UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI INGEGNERIA

CORSO DI LAUREA IN INGEGNERIA ELETTRONICA

ARCHITETTURE DI RETE IN AMBIENTE ENTERPRISE

NETWORK ARCHITECTURES IN ENTERPRISE ENVIRONMENT

Relatore:
PROF. ENNIO GAMBI

Tesi di laurea di:
MARCO FORTUNA

Correlatore:
PROF. ADELMO DE SANTIS

A.A. 2021/2022

Alla mia famiglia e a mia madre Carla,
che hanno sempre creduto in me, fino alla fine.

Indice

1 Introduzione

1.1 Il Networking

Nel mondo in cui viviamo è impossibile non aver mai sentito parlare di networking. Il termine stesso può essere poco conosciuto ma il suo significato pratico è ben noto a tutti. Questo in virtù del fatto che praticamente ogni edificio (che sia una casa, un capannone industriale o un ospedale) dispone di una rete di telecomunicazioni al suo interno che può servire semplicemente per navigare in internet piuttosto che per mandare e-mail, pec, documenti, etc. o anche per gestire dei dati in maniera centralizzata. Risulta evidente come la conoscenza del mondo del networking sia essenziale (nonché interessante) per la comprensione e la progettazione di una rete di telecomunicazioni.

Il termine "networking" deriva dalla parola "network", ovvero dall'unione delle parole "net" (rete) e "work" (lavoro), che in italiano viene spesso utilizzata come sinonimo di rete. Il networking invece fa riferimento a un sistema di collegamento in rete di più elaboratori e utenti, comprendente le piattaforme, i sistemi operativi, i protocolli e le architetture di rete. Per essere più specifici per quanto concerne la definizione data, il networking tratta l'installazione e la configurazione dei sistemi operativi negli apparati di rete (pc, switch, router, etc.), la definizione dei protocolli che verranno adoperati (ovvero di tutto quell'insieme di regole che permette lo scambio di dati in maniera ordinata e sensata fra due nodi della rete) e dell'architettura di rete. Quest'ultimo concetto merita una particolare attenzione. Per architettura di rete si intende una struttura logica che descrive il funzionamento di una rete, dalla trasmissione alla ricezione di dati applicativi.

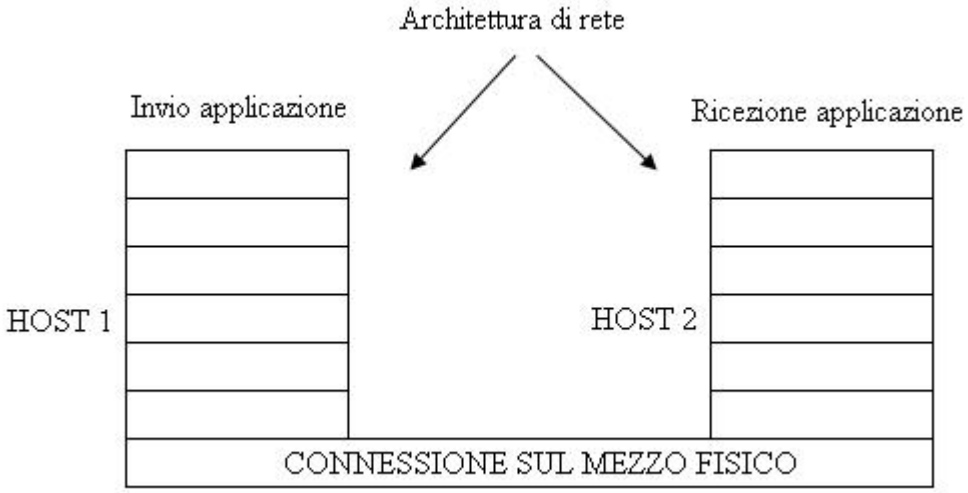


Figura 1.1: struttura generale di un'architettura di rete.

Strutture di questo tipo sono di solito composte da livelli dove ogni livello svolge una determinata mansione. L'interazione tra livelli porta all'esecuzione di varie funzioni che permettono lo scambio dati tra, ad esempio, due nodi di una rete. Queste funzionalità in buona parte non sono visibili all'utente, che al massimo può vedere solo l'interfaccia dell'applicativo che sta usando e parte dell'infrastruttura fisica. Tutti i restanti livelli si nascondono all'interno dei software di funzionamento del sistema. Esempi classici di architetture di rete sono ad esempio il modello TCP/IP o il modello OSI, che sono attualmente i più utilizzati. La *figura 1.1* mostra qual è in generale la struttura di un modello di architettura di rete.

Per fare qualche esempio, un problema di networking può essere la scelta dei dispositivi da adottare nella progettazione di una rete di telecomunicazioni (cercando di rispettare anche il principio di economicità), la scelta dei protocolli che meglio rispondono alle esigenze della rete, la ridondanza dei collegamenti per poter garantire l'affidabilità, le modalità di accesso ai dispositivi per rispondere a determinati canoni di sicurezza e via dicendo. Questo singolo vocabolo, quindi, va oltre la semplice realizzazione fisica di una rete ma si occupa dei suoi aspetti più interni.

In conclusione, credo siano a questo punto abbastanza evidenti le motivazioni che mi hanno portato ad affrontare lo studio del networking. In verità fin da adolescente sono stato interessato al mondo delle telecomunicazioni. Ho avuto modo di avvicinarmi a questo settore scegliendo un indirizzo di studi tecnico e poi con la scelta del corso di laurea in ingegneria. Nel mentre mi sono appassionato sempre di più al settore delle telecomunicazioni e in particolare a quello del networking, verificando facilmente da me quanto lo studio di queste discipline sia fondamentale per comprendere il reale funzionamento dello scambio dati tra stazioni ricetrasmittenti.

1.2 Tecnologie del Networking

Di seguito sono citati gli apparati di maggiore utilizzo nell'ambito del networking. Tali dispositivi collegati in rete possono comunicare tra loro e con altre reti, come ad esempio la rete internet. La loro conoscenza è dunque essenziale per fare una buona progettazione e configurazione di una rete di telecomunicazioni. Tra gli apparati più utilizzati annoveriamo:

- Switch (*figura 1.2*): è un dispositivo di rete che svolge prettamente funzioni di livello due (L2 di seguito) nel modello di architettura di rete OSI. Viene utilizzato all'interno delle LAN (Local Area Network) per la connessione e la gestione centralizzata dei terminali utente, di stampanti, server e dispositivi di rete. È composto da un numero variabile di porte alle quali possono essere connessi dei dispositivi. Lo switch è utilizzato principalmente nelle reti aziendali e permette la comunicazione tra terminali di una stessa LAN tramite l'inoltro di PDU (Protocol Data Unit) chiamate "frame". Gli switch hanno memorizzate a loro interno delle "mac-address table", che contengono l'associazione tra un indirizzo MAC e la relativa porta dello switch. Tramite queste tabelle lo switch decide su quale interfaccia dover inoltrare un frame, basandosi sull'indirizzo MAC sorgente e destinazione del frame stesso. Alcuni switch presentano anche delle funzionalità di livello 3 (L3 di seguito), ovvero non si limitano all'inoltro di frame nella propria LAN ma anche all'interconnessione di più reti. Tale funzionalità verrà spiegata più nel dettaglio nel capitolo 2, facendo riferimento ad un caso pratico.

Figura 1.2: switch Huawei della serie S5700.

- Router (*figura 1.3*): è un dispositivo di rete che svolge funzioni L3 nel modello di architettura di rete OSI. Viene utilizzato per l'interconnessione di reti e dunque il suo compito è quello di inoltrare PDU, chiamate "pacchetti". È costituito da un certo numero di interfacce di cui alcune sono L2 (le porte ethernet contrassegnate in blu nella *figura 1.3*) ed altre L3 (le porte gigabit ethernet contrassegnate in giallo nella *figura 1.3*). Osserviamo inoltre come nella parte superiore siano stati inseriti due moduli per aggiungere ulteriori interfacce L3 di tipo gigabit ethernet e per l'inserimento di porte seriali. Nel contesto WAN (Wide Area Network) il router viene utilizzato per veicolare il traffico verso global internet. Funge quindi

da instradatore e collega i computer di una rete con il resto del mondo. Al suo interno un router ha memorizzata una “routing table”, che contiene l’associazione tra un indirizzo di rete e l’interfaccia che rende possibile l’inoltro del pacchetto verso quella destinazione. L’inoltro avviene sulla base dell’indirizzo IP sorgente e destinazione del pacchetto. Il router inoltre offre anche altri tipi di funzionalità, oltre a quelli già citati di networking, in merito alla protezione delle informazioni da minacce esterne. Ad esempio, è possibile utilizzare un router come firewall per la protezione della rete, oppure possiamo configurare delle VPN (Virtual Private Network) che consentano un trasferimento dati sicuro e così via.

Figura 1.3: router Huawei della serie AR1220.

- Access point: dispositivo di rete che consente il collegamento di diverse apparecchiature (computer, telefoni, etc.) in modalità wireless e quindi senza l’uso di cavi. Esso permette l’accesso alla rete LAN a molti dispositivi contemporaneamente.
- Firewall: dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi. Costituisce dunque una barriera tra le reti interne di una azienda, sicure e controllate, e le reti esterne che possono essere affidabili o meno, come global internet. Il firewall può essere costituito da una componente hardware, software o entrambe.

Ovviamente questa è solo una panoramica delle tecnologie del networking dove ci si è soffermati in particolare su switch e router, poiché sono quei dispositivi che verranno utilizzati nel progetto pratico illustrato nel capitolo 2.

1.3 Riferimenti al corso Huawei

Huawei è un'importante azienda che si è affermata in tutto il mondo nel campo delle telecomunicazioni. Essa è produttrice di smartphone, personal computer, tablet, orologi e

apparati di rete (alcuni di essi sono stati illustrati nel paragrafo precedente). I suoi prodotti pervadono tutti i settori produttivi dell'economia. In questo contesto la Huawei ha creato un programma internazionale denominato "Huawei Accademy", dove vengono proposti ed erogati diversi corsi di certifica. La certifica non è nient'altro che un'attestazione che viene fornita direttamente da Huawei e che garantisce che il possessore dell'attestato abbia acquisito determinate conoscenze e competenze in un determinato ambito tecnologico. Queste vengono rilasciate tramite il superamento di un esame, la cui tipologia e complessità varia in base alla certifica da conseguire. Sul piano lavorativo, questi corsi sono molto ben visti, in quanto rilasciati direttamente dai colossi delle telecomunicazioni mondiali. La certifica da me conseguita è la HCIA Routing & Switching. Questa introduce le tecnologie indispensabili al funzionamento di ogni rete informatica di piccole e medie dimensioni, affrontando e approfondendo i protocolli di rete fondamentali da implementare sugli apparati Huawei (in particolare su router e switch). Nello specifico, nel mio corso è stato mostrato come realmente avviene lo scambio tra due nodi di una rete, quali siano i concetti teorici necessari alla comprensione e risoluzione di problemi di networking, come configurare gli apparati di rete, come migliorare le prestazioni di una rete e come ideare, progettare e configurare una topologia di rete enterprise. Personalmente, il mio giudizio su questo corso non può che essere positivo, visto che grazie ad esso sono riuscito a comprendere realmente il funzionamento di una rete di telecomunicazioni.

Figura 1.4: logo certificazione.

2 Descrizione topologia

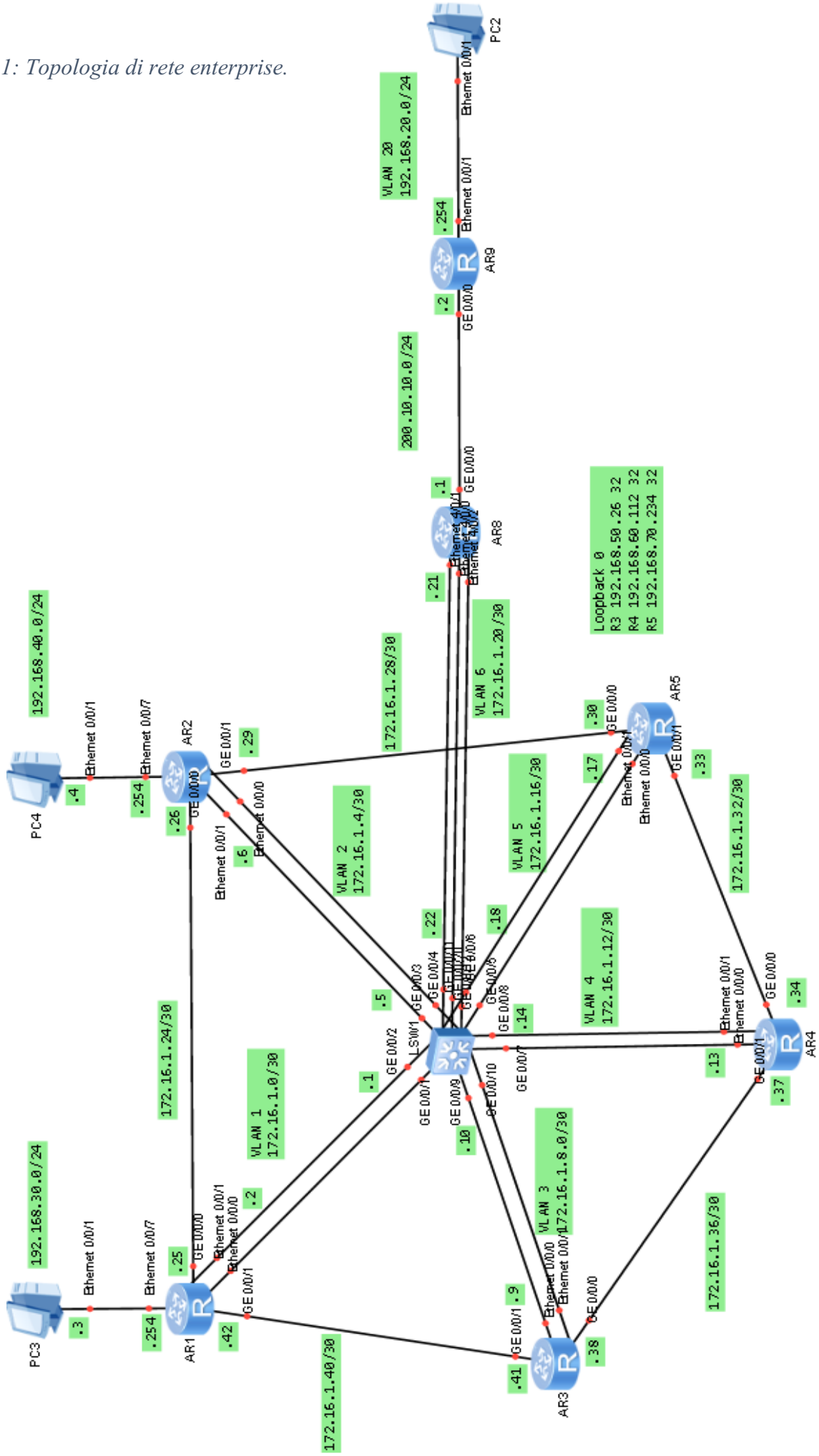
2.1 Introduzione alla topologia

L'introduzione precedentemente fatta risulta particolarmente utile per la comprensione di un lavoro complesso di configurazione degli apparati costituenti una comune topologia di rete. Tale topologia è stata realizzata utilizzando eNSP, un programma di simulazione delle reti, di proprietà di Huawei. La *figura 2.1* rappresenta a tutti gli effetti un esempio di topologia di rete aziendale. Essa risulta particolarmente utile per la comprensione degli argomenti teorici del networking e inoltre la configurazione degli apparati risulta essere un ottimo esercizio di applicazione della teoria.

Facendo riferimento alla *figura 2.1*, ogni router dell'anello (R1, R2, R3, R4, R5) potrebbe far capo ad uno specifico reparto dell'azienda. In particolare, sono state simulate due reti: la 192.168.30.0/24 e la 192.168.40.0/24. Inoltre, sono state configurate sui router R3, R4 ed R5 delle interfacce loopback per il testing, che simulano degli hosts appartenenti a reti differenti. Come si può ben notare è presente uno switch centrale che funge da router di centro stella. Essendo lo switch un dispositivo prettamente L2 sono state utilizzate le interfacce logiche VLANIF, alle quali è stato assegnato un indirizzo IP, in modo tale che lo switch possa supportare il traffico L3 (l'utilizzo delle VLAN per questa applicazione verrà approfondito nel paragrafo 2.2). Così, è proprio tale apparato che ha il compito di instradare il traffico delle varie reti verso le opportune destinazioni. I router sono stati così configurati in modo tale che il traffico utente venga sempre convogliato verso lo switch centrale mentre i collegamenti che formano l'anello esterno siano di backup. Il traffico utente verrà convogliato verso i collegamenti di ridondanza dell'anello solo in caso di rottura di uno dei collegamenti verso lo switch centrale. Questo è dunque un tipico esempio applicativo della topologia a stella, spesso menzionata durante lo studio delle telecomunicazioni. Notiamo inoltre come sia stato realizzato il "link aggregation" in tutti i collegamenti verso lo switch centrale e verso il router R8, che rappresenta il dispositivo di interfaccia con la rete esterna (i motivi per i quali sia conveniente fare link aggregation vengono riportati nel paragrafo 2.3). Su R8 è stato configurato un server NAT (Network Address Traslation) che permetta l'assegnazione di un indirizzo IP pubblico ad ogni indirizzo IP privato, appartenente alle reti 192.168.30.0/24 e 192.168.40.0/24, che debba comunicare con l'esterno. Dunque, tutto il

traffico delle due reti in uscita dalla topologia è “nattato” da R8 e può scambiare dati con la rete esterna (che è stata rappresentata con R9 e PC2). Per rete esterna si intende ad esempio un’altra rete aziendale ovunque dislocata raggiungibile mediante global internet o anche un’altra sede della stessa azienda. Infine, è stato configurato su R9 un server DHCP che assegni in maniera automatica l’indirizzo ip ai calcolatori della rete 192.168.20.0/24

Figura 2.1: Topologia di rete enterprise.



2.2 Topologia a stella

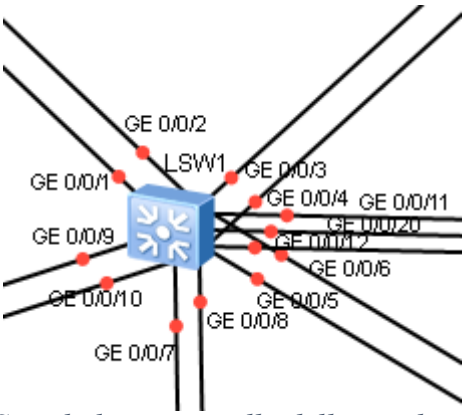


Figura 2.2: Switch di centro stella della topologia di figura 2.1.

Come già menzionato e come si evince facilmente dalla *figura 2.1* la rete è costituita da uno switch centrale che agisce come router di centro stella (*figura 2.2*). Questo vuol dire che tutto il traffico utente proveniente da una qualsiasi rete deve passare attraverso di esso per essere instradato verso la destinazione. Tale switch deve quindi necessariamente lavorare a L3 per poter inoltrare pacchetti provenienti da diverse reti. Dalla teoria sappiamo però che uno switch è di norma un dispositivo L2 utilizzato per inoltrare frame all'interno di una stessa LAN e non capace di fare routing (ricordiamo in tal senso che le porte dello switch sono delle porte L2). Come è possibile quindi far lavorare uno switch a L3? Una possibile soluzione potrebbe essere quella di cambiare lo stato delle interfacce L2 e farle diventare interfacce L3. Esiste un comando a tal fine che nei dispositivi Huawei permette di cambiare lo stato dell'interfaccia da "switch port" a "route port". Tale comando è *undo portswitch* e va applicato in interface view. Purtroppo, molti apparati Huawei non supportano questa funzionalità per cui è necessario ricorrere alle VLAN.

L'acronimo VLAN (Virtual Local Area Network) indica un insieme di tecnologie per la segmentazione del dominio di broadcast tipico di una LAN. Solitamente quest'ultima è composta da nodi utente e dagli switch, che permettono l'interconnessione di tali dispositivi. Il dominio di broadcast è unico e questo può generare dei problemi nel momento in cui il numero dei dispositivi diventi elevato. Le VLAN permettono così l'isolamento del traffico a livello data-link e consentono ad utenti fisicamente dispersi, tramite la suddivisione della LAN in diverse sottoreti, di essere parte di uno stesso dominio di broadcast. Tali sottoreti non potranno comunicare tra loro e quindi abbiamo in tal modo diminuito il traffico broadcast. La caratteristica essenziale di questa tecnica è che la segmentazione avviene a livello logico, ovvero la struttura fisica della rete non

viene alterata. Lo switch o il router identificano dunque la VLAN di appartenenza di un frame tramite l'analisi del campo "tag". Tale campo viene aggiunto al frame e contiene il relativo pvid. Analizziamo ora come quanto appena detto può tornare utile. Innanzitutto, osserviamo che le interfacce dei router che ospitano i collegamenti verso lo switch centrale e le interfacce dello switch sono tutte interfacce L2 (si fa sempre riferimento alla *figura 2.1*). Non potendo applicare il comando *undo portswitch* dobbiamo ricorrere alle VLAN. Il VLAN routing, quando si utilizza uno switch L3, si basa sull'implementazione di interfacce VLAN (chiamate VLANIF). Se più utenti in una rete appartengono a VLAN diverse, ogni VLAN richiede una VLANIF che funge da gateway per quella VLAN. Deve essere dunque associato un indirizzo IP a questa interfaccia che risieda nello spazio degli indirizzi associato ai nodi che appartengono a quella VLAN. In questo modo, associando ad ogni collegamento verso lo switch centrale una diversa VLAN, è abilitato il traffico L3 tra le diverse VLAN e conseguentemente tra tutte le reti della topologia (configurando le rotte tramite un opportuno protocollo di routing, argomento trattato nel paragrafo 2.6).

2.3 Link Aggregation

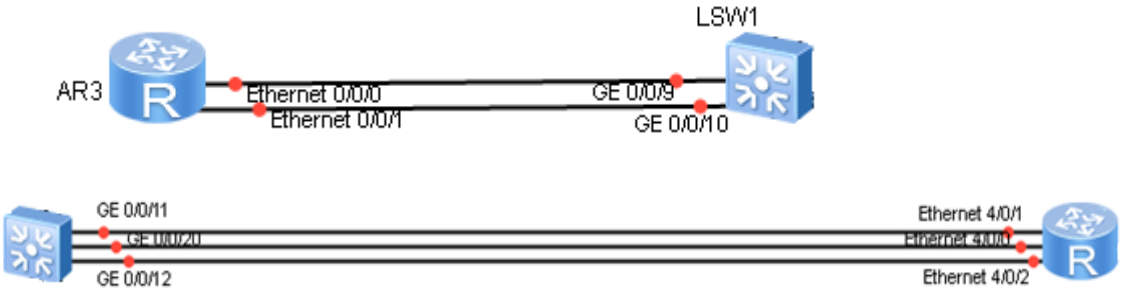


Figura 2.3: esempio di link aggregation estratto dalla topologia di figura 2.1.

Nella topologia di *figura 2.1* osserviamo come sia stata applicata la tecnica del link aggregation (LA) nei collegamenti verso lo switch centrale. Fisicamente, quindi, due apparati sono collegati da due o tre link fisici ma logicamente è come se ne avessimo uno unico, dove l'interfaccia logica prende il nome di ethernet trunk ("eth-trunk"). Ogni interfaccia logica può essere costituita da un massimo di otto interfacce fisiche.

Questa tecnica viene utilizzata principalmente per aumentare la banda di un collegamento che risulta essere la somma delle bandwidth dei vari link che formano l'interfaccia logica. Facendo riferimento alla *figura 2.3*, osserviamo che la trasmissione tra gli apparati avviene rispettivamente a 200 Mbit/s e 300 Mbit/s contro i 100 Mbit/s

nominali che si avrebbero utilizzando un unico link fisico. Parliamo di Mbit e non di Gbit poiché, per effetto dell'autonegoziazione tra gli apparati, questi impostano i parametri minimi di comunicazione garantiti. Essendo un link connesso tra delle interfacce ethernet e gigabit ethernet la velocità di trasmissione garantita sarà quella tipica delle interfacce ethernet, ovvero 100 Mbit/s per un singolo link fisico. È importante ricordare come non sia possibile creare una interfaccia logica con link fisici di tipo diverso. Ad esempio, non è possibile creare un eth-trunk unendo una interfaccia ethernet con una gigabit ethernet. Alcuni apparati, in fase di configurazione, restituiscono un messaggio di errore se si tenta di fare quanto appena detto mentre altri invece lo lasciano fare. Risulta però in quest'ultimo caso un pesante degrado delle prestazioni in termini di invio e ricezione dei dati. Esistono due modalità di configurazione del link aggregation. Nella modalità "manual mode load balance" il carico di lavoro viene bilanciato tra i link che fanno parte dell'interfaccia logica. In tal modo se i link fisici sono tre, il traffico verrà suddiviso (secondo precisi criteri di inoltro) in tutti e tre i link. Nella seconda modalità, la "LACP static", alcuni link fisici dell'interfaccia logica vengono tenuti di backup. I link attivi e quelli inattivi vengono decisi sulla base di determinati criteri di priorità (che l'utente può configurare) dal protocollo LACP (Link Aggregation Control Protocol).

La tecnica del link aggregation può essere utilizzata in molti scenari. Ad esempio, questa tecnica è una valida alternativa all'utilizzo della fibra, qualora gli apparati a disposizione non la supportino. Nel nostro caso, il suo utilizzo ci consente comunque di aumentare la velocità dei link verso lo switch centrale diminuendo quindi le probabilità di congestione degli stessi, tenendo conto che tali collegamenti sono soggetti a continuo traffico utente. Stiamo quindi aumentando l'affidabilità del sistema. Inoltre, osserviamo dalla *figura 2.1* come nel collegamento tra lo switch e il router R8 sia stato fatto link aggregation con tre link fisici. Tale link logico riveste una particolare importanza poiché tutto il traffico verso l'esterno della rete deve transitare attraverso di esso. È quindi una scelta saggia quella di aver aumentato di ulteriori 100 Mbit/s la banda di tale link.

2.4 Anello di ridondanza

Nella topologia di *figura 2.1* osserviamo la presenza di collegamenti diretti tra i vari router dell'anello. Abbiamo però già ribadito come il traffico utente debba solo transitare nei link verso lo switch centrale e non sui collegamenti esterni. Questo perché tali link sono

di backup e devono essere utilizzati solo nel momento in cui cada uno dei collegamenti verso lo switch centrale. In tal modo viene implementato un anello di ridondanza: la presenza di questi link gigabit ethernet fa sì che la rete sia più robusta ad eventuali outage dei link principali. Questa è una tecnica implementativa molto utile ed essenziale in quegli ambienti dove l'affidabilità della rete debba essere sempre garantita. La ridondanza e l'affidabilità hanno tuttavia un costo che deve essere valutato tenendo conto non solo del numero e della tipologia di apparati che vengono aggiunti, ma anche della complessità nella loro configurazione e manutenzione. In conclusione, l'inserimento in una rete di link di backup dipende da molteplici fattori, come ad esempio il budget che si ha a disposizione, la necessità o meno dell'affidabilità della topologia e così via.

2.5 Network Address Traslation

Il NAT consente ad uno o più hosts che non hanno un indirizzo IP registrato e globalmente unico di comunicare con altri hosts attraverso la rete internet. Per comprendere a fondo il significato del NAT è necessario però fare una piccola digressione sugli indirizzi IPv4 e sulle problematiche emerse nel corso degli anni.

IPv4, acronimo di Internet Protocol version 4, è un protocollo L3 utilizzato per l'inoltro di pacchetti lungo la rete internet. L'inoltro avviene sulla base di un indirizzo IP, che è un numero costituito da 32 bit. Alla luce di questo qualsiasi dispositivo debba essere connesso alla rete internet necessita di un indirizzo IP per poter essere riconosciuto in maniera univoca nella rete. IPv4 è nato nel 1980, in un periodo in cui i dispositivi connessi alla rete internet erano veramente pochi. Gli anni '90 hanno visto l'affermazione del computer, inizialmente solo per uso domestico e poi anche come "oggetto connesso in rete". Ciò ha aumentato in maniera esponenziale la richiesta di indirizzi IP. Parallelamente a questo si stava sviluppando anche la telefonia mobile che ha determinato un notevole aumento nel numero di dispositivi connessi in rete e quindi bisognosi di un indirizzo IP. Dunque, questi indirizzi, che erano stati elargiti con una certa leggerezza nei primi anni, incominciarono a scarseggiare rendendo necessario l'utilizzo di tecniche per il "risparmio" di indirizzi. In primo luogo, è stata adottata una suddivisione degli IP in due classi: indirizzi pubblici e privati. Gli indirizzi pubblici sono unici a livello globale mentre gli indirizzi privati sono utilizzabili sono all'interno delle LAN e non in global internet. In tal modo si diminuisce di molto lo spreco di indirizzi IPv4 ma sorge un

problema: essendo assegnato un indirizzo IP privato ad un dispositivo in una LAN, quest'ultimo non può scambiare dati tramite global internet dato che il suo indirizzo non è globalmente unico. Questa problematica viene risolta tramite l'inserimento di un router con funzione di NAT.

Il NAT consente l'associazione tra un indirizzo IP pubblico ed uno privato. In particolare, tale server deve essere un dispositivo L3, come un router, poiché deve manipolare l'indirizzo IP sorgente dei pacchetti che dalla LAN sono diretti alla WAN e deve modificare l'indirizzo IP destinatario di ogni pacchetto che dalla WAN è diretto alla LAN. In tal modo ogni dispositivo della LAN che ha necessità di scambiare dati con il mondo esterno viene mappato con un indirizzo pubblico con il quale sarà in grado di navigare in global internet in maniera univoca. Esistono quattro scelte implementative di NAT:

- Statico: ogni indirizzo privato viene direttamente mappato con un indirizzo pubblico. In termini di risparmio di indirizzi questo non è un metodo preferibile.
- Dinamico: il router ha un gruppo di indirizzi pubblici da assegnare. Può succedere che alcuni utenti non possano navigare in internet poiché tutti gli indirizzi del pool sono stati già assegnati.
- NAPT (Network Address Port Traslation): il router ha un gruppo di indirizzi pubblici da assegnare. Viene associato a diversi indirizzi privati lo stesso indirizzo pubblico dove la differenziazione dei client viene fatta mediante la porta relativa al servizio del quale vogliono usufruire. Tale tecnica è adatta per reti di medie-grandi dimensioni come reti aziendali.
- Easy IP: è un caso particolare del NAPT. In questo caso il traffico dati verso global internet viene mappato tramite un unico indirizzo IP pubblico. Tale indirizzo è quello che viene negoziato con l'ISP. Dunque, un solo indirizzo pubblico per tutti i dispositivi della LAN dove la differenziazione degli hosts avviene sempre mediante le porte. Tale tecnica è adatta alle reti domestiche.

Per quanto concerne la nostra topologia di *figura 2.1* osserviamo come R8 sia un server NAT che permette la comunicazione delle varie reti dell'anello con la rete esterna. A titolo informativo, è giusto menzionare il protocollo IPv6, che rappresenterebbe la vera soluzione all'esaurimento degli indirizzi IPv4 in quanto tale indirizzo è costituito da 128 bit e quindi mette a disposizione un numero spropositato di indirizzi.

2.6 Protocolli di routing

Ripercorriamo innanzitutto quelli che sono i concetti fondamentali del routing. Per inviare pacchetti in rete un calcolatore deve fare tutta una serie di check preliminari. In primo luogo, verifica l'esistenza di un path logico, ovvero verifica se l'indirizzo IP del mittente e del destinatario siano entrambi appartenenti allo stesso spazio degli indirizzi (se così non fosse ricorre al default gateway se configurato), e poi verifica l'esistenza di un path fisico, ovvero si ricerca l'indirizzo MAC di destinazione da inserire nel frame (se non è presente nella ARP cache viene eseguita una ARP request). Se l'indirizzo del destinatario non appartiene allo stesso spazio di indirizzi del mittente, è necessario utilizzare un router per "instradare" i pacchetti. Il router è quindi un dispositivo che decide il percorso che un pacchetto può fare in maniera ottimizzata sulla base, ad esempio, della velocità dei link, del numero di "salti" da fare e via dicendo. La decisione su gran parte dei router viene presa sulla base del cosiddetto "longest match", ovvero il router confronta bit a bit l'indirizzo destinatario del pacchetto con tutti gli indirizzi che sono presenti nella sua tabella di routing. Il pacchetto verrà poi inoltrato sull'interfaccia associata all'indirizzo con il quale si è avuto il longest match. Alla stregua di quanto detto la tabella di routing può essere popolata utilizzando due tecniche. La configurazione manuale delle rotte statiche, che richiede l'intervento dell'amministratore di rete, rende la rete poco dinamica e poco adatta ad eventuali cambiamenti. Una alternativa è quella di utilizzare un protocollo di routing che riesca a popolare autonomamente la tabella di routing, inserendo una entry per ogni spazio di indirizzi noto o appreso da altri dispositivi L3. Ovviamente il secondo metodo è quello preferibile, non solo per grandi reti ma anche per quelle di modeste dimensioni. L'utilizzo di un protocollo di routing rende la rete fortemente dinamica e adatta a cambiamenti topologici in quanto è il protocollo che si occupa di eliminare eventuali rotte obsolete e di ricrearne delle nuove. Il tutto è totalmente trasparente all'utente.

Nella topologia di *figura 2.1* è stato utilizzato un protocollo di routing per l'inoltro di pacchetti del tipo link-state, quale è OSPF (Open Shortest Path First). Il funzionamento dei protocolli link-state può essere suddiviso in tre sezioni: network discovery (conoscenza dei dispositivi vicini e delle informazioni che propagano), topology database exchange (informazioni sugli spazi di indirizzi gestiti e condivisione con gli atri router) e route computation (scelta dello shortest path). Questo algoritmo determina la scelta del

percorso migliore verso tutte le destinazioni possibili. Tale protocollo si comporta in maniera differente in base al tipo di rete sul quale va applicato (broadcast, point to point, NBMA, point to multipoint, etc.). Nel caso di nostro interesse tratteremo il suo funzionamento solo per reti di tipo broadcast. Nel momento in cui viene avviato un processo OSPF su un router questo incomincia a trasmettere o inviare degli hello packets ogni dieci secondi e si mette in ascolto sugli indirizzi multicast 224.0.0.5 e 224.0.0.6, che riguardano esclusivamente i processi OSPF. Tramite questi hello packets il router ricostruisce il numero ed il tipo di router ai quali è collegato ed acquisisce una serie di informazioni, tra cui la priorità, utili per l'elezione di DR e BDR. Per l'elezione viene usato il parametro di priorità e se questo dovesse essere uguale per tutti i router verrebbe eletto DR quello che ha il router-id più altro. Capire se un router è BDR e DR o è un DRother è fondamentale per capire che tipo di relazione deve essere stabilita con gli altri router. Se sono BDR o DR viene stabilita una relazione di adiacenza, dove avviene lo scambio e la condivisione di tutte le informazioni topologiche contenute nel link state database (LSDB). Con i router di tipo DRother verrà stabilita una semplice relazione di vicinanza, dove non vengono scambiate informazioni topologiche, tramite le link state advertisement (LSA), ma solo le informazioni di controllo. Questo rende il processo di scambio di informazioni più snello e più mirato poiché, se dovessimo scambiare con ogni router tutte le informazioni contenute nell'LSDB, sarebbe necessaria una grande quantità di tempo. Le informazioni vengono scambiate in continuazione, anche dopo che il processo di scambio dati tra router è in fase "full", tramite delle link state request (LSR) e delle link state update (LSU). Le informazioni scambiate sono molte ma rivestono molta importanza quelle riguardanti il costo dei link. Sulla base di un bandwidth reference ogni router calcola il costo di ogni sua interfaccia e lo trasmette ai router adiacenti, così che questi ultimi possano calcolare il miglior percorso verso una destinazione.

3 Implementazione della configurazione

3.1 Introduzione alla configurazione

Iniziamo ora un capitolo riguardante la configurazione degli apparati di rete. Ripercorreremo passo passo tutti gli step che si sono susseguiti per il raggiungimento del completo funzionamento della topologia di *figura 2.1*, sulla base delle specifiche di progetto. La configurazione dei dispositivi è stata fatta utilizzando un simulatore di reti quale eNSP, che mette a disposizione una ottima interfaccia grafica molto simile a quella presente nei dispositivi reali. Tramite questa GUI Huawei offre un laboratorio virtuale con tutti gli strumenti di routing e switching per la pianificazione, simulazione, progettazione e verifica di reti ICT (Information and Communication Technologies) aziendali. Fatta questa premessa, vediamo come è stato sviluppato il progetto fin dalle sue basi.

Fondamentale nella progettazione di una rete ICT è la chiarezza delle specifiche. Dobbiamo avere ben chiaro cosa dobbiamo realizzare e, sulla base di questo, provare a capire come realizzarlo (numero e tipo di apparati, numero e tipo di collegamenti, rete ridondata, presenza di apparati di backup e così via). Una volta che abbiamo strutturato la topologia dobbiamo stilare una serie di passi da seguire per il raggiungimento delle specifiche di progetto, per poi passare alla configurazione degli apparati. Durante la configurazione degli apparati è fortemente consigliato farsi degli schemi per tenere traccia, ad esempio, degli indirizzi assegnati, dei dispositivi e collegamenti di backup, degli apparati che fungono da server per determinate funzioni e via dicendo. Redigere un documento di questo tipo può risultare utile soprattutto a distanza di mesi o anni dalla messa in opera del sistema, quando si potrebbero presentare dei problemi e, complice il tempo trascorso, non ci si ricordi granché della configurazione. Tale approccio consente quindi di abbattere anche drasticamente i tempi di troubleshooting.

3.2 Assegnazione degli indirizzi IP

Il primo passo è stato la decisione degli spazi degli indirizzi da utilizzare. Ogni router rappresenta l'interfaccia tra una rete privata (come, ad esempio, un reparto di un'azienda) e l'anello. Per tali reti sono stati scelti gli spazi di indirizzi privati 192.168.X.X/24. In particolare:

R1 → 192.168.30.0/24

192.168.30.3/24 (indirizzo IP di PC3, connesso all'interfaccia ethernet 0/0/7 del router)

R2 → 192.168.40.0/24

192.168.40.4/24 (indirizzo IP di PC4, connesso all'interfaccia ethernet 0/0/7 del router)

R3 → 192.168.50.26/32 (interfaccia loopback 0 del router)

R4 → 192.168.60.112/32 (interfaccia loopback 0 del router)

R5 → 192.168.70.234/32 (interfaccia loopback 0 del router)

Osserviamo come sui router R3, R4 ed R5 non siano presenti delle vere e proprie reti ma siano state configurate delle interfacce logiche a scopo esemplificativo, mentre sui router R1 ed R2 sono stati posti due hosts di esempio. I collegamenti all'interno dell'anello sono invece caratterizzati dallo spazio di indirizzi privati 172.16.1.X/30. È stata scelta una subnet mask così piccola per minimizzare lo spreco di indirizzi, poiché ogni collegamento tra router-router e router-switch costituisce una rete a sé e quindi necessita di due soli indirizzi IP (con una subnet mask 255.255.255.252, ovvero una /30, abbiamo a disposizione quattro indirizzi di cui uno per l'indirizzo di rete, uno per l'indirizzo di broadcast e due per l'assegnazione). Vengono mostrati ora alcuni screenshot riguardanti la configurazione di un indirizzo IP su un host e su un apparato di rete.

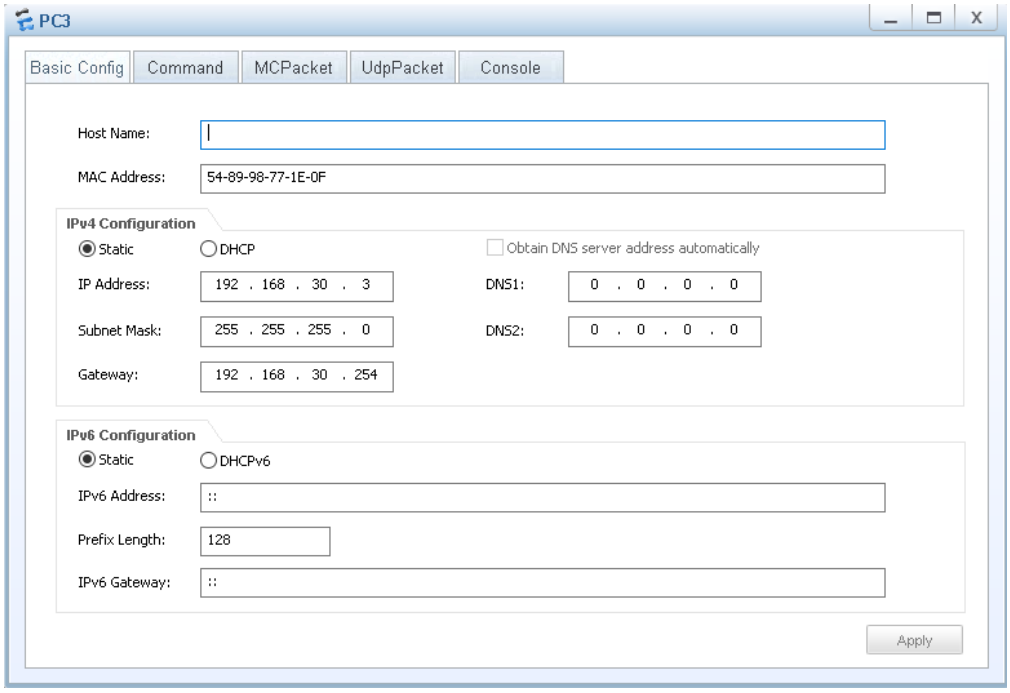


Figura 3.1: Configurazione indirizzo IP e gataway su PC3.

```
interface GigabitEthernet0/0/0
 ip address 172.16.1.25 255.255.255.252
```

Figura 3.2: Configurazione indirizzo IP sull'interfaccia GigabitEthernet0/0/0 del router R1.

Osserviamo come, nella *figura 3.1*, sia stata selezionata l'opzione "static" per l'inserimento manuale di un indirizzo IP e come sia anche presente un indirizzo di gateway per rendere possibile lo scambio di pacchetti verso nodi che sono al di fuori dello spazio di indirizzi della LAN. Qualora l'indirizzo IP sia fornito all'host tramite un DHCP server è sufficiente selezionare l'opzione "DHCP" (trattato nel paragrafo 3.8). È sempre opportuno verificare che l'host e l'apparato di rete abbiano preso correttamente l'indirizzo IP rispettivamente tramite il comando *ipconfig* dal prompt dei comandi (*figura 3.3*) e tramite il comando *display ip interface brief* da console (*figura 3.4*).

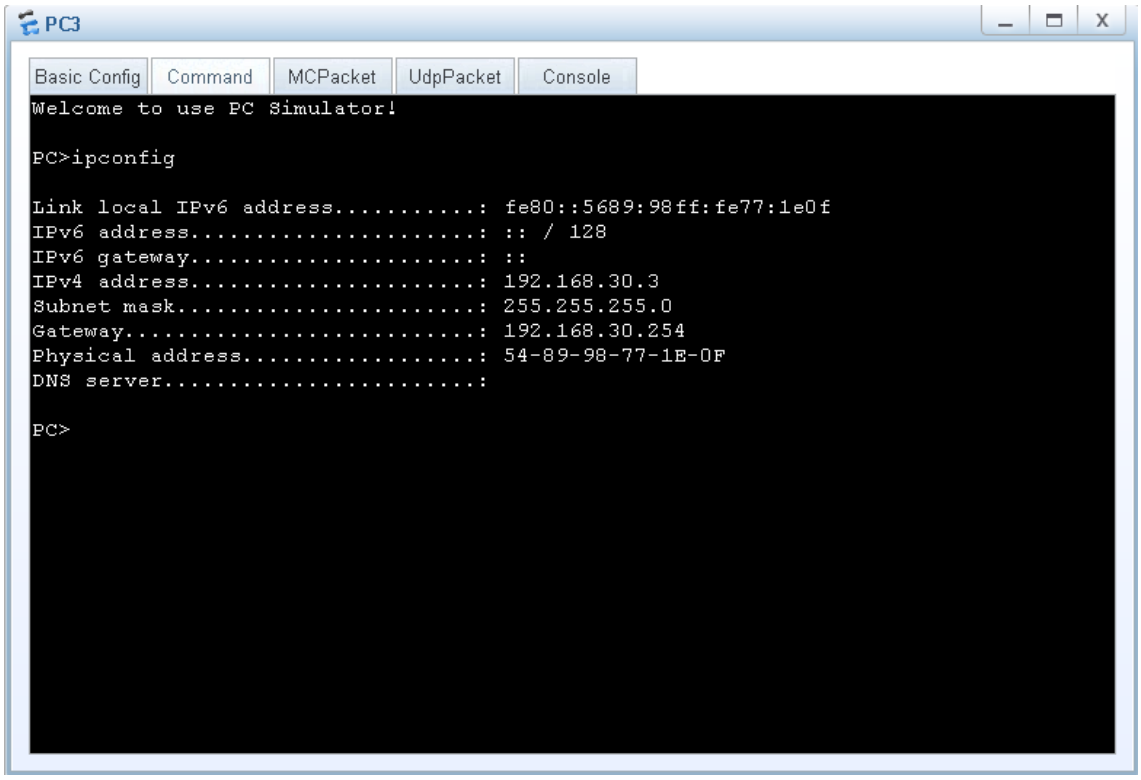


Figura 3.3: risultato del comando ipconfig dal prompt dei comandi di PC3.

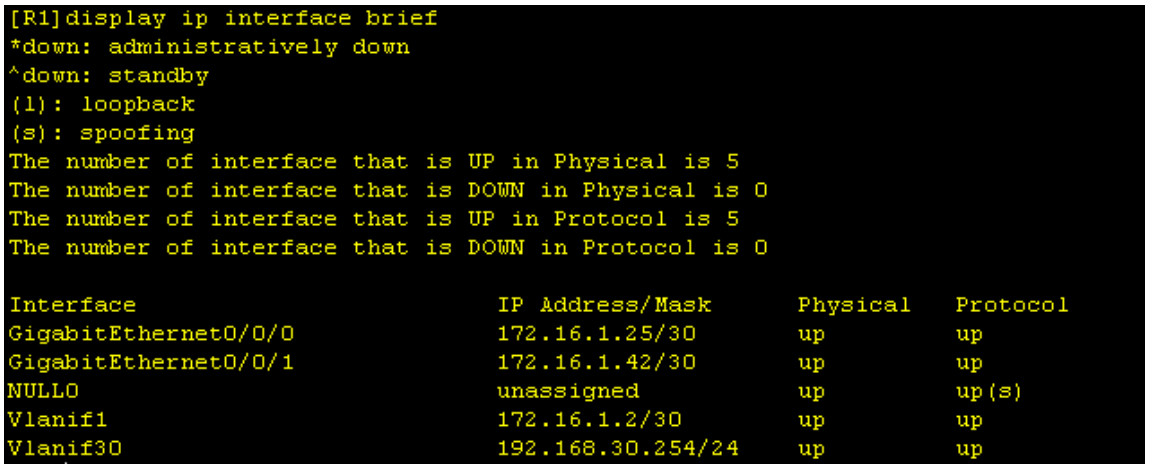


Figura 3.4: risultato del comando display ip interface brief sul router R1.

Per quanto concerne la configurazione sui router, riportata in *figura 3.2*, osserviamo che essa è stata fatta in interface view e che la configurazione delle interfacce L2 (tutte le porte ethernet dei router e le porte gigabit degli switch) è stata possibile tramite l'utilizzo delle VLAN, trattate nel paragrafo 3.4. Fatta questa doverosa introduzione, entriamo nel vivo della configurazione degli apparati.

3.3 Configurazione dei link aggregation

Partiamo dalle specifiche: viene richiesto che sia applicato il link aggregation su tutti i collegamenti verso lo switch centrale. Vengono riportati in *figura 3.5* i comandi da utilizzare:

```
[R1]int Eth-Trunk 1
[R1-Eth-Trunk1]mode manual load-balance
[R1-Eth-Trunk1]trunkport ethernet0/0/0
Info: This operation may take a few seconds. Please wait for a moment...done.
[R1-Eth-Trunk1]trunkport ethernet0/0/1
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Figura 3.5: configurazione link aggregation su R1.

Analizziamo la figura. La prima operazione eseguita è la creazione dell'interfaccia logica denominata "Eth-Trunk 1". Fatto questo è stato definito il tipo di link aggregation, in particolare è stata scelta la modalità "manual load-balance". Questa scelta è scaturita dal fatto che il link verso lo switch centrale è un collegamento presumibilmente molto trafficato, in quanto il traffico utente deve transitare proprio tramite esso per arrivare allo switch di centro stella. Scegliendo tale modalità quindi si è scelto di aumentare la bandwidth fino a 200 Mbit/s avendo il traffico bilanciato su entrambi i link fisici dell'interfaccia logica. Scegliendo la modalità "static LACP" uno dei due link fisici

sarebbe di backup e dunque la bandwidth sarebbe di 100 Mbit/s. Lo stesso ragionamento va applicato al link aggregation dallo switch centrale a R8. Tale collegamento rappresenta l'interfaccia della rete ad anello con la rete esterna e per cui è lecito pensare che ci possa essere un elevato traffico, visto che aggrega i dati provenienti da tutte le reti dell'anello. In tal modo può essere raggiunta una velocità massima di 300 Mbit/s. È giusto far presente, comunque, che la modalità "manual load-balance" è di default nei dispositivi Huawei e dunque il comando di per sé non sarebbe necessario, ma è stato riportato per una maggiore chiarezza. La configurazione si conclude con l'inserimento nell'interfaccia logica delle interfacce fisiche ethernet0/0/0 e ethernet0/0/1 mediante l'utilizzo del comando *trunkport*. Ricordiamo comunque che il link aggregation è una proprietà di interfaccia e dunque le interfacce fisiche facenti parte dell'ethernet trunk sono visibili solo tramite il comando *display current-configuration* (*figura 3.6*) o *display this* all'interno dell'interfaccia fisica (*figura 3.7*) ma non tramite il comando *display this* all'interno dell'interfaccia logica (*figura 3.8*).

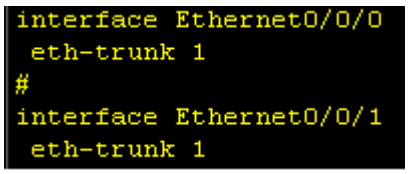


Figura 3.6: estratto del risultato del comando display current-configuration su R1.

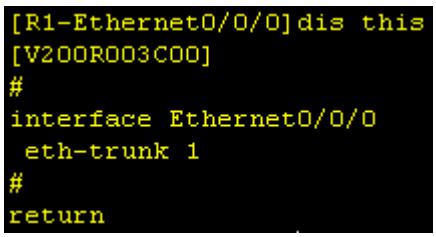


Figura 3.7: risultato del comando display this sull'interfaccia ethernet0/0/0 di R1.

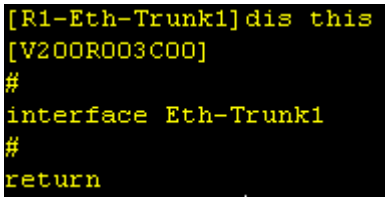


Figura 3.8: risultato del comando display this sull'interfaccia eth-trunk 1 di R1.

Per eliminare una interfaccia fisica dall'ethernet trunk dobbiamo entrare in interface view ed applicare il comando *undo eth-trunk 1*. Quello che abbiamo riportato è la sola configurazione per il router R1. Tale configurazione va ripetuta in maniera analoga per tutti gli altri dispositivi interessati dal link aggregation.

3.4 Configurazione delle VLAN

Come abbiamo già spiegato in precedenza, le VLAN rappresentano una buona soluzione per permettere l'assegnazione di un indirizzo IP alle interfacce L2 di router e switch. La configurazione del router R1 è illustrata nella *figura 3.9* e nella *figura 3.10*:

```
vlan batch 30
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 30
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
```

Figura 3.9: creazione delle vlan e assegnazione del tipo di porta sul router R1.

```
interface Vlanif1
 ip address 172.16.1.2 255.255.255.252
 ospf network-type p2p
#
interface Vlanif30
 ip address 192.168.30.254 255.255.255.0
 ospf network-type p2p
```

Figura 3.10: assegnazione degli indirizzi IP alle interfacce logiche vlanif del router R1.

Analizziamo nel dettaglio questi due screenshot. Nella *figura 3.9* osserviamo che è stata creata la "vlan 30". La "vlan 1" è esistente di default nei dispositivi Huawei e per cui non è necessario crearla. Attraverso il comando *port link-type* è stata configurata la tipologia dell'interfaccia: trunk o access. L'interfaccia ethernet0/0/7 è di tipo access, che è la tipologia di porta tipica per i collegamenti verso i nodi finali. Tale tipologia di porta tagga i frame in uscita dall'host con pvid 30 (port vlan id 30) mentre stagga i frame in uscita dal router, ovviamente solo se il pvid di tale frame corrisponde con il pvid della porta. In caso contrario scarta il frame. L'interfaccia eth-trunk1 è invece di tipo trunk. Attenzione a non confondersi: "eth-trunk1" è il nome dell'interfaccia logica relativa al link aggregation mentre "trunk" è il tipo di interfaccia relativa all'applicazione delle VLAN.

Questo tipo di porta è comunemente utilizzata nei collegamenti tra i dispositivi di rete. Tale porta inoltra i frame conservandone il tag, a meno che non appartengano alla VLAN definita "nativa" per quella particolare interfaccia. Nella *figura 3.10* sono stati invece assegnati gli indirizzi IP alle interfacce logiche, denominate VLANIF, relative alle VLAN 1 e 30 (due VLAN, due interfacce VLANIF). L'utilizzo delle VLAN permette l'assegnazione dell'indirizzo IP utilizzando il solito comando *ip address*. Per fare in modo che questa configurazione funzioni bisogna assegnare ad ogni link aggregation una VLAN differente tramite la procedura appena mostrata. Per i link aggregation sono state scelte le VLAN dalla 1 alla 6 mentre per i collegamenti verso le reti di PC3 e PC4 sono state scelte le VLAN 30 e 40, tenuto presente che avremmo comunque potuto utilizzare per tali reti una delle VLAN già utilizzate per il link aggregation.

3.5 Configurazione del routing

Abbiamo fin ora configurato gli aspetti legati a link aggregation e VLAN, assegnando così un indirizzo IP a tutte le interfacce dei dispositivi della topologia. È necessario a questo punto configurare un protocollo di routing che permetta lo scambio dati in tutta la topologia sfruttando il protocollo IP. Oltre che ad essere molto svantaggioso per motivi già citati, è impensabile scrivere tutte le rotte in maniera statica e si fa ricorso quindi ad un protocollo di routing quale OSPF. Vediamo ora nella *figura 3.11* la configurazione che è stata adottata:

```
ospf 1 router-id 2.2.2.2
 silent-interface Ethernet0/0/7
 silent-interface Vlanif30
 area 0.0.0.0
  network 172.16.1.2 0.0.0.0
  network 172.16.1.25 0.0.0.0
  network 172.16.1.42 0.0.0.0
  network 192.168.30.254 0.0.0.0
```

Figura 3.11: configurazione di ospf sul router R1.

Abbiamo creato il processo "ospf 1". Possono coesistere in una topologia più processi OSPF ma nel nostro caso abbiamo bisogno di uno solo. Fatto questo dobbiamo assegnare il router-id al nostro dispositivo. Il router-id è espresso nella forma X.X.X.X ma ha solo le sembianze di un indirizzo IP poiché in verità è un'etichetta. Questo può essere assegnato in modalità manuale (dall'amministratore di rete) oppure in modalità automatica dal router. Se si sceglie quest'ultima modalità il router sceglie come router-id

l'indirizzo IP più grande assegnato ad una delle sue interfacce attive. Questa scelta non è la migliore, poiché se tale interfaccia per qualche motivo cessasse di funzionare, automaticamente non funzionerebbe più il processo OSPF poiché sprovvisto di un router-id. Una buona soluzione, nel caso sempre di assegnazione automatica, può essere quella di far assegnare come router-id l'indirizzo IP di un'interfaccia logica (loopback) che è molto più robusta di un'interfaccia fisica (smette di essere funzionante solo quando è l'amministratore di rete a spegnerla). Nel caso in esame il router-id è stato assegnato in modo manuale, come risulta dalla *figura 3.11*. Il router-id viene utilizzato per identificare il router nel processo OSPF relativo e soprattutto per eleggere il DR e il BDR. In tale topologia però non ci sono collegamenti di più di due router. Lo switch centrale della topologia non deve trarre in inganno: esso è un dispositivo che lavora a L3 e, grazie alle VLAN, ogni link rappresenta una rete a sé. Alla luce di questo non è necessaria l'elezione di DR e BDR poiché i collegamenti sono P2P (Peer to Peer) anche se il tipo di collegamento nella realtà è di tipo broadcast (ethernet). Evitare di eleggere i designated router comporta un non indifferente risparmio di tempo e risorse e per cui su ogni porta dei dispostivi interessati è stato applicato il comando *ospf network-type p2p* come illustrato nella precedente *figura 3.10*. Proseguendo con la configurazione dobbiamo ora inserire l'area del nostro processo. Le aree in OSPF servono per segmentare la rete ed evitare che i link state database e, quindi, le tabelle di routing siano troppo grandi. Una situazione di questo tipo potrebbe comportare un allungamento dei tempi di inoltro dei pacchetti (ci vuole tempo per fare il matching tra tutti gli indirizzi IP e l'IP del pacchetto da inoltrare) e di scambio delle link state update. Sulla base di ciò si può optare per suddividere la rete in più aree dove queste ultime debbano essere sempre confinanti con l'area 0 e l'inoltro di dati tra le aree è permesso dall'area border router (ABR). Nel nostro caso si è scelto di configurare una sola area vista la buona efficienza della rete e visto che si tratta comunque di una simulazione e dunque le tabelle di routing non sono poi così grandi. Il comando *network* infine consente di comunicare ad OSPF quali sono le interfacce che "partecipano" al processo OSPF e che devono quindi essere dichiarate come raggiungibili via IP. La configurazione prevede che siano usate le wildcard mask: in tale maschera un uno binario ha il significato di ignorare il corrispondente bit dell'indirizzo IP mentre uno zero binario significa che il corrispondente bit dell'indirizzo IP deve essere preso in considerazione. Nell'esempio riportato tutte le wildcard mask

sono composte da trentadue zeri binari e quindi gli indirizzi riportati sono proprio gli indirizzi delle interfacce che devono far parte del processo OSPF. Nella fattispecie avremmo potuto sintetizzare i primi tre comandi

network 172.16.1.2 0.0.0.0

network 172.16.1.25 0.0.0.0

network 172.16.1.42 0.0.0.0

con il comando:

network 172.16.1.0 0.0.0.255

La wildcard mask in questo caso ci dice che i bit interessati sono i primi tre ottetti dell'indirizzo IP. Quindi con quest'ultimo comando stiamo dicendo che tutte le interfacce con IP 172.16.1.x fanno parte del processo OSPF. Se è vero che risparmiamo righe di configurazione è anche vero che in questo modo siamo tratti più facilmente in errore. È quindi preferibile il primo metodo illustrato, ovvero quello utilizzato nella *figura 3.11*. È stato infine applicato il comando *silent-interface* alle interfacce non interessate dagli hello packets, ovvero quelle verso gli end users. La configurazione è completa: le tabelle di routing sono popolate e siamo quindi in grado di inoltrare pacchetti IP all'interno della nostra rete. Da specifiche però lo switch centrale deve fungere da router di centro stella. La tecnica e la logica utilizzati per risolvere questo problema meritano menzione nel seguente paragrafo dedicato.

3.6 Configurazione router di centro stella ed anello di ridondanza

Allo stato attuale, il traffico utente può essere inoltrato su ogni collegamento della topologia e la differenziazione del percorso verso una destinazione avviene tramite il costo del link. Nel paragrafo 2.6 abbiamo già menzionato come ogni dispositivo possa calcolare il costo di una interfaccia tramite una semplice divisione tra la bandwidth reference e la velocità nominale dell'interfaccia stessa. Per i dispositivi da noi utilizzati, nel caso di esame di una interfaccia di tipo gigabit ethernet, il costo di tale porta risulta essere pari a uno poiché i dispositivi di default utilizzano una bandwidth reference di 1 Gbit/s. Modificando proprio tale proprietà di costo di un'interfaccia possiamo far sì che i router vedano i collegamenti che formano l'anello come delle vie "non convenienti" per inoltrare del traffico. In questo modo il traffico verrà convogliato dal router verso lo

switch centrale. Per quanto concerne la configurazione è stato scelto di assegnare un costo pari a duecento alle interfacce dei collegamenti dell'anello, come mostrato in *figura 3.12*:

```
interface GigabitEthernet0/0/0
 ip address 172.16.1.25 255.255.255.252
 ospf cost 200
 ospf network-type p2p
#
interface GigabitEthernet0/0/1
 ip address 172.16.1.42 255.255.255.252
 ospf cost 200
 ospf network-type p2p
```

Figura 3.12: assegnazione del costo alle interfacce dei link dell'anello sul router R1.

Sulla tabella di routing verranno così mostrate delle rotte che avranno costo 202 e altre che avranno costo 2, che saranno ovviamente quelle preferibili dal router (alcune tabelle di routing sono riportate nel paragrafo 4.2). Abbiamo così implementato anche l'anello di ridondanza. Vedremo meglio nel capitolo quattro la verifica di quanto appena esposto, mostrando come il traffico utente sia sempre convogliato verso lo switch centrale a meno di un outage di un link.

La configurazione effettuata fin ora non è sufficiente per ottenere il funzionamento dell'intera topologia. Sulle interfacce fisiche L2 dello switch e dei router, anche se sono state configurate delle interfacce logiche L3, è attivo il protocollo STP (Spanning Tree Protocol). Tale protocollo mitiga gli effetti dei loop a L2, come ad esempio il broadcast storm (essendoci dei loop i frame broadcast vengono inoltrati in continuazione e ovunque) e mac instability (le tabelle mac nei dispositivi vengono in continuazione aggiornate erroneamente e non sono dunque affidabili). STP viene a vanificare gli sforzi fatti nella creazione di link ridondanti tra lo switch centrale ed i router dell'anello. Ci si può rendere facilmente conto di questa situazione tramite il comando *display stp brief* che riporta lo stato delle interfacce (*figura 3.13*). È facile vedere come molte delle porte siano messe in "discarding" da STP, e quindi non siano in grado di inoltrare traffico.

```
[SW1]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Eth-Trunk1                  DESI  DISCARDING      NONE
   0    Eth-Trunk2                  DESI  DISCARDING      NONE
   0    Eth-Trunk3                  ROOT  FORWARDING      NONE
   0    Eth-Trunk4                  DESI  DISCARDING      NONE
   0    Eth-Trunk5                  DESI  DISCARDING      NONE
   0    Eth-Trunk6                  DESI  DISCARDING      NONE
```

Figura 3.13: risultato del comando display stp brief sullo switch di centro stella SW1.

Si rende dunque necessario disabilitare STP in tutti i dispositivi collegati con il router di centro stella, come mostrato in *figura 3.14*, per evitare che questo accada.

```
stp disable
```

Figura 3.14: applicazione del comando per disabilitare STP sullo switch SW1.

3.7 Configurazione NAT

Da specifiche viene richiesto che venga configurato su R8 un server NAT che sia in grado di "nattare" tutti i dispositivi appartenenti alle reti 192.168.30.0/24 e 192.168.40.0/24 che debbano comunicare con la rete esterna (simulata dal router R9 e PC2). La configurazione è riportata in *figura 3.15*:

```
acl number 2000
 rule 5 permit source 192.168.30.0 0.0.0.255
 rule 10 permit source 192.168.40.0 0.0.0.255
#
 nat address-group 1 200.10.10.50 200.10.10.55
#
interface GigabitEthernet0/0/0
 ip address 200.10.10.1 255.255.255.0
 ospf network-type p2p
 nat outbound 2000 address-group 1
#
```

Figura 3.15: configurazione NAT su router R8.

La prima cosa da osservare è che è stata creata una ACL (Access Control List). Le ACL vengono utilizzate essenzialmente per filtrare, selezionare e controllare il traffico che passa attraverso un certo dispositivo, al fine di compiere delle operazioni su di esso. Nel nostro caso, per poter configurare il NAT, abbiamo bisogno di selezionare tutto il traffico proveniente dalle reti sopra citate. Per fare questo viene utilizzata una ACL 2000, ovvero una di tipo basic. Con questo tipo di access control list possiamo soltanto selezionare il traffico sulla base dell'indirizzo IP sorgente del pacchetto ricevuto. Possiamo solo agire sul tipo di operazione da compiere, ovvero se permettere il pacchetto (permit) o se

scartarlo (deny). Nel nostro caso dobbiamo permettere tutti i pacchetti provenienti dalle sopracitate reti. Notiamo infatti che sono presenti due regole (la cinque e la dieci, una per rete) e che le wildcard mask ci dicono che i bit che devono matchare sono quelli dei primi tre ottetti. Una volta configurata la access control list dobbiamo definire che tipo di NAT vogliamo implementare. Per reti enterprise la soluzione migliore è l'implementazione del NAPT, poiché il NAT statico richiede troppi indirizzi pubblici, il NAT dinamico non permetterebbe la navigazione di tutti gli utenti della rete e l'easy NAT è adatto solo per reti domestiche. Per cui in primis dobbiamo definire un gruppo di indirizzi IP pubblici da rendere disponibili e questo viene fatto tramite il comando *nat address-group*. Sono stati scelti gli indirizzi dal 200.10.10.50 al 200.10.10.55 (sei indirizzi pubblici disponibili). Uno stesso indirizzo potrà così essere assegnato a più hosts e la differenziazione avverrà sulla base della porta TCP e quindi del servizio del quale si vuole usufruire. Rimane da configurare l'ultimo comando sull'interfaccia gigabitethernet0/0/0. Con il comando indicato con la freccia rossa stiamo dicendo al router che il NAT deve essere applicato a tutto il traffico in uscita (outbound) selezionato tramite la ACL 2000 e devono essere utilizzati gli indirizzi contenuti nell'address group 1. Il fatto che non ci sia la clausola "no-pat" indica che il tipo di NAT è proprio NAPT e non dinamico.

3.8 Configurazione DHCP

Analizziamo la configurazione del server DHCP sul router R9 in modo che PC2 assuma automaticamente un indirizzo IP. Tale configurazione è mostrata in *figura 3.16*:

```
dhcp enable
#
interface Vlanif20
 ip address 192.168.20.254 255.255.255.0
 dhcp select interface
#
```

Figura 3.16: configurazione del DHCP server sul router R9.

Innanzitutto, ricordiamo come su PC2 sia stata selezionata la modalità di assegnazione dinamica di un indirizzo IP, spuntando la casella "DHCP" nel riquadro riportato nella *figura 3.1*. In tal modo PC2 manda in continuazione dei messaggi "DHCP discover" in broadcast per trovare un dispositivo che sia in grado di fornirgli un indirizzo IP valido. Ovviamente, fin quando non configuriamo su R9 un server DHCP, PC2 non riceverà mai una "DHCP offer". Anche in questo caso possiamo scegliere due approcci differenti:

"interface pool configuration" o "global pool configuration". In generale, la prima modalità assegna all'host che ne fa richiesta un indirizzo IP appartenente allo spazio di indirizzi dell'interfaccia stessa, dove quest'ultima funge da indirizzo di gateway. Nella seconda modalità definiamo un pool che è globale e può essere utilizzato da qualsiasi interfaccia. Dunque, con questa seconda tecnica viene offerta una maggiore dinamicità alla configurazione ed è sicuramente preferibile alla prima. Per quanto riguarda la nostra configurazione, è stato scelto di utilizzare una "interface pool configuration", in quanto c'è necessità di assegnare l'indirizzo ad un solo host. Per cui, tornando alla *figura 3.16*, la prima cosa da fare è abilitare il DHCP sul nostro dispositivo tramite il comando *dhcp enable*. Bisogna poi, in interface view, selezionare l'interfaccia che dovrà erogare il servizio DHCP. Possiamo inoltre tramite altri comandi modificare il tempo di lease, indicare un server DNS, indicare degli indirizzi IP che devono essere esclusi dal pool e via dicendo. Nel caso in esame saranno quindi assegnabili gli indirizzi dal 192.168.20.1 fino al 192.168.20.253, considerando che 192.168.20.254 viene considerato il gateway e 192.168.20.0 è l'indirizzo della rete (la subnet mask è 255.255.255.0). A questo punto il router è in grado di rispondere alle "DHCP discover" con una "DHCP offer", che verranno seguiti da una "DHCP request" e da una "DHCP ack". Al termine di questo ultimo messaggio l'indirizzo IP viene ufficialmente assegnato all'host. In *figura 3.17* vengono mostrate tutte le informazioni relative al DHCP, alcune delle quali già citate:

```
[R9]dis ip pool interface Vlanif20
  Pool-name      : Vlanif20
  Pool-No        : 0
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Interface       Status          : Unlocked
  Gateway-0      : 192.168.20.254
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
    192.168.20.1  192.168.20.254   253     1        252(0)         0        0
 ------------------------------------------------------------------------------
```

Figura 3.17: Informazioni relative al DHCP configurato sul router R9.

3.9 Criticità riscontrate

Nel corso della configurazione sono stati riscontrate alcune criticità su cui è bene prestare particolare attenzione. Vengono di seguito elencate le principali:

- Nel corso della configurazione dei link aggregation, non risultava possibile eliminare una interfaccia fisica per il semplice motivo che il link aggregation è una proprietà dell'interfaccia fisica. Entrando nell'interfaccia logica eth-trunk non è possibile eliminare i link fisici che ne fanno parte.
- Configurato il routing gran parte dei ping fatti dai vari dispositivi non andava a buon fine. Questo perché STP bloccava alcuni collegamenti e li metteva in discarding. Tali link erano quindi incapaci di inoltrare traffico.
- La prima implementazione del NAT è stata con il tipo dinamico. In tal modo il ping fatto da PC3 a PC2 andava delle volte a buon fine e delle volte no. Questo perché con il NAT dinamico venivano assegnati gli indirizzi ad ogni richiesta di invio di un pacchetto e così, una volta esauriti questi indirizzi, il ping non andava a buon fine. È bastato cambiare la tipologia di NAT da dinamico a NAPT per far sì che l'IP assegnato sia sempre lo stesso e la differenziazione avvenga su base porta e non su base IP.

4 Verifica e test della topologia

4.1 Strumenti di verifica

Dopo un'attenta configurazione degli apparati è necessario fare una serie di verifiche per capire se ci sono eventuali errori, malfunzionamenti o modifiche da fare. Mostriamo gli strumenti di verifica e test. Dal prompt dei comandi di un elaboratore o dal terminale di un apparato di rete possiamo eseguire il comando *ping*, già introdotto in precedenza, per verificare la connettività di tale apparato con un altro nella rete. Per fare questo controllo vengono inviati cinque pacchetti ICMP (Internet Control Message Protocol) di tipo "echo request" all'indirizzo IP dell'interfaccia dell'host/apparato del quale si vuole verificare la connettività. Questo risponderà, se raggiungibile, con altrettanti pacchetti ICMP di tipo "echo reply" e al mittente dei pacchetti verrà mostrato un resoconto dei pacchetti persi e ricevuti. Questo comando è molto potente in quanto ci consente di fare facilmente il debugging della topologia. Ad esempio, la problematica illustrata nel paragrafo 3.9 relativa al NAT dinamico è emersa proprio facendo un semplice ping da PC3 a PC2. Per eseguire un debugging ancora più completo esistono una serie di opzioni che possono migliorare l'esecuzione del test di connettività. Queste ultime sono mostrate nella *figura 4.1*:

```
[SW1]ping ?
  -a              Select source IP address, the default is the IP address of the
                  output interface
  -c              Specify the number of echo requests to be sent, the default is
                  5
  -d              Specify the SO_DEBUG option on the socket being used
  -f              Set Don't Fragment flag in packet (IPv4-only)
  -h              Specify TTL value for echo requests to be sent, the default is
                  255
  -i              Select the interface sending packets
  -m              Time in milliseconds to wait for sending next packet, the
                  default is 500ms
  -n              Numeric output only. No attempt will be made to lookup host
                  addresses for symbolic names
  -name           Display the host name of the destination address
  -p              No more than 8 "pad" hexadecimal characters to fill out the
                  sent packet. For example -p f2 will fill the sent packet with
                  f and 2 repeatedly
  -q              Quiet output. Nothing is displayed except the summary lines at
                  startup time and when finished
  -r              Record route. Includes the RECORD_ROUTE option in the
                  ECHO_REQUEST packet and displays the route
  -s              Specify the number of data bytes to be sent, the default is
                  56bytes
  -si             Set the specified interface as the source interface of ping
                  packet
  -t              Timeout in milliseconds to wait for each reply, the default is
                  2000ms
  -tos            Specify TOS value for echo requests to be sent, the default is
                  0
  -v              Verbose output. ICMP packets other than ECHO_RESPONSE those
                  are received are listed
```

Figura 4.1: opzioni possibili sul comando ping.

Risulta inoltre utile (e lo vedremo sempre nel successivo paragrafo) sapere i nodi della rete che un pacchetto IP attraversa. Per soddisfare questa necessità esiste, sempre sul prompt dei comandi o sul terminale di un dispositivo di rete, il comando *tracert*. Tale comando consiste nell'inviare tre datagrammi UDP sulla porta 33434 con il TTL (Time To Live) del relativo pacchetto IP pari a uno, anche se il simulatore Huawei eNSP implementa questa funzionalità tramite soli pacchetti ICMP. Sappiamo che il TTL viene decrementato ogni qualvolta il pacchetto transita per un nodo della rete. In questo modo, quando il TTL di un pacchetto diventa zero viene inviato dal nodo che lo ha processato un pacchetto ICMP di tipo "time-to-live exceeded". Il pacchetto ritorna al nodo mittente che viene così a conoscenza del primo nodo di transito (viene memorizzato il suo indirizzo IP). I successivi tre pacchetti ICMP saranno inviati con TTL pari a due. Quando questo diventa zero viene generato dal nodo un pacchetto ICMP ancora di tipo "time-to-live exceeded". Questo viene inviato al nodo mittente che viene così a conoscenza del secondo nodo della rete. Il procedimento continua fin quando il pacchetto ICMP non arriva alla destinazione. Anche per il comando *tracert* esistono delle opzioni che possono aiutare nel debugging. Queste sono riportate nella figura 4.2:

```
<SW1>tracert ?
  -a              Set source IP address, the default is the IP address of the
                  output interface
  -f              First time to live, the default is 1
  -m              Max time to live, the default is 30
  -p              Destination UDP port number, the default is 33434
  -q              Number of probe packet, the default is 3
  -vpn-instance   Specify VPN-Instance of MPLS VPN
  -w              Timeout in milliseconds to wait for each reply, the default is
                  5000ms
```

Figura 4.2: opzioni possibili sul comando tracert.

4.2 Esecuzione dei test di verifica

Elencati i vari strumenti di verifica possiamo ora mostrare come la configurazione realizzata abbia portato ad un sistema funzionante. Innanzitutto, verifichiamo la connettività all'interno della rete ad anello:

Ping 192.168.30.3 → 192.168.40.4

```
PC>ping 192.168.40.4

Ping 192.168.40.4: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.40.4: bytes=32 seq=2 ttl=125 time=47 ms
From 192.168.40.4: bytes=32 seq=3 ttl=125 time=47 ms
From 192.168.40.4: bytes=32 seq=4 ttl=125 time=31 ms
From 192.168.40.4: bytes=32 seq=5 ttl=125 time=47 ms

--- 192.168.40.4 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/43/47 ms
```

Figura 4.3: ping da PC3 a PC4.

Osserviamo come non ci sia stata risposta al primo pacchetto inviato, avendo così cinque pacchetti inviati e quattro ricevuti, come esposto nelle statistiche. Questo deriva dalla necessità di popolare la ARP table da parte di nodi che sono coinvolti nell'inoltro del pacchetto.

Ping 192.168.40.4 → 192.168.60.112

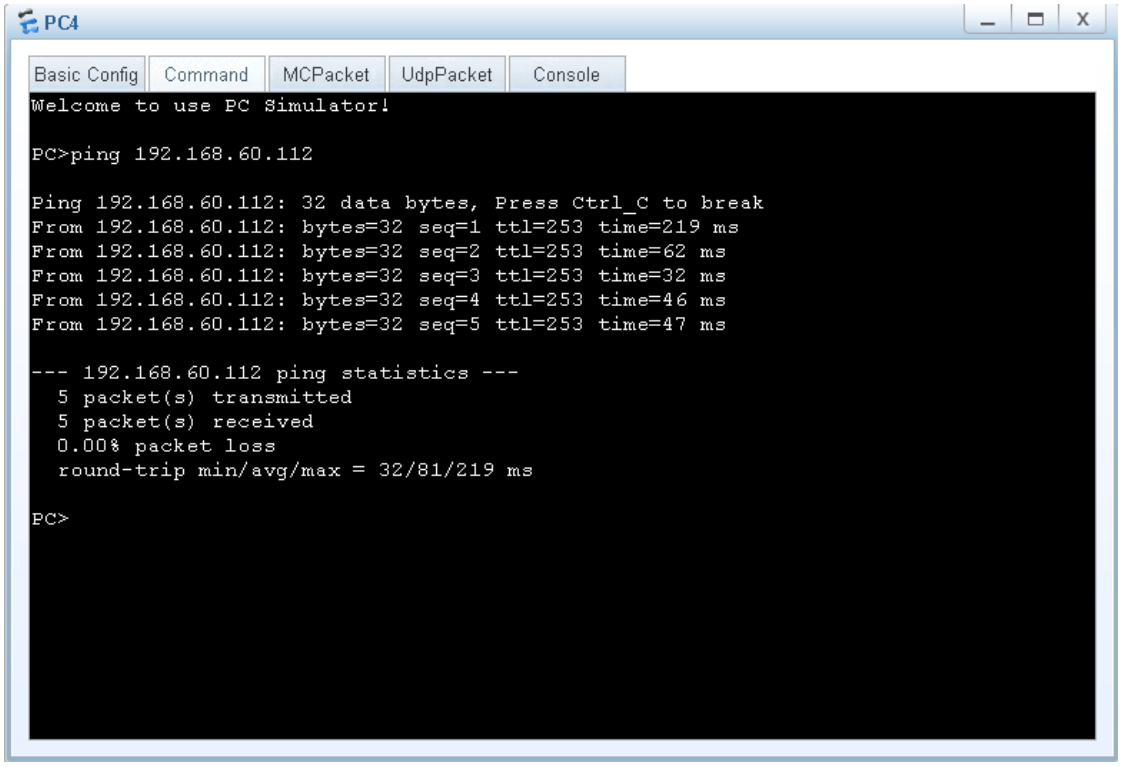


Figura 4.4: ping da PC4 a loopback0 di R4.

Ping 172.16.1.21 → 192.168.50.26

```
<R8>ping 192.168.50.26
  PING 192.168.50.26: 56  data bytes, press CTRL_C to break
    Reply from 192.168.50.26: bytes=56 Sequence=1 ttl=254 time=50 ms
    Reply from 192.168.50.26: bytes=56 Sequence=2 ttl=254 time=60 ms
    Reply from 192.168.50.26: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 192.168.50.26: bytes=56 Sequence=4 ttl=254 time=60 ms
    Reply from 192.168.50.26: bytes=56 Sequence=5 ttl=254 time=40 ms

  --- 192.168.50.26 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/52/60 ms
```

Figura 4.5: ping dalla eth-trunk6 di R8 alla loopback0 di R3.

Verifichiamo ora la connettività con la "rete esterna" (usciamo dall'anello), ovvero vediamo se PC2 è raggiungibile. Prima di eseguire il ping abbiamo bisogno di conoscere l'indirizzo IP che è stato assegnato dal DHCP server a PC2. Dunque, digitiamo dal prompt dei comandi di PC2 il comando *ipconfig* per sapere l'IP e troveremo che gli è stato assegnato l'indirizzo 192.168.20.253.

Ping 192.168.30.3 → 192.168.20.253

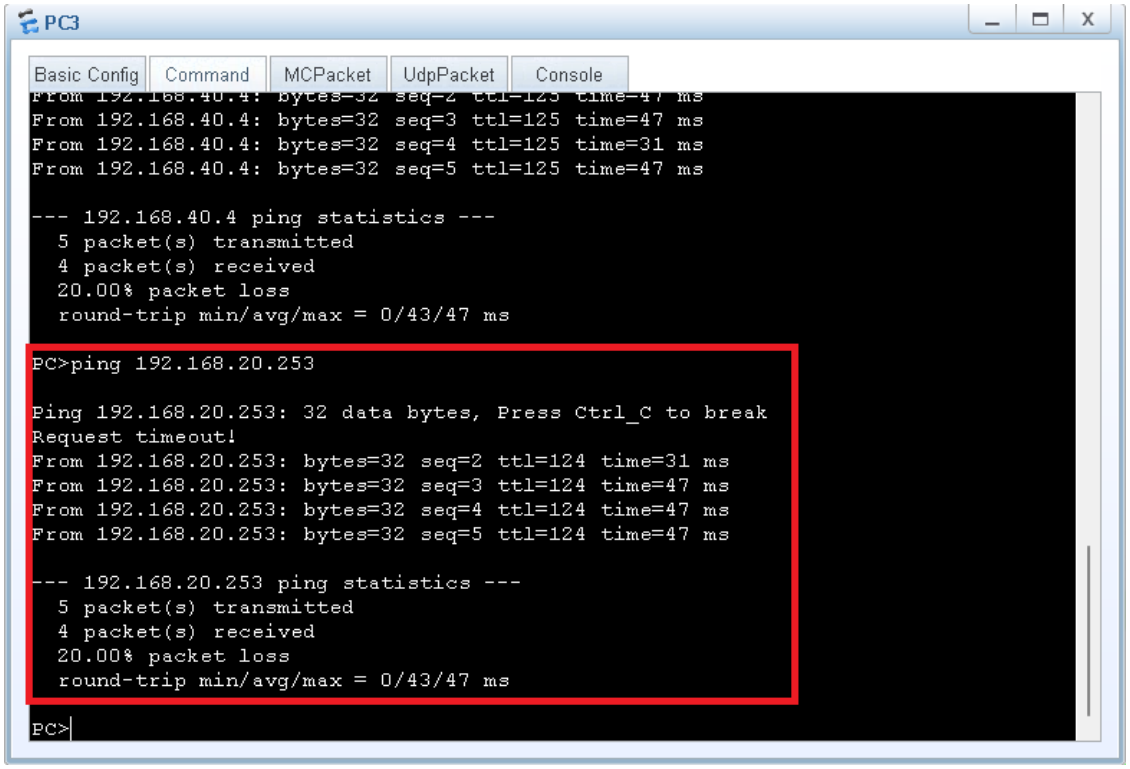
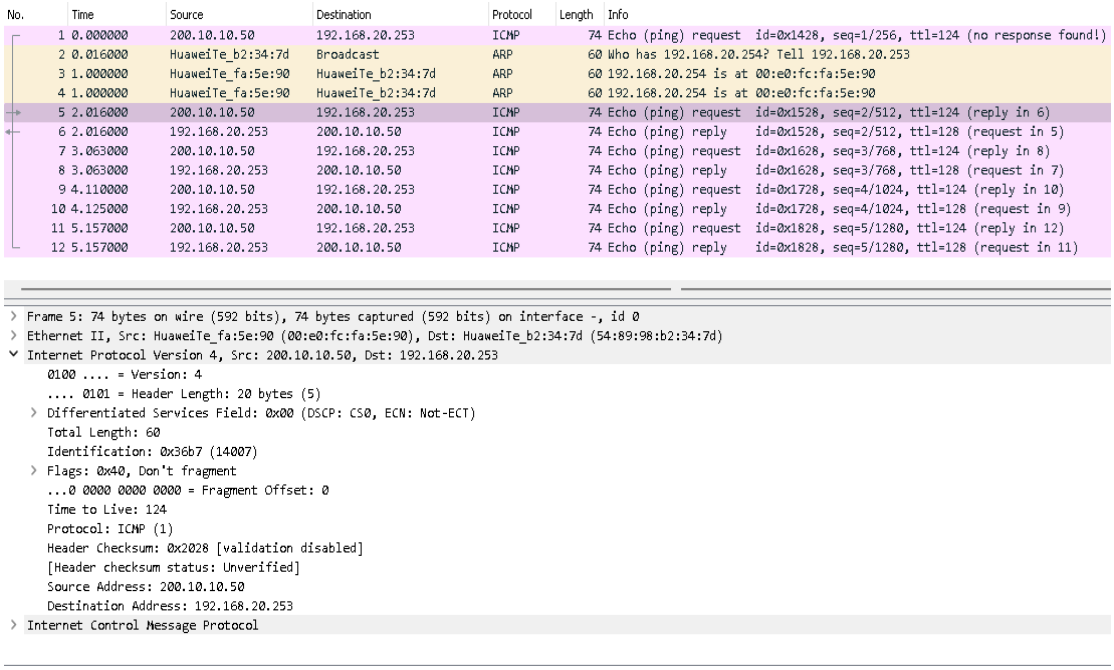


Figura 4.6: ping da PC3 a PC2.

Verificata la connettività dobbiamo anche constatare se effettivamente il server NAT abbia assegnato un indirizzo IP pubblico al traffico proveniente dalla rete di PC3. Per farlo ci serviamo di Wireshark, un software per la cattura dei pacchetti in rete che può essere richiamato dallo stesso simulatore eNSP. Per avviare la cattura dei pacchetti basta cliccare con il tasto destro su un nodo e scegliere la voce “start data capture”. Si aprirà così Wireshark. Nel caso del ping di *figura 4.6*, avviando la cattura sull’interfaccia ethernet0/0/1 di PC2, questo è stato il risultato:

Figura 4.7: cattura pacchetti ICMP con Wireshark.



Osserviamo che la sorgente dei pacchetti ICMP di tipo echo request è 200.10.10.50 e non 192.168.30.3 (pacchetti No. 1,5,7,9,11). Questo vuol dire che effettivamente gli host di tale rete sono “nattati” da R8. Inoltre, osserviamo che l’indirizzo IP pubblico assegnato da R8 è sempre lo stesso (ricordiamo che ce ne sono sei disponibili) poiché abbiamo configurato il NAPT. Nella cattura possiamo anche notare lo stack protocollare di un pacchetto ICMP e tutte le relative informazioni. Passiamo ora alla verifica del corretto funzionamento dell’anello di ridondanza. Vengono di seguito riportate alcune tabelle di routing, necessarie per una corretta comprensione:

```
[R1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 30        Routes : 30

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.16.1.0/30  Direct  0    0           D   172.16.1.2      Vlanif1
     172.16.1.2/32  Direct  0    0           D   127.0.0.1       Vlanif1
     172.16.1.3/32  Direct  0    0           D   127.0.0.1       Vlanif1
     172.16.1.4/30  OSPF    10   2           D   172.16.1.1      Vlanif1
     172.16.1.8/30  OSPF    10   2           D   172.16.1.1      Vlanif1
    172.16.1.12/30  OSPF    10   2           D   172.16.1.1      Vlanif1
    172.16.1.16/30  OSPF    10   2           D   172.16.1.1      Vlanif1
    172.16.1.20/30  OSPF    10   2           D   172.16.1.1      Vlanif1
    172.16.1.24/30  Direct  0    0           D   172.16.1.25     GigabitEthernet
0/0/0
    172.16.1.25/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    172.16.1.27/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    172.16.1.28/30  OSPF    10   202         D   172.16.1.1      Vlanif1
    172.16.1.32/30  OSPF    10   202         D   172.16.1.1      Vlanif1
    172.16.1.36/30  OSPF    10   202         D   172.16.1.1      Vlanif1
    172.16.1.40/30  Direct  0    0           D   172.16.1.42     GigabitEthernet
0/0/1
    172.16.1.42/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    172.16.1.43/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
   192.168.20.0/24  OSPF    10   4           D   172.16.1.1      Vlanif1
   192.168.30.0/24  Direct  0    0           D   192.168.30.254  Vlanif30
 192.168.30.254/32  Direct  0    0           D   127.0.0.1       Vlanif30
 192.168.30.255/32  Direct  0    0           D   127.0.0.1       Vlanif30
   192.168.40.0/24  OSPF    10   3           D   172.16.1.1      Vlanif1
  192.168.50.26/32  OSPF    10   2           D   172.16.1.1      Vlanif1
 192.168.60.112/32  OSPF    10   2           D   172.16.1.1      Vlanif1
 192.168.70.234/32  OSPF    10   2           D   172.16.1.1      Vlanif1
    200.10.10.0/24  OSPF    10   3           D   172.16.1.1      Vlanif1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 4.8: tabella di routing del router R1.

```
[SW1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 26        Routes : 31

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.16.1.0/30  Direct  0    0           D   172.16.1.1      Vlanif1
     172.16.1.1/32  Direct  0    0           D   127.0.0.1       Vlanif1
     172.16.1.4/30  Direct  0    0           D   172.16.1.5      Vlanif2
     172.16.1.5/32  Direct  0    0           D   127.0.0.1       Vlanif2
     172.16.1.8/30  Direct  0    0           D   172.16.1.10     Vlanif3
    172.16.1.10/32  Direct  0    0           D   127.0.0.1       Vlanif3
    172.16.1.12/30  Direct  0    0           D   172.16.1.14     Vlanif4
    172.16.1.14/32  Direct  0    0           D   127.0.0.1       Vlanif4
    172.16.1.16/30  Direct  0    0           D   172.16.1.18     Vlanif5
    172.16.1.18/32  Direct  0    0           D   127.0.0.1       Vlanif5
    172.16.1.20/30  Direct  0    0           D   172.16.1.22     Vlanif6
    172.16.1.22/32  Direct  0    0           D   127.0.0.1       Vlanif6
    172.16.1.24/30  OSPF    10   201         D   172.16.1.2      Vlanif1
                    OSPF    10   201         D   172.16.1.6      Vlanif2
    172.16.1.28/30  OSPF    10   201         D   172.16.1.6      Vlanif2
                    OSPF    10   201         D   172.16.1.17     Vlanif5
    172.16.1.32/30  OSPF    10   201         D   172.16.1.13     Vlanif4
                    OSPF    10   201         D   172.16.1.17     Vlanif5
    172.16.1.36/30  OSPF    10   201         D   172.16.1.13     Vlanif4
                    OSPF    10   201         D   172.16.1.9      Vlanif3
    172.16.1.40/30  OSPF    10   201         D   172.16.1.2      Vlanif1
                    OSPF    10   201         D   172.16.1.9      Vlanif3
   192.168.20.0/24  OSPF    10   3           D   172.16.1.21     Vlanif6
   192.168.30.0/24  OSPF    10   2           D   172.16.1.2      Vlanif1
   192.168.40.0/24  OSPF    10   2           D   172.16.1.6      Vlanif2
  192.168.50.26/32  OSPF    10   1           D   172.16.1.9      Vlanif3
 192.168.60.112/32  OSPF    10   1           D   172.16.1.13     Vlanif4
 192.168.70.234/32  OSPF    10   1           D   172.16.1.17     Vlanif5
    200.10.10.0/24  OSPF    10   2           D   172.16.1.21     Vlanif6
```

Figura 4.9: tabella di routing dello switch SW1.

```
[R8]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 32        Routes : 32

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.16.1.0/30  OSPF    10   2           D   172.16.1.22     Vlanif6
     172.16.1.4/30  OSPF    10   2           D   172.16.1.22     Vlanif6
     172.16.1.8/30  OSPF    10   2           D   172.16.1.22     Vlanif6
    172.16.1.12/30  OSPF    10   2           D   172.16.1.22     Vlanif6
    172.16.1.16/30  OSPF    10   2           D   172.16.1.22     Vlanif6
    172.16.1.20/30  Direct  0    0           D   172.16.1.21     Vlanif6
    172.16.1.21/32  Direct  0    0           D   127.0.0.1       Vlanif6
    172.16.1.23/32  Direct  0    0           D   127.0.0.1       Vlanif6
    172.16.1.24/30  OSPF    10   202         D   172.16.1.22     Vlanif6
    172.16.1.28/30  OSPF    10   202         D   172.16.1.22     Vlanif6
    172.16.1.32/30  OSPF    10   202         D   172.16.1.22     Vlanif6
    172.16.1.36/30  OSPF    10   202         D   172.16.1.22     Vlanif6
    172.16.1.40/30  OSPF    10   202         D   172.16.1.22     Vlanif6
   192.168.20.0/24  OSPF    10   2           D   200.10.10.2     GigabitEthernet
0/0/0
   192.168.30.0/24  OSPF    10   3           D   172.16.1.22     Vlanif6
   192.168.40.0/24  OSPF    10   3           D   172.16.1.22     Vlanif6
  192.168.50.26/32  OSPF    10   2           D   172.16.1.22     Vlanif6
 192.168.60.112/32  OSPF    10   2           D   172.16.1.22     Vlanif6
 192.168.70.234/32  OSPF    10   2           D   172.16.1.22     Vlanif6
    200.10.10.0/24  Direct  0    0           D   200.10.10.1     GigabitEthernet
0/0/0
    200.10.10.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
   200.10.10.50/32  Unr     64   0           D   127.0.0.1       InLoopBack0
   200.10.10.51/32  Unr     64   0           D   127.0.0.1       InLoopBack0
   200.10.10.52/32  Unr     64   0           D   127.0.0.1       InLoopBack0
   200.10.10.53/32  Unr     64   0           D   127.0.0.1       InLoopBack0
   200.10.10.54/32  Unr     64   0           D   127.0.0.1       InLoopBack0
   200.10.10.55/32  Unr     64   0           D   127.0.0.1       InLoopBack0
  200.10.10.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 4.10: tabella di routing del router R8.

Mostriamo ora, tramite il comando *tracert*, come il traffico sia indirizzato verso il router di centro stella e non transiti nei collegamenti dell'anello:

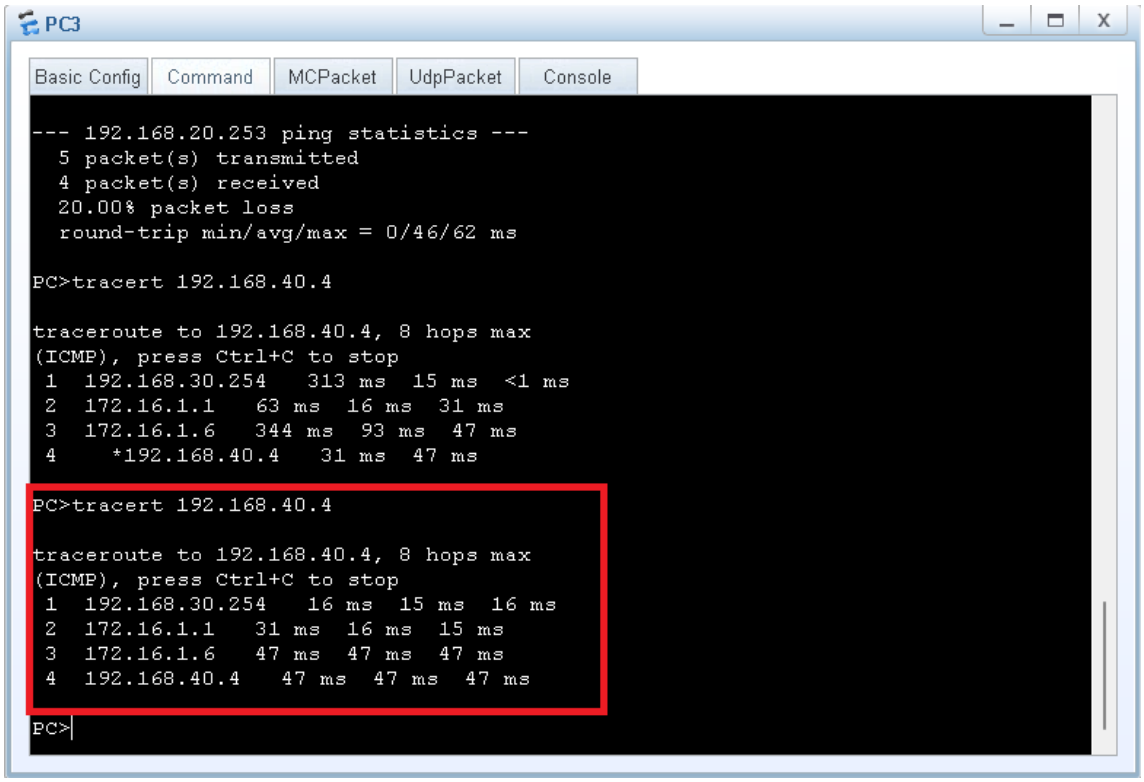


Figura 4.11

Questo rappresenta la prova di come il traffico utente venga convogliato verso lo switch centrale visto che i pacchetti transitano per i nodi 172.16.1.1 e 172.16.1.6, in condizione di perfetto funzionamento di tutti i link. Verifichiamo ora se il routing è stato correttamente configurato: simuliamo una failure del link che collega R1 al router di centro stella. Accediamo quindi nel router R1 e in interface view applichiamo il comando *shutdown* sull'interfaccia eth-trunk1. La situazione è la seguente:

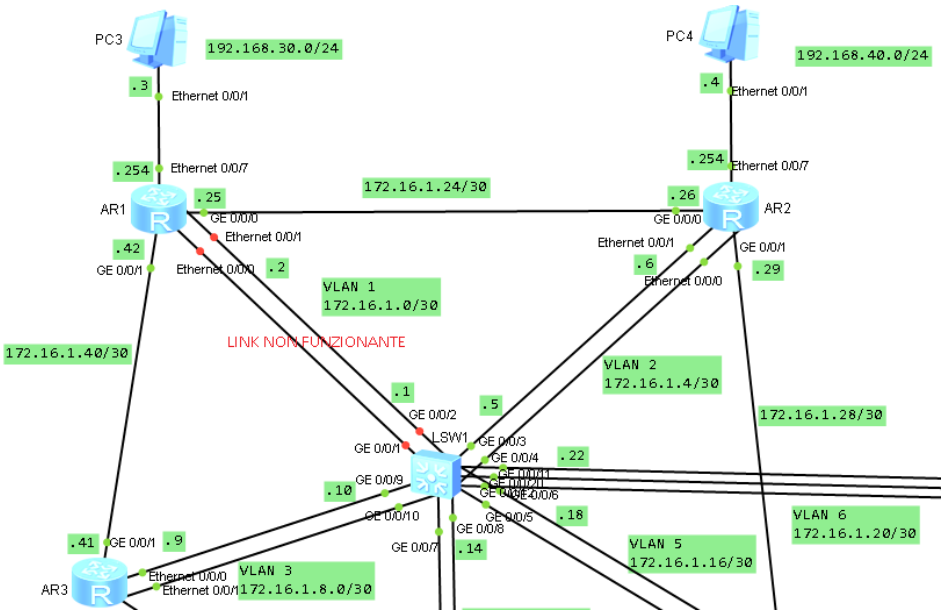


Figura 4.12

Andiamo di nuovo ad applicare il comando *tracert* per osservare quali sono i nodi di transito dei pacchetti:

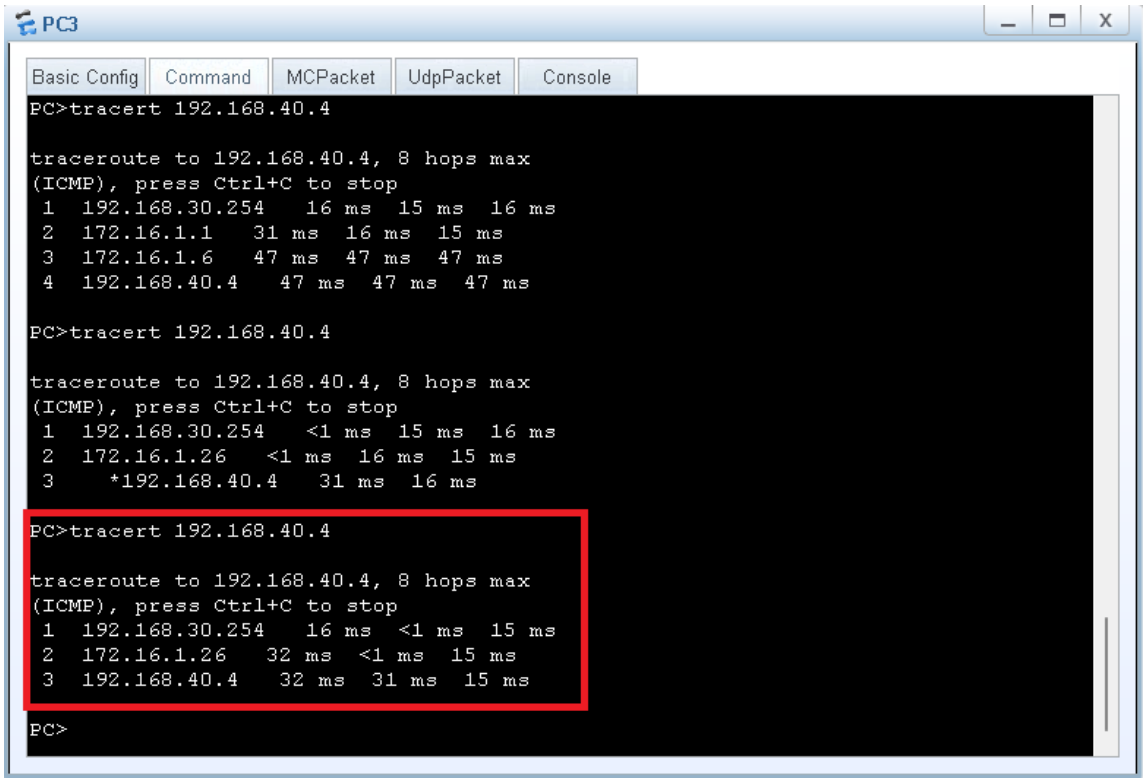


Figura 4.13

Come si può osservare PC4 è ancora raggiungibile anche se si è verificata una failure nella topologia. Il percorso compiuto stravolta utilizza un nodo dell'anello, ovvero

172.16.1.26. Osserviamo ora un ultimo caso: simuliamo un'altra failure proprio nel link appena citato. Quindi entriamo in R1 e applichiamo il comando *shutdown* in interface view sulla gigabitethernet0/0/0. La situazione è la seguente:

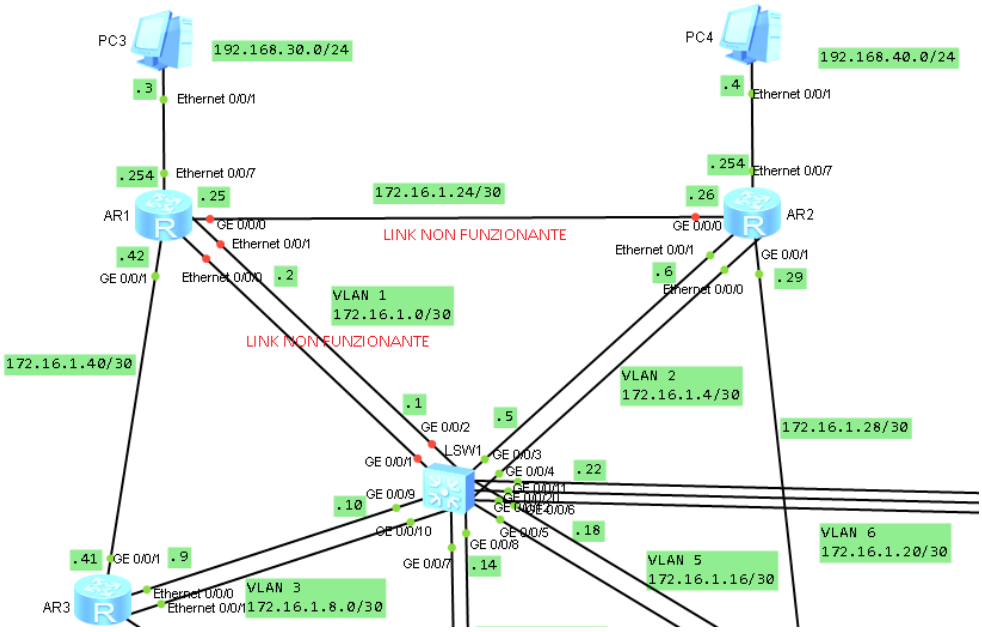


Figura 4.14

Andiamo di nuovo ad applicare il comando *tracert* per osservare quali sono i nodi di transito dei pacchetti:

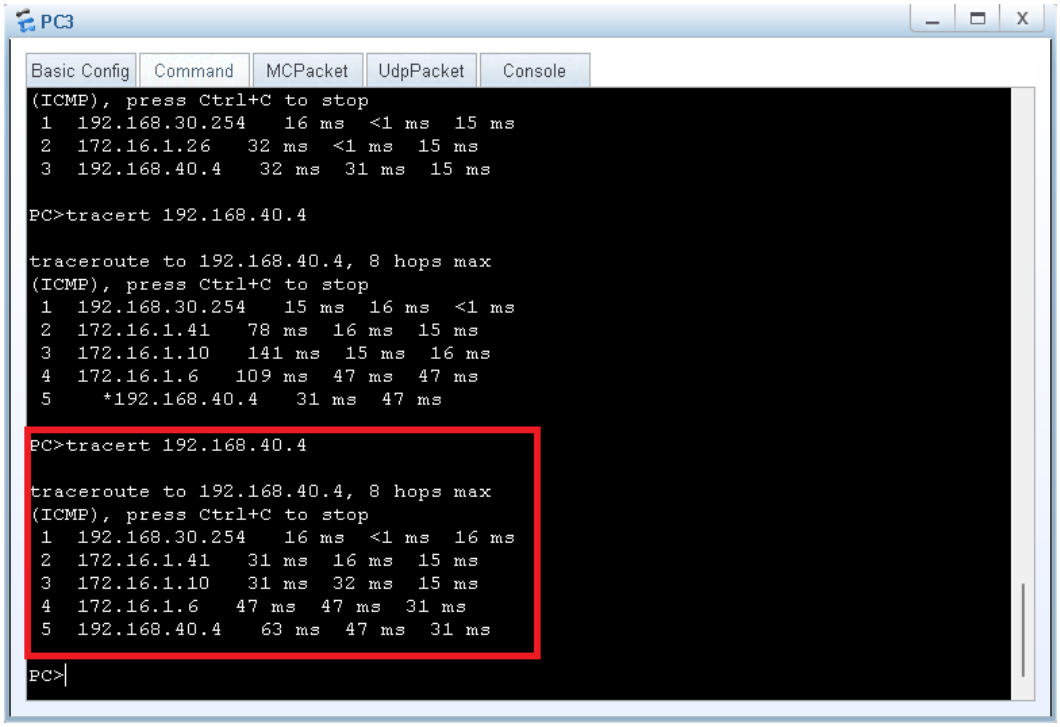


Figura 4.15

Ovviamente il percorso compiuto è il più lungo delle tre prove eseguite poiché questo risulta essere il percorso meno conveniente (i pacchetti passano per 172.16.1.41, 172.16.1.10, 172.16.1.6). Ciò però dimostra la robustezza della topologia: in caso di più failure PC2 è ancora in grado di comunicare con l'esterno.

5 Conclusioni

Il lavoro svolto mostra come sia possibile progettare e configurare una topologia di rete enterprise. Tale lavoro si è rivelato essere un progetto complesso che richiede specifiche conoscenze e competenze nel campo del networking. Senza di esse non si riuscirebbe ad eseguire una buona configurazione degli apparati e, tantomeno, il troubleshooting risulterebbe alquanto difficile, se non impossibile. In particolare, si pone l'accento sulla forte applicazione pratica che ricopre questo argomento: ad oggi qualsiasi struttura, che sia un'azienda, un ospedale, una struttura pubblica etc, richiede l'instaurazione di apparati di rete che rendano possibile il collegamento con l'esterno, anche solo per navigare in internet o per ricevere/inviare una mail. Nello specifico, abbiamo trattato l'aggregazione dei link per aumentare la velocità di trasmissione dati, la conversione delle interfacce L2 in interfacce L3, la configurazione di un protocollo di routing dinamico, l'implementazione di server NAT e DHCP e, in particolar modo, abbiamo visto come configurare una topologia di tipo centro stella ridondata da alcuni collegamenti che formano un anello intorno allo switch centrale. L'aspetto della ridondanza è a dir poco fondamentale e viene spesso richiesto nell'implementazione di una topologia. Dunque, questo lavoro può essere definito come un progetto a tutto tondo, che analizza ogni aspetto relativo all'implementazione di una rete di networking.

6 Bibliografia

- https://it.wikipedia.org/wiki/Architettura_di_rete
- https://www.cisco.com/c/it_it/solutions/small-business/resource-center/networking/networking-basics.html
- https://www.vegatraining.eu/corsi-huawei/corso-huawei-hcia-routing-and-switching/?gclid=EAIaIQobChMI34SI4Oa29QIVkLh3Ch2HugKqEAAYASAAEgLD3fD_BwE
- Dispensa “VLAN” corso HCIA Huawei.
- Dispensa “NAT” corso HCIA Huawei.
- Dispensa “OSPF” corso HCIA Huawei.
- Dispensa “Introduzione IPv6” corso HCIA Huawei.

7 Ringraziamenti

Ritengo opportuno dedicare un piccolo ma essenziale spazio alle persone che mi hanno permesso di raggiungere questo traguardo. Questo non è solo il mio successo ma il successo di tutti loro.

Ringrazio in primis la mia famiglia, in particolare mio padre Onelio e mio fratello Luca, che mi hanno supportato e sopportato durante questo lungo cammino colmo di insidie ma anche di grandi soddisfazioni.

Ringrazio il mio relatore, il professor Ennio Gambi, e il mio correlatore, il professor Adelmo De Santis, per avermi guidato in questo complesso ma affascinante lavoro.

Ringrazio i miei ex coinquilini, Luca e Alessio, con i quali ho condiviso la casa e i primi, duri, anni di università.

Ringrazio tutti i miei amici e tutti coloro che mi sono stati vicino e che sono riusciti ad attenuare le mie ansie nelle giornate più buie. Siete sempre riusciti a regalarmi attimi di spensieratezza nei momenti del bisogno.

Ringrazio infine mia madre Carla, senza la quale non sarei qui a scrivere queste righe. Mi hai trasmesso il tuo sapere e la tua fame di conoscenza. Porterò sempre con me i tuoi eleganti modi di fare e la tua grande cultura. Sei stata, sei e sarai fonte di ispirazione per me.