Escola Universitària
Politècnica de Mataró

Centre adscrit a:

UNIVERSITAT POLITÈCNICA
DE CATALUNYA

Ingeniería técnica de telecomunicaciones especialidad telemática

RED DE FERIA DE VALENCIA

HèctorLlovetArraut
PONENT: PERE BARBARAN

PRIMAVERA 2012

TecnoCampus
Mataró-Maresme

Dedicatoria

El trabajo esta dedicado a mis padres. Por insistir, por no dejarme nunca atrás y enseñarme cada día. A mis amigos a los que están ahora y los que perdí con los años.

Además agradecer a mis compañeros de trabajo por ayudarme en el proyecto.

Y a mi novia por soportarme en estos días de proyecto.

Resum

L'objectiu d'aquest projecte és realitzar el disseny de xarxa dels nous recintes de Fira de València. En aquest document s'especificarà les necessitats de xarxa.

Un cop coneguem l'escenari explicarem la topologia lògica, topologia física, encaminament de la xarxa i els components físics que utilitzarem.

Per acabar el treball s'exposarà la conclusió i el pressupost del projecte.

A més s'ha realitzat una pràctica ambGNS3explicant els enllaços d'alguns dels equips, per a una millor comprensió del enrutament dels protocols.

Resumen

El objetivo de este proyecto es realizar el diseño de red de los nuevos recintos de Feria de Valencia. En este documento se especificaran las necesidades de red.

Una vez conozcamos el escenario explicaremos la topología lógica, topología física, enrutamientos de la red y los componentes físicos que utilizaremos.

Para terminar el trabajo se expondrá la conclusión y el presupuesto del proyecto.

Además se ha realizado una práctica con GNS3 explicando los enlaces de algunos de los equipos para una mejor comprensión del enrutamiento de los protocolos.

Abstract

The objective of this project is to implement a network design of the new buildings of Feria de Valencia .This document will specify the necessities of the network.

Once we get to know the scene, we will explain the logic topology, physic topology, routing network, and the physical components that are going to be used.

To end the project, we will present a conclusion and a budget.

Also, there has been held a practice with GNS3 explaining the links of some of the equipment. This has been done for a better comprehension of the protocols.

Índice.

Índice de figuras.

Índice de tablas.

Glosario de términos.

PLC	Programable Logic Communications
MPLS	MultiProtocol Label Switching
LPD	Label Distribution Protocol
VPRN	Red privada virtual enrutado
VRF	Virtual Routing and Forwarding
BGP	Border Gateway Protocol
MP-BGP	MultiProtocol Border Gateway Protocol
PE	Provider Edge
CE	Costumer Edge
IP	INTERNET Protocol
VLAN	Virtual Local Area Network
EIGRP	ºEnhanced Interior Gateway Protocol
OSPF	Open Shortest Path First
Building Block	Pack de switches
MTU	Maximum Transfer Unit
Algi	Operadora de INTERNET (Orange)
Colt	Operadora de INTERNET
VSS	Virtual Switching Systems
VSL	Virtual Switch Link
Routers LSR	Label Switch Router
LDP	Label Distribution Protocol
GNS3	Simulador grafico de red
TCP	Transmisión Control Protocol

IOS	INTERNET working Operating System
VTP	Vlan Trunking Protocol
SVI	Switching Virtual Interface
ISP	INTERNET Service Provider
NAT	Network Address Translation

1. Introducción.

Para comenzar, es importante citar los momentos más destacados de INTERNET a nivel de la historia.

INTERNET o mejor dicho, la red, nació en 1969 en el departamento de Defensa de Estados Unidos. El objetivo básico era que los ordenadores conectados en la misma red tuvieran comunicación (peer-to peer).

A partir de 1972 se introdujeron los sistemas de correo eléctrico lo cual supuso un salto a la actividad de usuarios, permitiendo la interrelación entre unos y otros.

Durante los años 80 aparecieron las redes locales en las universidades y centros de investigación.

Hoy en día todas las empresas tienen su propio sistema de correo, su propia base de datos, etc...Por ello la comunicación vía red es primordial para el desarrollo del trabajo.

El ayuntamiento de Valencia ha realizado la construcción de unos recintos para poder realizar ferias y, poder convertirse en un referente europeo para las celebraciones de congresos y salones.

Realizaremos una auditoria del escenario y se propondrá la solución. Dicha solución se expondrá a lo largo de este proyecto. El desglosamiento general sería:

-Esquema lógico.

-Esquema Físicos.

-Componentes Físicos que utilizaremos.

-Enrutamientos.

-Presupuestos.

2. Objetivos.

Teniendo la idea expuesta con anterioridad, el objetivo de este proyecto será desarrollar dicha auditoria y poder dar la mejor solución para la integración de las nuevas tecnologías aprovechando el rendimiento de los equipos Cisco.

La empresa CISCO está reconocida mundialmente y ofrece fiabilidad y seguridad de los equipos.

Implementaremos una red MPLS-VPN en este escenario para dotarla de alta disponibilidad, para protegerla de un fallo que pueda afectar a todos los usuarios de Feria.

Los equipos más importantes estarán físicamente redundados para evitar que la avería de un dispositivo pueda provocar la pérdida de red en la Feria de Valencia.

En este proyecto se ha dado especial importancia a las redundancias para asegurar lo máximo posible las conexiones de red. En Feria de Valencia, donde se realizaran eventos es primordial tener la máxima seguridad.

3. Escenario.

Feria de Valencia quiere atraer más turismo a la ciudad. En ella quieren poder dar servicio a todo tipo de exposiciones: Salón náutico, de alimentación, Coches y, además de esto, poder dar lugar a diversas conferencias. Con la construcción, necesitan un proyecto específico de red para poder dar soporte a los expositores y las oficinas.

Los expositores serán las personas que mostrarán su producto en un stand durante los salones. Tendrán la posibilidad de contratar el servicio de INTERNET y para ello, contarán con un catalogo de 1Mb, 2MB, 4MB y 8MB. Estos anchos de banda serán simétricos, es decir, tendrán lo mismo de descarga que de subida de datos.

En las oficinas residirá el personal de Feria. Estos no tendrán limitaciones del ancho de banda para el mejor rendimiento de su trabajo y así, poder descargar los archivos con mayor velocidad.

Estas 2 redes serán primordiales en Feria de Valencia, por ello las separaremos.

Para todas las Feria hay disponible 4 palacios. Estos 4 palacios están separados en dos sedes, es decir, no están juntos, las sucursales serán:

1. Valencia.

2. Paterna.

Tendremos 4 palacios, 1 de ellos será utilizado como oficinas para el personal de Feria. Los otros 3 palacios se utilizarán exclusivamente para salones. Estos palacios ya disponen de:

- **Baños:** para los expositores y visitantes de los salones,…

- **Restaurantes:** para que el personal pueda comer sin necesidad de salir del recinto.

- **Puertas:** Hay 2 tipos de puertas. Una para entrada y salida del personal de la feria y otra para la entrada y salida de camiones. Son lo suficientemente grandes para que no tengan problemas de accesibilidad.

- **Internet:** En los Palacios 1, 2 y 3 instalaremos las líneas de red de expositores (1MB, 2MB, 4MB y 8MB). Además dispondremos de tomas de red fijas para las cámaras, TPVs y PLCs.

Como antes se ha dicho, la Feria está dividida en 2 sucursales: Valencia y Paterna.

3.1. Descripción de la sucursal de Valencia

La primera sucursal está en Valencia. Dispone de 2 palacios: un palacio para oficinas y otro para las ferias.

-**Palacio Oficinas** tiene 3 plantas:

Primera planta: Departamento comercial y departamento de acreditaciones

- **Departamento comercial:** Realizan las ventas de los expositores, mesas, sillas, cuadros eléctricos,…incluyendo la venta de líneas de INTERNET.

- **Departamento de acreditaciones:** Estarán divididos en dos equipos. Uno prestará el servicio en recepción, encargado de la venta de tickets. El otro estará pendiente de la atención al cliente. Pertenecerán a la red de oficinas.

En **la segunda planta** están los departamentos de “Eventplanning”y “Exhibitor Project”:

- **Departamento “Eventplanning”:** responsable de solucionar las peticiones de los organizadores de las ferias. Ejemplo: Contratación de auditorios, autocares,..

- **“Exhibitor Project”:** Departamento que dispone de personal que presta el soporte de control y vigilancia a petición del cliente.

En **la tercera planta** trabaja el departamento de proveedores:

- **Departamento Proveedores:** Empresas externas dedicadas a una parcela especifica de una Feria.

- **Cámaras:** La empresa VIGIT. Encargada de controlar las cámaras de los recintos. Necesitarán una red propia para poder controlar y vigilar las cámaras. Esta no tendrá acceso a INTERNET.

- **Controles eléctricos PLC:** La empresa ENDESA controlará la electricidad de los palacios. Estos PLC disponen de una toma de red para que desde "control" puedan verificar si la corriente esta activada. Por ello necesitarán una red privada e interna.

- **TPV restaurantes:** Los restaurantes esparcidos por los palacios necesitan de TPV para realizar las facturas de los clientes. Las TPV de los restaurantes se les configura una red interna para que puedan realizar las facturas.

- **Sistemas:** SISTEM, empresa responsable de los servidores (correo, base de datos,…) y asistencia al usuario.

- **Comunicaciones:** Nuestra empresa realizará tareas de configuración de líneas, administración de la red y monitorización de los equipos.

En este palacio o edificio las tomas de red estarán distribuidas por las plantas.

Palacio 1 de la sucursal de Valencia:

Ideado exclusivamente para albergar las ferias, en total tendrá 13.400m^2.Se han construido 2 entradas. Una de las entradas se utilizará para los camiones, la otra será para la entrada y salida de los visitantes. Los baños estarán uno en cada esquina del palacio, es decir, tendremos 2 baños en el palacio 1. Además, para los salones se pondrá en funcionamiento el restaurante. Como hemos comentado antes, los expositores podrán contratar líneas de INTERNET. En este Palacio las tomas de red estarán instaladas en las columnas para poder facilitar al técnico la instalación de la línea ya que el cableado hasta los switches, será por las columnas. Distribución de las líneas de red:

-**TPVs:** Como tendremos un restaurante instalaremos 2 líneas de TPVs.

-**PLCs:** Se instalaran 5 líneas para el control de electricidad.

-**Cámaras:** 10 líneas para realizar la vigilancia y controlar el Palacio.

-**Expositores:** Se prevé que tendrá una capacidad máxima de 70 stands. Se calcula aproximadamente la instalación de 150 líneas.

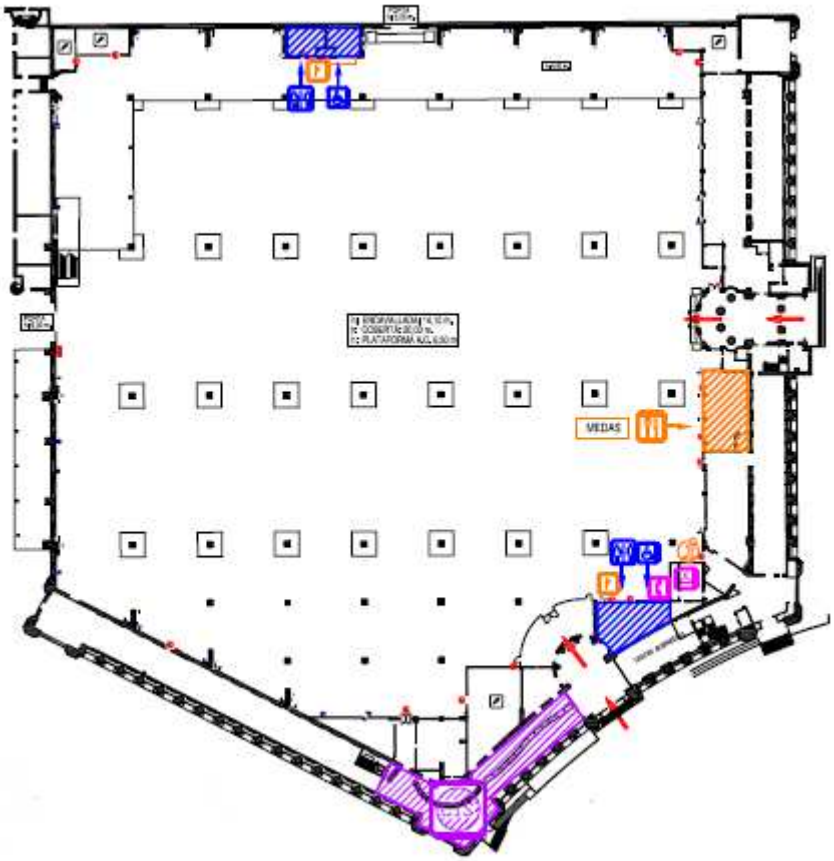


Fig. 3.1. Plano General del Palacio 1.

3.2 Descripción de la sucursal de Paterna

La sucursal 2 de Paterna esta destinada exclusivamente para ferias ya que esta se encuentra mucho mejor preparada que el Palacio 1 de Valencia.

El Palacio 2

El palacio 2 dispone de 2 niveles:

- **En el Nivel 0:**

Dispone de 23.400m^2. El segundo palacio con más m^2. Hay construidas 9 puertas. Dos de ellas se destinarán a la entrada y salida del personal del salón y las demás para la entrada y salida de los camiones. Él nivel 0 tiene 4 baños y 4 restaurantes. En este palacio las tomas de red se ubicarán en las arquetas ya que dispone de galerías subterráneas por donde pasará el cableado. Distribución de las líneas de red:

-**TPVs:** Como tendremos un restaurante instalaremos 8 líneas de TPVs.

-**PLCs:** Se instalaran 8 líneas para el control de electricidad.

-**Cámaras:** 15 líneas para realizar la vigilancia y control del Palacio

-**Expositores:** Se prevé que tendrá una capacidad máxima de 120 stands. Se calcula aproximadamente la instalación de 200 líneas.

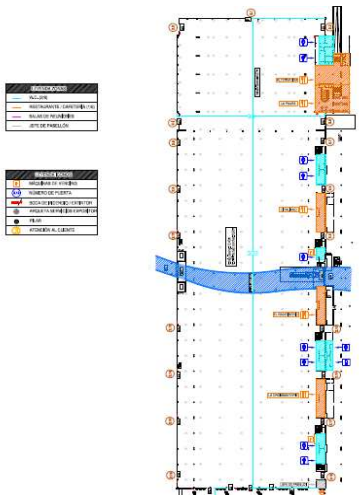


Fig. 3.2. Plano General del Palacio 2 nivel 0

- **Nivel 1:**

A diferencia de los otros palacios, este nivel contiene un auditorio para realizar conferencias y 4 salas para las reuniones y/o para personal de Feria de Valencia. Este nivel incluye un restaurante y 2 baños. Las tomas están distribuidas por las salas, auditorio y restaurantes. . Distribución de las líneas de red:

-**TPVs:** Como tendremos un restaurante instalaremos 4 líneas de TPVs.

-**PLCs:** Se instalarán 5 líneas para el control de electricidad.

-**Cámaras:** 6 líneas para realizar la vigilancia y control del Palacio

-**Expositores:** Dispone de 3 salas. En cada sala de reunión habrán 4 tomas de red. En el auditorio en total se instalarán 10 tomas de red. Además coloraremos tomas esparcidas por el nivel por futuros mostradores.

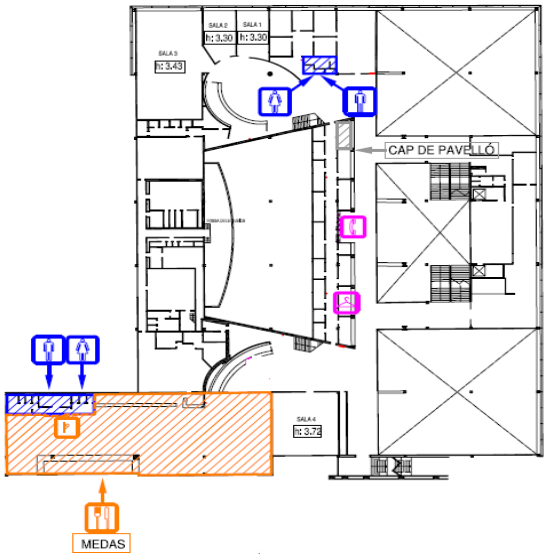


Fig. 3.3. Plano General del Palacio 2 nivel 1

El Palacio 3

El más grande de todos los palacios 43.000m^2. Tendrá accesibilidad a 6 restaurantes y 6 baños. Igual que el palacio 2, dispone de puertas grandes para la entrada de los camiones. En este palacio las tomas de red serán accesibles por arquetas ya que también dispone de galerías como el Palacio 2. . Distribución de las líneas de red:

-**TPVs:** Como tendremos un restaurante instalaremos 12 líneas de TPVs.

-**PLCs:** Se instalarán 16 líneas para el control de electricidad.

-**Cámaras:** 25 líneas para realizar la vigilancia y control del Palacio

-**Expositores:** Se prevé que tendrá una capacidad máxima de 220 stands. Se calcula la instalación de un promedio de 300 líneas.

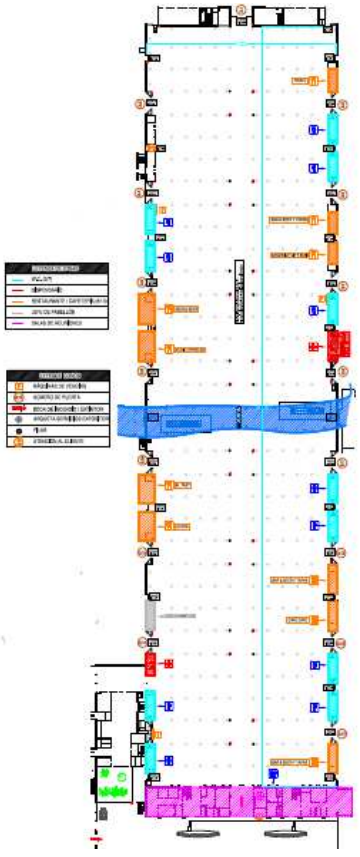


Fig. 3.4. Plano General del Palacio 3.

4. Entorno tecnológico de la red Feria de Valencia.

En este punto se comentarán los protocolos que más tarde se van a usar para el proyecto. Tras realizar un estudio de los demás tecnologías se ha escogido el protoco MPLS por las ventajas ofrecidas.

-**Escalabilidad:** Con el diseño MPLS la red podrá ir creciendo (más direcciones IP).

-**Transmisión de datos:** MPLS es más rápida y eficiente respecto (gracias al protocolo LDP) a otros ya que descongestiona la red. A diferencia de las vlans que realizan broadcast.

-**Rendimiento Mejorado: S**e podrán reducir el número de saltos entre los puntos. Mejorará los tiempos de respuesta y rendimiento de las aplicaciones.

-**VPN:** Permite un mecanismo sencillo y flexible para crear VPN.

-**QOS:** capacidad de integrar voz, video y datos con garantías.

4.1. Conceptos MPLS UNICAST.

MPLS UNICAST (enviamos 1 dirección IP): se basa en enviar paquetes mediante un sistema de etiquetado. Esto quiere decir que dentro del área MPLS enviaremos los paquetes utilizando las etiquetas y no direcciones IPs. Para realizar este proceso debemos asociar una dirección IP a una etiqueta. Los protocolos utilizados en nuestro proyecto para realizar esta asociación son OSPF (protocolo de routing, “conocer ips y las rutas para llegar a ellas”) y LDP (protocolo para intercambiar etiquetas dentro de la MPLS).

Proceso envío paquetes

Como hemos comentado, el envío mediante etiquetas se realiza dentro del área MPLS, lo cual quiere decir que el PC de un usuario final no enviará los paquetes utilizando etiquetas sinó IPs. Por lo tanto ha de haber un dispositivo (router) que inserte la etiqueta en la cabecera del paquete cuando entremos en el área MPLS. Este proceso recibe el nombre de PUSH y dicho router debe asociar una etiqueta a la IP de destino. A continuación los paquetes se enviarán mediante la etiqueta de su cabecera. El protocolo para conocer e

intercambiar etiquetas de los vecinos MPLS utilizado es LDP (a grandes rasgos LDP se encarga de conocer las etiquetas de los vecinos y asegurar que no estén repetidas en diferentes vecinos). Finalmente cuando el paquete sale del área MPLS el último dispositivo debe desfragmentarlo y eliminar de la cabera la etiqueta. A partir de este punto ya se utilizan direcciones IPs. La siguiente Fig. 4.1 muestra el proceso descrito:

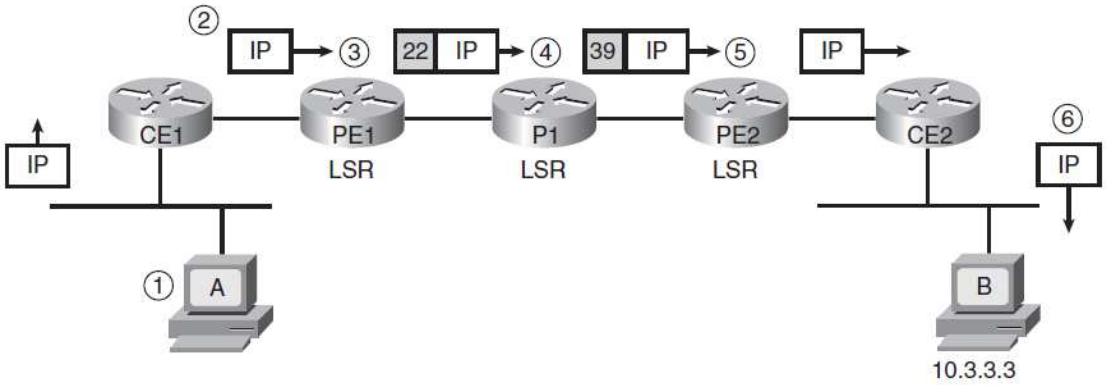


Fig.4.1. Ejemplo de vecindad MPLS con LDP.

4.2. MPLS VPN

Una de las aplicaciones más importantes y utilizadas de una red MPLS es la llamada MPLS VPN (*Virtual Private Network MPLS*). MPLS VPN proporciona direccionamientos privados e independientes entre sí. Por ejemplo, supongamos que un proveedor de servicios de Internet tiene diferentes clientes, los clientes de una entidad en concreto no desearán que su direccionamiento sea conocido por otro cliente del proveedor. Con MPLS VPN cada cliente es totalmente anónimo y privado para otro y su enrutamiento desconocido. Sería lo que podríamos decir entornos de routing independientes. MPLS VPN consigue las diferentes tablas de routing mediante las llamadas VRFs (*Virtual Routing and Forwarding*). Cada cliente tendría asignado su VRF y por lo tanto su propia tabla de enrutamiento. Al tratarse de tablas de routing independientes y privadas podemos duplicar IPs mientras éstas no se encuentren dentro de la misma VRF. Este hecho es una gran ventaja si lo comparamos con otro tipo de redes.

MPLS utiliza tres términos para describir el rol de los equipos que forman parte de una red MPLS.

CE (*Customer Edge*) → Dispositivo que se encuentra fuera de la MPLS y por lo tanto no utiliza sistema de etiquetado (generalmente es el cliente de un ISP).

PE (*Provider Edge*) → Equipo que comparte al menos un link con un CE y otro dentro de la MPLS. Se encargan de introducir las VRFs y realizar las funciones de PUSH y POP.

P (*Provider*) → Router que estaría totalmente dentro de la MPLS. No tendría ningún link conectado a un CE.

Entre los dispositivos del tipo P y PE se realiza el MPLS Unicast y como hemos comentado anteriormente utilizaremos el protocolo de routing OSPF y LDP para asociar etiquetas con IPs. El direccionamiento del OSPF no sería el de los clientes, síno el de los diferentes elementos de la MPLS, por lo tanto este no es el de los diferentes clientes.

Por otra parte el PE debe aprender las rutas del CE, por lo tanto las rutas de los clientes. Estas rutas aprendidas por el PE se deben intercambiarse con otros PE. Para ellos se utiliza el protocolo de routing BGP. BGP nos permite establecer vecinos sin que éstos estén directamente conectados e intercambiar las diferentes rutas (siempre y cuando un vecino BGP sepa como llegar hasta otro) Como internamente dentro de nuestra red MPLS hemos utilizado OSPF todos los PEs de nuestra red podrán formar vecindad BGP con otros PEs e intercambiar las rutas de los clientes.

4.3. Esquema de redes MPLS VPN aplicado a la red de Feria.

Después de visualizar el escenario, creemos que la tecnología más viable para el proyecto de red es MPLS VPN, ya que nos permitirá separar las redes de Feria. Las redes vrf de Feria serán:

-**Vrf OFICINAS:** Dedicada al personal de Feria y a los servidores. Donde también integraremos en la misma red el servidor DHCP.

-**Vrf EXPOSITORES:** Dedicada a los expositores. El servidor DHCP serán los equipos de Distribución (lo comentaremos más adelante).

-**Vrf CAMARAS:** Dedica a la red de vigilancia. IPs estáticas; no tendrá servidor DHCP.

-**Vrf PLC:** Dedica a la red eléctrica. IPs estáticas; no tendrá servidor DHCP.

-**Vrf TPV:** Dedica a la red restaurantes. IPs estáticas; no tendrá servidor DHCP

5. Esquema general de la red.

En los siguientes puntos de la memoria, explicaremos los equipos que se utilizarán. En el punto número 7 explicaremos por apartados el funcionamiento lógico de los equipos. Estos apartados se dividirán en “Building blocks”. Como muestra, en la Fig. 5.1. cada “building block” será representado con un color. Además, en cada apartado realizaremos una demostración del funcionamiento de la red.

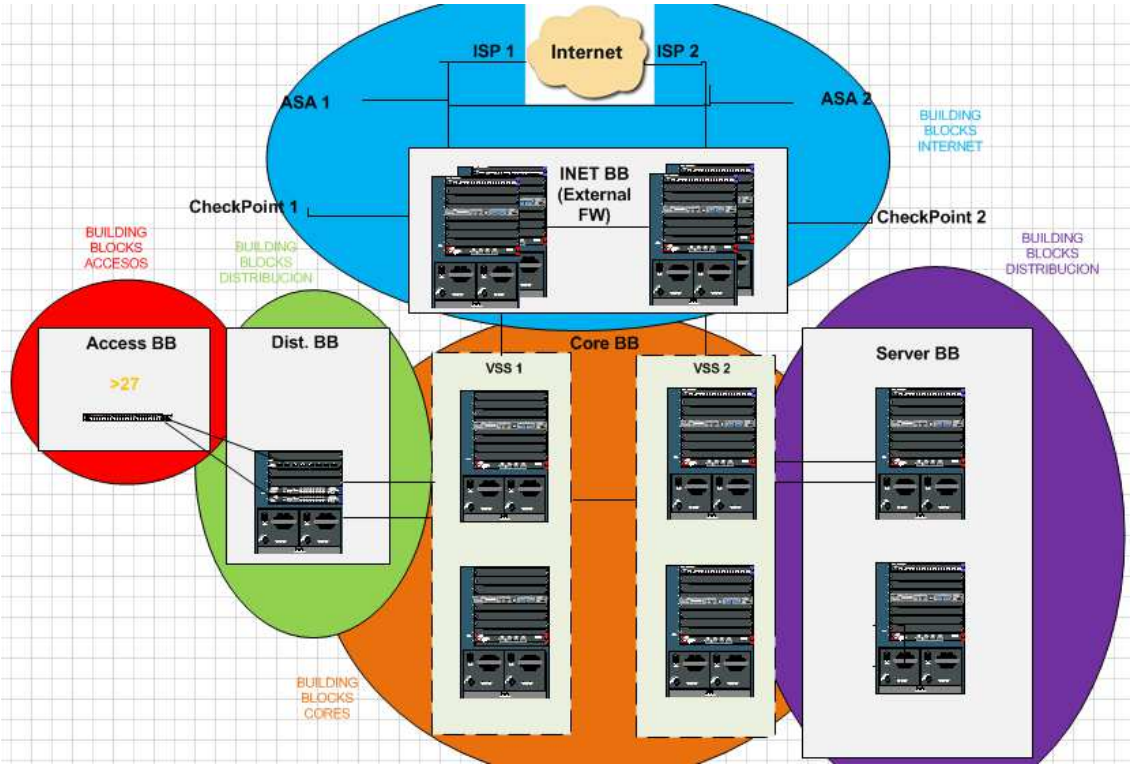


Fig. 5.1. Estructura física de la red.

6. Esquema lógico de la red.

En este apartado se explicaran las conexiones lógicas de los equipos.

Lo dividiremos en 2 partes. En la primera se explicará el comportamiento lógico de la red y la segunda parte realizaremos un esquema parecido con la aplicación GNS3.

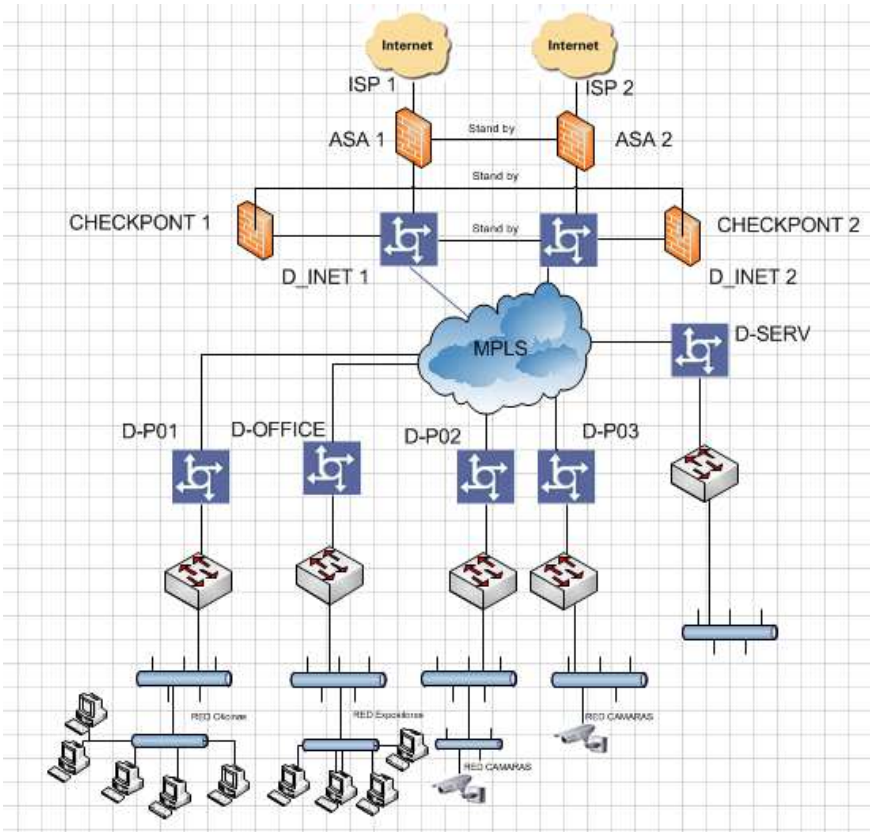


Fig. 6.1. Esquema lógico de la Red Feria de Valencia

6.1 Esquema lógico de los equipos.

En los siguientes apartados iremos explicando los enrutamientos de la red.

Se dividirá la Feria de Valencia en 4 Áreas. El área 0 será CORES, Distribuciones de INTERNET será Área 2; el área 1 será Valencia y área 3 será Paterna. En el protocolo OSPF, es necesario que todas las áreas tengan vecindad con área 0 (llamada área backbone).

En el punto número 4 hemos explicado los routers CE, PE y P. En nuestro esquema Building blocks CORES serán nuestros routers P y Building block Distribuciones, INTERNET y SERVIDORES serán los routers PE.

6.1.1 Esquema lógico de los CORES.

Recordemos que tenemos 2 sedes en las que necesitaremos que los equipos puedan intercambiar una gran cantidad de paquetes. Para definir el tamaño de paquetes se utiliza MTU (*Maximum Transfer Unit).* En nuestro proyecto utilizaremos una operadora de telecomunicaciones para poder realizar la conexión entre Valencia y Paterna.

Los CORE 1-A, CORE1-B y CORE 2-A, CORES2-B se unirán por dos enlaces físicos y así poder comportarse como una unidad lógica. Utilizaremos la tecnología de virtualización VSS1440. Así el CORE1 y CORE 2 podrán tener una mayor carga de datos.

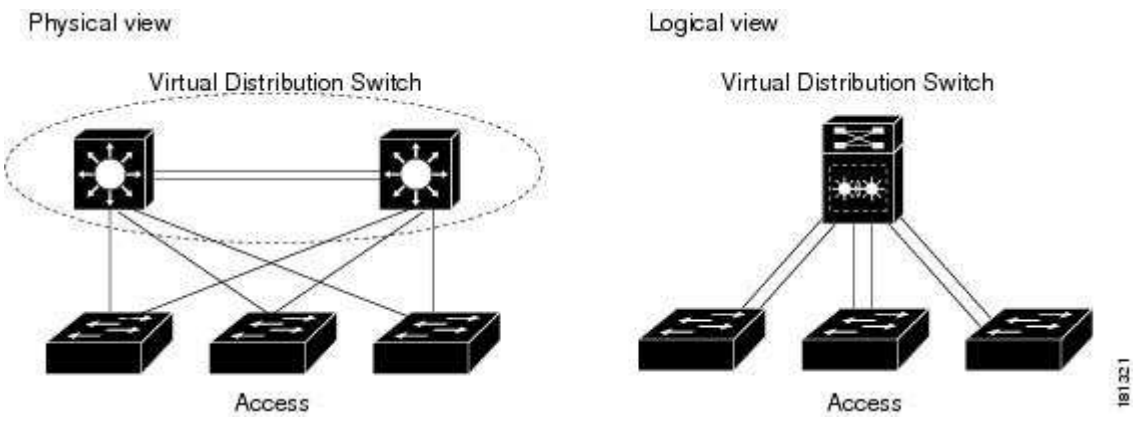


Fig. 6.2. Esquema VSS

Los beneficios VSS aumentan la eficacia operativa mediante la simplificación de la red. Los 2 switches dispondrán de solo una IP de gestión en lugar de 2 IPs lo cual facilitará la administración de la red. Los dos chasis de la VSS, se convertirán en una sola unidad para que actúe como un solo elemento de red y así, balancear el tráfico de datos.

El enlace del conmutador virtual (VSL "*Virtual Switch Link*") es un vínculo especial que lleva el control del tráfico y los datos entre los dos chasis de VSS. El VSL se implementa como un EtherChannel con hasta ocho enlaces. El VSL da prioridad al tráfico de datos para que los mensajes de control nunca se descarten. El tráfico de datos es equilibrado por la carga entre los enlaces de la VSL EtherChannel de balanceo de carga algorítmica.

Ejemplo de configuración VSS:

```
interface TenGigabitEthernet2/5/4
description VIRTUAL LINK 2
nosw
noip address
mlsqos trust cos
channel-group 2 mode on
end
interface Port-channel2
noswitchport
noip address
switch virtual link 2
mlsqos trust cos
nomlsqos channel-consistency
end
```

Nuestro esquema de CORES sería como la Fig.6.3.

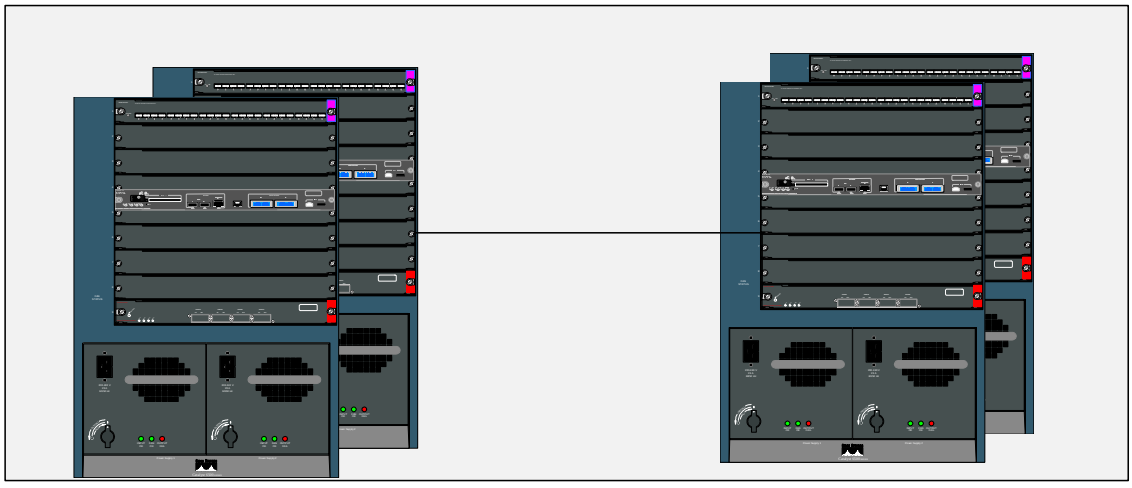


Fig. 6.3. Esquema de los CORES.

Para la conexión entre los CORES recordemos que se usara MPLS VPN. MPLS esta compuesta por routers LSR (*Label switch Router*) que serán nuestras CORES. Las tablas de enrutamiento se calcularán con un protocolo de enlace OSPF.

Además de esto, necesitaremos un protocolo de distribución de etiquetaje en las rutas. Utilizaremos el protocolo LDP (*Label Distribución Protocol*). Estos enlaces se comparan con las tablas de enrutamiento.

6.1.2 Esquema lógico de las Distribuciones de palacio.

En la red MPLS nuestros equipos de distribución realizarán la función de equipos PE.

Por ello declararemos las rutas OSPF en los Distribuciones para que los Distribuciones tengan conectividad. Solo tendremos un proceso para simplificar nuestra red.

Como en los CORES, creamos una interface loopback, forzaremos a que sea su identificativo en la gestión de los equipos. Se propagara por la red por OSPF.

En cambio BGP realizará tareas de enrutamiento de las redes VRF. Recordemos que BGP tendrá adyacencia gracias a la configuración del protocolo OSPF en los Distribuciones.

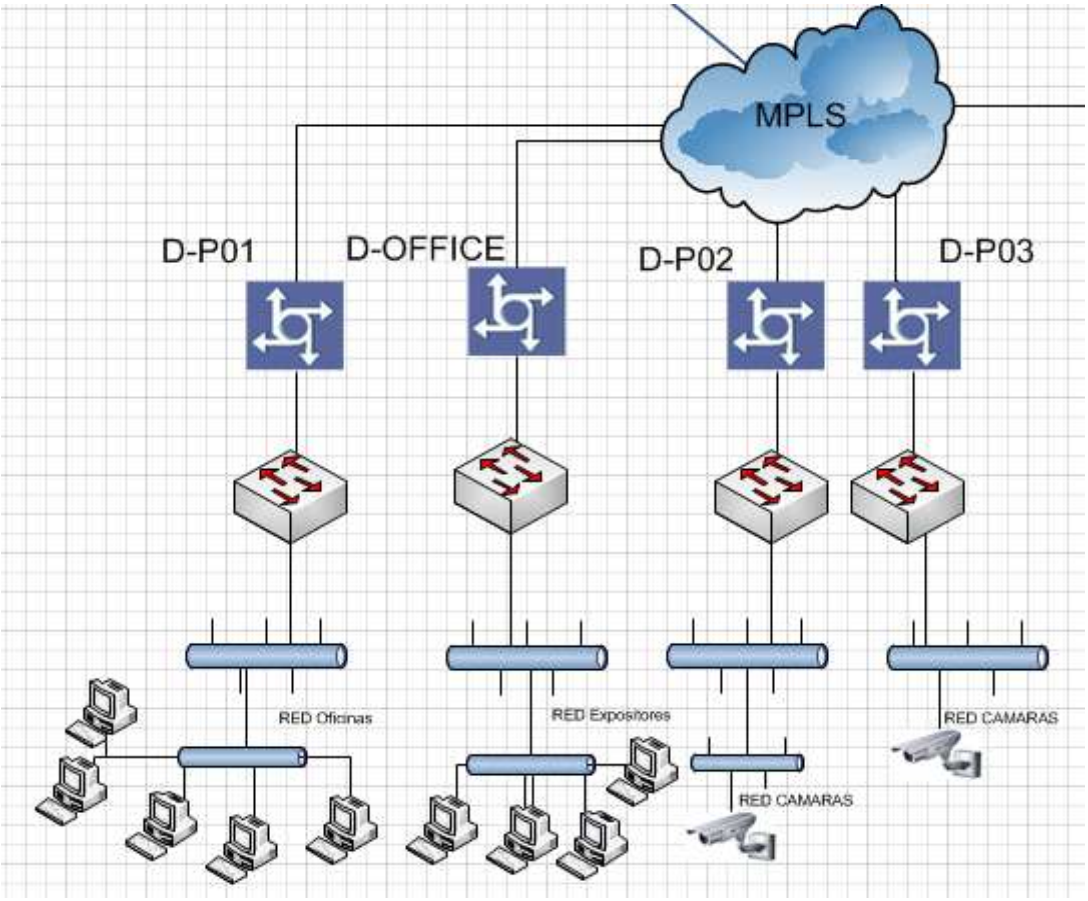


Fig. 6.4. Esquema lógico de los Distribuciones de los Palacios.

6.1.3 Esquema lógico de los Accesos.

Los Accesos trabajarán a nivel 2 (Capa de enlace) por ello no es necesario configurar un protocolo de routing. Solo se configurará una IP de nivel 3 para la gestión de la tecnología Switch virtual interface. Esta tecnología nos permitirá un nivel de capa 3 asociado a la VLAN. Sólo se asignará un SVI

Es decir, los Accesos están directamente configurados sin necesidad de ningún protocolo, sólo tendrán una ruta por defecto en la cual todo el tráfico estará dirigido al Distribución de cada palacio.

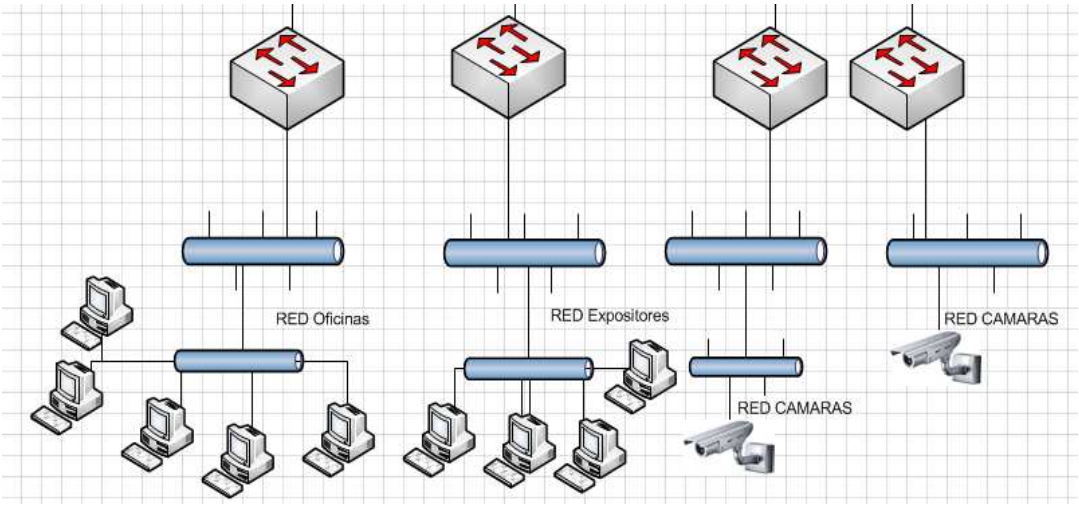


Fig. 6.5. Esquema lógico de los Accesos.

6.1.4 Esquema lógico de los equipos de INTERNET.

En la Fig. 6.6. visualizamos el esquema INTERNET. Se colocarán 2 equipos. Cada uno ubicado en su sucursal. Se hace esto para tener más disponibilidad, ya que si un equipo falla, dispondremos de otro. Para tener una mayor redundancia se contratarán 2 operadores diferentes. Los escogidos serán COLT isp1 y ALPI isp2. Recordemos que hay que dar servicio a las Ferias y es primordial no tener cortes en INTERNET.

Como en los equipos de Distribución, configuraremos 2 protocolos en los equipos de INTERNET.

El primero será OSPF para configurar nuestra IP de Gestión y la red del puerto que comunica con el CORE.

El siguiente protocolo que configuramos será BGP. Recordemos que en el protocolo BGP distribuimos la ruta conectada de la vrf específica. Además para que dicha vrf tenga Acceso a INTERNET pondremos una ruta estática dentro del protocolo BGP. Esta ruta estática se dirigirá hacia el Firewall. En nuestro caso, disponemos de 2 vrf con Accesos a INTERNET.

Las rutas estáticas:

-ip route vrf EXPOSITORES 0.0.0.0 .0.0.0.0 10.1.2.1

-ip route vrf OFICINAS 0.0.0.0 .0.0.0.0 10.2.2.1

Dichas rutas nos “enrutarán” para acceder a cualquier IP y con esto, nos podremos dirigir a la puerta de enlace de vrf EXPOSITOTES 10.1.2.1 y vrf 10.2.2.1

En nuestro proyecto tendremos 2 equipos de INTERNET por si un equipo fallara. Para realizar esta propuesta tendremos un punto a punto entre los dos equipos de las diferentes sucursales. Esta línea estará en stand by. Nos permitirá saber cuando el equipo D_INET 1 no funcione correctamente que el D_INET 2 sea el responsable de proporcionar la salida de INTERNET.

Los equipos ASA serán los responsables de realizar los NATs de las IPs para acceder a INTERNET. Igual que los equipos D-INET tendrán los Firewall ASAs un punto a punto. Para saber cuando un equipo no este funcionando correctamente.

Es decir, la vrf OFICINAS tendrá IPs privadas pero, cuando acceda a INTERNET, tendrá la IP 65.125.123.2; en cambio, vrf EXPOSITORES cuando acceda a INTERNET será 65.125.123.3.

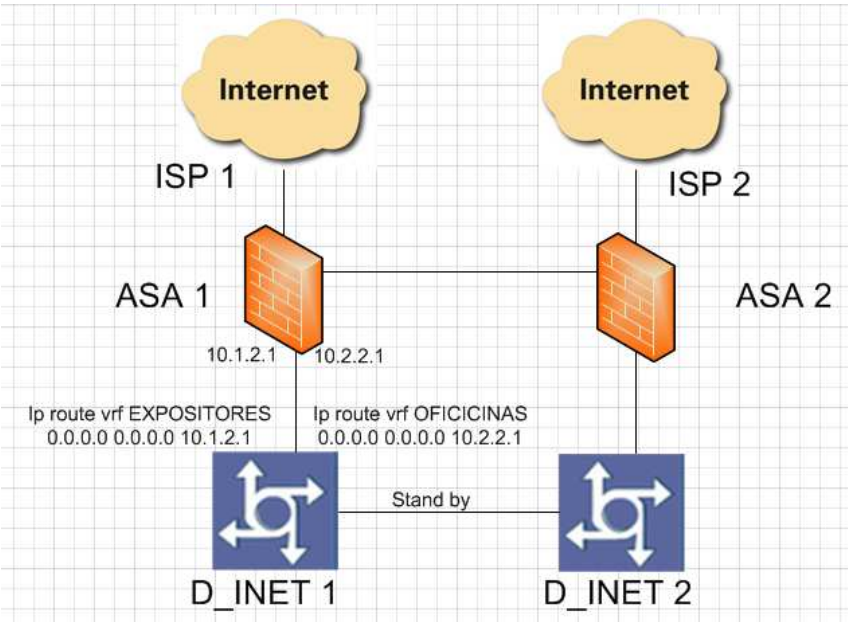


Fig. 6.6. Esquema del Building block de INTERNET.

6.1.5 Esquema lógico de los equipos de SERVIDORES.

En la figura 6.7 visualizamos el esquema lógico de las servidores. Los equipos de servidores se configuraran como los demás Distribuciónes. Es decir primero crearemos la loopback, después declaremos nuestra ruta OSPF y cuando los demás equipos tengan vecindad por protocolo OSPF crearemos el "router BGP". Los checkpoint serán los responsables de unir la vrf OFINICAS con los servidores. Igual los firewall ASA los chechpoint también tendrán un punto a punto. Para que se comuniquen si el equipo primario esta funcionando correctamente.

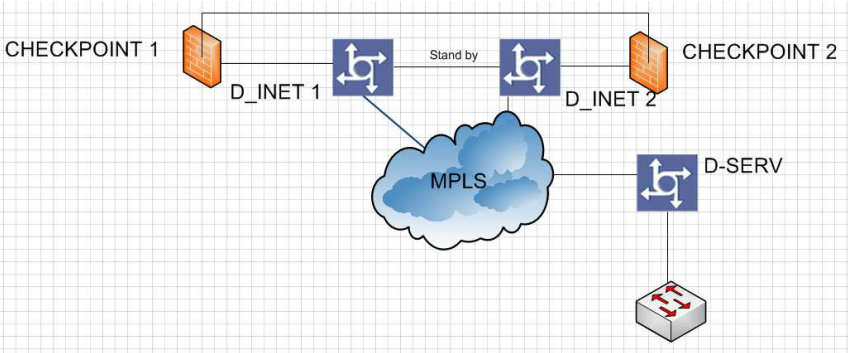


Fig. 6.7. Esquema lógico de servidores.

6.2Esquema en GNS3.

GNS3 es un simulador gráfico de red que permite diseñar tipologías de red complejas. Además se puede poner en marcha simulaciones sobre ello.

Los equipos los hemos simulado escogiendo los routers del modelo C3700 cargando la IOS c3745-adventerprisek9-mz.124-25. Hemos de recordar que no se puede realizar exactamente el esquema que nosotros deseamos. Pero las configuraciones serán parecidas.

En GNS3 cada vez que se apague el programa se tendrá que volver a crear las vlans ya que la aplicación no las guarda. Además en algunos casa para "up" los niveles 3 de Distribución tendremos que introducir el comando "no autostate".

6.2.1 Esquema GNS 3 lógico de los CORES

Hay que recordar que en los CORES se configurará el área 0 como muestra la Fig. 6.8.

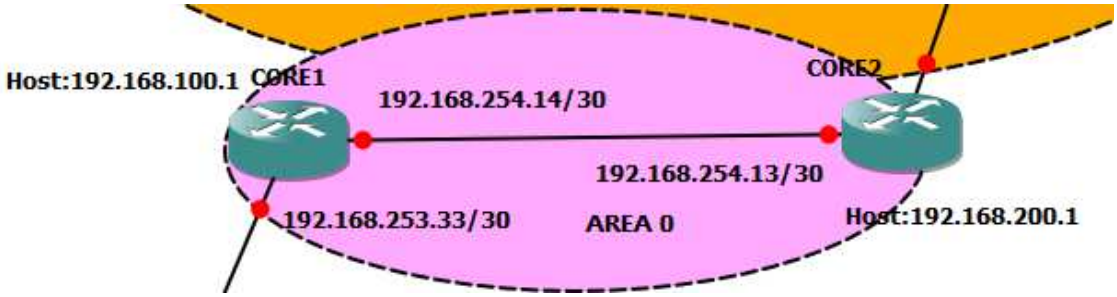


Fig. 6.8. Esquema de CORES en GNS3.

El CORE1 se ha configuro con la IP 192.168.100.1 y el CORE 2 con la IP 192.168.200.1

El primer paso será definir las IPs de los equipos en nuestros routers.

En el CORE1:

```
interface Loopback0
        ip address 192.168.100.1 255.255.255.255
        no sh
end
```

En el CORE2:

```
interface Loopback0
ip address 192.168.200.1 255.255.255.255
no sh
end
```

Después de saber las IPs de los equipos **configuraremos el protocolo OSPF**.

```
Router ospf 1
router-id 192.168.200.1
log-adjacency-changes
auto-cost reference-bandwidth 20000
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timer slsa arrival 80
network 192.168.100.100.0.0.0 area 0
!
```

CORE 1	CORE2
router ospf 1 router-id 192.168.100.1 log-adjacency-changes auto-cost reference-bandwidth 20000 timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80 network 192.168.100.1 0.0.0.0 area 0 !	router ospf 1 router-id 192.168.200.1 log-adjacency-changes auto-cost reference-bandwidth 20000 timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80 network 192.168.200.1 0.0.0.0 area 0 !

Tabla 6.1.Tabla de configuración del protocolo OSPF.

Explicación de la configuración:

Router ospf 1→ (*1 será nuestro número identificativo de proceso*).
router-id 192.168.100.1→ (*La IP de nuestro equipo*).
log-adjacency-changes→ (*Para enviar un mensaje al vecino de adyacencia*).
auto-cost reference-bandwidth 20000
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
network 192.168.100.1 0.0.0.0 area 0→ (*Nuestra área Backbone*).

!

Con estos comandos declaramos nuestro CORE a nuestros vecinos, los cuales conocerán la IP de nuestro host. Ahora configuraremos nuestros puertos para que tengan conectividad los equipos.

CORE 1	CORE2
interface FastEthernet0/0 dampening ip address 192.168.254.14 255.255.255.252 ip ospf network point-to-point ip ospf dead-interval minimal hello-multiplier 4 load-interval 30 carrier-delay msec 0 duplex auto speed auto mpls label protocol ldp mpls ip end	interface FastEthernet0/0 dampening ip address 192.168.254.13 255.255.255.252 ip ospf network point-to-point ip ospf dead-interval minimal hello-multiplier 4 load-interval 30 carrier-delay msec 0 duplex auto speed auto mpls label protocol ldp mpls ip end

Tabla 6.2. Enlace entro los CORES.

Los 2 puertos tendrán conectividad ya que están en la misma subred.

La IP 192.168.254.14 con máscara 255.255.255.252 tendrá como IP de host 192.168.254.13-14. La de red será 192.168.254.12 y la de broadcast 192.168.254.15.

Explicación de la configuración:

Interface FastEthernet X/X
dampening→ (*Evitará los caídas y subidas de los puertos de los puertos*).
Ip address 192.168.254.14 255.255.255.252→ *(IP del Puerto).*
Ip ospf networkpoint-to-point→ (*Tipo de red punto a punto para puertos conectados directamente*).
Ip ospf dead-interval minimal hello-multiplier 4→ *(Si en 40 segundos nuestro equipo no ha recibido la contestación de otro equipo nuestro Hello lo consideremos que el vecino esta "down" y se caería la adyacencia OSPF con el vecino).*
load-interval 30→ *(Recoger los datos de la interface en los últimos 30 segundos, por defecto utiliza cada 5minutos).*
carrier-delaymsec 0→ (*Para establecer el retardo de soporte en una interfaz física principal*).
duplex auto → (*Enviar y recibir paquetes en el mismo tiempo*).
speed auto → (*Velocidad del puerto*).
mpls label protocol ldp→ (*Protocolo de etiquetaje*).
mpls Ip→ (*Configuración de MPLS en interfaces físicas*).
End

Visualizamos la conectividad de los dos equipos.

```
CORE1#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/28/52 ms
CORE1#sh cdp ne
CORE1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
CORE2            Fas 0/0            173         R S I      3745      Fas 0/0
```

Fig. 6.9. Conectividad entre CORE1 al CORE2.

```
CORE2#ping 192.168.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/25/48 ms
CORE2#sh cdp ne
CORE2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port
 ID
CORE1            Fas 0/0            169         R S I      3745      Fas
0/0
```

Fig. 6.10. Conectividad entre CORE2 al CORE1.

Cuando los dos equipos tengan adyacencia por OSPF visualizaremos un mensaje:

> *Mar 1 00:00:24.255: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.200.1 on FastEthernet0/0 from LOADING to FULL, Loading Done

Los comprobaremos con el comando: # sh ip ospf neighbor

Forzaremos en nuestros equipos que el protocolo MPLS tenga como IP de host la configurada en la interface loopback.

En el CORE1 veremos cómo vecino IP del CORE2. Lo mismo realizaremos en el CORE2.

```
CORE1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.200.1     0   FULL/  -        848 msec    192.168.254.13  FastEthernet0/
0
```

Fig. 6.11. Vecindad por el protocolo OSPF.

Ahora comprobaremos la adyacencia entre los CORES por MPLS. Se realizará con el comando: #sh mpls ldp ne.

```
CORE1#sh mpls ldp ne
Peer LDP Ident: 192.168.200.1:0; Local LDP Ident 192.168.100.1:0
TCP connection: 192.168.200.1.25461 - 192.168.100.1.646
State: Oper; Msgs sent/rcvd: 145/144; Downstream
Up time: 01:59:12
LDP discovery sources:
FastEthernet0/0, Src IP addr: 192.168.254.13
Addresses bound to peer LDP Ident:
192.168.254.13  192.168.200.1.
```

Por nivel 2 de LDP CORE1 se visualiza el puerto del CORE2 y su IP de gestión. Además la conectividad se realiza por el protocolo TCP.

6.2.2 Esquema GNS 3 lógico de las Distribuciones de palacio.

En nuestra práctica simularemos los equipos de Distribución con un router c3745 con la IOS c3745-adventerprisek9-mz.124-25. Realizaremos una pequeña modificación. para que se comporte como un switch en el cual podamos realizar VTP, VLANs, InterVLANRouting, modos de puertos trunk, access y la encapsulación de datos (ISL & IEEE 802.1Q).

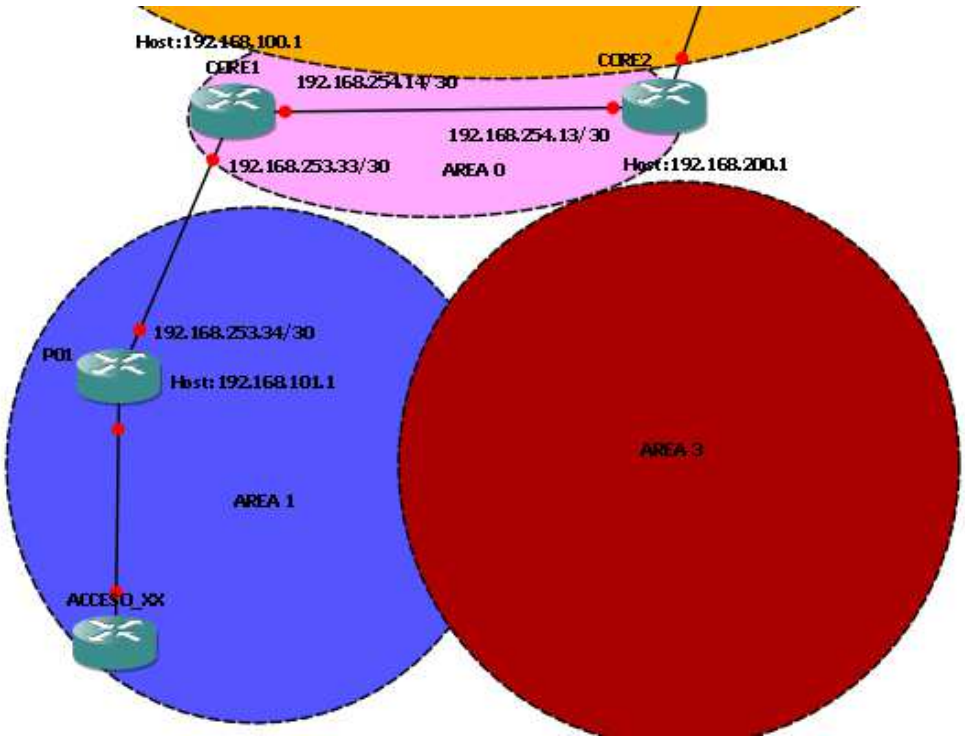


Fig. 6.12. Esquema de Distribuciones del Palacio en GNS3.

Como en los CORES, configuraremos primero la IP del host.

```
interface Loopback0
        ip address 192.168.101.1 255.255.255.255
        no sh
end
```

Primero introduciremos la IP del host. Los siguientes comandos los hemos explicado con anterioridad. Pero además, en los switches de Distribución, publicaremos las redes de los CORES y la red de Distribución.

En puerto que une con el CORE configuraremos:

P01->CORE	CORE->P01
interface FastEthernet0/0 ip address 192.168.253.34 255.255.255.252 ip ospf network point-to-point ip ospf hello-interval 3 ip ospf dead-interval 9 carrier-delay msec 0 duplex auto speed auto mpls label protocol ldp mpls ip end	interface FastEthernet0/1 ip address 192.168.253.33 255.255.255.252 ip ospf network point-to-point ip ospf hello-interval 3 ipo spf dead-interval 9 carrier-delay msec 0 duplex auto speed auto mpls label protocol ldp mpls ip end

Tabla 6.3. Enlace entre CORE y Distribución del Palacio 1.

Los dos puertos unidos físicamente tendrán conectividad ya que pertenecerán a la misma subred.

Por el protocolo LDP, D-P01 tendrá vecindad con el CORE 1. En la Fig 6.13. de abajo vemos que Distribución visualiza las 2 IPs de los puertos de CORE 1 y su IP de gestión. Lo comprobaremos.

```
P01#sh mpls ldp neighbor
    Peer LDP Ident: 192.168.100.1:0; Local LDP Ident 192.168.101.1:0
        TCP connection: 192.168.100.1.646 - 192.168.101.1.21069
        State: Oper; Msgs sent/rcvd: 69/69; Downstream
        Up time: 00:52:14
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.253.33
        Addresses bound to peer LDP Ident:
          192.168.254.14  192.168.100.1   192.168.253.33
```

Fig. 6.13. Pantalla vecindad MPLS.

Después **configuraremos el protocolo OSPF**

```
Router ospf 1
router-id 192.168.101.1
log-adjacency-changes
auto-cost reference-bandwidth 20000
timers throttle spf 10 100 5000
timers lsa arrival 80
network 192.168.101.1 0.0.0.0 area 1
network 192.168.253.32 0.0.0.3 area 1
!
```

Las redes que publicaremos en OSPF serán la de unión con el CORE y el host de Distribución Fig. 6.14.

```
P01#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.1     0   FULL/  -        00:00:07    192.168.253.33  FastEthernet0/
0
```

Fig. 6.14. Vecindad D-P01 con CORE1 por OSPF.

En el protocolo BGP declararemos D-INET 2 y CORE1. Pero como comentamos con anterioridad nuestras vrfs no visualizarán CORE1. Como vemos en el ejemplo, la vrf EXPOSITORES entiende que para acceder a INTERNET el próximo "host", será D-INET 1 y no CORE 1.

```
P01#sh ip bgp vpnv4 vrf EXPOSITORES
BGP table version is 15, local router ID is 192.168.101.1
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
Route Distinguisher: 65501:5 (default for vrf EXPOSITORES)
*> 10.1.108.0/22    0.0.0.0                  0         32768 ?
*> 10.2.108.0/22    0.0.0.0                  0         32768 ?
*> 10.4.108.0/22    0.0.0.0                  0         32768 ?
*> 10.8.108.0/22    0.0.0.0                  0         32768 ?
*>i192.168.224.160/28
                    192.168.200.3          200    100      0 ?
```

Fig. 6.15. Tabla de enrutamiento de vrf EXPOSIORES.

En esta práctica nuestro AS (sistema autónomo) será 65501. Es un número aleatorio. Nuestro BGP router-id será el mismo que el de OSPF y LDP.

Router bgp 65501
bgp router-id 192.168.101.1
no bgp default ipv4-unicast → (*BPG tiene reconfiguradas unos valores unicast. Lo deshabilitaremos.)*
bgp log-neighbor-changes→ *(Visualizaremos en nuestro equipo los cambios BGP de los equipos vecinos).*
neighbor 192.168.100.1 remote-as 65501 → *(Coincide el AS con la IP del host vecino.)*
neighbor 192.168.100.1 update-source Loopback0 → *(Especificamos la interface del router. Usualmete se utiliza la loopback.)*
neighbor 192.168.200.1 remote-as 65501
neighbor 192.168.200.1 update-source Loopback0
neighbor 192.168.200.3 remote-as 65501 → *(IP de Distribución INTERNET).*
neighbor 192.168.200.3 update-source Loopback0

address-family ipv4 → *(Para MPLS version IP version 4).*
No synchronization → *(Deshabilita la sincronización ente el BPG y IGP).*
Bgp dampening → *(Penalización de los flapeos del protocolo BGP).*
Redistribute connected → *(La rutas de mi palacios las conozca todos los palacios. Con 2 protocolos diferentes, en nuestro caso, OSPF y BGP).*
Redistribute static metric 50 → *(La ruta especifica la conozca otros palacios).*
no auto-summary → *(Deshabilitaremos la transmisión automática de la red).*
exit-address-family
address-family vpnv4
bgp scan-time import 5
bgp scan-time 5
neighbor 192.168.100.1 activate → *(vecino active).*
neighbor 192.168.100.1 send-community both → *(rutas prefijadas).*
neighbor 192.168.200.1 activate
neighbor 192.168.200.1 send-community both
neighbor 192.168.200.3 activate
neighbor 192.168.200.3 send-community both

6.2.3 Esquema GNS 3 los Accesos.

Como en el punto 6.2.2, el router de Acceso lo configuraremos para que se comporte como un switch. Como hemos explicado con anterioridad, los ACCESOS lo configuraremos con la tecnología SVI.

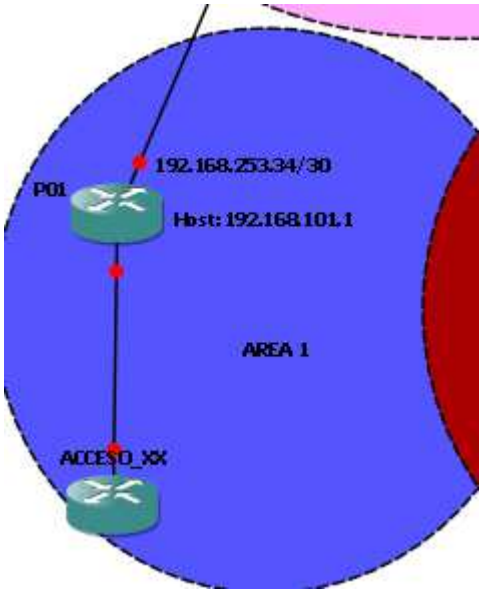


Fig. 6.16. Esquema en GNS3 de los Accesos.

```
hostname ACCESO_XX→ (Cambiamos el nombre del switch).
Vlan database → (Creamos vlan).
vlan 11 name GESITON
exit
interface Vlan 11 → (Creamos nivel 3 de la vlan)
ip address 192.168.101.131 255.255.255.128
!
ip default-gateway 192.168.101.129 → (puerta de enlace )
interface FastEthernet1/0
description A-P1-1
switchport mode trunk
!
```

Después configuraremos el equipo de Distribución.

```
Vlan database → (Creamos vlan)
vlan 11 name GESITON
exit
interface Vlan11
ip address 192.168.101.129 255.255.255.128 → (Creamos nivel 3 de la vlan)
no autostate→ (Levantamos la interface)
end
```

```
ACCESO_XX#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
P01              Fas 1/0            133        R S I      3745      Fas 1/0
P01#ping 192.168.101.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/47/96 ms
```

Fig. 6.17. Comprobación conectividad entre ACCESO_XX y D-P01.

6.2.4 Esquema GNS 3 de los equipos de INTERNET.

Ahora conectaremos el equipo de Distribución. En la Fig. 6.18. visualizamos como será el esquema de nuestra red en GNS3.

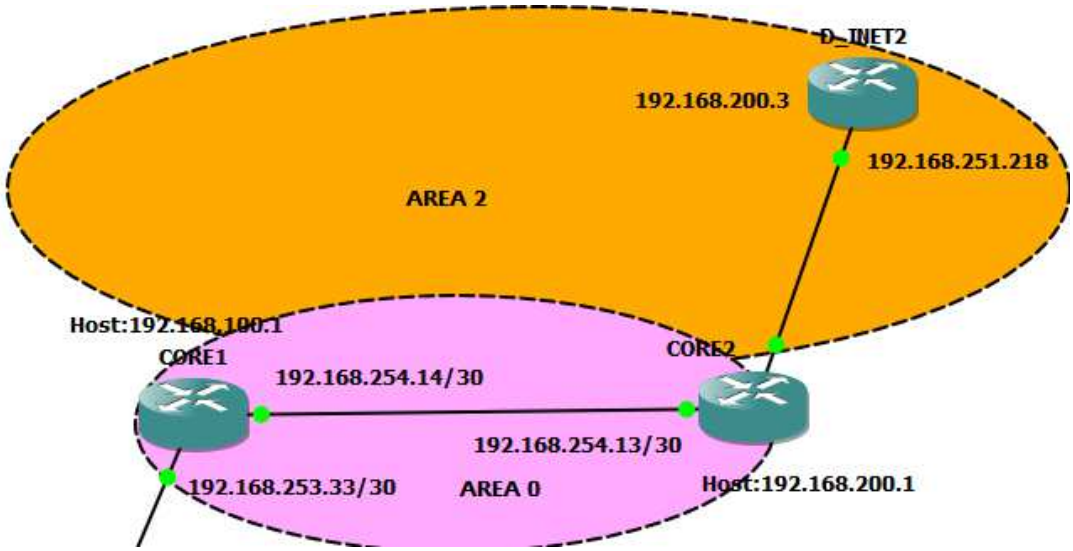


Fig. 6.18. Esquema INTERNET del GNS3.

El primer paso será configurar la IP del equipo:

```
interface Loopback0
ip address 192.168.200.3 255.255.255.255
!
```

Después, configuraremos el router para tener conectividad directa con el CORE.

Enlace Distribución INTERNET -> CORE 2	interface FastEthernet0/0 description PORTCHANNEL CORE2 dampening ip address 192.168.251.218 255.255.255.252 ip ospf network point-to-point ip ospf dead-interval minimal hello-multiplier 4 load-interval 30 carrier-delay msec 0 duplex auto speed auto mpls label protocol ldp mpls ip !

Tabla 6.4. Configuración de los puertos de enlace

En la figura se observa que tenemos visibilidad con el CORE2.

```
D_INET2#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
CORE2            Fas 0/0            143        R S I      3745      Fas 0/1
```

Fig. 6.19. Vecindad D-INET-2 y CORE2.

Después configuraremos en el router INTERNET el protocolo OSPF:

```
routerospf 1
router-id 192.168.200.3
log-adjacency-changes
network 192.168.200.3 0.0.0.0 area 2
network 192.168.251.216 0.0.0.3 area 2
!
```

Luego se configura el protocolo BGP:

```
routerbgp 65501
bgp router-id 192.168.200.3
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 192.168.100.1 remote-as 65501
neighbor 192.168.100.1 update-source Loopback0
neighbor 192.168.101.1 remote-as 65501
neighbor 192.168.101.1 update-source Loopback0
neighbor 192.168.200.1 remote-as 65501
neighbor 192.168.200.1 update-source Loopback0
default-metric 200
```

```
        !
        address-family ipv4
        redistribute connected metric 200
        redistribute static metric 200
        neighbor 192.168.100.1 activate
        neighbor 192.168.200.1 activate
        default-information originate
        default-metric 200
        no auto-summary
        no synchronization
        bgp dampening
        exit-address-family
        !
        address-family vpnv4
        neighbor 192.168.100.1 activate
        neighbor 192.168.100.1 send-community both
        neighbor 192.168.101.1 activate
        neighbor 192.168.101.1 send-community both
        neighbor 192.168.200.1 activate
        neighbor 192.168.200.1 send-community both
        bgp dampening
        bgp scan-time import 5
        bgp scan-time 5
        exit-address-family
!
```

En la Fig. 6.20 visualizamos que la adyacencia BGP y OSPF se realiza. Además nos avisa que el protocolo LDP entre los CORES se establece.

```
*Mar  1 00:00:40.027: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.200.1 on FastEthern
et0/0 from LOADING to FULL, Loading Done
*Mar  1 00:00:54.147: %LDP-5-NBRCHG: LDP Neighbor 192.168.200.1:0 (1) is UP
*Mar  1 00:01:04.391: %BGP-5-ADJCHANGE: neighbor 192.168.101.1 Up
```

Fig. 6.20. “Up” de los protocolos.

7. Esquema físico de la red.

En este apartado comentaremos los aspectos físicos de nuestra red. En la Fig. 5.1. hemos visualizado el esquema general de nuestra red.

7.1 Esquema físico de los CORES.

CORE1 y CORE2 estará formado por dos equipos. Cada uno como se visualiza en la Fig. 7.1.

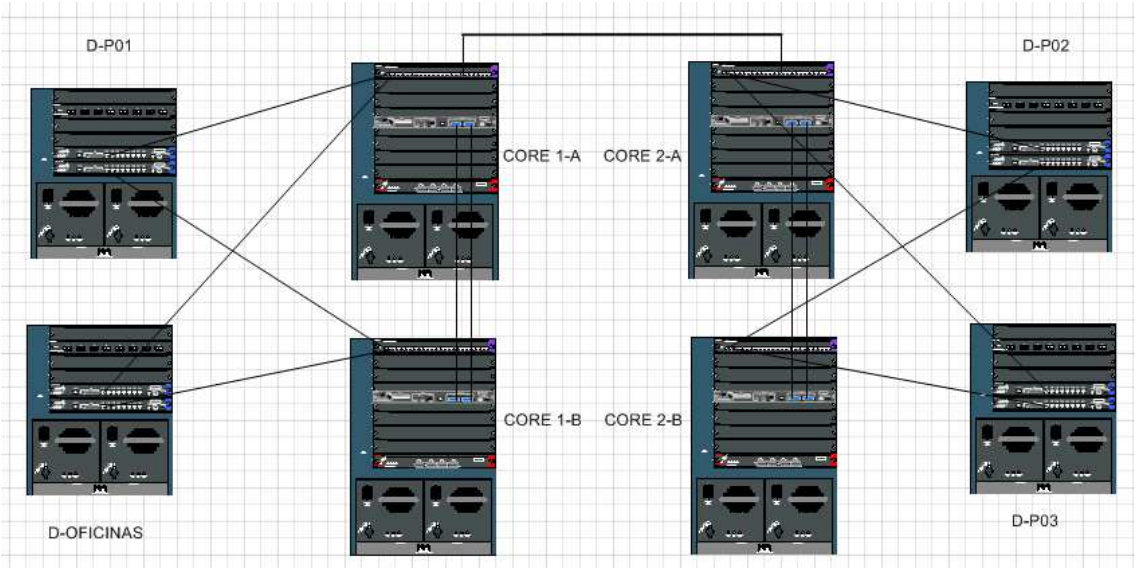


Fig. 7.1. Esquema físico entre CORE y Distribuciones

Los CORES dispondrán de 3 placas. La placa 1 dispondrá de 24 puertos SFP, la placa 5 destinada para las conexiones VSS y la placa 6 tenGigabitEthernet.

Es decir, CORE1-A y CORE1-B están conectados en los puertos tenGigabitEthernet correspondientes a la placa 5 de los CORES, lo mismo que en el CORE 2. El puerto ten 1/5/4 (del CORE1-A, switch 1 placa 5 puerto 4) del CORE1-A contra 2/5/4 (CORE1-B, switch 2 placa 5 puerto 4). Como tendremos redundancia, también uniremos los puertos ten 1/5/5 (del CORE1-A, switch 1 placa 5 puerto 5) contra el puerto ten 2/5/5 (del CORE1-B, switch 2 placa 5 puerto 5). Lo mismo realizaremos con el CORE 2.

	CORE 1-A	CORE 1-B
Enlaces	ten 1/5/4	ten 2/5/4
Enlaces	ten 1/5/5	ten 2/5/5

	CORE 2-A	CORE 2-B
Enlaces	ten 1/5/4	ten 2/5/4
Enlaces	ten 1/5/5	ten 2/5/5

Tabla 7.1. Muestra los enlaces entre CORE1-A, CORE1-B, CORE2-A y CORE2-B.

Los equipos de Distribuciones de los palacios los conectaremos a las placas 1 de los CORES ya que los puertos son gigabitEthernet. Se hace esto puesto que nuestros equipos están redundados.

EQUIPOS	CORE 1-A	CORE 1-B
D_P01	Gig 1/1/1	Gig 2/1/1
D_OFICINAS	Gig 1/1/2	Gig 2/1/2

EQUIPOS	CORE 2-A	CORE 2-B
D_P02	Gig 1/1/1	Gig 2/1/1
D_P03	Gig 1/1/2	Gig 2/1/2

Tabla 7.2. Conexiones de los CORES contra Distribuciones.

7.2 Esquema físico de los Distribuciones.

En la Fig.7.2. se visualiza el esquema contra los CORES.

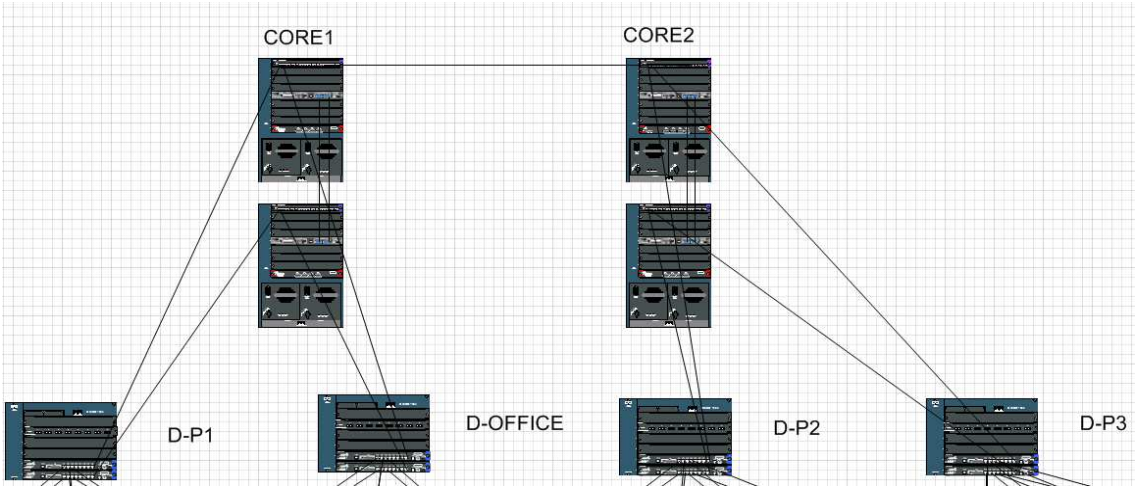


Fig. 7.2. Esquema entre los Distribuciones y los CORES

Cada Distribución dispondrá de 3 placas. La placa 2 dispone de 8 puertos GBIC y la placa 5 y 6 contiene 9 puertos gigabitEthernet cada una. Como nombramos con anterioridad, los Distribuciones tendrán doble enlace contra los CORES. Por ello, los enlaces los conectaremos en el puerto 5/8 (placa 5 puerto 8) y 6/8 (placa 6 puerto 8). En cada Palacio seguiremos el mismo esquema. Para poder seguir el esquema, realizaremos las mismas conexiones en todos los Distribuciones, como se observa en la tabla 7.3.

EQUIPOS	CORE 1-A	CORE 1-B
D_P1	Gig 5/8	Gig 5/8
D_OFFICE	Gig 5/8	Gig 5/8

EQUIPOS	CORE 2-A	CORE 2-B
D_P02	Gig 5/8	Gig 5/8
D_P03	Gig 5/8	Gig 5/8

Tabla 7.3. Conexión Distribución→ CORES

7.3 Esquema físico de los Accesos.

En los switches realizaremos las conexiones contra Distribuciones en los puertos SFP Gigabit Ethernet. Para las conexiones utilizaremos fibra multimodo ya que las distancias serán menores a 1 Km. Vemos los enlaces en la Fig. 7.3.

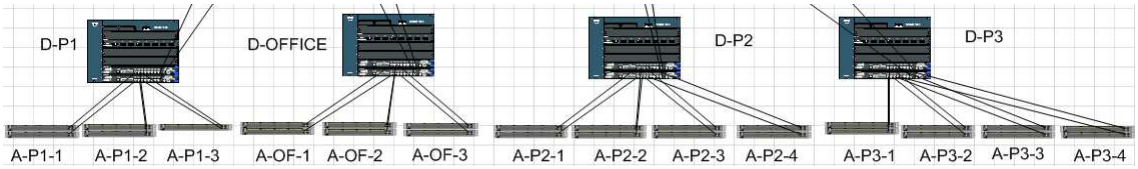


Fig. 7.3. Esquema entre los Distribuciones y los Accesos

En la tabla 7.4 se refleja las conexiones contra Distribución.

PALACIO 1		
EQUIPOS	D-P1	D-P1
A-P1-1	Gig 1/0/1	Gig 2/0/1
A-P1-2	Gig 1/0/1	Gig 2/0/1
A-P1-3	Gig 1/0/1	Gig 1/0/2

PALACIO OFFICE		
EQUIPOS	D-OFFICE	D-OFFICE
A-OF-1	Gig 1/0/1	Gig 2/0/1
A-OF-2	Gig 1/0/1	Gig 2/0/1
A-OF-3	Gig 1/0/1	Gig 1/0/2

PALACIO 2		
EQUIPOS	D-P2	D-P2
A-P2-1	Gig 1/0/1	Gig 2/0/1
A-P2-2	Gig 1/0/1	Gig 2/0/1
A-P2-3	Gig 1/0/1	Gig 1/0/2
A-P2-4	Gig 1/0/1	Gig 1/0/2

PALACIO 3		
EQUIPOS	D-P2	D-P2
A-P3-1	Gig 1/0/1	Gig 2/0/1
A-P3-2	Gig 1/0/1	Gig 2/0/1
A-P3-3	Gig 1/0/1	Gig 1/0/2
A-P3-4	Gig 1/0/1	Gig 1/0/2

Tabla 7.4. Las conexiones Accesos contra Distribuciones.

7.4 Esquema físico de INTERNET.

En la tabla 7.5 visualizamos las conexiones de los equipos de INTERNET. Cada D-INET tendrá 1 enlace contra cada CORE (A y B) de fibra multimodo con conector LC. 1 enlace con Checkpoint y 2 enlace con conectividad ASA (vrf EXPOSITORES y vrf OFICINAS) también.

Vemos además que los equipos ASA se conectarán a COLT isp1 y ALPI isp2.

Los equipos checkpoint y sus funciones, serán explicados en otro apartado.

D-INET 1	PUERTO	EQUIPO DE ENLACE
	1/24	CORE 1-A
	1/23	CORE 1-B
	1/22	Checkpoint
	1/21	vrf OFICINAS ASA
	1/20	vrf EXPOSITORES ASA

D-INET 2	PUERTO	EQUIPO DE ENLACE
	1/24	CORE 2-A
	1/23	CORE 2-B
	1/22	Checkpoint
	1/21	vrf OFICINAS ASA
	1/20	vrf EXPOSITORES ASA

Tabla 7.5. Puertos de enlace de los equipos de INTERNET contra CORES.

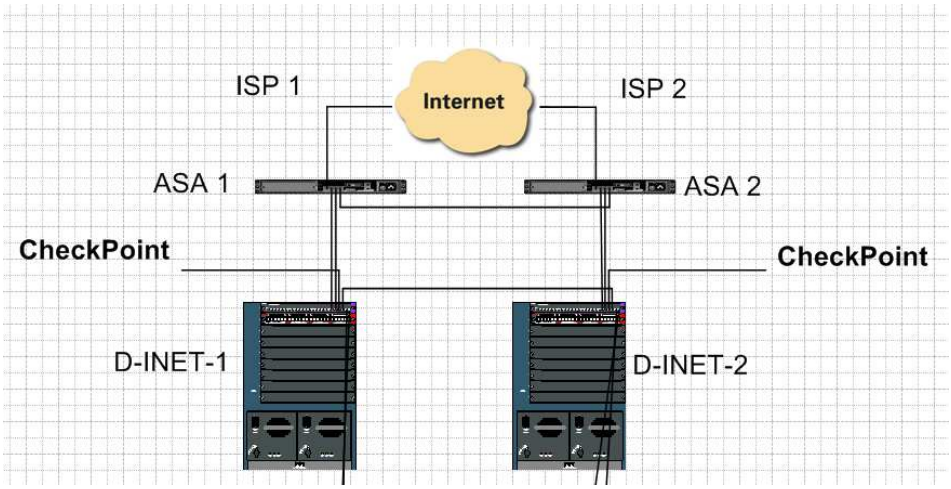


Fig. 7.4. Esquema Físico de INTERNET.

7.5 Esquema físico de servidores.

Instalaremos 2 equipos de Servidores, 1 servidor lo conectaremos al CORE 1-A y al CORE 1 B. Las dos fibras que utilizaremos para conectarnos serán multimodo con conector LC - SC. Además entre D-SERV 1 y D-SERV 2 conectaremos 2 enlaces para tener un mejor ancho de banda y por si una fibra fallara.

EQUIPOS	ENLACE
CORE1-A->D-SERV1	ten 1/9->ten ½
CORE1-B->D-SERV1	ten 1/10->ten 1/1

EQUIPOS	ENLACE
D-SERV1->D-SERV2	ten 5/4-> ten 5/4
D-SERV1->D-SERV2	Ten 5/5-> ten 5/5

Tabla 7.6. Enlaces D-SERV y CORE.

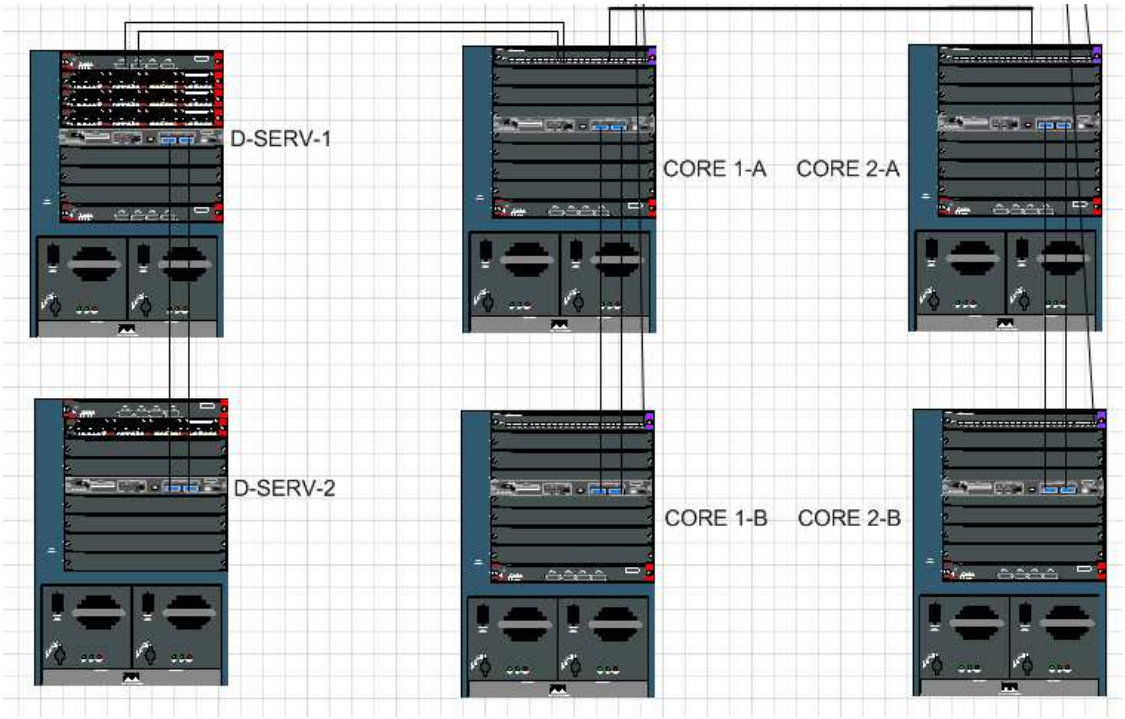


Fig. 7.5. Esquema Físico de SERVIDORES.

8. Distribución de los elementos de red.

8.1 Distribución de los elementos de red de la sucursal de Valencia.

8.1.1 Palacio oficinas.

En la tercera planta de la sucursal de Valencia se instalará un centro de procesamiento de datos (CPD). Se montará una pequeña sala acondicionada con las necesidades de los equipos. Los equipos de tendrán aire acondicionando, SAI para todos los equipos.

Fig. 8.1. Ejemplo de sala CPD.

En la sala CPD instalaremos nuestros equipos CORE1-A, CORE1-B, D-INET1, D-SERV1, D-SERV2, D-OFFICE, CHECKPOINT y ASA 1. Además se instalará en los racks LIUs (path panel para fibras) y path panels para tomas de red.

En este espacio también se sitúan los elementos de sistemas, es decir, sus servidores de correo, su base de datos, Oracle, entre otros.

En cada planta de Oficinas dispondremos de un pequeño almacén donde podremos situar nuestro rack. En el rack instalaremos nuestros switches. Además en cada rack incorporaremos path panel para las tomas, LIU y 1 SAI por si se produce un corte eléctrico.

En la tabla 8.1 vemos la situación de los switches de Oficinas.

	EQUIPO
PLANTA 1	A-OF-1
PLANTA 2	A-OF-2
PLANTA 3	A-OF-3

Tabla 8.1. Distribución de los Accesos.

8.1.2 Palacio 1

En la Fig.8.2.vemos la distribución de nuestros equipos. Palacio 1 tendrá un almacén para instalar el switch de distribución. Por otro lado los Accesos están ubicados en las columnas en la parte superior. Las columnas disponen de unas escaleras. Para poder instalar los switches, necesitaremos la contratación de un elevador. Cada rack debe tener SAIs, path panel y LIU.

Fig.8.2. Plano del Palacio 1 con la ubicación de los equipos

8.2 Distribución de los elementos de red de la sucursal de Paterna.

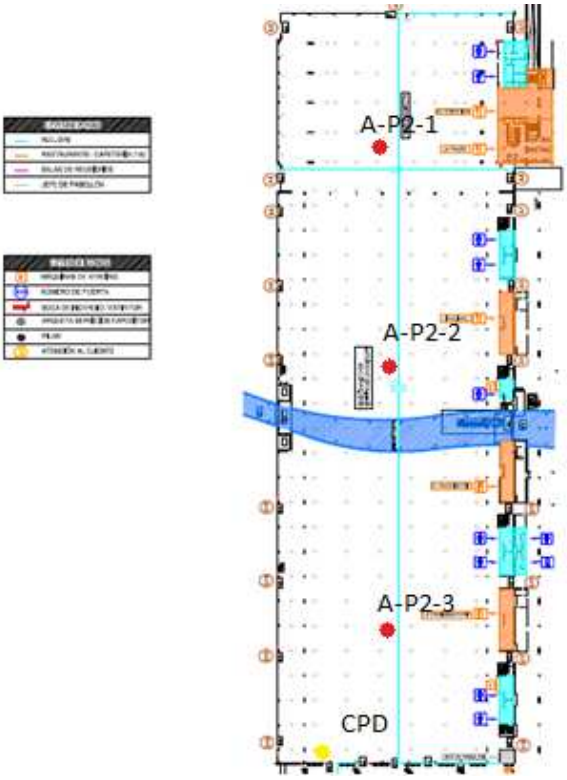
8.2.1 Palacio 2.

En la Fig. 8.3 se visualiza la ubicación de los Accesos. Debido a su magnitud de m^2 instalaremos 2 equipos de 48 puertos en stack por cada acceso.

Como comentamos con anterioridad, la sucursal de Paterna dispondrá de galerías subterráneas donde se instalará el cableado de red y nuestros racks con los switches, path paneles, LIU y SAIS.

En el recinto de Paterna necesitaremos un CPD para nuestros equipos (situado en las galerías). En el palacio 2 dispondremos de un sala acondicionada a las necesidades. En el CPD de Paterna colocaremos los equipos de CORE2-A, CORE2-B, D-P02, D_INTER2 y ASA 2. Recordemos que el CPD debe tener aire acondicionado, sistema anti incendios y SAIs.

En el nivel 1, debido a la distancia que podría tener una toma red (cable de UTP la distancia máxima es 100m) necesitaremos colocar un rack con sus switches en stack. Path panel (tomas de red), LIU y SAIS.



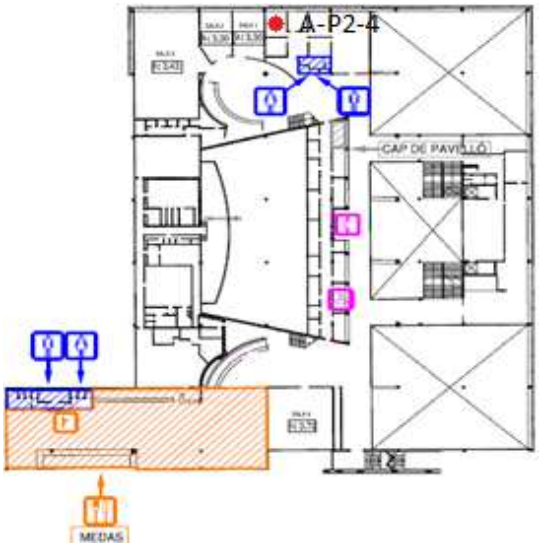


Fig.8.4. Palacio 2 nivel 1

Fig. 8.3. Palacio 2 nivel 0 (izquierda).

8.2.2 Palacio 3.

Como se observa en la Fig. 8.5. el palacio 3 cuenta con galerías subterráneas. Es aquí donde ubicaremos los equipos. Los switches dispondrán de racks, patch panel (tomas), LIU y SAI. Excepto el rack de Distribución, ya que sólo dispondrá de LIU.

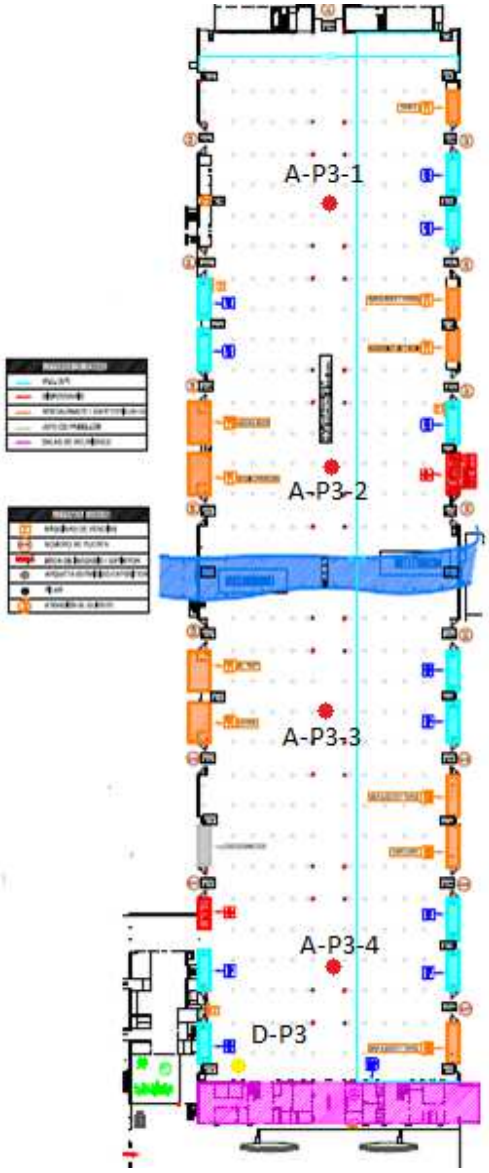


Fig. 8.5. Ubicación de los Accesos y Distribución.

9. Componentes físicos.

9.1 Building blocks-equipos

En este apartado comentaremos los elementos físicos de los equipos.

9.1.1 Building blocks-equipos CORES

En la Feria de Valencia utilizaremos dos CORES. Estos CORES están formados cada uno por 2 equipos switch catalyst de la serie 6500. Para estos CORES utilizaremos el chasis Cisco WS-C6509-E con el modelo E-Series 6-slot chasis.

Fig. 9.1. Chasis modelo WS-C6509-E.

Cada CORE dispondrá de 3 placas.

Mod	Ports	Card Type	Model	Serial No.
1	24	CEF720 24 port 1000mb SFP	WS-X6724-SFP	SAL1215M2N9
5	5	Supervisor Engine 720 10GE (Active)	VS-S720-10G	SAL1218PL3P
9	4	CEF720 4 port 10-Gigabit Ethernet	WS-X6704-10GE	SAL1217NUZV

Como podemos ver, la placa numero 1 dispondrá de 24 puertos gigabitEthernet. En la placa número 2 utilizaremos VS-S720-10G especializada en VSS 1440 (más tarde explicaremos la tecnología) y la placa 9 dispondrá de puertos tengigabitEthernet para una mayor capacidad de datos.

Utilizaremos la tecnología de virtualización VSS1440 en cada uno de los chasis activos para combinar una mayor capacidad de conmutación de 1400-GPs.

9.1.2 Building blocks-equipo Distribuciones

En la Feria de Valencia, los Distribuciones tendrán chasis CISCO7606-S. En la foto de abajo vemos el modelo.

Fig. 9.2. Chasis modelo CISCO7606-S.

Estos chasis de alto rendimiento están diseñados para la instalación de 6 placas. El switch puede realizar tareas de router y soporta MPLS, BGP, video IP, entre otros.

Para nuestra infraestructura utilizaremos 3 placas que serán (esto en cada Distribución):

Mod	Ports	Card Type	Model	Serial No.
2	8	8 port 1000mb GBIC Enhanced QoS	WS-X6408A-GBIC	SAL1218PCFC
5	9	Supervisor Engine 32 8GE (Hot)	WS-SUP32-GE-3B	SAL1218PLT9
6	9	Supervisor Engine 32 8GE (Active)	WS-SUP32-GE-3B	SAL1218PLSH

En este esquema la placa número 2 será WS-X6408A-GBIC:

Fig. 9.3. Placa WS-X6408A-GBIC.

Estos módulos son ideales para la fibra GBIC y la agregación de alta densidad. Soporta una alta velocidad y una gran cantidad de paquetes.

En la ranura 5 y 6 utilizaremos la placa WS-SUP32-GE-3B para realizar nuestras conexiones a los Accesos de nuestras conexiones port-channel. Además los equipos están redundados. Si una placa fallara tendríamos otra activa. Las placas WS-SUP32-GE-3B permiten control sobre el extremo con el que los usuarios pueden acceder a la red. Estos son los privilegios que se otorgan a través de la identidad basada en la creación de redes con el estándar IEEE 802.1x, seguridad basada en puertos.

Fig. 9.4. Placa WS-SUP32-GE-3B.

9.1.3 Building blocks- equipos Accesos

Los Accesos estarán conectados al patch panel para que los Expositores y Oficinas tengan acceso a INTERNET. Utilizaremos equipos de familia CISCO 3750: WS-C3750-24TS-S, WS-C3750-48PS-S, WS-C3750G-24PS-S.

Fig.9.5. Equipos serie 3750.

9.1.4 Building blocks- equipos INTERNET

Al igual que los CORES, el equipo que utilizaremos será el switchcatalyst de la serie 6500. El modelo es WS-C6509-E con modelo E-Series 6-slot chasis.

Fig. 9.6. ChasisWS-C6509-E.

La placa 1 se utilizará para conexiones de fibra y la placa 4 para conexiones de cable ethernet.

Mod	Ports	Card Type	Model	Serial No.
1	24	CEF720 24 port 1000mb SFP	WS-X6724-SFP	SAL1435S0T5
4	48	SFM-capable 48 port 10/100/1000mb RJ45	WS-X6548-GE-TX	SAL1215M8R1

9.1.5 Building blocks- equipos servidores

El servidor 1 tendrá el modelo WS-C6509-E como el servidor 2. La placa 1 se ha explicado en el apartado 9.1. La placa 2, 3 y 4 dispondrán de 48 puertos con conexión RJ gigabitEthernet. La placa 5 con conexiones tenGigabitEthernet.

Mod	Ports	Card Type	Model	Serial No.
1	4	CEF720 4 port 10-Gigabit Ethernet	WS-X6704-10GE	SAL1217NV0P
2	48	CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	SAL1218PF1M
3	48	SFM-capable 48 port 10/100/1000mb RJ45	WS-X6548-GE-TX	SAD072401XH
4	48	48-port 10/100/1000 RJ45 EtherModule	WS-X6148A-GE-TX	SAL1117MMWH
5	5	Supervisor Engine 720 10GE (Active)	VS-S720-10G	SAL1218PL7N

9.2 Firewalls

9.2.1. Firewall entre redes y Servidores. Checkpoint modelo Nokia IP390.

Nokia IP390 Security Platform se gestiona fácilmente con el software Check Point VPN-1. Dispositivo de seguridad que proporciona rendimiento de varios gigabits. Tiene cuatro puertos de velocidades 10/100/1000Ethernety, puede tener dos ranuras de expansión que admite hasta ocho puertos adicionales 10/100 Ethernet o hasta cuatro puertos Gigabit Ethernet para el Check Point VPN-1.

Fig. 9.7. NOKIA IP 390

9.2.2. Firewall ASA modelo 5510

Cisco ASA 5510 provee un alto rendimiento en servicios de Firewall y VPN, tres tarjetas de red integradas 10/100 y, opcionalmente, IPs con AIP-SSM o protección contra Malwares con CSC-SSM. Ofrece seguridad avanzada y servicios de red para empresas pequeñas y medianas.

Hasta cinco firewalls virtuales se pueden implementar para permitir el control compartimentado de las políticas de seguridad a nivel departamental. Esta virtualización refuerza la seguridad y reduce los costes de gestión y de apoyo, mientras que permite la consolidación de múltiples dispositivos de seguridad de un único dispositivo.

Fig. 9.8. ASA 5510.

9.3 Rack CORES, Distribuciones, Accesos y Servidores

El rack necesario para todos los equipos será de 42U (región de 3 grapas) y de 19” de ancho. Estos nos servirán para poder instalar todos los equipos servidores, Distribuciones y Accesos.

La marca RackMatic y gama LowCost de altura 42U y tamaño externo en mm de 600 (A) x 1000 (F) x 2055 (H). Con un fondo útil de 920 mm (desde bastidor frontal hasta la tapa posterior del armario). Distancia entre bastidor frontal y trasero recomendada de 850 mm (configurable por el usuario). Este rack lo podremos utilizar para todos los equipos.

Fig. 9.9. Imagen del rack.

9.4 Fibras.

9.4.1 Tipos de Fibra.

Fibra multimodo

Es un tipo de fibra óptica mayormente usada para la comunicación de corta distancia (<1Km). En una fibra multimodo, un haz de luz puede circular por más de un modo o camino. Esto supone que no llegue todo a la vez. En el diseño de nuestra red se utilizará la fibra multimodo en las siguientes conexiones:

-Accesos contra Distribuciones.

-D-INET 1 contra CORE 1.

-D-INET 2 contra CORE 2.

-CORE 1-A contra CORE 1-B.

-CORE 2-A contra CORE 2-B.

Fibra monomodo

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz que permite alcanzar grandes distancias, desde 2,3 Km hasta100 km de máximo. En el diseño de red se utilizará en los siguientes enlaces:

-CORES contra Distribuciones.

-CORE1 contra CORE 2.

-D-INET 1 contra D-INET 2.

9.4.2 Tipos de Conectores de Fibra

Estos elementos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor. Hay una extensa variedad de tipos de conector:

-FC: Se usa en la transmisión de datos y en las telecomunicaciones.

-FDDI: Se usa para redes de fibra óptica.

-LC y MT-Array: Utilizada en transmisiones de alta densidad de datos.

-SC y SC-Dúplex: Se utilizan para la transmisión de datos.

-ST o BFOC: se usa en redes de edificios y en sistemas de seguridad.

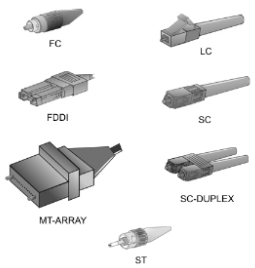


Fig. 9.10. Tipos de conectores.

En nuestro caso el tipo de conector que usaremos será LC y SC.

9.5 Tipos de SAI

9.5.1 SAI Distribución.

Para los equipos de Distribución (D-P01 y D-P03) necesitaremos un SAI potente. Nos permitirá que si se produce un corte o una bajada eléctrica el equipo siga funcionando. También protegerá el equipo de posibles picos eléctricos. Además el SAI lo podremos conectar a la red para su monitorización. Por ello utilizaremos el SAI UPS-RT-5000-VA de la empresa APC. El SAI tendrá Input 230V / Output 230V, la necesaria para los equipos de Distribución.

Fig. 9.11. Modelo de SAI UPS-RT-5000-VA.

9.5.2 SAI Accesos.

En los racks de Accesos instaláramos el SAI SUA750RMI2U también de la empresa APC. Esto SAIS también tendrán las características anteriores y tendrá un Input 230V y un Output 230V ya que será lo necesario para los accesos.

Fig. 9.12. Modelo de SAI SUA750RMI2U.

9.6 Path panel Fibras

Patch Panel (LIU) es el elemento encargado de recibir todos las fibras de los equipos. El LIU que montaremos será de la empresa Systimax.

Fig. 9.13. Modelo de LIU.

9.7 Path panel tomas

Patch Panel es el elemento encargado de recibir todos los cables del cableado estructurado. El path panel que instalaremos será de la empresa TRENDnet.

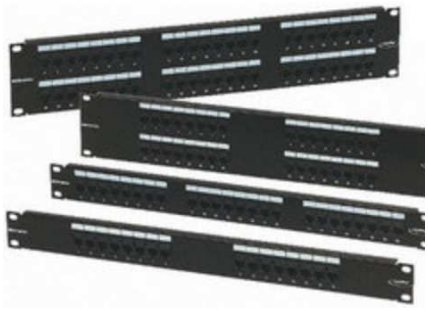


Fig. 9.14. Modelo de Patch panel

10. Red IP de Feria de Valencia

En este apartado comentaremos las IPs que tendremos en los equipos y la relación Vlan y redes.

10.1. Red de gestión

Primero estableceremos las IP de gestión de los equipos. En la tabla 10.1 visualizaremos nuestra tabla resumen. Para mantener una coherencia estableceremos un orden. Para ello se configurarán la 192.168.X0Y.Z en los equipos. “X” serán las sucursales (Valencia “1” y Paterna “2”) y “Y” será el reciento, mostrado en la tabla 10.2.

Excepción de CORE1, CORE2, D-INET1, D-INET2, D-SERV1 y D-SERV2 que la “Y” será “0”. “Z” en los equipos mencionados con anterioridad, tendrá una numeración distinta.

En los recintos Distribución la “Z” será “1” menos Distribución Oficinas será “6” y el Acceso 1 “131”, Acceso 2 “132”, Acceso 3 “133”, Acceso 4 “134”.

NOMBRE DEL EQUIPO	IP GESTION
CORE 1	192.168.100.1
CORE 2	192.168.200.1
D-INET 1	192.168.100.3
D-INET 2	192.168.200.3
D-SERV 1	192.168.100.4
D-SERV 2	192.168.100.5

PLACIO 1	
NOMBRE DEL EQUIPO	IP GESTION
D-P01	192.168.101.1
A-P1-1	192.168.101.131
A-P1-2	192.168.101.132
A-P1-3	192.168.101.133

PLACIO OFICINAS	
NOMBRE DEL EQUIPO	IP GESTION
D-OFFICE	192.168.100.6
A-OF-1	192.168.100.91
A-OF-2	192.168.100.92
A-OF-3	192.168.100.93

PLACIO 2	
NOMBRE DEL EQUIPO	IP GESTION
D-P02	192.168.202.1
A-P2-1	192.168.202.131
A-P2-2	192.168.202.132
A-P2-3	192.168.202.133
A-P2-4	192.168.202.134

PLACIO 3	
NOMBRE DEL EQUIPO	IP GESTION
D-P03	192.168.203.1
A-P3-1	192.168.203.131
A-P3-2	192.168.203.132
A-P3-3	192.168.203.133
A-P3-4	192.168.203.134

Tabla 10.1. Resumen IP de Gestión

RECINTOS	NUMERO
PALACIO 1	1
PALACIO OFICINAS	0
PALACIO 2	2
PALACIO 3	3

Tabla 10.2. Relación recinto Palacio números.

La red de gestión se publicará en OSPF pero en los Accesos necesitaremos VLAN para la conectividad con Distribución. Visualizamos en la tabla 10.3, las VLAN de los recintos XY. “X” será la sucursal y “Y” el palacio. En el caso de OFICINAS será siempre “9”.

	VLAN
GESTION PLACIO 1	11
GESTION PLACIO OFICINAS	19
GESTION PLACIO 2	22
GESTION PLACIO 3	23

Tabla 10.3. Relación recinto Palacio vlan.

10.2. Red de Feria de Valencia.

Como se ha comentado con anterioridad, nuestra red la dividiremos por vrf.

10.2.1 Vrf Expositores

La red dedicada para los expositores.

Recordemos que el expositor puede contratar 4 tipos de ancho de banda. Para ello los dividiremos en 4 VLANS como muestra la tabla 10.4 y 10.5. Seguiremos un orden 10.X.1Y0.Z. ”X” será el ancho de banda, “Y” el Palacio.

			PALACIO 1		PALACIO OFICINAS	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf EXPOSITORES	50	1MB	10.1.110.0	255.255.252.0	10.1.190.0	255.255.252.0
	51	2MB	10.2.110.0	255.255.252.0	10.2.190.0	255.255.252.0
	52	4MB	10.4.110.0	255.255.252.0	10.4.190.0	255.255.252.0
	53	8MB	10.8.110.0	255.255.252.0	10.8.190.0	255.255.252.0

Tabla 10.4. Resumen del direccionamiento de Palacio 1 y Palacio Oficinas.

			PALACIO 2		PALACIO 3	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf EXPOSITORES	50	1MB	10.1.120.0	255.255.252.0	10.1.130.0	255.255.252.0
	51	2MB	10.2.120.0	255.255.252.0	10.2.130.0	255.255.252.0
	52	4MB	10.4.120.0	255.255.252.0	10.4.130.0	255.255.252.0
	53	8MB	10.8.120.0	255.255.252.0	10.8.130.0	255.255.252.0

Tabla 10.5. Resumen del direccionamiento de Palacio 2 y Palacio 3

Configuración de los puertos.

Se crearan macros en cada switch de Accesos para la configuración de líneas de red de los expositores.

1 MB	2MB
macro name expositor1	macro name expositor2
descrip expositor_1Mb	descrip expositor_2Mb
switchport access vlan 50	switchport access vlan 51
switchport mode access	switchport mode access
service-policy input 1MB	service-policy input 2MB
speed auto 10	speed auto 10
srr-queue bandwidth limit 15	srr-queue bandwidth limit 20
shut	Shut
no shut	no shut
@	@

Tabla 10.6. Configuración de 1MB y 2MB.

4MB	8MB
macro name expositor4 descrip expositor_4Mb switchport access vlan 52 switchport mode access service-policy input 4MB speed auto 10 srr-queue bandwidth limit 40 shut no shut @	macro name expositor8 descrip expositor_8Mb switchport access vlan 53 switchport mode access service-policy input 8MB speed auto 10 srr-queue bandwidth limit 80 Shut no shut @

Tabla 10.7. Configuración de 4MB y 8MB.

Explicación de la configuración.

macroname X → (*Nombre de la macro*).
descrip expositor_1Mb→ (*Descripción del puerto*).
switchportaccessvlan X→ *(Vlan en el puerto).*
Switchport mode access→ *(El Puerto en modo vlan).*
service-policy input 1MB→ *(Ancho de banda de descarga).*
speed auto 10
srr-queuebandwidthlimit 15→(*Ancho de banda de subida*).
shut
noshut
@

1-Primero configuraremos una acces-list permitiendo todo el tráfico.

```
ip access-list extended MATCH_ACCES
                remark SELECCIONA EL TRAFICO ENTRANTE EN LOS PUERTOS DE ACCESO DE LOS
EQUIPOS DE ACCESO
permitipanyany
```

2-Crearemos un class-map para marcar el tráfico.

```
class-map match-all TRAFICO_EXPOSITORES//Marcarlo
        match access-group name MATCH_ACCES
```

3- Aplicamos el policy-map en la Vlan que deseamos

```
policy-map 8MB
                class TRAFICO_EXPOSITORES
                police 8000000 1000000 exceed-action drop
```

```
policy-map 4MB
class TRAFICO_EXPOSITORES
police 4000000 500000 exceed-action drop
policy-map 2MB
class TRAFICO_EXPOSITORES
police 2000000 250000 exceed-action drop
policy-map 1MB
class TRAFICO_EXPOSITORES
police 1000000 150000 exceed-action drop
```

10.2.2 VRF Oficinas

Para el personal del palacio de oficinas.

La tabla 10.8 muestra el direccionamiento de vrf OFICINAS. Como en los casos anteriores, el direccionamiento será 172.18.XY.0. En este caso "X" será la sucursal y "Y" el palacio. La máscara será "/24". En cada palacio dispondremos de 253 IP.

			PALACIO 1		PALACIO OFICINAS	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf OFICINAS	20	OFICINAS	172.18.11.0	255.255.255.0	172.18.19.0	255.255.255.0

			PALACIO 2		PALACIO 3	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf OFICINAS	20	OFICINAS	172.18.22.0	255.255.255.0	172.18.23.0	255.255.255.0

Tabla 10.8. Red de la vrf OFICINAS

Configuración de los puertos.

La configuración de los puertos de oficinas será:

```
descriptionOficinas
switchport access vlan X
switchport mode access
noshut
```

10.2.3 VRF internas

Las tres redes son similares. No tienen acceso de INTERNET, son redes internas. Estos direccionamientos serán 10.X.YZ0.0. “X” será la vlan de la vrf, “Y” la sucursal y “Z” el palacio.

La máscara de las redes será “/24”. Dispondremos de 253 IPs útiles para cada palacio. 10.X.YZ0.1 es para la puerta de enlace y 10.X.YZ0.255 es la broadcast. En la tabla 10.9. se visualiza las Vlans, IPs, máscara de cada palacio.

			PALACIO 1		PALACIO OFICINAS	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf CAMARAS	30	CAMARAS	10.30.110.0	255.255.255.0	10.30.190.0	255.255.255.0
vrf PLC	35	PLC ELECTRICIDAD	10.35.110.0	255.255.255.0	10.35.190.0	255.255.255.0
vrf TPV	40	TPV Restaurante	10.40.110.0	255.255.255.0	10.40.190.0	255.255.255.0

			PALACIO 2		PALACIO 3	
	VLAN	DESCRIPCION	RED	MASCARA	RED	MASCARA
Vrf CAMARAS	30	CAMARAS	10.30.220.0	255.255.255.0	10.30.230.0	255.255.255.0
vrf PLC	35	PLC ELECTRICIDAD	10.35.220.0	255.255.255.0	10.35.230.0	255.255.255.0
vrf TPV	40	TPV Restaurante	10.40.220.0	255.255.255.0	10.40.230.0	255.255.255.0

Tabla 10.9.Resumen del direccionamiento de vrf.

Configuración del puerto.

```
description X
switchport access vlanX
switchport mode access
storm-control broadcast level 1.00
storm-control action shutdown
spanning-treeportfast
spanning-treebpdufilter enable
spanning-tree guard root
noshut
```

11. Encaminamientos

11.1 Vrf Expositores

Primero configuraremos los Distribuciones de los palacios, la vrf de Expositores. Para ello configuramos el AS de Feria de Valencia con el "route-distinguisher" (RD). La red Expositores la propagaremos por todos los equipos por el protocolo BGP.

```
ipvrf EXPOSITORES
rd 65501:5
route-target export 65501:5
route-target import 65501:5
!
routerbgp 65501
address-family ipv4 vrf EXPOSITORES
redistribute connected
no synchronization
exit-address-family
!
```

Los Distribuciones serán los responsables que hagan de servidores DHCP. La configuración estándar se muestra en la tabla 11.1.

Ejemplo de configuración del servidor DHCP	
ipdhcp pool exp1	Nombre del pool
vrf EXPOSITORES	Pertenece a la vrf EXPOSITORES
network 10.1.108.0 255.255.252.0	El rango de IPs que asignaremos a los host
default-router 10.1.110.1	Puerta de enlace
dns-server 8.8.8.8 8.8.4.4	DNS públicos para acceder a INTERNET
lease 0 1	El tiempo que tendrá el host asignado la ip."0" días y 1 hora.
!	

Tabla 11.1 Configuración DHCP de vrf Expositores.

Configuración del Nivel 3 de los Distribuciones (tabla 11.2).

interface Vlan X	Interface de Expositores
ipvrf forwarding EXPOSITORES	Pertenece a la vrf Expositores.
ipaddress 10.1.110.1 255.255.252.0	Puerta de enlace
!	

Tabla 11.2 Configuración de nivel 3 de las vlans.

Ahora en los Distribuciones de INTERNET.

```
ipvrf EXPOSITORES
rd 65501:5
route-target export 65501:5
route-target import 65501:5
!
address-family ipv4 vrf EXPOSITORES
redistribute connected metric 200
redistribute static metric 200
default-information originate
default-metric 200
no synchronization
bgp dampening
exit-address-family
!
```

La Fig. 11.1. muestra como vrf EXPOSITORES tiene conectividad por el protocolo BGP. La red conoce la IP 192.168.224.160 que será conectividad con el Firewall ASA y sabrá que el host es el D-INET.

```
P01#sh ip bgp vpnv4 vrf EXPOSITORES
BGP table version is 15, local router ID is 192.168.101.1
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
Route Distinguisher: 65501:5 (default for vrf EXPOSITORES)
*> 10.1.108.0/22    0.0.0.0                  0         32768 ?
*> 10.2.108.0/22    0.0.0.0                  0         32768 ?
*> 10.4.108.0/22    0.0.0.0                  0         32768 ?
*> 10.8.108.0/22    0.0.0.0                  0         32768 ?
*>i192.168.224.160/28
                    192.168.200.3          200    100      0 ?
```

Fig. 11.1. vrf EXPOSITORES con el protocolo BGP.

11.2 Vrf Oficinas

Todas las vrfs tienen comunicación por BGP en los Distribuciones, inclusive con los equipos de INTERNET. En INTERNET cambiaremos de vlan de oficinas. Es decir, los Distribuciones será la vlan 20, en cambio en Distribuciones de INTERNET será la vlan 29.

Distribución de los Palacios	Explicación
ipvrf OFICINAS rd 65501:1 route-target export 65501:1 route-target import 65501:1 ! Rouert BGP address-family ipv4 vrf OFICINAS redistribute connected no synchronization exit-address-family ! interface Vlan20 description OFICINAS ip vrf forwarding OFICINAS ip address 172.18.11.1 255.255.255.0 no autostate !	Creamos la vrf. El direccionamiento se muestra en tabla de enrutamiento con el protocolo BGP. Nivel 3 de la vrf de oficinas.

Tabla 11.3.Creación de Vrf OFICINAS.

Distribución INTERNET	Explicación
address-family ipv4 redistribute connected metric 200 redistribute static metric 200 neighbor 192.168.100.1 activate neighbor 192.168.200.1 activate default-information originate default-metric 200 no auto-summary no synchronization bgp dampening exit-address-family !	Descripción del Host en el protocolo BGP.

Tabla 11.4. Configuración de nivel 3 de las vlans.

11.3 Vrf Internas

La vrfs internas serán Cámaras, PLC y TPV. Estas no tienen acceso a INTERNET.

Configuración estándar:

ipvrf CAMARAS rd 65501:30 route-target export 65501:30 route-target import 65501:30 ! ! interface Vlan30 description CAMARAS ipvrf forwarding CAMARAS ip address 10.30.110.1 255.255.255.0 no sh ! router bgp 65501 ! address-family ipv4 vrf CAMARAS no synchronization redistribute connected exit-address-family ! vlan 30 !	Creamos la vrf con el nombre correspondiente. Creamos la interface de nivel 3 dentro la vrf Direccionamiento Se configura el protocolo BGP Se distribuye los direccionamientos Creamos la vlan

Tabla 11.5.Ejemplo de configuración de vrf internas.

Tal como muestra la tabla de enrutamiento de las vrf internas, No tendrán salida a INTERNET, solo visualizarán las otras redes de los otros palacios.

```
D-P02#sh ip bgp vpnv4 vrf CAMARAS
BGP table version is 82413, local router ID is 192.168.202.1
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
Route Distinguisher: 65501:30 (default for vrf CAMARAS)
*>i10.30.110.0/24   192.168.201.1            0    100      0 ?
*> 10.30.220.0/24   0.0.0.0                  0         32768 ?
D-P02#pi
D-P02#ping vrf
D-P02#ping vrf CAMARAS 10.30.110.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.110.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Fig. 11.2. Rutas del protocolo BGP en la vrf Cámaras.

12. Conclusiones

El objetivo de este proyecto se ha cumplido se ha diseñado un red pensando en cubrir la necesidades de Feria de Valencia

Para ello, se ha decidido usar el protocolo global es decir, MPLS. Las redes se han dividido proporcionando una mayor seguridad (VPN). MPLS permite ofrecer QOS, lo cual será una mejora para el futuro. Esto nos permitirá un servicio de priorización.

El diseño de la infraestructura y el dibujo de topología de la red ha sido diseñada para que el cliente pueda disfrutar de una red de altas prestaciones. Por otra parte podemos decir que Feria dispone de una red fácilmente escalable.

Los CORES disponen de puertos libres para la construcción de futuros palacios y los Distribuciones de los palacios podrán tener más Accesos si el cliente lo desea.

Todas las líneas de conexión a los equipos han sido redundadas para mejorar el ancho de banda y proporcionar una mayor velocidad logrando así, no perder las conexiones de los usuarios. Además con la contratación de 2 ISPs Feria de Valencia dispondrá de alta disponibilidad.

Por ello podemos decir que Feria de Valencia es una red segura.

13. Referencias

Libros consultados:

[1] Libro CCNA (CiscoCertified Network Associate)

[2] Libro CCNP of Route (Cisco Certified Network Professional)

[3] Libro CCIP (Cisco Certified INTERNET Professional)

[4] Libro CCDA (Cisco Certified Desing Associate)

Enlaces webs:

[5] http://es.wikipedia.org/wiki/Wikipedia:Portada

[6] http://www.ramonmillan.com/tutoriales/mpls.php

[7] http:// www.cert.uy/historico/.../Presentación%2002%20-%20MPLS-VPN.p...

[8] http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_ example09186a0080093f23.shtml

[9] https://learningnetwork.cisco.com/thread/25187

[10] http://www.netcraftsmen.net/resources/archived-articles/373.html

[11] http://www.slideshare.net/thiland/BGPPub

[12] http://www.ietf.org/rfc/rfc4364.txt

[13] http://najcolabs.com/?p=149

[14] https://learningnetwork.cisco.com/thread/26628

[15] http://fengnet.com/book/ios_mpls/ch05lev1sec1.html

14. Presupuesto

Realizamos un presupuesto para tener conocimiento de la inversión necesaria.

14.1 Presupuesto de mano de obra

El precio de la hora de este proyecto será de 25 euros/hora.

TAREA	NUMERO DE HORAS	COSTE
Búsqueda de información y consulta de manuales	150	3750
Redacción de memoria y presupuesto	150	3750
Viajes Diestas y reuniones	20	500
	Total:	8000
	Coste hora:	25

Tabla 14.1. Presupuesto mano de obra

14.2 Presupuesto de los switches y placas.

Precios de los equipos

Chais	Unidades	Building-blocks	Precio
WS-C6509-E	4	CORES	34.200,00 €
Chais	Unidades	Building-blocks	Precio
CISCO7606-S	4	DISTRIBUNET	94.050,72 €
Chais	Unidades	Building-blocks	Precio
WS-C6509-E	2	SERVIDORES	17.100,00 €
Chais	Unidades	Building-blocks	Precio
WS-C6509-E	2	INTERNET	17.100,00 €

Tabla 14.2.Presupuesto Chasis.

Placas	UNIDADES	Building-blocks	Precio
WS-X6724-SFP	4	CORES	37.620,20 €
VS-S720-10G	4	CORES	93299,76
WS-X6704-10GE	4	CORES	50.160,40 €
Placas	UNIDADES	Building-blocks	Precio
WS-X6408A-GBIC	4	DISTRIBUCIONES	20.432,52 €
WS-SUP32-GE-3B	8	DISTRIBUCIONES	75.240,40 €
Placas	UNIDADES	Building-blocks	Precio
WS-X6704-10GE	2	SERVIDORES	25.080,20 €
WS-X6748-GE-TX	2	SERVIDORES	18.810,10 €
WS-X6548-GE-TX	1	SERVIDORES	7.718,11 €
VS-S720-10G	2	SERVIDORES	46649,88
Placas	UNIDADES	Building-blocks	Precio
WS-X6724-SFP	2	INTERNET	18.810,10 €
WS-X6548-GE-TX	2	INTERNET	15.436,22 €

Tabla 14.3. Presupuesto Placas.

14.3 Presupuesto de los Firewall

Firewall	Unidades	Precio
NOKIA IP 390	2	2037,06
ASA 5510	2	4.315,56

Tabla 14.4. Presupuesto de los Firewalls.

14.4 Presupuesto de los SAIS

MODELO	UNIDADES	PRECIO
SUA750RMI2U	14	6095,04
UPS-RT-5000-VA	2	6215,24

Tabla 14.5. Presupuesto de los SAIS.

14.5 Presupuesto de los Path Panels

MODELO	UNIDADES	PRECIO
Path Panel	27	1728
LIU	28	3696

Tabla 14.6. Presupuesto de los Path panels

.

14.6 Presupuesto Total

Chasssis	Precio Total	162.450,72 €
Placas	Precio Total	409.257,89 €
Firewall	Precio Total	6.352,62
SAIS	Precio Total	12.310,28
Path Panel	Precio Total	5.424,00
TAREA	Precio Total	8.000,00
	Precio Total	603.795,51 €

Tabla 14.7. Presupuesto Total