Universitat Oberta de Catalunya

Modelatge i Simulació de quatre centres de processament de dades connectats per WAN.

Memòria

Estudiant: Marc Benito Monllor
Tutors: Alberto García Villoria
Àngel Alejandro Juan Pérez

27 de diciembre de 2012

Índex

Índex Il·lustracions

1 Dedicatòria i agraïments

Aquest projecte és una adaptació d'un projecte real, gestionat per per l'empresa Telesistemes S.A, la qual ha proporcionat els recursos necessaris per a realitzar aquesta adaptació paral·lela al projecte real.

Així doncs, els meus agraïments van dirigits al meu consultor, Alberto Garcia, el qual ha estat en tot moment amb mi en el seguiment del projecte.

A més a més, vull donar les gràcies a Joel Samper "Responsable Tècnic", per el seguiment i ajuda en l'elaboració de l'adaptació, així mateix, també vull agrair a Jesús Torres "Director Tècnic", l'aprovació i motivació en la realització del projecte.

Finalment v ull agrair a tota la meva familia la comprensió i motivació d'aquests últims anys.

2 Resum

Avui en dia les empreses estan distribuïdes en diferents localitzacions, on aquestes localitzacions habitualment estan dintre del mateix país, però cada cop és més habitual trobar-se empreses amb localitzacions en diversos països inclús en diferents continents. Per aquesta raó, es necessari comunicar aquestes localitzacions per tal de tenir la informació actualitzada i sense redundar, en cas de mitjanes empreses o empreses amb dades poc rellevants, dites connexions no suposen cap inconvenient, però en el cas de Centres de Processament de Dades (CPDs) on la criticitat de les dades és rellevant la seva comunicació ha d'estar correctament dissenyada i verificada per garantir la seguretat de les dades i alhora el temps de resposta d'aquestes comunicacions.

Així doncs, aquest projecte de final de carrera té com a finalitat realitzar un estudi d'aquestes connexions entre CPDs i implementar-les en un entorn de proves real però limitat i alhora també en un entorn virtual de simulació, per tal de simular l'entorn real amb la major exactitud possible i poder supervisar els possibles errors de comunicació i/o de seguretat i millorar-los abans de ser implementats de manera definitiva en l'entorn real.

Per aconseguir-ho es farà un estudi dels diferents protocols de comunicació i de seguretat, així mateix com un estudi del hardware més eficient per al cas que s'estudiarà. Un cop realitzat aquest estudi es realitzarà les configuracions en un entorn de proves amb maquinari real i també amb un entorn de proves virtual a partir de l'eina de simulació OPNET IT Gurú, sent aquest un programari que es pot trobar al mercat i per tant accessible lliurement a tots els usuaris. A més, aquest programari és una potent eina de simulació, amb una llibreria de dispositius amb característiques de components subministrades per els mateixos fabricants.

El projecte es centrarà en l'estudi dels enllaços mitjançant línies WAN entre els diferents CPDs, aportant informació sobre els protocols d'enrutament i seguretat més eficients per tal millorar aquestes connexions per aconseguir uns

temps de resposta òptims sense comprometre la seguretat de les dades que viatgen per aquests enllaços.

Finalment, es realitzarà una comparació entre l'entorn de proves i l'eina de simulació virtual per mostrar els avantatges i inconvenients de cadascuna d'elles, per extreure conclusions de si és necessari o no continuar utilitzant entorns de proves reals.

3 Introducció

Aquest PFC es centrarà en l'estudi de les comunicacions entre 4 CPDs a partir d'enllaços WAN encriptats, centrant-se en els protocols d'enrutament i seguretat més eficients per aquestes connexions amb la finalitat d'aconseguir un temps de resposta dels enllaços acceptable. A més d'una diferenciació del tràfic que ha de sortir per cadascun dels enllaços i la redundància d'aquests.

3.1 Justificació del PFC

Actualment la gran part dels usuaris tenen dades digitalitzades, les quals poden estar en els seus ordinadors personals o bé en xarxes socials, servidors Cloud, oficina de treball, bancs, hospitals, etc. Les quals es troben emmagatzemades en bases de dades o en magatzems de dades.

Aquestes bases de dades o magatzems de dades es troben en CPDs, que tot i que la capacitat i processament de càlcul és molt elevat, molt sovint es necessari distribuir aquestes infraestructures per un cost d'inversió menor, varies oficines dintre del mateix país o bé en diferents països.

En el cas dels CPDs distribuïts és necessari comunicar-los amb una arquitectura capaç de donar suport a tots els serveis que pugui contenir el CPD amb rapidesa, fiabilitat, estabilitat, seguretat i escalabilitat, fent especialment èmfasi en la seguretat, degut a la rellevància de les dades que contenen.

A continuació, l'estudi es farà sobre quatre CPDs distribuïts que s'hauran de comunicar entre ells, els quals dos es troben en un país concretament en Andorra i dos més que estan a França. La comunicació entre els CPDs que estan en el mateix país es realitza de manera directa, és a dir, la teleoperadora ofereix un enllaç de fibra que proporciona una connexió directa entre els dos CPDs, en canvi la comunicació entre els CPDs d'Andorra i de França s'haurà de fer via WAN.

Per tant, la línia d'estudi serà les connexions via WAN entre els diferents CPDs, la qual ha de donar un retard de resposta mínim i una seguretat especialment significativa per la criticitat de les dades, a més d'una diferenciació del tràfic d'aquests CDPs, ja que dos d'ells un d'Andorra i un de França són de producció i els altres dos d'integració, així que el tràfic de producció ha de passar per els enllaços WAN dels firewalls de producció tan l'enviament com la resposta i evitar així un tràfic asimètric, de la mateixa manera que amb els enllaços dels firewalls d'integració, també en cas de caiguda d'un dels firewalls, el CPD que estigui actiu d'un país o d'un altre haurà de similar ambdós tràfics.

Per dur a terme aquesta línia d'estudi es realitzarà un anàlisis dels diferents productes del mercat per tal d'implementar-ho, amb els quals es farà un entorn de proves "maqueta" a nivell real, tot i que l'esforç més rellevant consistirà en el modelatge i simulació d'aquesta infraestructura amb l'eina OPNET i obtenir el major número de dades amb la finalitat d'extreure conclusions sobre el temps de resposta, seguretat, ample de banda, redireccionament dels firewalls i diferenciació dels resultats de l'eina OPNET amb els dels firewalls reals.

3.1.2 Objectius

Aquest projecte de final de carrera consisteix en un projecte real, el qual s'ha extret una part, que consisteix en la modelització i simulació dels diferents enllaços via WAN dels CPDs. Amb la finalitat d'obtenir les suficients dades per tal de millorar i aprovar la seva implementació en producció a partir de l'entorn de proves "maqueta" i l'eina OPNET.

Per tant, els objectius principals de projecte per dur-ho a terme són:

1. Realitzar el disseny i modelització de la infraestructura dels CPDs amb els diferents enllaços, protocols i sistemes de seguretat.
2. Simular el funcionament de les connexions amb l'entorn de proves, simulant els diferents tipus de tràfic, seguretat, retard de la connexió i caiguda d'un o dos firewalls, per estudiar el comportament i millora del mateix si s'escau.
3. Simular el funcionament de les connexions amb l'eina OPNET, simulant els diferents tipus de tràfic, seguretat, retard de la connexió i caiguda d'un firewall, per estudiar el comportament i millora del mateix si s'escau.
4. Amb els resultats i coneixements adquirits poder arribar a formular conclusions sobre els protocols de comunicació i de seguretat, redundància i escalabilitat de la infraestructura, així com la diferenciació dels resultat obtinguts amb l'entorn de proves i l'eina OPNET.

3.1.3 Enfocament i mètode seguit

Per tal de dur a terme els objectius anteriorment plantejats es realitzarà la següent metodologia:

1. **Modelització de la infraestructura.**

   1.1. Estudiar els diferents protocols d'enrutament i de seguretat que proporcionin el millor rendiment i major seguretat.

   1.2. Estudiar els diferents dispositius en el mercat que poden ser vàlids per la implementació.

   1.3. Seleccionar quins punts i/o components de l'arquitectura seran subjecte d'anàlisis.

   1.4. Confeccionar un llistat de proves que hauran de ser superades per la infraestructura, intentant que siguin el més pròxim a la realitat.

2. **Simulació del funcionament de la infraestructura.**

   2.1. Estudiar el hardware escollit i la seva configuració per tal de realitzar l'entorn de proves on es durà a terme la simulació.

   2.2. Estudiar el software OPNET que s'ha escollit per tal de dur ha terme la simulació.

   2.3. Cercar i recopilar informació d'ajuda per al desenvolupament i execució de la simulació.

3. **Conclusions i documentació final.**

   3.1. Comparar els resultat obtinguts i extreure les conclusions amb l'estudi dels mateixos.

   3.2. Amb les dades recollides de l'estudi i amb el treball de simulació realitzat es confeccionarà un informe com a memòria final i una presentació del treball realitzat.

3.1.4 Planificació del projecte

El projecte serà estructurat en 5 fases, el qual s'ha adaptat la metodologia que s'ha descrit en l'anterior apartat amb la planificació temporal que està associada a les fites del PFC ja preestablertes per l'assignatura.

Fases

1. Preliminar.

Es tria un projecte a dur a terme, en el qual es determinaran i es concretaran uns objectius per al PFC. Així mateix es confeccionarà un pla de treball per a la realització del PFC el qual es lliurarà en la PAC 1.

2. Modelització de la infraestructura.

En aquesta fase es realitzarà l'estudi dels diferents protocols d'enrutament i de seguretat de la infraestructura, així mateix es realitzarà un estudi paral·lel dels diferents dispositius que hi ha al mercat que poden dur a terme aquest projecte. Un cop aquest dos punts estiguin resolt es realitzarà el disseny de les comunicacions. Al mateix temps s'anirà el·laborant simultàniament un esborrany de la memòria que serà lliurada en la PAC 2.

3. Simulació del funcionament de l'entorn de proves "maqueta".

En aquesta fase es realitzarà la simulació de la infraestructura de comunicació dintre de l'entorn de proves real, on es farà un estudi del seu funcionament i un cop finalitzat aquest estudi es durà a terme la simulació amb el model construït amb la finalitat d'analitzar els resultats obtinguts.

4. Simulació del funcionament amb l'eina OPNET

Aquesta fase es realitzarà simultàniament amb la fase 3, on es realitzarà la simulació de la infraestructura de comunicació amb l'eina OPNET, on es farà un estudi del seu funcionament i un cop finalitzat aquest estudi es durà a terme la

simulació del model construït dins d'aquest entorn per analitzar els resultats obtinguts. Al mateix temps i en paral·lel s'elaborarà una versió avançada de la memòria que serà lliurada amb la PAC 3.

5. Conclusions i documentació final.

Un cop finalitzades les anteriors fases, s'obtindran una serie de conclusions, arxius de configuració i arxius de simulació que quedaran documentats de forma detallada en la memòria juntament amb una presentació de tot el treball elaborat. Al mateix temps es farà l'entrega d'aquest projecte en el lliurament de la PAC 4.

Identificació dels riscos.

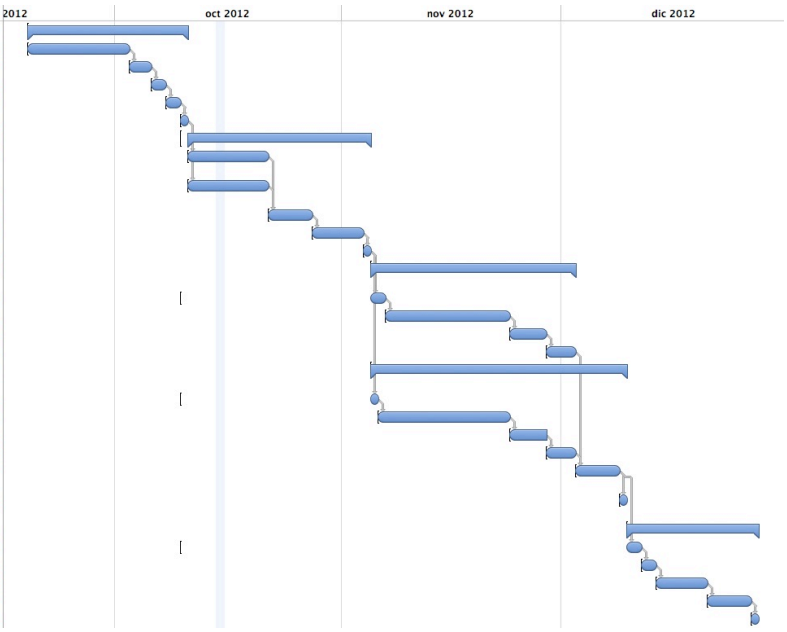
En l'elaboració del Pla de Treball s'han identificats els següents riscos que s'hauran de tindre en compte en l'elaboració del projecte:

- Una estimació errònia del temps en l'execució de les diferents tasques descrites, degut a la inexperiència i petits contratemps no tolerats des d'un principi.
- Limitacions de l'eina OPNET per tal de realitzar aquesta simulació amb la versió gratuïta.

Per tant, per tal d'evitar aquest riscos s'anirà realitzant de manera acurada cadascuna de les fases dintre del temps preestablert per tal de si apareix algun contratemps hi hagi temps suficient per solucionar-ho, tan mateix s'han buscat alternatives a l'eina OPNET gratuïta per si les limitacions d'aquesta versió no permeten realitzar la simulació.

Calendari de Treball.

Título	Inicio	Fin	Duración
1) Preliminar	19/09/12	10/10/12	22d
1.1) Elecció de projecte	19/09/12	02/10/12	14d
1.2) Redactar Esborrany Pla de Projecte	03/10/12	05/10/12	3d
1.3) Esborrany Temporització	06/10/12	07/10/12	2d
1.4) Finalització Pla de Treball	08/10/12	09/10/12	2d
1.5) PAC 1 – Entregar Pla de Treball	10/10/12	10/10/12	1d
2) Modelització de la infraestructura	11/10/12	04/11/12	25d
2.1) Cerca d'informació dels diferents protocols	11/10/12	21/10/12	11d
2.2) Estudi dels diferents dispositius que hi ha al mercat	11/10/12	21/10/12	11d
2.3) Modelització	22/10/12	27/10/12	6d
2.4) Elaboració esquema de memòria	28/10/12	03/11/12	7d
2.5) PAC 2 – Entregar Esquema de memòria	04/11/12	04/11/12	1d
3) Simulació del funcionament de l'entorn de proves	05/11/12	02/12/12	28d
3.1) Construcció de l'entorn de proves	05/11/12	06/11/12	2d
3.2) Configuració dels diferents dispositius	07/11/12	23/11/12	17d
3.3) Simulació	24/11/12	28/11/12	5d
3.4) Anàlisis dels Resultats	29/11/12	02/12/12	4d
4) Simulació del funcionament amb l'eina OPNET	05/11/12	09/12/12	35d
4.1) Instal·lació eina OPNET	05/11/12	05/11/12	1d
4.2) Aprenentatge i configuració de l'eina	06/11/12	23/11/12	18d
4.3) Simulació	24/11/12	28/11/12	5d
4.4) Anàlisis dels Resultats	29/11/12	02/12/12	4d
4.5) Elaboració versió avançada de la memòria	03/12/12	08/12/12	6d
4.6) PAC 3 – Entregar versió avançada de la memòria	09/12/12	09/12/12	1d
5) Conclusions i Documentació Final	10/12/12	27/12/12	18d
5.1) Comparació dels Resultats	10/12/12	11/12/12	2d
5.2) Elaboració de conclusions	12/12/12	13/12/12	2d
5.3) Elaboració versió final memòria	14/12/12	20/12/12	7d
5.4) Elaboració Presentació	21/12/12	26/12/12	6d
5.5) PAC 4 – Entrega Versió Final	27/12/12	27/12/12	1d



Il·lustració 1 Schedule pla de treball

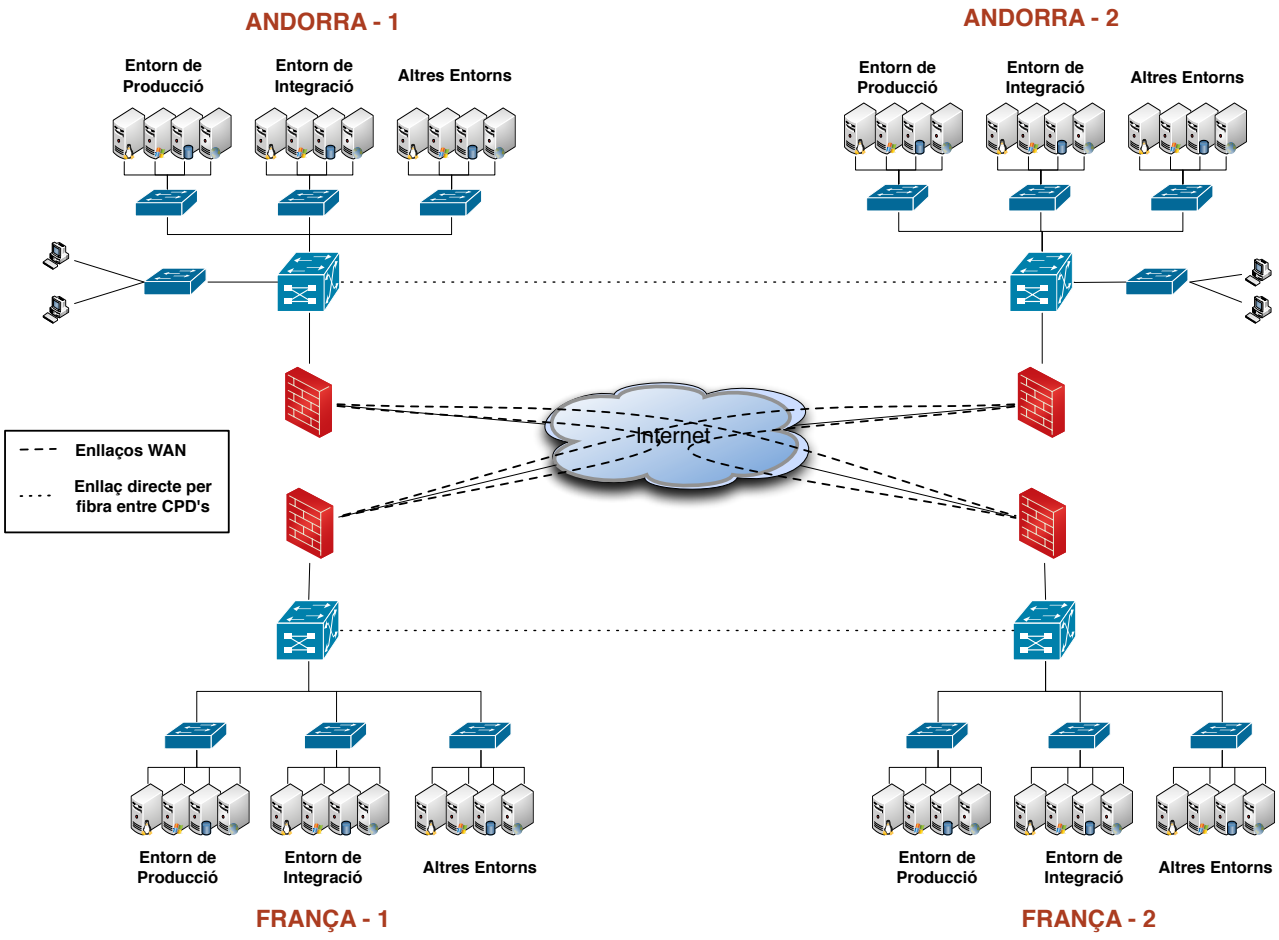
3.1.5 Productes Obtinguts

Els productes obtinguts amb aquest projecte de final de carrera serà una sèrie d'arxius amb les configuracions dels dispositius i un modelatge d'una part de la infraestructura, que anirà d'un model senzill a un model més complex, on es realitzaran una Simulació d'Esdeveniments Discrets (DES). El producte resultant d'aquest projecte serà un model totalment escalable i fiable dels enllaços i una comparació de la simulació a partir d'entorns de proves físics envers als virtuals.

4 Esquema del Sistema

Els quatre centres de processament de dades es troben distribuïts de manera física. Exactament hi ha dos centres de processament de dades a Andorra i uns altres dos centres de processament de dades a França. Els CPDs que estan situats dintre del mateix país la tele-operadora ha proporcionat un enllaç directe entre els 2 CPDs per fibra òptica sense la necessitat d'utilitzar la xarxa WAN.

En canvi, per tal d'unir els CPDs entre els dos països, no es pot realitzar una connexió directa, per lo que s'ha d'utilitzar la xarxa WAN, com es mostra en la següent topologia:

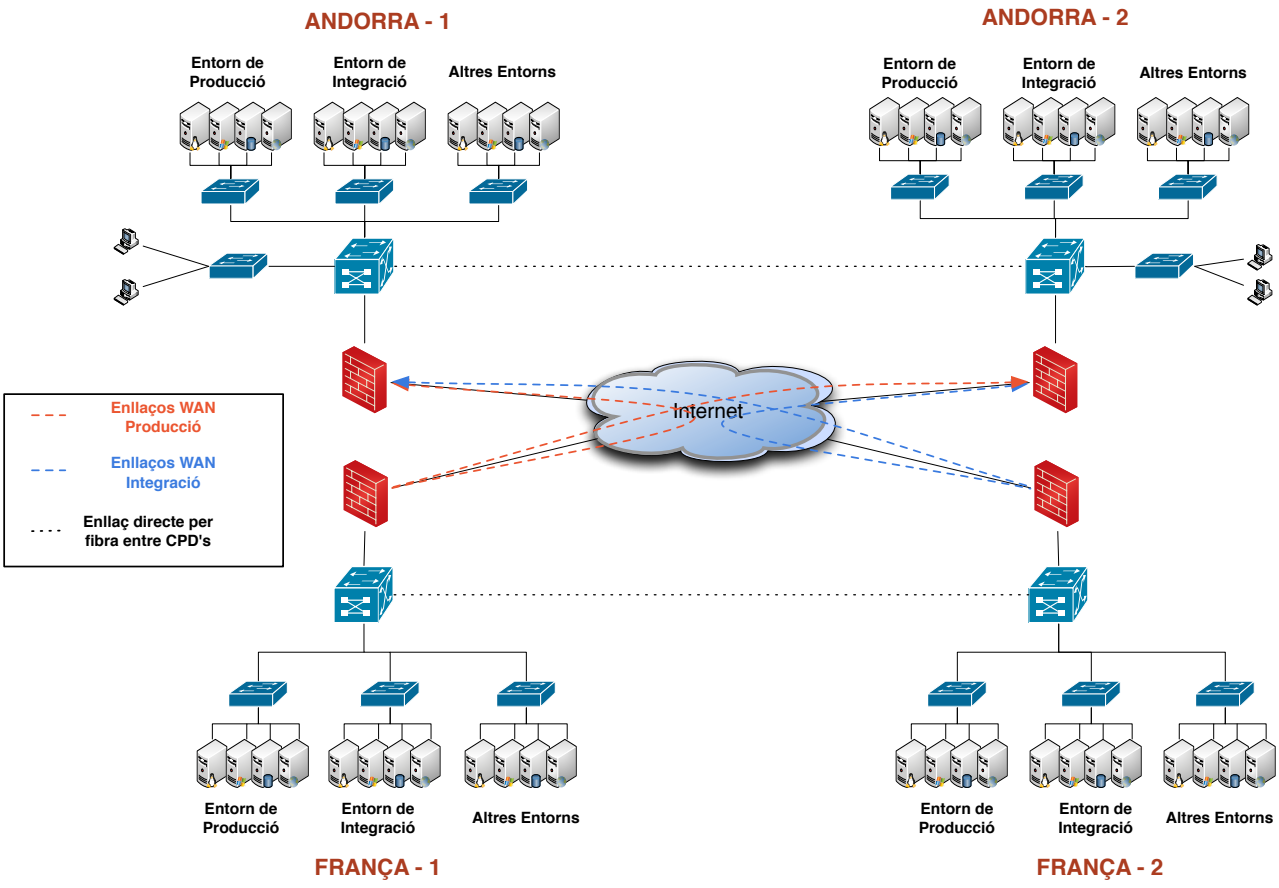


Il·lustració 2 Topologia inicial de la infraestructura

A partir de la il·lustració anterior podem observar com en cada un dels CPDs tenim varis entorns, en el nostre cas volem discriminar el tràfic generat per l'entorn de producció i integració en els CPDs de França, els quals faran ús dels enllaços WAN.

Aquesta discriminació es realitza per tal de no tenir tràfic asimètric i així destinar cadascun dels firewalls a un trafic en concret.

Si ens localitzem en els CPDs de França el tràfic seria gestionat tal i com es representa en la següent il·lustració:



Il·lustració 3 Topologia en detall dels enllaços WAN - França

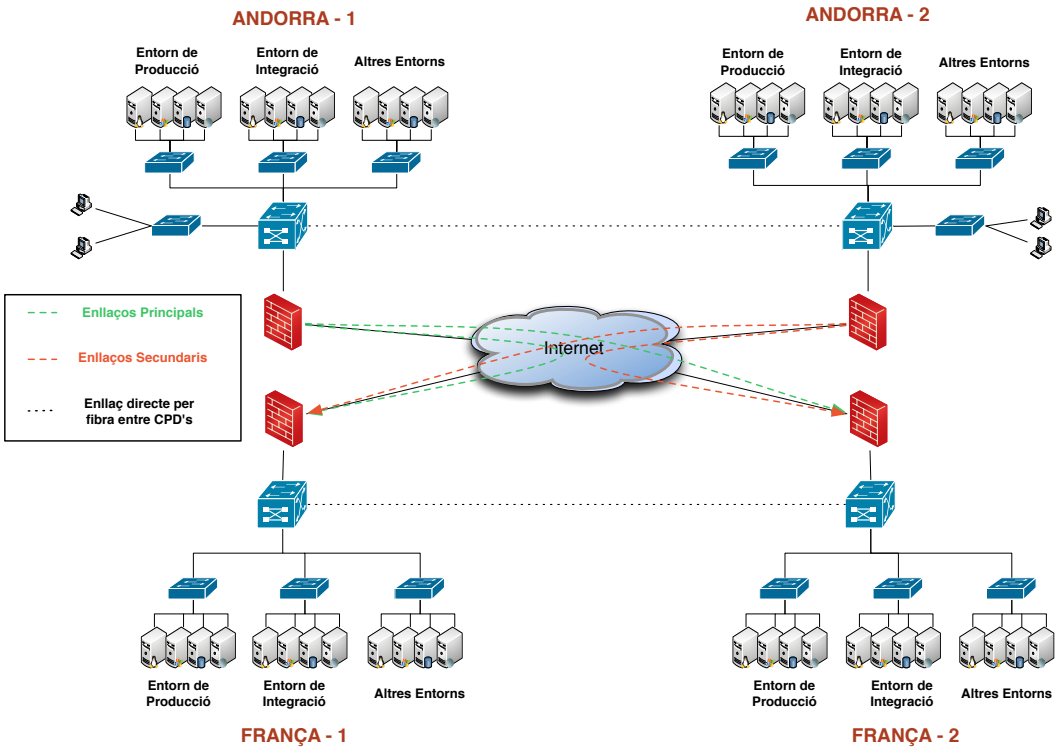
Com s'observa en la il·lustració anterior es veu com el tràfic de producció generat per els CPDs de França s'envia al CPD de Andorra - 1 o de Andorra -

2 a partir del firewall situat a França - 1. Amb aquest objectiu, s'aconsegueix que tot el tràfic generat per els servidors de producció en França, el seu flux sigui administrat preferentment per el firewall de França - 1, si aquest està actiu.

En canvi, el tràfic d'integració tal i com es mostra en la figura anterior, s'envia als CPDs de Andorra - 1 o Andorra - 2 mitjançant el firewall de França - 2, és a dir, el flux de tràfic d'integració generat per els servidors de França estarà gestionat per el firewall de França - 2 si està actiu.

D'aquesta manera, s'aconsegueix descriminar el tràfic de producció i d'integració en els CPDs de França de manera simètrica[1], és a dir, el flux de tràfic de producció entrant i sortint serà gestionat per el firewall de França - 1, i el tràfic d'integració serà gestionat per el firewall de França - 2.

D'altra Banda, si ens localitzem en els CPDs d'Andorra el tràfic seria gestionat tal i com es representa en la següent il·lustració:



Il·lustració 4 Topologia en detall dels enllaços WAN - Andorra

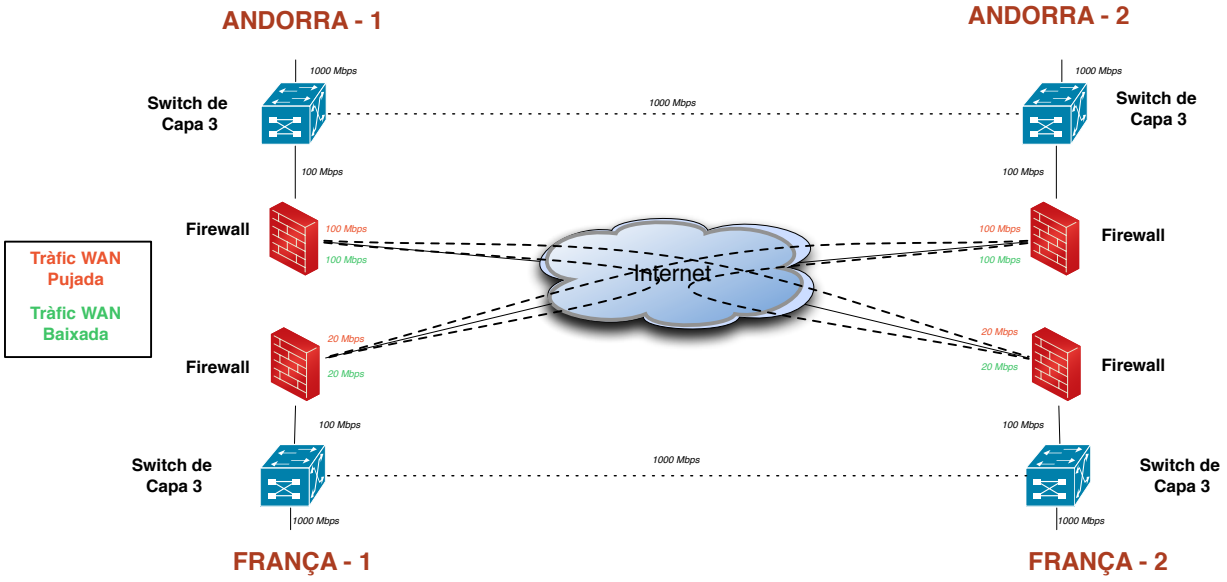
[1] Per defecte els firewalls, no toleren el tràfic asimètric, és a dir, un tràfic entrant per un firewall i la seva resposta sortint per un altre firewall ocasionaria errors, sinó es que es creen regles per tal d'assimilar-ho. Per tant, el gestionament ideal del flux és que sigui simètric.

Com s'observa en l'anterior topologia el gestionament del tràfic en Andorra és molt diferent, en aquest cas, el firewall d'Andorra - 1 és el firewall primari, és a dir, serà l'encarregat de gestionar tot el tràfic independentment de si és de producció o d'integració. I només s'activarà el firewall d'Andorra - 2, en el cas de que el firewall d'Andorra - 1 estigui no operatiu o els enllaços amb els altres firewalls estiguin caiguts, assumint tot el gestionament del firewall d'Andorra - 1 fins que aquest torni a estar operatiu. El que s'aconsegueix un tràfic simètric gestionat per un sol firewall sense discriminació del flux, recolzat per un segon firewall.

Finalment, en el cas de França, si un dels dos firewalls es troba no operatiu, o els seus enllaços caiguts, el flux del tràfic d'aquest firewall serà assumit per el que estigui operatiu. Per exemple, en cas de caiguda del firewall de França - 2, el qual gestiona el tràfic d'integració, el firewall de França - 1 assumiria aquest tràfic.

Per tant, l'objecte d'estudi de la topologia anteriorment detallada seria els quatre firewalls i els quatre switchos de capa 3, els quals seran els encarregats d'establir els enllaços WAN i la distribució del tràfic.

Finalment, podem ampliar l'esquema amb un grau més de detall de l'objecte d'estudi quedant de la següent manera:



Il·lustració 5 Esquema dels elements d'anàlisi

5 Protocols i Tecnologies Objectes d'Estudi

5.1 Protocol d'Enrutament

Els protocols d'enrutament són un conjunt de regles utilitzades per un router quan es comunica amb altres routers amb la finalitat de compartir informació d'enrutament Aquesta informació s'utilitza per construir i mantindre les taules d'enrutament.

En aquest projecte el protocol d'enrutament que s'ha triat és el OSPF la versió 3, ja que de tots els protocols d'enrutament interns és el més utilitzat en arquitectures empresarials a més de ser el més avançat. El qual ens aporta les següents avantatges:

I. **Dinamisme**: OSPF és un protocol dinàmic, qualsevol canvi en la xarxa es detectat i es torna a reestructurar les taules d'enrutament creant les rutes més curtes possibles sense generar cap bucle aconseguint un estat òptim de la xarxa.

II. **Latència**: OSPF funciona a partir de salts, quan més salts ha de realitzar per enviar un paquet, més costos és el seu enviament, per lo que les taules d'enrutament es realitzen amb els costos més baixos per obtenir una menor latència.

III. **Costos**: OSPF també permet manipular els costos de redireccionament d'un paquet, per lo que ens facilita la distribució del tràfic.

IV. **Escalabilitat**: OSPF és un protocol que s'actualitza contínuament, la seva última versió v3, ja incorpora l'enrutament amb IPv6 en el cas de que la infraestructura es quedes sense rang's de IP's IPv4 es podria adaptar fàcilment.

V. **Adaptabilitat**: OSPF també suporta un seguit de tipus d'enllaçaments com: Punt a punt, Punt a Multi-punt, Broadcast, Enllaç virtual i enllaç multiple d'accés, el que ens permet utilitzar-lo en una xarxa en que tingui una heterogeneïtat d'enllaços.

Finalment, com a inconvenient d'aquest protocol es pot destacar el seu increment en l'us de la CPU respecte als altres protocols, el qual és assumit amb facilitat per el hardware que s'utilitzarà en aquest projecte.

5.2 Tecnologia de Virtualització

Una manera de poder discriminar entre els diferents tipus de tràfic es redirigint-los cap a diferents direccions. Una possible manera de fer-ho seria assignant uns equips diferents per a cada tipus de tràfic el que fària que la infraestructura no fos òptima, per això s'utilitzarà la tecnologia VRF "Virtual Routing and Forwarding"

Aquesta tecnologia permet que varies instàncies d'una taula d'enrutament pugui coexistir en el mateix router al mateix temps, és a dir, podem crear taules d'enrutament on diferents direccions redireccionin a una mateixa interficie d'un router o switch.

- **Avantatges**: Amb el mateixos dispositius i sense incrementar l'ús de més ports en els dispositius podem discriminar un tipus de tràfic d'un altre canviat el seu redireccionament, utilitzant els mateixos ports.
- **Inconvenients**: El fet de poder virtualitzar diferents direccions IP's implica un increment en el cost del processament en el redireccionament d'aquest tràfic.

Així doncs, degut als equips hardware que es farà servir és pot utilitzar aquesta tecnologia sense el risc de quedar-se sense recursos de processament.

5.3 Protocol de Redundància

Un dels objectius que s'ha de mantenir en el projecte és la redundància dels equips, en cas de caiguda d'aquest, que un altre assimili el seu comportament de manera immediata i transparent.

Per aquest motiu un dels punts important a estudiar la seva redundància és en els switchos de capa 3 que gestionaran la major part del tràfic que generen els CPDs.

Per proporcionar redundància en aquest equips es farà servir el protocol HSRP "Hot Standby Router Protocol", és un protocol desenvolupat per cisco, que fa que un dels equips estigui actiu i l'altre en espera, si el dispositiu que està en espera no rep el missatge periòdic del router actiu durant 3 cops, aquest assimilarà el tràfic.

Els principals avantatges de fer servir aquest protocol, és que els equips actius poden ser un conjunt d'aquest equips en cluster de la mateixa manera que els equips en espera, el que proporciona una gran versatilitat.

En canvi, com a inconvenient, al ser un protocol propietari de cisco, tan sols pot ser utilitzat en màquines cisco.

No obstant, com els switchos que es fan servir en els CPDs són cisco es pot fer ús d'aquest protocol.

5.4 Protocol de Seguretat

La seguretat dels enllaços es farà a partir de IPsec (Pre-shared key) "Internet protocol security"

El protocol IPsec està dissenyat per un conjunt de protocols criptogràfics per assegurar el fluxe de paquets, garantir l'autenticació mútua entre els routers i establir paràmetres criptogràfics.

A més, IPsec ha estat dissenyat per proporcionar serveis de seguretat com :

- Xifrar el tràfic (De manera que no pugui ser llegit per ningú llevat de les parts a qui va dirigit).
- Validació de la integració (Assegura que el tràfic no estat modificat durant el trajecte).
- Autenticació dels extrems (Assegura que el tràfic prove d'un extrem de confiança).
- Anti-repetició (Protegeix en contra la repetició de la sessió segura) .

6 Hardware Objecte d'Estudi

Dos dels components que es troben en tots quatre CPDs són el switch i el firewall. Aquests components, són l'objecte d'estudi d'aquest projecte, ja que els enllaços i la distribució del tràfic es farà a partir de la configuració i capacitat d'aquest dispositius.

6.1 Firewall

El firewall serà l'encarregat de crear els diferents enllaços via WAN amb els altres dos CPDs. Hi haurà dos firewalls treballant de forma redundant per CPD, així d'aquesta manera, si cau un dels dos, l'altra agafa la funció del primer i la xarxa pot seguir treballant.

Ambdós aparells tenen una llista ordenada de permisos, així com les configuracions dels enllaços WAN.

El firewal que s'utilitzarà per aquest projecte és un Palo Alto PA-2050[2] el qual és un firewall amb unes característiques molt bones, ja que suporta fins a 2000 connexións VPN amb IPsec amb un ample de banda de fins a 300Mbps, poden aplicar 5000 regles de permisos.

Il·lustració 6 Firewall Palo Alto PA

El que permet executar sense cap inconvenient el disseny de comunicació que s'implementarà.

[2] http://www.paloaltonetworks.com/products/platforms/PA-2000_Series.html

6.2 Switch

Darrere de cada un dels firewalls hi haurà un cluster de switchos de capa 3 els quals gestionaran tot el tràfic ja que seran els encarregats de redireccionar el tràfic cap una direcció un altre.

Els switchos que es fan servir per aquest projecte son: cisco catalyst 3750G-PS-E[3] els qual són un switchos potents, capaços de virtualitzar diferents direccions IP's i gestionar aquest tràfic entre els diferents equips de la xarxa. A més aquest switchos, al ser del fabricant Cisco, se'ls pot implementar el protocol HSRP, que permet la seva redundància en cas de fallida d'un dels switchos o cluster de switchos.

Il·lustració 7 Switch Cisco Catalyst 3750G

El que permet executar sense cap inconvenient el disseny de comunicació que s'implementarà en aquest projecte.

[3] http://www.cisco.com/en/US/products/ps7077/prod_models_comparison.html

7 Entorn de proves i la simulació

Els entorns de proves reals, ha estat la manera clàssica de realitzar proves de les noves configuracions o fins i tot dels dissenys de les noves infraestructures de les xarxes. Aquest entorns, normalment es realitzen a partir del hardware que s'utilitzarà per a la nova xarxa i en els cas que sigui una modificació o adició a una xarxa ja creada, s'utilitza equips paral·les exactament iguals als que estan instal·lats on es provaran les noves configuracions.

7.1 Hardware Utilitzat

- Firewall Palo Alto 5050: El PA-5000 Sèries de la pròxima generació de servidors de seguretat està dissenyat per protegir els centres de processament de dades, els grans portals d'Internet de l'empresa i els entorns de proveïdors de serveis, on la demanda de trànsit exigeixen una gran protecció i rendiment sobre les amenaces. Aquestes plataformes d'alt rendiment estan fetes a mida per oferir una protecció empresarial a velocitats de rendiment de fins a 20 Gbps. Ideal tant per al centre de processament de dades i desplegaments de proveïdors de serveis.

A més, la seria PA-5000, no només és un firewall amb regles sobre els ports, sinó que també permet un filtratge per aplicació, analitzant el contingut de cadascun dels paquets. El processament d'aquest aparells es excepcional, ja que constra de més de 40 processadors distribuïts en 4 àrees funcionals.

Les característiques més rellevants són:

10 Gbps	Ample de banda del firewall
5 Gbps	Ampla de banda de prevenció d'amenaces
4 Gbps	Ample de banda de les VPN IPSec
2.000.000	Màxim nombre de sessions alhora
120.000	Màxim de noves connexions per segon
4.000	Túnels VPN IPSec
10.000	Usuaris amb VPN SSL
125	Router virtuals
500	Zones de seguretat
20.000	Màxim nombre de regles

- Switch Cisco Catalyst 5500: El Catalyst 5500 és un dispositiu de gamma alta commutació modular que proporciona l'escalabilitat, la flexibilitat, i la redundància requerida per a la construcció de grans intranets i centre de processament de dades. A més, compta amb 13 ranures i una arquitectura de gigabit Ethernet-ready que escala a més de 50 Gbps amb un rendiment de desenes de milions de paquets.

Les característiques més rellevants són:

2	Unitats de Rack
96	Màxim de ports
32	Ports a 10Gbps
16	Ports fixos SFP
3	Ranures d'expansió fins a 96 ports
1,92 Tbps	Màxim d'Ample de Banda.

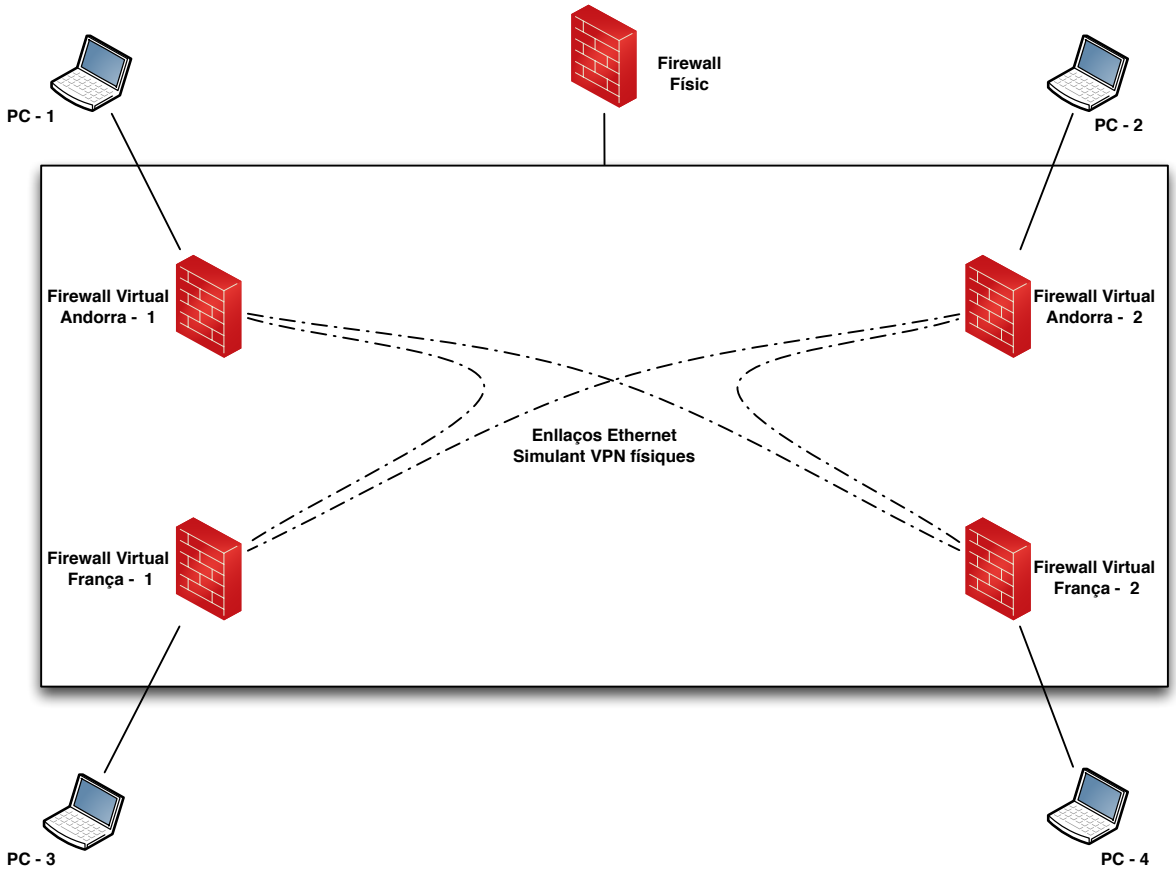
7.2 Esquema de l'entorn de proves

L'entorn de proves s'ha realitzat a partir d'un firewall que són els que estan instal·lats en els quatre centres de processament de dades. Els quals ofereixen la possibilitat de virtualitzar el firewall en 2 equips o més.

Per tant, la simulació ha consistit en dividir aquest firewall en 4, és a dir, assignar com a mínim 3 ports a cada entorn virtual del firewall on aquells 3 o més ports representaria 1 firewall virutal i així successivament fins a tenir els 4.

Un cop tenim aquesta configuració, fem connexions directes punt a punt amb els altres dos firewalls virtuals on 2 dels 3 ports ja queden ocupats. (Exemple: Andorra - 1 --> França - 1 & França - 2) El port restant, és per connectar un Ordinador, el qual realitzarà proves de tràfic, pings, tracert, etc, amb la finalitat de verificar el comportament d'aquesta configuració.

A continuació s'adjunta un esquema de la topologia de l'entorn de proves:



Il·lustració 8 Esquema de l'entorn de proves

7.3 Limitacions de les simulacions

Durant molt de temps les eines de la simulació de les xarxes han estat principalment el maquetatge de la xarxa amb els dispositus bàsics que formen part d'ella amb la finalitat d'estudiar-ne el seu comportatment i garantitzar-ne el el funcionament bàsic, és a dir, amb el màxim possible d'errors depurats i de restriccions analitzades.

Tot i així, al ser un modelatge amb els components bàsics, moltes de les configuracions es realitcen sota postulacions i no han estat verificades en l'entorn de proves, per la qual cosa, les limitacions a partir del modelatge tenen cert punts que no es poden analitzar

A continuació es detallen aquelles limitacions més principals que no es poden verificar en l'entorn de proves real. Les limitacions principals són:

- Anàlisis de la xarxa limitat:

  El maquetatge de l'entorn de proves acostuma a ser bàsic, és a dir, es realitza a partir dels dispositius que són bàsics per al funcionament de la xarxa. Això comporta una disminució dels costos econòmics i temporals, però repercuteix directament en l'anàlisis de la xarxa, en que al ser una xarxa bàsica, el seu comportament és equiparat.

  Per tant les proves que es realitzin dins d'aquest entorn, proporcionaran unes dades limitades, respecte al comportament de la xarxa que s'implementarà realment.

- Fluxe Precari:

  Un altre dels problemes que hi ha en l'entorn de proves real, és el fet de simular tot el flux de tràfic de paquets que faran ús de la xarxa. Aquesta simulació és pràcticament impossible d'aconseguir si la xarxa conté un gran nombre de servidors, balancejadors de càrrega, firewalls, switch, etc.

  Per tant, es realitza la simulació amb un flux de tràfic mínim que garanteix que el tràfic de paquets es realitza correctament i que passen per els punts correctes.

- Poca percepció de les restriccions o colls d'ampolla:

  Com s'ha detallat en l'anterior punt, el flux de tràfic és limitat, ja que si la xarxa conté un gran nombre de dispositius que generin tràfic, no és pot emular. El fet que no es pugui simular un flux de tràfic elevat, suposa que no hi ha una percepció acurada de les restriccions que poden haver en el sistema a més a més els colls d'ampolla que es poden originar en aquells punts de la xarxa on la transmissió de paquets és més lenta.

Per la qual cosa, suposa una limitació que és soluciona a partir de postulacions i experiències prèvies amb altres xarxes.

- Detecció de problemes lleugera:

Un altre limitació originat a partir de la impossibilitat de simular un flux real de les dades, és la detecció de problemes més exhaustiva. Amb un flux de tràfic lleuger que es realitzen en aquestes simulacions, només origina una part dels errors que poden haver-hi, ja que els altres errors, tan sols apareixen quan el tràfic és molt intens, com poden ser en entorns productius.

Per aquesta raó, la detecció de problemes en aquest entorns és lleugera i no garanteix l'absència d'errors en el moment d'implementar-ho en l'entorn real.

- Cost de la simulació elevat:

Un altre inconvenient de les simulacions amb dispositius reals és l'elevat cost d'aquest aparells, i el fet de comprar-ne més aparells per a la realització de l'entorn virtual (Tot i que s'utilitzen com backup en cas que dels principals quedin inutilitzats per qualsevol raó) suposa un augment en el cost econòmic, a més la configuració resulta ser densa i que requereix temps.

Per tant, suposa un increment en els costos econòmics i temporals.

- Impossibilitat de comprovar múltiples dissenys simultàniament:

Un dels inconvenients més importants, és la impossibilitat de comprovar múltiples dissenys simultàniament, ja que, si només disposem d'un entorn de proves (Es poden crear més entorn de proves però suposa un augment molt important en els costos econòmics) tan sols es pot comprovar un model que es desitgi simular, en el cas de voler simular un altre model, s'hauria de guardar els configuracions de l'anterior amb la finalitat de poder recuperar-ho més tard, a més de desar els resultats d'aquest model. Esborrar la configuració dels equips i tornar a configurar

els equips amb la nova versió, realitzar les proves i extreure els resultats i comprar-los amb els del altre model.

Com es pot observar, aquest procediment és molt elevat amb els costos temporals, el qual suposa una limitació important, quan es desitja comprar 2 o més models de xarxa.

- Dades d'anàlisi limitades i costoses:

Finalment, l'última limitació és el fet que les dades d'anàlisis que es poden extreure són molt precàries, normalment les dades que es poden extreure són: El seguiment dels paquets dins la topologia, cost de CPU, taules d'enrutament, ample de banda, retards, paquets perduts "no al 100%) i pocs més.

Aquest fet suposa una limitació, en primer lloc perquè les dades al no simular un flux de tràfic real, no són gaire representatives. Tampoc es pot analitzar acuradament el cost de la CPU, quin es el procés que més cicles consumeix, etc. A més, la pèrdua de paquets no és representativa, ja que el flux és lleuger, en cas d'augment del flux, normalment la pèrdua de paquets augmenta, es pot aproximar quin serà la seves pèrdues per un tràfic més intens, però no saber exactament.

Per la qual cosa, les dades d'anàlisis suposen una limitació, degut a la poca rellevància que se'ls pot donar.

7.4 Avantatges de la simulació amb equips reals

Com hem vist en l'anterior apartat la simulació amb equips reals, té moltes limitacions i proporciona resultats que la seva fiabilitat no és del 100%. Tot i així, la realització de les simulacions amb equips reals ofereix varis avantatges que es tenen de tenir en compte quan es vol simular un entorn de xarxes

Els avantatges principals de la simulació amb equips reals són:

- No hi ha restricció de dispositius:

  Un dels avantatges principals de la realització de les simulacions amb equips reals, és la possibilitat de fer la simulació directament amb l'equip que entrarà en producció, és a dir, que els resultats sobre el seu comportament que s'obtindran d'aquest equip seran exactament els mateixos que quan estigui en l'entorn principal

  Per la qual cosa, fa que sigui molt beneficiosa el extreure resultats directament de les màquines que estaran implementades en l'entorn real.

- Configuracions heterogènies i contacte directe amb els equips:

  Un altre avantatge, és el fet que les configuracions són heterogènies, el que proporciona un coneixement previ a l'usuari encarregat de la configuració, important, ja que en un primer anàlisis a partir de la configuració de cadascun dels equips podrà fer una primera valoració de les limitacions, restriccions i beneficis d'aquest equips.

  A més, el fet de realitzar la configuració en l'entorn de proves amb l'equip real, també, proporcionar coneixement, sobre com s'ha de realitzar aquesta configuració i dels possibles problemes que poden haver-hi. Reduint així, els problemes alhora de implementar-ho en l'entorn principal.

- Configuracions 100% portables als equips principals:

  un dels avantatges més importants de realitzar les configuracions directament en els equips reals, es la compatibilitat de traspassar aquestes configuracions als equips que estan en l'entorn principal.

  Com els equips de la simulació, són exactament els mateixos, la configuració es pot guardar en un fitxer i carregar-li directament a l'equip que està en l'entorn principal, sense haver-hi cap problema, ja que són 100% compatibles.

  Aquest punt és un avantatge important, ja que redueix el temps en la implementació de les noves configuracions en els entorns que ja estan en producció.

7.5 Descripció detallada de la configuració del Firewall

En aquest apartat, es farà una breu descripció amb algunes mostres de la configuració dels firewall real. En aquest cas, tan sols s'ha agafat la mostra de Andorra - 1 amb la finalitat de simplificar la documentació, ja que les altres 7 restants, són exactament igual tan sols es modifiquen les IPs.

Com es podrà observar en el cas de les VPN, es configura 8. Ja que, les peticions poden ser de Andorra - 1 a França - 1 o viceversa. Per tant, de 4 enllaços, hi ha 8 túnels. Es per aquest motiu, que en l'entorn real, parlarem de 8 configuracions i no de 4.

A continuació, s'adjunta una taula amb la configuració principal d'un dels enllaços VPN entre Andorra-1 i França-1:

Tipus de Configuració	Configuració
Configuració de la seguretat, en aquest cas es configura el tipus d'autenticació i el xifratge que s'aplicarà i dintre de quin grup	<entry name="IPSECP-1"> <esp> <authentication> <member>sha1</member> </authentication> <encryption> <member>aes256</member> </encryption> </esp> <lifetime> <hours>1</hours> </lifetime> <dh-group>group2</dh-group> </entry>

Tipus de Configuració	Configuració
Detall de la configuració dels túnels. En aquest cas es el túnel 1 de 8. Aquest túnel és el que comunica ANDORRA-1 amb FRANÇA-1	<entry name="tunnel.1"> <enable>yes</enable> <passive>no</passive> <authentication>OAP-hola</authentication> <metric>10</metric> <priority>1</priority> <hello-interval>10</hello-interval> <dead-counts>4</dead-counts> <retransmit-interval>5</retransmit-interval> <transit-delay>1</transit-delay> <link-type> <broadcast/> </link-type> </entry>
Es configura el gateway virtual, en aquest cas d'ANDORRA-1. Es pot observar com utilitza la configuració que s'ha detallat abans de la xifratge, el port que fa servir, la seva ip i quina es la clau de seguretat codificada.	<entry name="ANDORRA-1"> <protocol> <ikev1> <dpd> <enable>yes</enable> <interval>5</interval> <retry>5</retry> </dpd> <ike-crypto-profile>IPSECP-1</ike-crypto-profile> <exchange-mode>auto</exchange-mode> </ikev1> </protocol> <authentication> <pre-shared-key> <key>-AQ==mYALhdM4PjovtF630AZqSHmp2tA=+C10DAlKfnZeLmaFsn6p+Q==</key> </pre-shared-key> </authentication> <protocol-common> <nat-traversal> <enable>yes</enable> </nat-traversal> <passive-mode>no</passive-mode> </protocol-common> <peer-address> <ip>10.0.1.1</ip> </peer-address> <local-address> <interface>ethernet1/1</interface> </local-address> </entry>
Conté la configuració del túnel que es realitza de Andorra-1 a França-1. Es detalla el protocol de xifratge de la configuració que s'ha vist anteriorment, la ip del destí i quin túnel es farà servir.	<ipsec> <entry name="ANDORRA-1"> <auto-key> <ike-gateway> <entry name="FRANÇA-1"/> </ike-gateway> <ipsec-crypto-profile>IPSECP-1</ipsec-crypto-profile> </auto-key> <tunnel-monitor> <enable>yes</enable> <destination-ip>10.0.1.6</destination-ip> <tunnel-monitor-profile>MP1</tunnel-monitor-profile> </tunnel-monitor> <anti-replay>yes</anti-replay> <copy-tos>no</copy-tos> <tunnel-interface>tunnel.1</tunnel-interface> </entry>

7.6 Descripció detallada de la configuració del Switch

Tot i que en la simulació de l'entorn de proves no s'ha fet servir cap switch, ja que aquest, ja estan en producció i amb les vlans configurades, s'ha extret la configuració d'aquest detallant especialment la configuració de les vlans, perquè són presents en la simulació amb l'eina OPNET i així es pot realitzar un estudi comparatiu de la configuració en tots dos entorns.

Per tant, la configuració que es detalla a continuació, fa referència a al creació d'una vlan i el tipus de configuració que pot adaptar un port segons on estigui enllaçat.

Configuració Vlan switch França-2:

Tipus de Configuració	Configuració	Descripció
Vlan Producció	interface Vlan10 ip vrf forwarding PRODUCCIO ip address 192.0.1.10 255.255.255.0 ip ospf cost 5	Es definexis la Vlan, s'indica el nom que se li assigna, s'indica la ip del gateway principal d'aquesta Vlan, i el cost ospf per filtrar el tràfic
Vlan Integració	interface Vlan20 ip vrf forwarding INTEGRACIO ip address 192.0.7.10 255.255.255.0 ip ospf cost 10	Es definexis la Vlan, s'indica el nom que se li assigna, s'indica la ip del gateway principal d'aquesta Vlan, i el cost ospf per filtrar el tràfic
Port Vlan Integracio	interface FastEthernet1/0/3 switchport access vlan 10 switchport mode access spanning-tree bpduguard enable	S'indica el port que es configura, quin tipus de vlan configurem i quin sera el seu mode, en aquest cas d'accés. També s'activa el spanning-tree amb l'objectiu d'evitar bucles
Port Vlan Producció	interface FastEthernet1/0/4 switchport access vlan 20 switchport mode access spanning-tree bpduguard enable	S'indica el port que es configura, quin tipus de vlan configurem i quin sera el seu mode, en aquest cas d'accés. També s'activa el spanning-tree amb l'objectiu d'evitar bucles
Port en mode Trunk	interface FastEthernet1/0/1 description ENLLAC FIREWALL switchport trunk encapsulation dot1q switchport trunk allowed vlan 10,20 switchport mode trunk spanning-tree bpduguard enable	S'indica el port que es configura, en aquest també afegim una descrpció del port. Es defineix l'encapsulació que es farà servir, ja que és un Trunk Port, les vlans que es permeten que viatgin per aquest trunk port. Finalment, s'indica que el port estarà en mode trunl i s'activa el spanning-tree amb la finalitat d'evitar bucles.

8 OPNET i la Simulació D'Esdeveniments discrets

OPNET és una eina de simulació de xarxes basada en simulació d'esdeveniments discrets (DES) que permeten analitzar el funcionament de les aplicacions i el impacte de canvis obtenint d'aquesta manera una optimització de la xarxa i un augment del rendiment a baix cost sense fer ús del sistema real.

8.1 Hardware que s'ha triat en el simulador

El hardware que s'ha triat ha estat el que està més pròxim a la realitat del projecte, amb la finalitat que continguin les mateixes característiques o si més no, molt semblants.

A continuació es farà un descripció del equip escollit a més dels motius per els quals s'han triat. Els equips que s'han triat per la simulació d'aquest projecte són els següents:

-Firewall:

El firewall que s'ha triat, és el firewall genèric que ofereix l'eina OPNET IT Guru, conté les característiques generals que pot tenir qualsevol firewall, és a dir, control d'accessos per port, regles, diferents protocols d'enrutament, etc.

En aquest projecte, l'elecció d'aquest firewall ha estat de manera forçada, ja que el firewall de l'entorn real és un Palo Alto 5050, el qual és un firewall molt avançat, que a part de fer filtratge per port, també ho fa per aplicació, cosa que en la versió OPNET IT Guru no està disponible.

D'altra banda, com alternativa, s'hagués pogut triar un firewall d'ASA de Cisco, el qual la versió IT Guru, no té cap elecció. No obstant, la versió Modeler dona la possibilitat de triar un firewall PIX de Cisco, els quals són els predecessors dels ASA.

Finalment, com la finalitat de l'estudi era els enllaços punt a punt, la discriminació del tràfic a partir de costos i la redundància, s'ha optat per triar el firewall genèric el qual suporta correctament dites configuracions.

- **Router:**

El router que s'ha triat per a al simulació amb la finalitat de resoldre un error del Model Complert, consisteix en el Cisco 3660, el qual és un router bastant complert, el qual pot gestionar i processar un gran nombre de paquets, per el qual el fa un bon candidat tan per l'entorn de simulació com per l'entorn real.

Per tant, és el router que s'ha triat, ja que la seves característiques són les més indicades per a la simulació.

- **Switch:**

El switch, al ser l'encarregat principal de gestionar les VLANs, s'ha intentat que el switch de la realitat i de l'entorn virtual siguin el més similars possibles, ja que, al ser els principals protagonistes de les VLANs, el fet de que siguin diferents, poden modificar el temps de resposta i la pèrdua de paquets segons les característiques de cada switch.

En aquest cas, l'eina OPNET IT guru, contenia el mateix model de Switch que hi ha en l'entorn real, per el que s'ha triat un Cisco Catalyst 5500. El que permet que els resultats de la simulació virtual sigui sinó exacte el més pròxim als de l'entorn real.

- **Servidor Genèric:**

En aquest punt, les característiques del servidor no eren molt rellevants, ja que, el principal objectiu era configurar un servidor de Base de Dades amb la potencia suficient per executar un nombre important de querys, sense obtenir un temps de resposta molt elevat.

Per aquest motiu, s'ha triat el servidor genèric que ofereix l'eina, OPNET, ja que compleix suficientment les característiques principals que s'han descrit anteriorment.

La principal diferència és que l'entorn real, els servidors poden ser de diferents plataformes (Windows, GNU/Linux) En canvi, l'única plataforma disponible en l'entorn virtual de IT Guru és Solaris, (En la versió Modeler, es poden triar altres entorns) el qual no és un problema, ja que si l'entorn està correctament configurat no ha de representar grans variacions en el temps de resposta entre diferents entorns.

Per tant, el servidor genèric és el triat per la simulació virtual per les seves característiques.

- **Client Genèric:**

L'elecció del client genèric no ha suposat un estudi gaire complex, ja que tan sols s'ha triat un estació de treball simple, sense definir cap entorn la qual s'ha configurat per a que realitzes peticions a les bases de dades per observar el flux de tràfic a més de les configuracions dels pings, per tal d'estudiar l'adreçament del tràfic si era correcte o no.

Per la qual cosa, el client genèric compleix de lluny les característiques per realitzar la simulació.

- **Enllaç ethernet 100BaseT:**

Un dels punts que en principio no representava cap problema era l'elecció dels enllaços. En l'entorn real tenim heterogeneïtat en els enllaços, ja que entre Switchs els enllaços són de fibra, i entre els servidors de categoria 100T al igual que amb els firewalls.

Com els Switchs per tal de tindre els enllaços de fibra, se'ls ha d'instal·lar un annex, el qual l'eina IT Guru no contempla, s'ha decidit, que com els colls de botella estan a partir dels enllaços 100T, de homogeneïtzar tota la xarxa interna als enllaços 100T. El principal motiu, ha estat per no canviar el Switch i que la diferència d'utilitzar enllaços de

fibra als 100T es la velocitat de comunicació entre els servidors dels CPDs de la mateixa, la qual cosa no es simularà i no farà falta que els enllaços tinguin de ser de fibra.

Per tant, tots els enllaços LAN són 100T, els quals compleixen correctament les caracterxístiques per a realitzar la simulació.

- **Enllaç punt a punt PPP DS1:**

S'ha utilitzat enllaços punt a punt DS1 amb la finalitat de simular les VPNs entre els diferents firewalls de cada zona. S'ha triat aquests enllaços, en primer lloc, ja que són punt a punt, són els més pròxims a un enllaç virtual de VPN i en segon lloc per la velocitat que el màxim que pot oferir és de 2,5 Mbps, el qual amb el xifratge i desxifratge de la VPN és la configuració que més s'aproxima a la realitat.

8.2 Avantatges de la simulació

Les eines de simulació són una important ajuda per als dissenyadors de xarxes, administradors, operadors, tècnics i per a l'estudi de les mateixes. D'aquesta manera es pot fer un anàlisis molt pròxim de la realitat amb la finalitat de poder diagnosticar el funcionament i els problemes de la configuració del flux del tràfic, dels protocols, de les regles de filtratge, etc. D'aquesta manera, es poden validar modificacions i canvis en entorns reals de xarxes abans d'implementar-los, comprovant-los i corregint-los prèviament en els entorns de simulació virtual.

Així doncs hi ha una sèrie d'avantatges al fet de poder realitzar aquestes tasques sense tenir que construir una xarxa física o utilitzar la xarxa que ja està en funcionament per a poder observar-ho, amb el perill de que aquesta quedi inutilitzada. Per tant, els principals avantatges de les eines de simulació són:

- Anàlisis Complert de la xarxa:

  En l'entorn virtual un cop configurat es pot fer un anàlisis complert de cadascun dels components que composen la infraestructura de la xarxa. A més de l'estudi dels diferents protocols, així com el seu impacte dintre de la infraestructura.

  Aquest punt és important, ja que permet als dissenyadors i administradors de la xarxa analitzar exhaustivament cadascun dels components, abans de introduir-los o modificar-los en l'entorn real.

- Detectar restriccions i/o colls d'ampolla:

  Habitualment en la implementació de dissenys de xarxa, l'ús d'aquesta infraestructura s'esdevé en la majoria de casos de manera regular i amb poca modificació, el que fa difícil la detecció de restriccions i colls d'ampolla en aquells casos on el flux de tràfic sigui molt fluid i de poca intensitat.

  En aquest punt, l'entorn virtual permet modificar aquest flux, permeten simula la infraestructura de la xarxa amb diferents flux de tràfic de menys a més intens, de més a menys, regular, etc. El que permet detectar possibles restriccions mal configurades o colls d'ampolla quan el tràfic és molt intens.

  La qual cosa, beneficiaria molt aquest estudi, sobretot en aquells dissenys que volen que siguin escalables i estables.

- Detecció de problemes més exhaustiva:

  Un dels altres avantatges més importants de les eines de simulació, és el poder detectar els problemes i poder-los corregir abans de que el disseny o modificacions s'introdueixi en la infraestructura real.

  A més, en els entorns de simulació al poder gestionar lliurament el flux, les normes, el tràfic, la discriminació d'aquest, fa possible que la detecció

d'aquest errors sigui més exhaustiva i que un cop s'implementi en el sistema real, aquesta configuració, modificacions o agregacions estigui més que verificades.

- Seguretat en la implementació i comprovació de les noves configuracions:

Un dels punts més forts dels entorns de simulació és la seguretat en la implementació i comprovació dels dissenys i de les seves modificacions, és a dir, anteriorment, aquestes modificacions, es comprovaven en entorns reduïts o directament en l'entorn principal, la qual cosa si aquest originava un error o una fallida de seguretat, podria comprometre tot el sistema i s'hauria de realitzar un RollBack de totes les configuracions. La qual cosa, pot comprometre la seguretat de la infraestructura i fer-la més vulnerable durant les comprovacions.

Per aquest raó, el fet que els entorns de simulació permetin la verificació i comprovació dels dissenys o modificacions de les xarxes, fa que la seguretat i l'estabilitat de la infraestructura real es mantingui i que tan sols es modifiqui en un cop aquestes modificacions ja han estat verificades exhaustivament dintre de l'entorn de simulació, mantenint així la seguretat i estabilitat de l'entorn real.

- Reducció en el costos d'experimentació i implementació:

A més, un dels avantatges més beneficiosos a nivell d'empresa és la reducció de costos, és a dir, el fet de no desplaçar tècnics en els entorn físics, a més de la compra d'aparells de gran cost, dels temps de configuració, de la instal·lació i a més de la participació de més d'una persona. Fa que les eines de simulació siguin un punt clau en l'estalvi de recursos monetaris, temporals i de treball.

- Possibilitat de comprovar múltiples dissenys simultàniament:

Un altre punt molt important a tenir en compte a favor dels entorn de simulació és la comparació al mateix temps de múltiples dissenys, és a dir, podem comparar els resultats d'un disseny amb els d'un segon

disseny que s'ha decidit treballar paral·lelament per exemple i comprar els seus resultats.

Aquesta possibilitat, és pràcticament inviable en un entorn físic, degut a la gran inversió de recursos que s'hauria de fer, per la qual cosa és un dels punts més importants de la simulació virtual.

- Elaboració d'estadístiques de cadascun dels components:

Finalment, un dels avantatges principals de les eines de simulació virtual és l'elaboració d'estadístiques de cadascun dels components, ja siguin estacions de treball, routers, switch, etc com també dels enllaços, de les vlans, protocols d'enrutament etc.

Els quals, per a fer-ho a nivell físic requereix més configuració, a part de la compra de més equips i d'instal·lació de programes auditors.

Per la qual cosa, aquest també és un dels punts principals en els avantatges de les eines de simulació, que ens permet tindre valors estadístics de cadascun dels components.

8.3 Limitacions de la simulació via software

Com s'ha descrit en l'anterior subapartat les eindes de simulació virtuals o via software, ofereixen un gran ventall d'avantatges que per als dissenyadors i administradors de xarxes són mollt importants.

No obstant, també hi ha les seves contrapartides i les limitacions de les simulacions dintre d'entorns virtuals que poden ocasionar dificultats sobretot a l'hora d'implementar-ho en l'entorn físic.

A continuació les principals limitacions de la simulació via software són:

- Impossibilitat de contenir tot el ventall de dispositius del mercat:

  Un dels punts claus de la simulació, és que els equips que simulin el nou disseny siguin els méx pròxims als de l'entorn real, desitjablement que siguin exactament iguals.

  Aquest punt, la majoria de casos es pot aconseguir, però en casos puntuals o de dissenys d'infraestructures importants, on el hardware utilitzat és d'un cost elevat i la qual cosa poc utilitzat, fa que les eines de simulació virtual no continguin aquests equips.

  Aquest fet ocasiona que la simualció, no sigui del tot fiable, ja que el comportament d'un aparell a un altre pot ser molt diferent depenent de la topologia de la xarxa on sigui implementat.

- Diferenciació en les configuracions dels equips:

  Un punt important, que les eines de simulació que suposa una limitació, és la configuració dels equips. La configuració dels equips en l'eina virtual és molt diferent al de l'equips real.

  En el cas de les eines de simulació, es tracte en afegir paràmetres i deshabilitat o habilitat opcions. El que provoca que alhora de configurar l'equip real, la configuració entre equip virtual i real no sigui la mateixa i

que alhora de implementar-lo apareguin errors, que no apareixien en la simulació i que siguin causa de la configuració de l'equip.

- Configuració homogenia entre diferents equips:

Dintre de l'entorn de simulació, la configuració dels equips és molt similar, és a dir, configurar un firewall, un router, un servidor o una estació de treball no varia massa.

El punt on radica la diferenciació de la seva configuració en les opcions que apareixen dintre de cada un dels dispositius, però la seva configuració és exactament igual.

Aquest fet, ocasiona el mateix error que l'anterior punt, que alhora de passar-ho a l'entorn real, es generin problemes degut a que no es pot transmetre exactament la mateixa configuració que en l'entorn de simulació.

- Limitació en el comportament dels servidors:

Les eines de simulació majoritàriament i sobretot l'eina OPNET IT Gurú, el fet de configurar un servidor o relaciona directament amb el model "Client - Servidor".

Aquest fet, normalment és vàlid, ja que la major part dels cops s'utilitza aquest disseny, però en alguns dissenys de càrrega de backups o de retransmissió de les dades, en que la comunicació es realitza entre "Servidor - Servidor" l'eina de simulació no ho permet.

Per tant, implica una limitació tot i que és pot difuminar intensificant les peticions dels clients, per simular les connexions Servidor - Servidor, fa que la simulació no sigui pròxima a la de l'entorn real.

- Limitacions en la configuració de les VPN:

  Una de les limitacions que s'ha trobat en la realització d'aquest projecte és la configuració de les VPN i la selecció del xifratge i model de seguretat que es volia triar.

  Tot i que és una limitació pròpia de l'eina OPNET IT Gurú, en la qual versió completa (OPNET Modeler) apareix que aquesta funcionalitat es pot realitzar de manera més complexa, no arriba a ser exactament a com es configura en els equips reals.

- Limitacions en les virtualització dels equips:

  Un dels punts importants en el disseny de les xarxes és la virtualització dels equips, és a dir, cada vegada és més freqüent veure firewall, router i switch, que represente 2 o més equips virtualitzats. Amb la finalitat d'optimitzar els recursos i treure el màxim rendiment als aparells.

  Aquesta configuració no està disponible en l'entorn de simulació OPNET IT Gurú, tot i que en la versió Modeler, dintre de les seves especificacions es detalla que ho pot suportar, la documentació que hi ha relacionada en aquest àmbit és molt limitada, a més que sembla ser que ho fa de manera diferent, que en la realitat però amb els mateixos resultats.

  La qual cosa, també mostra una limitació en el traspas de les configuracions, que poden ocasionar més d'un problema en la implementació dels nous dissenys o modificacions.

8.4 Simulació d'Esdeveniments Discrets

La simulació d'esdeveniments discrets (DES) és quan l'estat dels processos que es volen estudiar van variant durant el temps de forma discreta. Aques tipus de simulació és la que fa servir l'eina OPNET per al seu estudi.

L'eina OPNET fa ús d'un rellotge per a realitzar aquesta simulació, és a dir, emula una evolució temporal del sistema que registra el temps virtual, el qual utilitza per modificar en els instants discrets de temps on introdueix un no esdeveniment, independentment del total del temps que es consumeix en la seva execució.

Així mateix, els elements bàsics per a la simulació d'esdeveniments discrets amb OPNET són: l'estat del sistema, les entitats, els atributs, els esdeveniments, les activitats, els recursos, els retards i els processos.

A continuació s'adjunta una taula[4] amb la descripció de cadascun d'aquest elements:

Element	Descripció	OPNET
Estat del Sistema	És el conjunt de totes les variables que contenen tota la informació que descriu l'estat del sistema en un punt exacte en el temps.	En l'eina OPNET aquest estat és ocult per l'usuari, en que la seva modificació només es permesa per a l'estat inicials per definir les condicions de la simulació
Entitats	Són tots els objectes que requereixen una representació dins del model.	Són tots els elements dels sistema, ja poden ser els nodes i els enllaços com els paquets que passen per ells.
Atributs	Són les propietats de cadascuna de les entitats. Indicant les seves característiques.	Tots els elements en OPNET estan caracteritzats pels seus atributs.
Esdeveniments	Són accions instantànies dins d'un marge de temps determinat que poden canviar l'estat del sistema.	Venen definits en els estats i les transicions dels models, queden ocults en el procés de simulació
Activitats	Són les operacions que reben les entitats i determinen el comportament del model de simulació. Tenen una durada determinada dintre del temps total	Estan definides, d'una banda, dins dels models de processos, indicant com i quan cal fer les transicions, i d'altra banda, en les característiques de les aplicacions.
Recursos	Un recurs és qualsevol element del sistema de capacitat restringida, que proporciona servei per a una o més entitats.	Cada node, enllaç o aplicació defineix quina capacitat té (recursos)

[4] Font principal de la Taula recollida a partir de la memòria de Norbert Martinez (2008 - pàgina 16)

Element	Descripció	OPNET
Retards	És una durada en els temps de longitud indefinida, que se sap quan comença però no quan finalitza, normalment per saturació de recursos o per sincronitzacions entre activitats.	Els retards són inherents als protocols definits dins d'OPNET
Processos	Es la descripció del conjunt d'activitats que una activitat pot desenvolupar dins del model	Ve determinat per la configuració de l'escenari, els seus elements i els atributs aleatoris, sempre vist com la simulació d'una xarxa de comunicacions.

8.5 OPNET IT Gurú

És un llenguatge de simulació orientat a les comunicacions. El qual, Proporciona accés directe al codi font, oferint un gran avantatge per als nous programadors a programar amb OPNET.

Actualment és utilitzat per grans empreses de telecomunicacions, per exemple per a desenvolupar projectes governamentals i de l'exèrcit, etc...

Aquest programari simula el comportament d'una xarxa per complet dintre d'un entorn virtual. Els components de xarxa que es poden implementar son routers, commutadors, protocols, servidors i aplicacions.

Esta compost d'un editor gràfic que incorpora diferents eines amb les que es pot dur a terme tot el cicle de modelització i simulació. Aquesta modelització i simulació es pot construir a diferents nivells de capa, descrivint a cada nivell diferents aspectes del models, establint d'aquesta manera una jerarquia.

Finalment, els diferents nivells d'aquesta estructura jeràrquica són, els de xarxa on s'especifica la topologia física, nodes on es defineixen aquests mateixos nodes i els fluxos de dades i el procés on es descriu el comportament i el flux lògic.

9 Modelat

Un vegada, en aquest punt del PFC, on ja s'ha triat i descrit els components que es fan servir en la connexió dels enllaços WAN dels dos CPDs d'Andorra i de França. S'ha realitzat l'estudi de l'eina de simulació OPNET IT GURU, la qual ja ha estat instal·lada, configurada i en funcionament, on s'ha pogut fer una sèrie de simulacions bàsiques seguint els models d'exemple que proporciona el mateix programari, a més dels manuals descarregats de la pàgina oficial i dels laboratoris de seguretat proporcionats per l'Universitat Ramon Llull present en la documentació oficial de l'eina.

Un cop estudiat, s'ha realitzat el modelat de la infraestructura amb l'objectiu de realitzar més endavant la seva simulació am l'objectiu de extreure'n resultats en el comportament del flux del tràfic i els seus temps de resposta.

A més, després de realitzar un estudi de l'eina s'ha detectat que la configuració de les VPN no permet triar els paràmetres de seguretat i que no hi ha l'opció de punt a punt, sense la necessitat de afegir un client remot. Per tant, s'ha decidit eliminat aquest punt de la simulació, ja que l'únic que afegia d'interes era l'increment en el temps de resposta en els enllaços, per el que s'ha decidit crear enllaços directes punt a punt amb connexions "PPP-DS1" que és l'opció que més s'aproxima a la realitat.

També, en el modelatge de les simulacions s'ha detectat un error en el Model Complert, el qual s'ha decidit crear dos nous models que solucionen aquest error, un per la simulació física, la qual s'implementarà en producció més endavant on també s'ha realitzat la simulació en OPNET per la comparació de resultat, i en segon lloc s'ha realitzat un model que soluciona aquest error de manera eficient, a més a més d'escalable.

Per tant, s'ha realitzar sis tipus diferents de model, cinc dels quals s'han simulats amb l'eina OPNET llevat del que s'ha detectat l'error, quedant de la següent manera:

- Model Bàsic: És el model més senzill el qual ens permetrà observar el funcionament del conjunt de clients, switchs, firewalls, servidors i enllaços d'aquest.
- Model Complert: És un model bastant més ampli que l'anterior en el qual s'ha detectat l'error, en el qual es detallarà i s'explicarà el motiu per el qual s'ha descartat aquest model i les seves dues solucions.
- Model Complert millorat paral·lel a la maqueta: En aquest model s'ha corregit l'error del Model Complert, de la mateixa manera que s'ha realitzat en l'entorn de proves físic, aquesta solució corregeix l'error, però limita la discriminació del tràfic, el seu objectiu serà la comparació directa amb l'entorn de proves i l'estudi d'aquest en quan al flux de tràfic i el temps de resposta en les diferents peticions.
- Model Complert millorat: En aquest model s'ha corregit l'error del Model Complert sense imposar cap limitació, aquest model no s'ha realitzat en l'entorn de proves físic per el seu valor econòmic afegit, per lo que es realitzarà més endavant quan estigui aprovat. L'objectiu de simular aquest model és l'estudi del comportament del xarxa i del seu flux alhora de que s'hagi d'implementar.
- Model Complert millorat amb un firewall caigut: És el mateix model que l'anterior però en aquest cas, deshabilitem un dels firewalls de Andorra, amb l'objectiu d'analitzar que el flux de tràfic, sigui redirigit de manera correcta cap l'altre firewall.
- Model Complert millorat amb dos firewalls caiguts: És el mateix model que el Model Complert millorat, amb la diferència que s'han deshabilitat dos firewalls, un d'Andorra i un altre de França, amb l'objectiu d'analitzar la redistribució del tràfic si es realitza de manera correcta i els retards que ocasiona aquesta.

- Model Complert millorat amb volum de tràfic real: És el mateix model que el Model Complert millorat, amb la diferència que s'han introduït més estacions de treball amb la finalitat d'augmentat el volum de tràfic de la xarxa al que tindrà el model real i comprovar possibles errors o comportament que no apareixien amb el volum mínim del Model Complert millorat

- Model Complert millorat amb volum de tràfic real i un firewall caigut: És el mateix model que el Model Complert millorat amb el volum de tràfic real, amb la diferència que en aquest model, el firewall de França - 2 el qual gestiona tot el flux de Integració de França estarà inactiu. La finalitat d'aquest model és observat el comportament de la xarxa amb el volum real de tràfic i verificar el comportament en front d'aquesta situació.

9.1 Model Bàsic

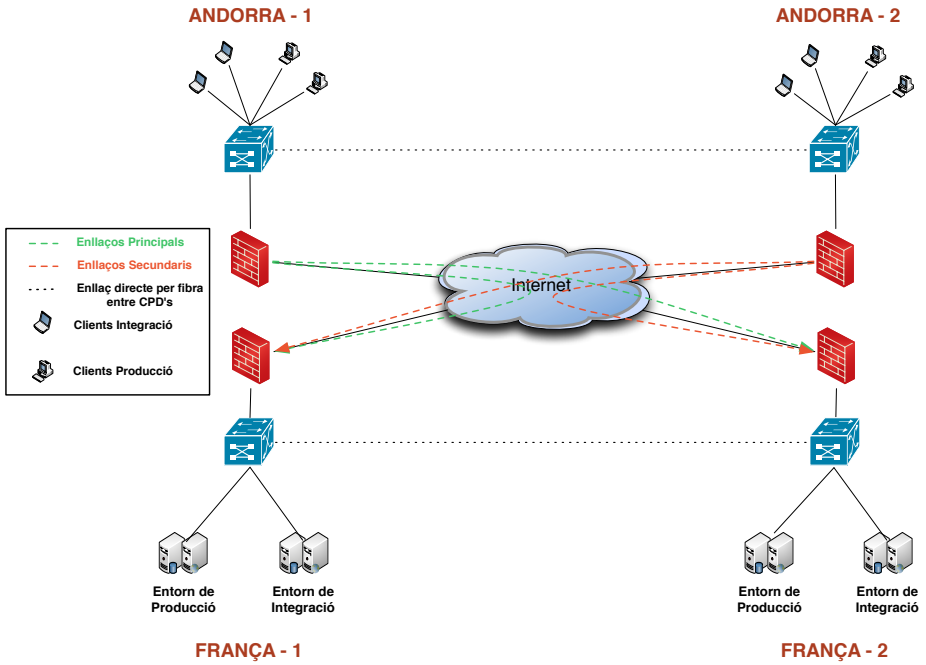
La configuració del model bàsic amb la finalitat de simplificar la infraestructura sense perdre element d'anàlisis, s'ha decidit deixar la part d'Andorra només amb les estacions de treball que realitzaran peticions als servidors localitzats en França. S'ha decidit aquesta configuració, ja que al afegir servidors i estacions de treball en tots dos CPDs, tan sols incrementaria el volum de dades minimitzant el volum de dades que passa per els enllaços WAN que són la prioritat d'anàlisis del projecte.

A més, la configuració s'ha deixat amb quatre estacions de treball per cadascun dels CPDs d'Andorra, és a dir, dos estacions de treball de producció i dos estacions de treball de integració per cada CPD.

D'altra banda, la configuració dels dos CPDs de França, s'ha deixat a cadascun d'ells amb servidor de Producció i un altre d'Integració.

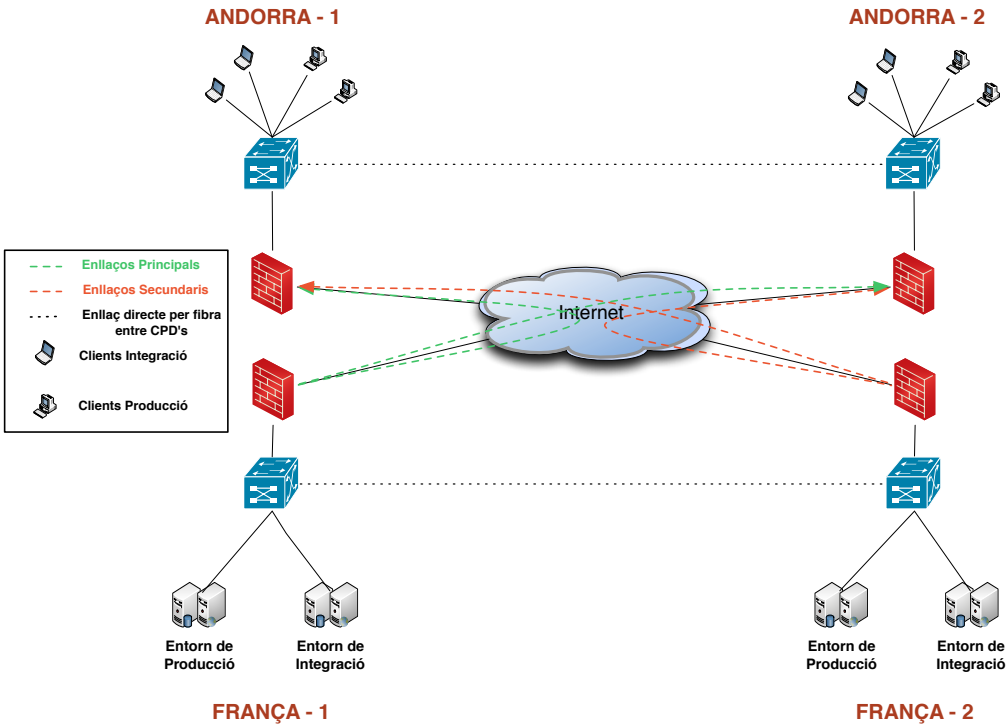
A continuació, s'ha homogeneïtzat els enllaços LAN a la categoria 100BaseT i els enllaços Punt a Punt a PPP DS1.

Per tant, si ens localitzem en la part d'Andorra el tràfic serà gestionat en primer lloc per el firewall de Andorra - 1, en cas de que aquest els seus enllaços estiguin caigut o no estigui operatiu el tràfic serà assumit per el firewall de Andorra - 2, tal i com es mostra en la següent figura:



Il·lustració 9 Model Bàsic Andorra

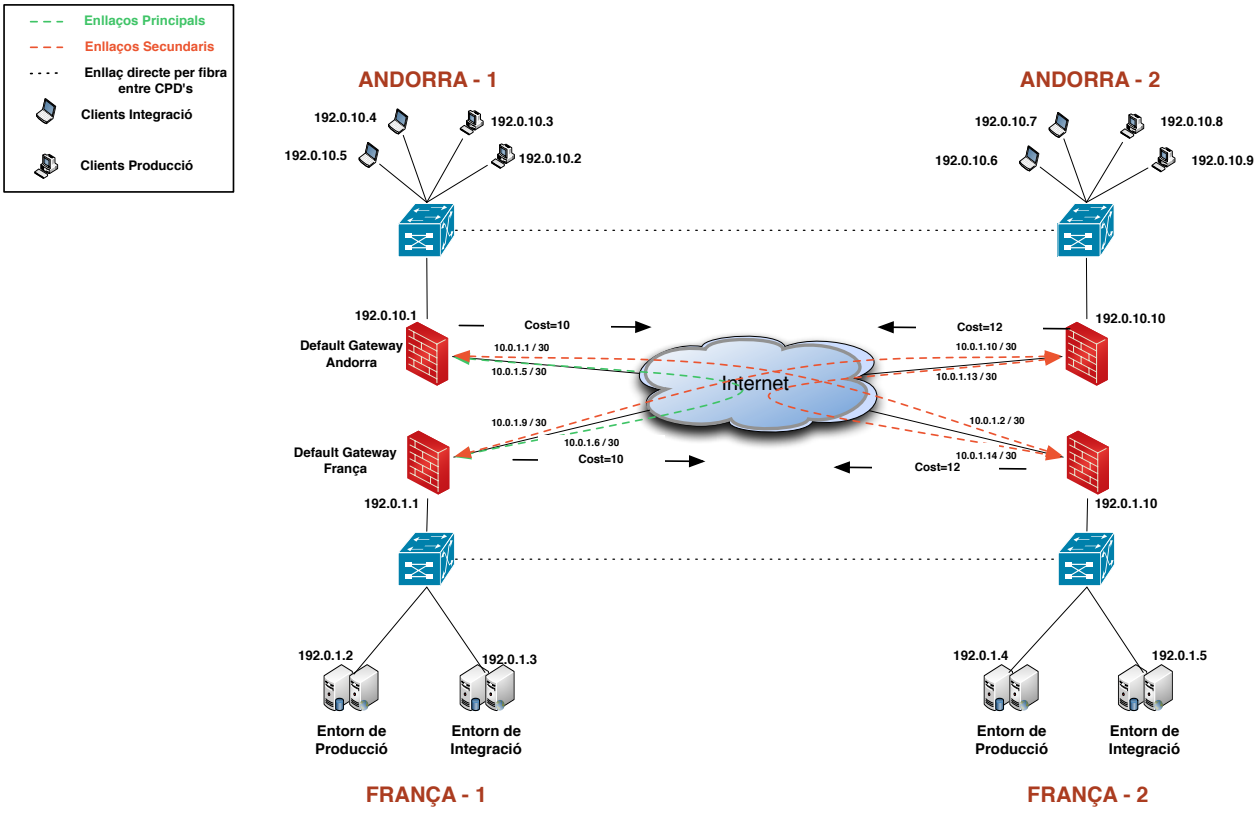
D'altra banda, si ens localitzem a França el tràfic es tractarà exactament que en Andorra, el firewall principal serà el de França - 1 i el firewall secundari o de backup ser`a el firewall de França - 2, quedant de la següent manera:



Il·lustració 10 Model Bàsic França

Per tal d'aconseguir que un firewall sigui el principal i l'altre el secundari es realitza a partir dels costos d'OSPF, en el quals els enllaços del firewall principal amb el seu switch tenen un cost de 10 i els dels firewall secundari un cost de 12 "en totes dues zones", d'aquesta manera, a partir d'aquest protocol podem dirigir el tràfic. Cal destacar, que el cost s'ha realitzat en els enllaços Firewall-Switch, perquè al no tenir la possibilitat de crear túnels via VPN, no es pot ficar un cost asimètric als enllaços punt a punt, és a dir, un firewall té un cost 10 per aquell enllaç i l'altre 12. Per lo que, s'ha triat l'opció descrita que té la mateixa validesa i rendiment la original.

Finalment, s'ha decidit a introduir totes les direccions IPs manualment, ja que la generació automàtica, no pot contemplar diferents rangs IPs, quan hi ha VLANs i connexions punt a punt. La distribució detallada de les direccions IPs es pot observar en la següent topologia:



Il·lustració 11 Model Bàsic Detallat

Com es pot observar, a nivell de LAN d'Andorra tan sols s'ha utilitzat el Rang IP 192.0.10.X / 24, tan per producció com integració, on el Gateway principal és el firewall d'Andorra-1.

En canvi, per França, s'ha fet servir el Rang IP 192.0.1.X / 24, tan per producció com per integració, on el Gateway principal és el firewall de França - 1.

Per concloure, els enllaços punt a punt s'ha decidit fer subnetting amb els següents rangs:

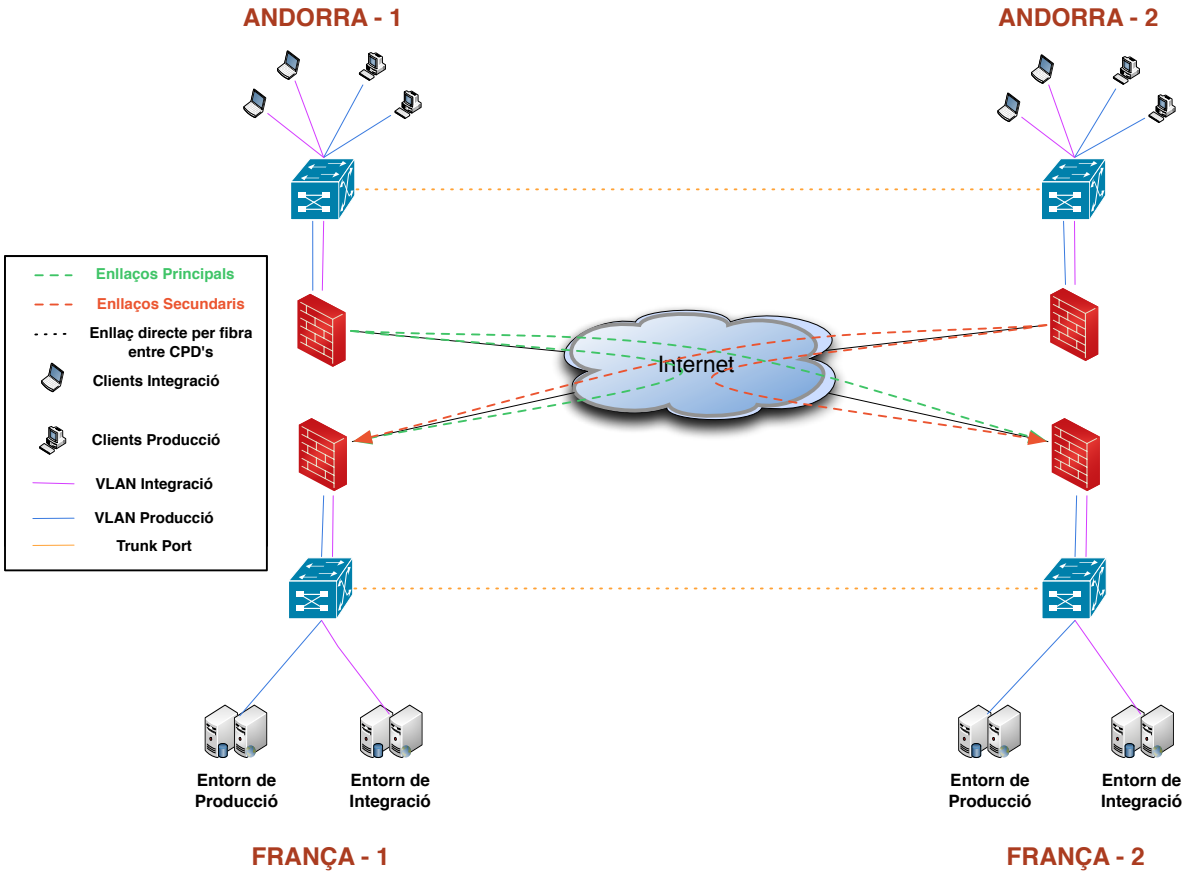
Direcció Xarxa	Firewall - 1	Firewall - 2	Direcció Broadcast
10.0.1.0 / 30	Andorra-1 - 10.0.1.1	França-2 - 10.0.1.2	10.0.1.3
10.0.1.4 / 30	Andorra-1 - 10.0.1.5	França-1 - 10.0.1.6	10.0.1.7
10.0.1.8 / 30	França-1 - 10.0.1.9	Andorra-2 - 10.0.1.10	10.0.1.11
10.0.1.12 / 30	Andorra-2 - 10.0.1.13	França-2 - 10.0.1.14	10.0.1.15

9.2 Model Complert

La configuració del Model Complert, segueix amb la mateixa línia que la configuració del Model Bàsic, és a dir, estacions de treball localitzades als CPDs d'Andorra i els servidors als CPDs de França. Aquesta configuració es mantindrà en tots els models, per els motius descrits anteriorment en el Model Bàsic.

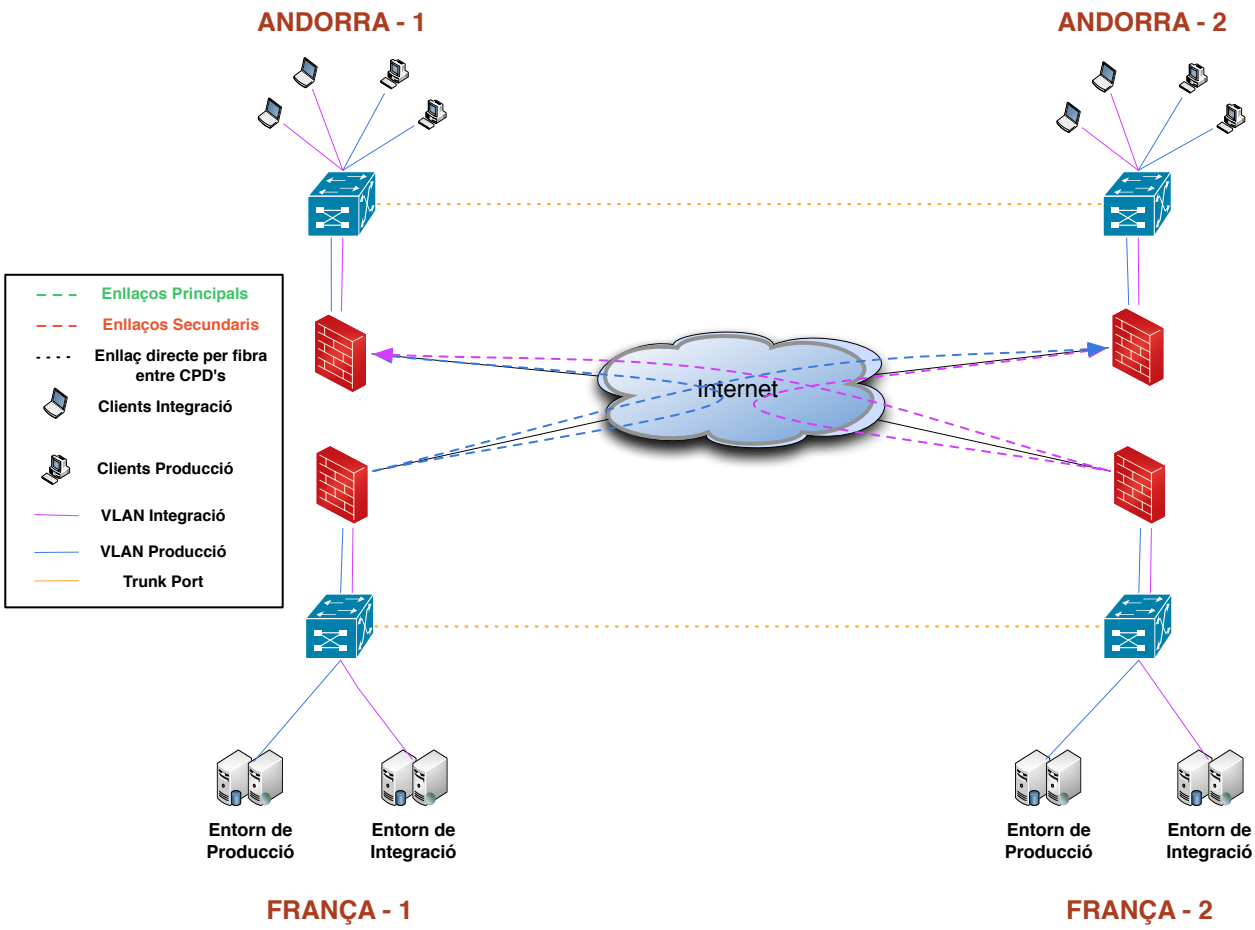
En aquest model, s'ha introduït les vlans per als dos CPDs, les quals es mostren les vlans de producció amb color blau i les d'integració amb color magenta.

Si ens situem en la part d'Andorra, la distribució del tràfic es realitzarà en primer lloc per el firewall de Andorra -1, en el cas que aquest tingui els enllaços caiguts o estigui inactiu, assumirà el flux de tràfic el firewall de Andorra - 2, tal i com es representa en la següent figura:



Il·lustració 12 Model Complert Andorra

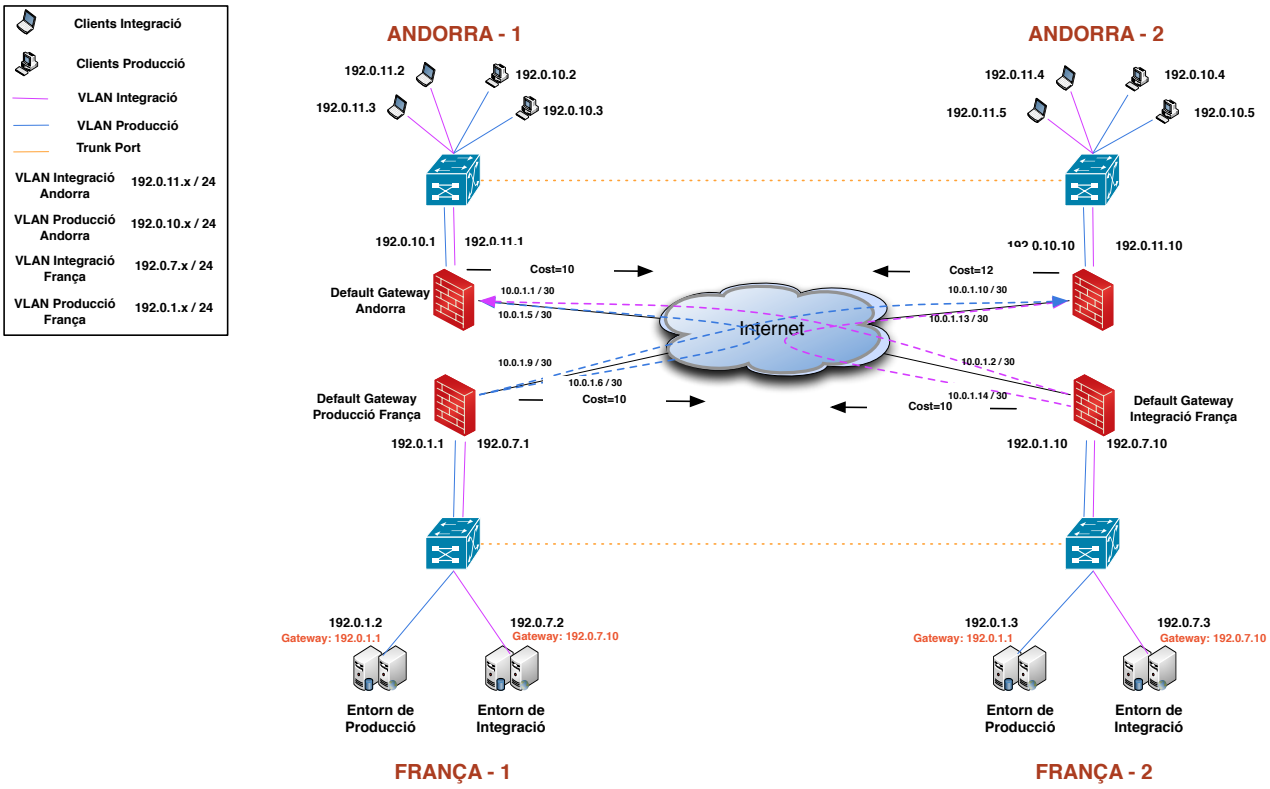
En canvi, si ens situem a la part de França, la distribució del tràfic és discriminada, és a dir, el tràfic de producció serà assumit per el firewall de França - 1 i el tràfic de integració serà assumit per el firewall de França - 2 tal i com es mostra en la següent figura:



Il·lustració 13 Model Complert França

A partir d'aquest disseny, el tràfic de producció serà gestionat de manera simètrica per el firewall 1 de França, en canvi el tràfic de integració tota la seva totalitat serà assumit per el firewall de França - 2. D'aquest manera es discrimina el tràfic de les vlans i repartix el flux de tràfic per més enllaços i equips proporcionant major rendiment.

Per tal de poder aconseguir aquesta discriminació del tràfic, es necessari la configuració de les vlans, amb diferents rangs de IPs i la configuració dels costos de OSPF, depenent d'on voler redirigir el tràfic tal i com es mostra en la següent figura:



Il·lustració 14 Model Complert Detallat

Com podem observar en la figura anterior, s'ha modificat gaire bé tot l'adreçament IP, llevat dels enllaços punt a punt entre els firewalls, els quals es conserven exactament igual.

En canvi, l'adreçament LAN de la zona d'Andorra i de França ha quedat modificat de la següent manera:

Zona	Vlan	Rang	Gateway Principal
Andorra	Producció	192.0.10.X /24	192.0.10.1 - Firewall - 1
Andorrra	Integració	192.0.11.X /24	192.0.11.1 - Firewall - 1
França	Producció	192.0.1.X /24	192.0.1.1 - Firewall - 1
França	Integració	192.0.7.X /24	192.0.7.10 - Firewall - 2

Com podem observar el Gateway principal de Producció i Integració en la zona de França és diferent, això s'ha configurat així per tal de discriminar el tràfic de Producció i Integració.

A més, la distribució del tràfic en el cas d'Andorra és exactament igual que el Model Bàsic, per el que els costos es mantenen exactament igual. En canvi, en la zona de França, al realitzar una discriminació del tràfic segons sigui Producció o Integració, s'ha de realitzar de la següent manera:

Firewall	Enllaç	Cost
França - 1	Producció	3
França - 1	Integració	10
França - 2	Producció	10
França - 2	Integració	3

Finalment, com podem observar si el tràfic està orientat cap a Producció el seu cost és de 3 per el firewall de França - 1 i de 10 per el firewall de França - 2, per lo que el tràfic que vagi dirigit a producció sempre passarà per el firewall de França - 1 si aquest està actiu. En canvi, el comportament del flux si el tràfic va dirigit cap als servidors de integració és a l'inrevés, com es pot observar el cost més baix el té el firewall de França - 2, per lo que si aquest està actiu serà el firewall que rebrà tot el tràfic de Integració.

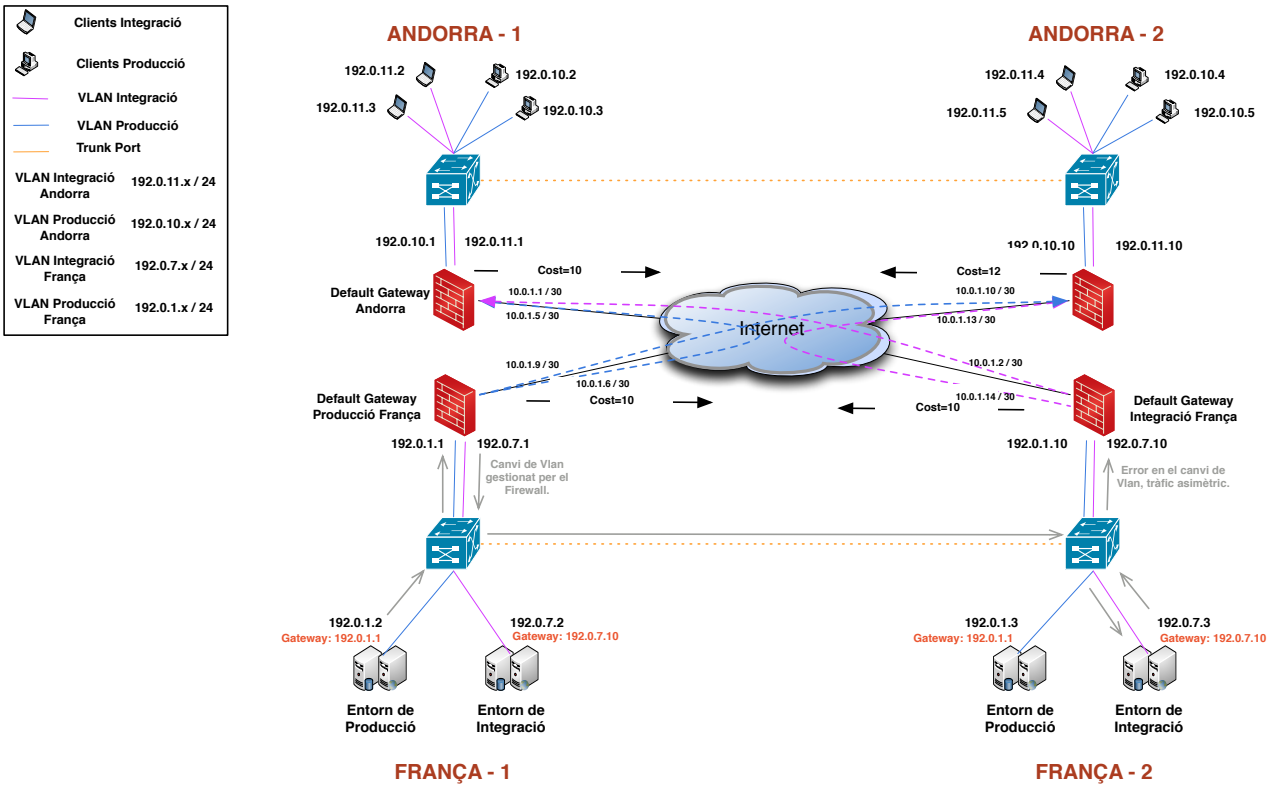
Error en el Model Complert:

Un cop, que s'ha dissenyat aquest model s'ha detectat un error, el qual impedeix que la discriminació del tràfic es pugui dur a terme.

Aquest error ve determinar per una de les condicions dels firewalls[5], en que per defecte el tràfic ha de ser simètric, és a dir, si un firewall rep un flux entrant de petició de dades o enviament, ha de ser el mateix firewall que gestioni la seva resposta. Aquesta condició es pot anular a partir de regles, però aquestes regles afecten a la seguretat del firewall per el que ha estat descartat.

[5] Cal destacar que aquest condició està per defecte en tots els firewals del mercat, però l'eina OPNET no la recrea per el que assumeix el tràfic asimètric sense reportar cap error.

L'error no es genera a partir dels enllaços WAN, ja que aquest al estar discriminat a partir dels costos i les vlans, sempre el tràfic entrant i sortint és gestionat per el mateix firewall. En canvi, el tràfic generat en la mateixa zona entre diferents VLANs recrea l'error, tal i com es mostra en la següent figura:



Il·lustració 15 Model Complert Error

Tal i com es pot observar en les línies grises de l'anterior topologia, si un servidor de producció, realitza una petició a un servidor d'integració segueix el següent recorregut:

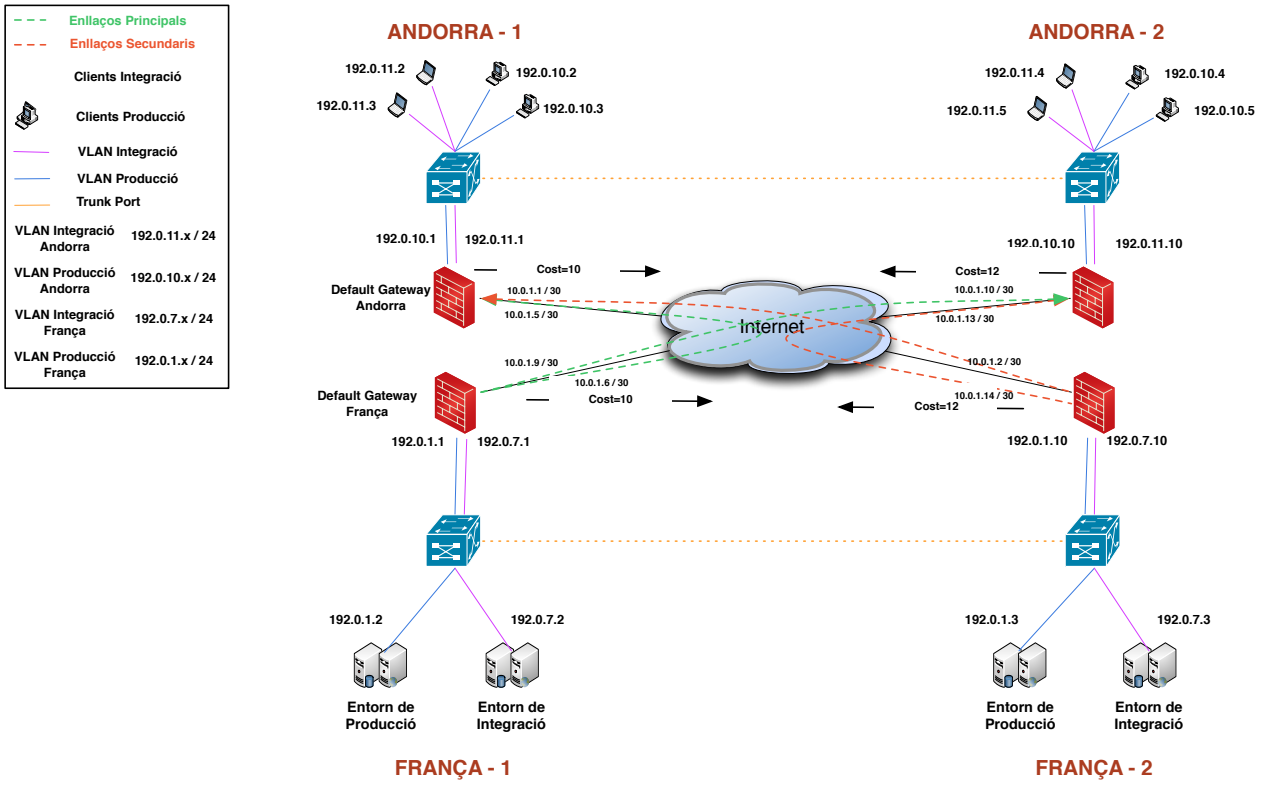
Inici	Destí	Descripció
Servidor Producció	Firewall / França - 1	Realitza el canvi de vlan de producció a integració
Firewall / França -1	Servidor Integració	Realitza l'entrega
Servidor Integració	Firewall / França - 2	Realitza el canvi de vlan, però com aquest firewall no ha executat la petició i no accepta tràfic asimètric destria el paquet i ocasionar l'error.

Finalment, com podem observar aquest error es causat per la condició del firewall i per la mateixa configuració de discriminació del tràfic on el gateway per defecte d'un entorn i de l'altre és diferent.

9.3 Model Complert Millorat paral·lel a la maqueta

La configuració del Model Complert Millorat en la maqueta, segueix amb la mateixa línia que la configuració del Model Bàsic, tan sols amb la diferència que s'ha introduït les vlans, però la discriminació del tràfic desapareix i es mantenen els mateixos costos que per al Model Bàsic, és a dir, els firewalls de França - 1 i Andorra - 1, són els firewalls principals i firewalls de França 2 i Andorra - 2 queden en segon lloc com backup dels primers.

Per tant, la topologia d'aquest model queda de la següent manera:



Il·lustració 16 Model Complert Corregit Paral·lel Maqueta

Com es pot observar en la topologia anterior, les vlan tenen la mateixa configuració que en el Model Complert, però el gateway per defecte ara només es el firewall de França - 1, i els costos són 10 per el firewall de França - 1 i 12 per el firewall de França - 2, d'aquesta manera s'anul·la l'error però perdem la discriminació del tràfic.

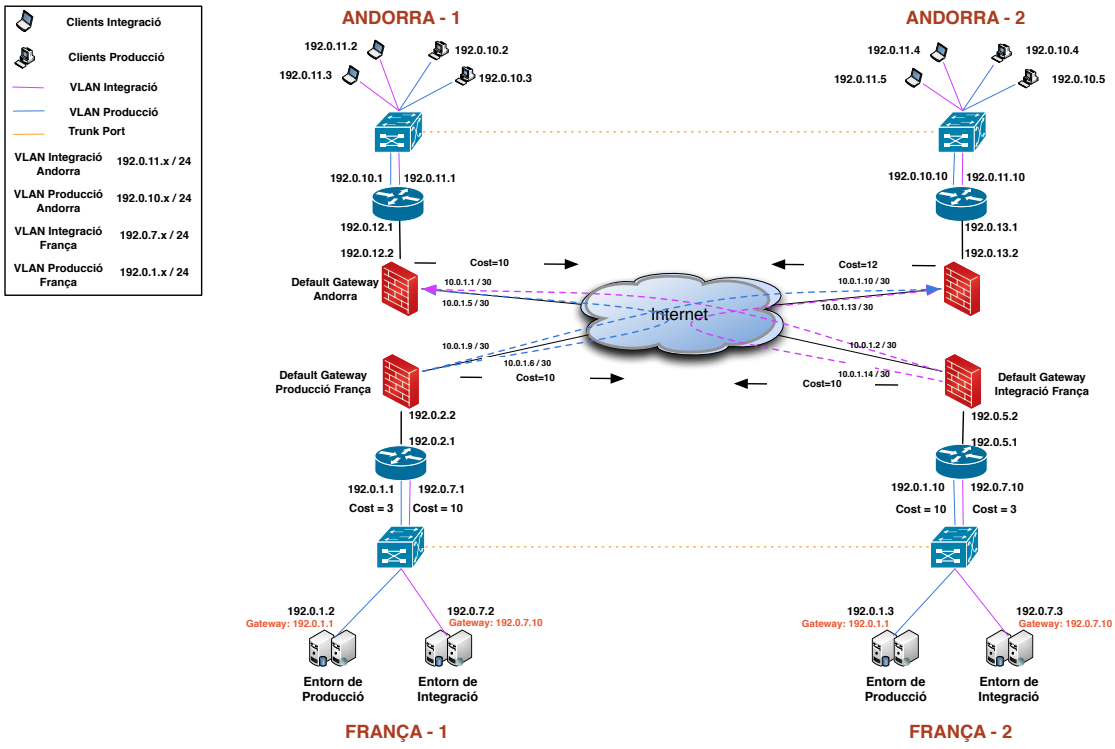
9.4 Model Complert Millorat

La configuració del Model Complert Millorat, segueix amb la mateixa línia que la configuració del Model Complert, és a dir, es manté la discriminació del tràfic i es corregeix l'error del tràfic asimètric entre firewalls. Per tal de poder corregir aquest error i no perdre la discriminació del tràfic, s'ha d'introduir nous equips, entre els firewalls i el switch.

Els equips que s'han triat són Routers, els quals encaminen els paquets i no verifiquen si el tràfic és simètric o asimètric, per tant, l'error anteriorment reproduït en el Model Complert, quedaria resolt, ja que els firewalls deixarien de ser els Gateway per defecte i ho serien els routers.

Aquesta solució, tan sols s'hauria d'aplicar a al zona de França que és la que es realitza la discriminació del tràfic, però com en un futur pot realitzar-se també en la zona d'Andorra, s'ha decidit introduir els routers a tots quatre CPDs per tal de mantenir la infraestructura escalable.

Per tant, un cop aplicada la solució el model quedaria de la següent manera:



Il·lustració 17 Model Complert Millorat

Com es pot observar en l'anterior il·lustració, el gateway per defecte de Producció és el router de França - 1 i el gateway per defecte d'integració és el router de França -2.

Al afegir 4 equips més en la topologia els costos de OSPF per tal de discriminar el tràfic en la zona de França i fer el firewall d'Andorra - 1 el principal, s'han de tornar a reassignar als diferents enllaços.

Zona Andorra			
Equip A	**Equip B**	**Vlan /port**	**Cost de l'enllaç**
Router Andorra -1	Firewall Andorra -1	Trunk Port	10
Router Andorra -2	Firewall Andorra -2	Trunk Port	12
Zona França			
Equip A	**Equip B**	**Vlan**	**Cost de l'enllaç**
Router França -1	Firewall França -1	Trunk Port	10
Router França -2	Firewall França -2	Trunk Port	10
Router Andorra -1	Switch / Andorra -1	Producció	3
Router Andorra -1	Switch / Andorra -1	Integració	10
Router Andorra -2	Switch / Andorra -2	Producció	10
Router Andorra -2	Switch / Andorra -2	Integració	3

Tal i com es mostra en la taula anterior, els enllaços entre firewall i router es mantenen els costos del Model Bàsic, entre firewall i switch, llevat del firewall i router de França - 2 on el cost es redueix a 10 per a que no quedi com de backup. A més, s'introdueix nous costos entre Router i Switch, depenent de la vlan on estigui l'enllaç tindrà un cost o un altre, per tal que França-1 gestioni tan sols producció i França-2 Integració.

A més a més, s'ha tingut d'introduir 4 rangs d'IPs més per a les connexions entre router i firewall, en aquest cas s'ha triat 4 adreces de categoria C, per tal de donar una major escalabilitat en cas de que es necessiti més adreçament.

Firewall	Router	Rang
Andorra -1	Andorra -1	192.0.12.X / 24
Andorra -2	Andorra -2	192.0.13.X / 24
França -1	França -1	192.0.2.X / 24
França -2	França -2	192.0.5.X / 24

Finalment, aquest model, no s'ha aplicat al model físic, ja que representa un inversió financera, la qual ha d'estar aprovada, per lo que la seva simulació només es durà a terme a partir de l'eina OPNET.

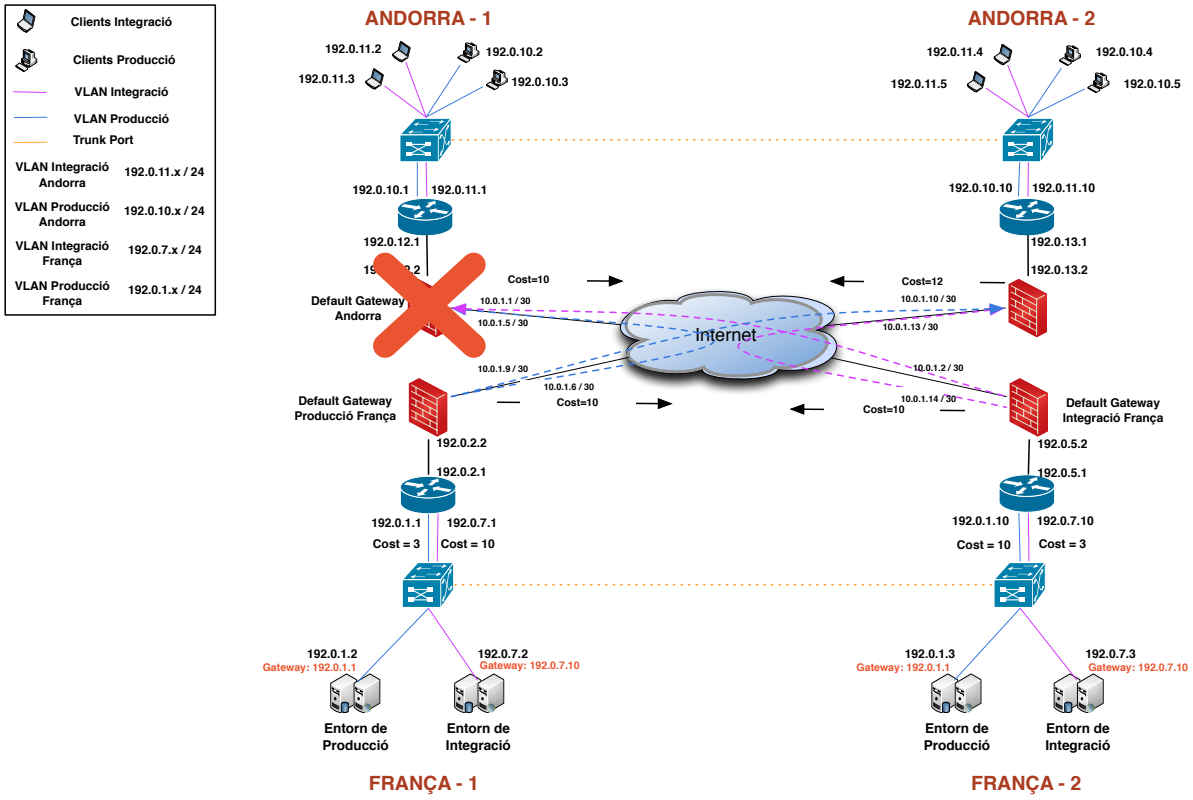
9.5 Model Complet Millorat amb un firewall caigut

La configuració del Model Complert Millorat amb un firewall caigut, segueix amb la mateixa línia que la configuració del Model Complert Millorat, és a dir, la configuració d'aquest model és exactament igual que l'anterior. La diferència radica en que en aquest Model, el firewall d'Andorra -1 estarà caigut.

Per tant, tal i com s'ha descrit en el Model Complert Millorat i en el Model Bàsic, aquest firewall és el principal en el cas de que estigui caigut el firewall d'Andorra - 2 haurà d'assumir la seva feina.

L'objectiu d'aquest model és simular en cas de fallida, la redundància del sistema, per tal d'analitzar si suposa errors, retards, pèrdua de paquets, etc.

Finalment, la topologia d'aquest model quedaria representada de la següent manera:



Il·lustració 18 Model Complert Millorat amb 1 firewall caigut.

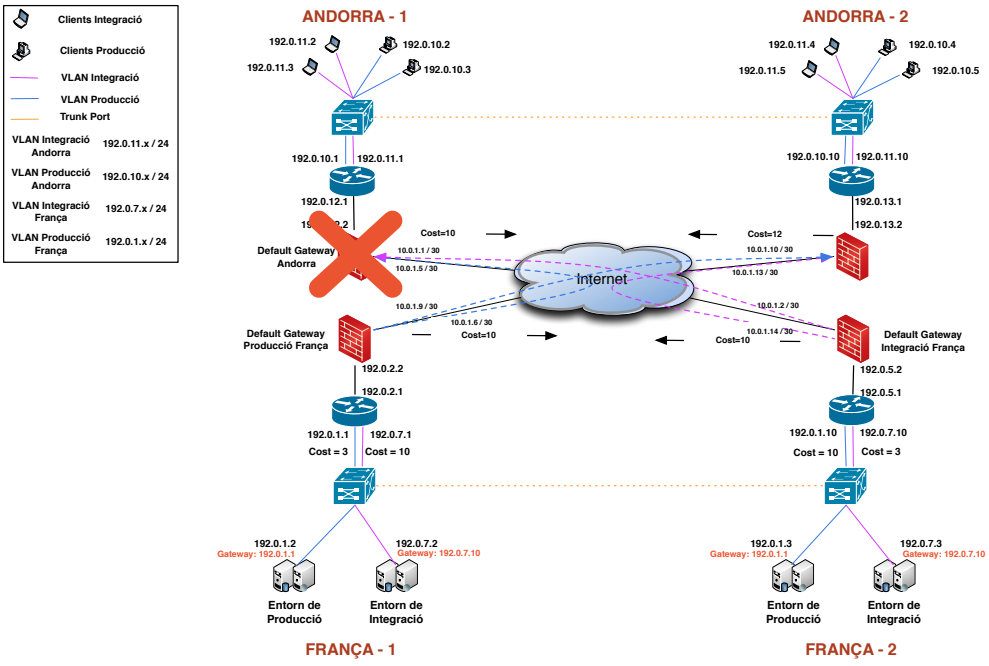
9.6 Model Complert Millorat amb dos firewalls caiguts

La configuració del Model Complert Millorat amb dos firewalls caiguts, segueix la mateixa configuració del Model Complert Millorat, és a dir, la configuració d'aquest model és exactament igual que l'anterior. La diferència radica en que en aquest Model, el firewall d'Andorra -1 estarà caigut i a més el firewall de França - 2 estarà també caigut.

Cal destacar que aquest fet és molt poc probable, però pot passar per la qual cosa la finalitat d'aquest model és poder analitzar la redundància de la configuració dissenyada i observar el seu comportament en la recerca de retards, pèrdua de paquets, hosts inaccessibles, etc.

El fet més rellevant d'aquest model és que la discriminació del tràfic de França deixar d'estar operativa, ja que el firewall de França - 2 no estarà operatiu, i tot el tràfic de Integració i Producció haurà d'estar assumit per el firewall de França - 1.

Finalment, la topologia d'aquest model quedaria representada de la següent manera:



Il·lustració 19 Model Complert Millorat amb 2 firewalls caiguts.

9.7 Model Complert Millorat amb volum de tràfic real

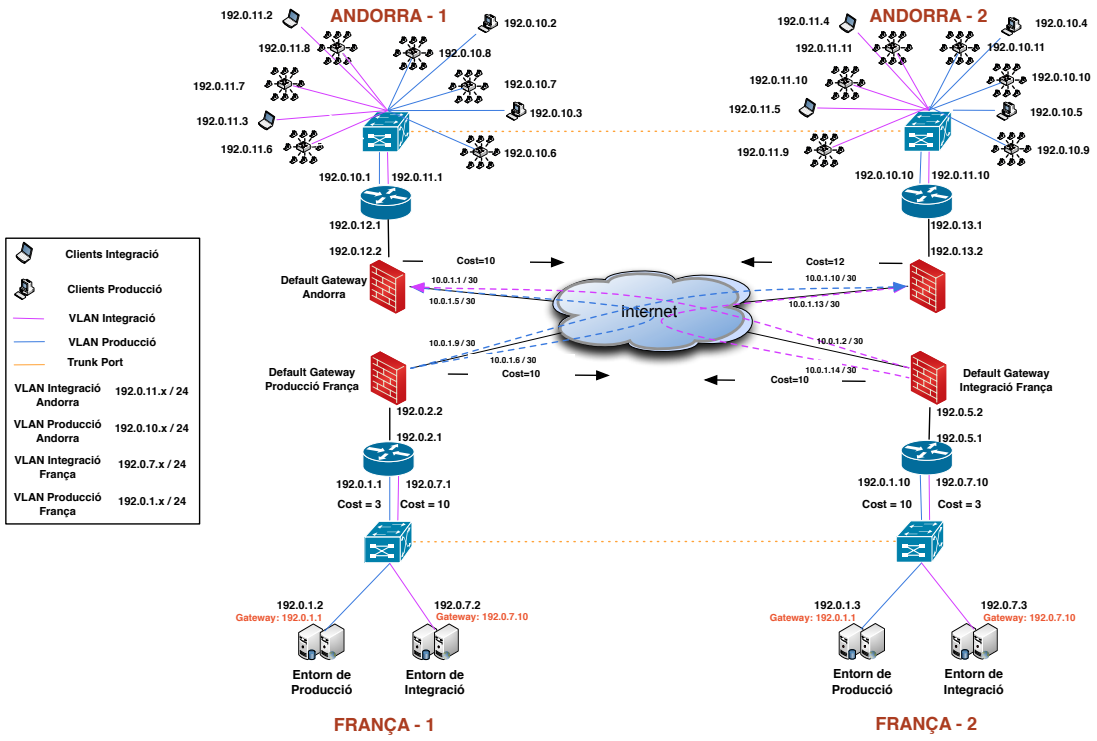
La configuració del Model Complert Millorat amb volum de tràfic real, segueix la mateixa configuració del Model Complert Millorat, la diferència radica en que en aquest model, s'ha afegit 12 estacions de treball més, cadascuna d'aquestes estacions representa 25 equips realitzant peticions als servidors.

Exactament, s'han afegit 6 estacions de treball per a Producció i 6 estacions de treball per Integració, el que representa 150 equips per Integració i uns altres 150 per Producció donant un total de 300 equips.

Amb aquest afegit es pretén omplir ambdues vlans, per realitzar una simulació el més pròxima a la realitat.

El punt més important d'anàlisis d'aquest model és la congestió dels servidors a les peticions dels equips.

Finalment, la topologia d'aquest model quedaria representada de la següent manera:



Il·lustració 20 Model Complert Millorat amb volum de tràfic real

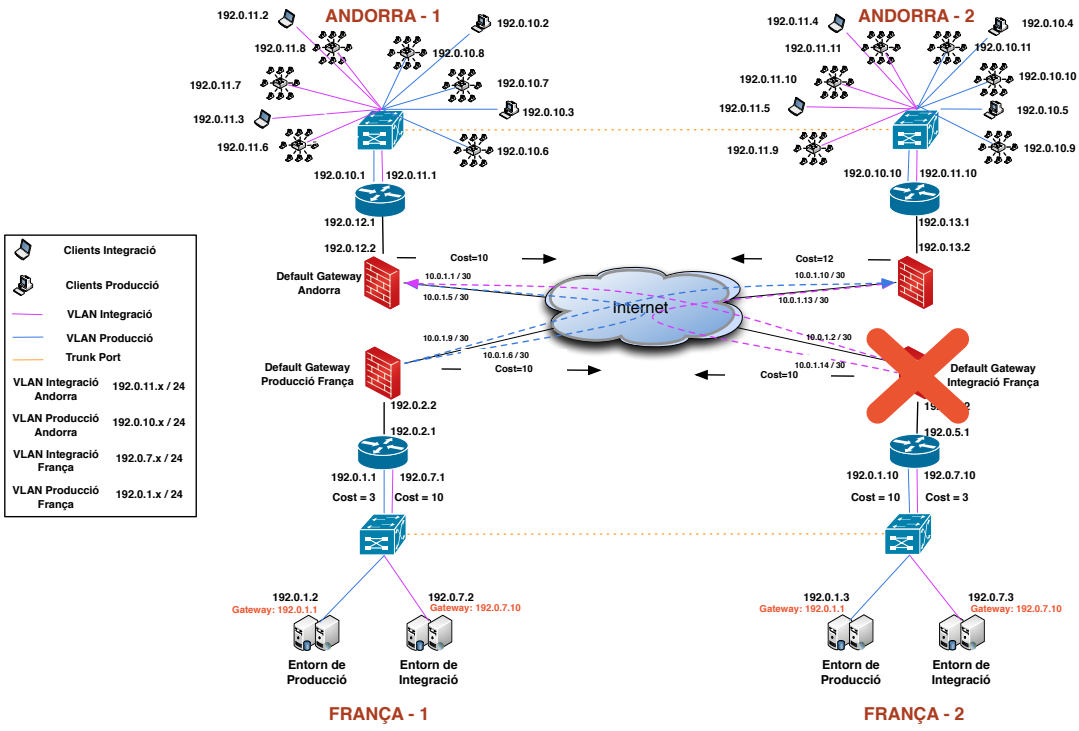
9.8 Model Complert Millorat amb volum de tràfic real i un firewall caigut

La configuració del Model Complert Millorat amb volum de tràfic real i un firewall, té exactament la mateixa configuració del Model Complert Millorat amb volum de tràfic, la diferència radica en que en aquest model, és que el firewall de França - 2 estarà caigut.

Per tant, el tràfic de Integració haurà de passar forçosament per el Firewall de França - 1. Al tenir un volum més gran de tràfic de gestionar, el retard del firewall es pot veure afectat al igual que l'ús de la CPU.

La finalitat d'aquest model, és la d'estudiar el comportament de flux de tràfic de la zona on està el firewall caigut, on s'estudiarà si amb un volum de tràfic real, el retard i la pèrdua de paquets es manté o no igual als models anteriors on el tràfic era mínim.

Finalment, la topologia quedarà de la següent forma:



Il·lustració 21 Model Complert Millorat amb volum de tràfic real amb 1 firewall caigut

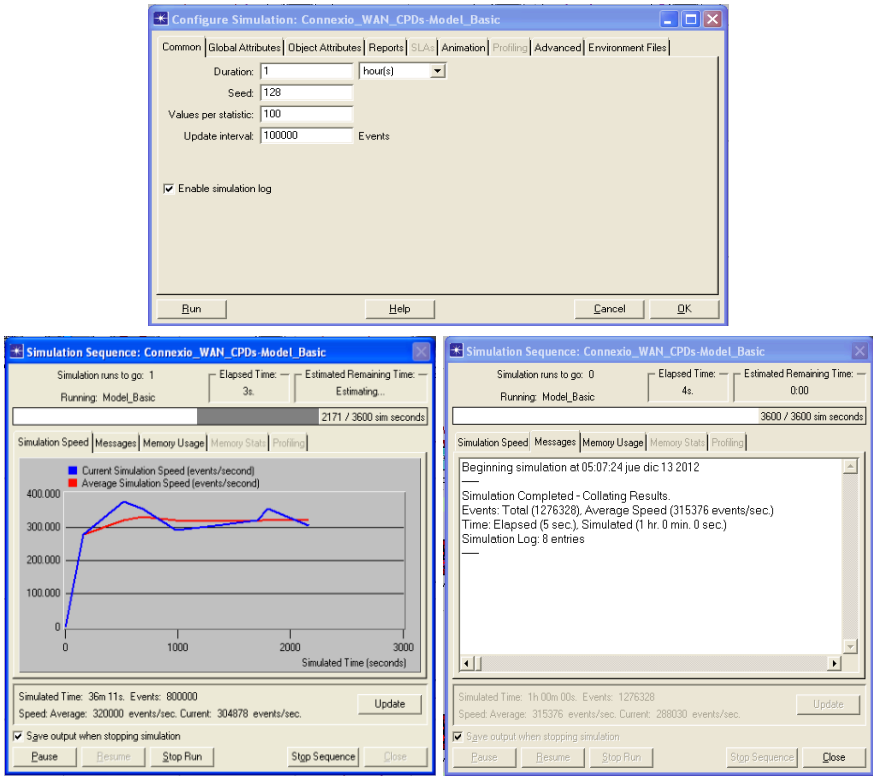
10 Simulacions

Una cop ja tenim construïts els models que es volen analitzar es passarà a simular el funcionament d'aquest amb la finalitat d' obtenir les estadístiques dels diferents nodes i enllaços que intervenen en cada escenari.

Aquesta simulació es dur a terme a partir del simulador que incorpora l'eina Opnet. En base dels resultats obtinguts en l'execució de la simulació es poden fer canvis i executar simulacions addicionals si es creu necessari, per a una millor comprensió del model estudiat.

Per a executar les simulacions es disposa de diferents opcions que es podent parametritzar com seran, el temps de durada, el valors, intervals i habilitar o deshabilitar diferents atributs, dependent del model que es vulgui simular.

Així mateix, quant la simulació esta en marxa es mostra una finestra de progrés i una vegada finalitzat aquest canvia per a mostrar-nos el resultat obtingut de la mateixa simulació amb els resultats, warnings i errors que s'han generat.



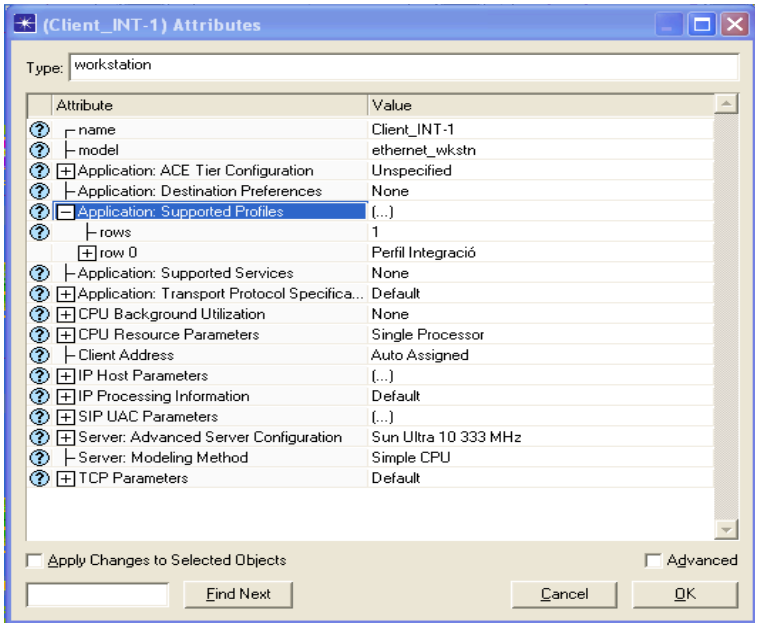
Il·lustració 22 Finestres d'Inici simulació, progrés i resultats

10.1 Simulació al Model Bàsic

La simulació que es realitzarà del model bàsic té com finalitat mostrar en una primera instància tots els components del modelat amb la seva configuració, funcionament i possibilitats que ens pot oferir per la simulació. D'aquesta manera obtenim la construcció d'una base per la resta de les simulacions.

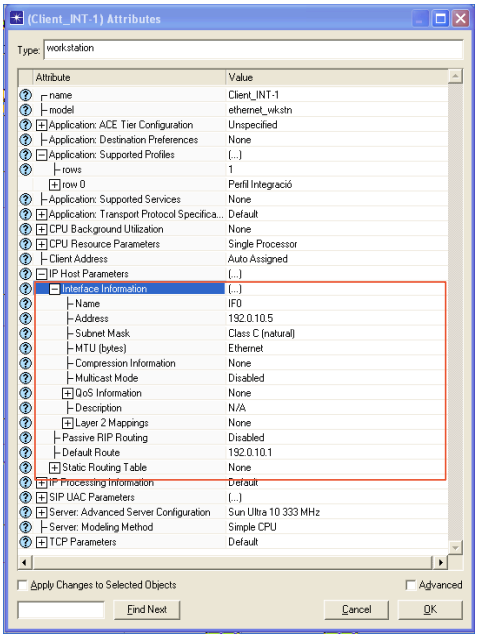
A continuació, es mostrarà les configuracions dels diferents nodes a partir de les següents imatges:

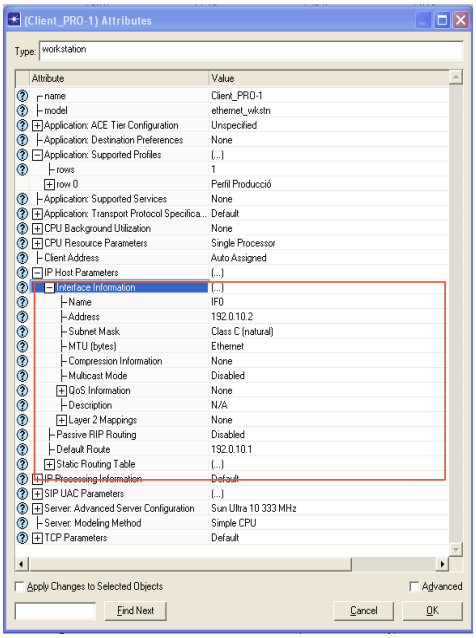
Per el que fa al tipus de clients, tenim dos tipus de clients, els clients de producció i els clients de Integració. De cadascun d'ells en tenim 4 de tipus ethernet workstation.



Il·lustració 23 Configuració Ethernet Workstation per Integració

Configuració de la interfície per assignar IP i default Gateway tan per Integració com per Producció

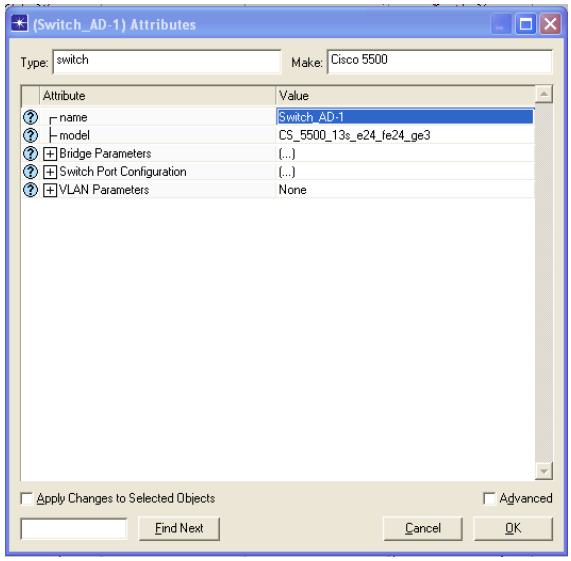




Il·lustració 24 Configuració Ethernet Workstation Integració

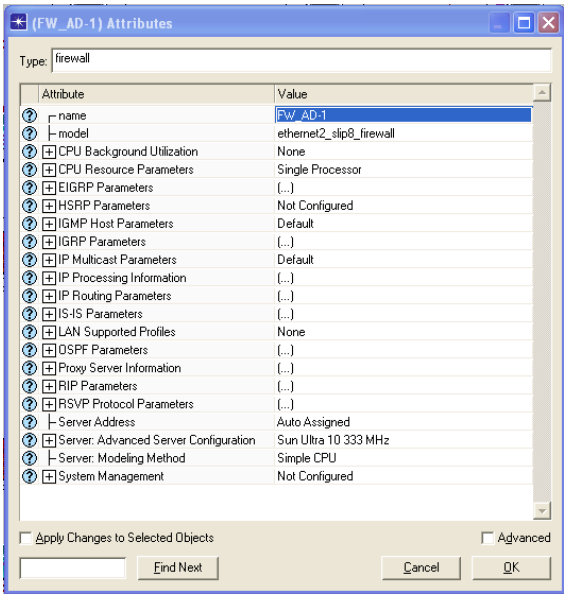
Il·lustració 25 Configuració Ethernet Workstation Producció

El Switch s'ha fet servir el Cisco Catalyst 5500, el qual en el model bàsic s'ha deixat la configuració que ve per defecte.



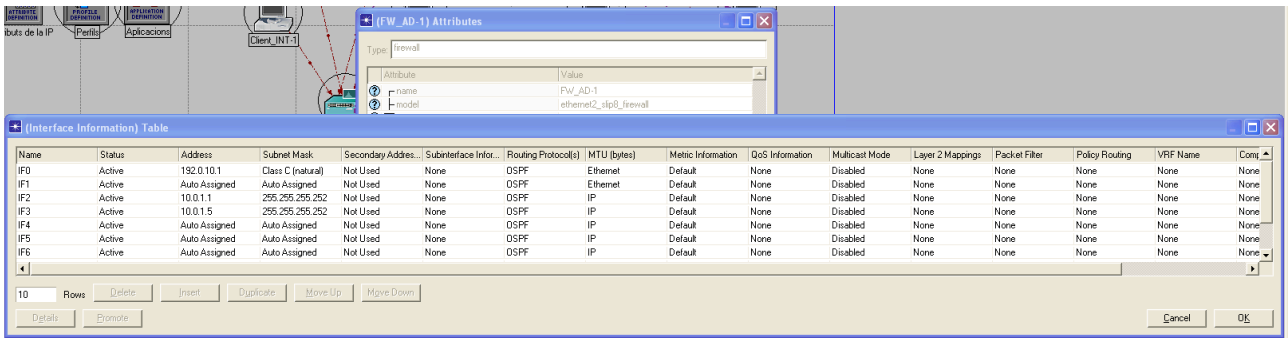
Il·lustració 26 Configuració Switch

Pel que es refereix al firewall, s'ha agafat el firewall genèric que disposa l'eina, ja que la versió IT Guru no conté cap firewall de Cisco. La configuració de filtratge per aplicació s'ha deixat per defecte "sense restriccions", ja que no és rellevant per aquest projecte.



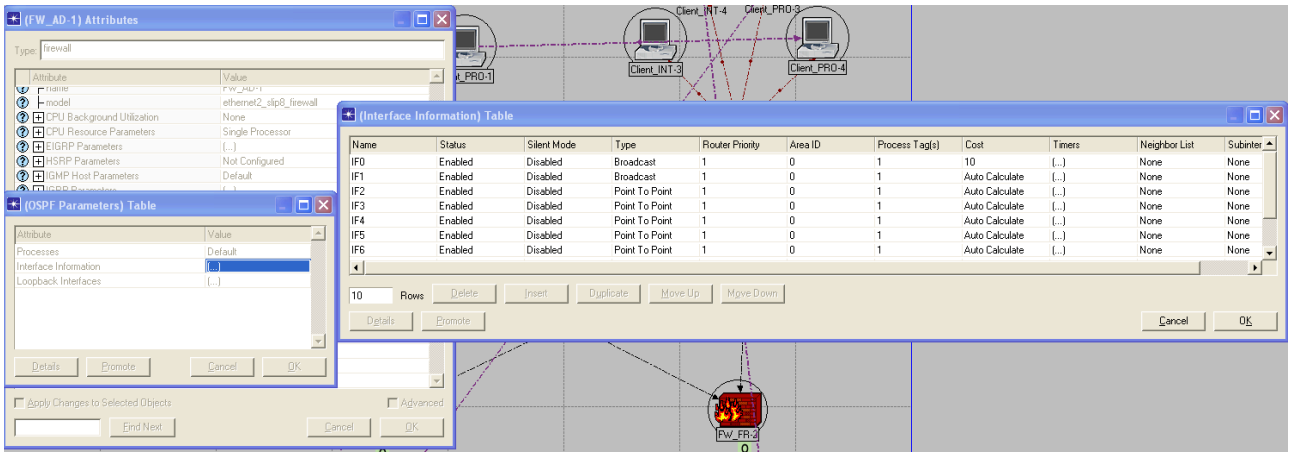
Il·lustració 27 Configuració Firewall

Pel que es refereix a la configuració del port ethernet i dels enllaços punt a punt, s'ha realitzat de la següent manera:



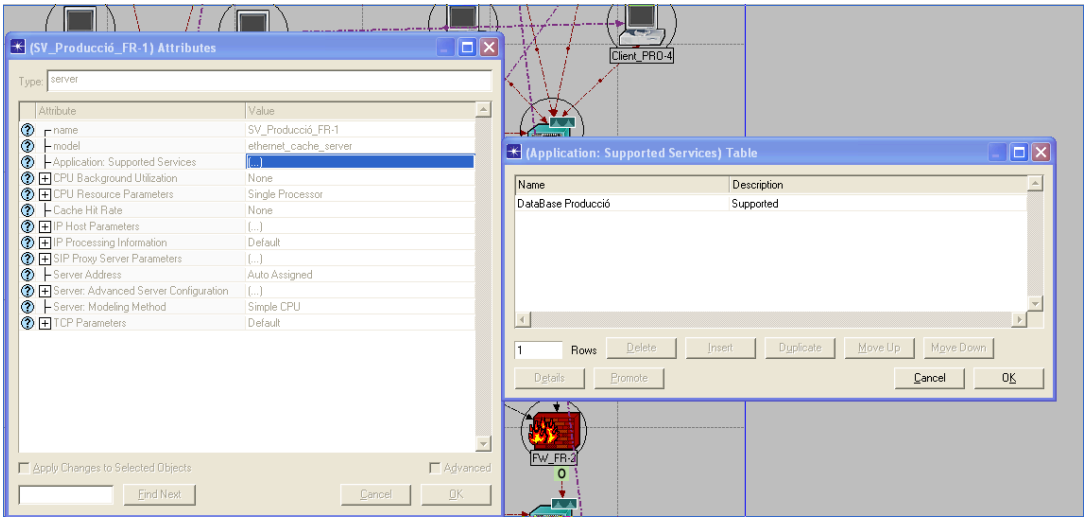
Il·lustració 28 Configuració enllaços firewall

Per tal de configurar dels costos dels enllaços del firewall, s'ha realitzat d'aquesta manera per al firewall de Andorra - 1



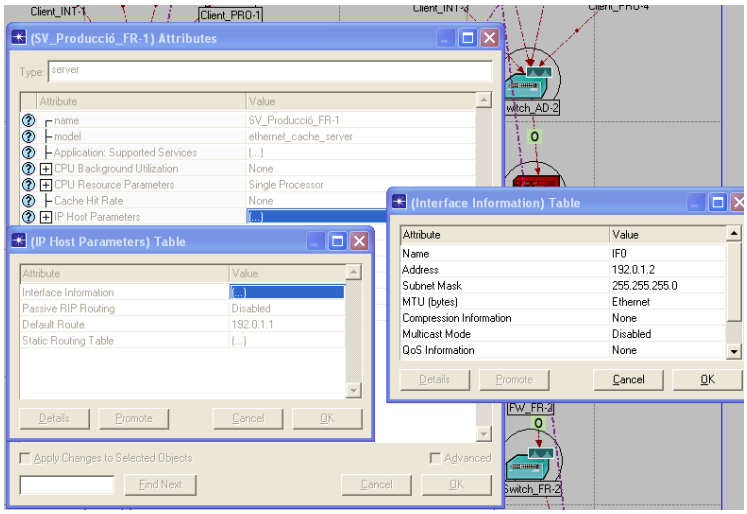
Il·lustració 29 Configuració Cost OSPF Firewall

La configuració dels servidors de Base de Dades de Producció, la seva configuració és la següent:



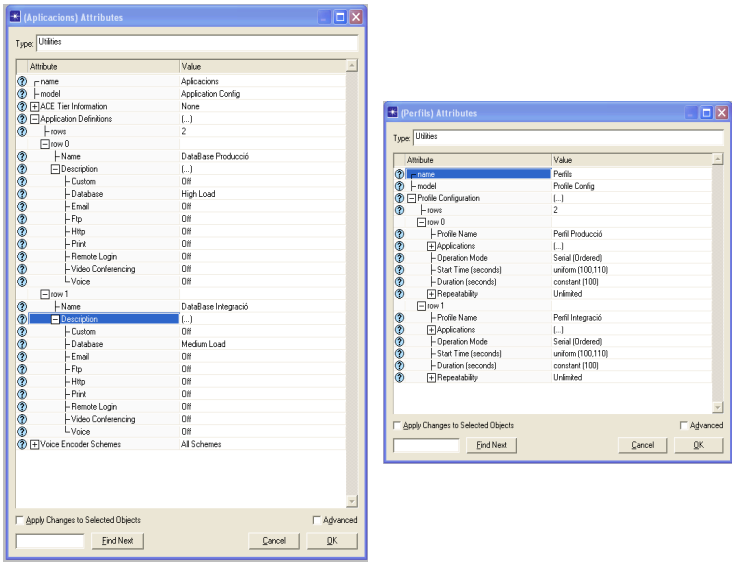
Il·lustració 30 Configuració Servidor Producció

La configuració de l'adreçament IP del servidor de dades de Producció es realitza de la següent manera:



Il·lustració 31 Configuració adreçament servidor de dades Producció

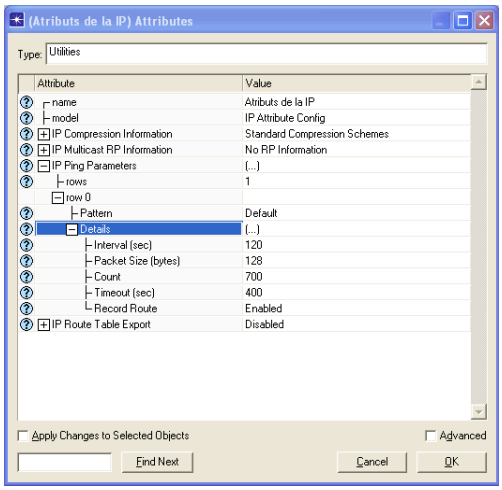
A la part de configuració de les aplicacions i els atributs el que configurem es per a poder fer servir aplicacions DataBase amb high load per als servidors de producció i medium load per als servidors d'Integració. Per a aquestes aplicacions creem els perfils Perfil Producció i Perfil Integració.



Il·lustració 32 Configuració Aplicacions

Il·lustració 33 Configuració Perfils

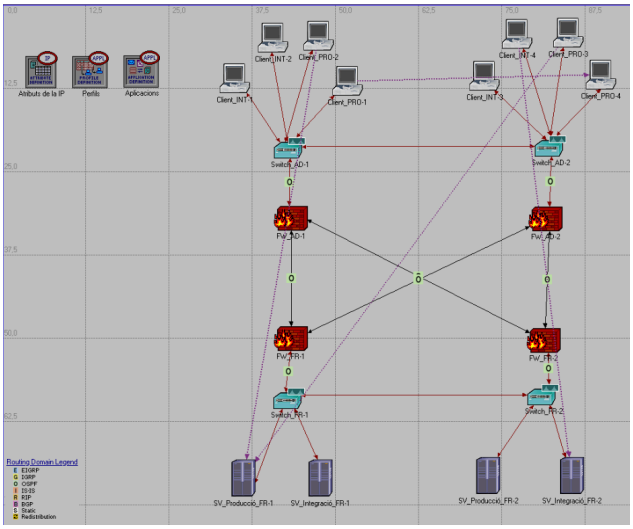
A la part de configuració dels Atributs de la IP amb la finalitat de poder realitzar pings i poder extreure els punts per on passa, s'ha configurat les peticions de ping de la següent manera:



Il·lustració 34 Configuració Atributs de la IP

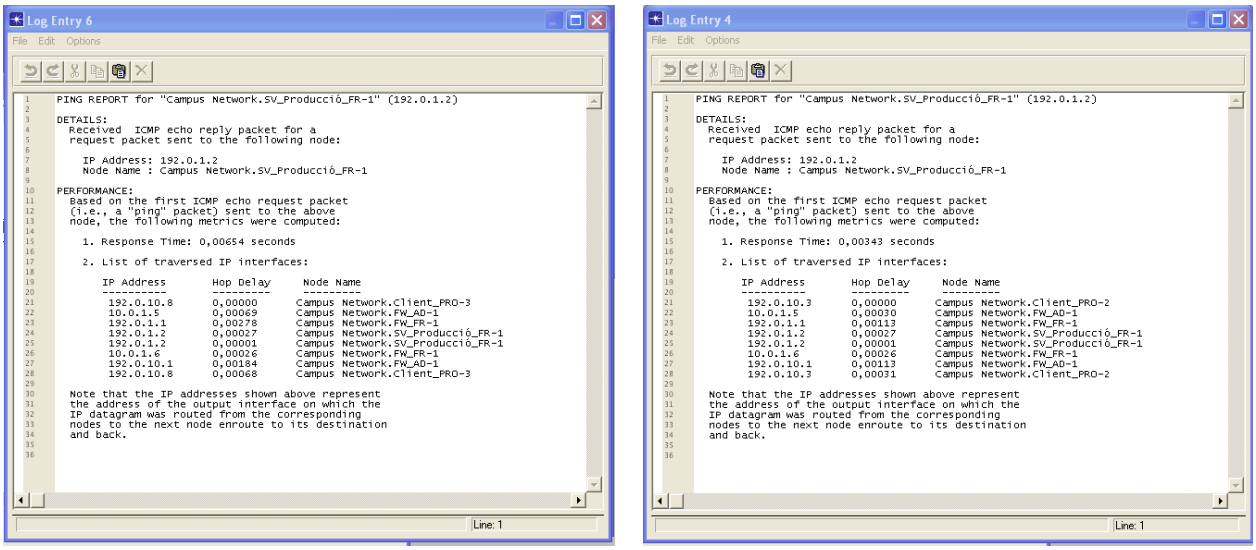
Les connexions entre nodes que es faran servir per a totes elles són de 100 BaseT, llevat de les connexions punt a punt entre els firewalls que són PPP DS1.

A continuació, es realitzarà la primera simulació de 60 minuts per al model bàsic.



Il·lustració 35 Model Bàsic OPNET

En primer lloc es mostraran els pings realitzat dels clients de Producció des de Andorra - 1 i de Andorra -2.

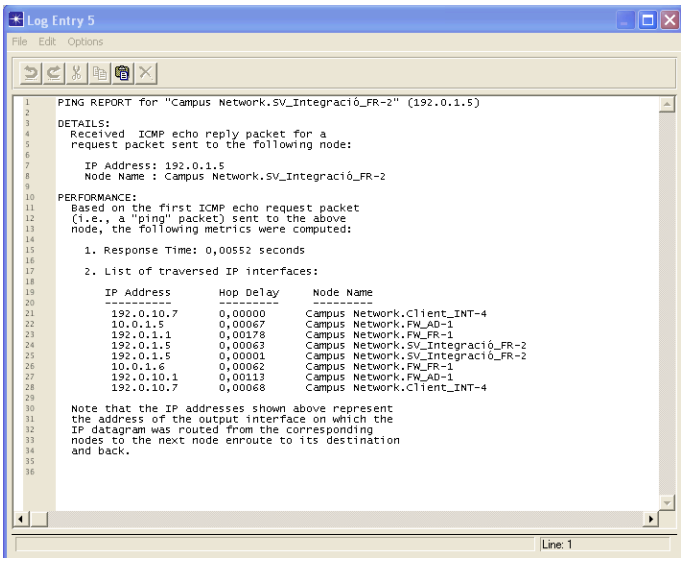


Il·lustració 36 Ping tràfic Producció Andorra-1 a França-1

Il·lustració 37 Ping tràfic Producció Andorra-2 a França-1

Com s'observar en els pings anteriors, tal i com s'ha dissenyat el model bàsic, tan si es fa d'Andorra 1 o d'Andorra 2, es surt per el firewall d'Andorra - 1 i es rep la resposta per aquest firewall.

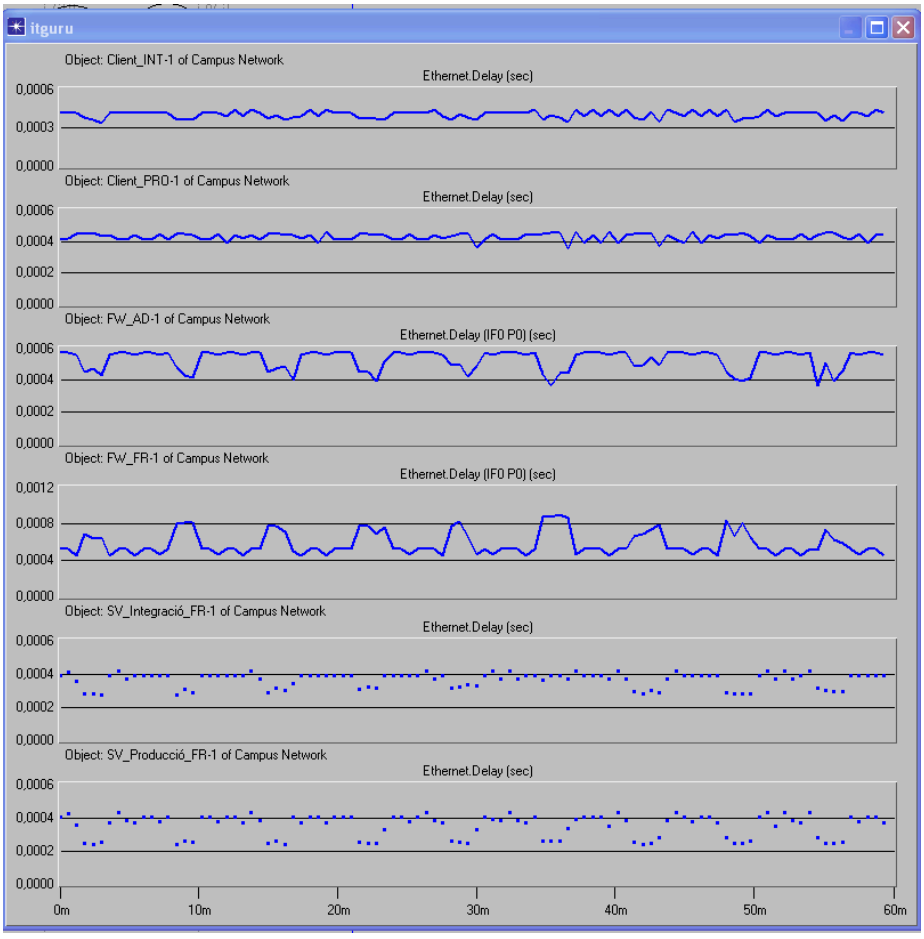
En segon lloc, es mostrarà un Ping realitzat d'un client d'Integració des de Andorra - 2 a França - 2.



Il·lustració 38 Ping tràfic Integració Andorra-2 a França-2

Podem observar que el disseny ha estat satisfactori, ja que el redireccionament funciona, ja que els firewalls de Andorra - 1 i França - 1 són els que estan gestionant completament el tràfic.

En tercer lloc, es mostrarà els temps de resposta de cadascun dels equips, per veure els equips que ocasionen major retard, cal destacar que el retard total es visualitza en els logs dels pings anteriorment vist, s'ha de recalcar que al no poder-se configurar la seguretat dels enllaços punt a punt, hem de penalitzar als firewall amb un retard de 20-30ms més per la xifratge i desxifratge dels paquets, que no s'ha pogut simular.

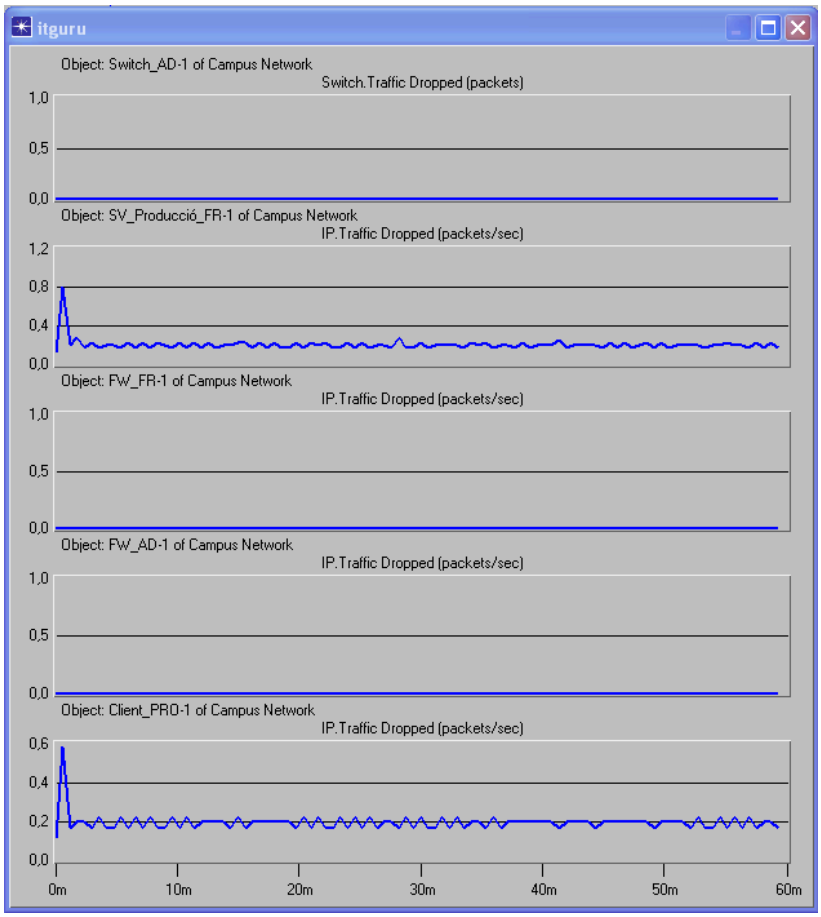


Il·lustració 39 Estadistica comparativa del retard dels principals equips.

Com es pot observar en l'anterior il·lustració els equips que proporcionen el major retard, són els firewalls, tot i que no tenen la penalització dels 20 - 30 ms per el xifratge i desxifratge del sistema de seguretat, segueix sent l'equip amb major retard degut al canvi de línia ethernet a punt a punt PPP DS1. També en

segon lloc hi ha els clients de producció, els qual el volum de dades és més gran i té un lleuger temps de resposta més gran que els de Integració.

Per últim es mostrarà els paquets perduts per alguns dels dispositius principals, per tal de verificar que el disseny sigui correcte.



Il·lustració 40 Estadistiques paquets perduts dels principals dispositius

Com es pot observar, els firewalls principals i els Switchs, no han tingut cap pèrdua de paquet, durant els 60 minuts de simulació. En canvi, els client de producció i el servidor de producció d'Andorra - 1 i França respectivament, tenen alguns paquets que han perdut, segurament per els retards de les peticions prèvies als paquets perduts, per la qual cosa, estan dintre dels valors normals de la simulació.

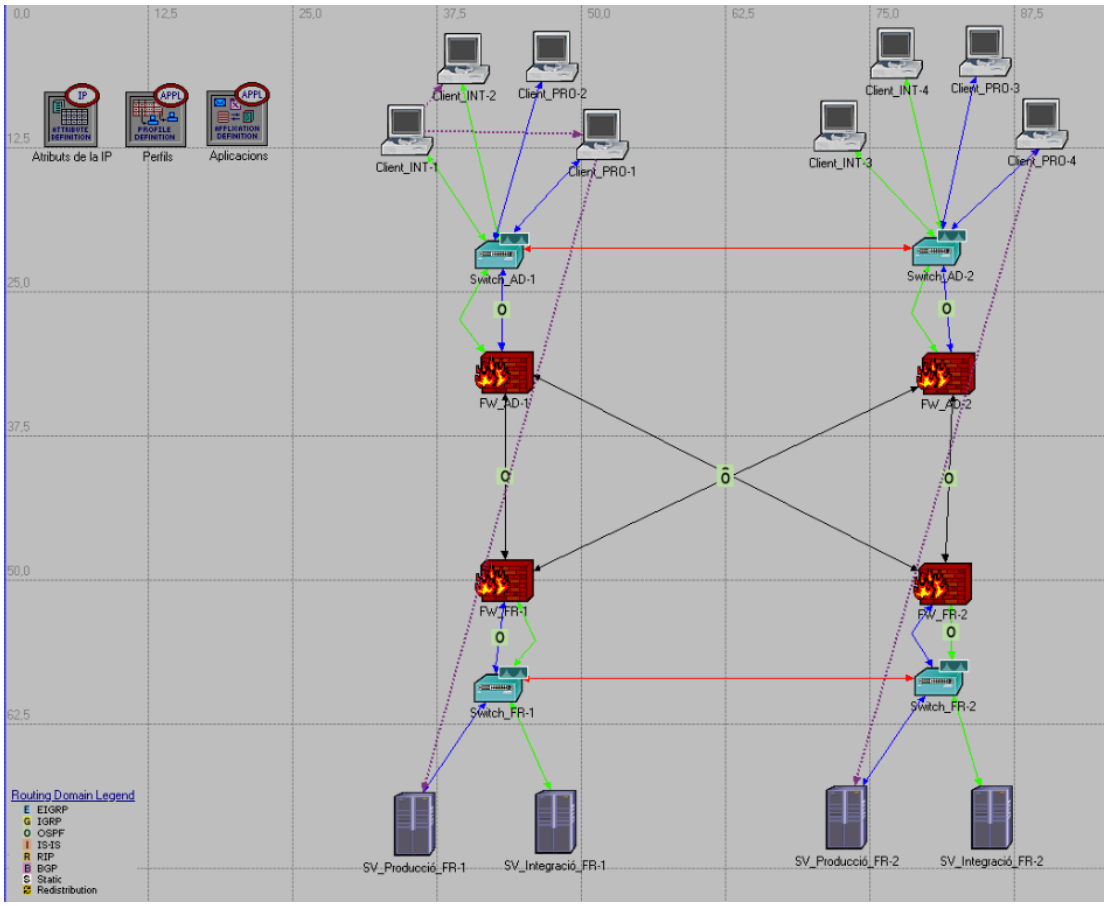
Per tant, el model bàsic, ha passat correctament la simulació, ja que, els temps de resposta han estat correctes, la distribució del tràfic ha estat correcta i la pèrdua de paquets està dintre dels marges de la normalitat.

10.2 Simulació al Model Complert Millorat paral·lel a la maqueta

La simulació que es realitzarà del model Complert Millorat paral·lel a la maqueta té com finalitat mostrar el comportament que tindrà la maqueta i l'entorn real on es ficarà en producció, on podrem extreure informació comparativa entre l'entorn de proves real i l'entorn virtualitzat.

En aquest entorn, es segueix la mateixa distribució que el model bàsic, però amb la implementació de les Vlans, per la qual cosa, s'haurà de mostrar la configuració dels switchos, per les vlans i la modificació de la configuració del firewall.

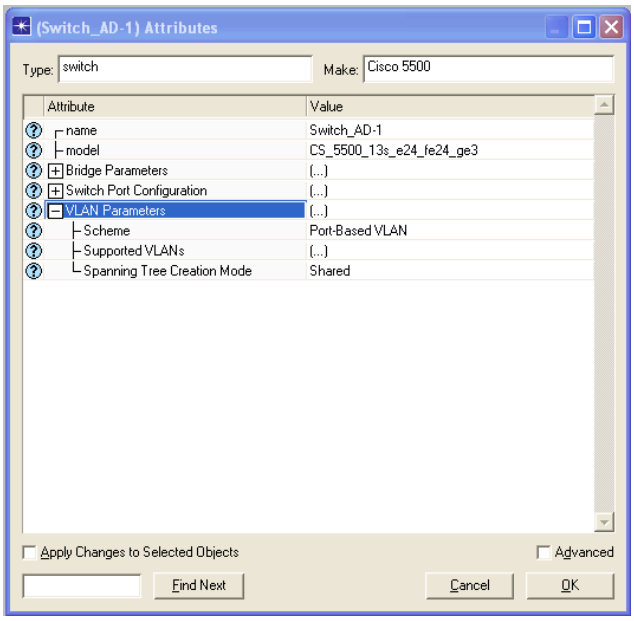
L'esquema del Model Complert Millorat paral·lel a la maqueta en l'eina OPNET és el següent:



Il·lustració 41 Esquema Model Complert Millorat Paral·el a la maqueta

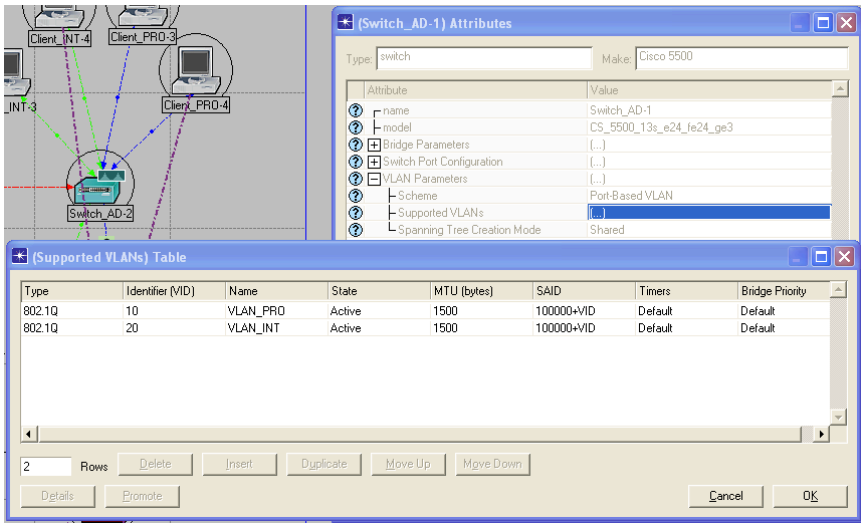
Per tal de dur a terme la simulació d'aquest model el switch ha de tindre configura l'opció de les vlans.

En primer lloc, mostrarem com s'activa aquesta opció dins del menú de configuració del switch, activant l'opció: Scheme en Port-Based-VLAN.



Il·lustració 42 Activar VLANS en el switch

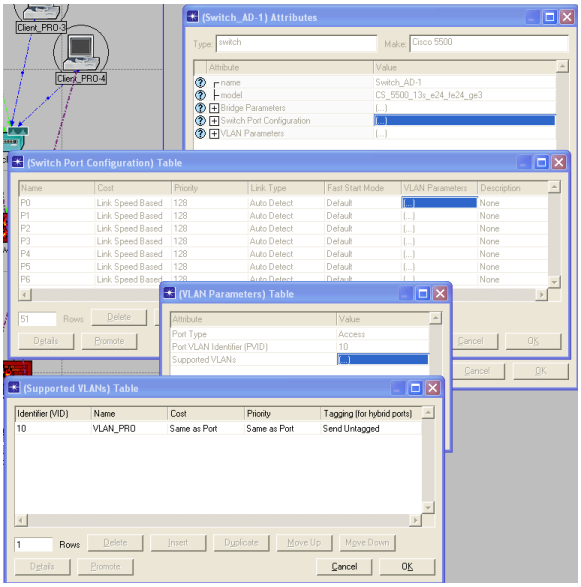
En segon lloc, es mostrarà com es configura cadascuna de les vlans, en aquest cas són dos, la vlan de Producció que tindrà el ID = 10 i la vlan de Integració que tindrà el ID = 20.

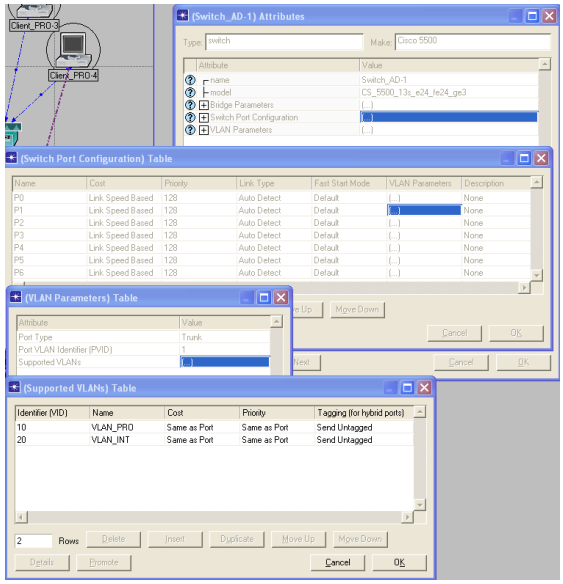


Il·lustració 43 Configuració Vlans en el switch

En tercer lloc, es mostrarà com es configura cadascun dels ports en el switch. Els equips que són de Producció se'ls s'ha de configurar el seu port en la vlan de Producció, en canvi els equips d'Integració se'ls a de configurar el port on estiguin connectats a la vlan d'Integració.

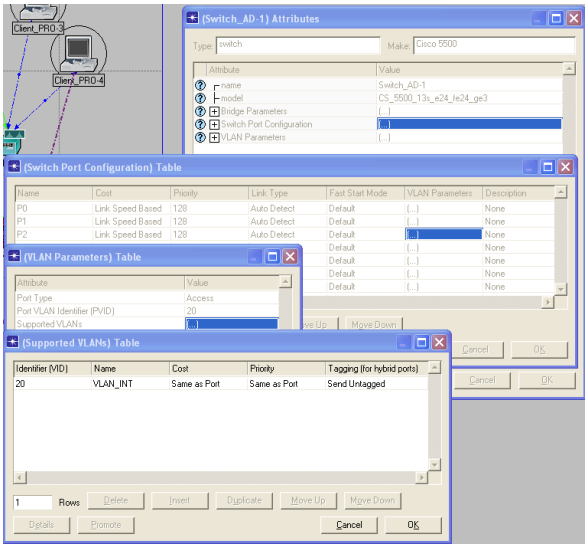
D'altra banda, hi ha connexions per on han de passar totes dues vlans, per lo que també es mostrarà com es configurà els Trunk ports que permeten passar dos o més vlans alhora.





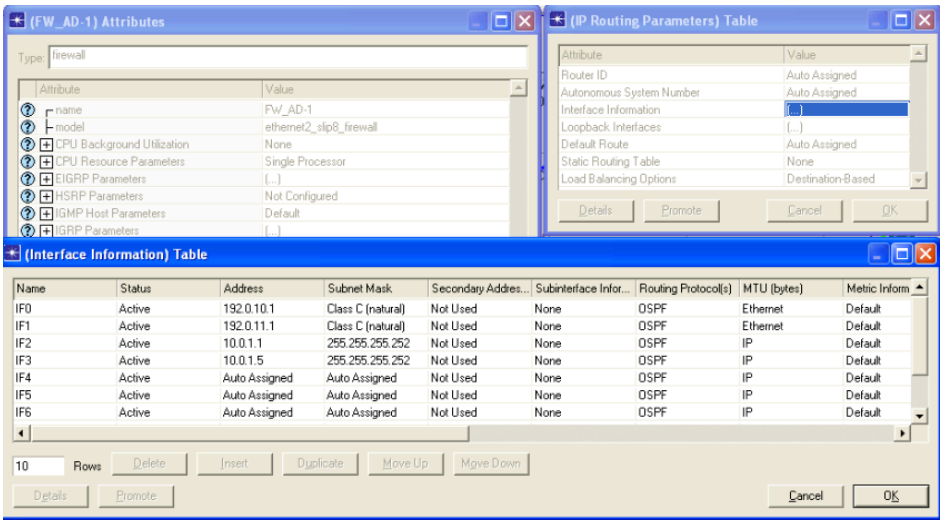
Il·lustració 44 Configuració d'un port del swtich per la vlan d'Integració

Il·lustració 45 Configuració d'un port del swtich com Trunk port

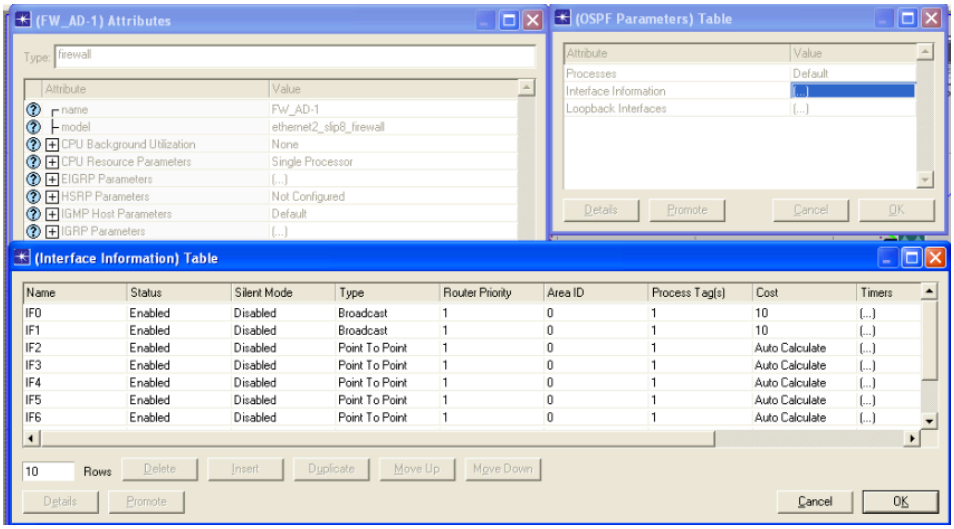


Il·lustració 46 Configuració d'un port del switch per la vlan d'Integració

En aquest model, els firewalls s'ha tingut d'introduir un enllaç més amb la finalitat de diferencia el tràfic de Producció amb el d'Integració, també s'hauria pogut fer amb un sol enllaç amb 2 VRF, però s'ha triat la primera opció per obtenir major rendiment.



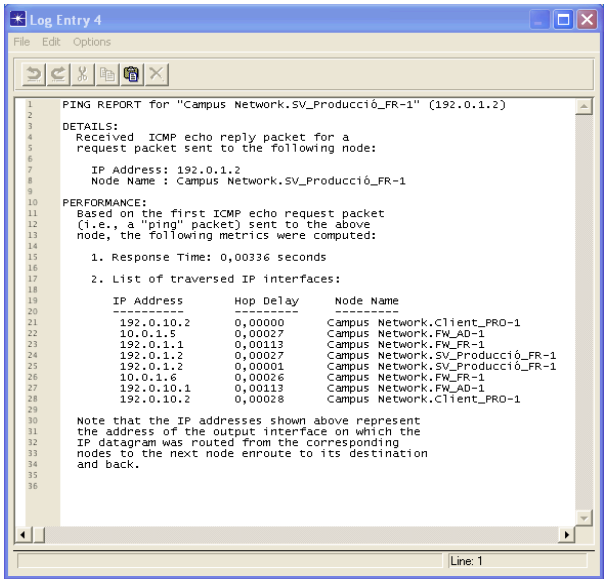
Il·lustració 47 Configuració firewall 2n enllaç per a les vlans

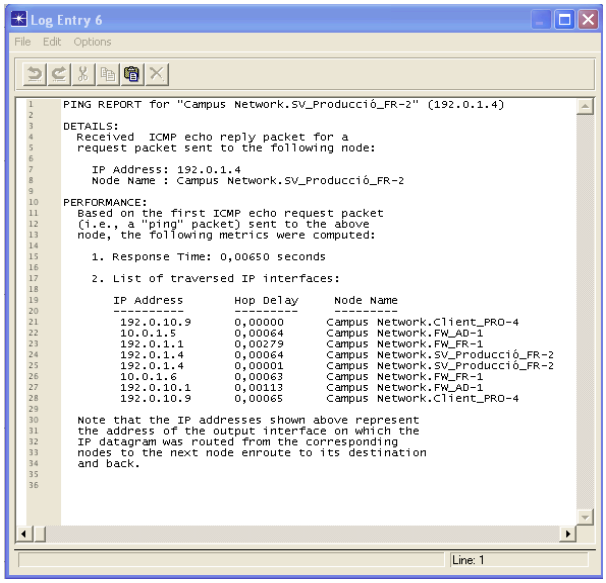


Il·lustració 48 Configuració del cost del 2n enllaç del firewall.

Com es pot observar en les dues anteriors il·lustracions, s'ha afegit el 2n enllaç per tal de que el firewall gestioni les dos vlans, i a més se li ha configurat el cost, que com no es fa discriminació de les vlans, és exactament el mateix que el del altre enllaç.

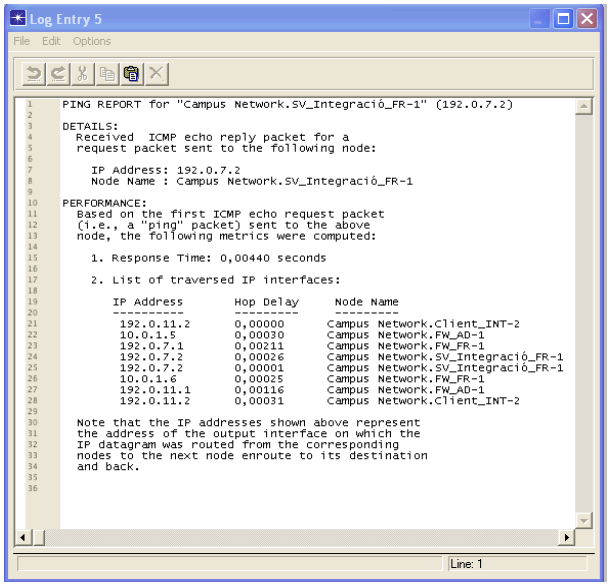
A continuació es mostrarà els resultats dels pings que s'han realitzat durant els 60 minuts que s'han emulat en l'eina OPNET, s'han triat 2 pings de Producció i 2 pings d'Integració cadascun d'ells en una zona diferent.

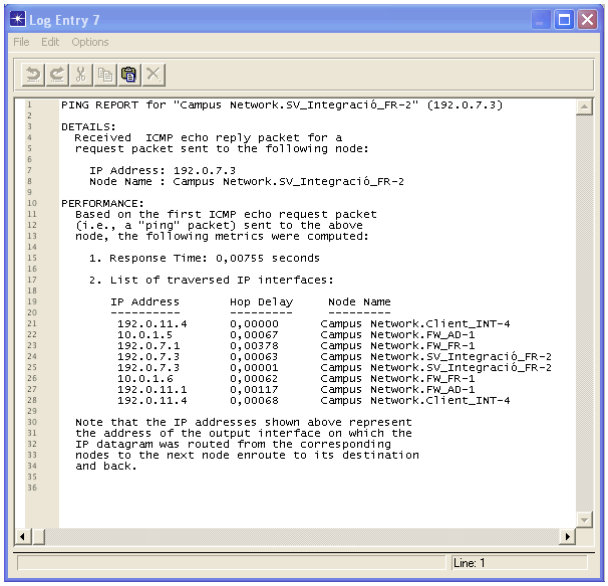




Il·lustració 49 Ping tràfic Vlan Producció Andorra-1 a França-1

Il·lustració 50 Ping tràfic Vlan Producció Andorra-2 a França-2



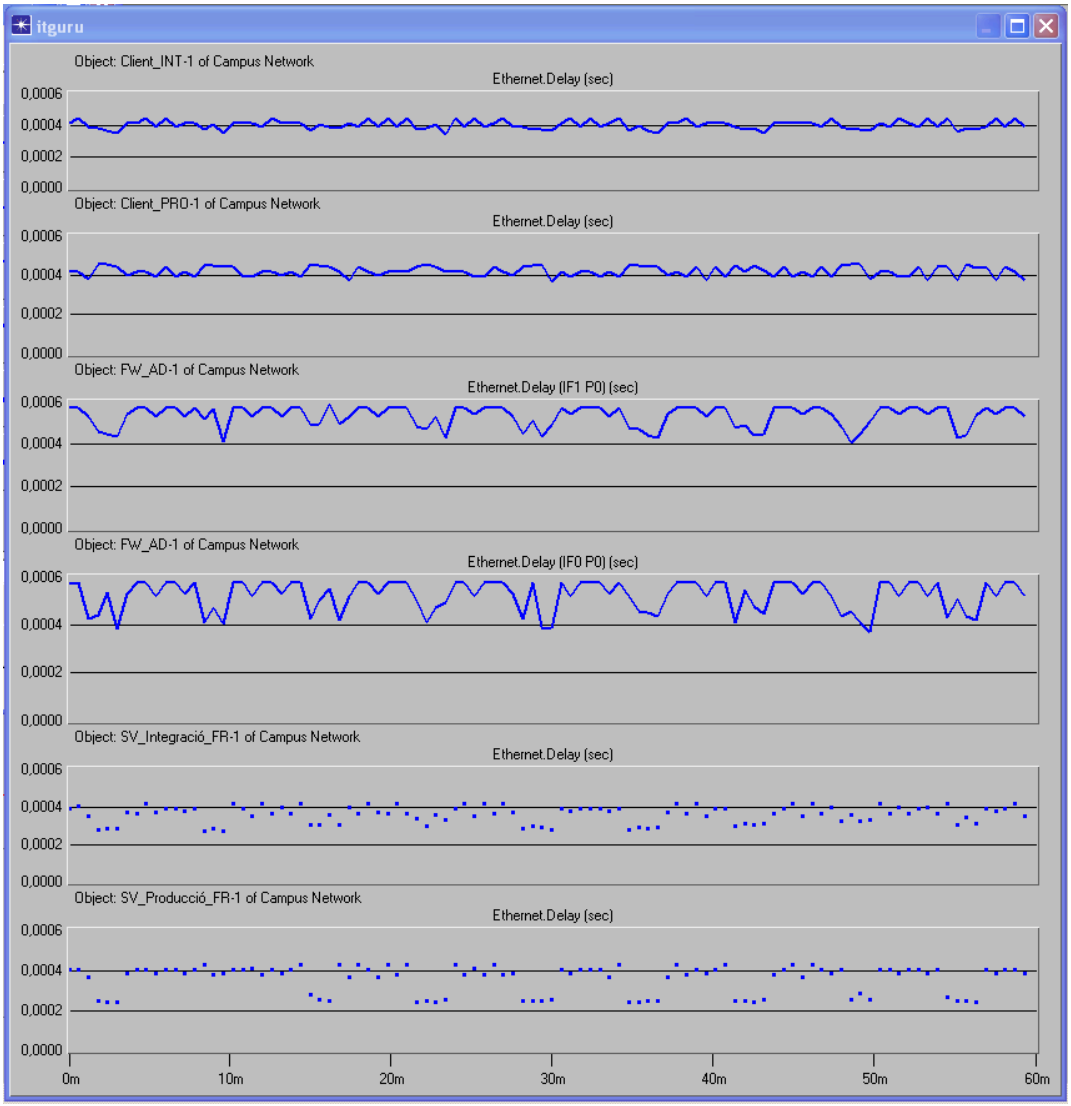


Il·lustració 51 Ping tràfic Vlan Integració Andorra-1 a França-1

Il·lustració 52 Ping tràfic Vlan Integració Andorra-2 a França-2

Com es pot observar en els 4 pings anteriors el tràfic passa sempre per els firewalls Andorra - 1 i França - 1 independentment de la zona on es trobi l'equip. com s'ha dissenyat, per tant el comportament d'aquesta xarxa és correcta.

D'altra banda, es mostrarà el temps de resposta o retard, dels principals dispositius que participen en la simulació, sense tenir en compte el retard generat pel xifratge i desxifratge com s'ha comentat abans, degut a que no es pot simular en aquesta versió.

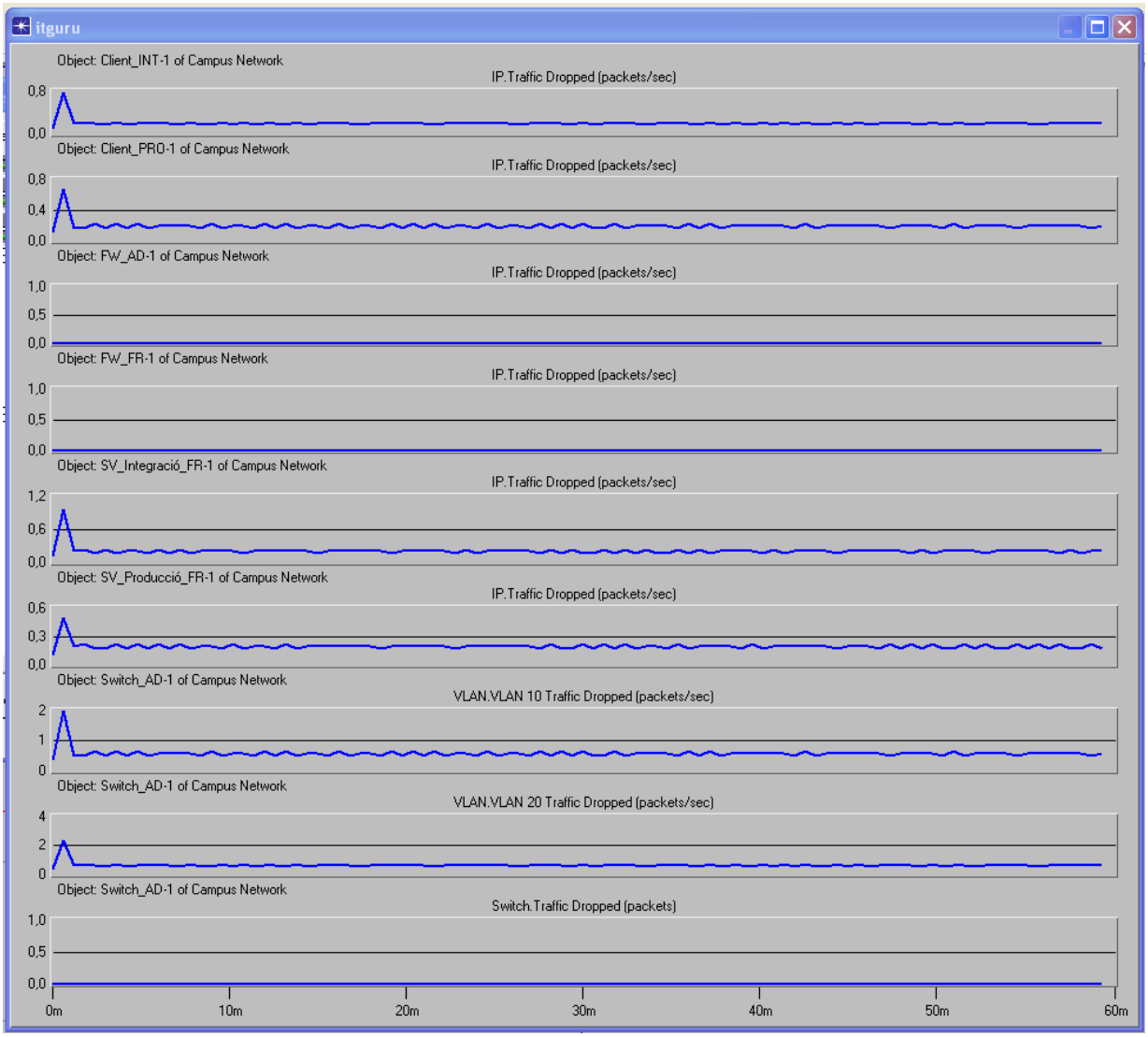


Il·lustració 53 Estadística comparativa del retard del Model Complert Millorat Maqueta

Un cop visualitzada les estadístiques de la il·lustració anterior, podem apreciar que el retard es manté gaire bé igual al del model bàsic, cal destacar que els

clients de producció s'ha estabilitzat el seu retard, sent igual que els clients de integració, segurament per les vlans. Igualment, veiem que el comportament de la xarxa és correcte i que els temps de resposta estan dins dels marges tolerables.

Per últim es mostrarà els paquets perduts per alguns dels dispositius principals, per tal de verificar que el disseny sigui correcte.



Il·lustració 54 Estadístiques paquets perduts dels principals dispositius Model Complert Maqueta

Les estadístiques dels paquets perduts són exactament iguals al del Model Bàsic, per lo que la inserció de les vlans no ha afectat en cap moment al

disseny de la xarxa. A més, ara al estar les vlans, el switch detectat els paquets perduts per cada vlan a partir del client - servidor, ja que els paquets perduts a causa d'ell són 0.

Finalment, podem concloure que la simulació d'aquest model és satisfactòria, i els resultats obtinguts estan dintre dels marges esperats.

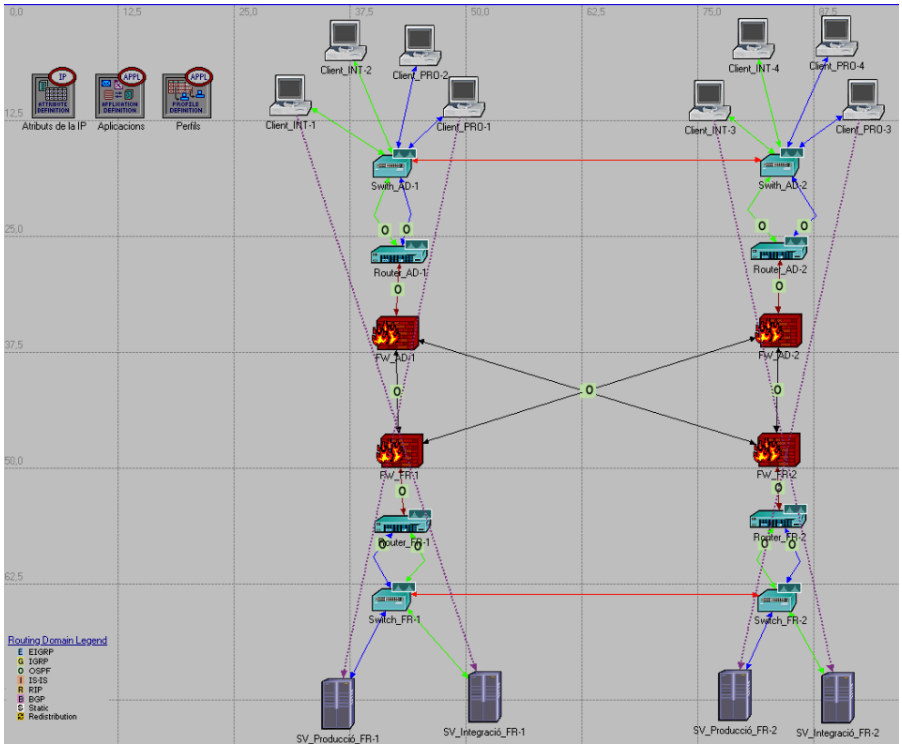
10.3 Simulació al Model Complert Millorat

La simulació que es realitzarà del model Complert Millorat té com finalitat mostrar el comportament que tindrà la xarxa al introduir els routers i quin serà el seu comportament, beneficis i contres de la seva implementació.

En aquest entorn, es segueix la mateixa distribució que el model bàsic, però només amb la implementació de les vlans, ja que, en aquest model es discriminarà el tràfic de Producció amb el d'Integració, en la zona de França. On el router i firewall de França - 1 només haurà de gestionar el tràfic de Producció i el router i firewall de França - 2 només haurà de gestionar el tràfic de Integració.

Per la qual cosa, s'haurà de mostrar la configuració de les interfícies i els costos d'un dels routers.

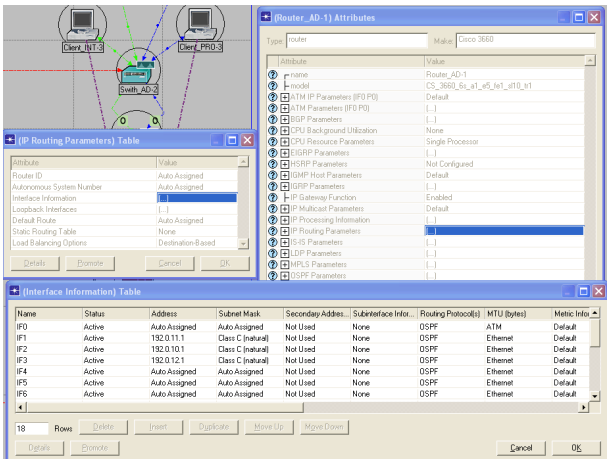
L'esquema de la simulació al Model Complert Millorat de l'eina OPNET és el següent:



Il·lustració 55 Esquema Model Complert Millorat

En primer lloc, mostrarem el router que s'ha triat que és un cisco 3660, el qual s'ha creat un enllaç amb el firewall i dos enllaços amb el switch per tal de gestionar les dues vlans.

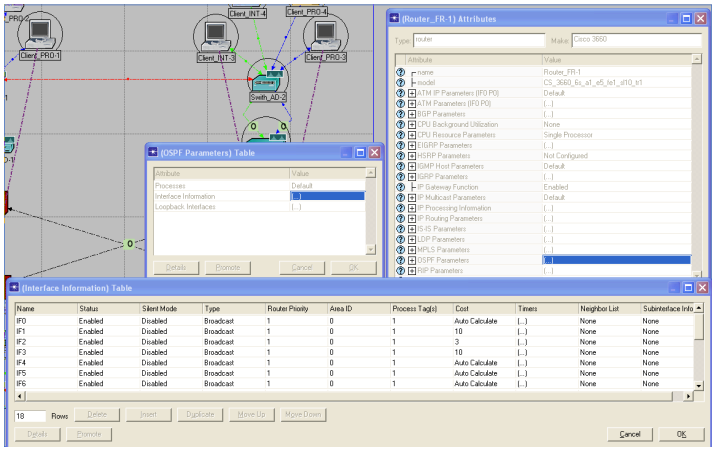
La configuració de cadascuna de les interfícies del router és la següent:



Il·lustració 56 Configuració interfícies router

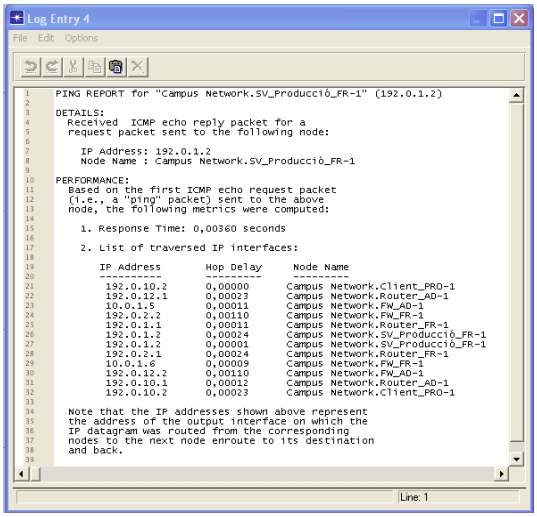
Per tal de realitzar una discriminació entre el tràfic de Producció i Integració, s'ha de modificar els costos dels enllaços de Producció i Integració de router de França - 1 i de França - 2. En el cas del router de França -1 el cost de l'enllaç de Producció serà més baix que el de Integració i viceversa per al router de França - 2. L'enllaç amb el firewall es deixarà un cost 10 en tots dos routers i firewalls.

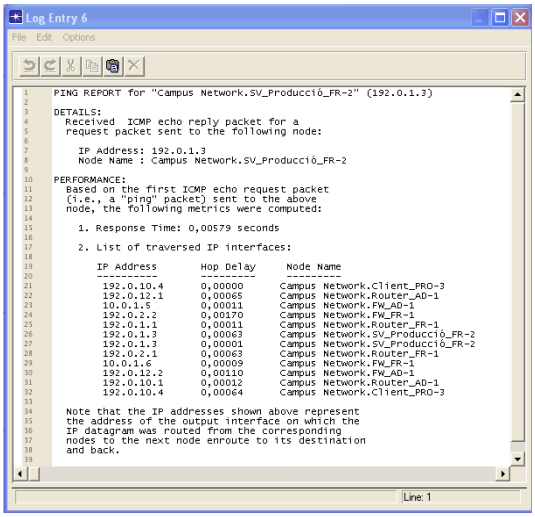
La configuració dels costos per el router de França - 1 és:



Il·lustració 57 Configuració cost OSPF interfície router

A continuació es mostrarà els resultats dels pings que s'han realitzat durant els 60 minuts que s'han emulat en l'eina OPNET, s'han triat 2 pings de Producció i 2 pings d'Integració cadascun d'ells en una zona diferent.

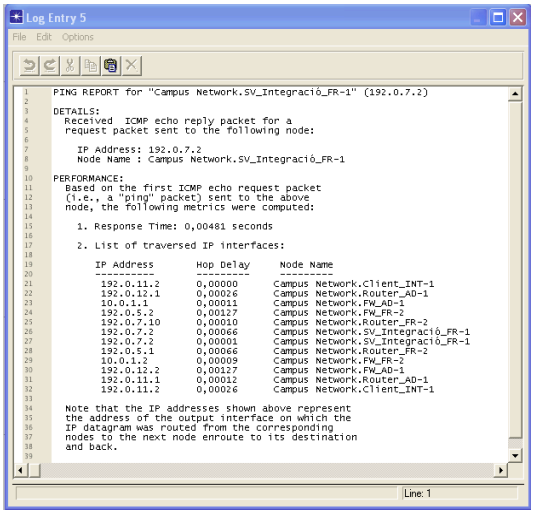


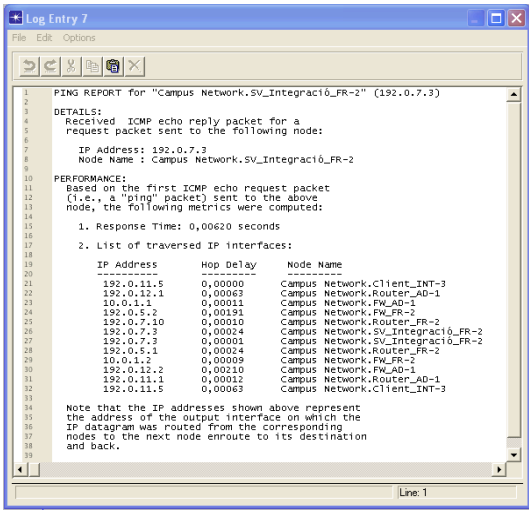


Il·lustració 58 Ping tràfic discriminat Producció Andorra-1 a França-1

Il·lustració 59 Ping tràfic discriminat Producció Andorra-2 a França-2

Com podem observar en el log dels dos pings del clients de Producció cap a els servidors de Producció de França, surten per el firewall de Andorra - 1, ja que és el que s'ha configurat com el principal per la zona d'Andorra. I passa l'entrada i la resposta el firewall i router d'Andorra - 1, ja que aquest, són els encarregats de gestionar el tràfic de producció.





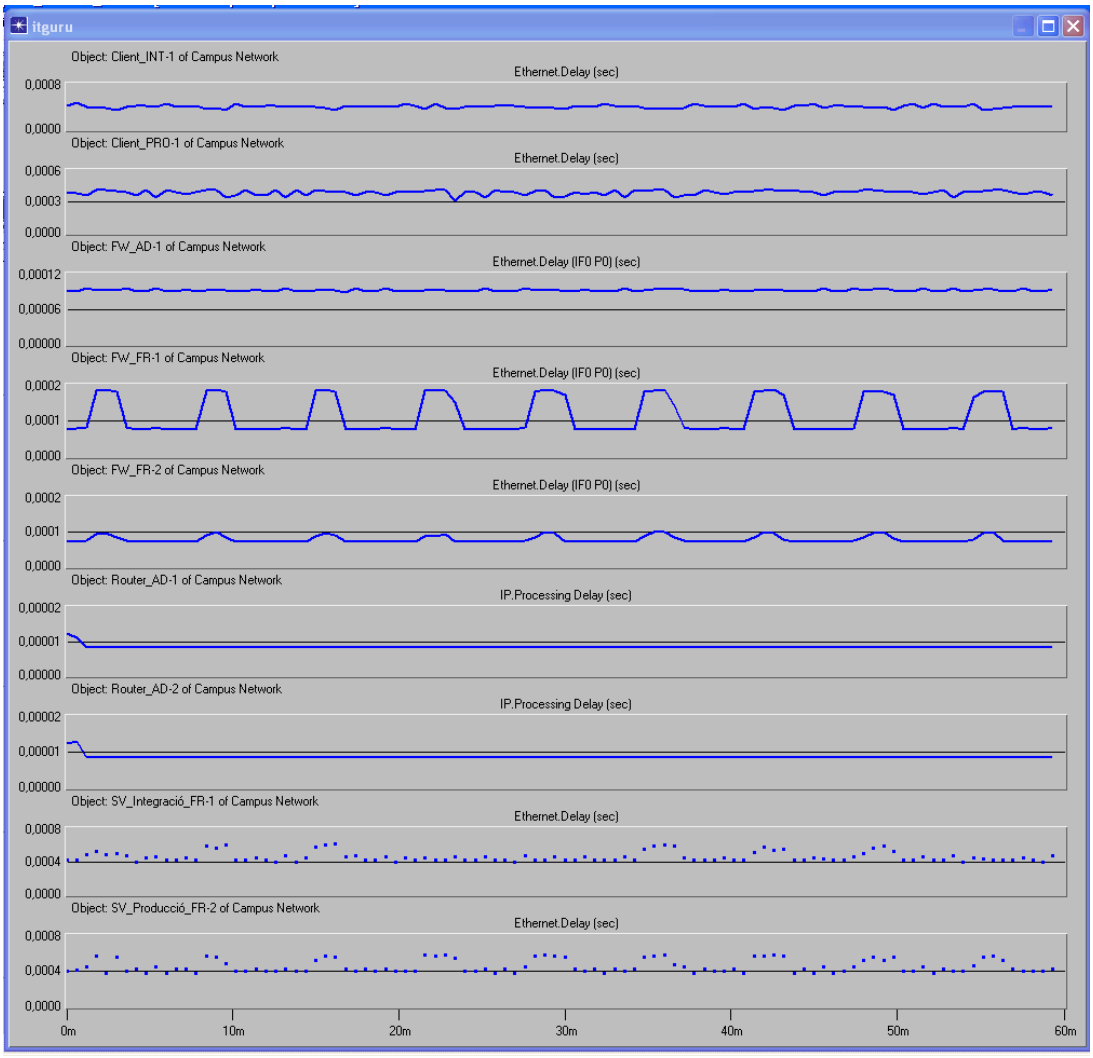
Il·lustració 60 Ping tràfic discriminat Integració Andorra-1 a França-1

Il·lustració 61 Ping tràfic discriminat Integració Andorra-2 a França-2

Com podem observar en el log dels dos pings del clients de Integració cap a els servidors de Integració de França, surten per el firewall de Andorra - 1, ja que és el que s'ha configurat com el principal per la zona d'Andorra de la mateixa que els de Producció. En canvi, l'entrada i sortida d'aquest tràfic en la zona de França és gestionada per el firewall i router de França - 2 el qual és l'encarregat de gestionar el tràfic d'Integració.

Per tant, la discriminació del tràfic es realitza correctament per lo que el disseny d'aquest model és correcte.

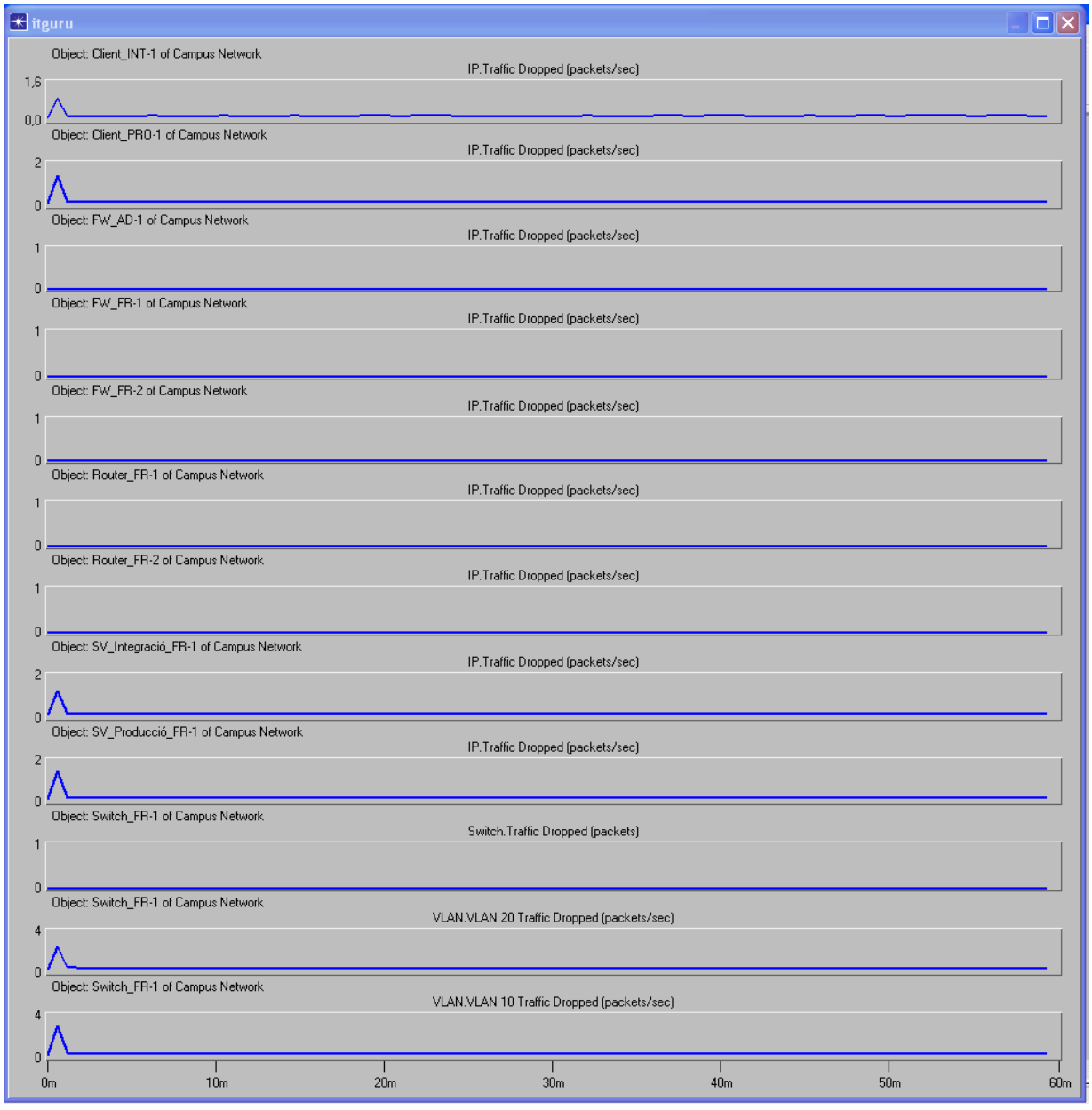
D'altra banda, es mostrarà el temps de resposta o retard, dels principals dispositius que participen en la simulació, sense tenir en compte el retard generat pel xifratge i desxifratge com s'ha comentat abans.



Il·lustració 62 Estadístiques temps de resposta dels equips principals del Model Complert Millorat

El temps de resposta es manté exactament igual a l'anterior model, per lo que la discriminació del tràfic no afecta al disseny i la eficiència de la xarxa, l'únic punt interessant a comentar el és el tràfic d'Integració del firewall de França - 2 on el seu retard és inferior al firewall de França - 1. Segurament això es degut a que el firewall de Andorra - 1 li arriben abans les peticions de França - 2 per lo que respon més ràpidament, per lo que el retard disminueix.

Per últim es mostrarà els paquets perduts per alguns dels dispositius principals, per tal de verificar que el disseny sigui correcte.



Il·lustració 63 Estadistiques paquets perduts dels principals dispositius Model Complert

Les estadístiques dels paquets perduts són exactament iguals als del model anterior i al del model bàsic, per lo qual, la discriminació del tràfic no implica la pèrdua de paquets.

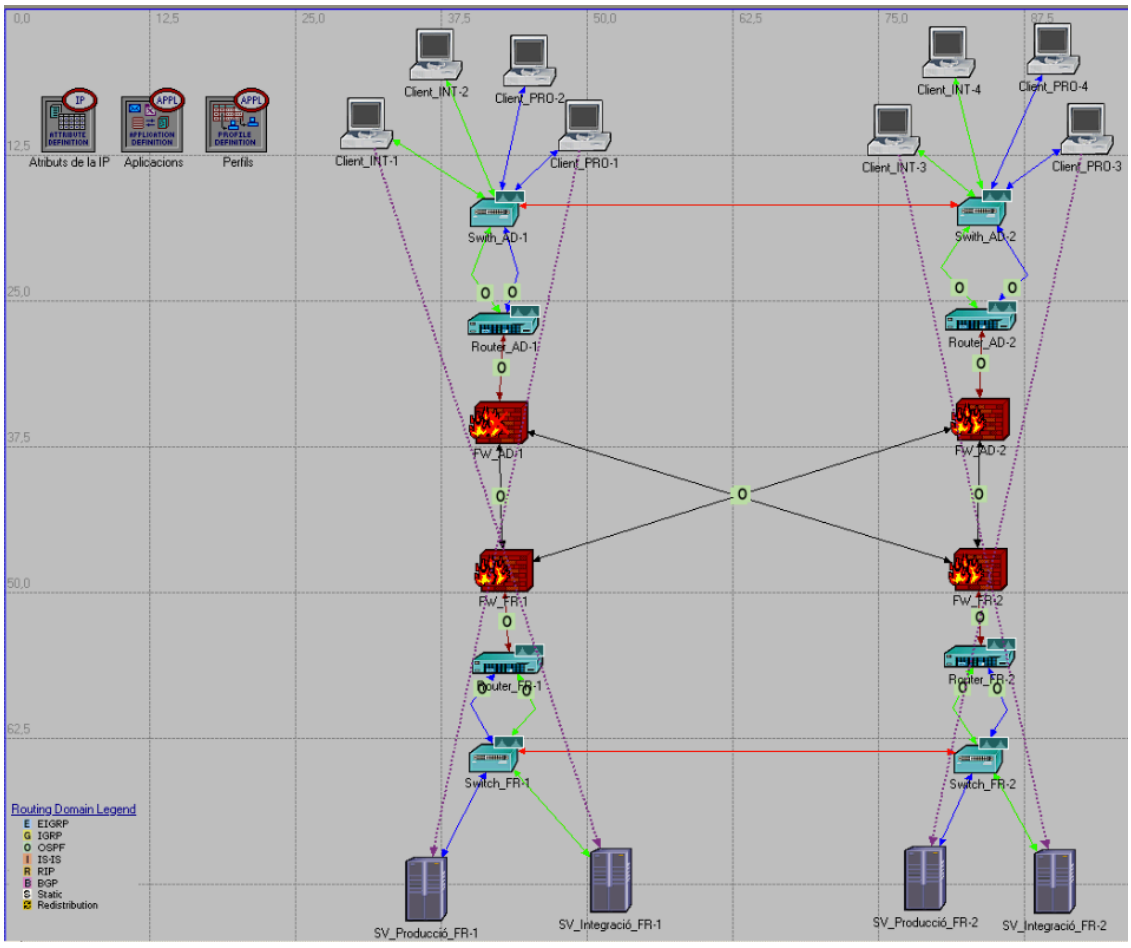
Per tant, es pot concloure que el disseny del Model Complert Millorat és correcte i no té cap repercussió en el disseny de la xarxa.

10.4 Simulació al Model Complet amb un firewall caigut

La simulació que es realitzarà del model Complert Millorat amb un firewall caigut té com finalitat mostrar el comportament que tindrà la xarxa en cas de que el firewall principal de la zona d'Andorra quedi inactiu.

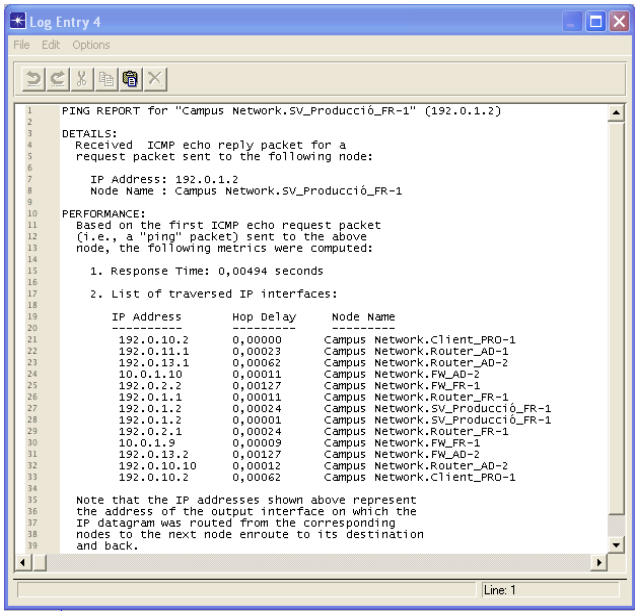
El principal objectiu d'aquest simulació, és obtenir informació de quina manera afecta la xarxa la caiguda d'aquest firewall i si el disseny assumeix correctament o no el redireccionament del tràfic al firewall de backup de la zona d'Andorra.

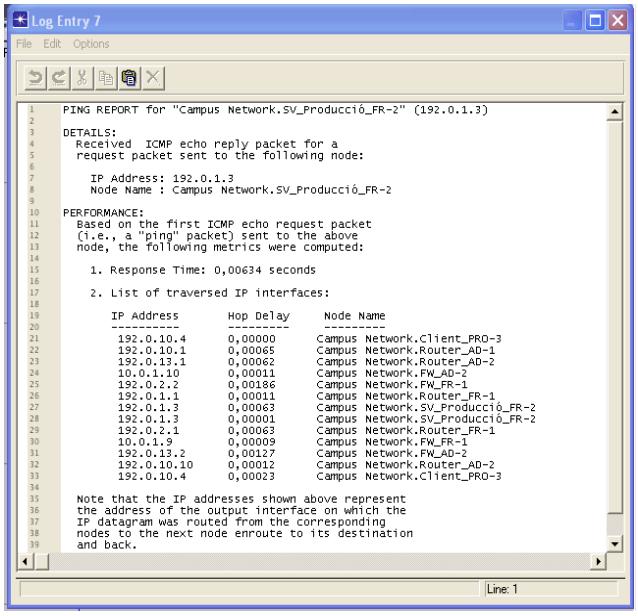
L'esquema de la simulació al Model Complert Millorat de l'eina OPNET és el següent:



Il·lustració 64 Esquema Model Complert Millorat amb 1 firewall caigut

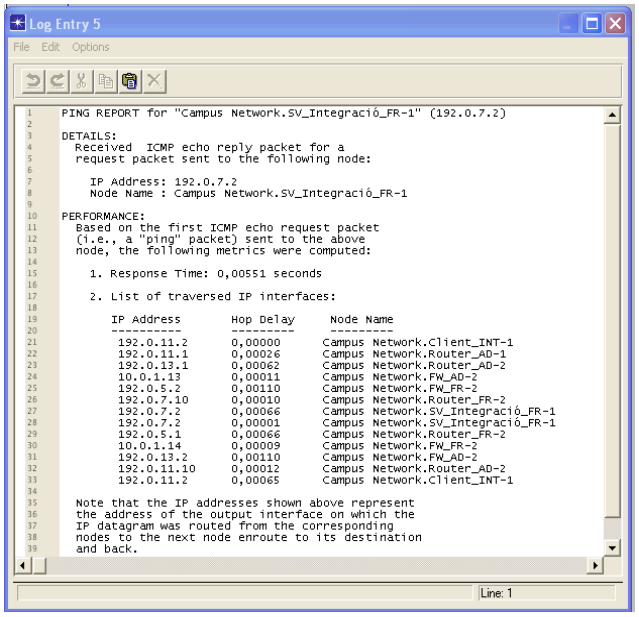
A continuació es mostrarà els resultats dels pings que s'han realitzat durant els 60 minuts que s'han emulat en l'eina OPNET, s'han triat 2 pings de Producció i 2 pings d'Integració cadascun d'ells en una zona diferent.

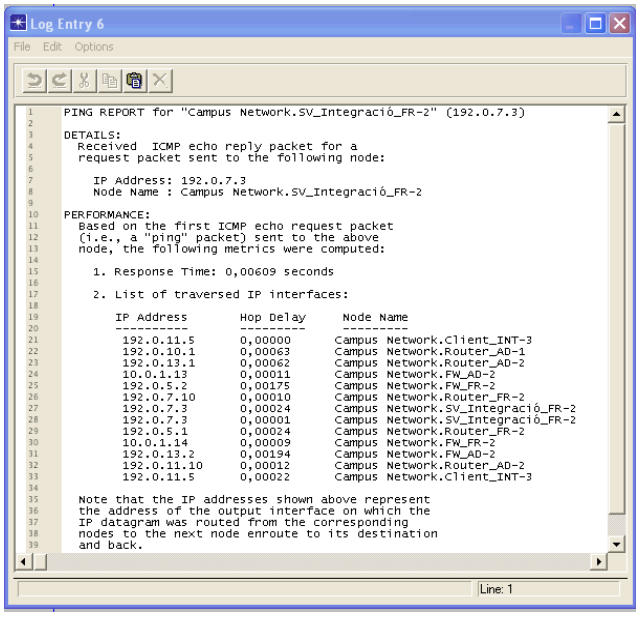




Il·lustració 65 Ping tràfic discriminat Producció Andorra-1 a França-1 "1 Firewall Caigut"

Il·lustració 66 Ping tràfic discriminat Producció Andorra-2 a França-2 "1 Firewall Caigut"



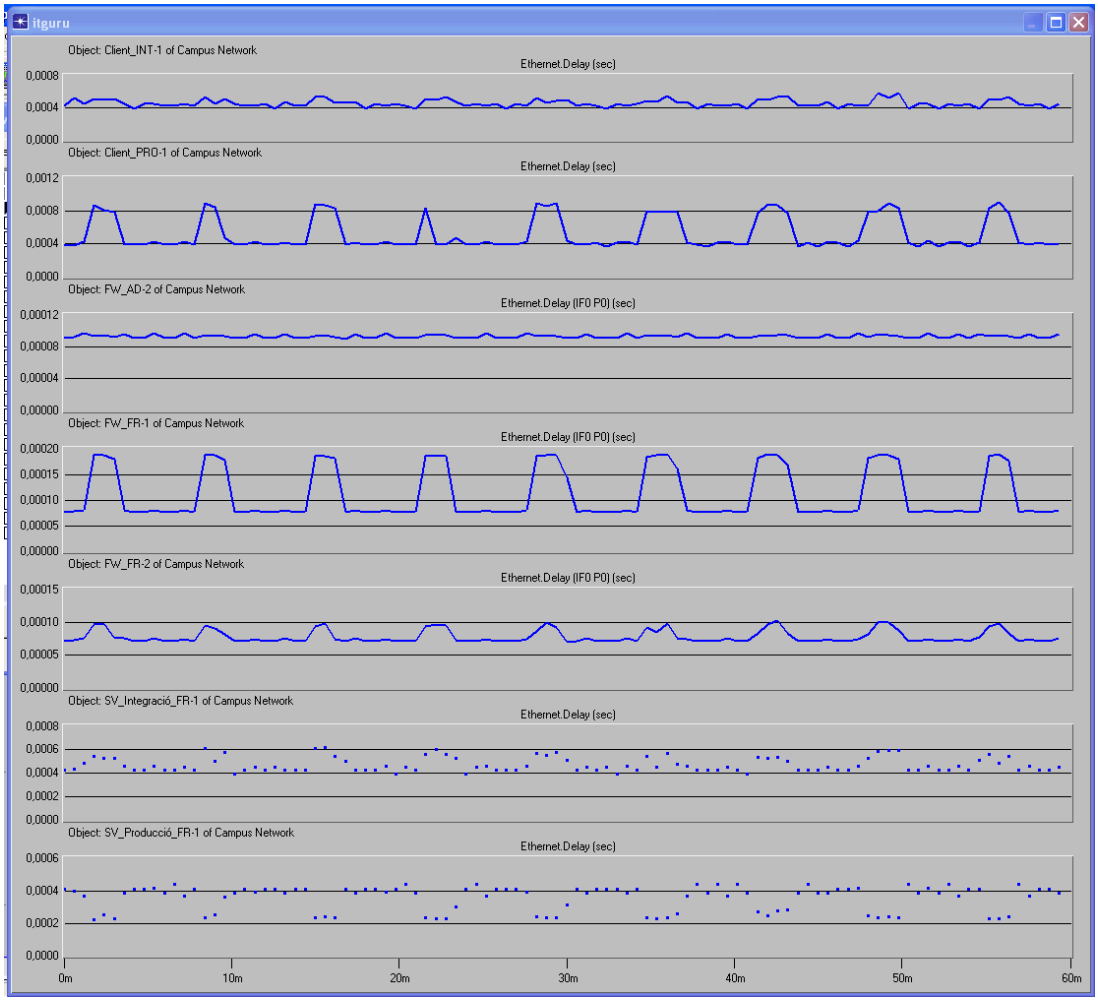


Il·lustració 67 Ping tràfic discriminat Integració Andorra-1 a França-1 "1 Firewall Caigut"

Il·lustració 68 Ping tràfic discriminat Integració Andorra-2 a França-2 "1 Firewall Caigut"

Com podem observar en els logs anteriors dels pings, al no estar operatiu el firewall d'Andorra - 1, tot el tràfic d'aquest firewall és redirigit el firewall d'Andorra - 2 el qual ha assumit tota la feina del firewall - 1 satisfactòriament.

D'altra banda, es mostrarà el temps de resposta o retard, dels principals dispositius que participen en la simulació.

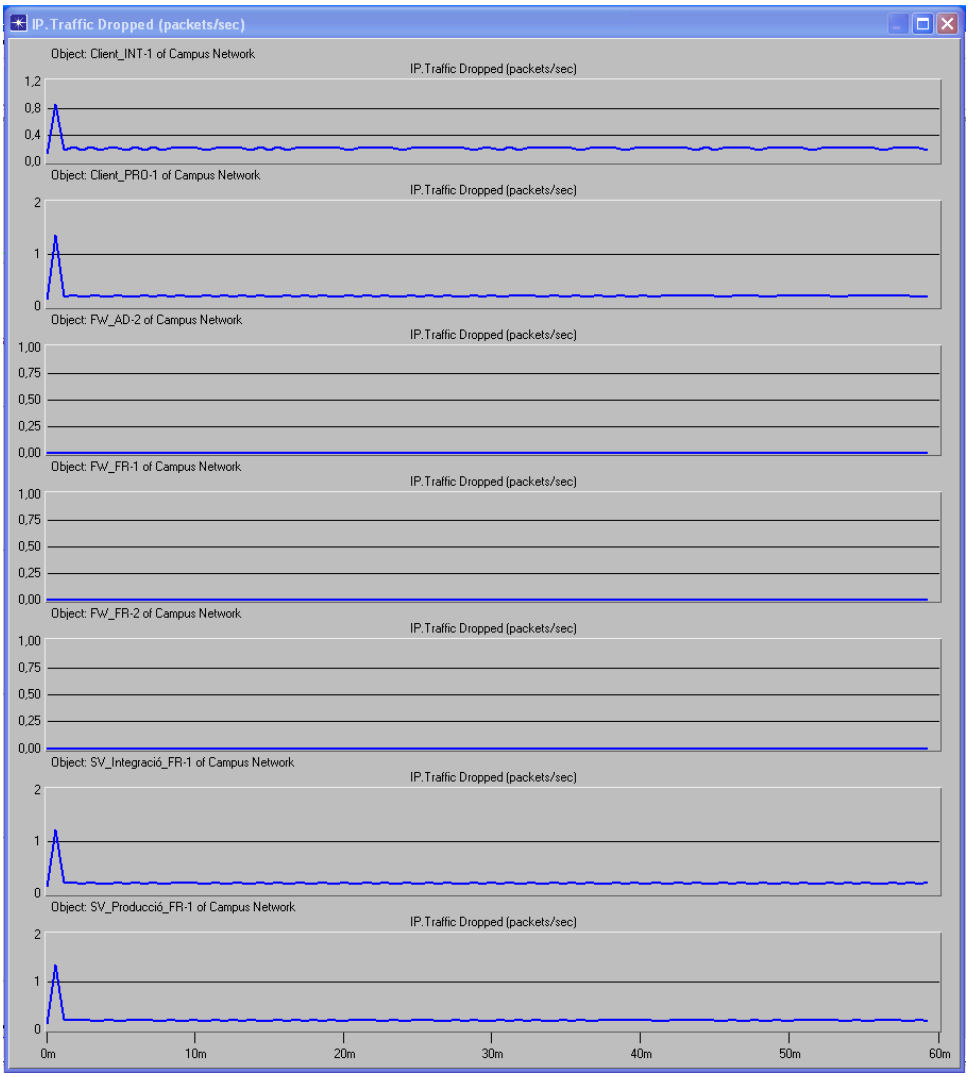


Il·lustració 69 Estadístiques temps de resposta dels equips principals del Model Complert Millorat "1 Firewall Caigut"

Com podem observar el temps de resposta o retards si que s'ha vist afectat al estar el firewall d'Andorra - 1 inactiu, s'ha incrementat lleugerament els valors del retard, degut que el router principal és el d'Andorra - 1 i aquest ara ha de derivar la feina al router d'Andorra - 2 per tal de poder sortir per el firewall de Andorra - 2.

Per tant, tot i que el retard s'incrementa lleugerament, s'haurà de tenir en compte en el cas quan el volum de dades sigui especialment gran.

Per últim es mostrarà els paquets perduts per alguns dels dispositius principals, per tal de verificar que el disseny sigui correcte.



Il·lustració 70 Estadístiques paquets perduts dels principals dispositius Model Complert " 1 firewall caigut "

Com podem observar en les estadístiques anteriors, el fet de que el firewall d'Andorra - 1 estigui caigut, no representa pèrdua de paquets, ja que els paquets perduts mostrats són exactament els mateixos que els de les anteriors simulacions.

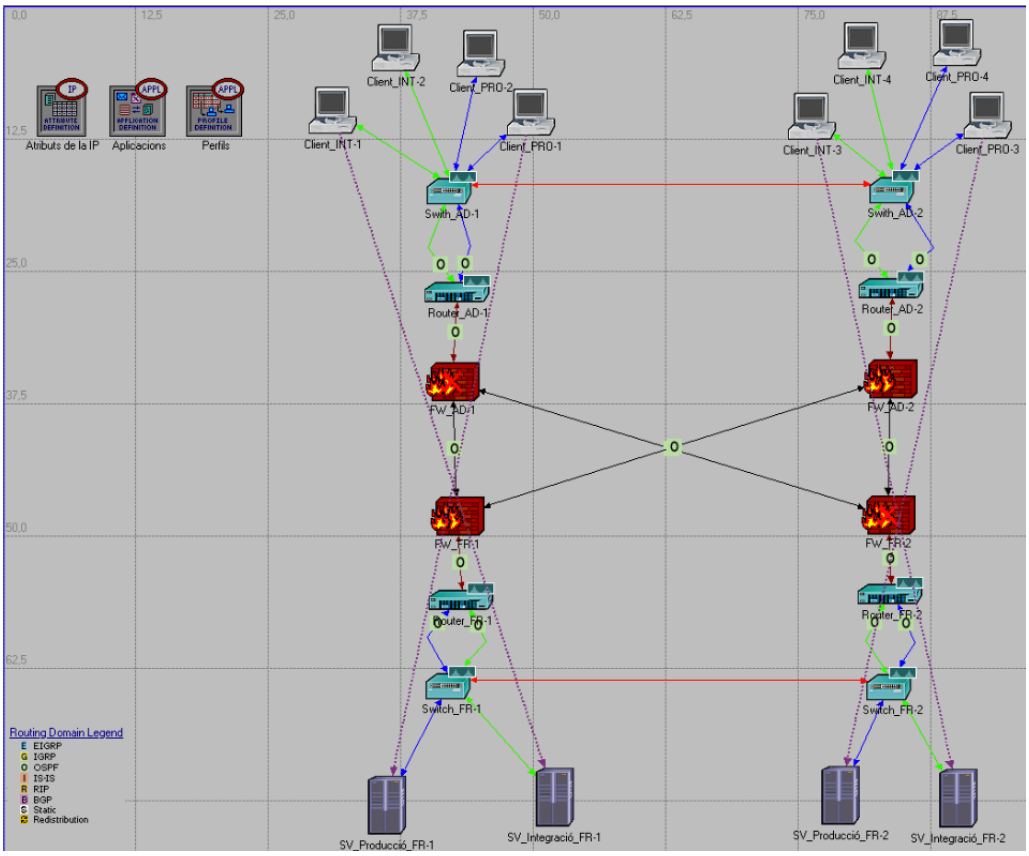
Per tant, l'única afectació que hi ha en la caiguda del firewall és el lleuger increment en els retards.

10.5 Simulació al Model Complert amb dos firewalls caiguts

La simulació que es realitzarà del model Complert Millorat amb dos firewalls caiguts té com finalitat mostrar el comportament que tindrà la xarxa en cas de que el firewall principal de la zona d'Andorra quedi inactiu i que el firewall de França - 2 quedi inactiu el qual gestiona el tràfic de Integració íntegrament.

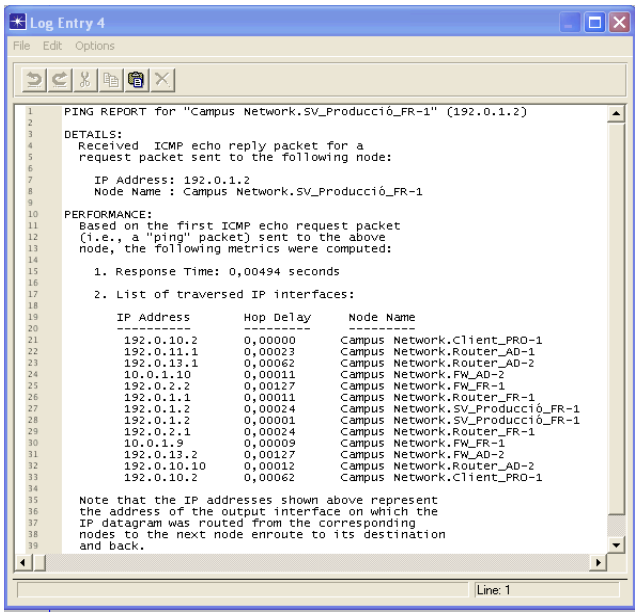
El principal objectiu d'aquest simulació, és obtenir informació de quina manera afecta la xarxa la caiguda d'aquest dos firewalls i si el disseny assumeix correctament o no el redireccionament del tràfic al firewall de backup de la zona d'Andorra, a més que el firewall de França - 1 assumeix el tràfic de Producció que ja té assignat més el tràfic d'Integració del firewall de França - 2 que està inactiu.

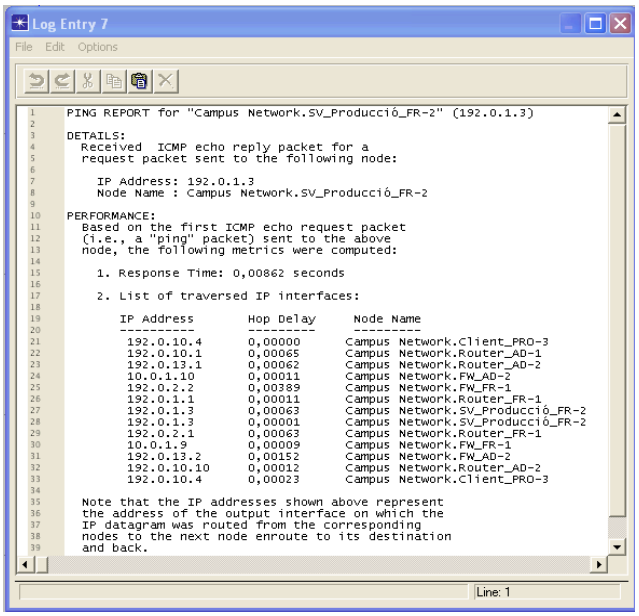
L'esquema de la simulació al Model Complert Millorat de l'eina OPNET és el següent:



Il·lustració 71 Esquema Model Complert Millorat amb 2 firewalls caiguts

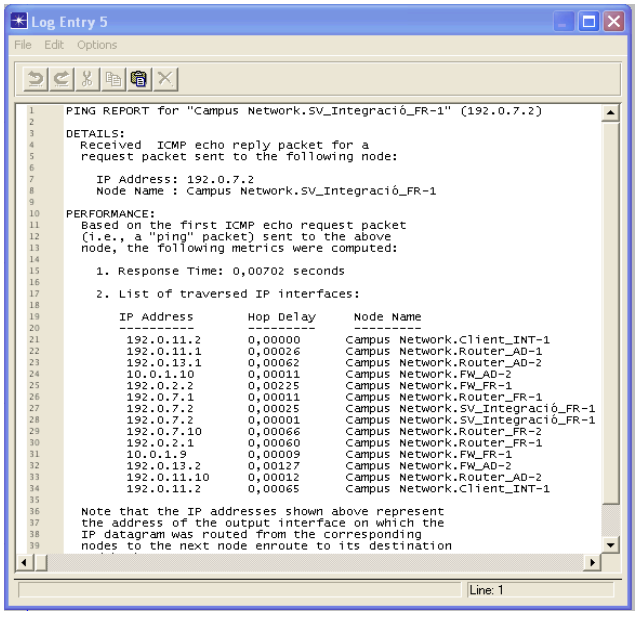
A continuació es mostrarà els resultats dels pings que s'han realitzat durant els 60 minuts que s'han emulat en l'eina OPNET, s'han triat 2 pings de Producció i 2 pings d'Integració cadascun d'ells en una zona diferent.

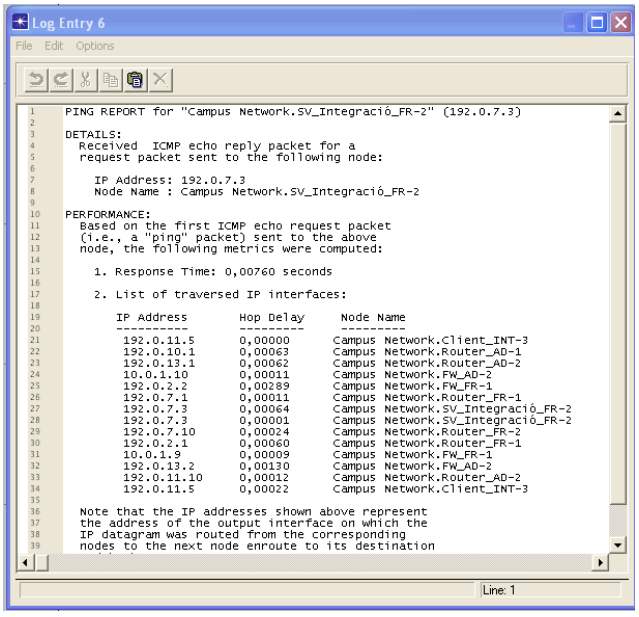




Il·lustració 72 Ping tràfic discriminat Producció Andorra-1 a França-1 "2 Firewalls Caiguts"

Il·lustració 73 Ping tràfic discriminat Producció Andorra-2 a França-2 "2 Firewalls Caiguts"





Il·lustració 74 Ping tràfic discriminat Integració Andorra-1 a França-1 "2 Firewalls Caiguts"

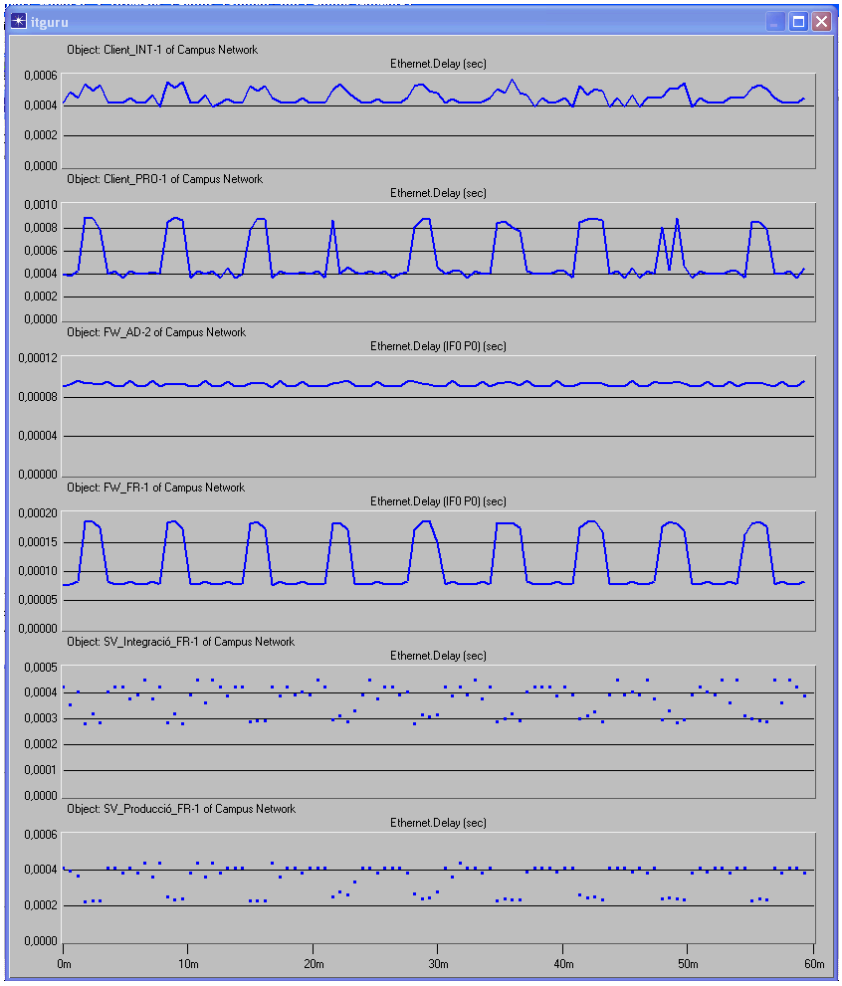
Il·lustració 75 Ping tràfic discriminat Integració Andorra-2 a França-2 "2 Firewalls Caiguts"

Com podem observar en els logs dels pings, tan de Producció com d'Integració, és que al estar el firewall de Andorra - 1 Caigut, tot el tràfic es redirigeix al firewall de Andorra - 2.

A més, al estar caigut el firewall de França - 2, el qual era el responsable, de tot el tràfic d'Integració, podem veure que el firewall de França - 1 ara treballa amb el tràfic de Producció i Integració assumint el flux de tràfic del firewall de França - 2-

Per tant, després d'analitzar els logs podem afirmar que el disseny està correctament redundat.

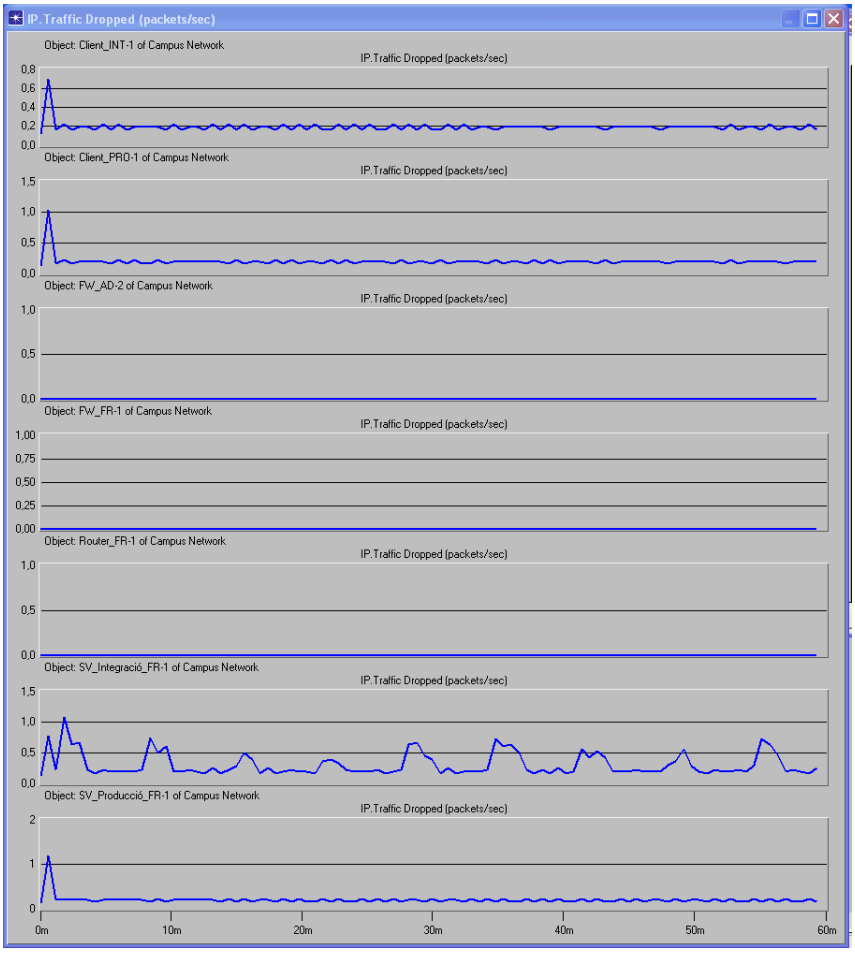
D'altra banda, es mostrarà el temps de resposta o retard, dels principals dispositius que participen en la simulació.



Il·lustració 76 Estadístiques temps de resposta dels equips principals del Model Complert Millorat "2 Firewalls Caiguts"

Com podem observar en les estadístiques de l'anterior il·lustració, l'increment en el temps de resposta o retard en que hi hagi 1 firewall o 2 caiguts no s'increment. Es manté el lleuger increment observat en l'anterior model al tenir un firewall caigut, però ara al tenir 2, no s'ha detectat cap incremente en els retards.

Per últim es mostrarà els paquets perduts per alguns dels dispositius principals, per tal de verificar que el disseny sigui correcte.



Il·lustració 77 Estadístiques temps de resposta dels equips principals del Model Complert Millorat "2 Firewalls Caiguts"

Els paquets perduts han estat sempre els mateixos des de la simulació del Model Bàsic, fins a l'actual, per la qual cosa, podem concloure que el disseny de la xarxa tot i que tingui caiguda d'algun dels seus equips redundats no repercuteix en la pèrdua de paquets.

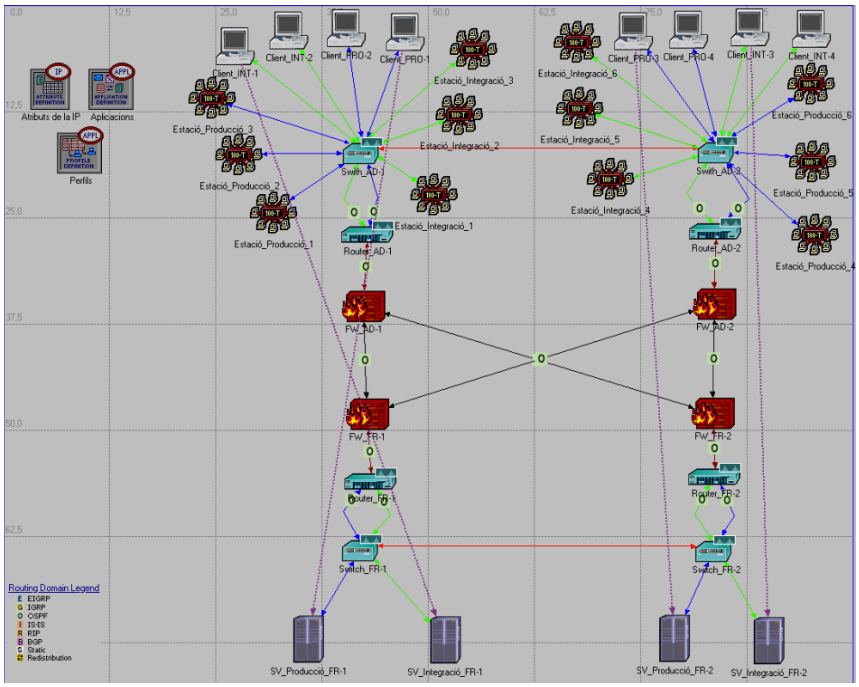
10.6 Simulació al Model Complert Millorat amb volum de tràfic real

La simulació que es realitzarà del model Complert Millorat amb volum de tràfic real té com finalitat mostrar el comportament que tindrà la xarxa amb un flux de tràfic el més pròxim a al realitat. Observant l'ús de la CPU dels Firewalls i de l'ample de banda dels enllaços que hi ha entre els servidors. A més del temps de resposat i la pèrduda de paquets.

Com s'ha explicat en l'inici del document, el firewalls no només gestionaran aquest entorns sinó també els altres entorns dels CPDs els quals s'han mencionat però no s'han detallat degut a que no participen dintre del proyecte. Per la qual cosa, és important l'estudi d'aquesta simulació, per observar el comportament dels dispositius i dels recursos que faràn servir.

A més, s'ha ampliat el temps de la simulació a 40 minuts[6]

L'esquema de la simulació al Model Complert Millorat amb volum de tràfic real de l'eina OPNET és el següent:



Il·lustració 78 Esquema Model Complert Millorat amb volum de tràfic real

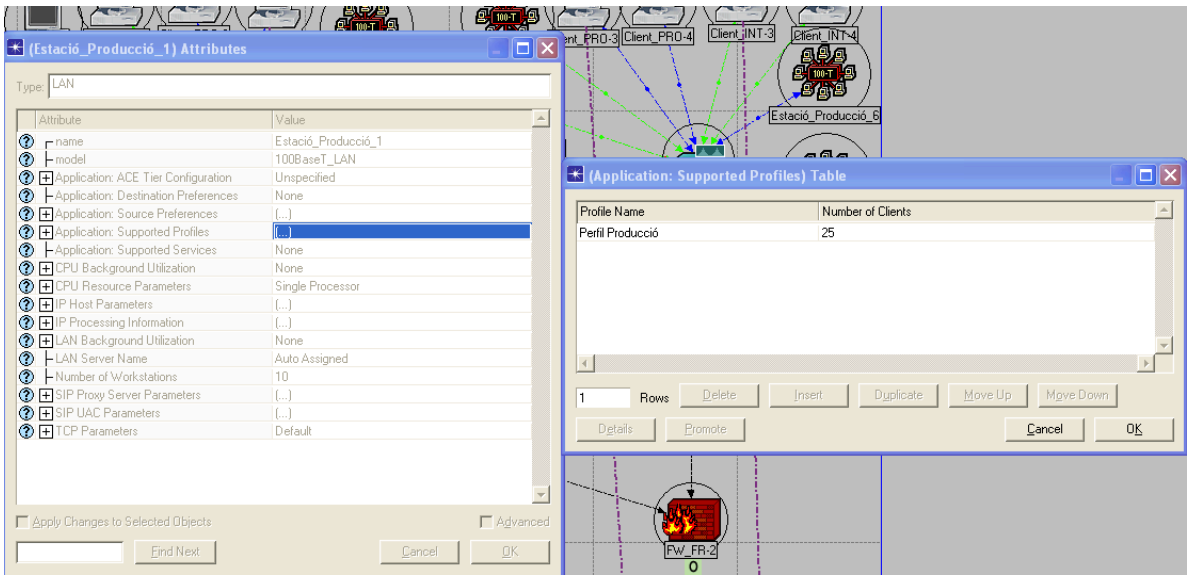
[6] No s'ha augmentat més el temps de la simulació, ja que la llicència de IT Guru, només permet un número d'events determinats que es superen als 45 minuts de la simulació.

Com podem observar en l'esquema del Model Complert Millorat anterior, per tal de reproduir un volum de tràfic real, s'ha afegit varies estacions de treball on cada una d'elles representa com si fossin 25 equips. Com s'han declarat 6 estacions de treball per cada entorn "Producció & Integració", la simulació estarà al voltant dels 308 equips, 154 per Integració i uns altres 154 per Producció.

En les estacions de treball s'ha detallat que serien 25 equips[7] i amb una sola direcció IP, per el que es dona per entès que s'aplica un protocol NAT dintre d'aquesta IP. A més s'ha definit que cada estació tan sols faci peticions a un dels entorns.

Per tant, la configuració ha quedat de la següent manera:

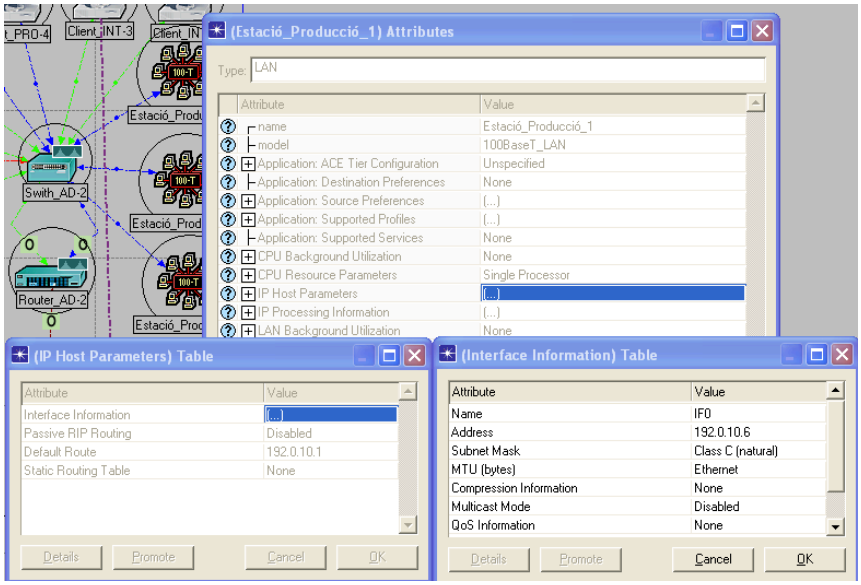
- Configuració de l'entorn on realitzarà les peticions i els equips que contindrà la LAN:



Il·lustració 79 Configuracio entorn i equips Estació Treball

[7] S'ha definit 25 per cada estació de treball, perquè al augmentar el nombre d'equips, apareixien logs de lentitud dintre de la LAN de l'estació de treball. Per el que s'ha deixat 25 per mantenir major estabilitat.

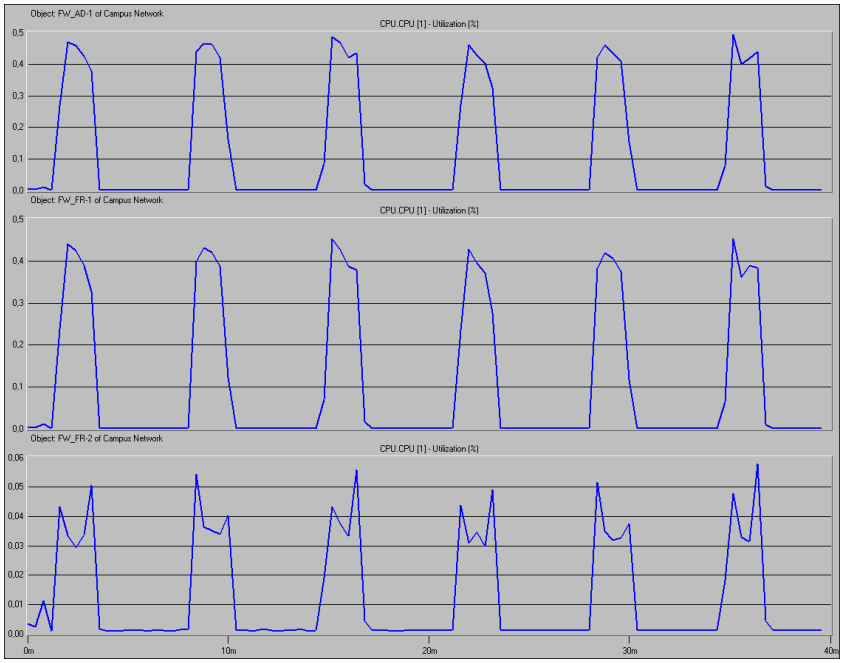
- Configuració de la direcció IP:



Il·lustració 80 Configuració IP Estació Treball

A continuació es farà un estudi de l'ús dels 3 firewalls que estan en funcionament, ja que el firewall de Andorra - 2 no està operatiu, ja que és el backup del firewall de Andorra -1.

Les estadístiques de les CPU de cadascun dels firewalls són les següents:



Il·lustració 81Estadístiques firewalls CPU

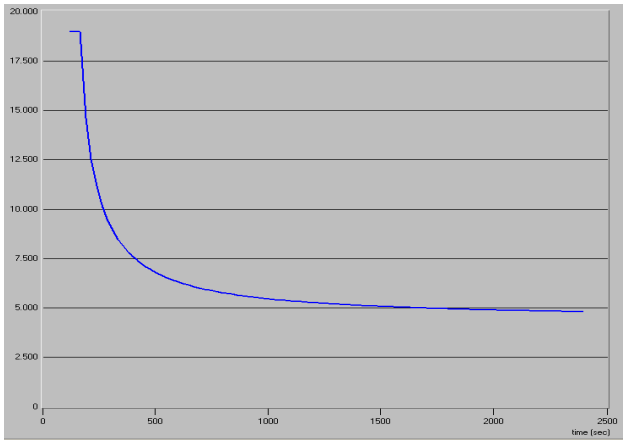
Com podem observar en la il·lustració anterior, l'ús de la CPU dels firewalls per el gestionament d'aquest tràfic, és del 0,5 % com molt. Cal destacar que com en la simulació, no s'ha pogut configurar les VPN i la configuració de seguretat d'aquesta, per el que l'ús de la CPU és inferior, ja que si aquest protocols estiguessin configurats, segurament estaria al voltant del 2 al 3% d'ús de la CPU.

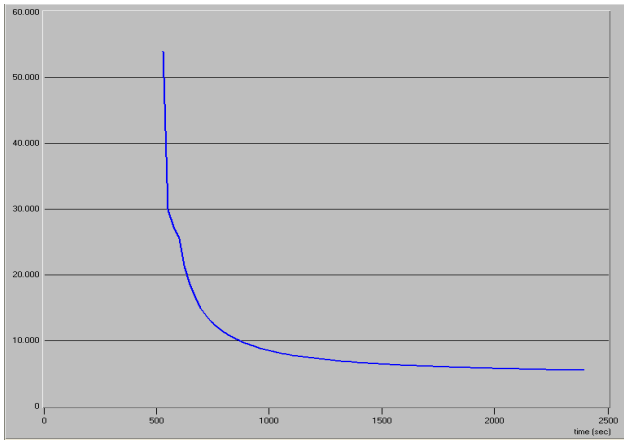
A més a més, com es pot veure en la il·lustració, el firewall de Andorra - 1, té una lleugera càrrega superior als altres 2 firewalls. D'altra banda el firewall de França -1 té una mica més d'ús de CPU, degut a que el tràfic de Producció és més intens que el de Integració que és gestionat per el Firewall de França - 2

Per tant, els resultats de les estadístiques de CPU dels firewalls és satisfactòria, ja que un 0,5% del gestionament més un 2 o 3% que seria del xifratge i desxifratge, fa que no s'arribi a un 4% d'ús de CPU del firewall, per el que el gestionament d'aquest entorn, no implicaria una reducció del rendiment del firewall envers als altres entorns.

També, s'ha realitzat una gràfica comparativa de la congestió que hi ha entre una petició del Client_PRO_2 al servidor SV_Producció_FR-1, entre el tràfic de la primera simulació de l'entorn millorat i del tràfic amb la simulació de l'entorn real.

Els resultats són els següents:





Il·lustració 82 Congestió Model Complert Millorat

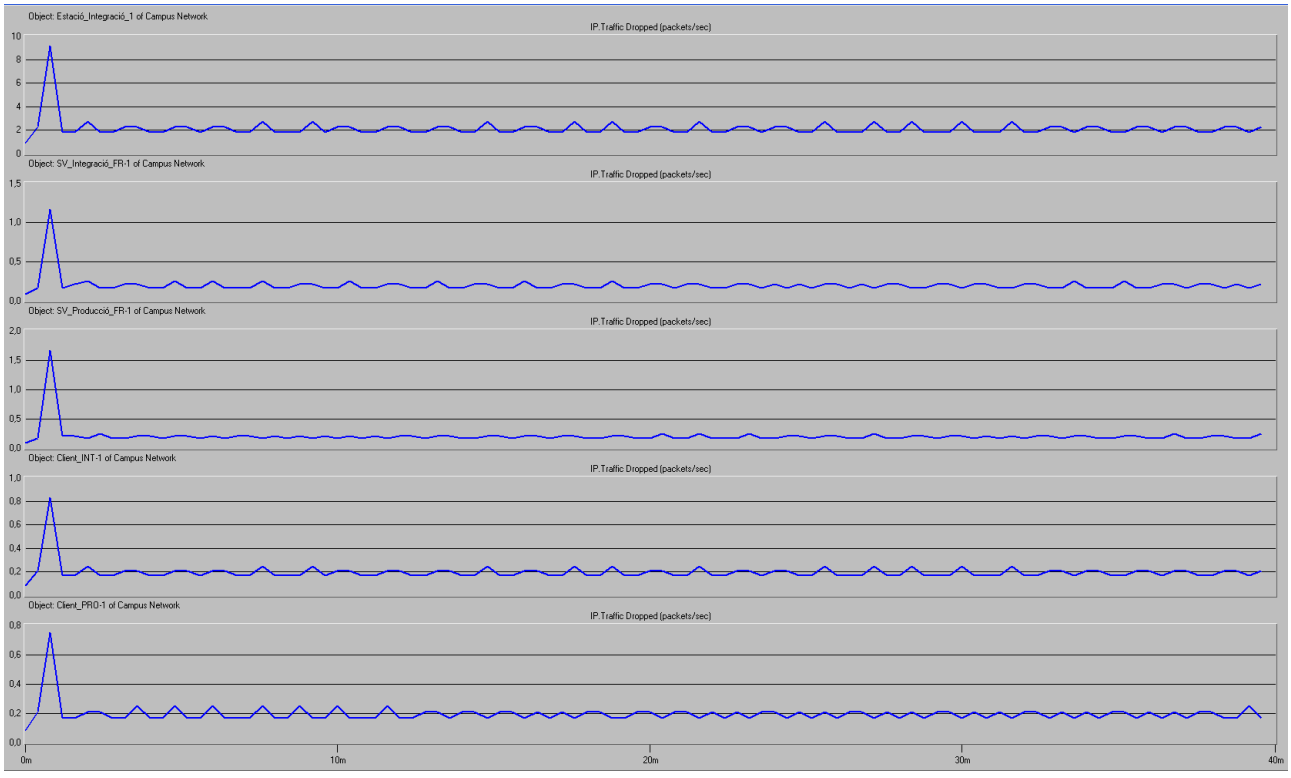
Il·lustració 83 Congestió Model Complert Millorat amb volum de tràfic real

Com podem veure en les dues anteriors il·lustracions, la congestió en el primer esquema no arriba a les 20.000 peticions, i es manté estable al llarg de 5.000 peticions. En canvi, en el model amb el volum de tràfic real, tenim un pic de més de 50.000 peticions i es manté a menys de 10.000.

Per el que els resultats, podem admetre que els pics de peticions es el que és veu més agreujat, tot i així la mitja de peticions al llarg del temps és manté estable, per el que els resultats obtinguts són bastant bons, ja que, la congestió de peticions no augmenta de manera significativa.

D'altra banda, la pèrdua de paquets és un punt important a mesurar, ja que al tenir un vòlum de tràfic més important, i com hem observant en l'anterior il·lustraicó la congestió ha augmentat. Fa que la possibilitat que la pèrdua de paquets augmenti i d'aquesta manera disminueixi el rendiment de la xarxa. Per el que és un punt important d'analitzar.

Les estadístiques estretes de la simulació són les següents:



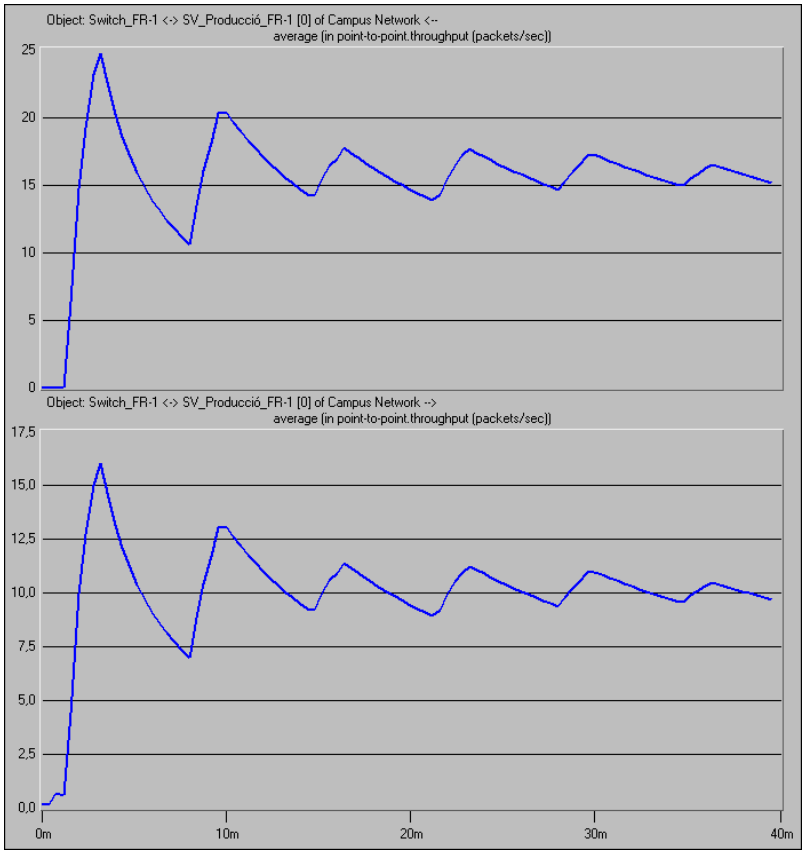
Il·lustració 84 Estadístiques pèrdua de paquets Tràfic Real.

Com podem observar en l'anterior il·lustració la pèrdua de paquets es manté estable, no ha augmentat. Ja que els servidors perden entre 0 i 2 paquets i els clients que realitzen les peticions perden entre 0 i 2 paquets. Per el que és manté exactament igual que en les simulacions sense el tràfic real.

No obstant, com es pot veure en la il·lustració l'estació de treball té un màxim de gairebé 10 paquets perduts. Els quals no realitzem una especial importància, ja que, poden ser causats per el mateix NAT, que gestiona els 25 equips interns.

El punt més important, són els paquets perduts per el servidor, els quals es mantenen estables, per el que els resultats de la simulació satisfactòries i el rendiment de la xarxa és estable.

L'últim punt a analitzar, és el ample de banda, per el que s'ha extret estadístiques de la mitjana de paquets per minut que gestiona l'ample de banda entre switch i servidor. Els resultats obtinguts són els següents:



Il·lustració 85 Estadístiques Ample de Banda

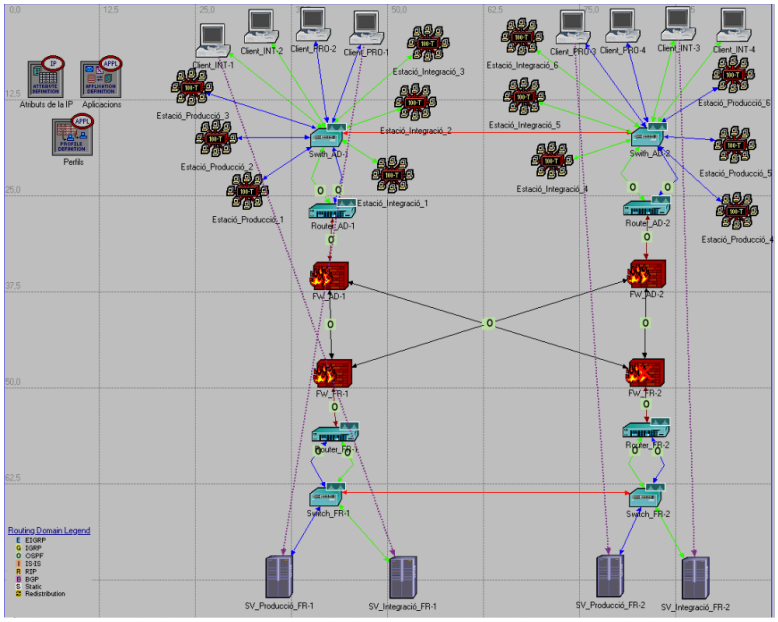
Com podem examinar en l'anterior il·lustració, la mitjana de paquets és entre 10 - 25 paquets per minut. El qual és un tràfic bastant lleuger i assumible per tota la xarxa. Per tant, podem afirmar que els resultats obtinguts de la simulació són satisfactoris i que es podria aplicar aquest model configuració a un entorn real, sense saturar la infraestructura.

10.7 Simulació al Model Complert Millorat amb volum de tràfic real i 1 firewall caigut

La simulació que es realitzarà del model Complert Millorat amb volum de tràfic real i 1 firewall caigut té com finalitat mostrar el comportament que tindrà la xarxa amb un flux de tràfic el més pròxim a al realitat i a més amb un firewall caigut. El firewall que s'ha triat per simular la seva caiguda és el d'Integració de França - 2, ja que el firewall de Andorra - 2 és el de Backup de Andorra -1 per el que comportament seria exactament el mateix. Per tant, s'ha triat el de França - 2 per observant l'increment de CPU, pèrdua de paquets i ample de banda.

La importància d'aquesta simulació radica, en que la probabilitat en que un dels firewall de França - 1 o França - 2, estigui inactiu és alta, ja que pot fallar el firewall en si o qualsevol dels enllaços de la VPN, per tant, és important realitzar aquesta simulació per observar el comportament de la xarxa i estudiar-ne així els seus errors.

L'esquema de la simulació al Model Complert Millorat amb volum de tràfic real i 1 firewall caigut de l'eina OPNET és el següent:



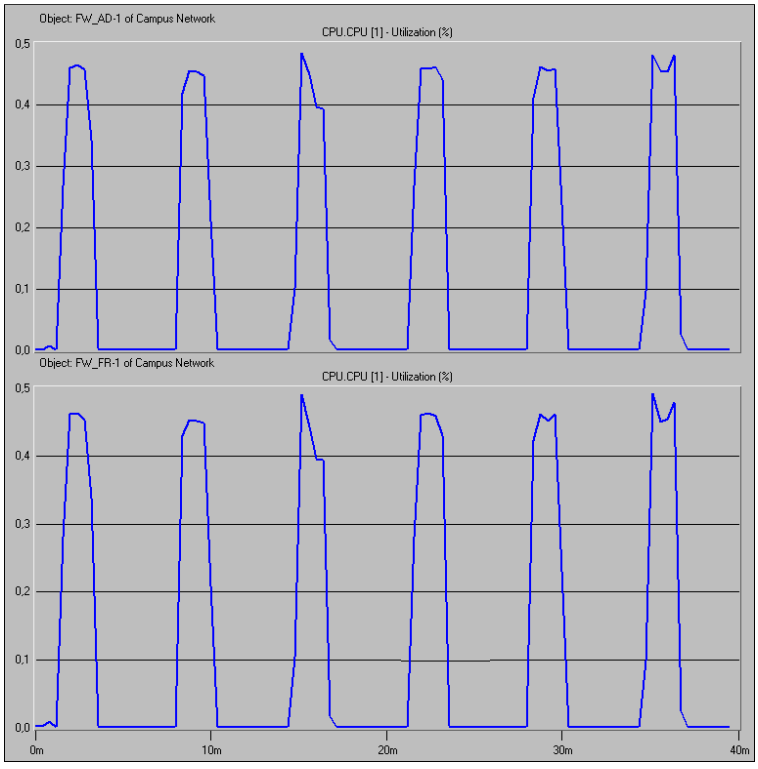
Il·lustració 86 Esquema Model Complert Millorat amb volum de tràfic real 1 FW Caigut

El punts que s'analitzaran en aquesta simulació són: l'increment en la CPU del firewall de França -1, ja que aquest ha d'assumir tot el tràfic de França - 2. A més a més, també es revisarà la pèrdua de paquets, si augmenta, ja que el firewall de França - 2 al ser el firewall principal d'Integració, pot ocasionar alguna pèrdua, degut a que aquest està inactiu i s'ha de redirigir el tràfic cap el firewall de França -1.

D'altra banda, en aquesta darrera simulació s'ha extret la simulació de la congestió de les peticions que es realitzen en el servidor, ja que aquestes peticions, fan referència al nombre de peticions que reben el servidors, aquests valors, no es veuran afectats en rendiment, ja que si reben el tràfic correctament, tindran els mateixos valors que l'anterior simulació.

De la mateixa manera els valors de l'ample de banda entre el switch i els servidors es mantindran iguals, si aquests reben el tràfic correctament, per tant, no es necessària la seva simulació.

Per tant, el primer punt que s'analitzarà és l'ús de la CPU dels dos firewalls, on les estadístiques han tingut els següents resultats:



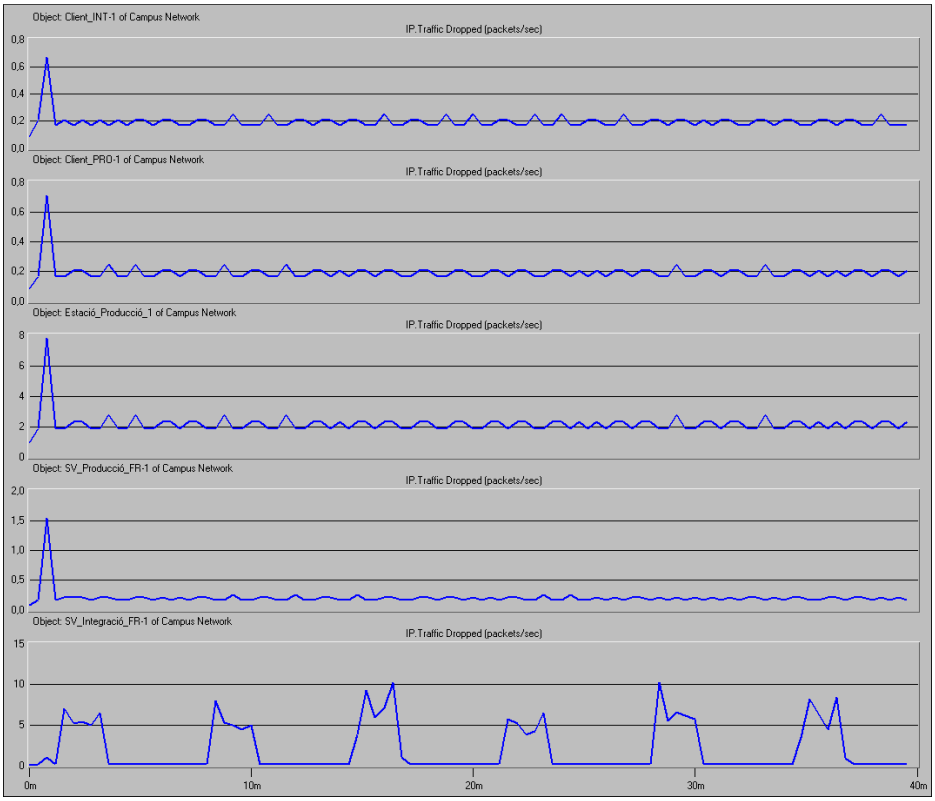
Il·lustració 87 Estadístiques firewalls Tràfic Real 1 firewall caigut

Com es pot observar en l'anterior il·lustració el firewall de Andorra - 1 té els mateixos valors que en l'anterior simulació, en canvi el firewall de França - 1, ha augmentat el cost de la CPU al mateix nivell que el firewall de Andorra - 1, ja que, ara mateix no només gestiona el tràfic de Producció, sinó també el tràfic de Integració, de la mateixa manera que ho realitza el firewall de Andorra - 1 on el cost de CPU és gaire bé simètric.

Per tant, el resultat de la simulació és satisfactori, ja que l'increment de de tràfic de França - 1, no implica un ús excessiu de la CPU, i es manté igual que el de Andorra - 1, tot i que el redireccionament de Producció i Integració sigui lleugerament més complexe que el que hi ha en els CPDs d'Andorra.

Per la qual cosa, la simulació amb un firewall caigut mostra, que la infraestructura de connexió de les CPDs i els mateixos CPDs no veuran una mitigació en el seu rendiment.

L'últim punt que s'anlitzarà serà la pèrdua de paquets en els difenrents equips, on les estadístiques de cadascun d'ells ha obtingut els següents resultats:



Il·lustració 88 Estadístiques pèrdua de paquets tràfic real amb 1 firewall caigut

Si observem detalladament l'anterior il·lustració veiem, que la pèrdua de paquets es manté estable en tots els equips mantenint com a referència l'anterior simulació.

Podem observar com els clients d'Integració, Producció i el servidor de Producció mantenen la mateixa pèrdua de paquets, de la mateixa manera que l'estació d'Integració.

No obstant, si analitzem l'última estadística, la qual fa referència al Servidor d'Integració passem d'una pèrdua de 0 a 2 paquets, a una pèrdua de 0 a 10 paquets. Aquesta pèrdua de paquets ve justificada pel que s'ha mencionat anteriorment, en que el gestionament del tràfic de Producció i Integració en la zona de França és més complexe que en la zona d'Andorra.

En la zona de França, al gestionar cada un dels firewalls tràfics diferents, els gateway principals són diferents, per tant, si un dels firewalls està inactiu, hi ha molts més redireccionament que no en la zona d'Andorra on el gateway es comú en totes dues xarxes. Per el que, l'augment de pèrdua de paquets, està justificat en el redireccionament extra per la caiguda del seu firewall principal.

Tot i que l'augment dels paquets perduts és mínim, i que la caiguda d'un firewall no ha de ser un estat fixe, sinó momentani, s'ha de tenir en consideració aquesta pèrdua de paquets, si quan un dels firewalls està caigut i el flux de xarxa és molt intens, el qual podria ocasionar algun error, tot i que amb els resultats que s'han obtingut és pràcticament poc probable.

Per tant, la simulació d'aquest model ha estat molt beneficiosa i indica un possible estat que s'ha de tenir en compte en cas que un cop en producció, s'origini aquesta situació, per tal d'evitar que la xarxa arribi a tindre un flux important de dades i així evitar possibles errors.

11 Conclusions i línies de recerca

L'objectiu d'aquest PFC, ha estat el dissenyar un topologia de comunicació de quatre centres de processament de dades que estiguessin comunicat via WAN, amb una discriminació del tràfic en la zona de França dels CPDs.

Aquest disseny tenia la finalitat de ser verificat en un entorn de proves real, amb maquinari físic i de les mateixes característiques que l'entorn que ja està en funcionament i a més en una eina de simulació virtual, en aquest cas l'OPNET IT Gurú.

El primer objectiu de la simulació consistia en verificar que el disseny, funcionés correctament i corregir-ne els seus errors. A més com a segon punt, un cop el primer punt estigués solucionat seria establir una comparació de simulació de tots dos entorns i extreure conclusions sobre quins dels dos és prescindible o no.

Per tant, en primer lloc podem concloure que les simulacions dels dissenys sempre són necessàries, encara que semblin el més simple. Com s'ha pogut observar en aquest PFC, el paràmetre més simple que podem trobar en un firewall i que no sempre es té en compte, ha fet que sigui necessari la remodelització del disseny, ja que el primer model no ho complia la condició de simetria que tenen inherentment els firewalls.

Aquest fet, demostra que les simulacions són un pas important en els dissenys de xarxes, ja que si no s'hagués realitzat, la implementació a l'entorn real, hagués ocasionat errors alhora de fer-ne les copies de seguretat, fet que implicaria una pèrdua de seguretat i recolzament important, per el simple fet de no poder realitzar-la.

No obstant, i fent referència al primer punt de la conclusió on es conclou que les simulacions ha de ser presents en tots els projectes de xarxes, s'ha de destacar que les simulacions no sempre poden ser el 100% fiables, i això s'ha pogut verificar a partir de la realització de dues linies de simulació paral·leles, una amb equips físic i l'altre amb un entorn virtual.

Dins de l'entorn físic, s'ha detectat ràpidament els errors de simetria inherents en els firewalls avançats, que ens ha fet remodelar el disseny principal. A més, ens ha permés realitzar les configuracions dels enllaços VPN i verificar-los a patir de la virtualització del firewall, poden reutilitzar dita configuració en els equips que ja estan en producció.

Tot i així, aquest entorn, tan sols ens ha pogut mostrar que en cas de que caigues un enllaç l'altre quedava operatiu i viceversa.Però no ha pogut mostrar la redirecció del flux, ni la pèrdua de paquets i tampoc els temps de resposta, ja que el fluxe tot és en local i amb 1 o 2 peces com a màxim 4. Aquest fet, ha presentat moltes limitacions i dubtes en si l'encapsulació del tràfic suposaria un problema en el retards o no.

En canvi, en l'entorn de simulació virtual s'ha pogut fer un anàlisis del flux del tràfic real, ja que aquest entorn ho permet, hem pogut analitzar si realitzava correctament la discriminació de tràfic segons si era de Producció o Integració, amb un flux de tràfic pròper a al realitat. A més a més, també s'ha pogut observar els temps de resposta de tots els equips, consumició dels recursos, paquets perduts i el temps de resposta d'una petició de quan es realitza a fins que reb la resposta.

No obstant, també s'han observat limitacions important en aquest entorn. En primer lloc, el fet que no es té un ampli repertori de dispositiu on es pugui triar, el que suposa que els valors i condicions de la simulació no siguin exacte. I aquest fet que un primer lloc pot passar desapercebut, és molt important, ja que en la simulació virtual l'error de la simetria del firewall no s'ha detectat ja que aquesta condició no està present en el firewall genèric que s'ha triat per la simulació.

A més a més, tampoc s'ha pogut simular la confiuració de les VPN amb la seva respectiva seguretat, per limitacions del software, el qual si s'hagués utilitzat una versió com OPNET Modeler, s'hagués pogut realitzar però no en les meteixes condicions. El qual representa una limitació en l'entorn, que no ens pot indicar el retràs exacte del xifratge i desxifratge que representa aquesta mesura de seguretat.

Per la qual cosa, després de realitzar l'estudi de tots dos entorns, crec que la millor simulació i la més profitosa és la combinació de tots dos entorn. Com s'ha descrit anteriorment, si combinem tots dos resultats podem extreure un temps de resposta molt aproximat a la realitat, podem extreure el temps de resposta global a partir del simulador virtual i el temps del xifratge a partir de l'entorn real, la combinació de tots dos temps, mostrarà un temps de resposta molt pròxim al de la realitat.

En conclusió, qualsevol disseny ha d'estar verificat i simulat amb la finalitat de depurar-lo el màxim possible, i per aconseguir-ho el mètode ideal es realitzar la combinació d'un entorn de proves real, per tal de conèixer les restriccions i configuracions del maquinaria que es farà servir i a més a més, verificar-lo amb un entorn virtual el qual ens permet simular els flux de tràfic i extreure estadístiques detallades del comportament del model que s'ha dissenyat. On els resultats de tots dos entorns ens verificarà de manera exhaustiva la eficiència del model que s'hagi dissenyat.

12 Bibliografia

Modelació i simulació:

UPC (2004): OPNET: Manual de usuario. Departament D'enginyeria Telemàtica.

UPV: Fundamentos de OPNET IT Gurú Edición Academica. Redes y computadoras.

Eines:

Applications and Network Performance: http://www.opnet.com/

Hardware:

Cisco Systems, Inc: http://www.cisco.com/

Palo Alto Networks: http://www.paloaltonetworks.com/

Protocols:

https://www.tlm.unavarra.es/research/seminars/slides/20070727_dmorato_simulacionyomnetpp.pdf

http://es.scribd.com/doc/26474639/07-Simulacion-de-Eventos-Discretos

http://www.vaticgroup.com/unlimitpages.asp?id=147

http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CFUQFjAI&url=http%3A%2F%2Fwww.arcos.inf.uc3m.es%2F~jdaniel%2Fseminarios%2Fomnet1%2Fintrosim.ppt&ei=Ue2WUN_xLsua1AX3iIHQDQ&usg=AFQjCNGqbcqh2X-ktjMN4lk1W1qQvwrk-A&sig2=PrDNW5iZ7mr1gnPq1tj-Hg

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

http://es.wikipedia.org/wiki/Open_Shortest_Path_First

http://bibdigital.epn.edu.ec/bitstream/15000/1760/1/CD-2355.pdf

http://www.ordenadores-y-portatiles.com/vrf.html

http://es.wikipedia.org/wiki/HSRP

http://www.redescisco.net/v2/art/redundancia-entre-routers-con-hsrp/

13 Annexos

Als arxius adjunts que es troben dintre de la carpeta OPNET_mbenitomo conté tots els fitxers que s'han generat i fet servir per a la realització de les proves amb el Opnet IT Gurú i que han servit per realitzar gran part del PFC.

També s'adjunta en la carpeta EP_mbenitomo les configuracions dels 2 switchs que s'ha fet servir en l'entorn de proves real. La configuració dels switchs són 2 arxius .txt amb la nomenclatura: switchX[8].

[8] Número de swith