Diseño de una red corporativa

Autora: Anna Obis Joan
Consultor: Antoni Morell Pérez
TFC-Integració de xarxes telemàtiques
Semestre 2013-2014

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN

Nosotros, como empresa proveedora intermedia (entre ISP y cliente) hemos diseñado el proyecto "Diseño de una red corporativa" que tiene el objetivo de implementar una red ip de datos y voz que comunique las 4 oficinas más importantes de una empresa cliente.

Para entender cual es el objetivo de este proyecto primero necesitamos saber que es una red corporativa. Una red corporativa permite comunicar o conectar todas las oficinas o delegaciones de una empresa cliente de forma privada, permanente y segura.

Por lo tanto, la solución está diseñada a medida de las necesidades presentadas por el cliente dotando al mismo de una comunicación completa y creando, al mismo tiempo, una red estable y convergente que optimiza los tiempos de respuesta.

Por otro lado, la telefonía ip, a parte de dotar al cliente de una comunicación de voz fiable, le proporcionará una base para ofrecer aplicaciones de comunicaciones más avanzadas, como por ejemplo videoconferencias o conferencias en línea y sobretodo la posibilidad de reducir en gastos ya que se aprovechará la red de datos existente para transportar la voz.

Para asegurar la correcta implementación del proyecto se realizarán reuniones de seguimiento semanales con el cliente y se le proporcionará asesoramiento técnico siempre que éste lo necesite.

1.2 OBJECTIVOS

La solución propuesta se basa en diferentes niveles de implantación de servicios, basados en infraestructuras de comunicaciones de red ip y equipamientos de voz y datos.

Por lo tanto, el presente documento tiene como objetivo la implementación de los siguientes grandes bloques:

- **Red WAN:** Red corporativa que conectara las dos delegaciones centrales del cliente de Madrid y Barcelona basada en tecnología de fibra con caudal simétrico.
  Se trata de una mejora en la red existente del cliente, a la que se le realiza una ampliación de caudal y una conexión más fiable y rápida.
  Para realizar la conexión se aprovisionarán un equipo cisco y un enlace de fibra a la red. Para dotar de redundancia al cliente en caso de fallos de equipamiento y/o caída de las líneas existentes, se aprovisionará también un equipo backup, de idénticas características para redundar el servicio y reducir puntos de falla.

- **Red LAN:** Se compone de toda la electrónica de LAN (switchs), que dan servicio a los edificios principales del cliente, que están interconectados a través de fibras.
  El proyecto contempla la total renovación de los switchs de planta del cliente, dando conexión a servidores, usuarios finales (PCs y Teléfonos IP) y disponiendo de puertos de enlace para la interconexión a las demás oficinas de la misma ciudad.

- **Sistema de Telefonía IP:** Se compone de una solución completa que da servicio de telefonía IP, basada en equipamiento Alcatel, a los principales edificios del cliente.
  Por otro lado, se aprovisionará equipamiento necesario para conservar la tecnología analógica existente (faxes, módems, terminales...).

- **Cableado:** Contempla el cableado necesario para interconectar los switchs de cliente dentro del mismo edificio.

- **Alimentación hardware de red:** Contempla la instalación de SAI's para la alimentación de la electrónica de red LAN. Los equipos de voz ip van aprovisionados con baterías propias del fabricante.

1.3 METODOLOGÍA

Después de diseñar con la ayuda del cliente una solución a su medida que se ajuste a las necesidades que requiere el servicio; se ha de estructurar un orden de implementación. De todos modos, antes de diseñar un orden de implementación deberemos tener en cuenta los siguientes puntos:

1. En la primera fase el cliente nos solicita que mejoremos su red WAN actual aportando más ancho de banda disponible y un caudal simétrico entre sus oficinas centrales. También nos solicita una conexión más fiable que la actual y con mayor redundancia.

2. Los edificios de Barcelona2 y Madrid 2 pertenecen a la fase 3, por lo que previamente se tienen que realizar la migración de los edificios de la fase 2 (Barcelona 1 y Madrid 1).

3. La instalación de los equipos de telefonía no se podrá realizar hasta retirar la electrónica de backbone antigua. Por ese motivo antes de realizar la instalación de los equipos de telefonía se tiene que realizar la migración de la LAN a los nuevos switchs.

4. En la última fase se instalará un sistema "backup" del circuito principal de WAN que conecta las dos oficinas centrales. Se contempla como la última fase ya que antes de realizar esta implantación necesitamos que Las centrales estén conectadas a nivel 2 con las delegaciones.

Por lo tanto la implementación se dividirá en 4 grandes fases:

1. Diseño de la solución
2. Modificación e implementación de la red WAN principal.
3. Implementación de la red LAN.
4. Implementación de VOIP.
5. Implementación de la red WAN redundante.

1.4 DESCRIPCIÓN DE LAS FASES

<u>Diseño de la solución</u>

Queremos identificar las necesidades del sistema de comunicaciones actual para realizar la renovación tecnológica en los centros principales de la empresa cliente de forma coherente a sus necesidades.

Los pasos son:

1.- Estudio de la situación actual de cliente.
2.- Diseño de una propuesta de mejora.
3.- Aceptación de la oferta por parte de cliente.

Modificación e implementación de la red WAN principal

Comprende la instalación, configuración y puesta en marcha de las líneas, circuitos y hardware de red de cada una de las sedes centrales del cliente, Madrid1 y Barcelona1.

Implementación de la red LAN

Contempla el subministro, instalación y configuración de toda la solución de switching acordada que incluye el hardware de red (switchs), cableado vertical de conexión entre equipos y alimentación.

Implementación de VOIP

Implantación y puesta en marcha de la solución VOIP que incluye el subministro de todo el equipamiento contemplado en al oferta y la configuración del mismo.

Implementación de la red WAN redundante.

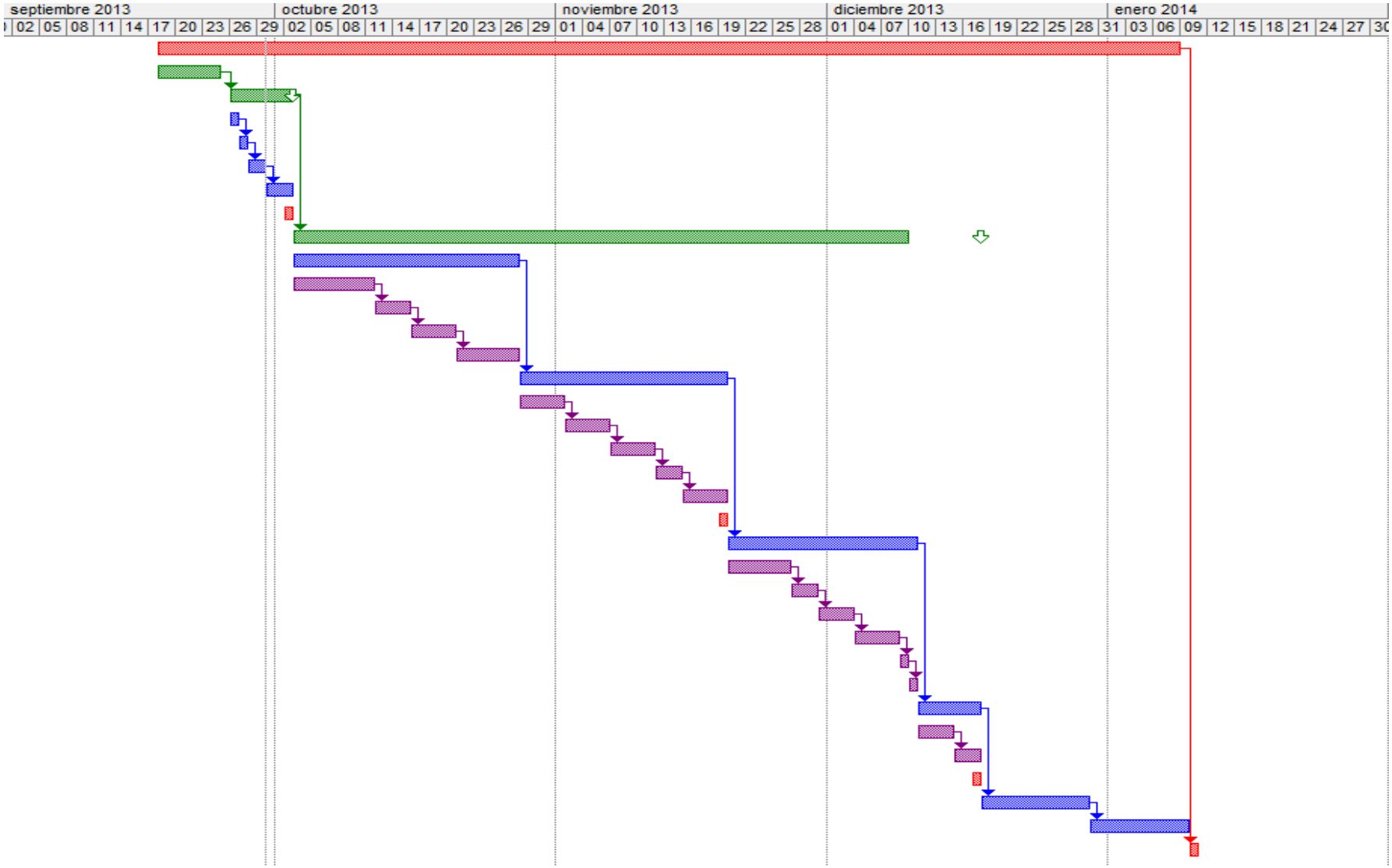
Contempla la implantación de la solución de contingencia en caso de fallo en el acceso WAN principal.

2 PLANIFICACIÓN

2.1 PLANIFICACIÓN Y DURACIÓN

En este apartado se describen las actuaciones necesarias para garantizar que podremos proporcionar la solución pactada con el cliente en los plazos y términos previstos, y que estos elementos cumplirán las especificaciones técnicas necesarias acordadas y descritas durante la presentación de la solución.

1	**PROYECTO TFC**	94 días	jue 19/09/13	jue 09/01/14
2	Decisión del proyecto	5 días	mié 18/09/13	mar 24/09/13
3	**PRIMERA PARTE INTRODUCTORIA**	7 días	jue 26/09/13	mié 02/10/13
4	Introducción	1 día	jue 26/09/13	jue 26/09/13
5	Planificación	1 día	vie 27/09/13	vie 27/09/13
6	Situación actual del cliente	2 días	sáb 28/09/13	dom 29/09/13
7	Solución propuesta	3 días	lun 30/09/13	mié 02/10/13
8	ENTREGA PAC1	1 día	mié 02/10/13	mié 02/10/13
9	**SEGUNDA PARTE - IMPLEMENTACIÓ**	56 días	jue 03/10/13	lun 09/12/13
10	RED WAN	22 días	jue 03/10/13	dom 27/10/13
11	Conceptos teóricos	8 días	jue 03/10/13	vie 11/10/13
12	Material contemplado	4 días	sáb 12/10/13	mar 15/10/13
13	Descripción del hardware contemplad	4 días	mié 16/10/13	dom 20/10/13
14	Configuración	6 días	lun 21/10/13	dom 27/10/13
15	RED LAN	18 días	lun 28/10/13	mar 19/11/13
16	Conceptos teóricos	5 días	lun 28/10/13	vie 01/11/13
17	Material contemplado	4 días	sáb 02/11/13	mié 06/11/13
18	Descripción del hardware contemplad	3 días	jue 07/11/13	lun 11/11/13
19	Alimentación equipos	3 días	mar 12/11/13	jue 14/11/13
20	Configuración	3 días	vie 15/11/13	mar 19/11/13
21	ENTREGA PAC2	1 día	mar 19/11/13	mar 19/11/13
22	RED TELEFONIA	17 días	mié 20/11/13	mar 10/12/13
23	Conceptos teóricos	5 días	mié 20/11/13	mar 26/11/13
24	Material contemplado	3 días	mié 27/11/13	vie 29/11/13
25	Descripción del hardware contemplad	3 días	sáb 30/11/13	mar 03/12/13
26	Configuración	4 días	mié 04/12/13	dom 08/12/13
27	Líneas públicas	1 día	lun 09/12/13	lun 09/12/13
28	Sistema rescate	1 día	mar 10/12/13	mar 10/12/13
29	ANEXO	7 días	mié 11/12/13	mar 17/12/13
30	RED WAN	4 días	mié 11/12/13	sáb 14/12/13
31	RED LAN	3 días	dom 15/12/13	mar 17/12/13
32	ENTREGA PAC3	1 día	mar 17/12/13	mar 17/12/13
33	**CONCLUSIÓN**	9 días	mié 18/12/13	dom 29/12/13
34	**BIBLIOGRAFIA**	9 días	lun 30/12/13	jue 09/01/14
35	ENTREGA FINAL PROYECTO	1 día	vie 10/01/14	vie 10/01/14


septiembre 2013
octubre 2013
noviembre 2013
diciembre 2013
enero 2014
02 05 08 11 14 17 20 23 26 29 02 05 08 11 14 17 20 23 26 29 01 04 07 10 13 16 19 22 25 28 01 04 07 10 13 16 19 22 25 28 31 03 06 09 12 15 18 21 24 27

3 SITUACIÓN ACTUAL DEL CLIENTE

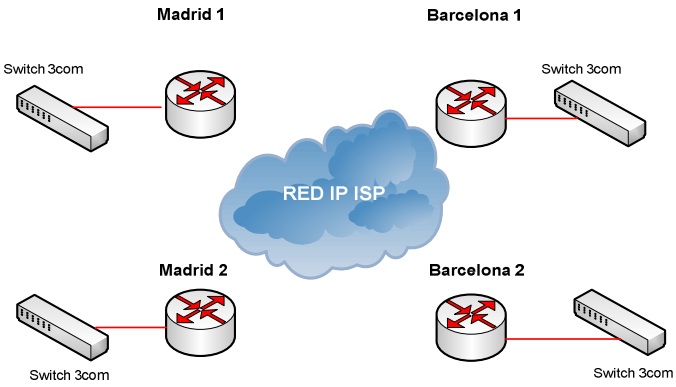
3.1 UBICACIÓN DE LAS OFICINAS

Actualmente el cliente dispone de dos oficinas centrales, una en Barcelona y la otra en Madrid. Dentro de ambas provincias existen varias delegaciones. En este proyecto tendremos en cuenta dos oficinas o delegaciones más, una en Madrid y otra en Barcelona.
La red de comunicación se dejará preparada para una futura ampliación que contemple las demás delegaciones en un segundo proyecto.

Para localizar más fácilmente las oficinas las llamaremos a las centrales Madrid1 y Barcelona 1 y a las delegaciones Madrid 2 y Barcelona2.

3.2 MAPA DE RED ACTUAL

Esquema genérico de la situación actual



El cliente dispone de una red WAN contratada con su ISP con una tecnología de acceso ADSL con un caudal contratado asimétrico de 8M/640k para comunicar todas las oficinas entre si. Se dará de baja este servicio con la correspondiente retirada de líneas y hardware de red.

Para la conexión de puestos de trabajo el cliente actualmente dispone de varios switch del fabricante 3com. Se mantendrán como añadido a la futura red LAN para dar servicio a usuarios finales.

Por otro lado, como sistema de voz, actualmente dispone de una centralita de voz Netcom Dkda 9 con teléfonos digitales y analógicos que conservaremos para su futura convivencia con el sistema de telefonía ip. Se retirará el equipo “centralita” Dkda de las 4 oficinas.

Finalmente, conservaremos todo el cableado UTP Cat 5e en buen estado de cliente para cablear los nuevos puestos de trabajo. En este proyecto solo contemplaremos el cableado para conectar los switch. El sistema de cableado horizontal será aprovisionado por cliente.

3.3 SALAS DE COMUNICACIÓN DEL EDIFICIO

- **Barcelona 1:** Existe una sala técnica principal, ubicada en la segunda planta.
  En esta sala disponemos de un rack de comunicación para soportar cableado horizontal de la segunda planta y el cableado vertical con la sala de la primera planta. Se aprovecharán los bastidores de comunicaciones de ambas plantas para alojar la nueva electrónica de red. Es necesario la instalación de de un panel de fibra.

- **Barcelona 2:** La sala técnica principal esta ubicada en la planta baja detrás de recepción. Existe un rack de comunicación con cableado diferenciado para voz y datos. El cableado de datos es de categoría 5e. El cableado de voz no es de categoría 5 y se debe cambiar por parte de cliente. Por otro lado no …
  Finalmente Se aprovecharán los bastidores de comunicaciones de ambas plantas para alojar la nueva electrónica de red. Aunque es necesario la instalación de de un panel de fibra.

- **Madrid 1:** La sala técnica principal esta ubicada en la primera planta y la sala secundaria en la tercera. Ambas salas están dentro del espacio de oficinas y son fácilmente accesibles. Se deberá preveer la renovación de armarios y paneles para substituir todo el cableado existente por uno nuevo tipo patch see. Este trabajo debe hacerlo cliente y se contempla mientras se esta realizando la implantación de Barcelona 1. Se aprovecharán los bastidores de comunicaciones de ambas plantas para alojar la nueva electrónica de red. Es necesario la instalación de de un panel de fibra.

- **Madrid 2:** Existe una única sala técnica ubicada en la planta baja. El espacio en el bastidor es suficiente para alojar toda la electrónica de red y el hardware de VOIP.
  Dispone de un panel de fibra que podemos utilizar.

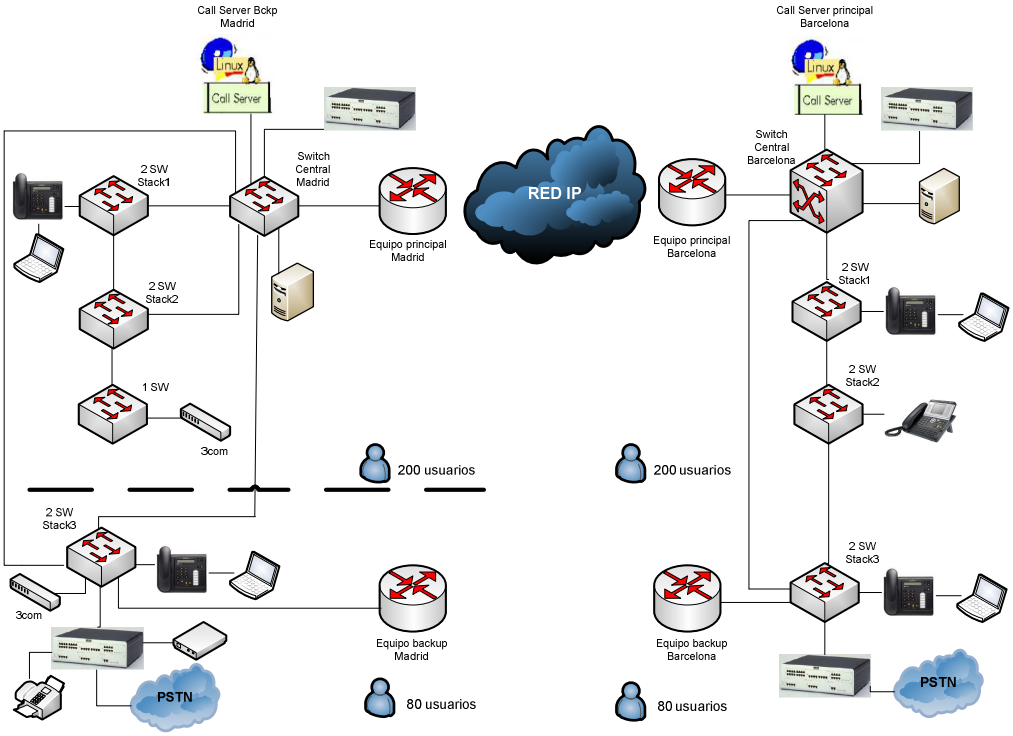
4 SOLUCION PROPUESTA

4.1-MAPA DE RED A IMPLANTAR

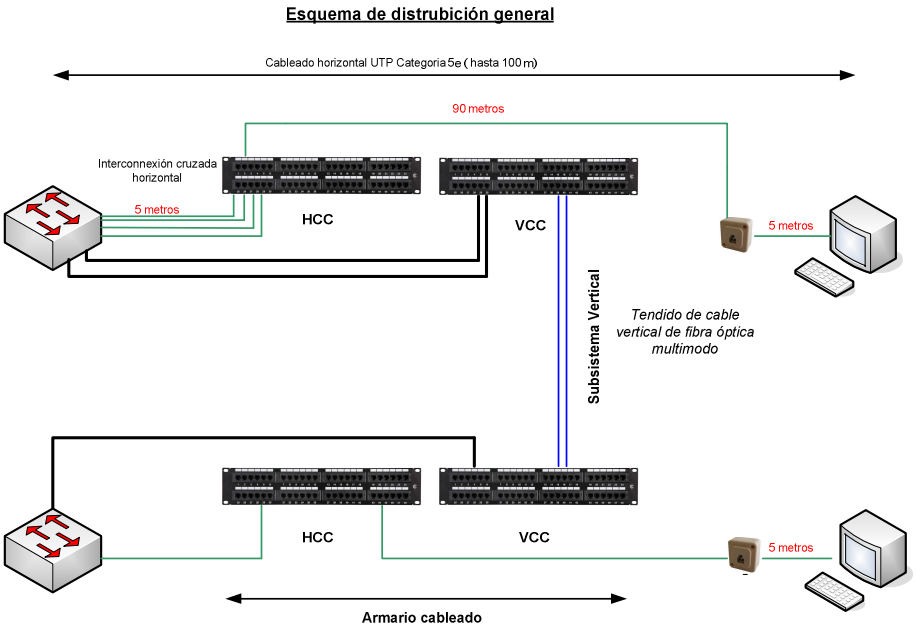
Como podemos observar en el mapa de red el cliente dispone de 4 oficinas, dos centrales y dos delegaciones en la misma capital. A nivel de red WAN se conectaran las oficinas Barcelona1 y Madrid 1 con tecnología de fibra y caudal simétrico de 100Mb. Se dispondrá de un sistema backup con las mismas características en Barcelona 2 y Madrid 2 de modo que si falla el acceso de Barcelona1 el tráfico se enrutará a través de Barcelona 2 hacia Madrid y si falla el acceso de Madrid 1 el enrutamiento del tráfico de Madrid a Barcelona se realizará a través de Madrid2.

Respecto a la red LAN dispondremos de un switch núcleo/CORE en Barcelona 1 y Madrid 1 que será capaz de trabajar a nivel 3 y gestionar el tráfico de la LAN. Todos los enlaces entre switch dentro de la misma oficina son mediante latiguillos de fibra multimodo.
El enlace de Barcelona 1 con Barcelona2 y Madrid 1 con Madrid 2 se establecerá a nivel 2 mediante fibras monomodo.

Finalmente para la red de voz dispondremos de dos centralitas, una en Barcelona 1 y otra en Madrid 1.Cada una dará servició a la oficina central de la provincia y sus delegaciones. También dispondremos de 4 Mediagateways, por un lado, para conectar la telefonía tradicional y, por otro lado, para realizar las funciones de rescate.



4.2-ESQUEMA GENÉRICO CONEXIONES EDIFICIO



En las instalaciones de los edificios que dispongan más de una planta, se realizará una distribución vertical que interconectará los equipos de comunicación situados en las diferentes plantas.

Por otro lado, disponemos de paneles de conexión cruzada horizontal y cableado HCC que se utiliza para conectar el cableado horizontal con los puertos del switch y el cableado horizontal para transportar el tráfico ip por la planta que será RJ-45 UTP categoría 5e y conectará el puesto de trabajo con el armario de comunicaciones. La distancia máxima serán 100m.

Finalmente, el enlace de fibra óptica monomodo entre edificios deberá hacerlo el ISP contratado.

4.3-RESUMEN SERVICIOS AFECTADOS

4.3.1- Red WAN

Actualmente se dispone de un enlace ADSL de caudal asimétrico 8 Mb/640 kb en las cuatro oficinas de la empresa cliente, las dos centrales y las dos delegaciones. El escenario de red va a cambiar y aprovisionaremos un acceso a la red de fibra con un caudal contratado simétrico 100 Mb y un equipo router Cisco Catalyst 3560 en las oficinas Barcelona 1 y Madrid 1.

También se incluye un equipo backup del servicio en la oficina Barcelona1 y Madrid 1 con características idénticas al principal que se aprovisionará en la última fase de la implantación.

4.3.2- Red LAN

Crearemos una red LAN que no solo conectara las estaciones de trabajo de un mismo edificio sino que conectara las centrales con sus delegaciones de la misma ciudad.

Esta nueva solución se plantea para mejorar la red existente. Teniendo en cuenta que la distancia entre las oficinas Barcelona 1 y Barcelona 2 y entre Madrid 1 y Madrid 2 no supera los 2 kilómetros y medio se propone crear un enlace de nivel 2 por fibra creando una sola red LAN entre ambas oficina proporcionando una conexión más rápida y eficaz con menos errores y retardos.

Para interconectar estas redes y dar acceso a los usuarios aprovisionaremos equipos switchs. Concretamente, por un lado, aprovisionaremos el modelo cisco Catalyst 3750 series, muy adecuado como switch de acceso ya que implementa la tecnología StackWise que nos aporta flexibilidad y puede funcionar a nivel 3 con lo que lo podemos incluir en el CORE de la LAN. Por otro lado para el CORE de la red de Barcelona usaremos el modelo cisco Catalyst 6500 series que tiene una alta densidad de puertos y además cisco lo recomienda como switch de capa de núcleo por su gran capacidad de procesamiento.

En otro sentido, se aprovecharán los switch 3com de cliente para conexión de usuarios sin terminal ip. La instalación de estos equipos será responsabilidad de cliente aunque nosotros configuraremos nuestra interfaz para su conexión a nuestros equipos.

Finalmente, los equipos deberán ir correctamente etiquetados antes de colocarlos en el rack de comunicaciones.

4.3.3- Cableado

Barcelona

- Instalación de un nuevo armario en la sala de comunicaciones de Barcelona 1.
- Instalación de un panel de fibra en el armario.
- Latiguillos de fibra óptica multimodo (conectores SC-LC) de 3 metros para conexión entre switch de la misma sala técnica.
- Cometidas de fibra óptica multimodo para interconectar la sala técnica secundaria con la sala técnica principal en los edificios de más de un CPD.

Madrid

- Instalación de un nuevo armario en la sala de comunicaciones de Madrid 1.
- Instalación de un panel de fibra en el armario.
- Latiguillos de fibra óptica multimodo (conectores SC-LC) de 3 metros para conexión entre switch de la misma sala técnica.
- Cometidas de fibra óptica multimodo para interconectar la sala técnica secundaria con la sala técnica principal en los edificios de más de un CPD.

4.3.4- Alimentación

Los equipos de LAN estarán alimentados y protegidos mediante SAIs.

Se instalarán varios tipos de SAI según la potencia requerida. Funcionan a 220 V con cable de 10 A para el 850 y para el 3000 con baterias un cable de 16 A. El cable de entrada viene con toma IEC por un lado y con Schucko en el otro extremo para la alimentación del mismo.

Las tomas de salida que llevan cada SAI están protegidas con batería y contra sobretensiones. El número de tomas por modelo de SAI es el siguiente.

- Evolution 850: 4 tomas IEC de 10 A
- Evolution 3000: 1 toma IEC 16 A y 8 tomas de IEC 10 A

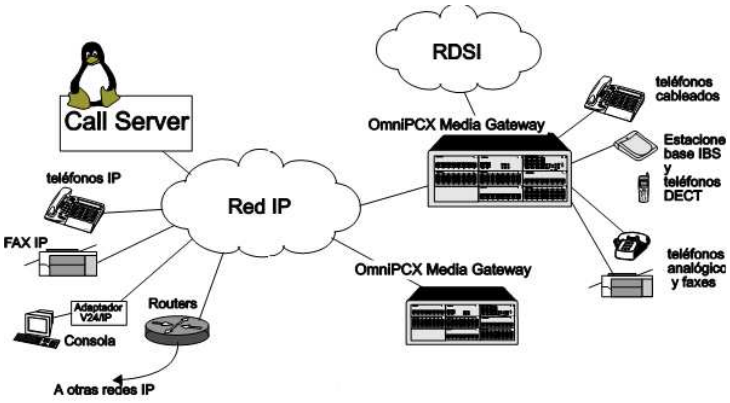
4.3.5- Telefonía IP

Como unidad de control e inteligencia del sistema VOIP OXE instalaremos una centralita OmniPCX Enterprise Call Server (servidor de llamadas) en cada oficina central. La centralita principal estará alojada en la oficina central Barcelona 1 y la centralita backup estará alojada en la central Madrid 1. Ambas centralitas se comunicarán gracias a la red WAN. Cuando exista un problema de comunicación entre Barcelona y Madrid ambas centralitas levantaran como principal dando servicio a todas oficinas de ambas capitales.

Para conservar la parte correspondiente a la telefonía analógica existente se aprovisionará un equipo OmniPCX mediagateway hardware común por oficina.

Con estos equipos se realizará la conexión de líneas analógicas de módems y calefacción, los terminales digitales, analógicos y faxes.

Para la parte de VOIP se aprovisionarán terminales ip Alcatel IPTOUCH modelos 4018,4028 y 4068 para poder disfrutar de las ventajas que ofrece la telefonía ip.



5 DATOS IMPLEMENTACIÓN

5.1 – WAN

5.1.1 – Conceptos teóricos

¿Que es una red WAN?

Es una red de área amplia que por lo tanto, cubre una extensa área geográfica y a menuda utiliza instalaciones de proveedores de servicio de telecomunicaciones (ISP) como por ejemplo compañías telefónicas. Básicamente sirve para interconectar las diferentes redes LAN del cliente.

Como dispositivo de esta red se utilizan los routers ya que operan en capa 3 del modelo OSI tomando decisiones basadas en el direccionamiento de red.

La función del router es la de seleccionar la mejor ruta para la conmutación de tramas hacia la interfaz que corresponda.

Finalmente, en la red WAN siempre se paga a la operadora el alquiler de la líneas y servicios añadidos.

¿Que es un protocolo de routing?

El routing consiste en redireccionar paquetes ip por diferentes enlaces en función de su destino y origen. Para ello es necesario, como hemos comentado, usar un dispositivo router. El router es el encargado de mantener una tabla de rutas donde se reflejan las redes que conoce el router y por donde alcanzarlas.

La tabla de rutas de un router se completa con varias estrategias:

- Con las redes directamente conectadas.
- Por medio de rutas estáticas.
- Gracias a protocolos de routing dinámico.

Por lo tanto, existen dos tipos de enrutamiento, el enrutamiento estático y el dinámico:

Enrutamiento Estático	Enrutamiento Dinámico
Necesita la supervisión de un administrador de la red y puede consumir gran tiempo de trabajo de éste. El administrador necesitará configurar manualmente el enrutamiento de cadared en el router.	No genera mucha carga administrativa ya que son los propios routers quien gestionan el enrutamiento con los demás routers de la red.
El router no comparte su tabla de enrutamiento con los routers vecinos.	El router comparte su tabla de enrutamiento con los routers vecinos.
Al no aprender la rutas de forma dinámica los routers tienen poca capacidad de reacción ante un fallo imprevisto en la red.	Los routers aprenden de forma dinámica las diferentes redes y tienen total capacidad de reacción ante un cambio en la red.

- Enrutamiento estático:
  El routing estático tiene la ventaja de que no sobrecarga los routers ni los enlaces y es sencillo de configurar y entender a simple vista.
  Lo administra y configura el administrador de la red y todas las rutas estáticas que éste ingrese son las que el router conocerá, de esta manera sabrá enrutar el tráfico hacia en host destino.
  El problema del routing estático es que si ampliamos las redes de host tendremos que añadir una línea de configuración a cada router y en redes grandes esto hace que el mantenimiento sea laborioso y se puedan generar muchos errores. Con routing dinámico usamos un protocolo de routing que establece las rutas de red con unos pocos comandos de configuración, simplificando el mantenimiento de la red y la posible ampliación de ésta.

- Enrutamiento dinámico:
  Esta tipo de protocolos se usan en los routers para descubrir de forma automática las nuevas rutas quitando trabajo a los administradores de la red dejando que ésta se regule de una forma automática.
  A pesar de estas ventajas produce un mayor consumo de ancho de banda y potencia del procesador en tareas de adquisición y mantenimiento de información de enrutamiento.

  En este tipo de enrutamiento tenemos tres clases:
  - *Vector-Distancia*: estos protocolos determinan la mejor ruta por el número de saltos hasta el destino. Cada paso por un router es un salto (hop). IGRP y RIP usan vector distancia para calcular rutas

  - *Estado-Enlace*: se usan tres tablas de rutas, en una se mantiene el estado de los routers vecinos, en otra se establece la topología completa de la red, la última es la tabla de rutas. OSPF es un protocolo de estado de enlace.

  - *Híbrido*: los protocolos híbridos usan elementos de Vector Distancia y de Estado Enlace, Por ejemplo EIGRP.

Vector Distancia	Estado de enlace
Vista de la topología de la red desde la perspectiva del vecino	Consigue una vista común de toda la topología de la red
Añade vectores de distancias de router a router	Calcula la ruta más corta hasta otros routers
Frecuentes actualizaciones periódicas, convergencia	Actualizaciones activadas por eventos, convergencia

En la convivencia de ambos tipos de enrutamientos aparece la distancia administrativa o métrica que es una medida de la veracidad de información de routing procedente de un router vecino. Es un entero de 0 a 255, donde 0 es la preferida o más fiable. En caso de una AD igual entrarían en juego las métricas del protocolo de routing. Si ambos valores son iguales se hace balanceo de cargas entre ambas rutas.

Entonces, el router ejecuta más de un protocolo de enrutamiento obtenido a partir de varias fuentes usará la ruta que provenga de la fuente con menor distancia administrativa. Tener en cuenta la distancia administrativa es muy interesante en el momento de crear escenarios de redundancia y en la convivencia de más de un protocolo en la red.

Protocolo	Distancia administrativa
Directamente Conectada	0
Ruta estática	1
eBGP	20
EIGRP (Interno)	90
IGRP	100
OSPF	110
ISIS	115
RIP 1	120
EGP	140
EIGRP (Externo)	170
iBGP	200

Otro punto importante a tener en cuenta en el momento de elegir nuestro protocolo de routing es el tiempo de convergencia. Este tiempo refleja el tiempo que transcurre hasta que todos los elementos se ponen de acuerdo y son concientes de la situación actual de la red. Se trata de una medida que refleja la eficacia del protocolo ante cambios en la red.

Finalmente queda por indicar que dentro del mismo router puede existir más de un protocolo de enrutamiento lo cual hará más sencilla la convivencia entre la red WAN y la red LAN y obtendremos más flexibilidad hacia las opciones que podemos presentar a cliente para administrar o adaptar su red LAN.

Por ejemplo podemos tener el protocolo BGP hacia la red WAN del ISP, el protocolo OSPF hacia la red LAN del cliente y rutas estáticas específicas hacia redes de gestión, firewalls o redes concretas dentro la LAN.

BGP

El protocolo BGP (Border Gateway Protocol) és un protocolo de pasarela externa (interdomain routing protocol) y se utiliza para el intercambio de información de routing entre diferentes AS (Sistemas Autónomos). Lo sistemas autónomos AS nos sirven para identificar de forma única un grupo de redes bajo una administración de enrutamiento común.

Cada sistema Autónomo se identifica con un número de 32 bits llamado ASN que esta delegado por la IANA (Internet Asigned Number Autorithy) a los RIR (Regional Internet Registries). Del 65512 al 65534 están reservados para uso privado y no se usan para la red pública de Internet.

Por otro lado, los sistemas Autónomos pueden ser:

- Multihomed:
  Está conectado a más de un proveedor y por lo tanto a más de un AS. Permanece conectado a Internet aunque falle alguna de sus conexiones.
- Stub:
  Es un nodo final (no es proveedor para ningún otro AS) y por lo tanto solo esta conectado a un AS.

- Transit:
  Es un proveedor para otros AS y proporciona conexión entre los distintos AS. Cada ISP será un AS de tránsito (como los troncales de Internet).

El encaminamiento entre los AS viene de la mano del protocolo BGP IPv4.

Entonces, BGP se considera un protocolo de vector trayectoria y por lo tanto, define una ruta como la correlación entre un destino y los atributos de la trayectoria dicho destino (es un híbrido entre un protocolo de estado de enlace y unote vector distancia).

El proceso de BGP és el siguiente:

1.- Recibe información de trayectoria de sus enrutadores pares (peers) . El resultado de la selección de trayectoria de BGP se coloca en la tabla de rutas de BGP y se marca la “mejor trayectoria”.

2.- Anuncia “mejor trayectoria” a sus pares. Las mejores trayectorias se instalan en la tabla de reenvío si:
  El prefijo y su longitud son únicos
  Tienen la menor “distancia al destino” desde el punto de vista del protocolo

Los tipos de mensajes enviados mediante TCP (puerto 179) son:

1.-Establecimiento (Open): establece relación con otro router frontera de AS.

2.- Actualización (Update): transmite información de encaminamiento.

  Estos mensajes de actualización que anuncian información de encaminamiento hacia rutas concretas constan de :

  - Un prefijo (Notación CIDR)
  - AS_PATH (Información de los AS a atravesar para llegar al destino)
  - ORIGIN (Identifica el origen de la ruta)
  - NEXT_HOP (Dirección router frontera de salto)
  - LOCAL_PREF (Solo para iBGP. Preferencia local hacia rutas externas)
  -MULTI_EXIT_DISC (Define la ruta “preferida” ante una situación de redundancia o más de un camino posible. El preferido será el valor menor.)

3.-Encaminador activo (Keepalive): confirma la recepción de un mensaje de establecimiento y también periódicamente la relación con otro encaminador frontera de AS.

4.-Notificación (Notification): informa de la detección de una condición de error y termina la conexión.

Calidad de Servicio

El protocolo IP sólo facilita un tipo de servicio, llamado Best-Effort (Mejor Esfuerzo):

- La red sólo se preocupa de entregar el datagrama a su destino (los retardos no importan).
- No hay garantías de entrega. Para conseguirlas hay que implementarlas en los sistemas finales (TCP o aplicación).

Por lo tanto si la red introduce un retardo entre el envío de paquetes y su recepción (latencia) al transmitir un datagrama, dependiendo de la aplicación, dicho retardo será aceptable o no así como por ejemplo Video/audio, etc.

Otro efecto de la red es que el retardo que sufre cada paquete no será constante (variación del retardo o jitter).

El jitter no afecta a los datos pero sí al vídeo o audio y se produce porque el llenado de los buffers de los routers, así como la cantidad de tráfico que confluye por los enlaces en cada momento no es predecible.

Así pues implementaremos QoS para dar un servicio prioritario a diferentes clases de tráfico.

Primero, para poder facilitar la opción de QoS, los routers tendrían que:

- Distinguir que tráfico corresponde a cada clase (clasificación).
- Tener colas separadas para cada una de las clases para, de este modo, poder atender a cada clase con una determinada prioridad.

Entonces en paquete dentro del router pasará por los siguientes estados:

1. Clasificación:
   Aquí indicamos como vamos a tratar el paquete y lo que vamos a hacer es clasificar el paquete según su dirección ip origen/destino. De esta forma haremos que un datagrama IP pertenezca a una clase o a otra, permitiendo tratar de forma diferente cada uno de estos datagramas según su clase

2. Función Policía y Marcado:
   Sirve para tratar los paquetes que llegan con adelanto. Así pues para que el resto de equipos de la red sean capaces de distinguir la clase a la que pertenece un determinado paquete IP sin necesidad de volver a clasificarlo se utiliza lo que se llama el marcado que lo que hace es hacerle una marca al paquete para que el resto de los equipos de la red sepan a que clase pertenecen. Este marcado consiste en dar un valor a un campo determinado del datagrama IP (Campo ToS) según la clase a la que pertenezca.
   La función policía consiste básicamente en “vigilar” que el tráfico generado por el cliente para cada una de las clases, no sobrepase los niveles máximos acordados o contratados, es decir, que el cliente no envíe tráfico a mayor velocidad que la que tiene contratada.
   Estas restricciones pueden ser más o menos suaves, haciendo que el tráfico por exceso se descarte directamente (Policing), o se almacene para ser transmitido más tarde (Shaping).

3. Encolado y Planificación.
   A la hora de utilizar Calidades de Servicio, se va a configurar una cola distinta para cada una de dichas clases, de esta forma tendremos cada tipo de tráfico por separado y en consecuencia podremos actuar sobre estos por separado.
   Para reenviar el paquete o descartarlo, según las normas establecidas.
   Cada interfaz de un nodo que permita QoS debe tener un planificador que indique que cola se debe servir en cada momento. El planificador puede determinar esta cola atendiendo a la velocidad máxima y/o mínima de cada una de las clases de servicio. Para ello se empleará un algoritmo.

Es necesario que las calidades de servicio se den en todo el trayecto, desde origen al destino, aunque el tramo más delicado es el punto de acceso (las líneas físicas donde el cliente se conecta a la red).

Deberemos preguntar al nuestro ISP que clases de servicio implementa y que clase de servicio debemos contratar para dar máxima prioridad al tráfico voz/multimedia.

5.1.2 – Material contemplado

Modelo equipo	Despiece	Descripción
Redundant Power System 2300	WR-RPS2300=	RPS 2300 chassis spare
	C3K-PWR-1150WAC=	Catalyst 3750-E/3560-E 1150WAC power supply
	BLWR-RPS2300=	Spare 45CFM Blower for Cisco Redundant Power System 2300
	CAB-RPS2300-E=	Spare RPS Cable RPS 2300 Cat 3750E/3560E Switches
	BLNK-RPS2300=	Spare Bay Insert for Cisco Redundant Power System 2300
	ACC-RPS2300=	Spare Accessory Kit for Cisco Redundant Power System 2300
Conversor de medios telnet CM-100	CM-100-Compacto-IB	Conversor de medio óptico-eléctrico.
WS-C3560V2-24TS-E	CAB-SFP-50CM=	Cisco Catalyst 3560 SFP Interconnect Cable (50 cm)
	CAB-ACE	AC Power Cord - Europe
	WS-C3560V2-24TS-E-[24 10/100 BaseT ports and 2 SFP ports]	Chassis Catalyst 3560-24TS-E
	SW IP Service	IOS por defecto
	Cable de red RJ-45	Latiguillo UTP clase 5, RJ45- RJ45 plano
	Cable de red RJ-45	Latiguillo UTP clase 5, RJ45- RJ45 plano

5.1.3 – Descripción del hardware contemplado

La red corporativa del cliente se soportará sobre un servicios de red de datos aprovisionado por el ISP. En concreto, contrataremos un servicio con acceso de fibra simétrico con un caudal contratado de 100Mb. Para ello nos indican que debemos aprovisionar un switch de nivel 3 (capaz de realizar routing) para poder crear el enlace con la red mallada de nivel dos de fibra llamada metrolan.

Equipo router

La familia de switches Catalyst 3560 son los más utilizados y comunes en capa 3. Elegimos el Cisco Catalyst 3560-24TS-E que ofrece enrutamiento IP de alto rendimiento, basado en su hardware. Posee la arquitectura "Express Forwarding-based routing" que permite una mayor escalabilidad y rendimiento en la red.

También provee de todas la funcionalidades de switching de capa 2 i ofrece las características de QoS para ayudar a asegurar que tráfico de la red está clasificado y priorizado, y que así evitamos la congestión en la mejor posible manera.
Puede clasificar, reclasificar, realizar policing, marcar i encolar cumpliendo las políticas basadas en capa 2 y 3.

Características principales:

- Switch Catalyst 3560 versión 2, de 24 puertos PoE 10/100/1000 + 2 SFP, software IP Service.
- Menor consumo eléctrico que sus predecesores.
- Totalmente compatible con equipos 3560 de la versión anterior.
- Soporte PoE para IEEE 802.3af y Cisco pre-estandard.
- Enrutamiento básico estático y dinámico.
- Full EnergyWise
- Seguridad mejorada.
- Soporte para IPv6
- Enrutamiento IP de alto rendimiento.
- Robusta disponibilidad y escalabilidad en capa 2 y 3.
- QoS avanzada.
- Multiples formas de administración incluyendo Command-line interface (CLI), CiscoWorks, Cisco Network Assistant con Cisco Smartports y Cisco Discovery Protocol.
- Cisco express setup.
- Montaje en rack.
- Compatible con el sistema de alimentación redundante RPS 2300.

El equipo incluye 24 puertos capaces de funcionar a 10/100 Mb (full o half duplex) para conexión de cable UTP Cat5 100BASE-TX RJ-45 y 2 puertos SFP (mini-GBIC) para conexión de 1000Base-SX o LX (fibra multimodo o monomodo).

También ofrece la posibilidad de conectar más de un equipo de la familia 3560 mediante el cable de interconexión SFP Cisco de 50 cm para realizar conexiones punto a punto mediante una conexión Gigabit Ethernet.

Finalmente, como añadido dispone de la tecnología Cisco EnergyWise, que es una arquitectura innovadora implementada en los switchs Cisco Catalyst 3560 que promueve la sostenibilidad de toda la compañía, reduciendo el consumo de energía en toda la infraestructura de la empresa. Cisco EnergyWise permite a las empresas poder medir el consumo de energía de la

infraestructura de red y los dispositivos conectados a la red y gestionar así el consumo, reduciéndolo y por lo tanto reduciendo también el coste.

Conversor de medios

A parte del switch de nivel 3 necesitaremos un conversor de medios aprovisionado por el ISP. En concreto se nos aprovisiona el modelo telnet

Este equipo realiza la conversión electro-óptica de la señal y actúa como punto de terminación de red entre el cliente y el operador ISP, permitiendo definir la responsabilidad de problemas o fallos en el enlace.

Estos conversores se instalan por parejas configuradas como maestro/esclavo. La gestión del enlace se efectúa en banda desde el equipo maestro de la central. El conversor de medios central estará alojado en la central ISP y el esclavo en las dependencias de cliente.

Este equipo realiza la conversión de señales ópticas a señales eléctricas, para circuitos de 10/100 Mb/s de caudal. Dispone de dos interfaces de tráfico:

- Interfaz 1: Interfaz de Red, 100 Base FX (fibra óptica monomodo).
- Interfaz2: Interfaz de Cliente, 100 Base TX/10base T, donde se conecta el equipo de usuario. El enlace eléctrico alcanza hasta 100m (estándar IEEE 802.3).

Características del Interfaz2:

TIPO INTERFAZ	EQUIPO	VELOCIDAD
Eléctrico RJ-45 Cable UPT cat. 5	CM-100	10/100 Mb/s (10/100 base T)

El equipo se alimenta con 220VAC y su consumo es 24W.

Puede reencaminar tramas de hasta una longitud de 1518 bytes si no incluyen tags VLAN, o de hasta 1522 bytes cuando se encuentran etiquetadas con tags VLAN. Descarta las tramas ilegales (IEEE802.3u), tramas de menos de 64 bytes y tramas con FCS incorrecto.

Tamboén realiza la propagación automática de las caídas de interfaz, es decir que la caída de un interfaz provoca la caída de la otra interfaz.

Finalmente, el diseño de este equipo permite que el tráfico de gestión no disminuya el ancho de banda al tráfico del cliente, garantizando en todo momento el 100% de la capacidad del enlace FastEthernet.

Fuente redundante

Finalmente dotaremos al equipo de una fuente redundante ya que todos los equipos catalyst tienen la opción de llevar fuente de alimentación.

El RPS 2300 Cisco proporciona una redundancia completa sobre la fuente de alimentación interna. Lo que nos proporciona es una alta disponibilidad para nuestros equipos 3560 de manera que si una fuente fallara tendríamos la otra fuente redundante.

En cuanto a características y funcionamiento puede apagar-se automáticamente cuando se reinicia el equipo switch 3560, puede gestionar-se de forma remota a través del switch 3560, el switch y el RPS pueden tener fuentes independientes de AC y finalmente el equipo es modular y puedes cambiar las piezas por separado como por ejemplo el ventilador.

Para conectar esta fuente al switch necesitamos un cable cisco RPS, concretamente un " PWR-RPS2300 Cisco RPS 2300 with one connector cable".

5.1.4 – Configuración

En este apartado explicamos los elementos más importantes para la configuración de nuestros routers que nos ayudaran a entender mejor la plantilla de configuración que encontraremos en el anexo.

El protocolo de routing

Para decidirnos por que protocolo de routing nos quedamos primero realizamos una comparativa.

Primero analizamos RIPv2 que es un protocolo de encaminamiento interno muy sencillo de configurar, abierto y soportado sobre la mayoría de fabricante. Por otro lado su principal desventaja consiste en que para determinar la mejor métrica, únicamente toma en cuenta el número de saltos, descartando otros criterios (Ancho de Banda, congestión, carga, retardo, fiabilidad, etc.), a parte de que no está diseñado para resolver cualquier posible problema de encaminamiento (El RFC 1720 (STD 1) describe estas limitaciones técnicas de RIP como graves y el IETF está evaluando candidatos para reemplazarlo) y tiene tiempos de convergencia bastante altos.

Por otro lado OSPF tiene un funcionamiento parecido a RIP y también se usa en la hacia redes internas. La forma de funcionar de este protocolo es bastante sencilla, dónde cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. De esta forma cada router sabe a que distancia está cada router y así en el momento que envía un

paquete lo envía por la ruta por la que tenga que dar menos saltos. Es un protocolo que se adapta de forma rápida y automática a los cambios de topología. A pesar de todo esto lo descartaremos porque esta orientado a redes muy extensas con conexiones entre varios proveedores de telecomunicaciones.

También tenemos EIGRP, un protocolo fácil de configurar que permite el incremento del crecimiento potencial de la red reduciendo el tiempo de convergencia, pero es un protocolo propietario de cisco y vamos a implementarlo hacia un enlace WAN con un ISP sobre el que casi podemos asegurar que no todo el equipamiento de red será cisco.

Finalmente tenemos el protocolo BGP que aporta mucha flexibilidad y eficacia ante los cambios de topología de la red, dando una convergencia más rápida que otros protocolos de enrutamiento.

CARCTERISTICAS	RIP	OSPF	IGRP	EIGRP	BGP
Tipo	Vector-Dist.	Estado-enlace	Vector-Dist	Vector-Dist.	Híbrido
Tiempo de converg.	Lento	Rápido	Lento	Rápido	Rápido
Soporta VLSM	No	Si	No	Si	Si
Consumo de A. B.	Alto	Bajo	Alto	Bajo	Bajo
Consumo de recursos	Bajo	Alto	Bajo	Bajo	Bajo
Mejor escalamiento	No	Si	Si	Si	Si
De libre uso o propietario	Libre Uso	Libre Uso	Propietario	Propietario	Libre Uso

Entonces, como protocolo de routing elegimos BGP ya que este protocolo mejora los tiempos de convergencia, aporta flexibilidad ante los posibles cambios en la red, consume pocos recursos y no es un protocolo propietario de Cisco.

Además es un protocolo híbrido y por lo tanto implementa las ventajas de un protocolo de vector-distancia y uno de estado de enlace.

Diversificación de los enlaces WAN:

En todo momento dispondremos de nuestro router principal en las oficinas centrales y de nuestro router backup en las delegaciones. Ambos equipos deben estar preparados para publicar las mismas redes y esto puede crearnos un conflicto.

Ahora que ya conocemos el concepto de métrica, nuestra idea es penalizar por métrica la publicación de la redes en los equipos backup.

Entonces, cuando configuremos el protocolo BGP en el equipo backup le pondremos una métrica de 200 en la publicación de las redes de cliente hacia la WAN para que en todo momento siempre prevalezca la publicación en el equipo principal.

Sistema de redundancia hacia la LAN:

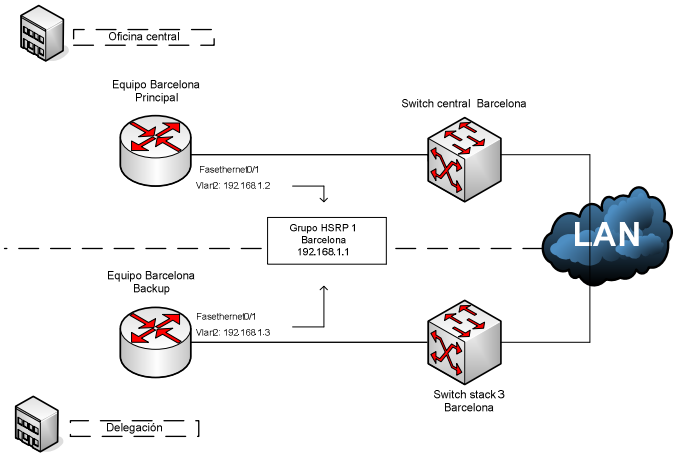
Para realizar la redundancia entre los dos routers de Barcelona y los dos routers de Madrid hacia la LAN utilizaremos el protocolo HSRP propietario de cisco.

El protocolo HSRP (Hot Standby Router Protocol) es un protocolo propietario de Cisco que está diseñado que permite poder redundar dos o más dispositivos Cisco. Funciona enviando mensajes IP Multicast en el puerto 1985/UDP hacia la dirección 224.0.0.2 en formato de paquetes Hello.

La idea es que la ip Gateway, de un host o de toda un ared de host, sea una ip virtual. Entonces, esta IP no es una dirección real, si no una dirección virtual que ambos routers, principal y backup van a compartir. Sin embargo, para mantener la conectividad de capa 3, capa router tiene su dirección IP habitual en su interfaz.
Mediante la configuración de unos valores de prioridad el router principal dispondrá siempre de la ip virtual de Gateway si éste falla o deja de responder, inmediatamente asume el control el router Standby. Esta operación es completamente transparente para el usuario.

Entonces, en nuestro proyecto toda la red LAN de cliente apuntará a un ip Gateway compartida entre router Barcelona principal y su router Barcelona backup en la delegación (lo mismo aplicable a Madrid). Realizaremos una configuración que asignará siempre la ip Gateway al equipo Barcelona principal a no ser que este deje de prestar servicio.
En caso de que el equipo backup detecte una pérdida de conectividad contra el equipo principal, el cogerá la ip de Gateway toda la red de cliente será redirigida al router backup.

Ejemplo Barcelona



Configuración de las Quos

Primero de todo debemos consultar a nuestro ISP que clases de servicio se ofertan.

En nuestro caso, preguntamos que QoS nos pueden ofrecer y nos indica 3 clases de servicio aplicables:

1.-Tráfico Multimedia – Prec: 5 – Prioritaria (LLQ)
2.-Tráfico Oro – Prec 3 – CBWFQ
3.-Tráfico Plata – Prec 1 – CBWFQ

Nosotros contrataremos clase plata para el tráfico de datos (ya que nos saldrá más económico y es suficiente) y clase multimedia para el tráfico de voz.

A partir de este punto es necesario realizar un cálculo para determinar que % del caudal contratado de 100Mb destinaremos el tráfico multimedia de voz y que % lo destinaremos al tráfico plata de datos.

Para realizar este cálculo primero necesitamos saber cuanto ocupa cada llamada. Este punto es sencillo, tan solo necesitamos conocer que códec estamos aplicando que en nuestro caso es G.729 (más detalle en la parte de telefonía ip).

Entonces, con G.729 sabemos que una llamada ocupa 32Kbps y teniendo en cuenta que tenemos 280 usuarios por provincia en el supuesto caso de que un 75% de los usuarios estuviera cursando voz de forma simultánea 210*32Kbps= 6,72 Mps.

Sabemos que disponemos de un caudal contratado de 100Mbs , si asignamos 7Mb para voz estamos usando un 7% del total. Como se nos ofrece la posibilidad de asignar un 25%, un 50% o un 75% a multimedia asignamos un 25% y, por lo tanto, un 75% al tráfico plata.

Se contemplan las siguientes redes

En este apartado tenemos en cuenta la red LAN que debemos configurar en el propio equipo. Las diferentes redes LAN de cliente vendrán especificadas en la parte de LAN. Por otro lado el ISP contratado deberá especificarnos que red WAN debemos configurar en el equipo.

Vlan	Descripción	Red	Ip interfaz Vlan
2	Red de datos Barcelona	192.168.1.0/29	192.168.1.1
20	**Red de gestión de los switch	192.168.14.0/24	192.168.14.1

** Crearemos una red interna con intención de asignar a cada switch una ip para que éste sea gestionable a nivel ip. Esto nos permitirá que por un lado podamos entrar en todos los equipos mediante el comando Telnet y por otro lado, podamos realizar una monitorización del estado del mismo. En un principio no tendría sentido configurar esta red en el router ya que para hacer una gestión interna no sería necesario, pero para que todos los switch sean gestionables des de Madrid y desde Barcelona publicaremos las ip de gestión /32 de cada switch por bgp a la otra oficina.

5.2 – LAN

5.2.1 – Conceptos teóricos

¿Que es una red LAN?

La red LAN (Local Área Network) como el propio nombre indica son redes de área local que conectan plantas o edificios con poca distancia, en definitiva en una área geográfica limitada.

En este tipo de red lo que buscamos es funcionalidad, escalabilidad, adaptabilidad y facilidad de administración ya que la red debe funcionar, debe poderse aumentar de tamaño, debe poder ser monitorizada des de un punto central y sobretodo debe diseñarse teniendo en cuenta futuras tecnologías.

Para el diseño de nuestra LAN tendremos en cuenta la función y la ubicación de los servidores de cliente, los dominios y de broadcast , una segmentación de la red apropiada a las necesidades del cliente y una buena comunicación de red entre los usuarios maximizando el ancho de banda y los recursos disponibles.

¿Qué es un switch?

Un switch esta diseñado para resolver problemas de rendimiento en la red LAN ya que es capaz de aprovechar un mayor ancho de banda y por lo tanto reducir los tiempos de espera, pero su uso básico es para conectar múltiples dispositivos de una misma red.

Estos equipos funcionan en la capa 2 de modelo OSI (nivel de enlace) y por lo tanto envían los paquetes en base tabla de Forwarding donde se relaciona cada MAC origen con el puerto donde ha sido vista.
Con esta información el switch toma las decisiones de por donde se tiene que propagar una trama. Para ello buscará en la tabla de forwarding la MAC destino de la trama, y la propagará por el puerto que se indique en dicha tabla. Por lo tanto, cuando le preguntemos a un switch por su tabla de MAC's nos indicara las que aprende de forma estática (los dispositivos directamente conectados) y las MAC's aprendidas dinámicamente des de otros equipos switch.

De esta forma, a diferencia de por ejemplo los Hubs, los paquetes van des de un Pc origen y un Pc destino (puerto origen – puerto destino) creando una especie de comunicación exclusiva y de esta manera más de un PC puede estar comunicándose a la vez (excepto cuando más de un PC intenta comunicarse con la misma máquina).

Esta característica del equipo switch también es una protección contra las colisiones en la LAN. Cuando un Pc/host se conecta a un puerto de switch, el switch crea una conexión dedicada y se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión. Por lo tanto los switch reducen el tamaño del dominio de colisión a un único enlace y mejorando el rendimiento de la redy un mayor aprovechamiento del ancho de banda disponible.

Por último indicar que existen dos tipos de switch, los gestionados y los no gestionados. Los no gestionados están preparados para funcionar de forma automática y no aceptan cambios de configuración por parte del administrador de la red. En nuestro caso usaremos switchs gestionables que permiten su configuración

Todo esto nos aportara mayor control, rendimiento y eficiencia sobre la red de cliente.

Switch de acceso

Los switch de acceso se usarán para permitir el acceso a la red a los usuarios finales.
Pertenece a la capa donde los usuarios finales se conectan a la red. Los switches de la capa de acceso por lo general ofrecen conectividad de Capa 2 (VLAN) entre los usuarios. Los dispositivos de esta capa deben tener estas opciones:

- Coste por puerto de switch bajo
- Alta densidad de puertos
- Escalabilidad de uplinks a capas superiores
- Funciones de acceso al usuario como VLANs, filtrado de tráfico y protocolos y Calidad de servicio (QoS)
- Capacidad a través de múltiples uplinks
- Local VLANs

Switch de núcleo

Esta capa ofrece conectividad a los dispositivos de la capa de distribución. En nuestro caso no tenemos switch que se dediquen únicamente ha distribución porque nuestra red es pequeña y queremos aprovechar todos los switch para conectar usuarios.

El core, también llamado backbone, debe ser capaz de mover tráfico los más eficientemente posible. Los dispositivos de esta capa deben tener estas opciones:

- Muy alto rendimiento en la Capa 3.
- Manipulación de paquetes sin coste ni penalización alguna (listas de acceso, filtrado de paquetes)
- Redundancia y capacidad para alta disponibilidad.
- Funciones avanzadas de calidad de servicio (QoS).

Fibra óptica

La luz que se utiliza en las redes de fibra óptica es un tipo de energía electromagnética. Esta energía en forma de ondas, viaja a través del vidrio en línea recta pasándose a llamar rayo de luz.

Entonces la energía de la luz de un rayo incidente que no se refleja entra el vidrio y se dobla desviándose de su trayecto original. Este rayo será un rayo refractado. El grado en que se doble el rayo de luz incidente depende del ángulo que forma el rayo incidente al llegar a la superficie del vidrio y las distintas velocidades a la que la luz viaja a través de los dos materiales.

La desviación de los rayos de luz en los límites de los dos materiales es la razón por la que éstos pueden recorrer una fibra óptica aún cuando la fibra tiene forma de círculo.
La densidad óptica del vidrio determina la desviación de los rayos de luz en el vidrio, sabiendo que la densidad óptica define cuánto se reduce la velocidad del rayo a atravesar ese material.
Por otro lado el índice de refracción de material es la velocidad de la luz en el vacío dividido por la velocidad de la luz en el medio. Así pues la densidad óptica del material es el índice de refracción de ese material y por lo tanto, cuánto mayor sea el índice del material menor velocidad tendrá la luz.

El vidrio permite aumentar ese índice de refracción, creando un vidrio muy puro y obteniendo así el núcleo del cable de fibra óptica que es la parte de la fibra óptica por la viajan los rayos de luz. Los rayos de luz sólo pueden ingresar al núcleo si el ángulo está comprendido en la apertura numérica de la fibra.

Entonces, una vez que los rayos han ingresado al núcleo de la fibra existen un número limitado de recorridos ópticos que puede seguir un rayo de luz a través de la fibra. Estos recorridos ópticos se llaman modos.

Si el diámetro del núcleo de la fibra es lo suficientemente grande como para permitir varios trayectos de luz, esta fibra se llamara fibra multimodo. La fibra monomodo tiene un núcleo más pequeño que permite que los rayos de luz viajen a través de la fibra por un solo modo.

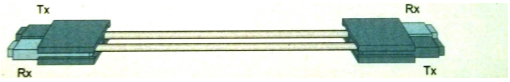
1.-Fibra óptica multimodo

> El hecho de que se propaguen más de un modo supone que no llegan todos a la vez al final de la fibra por lo que se usan comúnmente en aplicaciones de corta distancia, menores a 1 km.
>
> Nosotros para enlazar switch dentro del mismo edificio utilizaremos fibra multimodo.

2.- Fibra óptica monomodo

El diámetro del revestimiento de este tipo de fibra es de 125 µm, igual que en las multimodo aunque el diámetro del núcleo es mucho menor, de unas 9 µm, hecho que hace que su transmisión sea paralela al eje de la fibra y que, a diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de información. La fibra monomodo deberá aprovisionarla el ISP.

Finalmente, cada cable de fibra óptica que se usa en el networking está compuesto de dos fibras de vidrio envueltas en revestimientos separados. Una transporta los datos que transmitimos des de A a B y la otra los de B a A. DE esta manera conseguimos una comunicación full-duplex



5.2.2 – Material contemplado

Barcelona

BARCELONA 1
Switch C6509
1u Catalyst 6500 Chassis (9-Slot),fan, no p/s, Red Sup Capable
1u Catalyst 6000-SUP720 IOS IP SERVICES SSH(MODULAR)
2u Catalyst 6500 / Cisco 7600 Supervisor 720 Fabric MSFC3B
2u SP adapter with compact flash for SUP720
2u Catalyst 6500 Sup32 Compact Flash MEM 128 MB
1u Catalyst 6500 48 port 10/100/1000 Module - WS-X6748-GE-TX
50u Latiguillo LANDmark5e UTP RJ45-RJ45 LSZH-FR, 3m
1u Catalyst 6500 24 port GigE - WS-X6724-SFP
1u GE SPF, LC connector LX/LH transceiver (SM)
1u GE SFP, LC connector SX transceiver (MM)
Catalyst 6509-E Chasis Fan Tray
CAB-AC-2500W-EU: Power Cord 250VAC 16A Europe
WS-CAC-300W :Catalyst 6500 3000W AC power supply
Power Cord 250VAC 16A Europe :CAB-AC-2500W-EU Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512 MB: MEM-C6K-CPTFL512M Bootflash for SUP720-64MB-RP: BF-S720-64MB-RP Catalyst 6500 512MB DRAM on the Supervisior (SUP2 or SUP 720): MEM-S2-512MB Catalyst 6500 512MB DRAM on the MSFC2 or SUP720 MSFC3: MEM-MSFC2-512MB Catalyst 6500256MB DDR, xCEF720 (67xx interface, DFC3A)MEM-XCEF720-256M Catalyst 6500 Central Fwd card for WS-X67xx modules:WS-F6700-CFC
WS-C3750-48PS-S
2u Catalyst 3750 48 10/100/1000 PoE + 4 SFP
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
2u GLC-SX-MM=GE SFP, LC connector SX transceiver
2u Power Cord Europe: CAB-ACE
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
WS-C3750-48PS-S
2u Catalyst 3750 48 10/100/1000 PoE + 4 SFP
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
1u GLC-SX-MM=GE SFP, LC connector SX transceiver
1u GLC-LH-SM GE SPF, LC connector LX/LH transceiver
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
2u Power Cord Europe: CAB-ACE

BARCELONA 2
Switch C3750-48PS-S
2u Catalyst 3750 48 10/100 PoE + 4 SFP
Cisco StackWise 50CM Stacking Cable
1u GLC-LH-SM GE SPF, LC connector LX/LH transceiver
1u GLC-SX-MM=GE SFP, LC connector SX transceiver
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
2u Power Cord Europe: CAB-ACE

Madrid

MADRID 1
Switch WS-C3750G-12S-S
1u Catalyst 3750 12 SFP Standard Multilayer Image
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
2u GLC-LH-SM= GE SFP,LC connector LX/LH transceiver
1u GLC-SX-MM=GE SFP, LC connector SX transceiver
WS-C3750-48PS-S
2u Catalyst 3750 48 10/100 PoE + 4 SFP Standard Image
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
2u GLC-SX-MM=GE SFP, LC connector SX transceiver
2u Power Cord Europe: CAB-ACE
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
WS-C3750-48PS-S
2u Catalyst 3750 48 10/100 PoE + 4 SFP Standard Image
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
2u GLC-SX-MM=GE SFP, LC connector SX transceiver
2u Power Cord Europe: CAB-ACE
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
WS-C3750-48PS-S
1u Catalyst 3750 48 10/100 PoE + 4 SFP Standard Image
Cisco StackWise 1M Stacking Cable: CAB-STACK-1M
1u GLC-SX-MM=GE SFP, LC connector SX transceiver
48u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
2u Power Cord Europe: CAB-ACE

MADRID 2
Switch C3750-48PS-S
2u Catalyst 3750 48 10/100 PoE + 4 SFP
Cisco StackWise 50CM Stacking Cable
2u GLC-LH-SM GE SPF, LC connector LX/LH transceiver
100u Latiguillo LANDmark 5e UTP RJ45-RJ45 LSZH-FR, 3m
2u Power Cord Europe: CAB-ACE

5.2.3 – Descripción del hardware contemplado

Nuestra red LAN estará basada en la interconexión de los diferentes equipos switch Cisco de acceso y de núcleo o CORE de la red mediante fibras.

Switch de acceso Cisco Catalyst 3750-48PS-S:

Nosotros usaremos los switch Cisco Catalyst 3750, concretamente los WS-C3750-48PS-S que disponen de 48 puertos de acceso a usuarios que pueden funcionar a 10/100/1000 y de cuatro ranuras para inserción de transceptores de tipo Small Form Pluggable (SFPs) para la realización de conexiones de fibra óptica multimodo o monomodo.
También incorpora la tecnología PoE (Power over Ethernet) que permite que el switch subministre energía eléctrica al dispositivo conectado a él a través del propio cable de red. Esta opción es imprescindible si queremos alimentar nuestros terminales Ip Alcatel.

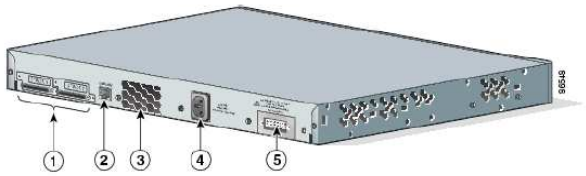
Además ofrece la posibilidad de encaminara nivel 3 y enrutar tráfico ip entre vlans lo cual es muy interesante si en un futuro queremos ampliar nuestra red LAN.

Por otro lado, sólo disponen de una única fuente de alimentación pero tienen la posibilidad de que se les conecte una fuente de alimentación adicional a través del conector RPS (Redundant Power System) y, a más a más, incorporan el concepto EnergyWise consiguiendo una de las series de switch cisco que menos energía consumen y por lo tanto nos ayuda a controlar el consumo de energía para la red y ayudar al medio ambiente.

Finalmente también tiene la gran ventaja de tecnología StackWise de Cisco en los Catalyst de las Series 3750E y 3750 que permite construir un un sistema de switching unificado y altamente flexible de hasta nueve switches.

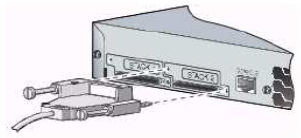
Stack switch de acceso

Los diferentes switch cisco catalyst 3750 se unen para formar una única unidad switch con los recursos de cada uno de ellos gracias a unos cables de stack y un software especial. La configuración y el routing se comparte creando una única unidad de switching. De esta manera todos los miembros del stack comparten un IP única de gestión y una configuración.



No.	Description
1	StackWise Ports
2	RJ−45 Console Port
3	Fan Exhaust
4	AC Power Connector
5	RPS Connector

El cable que utilizaremos es:



Cable Part Number	Description
CAB−STACK−50CM	Cisco StackWise 50−cm stacking cable

Cada miembro del stack tiene la posibilidad de ser el master o el slave/subordinate member en la jerarquía del stack. El que sea elegido como master tendrá el control de todo el stack. Podemos crear un stack de hasta 1 master y 8 slaves/miembros del stack.

Cuando añadimos un nuevo miembro al stack es el master quien configura en el nuevo switch la IOS y la configuración que deberá contener. El el stack quien recopilará toda la información para añadir a la tabla de forwarding las nuevas MAC.

Para la elección del master se siguen unas normas:

1.- Siempre será master el que ya lo es en un stack

2.- El switch con la prioridad más alta.

3.- El switch que no tiene la configuración por defecto.

4.- El switch con más prioridad de software/hardware:

a. Cryptographic IP services image software

b. Noncryptographic IP services image software

c. Cryptographic IP base image software

d. Noncryptographic IP base image software

5.- El switch que lleva más tiempo levantado.

6.- El switch con la MAC más baja.

¿Cuando se elige el master?

1.- Cuando se resetee todo el stack

2.- Cuando el master se apaga ya que cuando apagas el máter se resetea todo el stack.

3.- Cuando quitamos el master del stack.

4.- Cuando falla el master.

Si no pasa nada de esto el que es master siempre tiene preferencia a ser re-elegido.

Una unidad de stack puede aceptar nuevos miembros y eliminar antiguos sin sufrir una interrupción. Cuando el stack se da cuenta de que algunos puertos ya no están presentes se actualiza la información sin detener el correcto funcionamiento del stack.
Por lo tanto puede ser que nos interese quitar un miembro del stack.

¿Que pasos debemos seguir?

1.- Apagamos el switch.

2.- Debemos tener en cuenta que si este era el master los otros se reiniciaran para la reelección.

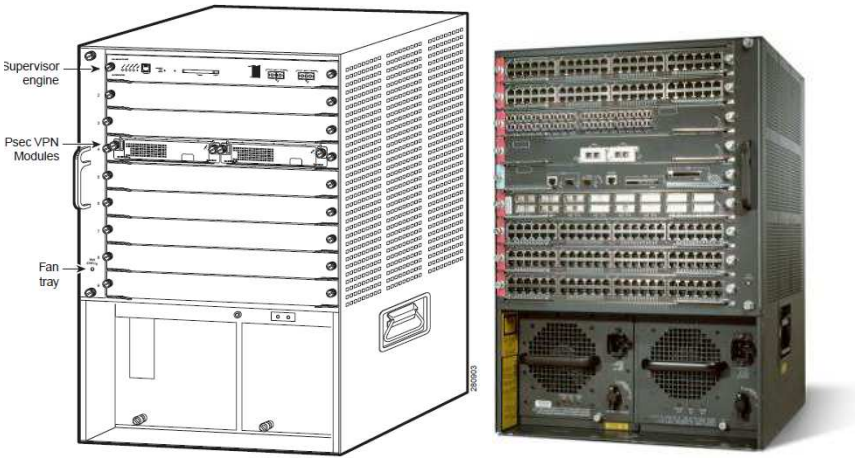
3.- Quitamos los cables.

Switch de Núcleo Cisco Catalyst 6509-E:

El chassis Cisco Catalyst 6500-E Series, proporciona innovación técnica con capacidad de gestión operativa, comunicaciones ininterrumpidas, unificación de la red, és muy versátil y proporciona escalabilidad y es ideal para una solución del alto rendimiento, de alta densidad de puertos Fast Ethernet, Gigabit Ethernet, y Ethernet 10 Gigabit (son líderes de la industria Gigabit Ethernet 10/100/1000, Ethernet 10 Gigabit y 40 Gigabit Ethernet).

Tienen la opción de doble supervisora y doble fuente de alimentación incrementando su disponibilidad. Es un equipo robusto que proporciona un alto nivel de resistencia y procesamiento de red. También es modular y dispone de 9 slots que proporciona flexibilidad y facilidad de crecimiento para nuestra red.

Así pues, esta serie de switchs son ideales para realizar las funciones de núcleo de la red de la empresa y de entornos de agregación.



Algunos servicios de los que es capaz de proporcionar son:

1.- Servicios y políticas para datos, voz, video y aplicaciones inalámbricas

2.- Configuración de IPv4, IPv6, IP Multicast y de hardware para un rendimiento

3.- Capacidad de buffer por puerto suficiente para poder dar funcionalidad a aplicaciones tales como Cisco TelePresence.

4.- Proporciona una gama extensa de fuentes de alimentación de doble voltaje con múltiples inputs independientes para proporcionar escalabilidad a la red.

5.- Puede proporcionar, High Power over Ethernet (PoE).

6.- Configuración de multi VRF

7.- Configuración de IPSec, generic routing encapsulation (GRE) tunnels y Multi-Virtual, etc.

a) Módulo de puertos WS-X6748-GE-TX:

Cisco Catalyst 6500 48-port 10/100/1000 Ethernet.

Especificaciones: 48 ports 10/100/1000 module (CFC 6748 TNET) Cisco Catalyst OS Version 8.1.2 or Cisco IOS® Software Release 12.2(17a)SX

Product Number	Primary Application	Ports, Connector, Maximum Distance, and Cable Type	PoE Support	Maximum Frame Size (jumbo frame) Support	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffer Size per Port
WS-X6748-GE-TX	Data center and server farm	48, RJ-45, 100m, Category 5 cable	No	Up to 9216 bytes per frame	Tx-1p3q8t; Rx-1q8t (when using Distributed Cisco Express Forwarding)	1.3 MB

Esta tarjeta tiene 48 puertos 10/100/1000 para conexión de cable RJ-45 Cat5 UTP.

Puede funcionar con la supervisora 720 y esta diseñado para funcionar con el chassis de la serie cisco Catalyst 6500 y 6500-E.

Como añadido tiene una tamaño de buffer por puerto de 1,3 MB y por lo tanto no tiene sobresuscripción y tiene suficiente backplane para que todos los puertos puedan funcionar a máxima velocidad.

La utilizaremos para conexión de servidores de cliente.

b) Módulo de puertos WS-X6724-SFP:

Este módulo es adecuado para conexiones Gigabit Ethernet con fibra monomodo o multimodo con adaptadores GBIC, agregación de alta densidad de 10/100, conexiones de granjas de servidores o data centres que trabajan a alta velocidad y también para conexiones de cobre. Adecuado para funcionar con la supervisora 720.

Primary Applications	Product Number	Interface Module Class	Ports/Optics Interface Type	Queues per Port (Tx = Transmit, Rx = Receive)*	Scheduler	Buffer Size per Port
High Performance Distribution, Core Layer and Data Center	WS-X6724-SFP	CEF720	24, SFP	• Tx-1p3q8T • Rx-1q8T (2q8T when using dCEF)	DWRR	• Rx-166KB • Tx-1.17MB

Esta tarjeta se utiliza en capas de distribución y núcleo. La usaremos para realizar las conexiones con otros equipos switch. Por otro lado, la idea es preparar este equipo para la ampliación que vendría en el segundo proyecto.

c) Cisco Catalyst 6500 Series Supervisor Engine 720-3B:

La supervisor engine es la CPU del sistema.

Una de las CPU de los equipos 6500 es la supervisor engine que es llamada Network Management Processor (NMP) o Switch Processor (SP).La otra es CPU se utiliza para el routing de capa 3 y se llama MSFC o Route Processor (RP).

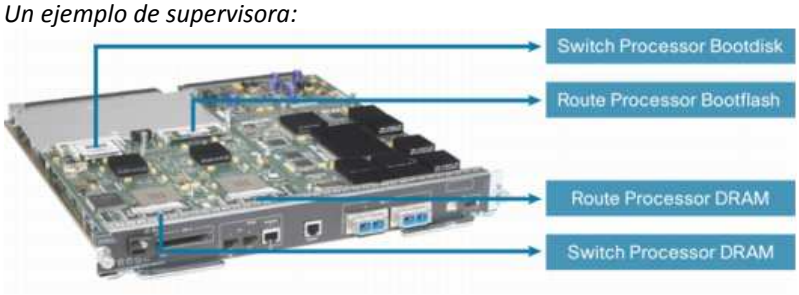
La CPU SP tiene las siguientes funciones:

- Mantiene la tabla de forwarding (aprende MAC's)
- Ejecuta protocolos y procesos que proporcionan control de la red (Spanning-Tree, CDP, VTP,DTP, etc)
- Maneja el tráfico de gestión de red que está destinado a la CPU del switch (HTTP,Telnet,SNMP,etc)

La CPU RP tiene las siguientes funciones:

- Realiza y actualiza las tablas ARP (Address Resolution Protocol Tables).
- Genera el Cisco Express Forwarding (CEF), el Forwarding Information Base (FIB) y las tablas adyacentes y descarga las tablas en el Olicy feature Card (PFC).
- Maneja el tráfico de gestión de red que está destinado a la RP (Telnet, HTTP,SNMP, etc)

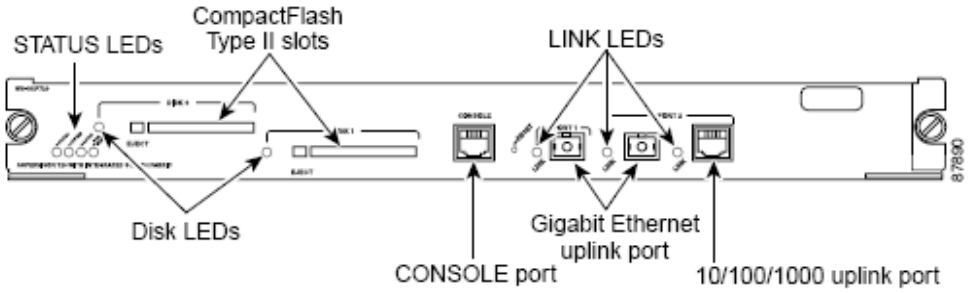
Un ejemplo de supervisora:



En resumen el SP = procesador switch processor y el RP = procesador de routing.

El modelo que nosotros vamos a implementar es el Supervisor Engine 720-3B:

Supervisor Engine	SP Bootflash/bootdisk	RP Bootflash	SP DRAM	RP DRAM
WS-Sup720 and WS-Sup720-3B	64 MB/512 MB*	64 MB	512 MB	512 MB

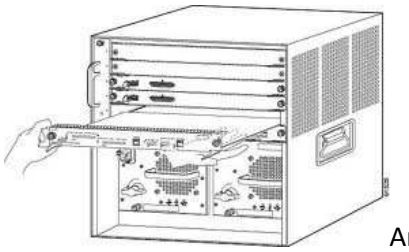


El módulo Supervisor Engine 720-3B tiene un puerto de consola, un puerto RJ-45 10/100/1000 Ethernet (posee un LED incativo del link), dos puertos Gigabit Ethernet que utilizan módulos transceptores SFP y dos ranuras PCMCIA para mantener los dispositivos de memoria Compact Flash.

Esta supervisora es un nuevo miembro de la serie Supervisor engine 720 y da soporte al hardware basado en Multiprotocol Label Switching (MPLS), a la configuración de access-control-list (ACL) y a la configuración tanto de IPv4 como IPv6.

En nuestro equipo tenemos doble supervisora para que la supervisora en redundancia asuma el relevo si se cae la supervisora definida como “activa”. Todas las funciones de red corren por la supervisora activa. La supervisora en stand-by no tiene activo el puerto de consola en estado “stand-by”.

Cuando instalamos ambas supervisoras la primera en encenderse coge el rol de “activa=principal” y la otra se queda en modo stand-by.

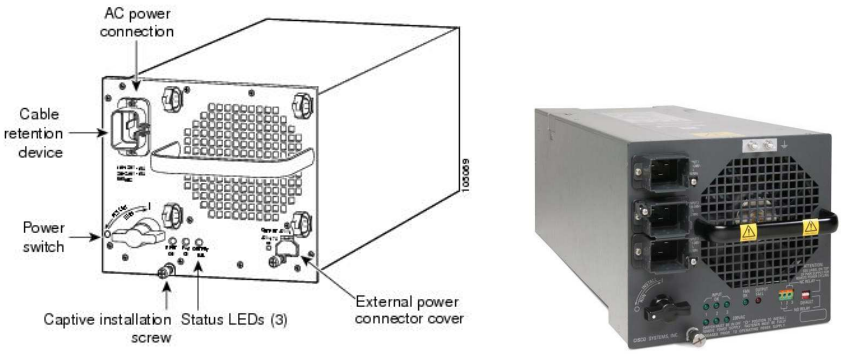


Ambos módulos son intercambiables en caliente. El sistema sigue funcionando correctamente cuando redundamos la supervisora.

d) Fuentes de alimentación redundantes:

Per al model Catalyst 6509-E elegimos la fuente de 3000w.

Imagen 3000 W AC-Input Power Supply

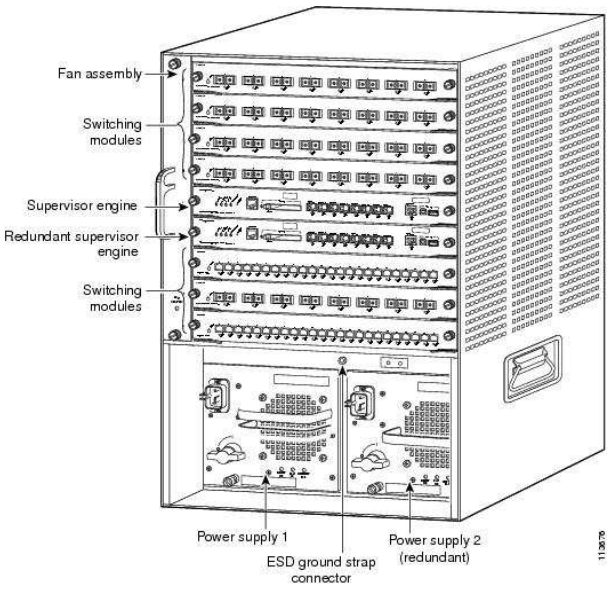


Consejos de cisco para nuestro equipo 6509-E:

Platform	Supported Power Supplies	Chassis/Power Supply Restrictions
Catalyst 6509-E	• 2500 W AC-input and DC-input • 3000 W AC-input • 4000 W AC-input and DC-input • 6000 W AC-input and DC-input • 8700 W AC-input	No restrictions.

El modelo de equipo Catalyst 6509-E soporta la funcionalidad de redundancia de fuente de alimentación para incrementar la disponibilidad del equipo. Por este motivo proporcionamos dos fuentes de alimentación al equipo.

En resumen el esquema del equipo con todo el hardware es la siguiente:



Módulos transceptores para puerto SFP (mini-GBIC)

En varias ocasiones hemos hablado de los puertos SFP. Un puerto SFP, definido como small form-factor pluggable, es un transceptor (insertable en caliente) que se emplea en los puertos de equipos de comunicaciones (switch, router, conversor de medios) para la conexión de enlace por fibra óptica (1000Base-SX).

a) Transceptor

Para conectar este switch con los demás switchs de la oficina utilizaremos fibra óptica multimodo conectándola a los puertos SFP del equipo mediante un GBIC GLC-SX-MM: 1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength, dual LC/PC connector.

Para decidir el modelo nos basamos en la información obtenida en las recomendaciones de cisco para nuestros equipos:

Plataforma	Modelo de switch	Módulo de transceptor GBIC	Versión mínima de IOS requerida
Catalyst 3750 series	WS-C3750G-12S WS-C3750G-24TS WS-C3750G-48TS WS-C3750G-24PS WS-C3750G-48PS	GLC-T (10/100/1000) GLC-SX-MM GLC-LH-SM GLC-SX-MMD GLC-LH-SMD GLC-ZX-SM GLC-ZX-SMD CWDM SFP	12.1.(14)EA1 12.1(14)EA1

Catalyst 6500/6000 Series

Modules	100M SFPs	Gigabit Ethernet SFPs	CWDM SFPs
WS-SUP720 WS-SUP32-8GE-3B WS-SUP32-10GE-3B WS-X6724-SFP WS-X6748-SFP	-	GLC-T GLC-SX-MM GLC-LH-SM GLC-ZX-SM GLC-BX-D GLC-BX-U	All CWDM SFPs

Por otro lado, para que el ISP pueda conectar su fibra monomodo proporcionamos el modelo, el GLC-LH-SM que como podemos ver en los cuadros de arriba también se recomienda para nuestros equipos.

GLC-SX-MM *GLC-SX-SM*

b) Fibra

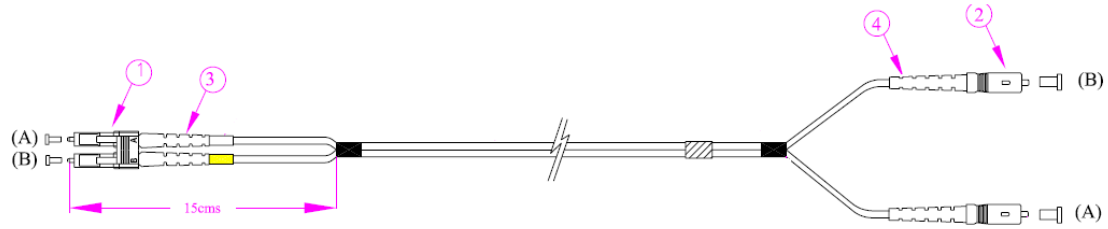
En este adaptador conectaremos latiguillo de fibra multimodo LC-SC.

Este latiguillo dispone de un conector LC (macho) y un conector SC (macho) a fin de proporcionar la conexión necesaria entre dispositivos de redes para transmitir datos a larga distancia y alta velocidad.

El conector SC (Set and Connect) es un conector de inserción directa que suele utilizarse en conmutadores Ethernet de tipo Gigabit . Son fáciles de conectar, logran mayor densidad de integración que sus antecesores (ST) y por permiten la funcionalidad duplex en la que los dos canales de transmisión/recepción Tx/Rx se pueden tener en el mismo modular. SC se considera un conector óptico de tercera generación, mejorando en tamaño, resistencia y facilidad de uso con respecto a la anterior.

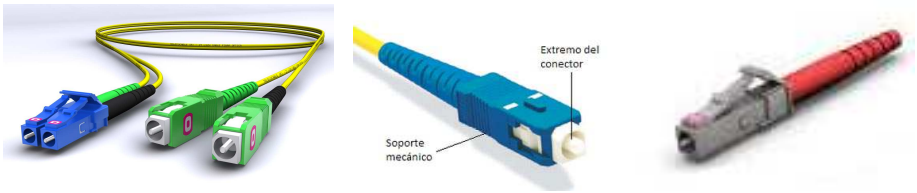
Los conectores LC tienen un aspecto exterior similar a un pequeño SC, con el tamaño de un RJ 45 y se utilizan para conexiones cruzadas o interconectadas de equipos
en aplicaciones backbone, horizontales y áreas de trabajo para transmisiones de datos a alta velocidad. Estos conectores contienen una ferrule de 1.25mm y cuerpo de plástico resistente. El cuerpo del conector sujeta la ferrule, ofreciendo una mejor alineación y previniendo movimientos. Las ferrules son fabricadas en cerámica de zirconia de alta precisión, ofreciendo una excelente alineación entre dos fibras.

Esquema del cable



1.	LC Connector	2
2.	SC Connector	2
3.	LC Boots	2
4.	SC Boots	2

Cable de fibra *Conector SC* *Conector LC*



En el transceptor viene indicado que puerto es Rx y cual Tx.

5.2.4 – Alimentación equipos

Material contemplado

En la siguiente tabla se indica el modelo y la cantidad de SAI's a proporcionar por delegación

Oficina	Ubicación	Descripción	SAIS a instalar	Tomas necesarias	Tomas SAI	Alimentación requerida
BCN1	Segunda planta	2 switchs C3750	1 SAI 850	2x8A	2x10A	1 x 220 V (10A)
BCN1	Primera planta	2 switchs C3750 1 switch C6509	1 SAI 3000 + baterias	1x16A + 2x10A	1x16A + 8x10A	1 x 220 V (10A) 1 x 220 V (16A)
BCN2	Planta baja	2 switchs C3750	1 SAI 850	2x8A	2x10A	1 x 220 V (10A)
M1	Primera planta	3 switchs C3750	1 SAI 850	3x8A	3x10A	1 x 220 V (10A)
M1	Tercera planta	3 switchs C3750	1 SAI 850	3x8A	3x10A	1 x 220 V (10A)
M2	Planta baja	2 switchs C3750	1 SAI 850	2x8A	2x10A	1 x 220 V (10A)

En Barcelona 1 para dotar de máxima redundancia y autonomía se han instalado dos SAI 3000 con baterías.

El motivo principal de poner un SAI es que tengamos unos minutos de ventaja si detectamos una caída eléctrica en la, sobretodo para poder salvaguardar la información de nuestros trabajos y equipos informáticos con garantías.

Un segundo motivo y no por eso menos importante es sobretodo para proteger nuestros equipos cisco de sobretensiones.

Elegimos Eaton la mejor relación precio-rendimiento y los modelos RT y rack de 1 U se suministran con los kits de rack. También nos proporciona un manual de instalación del equipo y una parte de troubleshooting. También dispone de un teléfono de atención técnica y una garantía de dos años.

Descripción de los equipos

Que nos proporcionan los SAI's Eaton?

Estos equipos nos proporcionan una máxima disponibilidad ya que las tomas de salida del Eaton Evolution están controladas individualmente para conmutar y gestionar la carga con el propósito de maximizar el tiempo de autonomía y proporcionar de serie las funciones de reinicio remoto y arranque secuencial. A parte, cuando funciona en modo batería, el Eaton Evolution sigue proporcionando una señal de salida de alta calidad para los equipos que estén conectados. Además las baterías pueden ser substituidas en caliente.

Por otro lado, Eaton amplia gama de opciones de supervisión utilizando la aplicación Eaton Software Suite, que incluye gestión de potencia punto a punto, SNMP, salidas de relé, etc.

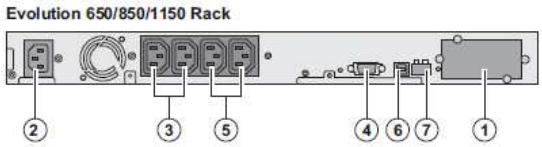
a) Eaton evolution UPS 850 (modelo tipo rack 1U)

ESPECIFICACIONES TÉCNICAS	650	850	1150	1550
Potencia (VA / W)	650 VA / 420 W	850 VA / 600 W	1150 VA / 770 W	1550 VA / 1100 W
Formato	Torre o rack 1 U	Torre o rack 1 U	Torre o rack 1 U	Torre o rack 1 U
Características				
Tecnología	Alta frecuencia en Line Interactive (elevador + atenuador)			
Tensión de entrada e intervalos de frecuencia sin usar baterías	160 V, 294 V (ajustable a 150 V, 294 V) De 47 a 70 Hz (sistema de 50 Hz), de 56,5 a 70 Hz (sistema de 60 Hz), hasta 40 Hz en modo de baja sensibilidad (programable usando el software Personal Solution-Pac).			
Tensión de salida y frecuencia	230 V (+6 / -10 %) (Ajustable a 200 V (disminución del 10 % de la potencia de salida) / 208 V / 220 V / 230 V / 240 V), 50-60 Hz ± 0,1 %			
Conexiones				
Entrada	1 toma IEC C14 (10 A)			
Salidas	4 conectores IEC C13 (10 A)	4 conectores IEC C13 (10 A)	4 conectores IEC C13 (10 A)	4 conectores IEC C13 (10 A)
Tomas controladas a distancia	2 grupos de 1 x IEC C13 (10 A)	2 grupos de 1 x IEC C13 (10 A)	2 grupos de 1 x IEC C13 (10 A)	2 grupos de 1 x IEC C13 (10 A)
Salidas adicionales con HS MBP	4 tomas FR / Schuko, 3 tomas BS, 6 tomas IEC 10 A o bloques de terminales (versión HW)			
Salidas adicionales con FlexPDU	8 tomas FR / Schuko, 6 tomas BS o 12 tomas IEC 10 A			
Baterías				
Tiempos de autonomía estándar para una carga del 50 y el 70 %	9 / 6 min	16 / 7 min	14 / 7 min	14 / 7 min
Gestión de la batería	Prueba semanal automática (periodo ajustable), reconocimiento automático de las baterías externas => maximización continua del tiempo de autonomía + protección contra descarga profunda			
Comunicación				
Puertos de comunicación	1 puerto USB + 1 puerto serie RS232 y contactos de relé (los puertos USB y RS232 no se pueden usar de forma simultánea) + 1 minibloque de terminales para apagado / encendido remoto y desconexión remota			
Ranuras para tarjeta de comunicación	1 ranura para la tarjeta NMC Minislot, NMC ModBus / JBus o MC Contacts / Serial			

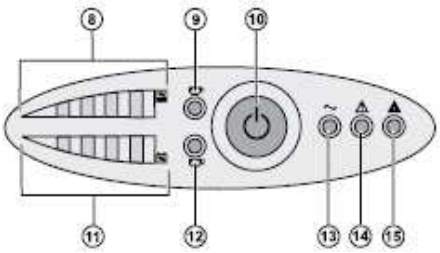
Esquema parte de atrás:

Conexiones equipo SAI 850

(1) Ranura para tarjeta opcional de comunicaciones
(2) Cable de alimentación de 6 pies con fusible 5-15P de 15A
(3) 2 NEMA 5-15R para conexión del equipo
(4) Puerto de comunicación RS232
(5) 2 salidas programables NEMA 5-15R
(6) Puerto de comunicación USB
(7) Conector para RPO/ROO remoto (Apagado remoto / Encendido-Apagado remoto)
(a) LED indicador de alarma por falla de cableado del sitio con botón de reseteo



Esquema parte de delante de control:



(8) Barra gráfica que indica el porcentaje de carga
(9) Salida programable 1 alimentada
(10) Botón ON/OFF para la UPS y las salidas
(11) Barra gráfica que indica el porcentaje de carga de la batería
(12) Salida programable 2 alimentada
(13) LED de carga protegida
(14) LED de funcionamiento reducido
(15) LED de carga no protegida

a) Eaton Evolution UPS S3000 RT (modelo tipo rack 3U) y baterías S EXB (3000 RT 2U)

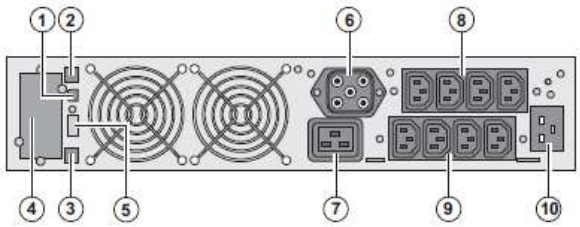
	Evolution S 1250	Evolution S 1750	Evolution 2000	Evolution S 2500	Evolution S 3000
Potencia de salida	1250VA/1150W	1750VA/1600W	2000VA/1600W	2500VA/2250W	3000VA/2700W
Red eléctrica de alimentación ▸ Tensión de entrada nominal ▸ Margen de tensión de entrada ▸ Margen de frecuencia de entrada	Monofásica 220~240 V de 160 V a 294 V (1) 47 Hz a 70 Hz (red 50 Hz), 56,5 Hz a 70 Hz (red 60 Hz) (2)				
Salida utilización en funcionamiento con batería ▸ Tensión ▸ Frecuencia	230 V (+6/-10%) (3) 50/60 Hz ±0,1%				
Batería (de plomo hermético sin mantenimiento) ▸ Estándar	4 x 12 V 7,2 Ah	4 x 12 V - 9 Ah		6 x 12 V 7,2 Ah	6 x 12 V 9 Ah
▸ Extensión posible (hasta 4 EXB)	Evolution S EXB 1250/1750 (4)		No	Evolution EXB S 2500/3000 (5)	
Medio ambiente ▸ Temperatura de funcionamiento ▸ Temperatura de almacenamiento ▸ Humedad	0°C a 40°C -25°C a 40°C 20% a 90% (sin condensación)				
▸ Nivel acústico	< 45 dBA			< 50 dBA	

(1) Umbrales alto y bajo ajustables con el software **Personal Solution-Pac**.
(2) Hasta 40Hz en modo de sensibilidad baja (programable con el software **Personal Solution-Pac**).
(3) Ajustable entre 200V (desclasificación de un 10% de la potencia de salida) / 208V / 220V / 230V / 240V
(4) Batería **Evolution S EXB 1250/1750**: 2 cadenas de 4 x 12V / 9Ah.
(5) Batería **Evolution S EXB 2500/3000**: 2 cadenas de 6 x 12V / 9Ah.

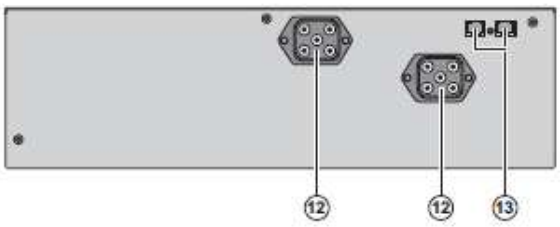
Esquema parte de atrás:

Conexiones equipo SAI 3000

(1) Puerto de comunicación USB
(2) Puerto de comunicación RS232
(3) Conector de reconocimiento automático de un módulo de batería adicional
(4) Emplazamiento para tarjeta de comunicación opcional.
(5) Conector para la conexión de un mando a distancia de Marcha/Parada o de una parada de emergencia.
(6) Conector para la conexión de un módulo de batería adicional (excepto **Evolution 2000**)
(7) Toma 16A para la conexión de los equipos
(8) 2 grupos de 2 tomas programables para la conexión de los equipos
(9) Grupo de 4 tomas para la conexión de los equipos
(10) Toma para la conexión a la red eléctrica de alimentación

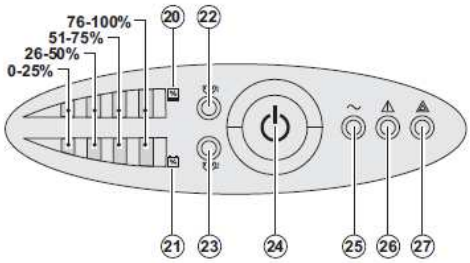


Baterías SAI 3000



(12) Conectores para la conexión de los módulos de batería (hacia el SAI o hacia los otros módulos de batería)
(13) Conectores de reconocimiento automático de los módulos de batería

Esquema parte de delante de control:



(20) Barra de leds del nivel de potencia consumido en la salida
(21) Barra de leds del nivel de carga de la batería
(22) Tomas programables 1 alimentadas
(23) Tomas programables 2 alimentadas
(24) Botón luminoso Marcha/Parada (ON/OFF) de las tomas de salida
(25) Indicador luminoso equipos protegidos
(26) Indicador luminoso de funcionamiento degradado
(27) Indicador luminoso equipos no protegidos

5.2.5 – Configuración

En este apartado explicamos los elementos más importantes para la configuración de nuestros routers que nos ayudaran a entender mejor la plantilla de configuración que encontraremos en el anexo.

Configuración de Stack

Si queremos ser nosotros el que elijamos si un equipo es el master o el slave debemos seguir estos pasos:

a) Como conseguimos que el nuevo switch conectado sea el slave?

1.- Cambiamos la prioridad del switch a añadir a 1.

2.- Apagamos el switch a añadir.

3.- Nos aseguramos de que el stack esta bien conectado.

4.- Encendemos el nuevo switch stackado.

b) Como conseguimos que el nuevo switch conectado sea el master?

1.- Cambiamos la prioridad del switch a un número >=5 por configuración.

2.- No apagamos el switch a añadir.

3.- Nos aseguramos de que el stack esta bien conectado.

4.- Cuando lo conectamos los otros switches se reinician para ver al nuevo master.

Finalmente, el número de stack define cada miembro del stack. Por defecto todos los equipos tienen el número 1 como número de stack , cuando se integran como miembros del stack se van ordenando del menor al mayor número disponible. El número dentro del stack de los diferentes miembros se puede cambiar mediante configuración.

De la misma forma si tu coges un miembro del stack y lo mueves a otro conjunto o stack también retiene el número a no ser que ya este utilizado por otro miembro.

Subnetting

La implementación de VLSM aparece a partir de la escasez de direcciones IP y nos ofrece la posibilidad de un uso más eficiente del espacio de direcciones IP, tanto en términos de subredes posibles como de dispositivos para subred.

El procedimiento seria el siguiente:

Nos proporcionaran una red definida dentro de una clase ip. Las clases pueden definirse en:

Clase A: 8 bits parte de red, 24 bits parte de host. (Redes grandes)
Clase B: 16 bits parte de red, 16 bits parte de host. (Redes medianas)
Clase C: 24 bits parte de red, 8 bits parte de host. (Redes pequeñas)

Usaremos una máscara de longitud variable para la implementación de subredes provenientes de la misma dirección de red basada en clase (no se puede subnetear una dirección de red sin Clase ya que ésta ya paso por este proceso).

Por ejemplo, una máscara de clase C (direccionamiento por clase) seria la siguiente:

11111111.11111111.11111111.00000000 = 255.255.255.0

CLASE C	RED			HOST
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Máscara por defecto	255	255	255	0

Tenemos 24 bits que identifican la red y 8 bits para la asignación de la parte de host que se traduce en 256-2=254 ip's libres para asignar a host (2^8 = 256 y a este valor le restamos la ip de red y la ip de broadcast).

Así pues la máscara se divide en dos partes, la porción de red que indica la dirección de red y la porción de host que identifica la parte de la dirección de red que se usa para asignar direcciones de host.

Ahora jugando con el tamaño de la máscara podemos crear subredes a partir de una red con clase teniendo en cuenta que la cantidad de subredes es igual a 2N, donde "N" es el número de bits "robados" a la porción de host y la cantidad de hosts por subred es igual a 2M -2, donde "M" es el número de bits disponible en la porción de host y "-2" es debido a que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.

Ahora conociendo el proceso calcularemos las redes a asignar a Barcelona y Madrid teniendo en cuenta que la RFC 1918 (address allocation for private Internets) define los rangos siguientes para ip's privadas:

Clase A: 10.0.0.0 - 10.255.255.255
Clase B: 172.16.0.0 - 172.31.255.255
Clase C: 192.168.0.0 - 192.168.0.255

Entonces tenemos una oficina con 2 departamentos (en plantas diferentes), una delegación con 80 usuarios, despachos de jefatura y servidores:

Disponemos de la direcciones de red privada 192.168.10.0/22 y 192.168.11.0/24 y nos solicitan que, para ahorrar ip's, dentro de esta red convivan los usuarios de departamento y los jefes de la empresa perteneciendo a diferentes redes. También nos indican que tenemos 20 jefes de departamento.

a) Queremos saber que red asignar a los 100 usuarios de la primera planta.
De los 8 bits de la máscara 24 usamos 7 para los usuarios del departamento.
Entonces nos quedan 2^7-2=126 host disponibles.
La fórmula aplicable es: 2^n-2 (donde n representa el número de bits no enmascarados, todos los bits que tiene valor 0 en la máscara).
Entonces, sabemos que la máscara de último octeto es 10000000=128.

Subred: 192.168.10.0
Máscara: 255.255.255.128
Primera dirección de rango: 192.168.10.1
Última dirección de rango: 192.168.10.126
Dirección broadcast: 192.168.10.127
Número de host: 126 host

b) Queremos saber que red asignar a los 100 usuarios de la segunda planta.
Como en el caso anterior cogemos 7 bits → 2^7-2=126 host disponibles.
Entonces, sabemos que la máscara de último octeto es 10000000=128.

Subred: 192.168.10.128
Máscara: 255.255.255.128
Primera dirección de rango: 192.168.10.129
Última dirección de rango: 192.168.10.254
Dirección broadcast: 192.168.10.255
Número de host: 126 host

c) Ahora asignamos 100 direcciones para los usuarios de la delegación de Barcelona:

Subred: 192.168.11.0
Máscara: 255.255.255.128
Primera dirección de rango: 192.168.11.1
Última dirección de rango: 192.168.11.126
Dirección broadcast: 192.168.11.127
Número de host: 126 host

d) Reservamos 60 direcciones para servidores de datos (virtuales y no virtuales). Para proporcionar 60 host utilizamos 6 bits → 2^6-2=62.

Entonces, sabemos que la máscara de último octeto es 11000000=192.

Subred: 192.168.11.128
Máscara: 255.255.255.192
Primera dirección de rango: 192.168.11.129
Última dirección de rango: 192.168.11.190
Dirección broadcast: 192.168.11.191
Número de host: 62 host

e) Ahora queremos 20 ip's para los jefes, por lo tanto vamos a calcular el número de host. Para proporcionar 20 host utilizamos 5 bits → 2^5-2=30.
Entonces, sabemos que la máscara de último octeto es 11100000=224.

Subred: 192.168.11.192
Máscara: 255.255.255.224
Primera dirección de rango: 192.168.11.193
Última dirección de rango: 192.168.11.222
Dirección broadcast: 192.168.11.223
Número de host: 30 host

Finalmente queda por decir que a nivel de WAN necesitaremos un protocolo de enrutamiento que permita soporte VLSM . En nuestro caso hemos elegido BGP.

VLAN

La vlan es un grupo virtual asociada a interfaces de equipos de red que se utilizan para segmentar los dominios de colisión y de broadcast.

Cada vez que una trama llega a un switch, lo primero que hace es comprobar si tiene la MAC de origen y de destino en su tabla de forwarding, para encaminar el paquete en función de esta información. Por lo tanto, podemos adivinar que lo primero que podríamos hacer para aislar un tráfico de otro, creando diferentes dominios de broadcast, es tener tablas de forwarding distintas para cada uno. De esta manera las direcciones MAC de un dominio nunca podrán intercambiar tráfico con las de otro dominio.

Debemos tener en cuenta de que la VLAN 1 viene configurada por defecto y no se puede eliminar y que a partir de la VLAN 1001/1002 son casos especiales.

Partiendo de este concepto, podemos añadir una VLAN a un puerto del switch de tal forma que cuando un paquete entra en ese puerto que pertenece a una única VLAN, el equipo buscará las MAC origen y destino en la tabla a la que correspondo ese puerto.
Esta configuración corresponde a una vlan de acceso (vlan access).

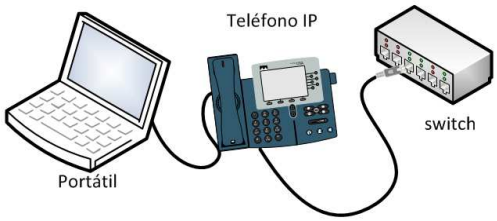
Teniendo en cuenta que un red LAN esta formada por más de un switch, la unión entre ellos estará compuesta por puertos que transportan información de varias VLAN's. Esta configuración corresponde a un troncal (VLAN trunk) que es un tipo de enlace especial que se utiliza para unir dos o más switch entre sí.

La característica principal de este tipo de puertos es que podrán transportar tráfico de más de una vlan y que será necesario realizar un etiquetado. En referencia al último punto, es así porque debemos tener en cuenta de que por el puerto llegarán paquetes de cualquier VLAN lo

que nos obliga a poner algún tipo demarca en el paquete para que el switch de destino sepa en que tabla debe buscar. El protocolo más extendido para etiquetar el ID de VLAN es el IEEE 802.1q.

En los puertos de acceso usuarios utilizaremos, por un lado la vlan de acceso para la parte de datos, sobre la que ya hemos hablado con anterioridad. Para la parte de la red de voz y en el mismo puerto utilizaremos una configuración únicamente disponible en cisco: “voice vlan”.

Esta configuración se utiliza para transportar tráfico de voz des de un teléfono IP i permite priorizar los paquetes de voz.



Otra configuración posible seria configurar un trunk en el puerto de acceso permitiendo el paso de las vlan de datos y voz con su correspondiente etiquetado como bien hemos explicado antes. Una de los puntos a tener en cuenta es que el tráfico del ordenador vendrá sin etiquetar. Para este tráfico utilizaremos la vlan nativa. De modo que si a un puerto llega una trama sin etiquetar, la trama se considerara perteneciente a la VLAN nativa de ese puerto.

Este tipo de configuración aunque es efectiva requiere más recursos de CPU y no se recomienda utilizarla en todos los puertos de acceso ya que puede sobrecargar el switch.

Nuestra tabla de configuración de red por vlan será la siguiente:

Vlan	Descripción	Red	Máscara	Usuarios	IP interfaz Vlan
10	Red Barcelona 1 usuarios planta 1	192.168.10.0	255.255.255.128	126	192.168.10.1
11	Red Barcelona 1 usuarios planta 2	192.168.10.128	255.255.255.128	126	192.168.10.129
12	Red Barcelona 1 jefatura planta 2	192.168.11.192	255.255.255.224	30	192.168.11.193
13	Red Barcelona 2 usuarios datos	192.168.11.0	255.255.255.128	126	192.168.11.1
14	Red Servidores Barcelona	192.168.11.128	255.255.255.192	62	192.168.11.129
10	Red Madrid 1 usuarios planta 1	192.168.12.0	255.255.255.128	126	192.168.12.1
11	Red Madrid 1 usuarios planta 2	192.168.12.128	255.255.255.128	126	192.168.12.129
12	Red Madrid 1 jefatura planta 2	192.168.13.192	255.255.255.224	30	192.168.13.193
13	Red Madrid 2 usuarios datos	192.168.13.0	255.255.255.128	126	192.168.13.1
14	Red Servidores Madrid	192.168.13.128	255.255.255.192	62	192.168.13.129
20	**Red de gestión de los switch	192.168.14.0	255.255.255.0	254	192.168.14.2
2	Red de datos con el router	192.168.1.2	255.255.255.252	2	192.168.1.2

Access-List

A nivel dos el uso de Vlan (privadas) nos permiten aislar los puertos de switch dentro de un mismo dominio de broadcast, evitando que los dispositivos conectados en estos puertos se comuniquen entre sí aunque pertenezcan a la misma VLAN y subred que explicaremos a continuación de este punto.

En este punto vamos a estudiar como aislar nuestras redes a nivel 3 en los equipos núcleo de la red LAN.

Una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

En resumen, las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switchs. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición preconfigurada.

Una vez creada la ACL debemos aplicarla a una interfaz (puede ser física o una interfaz vlan) indicando si la aplicamos al tráfico saliente o entrante.

Finalmente, dentro de la configuración de ACLs existen dos tipos:

1.- ACL estándar, donde solo tenemos que especificar una dirección de origen.

2.- ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.

En un principio nosotros usaremos las estándares denegando el acceso de un rango de red a otro.

El rango de las access-list estándar va de la 0 a la 99 y la sintaxis del comando seria el siguiente:

access-list <0-99> < permit/deny> < rango de red ip> <wilcard>

* permit/deny: permitimos o denegamos el acceso a esa red.

**wilcard: conocidas como máscaras de subred inversas, en las direcciones de la lista de acceso. Donde un bit de máscara a 0 significa comprobar el valor del bit correspondiente y un bit de máscara a 1 significa ignorar el bit correspondiente.

A continuación añadimos el comando de configuración: ip access-group < nº de acl> en la interfaz donde queremos aplicarla.

Configuración duplex y velocidad en los puertos

Duplex-Missmatch es un tipo de anomalía o error que se produce cuando existe un error en la negociación de dos puertos. Es uno de los problemas más frecuentes en el switching y de los más sencillos de solucionar.

Se produce cuando tenemos un puerto de un switch configurado como HALF-Duplex y el otro extremo configurado como FULL-Duplex.

Para evitar este problema es tan sencillo como:

a) Forzar la velocidad y el modo duplex en ambos extremos
b) Configurar ambos extremos en modo “Autonegociación”
c) Si uno de los dos extremos no es configurable debemos averiguar la velocidad y el modo duplex y forzarlo en el otro extremo.

Hay que tener en cuenta que este error solo se reproduce cuando hay cierto volumen de tráfico y se produce tanto en puertos de enlace con hosts como entre switch o routers.

Este fallo se produce porque cuando un extremos FD transmite lo hace independientemente de lo que esta recibiendo por el otro extremo ya que puede recibir y transmitir a la vez y no tiene en cuenta el concepto de colisión. En cambio cuando HD escucha lo que va recibiendo y en el momento de contestar se produce una colisión ya que recibe tráfico mientras lo esta transmitiendo. Al anotar una colisión detiene el tráfico y dicha trama se pierde. El otro extremo recibe una trama incompleta y la registra como CRC o frame error.

Por lo tanto es imprescindible que la negociación de velocidad y duplex sea la misma en ambos extremos.

En nuestra red configuraremos los puertos con duplex auto y speed auto.

VTP

El VLAN Trunk Protocol se utiliza para reducir la administración en una red de switchs. Cuando configuramos una VLAN nueva sobre un servidor VTP, la VLAN se distribuye a través de todos los switchs del dominio. Esto reduce la necesidad de configurar la misma VLAN en todos los equipos. VTP es un protocolo propietario de Cisco.

Para ello configuraremos un switch como servidor VTP, en nuestro caso los switch centrales de Barcelona y Madrid, y utilizando los enlaces configurados como trunk podemos enviar información de VLANs al resto de los equipos utilizando el protocolo 802.1q.

Los anuncios VTP se dividen en 3 tipos:

1.- Summary advertisement: Se envían cada 5 minutos del servidor al cliente para informar a los switch pertenecientes al grupo cual es el número de revisión de configuración actual, para su dominio de gestión.
Además se envía después de un cambio de configuración.

2.- Subset advertisement: Se envían ante cambios de configuración en la VLAN o en respuesta a una solicitud de anuncio.

3.- Advertisement request: es la petición de un “Advertisement summary” o de un “Subset advertisement” del servidor de dominio en questión. Se envían cuando:

- El nombre de dominio VTP ha sido modificado.
- Un switch recibe un “Advertisement summary” con una revision posterior a la suya.
- Un mensaje de “Subset advertisement” se ha perdido.
- El switch ha sido reseteado.

Estos mensajes se realizan a una dirección MAC multicast especial 01-00.0C-CC-CC-CC.

Las modalidades de funcionamiento VTP son:

1.- Servidor (Server): En este equipo podremos añadir, borrar o renombrar VLANs.
También anuncia el nombre de dominio VTP, la configuración de las VLANs y el número de revisión de configuración.
El Servidor VTP mantiene una lista de todas las VLANs del dominio en la memoria NVRAM y puede recuperar la información si el switch es reseteado.

2.- Cliente (Client): NO puede añadir, modificar o borrar VLANs. Mantiene una lista de todas las VLANs del dominio pero no almacena su infamación en la memoria NVRAM.

3.- Transparente (Transparent): No participa en el dominio VTP y por lo tanto ni envía ni acepta actualizaciones de VLANs (se mantiene al margen). Daremos de alta las VLANs de forma manual. Cuando estos equipos reciben un anuncio "Summary advertisement" lo retransmiten a los demás equipos

En resumen, en nuestra red crearemos dos dominios VTP llamado Barcelona y Madrid en sus respectivas redes LAN y los servidores serán los equipos switch centrales de ambas capitales. Los demás switch de la LAN estarán en modo cliente.

Para no crear un conflicto en la red VTP antes de conectar cualquier switch deberemos poner su número de revisión a 0 ya que si lo conectamos a nuestra red con un número mayor al actual y en modo servidor o cliente éste puede llegar a ser el nuevo servidor y eliminar todas las VLANs existentes.

Spanning-Tree

Por un lado es importante redundar las infraestructuras para minimizar al máximo los puntos de fallo, pero por otro lado, se deduce fácilmente que en consecuencia pueden aparecer bucles. Cuando no se conoce una dirección MAC ese paquete es retransmitido por todos los puertos excepto por el que se ha recibido y estos broadcast serán los responsables de los bucles en la red. Este problema tiene fácil solución y se llama Spanning-Tree.

El protocolo Spanning-Tree tiene el Standard 802.1d y por la IEEE y utiliza el algoritmo STA. Este algoritmo detecta si el switch tiene más de una manera de comunicarse con un nodo (más de un camino posible), y en consecuencia determina cual de todos los caminos es el mejor y bloquea el otro camino alternativo.

Existen varias modalidades de Spanning-Tree pero todos se basan en la misma idea : evitar y eliminar los bucles en una red Ethernet de nivel 2 posibilitando solamente un camino para llegar a un destino.

Los pasos que seguirá son los siguientes:

Primero debemos elegir el "Bridge" que tendrá la función de "Root" de Spanning-Tree. Este papel se determina por el llamado ID (campo configurable de prioridad) y la dirección MAC del propio equipo.
Concretamente, la cadena tiene un tamaño de 8 bytes y contiene 2 bytes de prioridad acompañada con la dirección MAC.

En nuestro caso los switches centrales de Barcelona y Madrid tendrán la mayor prioridad, la 4096 <priority 4096> para ser el Root de la red LAN en la misma provincia.

Si con el tiempo queremos ampliar el CORE de la LAN en ambas provincias, las prioridades de más alta a más baja de los diferentes equipos centrales irían así:

1.- 4096
2.- 8192
3.- 12288
4.- 16384

… (Múltiplos de 16)

De manera predeterminada los switch cisco tienen la prioridad 32768.

Seguidamente se calcula el coste de todos los caminos desde el root hasta cada nodo de la red. Para poder realizar este estudio se usan las llamadas BPDU's y son paquetes enviados por el Root y llegarán a cada nodo de la red por todos los puertos posibles. Están formadas por:

-El identificador root del bridge (BID) del propio bridge.
-El coste de ruta o path cost del root bridge que nos indica el coste para llegar al root.
-El identificador de puerto o Port ID, que identifica el puerto del switch por donde se envió la BPDU.

¿Como calculamos el Path Cost?

El Path Cost es la sumarización de los costes de cada uno de los puertos por los que ha pasado una BPDU para llegar al nodo destino des de el Root. De aquí se deduce que cada puerto tiene un coste y éste se calcula a partir del ancho de banda del mismo:

Link Speed	Port Cost
10 Gigabit Ethernet 10000 Mbps	1
Gigabit Ethernet : 1000 Mbps	4
Fast Ethernet : 100 Mbps	19
Ethernet : 10 Mbps	100

Por lo tanto, el camino con el menor Path Cost será el elegido como camino más cercano al root y por lo tanto más recomendable. Este puerto siempre tendrá en estado "Forwarding".

Un punto a tener en cuenta es que en el caso de que tengamos un mismo patch cost por dos caminos diferentes ganará el puerto que tenga la mac menor.

Finalmente, por configuración podemos modificar el coste de un puerto a mayor en caso de querer penalizar un camino.

Una vez calculados los distintos caminos y sus pesos hay que cambiar el estado de los puertos que no han sido "elegidos" como principales. Los posibles estados son los siguientes:

- Listening: El puerto se queda escuchando las BPDU's que recibe de Spanning-Tree:
  - Atiende la BPDU's recibidas, las procesa pero no las transmite.
  - No envía ninguna trama y descarta todo lo que reciba.
  - No añade ninguna MAC en su tabla de forwarding.

- Learning: Las funciones del puerto en este estado son las siguientes:
  - Atiende las BPDU's recibidas y las procesa y transmite por este mismo puerto.
  - No envía ninguna trama y descarta todo lo que reciba por el puerto en este estado.
  - Incorpora a su tabla de forwarding las MAC origen de las tramas recibidas.

- Blocking: En este estado en puerto no procesa ninguna trama.
  - Atiene las BPDU's pero no las procesa ni las retransmite.
  - No envía ninguna trama y descarta todo lo que recibe por él.
  - No añade ninguna MAC a su tabla de forwarding.

- Forwarding: En este estado el puerto es capaz de recibir tramas.
    - Atiene las BPDU's recibidas y las procesa y transmite por el mismo puerto.
    - Envía y recibe tramas.
    - Incorpora en su tabla de forwarding las MAC's origen de todas las tramas que recibe.
    - El puerto sencillamente esta operativo y puede recibir y enviar datos.

En resumen, lo que hacemos es dejar activo el mejor camino hasta en nodo destino y anular los caminos redundantes que podemos necesitar en caso de que alguno de los enlaces elegidos caiga. Por este motivo el algoritmo de spannning-tree se ejecuta periódicamente (El paquete Hello de la BPDU's es cada 2 seg.) y , lógicamente, cada vez que ocurre un cambio en la red.

El tiempo de convergencia de este algoritmo suele estar entre los 30 y 50 segundos, menor en las variantes del protocolo como Rapid Spanning-Tree.

En nuestro caso usaremos el Spanning-Tree modo pvst (por vlan) ya que opera en capa 2 y podemos bloquear o permitir el paso de vlans por puerto de manera separada. Tratará cada vlan como una red independiente.

Si la red creciera en un futuro y aumentará significativamente el número de vlans configuradas seria más recomendable usar Múltiple Spanning Tree MSTP ya que en caso de que existan gran cantidad de vlans permite que la CPU del switch trabaje más eficientemente.

Lo que hace básicamente es balancear la carga de vlans por puerto cuando tenemos un escenario donde tenemos switch redundantes conectados a un único switch.

Teniendo ahora claro el funcionamiento de Spanning-Tree, nos queda un punto por tratar y és el puerto de acceso a usuario que no deberá participar en el cálculo, ya que por un lado, no puede crear un bucle físico y por otro lado servirá para ahorrar trabajo y tiempo de convergencia al protocolo.

En el puerto de acceso del teléfono ip, ordenador, impresora…configuraremos dos parámetros solo disponibles en Cisco:

1.- PortFast: Para descartar una pérdida de tiempo innecesaria en el cálculo de puntos que no pueden causar bucles STP incorpora la configuración " PortFast" que indica al protocolo que ese puerto no pertenece al árbol y éste pasa directamente al estado Forwarding sin pasar por los demás estados.

2.- BPDU-Guard: A razón de que la configuración de Portfast puede causar una caída de la red ya que solamente sirve para poner el estado de Forwarding al puerto más rápidamente pero éste sigue estando bajo el dominio de STP y si llegan BPDU's se tratan de la misma manera.
La solución es BPDU-Guard que controla la llegada de BPDU's en el puerto bloqueando, o mejor dicho, deshabilitando el puerto.

Ambos parámetros deben ir siempre configurados de manera conjunta en el puerto de acceso.

Port Security

En el caso anterior hemos comentado que los puertos de acceso a usuario no van a participar en STP. Esto podría provocar un fallo si conectáramos un switch en ese puerto de acceso. Para evitar esto y tener un mayor control de los equipos conectados en nuestra red utilizaremos la configuración “Port Security”.

Lo que conseguimos con esta característica es restringir el tráfico de entrada a un puerto limitando las direcciones MAC que pueden hacerlo.

Podemos:

1.- Limitar el número máximo de MAC permitidas en el puerto y de esta manera cuando se supere dicho número la seguridad del puerto aplica el modo “violación”.

2.- Especificar que MAC perteneciente a un equipo puede conectarse a ese puerto y de esta manera cuando se conecte un equipo distinto la seguridad del puerto aplica el modo “violación”. La configuración se llama : Sticky MAC Addresses y si grabamos la configuración del equipo la configuración de Port Security guarda las direcciones MAC aprendidas dinámicamente en la configuración de inicio del equipo.

3.- En todos los casos cuando una dirección MAC permitida/aprendida de un puerto intenta acceder a otro puerto seguro en la misma VLAN la seguridad responde de la misma forma.

Cuando hemos “violado” la seguridad de un puerto podemos tener 3 respuestas posibles, todas ellas configurables:

1.- Protect: Se tiran los paquetes de direcciones de origen desconocidas hasta que se modifique el número de direcciones MAC.

2.- Restrict: Se tiran los paquetes de direcciones de origen desconocidas hasta q se modifique el número de direcciones MAC y incrementa el contador de violaciones de seguridad.

3.- Shutdown: El estado de la interfaz pasa a “error-disabled” y envía una notificación trap SNMP.

En nuestro caso permitiremos un máximo de dos MAC’s por puerto de acceso, una para el teléfono y otra para el ordenador/ impresora IP.

Otro punto a tener en cuenta de nuestra configuración es que en nuestro caso, como comentábamos con anterioridad, los puertos de acceso deben configurarse con vlan de acceso pero en el caso que decidamos configurarlo como trunk, la configuración de ese puerto debe contener estos parámetros:

switchport
switchport trunk encapsulation
switchport mode trunk
switchport nonegotiate

CDP

Para que al administrador de la red le sea más sencillo entender las conexiones entre los diferentes equipo Cisco habilitaremos el protocolo CDP dentro, únicamente, de la LAN.

Es un protocolo de red de nivel 2 desarrollado por la casa Cisco Systems. Se utiliza para compartir información sobre otros equipos Cisco que están directamente conectados, como por ejemplo, la versión de IOS y la dirección IP.

Este protocolo también se puede usar para realizar encaminamientos bajo demanda que se basa en incluir información de encaminamientos en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

Los dispositivos Cisco envían anuncios a la dirección de destino de multidifusión 01:00:0C:CC:CC:CC (usada también por VTP).

Los anuncios de CDP se envian por defecto cada 60 segundos por las interfaces que soportan cabeceras SNAP como por ejemplo Ethernet, Frame Relay y ATM.

Cada dispositivo cisco que soporta CDP almacena la información recibida de otros dispositivos en una tabla que se refresca cada vez que recibe un anuncio y la información de un dispositivo se descarta tras tres anuncios no recibidos por su parte (180 segundos).

Finalmente, la información contenida en los anuncios de CDP varía con el tipo de dispositivo y la versión de la IOS (sistema operativo). Esta información incluye la versión de la IOS, el nombre del equipo, todas las direcciones de todos los protocolos configurados en el puerto por donde se transmite la trama CDP, el identificador del puerto, el tipo y modelo del dispositivo, la configuración duplex/simples, el dominio VTP, la VLAN nativa , el consumo energético y demás información específica del dispositivo.

DHCP

El protocolo DHCP es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Un servidor DHCP es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes autoconfigurarse. Para que un PC solicite la configuración a un servidor, en la configuración de red de los PCs hay que seleccionar la opción 'Obtener dirección IP automáticamente'.
El servidor proporcionará al cliente al menos los siguientes parámetros:

- Dirección IP
- Máscara de subred

Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como:

- Puerta de enlace
- Servidores DNS
- Muchos otros parámetros más

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.

El cliente dispone de un servidor DHCP para administrar la asignación de las direcciones ip a los host de la red. Por este motivo en nuestros switch y router habilitaremos el paso de anuncios dhcp y indicaremos que ip de host tiene el servidor en el momento de la configuración de cada red de usuarios.

5.3 – TELEFONÍA

5.3.1 – Conceptos teóricos

Establecimiento de una llamada IP

La señalización es un proceso que se establece antes de que se curse una llamada.
Los pasos básicos en el establecimiento de una llamada IP son los siguientes:

1.- El terminal 1 descuelga el teléfono y marca numero de teléfono.
2.- Los números/extensiones cortos marcados son enviados al Call Server.
3.- El procesador relaciona la numeración con la dirección real de terminal llamado y determina donde enrutar la llamada.
4.- El procesador de llamadas señaliza la llamada para que el otro terminal empiece a sonar.
5.- Cuando el terminal 2 descuelga el teléfono se abre una sesión RTP (Real-time Transport Protocol) protocolo a tiempo real de capa 4, controla y mantiene la sesión entre ambos terminales y ya pueden mantener conversación

Establecimiento de una llamada entre IP y analógico/digital

Pasos:

1.-El teléfono descuelga y marca
2.- Media Gateway pasa los datos que obtiene del Teléfono al Call Server.
3.- El Call Server revisa los permisos de llamada, y las configuraciones que hayamos aplicado sobre el abonado.
4.- El Call Server establece la señalización entre GD de MG de la oficina.
5.- Cuando la Extensión X levante el teléfono, se establece la llamada que mantienen los 2 MG pero es supervisada por el CS.
6.- Debemos tener en cuenta que la GD realizará la conversión de la señal analógica/digital al tipo IP y al revés.

Factores que pueden influir en la calidad de servicio:

1.- Latencia: retardos acumulados en la transmisión de paquetes.

2.- JITTER: Variación de retardos acumulados entre paquetes, no es constante. Se trata de una latencia variable producida por la congestión de tráfico en el backbonede red, etc.

3.- Pérdida de paquetes: Se produce cuando uno o más paquetes que viajan a través de una red no llegan a su destino. Packet loss o pérdida de paquetes, se distingue como uno de los principales tipos de errores encontrados en las comunicaciones digitales.

4.- ECHO: Es un desajuste de la impedancia en los medios de transmisión. En cualquier red, incluyendo las de telefonía tradicional, siempre existe el eco, solo que a niveles tan bajos que no pueden ser percibidos por el oído humano. Este fenómeno puede controlarse con supresores o "canceladores" de eco.

DSP's

Digital Signaling Process, es un microprocesador para el tratamiento de señal digital, se trata de un componente hardware que realiza el tratamiento de compresión de voz, cancelación de eco, detención de actividad de voz.

En nuestro caso los encontraremos en la tarjeta "GD" y la tarjeta de expansión "GA".

Cancelación de ECO

Cuando una señal pasa de una línea de 4 hilos a una de 2 hilos analógicos se produce eco electrónico debido al cambio de características eléctricas y de adaptación de impedancias. Cuando en el propio teléfono el sonido del auricular se introduce en el micrófono se restrasmite la señal de nuevo al origen y esto es eco acústico. El eco es más apreciable con mayor retardo exista en la red. Por estos motivos son necesarios los canceladores de ECO.

Las tarjetas del mediagateway de conexión de terminal incluyen este cancelador.

Ruido de Confort

Es una muestra de ruido de fondo monótono para evitar que se perciba que la comunicación se ha cortado.

5.4.1 – Material contemplado

Lo principales elementos del OmniPCX Enterprise son el Call Server (CS) que es la unidad de control de la OXE (la CPU) y los Mediagateways que permiten conectar el mundo de la telefonía tradicional con el mundo TCP/IP. Éstos últimos se conectan al CS a través de una tarjeta controladora de MG llamada GD o INTIP en caso de los ACT (hardware cristal).
Primero realizamos una tabla con la cantidad de materia a aprovisionar:

Oficina	Enlaces	Terminal analógico cliente	Terminal IP 4018	Terminal IP 4028	Terminal IP 4068	Mediagateway	Call Server
Barcelona 1	2 PRI telefonía fija	10	100	80	20	2 MG	1
Barcelona2	7 enlaces bàsicos RDSI	6	50	25	5	1 MG	0
Madrid1	2 PRI telefonía fija	15	100	90	10	2 MG	1
Madrid2	4 enlaces básicos RDSI	8	60	15	5	1 MG	0

A continuación desglosamos en diferentes tablas lo que debemos pedir a Alcatel:

Equipo Procesador de llamadas	Modelo - Software	Edifici
Call Sever	Servidor IBM amb Alcatel OmniPCX Enterprise R7.1-f5.401-36-b-es-c80s1	Barcelona1
Call Sever	Servidor IBM amb Alcatel OmniPCX Enterprise R7.1-f5.401-36-b-es-c80s1	Madrid1

Rack del sistema - Mediagateway IP	Targetes	Edifici
OmniPCX Enterprise Media Gateway IP 150* 2Rack3 MADA3 220V + Bateria 12V/7AH Caja de baterias externas 36V	Placa UAI8 (8 usuarios digitals) Placa SLI16-1 (16 usuarios analógicos) 2 Placas PRA-T2 (d'un accéso primario E1 para cada T2) 4 Paquetes Adaptadores RJ45/COAX para T2 4 unidades Paquete MGA24-2 (GA/MADA3) (24 canales de compresión VOIP)	Barcelona1
Unidad Remota IP 12A* MADA3 220V 1Rack1 + Bateria 12V/7AH Caja de baterias externas 12V	2 Placa MIX4/4/8 (4 accesos básicos RDSI /4 terminales digitales/8 terminales analógicos)	Barcelona2
OmniPCX Enterprise Media Gateway IP 150* 2Rack3 MADA3 220V + Bateria 12V/7AH Caja de baterias externas 36V	Placa UAI8 (8 usuarios digitals) Placa SLI16-1 (16 usuarios analógicos) 2 Placas PRA-T2 (d'un accéso primario E1 para cada T2) 4 Paquetes Adaptadores RJ45/COAX para T2 4 unidades Paquete MGA24-2 (GA/MADA3) (24 canales de compresión VOIP)	Madrid1
Unidad Remota IP 12A* MADA3 220V 1Rack1 + Bateria 12V/7AH Caja de baterias externas 12V	1 Placa MIX4/4/8 (4 accesos básicos RDSI /4 terminales digitales/8 terminales analógicos)	Madrid 2

Modelo terminal	Características	Cantidad
IP Touch 4018	ALCATEL 4018 IP Touch gris	310
IP Touch 4028	ALCATEL 4028 IP Touch gris	210
IP Touch 4068	ALCATEL 4068 IP Touch gris	40

Los Call Servers vienen aprovisionados de un software que proporciona todas las funcionalidades del sistema OXE aún así muchos servicios están protegidos con licencias.

El sistema de licencias de Alcatel son paquetes de marketing que tienen una correspondiente llave (lock) en el call server para que así cuando se adquiere la licencia el usuario puede disfrutar de una funcionalidad añadida.

Por lo tanto deberemos aprovisionar al cliente de licencias para autorizar el uso de servicios concretos. Un ejemplo es que si el cliente quiere disfrutar del uso de 5 teléfonos ip debe adquirir 5 licencias para ello.

5.4.2 – Descripción del hardware contemplado

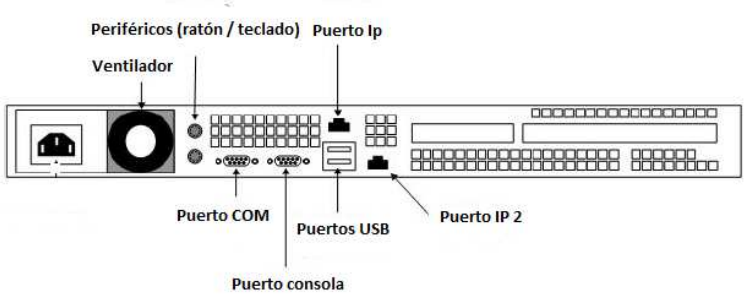
OmniPCX Enterprise Call Server:

Call Server es un programa software que se ejecuta en el sistema operativo Linux este programa se corresponde con la aplicación que controla cada objeto del sistema.

Como servicios adicionales proporciona una descarga por protocolo TFTP de los archivos de software a los teléfonos IP Touch y las Media Gateways IP, lo descarga a una memoria flash con formato de archivo binario

Funciona también como servidor DHCP que asigna de forma automática los parámetros IP y proporciona una asignación de Vlan Automática (AVA) basada en una solicitud de DHCP doble para la recepción de dirección IP y para la recepción de Vlan de Voz.

Este sistema esta montado en un Appliance Server que no deja de ser un servidor del fabricante IBM configurado y cargado por Alcatel para que funcione como Call Server. Es compatible tanto con el hardware OXO como con el hardware 4400 (sistema anterior al Enterprise).



Las capacidades básicas del Call Server son:

- Puede tener hasta 5000 teléfonos
- El número máximo de teléfonos IP permitidos es de 4000
- Un Call Server de un sistema OXE en solitario puede manejar hasta 90 Media Gateway.
- En una disposición en red se pueden tener hasta 50.000 usuarios.
- Existe total compatibilidad, para formar una red, entre nodos cuya versión sea 5.1, 5.0 (Ux o Lx) y 4.1
- Un Media Gateway puede tener hasta 12 accesos RDSI.
- No se tienen tarjetas de conexión a ATM.
- Sólo hay conexión de alvéolos remotos por IP.

Hardware común (OXO)

En este apartado solamente hacemos referencia los mediagateways y tarjetería que van a aprovisionarse con este proyecto.

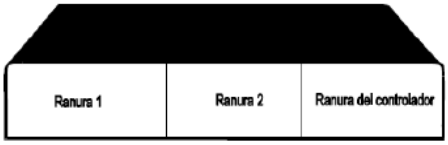
1.- Los Mediagateways harware común:

Como hemos indicado anteriormente permite la conexión de la telefonía tradicional con el mundo TCP/IP. Su principal función es garantizar la administración de las

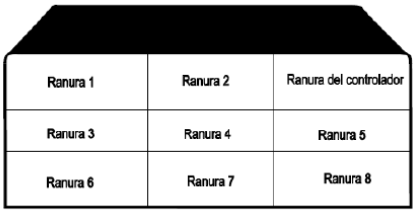
Interfaces "clásicas" como por ejemplo la analógica, digital, RDSI, etc, las funciones de Gateway VoIP (si es necesario), las conferencias telefónicas, las guías de voz, música en espera etc.
Esta formado por un chasis y una serie de tarjetas.

Respecto a los chasis tenemos dos medidas:

a) Tipo S (small) : Dispone de 3 posiciones para tarjetas.



b) Tipo L (Large) : Dispone de 9 posiciones para tarjetas.



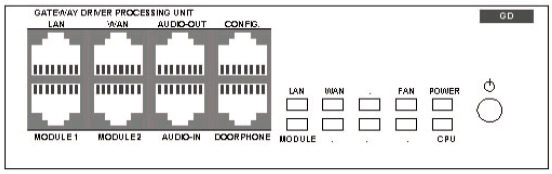
2.- Tarjeta GD:

La tarjeta GD, aparte de controlar la señalización de las llamadas que comiencen o terminen en terminales conectados al Media Gateway, será la encargada de convertir en Telefonía IP, las llamadas de terminales analógicos o digitales y al revés. Para ellos dispone de DSP's.

El slot de control de cada rack o mediagateway (posición 0) contiene una placa GD. Esta placa nos proporciona:

- La matriz de conmutación
- Posibilidad de conferencia a 3
- Generación y detección de tonos
- Transmisión de la señalización hacia la CPU (CS).
- Emisión y almacenamiento de guías de guías vocales.
- Pasarela señalización tipo H323
- Señalización para los teléfonos IP (aunque por defecto señaliza la CS).
- Compresores (DSP) para comunicaciones VoIP.

Imagen frontal de la placa:

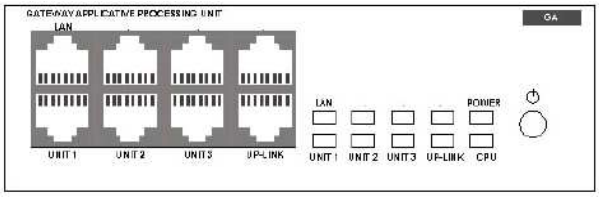


3.- Tarjeta GA:

Esta tarjeta permite augmentar los recursos que ya proporciona la GD.
Concretamente aumenta los siguientes recursos:

- Compresores VoIP (DSP).
- Almacenamiento de guías vocales
- Conferencias a 3

Imagen frontal de la placa:



4.- Tarjeta MIX 4/4/8:

Son tarjetas que combinan interfaces para terminales analógicos (Z), digitales (UA) y enlaces tipo T0 RDSI básico (BRA).

El tipo 4/4/8 permite la conexión de hasta 4 terminales digitales, 4 enlaces RDSI (T0) y 8 terminales analógicos.

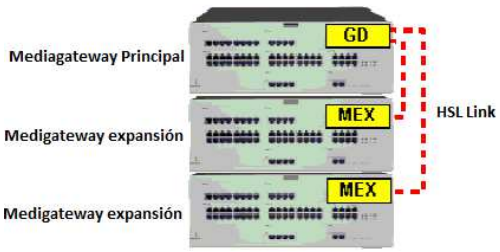
Solo debemos tener en cuenta que el los chasis tipo L no pueden ir en la ranura 5 y 8.

5.- Tarjeta MEX:

Tal como la GD se coloca en el slot de control de rack (slot 0) y permite expandir el rack principal.

Los Mediagateways puedes unirse entre si formando un solo mediagateway hasta un máximo de 3 racks (un rack será el principal y los otros dos serán una expansión del mismo):

La interconexión entre estos Racks se realiza a través de uniones HSL (High Speed Link). Este link conecta la GD principal con tarjetas MEX.



En las oficinas principales, Barcelona1 y Madrid1, disponemos de un Mediagateway formado por 2 racks.

Imagen frontal de la placa:

6.- Tarjeta APA 4:

Permite el enlace de 2,4 o 8 líneas analógicas. En nuestro caso 4 líneas.

7.- Tarjeta PRA:

Permite el enlace de un primario tipo T2/E1 de 2Mbits.
En nuestro caso con conexión de fibra.

5.4.3 – Configuración

La configuración de la red de Voz lógicamente se hará en los switchs centrales y routers.
En cuanto a la parte de los equipos VOIP solamente debemos configurar el Call Server, la GD del Mediagateway y finalmente configurar la vlan de red en el terminal IP.

Configuración de Red Call Server

1.- Configuración de red:

Vlan	Descripción	Red	Máscara	Usuarios	IP interfaz Vlan
21	Red de voz Barcelona 1	192.168.21.0	255.255.255.0	254	192.168.21.1
22	Red de voz Barcelona 2	192.168.22.0	255.255.255.128	128	192.168.22.1
23	Red Servidores de voz Barcelona	192.168.23.0	255.255.255.240	14	192.168..23.1
21	Red de voz Madrid 1	192.168.24.0	255.255.255.0	254	192.168.24.1
22	Red de voz Madrid 2	192.168.25.0	255.255.255.0	128	192.168.25.1
23	Red Servidores de voz Madrid	192.168.26.0	255.255.255.240	14	192.168.26.1

2.- Dominio IP:

Para realizar la configuración de dominio ip de la oficina iremos al menú IP dentro el programa MGR y dentro en la opción dominio IP crearemos un dominio asignándole un número. Entonces primero creamos el dominio dándole un número de dominio, un nombre y la dirección ip de la tarjeta GD de la oficina.

A continuación, bajamos por el menú y le asignamos un rango ip al dominio indicando la ip del rango más baja, la más alta y la máscara.

Debemos tener en cuenta que debemos usar dos direcciones ip del rango de voz para las interfaces vlan del router y el switch central.

3.- Servidor DHCP:

En Call Server hace a la vez de servidor DHCP integrado y asigna de forma automática los parámetros IP necesarios cuando se instala el teléfono IP, sin que tenga que intervenir el administrador del sistema.
El teléfono IP recibe la submáscara de red y proporciona igualmente la dirección TFTP, que permite al teléfono IP Touch recibir el archivo de software descargado.

La configuración en el Call Server la realizaremos en tres sencillos pasos:

1.- Dentro del programa MGR iremos al menú de configuración de DHCP indicaremos al Call Server que debe funcionar como servidor DHCP

2.- En el mismo menú crearemos el rango de subred de voz. Lo único que debemos indicar es la subred, la máscara de subred, la dirección de broadcast, el Gateway por defecto y el servidor TFTP (el propio Call Server).

3.- Una vez creada la subred debemos determinar un rango de direcciones ip asignables dentro de esta subred. En el menú indicando la subred creada indicaremos la primera dirección y la última asignable a los terminales ip de la subred.

4.- Validaremos todas estas configuraciones.

4.- Creamos una entidad lógica

Son subdivisiones lógicas de la centralita que nos permiten configurar de forma personalizada cada subdivisión. Por ejemplo, podemos diferenciar en el enrutamiento de llamadas (que una oficina saque las llamadas por un primario y otra por uno diferente), también podemos definir un comportamiento o otro dependiendo de un horario, configurar un número único de salida, etc.

5.- Configuración abonado:

En toda centralita nos encontraremos definidas por un lado la numeración externa (número de 9 dígitos que nos proporciona el proveedor) y por otro lado la numeración interna formada por las extensiones propias del cliente a las que solamente se puede llamar dentro de nuestra red y que están asociadas directamente al terminal.

En un primer instante debemos configurar la extensión o número interno en el Call Server para que luego la podamos asignar en el terminal.

Para la configuración de la extensión tendremos en cuenta:

Definiremos un número de directorio que esté vacante
Elegimos una dirección de equipo de interfaz de tarjeta (255 en ip)
Definimos el modelo de terminal
Asignamos un nombre de directorio al terminal

Finalmente, se nos presenta la opción de poder relacionar esa extensión con un número externo para que ésta pueda ser llamada des de fuera de nuestra red de VOIP. Para ellos solo debemos relacionar por configuración el número externo con el interno en el Call Server.

6.- Tabla de encaminamiento:

Crearemos una tabla de encaminamiento o tabla ARS para, como su nombre indica, encaminar las llamadas hacia un grupo de enlace u otro.

7.- Configuración grupo de enlace:

Cada grupo de enlace esta formado por una o más líneas T0 (RDSI básicas) o T2 (primarios de voz) de manera que si lo asociamos con una tabla de encaminamiento de llamadas podemos encaminar las llamadas hacia una salida a la RTC o otra.

Las líneas a agrupar las decidimos nosotros siguiendo una lógica, por ejemplo, si tenemos primarios de fijos y primarios de móviles, agrupamos en un grupo de enlace los primarios del mismo tipo de modo que cuando encaminemos las llamadas hacia una salida podremos diferenciar entre una salida de móviles o fijos y a la vez proporcionar más canales de salida (agrupando más de una línea). A mi modo de ver, nos sirve para dar un nombre a esas líneas para usarlas en la configuración.

Configuraremos un grupo de enlace para los primarios de salida de Madrid, otro para los de Barcelona y otros dos diferentes para las agrupaciones de líneas RDSI de rescate.

Configuración de un mediagateway

Primero debemos configurar nuestra tarjeta GD. Esta configuración la realizará por consola en instalador. Configurará la red de la misma. Cuando ya este configurada podemos realizar un Telnet a la misma para revisar su configuración si disponemos de permisos y usuario.
La GD como hemos comentado con anterioridad es la CPU del sistema y es la que se comunicará con el Call Server.
Des de el menú de configuración de el call Server podemos sacar la configuración de la misma.

Podemos consultar el estado de las diferentes tarjetas de un Mediagateway des de su Call Server por consola de comandos en el mismo.

Finalmente debemos tener en cuenta que al iniciar un sistema OXE, de forma automática se crean varios alvéolos virtuales no son físicos. El alveolo 0, contiene la CPU del sistema , el alveolo 18, se crea en el sistema solo si se declara una mensajería e-VA y el alveolo 19, se encarga de proporcionar funciones para manejar los enlaces de señalización IP

Arteria Híbrida

Para comunicar los dos Call Servers, el de Madrid y el de Barcelona, usaremos lo que se llama Arteria Híbrida.

Así pues, las arterías híbridas (HA) se utilizan para realizar enlaces entre dos call servers y el canal de señalización se soporta sobre una red ethernet donde se utiliza el protocolo IP.

Concretamente son las conexiones ip entre nodos call server donde la aplicación híbrida es la encargada de transferir los datagramas entre los dos nodos, donde cada uno de ellos tiene la dirección IP del nodo remoto declarada en el acceso del enlace lógico híbrido.

Introducir la vlan en nuestro terminal IP

Por un lado, en la red LAN hemos creado la red una vlan con la red ip de voz donde pertenecerán nuestras extensiones IP. Debemos introducir ésta vlan en nuestro terminal ip

para que a nivel de red éste pueda comunicarse con el Call Server y pueda descargarse su ip por dhcp y su archivo software para poder funcionar.

Son pasos sencillos que debemos conocer en el momento de conectar nuestro terminal:

- Paso 1/5 →Empezando
- Paso 2/5→Debemos introducir los parámetros IP. En nuestro caso la vlan. Como?:
  - Apretamos la tecla de "i" (info) y a continuación "#".
  - Entramos en un menú y seleccionamos la opción de parámetros ip
  - Usamos la opción de vlan e indicamos la vlan a usar.
- Paso 3/5→ El Terminal intenta conseguir el fichero lanpbx.
- Paso 4/5 → Intercambio de binario.
- Paso 5/5 → Señalización del sistema.

5.4.4 – Líneas públicas

Se contempla la instalación de dos primarios fijos en Barcelona 1 y otros dos en Madrid 1. En cada oficina central los dos primarios están en grupo ISPBX y recogen todo el tráfico fijo del del cliente. Adicionalmente se cuenta con un primario de móviles en cada oficina central.

En las sedes restantes se han instalado líneas RDSI que permitan el rescate de la sede mediante llamada RDSI. Para ello se ha instalado una RDSI para permitir la señalización y diversas RDSIs para realizar el rescate.

Debemos realizar la petición de estas líneas a nuestro ISP.

5.4.5 – Sistema rescate

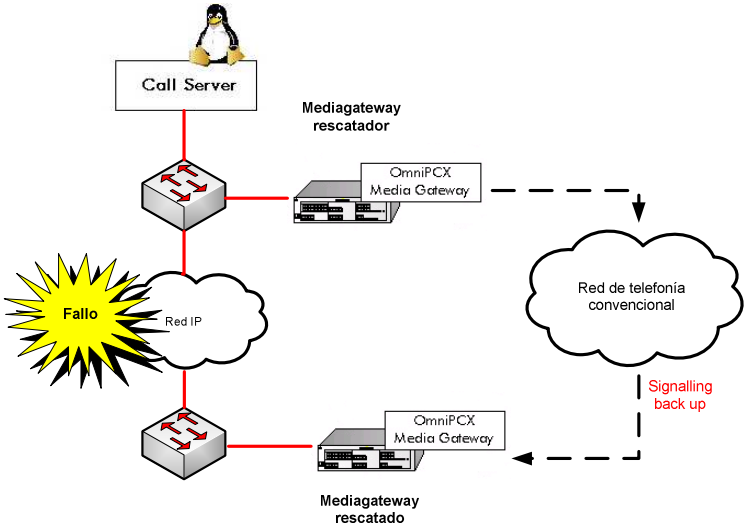
Para proporcionar un sistema de contingencia a las oficinas Barcelona 2 y Madrid 2 en caso de que fallará la comunicación IP con Madrid 1 y Barcelona 1, disponemos de un mecanismo de backup por RDSI que restaura el link de señalización entre los Call Servers y la sede aislada de la misma provincia.

Este mecanismo requiere un MG con unos enlaces RDSI de emergencia con la red pública. Este proceso se activa cuando el CS pierde la comunicación IP con el mediagateway de la oficina a rescatar durante al menos 2 minutos. En ese momento se establece una llamada entre la MG rescatador a un número RDSI ubicado en el primer puerto del MG de la oficina a rescatar.

Esto implica que los mediagateways deben estar en diferentes dominios ip y el servidor DHCP (de CS o externo) debe asignar rangos IP diferentes para cada sede rescatable. Por otro lado una MG rescatadora sólo puede rescatar un dominio IP simultáneamente.

De este modo, el objetivo de la funcionalidad signalling back up es rescatar el enlace de señalización entre el CS y el MG en caso de caída de la red IP. La implementación se basa en el IPSLB (IP Signalling Link Backup). El mecanismo establece una conexión temporal para reemplazar el Ip Link que se basa en un canal de comunicación a través de la red pública. Como dato añadido el IP link de rescate ocupa un sólo canal B de 64Kpbs con lo que usaremos solo una línea RDSI para realizar esta señalización.

Para realizar esta llamada a través de la red pública se utiliza el módem interno de la GD pero solamente se utiliza para la señalización de llamadas con el Call Server, nunca para transportar tráfico de voz.



Por configuración en el Call Server definiremos el dominio 1 para la oficina rescatadora y el dominio 2 para la oficina rescatable. También definiremos una ip estática en ambas GD's de ambos mediagateways, rescatador y rescatable. A continuación definiremos un mediagateway como rescatador y a continuación definiremos el grupo de enlace y el número de teléfono público que debe marcar el dsp de la GD rescatadora y donde esta alojada la línea RDSI de rescate en el mediagateway. En resumen, si tenemos una línea RDSI para el rescate con un número X definiremos #grupodeenlace&números y a continuación el cristal+placa+puerto donde va conectada esa línea.

6 CONCLUSIONES

La idea era diseñar una red de comunicaciones para un cliente en expansión. Cogimos a un cliente insatisfecho con su sistema de comunicaciones y mejoramos su red corporativa proporcionándole, más robustez en su sistema de comunicación, más escalabilidad de su red, mejores parámetros de disponibilidad de sus equipos y mejores tiempos de respuesta.

Hemos exprimido al máximo toda nuestra experiencia y conocimiento para proporcionar al cliente la mejor solución tecnológica que pueda aportarle beneficios que puedan quedar reflejados en su productividad día a día.

En este proyecto se ha implantado una solución unificada de 3 servicios, WAN, LAN y VOZ IP. A nivel de WAN hemos mejorado sus conexiones aportando más velocidad, redundancia, más fiabilidad de conexión y mejores tiempos de convergencia.

A nivel LAN hemos creado una solución que nos proporciona mucha más velocidad de conexión, una red más centralizada y fácil de administrar, un ahorro de coste ya que nos ahorramos equipos alquilados a nuestro ISP entre oficinas de la misma provincia y con más posibilidades y facilidades de crecimiento que la anterior.

Y finalmente un sistema de voz mucho más centralizado y sencillo de administrar, totalmente gestionable y llamadas sin coste entre teléfonos de la empresa, tanto móvil como fijo, que, como se puede leer en varios artículos de prensa puede llegar a resultar un 40% de ahorro en

el gasto de la empresa. Por otro lado permitirá a la empresa disfrutar de las prestaciones avanzadas que este nuevo sistema ofrece(servicio de mensajería unificada, videoconferencias, facilidades de los terminales ip, informes a medida, etc) y a la vez sacar el máximo provecho a su red.

También en este sentido hemos proporcionado un sistema escalable ya que Alcatel es una de las empresas punteras en sistemas de comunicaciones ip y ofrece multitud de posibilidades en su sistema, que a la larga, el cliente puede ir adquiriendo y añadiendo a su sistema actual.

Por otro lado, ha sido muy importante realizar un buen seguimiento y control de nuestro proyecto. Gracias al estudio de las necesidades del cliente y la planificación inicial de tareas realizada hemos podido cumplir con éxito el calendario establecido, dando una imagen profesional y aportando satisfacción a nuestro cliente.

A nivel personal este proyecto me ha servido para profundizar en gran medida sobre mis conocimientos de VOZ Ip y switching. También he aprendido a relacionar todos los ámbitos de la red WAN, LAN, VOZ, etc. para que todo funcione como un conjunto y, realmente, como empresa, podamos sacar un rendimiento óptimo de ésta.

He aprendido también a interpretar la necesidad de un cliente y diseñar diferentes soluciones a medida hasta encontrar la que en mi parecer fue la más adecuada a sus necesidades y a prepararla para una futura expansión de la empresa. Mi red seguirá siendo útil aunque la empresa crezca, solamente deberemos añadir equipamiento pero la interconexión de equipos seguirá siendo la misma, con lo que en un futuro seguirá siendo rentable.

Finalmente he podido dar uso a todos los conocimientos de las asignaturas de redes que he ido realizando a lo largo de la carrera.

7 BIBLIOGRAFIA

1.- Página oficial de Cisco: http://www.cisco.com

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd8017a5e7.html

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_data_sheet09186a0080159856.html

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd800f6e27.html

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.html

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/data_sheet_c78-530976.html

http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/01over.html

http://www.cpssales.com/documents/cisco/Cisco-Catalyst-6509-V-E-Chassis-Datasheet.pdf

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/0apwsply.html

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd80673385.html

http://www.cisco.com/en/US/products/hw/switches/ps708/products_relevant_interfaces_and_modules.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/port_sec.html

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807811ad.shtml

2.- Apuntes CCNA v3.2

3.- Apuntes CCNP (routing y switching)

4.- URL foro Alcatel: http://www.alcatelunleashed.com/

5.- Página oficial de Eaton : http://pulsar.eaton.com

http://powerquality.eaton.com/EVLL850R-1U.aspx?CX=3&GUID=10917A2B-DE0D-408B-8C87-AC5D36AE475F

http://pulsar.eaton.com/Spain/Products-Services/default.asp

6.- Página ADSLzone

7.- Apuntes CCVOICE

8.- Foro: http://www.sadikhov.com

9.- Apuntes curso Voz IP empresa

10.- Estudio de una maqueta en funcionamiento con Alcatel OXE.

11.- Pruebas con el Packet tracer.

12.- Apuntes asignatura Redes de Computadores de la UOC.

13.- Información Conversor de Medios

http://www.telnet-ri.es/fileadmin/user_upload/hojas_producto/BANDA_ANCHA/CM-100-IB_compacto_ES_V1R1.pdf

14.- Información modelo OSI:

http://blog.s21sec.com/2009/06/ataques-sobre-el-nivel-2-del-modelo-osi_25.html

8 DESGLOSE ECONÓMICO

Alta Servicio WAN			
Servicio	**Unidades**	**Coste/U**	**Coste total**
Acceso fibra 100Mb	4	605,99 €	2.423,96 €
Latiguillo FO	4	29,94 €	119,76 €
GE SFP LC connector SX Transceiver	4	220,53 €	882,12 €
Latiguillo RJ45-RJ45 2m	4	2,69 €	10,76 €
WS-C3560V2 24TS	4	1.673,30 €	6.693,20 €
Instalación y puesta en servicio		1.716,17 €	1.016,17 €
Alta Servicio LAN			
Servicio	**Unidades**	**Coste/U**	**Coste total**
GE SFP LC connector SX Transceiver	5	220,53 €	1.102,65 €
GE SFP,LC connector LX/LH transceiver	9	571,37 €	5.142,33 €
Chassis WS-C6509-E	1	3.598,00 €	3.598,00 €
WS-SUP720-3BXL	2	20.339,00 €	40.678,00 €
WS-X6748-GE-TX	1	10.896,00 €	10.896,00 €
WS-X6724-SFP	1	10.170,00 €	10.170,00 €
Catalyst 3750 48 10/100/1000T PoE + 4 SFP + IPB Image	14	8.151,35 €	114.118,90 €
Latiguillos monomodo	100	17,67 €	1.767,00 €
SAI Evolution 3.000	1	1.135,04 €	1.135,04 €
SAI Evolution 850	5	262,44 €	1.312,20 €
Instalación y puesta en servicio		3.230,35 €	3.230,35 €
Alta Servicio VOZ IP			
Servicio	**Unidades**	**Coste/U**	**Coste total**
Primario de voz	4	362,36 €	1.449,44 €
Líneas RDSI/ISDN	11	26,24 €	288,64 €
Terminal Ip básico IP Touch 4018	310	181,06 €	56.128,60 €
Terminal IP de gama media IP Touch 4028	210	296,61 €	62.288,10 €
Terminal Ip de gama avanzada IP Touch 4068	40	578,68 €	23.147,20 €
Licencia Analógico	20	49,99 €	999,80 €
Licencia SW servidor G729A	2	0,08 €	0,16 €
Licencia SW cliente G729A	2	0,08 €	0,16 €
Licencia Sw e-CS engine actualización de 81 a 150 usuarios	2	565,01 €	1.130,02 €
Licencia Sw e-CS engine actualización de 151 a 350 usuarios	2	565,01 €	1.130,02 €
Licencia Call by Name	2	105,93 €	211,86 €
Licencia Sw para operadora automática más de 6 guías vocales	2	625,02 €	1.250,04 €
Licencia Sw de Servicio de Selección Automática de Ruta y desbordamiento	2	154,71 €	309,42 €
Licencia Sw de Tarificación para el motor Sw OXE con 350 usuarios	2	64,70 €	129,40 €
Licencia Sw de gestión de Configuración para el motor Sw OXE con 350 usuarios	2	225,03 €	450,06 €
Licencia Registro de las guías vocales	2	180,02 €	360,04 €
Omnipcx Enterprise Versión R9.1Ngp	2	0,03 €	0,06 €
Omnipcx Enterprise Appliance Server -Ibm	2	3.207,20 €	6.414,40 €
Placa GD	4	2.396,83 €	9.587,32 €
Placa GA	8	334,17 €	2.673,36 €
Placa PRA T2	4	3.111,26 €	12.445,04 €
Placa UAI8	2	308,82 €	617,64 €
Tapas para slots libres (x1)	10	21,92 €	219,20 €
Placas de extensiones analógicas SLI16-1	2	366,04 €	732,08 €
Placa mixta RDSI / 4 T0 + 4 UAI + 8 SLI	2	239,69 €	479,38 €
Cable de alimentación genérico	6	13,77 €	82,62 €
Batería 7AH/12v	4	55,34 €	221,36 €
Caja de batería externa 12V Para OXO Rack 1&2	2	55,37 €	110,74 €
Latiguillo UTP 1P RJ45-RJ45 cat3 2m	200	40,30 €	8.060,00 €
Latiguillo RJ45-RJ45 2m	600	2,69 €	1.614,00 €
Instalación, puesta en servicio y formación		2.213,34 €	2.213,34 €
Total			**399.039,94 €**

9 ANEXO

Este apartado nos sirve para explicar la configuración que van a llevar los diferentes equipos del proyecto.

9.1 Plantillas de configuración Red WAN

Madrid 1 y Barcelona 1

Son los dos routers que comunicaran a nivel de WAN las oficinas de Barcelona con la de Madrid. Sobre este punto debemos tener en cuenta que será el ISP quien nos indique que ip's debemos configurar para la red WAN y que debemos configurar en la interfaz de conexión con el enlace WAN.

Así pues, vamos la desglosar la configuración de ambos equipos por partes:

Borramos al configuración del equipo para cargar nuestra configuración:

```
erase startup-config
delete flash:vlan.dat
```

Parámetros generales:

```
hostname < Barcelona1 o Madrid1 >

service nagle
service tcp-keepalives-in
ip subnet-zero
service timestamps debug datetime localtime msec show-timezone
service timestamps log datetime localtime msec show-timezone
no ip http server
```

Creamos un banner que identifica nuestro cliente

```
banner #
        ************************************************************
        **    Esta usted accediendo a una maquina privada          **
        **    si no esta autorizado cierre inmediatamente su conexión **
        **                                                         **
        ************************************************************
        #
```

Configuramos la fecha:

clock set <hh(0-23):mm(0-59):ss(0-59)> <día(1-31)> <mes(January..December)> <año>

Activamos el routing:

ip routing

sdm prefer routing

Acceso por telnet a nuestro EDC:

service password-encryption
enable secret <Password de enable>

line con 0
password <Password de consola>
exec-timeout <Minutos>

vty 0 15
password <Password de telnet>
exec-timeout <Minutos>

Tamaño de nuestro LOG:

logging buffered <Tamaño de buffer> informational

Servidor ntp:

ntp server <Ip servidor NTP cliente>

Puerto cliente:

interface <Puerto de conexión contra el switch>
description Puerto LAN cliente
switchport access vlan 2
switchport mode acces
speed auto
duplex full
priority-queue out →*el tráfico que venga marcado preferente se va a priorizar.*
no shutdown
exit

interface <Puerto de conexión contra el switch para gestión>
description Puerto LAN cliente
switchport access vlan 20
switchport mode acces
speed auto
duplex auto
no shutdown
exit

Interfaz loopback del equipo:

interface Loopback60
description Gestión del equipo
ip address <ip para gestión del equipo> 255.255.255.255

ip tftp source-interface Loopback 60

ip ftp source-interface Loopback 60

logging source-interface Loopback 60

snmp-server trap-source Loopback 60

ntp source Loopback 60

Creación de vlan de servicio:

vlan 2
name Red LAN cliente
exit

vlan 20
name Red gestión de switch
exit

interface Vlan2
ip address 192.168.1.2 255.255.255.248
no ip redirects
standby 1 ip 192.168.1.1 → configuramos el HSRP con el equipo backup
standby 1 priority 200 → mas prioridad para que el equipo principal tenga la ip virtual por defecto
standby 1 preempt delay minimum 30
standby 1 track < Puerto WAN equipo>

interface Vlan20
description Gestion switchs
ip address 192.168.14.2 255.255.255.0
no ip redirects

Configuración de routing

router bgp <AS Propio>

no synchronization
redistribute connected
redistribute static
set metric 100
bgp router_id <IP Gestión equipo>
neighbor EQISP peer-group
neighbor EQISP remote-as <AS Remoto ISP>
neighbor EQISP timers 10 30
neighbor <Vecino BGP> peer-group EQISP
no auto-summary
no synchronization
network <Red de cliente a publicar> <Máscara>
network <IP de gestión equipo> mask 255.255.255.255
exit

Rutas estáticas:

Rutas hacia las ip's de gestión del los switch

ip route < ip gestión switch> 255.255.255.255 Vlan20

ip route 0.0.0.0 0.0.0.0 < ip Firewall cliente>

Calidad de Servicio:

Crearemos unas Acl's para asignar un tipo de preferencia a cada tipo de red. Las redes de voz irán marcadas como tráfico multimedia y los datos como tráfico plata.

Activamos la QoS:

mls qos

Tráfico Plata:

access-list 11 permit ip any any → *tráfico plata*

class-map match-all Clase_Plata
match access-group 11

policy-map QoS_In
class Clase_Plata
set ip dscp cs1

Tráfico Multimedia:

access-list 10 permit ip < red de voz> 0.0.0.255 any
access-list 10 permit ip < red de servidores de voz> 0.0.0.15 any

class-map match-all Clase
match access-group 10

mls qos aggregate-policer multimedia 100000000 8000 exceed-action drop

policy-map QoS_In
class Clase_Voz
set ip dscp cs5
police aggregate multimedia

SNMP:

snmp-server community <community creada en el servidor de cliente>
snmp-server trap-source Loopback60
snmp-server location < Barcelona o Madrid >
snmp-server contact < contacto o nombre empresa cliente >
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps flash insertion renoval
snmp-server enable traps bgp

snmp-server enable traps hsrp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete

De momento le dejamos estos traps habilitados, el cliente debe indicarnos si necesita alguno más, a parte de su community.

Madrid 2 y Barcelona 2

La configuración debe ser la misma solo cambian ciertos parámetros de routing, ya que vamos a penalizar la publicación de rutas por el equipo backup, y la configuración de HSRP:

BGP

Dentro de la configuración de bgp cambiamos la metrica de 100 a 200

router bgp <AS Propio>
set metric 200

Rutas estáticas

En las rutas estáticas también penalizamos la métrica

ip route < ip gestión switch> 255.255.255.255 Vlan20 **252**

ip route 0.0.0.0 0.0.0.0 < ip Firewall cliente> **252**

Configuramos la interfaz vlan sobre la LAN del equipo backup del siguiente modo con penalización en HSRP:

interface Vlan2
ip address 192.168.1.3 255.255.255.248
no ip redirects
standby 1 ip 192.168.1.1
standby 1 priority 100
standby 1 preempt delay minimum 30
standby 1 track < Puerto WAN equipo>

9.2 Plantillas de configuración Red LAN

Equipo central Barcelona y Madrid

Configuración genérica

hostname < nombre switch>

no ip http Server

cdp run → *activamos el protocolo cdp para ver a nuestros "vecinos"*

password encryption aes
enable secret < password de enable>

line con 0
exec-timeout 0 0
password < password>
line vty 0 4
password < password>
login

Configuración Spanning-tree

spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1-1000 priority 4096

Rutas estáticas:

ip route 0.0.0.0 0.0.0.0 < ip host firewall >

ip route < ip de la red LAN * > <máscara> 192.168.1.1
..etc

* Si estamos en Madrid pondremos las ip's de la red LAN de Barcelona y si estamos en Barcelona, la lista de ip's LAN de Madrid.

Configuración VTP

vtp domain TFC
vtp mode server
vtp password TFC1

Creación de Vlan

vlan internal allocation policy ascending
vlan access-log ratelimit 2000

vlan <número de vlan>
name < descripción que le damos>

interface Vlan<número de vlan>
description - < descripción que le damos>
ip address < red ip de esa vlan> < máscara>
* ip access-group < número de acl si se la aplicamos> out
** ip helper-address < ip host Call Server>

*Solo lo introducimos si queremos aplicar una acl a esa red.

**Cuando creemos la vlan de voz debemos indicarle cuál es su servidor dhcp , que en el caso de la red de voz es el Call Server asignado a esa delegación.

Creación vlan de gestión

ip tftp source-interface Vlan20
ip ftp source-interface Vlan20

interface Vlan20
description Gestion del Switch < nombre asignado al switch>
ip address < ip de gestión de este equipo en concreto> 255.255.255.0
no shutdown

Creación vlan de Servidores de Telefonía

interface Vlan23
description Servidor de Telefonía < Ubicación, Madrid o Barcelona>
ip address < ip de gestión de este equipo en concreto> 255.255.255.240
ip access-group 23 out
no shutdown

Access-list

Definimos una acl por cada red de datos (excepto jefatura):

access-list <nº de acl> remark vlan < número de vlan donde la aplicamos> - <Descripción>
access-list <nº de acl> deny 192.168.14.0 0.0.0.255 →*Acceso a la red de gestión*
access-list <nº de acl> deny 192.168.11.192 0.0.0.31 → *Acceso a jefatura*
access-list <nº de acl> deny 192.168.13.192 0.0.0.31 → *Acceso a jefatura*
access-list <nº de acl> deny <red ip de voz> <wilcard de esa red> → *Acceso a la red de voz*
access-list <nº de acl> deny <red ip servidor Tel.> 0.0.0.15 → *Acceso a la red de servidores de Telefonía*
access-list 29 permit any

Definimos una acl para los servidores de telefonía:

access-list 23 remark Vlan 23 - Servidores Telefonía IP
access-list 23 permit 192.168.21.0 0.0.0.255
access-list 23 permit 192.168.22.0 0.0.0.127
access-list 23 permit 192.168.24.0 0.0.0.255
access-list 23 permit 192.168.25.0 0.0.0.127
access-list 23 permit 192.168.23.0 0.0.0.15
access-list 23 permit 192.168.26.0 0.0.0.15

Puerto de conexión contra el router

description ----- Conexión a contra el router -----
switchport
switchport trunk allowed vlan 1-1000
switchport mode trunk
no ip address
logging event link-status

Puertos de conexión Servidor de Telefonía

description Call Server < Barcelona o Madrid>
switchport
switchport access vlan 23
switchport mode access
no ip address
logging event link-status
spanning-tree portfast
spanning-tree bpduguard enable

SNMP

snmp-server community <community creada en el servidor de cliente>
snmp-server trap-source Loopback60
snmp-server location < Barcelona o Madrid >
snmp-server contact < contacto o nombre empresa cliente >
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps flash insertion renoval
snmp-server enable traps bgp
snmp-server enable traps hsrp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps vtp
snmp-server enable traps bridge newroot topologychange

Switch de acceso Barcelona y Madrid

Configuración genérica

hostname <nombre switch>

no ip http Server

cdp run → *activamos el protocolo cdp para ver a nuestros "vecinos"*

service password-encryption
enable secret < password de enable>

line con 0
exec-timeout 0 0
password < password>
line vty 0 4

password < password>
login

ip tftp source-interface Vlan20

logging buffered 100000

Configuración Spanning-tree

spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id

VTP

vtp domain TFC
vtp mode client
vtp password TFC1

Creación vlan de gestión

interface Vlan20
description Gestion del Switch < nombre asignado al switch>
ip address < ip de gestión de este equipo en concreto> 255.255.255.0
no shutdown

Puertos de acceso a terminales

description ----- Puerto usuario y teléfono ----
switchport access vlan <nº vlan datos>
switchport mode access
switchport nonegotiate
switchport voice vlan <nº vlan voz>
switchport port-security maximum 2 → *permitimos un PC +Terminal IP*
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast trunk
spanning-tree bpduguard enable →*liberamos al protocolo de spanning-tree de más cálculo*
no shutdown

Recuperación port-security

Para que los puertos vuelvan a levantar en caso de que ya no se este produciendo una violación de seguridad del puerto, introducimos el siguiente comando:

errdisable recovery cause security-violation

Puertos entre switch

description --- Conexión a <equipo con el que creamos el enlace> ----
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-1000
switchport mode trunk
no shutdown

Puertos de conexión de un Mediagateway

description Conexión Mediagateway
switchport access vlan < nº vlan de voz>
switchport mode access
no ip address
spanning-tree portfast
spanning-tree bpduguard enable

SNMP

snmp-server community <community creada en el servidor de cliente>
snmp-server trap-source Loopback60
snmp-server location < Barcelona o Madrid >
snmp-server contact < contacto o nombre empresa cliente >
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps flash insertion renoval
snmp-server enable traps bgp
snmp-server enable traps hsrp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps vtp
snmp-server enable traps bridge newroot topologychange

Switch de Barcelona 2 y Madrid 2

La configuración es exactamente igual que la anterior, solamente añadimos las siguientes líneas:

interface <puerto de conexión con el router>
description ---- BACKUP router < Barcelona o Madrid> ----
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-1000
switchport mode trunk

9.3 Glosario de términos

-A
AS Autonomous System

-B
BGP Border Gateway Protocol
BPDU Bridge Protocol Data Unit
BW Bandwidth

-C
CBWFQ Class Based Weigthed Fair Queuing
CDP Cisco Discovery Protocol
CIDR Classless Inter-Domain Routing
CODEC Codificador-Decodificador
CS Call Server de Alcatel OXE

-D
DHCP Dynamic Host Configuration Protocol
DSCP Differentiated Services Code Point
DSP Digital Signal Processor

-E
EIGRP Enhanced Interior Gateway Routing Protocol

-H
HA Hybrid Attery
HCC Horizontal cross connect
HSRP Hot Standby Router Protocol

-I
IP Internet Protocol
ISDN Integrated Service Digital Network
ISP Internet Service Provider

-L
LAN Local Area Network

-M
MAC Media Access Control Address
MG Mediagateway Alcatel OXE

-O
OSPF Open Shortest Path First

-P
PC Personal Computer
PoE Power Over Ethernet
PQ Priority Queuing
PSTN Public Switched Telephone Network

-Q

QoS Quality of Service

-R

RIP Routing Information Protocol
RTP Real Time Protocol

-S

SAI Sistema de Alimentación Ininterrumpida
SFP Smart Form-factor Pluggable
STP Spanning Tree Protocol

-T

TFTP Trivial File Transfer Protocol

-U

UTP Unshielded Twisted Pair (Par trenzado no blindado)

-V

VLAN Virtual LAN
VLSM Variable Length Subnet Mask
VoIP Voice over IP
VTP VLAN Trunking Protocol

-W

WAN Wide Area Network