

Implantació i emulació d'una VPN sobre VPLS



Alumne: José R. Hidalgo

Consultor: José López Vicario

Titulació: Enginyeria Tècnica en Telecomunicacions, especialitat en Telemàtica

DESCRIPCIÓ DEL PROJECTE

- **Implantació d'una VPN nacional per a Transports Express S.A.**
- **L'empresa disposa de 52 seus:**
 - 2 seus principals: Barcelona i Madrid, amb CPDs preparats
 - 50 seus remotes distribuïdes per províncies
- **Accés WAN amb fibra òptica a totes les seus**
- **Tecnologia i equipament escollit per a la solució**
- **Emular amb GNS3 la xarxa**



DESCRIPCIÓ DE LES SEUS

○ Barcelona:

- Doble router i accés d'1 Gb (cabal de 300 Mbps)
- Dues xarxes:
 - Treballadors: 10.0.0.0/24
 - Servidors: 10.0.255.0/24

○ Madrid:

- Accés d'1 Gb (cabal de 300 Mbps)
- Dues xarxes:
 - Treballadors: 10.0.1.0/24
 - Servidors redundants: 10.0.254.0/24

○ Seus remotes:

- Direccionament 10.0.x.0/24¹
- Accés WAN de 10 Mb simètrics

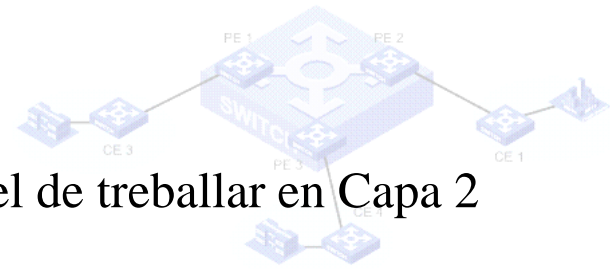
¹ Direccionament disponible a la memòria: Taula 1 – Direccionament LAN



TECNOLOGIA

○ VPN sobre VPLS:

- Treballa en Capa 2 del model OSI
- Combina els avantatges de la MPLS amb el de treballar en Capa 2



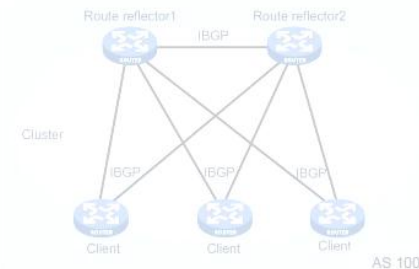
○ Equipament Cisco:

- Àmplia experiència i líder en el sector de les telecomunicacions
- CLI de Cisco senzill i intuïtiu
- 3 routers Cisco 7206VRX per a les seus principals
- 50 routers Cisco 2621XM per a les seus remotes



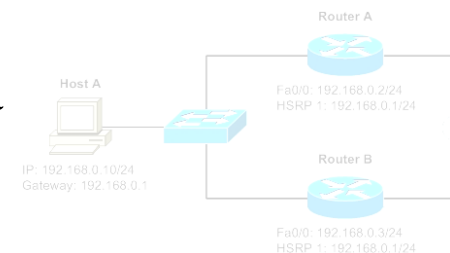
○ Protocol d'enrutament:

- BGP (iBGP), AS 100
- Creació de 2 Route Reflector (RR)

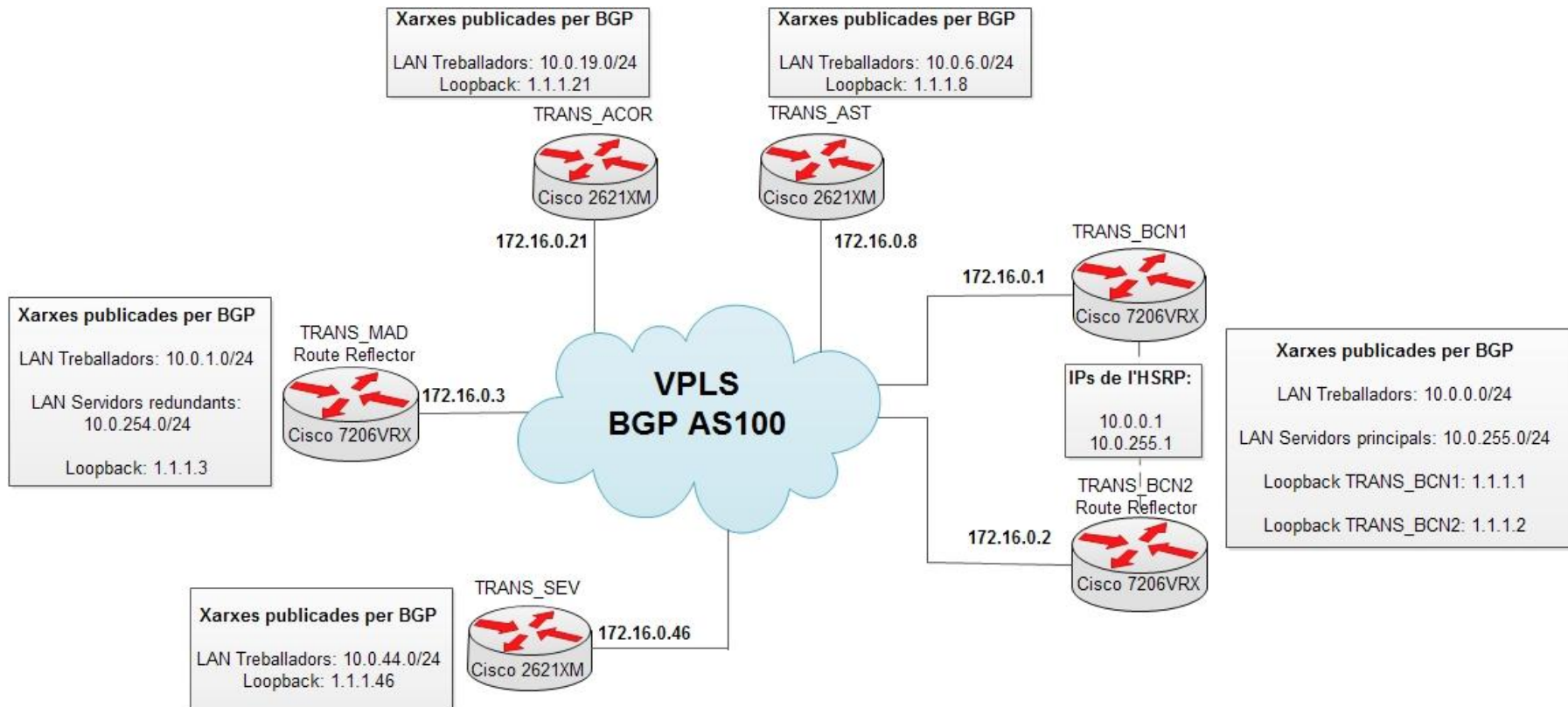


○ Protocol de redundància:

- HSRP (propietat de Cisco) en la seu de Barcelona



ESQUEMA REPRESENTATIU DE LA XARXA



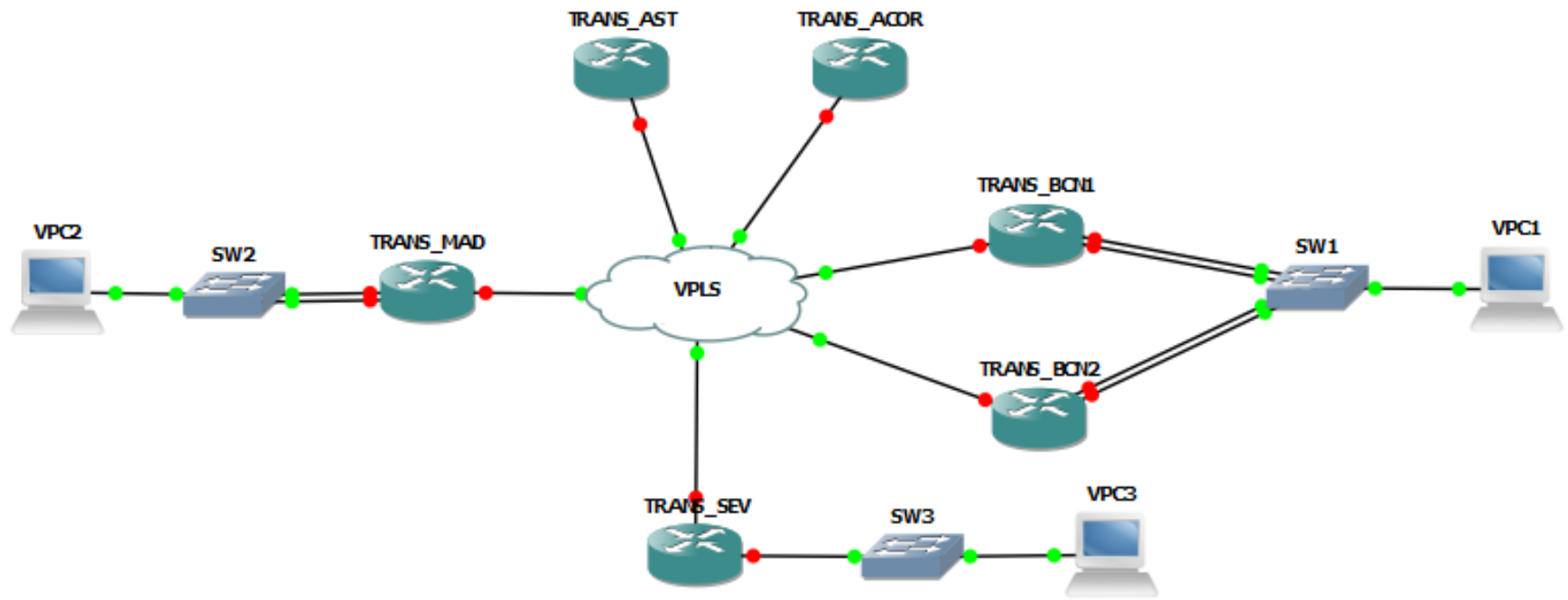
○ Topologia representativa de 5 seus de la xarxa VPN:

- Barcelona → 2 x Cisco 7206VRX
- Madrid → 1 x Cisco 7206VRX
- Astúries → 1 x Cisco 2621XM
- A Corunya → 1 x Cisco 2621XM
- Sevilla → 1 x Cisco 2621XM



EMULACIÓ AMB GNS3

○ Topologia creada al GNS 3:



- VPC: Virtual PC per realitzar comprovacions de LAN a LAN
- VPLS: S'afegeix un *switch* per a simular la VPLS
- Configuració dels routers:
 - Seus centrals → Disponible a l'Annex de la memòria
 - Seus remotes → Auto plantilla: <http://goo.gl/28nhZx>
- Vídeo amb la creació de la topologia: <http://youtu.be/KmdMp7RZFx0>



EMULACIÓ AMB GNS3

○ Comprovacions de la xarxa amb un funcionament normal:

1- Router principal de Barcelona actiu:

```
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
```

2- Track vinculat a l'HSRP de Barcelona:

```
TRANS_BCN1#show track
Track 1
  List boolean or
  Boolean OR is Down
    1 change, last change 00:03:13
  Tracked by:
    HSRP GigabitEthernet1/0 10
    HSRP GigabitEthernet2/0 20
Track 2
  Response Time Reporter 1 reachability
  Reachability is Up
    2 changes, last change 00:01:54
  Delay up 8 secs, down 8 secs
  Latest operation return code: OK
  Latest RTT (milliseconds) 36
Track 3
  Response Time Reporter 2 reachability
  Reachability is Up
    2 changes, last change 00:00:14
  Delay up 8 secs, down 8 secs
  Latest operation return code: OK
  Latest RTT (milliseconds) 115
```

3- Taula de rutes d'una seu remota:

```
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
```

○ Vídeo de les proves: <http://youtu.be/t45N3bcSNUA>



EMULACIÓ AMB GNS3

○ Caiguda LAN del router TRANS_BCN1. Actuació de l'HSRP:

1- *Shutdown* a les interfícies LAN:

```
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
```

2- Estat de l'HSRP dels routers de Barcelona:

```
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
```

3- Taula de rutes d'una seu remota amb TRANS_BCN2 actiu:

```
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

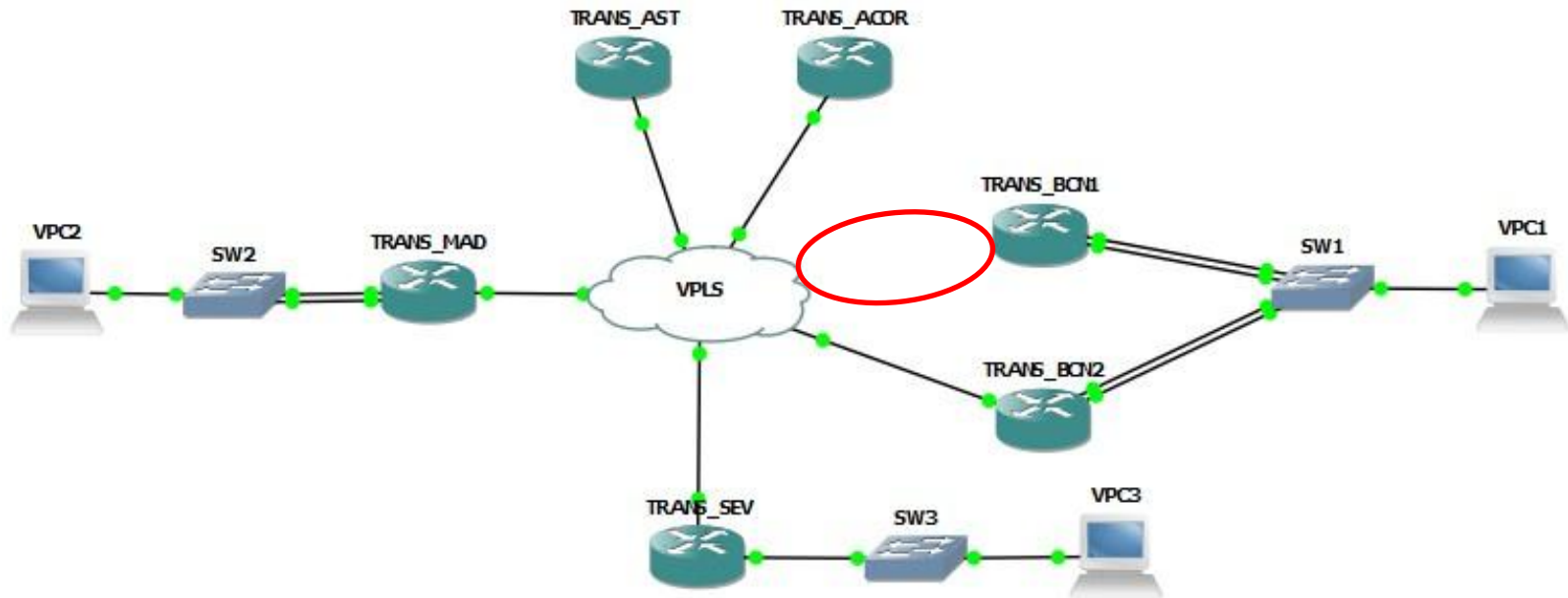
1.0.0.0/32 is subnetted, 6 subnets
B 1.1.1.1 [200/0] via 172.16.0.1, 00:32:53
B 1.1.1.3 [200/0] via 172.16.0.3, 00:32:52
B 1.1.1.2 [200/0] via 172.16.0.2, 00:32:53
B 1.1.1.8 [200/0] via 172.16.0.8, 00:32:53
B 1.1.1.21 [200/0] via 172.16.0.21, 00:20:04
C 1.1.1.46 is directly connected, Loopback0
C 172.16.0.0/25 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
```

○ Vídeo de les proves: <http://youtu.be/1Dpkap8gJGg>

EMULACIÓ AMB GNS3

○ Caiguda de l'accés WAN principal de Barcelona. Actuació HSRP i tracks:

1- S'elimina l'accés principal de Barcelona:



EMULACIÓ AMB GNS3

○ Caiguda de l'accés WAN principal de Barcelona. Actuació HSRP i tracks:

2- Router principal de Barcelona en mode Standby:

```
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
```

3- Router redundant de Barcelona actiu:

```
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
```

4- Taula de rutes d'una seu remota amb TRANS_BCN2 actiu:

```
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
```

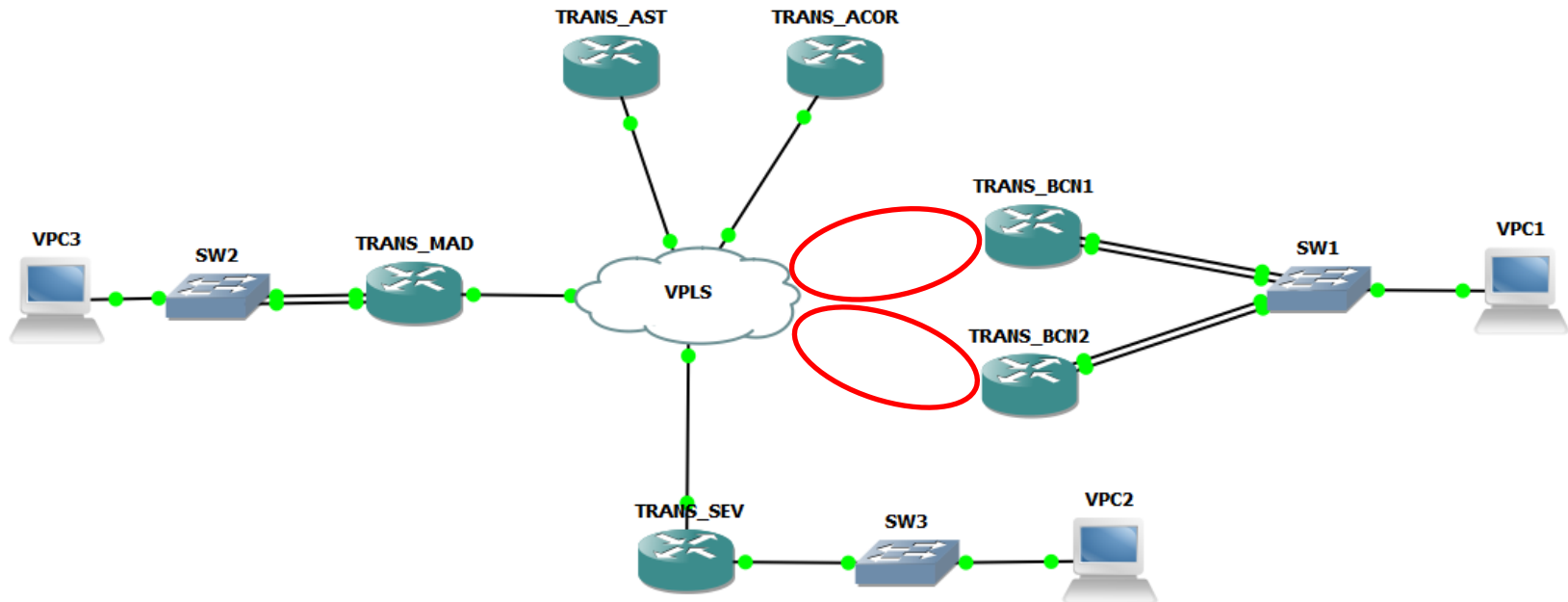
○ Vídeo de les proves: <http://youtu.be/1BndSfn4UOI>



EMULACIÓ AMB GNS3

○ Incomunicació total de la seu de Barcelona:

1- S'elimina els dos enllaços WAN de Barcelona:



EMULACIÓ AMB GNS3

o Incomunicació total de la seu de Barcelona:

2- La xarxa continua treballant amb un sol RR (TRANS_MAD):

```
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    00:02:27 Active
172.16.0.3    4 100    278    260     32    0    00:42:16 9
```

3- Els servidors de l'empresa continuaran funcionant a través d'una ruta estàtica de la seu de Madrid:

```
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
```

4- Taula de rutes d'una seu remota:

```
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
```

o Vídeo de les proves: <http://youtu.be/Ez5pnAc9Vys>

EMULACIÓ AMB GNS3

○ Restricció de l'accés per Telnet als routers:

- Accés permès únicament des de la IP 10.0.0.200:

1- Es configura el PC amb la IP 10.0.0.10. Telnet denegat:

```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Jose>telnet 1.1.1.1
Conectándose a 1.1.1.1...No se puede abrir la conexión al host, en puerto 23: Er
ror en la conexión

C:\Users\Jose>
```

2- Es configura el PC amb la IP 10.0.0.200. Telnet permès:

```
Telnet 1.1.1.1

User Access Verification
Username: uoc
Password:
TRANS_BCN1#en
Password:
TRANS_BCN1#show ip interface brief
Interface          IP-Address      OK? Method Status  Prot
Ethernet0/0        unassigned      YES NURAM  administratively down down
GigabitEthernet0/0 172.16.0.1      YES NURAM  up      up
GigabitEthernet1/0 10.0.0.2        YES NURAM  up      up
GigabitEthernet2/0 10.0.255.2     YES NURAM  up      up
Loopback0          1.1.1.1         YES NURAM  up      up
TRANS_BCN1#
```

3- Comptador ACL 100. Telnet permès:

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

- Possibilitat de realitzar Telnet a les IP de WAN o *Loopback*

○ Vídeo de les proves: <http://youtu.be/45L-P8EIZa4>



EMULACIÓ AMB GNS3

○ Limitació de l'ample de banda:

- Es limita l'ample de banda entre Barcelona i Madrid a 100 Mbps
- S'utilitza l'ACL 110 per a detectar l'origen i el destí del paquet
- L'ACL 110 està vinculada a un *Rate-Limit* de 100 Mbps

1- Prova amb origen 10.0.0.0/24 i destí 10.0.1.0/24 i viceversa de 100 paquets:

```
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
```

- Vídeo de les proves: <http://youtu.be/UcPgXffZbMw>



PRESSUPOST

○ Taules resum del pressupost:

- Preu 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 €

- 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 €

* Preus genèrics dels operadors al mercat espanyol i sense descompte (vinculats a la permanència)

VIABILITAT I CONCLUSIONS DEL PROJECTE

- Solució tecnològica viable
- Necessitats de Transports Express S.A. cobertes
- VPN sobre VPLS, tecnologia d'avantguarda
- Xarxa amb privacitat i preparada per a futures expansions
- Projecte extrapolable a la realitat





Gràcies per la seva atenció

