Entorn de simulació de xarxes focalitzat en Routing IP

Carla van den Bogaart Marzola

Resum– Les comunicacions a distància han permès augmentar la qualitat de vida dels ciutadans i afavorir el creixement econòmic. Des de la implementació del teletreball, la gestió de tràmits amb l'administració pública, la consulta d'informes sanitaris, reduint els desplaçaments en cotxe, etc. Tot això és possible gràcies a la implementació d'Internet, i la recerca feta sobre els protocols que el fonamenten. Per seguir desenvolupant aquestes tecnologies i augmentant els avantatges que això ens aporta, és bàsic formar bons professionals dedicats en aquesta àrea. Per això aquest projecte pretén crear un entorn que serveixi com a eina als estudiants, per entendre millor com la informació viatja a través d'Internet i com els diferents dispositius interaccionen entre ells mitjançant protocols. Sobretot es focalitza en el protocol IP i la fragmentació de paquets.

Paraules clau– GNS3, VMware, Entorn de Simulació, IP, fragmentació, ping, UDP, traceroute, router, Wireshark

Abstract– Remote communications have made it possible to increase the quality of life of citizens and promote economic growth. From the implementation of telework, the management of procedures with the public administration, the consultation of health reports, reducing car journey, etc. All this is possible thanks to the implementation of the Internet, and the research done on the protocols that underpin it. To continue developing these technologies and increasing the advantages that this brings us, it is essential to train good professionals dedicated to this area. That is why this project aims to create an environment that serves as a tool for students, to better understand how information travels through the Internet and how different devices interact with each other through protocols. It mainly focuses on the IP protocol and packet fragmentation.

Keywords– GNS3, VMware, Simulation Environment, IP, fragmentation, ping, UDP, traceroute, router, Wireshark

1 Introducció

AQUEST treball té com a objectiu principal la creació d'un entorn didàctic de simulació de xarxes focalitzat en Routing IP. Per fer-ho se'ns és absolutament necessari poder definir un conjunt de xarxes interconnectades per routers. I que el software ajudi als estudiants de xarxes d'enginyeria informàtica a entendre millor el funcionament del protocol IP, i molt específicament com funcionen les adreces físiques i lògiques implicades, i com funciona el mecanisme de la fragmentació. Complir amb aquest fet, és primordial que es pugui visualitzar de forma gràfica, com per exemple la visualització dels camps associats a la fragmentació IP.

Per fer-ho haurem d'assolir diferents fites de disseny que són la definició del rang IP per cadascuna de les xarxes, la caracterització de les interfícies dels routers a cadascuna de les subxarxes, per cada host de cada subxarxa com la IP, la màscara i el default router. Això ens permetrà una millor qualitat del producte i ens facilitarà la implementació posterior.

Un cop realitzat el disseny es pretén desenvolupar l'entorn que ha de permetre als usuaris del software poder definir rutes estàtiques als diferents routers, la definició de diferents tamanys de MTU per cada subxarxa, la simulació d'un ping entre hosts ubicats a diferents xarxes, i la gestió dels missatges ICMP i dels diferents camps de fragmentació IP.

• E-mail de contacte: carla.vandenbogaart@autonoma.cat
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Juan Antonio Martinez Carrascal (Departament d'Enginyeria de la Informació i les Comunicacions)
• Curs 2022/23

1.1 Requeriments Funcionals

- El sistema ha de permetre la comunicació IP entre host de diferents xarxes.
- En l'entorn s'han de poder definir rutes estàtiques als diferents routers que el formen.
- S'han de poder realitzar pings entre els diferents hosts de la xarxa.
- La fragmentació IP ha de poder ser visualitzable amb els seus diferents camps.
- Els missatges ICMP, han de poder ser gestionats.
- Ha de ser un entorn user friendly, perquè els diferents estudiants puguin entendre els conceptes apresos a l'assignatura de xarxes.

1.2 Requeriments No Funcionals

- L'entorn ha de tenir routers i hosts distribuïts entre diferents subxarxes interconnectades.
- S'hauran de caracteritzar les diferents interfícies dels routers per cada subxarxa.
- La definició del rang IP per cada xarxa.
- Per cada host definir la seva IP, la màscara de la subxarxa i el default router.
- La interfície ha de permetre la visualització dels diferents paràmetres, com els camps associats a la fragmentació IP.
- Els tamanys de la MTU s'han de poder definir per cada una de les subxarxes.

2 ESTAT DE L'ART

El projecte es durà a terme mitjançant l'ús d'un simulador gràfic de Xarxa anomenat GNS3 (Graphic Network Simulator-3). S'ha decidit utilitzar aquest software existent com a punt de partida, ja que ha estat desenvolupat i revisat per un equip de professionals, i des del seu llançament el 2008 l'han utilitzat grans organitzacions com la NASA o la multinacional Walmart, fet que verifica el seu bon funcionament. Ens centrarem al desenvolupament de l'entorn partint d'aquest punt inicial, fet que ens permetrà arribar més lluny i poder complir més objectius desenvolupant noves funcionalitats, centrant-nos en el compliment dels objectius més que en la creació de funcionalitats base a les quals aquest programari dona solució.

Els simuladors de xarxes ens permeten fer proves sobre una xarxa virtual, això pot ser de gran ajuda quan volem implementar una xarxa real, abans de fer-ho podem simular-la i comprovar el seu funcionament, de manera que podem detectar errors abans de fer la instal·lació real, el qual comportaria un augment dels costos. En l'àmbit educatiu també són àmpliament utilitzats, ja que permeten la creació d'entorns que es poden fer servir com a laboratoris virtuals, ajudant als alumnes a entendre millor els conceptes i permetent-los simular implementacions. Com ja podem intuir aquestes eines han estat àmpliament utilitzades, de manera que sempre que un usuari ha detectat un error o mancança, l'equip de professionals que treballen darrere un software comercial, han pogut corregir-los. Això fa que aquest tipus de backend tinguin una taxa d'errors més baixa, pel fet que són molt més competitius.

Cisco Packet Tracet és un simulador d'administració i simulador de xarxes, centrat en dispositius Cisco, per tant, té les seves funcions limitades, ja que no simula dispositius que no siguin Cisco. L'avantatge principal és que és senzill d'instal·lar. En canvi, GNS3 té més opcions de configuració i són més avançades. La configuració del GNS3 és més complicada, però un cop instal·lat ens permet crear xarxes més complexes.[1]

Dins del ventall de simuladors que existeixen s'ha escollit el GNS3 (Graphical Network Simulator), perquè és el que millor s'adapta a les nostres necessitats. Les característiques més destacables són: que les simulacions són molt realistes i ens permeten implementar un gran nombre de paràmetres, és de codi obert el que permetrà a qualsevol alumne poder-lo descarregar sense haver d'adquirir cap llicència, i és multiplataforma el que permet la seva instal·lació en dispositius de diferent tipus.[2][3]

3 PLANIFICACIÓ

La planificació es basa en un diagrama temporal de Gantt, on s'hi poden observar les dates d'entrega i les precedències. S'ha decidit utilitzar el Project Manager com a eina per gestionar les diferents tasques, en l'Annex A.1 hi podem trobar el diagrama de Gantt des d'una visió d'alt nivell.[4]

Les tasques s'han organitzat en 6 blocs:

1. Definir els objectius del treball: en aquest bloc es defineixen i descriuen les diferents funcions que ha de tenir l'entorn que hem de realitzar.
2. Definir i implementar la metodologia a seguir: es buscarà informació sobre les diferents metodologies de planificació de projectes, s'escollirà la que hem de seguir, i posteriorment s'implementarà. També s'inclou la contextualització del projecte i es decidiran les eines amb les quals treballarem, s'instal·larà també el programari necessari pel desenvolupament del treball.
   - 2.1 Referent a la metodologia Àgil.
     - 2.1.1 Definició del context de treball.
     - 2.1.2 Cerca dels diferents tipus de metodologies Àgil.
     - 2.1.3 Comparativa dels avantatges i inconvenients de cada tipus.
     - 2.1.4 Escollir la metodologia Àgil més adequada.
     - 2.1.5 Implementació de la metodologia Àgil escollida.
       - 2.1.5.1 Descripció detallada de la metodologia escollida.
       - 2.1.5.2 Caracterització de rols.
       - 2.1.5.3 Utilització del software adequat.
   - 2.2 Referent a la creació de l'entorn de treball.
     - 2.2.1 Definir els requeriments.
     - 2.2.2 Buscar com es pot implementar.

2.2.3 Escollir un mètode a seguir.
2.2.4 Justificar mètode escollit realitzant una comparativa amb les alternatives.
2.2.5 Instal·lació del software necessari.

3. Disseny de l'entorn: aquest bloc inclou totes les tasques de disseny de l'entorn, des de la creació d'un esquema descriptiu de la xarxa que s'implementarà, fins a la caracterització dels diferents elements de la xarxa. Aquest bloc té com a objectiu englobar totes les tasques de disseny que ens permetran complir amb tots els objectius de forma més eficient.
   3.1 Definició de l'entorn de xarxa que volem implementar.
   3.2 Creació d'un esquema gràfic sobre la xarxa.
   3.3 Requeriments que volem per cada dispositiu que integra la xarxa.
      3.3.1 Definir el rang IP per cadascuna de les xarxes.
      3.3.2 Definir les interfícies dels routers a cadascuna de les subxarxes.
      3.3.3 Definir paràmetres de configuració dels hosts per cadascuna de les subxarxes.
         3.3.3.1 IP del host.
         3.3.3.2 Màscara de la subxarxa.
         3.3.3.3 El default router.
   3.4 Definició de rutes estàtiques pels diferents routers.
   3.5 Definir tamany de la MTU de cada xarxa.
   3.6 Definir els camps associats a la fragmentació IP.

4. Implementació de l'entorn dissenyat: aquest bloc es realitzarà posteriorment a l'anterior, i s'englobarà tota la instal·lació i creació de l'espai dissenyat.
   4.1 Descàrrega de les imatges dels dispositius necessaris.
   4.2 Creació de l'entorn.
      4.2.1 Posar els dispositius.
      4.2.2 Configuració dels routers.
         4.2.2.1 Implementació de les interfícies per cada subxarxa.
         4.2.2.2 Taula de Routing.
         4.2.2.3 Implementació del NAT.
         4.2.2.4 Permetre el tràfic de xarxa.
      4.2.3 Configuració dels hosts.
         4.2.3.1 Assignació de la IP.
         4.2.3.2 Assignació de la màscara.
         4.2.3.3 Assignació del default router.
      4.2.4 Implementació de les rutes estàtiques.
      4.2.5 Caracterització de la MTU de cada subxarxa.
      4.2.6 Gestionar els camps associats a la fragmentació IP.

5. Testatge de l'entorn: s'hi faran totes les feines de testeig per assegurar que l'entorn creat en el bloc anterior compleixi amb tots els requeriments del projecte.
   5.1 Simulació d'un ping entre hosts ubicats en diferents xarxes.
   5.2 Testos sobre els missatges ICMP.
   5.3 Visualitzar els camps associats a la fragmentació IP.

6. Documentació del treball: aquest bloc es realitza simultàniament amb els altres, ja que s'hi troben la redacció dels diferents informes entregables, els quals estan restringits per una data d'entrega.
   6.1 Realització de l'informe inicial.
   6.2 Realització de l'informe progrés 1.
   6.3 Realització de l'informe progrés 2.
   6.4 Realització informe final.
   6.5 Realització de la presentació.
   6.6 Realització del dossier a entregar.
   6.7 Realització del pòster.
   6.8 Creació del manual d'ús per l'alumnat.

3.1 Desviacions respecte a la planificació inicial

En l'Annex A.1, podem veure el diagrama de Gantt, el qual no ha tingut desviacions en les dates planificades, malgrat que la dedicació d'algunes fases ha requerit més temps de l'estimat inicialment. La principal diferència és la introducció d'una nova tasca "Creació del manual d'ús per l'alumnat", dins l'apartat de documentació del treball.

4 METODOLOGIA

Per fer el treball s'utilitzarà una metodologia Kanban, la qual es basa en un cartell visual, que ens permet gestionar el procés de creació de software. A diferència de la metodologia Scrum que també es basa en els principis Àgil. No tindrem sprints, i les tasques seran més globals, és a dir, hi haurà menys quantitat, però seran més grans.[5]

L'avantatge que ens pot aportar en aquest cas, és que el treball al ser realitzat per una sola persona, les tasques de control no són tan necessàries i ens les podem estalviar, disposant així de més temps per dedicar a les tasques de desenvolupament del projecte, com per exemple a la codificació. Com podem veure, Kanban se centra en la tasca, i es basen en el fet que un mateix equip realitza la tasca de principi a fi. Podem tenir fites, però no és necessari estimar el temps per executar cada tasca, ja que aquest pot ser variable i al no existir els sprints no és un requisit indispensable a diferència de la metodologia Scrum. Les fites que ens marcaran el desenvolupament són les diferents entregues del projecte i estan detallades amb més profunditat a l'apartat de planificació.

Els beneficis que aporta Kanban són la versatilitat, podem afegir noves tasques mitjançant les targetes de forma senzilla i visual a mesura que el projecte avança, la capacitat de resposta, això ens permet adaptar-nos de forma ràpida als comentaris del tutor, i la visibilitat, les tasques es poden veure fàcilment per qualsevol observador, fent així que el treball sigui més visible.

Per implementar-ho utilitzarem Trello, que ens permetrà crear i gestionar el cartell, el qual tindrà les següents columnes:

1. `Pendent`: aquí hi haurà totes les tasques que encara s'han d'iniciar, les quals estaran ordenades de major a menor prioritat.
2. `En curs`: s'hi situaran les que s'estiguin realitzant actualment.
3. `Completades`: on hi haurà tot el treball ja finalitzat.

5 DESENVOLUPAMENT

Per l'elaboració de l'entorn primer s'ha dut a terme les tasques referents al seu disseny, i posteriorment s'ha implementat en el sistema operatiu macOS Ventura. La instal·lació del Software GNS3 s'ha dut a terme mitjançant GNS3 VM per VMware, la qual se li ha assignat 4 processadors per la seva execució i 4 GB de RAM. S'utilitza també el GNS3 WebClient, que ens permet tenir la interfície web del sistema de simulació de xarxes, el qual podem accedir a través del navegador Chrome o Firefox, amb la direcció IP assignada a la nostra màquina virtual de GNS3 en el port 80.
Malgrat que la configuració ha estat complexa, la dedicació en aquesta etapa permetrà poder assolir en el temps planificat els requeriments funcionals plantejats en aquest projecte.

5.1 Disseny de l'entorn

En aquest primer bloc s'ha definit l'entorn, creant un diagrama de la topologia de xarxa que volem implementar, la qual es pot veure a la imatge de la *Figura 1*.

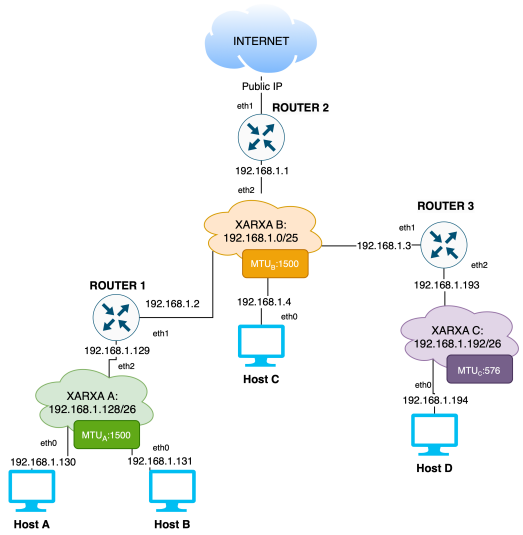

Fig. 1: Diagrama de la topologia de xarxa de l'entorn.

Aquesta topologia permet valorar la fragmentació de datagrames a diferents xarxes i per diferents casos, per exemple:

- Fent un ping en el Host A cap al Host C, no s'hauria d'observar cap datagrama fragmentat ni en la xarxa A ni en la xarxa B, ja que les MTUs són iguals.
- Fent un ping des del Host A cap al Host D, s'hauria d'observar que el datagrama ICMP request viatja sense fragmentar per la xarxa A i per la B, però en la xarxa C, estaria fragmentat ja que la MTU d'aquesta xarxa és menor i el Router3, fragmentaria el datagrama per poder enviar-lo a través d'aquesta xarxa i així poder-lo entregar en el host D.
- També és interessant el fet de poder observar el camí que segueixen els paquets a través de les subxarxes i com els diferents routers els encaminen, modificant el TTL. Poder veure com funciona el protocol ARP, veient els missatges que es generen en les diferents xarxes i com les adreces mac es van substituint.
- En el cas de tenir entrega directa podem veure que el datagrama no s'encamina, i que, per tant, el TTL no es decrementa.
- Tots els hosts tenen connexió a Internet. Si executem un ping cap a una IP d'Internet i observem el tràfic en la xarxa B i la xarxa C, es pot veure com actua el protocol NAT, i com les adreces s'han substituït perquè els datagrames puguin viatjar a través d'Internet.
- Si fem un ping a un host que no existeix podrem observar el ICMP host unreachable.

5.1.1 Disseny dels hosts

S'ha escollit el VPCS que ens subministra la mateixa app GNS3 per defecte, per tant, no és necessari l'ús d'imatges addicionals. Aquest simulador de PC Virtual ocupa només 2MB de RAM, la qual cosa ens permetrà tenir més host executant-se a l'hora. S'utilitza una consola que simula una terminal, creada per defecte mitjançant Telnet. I disposem de totes les funcions necessàries com l'assignació manual de la IP, la utilització de DHCP, l'execució de les eines ping i traceroute, com la possibilitat de guardar les configuracions.[6]

Hi ha altres tipus d'imatge que es poden trobar en el MarketPlace són Windows, macOS, Ubuntu, Kali, Ubuntu, CentOS entre altres. Les quals ens permeten simular els seus sistemes operatius, en aquests casos s'ocupa més memòria RAM que en el cas de la VPCS, i se'ns requereix la instal·lació de software addicional, com Royal TSX, per poder visualitzar la màquina virtual amb la seva interfície gràfica[7]. En el cas que la implementació d'una topologia més complexa s'hauria d'avaluar la utilització d'alguna d'aquestes màquines, ja que la VPCS podria no ser suficient, però per la topologia anteriorment dissenyada optarem per la VPCS, ja que ens ofereix totes les funcions necessàries, ocupa menys memòria RAM i no requereix la instal·lació de software addicional.

Podem observar la IP i la mascarà assignada a cada Ordinador, en la Figura1. Els Host A i B tenen el router1 configurat com a Gateway per defecte amb la IP 192.168.1.129. El Host D té el router3 amb la IP 192.168.1.193. En el cas del Host C, el router2 és el que s'utilitza per defecte amb la interfície 192.168.1.1, aquest serà l'encarregat d'encaminar els paquets que van cap a la xarxa A i C, ja que el Host C no disposa de taula d'encaminament.

5.1.2 Disseny dels routers

L'actual versió de GNS3 2.2.38 no subministra cap imatge de router, així que s'ha de subministrar i baixar l'appliance corresponent. S'ha escollit el router MikroTik CHR (versió 7.7)[8], ja que està disponible per la majoria de hipervisors, i la imatge és subministrada per GNS3 tenint una compatibilitat total i sense necessitat d'obtenir cap llicència. L'altre principal competidor que és Cisco, també disposa d'appliance, però la imatge del dispositiu ha de ser subministrada pel mateix usuari, ja que la mateixa companyia GNS3 no la pot subministrar, en aquest cas pot ser que haguem d'obtenir una llicència VIRL o copiar-la d'un dispositiu físic[9]. S'ha de tenir en compte que Mikrotik no utilitza Linux com a sistema operatiu, sinó Mikrotik-RouterOS, això farà que algunes comandes s'executin de forma diferent.

Perquè tots els hosts tinguin connexió entre ells, i disposin de connexió a Internet se'ls definiran les rutes estàtiques, a partir de les taules d'encaminament, que es mostren en les imatges de la *TAULA 1*, *TAULA 2* i *TAULA 3*. En el cas del Router2, la IP pública de la interfície ether1, i la seva corresponent adreça de xarxa i mascarà, serà obtinguda amb el protocol DHCP, ja que no podem saber aquesta adreça a priori.[10]

Network	Next Hop	Interface
192.168.1.0/25	Direct Delivery	ether1
192.168.1.128/26	Direct Delivery	ether2
192.168.1.192/26	192.168.1.3	ether1
0.0.0.0/0	192.168.1.1	ether1

TAULA 1: LA TAULA D'ENCAMINAMENT DEL ROUTER1.

Network	Next Hop	Interface
192.168.1.0/25	Direct Delivery	ether2
192.168.1.128/26	192.168.1.2	ether2
192.168.1.192/26	192.168.1.3	ether2

TAULA 2: LA TAULA D'ENCAMINAMENT DEL ROUTER2.

Network	Next Hop	Interface
192.168.1.0/25	Direct Delivery	ether1
192.168.1.192/26	Direct Delivery	ether2
192.168.1.128/26	192.168.1.2	ether1
0.0.0.0/0	192.168.1.1	ether1

TAULA 3: LA TAULA D'ENCAMINAMENT DEL ROUTER3.

Cal destacar que per disposar d'accés a Internet per part de tots els ordinadors serà necessària la utilització de NAT en el router2. No es pretén la utilització de servidor DNS, demanarà que per accedir a Internet s'haurà de fer a través de la IP i no del domini.

5.2 Implementació de l'entorn

En el GNS3 s'ha implementat l'entorn mostrat en la *Figura 2*[11]. Com podem veure s'ha utilitzat hubs com a dispositius de la capa física per interconnectar els diferents hosts. El hub, que té una topologia física d'estrella, però la topologia lògica és un bus, i, per tant, no ens permet separar els dominis de col·lisió (com sí que permet un switch), ni tenir diferents dominis de broadcast. En una implementació real, és més segur utilitzar un switch el qual permet separa per interfície. En aquest entorn dedicat a l'aprenentatge de l'assignatura de xarxes, s'ha optat per un hub, ja que ens volem centrar a les capes d'Internet i de Transport, del model TCP/IP. Aquesta implementació, també permetrà visualitzar els camps d'Ethernet, que és el protocol de Capa 1 (Accés al medi) més estudiat a l'assignatura, i que té una àmplia utilització a la vida real. El dispositiu hub no necessita cap configuració, ja que actua com un hub.

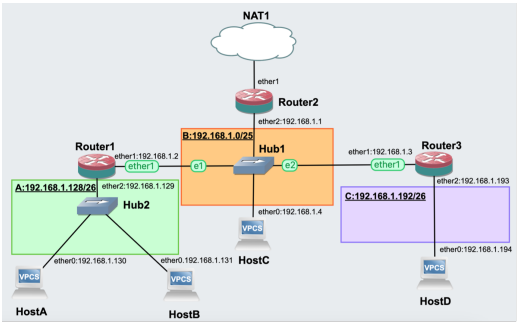

Fig. 2: Entorn implementat en GNS3.

5.2.1 Configuració dels ordinadors

Els ordinadors són de tipus VPCS, les imatges dels quals ja es troben per defecte a GNS3, i no s'ha hagut de descarregar cap mena d'imatges ni afegir l'appliance. Les VPCS només permeten tenir una sola interfície. En el nostre entorn hi trobem 4 ordinadors d'aquest tipus, i seguint la descripció del disseny de l'apartat 5.1.1, hem executat la comanda "ip ip_host mascara ip_gateway"[6]. On la ip_host és la ip que es vol assignar a la interfície ethernet0, seguit de la màscara de xarxa que pertany la interfície, i la IP del gateway, que serà el router on enviarà els paquets per defecte. En el cas del host C, s'ha configurat el router2 per defecte, ja que és el que ens connecta a Internet de forma més directa. Per tant, quan el Host C vulgui connectar-se a una IP de la xarxa A o xarxa C, primer s'enviarà en el router2, el qual s'encarregarà d'encaminar-lo cap el router1 o el router3, respectivament. Les configuracions es poden trobar a l'Annex A.2.1.

5.2.2 Configuració de l'Internet

Perquè els ordinadors tinguin accés a Internet s'ha afegit un node NAT, el qual ens permet connectar la topologia a Internet a través de NAT, però a diferència del node Cloud, aquesta no serà accessible directament des d'Internet o de la LAN local, de manera que és més segur[12].

Aquest node té un servidor DHCP que té el rang 192.168.122.0/24 per defecte. Haurem de tenir en compte aquest fet per configurar la interfície ether1 del router2, el qual haurà de sol·licitar la IP corresponent via dhcp. A més aquest node només farà NAT de la IP del router2, perquè la resta de dispositius de la topologia tinguin accés a Internet, haurem de configurar NAT en el router2, de manera que tots els paquets que surtin per la interfície ether1, del router2, tinguin la IP corresponent a aquesta interfície.

El canvi d'adreces fet a partir de la configuració NAT ha de permetre el canvi d'adreces per la sortida de paquets, però també el canvi en l'entrada dels paquets de resposta. No tenim un servidor DNS, així que l'usuari haurà de subministrar l'adreça IP destí.

5.2.3 Configuració dels routers

GNS3 no ens subministra cap router per fer l'entorn, per tant, s'ha hagut d'instal·lar el seu corresponent appliance i la seva imatge, a través de la web [13][14]. El primer que s'ha configurat és les característiques de les interfícies dels routers, hem assignat el speed a 1Gbps, i la mtu, que per defecte té un valor de 1500 bytes, podrem veure que en el cas del router3 ethernet2, és 576 bytes [15]. Aquesta configuració es troba a "/interface ethernet", i les interfícies ether1 i ether2. Consultar l'Annex A.2.2, per veure l'assignació d'adreces IP per cada interfície.

Seguint les característiques del disseny descrites a l'apartat 5.1.2 s'ha configurat la ip estàtica de les interfícies amb la xarxa corresponent, en l'apartat "/ip address". En el router2, la interfície eth1, no serà definida de forma estàtica, sinó que configurarem el client dhcp en aquesta interfície, perquè la sol·liciti en el node NAT, es pot trobar en l'apartat "/ip dhcp-client". Per configurar la taula Routing, ho hem de fer a l'apartat "/ip route", el qual tindrà totes les routes estàtiques. En el cas de la default route del Router2, tindrà com a gateway la ip del Cloud NAT. Consultar l'AnnexA.2.3, per veure les taules d'encaminament.

En el Router2, hem de configurar NAT, el qual serà de tipus Source NAT [16], que tradueix les direccions IP de la nostra LAN a la IP de la interfície eth1 del mateix router. També realitza la traducció d'adreces de forma automàtica pel tràfic entrant. I permetrem el flux de tràfic, habilitantlo en l'apartat "/ip traffic-flow". Aquesta configuració ens permet fer un ping des de qualsevol host de la xarxa cap a una IP d'Internet, i obtenir la seva resposta. Consultar l'Annex A.2.4 per consultar la configuració NAT.

5.2.4 Configuració de les mtus

Les mtus per defecte són 1500 bytes per la xarxa A i B, i 576 bytes per la xarxa C. Aquestes mtus són implementades a través de les configuració de les interfícies de cada un dels routers. Amb l'objectiu de que els usuaris de la plantilla, puguin experimentar amb diferents fragmentacions i com les mtus afecten a aquests procés, s'ha creat un System Script en els routers perquè l'alumnat pugui canviar de forma ràpida i senzilla la mida de les mtus [17][18]. De manera que definint primer les mtus que volem en variables globals, i després executant el script, les mtus es veuran modificades. En e l'Annex A.2.5 podem observar la configuració del Script i com executar-lo.

5.3 Creació de la plantilla

Per facilitar la utilització de la plantilla per part de l'alumnat, s'ha exportat el projecte, obtenint així un projecte portable. En l'exportació s'han inclòs les imatges dels diferents dispositius, fent que el projecte tingui una mida més grossa, però facilitant la seva utilització, ja que l'usuari no haurà d'instal·lar les imatges dels diferents dispositius[19].

5.4 Configuració del Wireshark

Per visualitzar el tràfic de les diferents xarxes, es pot iniciar la captura en qualsevol dels enllaços de la topologia. El fitxer resultant es guarda a la carpeta "/project-files/captures", el programa ens dona la possibilitat d'escollir el nom del fitxer i poder obrir el Wireshark per poder visualitzar la captura del tràfic en temps real. Per facilitar la visualització dels datagrames fragmentats i els que no, s'ha definit unes normes de coloració, que l'alumnat pot fàcilment importar. De manera que els datagrames no fragmentats es visualitzaran amb un fons blau i lletres de color taronja. Els datagrames que formen part de la fragmentació es visualitzaran amb un fons rosa i lletres grogues. Per la utilització del IO Graphs s'han implementat els filtres equivalents, de manera que es mostrin els paquets que s'envien fragmentats o no, en 1ms. Podem veure les configuracions en l'Annex A.2.6.

6 RESULTATS

S'han definit una sèrie de test per garantir el correcte funcionament de l'entorn. S'han realitzat captures de pantalla de les comandes executades, i les captures del tràfic en les diferents xarxes.

6.1 Test 1

S'ha executat un ping amb una llargària de 1450 bytes en el Host A cap al Host C, i s'ha capturat el tràfic en les xarxes A i B. S'ha capturat en la xarxa A i xarxa B, i s'observa com els paquets ICMP request i reply no s'han fragmentat en cap moment. Això és el que s'espera, ja que les mtus de les dues xarxes són 1500 bytes, per tant, no s'han de fragmentar. En l'Annex A.3.1 es pot observar els camps de fragmentació IP d'un ICMP request capturat a la xarxa B.

6.2 Test 2

S'ha executat un ping amb una llargària de 1450 bytes en el Host A cap al Host D, i s'ha capturat el tràfic en les xarxes A, B i C. En aquest cas la xarxa A i B tenen configurades les mtus a 1500 bytes, i la xarxa C a 576 bytes. De manera que en la xarxa A i B no s'observa fragmentació, però en la xarxa C, s'observen 3 fragments del datagrama de l'ICMP request. Això, correspon al que esperàvem. També és interessant observar l'ARP, sol·licitant l'adreça mac del host que li correspon la IP 192.168.1.194, i com el host respon a aquesta petició amb la seva adreça mac. Comentar que el missatge ICMP reply, no viatge fragmentat perquè el Host D, que és una VPC té una mtu de 1500 bytes per defecte a la interfície i no s'ha modificat degut a les limitacions d'aquest software. Per tant, el router 3 el rebrà no fragmentat i quan l'encamini cap a la eth1, veurà que la xarxa B té una mtu de 1500 i no el fragmentarà. Per tant, els ICMP reply no es veuran fragmentats en cap de les 3 xarxes. El TTL ens indica els hosts intermedis entre A i D, els paquets s'envien per defecte amb 64, i veiem que quan arriben els ICMP reply el TTL és 62, per tant, hi ha 2 routers en el camí, i això encaixa amb la topologia dissenyada. En l'Annex A.3.2 podem observar els fragments de l'ICMP request i els missatges ARP en la xarxa C.

6.3 Test 3

S'ha executat un ping amb una llargària de 1450 bytes en el Host A cap al Host B, i s'ha capturat el tràfic en les xarxes A. S'observa que els ICMP no s'han fragmentat, i que el TTL és 64, ja que no s'ha encaminat. El host A coneix la xarxa on es troba i a l'enviar al 192.168.1.131, sap que hi ha de tenir entrega directa de manera que ja no l'envia a la Gateway sinó que busca directament la IP del host B. El host A sol·licita la mac del host 192.168.1.131, el qual li respon amb la seva mac. En l'Annex A.3.3 podem observar els datagrames que s'observen en la xarxa A.

6.4 Test 4

S'ha executat un ping amb una llargària de 1450 bytes en al Host A cap a la IP 192.168.1.195, i s'ha capturat el tràfic en les xarxes A, B i C. En la xarxa A i B s'observa l'ICMP request sense fragmentar com que les mtus són 1500 bytes. En la xarxa C no s'observa els ICMP request, sinó que per cada petició s'ha realitzat un ARP preguntant per la mac de la IP 192.168.1.195, no hi ha cap host en aquesta xarxa amb aquesta IP així que ningú respon als missatges ARP, el router 3 al no obtenir resposta, envia un ICMP Destination Unreachable (Host Unreachable) cap al host A, el qual no es fragmentarà en cap moment com que les mtus de la xarxa A i B són 1500 bytes. En l'Annex A.3.4 podem veure els datagrames de la xarxa C i B.

6.5 Test 5

S'ha executat un ping amb una llargària de 1450 bytes en el Host A, C i D, cap a la IP 216.58.215.131, i s'ha capturat el tràfic en les xarxes B i la que ens connecta amb el Cloud NAT. Podem observar que la petició de ping és resposta en tots els casos, i observem com el router2 fa NAT, de manera que tots els ICMP request que s'observen tenen una IP origen corresponent a 192.168.122.151 que és la IP de l'eth1 del router2, aquesta IP també és la de destí dels ICMP reply. En la xarxa B podem observar que les adreces corresponen als hosts que han fet els pings, així que el Router2 està realitzant NAT correctament. En l'Annex A.3.5 podem observar els diferents ICMP observats en la xarxa B i la xarxa Cloud NAT.

6.6 Test 6

S'ha executat traceroute des del Host A cap al D, capturant en la xarxa A, B i C. S'observa com el host A envia un paquet UDP amb TTL=1, i rep un ICMP Time-to-live exceeded procedent del Router1, després envia un paquet UDP amb TTL=2, i rep un ICMP Time-to-live exceeded procedent del Router3, finalment envia un UDP amb TTL=3 que ja és rebut pel Host D. La comanda traceroute ja executat completament. Aquests paquets són observats a la xarxa A. En la xarxa B, s'observen els paquets que el Host A envia amb TTL 2 i 3, quan s'observen en aquesta xarxa els TTLs són 1 i 2 respectivament, ja que el Router 1, ja l'ha decrementat una unitat i els ICMP de resposta corresponents. En la xarxa C només observa l'UDP que envia el Host A amb TTL 3, quan s'observa a la xarxa C el TTL és 1, i veurem l'ICMP de resposta que serà Port Unreachable, ja que el Host D no té el port actiu. En l'Annex A.3.6 podem observar el tràfic capturat.

6.7 Test 7

S'ha canviat la mtu de la xarxa B per 700 bytes, i s'ha realitzat un ping amb una llargària de 1450 bytes des del Host A cap al D, i s'ha capturat el tràfic de xarxa en la A, la B i la C. El ICMP request del host A a la xarxa A, no s'envia fragmentat, ja que la mtu de la xarxa A és 1500 bytes, aquesta ICMP request quan arriba al router1, abans d'enviar-lo per l'eth1 es fragmenta per complir amb la mtu de 700 bytes, el router3 rep els fragments i no els reagrupa, abans d'enviar cada fragment individualment, torna a aplicar la fragmentació per complir amb la mtu de la xarxa C que és 576 bytes. El host D, respon amb un ICMP reply el qual s'envia no fragmentat com que el host D, en ser una VPC no es permet modificar la mtu de la interfície. Aquest paquet el rep el Router2, el qual abans d'enviar-lo per l'eth1 es fragmenta per complir amb la mtu 700 bytes, el router1 els rep i els entrega al Host A, en aquest cas la xarxa A té una mtu de 1500 bytes i, per tant, no requereix més fragmentació. En l'Annex A.3.7 es pot observar els resultats d'aquest test.

6.8 Anàlisi dels resultats

Els resultats dels testos han estat coherents amb els esperats i amb els coneixements teòrics. No s'ha detectat cap mal funcionament durant la simulació.

7 Conclusions

Com s'acaba de comentar, els resultats dels tests realitzats corresponent als esperats. Alhora, són molt comprensibles visualment. Aquests dos factors fan pensar en la utilitat de l'entorn creat com a simulador.

El projecte aporta un entorn de simulació de xarxes focalitzat en Routing IP, pels estudiants de xarxes, on es pot visualitzar la fragmentació, i els diferents protocols que interactuen en la topologia. S'ha complert amb els objectius proposats, tant a nivell de funcionalitat com d'usabilitat, tal i com, podem veure amb els resultats obtinguts.

La metodologia i planificació seguides, s'expliquen anteriorment en aquest mateix article. De forma general es pot dir que s'ha seguit una metodologia Kanban en tot moment, i s'ha dut a terme en el temps planificat, no s'han introduït més tasques ni ampliat el projecte, ja que ja s'han dedicat més hores de les previstes al treball. Sent la introducció de la tasca de redactar un manual d'ús per l'usuari, la modificació més rellevant, respecte a la planificació inicial.

Focalitzant-nos en les línies futures que pot seguir aquest treball, es proposa la configuració d'un servidor remot, el qual exerceixi de servidor GNS3, executant les diferents comandes i allotjant les diferents simulacions. De manera que els alumnes s'hi puguin connectar remotament i no hagin de descarregar el servidor GNS3 en els seus ordinadors, podent utilitzar la interfície del navegador web. Aquest entorn serveix també per observar el comportament del protocol NAT, ARP i DHCP.

Es podria escalar a altres protocols expandint l'entorn o canviant-ne la seva topologia. Una extensió natural seria fonamentar-se en el projecte realitzat per simular TCP, i incloure serveis com la resolució DNS. Per ampliar la interfície gràfica el GNS3 es veu limitat degut a què el protocol per connectar-se al servidor només és http, sent necessari la utilització de VPNs per garantir la seguretat. I dificulta la creació d'una interfície alternativa diferent de la subministrada per GNS3. Es requereix la utilització del Wireshark per visualitzar el tràfic de paquets, ja que l'entorn visualitza les terminals dels diferents nodes executant Telnet, i no integra el Wireshark dins la interfície de l'entorn.

De l'entorn s'espera que ajudi a entendre millor el funcionament del protocol IP i molt particularment de la fragmentació, un dels problemes principals que té l'estudiant de xarxes.

AGRAÏMENTS

Agraeixo al meu tutor del treball de fi de grau Juan Antonio Martinez Carrascal, per haver-me orientat, ajudat i motivat en la realització d'aquest projecte.

REFERÈNCIES

[1] J. Jiménez, ≪Simuladores para virtualizar redes y aprender routing y switching,≫ RedesZone, 20 Gener 2023. [En línia]. Available: https://www.redeszone.net/tutoriales/redes-cable/programas-simular-red/. [Últim accés: 5 Març 2023].

[2] ≪Getting started with GNS3: GNS3 documentation,≫ GNS3 Docs, [En línia]. Available: https://docs.gns3.com/docs/. [Últim accés: 5 Març 2023].

[3] ≪Welcome to API documentation!,≫ GNS3 2.2.38 documentation, [En línia]. Available: https://gns3-server.readthedocs.io/en/stable/. [Últim accés: 5 Març 2023].

[4] E. Caamaño, Project Management Práctico Técnicas, Herramientas y Documentos, España: Deniedbooks, 2016.

[5] J. Edge, Kanban: La guía definitiva de la metodología Kanban para el desarrollo de software ágil, 2018.

[6] GNS3, ≪VPCS,≫ Galaxy Technologies LLC, [En línia]. Available: https://docs.gns3.com/docs/emulators/vpcs/. [Últim accés: 15 Abril 2023].

[7] D. Bombal, ≪GNS3 Talks: Chicken of the VNC, Royal TSX to fix console issues with GNS3 on a Mac,≫ YouTube, 3 Març 2017. [En línia]. Available: https://www.youtube.com/watch?v=n3b7_d8EQII. [Últim accés: 15 Abril 2023].

[8] J. Duponchelle, ≪MikroTik CHR,≫ GNS3, 7 Gener 2016. [En línia]. Available: GNS3 Talks: Chicken of the VNC, Royal TSX to fix console issues with GNS3 on a Mac. [Últim accés: 1 Abril 2023].

[9] GNS3, ≪Getting Started with GNS3,≫ Galaxy Technologies LLC, [En línia]. Available: https://docs.gns3.com/docs/. [Últim accés: 1 Abril 2023].

[10] D. E. Comer, Internetworking with TCP/IP Principles, Protocol, and Architecture, Vols. Volume-I, Pearson, 2013.

[11] GNS3, ≪The GNS3 GUI,≫ Galaxy Technologies LLC, [En línia]. Available: https://docs.gns3.com/docs/using-gns3/beginners/the-gns3-gui/. [Últim accés: 16 Abril 2023].

[12] GNS3, ≪The NAT node,≫ Galaxy Technologies LLC, [En línia]. Available: https://docs.gns3.com/docs/using-gns3/advanced/the-nat-node/. [Últim accés: 1 Abril 2023].

[13] GNS3, ≪Marketplace,≫ SolarWinds Worldwide, LLC, [En línia]. Available: https://gns3.com/marketplace/appliances. [Últim accés: 1 Abril 2023].

[14] GNS3, ≪Import GNS3 appliance,≫ Galaxy Technologies LLC, [En línia]. Available: https://docs.gns3.com/docs/using-gns3/beginners/import-gns3-appliance. [Últim accés: 1 Abril 2023].

[15] mikrotik, ≪RouterOS - Getting started - First Time Configuration,≫ Atlassian Confluence, [En línia]. Available: https://help.mikrotik.com/docs/display/ROS/First+Time+Configuration. [Últim accés: 16 Abril 2023].

[16] a. xperts, ≪Capítulo 3.5 – Source NAT,≫ abcxperts.com, [En línia]. Available: https://abcxperts.com/docs/capitulo-3-5-source-nat/. [Últim accés: 1 Abril 2023].

[17] ≪Manual:Scripting,≫ MikroTik, 9 Setembre 2020. [En línia]. Available: https://wiki.mikrotik.com/wiki/Manual:Scripting#Variables. [Últim accés: 7 Maig 2023].

[18] ≪Manual:Scripting-examples,≫ MikroTik, 18 Octubre 2017. [En línia]. Available: https://wiki.mikrotik.com/wiki/Manual:Scripting-examples. [Últim accés: 7 Maig 2023].

[19] D. Bombal, ≪GNS3 Talks: GNS3 2.0 Portable Projects - easily export and import GNS3 projects,≫ YouTube, 8 Març 2017. [En línia]. Available: https://www.youtube.com/watch?v=DfjnQNbSUyY. [Últim accés: 7 Maig 2023].

[20] ≪parameters for scripting,≫ mikrotik, 7 Febrer 2007. [En línia]. Available: https://forum.mikrotik.com/viewtopic.php?f=9&t=23041. [Últim accés: 7 Maig 2023].

[21] «run script from terminal,» MikroTik, 28 Maig 2014. [En línia]. Available: https://forum.mikrotik.com/viewtopic.php?t=3294. [Últim accés: 7 Maig 2023].

ANNEX

A.1 Diagrama de Gantt

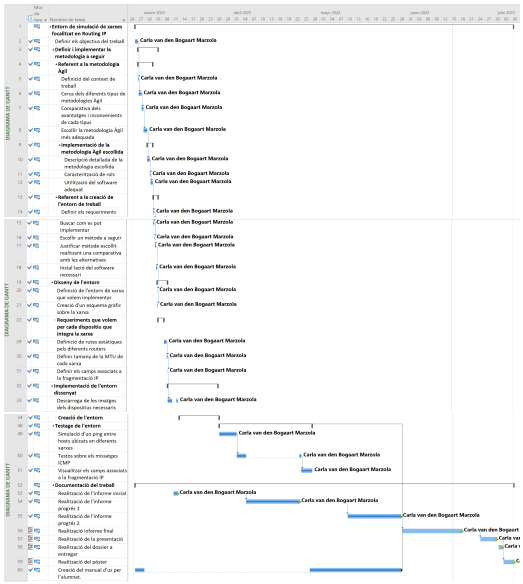

Fig. 3: Diagrama de Gantt.

A.2 Configuracions dels Hosts

A.2.1 Configuracions ordinadors

```
VPCS> show

NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
VPCS1  192.168.1.130/26     192.168.1.129     00:50:79:66:68:00  20066  127.0.0.1:20067
       fe80::250:79ff:fe66:6800/64
```

Fig. 4: Configuració HostA.

```
VPCS> show

NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
VPCS1  192.168.1.131/26     192.168.1.129     00:50:79:66:68:01  20068  127.0.0.1:20069
       fe80::250:79ff:fe66:6801/64
```

Fig. 5: Configuració HostB.

```
VPCS> show

NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
VPCS1  192.168.1.4/25       192.168.1.1       00:50:79:66:68:02  20070  127.0.0.1:20071
       fe80::250:79ff:fe66:6802/64
```

Fig. 6: Configuració HostC.

```
VPCS> show

NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
VPCS1  192.168.1.194/26     192.168.1.193     00:50:79:66:68:03  20072  127.0.0.1:20073
       fe80::250:79ff:fe66:6803/64
```

Fig. 7: Configuració HostD.

A.2.2 Configuracions adreces IPs dels routers

```
[admin@Router1] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS            NETWORK         INTERFACE
0 192.168.1.2/25     192.168.1.0     ether1
1 192.168.1.129/26   192.168.1.128   ether2
```

Fig. 8: Taula d'adreces de les interfícies del Router1.

```
[admin@Router2] > /ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS              NETWORK         INTERFACE
0   192.168.1.1/25       192.168.1.0     ether2
1 D 192.168.122.151/24   192.168.122.0   ether1
```

Fig. 9: Taula d'adreces de les interfícies del Router2.

```
[admin@Router3] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS            NETWORK         INTERFACE
0 192.168.1.3/25     192.168.1.0     ether1
1 192.168.1.193/26   192.168.1.192   ether2
```

Fig. 10: Taula d'adreces de les interfícies del Router3.

A.2.3 Configuracions taules d'encaminament dels routers

```
[admin@Router1] > /ip route print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY        DISTANCE
0  As  0.0.0.0/0          192.168.1.1           1
   DAc 192.168.1.0/25     ether1                0
   DAc 192.168.1.128/26   ether2                0
1  As  192.168.1.192/26   192.168.1.3           1
```

Fig. 11: Routing table del Router1.

```
[admin@Router2] > /ip route print
Flags: D - DYNAMIC; A - ACTIVE; c, s, d, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY        DISTANCE
   DAd 0.0.0.0/0          192.168.122.1         1
   DAc 192.168.1.0/25     ether2                0
0  As  192.168.1.128/26   192.168.1.2           1
1  As  192.168.1.192/26   192.168.1.3           1
   DAc 192.168.122.0/24   ether1                0
```

Fig. 12: Routing table del Router2.

```
[admin@Router3] > /ip route print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY        DISTANCE
0  As  0.0.0.0/0          192.168.1.1           1
   DAc 192.168.1.0/25     ether1                0
1  As  192.168.1.128/26   192.168.1.2           1
   DAc 192.168.1.192/26   ether2                0
```

Fig. 13: Routing table del Router3.

A.2.4 Configuració taula NAT del Router2

```
[admin@Router2] > /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=src-nat to-addresses=192.168.122.151 src-address=192.168.1.0/24 out-interface=ether1
```

Fig. 14: Configuració NAT Router2.

A.2.5 Configuració de les mtus

```
[admin@Router3] > /system script print
Flags: I - invalid
 0   name="change_mtu" owner="admin"
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
     dont-require-permissions=no run-count=0 source=

       :global mtu1;
       :global mtu2;
       /interface ethernet set [ find default-name=ether2 ] disable-running-check=no mtu=$mtu2 speed=1Gbps
       /interface ethernet set [ find default-name=ether1 ] disable-running-check=no mtu=$mtu1 speed=1Gbps
```

Fig. 15: Configuració del System Script per modificar les mtus.

```
[admin@Router3] > :global mtu1 422
[admin@Router3] > :global mtu2 255
[admin@Router3] > /system script run change_mtu
[admin@Router3] > /interface ethernet print
Flags: R - RUNNING
Columns: NAME, MTU, MAC-ADDRESS, ARP
#    NAME      MTU   MAC-ADDRESS         ARP
0 R  ether1    422   0C:CE:02:F5:00:00   enabled
1 R  ether2    255   0C:CE:02:F5:00:01   enabled
2    ether3   1500   0C:CE:02:F5:00:02   enabled
3    ether4   1500   0C:CE:02:F5:00:03   enabled
4    ether5   1500   0C:CE:02:F5:00:04   enabled
5    ether6   1500   0C:CE:02:F5:00:05   enabled
6    ether7   1500   0C:CE:02:F5:00:06   enabled
7    ether8   1500   0C:CE:02:F5:00:07   enabled
```

Fig. 16: Canvi de les mtus.[20][21]

A.2.6 Configuració del Wireshark

Fig. 17: Definició de les normes de coloració.

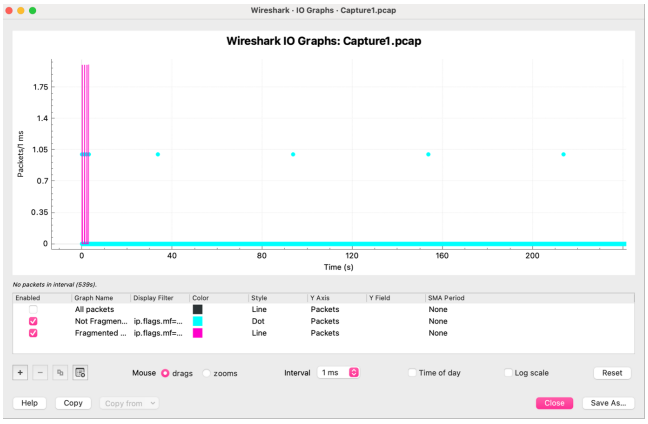

Fig. 18: Utilització del IO Graphs per mostrar els datagrames fragmentats i els que no ho són.

A.3 Resultats del Test

A.3.1 Test 1

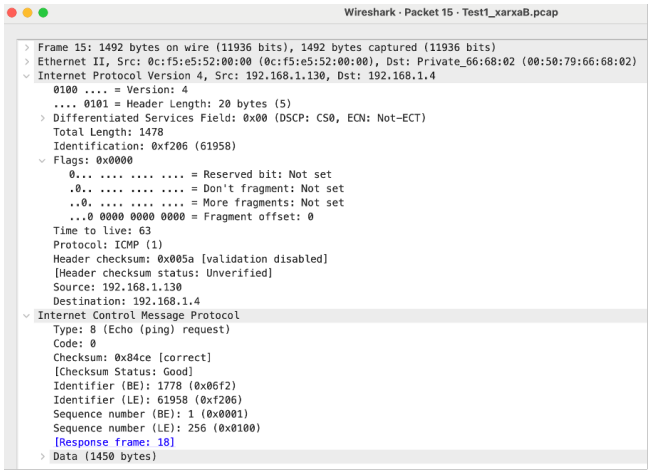

Fig. 19: ICMP request camp de fragmentació en la xarxa B.

A.3.2 Test 2

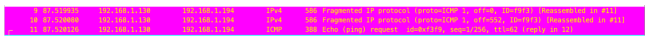

Fig. 20: ICMPs request en la xarxa C.

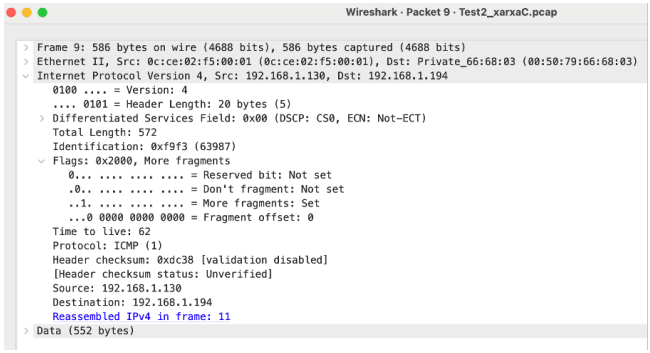

Fig. 21: ICMP request camp de fragmentació en la xarxa C fragment 1.

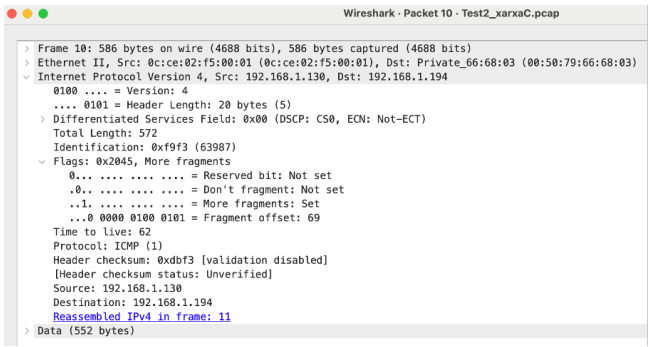

Fig. 22: ICMP request camp de fragmentació en la xarxa C fragment 2.

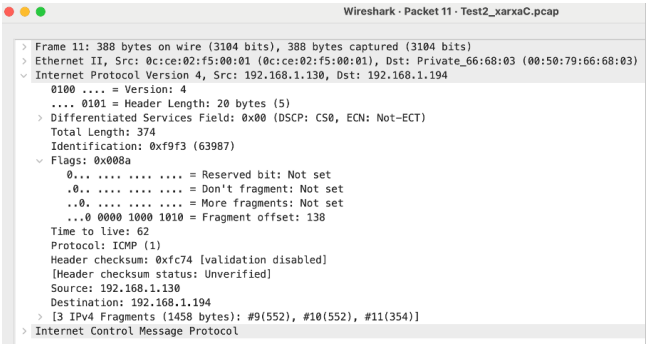

Fig. 23: ICMP request camp de fragmentació en la xarxa C fragment 3.

Fig. 24: Missatges ARP en la xarxa C.

A.3.3 Test 3

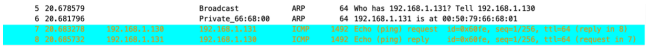

Fig. 25: Datagrames observats en la xarxa A.

A.3.4 Test 4

Fig. 26: Datagrames observats en la xarxa C.

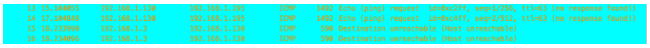

Fig. 27: Datagrames observats en la xarxa B.

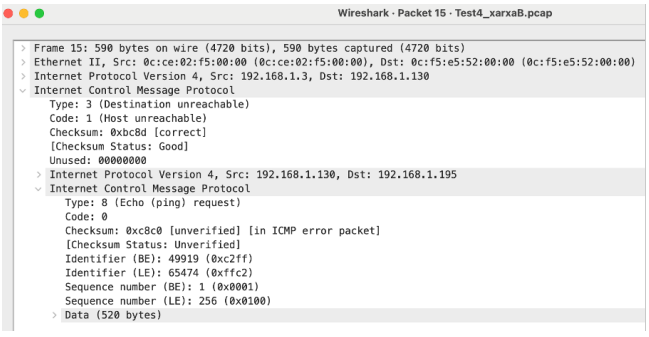

Fig. 28: ICMP Destination Unreachable.

A.3.5 Test 5

Fig. 29: ICMPs observats en la xarxa B del ping del Host A.

Fig. 30: ICMPs observats en la xarxa B del ping del Host C.

Fig. 31: ICMPs observats en la xarxa B del ping del Host D.

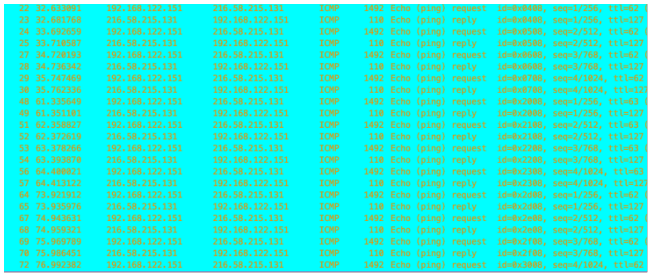

Fig. 32: ICMPs observats en la xarxa Cloud NAT.

A.3.6 Test 6

```
VPCS> trace 192.168.1.194
trace to 192.168.1.194, 8 hops max, press Ctrl+C to stop
 1   192.168.1.129   1.953 ms  1.372 ms  0.996 ms
 2   192.168.1.3     3.280 ms  3.725 ms  3.401 ms
 3   *192.168.1.194   11.630 ms (ICMP type:3, code:3, Destination port unreachable)
```

Fig. 33: Resultat d'executar la comanda Traceroute des del Host A cap el D.

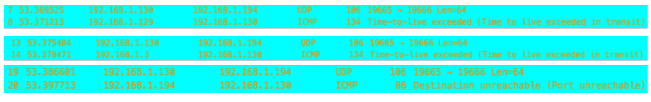

Fig. 34: Datagrames observats en la xarxa A.

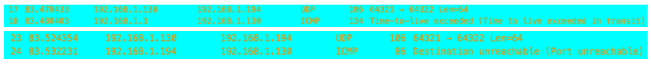

Fig. 35: Datagrames observats en la xarxa B.

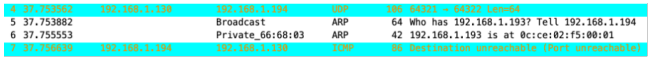

Fig. 36: Datagrames observats en la xarxa C.

A.3.7 Test 7

```
[admin@Router1] > :global mtu1 700
[admin@Router1] > :global mtu2 1500
[admin@Router1] > /system script run change_mtu
[admin@Router1] > /interface ethernet print
Flags: R - RUNNING
Columns: NAME, MTU, MAC-ADDRESS, ARP
#    NAME      MTU   MAC-ADDRESS         ARP
0 R ether1     700   0C:F5:E5:52:00:00   enabled
1 R ether2    1500   0C:F5:E5:52:00:01   enabled
2   ether3    1500   0C:F5:E5:52:00:02   enabled
3   ether4    1500   0C:F5:E5:52:00:03   enabled
4   ether5    1500   0C:F5:E5:52:00:04   enabled
5   ether6    1500   0C:F5:E5:52:00:05   enabled
6   ether7    1500   0C:F5:E5:52:00:06   enabled
7   ether8    1500   0C:F5:E5:52:00:07   enabled
```

Fig. 37: Configuració de les interfícies del Router1.

```
[admin@Router3] > :global mtu1 700
[admin@Router3] > :global mtu2 576
[admin@Router3] > /system script run change_mtu
[admin@Router3] > /interface ethernet print
Flags: R - RUNNING
Columns: NAME, MTU, MAC-ADDRESS, ARP
#    NAME      MTU   MAC-ADDRESS         ARP
0 R ether1     700   0C:CE:02:F5:00:00   enabled
1 R ether2     576   0C:CE:02:F5:00:01   enabled
2   ether3    1500   0C:CE:02:F5:00:02   enabled
3   ether4    1500   0C:CE:02:F5:00:03   enabled
4   ether5    1500   0C:CE:02:F5:00:04   enabled
5   ether6    1500   0C:CE:02:F5:00:05   enabled
6   ether7    1500   0C:CE:02:F5:00:06   enabled
7   ether8    1500   0C:CE:02:F5:00:07   enabled
```

Fig. 38: Configuració de les interfícies del Router3.

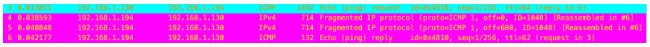

Fig. 39: Datagrames capturats a la xarxa A.

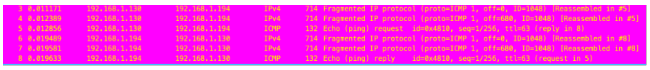

Fig. 40: Datagrames capturats a la xarxa B.

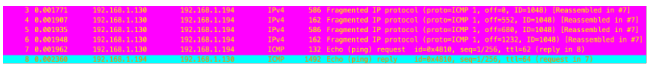

Fig. 41: Datagrames capturats a la xarxa C.