possiede corrispondono esattamente a quelle aggiunte attraverso il comando *trunkport*, anch'esse con stato UP, quindi attive.

Discorso analogo vale per il collegamento logico Ethernet-trunk 3 che collega i dispositivi S2-R1, il quale si differenzia unicamente nelle interfacce che verranno incluse con il comando *trunkport*. Infatti, osservando la figura 15, si può constatare che le interfacce del router R1 da incorporare nell'Ethernet-trunk 3 sono la GE 6/0/3 e GE 6/0/4. Ciò significa che la lista di comandi da configurare nel terminale del router R1 sarà la seguente:

```

interface Eth-Trunk 3
trunkport GigabitEthernet 6/0/3
trunkport GigabitEthernet 6/0/4

```

Figura 19 - Ethernet-trunk S2-R1 in R1

Per ultima, la configurazione dell'Ethernet-trunk 3 da parte dello switch S2 consiste nell'inclusione delle proprie interfacce fisiche, le quali consistono nella GE 0/0/4 e GE 0/0/5; quindi, i comandi configurati nel terminale dello switch S2 sono i seguenti:

```

interface Eth-Trunk 3
trunkport GigabitEthernet 0/0/4
trunkport GigabitEthernet 0/0/5

```

Figura 20 - Ethernet-trunk S2-R1 in S2

Relativamente al collegamento che unisce i due switch S1 e S2, a cui si è assegnato il nome Ethernet-trunk 1, è stata applicata una scelta progettuale esattamente opposta a quella precedentemente illustrata. Infatti, trattandosi di un collegamento tra due switch, si è considerato il fatto che questi sono dispositivi caratterizzati dal possedere un elevato numero di interfacce e di conseguenza difficilmente gestibili dall'amministratore di rete, ad esempio, nel caso in cui si dovesse gestire un Ethernet-trunk composto da un numero di interfacce fisiche pari al massimo, ovvero 8. A tal proposito, in questo caso, è stata adoperata la modalità di implementazione Static LACP mode.

Dunque, dopo aver creato l'Ethernet-trunk utilizzando l'istruzione *interface Eth-Trunk <trunk-id>*, è necessario specificare la modalità di implementazione, non trattandosi di quella predefinita (Load balancing), per cui il comando successivo sarà *mode lacp-static*. Di seguito vi è la fase di inserimento delle interfacce fisiche analogamente al caso precedente; in aggiunta è però necessaria la configurazione di un comando che ha come scopo quello di abilitare il passaggio di BPDU, i quali verranno trattati nel capitolo relativo a STP, attraverso il comando *bpdu enable*.

Ricapitolando, prendendo in considerazione lo switch S1, i comandi configurati all'interno del suo terminale sono:

```
interface Eth-Trunk 1
mode lacp-static
trunkport GigabitEthernet 0/0/10
trunkport GigabitEthernet 0/0/11
bpdu enable
```

Figura 21 - Ethernet-trunk S1-S2 in S1

La configurazione dell'interfaccia Ethernet-trunk 1 da parte dello switch S2 sarà analoga a quella appena illustrata, ad eccezione delle interfacce fisiche da includere all'interno del collegamento logico stesso, le quali dovranno essere quelle appartenenti allo switch S2, ovvero GE 0/0/10 e GE 0/0/11.

```
interface Eth-Trunk 1
mode lacp-static
trunkport GigabitEthernet 0/0/10
trunkport GigabitEthernet 0/0/11
bpdu enable
```

Figura 22 - Ethernet-trunk S1-S2 in S2

5.0 Vlan

In questa sezione verrà illustrato un argomento chiave di questa topologia, ma più in generale, di tutto il mondo del networking.

VLAN, acronimo di *Virtual Local Area Network*, è una particolare tipo di LAN (*Local Area Network*) contraddistinta dal fatto che consente ad un insieme di dispositivi ubicati in reti fisiche differenti di essere raggruppati in un'unica rete logica, formando a tutti gli effetti un dominio di broadcast distribuito su più dispositivi fisici geograficamente dispersi.

A ciascuna VLAN è tipicamente associato uno spazio di indirizzi dedicato: da questa informazione si può intuire che nodi appartenenti a VLAN differenti non possono comunicare tra loro in quanto fanno capo a domini di broadcast diversi.

In particolare, per rendere possibile la comunicazione tra dispositivi appartenenti alla stessa VLAN è sufficiente l'utilizzo di uno switch, mentre nel caso in cui si voglia permettere la comunicazione tra dispositivi appartenenti a VLAN differenti, è doveroso l'utilizzo di un router oppure di uno switch di livello 3, i quali hanno le capacità di inoltrare i pacchetti a livello 3 e consentono quindi di realizzare il cosiddetto VLAN Routing.

La tecnologia delle VLAN è caratterizzata da tre diverse tipologie di collegamenti, chiamati anche link, i quali possono essere classificati in: *access*, *trunk* ed *hybrid*.

I link di tipo "foglia" sono dei link *access*, vale a dire tutti quei collegamenti che coinvolgono un dispositivo terminale come gli host della topologia di rete ed uno switch. Infatti, i link di tipo *access* sono caratterizzati dal fatto che possono far parte solamente di un'unica VLAN: questa descrizione rispecchia perfettamente le caratteristiche degli host, i quali sono gli unici dispositivi della topologia a poter appartenere ad un'unica VLAN.

In riferimento alla topologia di rete, i collegamenti tra gli switch S3, S4, S5 e gli host PC1, PC2, PC3, PC4, Client3, Client2 sono tutti link di tipo *access*.

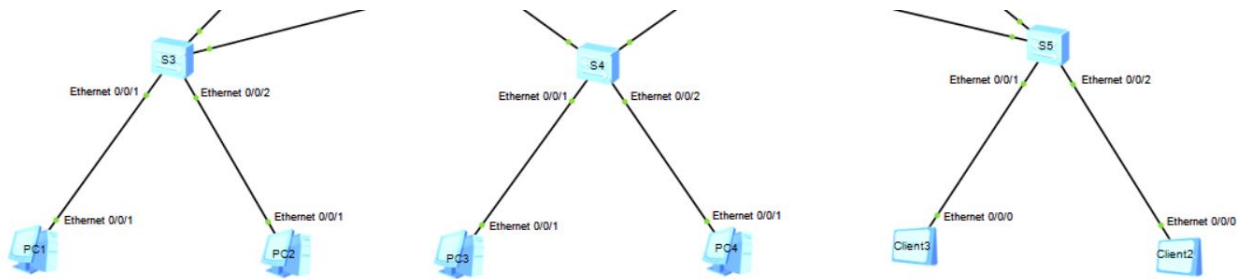


Figura 23 - Link di tipo access della topologia di rete

I link di tipo *trunk* collegano due switch oppure uno switch ed un router. Essi si contraddistinguono dai link di tipo *access* poiché non sono assegnati ad una specifica VLAN e possiedono la capacità di trasportare il traffico di molteplici VLAN; per questo motivo i collegamenti che uniscono i dispositivi R1, S1, S2, S3, S4, S5 sono tutti di tipo trunk.

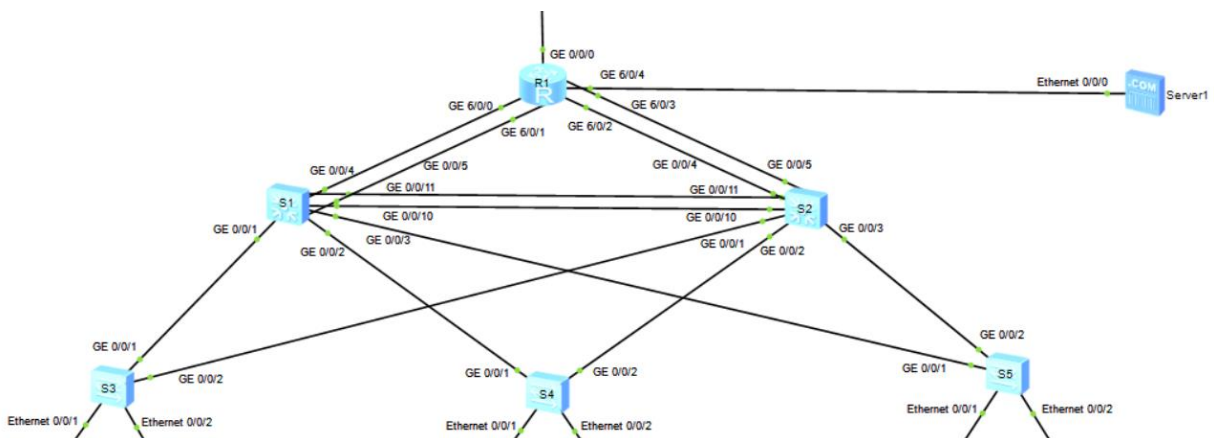


Figura 24 - Link di tipo trunk della topologia di rete

Infine, i link di tipo *hybrid*, i quali rappresentano il tipo di porta predefinito per i dispositivi che supportano le VLAN.

Ciascuna interfaccia dei dispositivi possiede un PVID (Port VLAN ID), il quale rappresenta la VLAN di default per quella data interfaccia. Il valore di default del PVID è VLAN 1 ma può essere modificato in base alle necessità.

All'interno dei frame trasmessi in una comunicazione tramite le VLAN, è inoltre presente un valore di 12 bit chiamato VLAN ID, il quale indica la VLAN a cui il frame è associato. I valori del VLAN ID sono compresi tra 0x000 e 0xFFF, che significa avere a disposizione un massimo di 4096 possibili

VLAN; tenendo conto che la VLAN 0 e la VLAN 4095 (la prima e l'ultima), sono riservate, per cui inutilizzabili, si può determinare quindi che il numero massimo di VLAN istanziabili è 4094.

Relativamente alla topologia di rete, una specifica di progetto è quella di implementare tre VLAN:

1. VLAN 10, composta dagli host PC1, PC4 e Client3.
2. VLAN 20, composta dagli host PC2, PC3, e Client2.
3. VLAN 30, composta unicamente dal Server 1.

Con l'obiettivo di ottenere una visualizzazione grafica più diretta delle VLAN presenti nella topologia di rete è stato assegnato un colore che identifica univocamente le VLAN stesse. In particolare, i dispositivi appartenenti alla VLAN 10 sono stati contraddistinti da un'area di color verde, quelli appartenenti alla VLAN 20 da un'area di colore azzurro ed infine il server, unico dispositivo della VLAN 30, da un'area di color rosa.

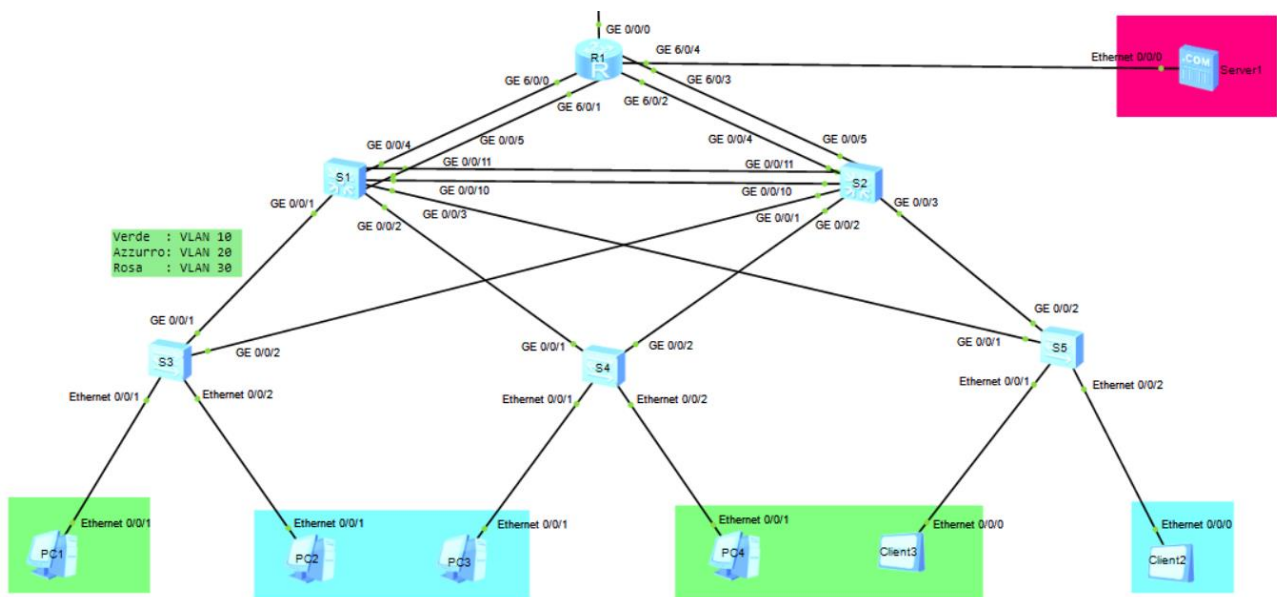


Figura 25 - Aree colorate indicanti le VLAN 10, 20 e 30

5.1 Configurazione VLAN

Di seguito, verranno illustrati i comandi specifici necessari per una configurazione completa delle VLAN 10, 20 e 30.

Esaminando uno qualunque dei cinque switch presenti nella topologia di rete, in questo caso lo switch S4, dopo essere entrati in system-view, per creare le tre VLAN richieste è sufficiente digitare nel terminale dello switch il comando *vlan batch 10 20 30*.

```

<S4>system-view
Enter system view, return user view with Ctrl+Z.
[S4]display this
#
sysname S4
#
vlan batch 10 20 30

```

Figura 26 - Creazione delle VLAN 10, 20 e 30

Per completare la configurazione è necessaria la definizione della tipologia di link associata alle interfacce dello switch, le quali possono essere impostate come *access* o *trunk*; i link di tipo *access*, ai quali sono collegati i nodi terminali della rete, richiedono che sia configurato il VLAN ID sull'interfaccia. Questo viene utilizzato per aggiungere il tag ai frames in ingresso allo switch e per rimuoverlo dai frames in uscita.

I link di tipo *trunk* trasportano frames che fanno capo a diverse VLAN. I frames viaggiano tipicamente taggati, ad eccezione di quelli che appartengono alla VLAN “nativa” del link. Per questo motivo, in fase di configurazione, è necessario specificare il valore del PVID della VLAN nativa e l'elenco delle VLAN che sono autorizzate ad attraversare il link.

Gli switch della topologia di rete che si interfacciano con i dispositivi terminali, a cui è quindi necessaria la configurazione relativa ai link *access*, sono S3, S4 e S5.

In figura 27 è riportata la configurazione effettuata nel terminale dello switch S4 dopo aver eseguito l'accesso in interface-view nell'interfaccia Ethernet 0/0/1 attraverso il comando *interface Eth0/0/1*, con l'obiettivo di configurare il link che collega lo switch S4 e l'host PC3 appartenente alla VLAN 20, caratterizzato quindi da un VLAN ID pari a 20.

```

[S4]interface Eth0/0/1
[S4-Ethernet0/0/1]display this
#
interface Ethernet0/0/1
port link-type access
port default vlan 20

#
return

```

Figura 27 - Configurazione link access S4-PC3

Il procedimento è analogo per tutti gli altri link di tipo *access*, poiché si tratta sempre di entrare in *interface-view* delle interfacce che si collegano agli host e configurare successivamente la coppia di comandi *port link-type access* e *port default vlan <vlan-id>* con *vlan-id* pari all'identificatore della VLAN cui l'host associato al link di tipo *access* che si sta configurando appartiene. Quindi, le interfacce Ethernet0/0/1 ed Ethernet0/0/2 dello switch S3 possiedono un *vlan-id* rispettivamente pari a 10 e 20, poiché il PC1 appartiene alla VLAN 10 e il PC2 appartiene alla VLAN 20; l'interfaccia Ethernet0/0/2 dello switch S4 vedrà assegnarsi un *vlan-id* pari a 10, poiché il PC4 appartiene alla VLAN 10 ed infine le interfacce Ethernet0/0/1 ed Ethernet0/0/2 dello switch S5 possiedono un *vlan-id* rispettivamente pari a 10 e 20, poiché il Client3 appartiene alla VLAN 10 ed il Client2 alla VLAN 20. Di seguito si mostrano le restanti configurazioni appena descritte:

```
[S3]interface Ethernet0/0/1      [S3]interface Ethernet0/0/2
[S3-Ethernet0/0/1]display this [S3-Ethernet0/0/2]display this
#                                #
interface Ethernet0/0/1        interface Ethernet0/0/2
port link-type access          port link-type access
port default vlan 10           port default vlan 20

#                                #
return                          return
```

Figura 28 - Configurazione link access S3-PC1

Figura 29 - Configurazione link access S3-PC2

```
[S4]interface Ethernet0/0/2
[S4-Ethernet0/0/2]display this
#
interface Ethernet0/0/2
port link-type access
port default vlan 10

#
return
```

Figura 30 - Configurazione link access S4-PC4

```

[S5]interface Ethernet0/0/1      [S5]interface Ethernet0/0/2
[S5-Ethernet0/0/1]display this  [S5-Ethernet0/0/2]display this
#                                  #
interface Ethernet0/0/1          interface Ethernet0/0/2
port link-type access            port link-type access
port default vlan 10             port default vlan 20

#                                  #
return                            return

```

Figura 31 - Configurazione link access S5-Client3 Figura 32 - Configurazione link access S4-Client2

Relativamente alla configurazione dei link di tipo *trunk* presenti nella topologia di rete, prendendo inizialmente in considerazione lo switch S4, si può notare come sia necessaria la definizione di due link di tipo *trunk* che collegano lo switch S4 stesso con gli switch S1 e S2 posizionati al di sopra.

In figura 33 si mostra la configurazione del link *trunk* che collega lo switch S4 con lo switch S1; a partire dal terminale dello switch S4 ed entrando quindi in interface-view utilizzando il comando *interface GigabitEthernet0/0/1*, essendo questa l'interfaccia interessata, è innanzitutto necessario specificare che si tratta di un link di tipo *trunk* utilizzando il comando *port link-type trunk*. È stato poi definito un PVID qualsiasi tra 10 e 20, il quale influirà esclusivamente nel processo di frames *tagged* o *untagged* in fase di comunicazione. Sono stati infine applicati i requisiti per i frames delle VLAN a cui è concesso il transito nel link *trunk* in questione, ovvero tutti i frames che hanno come valore dell'attributo VLAN ID 10, 20 e 30. In questo modo, tutto il traffico scambiato tra i vari dispositivi verrà sempre processato.

```

[S4]interface GigabitEthernet 0/0/1
[S4-GigabitEthernet0/0/1]display this
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 20 30
#
return

```

Figura 33 - Configurazione link trunk S4-S1

La configurazione effettuata nello switch S1 è analoga a quella appena illustrata e lo stesso procedimento è stato applicato per tutti i link di tipo *trunk* restanti.

Se si avesse la necessità di limitare il traffico di qualche particolare host, sarebbe sufficiente non includere nel comando *port trunk allow pass* il VLAN ID della VLAN a cui l'host appartiene.

Al contrario, se si volesse consentire il passaggio di tutte le VLAN presenti in una topologia di rete, incluse quelle che potranno essere create in un secondo momento, si può definire l'istruzione *port trunk allow-pass vlan all*, utilizzando quindi la parola chiave *all*.

5.2 VLAN Routing

In relazione a quanto detto precedentemente, per far comunicare host appartenenti a VLAN differenti è necessaria la presenza di un router oppure di uno switch di livello 3: questo processo prende il nome di VLAN routing.

L'implementazione di uno switch di livello tre offre un mezzo ideale per supportare il VLAN routing, poiché risulta essere in grado di eseguire sia le funzionalità dello switch che, in parte, del router, in un singolo dispositivo, motivo per cui generalmente si ottiene una riduzione dei costi operativi.

Esistono due tecnologie utili per la configurazione del VLAN routing:

1. *Sub-interfaces*, applicabili in ciascun router o switch L3, a patto che possiedano porte fisiche di livello tre, quindi capaci di lavorare con gli indirizzi IP.
2. *VLANIF*, trattasi di una interfaccia logica che consente anche a porte fisiche di livello due di ricevere una configurazione IP, quindi comunicare al terzo livello del modello ISO/OSI (Network Layer). A ciascuna VLANIF corrisponde una VLAN ed è associata a tutte le porte fisiche dei dispositivi che fanno capo alla VLAN stessa.

I router sono dispositivi caratterizzati dal possedere un numero di porte fisiche limitato; a tal proposito, il router R1 della topologia di rete è stato modificato a priori nelle sue componenti hardware, in particolare con l'integrazione di una scheda chiamata *24GE card* composta da 24 porte GigabitEthernet di livello due, le quali non possiedono quindi la capacità di lavorare a livello *network* e, di conseguenza, con gli indirizzi IP.

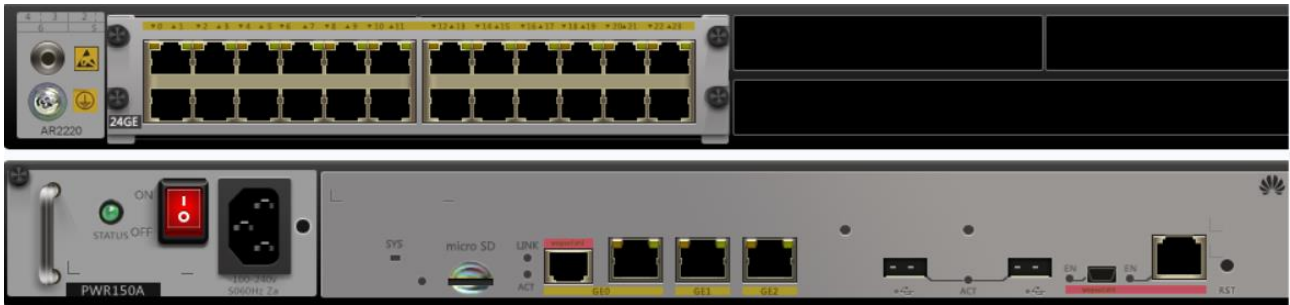


Figura 34 - Componenti hardware del router R1; nella parte superiore la scheda 24GE

Per questo motivo, con l'obiettivo di sviluppare il VLAN Routing e permettere la comunicazione tra host appartenenti a VLAN differenti, è risultato obbligatorio l'utilizzo della tecnologia delle VLANIF.

Considerando quindi la situazione in cui vi sono tre VLAN differenti i cui host che ne fanno parte desiderano comunicare tra loro, saranno automaticamente necessarie tre VLANIF, le quali fungeranno da default gateway per ciascun host all'interno delle VLAN stesse ed avranno associato un indirizzo IP appartenente allo stesso segmento di rete della VLAN per la quale sono state create.

Per applicare questi concetti teorici nella pratica, quindi implementare una soluzione che permetta la comunicazione tra le VLAN 10, 20 e 30 della nostra topologia di rete, si può notare come il router R1 funga da vertice che lega tutta la rete privata; di conseguenza, è proprio il router R1 il dispositivo all'interno del quale sono state configurate le VLANIF.

Le interfacce del router R1 che realizzano la connessione con la LAN sono quelle che fanno capo alla scheda integrata 24GE inserita nello slot 6. Questa ha un funzionamento assimilabile a quello di uno switch di livello 2, pertanto le interfacce fisiche non potranno ricevere configurazione IP.

Applicando la tecnologia delle VLANIF è stata data al router R1 la possibilità di creare delle interfacce logiche capaci di esercitare le funzionalità di livello tre come l'assegnamento di indirizzi IP e, conseguentemente, il processo di determinazione dei percorsi verso le destinazioni.

Da questo momento in poi, il router R1 verrà considerato come uno switch di livello tre. Esso è visto come un dispositivo che, al suo interno, possiede un router, il quale può essere attivato a seconda della configurazione.

5.2.1 Configurazione VLAN Routing

Relativamente alla configurazione, sono state create tre interfacce logiche VLANIF, una per ciascuna delle tre VLAN, utilizzando il comando `interface vlanif <vlan-id>` dove `vlan-id` corrisponde alla VLAN associata. Conseguentemente, a ciascuna VLANIF è stato assegnato un indirizzo IP che funge

da default gateway per gli host della topologia di rete, attraverso il comando *ip address <ip-address> <subnet-mask>*. Per una corretta implementazione e quindi un regolare funzionamento del processo di trasmissione, è necessario utilizzare degli indirizzi IP appartenenti allo stesso segmento di rete delle VLAN associate alle VLANIF che si stanno implementando. Riportando quanto discusso nel capitolo 3, per ciascuna VLAN sono stati assegnati tre diversi spazi di indirizzi, ovvero:

- 192.168.10.0/24 per la VLAN 10.
- 192.168.20.0/24 per la VLAN 20.
- 192.168.30.0/24 per la VLAN 30.

Dovendo assegnare un indirizzo IP che funga da default gateway per tutti gli host di ciascuna VLAN, come illustrato nel capitolo 3, sono stati assegnati i seguenti indirizzi:

- 192.168.10.254/24 per la VLAN 10.
- 192.168.20.254/24 per la VLAN 20.
- 192.168.30.254/24 per la VLAN 30.

Infatti, osservando la tabella riepilogativa degli indirizzi IP assegnati a ciascun host mostrata nel sotto capitolo 3.1, si può osservare come il valore dei campi *default gateway* di ciascuno degli host stessi contenga uno dei tre indirizzi sopra riportati, in relazione alla VLAN a cui fanno capo.

Di seguito si mostrano i comandi assegnati nel terminale del router R1 per una completa creazione delle interfacce logiche VLANIF:

```
[R1]interface Vlanif 10
[R1-Vlanif10]display this
[V200R003C00]
#
interface Vlanif10
 ip address 192.168.10.254 255.255.255.0
#
return
[R1-Vlanif10]|
```

Figura 35 - Configurazione VLANIF 10

```
[R1]interface Vlanif 20
[R1-Vlanif20]display this
[V200R003C00]
#
interface Vlanif20
 ip address 192.168.20.254 255.255.255.0
#
return
[R1-Vlanif20]|
```

Figura 36 - Configurazione VLANIF 20

```

[RL]interface Vlanif 30
[RL-Vlanif30]display this
[V200R003C00]
#
interface Vlanif30
 ip address 192.168.30.254 255.255.255.0

#
return
[RL-Vlanif30]|

```

Figura 37 - Configurazione VLANIF 30

A seguito della configurazione, nel caso in cui, ad esempio, l'host PC1 appartenente alla VLAN 10 volesse comunicare con l'host Client2 appartenente alla VLAN 20, il trasferimento dei pacchetti andrà a buon fine.

Per confermare questa affermazione è possibile effettuare un ping all'interno del terminale dell'host PC1 diretto verso l'host Client2 attraverso il comando *ping 192.168.20.22*, dove l'indirizzo IP 192.168.20.22 è quello dell'host di destinazione. Il risultato è il seguente:

```

PC1>ping 192.168.20.22

Ping 192.168.20.22: 32 data bytes, Press Ctrl_C to
break
From 192.168.20.22: bytes=32 seq=1 ttl=254 time=109 ms
From 192.168.20.22: bytes=32 seq=2 ttl=254 time=94 ms
From 192.168.20.22: bytes=32 seq=3 ttl=254 time=78 ms
From 192.168.20.22: bytes=32 seq=4 ttl=254 time=94 ms
From 192.168.20.22: bytes=32 seq=5 ttl=254 time=109 ms

--- 192.168.20.22 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss

```

Figura 38 - Risultato ping da PC1 a Client2

In figura 38 si può osservare come, dei cinque pacchetti totali trasmessi, tutti quanti sono giunti a destinazione e ricevuti dall'host Client2, con una percentuale di perdita di pacchetti pari al 0%.

Inoltre, attraverso lo strumento software Wireshark, è possibile verificare il percorso effettuato dai pacchetti ispezionando nel dettaglio il traffico ricevuto dalle interfacce fisiche di ciascun dispositivo.

Ispezionando ad esempio l'interfaccia Ethernet 0/0/1 dello switch S3, ovvero quella che collega direttamente l'host PC1 con lo switch S3, ed eseguendo il comando `ping 192.168.20.22` nel terminale dell'host PC1 analogamente a quanto fatto prima, il risultato mostrato da Wireshark è il seguente:

No.	Time	Source	Destination	Protocol	Length	Info
9	8.391000	192.168.10.1	192.168.20.22	ICMP	74	Echo (ping) request id=0x20e7, seq=1/256, ttl=128 (reply in 10)
10	8.484000	192.168.20.22	192.168.10.1	ICMP	74	Echo (ping) reply id=0x20e7, seq=1/256, ttl=254 (request in 9)
11	9.031000	HuaweiTe_16:49:5a	Spanning-tree-(for-...	STP	60	RST. Root = 4096/0/00:e0:fc:0b:49:fd Cost = 30000 Port = 0x8001
12	9.500000	192.168.10.1	192.168.20.22	ICMP	74	Echo (ping) request id=0x21e7, seq=2/512, ttl=128 (reply in 13)
13	9.578000	192.168.20.22	192.168.10.1	ICMP	74	Echo (ping) reply id=0x21e7, seq=2/512, ttl=254 (request in 12)
14	10.504000	192.168.10.1	192.168.20.22	ICMP	74	Echo (ping) request id=0x22e7, seq=3/768, ttl=128 (reply in 15)

> Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0
 > Ethernet II, Src: HuaweiTe_fb:6d:0e (54:89:98:fb:6d:0e), Dst: HuaweiTe_0b:49:fd (00:e0:fc:0b:49:fd)
 > Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.20.22
 > Internet Control Message Protocol

Figura 39 - Risultato di Wireshark a seguito dell'invio dei pacchetti tramite il comando ping

Come previsto, il traffico inviato dall'host PC1 diretto verso l'host Client2 ha attraversato l'interfaccia Ethernet 0/0/1 ispezionata, poiché sono stati inviati (*request*) e ricevuti (*reply*) i cinque pacchetti in relazione al protocollo che si occupa di trasmettere messaggi tra i vari componenti di una rete di calcolatori [3], ovvero ICMP, corrispondenti alle righe di color rosa; inoltre, nella voce *Internet Protocol Version 4*, si ottiene una conferma dell'indirizzo sorgente e di destinazione, ovvero 192.168.10.1 dell'host PC1 e 192.168.20.22 dell'host Client2.

Si ricorda che prima di giungere a destinazione, ovvero all'host Client2, i pacchetti devono prima essere processati dal router R1: poiché gli host in questione appartengono a due VLAN differenti, ovvero la VLAN 10 e la VLAN 20, gli switch intermedi di livello due non hanno le capacità di inoltrare pacchetti destinati a VLAN o segmenti di rete diversi.

Una volta giunti allo switch S3, i pacchetti possono effettuare due percorsi differenti per arrivare al router R1, attraverso l'interfaccia GE 0/0/1 oppure l'interfaccia GE 0/0/2 dello switch S3; effettuando nuovamente un'ispezione in entrambe le interfacce con l'ausilio di Wireshark, si può notare che il traffico dati inviato dall'host PC1 "scorre" sempre attraverso l'interfaccia GE 0/0/2 dello switch S3, ovvero quella che si collega direttamente con lo switch S2.

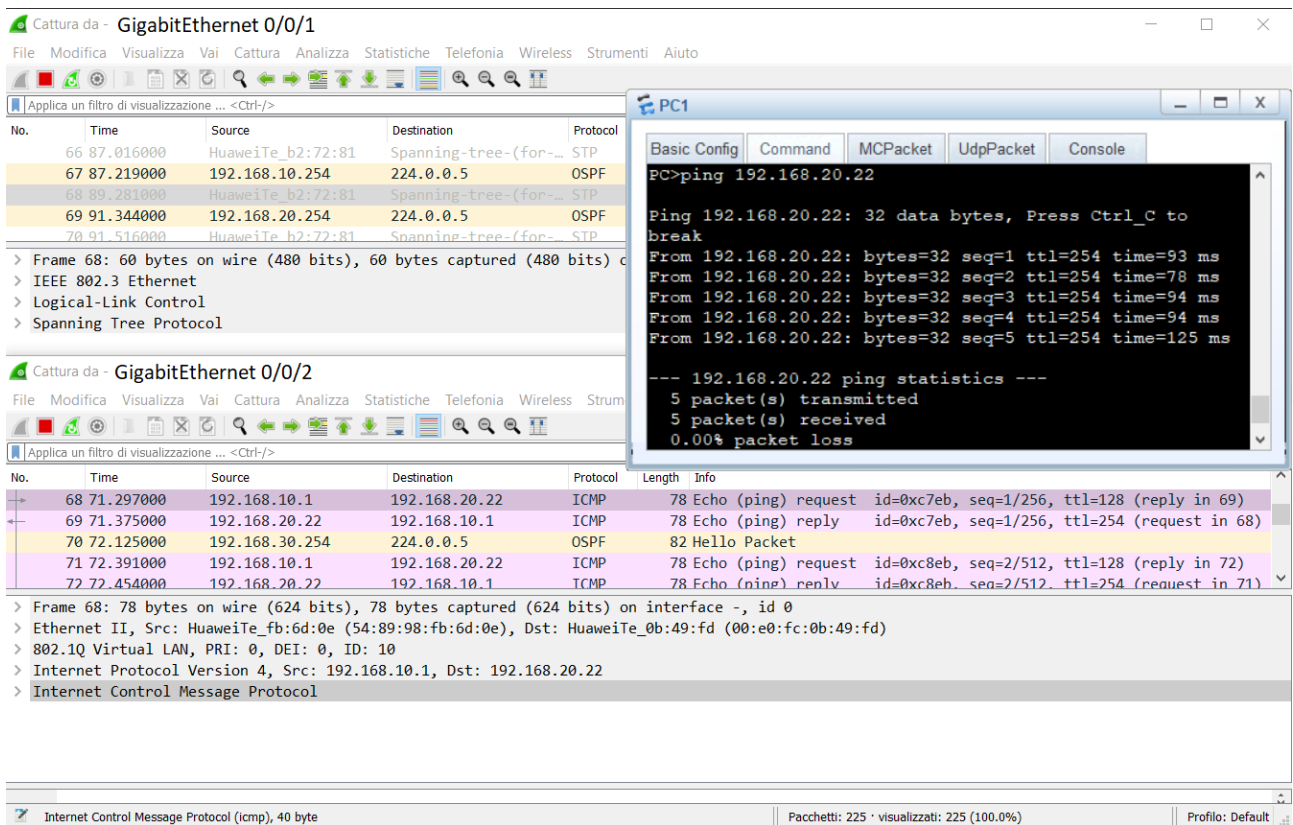


Figura 40 - Ispezione delle interfacce GE0/0/1 e GE0/0/2 dello switch S3

Come mostra la figura 40, all'atto del comando di ping 192.168.20.22, l'interfaccia GE 0/0/1 non vede il passaggio di alcun pacchetto con protocollo ICMP prodotto dal ping stesso, mentre la situazione è opposta nell'interfaccia GE0/0/2, attraverso la quale sono transitati tutti i pacchetti.

A questo punto è intuibile che i pacchetti verranno ricevuti dallo switch S2 attraverso l'interfaccia GE 0/0/1 dello stesso e poi inoltrati al router R1, il quale li processerà facendo riferimento alla propria tabella di routing, che indicherà al router il percorso che i pacchetti dovranno effettuare per un corretto trasferimento del traffico fino a destinazione.

Ci si potrebbe però chiedere quale sia il motivo per il quale il traffico dati inviato dall'host PC1 e destinato ad un host appartenente ad una VLAN differente dalla propria effettui sempre il medesimo percorso, ma più in generale, che cosa influisce sul percorso del traffico presente nella topologia di rete.

La risposta al quesito risiede nel protocollo STP e nella sua evoluzione chiamata RSTP, la quale è stata configurata per la progettazione della topologia di rete come richiesto dalle specifiche di progetto.

6.0 STP

In questa sezione verranno illustrate le caratteristiche e le funzionalità dei protocolli STP e RSTP.

La crescente espansione delle reti aziendali di tipo *large enterprise* introduce la necessità di ricorrere a reti multi-switch, con l'obiettivo di fornire servizi ad un numero di host terminali in continuo aumento; è quindi importante moltiplicare i collegamenti e gli apparati, incrementando conseguentemente l'effettiva ridondanza della rete stessa.

Dunque, la ridondanza riduce al minimo l'impossibilità di comunicare tra host, grazie alla creazione di collegamenti secondari che verranno adoperati automaticamente in caso di guasto dei primari. D'altro canto, potrebbe provocare un aumento degli errori di commutazione a causa della creazione dei cosiddetti loop, i quali portano a drastiche interruzioni del servizio di comunicazione.

In particolare, un possibile effetto del fenomeno dei loop prende il nome di broadcast storm. Ciò si verifica quando un dispositivo terminale tenta di scoprire, inviando un qualsivoglia numero di pacchetti, una destinazione di cui né sé stesso, né gli switch lungo il percorso dei pacchetti stessi, sono a conoscenza.

Nel momento in cui l'host sorgente invia i pacchetti con destinazione broadcast, essi vengono inizialmente ricevuti dallo switch a cui l'host è direttamente collegato, il quale li inoltra conseguentemente attraverso tutte le sue interfacce ad eccezione di quella dalla quale li ha ricevuti. Tale procedimento viene quindi ripetuto per tutti gli switch che riceveranno i pacchetti, poiché è stato supposto che la destinazione, in realtà, non sia nota; questo processo prende il nome di *flooding* (allagamento) e porta ad un degrado estremo delle prestazioni dello switch.

Dunque, si può intuire che la sfida risiede nella capacità di conservare i vantaggi della ridondanza, in modo da evitare l'isolamento dei dispositivi terminali nel caso di guasto dei sistemi o collegamenti primari e, contemporaneamente, nell'abilità di trovare una soluzione che annulli la possibile creazione di loop e, di conseguenza, di tutti i suoi effetti dannosi.

Tale soluzione consiste nel protocollo STP (Spanning Tree Protocol), ed ancor meglio, nella sua versione Rapid, chiamata RSTP (Rapid Spanning Tree Protocol).

Entrambi i protocolli STP e RSTP operano al secondo livello dello standard ISO/OSI, quindi al livello datalink. Il loro principio è quello di disabilitare logicamente i collegamenti ridondanti con lo scopo di ottenere la certezza che non si verifichi la creazione di alcun loop, ma essere allo stesso tempo in grado di abilitarli nel momento in cui venga riscontrato un guasto all'interno della rete.

Il protocollo STP è caratterizzato, innanzitutto, da un *Root Bridge/Switch*, il quale rappresenta il centro logico, ma non necessariamente il centro fisico, della rete e può cambiare dinamicamente nel caso in cui l'attuale root switch subisca un malfunzionamento e non riesca più ad effettuare il suo lavoro; in una rete che implementa STP può esistere un solo root switch.

Il processo che sta alla base della definizione del root switch è l'elezione, attraverso la quale viene anche definito il ruolo di tutti gli altri switch appartenenti alla rete. In particolare, l'elezione del root switch si basa sull'analisi di quello che viene definito Bridge ID (Bridge Identifier). Si tratta di un identificatore univoco caratterizzato dalla coppia:

1. Priorità, con dimensione pari a 16 bit.
2. Indirizzo MAC, con dimensione pari a 48 bit.

per un totale di 64 bit.

Il dispositivo che detiene la priorità più alta, il che corrisponde al valore di priority numericamente più piccolo, viene eletto come root switch. Nel caso in cui tutti gli switch possiedano lo stesso valore di priority, viene analizzato l'indirizzo MAC, eleggendo come root switch il dispositivo con l'indirizzo MAC più piccolo in termini di comparazione esadecimale; essendo l'indirizzo MAC univoco per ciascun dispositivo si ha quindi la certezza di eleggere sicuramente un root switch.

L'architettura di rete sulla quale il protocollo STP, a livello logico, agisce, prende il nome di "albero invertito".

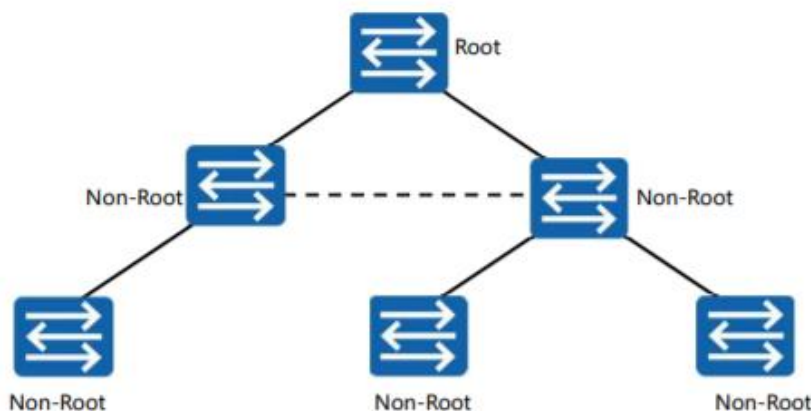


Figura 41 - Architettura ad albero invertito

Come riporta la figura 41, il ruolo assunto dal root switch prima definito è quello di radice, mentre tutti i restanti switch facenti parte dell'albero invertito assumono il ruolo di non-root switch, i quali sono considerati essere downstream rispetto al root switch.

Osservando la rete privata della nostra topologia di rete, è possibile cogliere immediatamente la somiglianza con l'albero di figura 41. Per questo motivo, con il fine di rimanere coerenti con l'architettura predefinita sulla quale opera il protocollo STP, si è stabilito che il dispositivo deputato a maturare il ruolo di root switch è il router R1. Relativamente ai rimanenti switch, quindi S1, S2, S3, S4 e S5, anche in questo caso concordemente con l'architettura ad albero invertito, svolgono il ruolo di non-root switch.

Nel caso si avessero necessità di ottimizzazione progettuali, è possibile forzare l'elezione di uno specifico switch affinché diventi root switch, modificando manualmente il valore della priorità del proprio Bridge ID, la quale può assumere un valore compreso tra 0 e 61440 a step di 4096.

Come ribadito precedentemente, una maggior probabilità di esser eletto root switch si ottiene configurando il valore della priorità ad un valore numericamente minore, per cui, un valore di priorità pari a 0 corrisponde alla più alta probabilità di essere eletto root switch. A tal proposito, poiché il valore di default della priorità di ciascuno switch che esegue STP è pari 32768, per modificare la priorità del router R1 si è fatto affidamento al comando *stp priority [valore priority]*, in particolare

```
stp priority 4096
```

Figura 42 - Priorità di R1 fissata a 4096

eseguito all'interno del suo terminale in system-view; in questo modo, il valore di priorità del router R1 è diventato 4096, mentre quello di tutti i restanti switch permane 32768, ottenendo la certezza dell'auto elezione del router R1 per il ruolo di root switch.

In una topologia di rete Spanning Tree si ha uno scambio costante di pacchetti, chiamati BPDU, acronimo di Bridge Protocol Data Unit, i quali contengono specifiche informazioni con l'obiettivo di determinare, in ogni istante, il ruolo e lo stato di ciascuno switch all'interno della rete.

In particolare, i *Configuration BPDU* vengono immessi dal root switch per poi essere propagati downstream verso i non-root switch, in modo da tener aggiornati quest'ultimi sullo stato della topologia di rete e del root switch. Essi trasportano una serie di parametri, tra cui, il Root Bridge ID, il quale viene utilizzato dai non-root switch per determinare costantemente la presenza di un root switch e garantire quindi che quest'ultimo rimanga il dispositivo con la più alta priorità.

I *Configuration BPDU* vengono automaticamente inoltrati sulla base di un *Hello timer* con valore predefinito di 2 secondi. È presente anche un *Max age timer* fissato a 20 secondi che rappresenta la durata temporale oltre la quale un generico switch considera il contenuto della BPDU ricevuta come

obsoleta, presumendo quindi che sia avvenuto un errore durante il processo performato dal protocollo STP e che l'attuale root switch non è più valido.

Ciascuna porta dello switch possiede un ruolo ed uno stato specifico.

I ruoli delle porte vengono utilizzati per definire il comportamento delle porte degli switch della topologia di rete. In particolare, STP definisce tre possibili ruoli di porta: designated, root ed alternate.

Il root switch possiede tutte le porte di tipo designated, le quali definiscono il percorso downstream lungo cui i *Configuration BPDU* vengono inoltrati, mentre le porte di un non-root switch che è direttamente collegato al root switch sono di tipo root; data una porta di tipo designated di un root switch, il secondo estremo del collegamento è sempre una porta di tipo root, definendo una relazione fissa tale per cui si ha sempre un collegamento $D \rightarrow R$. Un non-root switch può possedere a sua volta altre porte di tipo designated.

Qualsiasi porta a cui non è assegnato un ruolo designated o root è considerata una porta di tipo alternate, la quale può appartenere esclusivamente ad un non-root switch ed è in grado di ricevere BPDU attraverso porte designated di altri switch. Le porte con ruolo alternate monitorano lo stato dei collegamenti ridondanti, ma non elaborano/processano mai i BPDU ricevuti; il loro scopo è quindi quello di rompere il loop non inoltrando il traffico.

Infine, una porta con ruolo alternate è sempre collegata ad una porta con ruolo designated, definendo quindi la relazione $D \rightarrow A$.

Oltre ad un ruolo, ciascuna porta di uno switch può assumere cinque stati logici differenti: disabled, blocking, listening, learning e forwarding. Una porta è nello stato disabled solo nel caso in cui è l'utente ad aver disabilitato manualmente la porta stessa utilizzando il comando *shutdown* in interface-view. Abilitando invece una porta attraverso il comando *undo shutdown*, oppure semplicemente alla sua prima istanziazione, si trova nello stato di blocking. Infine, lo stato forwarding è considerato come lo stato finale, nel quale la porta associata può essere considerata stabile e funzionante, svolgendo correttamente tutti le proprie operazioni di inoltro del traffico utente e delle BPDU. Gli stati listening e learning sono invece quelli intermedi che una porta deve necessariamente percorrere per giungere allo stato forwarding, prima del quale il traffico utente non verrà inoltrato.

Attraverso il comando

```
display stp brief
```

Figura 43 - Comando per visualizzare stato e ruolo delle porte

applicabile in system-view all'interno di ciascuno switch/router che adopera il protocollo STP, è possibile visualizzare le informazioni riguardanti il ruolo e lo stato di ciascuna delle loro porte.

```
[R1]display stp brief
MSTID  Port                Role  STP State  Protection
  0    GigabitEthernet6/0/4  DESI  FORWARDING  ROOT
  0    Eth-Trunk2           DESI  FORWARDING  ROOT
  0    Eth-Trunk3           DESI  FORWARDING  ROOT
```

Figura 44 - Risultato del comando applicato nel dispositivo R1

```
[S1]display stp brief
MSTID  Port                Role  STP State  Protection
  0    GigabitEthernet0/0/1  DESI  FORWARDING  NONE
  0    GigabitEthernet0/0/2  DESI  FORWARDING  NONE
  0    GigabitEthernet0/0/3  DESI  FORWARDING  NONE
  0    Eth-Trunk1           ALTE  DISCARDING  NONE
  0    Eth-Trunk2           ROOT  FORWARDING  NONE
```

Figura 45 - Risultato del comando applicato nel dispositivo S1

```
[S2]display stp brief
MSTID  Port                Role  STP State  Protection
  0    GigabitEthernet0/0/1  DESI  FORWARDING  NONE
  0    GigabitEthernet0/0/2  DESI  FORWARDING  NONE
  0    GigabitEthernet0/0/3  DESI  FORWARDING  NONE
  0    Eth-Trunk1           DESI  FORWARDING  NONE
  0    Eth-Trunk3           ROOT  FORWARDING  NONE
```

Figura 46 - Risultato del comando applicato nel dispositivo S2

```
[S3]display stp brief
MSTID  Port                Role  STP State  Protection
  0    Ethernet0/0/1         DESI  FORWARDING  BPDU
  0    Ethernet0/0/2         DESI  FORWARDING  BPDU
  0    GigabitEthernet0/0/1  ALTE  DISCARDING  NONE
  0    GigabitEthernet0/0/2  ROOT  FORWARDING  NONE
```

Figura 47 - Risultato del comando applicato nel dispositivo S3

```
[S4]display stp brief
MSTID  Port                Role  STP State  Protection
  0    Ethernet0/0/1         DESI  FORWARDING  BPDU
  0    Ethernet0/0/2         DESI  FORWARDING  BPDU
  0    GigabitEthernet0/0/1  ALTE  DISCARDING  NONE
  0    GigabitEthernet0/0/2  ROOT  FORWARDING  NONE
```

Figura 48 - Risultato del comando applicato nel dispositivo S4

```
[S5]display stp brief
MSTID Port Role STP State Protection
0 Ethernet0/0/1 DESI FORWARDING BPDU
0 Ethernet0/0/2 DESI FORWARDING BPDU
0 GigabitEthernet0/0/1 ALTE DISCARDING NONE
0 GigabitEthernet0/0/2 ROOT FORWARDING NONE
```

Figura 49 - Risultato del comando applicato nel dispositivo S5

Una regola del protocollo STP consiste nel fatto che ciascuna porta del root switch possiede sempre ruolo di porta designated e stato logico forwarding: come si può osservare dalle figure sopra riportate, questa situazione si verifica esclusivamente nelle porte GE 6/0/4, Eth-Trunk2 e EthTrunk3 del router R1, il che conferma il suo effettivo incarico di root switch.

Il capitolo 5.2.1 è terminato con il seguente quesito: qual è il motivo per il quale il traffico dati inviato dall'host PC1 e destinato ad un host appartenente ad una VLAN differente dalla propria effettua sempre il medesimo percorso, ma più in generale, che cosa influisce sul percorso del traffico presente nella topologia di rete?

Dopo aver introdotto il protocollo STP, in particolare il concetto di BPDU, ruolo di porta e stato logico delle porte stesse, è possibile affermare che la risposta al precedente quesito corrisponde al fatto che, come si può osservare dalla figura 47 sopra riportata, la porta GE0/0/1 dello switch S3 possiede il ruolo impostato come alternate e stato logico discarding. Ciò significa che il suddetto collegamento è stato logicamente disabilitato con il fine di prevenire la creazione dei loop e quindi impossibilitata ad inoltrare traffico.

Pertanto, nel caso in cui all'interno della topologia di rete fosse presente il rischio relativo alla creazione di loop, il protocollo STP imposta automaticamente una porta con ruolo alternate e corrispondente stato in discarding, in modo tale da inibirle l'inoltro del traffico. Nel momento in cui dovesse avvenire un guasto ad un collegamento o dispositivo appartenente alla rete, le porte con ruolo alternate verranno attivate e potranno inoltrare il traffico dati, salvando effettivamente la comunicazione e lo stato dell'infrastruttura di rete stessa.

Di seguito si propone una figura riepilogativa di tutti i ruoli delle porte di ciascuno switch appartenente alla LAN della topologia di rete.

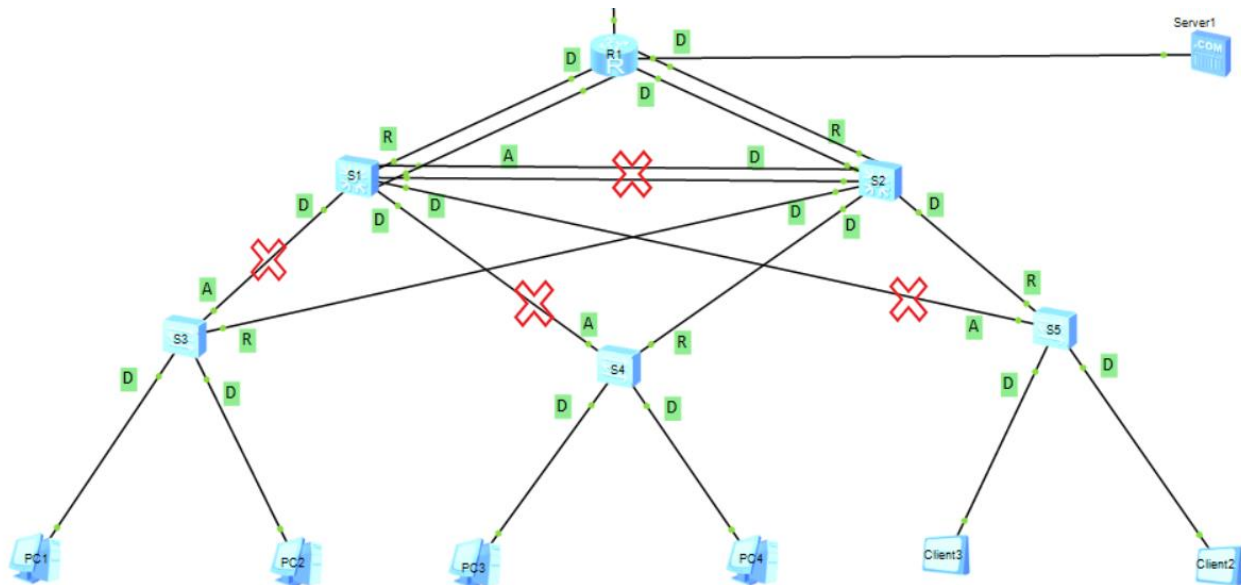


Figura 50 - Riepilogo dei ruoli di porta secondo STP

Sono presenti tre tipologie di etichette e un'icona rossa a forma di croce, in particolare:

1. L'etichetta D indica che la porta a cui è associata possiede ruolo designated.
2. L'etichetta R indica che la porta a cui è associata possiede ruolo root.
3. L'etichetta A indica che la porta a cui è associata possiede ruolo alternate.
4. La croce di color rosso indica che il collegamento a cui è associata non inoltra traffico per prevenire la creazione di loop.

Si può inoltre osservare come varie porte possiedono un particolare tipo di protezione. Relativamente al root switch è stata impostata una protezione di tipo *root*, chiamata *root protection*, a tutte le proprie porte. Questo tipo di protezione si applica al root switch attraverso il comando

```
stp root-protection
```

Figura 51 - Comando per impostare la *root-protection*

in *interface-view*, per evitare il caso in cui, a causa di attacchi malevoli o errori di configurazione, esso possa ricevere BPDU con priorità più alta, il che porterebbe ad un declassamento del root switch ad un generico non-root switch, causando una modifica della topologia di rete e presumibilmente gravi problemi a quest'ultima. La funzione di *root protection* è quella di conservare sempre il ruolo di porta designated a tutte le porte del root switch.

Il tempo totale necessario per la transizione dallo stato listening fino a giungere lo stato forwarding di inoltrare del traffico dati, è di 30 secondi, di cui 15 secondi corrispondono allo stato listening mentre i restanti 15 secondi allo stato learning: questo processo prende il nome di convergenza.

Esiste inoltre una seconda variante di convergenza, chiamata anche ri-convergenza, la quale necessita l'ulteriore passaggio per lo stato blocking, il quale ha una durata di 20 secondi e si applica qualora si verificasse un errore all'interno della rete nella precedente convergenza, ad esempio in caso di guasto del root switch. Pertanto, sommando questi 20 secondi ai precedenti 30 secondi della convergenza standard, si ottiene un totale di 50 secondi che corrisponde al tempo impiegato dal protocollo STP per consentire alle porte degli switch di iniziare ad inoltrare il traffico dati.

6.1 RSTP

È stato necessario introdurre i concetti chiave del protocollo STP per poter trattare ora la versione Rapid applicata nella topologia di rete, chiamata appunto RSTP.

STP garantisce senza dubbio una rete priva di loop, ma con il passare degli anni sono state scoperte alcune limitazioni, in particolare l'elevato tempo necessario ad effettuare la convergenza della topologia di rete, la quale potrebbe avvenire frequentemente.

RSTP adopera un processo di *proposal and agreement*, il cui scopo è quello di consentire una negoziazione immediata, limitando efficacemente il tempo impiegato per la convergenza basata su timer fissi come quella di STP.

Questo processo tende a seguire un effetto a cascata in cui, a partire dal root switch, ciascuno switch downstream abbia la possibilità di conoscere direttamente l'identità del root switch ed il percorso attraverso cui può essere raggiunto. In RSTP, il tempo necessario per completare la convergenza corrisponde al tempo richiesto dalle BPDU per attraversare la topologia di rete, dunque, non sono presenti timer ed il tutto avviene velocemente; per questi motivi si è stabilito di impiegare RSTP piuttosto che STP.

6.1.1 Configurazione RSTP

Relativamente alla sua attivazione è necessario configurare il comando

```
stp mode rstp
```

Figura 52 - Comando per avviare RSTP

in system-view all'interno del terminale di ciascuno switch appartenente alla LAN della topologia di rete, quindi R1, S1, S2, S3, S4 e S5.

Inoltre, RSTP prevede la configurazione delle porte perimetrali della topologia di rete, ovvero le porte che collegano direttamente i dispositivi terminali, come *edge port*. Una porta edge si contraddistingue dal fatto di non partecipare al processo RSTP poiché non riceve alcun *Configuration BPDU*; pertanto, il loro scopo è unicamente quello di inoltrare il traffico e la principale abilità risiede nel poter transitare dallo stato disabled allo stato forwarding di inoltro del traffico senza alcun tipo di ritardo, garantendo una rapida transizione dello stato della porta.

Per abilitare una generica porta come *edge port* è sufficiente configurare il comando

```
stp edged-port enable
```

Figura 53 - Comando per assegnare una *edged-port*

in interface-view all'interno del terminale degli switch che si interfacciano direttamente con gli host appartenenti alla rete privata della topologia di rete, dunque, alle porte Ethernet0/0/1 ed Ethernet0/0/2 degli switch S3, S4 ed S5.

Di seguito è riportata la configurazione applicata allo switch S3 in interface-view, in particolare alle interfacce Ethernet0/0/1 ed Ethernet0/0/2.

```
[S3]interface Ethernet0/0/1
[S3-Ethernet0/0/1]display this
#
interface Ethernet0/0/1
  stp edged-port enable
#
return
```

Figura 54 - *Edged-port Eth0/0/1*

```
[S3]interface Ethernet0/0/2
[S3-Ethernet0/0/2]display this
#
interface Ethernet0/0/2
  stp edged-port enable
#
return
```

Figura 55 - *Edged-port Eth0/0/2*

Lo stesso procedimento è stato eseguito per i due switch residui, ovvero S4 e S5.

Come si può osservare dalle figure 47, 48 e 49, oltre alla protezione *root protection* è presente un'ulteriore tipologia di protezione introdotta con RSTP, chiamata *BPDU protection*.

La protezione *BPDU protection* si applica in tutti gli switch che possiedono delle porte con ruolo *edge port*, per cui, in questo caso, agli switch S3, S4 ed S5. Essa consente di proteggere gli switch

nell'evenienza in cui ricevessero BPDU ostili, le quali potrebbero modificare il ruolo delle porte edge in porte non-edge, portando quindi a ripetute convergenze che provocherebbero una dannosa instabilità di rete.

Dopo aver abilitato la protezione *BPDU protection* attraverso il comando

```
stp bpdu-protection
```

Figura 56 - Comando per impostare la bpdu-protection

in system-view all'interno del terminale di ciascuno dei tre switch sopra elencati, nel caso in cui una porta con ruolo *edge port* dovesse ricevere una BPDU, verrà automaticamente disabilitata e potrà tornare operativa solo a seguito dell'avviamento manuale da parte dell'amministratore di rete.

Con RSTP termina la sezione riguardante le tecnologie risultate necessarie per il corretto funzionamento della LAN presente nella topologia di rete oggetto di studio.

Per esaminarla nel suo complesso, considerando anche la sezione pubblica rappresentante Internet, è necessario instaurare una comunicazione tra il router R1, ovvero il router della rete privata, ed il router R2, il quale può essere considerato il router dell'ISP.

In particolare, R2 è il dispositivo che riceve le richieste di servizi provenienti dagli host appartenenti alla rete privata per poi inoltrarle fino a destinazione, come ad esempio un web server ubicato nella rete pubblica che fornisce un sito web agli utenti.

7.0 OSPF

OSPF è un protocollo di routing di tipo link-state, quindi basato su un algoritmo in cui la topologia di rete ed i costi dei collegamenti sono noti al router [4], in grado di rilevare rapidamente i cambiamenti all'interno della topologia di rete e capace di determinare, in un breve lasso di tempo, il percorso migliore da usufruire per raggiungere un determinato spazio di indirizzi.

Trattandosi di un protocollo di routing, il suo obiettivo è quello di permettere ai router di scambiarsi informazioni tra loro con il fine di costruire le tabelle di routing, permettendo quindi il corretto instradamento dei pacchetti verso la loro destinazione. Il ricorso ad un protocollo di routing per la costruzione automatica e dinamica delle tabelle di routing diventa necessario quando il numero di sottoreti interconnesse è elevato, come nel caso della rete Internet.

Utilizzando il protocollo OSPF, ciascun router all'interno di una qualunque topologia di rete è in grado di conoscere lo stato di tutte le interfacce dei router adiacenti, con il fine di stabilire il percorso migliore per raggiungere ogni rete. Questa situazione si verifica innanzitutto attraverso il flooding di LSA (Link State Advertising) tra i router interessati, ovvero l'inoltro di particolari dati contenenti le informazioni e lo stato delle interfacce dei router adiacenti. Successivamente, ciascun router utilizzerà i LSA ricevuti per creare un proprio database LSDB, il quale fornisce l'insieme di tutte le informazioni che permettono di stabilire il percorso più breve verso uno spazio di indirizzi noto, andando quindi a popolare la tabella di routing con i percorsi stessi.

OSPF si occupa inoltre di risolvere i problemi di scalabilità che altri protocolli di routing introducono, ovvero quando la comunicazione avviene tra un numero in espansione di router, il che può portare ad una instabilità nociva all'interno della topologia di rete. Ciò è gestito attraverso l'uso di aree, le quali limitano la portata del traffico dei router ad un gruppo isolato, consentendo in questo modo anche la gestione di reti di grandi dimensioni da parte di OSPF; gli LSDB dei router appartenenti alla stessa area saranno equivalenti e conterranno dunque le medesime informazioni.

Per concludere i concetti chiave riguardanti OSPF, occorre introdurre il router-id. Si tratta di un valore di 32 bit assegnato a ciascun router che esegue il protocollo OSPF, il quale identifica in modo univoco il router all'interno della topologia di rete.

Esistono due possibilità di assegnamento del router-id: manuale oppure automatica.

Nel caso in cui si volesse effettuare una configurazione manuale del router-id è semplicemente necessario assegnare un generico indirizzo di 32 bit, come ad esempio 1.1.1.1, mentre qualora lo si

volesse estrarre automaticamente, il router sceglierà come valore di router-id il più alto indirizzo IP tra le interfacce logiche o fisiche in esso configurate.

Applicando il protocollo OSPF ed i relativi concetti teorici alla nostra topologia di rete, è quindi necessario configurare opportunamente i router R1 e R2.

La corretta configurazione di OSPF richiede innanzitutto che ogni router partecipante abiliti prima il processo OSPF. Ciò si ottiene utilizzando il comando *ospf [process-ID]*, dove il process-id rappresenta l'identificatore univoco del processo a cui il router è associato. Di seguito, è necessario specificare il router-ID univoco per ciascun router attraverso il comando *router-id [router-id]*.

Successivamente, il terminale entra in automatico nella *ospf-view*, ovvero la view corrispondente al processo OSPF configurato, all'interno della quale è necessario definire l'area a cui ciascuna interfaccia dei router è associata, attraverso il comando *area [area-id]*, dove area-id corrisponde ad una qualsiasi cifra intera maggiore o uguale a zero.

Infine, per comunicare quali sono le interfacce logiche o fisiche (ed i segmenti di rete associati) partecipanti al processo OSPF e che devono quindi essere dichiarate raggiungibili, si fa uso del comando *network [IP address] [wildcard mask]*.

La wildcard mask, chiamata anche maschera inversa, è una sequenza di 32 bit utilizzata per specificare un range di indirizzi di rete. In particolare, la wildcard mask segue la stessa regola delle subnet mask secondo cui le sequenze di 0 ed 1 devono essere continue, ma il significato dello 0 e dell'1 è esattamente opposto. Se da una parte la subnet mask identifica il campo network ed il campo host di un indirizzo IP, la wildcard mask utilizza i bit 0 ed 1 per identificare i singoli indirizzi IP oppure un gruppo di essi usufruendo di una metodologia decisamente più flessibile rispetto alla rigidità della subnet mask.

Le regole che la wildcard mask applica sono:

- Bit 0 significa che, all'atto del confronto con l'indirizzo IP associato, il corrispondente bit di quest'ultimo verrà "controllato".
- Bit 1, al contrario, significa che il corrispondente bit dell'indirizzo IP verrà ignorato.

Un esempio che ha come scopo quello di consolidare il concetto di wildcard mask potrebbe essere il seguente:

Indirizzo IP: 192.168.1.0/24 = 11000000.10101000.00000001.00000000

Wildcard Mask: 0.0.0.255 = 00000000.00000000.00000000.11111111

Ciò significa che, applicando la maschera 0.0.0.255 all'indirizzo IP 192.168.1.0, si ottiene una selezione di tutti gli indirizzi IP che hanno i primi 3 byte posti a 192.168.1, mentre l'ultimo byte, in fase di confronto, verrà ignorato, e potrà dunque assumere un qualsiasi valore compreso tra 1 e 254, ottenendo una selezione di tutti gli indirizzi nel range 192.168.1.1-192.168.1.254.

La Wildcard mask può essere agevolmente calcolata a partire dalla subnet mask, sottraendo ciascun byte della subnet mask alla cifra 255, per cui:

Indirizzo IP: 192.168.1.0/24 = 11000000.10101000.00000001.00000000

Subnet mask: 255.255.255.0 = 11111111.11111111.11111111.00000000

Wildcard mask: 0.0.0.255 = 00000000.00000000.00000000.11111111

Per controllare con la massima efficienza il processo OSPF e, in questo caso, gli spazi di indirizzi a cui sarà permessa la comunicazione con Internet, è buona pratica identificare l'indirizzo IP di una singola interfaccia logica o fisica del router. A tal proposito, è sufficiente utilizzare una wildcard mask nella quale tutti i 32 bit sono settati a 0, poiché ciò significherebbe che deve essere presente una corrispondenza con ciascun bit dell'indirizzo IP.

Per questo motivo, una wildcard mask pari a 0.0.0.0 = 00000000.00000000.00000000.00000000 identifica esattamente il singolo indirizzo IP al quale la wildcard mask viene applicata.

7.1 Configurazione OSPF

Di seguito si mostrano i comandi precedentemente illustrati applicati ai router R1 e R2, i quali permettono una completa configurazione del protocollo OSPF.

```
[R1]ospf 1
[R1-ospf-1]display this
[V200R003C00]
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 100.0.0.2 0.0.0.0
  network 192.168.10.254 0.0.0.0
  network 192.168.20.254 0.0.0.0
  network 192.168.30.254 0.0.0.0
#
return
```

Figura 57 - Configurazione OSPF nel router R1

```
[R2]ospf 1
[R2-ospf-1]display this
[V200R003C00]
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 100.0.0.1 0.0.0.0
  network 150.0.0.254 0.0.0.0
  network 160.0.0.254 0.0.0.0
#
return
```

Figura 58 - Configurazione OSPF nel router R2

Analizzando più dettagliatamente le figure 57 e 58, attraverso il comando *network* si comunica quali sono le interfacce che partecipano al processo OSPF e che devono quindi essere dichiarate come raggiungibili.

Difatti, all'interno del terminale del router R1 sono stati dichiarati i seguenti indirizzi IP:

- 100.0.0.2, il quale corrisponde all'indirizzo dell'interfaccia GE0/0/0.
- 192.168.10.254, essendo l'indirizzo dell'interfaccia VLANIF 10.
- 192.168.20.254, essendo l'indirizzo dell'interfaccia VLANIF 20.
- 192.168.30.254, essendo l'indirizzo dell'interfaccia VLANIF 30.

Con lo stesso ragionamento, all'interno del terminale del router R2 sono stati dichiarati i seguenti indirizzi IP:

- 100.0.0.1, il quale corrisponde all'indirizzo dell'interfaccia GE0/0/0.
- 150.0.0.254, essendo l'indirizzo dell'interfaccia GE0/0/1, la quale si collega direttamente con l'host pubblico PC5.
- 160.0.0.254, essendo l'indirizzo dell'interfaccia GE0/0/2, la quale si collega direttamente con l'host pubblico Client1.

In relazione alle motivazioni precedentemente illustrate, è stata assegnata una wildcard mask con valore 0.0.0.0 a tutti gli indirizzi definiti; in questo modo si ottiene la certezza che gli host appartenenti alla rete privata potranno comunicare esclusivamente con gli host pubblici PC5 e Client1 e, in generale, un maggior controllo sul processo OSPF.

Dopo l'avvenuta configurazione di OSPF in ambo i router sarà possibile la comunicazione tra un host appartenente alla rete privata ed uno dei due host pubblici.

Eseguendo una prova del corretto trasferimento dei pacchetti tra l'host PC1 e l'host PC5 attraverso il comando *ping 150.0.0.5* all'interno del terminale dell'host PC1, è possibile verificare quanto appena detto.

```
PC1>ping 150.0.0.5

Ping 150.0.0.5: 32 data bytes, Press Ctrl_C to
break
From 150.0.0.5: bytes=32 seq=1 ttl=126 time=47 ms
From 150.0.0.5: bytes=32 seq=2 ttl=126 time=62 ms
From 150.0.0.5: bytes=32 seq=3 ttl=126 time=63 ms
From 150.0.0.5: bytes=32 seq=4 ttl=126 time=47 ms
From 150.0.0.5: bytes=32 seq=5 ttl=126 time=47 ms

--- 150.0.0.5 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
 round-trip min/avg/max = 47/53/63 ms
```

Figura 59 - Risultato ping PC1-PC5

Osservando quanto riporta la figura 59, il trasferimento dei 5 pacchetti inviati dal PC1 sono stati trasmessi e ricevuti correttamente, con una percentuale di perdita di pacchetti pari al 0%.

8.0 ACL

In questo capitolo e nei successivi verranno illustrate le tecnologie necessarie al completamento delle seguenti specifiche di progetto:

- ✓ Configurare NAT per la VLAN 10 e verificarne il funzionamento.
- ✓ Considerare il Server1 appartenente ad una DMZ:
 - I. La porta 80 deve essere raggiungibile dall'esterno (PC5 - Client1)
 - II. Non deve essere raggiungibile dalla VLAN 20

Tuttavia, è prima necessario introdurre un concetto chiave che prende il nome di ACL.

ACL, acronimo di Access Control List, è una lista di istruzioni che definisce le regole applicate alle interfacce di un router, le quali indicano al router i pacchetti che deve accettare o scartare in base alle specifiche descritte all'interno delle ACL stesse.

Le ACL sono utilizzate per filtrare, classificare e selezionare i pacchetti in ingresso o in uscita da una interfaccia di rete e possono essere quindi applicate con l'obiettivo di controllare il flusso del traffico. A prescindere dalla funzione che si vuole implementare, il modo in cui si realizza una ACL è sempre lo stesso:

- Il pacchetto viene “catturato” dalla ACL sulla base del matching, ovvero quando i parametri del pacchetto, in termini di indirizzo IP, corrispondono a quelli delle ACL.
- Dopo che il pacchetto è stato catturato, viene eseguita su di esso una operazione che può essere:
 1. *permit*, la quale permette il trasferimento del pacchetto.
 2. *deny*, la quale nega il trasferimento del pacchetto.
 3. *log*, la quale produce un messaggio di log.

Dunque, filtrare il traffico significa definire una serie di parametri che consentiranno di identificare i pacchetti che possono attraversare l'interfaccia o meno.

Esistono tre tipi di ACL:

- Basic ACL, sono in grado di filtrare il traffico esclusivamente in base all'indirizzo IP sorgente dei pacchetti e possono assumere un valore compreso tra 2000 e 2999.

- Advanced ACL, forniscono una estensione nella definizione dei parametri utilizzati per filtrare il traffico, consentendo un match basato su:
 1. l'indirizzo IP della sorgente e della destinazione.
 2. i numeri di porta della sorgente e della destinazione.
 3. il tipo di protocollo adoperato.

Una advanced ACL può essere istanziata applicando un valore compreso nel range 3000-3999.

- Layer 2 ACL, filtrano il traffico in base ad informazioni di livello 2, come l'indirizzo MAC della sorgente o della destinazione.

In particolare, le ACL vengono applicate sull'interfaccia nella direzione di uscita del traffico, dopo la quale solo i pacchetti che soddisfano i criteri definiti dalle ACL saranno inoltrati.

Esistono delle best practices riguardo la posizione in cui configurare determinate ACL. È preferibile configurare le advanced ACL il più vicino possibile alla sorgente dei pacchetti che si vogliono filtrare, poiché essendo delle regole lunghe e stringenti, consentono di limitare il traffico.

Al contrario, le basic ACL debbono essere configurate il più vicino possibile alla destinazione dei pacchetti, perché essendo delle regole molto generiche, in questo modo si contiene l'effetto di eventuali errori nel filtraggio del traffico.

9.0 NAT

NAT, acronimo di Network Address Translation, è un meccanismo diventato fondamentale dal momento in cui gli indirizzi IP pubblici del protocollo IPv4 (circa 4 miliardi e 300 milioni) hanno cominciato a scarseggiare, visto l'aumento esponenziale dei dispositivi connessi alla rete in tutto il mondo.

In attesa dell'introduzione di soluzioni a lungo termine, ovvero del protocollo IPv6 e dei relativi indirizzi IPv6, è stata adottata la tecnologia NAT, la quale permette di modificare l'indirizzo IP dei pacchetti in transito durante la comunicazione tra due o più dispositivi nel momento in cui attraversano un router, o, più in generale, un dispositivo di livello 3.

In particolare, NAT viene utilizzato per nascondere dietro ad un unico indirizzo IP pubblico uno o più indirizzi IP privati.

Nonostante l'avvento del nuovo protocollo di assegnazione di indirizzi IP IPv6, questa tecnica di mascheramento degli indirizzi privati è rimasta molto utilizzata per la sua comodità; difatti, grazie a NAT, tutti i dispositivi connessi ad una LAN potranno accedere ad Internet utilizzando, e quindi "consumando", un singolo indirizzo IP pubblico.

Quando un host della rete privata effettua una richiesta di comunicazione con un host appartenente alla rete pubblica, il router modificherà il contenuto del campo *Source IP address* dei pacchetti trasmessi nel momento in cui questi lasciano la rete privata stessa. Allo stesso modo, durante la risposta effettuata dall'host pubblico, il router riceve i pacchetti e ne modifica il contenuto del campo *Destination IP address*, nell'istante in cui questi entrano nella LAN.

Dunque, il dispositivo che effettua la traduzione degli indirizzi IP deve essere necessariamente un dispositivo di livello tre, in quanto deve manipolare gli indirizzi IP della sorgente e della destinazione; è importante sottolineare che la traduzione degli indirizzi IP viene eseguita nel confine tra la rete privata e la rete pubblica.

Per apprendere meglio il funzionamento di NAT e il processo di modifica dell'header IP da parte del traduttore di indirizzi, quindi il router, si propone il seguente esempio:

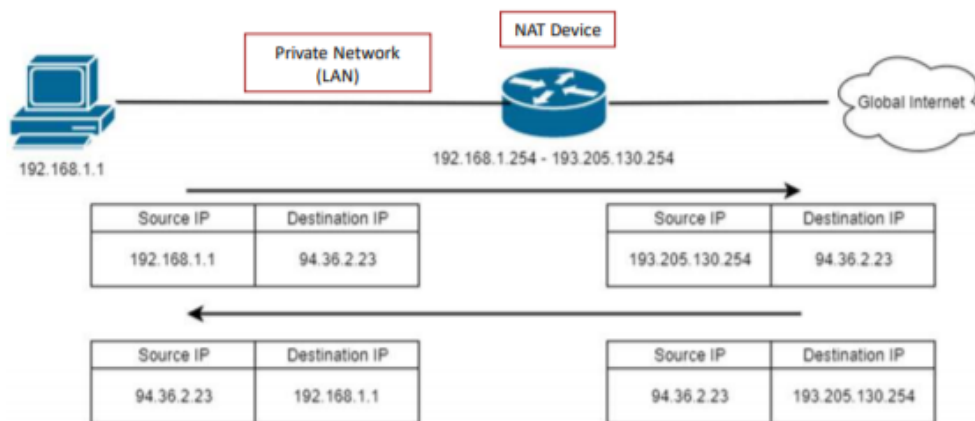


Figura 60 - Esempio del meccanismo NAT

Si consideri la situazione in cui l'host A con indirizzo IP 192.168.1.1 appartenente alla rete privata debba comunicare con un dispositivo della rete pubblica, con indirizzo IP 94.36.2.23. Essendo l'indirizzo IP di destinazione al di fuori del suo spazio di indirizzi ed a lui sconosciuto, l'host A invia i pacchetti al suo default gateway, in questo caso, all'interfaccia del router con indirizzo IP 192.168.1.254. Il router, una volta ricevuti i pacchetti, effettua il NAT: l'indirizzo IP sorgente dei pacchetti viene modificato e sostituito con un indirizzo IP pubblico, in questo caso, 193.205.130.254, in modo che il dispositivo di destinazione riceva un pacchetto con un indirizzo IP pubblico valido, attraverso il quale potrà indirizzare correttamente un eventuale pacchetto di risposta; l'indirizzo IP di destinazione nell'header IP dei pacchetti rimane il medesimo. In questo momento verrà compilata anche una tabella che tiene traccia delle traduzioni di indirizzi effettuate, in questo caso, la traduzione 192.168.1.1-193.205.130.254.

Salvo errori esterni, il destinatario riceve i pacchetti e si prepara ad inviare una risposta, la quale sarà indirizzata all'indirizzo pubblico 193.205.130.254 ed avrà come indirizzo sorgente il proprio indirizzo IP, 94.36.2.23. Quando il router riceve i pacchetti di risposta, controlla la tabella delle traduzioni precedentemente istanziata per verificare l'indirizzo a cui deve realmente inoltrarli: il destinatario reale è proprio l'host A con indirizzo IP 192.168.1.1, pertanto avverrà nuovamente una traduzione dell'header IP dei pacchetti che hanno indirizzo IP sorgente 94.36.2.23 ed indirizzo IP di destinazione 192.168.1.1.

Esistono molteplici tipologie di implementazione del meccanismo NAT, ciascuna adattabile in base alle proprie esigenze.

Ad esempio, l'implementazione Easy IP viene applicata laddove si avesse a che fare con pochi host all'interno di una LAN su piccola scala che hanno la necessità di accedere ad Internet, adoperando

una politica molti a uno. Il suo funzionamento si basa sull'utilizzo di numeri di porta differenti per distinguere gli host interni alla LAN e si contraddistingue dal fatto che è presente un singolo indirizzo IP pubblico temporaneo, il quale corrisponde all'indirizzo IP di un'interfaccia di rete del router stesso, utilizzabile da tutti gli host privati per comunicare con Internet.

Relativamente alle specifiche di progetto che devono essere implementate alla topologia di rete, è richiesta la configurazione di NAT per la VLAN 10 e, conseguentemente, verificarne il funzionamento. Dunque, la situazione che si vuole ottenere è quella in cui tutti gli indirizzi IP privati degli host appartenenti alla VLAN 10, quindi quelli evidenziati dall'area verde, abbiano la possibilità di essere tradotti con un indirizzo IP pubblico avente differenti numeri di porta per ciascun host, il quale consentirà l'accesso ad Internet.

Gli host che nell'attuale topologia di rete potrebbero richiedere la comunicazione con Internet e, di conseguenza, la possibile traduzione del proprio indirizzo IP, sono limitati; per questo motivo, nell'ottica in cui la rete privata rimanga contenuta, NAT è stato implementato usufruendo della tecnica Easy IP.

Viceversa, nel caso in cui si abbiano margini di crescita in termini di host appartenenti alla rete privata, è consigliato applicare la tipologia di NAT che prende il nome di Dynamic NAT. In Dynamic NAT si utilizza un pool di indirizzi IP pubblici usufruibili dagli host della rete privata che desiderano comunicare con Internet, per cui l'associazione è molti a molti; questa tecnica è quindi adatta per le realtà che possiedono un elevato numero di host. Chiaramente, il numero di indirizzi IP pubblici è sempre minore al numero di indirizzi IP privati: nel caso in cui il numero di indirizzi IP pubblici presenti nel pool fosse limitato si potrebbe verificare la situazione in cui, alcuni host della rete privata, non riescano a comunicare con Internet, poiché tutti gli indirizzi del pool stesso sono attualmente in utilizzo, rendendo impossibile una comunicazione contemporanea da parte di tutti gli host della LAN.

9.1 Configurazione NAT

La configurazione di Easy IP risiede fondamentalmente nella creazione di una ACL che ha come scopo quello di definire l'intervallo di indirizzi IP a cui dovrà essere applicata la traduzione, vale a dire, tutti gli indirizzi IP della VLAN 10, e conseguentemente nell'applicazione del comando *nat outbound* in interface-view all'interno dell'interfaccia del router R1 che si collega al router R2, il quale rappresenta il dispositivo dell'ISP che fornisce l'accesso ad Internet.

```
[R1]acl 2000
[R1-acl-basic-2000]display this
[V200R003C00]
#
acl number 2000
 rule 5 permit source 192.168.10.0 0.0.0.255
#
return
```

Figura 61 - Creazione ACL 2000

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]display this
[V200R003C00]
#
interface GigabitEthernet0/0/0
 nat outbound 2000
#
return
```

Figura 62 - Completamento configurazione easy-IP

Osservando le figure 61 e 62, la ACL è stata creata applicando il comando *acl number 2000* in system-view all'interno del terminale del router R1, ovvero il dispositivo deputato alla traduzione degli indirizzi tra rete privata ed Internet. In questo caso, trattandosi di una specifica di filtraggio molto semplice, è stata definita come Basic ACL, la quale, come discusso nel capitolo 8, è rappresentata da una cifra compresa nel range 2000-2999, quindi 2000.

Successivamente è necessario istanziare la regola che raggruppa tutti gli indirizzi della VLAN 10, quindi appartenenti allo spazio di indirizzi 192.168.10.0/24. Applicando quindi il comando *rule 5 permit source 192.168.10.0 0.0.0.255* si raggruppa tutto il traffico proveniente dallo spazio di indirizzi della VLAN 10 con una clausola permit, a cui è quindi concesso il transito verso Internet. Si può notare come nel comando venga adoperata la wildcard mask 0.0.0.255 corrispondente alla subnet mask /24.

Dopo aver creato l'ACL è necessario accedere in interface-view all'interno dell'interfaccia del router che si collega ad Internet. Osservando la topologia di rete, l'interfaccia in questione corrisponde a GE 0/0/0 del router R1, la quale si collega con il router R2, ovvero il router dell'ISP. Pertanto, dopo esser entrati in interface-view attraverso il comando *interface GigabitEthernet 0/0/0*, è stato applicato il comando *nat outbound 2000*, il quale rappresenta il legame tra l'operazione di traduzione NAT e l'ACL precedentemente creata che specifica l'intervallo di indirizzi a cui verrà applicata la traduzione stessa. Il dispositivo sul quale sono stati configurati i comandi per eseguire Easy-IP è il router R1 poiché si trova nel confine tra rete privata ed Internet e l'indirizzo pubblico che verrà messo a disposizione per eventuali traduzioni sarà 100.0.0.2, il quale corrisponde all'indirizzo dell'interfaccia GE 0/0/0 del router R1 stesso.

Applicando il funzionamento di NAT alla topologia di rete, si può concludere che tutti i pacchetti inviati dagli host appartenenti alla VLAN 10 ed indirizzati verso un dispositivo appartenente ad Internet, vedranno cambiarsi il valore dell'attributo *Source IP address* dell'header dei pacchetti stessi nell'indirizzo IP pubblico dell'interfaccia GE 0/0/0, ovvero 100.0.0.2, ottenendo quindi un corretto meccanismo di traduzione e l'effettiva possibilità di comunicare con Internet.

Il comando `display nat outbound` può essere utilizzato per verificare l'implementazione della dell'istruzione `nat outbound`, osservando:

- il binding dei valori degli attributi *Interface* e *Acl*, quindi GE 0/0/0 e 2000.
- il valore dell'attributo *Interface* che corrisponde all'indirizzo pubblico impiegato per il meccanismo di traduzione, quindi 100.0.0.2.
- il valore dell'attributo *Type* correttamente impostato a `easyip`.

```
[R1]display nat outbound
NAT Outbound Information:
-----
Interface                Acl      Address-group/IP/Interface  Type
-----
GigabitEthernet0/0/0    2000     100.0.0.2                   easyip
-----
Total : 1
```

Figura 63 - Risultato del comando eseguito in R1

Infine, per analizzare il meccanismo NAT, è possibile effettuare una doppia ispezione parallela, in particolare delle interfacce GE 6/0/2 e GE 0/0/0 del router R1 stesso, tramite Wireshark.

Eseguendo quindi un ping all'interno del terminale dell'host PC1 con indirizzo 192.168.10.1 appartenente alla VLAN 10 verso l'host PC5 con indirizzo 150.0.0.5, che possiamo ipotizzare essere un qualunque host appartenente alla rete pubblica, e prendendo in considerazione il primo pacchetto *request* che viaggerà a partire dall'host PC1 fino ad arrivare all'host PC5, il risultato fornito da Wireshark è il seguente:

```
GigabitEthernet 6/0/2
No.    Time           Source           Destination      Protocol  Length  Info
-----
12 20.281000     192.168.10.1    150.0.0.5       ICMP      78      Echo (ping) request id=0x4be1, seq=1/256, ttl=128 (reply in 13)
13 20.297000     150.0.0.5       192.168.10.1    ICMP      78      Echo (ping) reply id=0x4be1, seq=1/256, ttl=126 (request in 12)
-----
> Frame 12: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface -, id 0
> Ethernet II, Src: HuaweiTe_fb:6d:0e (54:89:98:fb:6d:0e), Dst: HuaweiTe_0b:49:fd (00:e0:fc:0b:49:fd)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 150.0.0.5
  0100 ... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xe14b (57675)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xb8c6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.1
    Destination: 150.0.0.5
> Internet Control Message Protocol
```

Figura 64 - Ispezione sull'interfaccia GE6/0/2 del router R1

```
GigabitEthernet 0/0/0
No.    Time                Source                Destination           Protocol  Length  Info
-----
5 18.485000          100.0.0.2            150.0.0.5             ICMP      74      Echo (ping) request  id=0x0528, seq=1/256, ttl=127 (reply in 6)
6 18.500000          150.0.0.5            100.0.0.2             ICMP      74      Echo (ping) reply    id=0x0528, seq=1/256, ttl=127 (request in 5)

> Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0
> Ethernet II, Src: HuaweiTe_0b:49:fd (00:e0:fc:0b:49:fd), Dst: HuaweiTe_64:4b:a6 (00:e0:fc:64:4b:a6)
v Internet Protocol Version 4, Src: 100.0.0.2, Dst: 150.0.0.5
  0100 ... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xe081 (57473)
  > Flags: 0x4000, Don't fragment
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 127
  Protocol: ICMP (1)
  Header checksum: 0x2138 [validation disabled]
  [Header checksum status: Unverified]
  Source: 100.0.0.2
  Destination: 150.0.0.5
> Internet Control Message Protocol
```

Figura 65 - Ispezione sull'interfaccia GE0/0/0 del router R1

Come mostra la figura 64, nel momento in cui il pacchetto oltrepassa l'interfaccia GE 6/0/2 del router R1, il valore dell'attributo *Source* è equivalente a 192.168.10.1, ovvero esattamente l'indirizzo IP privato dell'host PC1, mentre il valore del campo *Destination* è 150.0.0.5, essendo l'indirizzo IP dell'host PC5.

Quando il pacchetto attraverserà il collegamento che connette i due router R1 e R2 avverrà la traduzione, in particolare l'interfaccia GE 0/0/0 del router R1, la quale corrisponde esattamente all'interfaccia in cui è stato precedentemente configurato il comando *nat outbound 2000*. Il risultato fornito da Wireshark relativamente all'ispezione eseguita sull'interfaccia GE 0/0/0 del router R1, come mostrato nella figura 65, consente di notare il processo di traduzione secondo il meccanismo del NAT. Infatti, ora il valore dell'attributo *Source* equivale a 100.0.0.2, il quale è esattamente l'indirizzo IP pubblico dell'interfaccia GE 0/0/0 del router R1 che consente al pacchetto di giungere a destinazione ed essere ricevuto correttamente dall'host PC5.

A seguito della prima traduzione, il router R1 ha registrato all'interno di una tabella allocata in memoria la coppia di indirizzi tradotti, ovvero 192.168.10.1-100.0.0.2. In questo modo, nel momento in cui l'host PC5 invierà un pacchetto di risposta (*reply*), il quale effettuerà esattamente il percorso inverso del pacchetto di richiesta (*request*), verrà applicata automaticamente un'ulteriore traduzione speculare alla prima tra i medesimi indirizzi IP. Quindi, il pacchetto di risposta che il router R1 riceverà avrà come valore del campo *Destination* esattamente indirizzo IP 100.0.0.2, il quale verrà poi tradotto in 192.168.10.1 ed inoltrato all'host PC1.

Per rendere questo processo ancora più pratico è possibile fare un'analogia con la quotidianità che viviamo tutti i giorni. Infatti, il classico modem di casa opera proprio come il router R1 della topologia

di rete: utilizza un indirizzo IP pubblico fornito direttamente dall'ISP per eseguire il NAT, eseguendo la traduzione tra l'indirizzo IP privato del nostro computer e l'indirizzo IP pubblico prima citato ad ogni richiesta da noi effettuata verso Internet.

10.0 DMZ

In una realtà aziendale che offre servizi rivolti all'esterno, come, ad esempio, un sito web, è necessario rendere il proprio server web accessibile agli utenti pubblici di Internet, ma ciò significherebbe mettere a rischio tutta la rete interna.

Con il fine di evitare che ciò accada, l'azienda potrebbe decidere di ospitare il server web all'interno di una DMZ, acronimo di Demilitarized Zone, ovvero una zona demilitarizzata, ed è proprio questa la specifica di progetto da applicare alla topologia di rete oggetto di studio: allocare il Server1 all'interno di una DMZ.

Una DMZ è una sottorete fisica o logica che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura, come ad esempio Internet. Lo scopo di una DMZ è di proteggere la rete LAN aziendale di un'organizzazione, aggiungendo un ulteriore strato di sicurezza, dove un nodo appartenente ad una rete esterna può accedere soltanto ai servizi messi a disposizione, senza mettere a rischio e compromettere la sicurezza dell'intera rete.

Una zona demilitarizzata può essere creata attraverso la definizione di policy su uno o più firewall. Un firewall è un componente hardware o software utilizzato per la sicurezza della rete, che permette di monitorare il traffico di dati, sia in entrata che in uscita, definendo una serie di regole specifiche, le quali permettono di bloccare le trasmissioni pericolose o indesiderate.

Il firewall si interpone tra la rete esterna, che comprende Internet, e la rete interna dell'azienda. Da un punto di vista teorico, la rete interna è considerata conosciuta, sicura, attendibile e protetta, mentre quella esterna è la presunta fonte di potenziali minacce, in quanto, nel complesso, è sconosciuta, insicura e non attendibile.

10.1 Configurazione DMZ

Applicando questi concetti teorici alla nostra topologia di rete, è possibile identificare il router R1 nel dispositivo che agisce da firewall, poiché si interpone tra la rete esterna, che comprende Internet, e la rete interna dell'azienda.

Le specifiche di progetto richiedono che il Server1 debba essere collocato all'interno di una DMZ e la definizione di due regole che filtreranno il traffico proveniente Internet:

1. La porta 80 del Server1 deve essere raggiungibile dall'esterno, quindi dal PC5 e dal Client1, i quali rappresentano due generici host di Internet.

2. Il Server non deve essere raggiungibile dalla VLAN 20.

La porta 80 corrisponde alla porta sulla quale il Server1, che in questo caso possiamo considerare essere un Web Server [5], resta in ascolto delle richieste di tipo HTTP [6] da parte dei client, come, ad esempio, la richiesta di accedere ad un sito web che risiede nel Server1 stesso.

Per istanziare la prima regola si è fatto affidamento ad una tipologia di NAT che prende il nome di NAT Internal Server.

NAT Internal Server consente di tradurre l'indirizzo IP pubblico ed il numero di porta di una richiesta proveniente da un host appartenente ad Internet nel corrispondente indirizzo IP privato e numero di porta, in base alla mappatura preconfigurata.

In particolare, ad ogni nuova richiesta proveniente da Internet, il router R1 compila una tabella che consente di tener traccia delle traduzioni di indirizzi IP effettuate.

Si consideri il caso in cui un host appartenente ad Internet, ad esempio l'host PC5, effettui una richiesta indirizzata al Server1, appartenente alla rete privata. Per eseguire la richiesta è innanzitutto necessario definire un indirizzo IP pubblico che identifichi univocamente il Server1 su Internet, ovvero tale per cui ciascuna richiesta proveniente da Internet abbia come valore dell'attributo *Destination IP address* dei pacchetti esattamente l'indirizzo IP in questione. Questo passaggio è doveroso poiché gli host su Internet non sono a conoscenza dell'indirizzo IP privato del Server1 e, per questo motivo, è stato selezionato un indirizzo IP pubblico pari a 100.0.0.30.

Per abilitare il meccanismo di traduzione secondo NAT Internal Server, è prima di tutto necessario accedere in interface-view all'interno dell'interfaccia GE 0/0/0 del router R1 attraverso il comando *interface GigabitEthernet 0/0/0*, poiché si tratta del dispositivo che agisce da firewall.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]display this
[V200R003C00]
#
interface GigabitEthernet0/0/0
 nat server protocol tcp global 100.0.0.30 www inside 192.168.30.1 www
#
return
```

Figura 66 - Configurazione NAT Internal Server

Successivamente, come mostra la figura 66, è stato applicato uno specifico comando che configura correttamente NAT Internal Server. Esaminandolo più dettagliatamente:

- *tcp* indica il tipo di protocollo utilizzato dall'host appartenente ad Internet per effettuare la richiesta. Dovendo stabilire una connessione e rendere raggiungibile la porta 80 del Server1, è intuibile come le richieste saranno di tipo http e il protocollo impiegato per trasportare questo tipo di richieste è TCP [7]. Nel caso in cui la richiesta fosse stata, ad esempio, quella di guardare un video in streaming, quindi applicativi che necessitano di trasmissioni broadcast, il protocollo adoperato avrebbe dovuto essere *udp*.
- *100.0.0.30*, corrisponde all'indirizzo IP pubblico precedentemente trattato. Ciò significa che questa regola prenderà in considerazione solamente i pacchetti che hanno come valore dell'attributo *Destination IP address* l'indirizzo 100.0.0.30, che identifica univocamente il Server1 su Internet.
- *www* ha esattamente lo stesso significato della cifra 80, identificando il fatto che la richiesta è di tipo http. Dunque, il servizio offerto potrebbe essere, ad esempio, l'accesso ad un sito web allocato all'interno del Server1.
- *192.168.30.1*, corrisponde all'indirizzo IP privato del Server1. Esso permette quindi al router R1 di effettuare la traduzione per poi conseguentemente essere in grado di inoltrare i pacchetti di richiesta esattamente al Server1.

Riassumendo, attraverso questo comando si comunica al router R1 che qualsiasi richiesta di tipo http, quindi trasportata dal protocollo tcp e destinata all'indirizzo IP pubblico 100.0.0.30 con numero di porta 80, deve essere inoltrata al Server1 con indirizzo IP privato 192.168.30.1.

Nel momento in cui il Server 1 processerà le richieste e produrrà i corrispondenti risultati, i pacchetti di risposta riceveranno il medesimo meccanismo di traduzione tra la coppia di indirizzi IP 100.0.0.30-192.168.30.1 ed effettueranno il percorso inverso rispetto a quello della prima richiesta dell'host pubblico. Il router R1 sarà quindi in grado di realizzare la traduzione grazie alla tabella che aveva creato durante la prima richiesta, inoltrando correttamente la risposta all'host interessato.

Il comando *display nat server* applicato in system-view all'interno del router R1 permette di verificare la corretta implementazione di NAT Internal Server:

```

[R1]display nat server

Nat Server Information:
Interface   : GigabitEthernet0/0/0
Global IP/Port   : 100.0.0.30/80 (www)
Inside IP/Port   : 192.168.30.1/80 (www)
Protocol   : 6 (tcp)
VPN instance-name : ----
Acl number    : ----
Description   : ----

Total :    1

```

Figura 67 - Risultato comando definito in R1

Relativamente alla figura 67, il campo *Interface* definisce il punto in cui avverrà la traduzione degli indirizzi mentre i campi *Global IP/Port* e *Inside IP/Port* indicano rispettivamente l'indirizzo IP pubblico ed il numero di porta e l'indirizzo IP privato ed il numero di porta che verranno tradotti.

È importante notare come, attualmente, il router R2 non sia a conoscenza dell'indirizzo IP pubblico 100.0.0.30 che identifica il Server1, per cui non sarebbe in grado di instradare i pacchetti di richiesta http inviati dagli host pubblici verso il Server1 stesso. È quindi necessario specificare una rotta statica all'interno del router R2 che permetta di definire il comportamento del router R2 stesso nel momento in cui dovesse ricevere pacchetti con il valore del campo *Destination IP address* pari a 100.0.0.30.

A tal proposito, è stata configurata una *static-route* in system-view all'interno del router R2 attraverso il seguente comando:

```

[R2]display this
[V200R003C00]
#
ip route-static 100.0.0.30 255.255.255.255 100.0.0.2
#
return

```

Figura 68 - Configurazione static-route

Come è mostrato in figura 68, attraverso il comando *ip route-static 100.0.0.30 255.255.255.255 100.0.0.2*, si comunica al router R2 che tutti i pacchetti da lui ricevuti con valore dell'attributo *Destination IP address* pari a 100.0.0.30 e subnet mask uguale a 255.255.255.255, che identifica quindi il singolo indirizzo IP, devono essere inoltrati all'indirizzo IP 100.0.0.2, il quale corrisponde all'interfaccia GE 0/0/0 del router R1; successivamente, una volta ricevuti i pacchetti grazie al

comando NAT Internal Server precedentemente configurato, il router R1 saprà sicuramente inoltrarli correttamente verso la destinazione corretta, ovvero il server Server1.

Per effettuare una verifica del funzionamento di NAT Internal Server, dell'effettiva raggiungibilità della porta 80 a partire dagli host pubblici e del corretto scambio di dati tra gli host PC5 e Client 1 con il Server1, all'interno della cartella di progetto eNSP è stata appositamente creata un'ulteriore cartella contenente un file HTML molto semplice, il quale rappresenta l'ipotetico servizio offerto dal Server1.

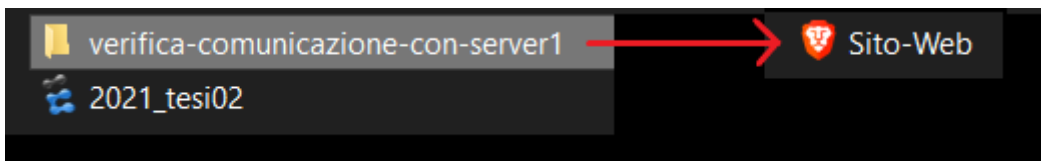


Figura 69 - Path del file Sito-Web

Il simulatore eNSP consente di attivare un Web Server, all'interno del quale è possibile impostare il numero di porta, ovvero 80, ed il percorso (*Root Path*) nel file system locale che permette di raggiungere la cartella in cui è stata salvata la pagina HTML, chiamata Sito-Web.

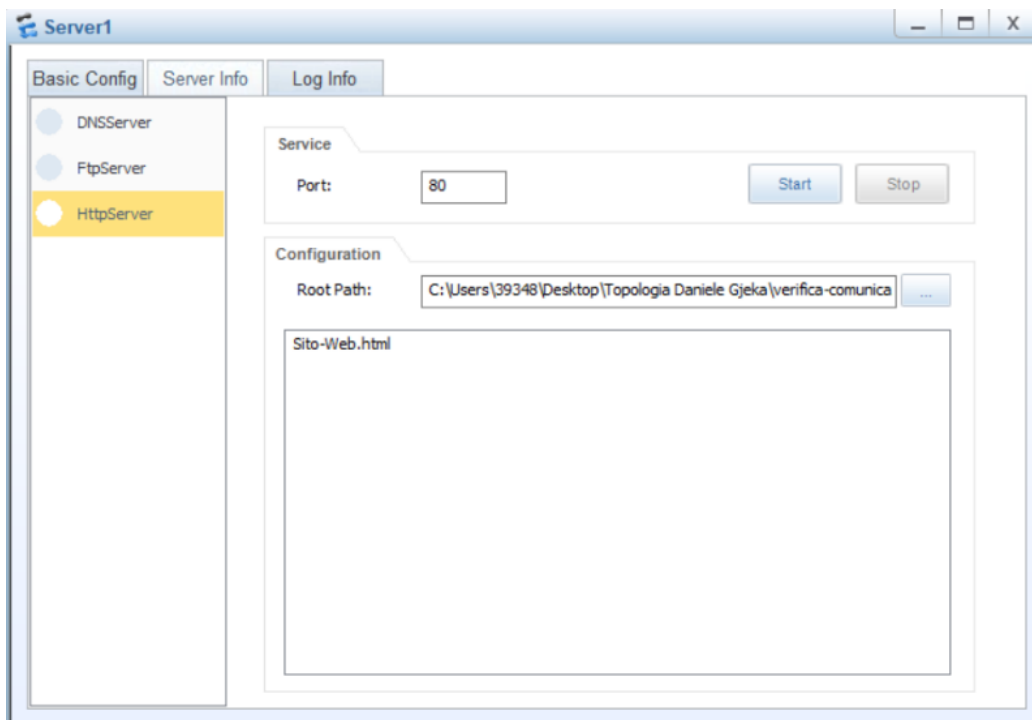


Figura 70 - Interfaccia HttpServer

Inoltre, è possibile avvalersi dell'host Client1 e specializzarlo come *HttpClient*, ottenendo la possibilità di effettuare una richiesta al Web Server specificando il documento che si vuole ricevere tramite URL, come se fosse un classico browser.

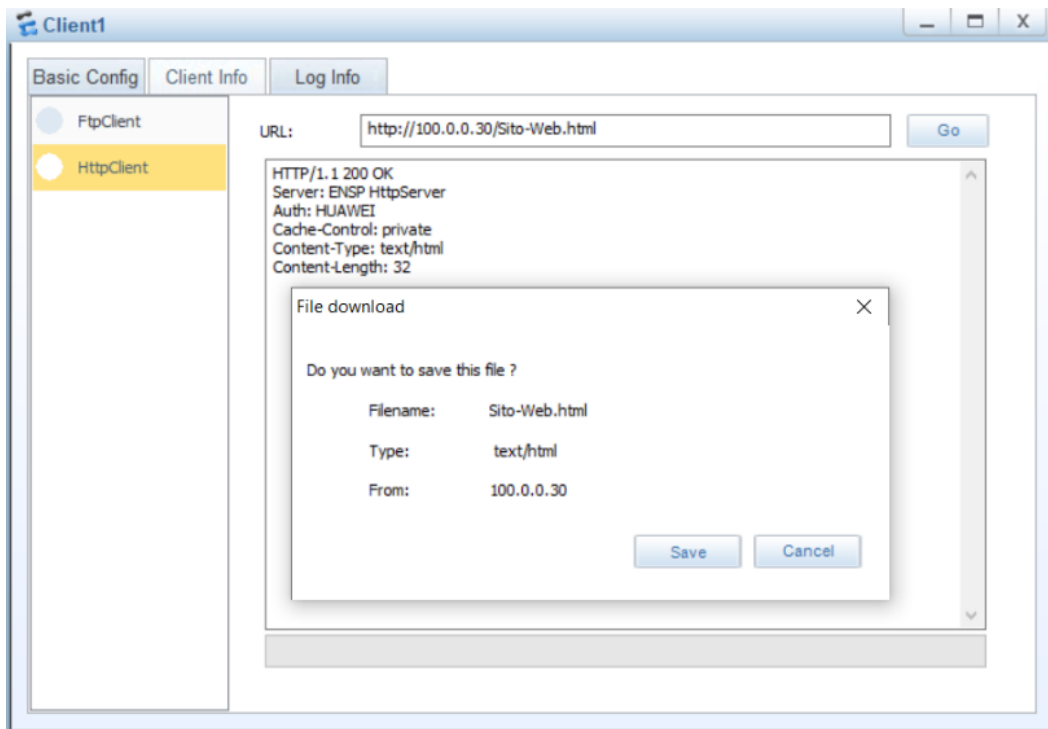


Figura 71 - interfaccia HttpClient

Dopo aver avviato il Web Server premendo il bottone *Start*, digitato l'URL secondo la sua sintassi ed infine premuto il bottone *Go* per effettuare la richiesta, il risultato è stato quello atteso: la richiesta ha avuto esito positivo, il che si può constatare dal codice dell'interazione http pari a 200 e dalla finestra di download del file *Sito-Web.html* mostrata da eNSP.

Attraverso queste componenti è stato possibile verificare il corretto funzionamento di NAT Internal Server e l'effettiva comunicazione tra il Client1, quindi un host pubblico appartenente ad Internet, ed il Server1, il quale ha fornito il servizio di accesso alla pagina html *Sito-Web.html*.

In conclusione, per completare le regole che definiscono la DMZ, è necessario fare in modo che ogni host appartenente alla VLAN 20 non riesca a raggiungere il Server1. È stata quindi creata un'apposita ACL con identificativo pari a 2001 eseguendo il comando *acl 2001* in system-view all'interno del router R1, contenente un'unica regola con clausola *deny*.

```
[R1]acl 2001
[R1-acl-basic-2001]display this
[V200R003C00]
#
acl number 2001
 rule 5 deny source 192.168.20.0 0.0.0.255
#
return
```

Figura 72 - Creazione ACL 2001

```
[R1]interface Vlanif 30
[R1-Vlanif30]display this
[V200R003C00]
#
interface Vlanif30
 traffic-filter outbound acl 2001
#
return
```

Figura 73 - Applicazione ACL 2001

Ad un maggior livello di dettaglio, attraverso il comando *rule 5 deny source 192.168.20.0 0.0.0.255* è stata definita una regola tale per cui tutti i pacchetti che il router R1 riceverà aventi come valore dell'attributo *Destination IP Address* un indirizzo compreso tra 192.168.20.1 e 192.168.20.254, ovvero tutto lo spazio di indirizzi della VLAN 20, verranno scartati a causa della clausola *deny* specificata, come è stato trattato nel capitolo 8.

In effetti, eseguendo una verifica di comunicazione a partire terminale dell'host PC2, il quale appartiene alla VLAN 20, verso il server Server1 con indirizzo 192.168.30.1 attraverso il comando *ping 192.168.30.1*, il risultato è il seguente:

```
PC>ping 192.168.30.1

Ping 192.168.30.1: 32 data bytes, Press
Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.30.1 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```

Figura 74 - Risultato ping PC2-Server1

Come riporta la figura 74, nessuno dei cinque pacchetti inviati è giunto a destinazione, ottenendo una percentuale pari al 100% di perdita di pacchetti.

11.0 Conclusioni

L'obiettivo finale della risoluzione della topologia di rete era quello di fare in modo che i nodi di tutte le VLAN potessero comunicare tra loro e, grazie a tutte le tecnologie applicate, è stato pienamente raggiunto.

In questo elaborato di tesi sono stati introdotti i concetti teorici e le corrispondenti configurazioni pratiche solamente di una parte dei protocolli e delle tecnologie esistenti nel mondo del network ed appresi nel periodo di studio del corso HCIA, il che fa capire quanto questo settore sia in crescita.

12.0 Bibliografia

- [1] https://it.wikipedia.org/wiki/Classi_di_indirizzi_IP
- [2] <https://it.wikipedia.org/wiki/Duplex>
- [3] https://it.wikipedia.org/wiki/Internet_Control_Message_Protocol
- [4] https://it.wikipedia.org/wiki/Link_state
- [5] https://it.wikipedia.org/wiki/Server_web
- [6] <https://www.ionos.it/digitalguide/hosting/tecniche-hosting/richiesta-http/>
- [7] https://it.wikipedia.org/wiki/Transmission_Control_Protocol