Universitat Oberta de Catalunya

www.uoc.edu

Treball Final de Carrera

Implantació i emulació d'una VPN sobre VPLS

Alumne: José R. Hidalgo
Consultor: José López Vicario
Titulació: Enginyeria Tècnica en Telecomunicacions, especialitat en Telemàtica

Índex general

Índex d'imatges

Índex de taules

1.- Introducció

1.1.- Descripció del projecte

Aquest projecte vol implantar una VPN a nivell nacional per a *Transports Express S.A*. Aquest client es dedica al transport de paquets de petit i gran volum (des de sobres fins a caixes de grans dimensions). Disposa d'una sucursal en cada província, per així garantir els temps d'enviament dels seus paquets. Les seus principals estan situades en Barcelona i Madrid, on tenen tots els servidors de gestió allotjats en CPDs (Centre de Processament de Dades) totalment condicionats.

Fins ara, per fer servir els seus servidors es connectaven utilitzant un programari que permet la creació d'un túnel VPN des d'una seu remota, amb ADSL asimètrica de velocitat 7296 kbps de baixada i 640 kbps de pujada (amb un 10% de la velocitat garantida), cap a la seva seu central de Barcelona o Madrid. Les seus principals disposen de connexions de fibra òptica amb 10 Mb en cada seu.

Gràcies a la injecció de nou capital estranger volen millorar el funcionament i la seguretat de les seves gestions; s'ha decidit implantar una VPN utilitzant fibres òptiques a totes les seus i millorar la connexió de les seus de Barcelona i Madrid. Per tant, això suposarà una millora substancial de la velocitat de connexió a les seus provincials, podent donant un servei de millor qualitat als seus clients.

Per a implantar el projecte que l'empresa demana es realitzarà la configuració dels routers de tota la xarxa, prenent cura de cobrir les seves necessitats i escollint les que més s'ajustin al seu treball diari.

Finalment, per a comprovar que tot el que s'ha proposat en els diferents punts del projecte funciona, es farà una emulació d'una part de les seus de *Transports Express S.A*. En l'emulació s'utilitzarà el programari GNS 3, que emula routers de l'empresa Cisco, utilitzant IOS reals de cada model de router i aconseguint així uns resultats molt propers a la realitat. D'aquesta manera, es farà la configuració d'una sèrie de routers que representaran les seus i es realitzaran diferents proves per a confirmar que la comunicació entre seus funciona, i així veure com s'acompleix tot el plantejat en el projecte i que cobreix les necessitats de *Transports Express S.A*.

1.2.- Objectiu del projecte

L'objectiu d'aquest projecte és la implantació d'una VPN en una empresa fictícia. Es portarà a terme la configuració de tots els routers de la xarxa WAN del client, explicant perquè s'ha arribat a aquesta decisió, i exposant la configuració final escollida (routing dinàmic/estàtic, direccionament de cada seu...). També es realitzarà la simulació de les configuracions escollides per a demostrar que funciona perfectament en la pràctica.

Per tant, l'objectiu principal d'aquest projecte serà comprendre les necessitats de comunicació d'una empresa i crear una solució real que es pugui aplicar a una empresa.

2.- Diagrama Gantt del projecte

Segons les entregues que s'han de realitzar i dels punts que ha de tenir aquest projecte, s'ha elaborat un diagrama de Gantt on s'indica el temps de duració de cada tasca per arribar al dia d'entrega:

Implantació d'una VPN sobre VPLS	**87 días**	**mié 18/09/13**	**jue 16/01/14**
Decisió del projecte	6 días	mié 18/09/13	mié 25/09/13
PAC 1	**6 días**	**jue 26/09/13**	**jue 03/10/13**
Recerca d'informació tècnica bàsica	3 días	jue 26/09/13	lun 30/09/13
Descripció detallada del projecte	1 día	mar 01/10/13	mar 01/10/13
Objectius del projecte	1 día	mié 02/10/13	mié 02/10/13
Aproximació dels apartats del projecte	1 día	jue 03/10/13	jue 03/10/13
PAC 2	**33 días**	**vie 04/10/13**	**mar 19/11/13**
Necesitats WAN de Transports Express S	5 días	vie 04/10/13	jue 10/10/13
Recerca informació VPN	4 días	vie 11/10/13	mié 16/10/13
Recerca infomació routers	4 días	jue 17/10/13	mar 22/10/13
Recerca informació Routing dinàmic	5 días	mié 23/10/13	mar 29/10/13
Material, tecnologia i configuració escol	5 días	mié 30/10/13	mar 05/11/13
Configuració dels routers	10 días	mié 06/11/13	mar 19/11/13
PAC 3	**20 días**	**mié 20/11/13**	**mar 17/12/13**
Emulació de la xarxa amb GNS 3	10 días	mié 20/11/13	mar 03/12/13
Realització pressupost	10 días	mié 04/12/13	mar 17/12/13
Lliurament final de la memòria	**18 días**	**mié 18/12/13**	**vie 10/01/14**
Revisio del projecte	8 días	mié 18/12/13	vie 27/12/13
Presentació Power Point	10 días	lun 30/12/13	vie 10/01/14
Entrega de la presentació	**5 días**	**sáb 11/01/14**	**jue 16/01/14**
Revisió de la presentació Power Point	5 días	sáb 11/01/14	jue 16/01/14

3.- Necessitats WAN de Transports Express S.A.

L'empresa té un total de 52 seus repartides per tota Espanya. Existeixen dos tipus de seu: les centrals i les remotes. Hi han 2 seus centrals que són les que tenen més volum de treball i per tant més treballadors. Després hi han 50 seus remotes que es dispersen per tota la península (una per província en la península, a Ceuta, a Melilla, a les Illes Balears i dues a les Illes Canàries).

Transports Express S.A. ja ens avança que vol totes les seus amb un accés simètric de 10 MB excepte a les seus centrals que el voldrà d'1GB amb un cabal encara per definir.

3.1- Seus Centrals

Transports Express S.A. té dues seus principals, una a Barcelona i una altre a Madrid. Aquestes instal·lacions estan situades en CPDs a les pròpies oficines de l'empresa i és on es troben ubicats els seus servidors. Les instal·lacions tenen tots els equipaments

necessaris (per exemple: cablejat sobredimensionat per futures ampliacions, racks, aire condicionat, grups electrògens per evitar talls elèctrics, sistema antiincendi...).

La seu de Barcelona és on s'allotgen els servidors principals de tota l'empresa i per tant disposarà de doble accés i doble router, de tal manera que un treballarà com a principal i l'altre en mode redundant.

La seu de Madrid s'utilitza per a realitzar les còpies de seguretat dels seus servidors que periòdicament fa l'empresa.

En cas d'incomunicació total de la seu de Barcelona, és la seu de Madrid la que assumiria tots els tràmits dels servidors interns de forma temporal.

3.2- Seus remotes

Disposen d'una delegació per província i cadascuna d'aquestes té entre 5 i 20 treballadors entre empleats d'oficina i repartidors.

Aquests tipus de seus ens indiquen que no necessiten accés o router redundant; és a dir que cada seu remota tindrà únicament un router i una línia d'accés. Les províncies on hi haurà una seu remota es descriuen en el proper punt.

3.3- Direccionament LAN

Transports Express S.A. ja disposa d'un direccionament LAN assignat que ha de mantenir, existint una llista per seu on s'indica quina direcció LAN tindrà cada router i quina xarxa publicarà a la resta de seus. Tenen un rang LAN 10.0.0.0/16 (Clase A, des de la IP 10.0.0.0 fins la 10.0.255.255), fent divisions de subxarxes amb màscara 255.255.255.0 (en decimal 24). No tenen tot el rang ocupat, però volen deixar subxarxes lliures per a futures ampliacions de servidors o diferents serveis. Adjuntem la taula del direccionament LAN de totes les seus:

Província	Xarxa LAN
Barcelona	10.0.0.0/24 [rang treballadors] 10.0.255.0/24 [rang servidors]*
Madrid	10.0.1.0/24 [rang treballadors] 10.0.254.0/24 [rang servidors redundants]*
Àlaba	10.0.2.0/24
Alacant	10.0.3.0/24
Albacete	10.0.4.0/24
Almeria	10.0.5.0/24
Astúries	10.0.6.0/24
Àvila	10.0.7.0/24
Badajoz	10.0.8.0/24
Biscaia	10.0.9.0/24
Burgos	10.0.10.0/24
Càceres	10.0.11.0/24

Cadis	10.0.12.0/24
Cantàbria	10.0.13.0/24
Castelló	10.0.14.0/24
Ceuta	10.0.15.0/24
Ciutat Real	10.0.16.0/24
Conca	10.0.17.0/24
Còrdova	10.0.18.0/24
A Corunya	10.0.19.0/24
Girona	10.0.20.0/24
Granada	10.0.21.0/24
Guadalajara	10.0.22.0/24
Guipúscoa	10.0.23.0/24
Huelva	10.0.24.0/24
Illes Balears	10.0.25.0/24
Jaén	10.0.26.0/24
La Rioja	10.0.27.0/24
Les Palmes de Gran Canaria	10.0.28.0/24
Lleida	10.0.29.0/24
Lleó	10.0.30.0/24
Lugo	10.0.31.0/24
Màlaga	10.0.32.0/24
Melilla	10.0.33.0/24
Múrcia	10.0.34.0/24
Navarra	10.0.35.0/24
Osca	10.0.36.0/24
Ourense	10.0.37.0/24
Palència	10.0.38.0/24
Pontevedra	10.0.39.0/24
Salamanca	10.0.40.0/24
Santa Cruz de Tenerife	10.0.41.0/24
Saragossa	10.0.42.0/24
Segòvia	10.0.43.0/24
Sevilla	10.0.44.0/24
Sòria	10.0.45.0/24
Tarragona	10.0.46.0/24
Terol	10.0.47.0/24
Toledo	10.0.48.0/24
València	10.0.49.0/24
Valladolid	10.0.50.0/24
Zamora	10.0.51.0/24

Taula 1 - Taula direccionament LAN

El direccionament de les seus remotes és molt fàcil d'entendre, ja que s'ha assignat un rang /24 sencer a cada seu segons el que ens indica l'empresa.

Pel que fa al direccionament de la seu de Barcelona, em vist a la taula que té dues xarxes (una és la que utilitzen els treballadors de la seu 10.0.0.0/24 i una altre el rang dels servidors interns 10.0.255.0/24). La seu de Madrid té també dues xarxes, la LAN dels treballadors amb subxarxa 10.0.1.0/24 i la LAN que es destinarà a la còpia de seguretat dels servidors de Barcelona, que es realitzarà a través de xarxa 10.0.254.0/24.

4.- Estudi tecnològic

Es realitzarà un estudi de totes les tecnologies i equipament que intervinguin en la realització d'una VPN per aquest projecte. Això implica fer una recerca sobre tecnologies de VPN, protocols i el propi equipament de les seus.

4.1.- VPN

Una VPN (*Virtual Private Network*) és l'extensió d'una xarxa LAN, mantenint la seguretat i funcionalitats d'aquesta i connectant, principalment, dues o més xarxes privades.

Les primeres VPN utilitzaven enllaços dedicats i això suposava un gran cost. Als darrers anys les VPN utilitzen la infraestructura pública per a transportar les dades de forma segura i per tant els costos es redueixen molt. Per a proporcionar la màxima seguretat es poden utilitzar sistemes de xifratge com: túnels IPSec, túnels *VPN Secure Socket Layer* (SSL) o altres tecnologies d'autentificació.

Actualment, la tecnologia més utilitzada pels operadors consisteix en la creació d'una VPN sobre MPLS/VPLS (*Multiprotocol Label Switching/Virtual Private LAN Service*) que pot crear una VPN en capa 2 o capa 3. Això el que permet és publicar totes les xarxes LAN del client i només seran visibles per aquest propi client donat que es separa cada client en diferents VRF (*Virtual Routing Forwarding*). A nivell pràctic, cada client tindrà únicament connectivitat amb les xarxes incloses a la seva VRF.

Els motius pels quals aquesta darrera tecnologia de VPN és la que més s'ajusta a aquest client són: l'escalabilitat que té per a futures ampliacions i la ràpida resposta que té al no haver de crear cap túnel mitjançant un software.

4.1.1.- VPN sobre MPLS

La tecnologia MPLS, de l'anglès *Multiprotocol Label Switching*, integra la commutació de paquets i la commutació de circuits. MPLS és una tecnologia emergent dins dels proveïdors de telecomunicacions, però no pretén substituir a l'ATM, ja que el protocol MPLS també suporta ATM o FR, el que és un gran avantatge.

MPLS opera en la capa 2 i 3 del model OSI. El principal avantatge d'operar en aquestes capes és la possibilitat d'intercanviar etiquetes en comptes de direccions IP, realitzant aquest intercanvi a nivell de hardware a una velocitat molt alta.

Com ja s'ha dit amb anterioritat, també pot utilitzar-se amb diferents protocols com ATM, FR o Ethernet, ja que permet etiquetar les trames de nivell 2.

Amb MPLS es pot crear, d'una forma molt senzilla, una VPN per a interconnectar diferents seus d'un mateix client. Per a fer això possible, els equips MPLS són capaços de realitzar varies taules d'encaminament virtual (VRF) en una mateixa interfície i d'aquesta manera es pot utilitzar una interfície per a connectar diferents clients (així s'aconsegueix reduir el cost que tindria un cablejat dedicat). En principi la informació

d'un client no pot ser vista pels altres clients però, si les necessitats d'un client ho requereixen, és possible interconnectar dues o més VRFs canviant la configuració.

Elements que intervenen en una MPLS:

- **LER (*Label Edge Router*):** És l'element que es troba a l'entrada/sortida de la MPLS i fa l'etiquetatge depenent del destí.

- **LSR (*Label Switching Router*):** És l'element que commuta les etiquetes.

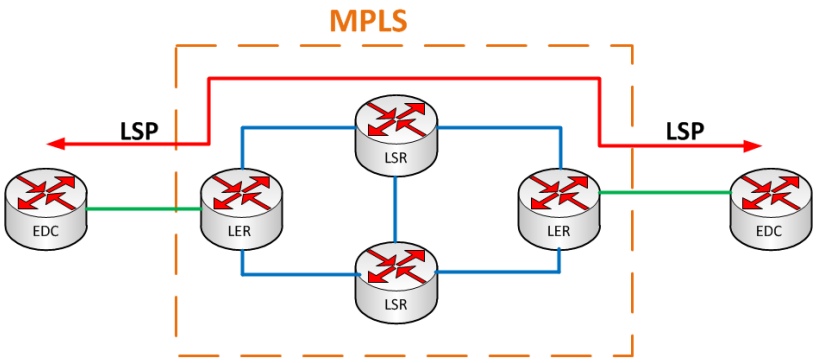
- **LSP (*Label Switched Path*):** És el camí que seguirà cert tràfic (també anomenat FEC) per la MPLS. És un tràfic unidireccional.

- **LDP (*Label Distribution Protocol*):** És el protocol encarregat de distribuir les diferents etiquetes per tots els equips de la MPLS.

- **FEC (*Forwarding Equivalence Class*):** És el nom que se li dóna al tràfic que s'encamina sota una etiqueta.

- **EDC (Equip De Client):** Fa referència al router que es troba a la seu del client.

En la imatge 1 podem veure un gràfic per entendre els punts anteriors:



Imatge 1 - Elements MPLS

Els elements que pertanyen a la MPLS i el seu cablejat, forma part de la infraestructura del ISP. Per a poder connectar els diferents punts d'una MPLS es necessita realitzar Routing en els EDCs, ja sigui estàtic o dinàmic, per tal que la xarxa MPLS sàpiga el camí per arribar al destí.

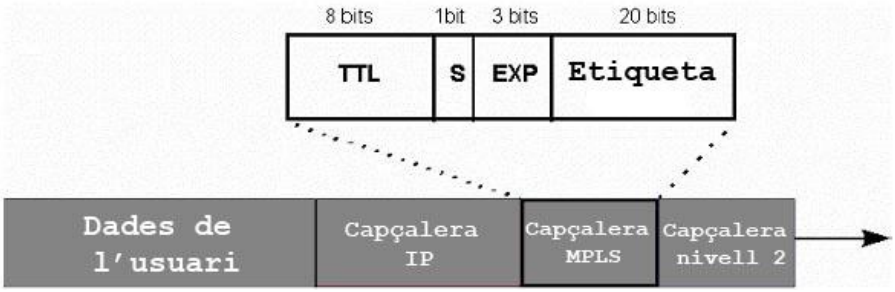
L'encaminament dels diferents paquets en una MPLS es basa en les rutes emmagatzemades en les VRF. La forma d'etiquetatge que té un paquet des de l'origen fins al destí és la següent:

1- El CE (*Customer Edge* o EDC) envia un paquet al PE (*Provider Edge* o LER), aquest afegeix una etiqueta depenen el CE i l'envia, ja que sap com arribar al destí gràcies a la taula d'encaminament de la seva VRF.

2- El LSR encamina el paquet llegint l'etiqueta que li ha enviat LER i també gràcies a la VRF.

3- El PE destí rep el paquet, treu l'etiqueta i l'envia al CE destí.

La forma genèrica d'un etiquetatge MPLS es pot veure en la imatge 2:



Imatge 2 - Etiqueta MPLS

TTL: 8 bits per a indicar el temps de vida el paquet

S: 1 bit que estarà a 0 per a totes les etiquetes i valdrà 1 quan sigui l'etiqueta final

EXP: Bits experimentals relacionats amb la qualitat del servei (QoS)

Etiqueta: 20 bits per a l'etiqueta (valor numèric del 0 al 1048572)

4.1.2.- VPN sobre VPLS

Una VPLS, *Virtual Private LAN Service*, ofereix una comunicació Ethernet realitzant una comunicació punt a multipunt sobre xarxes IP MPLS. Aquesta tecnologia treballa en la capa 2 del model OSI. La xarxa del ISP realitza la funció d'un commutador, com és el cas d'un switch, d'aquesta manera el que es considera una WAN ara es pot considerar una LAN. VPLS reprodueix el funcionament d'un switch, que separa la xarxa en dominis de col·lisió i així permet ampliar els segments Ethernet.

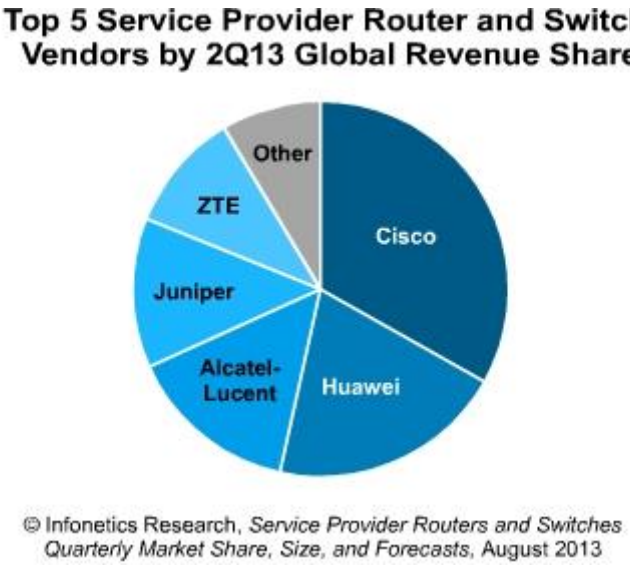
VPLS utilitza els mateixos protocols que s'utilitza en la tecnologia MPLS, així doncs es pot aprofitar la mateixa infraestructura. Les principals avantatges que té són:

- No necessita cap tipus de Routing al equips per a interconnectar els seus nodes.
- VPLS suporta igualment protocols d'enrutament (BGP, RIP, OSPF...).
- Pot utilitzar els mateixos *switches* de la LAN per a connectar les seus

Aqueta tecnologia té tots els avantatges de la xarxa MPLS però afegint la senzillesa que té poder treballar a nivell de la capa 2.

4.2.- Routers

El món de les telecomunicacions actuals és dominat principalment per quatre fabricants de routers: Cisco, Juniper, Alcatel-Lucent i Huawei (segons informe d'Infonerics[1]). Aquestes empreses tenen el 90% de la quota de mercat de routers (*edge* i *core*). Cisco continua sent líder en vendes en el segon quadrimestre del 2013, encara que aquest any Huawei s'està expandint molt. En la imatge 3 es veu el percentatge de vendes en aquest període del 2013:



Imatge 3 - Venda de routers 2Q13

Com podem veure al gràfic, Cisco continua liderant les vendes, però en aquest segon quadrimestre Huawei ha augmentat en 4 punts de mercat consolidant-se en la segona posició.

Després de veure els possibles fabricants, s'analitzaran els quatre que tenen major vendes i s'escolliran dues games de routers per fabricant.

En el cas de *Transports Express S.A.* donat que hi ha dos tipus de seu (la central i la remota), en cada model de router es descriurà una breu explicació de les característiques més destacables que interessen per portar a terme aquest projecte.

4.2.1.- Cisco

El fabricant Cisco System, com la majoria, té diferents models per a cada gama de routers. Després de revisar les diferents games disponibles s'ha escollit la gama Cisco 2600 i Cisco 7200. En concret, els models escollits dins d'aquestes games són: Cisco 2621XM i Cisco 7206VRX. Detallem les seves característiques:

[1] http://www.infonetics.com/pr/2013/2Q13-Service-Provider-Routers-Switches-Market-Highlights.asp

Cisco 2621XM

El model 2621XM es situa en la gama mitjana de Cisco. Consta de múltiples targetes amb diferents tecnologies i això comporta que sigui un router molt polivalent per a utilitzar-se en diversos escenaris.

Imatge 4 - Cisco 2621XM

Interfícies fixes	2x10/100BASE-T 1x Console 1x AUX	
Ranures d'expansió	2 x WIC 1 x AIM	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques	IP/IPv6 IPSec VPN VRRP 802.1q VLAN
Hardware	128 DRAM 32 MB Flash	

Taula 2 - Hardware Cisco 2621XM

Cisco 7206VRX

En la gama més alta de routers per l'àmbit empresarial, trobem el 7206VRX. Consta d'un xassís amb font d'alimentació i una sèrie d'entrades estàndards, però el més interessant és que consta de tres tipus de targetes amb processador que alhora incorporen diferents connexions. També disposa de ranures d'expansió on es poden introduir diferents targetes amb múltiples connexions en funció de les necessitats canviants del client. En el nostre cas s'ha escollit el Cisco 7206VRX amb NPE-G2, que consta de les següents opcions i connexions:

Imatge 5 - Cisco 7206VRX

Interfícies fixes	3x10/100/1000BASE-T 3 x Gigabit Ehernet en SFP (fibra òptica) 1x Console
Ranures d'expansió	1 x I/O targetes 6 x Slots d'expansió
Funcionalitats	BGP IP/IPv6 OSPF IPSec VPN RIP/RIPv2 VRRP Rutes estàtiques 802.1q VLAN
Hardware	Processador 700 MHz BCM1250 64 MB Compact Flash 256 MB DRAM (fins a 2GB)

Taula 3 - Hardware Cisco 7206VRX

4.2.2.- Juniper

El proper fabricant que s'analitzarà és Juniper; aquest és conegut sobretot perquè el fan servir diferents proveïdors de comunicacions com a *Providge Edge*, fent servir les games més altes del fabricant. En el nostre cas concret, s'han escollit les games CTP sèries i J sèries, més concretament els model CTP 150 i J2330. Les seves característiques principals són:

Juniper CTP 150

La gama CTP és la gama baixa-mitjana, dissenyada per a petites empreses sense moltes exigències.

Imatge 6 - Juniper CTP 150

Interfícies fixes	2x 100/1000BASE-T 1x Console 1x AUX
Ranures d'expansió	2 → Mòduls tipus T1/E1 o Serial
Funcionalitats	RIP/RIPv2 Rutes estàtiques OSPF VRRP BGP 802.1q VLAN IPv4/IPv6
Hardware	Sense informació

Taula 4 - Hardware Juniper CTP 150

Juniper J2320

La sèrie J de Juniper ja és una gama alta dins del món empresarial i és creada per a oficines amb un tràfic major de rutes i unes majors exigències.

Imatge 7 – Juniper J2320

Interfícies fixes	4x10/100/1000 BASE-T 1x Console 1x AUX	
Ranures d'expansió	3 x PIM	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques	IP/IPv6 IPSec VPN VRRP 802.1q VLAN
Hardware	1 GB DRAM Compact Flash 1GB Acceleració d'encriptació de hardware opcional	

Taula 5 - Hardware Juniper J2320

4.2.3.- Huawei

Huawei és un fabricant xinès que en els darrers anys s'està expandint molt en el món de les telecomunicacions, i fabrica des de routers particulars o empresarials fins a telèfons mòbils. Com s'ha indicat amb anterioritat, en els darrers anys està creixent molt, fins arribar a aquest últim quadrimestre del 2013 amb un augment considerable en les seves vendes.

Després de fer una recerca sobre els models que disposen, s'ha escollit els routers AR28-10 i AR2200.

Huawei AR28-10

Destinat a les petites i mitjanes empreses, disposa de dues ranures d'expansió SIC i una altre MIM per tal de poder tenir diferents interfícies.

Imatge 8 - Huawei AR28-10

Les característiques principals són:

Interfícies fixes	4x 10/100BASE-T 1x Console 1x Aux	
Ranures d'expansió	2x SIC 1xMIM	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques IPv4	IPSec VPN VRRP 802.1q VLAN SIP
Hardware	128 MB DRAM 32 MB Flash	

Taula 6 - Hardware Huawei AR28-10

Huawei AR2200

La gama AR2200 és la gama empresarial de Huawei i es basa en la tecnologia pròpia de la marca, Versatile Routing Platform (VRP). Aquesta tecnologia agrupa les comunicacions *wireless*, accés a la xarxa, *swtching*, 3G, veu i funcions de seguretat.

Imatge 9 - Huawei AR2200

Les característiques a destacar d'aquest model són:

Interfícies fixes	3x 10/100/1000BASE-T 1x Console 1x Aux	
Ranures d'expansió	4x SIC 2x WSIC 1x DSP	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques IPv4	IPSec VPN VRRP 802.1q VLAN SIP
Hardware	2 GB DRAM 2 GB Flash	

Taula 7 - Hardware Huawei AR2200

4.2.4.- Alcatel-Lucent

Alcatel-Lucent (resultat de la fusió de l'empresa francesa Alcatel amb la nord-americana Lucent), al igual que Huawei, és molt coneguda pels proveïdors de telecomunicacions, ja que l'utilitzen com a *Provider Edge* i DSLAM. A la vegada, té routers i equipament de totes les games, des de games per a una petita empresa fins a games per grans empreses que requereixen un alt rendiment. En el nostre cas s'han escollit les games OmniAccess 5800 i 7705 SAR:

Alcatel-Lucent OmniAccess 5840

El OmniAccess 5840 és un router que pot ser utilitzat com a router i servidor a la vegada, gràcies al seu robust hardware. Es pot fer servir per a connectar tot tipus de maquinari de LAN i a la vegada com a router professional.

Imatge 10 - Alcatel-Lucent OmniAccess 5840

Les característiques principals són:

Interfícies fixes	2x 10/100/1000BASE-T 8x FastEthernet PoE 1x Console	
Ranures d'expansió	1x Multi-interfícies 1x Sistemes DSL	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques IPv4/IPv6	IPSec VPN VRRP HSRP 802.1q VLAN SIP
Hardware	Processador Dual Core 800 MHz 64 MB Flash 512 MB RAM	

Taula 8 - Hardware Alcatel-Lucent OmniAccess 5840

Alcatel-Lucent 7705 SAR-M

El 7705 SAR-M està dirigit a les noves tecnologies com son Ethernet i IP/MPLS, però continuen treballant amb ATM, FR o TDM. Com els routers anteriors, és capaç de treballar en capa 2 o capa 3 del model OSI.

Imatge 11 - Alcatel-Lucent 7705 SAR-M

Les característiques principals són:

Interfícies fixes	3x 10/100/1000BASE-T 4x 10/100/1000BASE-TX 1x Console	
Ranures d'expansió	1x Multi-interfícies	
Funcionalitats	BGP OSPF RIP/RIPv2 Rutes estàtiques IPv4/IPv6	IPSec VPN VRRP HSRP 802.1q VLAN SIP
Hardware	2 GB Compact Flash 1 GB RAM	

Taula 9 - Hardware Alcatel-Lucent 7705 SAR-M

4.3.- Protocols

Un protocol en les comunicacions és un conjunt de normes que regulen una comunicació entre diferents equips. Hi ha diferents tipus de protocols que s'instrumentalitzen en diferents paquets.

Arribats a aquest punt del projecte, on ja tenim clar el que *Transports Express S.A.* necessita, hem del parlar dels protocols que implementarem a la xarxa, com són els protocols d'enrutament o de redundància.

Indagarem en els més coneguts i els que més s'apropen a les característiques de la xarxa que volem implementar.

4.3.1.- Protocols d'enrutament dinàmic

En un entorn en que diferents elements de xarxa, com el router i el switch, han de comunicar-se entre si, hem d'estar segurs que el tràfic seguirà un camí el més estable i eficient possible.

Desestimant l'opció de realitzar enrutament estàtic per la seva ineficiència en xarxes de comunicacions de gran mida, tenim que realitzar enrutament dinàmic, i així poder tenir una major escalabilitat de la xarxa i aconseguir guiar el tràfic d'una forma més eficient fins al seu destí.

4.3.1.1.- RIP

Routing Information Protocol (RIP), és un protocol vector-distància, és a dir, utilitza el número de salts que hi ha de l'origen fins al destí, i en funció d'aquests tindrà una "mètrica" diferent. El número de salts màxim per arribar al destí són 15 i si arriba a 16 es dóna com a destí inaccessible.

Actualment hi ha tres versions de RIP:

RIPv1

El major inconvenient de la versió 1 és la incompatibilitat amb màscara variable (VLSM) i CIDR. Fa uns anys, quan la quantitat de xarxes era molt inferior no era un gran problema, però actualment és un inconvenient molt gran. Tampoc té cap autenticació de missatge i això provoca que sigui més vulnerable a atacs.

RIPv2

La principal millora és la introducció de la compatibilitat amb VLSM i CIDR, permetent fer subxarxes de diferent mida. També incorpora l'autentificació mitjançant contrasenya o bé autentificació de contrasenya amb MD5.

La limitació de 15 salts de la versió 1 es continua mantenint.

RIPng

Aquesta versió s'actualitza mirant al futur. S'incorpora la compatibilitat amb IPv6. La resta de característiques les hereta de RIPv2, exceptuant la compatibilitat amb les autentificacions d'actualitzacions de RIPv1.

En totes les versions, la taula de rutes s'actualitza completament cada 180 segons, per tant, si una ruta es deixa de rebre quan s'actualitza la taula (la seva mètrica es posa com a infinit a la taula), passat 60 segons més l'esborra completament.

4.3.1.2.- OSPF

Open Shot Path First (OSPF) és un enrutament basat en l'estat de l'enllaç i implementa l'algoritme de Dijkstra per calcular la ruta més curta fins a cada destí. Està pensat tant per entorns d'Internet com a protocol intern ja que distribueix la informació entre els equips que pertanyen al mateix sistema autònom (en anglès Autonomous System, o AS). El cost de l'enllaç el calcula tenint en compte l'ample de banda, per tant és molt important tenir ben configurat aquest paràmetre a la interfície on s'implementi OSPF.

OSPF envia paquets per a veure l'estat dels veïns i per defecte aquest temps és de 10 segons. Un router espera quatre vegades aquest temps per a declarar un host sense connexió. Per enviar aquest paquet no s'utilitza TCP ni UDP sinó que fa servir el protocol IP.

Els paquets que s'envien entre routers poden ser:

- **Paquets *Hello*:** S'envia periòdicament un paquet, i així s'estableix i descobreix relació amb els veïns.

- **Paquets *Link State Rquest*:** Sol·liciten informació d'adjacències als routers veïns en fase d'establiment i intercanvi.

- **Paquets *Link State Update*:** S'envia informació als veïns.

- **Paquets *Link State Acknowledgmen*":** Confirma els missatges rebuts.

- **Paquets *Database Description*:** Intercanvien dos routers la base de dades de l'enllaç-estat.

Depenent de la situació de cada router, tindrà unes o altres connexions, donant-li unes funciones o altres. El rol que pot tindre cada router son:

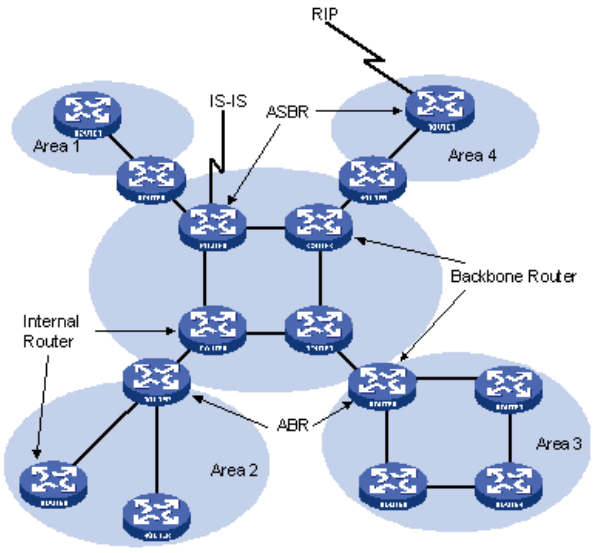
- ***Internal Router* (IR):** Només tindrà com a veïns equips de la seva mateixa àrea.

- ***Area Border Router* (ABR):** Router que fa frontera amb una altra àrea, interconnectant aquestes dues. Tindrà connexió amb l'àrea cero (la seva pròpia) i una altra.

- ***Backbone Router* (BR):** Aquest router té com a mínim una interfície connectada a l'àrea cero. Pot ser BR o ABR si té més d'una connexió.

- ***Autonomous System Border Router* (ASBR):** Tindrà connexions fóra del seu AS amb xarxes que no pot administrar. S'encarregarà de distribuir les xarxes del seu AS cap a altres xarxes.

A la imatge 12 es pot veure un exemple de topologia i el rol que té cada router:



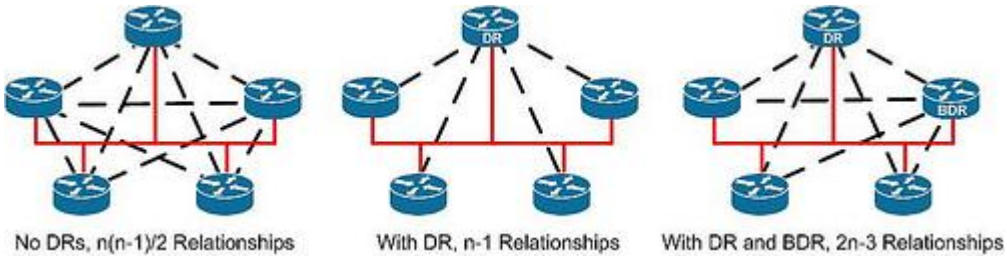
Imatge 12 - Rol routers OSPF

Pot donar-se el cas, com en xarxes Ethernet, que hi hagi un accés múltiple cap a un mateix destí, i això suposa una càrrega molt gran de tràfic ja que es crea una relació de tots amb tots. Per a evitar aquest problema, OSPF té dos tipus de rol que poden tenir els routers de la xarxa:

- ***Designated Router* (DR):** Aquest router rep totes la informació de la resta de routers de la xara, i és el DR l'encarregat de retransmetre a tots la informació. D'aquesta manera s'evita de que cada router hagi de transmetre tota la informació a la resta de routers.

- ***Backup Designated Router* (BDR):** El router BDR té la mateixa informació que el DR, però només retransmet la informació a la resta de routers quan no hi ha connexió amb DR; en altres paraules seria com una còpia de seguretat de la informació referent a les rutes.

En la imatge 13 es pot veure segons quin rol tingui cada router el número de relacions que hi haurà a tota la xarxa:



Imatge 13 – Rol routers topologia OSPF

Tenint en compte els rols que poden agafar cada tipus de router depenent la seva situació dins l'àrea, existeixen els següents tipus d'àrees:

- **Àrea *stub*:** S'anomena així a la xarxa que no accepta cap mena de rutes externes al AS (redistribució). Per aconseguir això, s'ha de realitzar un ruta predeterminada, ja sigui per defecte (ruta 0.0.0.0) o bé reenviant el tràfic al següent salt corresponent.

- **NSSA (*Not-So-Stubby Area*):** Aquest tipus tampoc pot rebre cap ruta externa redistribuïda, però si és pot rebre rutes d'un altre AS utilitzant un altre protocol d'enrutament (RIP, EIGRP...).

4.3.1.3.- EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) és una millora del seu antecessor IGRP, on tots dos protocols són propietat de Cisco System. EIGRP utilitza els algoritmes de vector distància i estat de l'enllaç. Com en l'OSPF, també es separa en diferents sistemes autònoms per a un major control de la xarxa.

EIGRP utilitza el protocol RTP (*Real-Time Transport Protocol*), i així poder garantir que els paquets arriben als seus veïns de forma ordenada i amb confirmació de recepció. EIGRP envia cinc tipus de paquets diferents:

- ***Hello*:** S'envia per a descobrir nous veïns.
- ***Update*:** S'envia quan hi ha canvis a les rutes i només són per als routers afectats. Pot ser *unicast* (per a un únic router) o bé *multicast* (per a varis routers). L'algoritme que es fa servir és el DUAL (*Diffusing Update Algorithm*).
- ***Query*:** S'envia quan es perd la connexió amb un veí. Sempre és de tipus *multicast* i s'envia a tots els seus veïns.
- ***Reply*:** S'envia com a resposta d'un paquet *Query* i sempre és *unicast*.
- **ACK:** S'envia com a confirmació que s'ha rebut un paquet. S'utilitza únicament amb paquets *Update*, *Query* i *Reply*.

EIGRP té tota la informació de rutes i topologia per aconseguir arribar a un destí pel millor camí possible. Per aconseguir-ho es disposa de tres tipus de taules diferents:

- **Taula de veïns:** S'emmagatzema les rutes cap als seus veïns.
- **Taula de topologia:** S'emmagatzema totes les taules d'enrutament que rep dels seus routers veïns. Amb aquestes dades, EIGRP calcula les rutes amb menor cost cap a cada destí.
- **Taula d'enrutament:** S'emmagatzema la millor ruta per arribar a cada destí, que l'extreu de la taula de topologia.

La mètrica pot obtenir un valor de 1 a 4294967296. Per a calcular-la, EIGRP utilitza una fórmula bastant complexa:

$$Métrica = 256 * \left[\left(K1 * \frac{10^7}{BW} + \frac{K2 * BW}{256 - Load} + K3 * \left(\frac{\sum DLY}{10}\right)\right) * \frac{K5}{K4 * Rely}\right]$$

La fórmula té dos tipus de paràmetres, els que són modificables i els que no ho són:

- Paràmetres no modificables:
    - **BW:** Bandwith, que és l'ample de banda de la interfície
    - **Load:** Càrrega de tràfic que té la interfície
    - **DLY:** Delay, que és la suma de tots els retards entre l'origen i el destí
    - **Rely:** Fiabilitat que té l'enllaç
- Paràmetres modificables:
    - **K1:** Modificador d'ample de banda, per defecte 1
    - **K2:** Modificador de la carda de l'enllaç, per defecte 0
    - **K3:** Modificador de retràs, per defecte 1

- **K4:** Modificador de la fiabilitat, per defecte 0
- **K5:** Modificador de la MTU, per defecte 0

Si els paràmetres modificables es deixen amb el seu valor per defecte, la fórmula es simplifica molt:

$$Métrica = 256 * \left[\frac{10^7}{BW} + \frac{\sum DLY}{10}\right]$$

Si es modifica els paràmetres modificables 'K', s'ha de tenir en compte que tots els routers que vulguin tenir veïnatge (dos o més router que siguin veïns), han de tenir el mateix valor de 'K' i el mateix AS.

4.3.1.4.- BGP

BGP (*Border Gateway Protocol*) és un protocol que també es divideix en sistemes autònoms. L'ús del BGP està més estès entre els proveïdors d'Internet. Cada proveïdor té assignat un únic AS i per a comunicar-se entre els diferents AS utilitzen BGP per a intercanviar les seves rutes. Aquest intercanvi de rutes es realitza entre els routers frontera de cada AS.

BGP accepta connexions tant dins del seu propi AS com AS externs. Si les connexions són dins del seu AS, estarem parlant de iBGP (*internal* BGP). Si les connexions són amb un AS extern, parlem de eBGP (*external* BGP).

El protocol BGP està basat en el protocol de vector camins per a l'intercanvi d'informació de l'enrutament. A diferència dels protocols com OSPF, RIP o EIGRP, BGP no utilitza els números de salts, ample de banda o retard per a obtenir una mètrica; sinó que l'obté directament de la política de xarxa o diferents atributs que s'especifiquen directament en la configuració del protocol BGP.

Per a l'intercanvi d'informació entre la pròpia o diferents xarxes, s'utilitza una sessió basada en TCP pel port 179. Aquestes sessions es mantenen connectades ja que periòdicament s'han d'intercanviar informació. Els missatges que es poden intercanviar són:

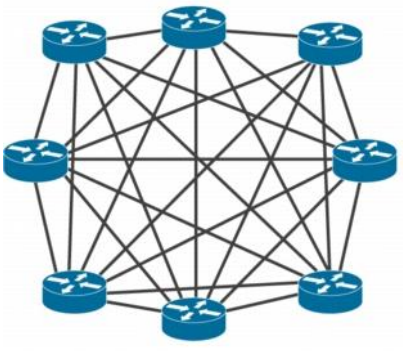
- ***OPEN*:** S'utilitza per a l'establiment de la sessió BGP, on es negocia diferents paràmetres (versió BGP que s'utilitzarà, temps d'espera màxims sense respondre un destí...).
- ***UPDATE*:** És un missatge d'actualització de les rutes. En aquest missatge s'anuncien el nous prefixes.
- ***KEEPALIVE*:** Quan la sessió ja està establerta, s'envia aquest tipus de missatge de forma periòdica. El que fa aquest missatge és confirmar que l'altre extrem continua actiu.
- ***NOTIFICATION*:** S'envia aquest missatge quan es tanca una sessió BGP.

Un protocol d'encaminament indica quin o quins camins es poden seguir per arribar a un destí. En BGP s'utilitza diferents atributs per aconseguir-ho:

- ***ORIGIN*:** Identifica el mecanisme en que s'ha anunciat un prefix. Pot ser IGP (*Internal Gateway Protocol*), EGP (*External Gateway Protocol*) o bé INCOMPLETE (normalment quan és per ruta estàtica).
- ***AS-PATH*:** Emmagatzema una llista dels diferents AS que identifica la ruta de AS pels quals ha passat l'anunci.
- ***NEXT-HOP*:** Identifica la direcció IP del següent salt cap a una IP de destí.
- **MED (*Multi-Exit-Discriminator*):** Identifica quan hi ha múltiples accessos cap a un mateix AS. Es pot utilitzar per a realitzar un balanceig de càrrega entre dos accessos. Tindrà preferència el que tingui un valor inferior de MED.
- ***LOCAL-PREFERENCE*:** És un paràmetre molt útil quan tenim dos camins iguals per arribar a un mateix destí. Aquest paràmetre s'utilitza dins del mateix sistema autònom, i donarà preferència a l'enllaç que tingui un valor de LOCAL-PREF més alt, sent el valor per defecte 100.
- ***COMMUNITY*:** S'utilitza per a agrupar diferents destins, i així poder tractar-los de la mateixa manera d'una forma més simplificada.

En eBGP s'utilitza l'atribut AS_PATH. Quan un router anuncia un prefix a un AS veí, li afegeix el seu número d'AS. Això fa que quan un router rep un prefix amb el seu propi AS, rebutja l'anunci.

IBGP no és pràctic implementar-lo en una xarxa d'una mida mitjana/gran donat que es crea una topologia *full-mesh* (Imatge 14, tots els routers tenen les rutes de tots els destins):



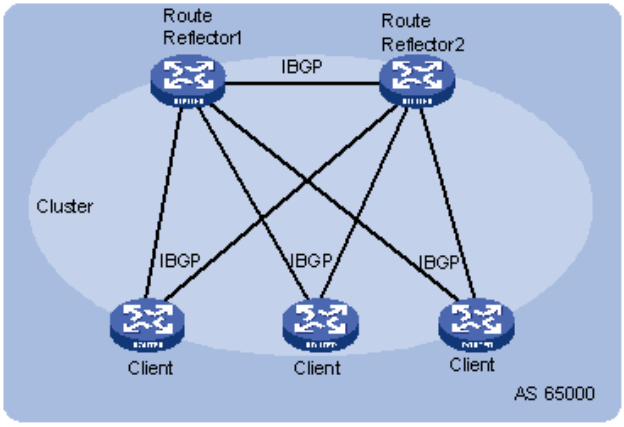
Imatge 14 - Topologia BGP full-mesh

Això implica una sèrie d'inconvenients:

- **Topologia poc pràctica:** Si s'afegeix o s'elimina un router, s'hauria de reconfigurar la resta de routers, per treure o afegir la xarxa.

- **Gran quantitat de missatges BGP:** Quan hi ha un petit canvi a la xarxa, aquest es replica de tots els routers a tots els routers, incloent els que no es veuen afectats per aquest canvi.
- **Gran quantitat de sessions BGP:** Com es veu en la imatge 14, cada router té la ruta de la resta. Això provoca una quantitat molt gran de sessions BGP en tota la xarxa, en concret el número de sessions es calcula amb la fórmula [N·(N-1)] / 2, on N és el número de routers que hi ha a la xarxa.

Per a resoldre els inconvenients d'utilitzar iBGP en una xarxa de gran mida , s'utilitza la creació de *Route-Reflectors* (RR). Tots els veïns anuncien les seves rutes al RR, i és el RR qui les reenvia a la resta. D'aquesta manera, tenim una xarxa molt més escalable i amb un consum de recursos contingut. A la imatge 15 es pot veure una topologia amb dos RR:



Imatge 15 - Topologia BGP Route-Reflector

El motiu de tindre dos RR és per redundància, ja que si només hi hagués un RR i aquest perd la connexió, tota la xarxa deixaria de conèixer les rutes. D'aquesta manera, són dos els routers que tenen totes les rutes de la xarxa, i per tant són veïns dels routers clients. Tots els routers formen un clúster, que no és més que el conjunt de RRs i els seus clients.

4.3.1.5.- Comparació protocols d'enrutament dinàmic

S'ha comentat varis protocols d'enrutament dinàmic. Per aclarir conceptes i diferències, afegirem una breu taula dels aspectes més importants de cada protocol per a distingir els avantatges i inconvenients dels mateixos:

	RIPv1	RIPv2	EIGRP	OSPF	BGP
Vector distància	Si	Si	Si	No	Si
Estat d'enllaç	No	No	No	Si	No
Direccionament sense classe	No	Si	Si	Si	Si
VLSM	No	Si	Si	Si	Si
Sumarització automàtica	Si	Si	Si	-	Si
Sumarització manual	No	Si	Si	Si	Si
Compatibilitat	Universal	Universal	Cisco	Universal	Universal
Mida de la xarxa	Petita	Petita	Gran	Gran	Molt gran
Selecció de ruta	Salts	Salts	Varies mètriques	Cost	Atributs de ruta
Temps de convergència	Lent	Lent	Molt ràpid	Ràpid	Lent
Distancia administrativa (AD)	120	120	5/90/170	110	200

Taula 10 - Comparativa protocols d'enrutament

4.3.2.- Protocols de redundància

El protocol de redundància permet tenir dos o més routers amb la mateixa porta d'enllaç, configurats un com a principal i els altres com a redundants. Això el que fa és tenir una redundància de router on el propi protocol crea una porta d'enllaç virtual comú en els routers i que tenen tots els equips; i la IP de la interfície física té una diferent cada router. Si el router principal no funciona, el redundant assumeix tot el tràfic gràcies a aquest protocol.

Aquest protocol s'implementarà a la seu de Barcelona, com ja s'ha explicat al punt 3.2, tindrà doble router i accés, per tant s'ha de controlar quin router és el principal. Protocols de redundància hi ha varis, ja sigui propietari o estàndard. En parlarem dels dos més estesos.

4.3.2.1.- HSRP

Hot Standby Router Protocol (HSRP), és un protocol de redundància propietat de Cisco. El funcionament és el següent: Es crea un grup de routers (clúster) on un d'ells és el principal assumint tot el tràfic, i la resta es queden com a redundància a la espera que el principal tingui algun problema.

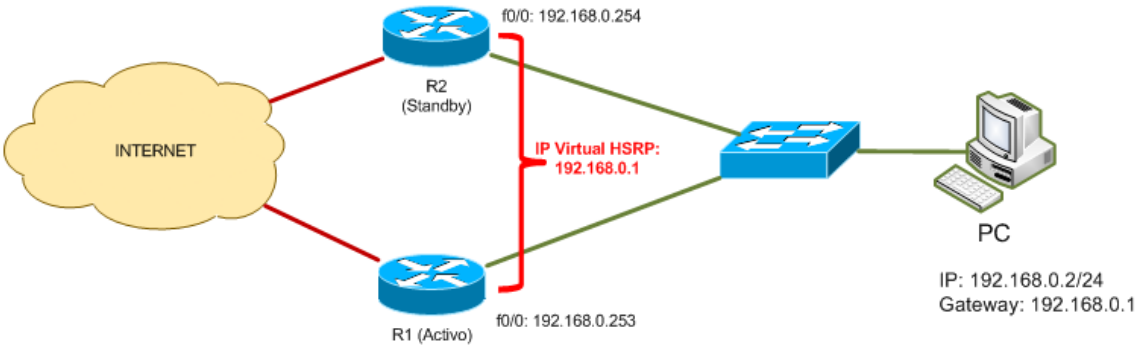
Cada router se li assigna una preferència (per defecte és 100). El router que tingui la preferència més alta dins del seu clúster, serà el router principal.

Per saber quin és l'estat de cada router, s'envien paquets *'Hello'* entre els routers (*multicast*) utilitzant UDP pel port 1985. Quan un router no contesta llavors el seu estat canvia.

Els routers poden tenir diferents estats:

- ***Initial*:** Encara no ha començat a treballar el HSRP. Està en aquest estat en el moment en que la interfície es connecta.
- ***Listen*:** Està escoltant els paquets *Hello*.
- ***Speak*:** Envia *Hello* i està negociant el rol de cada router (*Active* o *Standby*).
- ***Active*:** El router ha agafat el rol d'actiu, per tant serà el router que tingui el tràfic.
- ***Standby*:** El router està en mode d'espera, i començaria a funcionar en cas que l'actiu tingués algun problema.

En la imatge 16 podem veure un escenari amb dos routers i HSRP:



Imatge 16 - Escenari HSRP

Podem apreciar com la IP de la porta d'enllaç de l'ordinador és la virtual del HSRP, i després tenim dues IPs físiques, totes elles dins de la mateixa subxarxa.

4.3.2.2.- VRRP

Virtual Router Redundancy Protocol (VRRP), és l'estàndard d'aquest tipus de protocol. En realitat, primer va sortir el HSRP de Cisco i posteriorment l'estandardització, per tant el seu funcionament base és igual al del HSRP però no compatibles entre ells.

El router virtual sempre tindrà la MAC 00-00-5E-00-01-XX, on XX serà VRID (*Virtual Router IDentifier),* que és diferent per a cada router virtual de la xarxa. Com la MAC només la pot fer servir un únic router físic a la vegada, el VRID és la forma que altres router físics sàpiguen qui és el router principal. Els routers es comuniquen entre ells de forma *multicast* utilitzant el protocol IP pel port 112. El router principal per defecte té prioritat 255, i els *backups* entre 1 i 254.

En VRRP els estats són:

- ***Master*:** El router està com actiu, cursant tot el tràfic del grup VRRP.
- ***Backup*:** El router està esperant si falla el *Master*.
- ***Initialize*:** Estan parlant per veure qui té el rol de *Master* i *Backup*.

5.- Tecnologia escollida

S'ha fet un estudi tecnològic d'aquest projecte i en funció de les necessitats que té *Transports Express S.A.* s'argumentaran les diferents eleccions escollides.

5.1- Tipus VPN

Després de portar a terme un estudi sobre les possibles VPN que podrien utilitzar-se per aquest projecte, s'ha escollit la creació d'una VPN sobre VPLS (VPLS permet la creació d'una VPN molt polivalent).

Suporta Ethernet i per tant permet tant la creació des d'una xarxa senzilla VPN amb la mateixa xarxa a totes les seus, com la realització d'una xarxa complexa amb diferent direccionament.

A més a més, VPLS combina els avantatges de la MPLS amb les àmplies possibilitats que dóna treballar amb Capa 2. Podríem dir que a nivell topològic és com si totes les seus estiguessin connectades a un mateix *switch* de Capa 2.

Necessitarem tres accessos d'1Gbps per a les seus principals amb un cabal de 300 Mbps; i per les seus remotes tindrem 50 línies de 10 Mbps. Recordem que una exigència del client era que volia tenir totes les seves seus amb fibra òptica, i així poder tenir l'ample de banda que necessiten. Cada seu tindrà un convertidor de medis propietat del ISP, que passarà la senyal òptica de la fibra a cable Ethernet per a poder connectar-lo a la interfície del router.

Com hem dit, hi ha 50 seus remotes, cadascuna amb un cabal màxim de 10 Mbps. Pràcticament en cap moment estaran generant tràfic les 50 seus al 100% de la seva

velocitat i per això s'ha contractat un cabal de 300 Mbps a les seus principals (Barcelona i Madrid) per tal d'obtenir un pressupost ajustat. Així doncs, si no posem cap tipus de limitació entre les seus principals deixarem quasi sense ample de banda a les seus remotes. Per tant, hem de limitar el tràfic entre les dues seus a 100 Mbps i així deixem un ample de banda suficient per quan es realitzin les còpies de seguretat de Barcelona a Madrid. Ens quedarà un ample de banda de 200 Mbps per a les 50 seus remotes.

5.2.- Tipus de routers

El fabricant de routers que s'ha escollit ha sigut Cisco System, concretament tal com s'assenyalava al punt 4.2.1 els dos models Cisco 2621XM i Cisco 7206VRX. Aquest router tenen un preu més elevat que la resta de models plantejats dels altres fabricants. De tota manera, els ISP donen la possibilitat d'arrendar els routers amb una quota mensual que inclou el manteniment integral (canvi de router, canvi de peces espatllades, substitució de model en cas que no hi hagi recanvis al ser model obsolet etc.). Per tant el cost mensual entre diferents marques de routers es mínim, i d'aquesta manera l'impacte econòmic inicial és inferior, al no requerir la compra de material.

Cisco té una llarga experiència al sector de les telecomunicacions i és líder en vendes. El seu hardware és molt robust i té múltiples targetes d'ampliació. També és compatible amb totes les tecnologies i protocols i alhora disposa dels seus propis protocols.

Pel que fa al software, Cisco té un CLI (*Command-Line Interface*) molt senzill i intuïtiu que implementa als seus routers. La comunitat Cisco té molta presència a internet (tant a nivell d'aficionats com de professionals o del propi fabricant). Algunes formes d'ajuda a l'hora d'implementar una configuració poden ser: vídeo tutorials, amplis exemples de configuració, suport en fòrums...

S'instal·laran tres routers Cisco 7206VRX a les seus principals, dos a Barcelona i un a Madrid; per les seus remotes es necessitaran 50 routers Cisco 2621XM.

5.3.- Tipus de protocol d'enrutament

Generalment a una xarxa VPLS que treballa en capa 2 no seria necessari escollir un protocol d'enrutament, però en el cas de *Transports Express S.A.* al tenir diferents subxarxes a cada seu si es necessitarà un protocol d'enrutament per a comunicar una seu amb una altre.

S'ha escollit el protocol BGP, més concretament serà iBGP ja que només tindrà un únic AS. Els altres protocols eren massa complexos (OSPF, EIGRP) o massa obsolets (RIP) per a l'escenari que estem plantejant, ja que no es necessita que el protocol calculi diferents camins depenent de l'estat de la xarxa.

Es configurarà dos RR en tota la xarxa per evitar inundar la xarxa de sessions BGP. Els routers escollits són el de la seu de Madrid i el router redundant de la seu de Barcelona.

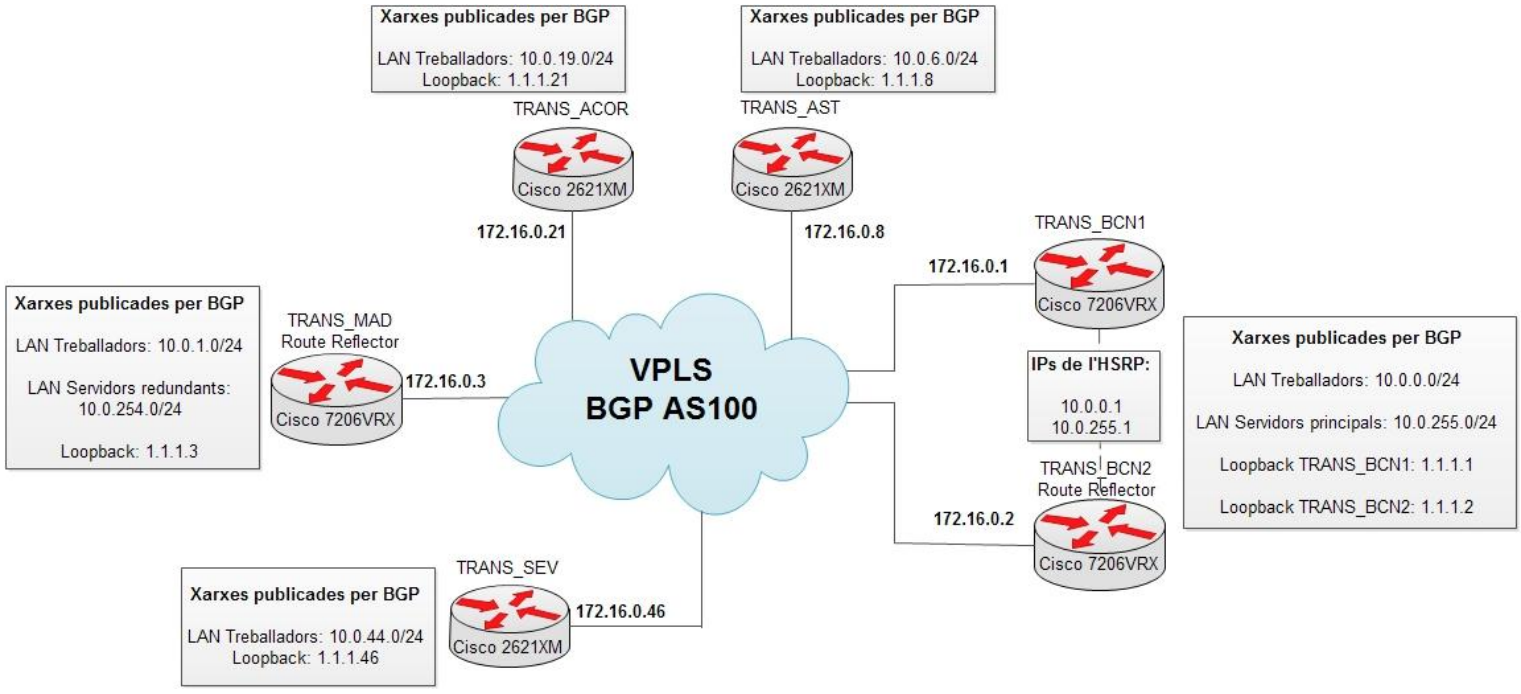
5.4.- Tipus de protocol de redundància

Aprofitant que s'han escollit els routers Cisco, s'utilitzarà en la seu de Barcelona el protocol HSRP (l'elecció d'aquest en comptes del VRRP ha estat que tot i que tenen el mateix concepte, Cisco és propietari de HSRP).

No és necessari configurar un protocol estandarditzat ja que els dos routers de la seu de Barcelona són Cisco. HSRP té diferents estats de negociació i això facilita la possible tasca de saber perquè està fallant la xarxa o perquè està fallant la configuració de HSRP davant una possible actuació d'aquest protocol.

5.5.- Topologia representativa

Ara que es té tota la tecnologia escollida, es farà una topologia representativa de la xarxa que tindrà *Transports Express S.A.* :



Imatge 17 – Topologia resum d'exemple

Es pot veure com s'ha posat un exemple de tres seus remotes a part de les seus de Barcelona i Madrid. La resta de seus s'afegiran de la mateixa manera però canviant les IPs corresponent a la seu, tenint en compte la Taula 10 – Resum dades dels routers.

6.- Configuració dels routers

S'ha de començar a fer la configuració dels routers Cisco de les 2 seus centrals i de les 50 remotes. Realment hi haurà quatre tipus de plantilles de configuracions:

- Routers de les seus remotes. La configuració entre routers remots únicament canviarà les IPs de LAN i de WAN, la resta serà igual a tots

- Router principal de Barcelona
- Router redundant de Barcelona
- Router de Madrid

Abans de començar amb la configuració, caldria assenyalar tres paràmetres que són únics per seu:

- El nom del router (*hostname*)
- La IP de WAN
- La IP de gestió (*loopback*)

Tots el *hostname* tindran el patró *TRANS_XXX*, on XXX serà una o varies lletres que faran referència a la província on es troba el router.

La xarxa d'IPs de WAN també es deixen sobre dimensionades per a futures delegacions noves, per tant tindrem la subxarxa 172.16.0.0 amb màscara 255.255.255.128 (25 en decimal), que va de la 172.16.0.0 fins la 172.16.0.127.

Pel que fa a la gestió dels routers, cada seu tindrà la *loopback* 1.1.1.X amb màscara 255.255.255.255 (32 en decimal) i el darrer octet coincidirà amb el de la IP de WAN.

A continuació, s'exposarà una taula resum amb totes les IPs de LAN i WAN, *hostname* i *loopback* dels routers de cada província, tenint en compte que en Barcelona hi hauran dos routers:

Província	**Hostname**	**Xarxa LAN**	**Direcció WAN**	**Loopback**
Barcelona	TRANS_BCN1 TRANS_BCN2	10.0.0.0/24 [rang treballadors] 10.0.255.0/24 [rang servidors]*	172.16.0.1/25 172.16.0.2/25	1.1.1.1 1.1.1.2
Madrid	TRANS_MAD	10.0.1.0/24 [rang treballadors] 10.0.254.0/24 [rang servidors redundants]*	172.16.0.3/25	1.1.1.3
Àlaba	TRANS_ALA	10.0.2.0/24	172.16.0.4/25	1.1.1.4
Alacant	TRANS_ALAC	10.0.3.0/24	172.16.0.5/25	1.1.1.5
Albacete	TRANS_ALB	10.0.4.0/24	172.16.0.6/25	1.1.1.6
Almeria	TRANS_ALM	10.0.5.0/24	172.16.0.7/25	1.1.1.7
Astúries	TRANS_AST	10.0.6.0/24	172.16.0.8/25	1.1.1.8
Àvila	TRANS_AVI	10.0.7.0/24	172.16.0.9/25	1.1.1.9
Badajoz	TRANS_BAD	10.0.8.0/24	172.16.0.10/25	1.1.1.10
Biscaia	TRANS_BIS	10.0.9.0/24	172.16.0.11/25	1.1.1.11
Burgos	TRANS_BUR	10.0.10.0/24	172.16.0.12/25	1.1.1.12
Càceres	TRANS_CC	10.0.11.0/24	172.16.0.13/25	1.1.1.13
Cadis	TRANS_CAD	10.0.12.0/24	172.16.0.14/25	1.1.1.14
Cantàbria	TRANS_CANT	10.0.13.0/24	172.16.0.15/25	1.1.1.15
Castelló	TRANS_CS	10.0.14.0/24	172.16.0.16/25	1.1.1.16

Ceuta	TRANS_CEU	10.0.15.0/24	172.16.0.17/25	1.1.1.17
Ciutat Real	TRANS_CR	10.0.16.0/24	172.16.0.18/25	1.1.1.18
Conca	TRANS_CO	10.0.17.0/24	172.16.0.19/25	1.1.1.19
Còrdova	TRANS_CORD	10.0.18.0/24	172.16.0.20/25	1.1.1.20
A Corunya	TRANS_ACOR	10.0.19.0/24	172.16.0.21/25	1.1.1.21
Girona	TRANS_GIR	10.0.20.0/24	172.16.0.22/25	1.1.1.22
Granada	TRANS_GR	10.0.21.0/24	172.16.0.23/25	1.1.1.23
Guadalajara	TRANS_GUA	10.0.22.0/24	172.16.0.24/25	1.1.1.24
Guipúscoa	TRANS_GUI	10.0.23.0/24	172.16.0.25/25	1.1.1.25
Huelva	TRANS_HU	10.0.24.0/24	172.16.0.26/25	1.1.1.26
Illes Balears	TRANS_IB	10.0.25.0/24	172.16.0.27/25	1.1.1.27
Jaén	TRANS_JA	10.0.26.0/24	172.16.0.28/25	1.1.1.28
La Rioja	TRANS_LR	10.0.27.0/24	172.16.0.29/25	1.1.1.29
Les Palmes de Gran Canaria	TRANS_GC	10.0.28.0/24	172.16.0.30/25	1.1.1.30
Lleida	TRANS_LL	10.0.29.0/24	172.16.0.31/25	1.1.1.31
Lleó	TRANS_LLE	10.0.30.0/24	172.16.0.32/25	1.1.1.32
Lugo	TRANS_LUG	10.0.31.0/24	172.16.0.33/25	1.1.1.33
Màlaga	TRANS_MAL	10.0.32.0/24	172.16.0.34/25	1.1.1.34
Melilla	TRANS_MEL	10.0.33.0/24	172.16.0.35/25	1.1.1.35
Múrcia	TRANS_MUR	10.0.34.0/24	172.16.0.36/25	1.1.1.36
Navarra	TRANS_NAV	10.0.35.0/24	172.16.0.37/25	1.1.1.37
Osca	TRANS_OSC	10.0.36.0/24	172.16.0.38/25	1.1.1.38
Ourense	TRANS_OUR	10.0.37.0/24	172.16.0.39/25	1.1.1.39
Palència	TRANS_PAL	10.0.38.0/24	172.16.0.40/25	1.1.1.40
Pontevedra	TRANS_PONT	10.0.39.0/24	172.16.0.41/25	1.1.1.41
Salamanca	TRANS_SAL	10.0.40.0/24	172.16.0.42/25	1.1.1.42
Santa Cruz de Tenerife	TRANS_SCT	10.0.41.0/24	172.16.0.43/25	1.1.1.43
Saragossa	TRANS_SAR	10.0.42.0/24	172.16.0.44/25	1.1.1.44
Segòvia	TRANS_SEG	10.0.43.0/24	172.16.0.45/25	1.1.1.45
Sevilla	TRANS_SEV	10.0.44.0/24	172.16.0.46/25	1.1.1.46
Sòria	TRANS_SOR	10.0.45.0/24	172.16.0.47/25	1.1.1.47
Tarragona	TRANS_TAR	10.0.46.0/24	172.16.0.48/25	1.1.1.48
Terol	TRANS_TER	10.0.47.0/24	172.16.0.49/25	1.1.1.49
Toledo	TRANS_TOL	10.0.48.0/24	172.16.0.50/25	1.1.1.50
València	TRANS_VAL	10.0.49.0/24	172.16.0.51/25	1.1.1.51
Valladolid	TRANS_VLL	10.0.50.0/24	172.16.0.52/25	1.1.1.52
Zamora	TRANS_ZM	10.0.51.0/24	172.16.0.53/25	1.1.1.53

Taula 11 - Resum dades dels routers

6.1.- Configuració seus centrals

Abans de començar amb les configuracions de cada router, s'ha definit una sèrie de decisions que són necessàries abans de començar a configurar i de les quals no s'ha parlat fins ara.

Com s'ha explicat al punt 5.3, el *Routing* tindrà dos RR que seran els que distribuiran la taula de rutes a totes les seus (TRANS_BCN2 i el TRANS_MAD).

Pel que fa referència a la IP de gestió dels equips, es restringirà l'accés als routers per Telnet, i només es permetrà l'accés des d'un equip amb IP 10.0.0.200.

6.1.1.- Router principal Barcelona – TRANS_BCN1

Configuració interfícies

S'utilitzarà tres interfícies Giga Ethernet i una *loopback* per a la gestió:

- LAN treballadors: 10.0.0.0/24
- Servidors: 10.0.255.0/24
- WAN que connecta a la VPLS
- Gestió: 1.1.1.1/32

La configuració de les interfícies és la següent:

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255

interface GigabitEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.1 255.255.255.128
 duplex full
 speed 1000

interface GigabitEthernet1/0
 description Connexio LAN treballadors
 ip address 10.0.0.2 255.255.255.0
 duplex full
 speed 1000

interface GigabitEthernet2/0
 description Connexio Servidors BCN
 ip address 10.0.255.2 255.255.255.0
 duplex full
 speed 1000
```

Configuració HSRP

Es realitzarà un HSRP entre els routers TRANS_BCN1 i TRANS_BCN2. Aquest HSRP previndrà les caigudes físiques i lògiques. Les caigudes lògiques succeeix qual la interfície continua *up* però en realitat no hi ha connexió de la WAN i LAN.

```
ip sla 1
 icmp-echo 1.1.1.2
 request-data-size 100
 frequency 5
ip sla schedule 1 life forever start-time now
```

```
ip sla 2
 icmp-echo 1.1.1.3
 request-data-size 100
 frequency 5
ip sla schedule 2 life forever start-time now

track 2 rtr 1 reachability
 delay down 8 up 8

track 3 rtr 2 reachability
 delay down 8 up 8

track 1 list boolean or
 object 2
 object 3

interface GigabitEthernet1/0
 standby 10 ip 10.0.0.1
 standby 10 priority 120
 standby 10 preempt
 standby 10 track 1 decrement 30

interface GigabitEthernet2/0
 standby 20 ip 10.0.255.1
 standby 20 priority 120
 standby 20 preempt
 standby 20 track 1 decrement 30
```

Com es pot veure, s'han realitzat dos grups d'HSRP, un per a la xarxa dels treballadors i un altre per a la xarxa dels servidors. Respecte a la LAN, com va connectat a un switch sense cap tipus d'encaminament, només pot tindre una caiguda a nivell físic, i aquest tipus de problemes queda coberta pel propi protocol HSRP.

Pel que fa a la WAN, té una configuració una mica més complexa. S'han creat dos *"ip sla*" que fan un ping cada 8 segons a les IP de gestió de TRANS_BCN2 i TRANS_MAD. Després tenim el *"track 1"* i *"track 2"* configurats que controlen els *"ip sla"* quan estan caiguts (*down*) i esperen els 5 segons indicats quan el *ping* contesta o deixa de contestar per realitzar el canvi d'estat del *track*. La part més important de tota aquesta configuració és el *"track 1 list"*. Aquest *"track list"* fa una comparació lògica entre els *tracks* 2 i 3, i únicament fa el decrement de 30 indicat a la interfície quan els *tracks* 2 i 3 estan d*own*. Amb aquesta comparació evitem que es faci el decrement únicament al no arribar a un sol *track*, ja que si només deixem un del *tracks* cap a TRANS_BCN2 o TRANS_MAD, únicament detectaríem les caigudes d'aquests *routers* i no les de TRANS_BCN1.

En un hipotètic cas que els dos routers TRANS_BCN2 i TRANS_MAD estiguessin incomunicats, i per tant tots dos *tracks* com a *down*, no cal plantejar-ho ja que estarien incomunicats els dos RR i tampoc podria funcionaria la xarxa.

Amb tota aquesta configuració de HSRP a la WAN prevenim les incomunicacions que no comportin una caiguda física de l'enllaç, i alhora actuarà com a principal TRANS_BCN2 al baixar la prioritat de TRANS_BCN1 quan no té connexió amb els dos *tracks* creats.

Configuració del BGP

Per al BGP, hem creat l'AS 100. A nivell de *routing*, aquesta seu es comportarà de manera similar a les seus remotes, de fet hi són dins dels mateix *peer-group*.

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 10.0.0.0 mask 255.255.255.0 route-map Local
 network 10.0.255.0 mask 255.255.255.0 route-map Local
 neighbor RR peer-group
 neighbor RR remote-as 100
 neighbor RR timers 10 30
 neighbor 172.16.0.2 peer-group RR
 neighbor 172.16.0.3 peer-group RR
 no auto-summary

route-map Local permit 10
 set local-preference 300
```

Tenim un *route-map* anomenat Local, que li dóna un *local-preference* de 300 a les xarxes LAN (tenint en compte que aquestes dues xarxes es publicaran també al TRANS_BCN2).

S'ha creat un *peer-group* per als RR, utilitzant la IP de WAN dels routers TRANS_BCN2 i TRANS_MAD.

Accés remot

L'accés remot per a configurar qualsevol router es podrà realitzar únicament des de la IP 10.0.0.200; per tant necessitarem un *Access Control List* (ACL) que s'haurà d'aplicar sobre la part de configuració del *virtual terminal*. Es configurarà un nom d'usuari i contrasenya per poder entrar al router, i una altra contrasenya per a entrar en mode privilegiat (a mode d'exemple es posarà uoc tant a les contrasenyes com a l'usuari).

```
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any

line vty 0 4
 access-class 100 in
 login local

username uoc secret uoc
```

```
enable secret uoc
```

Les ACL quan tenen un o més *permit* tenen un *deny* implícit que denega la resta de connexions, de tal manera que permetrà l'accés a la IP 10.0.200 i a la resta ho denegarà. A la configuració del router, totes les contrasenyes sortiran encriptades.

Limitació de l'ample de banda Barcelona-Madrid

Els accessos de Barcelona i Madrid és d'1Gbps amb un cabal de 300 Mbps. S'ha de limitar l'ample de banda entre les seus a 100Mbps (velocitat suficient per a realitzar les còpies), i així assegurem que les seus remotes tinguin una velocitat raonable en cas de generar molt tràfic a tota la xarxa.

Es realitzarà aquesta limitació utilitzant el mètode *QoS Policy*. Primer una *ACL* detecta el tràfic amb origen les xarxes LAN de Barcelona i destí la LAN de Madrid. Es fa referència aquesta *ACL* en un *QoS class-map*. Després, en un *policy-map* especifiquem les QoS que volem aplicar, i llavors es limita la velocitat a 100000000 bps i la resta es descarta. Per últim, s'ha d'aplicar el *policy-map* en la interfície WAN en sentit sortida i ja tenim limitat l'accés des de la xarxa de Barcelona a la de Madrid:

```
access-list 110 remark ACL xarxes limitacio BW
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.254.0 0.0.0.255
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255

class-map match-all Limitacio_100Mbps
 match access-group 110

policy-map Limitacio_100Mbps
  class Limitacio_100Mbps
  police rate 100000000 bps
    exceed-action drop

interface GigabitEthernet0/0
 service-policy output Limitacio_100Mbps
```

6.1.2.- Router backup Barcelona – TRANS_BCN2

El router TRANS_BCN2 serà el router redundant de TRANS_BCN1. La configuració serà molt similar, però el BGP tindrà més configuració al tractar-se d'un dels dos RR.

Configuració interfícies

S'utilitzarà tres interfícies Giga Ethernet i una *loopback* per a la gestió:

- LAN treballadors: 10.0.0.0/24
- Servidors: 10.0.255.0/24
- WAN que connecta a la VPLS
- Gestió: 1.1.1.2/32

Configuració de les interfícies amb les IPs que requereix aquest router:

```
interface Loopback0
 ip address 1.1.1.2 255.255.255.255

interface GigabitEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.2 255.255.255.128
 duplex full
 speed 1000
 media-type gbic
 negotiation auto

interface GigabitEthernet1/0
 description Connexio LAN treballadors
 ip address 10.0.0.3 255.255.255.0

interface GigabitEthernet2/0
 description Connexio Servidors BCN
 ip address 10.0.255.3 255.255.255.0
```

Configuració HSRP

Per a l'HSRP d'aquest router s'ha de tenir present la configuració que té TRANS_BCN1:

```
interface GigabitEthernet1/0
 standby 10 ip 10.0.0.1
 standby 10 preempt

interface GigabitEthernet2/0
 standby 20 ip 10.0.255.1
 standby 20 preempt
```

Com es pot veure no se li dóna cap valor de prioritat, per tant la prioritat que tindran tots dos grups d'HSRP serà de 100. No fa falta cobrir les caigudes de la WAN al tractar-se d'una línia redundant.

Configuració del BGP

TRANS_BCN2 s'ha escollit com a RR de totes les seus. Haurà de tenir com a veí tota la resta de routers:

```
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 neighbor SEUS peer-group
 neighbor SEUS remote-as 100
```

```
neighbor SEUS timers 10 30
neighbor 172.16.0.1 peer-group SEUS
neighbor 172.16.0.3 remote-as 100
neighbor 172.16.0.3 timers 10 30
neighbor [IP WAN seu remota] peer-group SEUS

address-family ipv4
 neighbor SEUS route-reflector-client
 neighbor 172.16.0.1 activate
 neighbor 172.16.0.1 weight 40000
 neighbor 172.16.0.3 activate
 neighbor [IP WAN seu remota] activate
 no auto-summary
 no synchronization
 bgp redistribute-internal
 network 1.1.1.2 mask 255.255.255.255
 network 10.0.0.0 mask 255.255.255.0 route-map Local
 network 10.0.255.0 mask 255.255.255.0 route-map Local
 exit-address-family

route-map Local permit 10
 set local-preference 200
```

Només s'ha posat un exemple de BGP amb les IPs de la seu principal de Barcelona i la de Madrid. Per a configurar tot l'escenari, només s'hauria de copiar les línies en negreta i posar les IPs de WAN de la seu remota, i llavors ja tindríem totes les seus com a veïnes.

S'ha creat un *peer-group* per a tractar totes les seus remotes de la mateixa forma, i s'indica a aquest *peer-group* que són RR client del router. També tenim un *clúster-id* per als dos RR de la xarxa.

Els temps del BGP davant una caiguda d'un veí s'han modificat. Ara s'envia cada 10 segons (per defecte 60 segons) un missatge de *keepalive* per veure si un veí continua actiu. Després de no arribar el *keepalive*, concretament 30 segons més tard, es dóna el destí com a perdut (per defecte 180 segons).

Es pot diferenciar, com per al veí 172.16.0.1 (TRANS_BCN1), té afegit un pes (*weight*) de 40000, major al 32768 que té BGP per defecte. Això, fa que els routers tinguin preferència per aquesta ruta que, conjuntament amb el *local-preference*, fa que escullin com a primera opció de camí aquest enllaç per arribar a les xarxes 10.0.0.0/24 i 10.0.255.0/24.

Aquest router també publica les mateixes xarxes que TRANS_BCN1, però el *route-map* que té fa que tingui un *local-preference* inferior al del router principal, llavors serà la segona opció dins del *routing* per aquestes dues subxarxes.

Accés remot

L'accés remot es configurarà de la mateixa forma que al router TRANS_BCN1:

```
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
line vty 0 4
 access-class 100 in
 login local

username uoc secret uoc
enable secret uoc
```

Limitació de l'ample de banda Barcelona-Madrid

La limitació haurà de ser la mateixa que al router principal i així en cas de fallida de TRANS_BCN1, TRANS_BCN2 començaria a funcionar limitant el tràfic de la mateixa forma:

```
access-list 110 remark ACL xarxes limitacio BW
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.254.0 0.0.0.255
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255

class-map match-all Limitacio_100Mbps
 match access-group 110

policy-map Limitacio_100Mbps
  class Limitacio_100Mbps
  police rate 100000000 bps
    exceed-action drop

interface GigabitEthernet0/0
 service-policy output Limitacio_100Mbps
```

6.1.3.- Router Madrid – TRANS_MAD

El router que hi ha a la seu de Madrid tindrà la seva pròpia xarxa pels treballadors de la seu, i una segona xarxa destinada a la còpia dels servidors de *Transports Express S.A.*. També farà de RR juntament amb el TRANS_BCN2.

Configuració interfícies

Com als routers anteriors, hi haurà 3 interfícies, tot tenint en compte les IPs que s'han assignat a aquesta seu:

```
interface Loopback0
 ip address 1.1.1.3 255.255.255.255

interface GigabitEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.3 255.255.255.128
 duplex full
 speed 1000

interface GigabitEthernet1/0
 description Connexio LAN treballadors
 ip address 10.0.1.1 255.255.255.0

interface GigabitEthernet2/0
 description Connexio LAN Copia servidors
 ip address 10.0.254.1 255.255.255.0
```

La configuració és més simple al no tenir router redundant i per tant, no tenir configuració d'HSRP.

Configuració del BGP i ruta estàtica

Com ja s'ha descrit, aquest router serà l'altre RR. La configuració serà molt similar a la del TRANS_BCN2:

```
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 neighbor SEUS peer-group
 neighbor SEUS remote-as 100
 neighbor SEUS timers 10 30
 neighbor 172.16.0.1 peer-group SEUS
 neighbor 172.16.0.2 remote-as 100
 neighbor 172.16.0.2 timers 10 30
 neighbor [IP WAN seu remota] peer-group SEUS

 address-family ipv4
  redistribute static
  neighbor SEUS route-reflector-client
  neighbor 172.16.0.1 activate
  neighbor 172.16.0.1 weight 40000
  neighbor 172.16.0.2 activate
  neighbor 172.16.0.2 weight 40000
  neighbor [IP WAN seu remota] activate
```

```
 no auto-summary
 no synchronization
 bgp redistribute-internal
 network 1.1.1.3 mask 255.255.255.255
 network 10.0.1.0 mask 255.255.255.0
 network 10.0.254.0 mask 255.255.255.0
  exit-address-family

ip route 10.0.255.0 255.255.255.0 10.0.254.2 250
```

Es configurarà el mateix número de *clúster-id* als dos routers RR. Com ja s'ha descrit, en aquesta seu es farà la còpia de seguretat del servidors principals (xarxa 10.0.255.0/24) realitzant-se a través de la xarxa 10.0.254.0/24. En cas d'incomunicació total de la seu de Barcelona, el router de Madrid publicarà una ruta estàtica amb major distància administrativa que la del BGP, el que indica que serà la tercera opció per arribar a aquesta xarxa. El tràfic amb destí 10.0.255.0/24 s'encamina a la IP 10.0.254.2, que correspon a un equip de client que realitzarà dues tasques: fer les còpies periòdicament i encaminar el tràfic cap al servidor corresponent.

Accés remot

L'accés remot es realitzarà amb les mateixes limitacions dels routers anteriors:

```
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
line vty 0 4
 access-class 100 in
 login local

username uoc secret uoc
enable secret uoc
```

Limitació de l'ample de banda Madrid-Barcelona

La limitació de la connexió entre Madrid i Barcelona es realitzarà utilitzant el mateix mètode que al TRANS_BCN1. L'únic que canviarà serà l'*ACL* del router, que tindrà origen la xarxa de Madrid i destí les de Barcelona:

```
access-list 110 remark ACL xarxes limitacio BW
access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.255.0 0.0.0.255
access-list 110 permit ip 10.0.254.0 0.0.0.255 10.0.255.0 0.0.0.255
access-list 110 permit ip 10.0.254.0 0.0.0.255 10.0.0.0 0.0.0.255

class-map match-all Limitacio_100Mbps
 match access-group 110

policy-map Limitacio_100Mbps
```

```
 class Limitacio_100Mbps
 police rate 100000000 bps
   exceed-action drop

interface GigabitEthernet0/0
 service-policy output Limitacio_100Mbps
```

6.2.- Configuració seus remotes

En els routers de les seus remotes tindrem una configuració molt senzilla i estàndard. Només canviarà les IPs que li corresponguin a cada seu, i la configuració del BGP serà la mateixa en tots:

Configuració interfícies

La configuració de les interfícies és estàndard per a totes les seus, únicament variarà les IPs de cada seu:

```
interface Loopback0
 ip address 1.1.1.x 255.255.255.255

interface FastEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.x 255.255.255.128
 duplex auto
 speed auto

interface FastEthernet0/1
 description Connexio LAN
 ip address 10.0.x.1 255.255.255.0
 duplex auto
 speed auto
```

On les 'x' variaran depenen la seu on es configuri.

Configuració del BGP

La configuració del BGP només ha de tenir els dos RR com a veïns i publicar la xarxa LAN de la seu que li correspongui:

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 1.1.1.x mask 255.255.255.255
 network 10.0.x.0 mask 255.255.255.0
 neighbor RR peer-group
 neighbor RR remote-as 100
 neighbor RR timers 10 30
 neighbor 172.16.0.2 peer-group RR
```

```
neighbor 172.16.0.3 peer-group RR
no auto-summary
```

Només canviarà les línies en negreta, on s'ha d'anar canviant la 'x' depenen la seu remota.

Accés remot

L'accés remot es realitzarà amb les mateixes limitacions dels routers anteriors:

```
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
line vty 0 4
 access-class 100 in
 login local

username uoc secret uoc
enable secret uoc
```

7.- Emulació de la xarxa amb GNS3

GNS3, *Graphical Network Simulator 3*, és un emulador de xarxes que utilitza equips Cisco i Juniper. A diferencia de la simulació de xarxes com seria el cas de Cisco Packet Tracer, l'emulació utilitza IOS reals dels propis routers, per tant estem creant un o varis routers virtuals que interactuen entre ells en un mateix ordinador. A part d'interactuar routers creats en un mateix ordinador, també es pot connectar amb la xarxa real o fins i tot amb una màquina virtual creada amb Virtual Box.

L'avantatge principal que té GNS 3 envers altres similars, com Cisco Packet Tracer, és que GNS3 utilitza Dynamips per a la emulació dels routers Cisco, a més de poder emular Cisco PIX/ASA (que són els tallafocs de Cisco). Així doncs, podem veure com GNS3 és la part gràfica de Dynamips que realment és qui emula les IOS dels routers Cisco.

GNS3 és molt popular entre la gent que s'està preparant certificacions oficials de Cisco (CCNA, CCNP, CCIP, CCSP, CCVP o CCIE) o Juniper (JNCIA, JNCIS or JNCIE).
Com s'ha escollit treballar amb routers Cisco, ens centrarem en l'emulació que té GNS3 d'aquests routers. GNS3 només és compatible amb unes determinades sèries de routers Cisco que són per les quals es va crear Dynamips:

- Cisco 1700
- Cisco 2600
- Cisco 3600
- Cisco 3700
- Cisco 7200

Totes les sèries tenen determinats models de routers que es poden escollir, i cada model és compatible amb unes targetes WIC. Es pot concretar tot el *hardware* compatible amb GNS3 a la seva pròpia web[2].

7.1.- Presentació i configuració bàsica de GNS3

GNS3 està disponible per als sistemes operatius Windows, Linux i MAC. En el nostre cas, la simulació es realitzarà sobre Windows 7 64 Bits. La instal·lació del programari s'ha realitzat seguint el manual que es pot trobar a la seva web[3]. En la descàrrega per a Windows 7 64 Bits, podem trobar dos programes més que ens seran útils durant la part de l'emulació per a realitzar comprovacions:

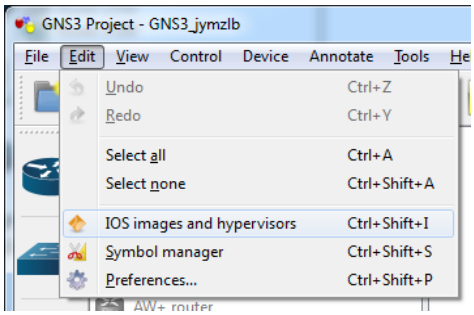
- **Putty:** És el client que s'utilitzarà per connectar-nos via consola a cada router.

- **VPCS:** Virtual PC Simulator, que ens permet simular varis PCs virtuals en una topologia creada amb GNS3.

Una vegada instal·lat GNS3, s'ha de carregar les IOS dels routers amb les que volem treballar. Les IOS es poden descarregar de diferents pàgines web cercant per Internet. En aquesta simulació s'han utilitzat les següents versions per a simular els Cisco 2621XM i Cisco 7206VRX:

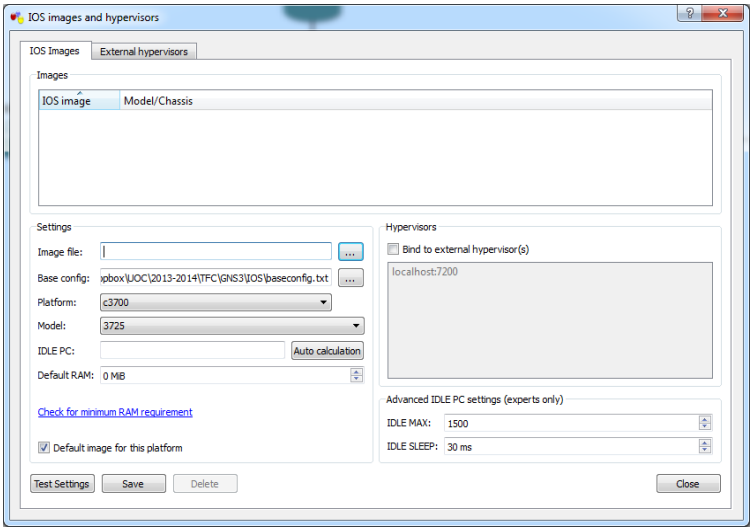
- c2600-advsecurityk9-mz.124-15.T9.bin[4]
- c7200-advipservicesk9-mz.124-4.T1.bin[5]

Per a carregar les IOS hem d'anar al menú **Edit – IOS images and hypervisors**:

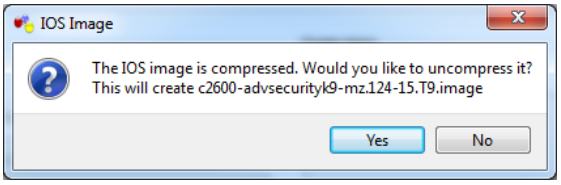


[2] Hardware emulat per GNS3: http://www.gns3.net/hardware-emulated/
[3] Manual d'instal·lació GNS3: http://www.gns3.net/documentation/gns3/quick-start-guide-for-windows-users/
[4] IOS c2600-advsecurityk9-mz.124-15.T9.bin: http://goo.gl/FUyCQZ
[5] IOS c7200-advipservicesk9-mz.124-4.T1.bin: http://goo.gl/YsLNr6

Veurem el següent menú:

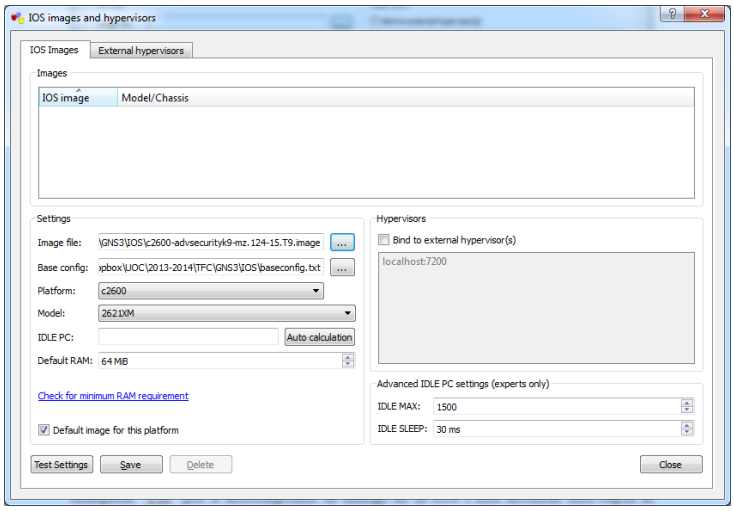


En el menú de **Settings – Image file** hem de posar la ruta on es troba la IOS i ens sortirà el següent missatge:



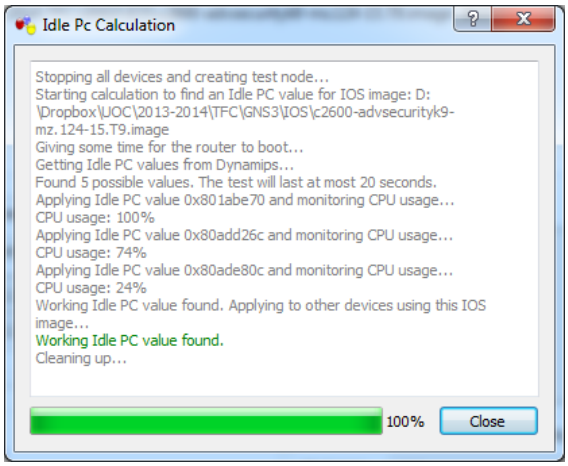
Indiquem **'Yes'** per a descomprimir la imatge de la IOS i així arrencar més ràpid la simulació dels routers.

Després hem d'escollir dins de la sèrie Cisco 2600 quin model volem, per tant agafem Cisco 2621XM:

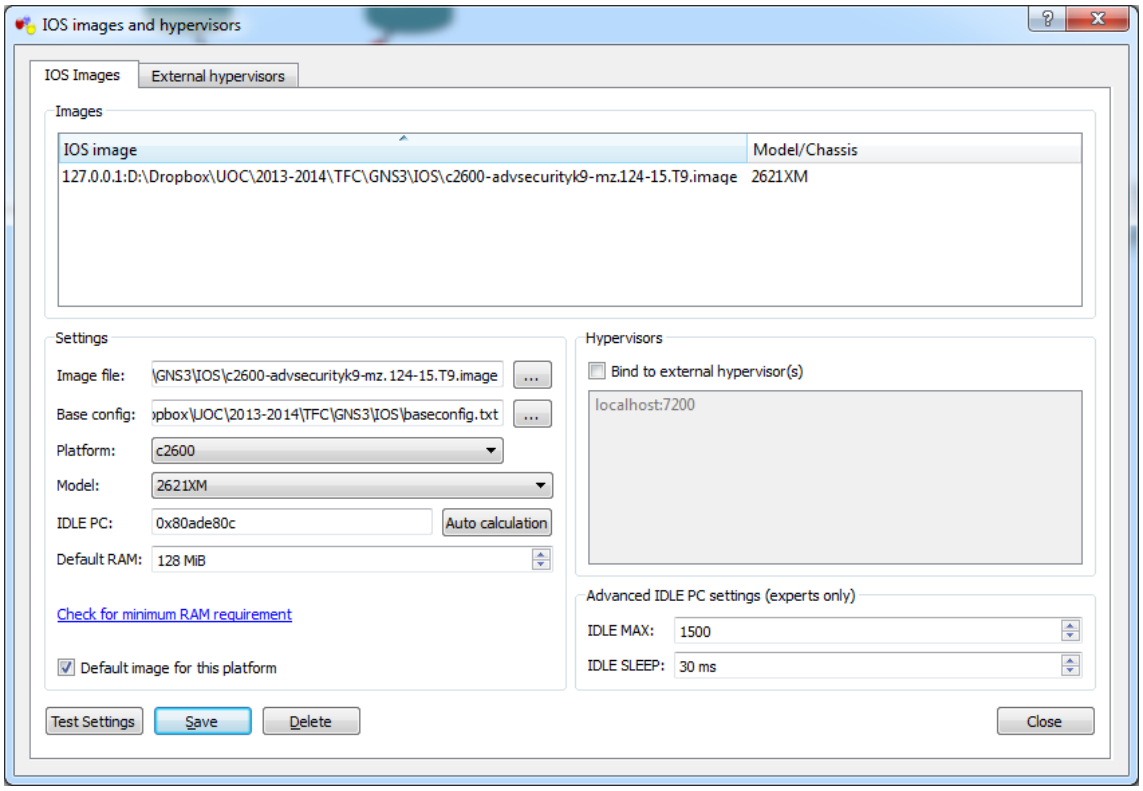


Un paràmetre molt important a tenir en compte és el IDLE PC. L'IDLE PC és una configuració que varia depenent el hardware i software on es simuli, i ens ajuda a optimitzar els recursos que utilitzarà cada router quan s'emuli, ja que sinó tant l'emulació com el propi ordinador no funcionaria correctament. Es prem sobre el botó **"Auto calculation"** i confirmem amb **"Yes"** per a començar a calcular-ho (ens indica que el ordinador es pot quedar bloquejat durant el temps de la prova).

Podem seguir el procés indicat en percentatge en la finestra:



Una vegada acaba de calcular IDLE PC cliquem en **"Close"** i veiem com queda la configuració d'aquest router:

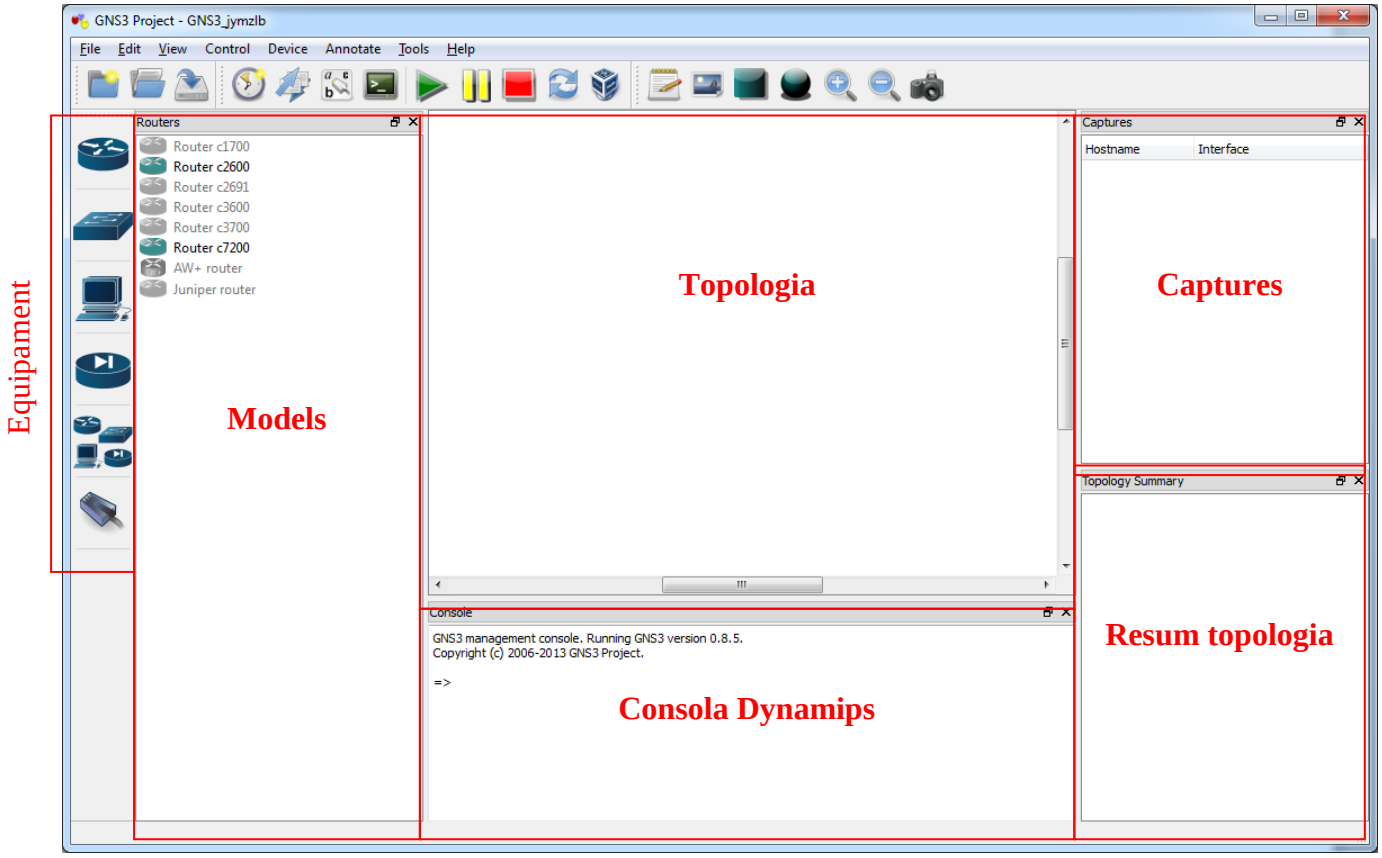


Imatge 18 - Afegir IOS al GNS3

La RAM l'augmentem fins els 128 MB. Cliquem sobre **"Save"** i ja queda guardada la configuració d'aquest router.

Per a carregar la IOS del Cisco 7206VRX s'ha fet el mateix procés ja explicat, però en aquest cas deixant la memòria RAM per defecte (256 MB).

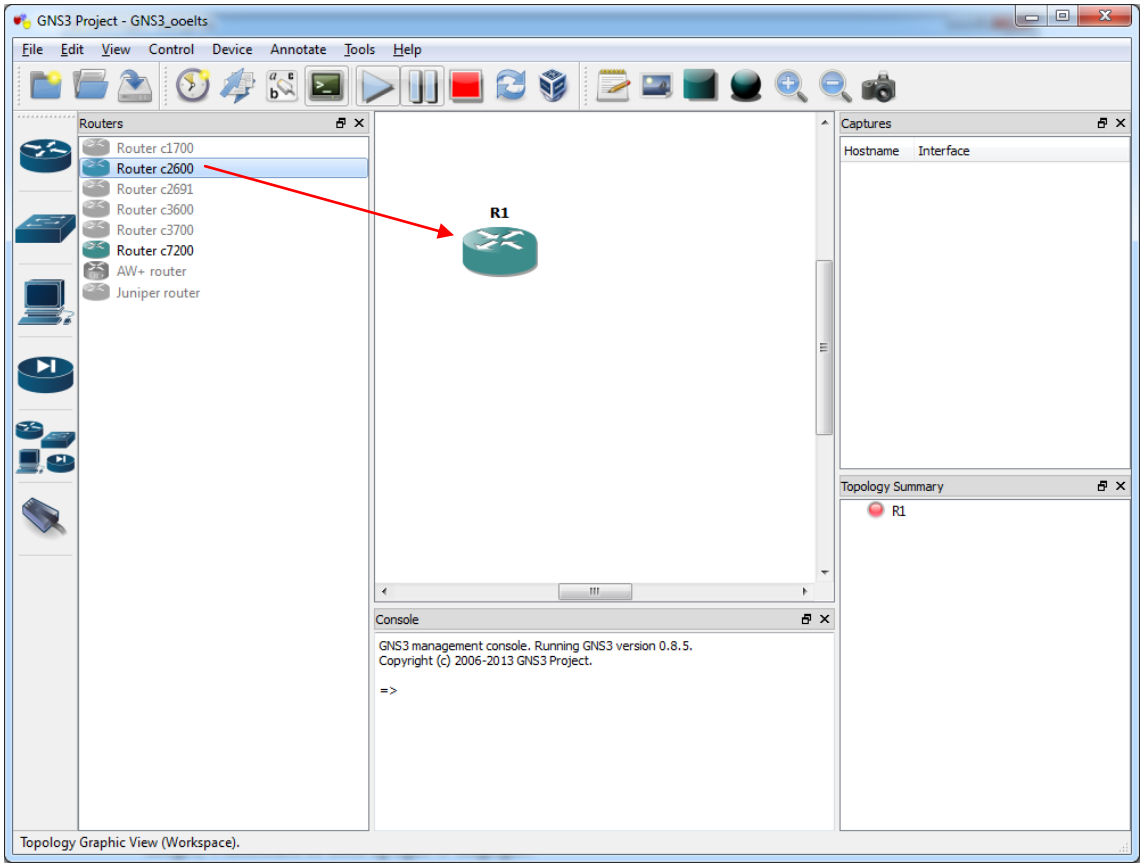
Ara ja podem crear un nou projecte. L'entorn de treball principal d'un projecte és el següent:



Imatge 19 - Entorn de treball GNS3

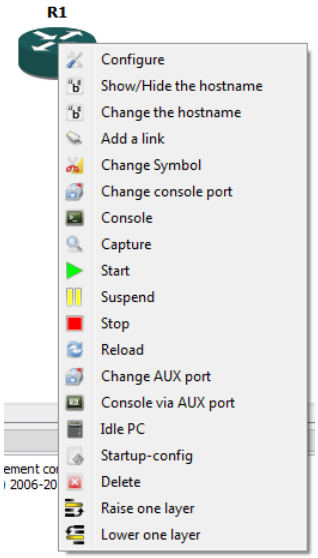
El primer requadre a mà esquerre veiem les famílies del diferent equipament disponible (routers, *switch*, PC...). Al requadre de "models" veurem els models de *hardware* de la família que s'ha escollit. En la "topologia" és on s'afegeix tot l'equipament i es fan les connexions entre ells. La consola Dynamips va sortint tota la informació sobre Dynamips que va succeint. A "captures" sortiran les diferents captures del tràfic que es facin sobre un router. I per últim, el "resum de topologia" mostrarà tot el *hardware* que s'ha afegit, i indicarà si està apagat o engegat.

Per a crear un topologia s'ha d'arrossegar des de l'apartat de "models" fins a topologia l'equipament necessari:



Imatge 20 - Afegir router al GNS3

Una vegada tenim el router en la topologia, si cliquem sobre el botó dret tenim diferents opcions a fer amb ell:



Les opcions principals que utilitzarem seran:

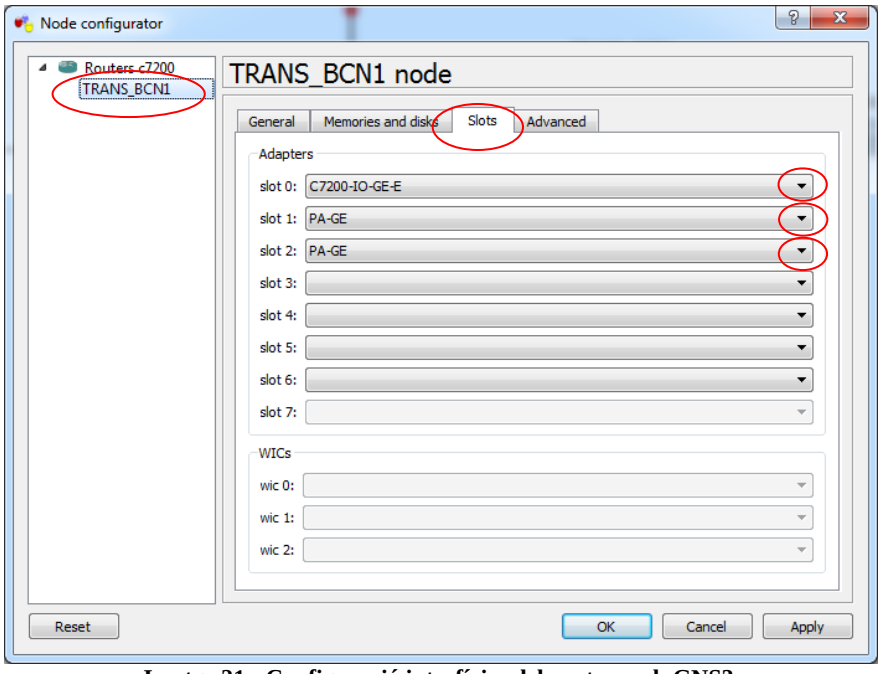
- **Configure:** Configuració del router on podrem afegir als slots disponibles diferents interfícies per a utilizar-les
- **Change the hostname:** Canvia el *hostname* del router
- **Add a link:** Crear una connexió des d'aquest dispositiu fins a un altre
- **Console:** Entrar a la consola del router per a modificar la configuració
- **Start:** Comença l'emulació del router
- **Stop:** Para l'emulació del router

7.2.- Emulació d'una part de la xarxa

Una vegada ja tenim configurades les IOS de cada router que utilitzarem, només hem d'anar afegint els routers, els adaptador de ports necessaris i anar connectant les interfícies.

Segons la configuració de les interfícies que s'ha exposat en els apartats 6.1 i 6.2, pels Cisco 2621XM no fa falta afegir cap *slot*, ja que per defecte ja ve amb dues interfícies Fast Ethernet. En canvi, per a emular Cisco 7206VRX (al GNS3 serà 7200) hem d'afegir tres interfícies Giga Ethernet:

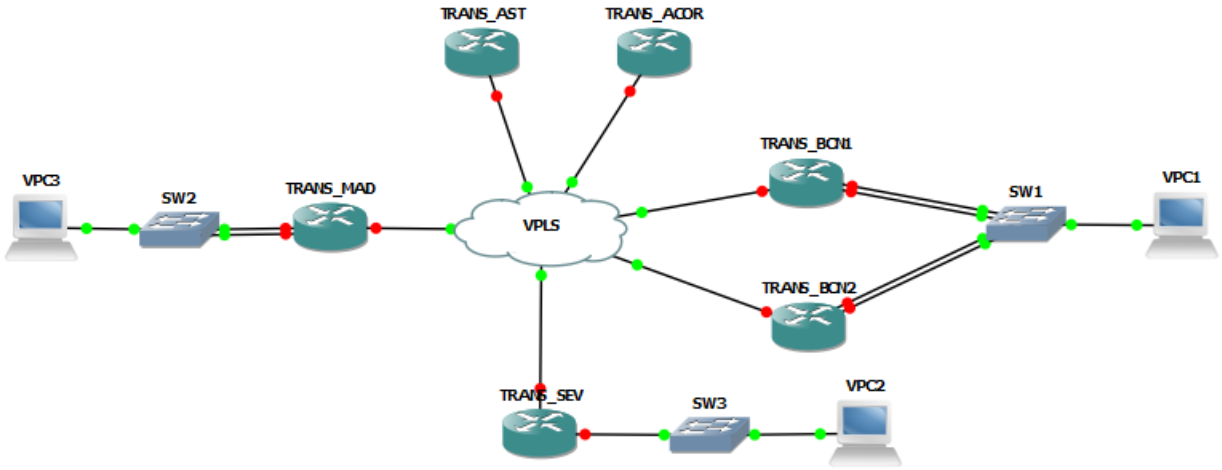
Per a modificar-ho, cliquem sobre el router botó dret, **Configure**. Després cliquem sobre el *hostname* i ja podem anar a la pestanya de **Slots**:



Imatge 21 - Configuració interfícies del router amb GNS3

Per agafar els tres ports Giga Ethernet que necessitem, hem d'escollir del desplegable la targeta PA-GE dels *slots* 1 i 2, i el C7200-IO-GE-E de *l'slot* 0.

A la imatge 22 es pot veure com queda la topologia que s'utilitzarà d'exemple en aquesta emulació amb GNS3:



Imatge 22 - Topologia simulació GNS3

Una vegada tenim la topologia segons es veu en la imatge 22, s'ha de configurar els VPC. El mètode de configuració es pot veure en la imatge 23:

```
VPCS[1]> ip 10.0.0.200 10.0.0.1 24
Checking for duplicate address...
PC1 : 10.0.0.200 255.255.255.0 gateway 10.0.0.1

VPCS[1]> 2
VPCS[2]> ip 10.0.1.200 10.0.1.1 24
Checking for duplicate address...
PC2 : 10.0.1.200 255.255.255.0 gateway 10.0.1.1

VPCS[2]> 3
VPCS[3]> ip 10.0.44.200 10.0.44.1 24
Checking for duplicate address...
PC3 : 10.0.44.200 255.255.255.0 gateway 10.0.44.1

VPCS[3]> 1
VPCS[1]>
```

Imatge 23 - Configuració VPC

S'ha de posar un 1, 2 o 3 per indicar quin VPC volem configurar. Després la primera IP indica la IP del host, la segona la porta d'enllaç i l'últim la màscara en decimal.

Als propers punts es realitzaràn comprovacions per confirmar que les opcions escollides als punts anteriors permeten un correcte funcionament de la emulació. Les comprovacions es podràn veure tant en captures de pantalla com en vídeos explicatius. **Els vídeos es podràn veure a través d'enllaços a http://www.youtube.com. En tots els vídeos es recomana escollir l'opció de visualització de 720p HD o 1080p HD, tot prement el botó ⚙ i escollint aquesta resolució (la rapidessa del canvi de resolució depén de la qualitat de connexió a Internet que es tingui). Sino s'escolleix aquesta resolució, els vídeos es veuran borrossos.**

Al proper enllaç es pot veure un vídeo que s'ha realitzat durant la creació de la topologia:

http://youtu.be/KmdMp7RZFx0

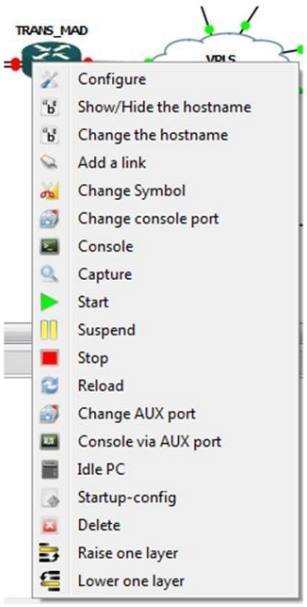
Una vegada ja tenim la topologia creada, s'ha d'afegir als routers la configuració segons s'ha estipulat als punts 6.1.1, 6.1.2 i 6.1.3, pel que fa als routers centrals, i al punt 6.2 pels remots. Per l'emulació s'han escollit 7 routers que corresponen a 6 seus: Barcelona (té dos routers), Madrid, Astúries, Sevilla i A Corunya. S'ha tingut en compte les IPs de cada seu que s'han especificat a la Taula 11 - Resum dades dels routers.

La configuració sencera dels routers centrals es pot trobar a l'Annex. Pel que fa a la configuració dels routers de les seus remotes, s'ha creat un arxiu Excel que serveix com a auto plantilla, anomenada *"Plantilla configuracio seus remotes.xlsx"* i la podem descarregar al següent enllaç: http://goo.gl/28nhZx. En aquest document s'ha d'introduir uns paràmetres de la seu que volem configurar i ens genera la configuració sencera d'aquesta seu i només s'ha de copiar i enganxar la configuració al router.

Prèviament a la emulació, s'han afegit les configuracions dels routers.

7.2.1.- Comprovació de la topologia amb un funcionament normal

Posem tots el routers en funcionament (botó dret a sobre del router i escollim **"Start"**). Per a entrar en cada router, fem botó dret sobre el router i escollim **"Console"**, i s'obre una finestra com si ens connectéssim per cable de consola al propi router:



Una vegada obrim les consoles podem fer comprovacions directament des del propi router.

El funcionament normal seria quan la xarxa està treballant sense cap tipus de problema. Podem veure a la imatge 24 com en estat normal de la xarxa, el router principal de la seu de Barcelona és el TRANS_BCN1, amb prioritat 120:

```
TRANS_BCN1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       10   120 P Active  local           10.0.0.3        10.0.0.1
Gi2/0       20   120 P Active  local           10.0.255.3      10.0.255.1
```

Imatge 24 - HSRP TRANS_BCN1

El *track* que s'ha creat monitoritza les *loopbacks* dels dos RR, i així es pot detectar que en cas que no arribés per ping a les dues IPs, voldria dir que l'enllaç de TRANS_BCN1 està caigut, i per tant el *track* 1 estaria com a *down* ja que és qui compara els *tracks* 2 i 3 que també estarien *down*. En la imatge 25 es veu que en estat normal, els *tracks* estan com a *up*:

```
TRANS_BCN1#sh track
Track 1
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:00:09
    object 2 Up
    object 3 Up
  Tracked by:
    HSRP GigabitEthernet1/0 10
    HSRP GigabitEthernet2/0 20
Track 2
  Response Time Reporter 1 reachability
  Reachability is Up
    2 changes, last change 00:11:17
  Delay up 8 secs, down 8 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 80
  Tracked by:
    Track-list 1
Track 3
  Response Time Reporter 2 reachability
  Reachability is Up
    2 changes, last change 00:10:27
  Delay up 8 secs, down 8 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 144
  Tracked by:
    Track-list 1
```

Imatge 25 - Estat track TRANS_BCN1

A la imatge 26 es veu com el TRANS_BCN2 està en mode redundant a la espera d'algun problema amb el router principal:

```
TRANS_BCN2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       10   100 P Standby 10.0.0.2        local           10.0.0.1
Gi2/0       20   100 P Standby 10.0.255.2      local           10.0.255.1
```

Imatge 26 - HSRP TRANS_BCN2

En la imatge 27, es veu com el router TRANS_BCN1 té dos veïns BGP, i per les WANs podem confirmar que corresponen a les IPs dels dos RR:

```
TRANS_BCN1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 14, main routing table version 14
13 network entries using 1521 bytes of memory
21 path entries using 1092 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
4 BGP rrinfo entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3329 total bytes of memory
BGP activity 13/0 prefixes, 24/3 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.2      4   100     127     118       14    0    0 00:18:50        9
172.16.0.3      4   100     112     108       14    0    0 00:17:01        8
```

Imatge 27 - Veïns BGP de TRANS_BCN1

Tots dos RR tindran els mateixos veïns BGP, i aquestes seran totes les IPs WAN dels seus veïns que rebran per a redistribuir-les. A la imatge 28 veiem els veïns del RR TRANS_BCN1 i a la imatge 29 els de TRANS_MAD:

```
TRANS_BCN2#show ip bgp summary
BGP router identifier 1.1.1.2, local AS number 100
BGP table version is 21, main routing table version 21
14 network entries using 1638 bytes of memory
20 path entries using 1040 bytes of memory
6/4 BGP path/bestpath attribute entries using 744 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3422 total bytes of memory
BGP activity 14/0 prefixes, 20/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.1      4   100     165     175       21    0    0 00:26:44        4
172.16.0.3      4   100     161     162       21    0    0 00:24:54        3
172.16.0.8      4   100     156     168       21    0    0 00:25:34        3
172.16.0.21     4   100     155     167       21    0    0 00:25:28        3
172.16.0.46     4   100     155     164       21    0    0 00:24:56        3
```

Imatge 28 - Veïns BGP RR TRAS_BCN2

```
TRANS_MAD#show ip bgp summary
BGP router identifier 1.1.1.3, local AS number 100
BGP table version is 16, main routing table version 16
14 network entries using 1638 bytes of memory
18 path entries using 936 bytes of memory
6/5 BGP path/bestpath attribute entries using 744 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3318 total bytes of memory
BGP activity 14/0 prefixes, 19/1 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.1      4   100     162     168       16    0    0 00:26:00        4
172.16.0.2      4   100     169     168       16    0    0 00:26:00        1
172.16.0.8      4   100     162     172       16    0    0 00:26:29        3
172.16.0.21     4   100     159     170       16    0    0 00:26:04        3
172.16.0.46     4   100     161     170       16    0    0 00:26:04        3
```

Imatge 29 - Veïns BGP RR TRANS_MAD

A continuació, es veuen totes les rutes amb les seves prioritats que té el RR TRANS_BCN2:

```
TRANS_BCN2#show ip bgp
BGP table version is 20, local router ID is 1.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i1.1.1.1/32       172.16.0.1               0    100  40000 ?
*> 1.1.1.2/32       0.0.0.0                  0         32768 ?
*>i1.1.1.3/32       172.16.0.3               0    100      0 ?
*>i1.1.1.8/32       172.16.0.8               0    100      0 ?
*>i1.1.1.21/32      172.16.0.21              0    100      0 ?
r>i10.0.0.0/24      172.16.0.1               0    300  40000 i
r                   0.0.0.0                  0    200  32768 i
*>i10.0.1.0/24      172.16.0.3               0    100      0 i
*>i10.0.6.0/24      172.16.0.8               0    100      0 i
*>i10.0.19.0/24     172.16.0.21              0    100      0 i
*>i10.0.44.0/24     172.16.0.46              0    100      0 i
*>i10.0.254.0/24    172.16.0.3               0    100      0 i
r>i10.0.255.0/24    172.16.0.1               0    300  40000 i
r                   0.0.0.0                  0    200  32768 i
r i172.16.0.0/25    172.16.0.21              0    100      0 ?
r i                 172.16.0.8               0    100      0 ?
r>i                 172.16.0.1               0    100  40000 ?
   Network          Next Hop            Metric LocPrf Weight Path
r                   0.0.0.0                  0         32768 ?
```

Imatge 30 - Rutes BGP conegudes per RR TRANS_BCN2

En la imatge 30 veiem les subxarxes que coneix i el proper salt on s'ha d'enviar el tràfic per anar a aquesta subxarxa. La subxarxa 10.0.0.0/24 la coneix a través de la IP WAN del TRANS_BCN1 amb *local-preference* 300 (major que la resta) i pes 40000, també major que la resta. Això farà que distribueixi com a enllaç preferent el del router TRANS_BCN1 per arribar a la 10.0.0.0/24. Passa el mateix amb la subxarxa de servidors 10.0.255.0/24. Com a segona opció, amb *local-preference* de 200 es troba el propi TRANS_BCN2.

La taula de rutes d'una seu remota quan la xarxa està treballant correctament es pot veure a la imatge següent:

```
TRANS_SEV#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 6 subnets
B       1.1.1.1 [200/0] via 172.16.0.1, 00:26:57
B       1.1.1.3 [200/0] via 172.16.0.3, 00:26:57
B       1.1.1.2 [200/0] via 172.16.0.2, 00:26:57
B       1.1.1.8 [200/0] via 172.16.0.8, 00:26:57
B       1.1.1.21 [200/0] via 172.16.0.21, 00:14:09
C       1.1.1.46 is directly connected, Loopback0
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 7 subnets
B       10.0.0.0 [200/0] via 172.16.0.1, 00:27:00
B       10.0.1.0 [200/0] via 172.16.0.3, 00:26:59
B       10.0.6.0 [200/0] via 172.16.0.8, 00:27:00
B       10.0.19.0 [200/0] via 172.16.0.21, 00:27:00
C       10.0.44.0 is directly connected, FastEthernet0/1
B       10.0.254.0 [200/0] via 172.16.0.3, 00:26:59
B       10.0.255.0 [200/0] via 172.16.0.1, 00:27:00
```

Imatge 31 - Taula de rutes d'una seu remota

Al següent enllaç es pot veure les mateixes proves però en vídeo:

http://youtu.be/t45N3bcSNUA

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuran tan nítides.

7.2.2.- Caiguda LAN del router TRANS_BCN1. Actuació HSRP

Ara provarem l'HSRP de la seu de Barcelona, concretament quan es perd el *link* amb les interfícies de LAN. Simularem una caiguda d'interfície posant les interfícies en *shutdown*, ja que amb GNS3 si es treu un enllaç la interfície continua en estat *up*. En la realitat quan es treu un cable, el *link* de la interfície passa a estat *down* i actuaria de la mateixa manera.

L'estat de les interfícies GigaEthernet1/0 i GigaEthernet2/0 en *shutdown* mitjançant la configuració es pot veure a la imatge 32:

```
TRANS_BCN1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         172.16.0.1      YES NVRAM  up                    up
GigabitEthernet1/0         10.0.0.2        YES NVRAM  administratively down down
GigabitEthernet2/0         10.0.255.2      YES NVRAM  administratively down down
Loopback0                  1.1.1.1         YES NVRAM  up                    up
```

Imatge 32 - TRANS_BCN1 LAN caiguda

Quan la LAN està *down*, el HSRP dels routers passa a tindre el següent rol:

```
TRANS_BCN1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       10   120 P Init    unknown         unknown         10.0.0.1
Gi2/0       20   120 P Init    unknown         unknown         10.0.255.1
```

```
TRANS_BCN2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       10   100 P Active  local           unknown         10.0.0.1
Gi2/0       20   100 P Active  local           unknown         10.0.255.1
```

Imatge 33 - Router TRANS_BCN1 i TRANS_BCN2 actuant HSRP, caiguda LAN

Al router TRANS_BCN1 la seva prioritat continuarà a 120, però el seu estat, que és *Init*, indica que no hi ha connectivitat amb l'altre router ja que la seva interfície està amb el *link down*. El TRANS_BCN2 té la seva prioritat a 100, però el seu estat és actiu. Veiem com a la columna s*tandby* indica *unknown*, que vol dir que no veu l'altre router, i per tant serà aquest router qui passarà a estar en mode actiu.

La resta de les seus hauran canviat la seva taula de rutes. Si posem la comanda per a veure la taula de rutes sencera d'un router, veiem que per arribar a les xarxes 10.0.0.0/24 i 10.0.255.0/24 el salt és la IP WAN 172.16.0.2 del router redundant TRANS_BCN2:

```
TRANS_SEV#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 6 subnets
B       1.1.1.1 [200/0] via 172.16.0.1, 00:32:53
B       1.1.1.3 [200/0] via 172.16.0.3, 00:32:52
B       1.1.1.2 [200/0] via 172.16.0.2, 00:32:53
B       1.1.1.8 [200/0] via 172.16.0.8, 00:32:53
B       1.1.1.21 [200/0] via 172.16.0.21, 00:20:04
C       1.1.1.46 is directly connected, Loopback0
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 7 subnets
B       10.0.0.0 [200/0] via 172.16.0.2, 00:00:01
B       10.0.1.0 [200/0] via 172.16.0.3, 00:32:56
B       10.0.6.0 [200/0] via 172.16.0.8, 00:32:57
B       10.0.19.0 [200/0] via 172.16.0.21, 00:32:57
C       10.0.44.0 is directly connected, FastEthernet0/1
B       10.0.254.0 [200/0] via 172.16.0.3, 00:32:56
B       10.0.255.0 [200/0] via 172.16.0.2, 00:00:01
```

Imatge 34 - Taula de rutes seu remota, TRANS_BCN2 actiu

També es realitza un *traceroute* des del router de Sevilla cap al VPC1, i així verificar els salts que es realitzen fins arribar al destí:

```
TRANS_SEV#traceroute 10.0.0.200

Type escape sequence to abort.
Tracing the route to 10.0.0.200

  1 172.16.0.2 1274 msec 144 msec 29 msec
  2  *
     10.0.0.200 93 msec 60 msec
```

Imatge 35 - Traceroute, TRANS_BCN2 actiu

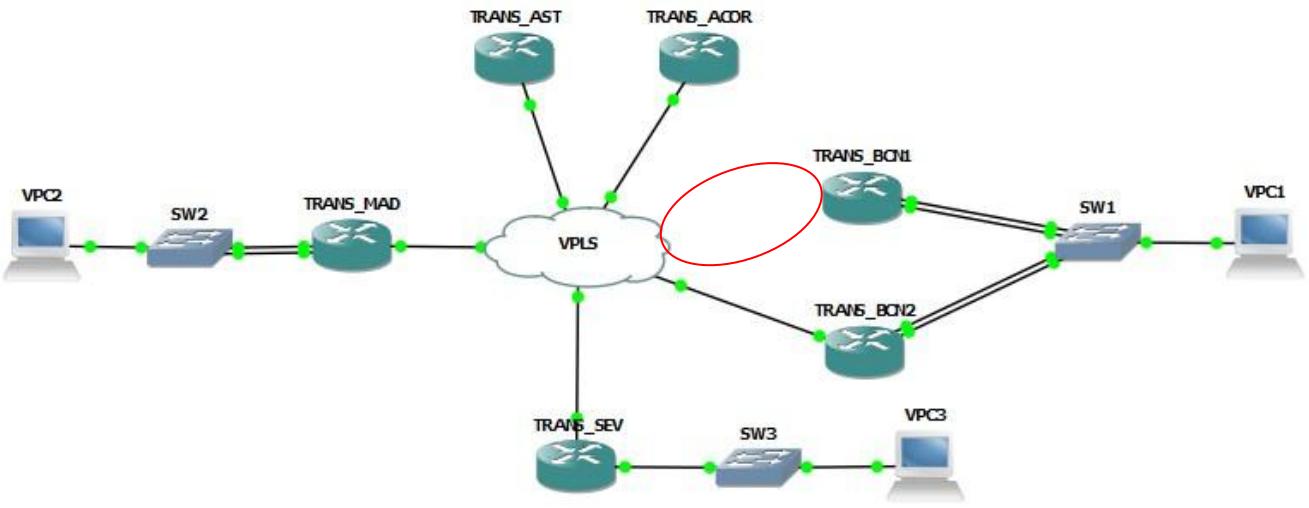
Al següent enllaç es pot veure les mateixes proves però en vídeo:

http://youtu.be/1Dpkap8gJGg

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuran tan nítides.

7.2.3.- Caiguda de l'accés WAN principal de Barcelona. Actuació HSRP i tracks

En aquest punt posarem a prova una caiguda física/lògica de la WAN del router principal de Barcelona TRANS_BCN1. Els equips de la VPLS poden sofrir caigudes que a nivell d'interfície del router no perdi el *link*, per tant provarem els *tracks* creats.
Per a simular una caiguda lògica de la interfície de WAN Giga Ethernet 0/0, eliminarem la connexió d'aquesta interfície amb la VPLS, així deixarem la interfície en estat *up* però el ping del *track* no arribarà:



Imatge 36 - Topologia amb WAN principal caiguda

Una vegada detecta el *track* que no pot arribar a les IPs de *loopback* de TRANS_BCN2 (*track* 2) i TRANS_MAD (*track* 3), aquests *tracks* passen a estat *down*, i per tant l'HSRP fa un decrement de 30 quedant-se amb un valor de 90 quan el *track* 1 realitza la comparació lògica i canvia el seu estat a *down*. Podem veure en la imatge 37 com TRANS_BCN1 entra en mode *standby* al comprovar el *track* 1 que no arriben els pings dels *track* 2 i 3:

```
TRANS_BCN1#show standby brief
                     P indicates configured to preempt.
                     |
Interface Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0     10   90  P Standby 10.0.0.3        local           10.0.0.1
Gi2/0     20   90  P Standby 10.0.255.3      local           10.0.255.1
TRANS_BCN1#show track
Track 1
  List boolean or
  Boolean OR is Down
    3 changes, last change 00:00:26
    object 2 Down
    object 3 Down
  Tracked by:
    HSRP GigabitEthernet1/0 10
    HSRP GigabitEthernet2/0 20
Track 2
  Response Time Reporter 1 reachability
  Reachability is Down
    3 changes, last change 00:00:26
  Delay up 8 secs, down 8 secs
  Latest operation return code: Timeout
  Tracked by:
    Track-list 1
Track 3
  Response Time Reporter 2 reachability
  Reachability is Down
    3 changes, last change 00:00:26
  Delay up 8 secs, down 8 secs
  Latest operation return code: Timeout
  Tracked by:
    Track-list 1
```

Imatge 37 - Track TRANS_BCN1 down

El router TRANS_BCN2 està com *active*, ja que la seva prioritat és 100 i per tant en aquest moment és major que el TRANS_BCN1:

```
TRANS_BCN2#show standby brief
                     P indicates configured to preempt.
                     |
Interface Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0     10   100 P Active  local           10.0.0.2        10.0.0.1
Gi2/0     20   100 P Active  local           10.0.255.2      10.0.255.1
```

Imatge 38 - Router TRANS_BCN2 actiu

La taula de rutes d'una seu remota serà la mateixa que en el cas que caigui la LAN del router principal de Barcelona, com ja hem vist en el punt 7.2.2.- Caiguda LAN del router TRANS_BCN1. Actuació HSRP:

```
TRANS_AST#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 5 subnets
B       1.1.1.3 [200/0] via 172.16.0.3, 00:37:09
B       1.1.1.2 [200/0] via 172.16.0.2, 00:37:35
C       1.1.1.8 is directly connected, Loopback0
B       1.1.1.21 [200/0] via 172.16.0.21, 00:24:24
B       1.1.1.46 [200/0] via 172.16.0.46, 00:13:17
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 7 subnets
B       10.0.0.0 [200/0] via 172.16.0.2, 00:04:20
B       10.0.1.0 [200/0] via 172.16.0.3, 00:37:12
C       10.0.6.0 is directly connected, FastEthernet0/1
B       10.0.19.0 [200/0] via 172.16.0.21, 00:37:12
B       10.0.44.0 [200/0] via 172.16.0.46, 00:37:12
B       10.0.254.0 [200/0] via 172.16.0.3, 00:37:12
B       10.0.255.0 [200/0] via 172.16.0.2, 00:04:22
```

Imatge 39 - Taula rutes d'una seu remota amb la WAN de Barcelona caiguda

El *track* 1 fa una comprovació booleana OR. Això fa que només es realitzi el decrement a l'HSRP quan el *track* 2 i *track* 3 estiguin *down*. Si només falla un dels dos *tracks*, el *track* 1 continua *up*. La comprovació la farem eliminant la connexió WAN de TRANS_MAD i tornant a connectar la WAN de TRANS_BCN1. Comprovem-ho:

```
TRANS_BCN1#show track
Track 1
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:00:22
    object 2 Up
    object 3 Down
  Tracked by:
    HSRP GigabitEthernet1/0 10
    HSRP GigabitEthernet2/0 20
Track 2
  Response Time Reporter 1 reachability
  Reachability is Up
    2 changes, last change 00:00:22
  Delay up 8 secs, down 8 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 104
  Tracked by:
    Track-list 1
Track 3
  Response Time Reporter 2 reachability
  Reachability is Down
    1 change, last change 00:13:23
  Delay up 8 secs, down 8 secs
  Latest operation return code: Timeout
  Tracked by:
    Track-list 1
```

Imatge 40 - TRANS_BCN1: Track 2 up, track 3 *down*

El *track* 2 correspon a la *loopback* del router TRANS_BCN2. El track 3 correspon al ping cap a la *loopback* de TRANS_MAD. Veiem com el *track* 2 cap a TRANS_BCN2 està *up* i el *track* 3 de TRANS_MAD està *down*, i per tant la comparació que realitza el *track* 1 estarà *up*. Fins que els *tracks* 2 i 3 no estiguin *down*, el *track* 1 continuarà com a up i per tant el router TRANS_BCN1 com a actiu.

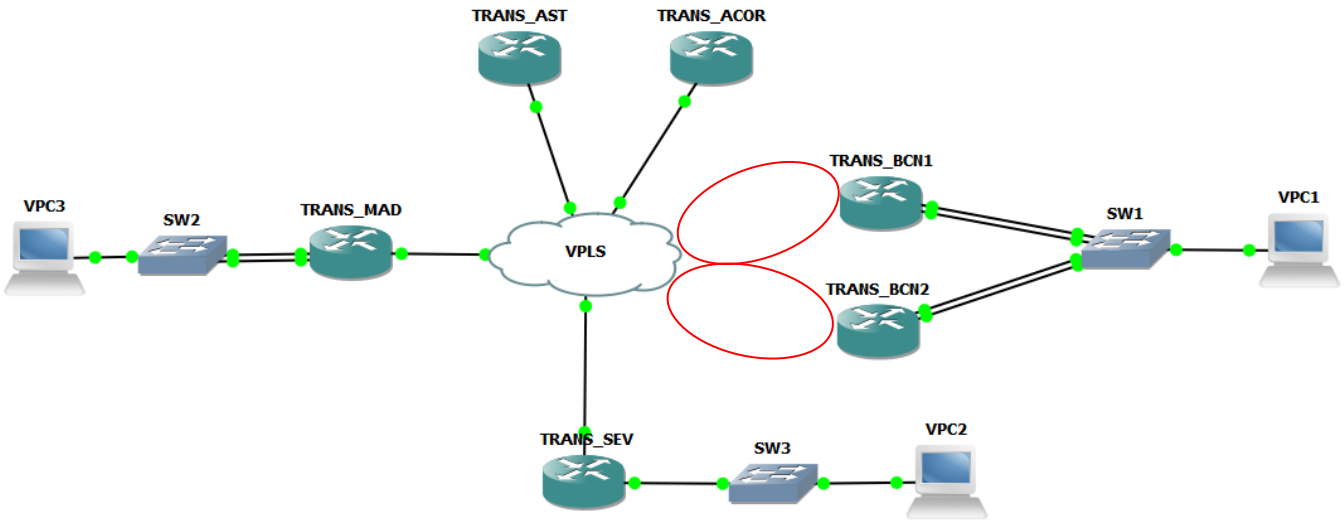
Al següent enllaç es pot veure les mateixes proves però en vídeo:

http://youtu.be/1BndSfn4UOI

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuran tan nítides.

7.2.4.- Incomunicació total de la seu de Barcelona

En aquest apartat verificarem com la xarxa LAN dels servidors 10.0.255.0/24 continua treballant per la seu de Madrid, encara que la seu de Barcelona estigui totalment incomunicada. Per a realitzar la simulació eliminarem els dos enllaços WAN de la seu de Barcelona



Imatge 41 - Topologia de la seu de Barcelona incomunicada

Quan la topologia es troba com en la imatge 41, el router de Madrid TRANS_MAD ha d'assumir el tràfic que abans anava cap a la LAN de servidors que es trobava en Barcelona. TRANS_MAD publica la xarxa LAN 10.0.255.0/24 utilitzant una ruta estàtica que envia totes les connexions que van cap aquesta xarxa a l'equip de client 10.0.254.2, que serà l'encarregat de encaminar el tràfic cap als servidors redundants necessaris.

La taula de rutes que podem veure a les seus remotes són:

```
TRANS_SEV#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 4 subnets
B       1.1.1.3 [200/0] via 172.16.0.3, 00:39:41
B       1.1.1.8 [200/0] via 172.16.0.8, 00:00:11
B       1.1.1.21 [200/0] via 172.16.0.21, 00:00:11
C       1.1.1.46 is directly connected, Loopback0
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 6 subnets
B       10.0.1.0 [200/0] via 172.16.0.3, 00:39:41
B       10.0.6.0 [200/0] via 172.16.0.8, 00:00:11
B       10.0.19.0 [200/0] via 172.16.0.21, 00:00:13
C       10.0.44.0 is directly connected, FastEthernet0/1
B       10.0.254.0 [200/0] via 172.16.0.3, 00:39:43
B       10.0.255.0 [200/0] via 10.0.254.2, 00:00:11
```

Imatge 42 - Taula rutes amb la seu de Barcelona incomunicada

En la imatge 42 podem veure com per arribar a la xarxa 10.0.255.0/24 ha d'anar cap a la IP 10.0.254.2, i la xarxa 10.0.254.0/24 la coneix a través de la IP WAN 172.16.0.3, que és la IP WAN del router TRANS_MAD.

Podem confirmar en la imatge 43 com la seu de Madrid publica utilitzant una ruta estàtica amb distància administrativa 250, que penalitza més que el 200 que té el nostre BGP:

```
TRANS_MAD#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 4 subnets
C       1.1.1.3 is directly connected, Loopback0
B       1.1.1.8 [200/0] via 172.16.0.8, 00:41:06
B       1.1.1.21 [200/0] via 172.16.0.21, 00:28:11
B       1.1.1.46 [200/0] via 172.16.0.46, 00:16:56
     172.16.0.0/25 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, GigabitEthernet0/0
     10.0.0.0/24 is subnetted, 6 subnets
C       10.0.1.0 is directly connected, GigabitEthernet1/0
B       10.0.6.0 [200/0] via 172.16.0.8, 00:41:06
B       10.0.19.0 [200/0] via 172.16.0.21, 00:41:06
B       10.0.44.0 [200/0] via 172.16.0.46, 00:41:06
C       10.0.254.0 is directly connected, GigabitEthernet2/0
S       10.0.255.0 [250/0] via 10.0.254.2
```

Imatge 43 - Taula de rutes de la seu de Madrid amb Barcelona incomunicada

Ara es verificarà que realment segueix la ruta cap a la IP 10.0.254.2 quan es vol anar a la xarxa 10.0.255.0/24. Per a realitzar-ho hem configurat el VPC3 amb la IP 10.0.254.2, i es realitzarà un *traceroute* des d'una seu i veurem els salts que realitza:

```
TRANS_SEV#traceroute 10.0.255.10

Type escape sequence to abort.
Tracing the route to 10.0.255.10

  1 172.16.0.3 104 msec 60 msec 32 msec
  2 10.0.255.10 168 msec 65 msec 140 msec
```

Imatge 44 - Traceroute cap a 10.0.255.0/24 amb Barcelona incomunicada

El primer salt és la IP WAN de la seu de Madrid, i el següent ja ens contesta l'equip fictici al que li hem fet el *traceroute*, el 10.0.255.10. En realitat qui contesta és el VPC1 configurat amb la IP 10.0.254.2. Quan es configuri aquest escenari en una xarxa real, aquest equip encaminaria el tràfic cap a l'equip necessari o bé seria ell mateix el que assumiria la contestació.

Hem eliminat la connexió d'un dels dos RR, llavors ara totes les seus coneixeran les rutes únicament a través del RR de Madrid:

```
TRANS_SEV#show ip bgp summary
BGP router identifier 172.16.0.46, local AS number 100
BGP table version is 32, main routing table version 32
11 network entries using 1320 bytes of memory
12 path entries using 624 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP rrinfo entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 2644 total bytes of memory
BGP activity 14/3 prefixes, 30/18 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.2      4   100     256     246        0    0    0 00:02:27 Active
172.16.0.3      4   100     278     260       32    0    0 00:42:16        9
```

Imatge 45 - Treballant únicament amb un RR

Podem veure com el veí 172.16.0.3, router TRANS_MAD, està operatiu i enviant 9 rutes (s'indica en la columna Pfx/Rcd). Pel que fa al veí 172.16.0.2, router TRANS_BCN2, veiem que l'estat és *Active*, és a dir no està establerta la connexió amb aquest veí i està a l'espera de poder establir-la.

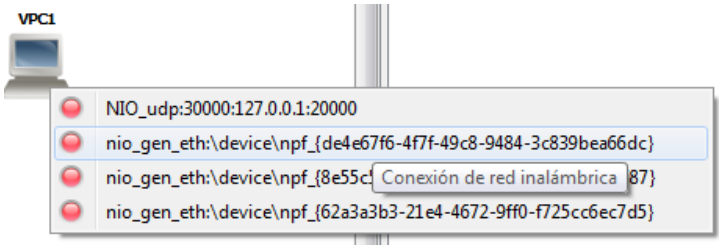
Al següent enllaç es pot veure les mateixes proves però en vídeo:

http://youtu.be/Ez5pnAc9Vys

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuran tan nítides.

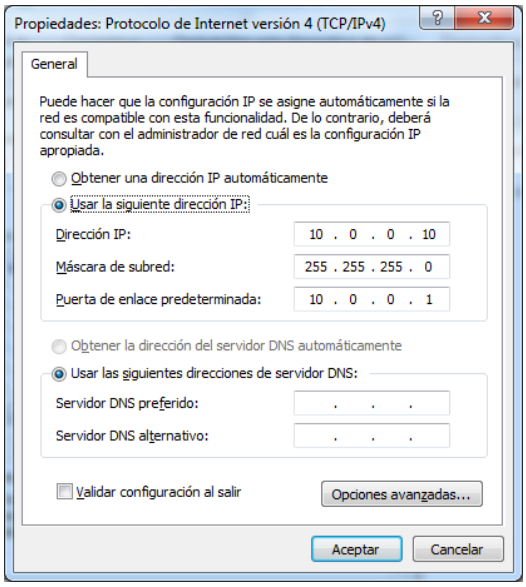
7.2.5.- Comprovació ACLs. Restricció de l'accés per Telnet

Per restringir l'accés per Telnet als routers s'ha creat una ACL de restricció. Aquesta ACL només permet a l'equip amb IP 10.0.0.200 accedir per Telnet i a la resta li denega l'accés. El VPC1 es connectarà a la targeta sense fils del meu ordinador i es configurarà amb la mateixa xarxa que la seu de Barcelona, així es podrà realitzar les comprovacions des del CMD de Windows del meu ordinador. Llavors, en aquesta comprovació el VPC1 es connectarà a la següent interfície:



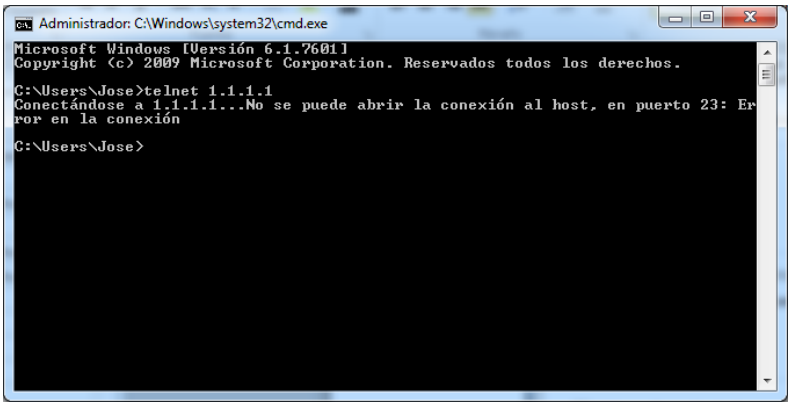
Imatge 46 – Connexió GNS3-Targeta Wifi

I aquesta interfície la configurarem de la següent forma:



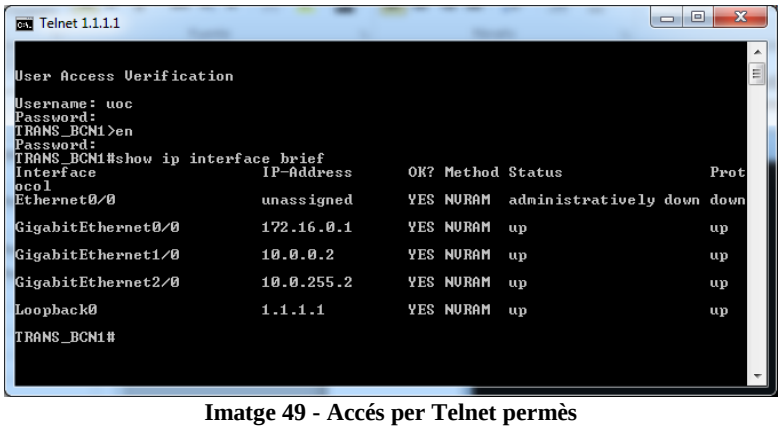
Imatge 47 - Configuració interfície Wifi

Es pot veure com la IP assignada és la 10.0.0.10, per tant quan intentem fer un Telnet des del CMD de l'ordinador a una IP de gestió dels routers no ens deixarà connectar-nos:



Imatge 48 - Accés per Telnet denegat

Ara canviem la configuració de la interfície per la 10.0.0.200, que és la única que permet l'accés per Telnet als routers, i veiem el resultat:



Imatge 49 - Accés per Telnet permès

Només posar la comanda *"telnet 1.1.1.1",* ja ens demana usuari i contrasenya. S'ha posat *uoc* tant en l'usuari com en les contrasenyes. El Telnet el podem fer a qualsevol IP de *loopback* o de WAN del router al que ens vulguem connectar.
A continuació també veiem com el comptador de l'ACL 100 ha pujat quan hem fet les connexions. L'ACL té una denegació per defecte, és a dir es denega l'accés a totes les IPs que no estiguin expressament acceptades:

```
TRANS_BCN1#show access-lists 100
Extended IP access list 100
    10 permit ip host 10.0.0.200 any (2 matches)
```

Imatge 50 – Comptador ACL 100, accés per Telnet

Al següent enllaç es pot veure les mateixes proves de l'ACL però en vídeo:

http://youtu.be/45L-P8EIZa4

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuen tan nítides.

7.2.6.- Comprovació ACLs. Limitació de l'ample de banda

Les seus de Barcelona i Madrid tenen una limitació entre ambdues seus de 100 Mbps. En aquesta simulació no és viable realitzar una prova real realitzant un tràfic gran i veure com és limita. La forma que tenim és mirar l'ACL 110 com puja el comptador quan, per exemple, és realitza un ping entre les dues seus. Realitzem un ping entre VPC amb origen el 10.0.0.200 i destí 10.0.1.200. El comportament de les ACL als routers són:

```
TRANS_BCN1#sh access-lists 110
Extended IP access list 110
    10 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255 (100 matches)
    20 permit ip 10.0.255.0 0.0.0.255 10.0.1.0 0.0.0.255
    30 permit ip 10.0.255.0 0.0.0.255 10.0.254.0 0.0.0.255
    40 permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255
```

```
TRANS_MAD#sh access-lists 110
Extended IP access list 110
    10 permit ip 10.0.1.0 0.0.0.255 10.0.0.0 0.0.0.255 (100 matches)
    20 permit ip 10.0.1.0 0.0.0.255 10.0.255.0 0.0.0.255
    30 permit ip 10.0.254.0 0.0.0.255 10.0.255.0 0.0.0.255
    40 permit ip 10.0.254.0 0.0.0.255 10.0.0.0 0.0.0.255
```

Imatge 51 - Comptador ACL 110

Les línies de l'ACL amb origen/destí les xarxes des de les quals s'han realitzat les proves, tenen el comptador (*matches)* a 100, el que indica que s'ha aplicat aquesta ACL en 100 paquets (el número de repeticions de ping que s'ha realitzat) i per tant la limitació a 100 Mbps s'estarà aplicant ja que aquesta ACL va vinculada a un *rate-limit*.

Al següent enllaç es pot veure les mateixes proves de l'ACL però en vídeo:

http://youtu.be/UcPgXffZbMw

Es recomana escollir la qualitat de reproducció en 720p HD, ja que sinó les lletres no es veuen tan nítides.

8.- Pressupost

S'ha de mirar la viabilitat d'aquest projecte a nivell econòmic. Per això, s'exposarà una aproximació dels preus dels operadors actuals que operen a Espanya, sense concretar cap operador en concret.

Preus d'instal·lació

Descripció	Unitats	Preu unitari	Total
Instal·lació de fibra òptica VPLS: 2xGigabit Ethernet (Seu de Barcelona)	1	14500 €	14500 €
Instal·lació de fibra òptica VPLS: 1xGigabit Ethernet (Seu de Madrid)	1	9500 €	9500 €
Instal·lació de fibra òptica VPLS: 1x10 MB (Seus remotes)	50	2900 €	145000 €
Instal·lació de routers	53	200 €	10600 €
TOTAL:			179600 €

Taula 12 - Taula dels preus d'instal·lació

Preu mensual

Descripció	Unitats	Preu unitari	Total
Connexió de fibra òptica VPLS: 2xGigabit Ethernet (Seu de Barcelona: Cabal de 300 Mbps)	1	9000 €	9000 €
Connexió de fibra òptica VPLS: 1xGigabit Ethernet (Seu de Madrid: Cabal de 300 Mbps)	1	4500 €	4500 €
Connexió de fibra òptica VPLS: 1x10 MB (Seus remotes: Cabal de 10 Mbps)	50	900 €	45000 €
Arrendament Cisco 7206VRX (manteniment integral)	3	200 €	600 €
Arrendament Cisco 2621XM (manteniment integral)	50	90 €	4500 €
TOTAL:			63600 €

Taula 13 - Taula de preus mensuals

Els costos d'instal·lació contenen el preu d'introduir la fibra òptica fins al domicili de client. Aquests preus és una aproximació del preu de mercat actual per a VPNs amb fibra òptica.

El preu mensual inclou el manteniment dels accessos i els cabals contractats en cada seu. Pel que fa als routers, s'ha escollit el mètode d'arrendament amb l'operador, que té un cost mensual que integra la substitució total o parcial dels routers. Això té l'avantatge que *Transports Express S.A.* no ha de comprar els router ni disposar d'estoc de routers per a substituir-los, i així reduir el pressupost necessari.

El pressupost no té cap tipus de descomptes, però quan existeix un lligam de permanència amb un operador, aquests costos d'instal·lació i mensual es redueixen de forma considerable i depenen del temps de permanència.

Per altra banda, el disseny de la xarxa del projecte es portarà a terme per part del Departament de Comunicacions de *Transports Express S.A.*, per tant no tindrà un augment del pressupost. Això és possible ja que, com s'ha comentat amb anterioritat, la VPLS és una extensió de la LAN, per tant el client pot dissenyar el seu direccionament. El cost de configuració als nodes de l'ISP per tal de crear una VPN de capa 2 per al client va inclòs en el cost d'instal·lació de cada accés.

9.- Viabilitat i conclusions del projecte

Hem demostrat com la solució tecnològica proposada es pot portar a terme en la realitat. En totes les opcions escollides s'ha tingut en compte les necessitats que requeria *Transports Express S.A.* i s'ha intentat trobar el punt mig entre tecnologia i preu.

En aquest projecte s'ha creat una VPN d'última generació que millora de forma important les comunicacions del client a nivell d'innovació, velocitat i privacitat. A més, la solució donada deixa la xarxa totalment preparada per a crear una sortida a Internet comuna a totes les seus, sense interferir en la privacitat de les comunicacions internes ja que es podria tenir un *Firewall* comú. Això implicaria poder expandir el seu treball al món virtual i poder obtenir més clients.

En definitiva, i tot i no havent pogut confirmar un pressupost, podem afirmar la viabilitat del projecte. Totes les solucions plantejades han estat escollides amb una visió realista del món de les comunicacions actuals, i això comporta que tots els plantejaments siguin realitzables i tinguin un funcionament correcte.

10.- Bibliografia

Informació proveïdors de hardware:

Fabricant i model	Direcció web
Cisco 2621XM	http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd800fa5be.pdf
Cisco 7206VRX	http://www.cisco.com/en/US/prod/collateral/routers/ps341/data_sheet_c78_339749.pdf http://www.cisco.com/en/US/prod/collateral/modules/ps3931/product_data_sheet09186a00800c6bd6.pdf
Juniper CTP 150	http://www.juniper.net/us/en/local/pdf/datasheets/1000139-en.pdf
Juniper J2320	http://www.juniper.net/us/en/local/pdf/datasheets/1000206-en.pdf
Huawei AR28-10	http://www.huawei.com/es/products/data-communication/ar-routers/ar28/index.htm
Huawei AR 2220	http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093991.pdf
Alcatel-Lucent OmniAccess 5840	http://enterprise.alcatel-lucent.com/?product=OmniAccessESRModularRouters&page=overview
Alcatel-Lucent	http://resources.alcatel-lucent.com/?cid=152948

7705 SAR-M	

Informació sobre MPLS i VPLS:

http://www.normes-internet.com/normes.php?rfc=rfc4761&lang=es

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

http://datatracker.ietf.org/wg/mpls/charter/

http://www.cert.uy/wps/wcm/connect/3f5c2e804edd1794962896f04da0fafa/Presentaci%C3%B3n+02+-+MPLS-VPN.pdf?MOD=AJPERES

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

Informació sobre protocols de Routing:

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

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

http://www.redescisco.net/v2/art/tipos-de-areas-en-ospf/

http://networkninja.co.za/cisco-systems/open-shortest-path-first-ospf-fundamentals-dr-and-bdr/

http://www.redespracticas.com/?Njs=t&pag=txtEnrutamientoEIGRPcsco.php

http://www.geocities.ws/mpss1230/eigrp.html

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

http://lacnic.net/documentos/lacnicxii/presentaciones/08_bgp.pdf

http://ccgrupo6.webcindario.com/expo10.pdf

http://www.h3c.com/portal/Products___Solutions/Technology/IP_Routing/Technology_Introduction/200702/201386_57_0.htm

http://cisconetworkingcenter.blogspot.com.es/2013/01/comparison-of-routing-protocols-eigrp.html
http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

Informació sobre protocols de redundància:

http://blog.capacityacademy.com/2013/01/07/cisco-ccnp-que-es-y-como-configurar-el-protocolo-hsrp/

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

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

http://www.the-evangelist.info/2010/06/ccnp-switch-13-alta-disponibilidad-en-capa-3/

http://tools.ietf.org/html/rfc3768#section-6.3

http://www.ietf.org/rfc/rfc2281.txt

Informació sobre configuració pràctica dels routers

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25ewa/configuration/guide/qos.pdf

http://www.powerfast.net/bgp/BGP_Nd60.html

http://blog.regisdonovan.org/2010/10/bgp-basics-active-is-not-good-state.html

http://www.aprenderedes.com/

11.- Acrònims

ABR: Area Border Router

ACK: Acknowledgement

ADSL: Asymmetric Digital Subscriber Line

ASBR: Autonomous System Border Router

ATM: Asynchronous Transfer Mode

BDR: Backup Designated Router

BGP: Border Gateway Protocol

BR: Backbone Router

BW: Bandwidth

CIDR: Classless Inter-Domain Routing

CLI: Command-Line Interface

CMD: Command prompt

CPD: Centre de Processament de Dades

DR: Designated Router

EDC: Equip De Client

EIGRP: Enhanced Interior Gateway Routing Protocol

FEC: Forwarding Equivalence Class

FR: Frame Relay

GNS 3: Graphical Network Simulator 3

HD: High Definition

HSRP: Hot Standby Router Protocol

IOS de Cisco: Internetwork Operating System de Cisco

IP: Internet Protocol

IPSec: Internet Protocol security

IR: Internal Router

ISP: Internet Service Provider

LAN: Local Area Network

LDP: Label Distribution Protocol

LER: Label Edge Router

LSP: Label Switched Path

LSR: Label Switching Router

MPLS: Multiprotocol Label Switching

OSI: Open System Interconnection

OSPF: Open Shortest Path First

QoS: Quality Of Service

RIP: Routing Information Protocol

RR: Route Reflector

SSL: Secure Sockets Layer

VLAN: Virtual Local Area Network

VLSM: Variable Length Subnet Mask

VPC: Virtual Personal Computer

VPLS: Virtual Private LAN Service

VPN: Virtual Private Network

VRF: Virtual Routing Forwarding

VRRP: Virtual Router Redundancy Protocol

WAN: Wide Area Network

WIC: WAN Interface Card

Annex

Configuració router TRANS_BCN1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TRANS_BCN1
!
boot-start-marker
boot-end-marker
!
no logging console
enable secret 5 $1$GcDG$EuYVA0xmEB9JgLPtaZDgH.
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
no ip domain lookup
ip sla 1
 icmp-echo 1.1.1.2
 request-data-size 100
 frequency 10
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 1.1.1.3
 request-data-size 100
 frequency 10
ip sla schedule 2 life forever start-time now
!
username uoc secret 5 $1$pOuI$PYShB6zlZNHw3C2d4FS111
!
track 2 rtr 1 reachability
 delay down 8 up 8
!
track 3 rtr 2 reachability
 delay down 8 up 8
!
track 1 list boolean or
 object 2
 object 3
```

```
!
class-map match-all Limitacio_100Mbps
 match access-group 110
!
!
policy-map Limitacio_100Mbps
  class Limitacio_100Mbps
  police rate 100000000 bps
    exceed-action drop
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.1 255.255.255.128
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 service-policy output Limitacio_100Mbps
!
interface GigabitEthernet1/0
 description Connexio LAN treballadors
 ip address 10.0.0.2 255.255.255.0
 load-interval 30
 negotiation auto
 standby 10 ip 10.0.0.1
 standby 10 priority 120
 standby 10 preempt
 standby 10 track 1 decrement 30
!
interface GigabitEthernet2/0
 description Connexio Servidors BCN
 ip address 10.0.255.2 255.255.255.0
 load-interval 30
 negotiation auto
 standby 20 ip 10.0.255.1
 standby 20 priority 120
 standby 20 preempt
 standby 20 track 1 decrement 30
!
router bgp 100
 no synchronization
```

```
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 10.0.0.0 mask 255.255.255.0 route-map Local
 network 10.0.255.0 mask 255.255.255.0 route-map Local
 neighbor RR peer-group
 neighbor RR remote-as 100
 neighbor RR timers 10 30
 neighbor 172.16.0.2 peer-group RR
 neighbor 172.16.0.3 peer-group RR
 no auto-summary
!
ip classless
no ip http server
no ip http secure-server
!
!
logging alarm informational
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
access-list 110 remark ACL xarxes limitacio BW
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.254.0 0.0.0.255
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255
!
route-map Local permit 10
 set local-preference 300
!
!
control-plane
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 100 in
 logging synchronous
 login local
!
!
end
```

Configuració router TRANS_BCN2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TRANS_BCN2
!
boot-start-marker
boot-end-marker
!
no logging console
enable secret 5 $1$P50d$4c0I3MwOJvPmzqxUvOPnf/
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
no ip domain lookup
!
!
username uoc secret 5 $1$bGMi$EQMQCW7o8dWhLQP5zjhTE.
!
!
class-map match-all Limitacio_100Mbps
 match access-group 110
!
!
policy-map Limitacio_100Mbps
  class Limitacio_100Mbps
  police rate 100000000 bps
    exceed-action drop
!
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description Connexio WAN VPLS
```

```
 ip address 172.16.0.2 255.255.255.128
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 service-policy output Limitacio_100Mbps
!
interface GigabitEthernet1/0
 description Connexio LAN treballadors
 ip address 10.0.0.3 255.255.255.0
 negotiation auto
 standby 10 ip 10.0.0.1
 standby 10 preempt
!
interface GigabitEthernet2/0
 description Connexio Servidors BCN
 ip address 10.0.255.3 255.255.255.0
 negotiation auto
 standby 20 ip 10.0.255.1
 standby 20 preempt
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 neighbor SEUS peer-group
 neighbor SEUS remote-as 100
 neighbor SEUS timers 10 30
 neighbor 172.16.0.1 peer-group SEUS
 neighbor 172.16.0.3 remote-as 100
 neighbor 172.16.0.3 timers 10 30
 neighbor 172.16.0.8 peer-group SEUS
 neighbor 172.16.0.21 peer-group SEUS
 neighbor 172.16.0.46 peer-group SEUS
 !
 address-family ipv4
 neighbor SEUS route-reflector-client
 neighbor 172.16.0.1 activate
 neighbor 172.16.0.1 weight 40000
 neighbor 172.16.0.3 activate
 neighbor 172.16.0.8 activate
 neighbor 172.16.0.21 activate
 neighbor 172.16.0.46 activate
 no auto-summary
 no synchronization
 bgp redistribute-internal
 network 1.1.1.2 mask 255.255.255.255
 network 10.0.0.0 mask 255.255.255.0 route-map Local
 network 10.0.255.0 mask 255.255.255.0 route-map Local
 exit-address-family
!
ip classless
```

```
no ip http server
no ip http secure-server
!
logging alarm informational
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
access-list 110 remark ACL xarxes limitacio BW
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 110 permit ip 10.0.255.0 0.0.0.255 10.0.254.0 0.0.0.255
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255
!
route-map Local permit 10
 set local-preference 200
!
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 100 in
 logging synchronous
 login local
!
!
end
```

Configuració router TRANS_MAD

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TRANS_MAD
!
boot-start-marker
```

```
boot-end-marker
!
no logging console
enable secret 5 $1$l1VB$CLXSULZyMm97Yk7k3qlih1
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
no ip domain lookup
!
!
username uoc secret 5 $1$sZvL$3KoQ7v5tL4EaWw2xUEBqo/
!
!
class-map match-all Limitacio_100Mbps
 match access-group 110
!
!
policy-map Limitacio_100Mbps
  class Limitacio_100Mbps
  police rate 100000000 bps
    exceed-action drop
!
!
interface Loopback0
 ip address 1.1.1.3 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description Connexio WAN VPLS
 ip address 172.16.0.3 255.255.255.128
 ip virtual-reassembly
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 service-policy output Limitacio_100Mbps
!
interface GigabitEthernet1/0
```

```
 description Connexio LAN treballadors
 ip address 10.0.1.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2/0
 description Connexio LAN Copia servidors
 ip address 10.0.254.1 255.255.255.0
 ip virtual-reassembly
 negotiation auto
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 neighbor SEUS peer-group
 neighbor SEUS remote-as 100
 neighbor SEUS timers 10 30
 neighbor 172.16.0.1 remote-as 100
 neighbor 172.16.0.1 timers 10 30
 neighbor 172.16.0.2 remote-as 100
 neighbor 172.16.0.2 timers 10 30
 neighbor 172.16.0.8 peer-group SEUS
 neighbor 172.16.0.21 peer-group SEUS
 neighbor 172.16.0.46 peer-group SEUS
 !
 address-family ipv4
 redistribute static
 neighbor SEUS route-reflector-client
 neighbor 172.16.0.1 activate
 neighbor 172.16.0.1 weight 40000
 neighbor 172.16.0.2 activate
 neighbor 172.16.0.2 weight 40000
 neighbor 172.16.0.8 activate
 neighbor 172.16.0.21 activate
 neighbor 172.16.0.46 activate
 no auto-summary
 no synchronization
 network 1.1.1.3 mask 255.255.255.255
 network 10.0.1.0 mask 255.255.255.0
 network 10.0.254.0 mask 255.255.255.0
 exit-address-family
!
ip classless
ip route 10.0.255.0 255.255.255.0 10.0.254.2 250
no ip http server
no ip http secure-server
!
!
logging alarm informational
access-list 100 remark ACL de restriccio del Telnet
access-list 100 permit ip host 10.0.0.200 any
access-list 110 remark ACL xarxes limitacio BW
```

```
access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.255.0 0.0.0.255
access-list 110 permit ip 10.0.254.0 0.0.0.255 10.0.255.0 0.0.0.255
access-list 110 permit ip 10.0.254.0 0.0.0.255 10.0.0.0 0.0.0.255
!
control-plane
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 100 in
 logging synchronous
 login local
!
end
```