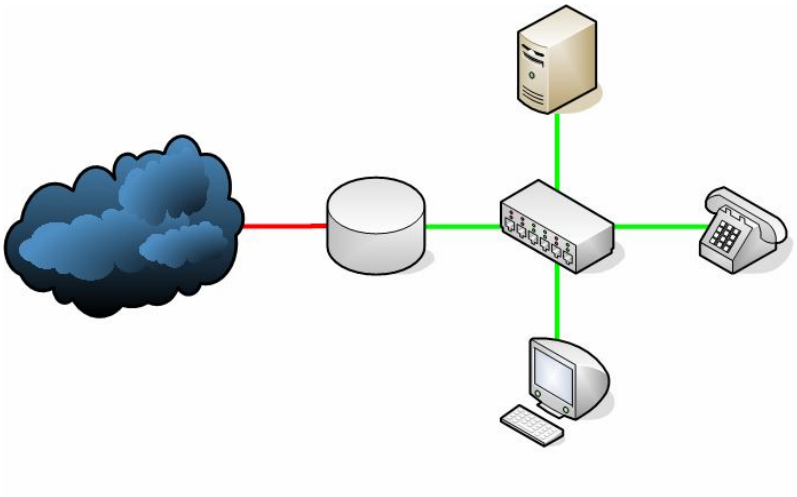
IMPLANTACION DE SWITCHING Y TELEFONIA IP SOBRE UNA RED WAN



Autor: Ivan Pique Palacin
Consultor: Jose Lopez Vicario
E.T.T Telematica
Febrero 2013

1 INTRODUCCION

1.1 DESCRIPCION

Este proyecto tiene como objeto el diseño y la implementación de servicios de comunicaciones de Lan (Switching) y Telefonía ip (ToIP), todos ellos integrados sobre una red wan nacional ya existente y funcionando, gestionada por un ISP.

La tendencia actual de los proveedores es abarcar y gestionar el número máximos de servicios y negocio de los grandes clientes, ya no solo se limitan al mantenimiento de una red Wan de comunicaciones sino que la clave es gestionar más servicios cada vez manteniendo un único interlocutor o ISP, la Gestión de LAN, ToIP, seguridad a través de Firewalls, Gestión del puesto de trabajo,…son algunos ejemplos.

Todo esto facilita la gestión de los servicios dando una visión global en este caso al proveedor de comunicaciones.

1.2 OBJETIVOS

Los objetivos principales de este proyecto son:

-Unificación de varios servicios en una misma red wan nacional para un cliente que posee sedes en diferentes puntos geográficos de la península

-Facilitar la gestión de los servicios centralizándolos en un mismo proveedor

-Obtener una red estable y optima con diferentes tecnologías.

-Reducción de la carga de trabajo del área informática de cliente, delegando funciones de gestión y monitorización de equipamiento en el proveedor de comunicaciones.

-Aumentar la seguridad de toda la red, evitando problemas originados en Lan de cliente donde hasta ahora el proveedor no intervenía, y que pueden afectar al servicio del cliente o incluso de otros clientes del ISP.

-Obtención de una red convergente optimizando tiempos de respuesta

-Redundancia ante posibles fallos del equipamiento y/o caídas de las líneas existentes, evitando afectación sobre los servicios finales que ofrece el cliente o reduciendo el impacto de los mismos.

-Reducción de costes destinado a comunicaciones a medio/largo plazo.

1.3 METODOLOGIA A IMPLEMENTAR

Para realizar el diseño/implementación de los nuevo servicios, antes se debe analizar el estado actual de la red y el equipamiento que tiene el cliente.

Una vez tengamos esta información de manera detallada, se debe valorar junto con cliente cual es la solución más adecuada a los requerimientos del mismo, y sobre todo valorar económicamente junto con cliente si las soluciones propuestas son viables.

Una vez decidido y concretado los trabajos a implementar, se aplicaran en 3 fases diferentes

-Modificaciones red Wan actual
-Modificaciones red Lan
-Implementación ToIP

Es importante realizar estas tareas en este orden ya que son directamente dependientes entre si, y la incorrecta implementación de una puede ocasionar problemas o funcionamientos erróneos en otra.

1.4 DESCRIPCION DE CAPITULOS

A continuación se detalla una breve descripción de los capítulos del proyecto.

2- Situación Actual del Cliente: se muestra la disposición de las sedes, servicios y el equipamiento del que dispone actualmente el cliente

3- Necesidades y Requerimientos del Cliente: una vez visto que es lo que tiene nos centramos en las necesidades sobre la red que se plantean en el proyecto

4-Modificaciones Red Wan Datos: Descripción de cambios sobre la red de Datos actual para la adaptación de posteriores servicios equipamiento,…

5- Solución comunicación de datos en LAN (Switching): Detalle de la solución de Switching a implementar, arquitectura, ventajas y equipamiento.

6- Solución comunicación de Telefonia IP (ToIP): Detalle de la solución de ToIP a implementar, arquitectura, ventajas, encaminamiento de las llamadas, contingencia y equipamiento.

7- Presupuesto: presupuesto de todos los elementos y trabajos implicados en el proyecto

8- Conclusiones: conclusiones extraídas de la realización del proyecto.

9- Glosario de Terminos

10- Bibliografía

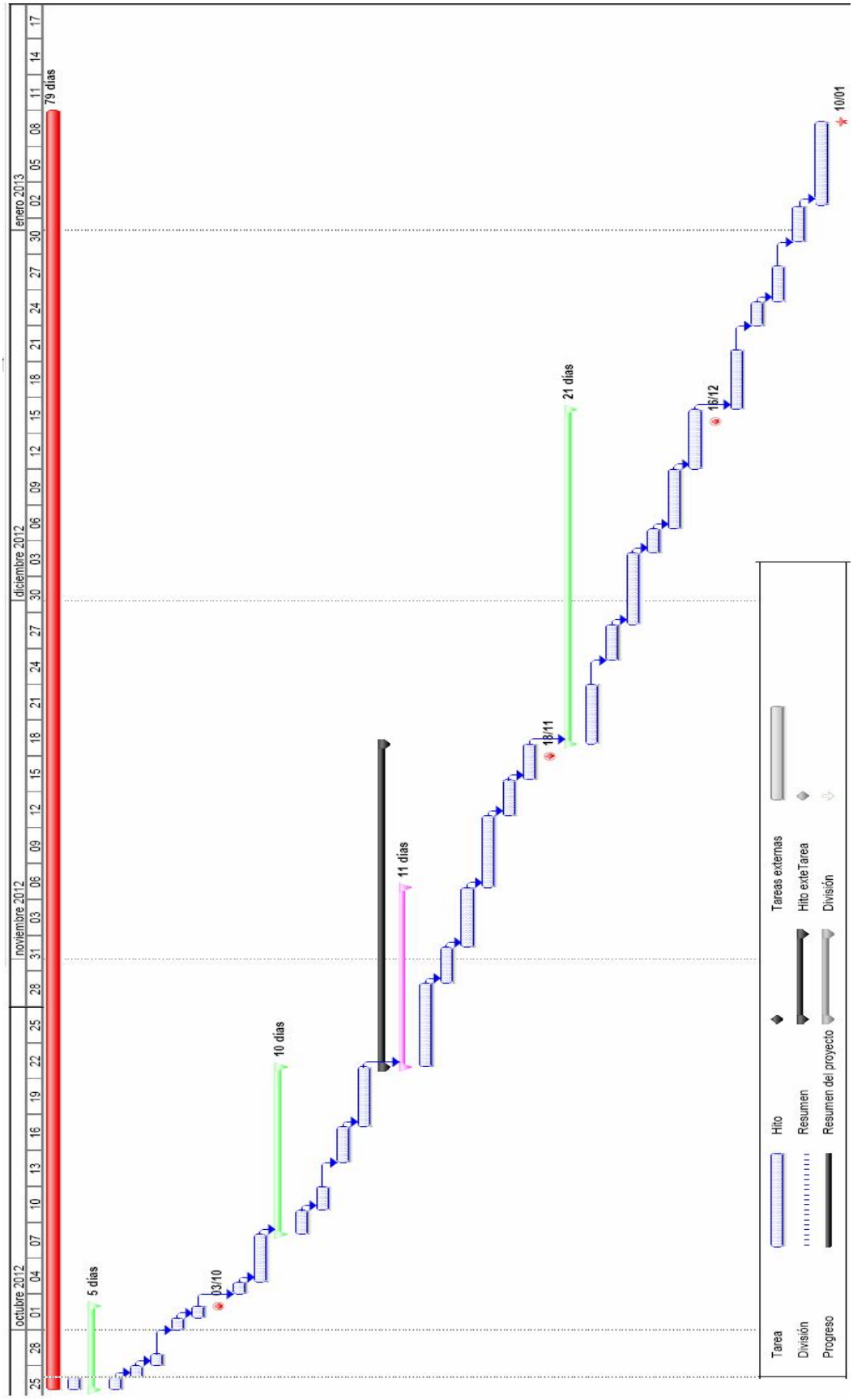
11- Anexos: se incluye información adicional

1.5 PLANIFICACION

1.5.1 Planificación y duración

Id	Tareas	Duración	Inicio	Fin
1	# REALIZACION DEL TFC #	79 días	mié 26/09/12	jue 10/01/13
2	Eleccion del TFC	1 día	mié 26/09/12	mié 26/09/12
3	**INTRODUCCION**	**5 días**	**mié 26/09/12**	**mar 02/10/12**
4	Introduccion	1 día	mié 26/09/12	mié 26/09/12
5	Objetivos	1 día	jue 27/09/12	jue 27/09/12
6	Metodologia a implementar	1 día	vie 28/09/12	vie 28/09/12
7	Descripcion de capitulos	1 día	lun 01/10/12	lun 01/10/12
8	Planificacion	1 día	mar 02/10/12	mar 02/10/12
9	## PAC 1 ##	1 día	mié 03/10/12	mié 03/10/12
10	**SITUACION ACTUAL DEL CLIENTE**	1 día	jue 04/10/12	jue 04/10/12
11	**NECESIDADES Y REQUERIMIENTOS DEL CLIENTE**	2 días	vie 05/10/12	lun 08/10/12
12	**MODIFICACION RED WAN DATOS**	**10 días**	**mar 09/10/12**	**lun 22/10/12**
13	Sedes centrales	2 días	mar 09/10/12	mié 10/10/12
14	Routing Wan	2 días	jue 11/10/12	vie 12/10/12
15	Calidades del Servicio (QOS)	3 días	lun 15/10/12	mié 17/10/12
16	Despiece de equipamiento	3 días	jue 18/10/12	lun 22/10/12
17	**SOLUCION COMUNICACIONES Switching**	**20 días**	**mar 23/10/12**	**dom 18/11/12**
18	**Arquitectura de la solucion**	**11 días**	**mar 23/10/12**	**mar 06/11/12**
19	Escenario CPD	5 días	mar 23/10/12	lun 29/10/12
20	Escenario Sedes remotas	3 días	mar 30/10/12	jue 01/11/12
21	Direccionamiento y VLANs	3 días	vie 02/11/12	mar 06/11/12
22	Ventajas de la solucion implementada	4 días	mié 07/11/12	lun 12/11/12
23	Equipamiento en Sede Central (CPDs)	3 días	mar 13/11/12	jue 15/11/12
24	Equipamiento en Sedes remotas	2 días	vie 16/11/12	dom 18/11/12
25	## PAC 2 ##	1 día	dom 18/11/12	dom 18/11/12
26	**SOLUCION COMUNICACIONES ToIP**	**21 días**	**lun 19/11/12**	**dom 16/12/12**
27	Arquitectura de la solucion	5 días	lun 19/11/12	vie 23/11/12
28	Ventajas de la solucion implementada	3 días	lun 26/11/12	mié 28/11/12
29	Equipamiento en Sede Central (CPDs)	4 días	jue 29/11/12	mar 04/12/12
30	Equipamiento en Sedes remotas	2 días	mié 05/12/12	jue 06/12/12
31	Enrutamiento de llamadas	3 días	vie 07/12/12	mar 11/12/12
32	Contingencia y redundancia del servicio	4 días	mié 12/12/12	dom 16/12/12
33	## PAC 3 ##	1 día	dom 16/12/12	dom 16/12/12
34	**PRESUPUESTO**	5 días	lun 17/12/12	vie 21/12/12
35	**CONCLUSIONES**	2 días	lun 24/12/12	mar 25/12/12
36	**GLOSARIO DE TERMINOS**	3 días	mié 26/12/12	vie 28/12/12
37	**BIBLIOGRAFIA**	3 días	lun 31/12/12	mié 02/01/13
38	**ANEXOS**	5 días	jue 03/01/13	mié 09/01/13
39	## Entrega TCF ##	1 día	jue 10/01/13	jue 10/01/13

1.5.2 Diagrama de GRANT



2 SITUACION ACTUAL DEL CLIENTE

El cliente actualmente dispone de sus sedes Centrales (Oficinas + CPD) en Barcelona y en Madrid, el resto de sucursales que se trata de 150 delegaciones, están repartidas por toda la península. Entre estas dispone de 3 Sedes secundarias importantes que son Valencia, Zaragoza y Vigo

Sobre esta Red Wan nacional el cliente dispone de servicios de Datos y VoIP, todos ellos trabajando con un mismo direccionamiento de red (192.100.0.0/20)

-En cuanto a equipamiento:

-<u>CPD Sedes Centrales Barcelona y Madrid</u>

Tanto en el CPD de Barcelona como el CPD de Madrid, referente a comunicaciones el cliente dispone de un Switch de nivel 3 con routing RIP, modelo Juniper EX 4200 conectado a la Red Wan a través de fibra óptica con un enlace de 100 mb/s
(Propiedad del ISP)

Tambien dispone de:

-4 Switches de nivel 2 del fabricante 3COM (Propiedad de cliente) en CPD Barcelona

-3 Switches de nivel 2 del fabricante 3COM (Propiedad de cliente) en CPD Madrid

-Sistema de telefonía Call Manager v.3.0 para la sede central y delegaciones. (Propiedad de cliente) en el CPD de Barcelona

-1 Gateway de voz Cisco 2801 con primarios Fijos y Móviles respectivamente, para salida llamadas externas a la red. (Propiedad de cliente) en CPD Barcelona y CDP Madrid.

-1 Gateway de voz Cisco 2801 con un primario Fijo y uno de Móviles para salida llamadas externas a la red. (Propiedad de cliente) en las sedes de Valencia, Zaragoza y Vigo

-200 terminales ATA repartidos entre todas las sedes

Actualmente el encaminamiento de llamadas al exterior se realiza a través de los gateways del CDP de Barcelona, y como contigencia se utiliza el gateway del CPD de Madrid.

*****Es importante conocer que el cliente dispone de diferentes servicios en cada CPD, por lo tanto las Sedes Remotas acceden tanto a servidores del CPD de Barcelona como de Madrid

-Sedes Remotas

En cada Sede remota el cliente dispone de un router Cisco 1801 con una línea ADSL para la conexión a la red Wan (Propiedad del ISP)

Tambien dispone de:
-Dispositivos Cisco ATA conectados a teléfonos analógicos (Propiedad Cliente)
-1 Switch nivel 2 de la marca 3COM no gestionable (Propiedad Cliente)

3 NECESIDADES Y REQUERIMIENTOS DE CLIENTE

Las necesidades actuales del Cliente en los diferentes ámbitos son:

Red Wan Datos

-Solventar los problemas que esta teniendo con la VoIP al no disponer de QoS

-Sistema de redundancia para las comunicaciones de los CPDs, al tratarse de sedes criticas y cada una poseer unos servicios diferentes.

-Necesidad de caudales independientes para los diferentes tipos de trafico (voz, datos…) para un tratamiento y funcionamiento correcto de cada uno de estos.

-Mejorar la convergencia y optimización de la red

Comunicaciones de datos en Lan (Switching)

-Evitar problemas en Lan generados por la no separación del trafico y equipamiento insuficiente

-Ahorro en infraestructura y desplazamiento del personal propio por incidencias en Switches de nivel 2

Comunicaciones de Telefonia IP (ToIP)

-Sustitución de servidor de llamadas obsoleto, en parte debido a ampliación de puestos de trabajo con teléfono

-La necesitad de un segundo servidor de llamadas en el CDP de Madrid que actúe en caso de contingencia a posibles caídas del servidor de llamadas principal (CPD Barcelona)

-Eliminación de adaptadores ATA y teléfonos analógicos sustituyéndolos por terminales ToIP, se requiere aprovechar todas las funcionalidades y ventajas que ofrece ToIP respecto VoIP

-Necesidad de un sistema de redundancia para las sedes de Valencia, Zaragoza y Vigo en caso de incomunicación con el Servidor de llamadas

4 MODIFICACION RED WAN DATOS

Una vez vistas las necesidades del cliente para la red wan de Datos, las modificaciones a aplicar serán las siguientes.

-Modificación de caudales contratados e implementación de QoS (Quality Of Service) y así se evitaran problemas surgidos sobre la telefonía del cliente.

-Alta de un nuevo Switch nivel 3 para cada uno de los CPDs que actúe como sistema de backup o redundancia del actual equipo, conexión con la red Wan

-Cambio de protocolo de Routing en toda la red Wan para mejora de convergencia (De RIP a BGP)

4.1 Sedes Centrales

Para el caso de las Sedes Centrales - CPD de Barcelona y Madrid, se debe dar de alta un nuevo Switch de nivel 3 para proveer redundancia a la interconexión con la red Wan.

Se provisionará en ambos casos un equipo como el ya existente Juniper EX 4200. La funcionalidad de este será actuar como sistema de backup del actual equipo principal. Es muy importante proporcionar contingencia a este tipo de Sedes Centrales ya que todas las Sedes remotas acceden a los servicios de los servidores de los CPD.

-**Diversificación en la parte LAN (VRRP)**

El sistema de activación del router de backup se realizará mediante el protocolo de router VRRP, se trata de un protocolo de redundancia no propietario, por lo tanto lo podemos aplicar en nuestro equipamiento Juniper.

Este sistema se utiliza para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. Dos routers se configuran representando al router virtual, pero sólo uno de ellos esta realizando el enrutamiento, en caso de caída física del enlace o router Principal, el router de Backup negocia para sustituirlo.

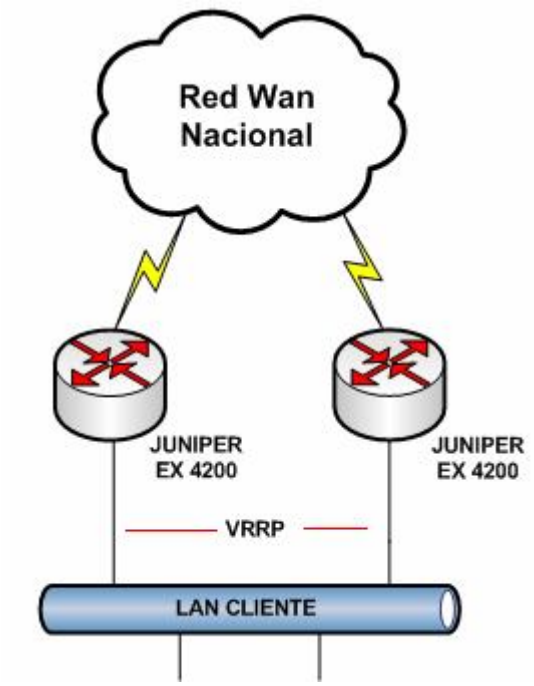
*(Se incluye configuración en ANEXO)

-**Diversificación en la parte WAN**

Queremos tener los dos routers trabajando de cara hacia la red Wan sin que haya conflictos sobre las mismas redes que esta propagando hacia el exterior de la Sede.

Esto lo aplicaremos variando las métricas del protocolo de routing.
Si anunciamos las mismas redes exactamente por el enlace de backup con peor métrica, cualquier conexión entrante preferirá el router Principal, y en caso de caida preferira el router de Backup.
De esta manera conseguimos que convivan los dos routers activos tanto principal como backup, sin ningún tipo de conflicto de cara hacia la Wan.

*(Se incluye configuración en ANEXO)



4.2 Routing Wan

Los protocolos de enrutamiento permiten a los routers determinar la ruta mas óptima hacia una red destino o host haciendo posible el encaminamiento del tráfico hacia ese destino.

Las funciones básicas de estos algoritmos son determinación de una ruta para enviar los paquetes por el interfaz seleccionado más apropiado y conmutación de la ruta, permitiendo aceptar paquetes por un interfaz y reenviándolos por otro diferente.

Existen protocolos de enrutamiento estático y dinámico:

-Routing Estático

El routing estatico es un tipo de enrutamiento que no sobrecarga los routers ni los enlaces y fácil de configurar.
Es generado por el propio administrador, todas las rutas estáticas que este ingrese son las que el router conocerá, de esta manera sabrá enrutar el tráfico hacia dichas redes.

Por otra parte presenta graves limitaciones como poca escalabilidad y falta de adaptabilidad antes fallos.

-Routing Dinámico

Para resolver algunos problemas que presenta el routing estatico aparecen los protocolos de enrutamiento dinámico.
El administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos en todos los routers de la red, estos automáticamente intercambiaran sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de los otros dispositivos.

Todo esto al precio de un mayor consumo de ancho de banda y potencia del procesador en tareas de adquisición y mantenimiento de información sobre el enroutamiento.

Algunas características de estos protocolos son:

-Escalables y adaptables
-Originan sobrecargas en la red
-Presentan recuperación antes fallos

Los protocolos de enrutamiento dinámicos se clasifican en:

-Vector Distancia: su métrica se basa en el “número de saltos”, es decir la cantidad de routers por los que tiene que pasar el paquete antes de llegar a su destino, la ruta que tenga el menor número de saltos es la más optima y la que se publicará. (Cuanto mejor métrica mejor es la ruta)

Estos algoritmos basados en vectores, pasan copias periódicas de la tabla de enrutamiento entre routers que comunican los cambios en la topologia.

-Estado de enlace: su métrica se basa en el retardo, ancho de banda, carga y confiabilidad de los distintos enlaces posibles para llegar a un destino, en base

a estos conceptos el protocolo prefiere una ruta sobre otra. Estos protocolos utilizan un tipo de publicaciones llamadas de estado de enlace (LSA) que intercambian los routers, mediante estas publicaciones cada router crea una base de datos de la topología de la red completa.

Estos protocolos solo envían actualizaciones cuando hay cambios de topologia y soportan direccionamiento sin clase.

-Hibrido: son algoritmos que toman las características más sobresalientes del vector de distancia y las del estado de enlace. Utilizan la métrica de los protocolos vector distancia, sin embargo utilizan las actualizaciones de los cambios de topologia como los protocolos de estado enlace.

A continuación se muestra una tabla comparativa entre vector distancia y estado enlace:

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 lenta	Actualizaciones activadas por eventos, convergencia rápida
Pasa copias de la tabla de enrutamiento a los routes vecinos	Pasa las actualizaciones de enrutamiento de estado del enlace a los otros routers

---

Actualmente el cliente dispone de RIPv2 como protocolo de routing en todos sus routers. Analizamos este protocolo y vemos que no es el más apropiado en cuanto aplicamos ToIP en nuestra red.

-RIPv2

Se trata de uno de los protocolos de enrutamiento interior más sencillos y utilizados, es un protocolo vector-distancia lo que significa que se basa en los saltos intermedios que tiene hasta su destino. (Como máximo 15 saltos).

Algunas características són:

-Protocolo vector-distancia
-RIPv2 envia actualizaciones de enrutamiento a través de multicast
-Sumariza actualizaciones de enrutamiento automáticamente

-Su métrica es la cuenta de saltos.

Su funcionamiento es sencillo, el equipo envía la tabla de enrutamiento completa a todos los vecinos cada 30 segundos. Es sensible a la aparición de bucles de enrutamiento al ser un protocolo de vector distancia.

Por lo tanto no es la mejor opción para una red amplia donde se necesiten tiempos de convergencia cortos y actualizaciones de la topología óptimas, debido a la sensibilidad de la Telefonía IP.

Vemos algunos protocolos de enrutamiento que se plantean como alternativas a RIPv2, por ejemplo: EIGRP, OSPF o BGP

-EIGRP

Se trata de un protocolo de routing hibrido ya que tiene características tanto de protocolos de vector distancia como de estado enlace. Propietario de Cisco, tiene unos tiempos de convergencia altos debido al algoritmo que utiliza (Cuando hay cambios de routing solo se anuncian estos cambios y a los routers afectados)

Algunas características son:

-Protocolo de routing hibrido
-Utiliza ancho de banda de manera mas eficiente que protocolos de vector-distancia
-Anuncios de routing solo cuando hay cambios
-Para valorar métrica utiliza ancho de banda, retardo, confianza, carga y tamaño MTU
-Split Horizon (No puede aprender una ruta por el mismo interfaz que la esta anunciando)

-OSPF

Protocolo de routing de tipo estado-enlace, se trata de un estandar utilizado normalmente para implementar el routing en grandes redes cuando intervienen varios proveedores o ISP diferentes.

Algunas características son:

-Protocolo de estado-enlace
-Ultiliza “areas” para la creación de diferentes grupos de routers que establecen adyacencia entre sí.
-Realiza actualizaciones cuando hay cambio de información en rutas
-Analiza métrica viendo el coste de cada router intermedio hasta

destino
-Permite balanceo de carga a través de 4 rutas de igual coste.

-BGP

Se considera un protocolo exterior de gateway, utilizado para el intercambio de información de routing entre diferentes AS (Sistemas Autonomos).
Cada Sistema Autonomo puede tener sesiones internas iBGP y sesiones con el exterior eBGP contra otro Sistema Autonomo donde se intercambia la información.

Algunas características son:

-Protocolo más utilizado por los ISP en Internet
-Toma decisiones de routing basándose en políticas de red que utilizan varios atributos de ruta BGP
-Admite routing con redes sin clase (CIDR)

-Analizamos cada protocolo de routing viendo si es posible aplicarlo en nuestro caso particular

EIGRP: Se trata de un protocolo de routing ideal viendo nuestras necesidades, el único inconveniente es que solo se implementa con equipamiento del fabricante Cisco, y en nuestra red tenemos equipamiento Cisco y Juniper.
Otra opción es sustituir los equipos Juniper de los CPD por equipamiento Cisco, esto incrementaría el presupuesto inicial y el tiempo de implementación, por lo tanto queda descartada esta posibilidad

OSPF: A pesar de tratarse de un protocolo muy acertado y con rápida convergencia, queda descartado ya que esta orientado principalmente para conexiones entre varios proveedores y redes muy extensas.

BGP: aporta mucha flexibilidad y eficacia ante los cambios de topología de la red, dando una convergencia más rápida que RIPv2. Al tratarse de un protocolo de routing hibrido aprovecha las funcionalidades de un protocolo vector distancia y las mejoras en cambios de topologia que ofrece un protocolo estado enlace.
Por lo tanto este es el protocolo más apropiado para implementar como alternativa a RIPv2

*(Se incluye configuración en ANEXO)

-A continuación se muestra una tabla comparativa de cada protocolo de routing y sus características de manera resumida

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

4.3 Calidades de Servicio (QoS)

Las redes fueron originalmente diseñadas para transportar trafico de datos, a medida que estas redes deben adoptar también trafico en tiempo real como la voz se requieren mecanismos que aseguren que la voz tendrá prioridad.

Las conversaciones ocurren en tiempo real, lo que significa que es inaceptable que los paquetes de ToIP lleguen tarde o nunca.

Para solventar estas adversidades se han creado mecanismos que aseguran que los paquetes ToIP sean priorizados dentro de una red, denominados QoS. De esta manera se trata de manera selectiva el tráfico IP en cada nodo de la red.

Los factores que intervienen en la calidad de la voz son:

-Codec
-Ancho de Banda
-Latencia
-Jitter
-Perdidas de paquetes

La capacidad para permitir la perdida de paquetes en ToIP se muy baja (2% máxímo) para que no afecte a la calidad de manera notoria.
Pero los problemas que mas afectan son la Latencia, Jitter y ECO

-Codec

La comunicación de voz es analogica, mientras que la red de datos es digital.
El proceso de convertir de ondas analógicas a información digital se realiza con un codificador-decodificador (CODEC).

Ademas de la conversión el CODEC comprime la secuencia de datos ahorrando ancho e banda y proporciona cancelación del eco.
A continuación se muestra una tabla con los Codecs G.711 y G.729, auque existen muchos mas.

Nombre	Estandarizado	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS (Mean Opinion Score)
G.711 *	ITU-T	Pulse code modulation (PCM)	64	8	Muestreada	Tiene dos versiones u-law (US, Japan) y a-law (Europa) para muestrear la señal	4.1
G.729 **	ITU-T	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	8	8	10	Bajo retardo (15 ms)	3.92

-Latencia

Se define como el retardo entre envió de paquetes y su recepción. Puede tratarse de retardos producidos por retardos acumulados durante la transferencia de paquetes o retardos de procesamiento, compresión....
Los retardos de compresión se pueden reducir utilizando el codec G.711 en lugar del G.729 siempre que sea posible.
Los retardos debido a la red suelen ajustarse prestando atención a los componentes físicos de la red que a menudo se pasan por alto como conectores en mal estado, campos eléctricos interferentes, etc.

-Jitter

es la variación de los retardos en la llegada de los paquetes entre origen y destino, normalmente se suele producir por la congestión del tráfico en algún punto de la red o diferencia del tiempo de transito de los paquetes cuando viajan por diferentes rutas.
La solución es implementar un buffer que almacene los paquetes antes de entregarlos a destino asegurando que todos lleguen en orden correcto (aunque esto incluya un retardo adicional), cuando se trata den redes Lan/Wan se suele corregir incrementando el ancho de banda.

-Eco

Cuando tenemos latencia y jitter en una comunicación ToIP se puede producir el fenónmeno del Eco. Normalmente se puede resolver utilizando "canceladores de eco", se pueden implementar a través de software o hardware.

-Perdida de Paquetes

La perdida de paquetes puede producirse por erroresw en alguno de los equipos de la red o por sobrepasar las capacidades de algun buffer de algún equipo o aplicación en momentos de congestión.

La calidad de servicio QoS se encarga de proveer un nivel de servicio para que las diferentes aplicaciones que usen la red puedan beneficiarse de ella de manera apropiada, en nuestro caso para la ToIP.

-Implementacion de QoS

El proceso de aplicación de la QoS se llevara a cabo en la salida de cada router hacia la red Wan de la siguiente manera:

-Clasificacion: Todo el tráfico de que entra por la LAN se pasa por unas listas de acceso (Se puede aplicar esta selección de varias maneras) para separar cada tipo de tráfico, se machea y clasifica en diferentes grupos.

- Marcado: Una vez clasificado, se marcará para distinguirlo del resto (Precendencia IP)

A continuación se muestra una tabla de equivalencias de las Precendence IP y sus posibles valores.

ToS dec	ToS hex	ToS bin	ToS Prec. (bin)	ToS Prec. (dec)	ToS Delay Flag	ToS Throgh-put Flag	ToS Relia-bility FLag	DSCP bin	DSCP hex	DSCP dec	DSCP Class
0	0×00	00000000	000	0	0	0	0	000000	0×00	0	none
32	0×20	00100000	001	1	0	0	0	001000	0×08	8	cs1
40	0×28	00101000	001	1	0	1	0	001010	0x0A	10	af11
48	0×30	00110000	001	1	1	0	0	001100	0x0C	12	af12
56	0×38	00111000	001	1	1	1	0	001110	0x0E	14	af13
64	0×40	01000000	010	2	0	0	0	010000	0×10	16	cs2
72	0×48	01001000	010	2	0	1	0	010010	0×12	18	af21
80	0×50	01010000	010	2	1	0	0	010100	0×14	20	af22
88	0×58	01011000	010	2	1	1	0	010110	0×16	22	af23
96	0×60	01100000	011	3	0	0	0	011000	0×18	24	cs3
104	0×68	01101000	011	3	0	1	0	011010	0x1A	26	af31
112	0×70	01110000	011	3	1	0	0	011100	0x1C	28	af32
120	0×78	01111000	011	3	1	1	0	011110	0x1E	30	af33
128	0×80	10000000	100	4	0	0	0	100000	0×20	32	cs4
136	0×88	10001000	100	4	0	1	0	100010	0×22	34	af41
144	0×90	10010000	100	4	1	0	0	100100	0×24	36	af42
152	0×98	10011000	100	4	1	1	0	100110	0×26	38	af43
160	0xA0	10100000	101	5	0	0	0	101000	0×28	40	cs5
184	0xB8	10111000	101	5	1	1	0	101110	0x2E	46	ef
192	0xC0	11000000	110	6	0	0	0	110000	0×30	48	cs6
224	0xE0	11100000	111	7	0	0	0	111000	0×38	56	cs7

- Conformado (Shaping): Debemos limitar el tráfico de cada clase para que en caso de congestión no se curse más de lo debido.

- Encolado: Finalmente en el interfaz de salida, se define la política de encolado y el tamaño de las colas.

Hay diferentes políticas de encolado que se pueden implementar y dependerá del ISP

-FIFO: First In First Out: Comportamiento por defecto del Interfaz Físico

-PQ: Priority Queuing: Las colas son atentidas de manera estricta según su prioridad

-CBWFQ: Class Based Weigthed Fair Queuing: cada cola le corresponde un porcentaje dentro de la planificación de un “scheduler”, garantiza un ancho de banda mínimo.

-LLQ: Low Latency Queuing: Límita y garantiza un ancho de banda mínimo además de añadir prioridad estricta

La manera de implementar la QoS varia en función de las decisiones que tome el provedor de servicios en la red Wan, independientemente debemos reservar un trafico para el uso de ToIP evitando problemas con el tráfico de datos y garantizando el correcto funcionamiento de la Telefonia IP del cliente.

En nuestro caso el ISP aplica 3 calidades de servicio para el cliente

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

En nuestro proyecto para cada línea ADSL y F.O se modificaran los caudales (Hasta ahora no había distinción del tráfico en la red) utilizando
75% Tráfico Plata + 25% Tráfico Multimedia garantizado en las Sedes remotas y 90% Tráfico Plata + 10% Tráfico Multimedia en las Sedes centrales (CPD)

-Calculo BW destinado a ToIP

El BW destinado a la Telefonia IP depende de varios factores, utilizamos una tabla para ver cuanto ocupará cada llamada aproximadamente en nuestro caso, utilizaremos para la Wan el codec G.729

Codec Information				Bandwidth Calculations					
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80 Bytes	10 ms	4.1	160 Bytes	20 ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	26.8 Kbps	11.6 Kbps	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	18.9 Kbps	8.8 Kbps	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	17.9 Kbps	7.7 Kbps	20.8 Kbps

Utilizando G.729 cada llamada ocupa aproximadamente unos 32 Kbps

-Sedes remotas: tenemos 3 Telefonos, por lo tanto 3 llamadas a la vez como máximo (32 Kpbs x 3 = 96 Kbps) , suponiendo que disponemos en cada linea una velocidad de subida de 512 Kbps y destinamos un 25% del BW a Voip nos queda 128 Kbps.

128 Kbps > 96 Kbps

Por lo tanto sera posible cursar 3 llamadas al mismo tiempo dejando un margen de BW

-Centrales CPDs: tenemos 225 Telefonos, estadísticamente no se considera que todos los Telefonos puedan llamar al mismo tiempo, aun así el calculo (32 Kbps x 225 = 7,2 Mbps), si destinamos el 10% del BW (100 Mbps) nos queda 10 Mbps

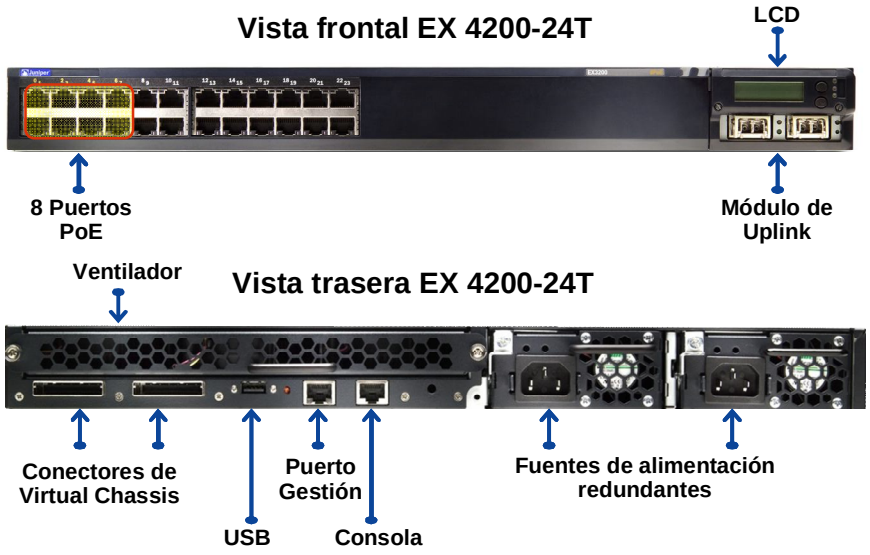
10 Mbps > 7,2 Mbps

Aunque disponemos de un margen considerable teniendo en cuenta que los teléfonos no llamaran al mismo tiempo, el BW destinado a Multimedia puede

aumentar en un futuro con el crecimiento de la empresa o el uso de nuevos servicios relacionados con la Telefonia IP, como por ejemplo recursos multimedia centralizados o nuevos servidores.

4.4 Despiece del equipamiento

JUNIPER EX 4200



-<u>Descripción</u>:

La línea de conmutadores Ethernet EX4200, diseñados para despliegues de acceso y agregación, proporciona lo mejor de los sistemas modulares basados en estructuras en un factor de forma compacto y eficiente.

La línea EX4200 ofrece plataformas 10/100/1000BASE-T de configuración fija de 24 y 48 puertos con opciones de alimentación por Ethernet (PoE) completa (todos los puertos) y parcial (ocho puertos). También está disponible una plataforma de fibra basada en SFP 100BASE-FX/1000BASE-X de 24 puertos diseñada para despliegues de agregación en gigabits que requieren soporte para enlaces de larga distancia.

También se hallan disponibles módulos de enlace ascendente de cuatro puertos Gigabit Ethernet (GbE) y dos puertos 10GbE opcionales con óptico conectable.

-Especificaciones:

Factor de forma

- Plataforma fija (conmutador único)
- Configuración de Virtual Chassis compuesta por 10 conmutadores

Dimensiones

- (An x Al x P) 17,4 x 1,7 x 16,4 pulg. (44,2 x 4,3 x 41,7 cm)
- 1 unidad de bastidor (conmutador único)

Velocidad de plano posterior
128 Gbps (Virtual Chassis)

Velocidad de datos

- EX4200-24P/24T/24F: 88 Gbps
- EX4200-48P/48T: 136 Gbps

Procesamiento

- EX4200-24P/24T/24F: 65 Mpps (velocidad de cable)
- EX4200-48P/48T: 101 Mpps (velocidad de cable)

Densidades de puertos 10/100/1000BASE-T

- 24/48 por plataforma
- Hasta 480 en la configuración de Virtual Chassis

Densidades de puertos 100BASE-FX/1000BASE-X (SFP)

- 24 por conmutador; 28 con módulo opcional de enlaces ascendentes GbE de cuatro puertos
- Hasta 280 en la configuración de Virtual Chassis

Densidades de puertos 10GBASE-X

- 2 por conmutador (mediante módulo opcional de enlaces ascendentes 10GbE de dos puertos)
- Hasta 20 en la configuración de Virtual Chassis

Resistencia
Sistema de alimentación interno, redundante e intercambiable en caliente; bandeja de tres ventiladores reemplazables en campo; conmutación sin problemas de motor de ruta (GRES) en la configuración de Virtual Chassis

Opciones de alimentación

- CA: detección automática de 320 W, 600 W y 930 W; 100-120 V/200-240 V; sistemas de alimentación internos, redundantes, duales, de carga compartida e intercambiables en caliente
- CC: 190 W: tensión de entrada de 36 V a 72 V; alimentación de entrada dual, sistemas de alimentación internos, redundantes, duales, de carga compartida e intercambiables en caliente

Sistema operativo
Junos

Supervisión de tráfico
sFlow

Colas de QoS por puerto
8

Direcciones MAC
32,000

Tramas gigantes
9216 Bytes

Rutas unicast/multicast IPv4
16,000 / 8,000

Número de redes VLAN
4,096

Entradas ARP
16,000

Garantía
Garantía de hardware del conmutador de duración limitada

-Funcionalidades:

Routing	Dynamic Host Configuration	VLAN infraestructur, link aggregation, OAM, Metro Ethernet	QoS	Security(ACL´s) and Authentication
Static routes	DHCP (client y server)	RVI (routed VLAN interface)	EZQoS	Stateful firewall, stateless filters (ACL´s)
RIPv2	DHCP relay	GVRP	L2 QoS (classification, rewrite, queuing)	802.1x
OSPF/OSPFv3	**STP**	Link Aggregation and LACP	Per interface rewrite	Port security
BGP	VSTP	802.1q VLAN Trunking	CoS on L3 VLAN	**IPv6**
MBGP	BPDU, loop and Root protect	802.1Q Ethertype	L3 QoS (classification, rewrite, queuing)	OSPFv3
IS-IS	802.1D, 802.1w (RSTP), 802.1s (MST)	Layer 3 vlan-tagged sub-interface	SDWRR (egress scheduling)	RIPng
BFD(for RIP, OSPF, ISIS,BGP, PIM)	**SLA, Measurement, and Monitoring**	LLDP	Remarking of bridged packets	IPv6 Multicast Listener Discovery (MLD)
Multicast (IGMPv1/2/3), PIM-SM/DM/SSM, MSDP	Real-time perfor. monitoring (RPM)	Redundant Trunk Group	Strict priority queuing (LLQ)	BGP
MPLS (RSVP, LDP)	RMON	802.3ah (OAM)	**Administration**	ISIS
Virtual Router(VRF-LITE)	Mirroring	802.1 ag	Managers support	**High Availability**
Logging	S-Flow monitoring and accounting services	QinQ	External adm. database (RADIUS, TACACAS+)	VRRP
Syslog			Juniper TELNET , SSH	VCP Fast Failover (<50 mSec)
Traceroute				

De todas estas funcionalidades, vemos cuales son las más destacadas en la implantación del proyecto

- **Protocolo BGP:** protocolo de routing a implementar en la wan descrito anteriormente

- **QoS:** implementaciñon de clasificación, remarcado y encolado para calidades de servicio

- **Monitoring (RMON)** agente software para el tratamiento y monitorización de alarmas, estadisticas y eventos del equipo.

- **VRRP:** protocolo de redundancia esplicado anteriormente, permite conmutación a Backup en caso de caída física del enlace o router Principal

- **TACACS+ / Radius autenticacion:** aporta restricciones de acceso al equipamiento de usuarios no autorizados.

5 SOLUCION COMUNICACIONES DE DATOS EN LAN (Switching)

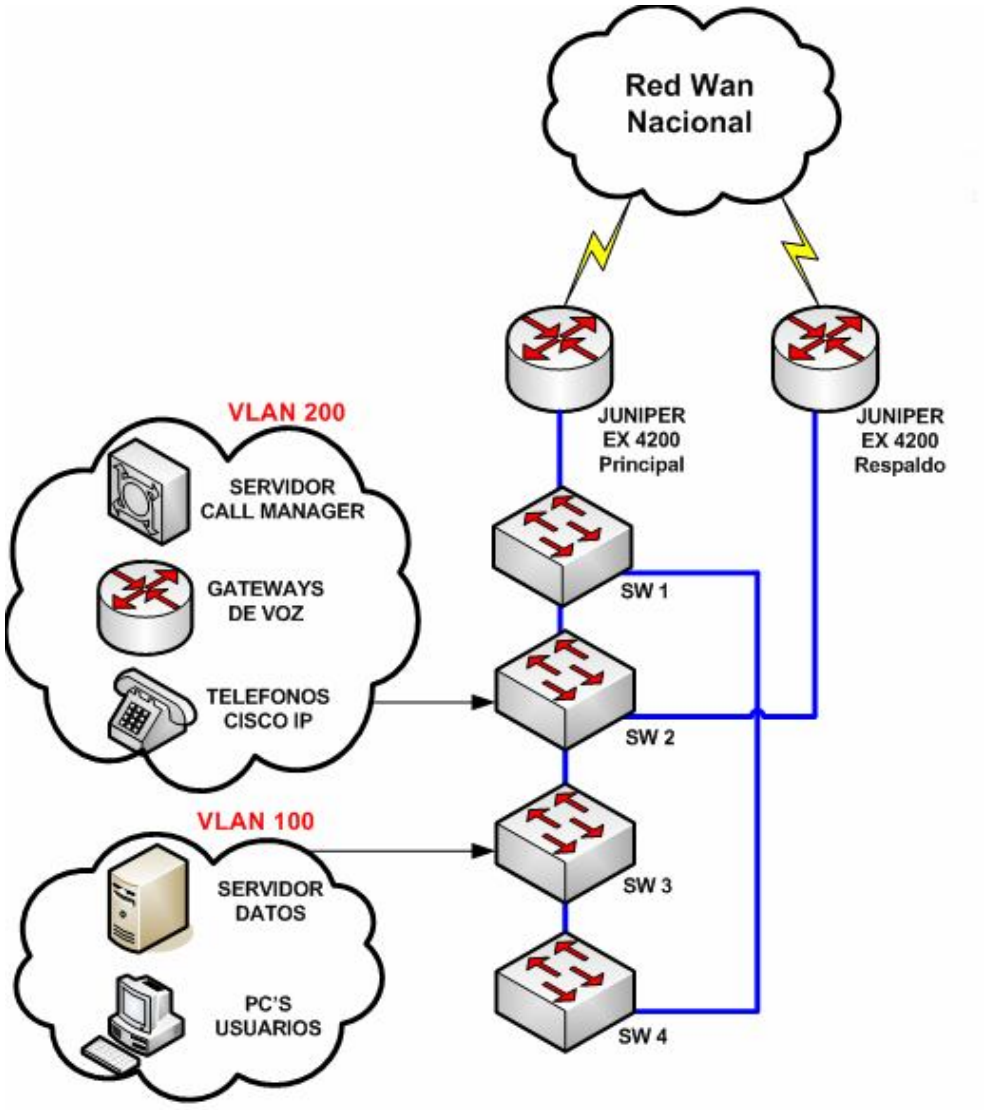
Una vez vistas las necesidades del cliente para la red de comunicaciones de datos en LAN, las modificaciones a aplicar serán las siguientes.

-Sustitución de todos los Switches de nivel 2 del cliente por Switches de nivel 3 gestionables y con sus nuevas funcionalidades

5.1 Arquitectura de la solución

5.1.1 Escenario CPDs

-Esquema topología CPDs

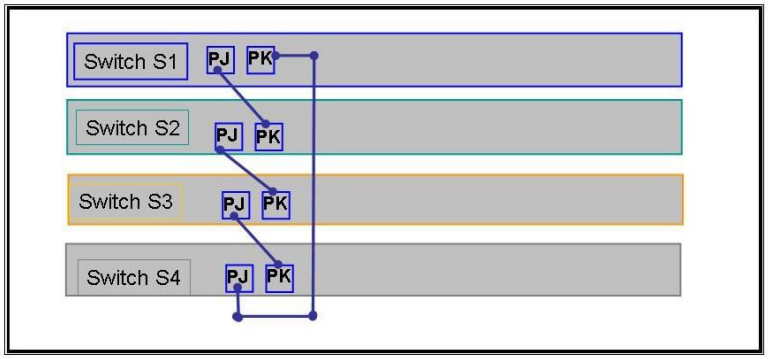


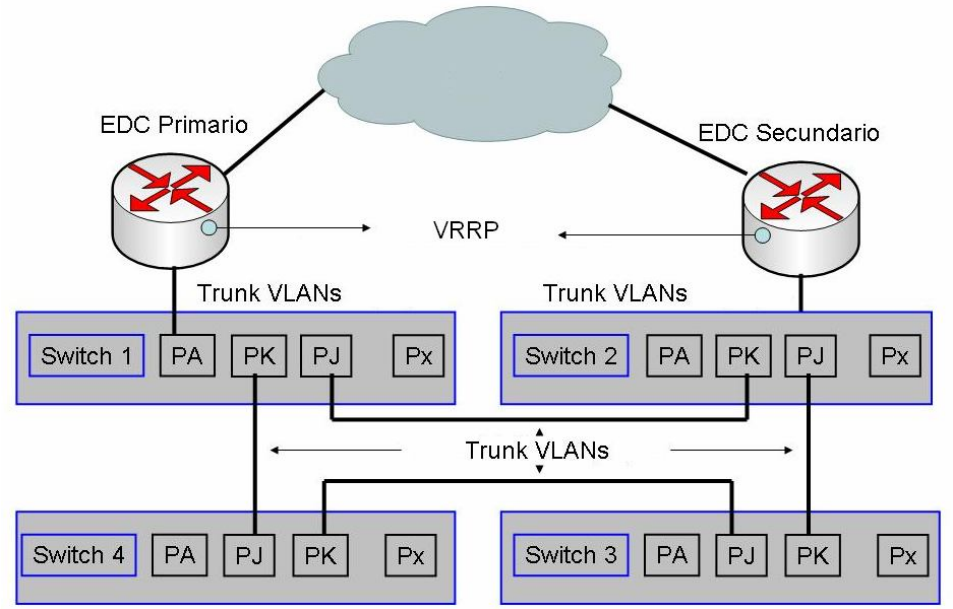
(La topología es la misma tanto para Barcelona como Madrid, la única diferencia recae en el número de Switches. Barcelona 4 switches y Madrid 3 switches)

Nombre del Switch	Conexiones
Switch 1 (Switch principal Acceso/Distribución N3)	Será el Switch al que se conecte el EDC principal. Tendrá una conexión al Switch 2 (si existe) o al Switch 3 (si existe) o al Switch 4 (si existe) Realizará funciones de distribución cuando se utilice Nivel 3.
Switch 2(Acceso/Distribución N3)	Será el Switch al que se conecte el EDC secundario Este Switch se conectara al Switch 1 y al Switch 3 (si existe).
Switch 3(Acceso)	Será el Switch que se conecte con el Switch 2 y con el Switch 4 (si existe). Si no existe el Switch 4, el Switch 3 se conectara al Switch 1 para proporcionar redundancia de caminos.
Switch 4(Acceso)	Será el switch que se conecte al Switch 3 y al Switch 1 para proporcionar redundancia de caminos.

-Interconexión entre cuatro Switches (CPD Barcelona)

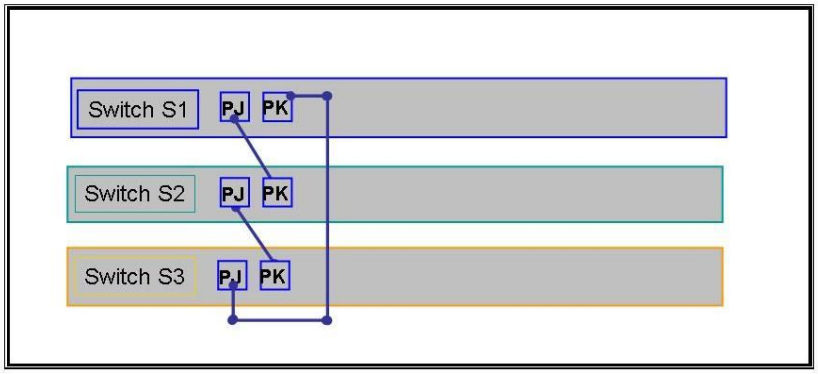
A continuación se muestra como se conectan 4 Switches entre sí.
El Switch 4 se conecta al Switch 1 para proporcionar redundancia de caminos.
En este caso hay que activar STP para evitar bucles

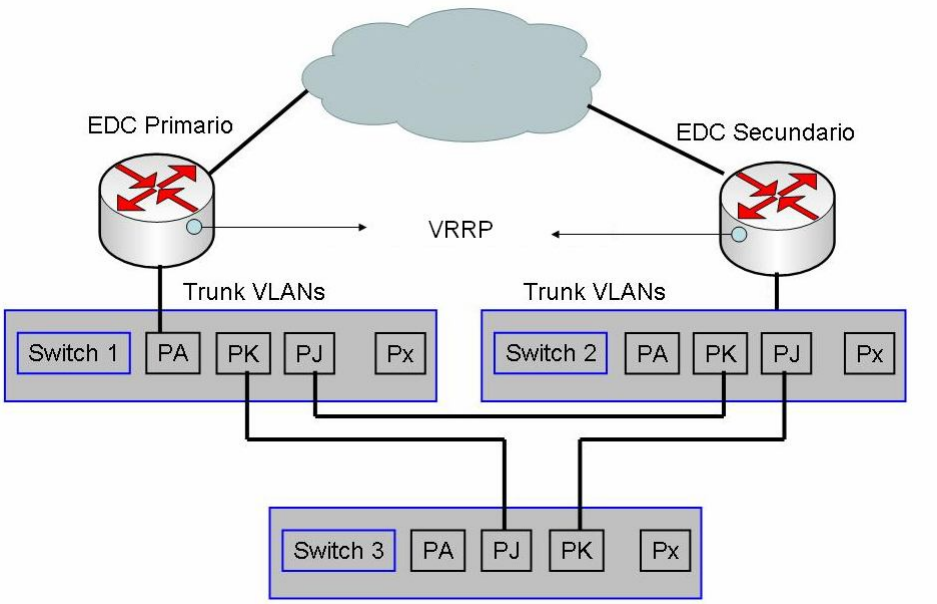




-Interconexion entre tres Switches (CPD Madrid)

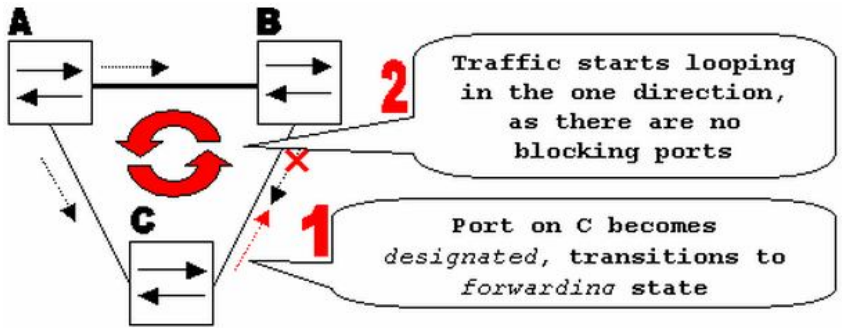
A continuación se muestra como se conectan tres Switches entre si
El Switch 3 se conecta al Switch 1 para proporcionar redundancia de caminos, en este caso habrá que activar también spaning tree para evitar bucles.





Bucles de nivel 2

En los escenarios de Switching implantados en los CPD, hay que tener muy en cuenta varios factores para evitar que aparezca cualquier bucle de nivel 2.
Los bucles se pueden dar siempre que tratemos escenarios con redundancia, en escenarios simples estos problemas quedan descartados.



Spanning Tree

El protocolo Spanning Tree ha sido diseñado para evitar posibles bucles en entornos de Switching. Para localizar enlaces redundantes STA elige un punto de referencia y calcula todos los camino redundantes hacia dicho punto.
Si descubre varios caminos redundantes hacia el mismo punto, elige un camino entre todos estos que será el que utilizara para propagar las tramas, el resto los deja bloqueados.

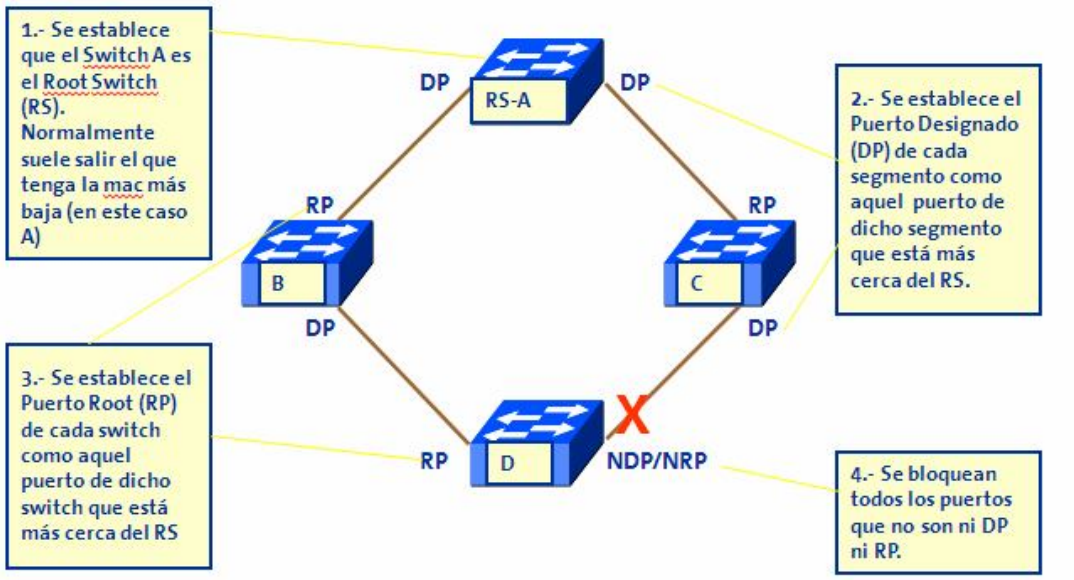
Cada vez que se da algún cambio a nivel físico en alguno de estos enlaces, STA recalcula todos los caminos y si es necesario desbloquea alguno de los caminos anteriormente bloqueados para mantener la conectividad.

Todos los switches que forman parte de la LAN participan en el protocolo STP mediante el intercambio de mensajes, estos mensajes reciben el nombre de Bridge Protocol Data Unit (BPDU)

En resumen, el proceso de Spanning Tree para decidir que puertos de bloquea y cuales no es el siguiente:

1- Se elige a un switch como RS (Switch Root)
2- Se calcula el camino más corto del RS a cada switch
3- En cada switch se decide cual de todos los puertos es el más cercando al RS y se marca como RP (Port Root)
4- En cada segmento formado por varios switches se decide quien es switch designado (DS), este es el switch de ese segmento mas cercano al RS. En el RS todos sus puertos son DP.
5- Todos los puertos que son DP o RP se ponen en estado “forwarding”, el resto de puertos de deja en estado “blocking”.

-Esquema de construcción árbol STP



A continuación se detallan la causas más frecuentes por las que se puede generar un bucle en un entorno de Switching.

-Error de configuración: si por error se deshabilita Spanning Tree en un puerto en el que debería estar activo
-Duplex Mismatch: si aparece una discrepancia de negociación de este tipo en un enlace donde corre STP y el volumen de perdidas es muy alto, la perdida de paquetes BPDU puede llevar como consecuencia que STP no detecte una posible situación de bucle y se quede en modo “forwarding” en vez de “ blocking”.

-Bloqueo de interfaz: si un interfaz se bloquea en recepción, pero no es capaz de darse cuenta de que esta bloqueado, mantiene el enlace levantado, lo que provoca que quede en modo “forwarding” en vez de “blocking”.

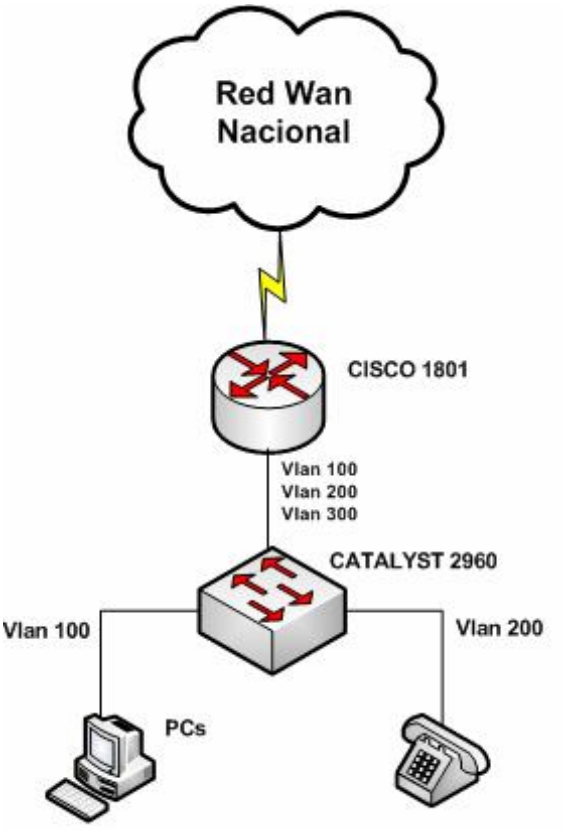
-Errores en interfaz: si surgen problemas de nivel físico y el porcentaje de tramas erróneas es muy elevado, se pueden perder muchas tramas BPDU generando una situación de bucle.

-Falta de recursos: si el consumo de CPU es muy alto, puede hacer que el router descarte tramas BPDU, con lo que se puede generar una situación de bucle. Esta situación se agravaría hasta dejar el Switch caído debido a que los bucles afectan directamente a la CPU causándole un incremento de procesos.

-Fallo de software: una incorrecta implementación de STP puede causar la aparición de bucles.

5.1.2 Escenario Sedes remotas

-Esquema topología Sedes Remotas



(En las sedes que dispongan de Gateway de Voz se encontrará conectado a la Vlan 200 de VOZ)

5.1.3 VLANs, Seguridad y Direccionamiento

Hasta ahora, en la red de cliente no había separación en el tráfico que va a través de su red, el trafico de datos viajaba conjuntamente con el trafico de voz, gestión,…etc.
Esto implica entre otras cosas la afectación del trafico de datos sobre la voz, dificultad para solventar errores o problemas en la red, falta de seguridad al contener todas las máquinas en la misma red,….

-Implementación VLAN

En una LAN que utiliza dispositivos de conmutación, la tecnología VLAN es una manera económica y eficiente de agrupar usuarios/máquinas de la red en una red conmutada lógica más allá de su ubicación física en la red.

Algunas de las características de implementar VLAN son:

-Las VLAN funcionan a nivel Capa 2 y Capa 3 del modelo OSI, por lo tanto son capaces de transportar trafico entre Switches y Routers de una misma red.
-Implementa filtrado, etiquetado e identificación de tramas
-Aísla trafico entre segmentos y aumenta ancho de banda para cada usuario mediante creación de dominios de colisión más pequeños.
-Controlan la actividad de broadcast
-Cada puerto de Switch se puede asignar a una Vlan concreta
-Mecanismo que reducen traslados físicos cuando hay cambios de ubicación de usuarios o máquinas
-Brindan seguridad a la red
-Reducción de costes relacionados con diagnostico de problemas, uso de hubs,....

Existen dos tipos de modos de configuración VLAN en cada puerto, modo “Access” y modo “Trunk”

-VLAN Access

Nos permite asignar un puerto de un Switch a una VLAN concreta, si se trata de acceso significa que solo se cursará tráfico de la VLAN concreta por ese enlace, se suele utilizar cuando conectamos dispositivos finales.

-VLAN Trunk

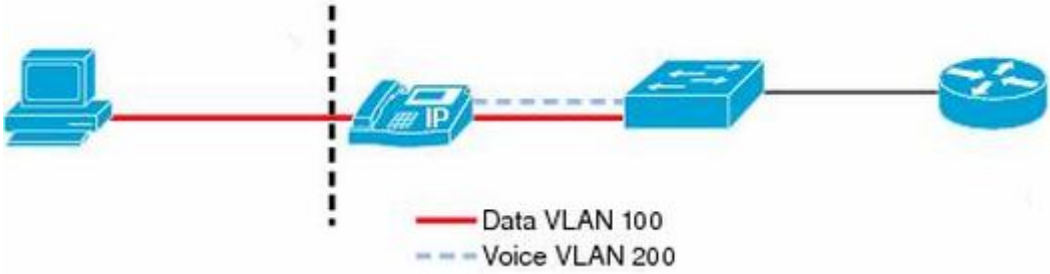
Este modo es utilizado para crear enlaces entre 2 equipos, donde pasaran varias VLANs por el mismo enlace. Es posible limitarlo por configuración para que pasen unas VLANs concretas, para distinguirlas se suelen etiquetar con el protocolo IEEE 802.1Q.

-En nuestro caso agruparemos la red con 3 Vlans diferentes:

-VLAN 100 → Tráfico de Datos
-VLAN 200 → Tráfico de Voz
-VLAN 333 → Tráfico de Gestión de Switches

En las conexiones con dispositivos finales las VLAN estarán configuradas en modo Acceso, y en los enlaces entre Switches y Router se pasaran en modo Trunk.

A excepción de que queramos conectar en el mismo enlace final un PC (Vlan Datos) y un Telefono IP (Vlan Voz), para este caso CISCO permite la funcionalidad "VLAN VOICE" para facilitar en gran parte la configuración y la convivencia de ambos.



-Seguridad

El cliente podrá conectar su electrónica en los Switches tanto de Datos como de ToIP, pero hay que tener en cuenta que debemos proveer de seguridad en las conexiones finales dado que un problema generado en la LAN del cliente podría extenderse por toda la red afectando al ISP incluso.

Algunos de estos mecanismos de CISCO en cuanto a Switches de Acceso para aumentar la seguridad en la red que aplicaremos són:

-Separación en VLANs (Explicado anteriormente)

-Port Security: funcionalidad que permite retener las direcciones MAC conectadas a un puerto y permitir solamente a esas direcciones la comunicación a través de ese puerto del Switch.
Permite restringir el acceso según la MAC, el número de maquinas conectadas, realizar acciones en función de las diferentes violaciones anteriores,…

-Storm Control: mecanismo para prevenir tráfico que viene por un puerto originado por un broadcast, multicast o unicast. Para esto se determinan

unos humbrales de tráfico donde el switch deberá bloquear el puerto evitando cualquier amenaza.

-BPDU Guard: permite limitar y asegurar el dominio de STP evitando cualquier conexión de nuevos switches o dispositivos de cliente a la red en los que corra spaning tree. En cuanto se habilita BPDU Guard en un puerto, si este recibe tramas BPDU automáticamente deshabilita el puerto.

-TACACS+ / Radius autenticacion: aporta restricciones de acceso al equipamiento de usuarios no autorizados

*(Se incluye configuraciones en ANEXO)

-Direccionamiento

A nivel 3, el direccionamiento también será modificado para añadir dos rangos más adicionales al que actualmente tiene el cliente y utiliza para tráfico de datos

-Red 192.100.0.0/20 → Tráfico de Datos
-Red 192.200.0.0/20 → Tráfico de Voz
-Red 192.300.0.0/22 → Tráfico de Gestión de Switches

Los rangos son bastante más grandes y permiten más máquinas de las necesarias, esto se deja así para prevenir posible crecimiento de la empresa y mejorar escalabilidad.

5.2 Ventajas de solución implementada

-Segmentación de la red para separación de diferentes tipos de tráfico a través de direccionamientos e implementación de VLANs

-Seguridad, se incrementa la seguridad de la red con algunas funcionalidades del fabricante CISCO que permite aplicar en los Switches Catalyst.

-Ahorro de costes, a partir de ahora el cliente no necesitará infraestructura de LAN ni recursos para la interconexión de sus equipos finales.

-Sustitución de todo el equipamiento de Switches nivel 2 de cliente por Switches de nivel 3

Algunas ventajas se muestran en la siguiente tabla:

CARACTERISTICAS	SWITCHES DE CAPA 2	SWITCHES DE CAPA 3
CONTROL DE TRÁFICO	Solo puede contener colisiones, pero **no hay un control de tráfico** de paquetes Broadcast o Multicast. En cuanto se presente una ráfaga de este tipo de tráfico la red se puede colapsar.	Existe un control de tráfico eficiente y de manera nativa. Este tipo de Switches previenen el colapso de la red, ante la presencia de tormentas de Broadcast y manejan eficientemente el tráfico multicast.
ESCALABILIDAD PARA EL SOPORTE DE NUEVAS APLICACIONES	Prácticamente no hay escalabilidad en un Switch de Capa 2, pues no cuenta con la inteligencia para "detectar" los tipos de trafico que se presentan en las redes switcheadas actuales. Aunque exista un "upgrade" por software para convertirlo a Capa 3, esto no es eficiente pues requiere de procesadores de uso general, mas un sistema operativo, lo cual se refleja en el pobre rendimiento medido en paquetes procesados por segundo, que un switch de Capa 3 de este tipo tiene.	Aplicaciones que hoy en día se instalan en las redes actuales como Voz sobre IP, Multimedia para videoconferencia en PC's conectadas en red. Calidad de Servicio y Manejo de los Recursos de Red, demandan mayor capacidad e inteligencia en las redes switcheadas. Un switch de Capa 3 viene preparado para el manejo de este tipo de ambientes.
RENDIMIENTO EN EL MANEJO DEL TRÁFICO DE LA RED	Un Switch de Capa 2 conectado a un Switch Central de Backbone, no puede discriminar cuando una conexión de Capa 3 tiene lugar localmente en el mismo switch, pues cuando se presente esta situación, el Switch de Capa 2 transfiere todos los paquetes hacia el Switch de Backbone, consumiendo innecesariamente recursos y tiempo en el backbone.	Un Switch de Capa 3 es capaz de identificar si el tráfico que arriba a sus puertos tiene que ser switcheado en Capa 2 o Capa 3, y si éste debe de tratarse de manera local, o switchearlo al backbone. De esta manera este equipo toma la decisión de manejarlo con sus propios recursos, sin consumir ancho de banda ni generar tráfico innecesario en el backbone.
MANEJO DE REDES VIRTUALES	Un switch de Capa 2 solo puede manejar Redes Virtuales a nivel de Capa 2, por lo tanto, cuando se configuren VLANs en este switch, este switch no puede pasar (rutear o switchear), tráfico de una VLAN a otra en el mismo switch, y tiene que enviar dos veces los paquetes hacia el switch central, consumiendo ancho de banda, generando tráfico innecesario, y consumiendo tiempo de procesamiento en el switch Central.	Un switch de Capa 3, puede switchear o rutear tráfico entre cualquier VLAN que haya sido definida en el Switch.
SEGURIDAD	Un Switch de Capa 2 no cuenta con mecanismos de seguridad en la red. Cualquiera puede conectarse a sus puertos y generar cualquier tipo de tráfico, e inclusive puede "escuchar" información sensible que este viajando por la red, como passwords y/o claves de seguridad, así como información confidencial, o simplemente "saturar" la red, provocando el colapso de la misma. Con un simple generador de tráfico tipo "shareware", se puede conseguir esto.	Un Switch de Capa 3 tiene todos los niveles de control y seguridad con los que un ruteador normalmente cuenta. Existen mecanismos de seguridad para prevenir que un usuario indeseado se conecte a la red, incluso a nivel físico. Estos switches pueden filtrar información no deseada incluso de los usuarios que tienen permitido el acceso a la red, para prevenir ataques a servidores, bases de datos, o proteger aplicaciones con ciertos niveles de seguridad. También cuentan con mecanismos de protección para evitar que un usuario no deseado pueda infiltrarse a la configuración del switch.
TOLERANCIA A FALLAS	Un Switch de Capa 2 no cuenta con muchos mecanismos para tolerancia a fallas, normalmente no cuenta con enlaces redundantes, y si los tiene, solo puede hacer uso de Spanning Tree, que es un protocolo lento y no distingue inteligentemente entre las rutas de respaldo, hacia donde debe enviar el tráfico. Tampoco puede agregar "ancho de banda" entre diferentes puertos, en caso de ser necesario, lo cual es otra característica de su pobre escalabilidad.	Un Switch de Capa 3 cuenta con variados mecanismos de control de fallas y de respaldo tanto de Capa 2 como de Capa 3. Protocolos como VRRP, ESRP y OSPF se utilizan hoy en día, para manejar eficientemente las rutas de respaldo. Con estos protocolos, los switches de Capa 3 participan de los mecanismos de control de fallos en los enlaces, junto con los ruteadores para recuperar rápida e inteligentemente la conexión entre los recursos de la red. Un switch de Capa 2, sencillamente no tiene capacidad para hacer esto.
TENDENCIAS TECNOLÓGICAS	Todos los fabricantes de tecnologías de información, así como de productos de comunicaciones para redes, están de acuerdo que mientras más "inteligente" es un dispositivo de red, funciona y se controla mejor, y la tecnología viene avanzando que este tipo de switches no solo son inteligentes sino muy rápidos, gracias a la tecnología de ASICs, que emplea circuitos integrados diseñados específicamente para las funciones de Switcheo, y esto los hace más rápidos que un Switch de viejas arquitecturas basadas en procesadores de uso general. Los switches de capa 2 cada vez más están en desuso dado que no están preparados para las demandas de aplicaciones del tipo Intranet o de interacción con la Internet.	Un Switch de Capa 3 cuenta con la suficiente "inteligencia" para interactuar con el tráfico que va o viene de la Internet, y participa con ella en el manejo eficiente de los diferentes tipos de tráfico como Voz sobre IP por ejemplo, que ya es una realidad. Un switch de Capa 2 simplemente no tiene nada que hacer al respecto. Además, a un Switch de Capa 3 se le pueden agregar funcionalidades que van más allá de la Capa 3, como Server Load Balancing, por ejemplo. Un Switch de Capa 3 tiene la capacidad para distinguir cuando los puertos donde se conectan los servidores de la empresa están, ocupados, saturados o caídos, de tal manera que pude reenviar eficientemente el tráfico y las peticiones de los usuarios de la red, hacia aquellos puertos que puedan responder. Un Switch de Capa 2, no entiende este concepto y en el caso de que se presente esta situación, no hacen más que reintentar y retransmitir, generando más tráfico y empeorando la situación. La tendencia tecnológica es así como de switcheo en Capa 3, están sustituyendo a los switches de Capa 2, por sus rendimientos, sus altas funcionalidades, sus mecanismos redundantes y de tolerancia a fallas, su mejor control y su escalabilidad. Eventualmente una empresa que requiera de nuevas aplicaciones, que demande comunicación hacia y de la Internet, y que requiera de altos mecanismos de seguridad, tendrá que migrar hacia el switcheo de Capa 3.

5.3 Equipamiento en Sedes Centrales (CPDs) y Sedes Remotas

CATALYST 2960-P

Catalyst 2960-24PC-L

Catalyst 2960-48PST-L

Se implementaran los modelos de 24 puertos en Sedes remotas y los modelos de 48 puertos en las Sedes Centrales

-<u>Descripción</u>:

La serie de switches Catalyst 2960 proveen de facilidades mejoradas respecto otros modelos, alta seguridad, sostenibilidad mejorada, y experiencia en networking sin fronteras. Estos dispositivos están diseñados para interconexión de redes en empresas, mercado medio y oficinas.

-<u>Especificaciones</u>:

Las especificaciones tecnicas más destacadas de esta gama de Switches para nuestro proyecto son:

- 24 o 48 puertos Gigabit Ethernet para dar conectividad
- 20 Gbps de throutghtput (Paquetes totales que conmuta y envia por segundo)
- PoE, alimentacion Power over Ethernet con mas de 30W por puerto. Esto nos permitira prescindir de alimentadores externos para los Terminales IP, facilitando su instalación y hubicación.
- Una amplia gama de funcionalidades software y una larga experiencia en implantación de resdes
- Garantia de por vida limitada en hardware, incluyendo soporte tecnico siempre disponible.

-**Funcionalidades:**

Esta gama de Swtches dispones de las siguientes funcionalidades:

- Automatic QoS (AutoQoS)
- Stacking Master configuration management
- Dynamic Host Configuration Protocol (DHCP)
- Auto-negotiation
- Dynamic Trunking Protocol (DTP)
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Automatic media-dependent interface crossover (MDIX)
- Unidirectional Link Detection Protocol (UDLD)
- Switching Database Manager (SDM)
- Local Proxy Address Resolution Protocol (ARP)
- Internet Group Management Protocol (IGMP)
- Multicast VLAN Registration (MVR)
- Per-port broadcast, multicast, and unicast storm control
- Voice VLAN
- Cisco VLAN Trunking Protocol (VTP)
- Remote Switch Port Analyzer (RSPAN)
- Remote Monitoring (RMON)
- Layer 2 traceroute .
- Trivial File Transfer Protocol (TFTP)
- Network Timing Protocol (NTP)
- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP source guard
- Flexible authentication
- Open mode
- Integration of device profiling technology and guest access
- RADIUS Change of Authorization and downloadable calls
- 802.1X Supplicant with Network Edge Access Transport (NEAT)
- Private VLANs
- Private VLAN Edge
- Multidomain Authentication
- Port-based ACLs
- Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3)
- Switched Port Analyzer (SPAN)
- TACACS+ and RADIUS authentication
- MAC Address Notification
- Multilevel security on console access
- Bridge protocol data unit (BPDU) Guard

- Spanning Tree Root Guard (STRG)
- IGMP filtering
- Dynamic VLAN assignment

De todas estas funcionalidades, vemos cuales son las más destacadas en la implantación del proyecto con algo más de detalle:

- **Automatic QoS (AutoQoS**) simplifica la configuracion de QoS detectando los terminals Cisco IP Phones, clasificando el trafico y configuranod las politicas de encolamiento en el Switch

- **Automatic media-dependent interface crossover (MDIX**) el equipo ajusta los pares de transmission independientemente si el cable conectado es de tipo cruzado o plano, por lo tanto evitamos problemas de conectividad cuando el cliente no utilize el cableado adecuado al conectar su electronica a nuestro Switch.

- **Per-port broadcast, multicast, and unicast storm control**: previene tormentas de broadcast generadas por dispositivos finales de cliente, filtrando estas en los puertos para que no se propaguen por la red y tengan una mayor afectación.

- **Voice VLAN:** funcionalidad que simplifica la instalacion de telefonos IP, manteniendo el trafico de voz en una Vlan separada para facilitar la administracion y el troubleshooting.

- **Monitoring (RMON)** agente software para el tratamiento y monitorización de alarmas, estadisticas y eventos del equipo.

- **Port Security:** brinda seguridad de acceso a los puertos, limitando el numero de direcciones MAC aprendidas y evitando cualquier possible ataque “Mac flooding”

- **VLANs Privadas:** proporciona segmentacion restringiendo el trafico entre máquinas en el mismo segmento, separando el trafico a nivel 2 a través de Vlans

- **TACACS+ / Radius autenticacion:** aporta restricciones de acceso al equipamiento de usuarios no autorizados.

- **Bridge Protogol Data Unit (BPDU) Guard:** previene bucles de nivel 2, deshabilitando los interfaces en los que recibe paquetes BPDU cuando no deberia.

6 SOLUCION COMUNICACIONES DE TELEFONIA IP (ToIP)

Una vez vistas las necesidades del cliente para la red de comunicaciones de Telefonia IP, las modificaciones a aplicar serán las siguientes.

-Sustitución de servidor de llamadas Call Manager v.3.0 obsoleto por cluster de servidores Call Manager v.7.1

-Eliminación de adaptadores ATA y sustitución de terminales analógicos por teléfonos IP, se realiza un incremento del número de telefonos.

-Implementación de sistema de redundancia SRST en Gateways de Voz existentes para Valencia, Zaragoza y Vigo

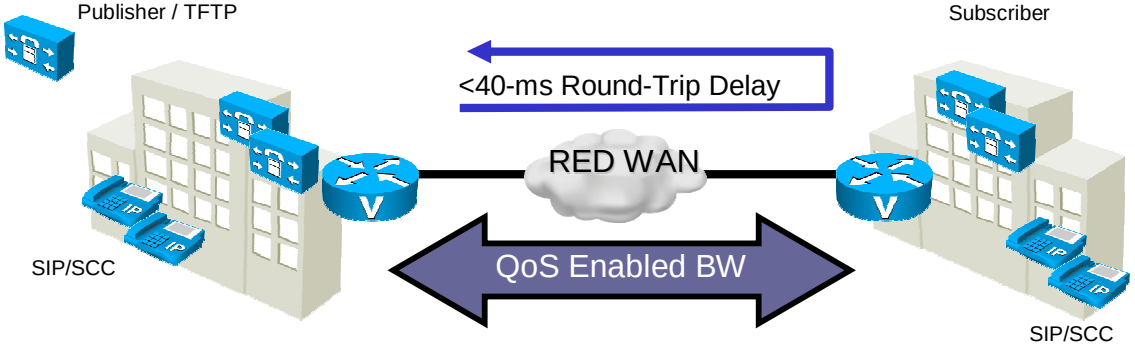
6.1 Arquitectura de la solución

La solución de comunicaciones ToIP constará de un cluster de dos servidores Call Manager v.7.1, con licencias necesarias para dar servicio a todas las extensiones del cliente. Adicionalmente se instalaran 900 terminales Cisco ToIP repartidos entre todas las delegaciones.

Las funciones básicas del Call Manager son

-Procesado de llamadas
-Señalización y control
-Administración del Dial plan
-Prestaciones de los teléfonos
-Servicios de Directorio
-Programación de interfaces para aplicaciones externas
-Incluye una herramienta de backup-and-restore DSR (disaster recovery system)

El cluster se implementará sobre la red wan nacional, ésta será la encargada de transportar las comunicaciones del servidor y la señalización.



Este diseño implica:

- 40-ms round-trip delay en cualquiera de los CCM del cluster para mantener la BB.DD. activa
- Hasta ocho dependencias remotas en el cluster
- Tolerancia a fallos sobre la WAN

Los servidores implicados en el cluster serán Publisher, Subscriber y servidor TFTP, con la siguiente distribución geográfica.

- Publisher + TFTP + Subscriber backup ubicado en CPD Barcelona
- Subscriber principal ubicado en CPD Madrid

Por otra parte se mantendrán los Gateways de voz ya existentes en sus actuales localizaciones.

-Al tratarse de una red entre 500 y 1000 usuarios (A previsión de futura expansión de la empresa):

-El Publisher es el nodo de backup del único Suscriber
-Se debe crear un CallManager Group con el Suscriber como primera opción y después en Publisher.
-Se debe asignar este grupo a todos los dispositivos de la red. El servidor TFTP se debe activar en el Publisher.

A continuación se detalla el funcionamiento de cada equipo

Publisher

-Hay uno por clúster. Es el primero en instalarse y proporciona el servicio de base de datos al resto de miembros del clúster.

-El Publisher es el único servidor que tiene acceso a la configuración de la base de datos. Cuando la configuración cambia se produce una copia de base de solo lectura en el resto de los miembros el clúster.

-En sistemas de más de 1250 usuarios, Cisco recomienda un Publisher dedicado para prevenir que las operaciones administrativas afecten a los usuarios.

-Si el Publisher no es accesible, los servidores del clúster usan la copia de la base de solo lectura que tienen en su disco duro. Las siguientes operaciones no se pueden realizar:

- Cambios en las llamadas establecidas (Call forwarding changes)
- Operaciones que requieran el servicio de licencias.
- Cambios en la configuración
- Logar o desloar extensiones móviles

-Las extensiones móviles no pueden funcionar sin el Publisher ya que requieren el acceso a la base de datos, por lo que Cisco recomienda instalar este servicio solo en el Publisher.

-La elección de la plataforma hardware del Publisher se basa en el tamaño y rendimiento del clúster, debe tener la misma capacidad que los Subscribers. Lo ideal es que sea un servidor con alta disponibilidad, para minimizar el impacto por fallo del hardware.

Subscriber

-Un Call Processing Subscriber es un servidor que tiene permitido el servicio Cisco CallManager. Todos los subscribers deben suscribirse en el Publisher para obtener una copia de solo lectura de la base de datos de información

-El Cisco CallManager Service no puede darse de alta si el publisher no esta accessible, ya que el publisher actua como servidor de licencias

-Dispositivos tales como telefonos, gateways, y media resources pueden registrase y realizar llamadas solo en los subscribers

-Cisco Unified CM 7.1 soporta hasta ocho servidores en un cluster, con el servicio Cisco CallManager Service.

-En un cluster de gran tamaño o alto rendimiento, el servicio de procesamiento de llamadas no se debe habilitar en el publisher y el servidor TFTP

Servidor TFTP

-El servidor TFTP realiza dos funciones principales:

- Fuente de ficheros para servicios tales como MoH, ficheros de configuración para los dispositivos (teléfonos y gateways), ficheros binarios para el upgrade de los teléfonos y algunos gateways, y varios ficheros de seguridad.
- Generación de ficheros de configuración y seguridad. La mayor parte de los ficheros generados por el servicio TFTP son firmados y en algunos casos encriptados antes de que se puedan descargar.

-El servicio TFTP se puede habilitar en cualquier servidor del clúster.

-Para más de 1250 usuarios, con extensiones móviles u otros servicios que causen cambios de configuración, Cisco recomienda un servidor específico para el servicio TFTP, ya que otros servicios se pueden ver afectados en los cambios de configuración.

-No hay restricción en el numero de servidores que pueden tener el servicio TFTP, sin embargo Cisco recomienda la utilización de 2 servidores TFTP para clústers grandes, de este modo se proporciona redundancia.

-Cuando se cambia la versión del Unified CM clúster, Cisco recomienda que se cambie la versión de los servidores TFTP después del Publisher y antes que cualquier otro servidor

Gateway de Voz

-Instalados en las dependencias centrales y sedes remotas

-Proporcionan la interconexión con el mundo de la telefonía tradicional (redes públicas y PBXs).

-Se recomienda tener un Gateway de voz dedicado

-N interfaces digitales PRI conectados:

- Red Pública o GSM
- PBX (Q.SIG, Euro-ISDN)

-Tarjetas HW con DSPs para codificación de llamadas y transcoding para multiconferencias.

-Se controla desde el CCM mediante el protocolo MGCP. La configuración de enrutamiento de llamadas reside en el CCM.

-Gestionable como router de 2º nivel.

6.2 Ventajas de solución implementada

Las ventajas que implica la implementación del Cluster CCM son

-Un único punto de administración para los usuarios de todas las sedes dentro del cluster

-Movilidad de las extensiones dentro del cluster

-Dial plan (Plan de marcado) unificado

-Ahorro de costes de llamadas a la PSTN por el uso de la Red Wan

-La máxima utilización de ancho de banda disponible por permitir tráfico de voz que comparte la IP WAN con otros tipos de tráfico.

-Soporta fallo a través de la Red wan. (Redundancia geográfica)

Algunas otras ventajas son:

-Convergencia del tráfico de voz y datos en una misma red

-Nuevas funcionalidades en la telefonía, con los teléfonos IP se aprovechan muchas funciones que hasta ahora no era posible implementar

-Redundancia ante caídas de Primarios e implementación del modo supervivencia SRST para la sedes con Gateway Local.

-Redundancia ante perdidas de base de datos mediante copias de seguridad

6.3 Equipamiento en Sede Central (CPDs) y Sedes Remotas

CPD Barcelona

Se deberá instalar el siguiente equipamiento:

-Servidor Call Manager con funciones de Publisher+ TFTP+ Subscriber de backup

-200 Teléfonos 7911

-25 Teléfonos 7962

CPD Madrid

Se deberá instalar el siguiente equipamiento:

-Servidor Call Manager con funcion de Subscriber
-200 Telefonos 7911
-25 Telefonos 7962

Sedes Remotas

Se deberá instalar el siguiente equipamiento en las 150 delegaciones restantes:

-3 Teléfonos 7911 para cada Sede (Total 450 Telefonos)

-SERVIDORES CALL MANAGER (MCS7816-K9-CMC2)

-Descripción:

Cisco Unified Communications Manager (CUCM), se trata de una parte integral de una completa arquitectura para una nueva generación de soluciones de comunicaciones de calidad. Esta potente plataforma brinda el alto rendimiento y disponibilidad que una red empresarial necesita hoy en dia.
Cisco Unified Communications Manager es altamente operacional desde su arranque, necesitando la entrada minima de configuración como la dirección IP y dominio.

-<u>Especificaciones</u>:

Las especificaciones tecnicas más destacadas de este servidor para nuestro proyecto son:

- 2 Discos duros en raid, eficaz ante problemas con almacenamiento
- 2 tarjetas Ethernet para redundancia de conectividad LAN
- Funciones de Seguridad, entre otras password de arrancado, IPMI (Intelligent Plattform Management Inferface), seguridad de administrador,…

-<u>Funcionalidades y capacidades</u>:

De todas las funcionalidades, vemos cuales son las más destacadas

- Fiabilidad
- Bajo coste para el propietario
- Soporte estandar del equipamiento por personal de Cisco
- Escalabilidad para mas de 40.000 usuarios (al principio se da servicio a 900 usuarios)
- Facilidad de telepresencia, para la realización de reuniones de manera remota, evitando costes de desplazamiento del personal entre otros.
- Simplificacion de la provision y mantenimiento de los sistemas de voz
- Facilidad de movilidad, hacen posible el desplazamiento del personal con su extension independientemente de su localización física.
- Unificacion, es posible disponer de la mayoria de necesidades básicas para toda una empresa solo con un servidor (voz, video, movilidad, mensajeria,...)

-CISCO IP PHONE 7911-G

-<u>Descripción</u>:

El Cisco Unified IP Phone 7911G cubre las necesitades para cualquiera que lleve a cabo un tráfico moderado de voz.

Cuatro teclas de función dinámica guían a los usuarios a través de las funciones principales y facilidades, mientras una pantalla combina funcionalidades intuitivas, información de llamada, y un servicio extenso lenguaje de marcado (XML) para usuarios más expertos.

-<u>Especificaciones</u>:

Las especificaciones tecnicas más destacadas de este terminal para nuestro proyecto son:

- Posibilidad de Upgrade de software del terminal ante mejoras o problemas
- Facilidad de alimentación a través de PoE
- Soporte de temperaturas relativamente extremas (0 a 40º), podemos situar los terminales independientemente del clima ambiental. (Especialmente si se trata de fabricas,…etc)

-<u>Funcionalidades</u>:

- Disponibilidad de Display y manejo de funcionalidades
- Protocolo CDP de Cisco para facilitar instalacion y configuración
- Facilidad de Switch para la interconexión de un PC al teléfono como dispositivo final

- Soporte de diferentes codecs (G.711a, G.711, G.729a, G.729b,...)
- Soporte protocolo Skinny (SCCP) de señalización, propietario de Cisco
- Sistema de deteccion de voz de alta calidad (VAD)
- Configuración de parametros del terminal a través del protocol DHCP
- Funcionalidades de Seguridad (Certificados, encriptación,...)

-CISCO IP PHONE 7962-G

-<u>Descripción</u>:

El Cisco Unified IP Phone 7962G es un teléfono IP muy completo en cuanto a funcionalidades, con un altavoz y auricular diseñado para audio con banda ancha. Intenta satisfacer las necesidades de los directores y administrativos.

Posee seis botones luminosos programables y cuatro teclas de función interactivas que te guían a través de todas las características y opciones en las llamadas.

El teléfono dispone de una pantalla LCD que brinda funcionalidades como fecha y hora, persona llamante, persona llamada, dígitos marcados e información de presencia. Un altavoz manos libres y auricular diseñados para alta fidelidad de audio son estandars en el Cisco Unified IP Phone 7962G

-<u>Especificaciones</u>:

Las especificaciones tecnicas destacadas de este terminal para nuestro proyecto son las mismas que el modelo IP Phone 7911-G

-<u>Funcionalidades</u>:

Las funcionalidades son las mismas que el modelo IP Phone 7911-G añadiendo algunas más, al tratarse de un terminal de gama más alta, entre otras:

- Display de gran tamaño (12,5 cm) y alta resolución (320x222)
- Altavoz (manos libres), con cancelador de eco
- Acceso directo al buzon de voz y a funcionalidades del terminal
- Soporte modulo expansion 7914, permite añadir un panel con 14 botones adicionales para la programación de extensions o speed dials (Ideal para telefonos de operadora)
- Soporte DSCP para implementación de QoS
- Seguridad, es posible programar el terminal para el uso de encriptación mediante AES-128 en la comunicacion contra el Call Manager.
- Terminal dispone de 30 idiomas diferentes

6.4 Enrutamiento de llamadas

El encaminamiento de las llamadas será que el cliente

- <u>Llamadas dentro de la red de cliente</u>

  -Las llamadas entre Sedes y por lo tanto dentro de la red de cliente, se encaminaran a través de la red de datos como tráfico ToIP.

- <u>Llamadas al exterior de la red de cliente</u>

  -Las llamadas con destino numeración fija y numeración móvil deberán encaminarse a través de los accesos primarios localizados en los Gateways de Voz.

-Si se trata de una Sede con Gateway propio (CPDs, Valencia, Zaragoza o Vigo) , utilizará su propio equipo para las llamadas salientes.

-Si se trata de las Sedes que no disponen de Gateway propio, se repartirán en grupos de forma equitativa el enrutamiento entre las que sí disponen de Gateway

- Llamadas al interior de la red de cliente

-Las llamadas entrantes a la red de cliente se encaminaran directamente a través de la numeración de los primarios localizados en los Gateways de voz

6.5 Contingencia y redundancia del servicio

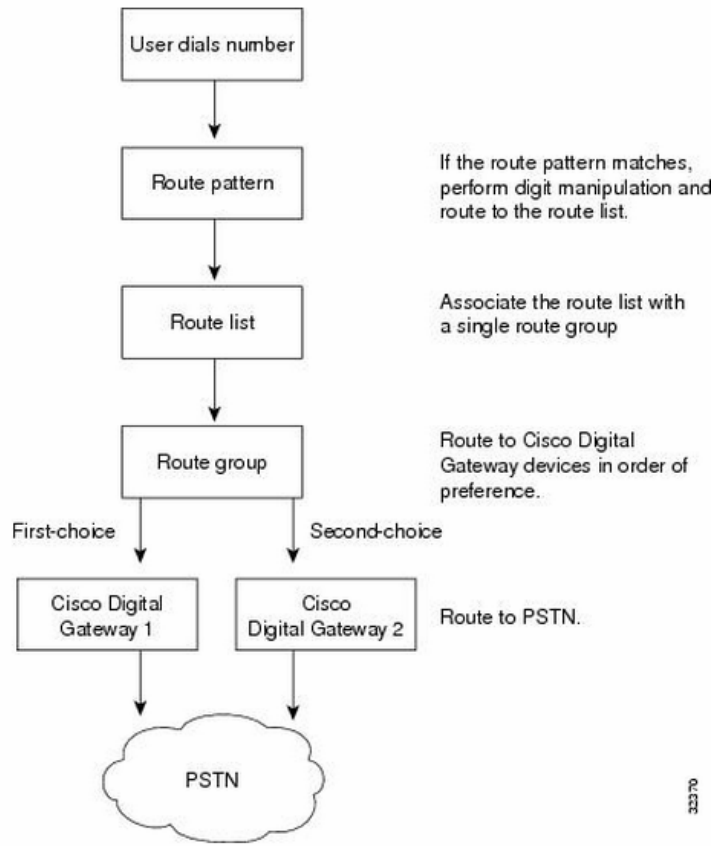
Existen diferentes mecanismos implementados para dar contingencia y redundancia al servicio de Telefonía IP.

-**REDUNDANCIA DE PRIMARIOS**

En caso de caída de un primario de un Gateway en una Sede, lo que se debe de hacer es encaminar las llamadas de dicha Sede por otro Gateway diferente. Esta funcionalidad la permite aplicar directamente el Call Manager a través de los “Route Group” en el plan de marcado (Route Plan), esto permite la distribución de llamadas entre los diferentes Gateways a través de varios algoritmos, y uno de ellos que se puede configurar es que en caso de que no pueda cursar esa llamada por la ruta primaria, la realice por una ruta secundaria.

*Por lo tanto en nuestro caso se configurá una ruta secundaria (RG) para todas las Sedes Remotas para que vayan por los Gateways de los CPDs en caso de caída de su Gateway local. Y para el caso de los CPDs se darán redundancia entre ellos.

Figure 16-2 Route Plan Summary Diagram for Cisco Digital Gateways



-REDUNDANCIA DE SERVIDORES

El cluster de Call Managers dispone de redundancia geográficamente, tenemos la siguiente distribución

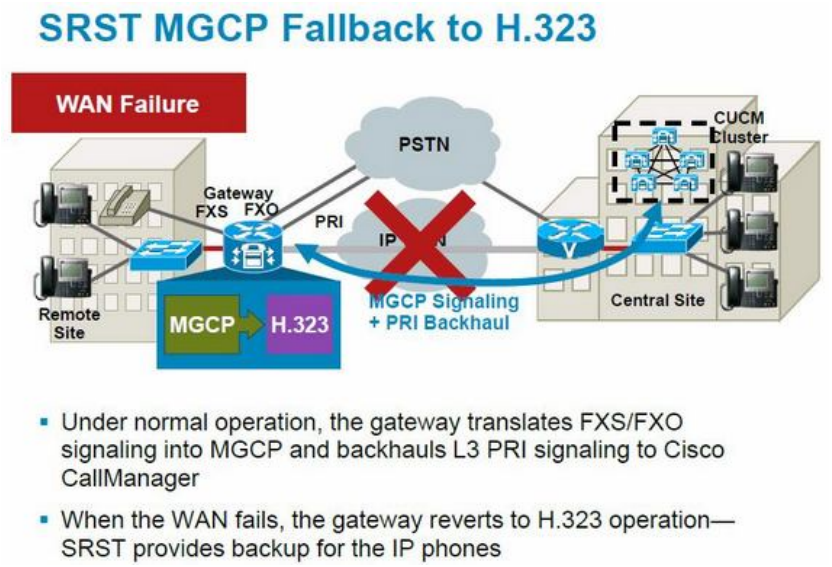
- Publisher + TFTP + Subscriber backup ubicado en CPD Barcelona
- Subscriber principal ubicado en CPD Madrid

Por lo tanto en caso de caída del Subscriber Principal, el Subscriber de Backup asume las funciones de servidor de llamadas, registrando todos los teléfonos.

-SISTEMA SRST

El sistema SRST (Servible Remote Site Telephony) de CISCO permite que en caso de que una Sede pierda la comunicación con el Call Manager debido a una caída de la Wan por ejemplo, el Gateway de voz local asume unas

funcionalidades mínimas de Servidor de llamadas actuando de manera independiente como centralita y dando servicios mínimos a los teléfonos.



*Esta funcionalidad solo podremos utilizarla en las sedes que dispongan de Gateway de voz local

-**SISTEMA DRS**

El sistema DRS (Disaster Recovery System), proporciona un backup completo de la base de datos principal del Call Manager y su recuperación para cualquier servidor que pertenezca al cluster del Call Manager.

Esta sistema incluye las siguientes funcionalidades:

-Interfaz de usuario para la configuración de backups y recuperación de los mismos

-Un sistema distribuido para la realización de backups y posibilidad de programar copias en una fecha concreta.

-Almacenamiento de copias de seguridad o backups en un dispositivo físico o servidor SFTP remoto.

-Obtención de una red de Telefonía IP total, eliminando equipamiento analógico y obsoleto. También se eliminan los terminales ATA, posible punto de fallo intermedio.

7 PRESUPUESTO

A continuación se detalla el presupuesto de la solucion ofertada de todos los servicios de manera conjunta y desglosada.

			UNIDADES	PRECIO € (Unidad)	TOTAL
MODIFICACION RED WAN DATOS					
MODIFICACION CAUDALES WAN					
	Alta de caudal 25% Multimedia Sedes		150	35	5250
	Alta de caudal 10% Multimedia Centrales		4	50	200
CAMBIO PROTOCOLO ROUTING					
	Reconfiguracion de protocolo RIP a BGP		154	20	3080
EQUIPAMIENTO HARDWARE					
	Juniper EX4200		2	2500	5000
	Instalacion y configuración del equipamiento		2	50	100
OTROS					
	Mantenimiento Anual del equipamiento		2	50	100
SUBTOTAL					13730
SOLUCION COMUNICACIONES DE DATOS EN LAN					
EQUIPAMIENTO HARDWARE					
	SEDES CENTRALES				
	Swtich Catalyst 2960- 48 Puertos		7	700	4900
	Instalacion y configuración del equipamiento		7	20	
	SEDES REMOTAS				
	Swtich Catalyst 2960- 24 Puertos		150	500	75000
	Instalacion y configuración del equipamiento		150	20	3000
OTROS					
	Mantenimiento Anual del equipamiento		157	20	3140
SUBTOTAL					86040
SOLUCION COMUNICACIONES DE TELEFONIA IP					
EQUIPAMIENTO HARDWARE					
	SEDES CENTRALES				
	Servidores de llamadas CCUM Call Manager MCS7816-K9-CMC2		2	4000	8000
	Pack Licencias para 100 Terminales ToIP		10	200	2000
	Telefono Cisco IP PHONE 7911-G		400	80	32000
	Telefono Cisco IP PHONE 7962-G		50	150	7500
	Instalacion y configuración del equipamiento		462	9	4158
	SEDES REMOTAS				
	Telefono Cisco IP PHONE 7911-G		450	80	36000
	Instalacion y configuración del equipamiento		450	9	4050
RECONFIGURACION GW (SRST)					
	Preparacion y reconfiguracion de Gateways 2801 para funcionalidad SRST		3	100	300
OTROS					
	Mantenimiento Anual del equipamiento		912	10	9120
SUBTOTAL					103128
TOTAL					**202.898**
					€ (Euros)

(Los precios son orientativos debido a que algunos fabricantes no venden equipamiento si no es a través de un proveedor de servicios)

8 CONCLUSIONES

Durante este proyecto se ha implementado una solucion unificada de servicios de Switching y Telefonia IP sobre una plataforma ya existente, la red Wan de la que dispone una gran empresa a nivel nacional.

Para esto se ha realizado un analisis completo sobre la red de cliente y su equipamiento, para posteriormente ver las soluciones mas adecuadas en función de las necesidades que se nos exponen, es importante remarcar las modificaciones necesarias que hay que realizar para que la red actual trabajando como base, soporte con fiabilidad las nuevas implementaciones sobre esta.

A nivel personal, al realizar un proyecto de varios servicios uno se da cuenta de la complejidad y trabajo que supone la implementacion de cambios cuando se trata de una red tan amplia y con sus propias particularidades, todos estos cambios se ven reflejados en varios niveles diferentes (Capa OSI), donde unos dependen directamente de otros.

Entre otros:

-Nivel 1 Fisica -> Cambios físico, sustitución de equipamiento, cableado…
-Nivel 2 Enlace de datos -> Implementacion de Vlans, port-security,..
-Nivel 3 Red -> Cambios de direccionamiento, protocolo de routing,..
…

La importancia del buen seguimiento y preparacion para realizar cualquier modificación es vital, priorización y orden en las fases (diagrama de Grant) ,tratamiento de compatibilidades de todo el hardware y software, viendo la necesidad de brindar al cliente lo que requiere, una solución que sea eficiente, unificada y en un tiempo establecido previamente.

De cara a futuros proyectos posteriores, se presenta la posibilidad de gestionar cualquier nuevo equipamiento de la electronica de cliente, una vez gestionada la solucion de Switching los cambios deberian ser minimos para integrar cualquier dispositivo (Pcs, impresoras, servidores...) , se ha conseguido un nivel alto de escalabilidad.

Por otra parte al disponer ya de una plataforma unica de telefonia, tambien será posible implementar nuevas funcionalidades como Videoconferencias, Servidores destinados a mensajeria (Buzon de voz), Call Centers, móviles corporativos, Tarificadores...

Tambien hay que añadir la importante mejora en cuanto a disponibilidad de las soluciones, aumentando la seguridad e incluyendo sistemas de redundancia.

Aunque a priori se muestre una inversión importante de capital, se amortizará con el tiempo debido a la relevancia y criticidad de los servicios que el cliente ofrece, y la necesidad de disponer de una red integrada, fiable y escalable.

El proyecto remarca la tendencia a la integración y unifiacion en un solo proveedor de servicios, algo que resulta tan bueno e interesante para cliente como para el ISP
Por una parte al cliente le resultará mas económico el mantenimiento global de una solución completa y dispondrá de un interlocutor único de relación para cualquier modificación y/o averia.

De cara al proveedor se facilita el mantenimiento de los servicios llegando más allá de los Routers que interconectan con la red Wan y pudiendo realizar una monitorización y un tratamiento de los problemas más exhaustivo, todo esto conlleva una via de negocio muy rentable y por explotar para muchos ISPs debido a que la inversión de infraestructura para la gestión de nuevos servicios es relativamente mínima una vez ya se dispone de una red wan desplegada sobre un cliente.

9 GLOSARIO DE TERMINOS

-**A**

AS	Autonomous System
ATA	Adaptador Telefono Analogico

-**B**

BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BW	Bandwidth

-**C**

CBWFQ	Class Based Weigthed Fair Queuing
CIDR	Classless Inter-Domain Routing
CODEC	Codificador-Decodificador
CPD	Centro de Proceso de Datos
CUCM	Cisco Unified Communications Manager

-**D**

DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processor
DSR	Disaster Recovery System

-**E**

EIGRP	Enhanced Interior Gateway Routing Protocol

-**F**

FIFO	First In First Out

-**G**

GSM	Global System Mobile

-**I**

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

-**L**

LAN	Local Area Network
LCD	Liquid Crystal Display
LLQ	Low Latency Queuing
LSA	Link State Advertisement

-**M**

MAC	Media Access Control Address
MDIX	Media-Dependent Interface Crossover
MGCP	Media Gateway Control Protocol
MoH	Music On Hold

-**O**

OSPF	Open Shortest Path First

-**P**

PBX	Private Branch Exchange
PoE	Power Over Ethernet
PQ	Priority Queuing
PSTN	Public Switched Telephone Network

-**Q**

QoS	Quality of Service
QSIG	Q. Signaling

-**R**

RADIUS	Remote Authentication Dial In User Service
RG	Route Group
RIP	Routing Information Protocol
RMON	Remote Monitoring

-**S**

SCCP	Skinny Client Control Protocol
SFP	Smart Form-factor Pluggable
SRST	Servible Remote Site Telephony
STP	Spanning Tree Protocol

-**T**

TACACS	Terminal Acces Controller Access Control System
TFTP	Trivial File Transfer Protocol

ToIP	Telephony over IP

-**V**

VAD	Voice Activity Detection
VLAN	Virtual LAN
VLSM	Variable Length Subnet Mask
VoIP	Voice over IP
VRRP	Virtual Router Redundancy Protocol

-**W**

WAN	Wide Area Network

-**X**

XML	Extensible Mark up Language

10 BIBLIOGRAFIA

-Cisco CATALYST

http://www.cisco.com/en/US/products/ps6406/index.html

-Codecs y BW

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

-CUCM Call Manager

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/data_sheet_c78-478942.html

http://www.cisco.com/en/US/products/sw/voicesw/ps556/index.html

-DRS (Disaster Recovery System)

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/drs/7_0_1/DRS_CUCM/drsag701.html

-JUNIPER

http://www.juniper.net/es/es/products-services/switching/ex series/ex4200/#overview

-Port Security

http://infodocs.net/articulo/networking/port-security-en-switches-cisco

-Protocolos Routing

http://www.sadikhov.com/forum/index.php?/forum/35-ccnp/

http://ezinearticles.com/?Network-Routing-Protocols---IGRP,-EIGRP,-OSPF,-ISIS,-BGP&id=2891289

http://librosnetworking.blogspot.com.es/2006/07/principios-bsicos-de-ripv2.html

http://www.arqhys.com/construccion/protocolos-introduccion.html

http://gilabeni.wordpress.com/2010/01/07/introduccion-a-los-protocolos-de-enrutamiento/

http://leonformacion.site90.net/pdf/protocolos_de_enrutamiento.pdf

http://vnanock.wordpress.com/2007/05/06/protocolos-de-enrutamiento-dinamicointroduccion/

-QoS

http://www.monografias.com/trabajos16/telefonia-senalizacion/telefonia-senalizacion.shtml

http://www.iponline.com.ar/es/calidad-de-servicio_QoS.php

http://es.wikipedia.org/wiki/Enrutamiento_basado_en_pol%C3%ADticas

-Route Group

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/4_1_3/ccmcfg/b03rtgrp.html
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_5_1/ccmsys/a03rp.html

-Spaning Tree

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml

-SRST

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2169/prod_qas0900aecd8028d113.html

-Storm Control

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22ea/SCG/swtrafc.html

-Switching

http://es.scribd.com/doc/87087243/Diferencia-Entre-Switch-Capa-2-y-Capa-3

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094640.shtml

-Telefonos IP

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps6565/product_data_sheet0900aecd8039de52.html

http://www.cisco.com/en/US/products/ps8536/index.html

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8536/product_data_sheet0900aecd8069bd41.html

-ToIP

http://www.telefoniavozip.com/voip/ventajas-de-la-telefonia-ip.htm

http://www.monografias.com/trabajos16/telefonia-senalizacion/telefonia-senalizacion.shtml

http://diec.unizar.es/intranet/articulos/uploads/Auditoria%20de%20VoIP:%20Analisis%20de%20la%20QoS%20objetiva%20y%20subjetiva%20en%20la%20transmision%20de%20voz%20extremo%20a%20extremo%20sobre%20un%20acceso%20ADSL.pdf

http://www.iponline.com.ar/es/calidad-de-servicio_QoS.php

-VLANs

http://www.elportal.info/etc/sem3/Cap3.txt

http://programoweb.com/71578/%C2%BFpor-que-segmentar-las-lan/

http://informatica.gonzalonazareno.org/plataforma/mod/wiki/view.php?id=3813

-VRRP

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

11 ANEXOS

ANEXO 1: CONFIGURACIONES

-**VRRP**

• La configuración de VRRP se realiza sobre la interfaz IP en cuestión. Será necesario configurar tantos grupos de VRRP como Vlans de nivel 3 (Con IP) tengamos.

En el Juniper Principal (Master para el proceso VRRP1) será la siguiente

```
interfaces {
   <Puerto_LAN_Cliente> {
      unit <ID_Unidad _Logica> {
         family inet {
            address <IP_LAN_Cliente>/<MASCARA> {
               vrrp-group <Id_Grupo_VRRP_1> {
                  virtual-address <IP_Virtual_1>;
                  priority 105;
                  preempt;
                  accept-data;
                  track {
                    interface <Interfaz_Wan>;
                  }
            }
         }
      }
   }
}
```

Donde:

<ID_Unidad _Logica> Es el identificador de la unidad logica. Si el puerto no lleva encapsulado tomará el valor 0, sino se corresponderá con el identificador de la VLAN de cliente.

<Id_Grupo_VRRP_1> Es el identificador del grupo VRRP1. Puede tomar valores entre 1 y 255. Se recomienda utilizar el valor 1.

<IP_Virtual_1> Es la dirección IP virtual del grupo VRRP1.

<IP_LAN_Cliente> Es la dirección IP de la conexión de cliente.

<Interfaz_Wan> Es el Interfaz Wan que monitorizamos, cuando cae fisicamente se realiza la conmutación mediante VRRP al backup.

• La configuración en Juniper Secundario es similar a la anterior, cambiando el valor de las prioridad en el grupo

```
interfaces {
    <Puerto_LAN_Cliente> {
        unit <ID_Unidad _Logica> {
            family inet {
                address <IP_LAN_Cliente>/<MASCARA> {
                    vrrp-group <Id_Grupo_VRRP_1> {
                        virtual-address <IP_Virtual_1>;
                        priority 100;
                        preempt;
                        accept-data;
                        }
                }
            }
        }
    }
}
```

-PROTOCOLO BGP Y METRICAS

Independientemente del protocolo de routing utilizado con el cliente (En nuestro caso BGP), desde el EDC que actúe como respaldo se anunciarán todas las redes con la Metrica configurada a 200, de manera que siempre sean peores que las anunciadas desde el Router principal. Por tanto sólo hay que configurar la métrica a 200 en el EDC de respaldo.

• Configuración BGP Juniper Principal

```
protocols {
    bgp {
        group <Grupo> {
            type external;
            metric-out 100;
            export <Redes_Anunciadas>;
            peer-as <AS_Remoto>;
            neighbor <Vecino_BGP>{
                hold-time 30;
            }
        }
    }
}
```

Donde:

<Grupo> Nombre del Grupo BGP, para cuando tenemos varios.

<Redes_Anunciadas> Termino de redes a anunciar al vecino

<AS_Remoto> Sistema autonomo remoto de la Red Wan

<Vecino_BGP> Vecino con el que se establece la sesion BGP

• Configuración BGP Juniper Secundario

```
protocols {
    bgp {
        group <Grupo> {
            type external;
            metric-out 200;
            export <Redes_Anunciadas>;
            peer-as <AS_Remoto>;
            neighbor <Vecino_BGP>{
                hold-time 30;
            }
        }
    }
}
```

-**VLANS EN SWITCHES**

• Realizaremos la siguiente configuración en todos los puertos donde el cliente quiere conectar Vlan de Datos y Vlan de Voz.

```
interface <Puerto_Fisico>
        switchport access vlan <ID_Vlan_DATOS>
        switchport mode access
        switchport nonegotiate
        switchport voice vlan <ID_Vlan_ToIP>
        switchport port-security
        switchport port-security maximum 3
        switchport port-security aging time 1
        switchport port-security violation restrict
        priority-queue out
        mls qos trust device cisco-phone
        mls qos trust cos
        storm-control broadcast level 3.00 0.00
        storm-control action trap
```

```
        spanning-tree portfast
        spanning-tree bpduguard enable
        no shutdown
exit
```

Donde:

<Puerto_Fisico> Puerto fisico donde el cliente conecta su electronica de LAN

<ID_Vlan_DATOS> Vlan definida para Datos (En nuestro caso 100)

<ID_Vlan_ToIP> Vlan definida para ToIP (En nuestro caso 200)

• Realizaremos la siguiente configuracion en todos los puertos donde el cliente quiere solo conectar equipos de Datos

```
interface <Puerto_Fisico>
        switchport mode access
        switchport nonegotiate
        switchport access vlan <ID_Vlan_DATOS>
        switchport port-security maximum 2
        switchport port-security
        switchport port-security aging time 1
        switchport port-security violation restrict
        mls qos cos override
        storm-control broadcast level 3.00 0.00
        storm-control action trap
        spanning-tree portfast
        spanning-tree bpduguard enable
        no shutdown
exit
```

-TACACS+

• Realizaremos la siguiente configuración para la funcionalidad de TACACS+ en los equipos:

```
tacacs-server host <IP_Servidor_TACACS+>
tacacs-server timeout 10
no tacacs-server directed-request
tacacs-server key <Clave_Servidor_TACACS+>

tacacs-server aaa new-model
aaa authentication login default group tacacs+ line
```

```
aaa authentication enable default group tacacs+ enable
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+

aaa authorization commands 0 default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa authorization exec default group tacacs+ if-authenticated
```

Donde:

<IP_Servidor_TACACS+> Se trata de la IP del servidor “AAA” destino donde debe validar la Autorización, Autenticacion y Acounting del usuario

<Clave_Servidor_TACACS+> Clave del usuario para el acceso al equipo