PROJECTE FI DE CARRERA

TÍTOL: Implantación de un sistema de videoconferencia CUVM sobre una red MPLS

AUTOR: Elena Centelles Celma

TITULACIÓ: Enginyeria Tècnica en Informàtica de Gestió

DIRECTOR: Sergio Sánchez López

DEPARTAMENT: Arquitectura de Computadors

DATA: 7 de febrer de 2012

TÍTOL: Implantación de un sistema de videoconferencia CUVM sobre una red MPLS

COGNOMS: Centelles Celma **NOM: Elena**

TITULACIÓ: Enginyeria Tècnica

ESPECIALITAT: Informàtica de Gestió **PLA: 92**

DIRECTOR: Sergio Sánchez López

DEPARTAMENT: Arquitectura de Computadors

QUALIFICACIÓ DEL PFC

TRIBUNAL

PRESIDENT **SECRETARI** **VOCAL**

DATA DE LECTURA:

Aquest Projecte té en compte aspectes mediambientals: □ Sí X No

PROJECTE FI DE CARRERA

RESUM (màxim 50 línies)

El objetivo del proyecto es la implantación de un sistema de videoconferencia para realizar formación a distancia sobre una red MPLS en Caixa Penedès.

El sistema elegido, tras un estudio previo de la infraestructura y de la posible integración, es el Cisco Unified Videoconferencing Manager (CUVM). Este sistema permite realizar "clases interactivas" desde un pc conectado en una oficina o desde un pc conectado a internet. Las clases o reuniones constan de una interfaz web que permite compartir cualquier aplicación, permite chat, además de videoconferencia (audio+ video).

La implantación sobre la infraestructura de Caixa Penedès tiene que garantizar la calidad suficiente para que cada alumno pueda atender a una "clase" sin que haya problema de retardos en la información. Se ha requerido realizar un estudio de la red MPLS (contratada a Telefónica) para poder realizar una recomendación posterior en función de las necesidades del sistema CUVM.

CUVM es un sistema cliente/servidor, donde el servidor esta centralizado en Servicios Centrales. Internamente se comunica con diferentes componentes, para la integración la telefonía (Call Manager) y para buscar los recursos de video necesarios (MCU y Gatekeeper). A parte de estas conectividades es necesaria la conectividad con el servidor de correo (para la programación de reuniones y envío de e-mails) y con los servidores DNS.

El sistema consta de dos componentes diferenciados:

1- Cisco Unified Videoconferencing Manager: Componente para la programación de reuniones y para la administración de recursos de videoconferencia

2- Cisco Unified Videoconferencing Desktop: Componente para la realización de las reuniones interactivas y de streaming.

Paraules clau (màxim 10):

Videoconferencia	MPLS	H323	Internet
LAN	WAN	Telefónica	Streaming

Índice

ANEXOS

I- INTRODUCCIÓN

1.- Internet

1.1.- Que es Internet?

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web www, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

1.2.- Historia

En el mes de julio de 1961 Leonard Kleinrock publicó desde el MIT (Massachusetts Institute of Technology) el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

1969. La primera red interconectada nace el 21 de noviembre de 1969, cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, y gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde 1959. El mito de que ARPANET, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, este no fue el único motivo. Si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables, tal y como se atestigua en la siguiente cita:

A raíz de un estudio de RAND, se extendió el falso rumor de que ARPANET fue diseñada para resistir un ataque nuclear. Esto nunca fue cierto, solamente un estudio de RAND, no relacionado con ARPANET, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores

enfatizaron la robustez y capacidad de supervivencia de grandes porciones de las redes subyacentes.

1972. Se realizó la Primera demostración pública de ARPANET, una nueva red de comunicaciones financiada por la DARPA que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva arquitectura sirvió para que, en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

1983. El 1 de enero, ARPANET cambió el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB (Internet Architecture Board) con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet. Por otra parte, se centró la función de asignación de identificadores en la IANA (Internet Assigned Numbers Authority) que, más tarde, delegó parte de sus funciones en el Internet registry que, a su vez, proporciona servicios a los DNS (Domain Name System).

1986. La NSF comenzó el desarrollo de NSFNET que se convirtió en la principal *Red en árbol* de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.

1989. Con la integración de los protocolos OSI (open system interconnection) en la arquitectura de Internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En el CERN de Ginebra, un grupo de físicos encabezado por Tim Berners-Lee creó el lenguaje HTML, basado en el SGML. En 1990 el mismo equipo construyó el primer cliente Web, llamado World Wide Web y el primer servidor web.

2008. El 3 de enero, Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la Red aumentará a 2.000 millones.

1.3.- La Evolución de Internet y la Sociedad

Inicialmente Internet tenía un objetivo claro. Se navegaba en Internet para algo muy concreto: búsquedas de información, generalmente.

Ahora quizás también, pero sin duda alguna hoy es más probable perderse en la red, debido al inmenso abanico de posibilidades que brinda la red. Hoy en día, la sensación que produce Internet es un ruido, una serie de interferencias, una explosión o cúmulo de ideas distintas, de personas diferentes, de pensamientos distintos de tantas y tantas posibilidades que, en ocasiones, puede resultar excesivo.

El crecimiento o más bien la incorporación de tantas personas a la red hace que las calles de lo que en principio era una pequeña ciudad llamada Internet se conviertan en todo un planeta extremadamente conectado entre sí entre todos sus miembros.

El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas. Conociendo este hecho y relacionándolo con la felicidad originada por las relaciones personales, es posible concluir que cuando una persona tenga una necesidad de conocimiento popular o de conocimiento no escrito en libros, puede recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet, dicha persona preferirá prescindir del obligado protocolo que hay que cumplir a la hora de acercarse a alguien personalmente para obtener dicha información y, por ello, no establecerá, para ese fin, una relación personal sino virtual. Este hecho implica la existencia de un medio capaz de albergar soluciones para diversa índole de problemas.

Como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas creados a partir de soluciones anteriores. Algunos sienten que Internet produce la sensación que todos han sentido sin duda alguna vez; produce la esperanza que es necesaria cuando se quiere conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios Internet genera una sensación de cercanía, empatía, comprensión y, a la vez, de confusión, discusión, lucha y conflictos que los mismos usuarios consideran la vida misma.

Internet tiene un impacto profundo en el trabajo, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo de esto es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source por ejemplo GNU, Linux, Mozilla y OpenOffice.org.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante

2.- MPLS

2.1.- Introducción

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como DWDM (Dense Wavelength Division Multiplexing), proporcionan una eficaz alternativa al ATM (Asynchronous Transfer Mode) para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como MPLS (Multi-Prototocol Label Switching). MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet del siglo XXI.

Uno de los factores de éxito de la Internet actual está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones. La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública de este siglo. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort".

Si el modelo Internet ha de consolidarse como la red de datos del futuro, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinada y menos aleatoria. Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF2 que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM; también como un protocolo para hacer túneles o bien, como

una técnica para acelerar el encaminamiento de paquetes o incluso, ¿para eliminar por completo el routing ?. En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (enlace) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2. Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

2.2.- Convergencia de los Niveles 2 y 3: IP Sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso. Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio habían empezado a desplegar en esos años, estaban construidos basados en routers conectados por líneas dedicadas. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. Las respuesta de los proveedores de servicio fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los proveedores de servicio se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los operadores de servicio. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinadas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de proveedores, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia.

Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 1 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

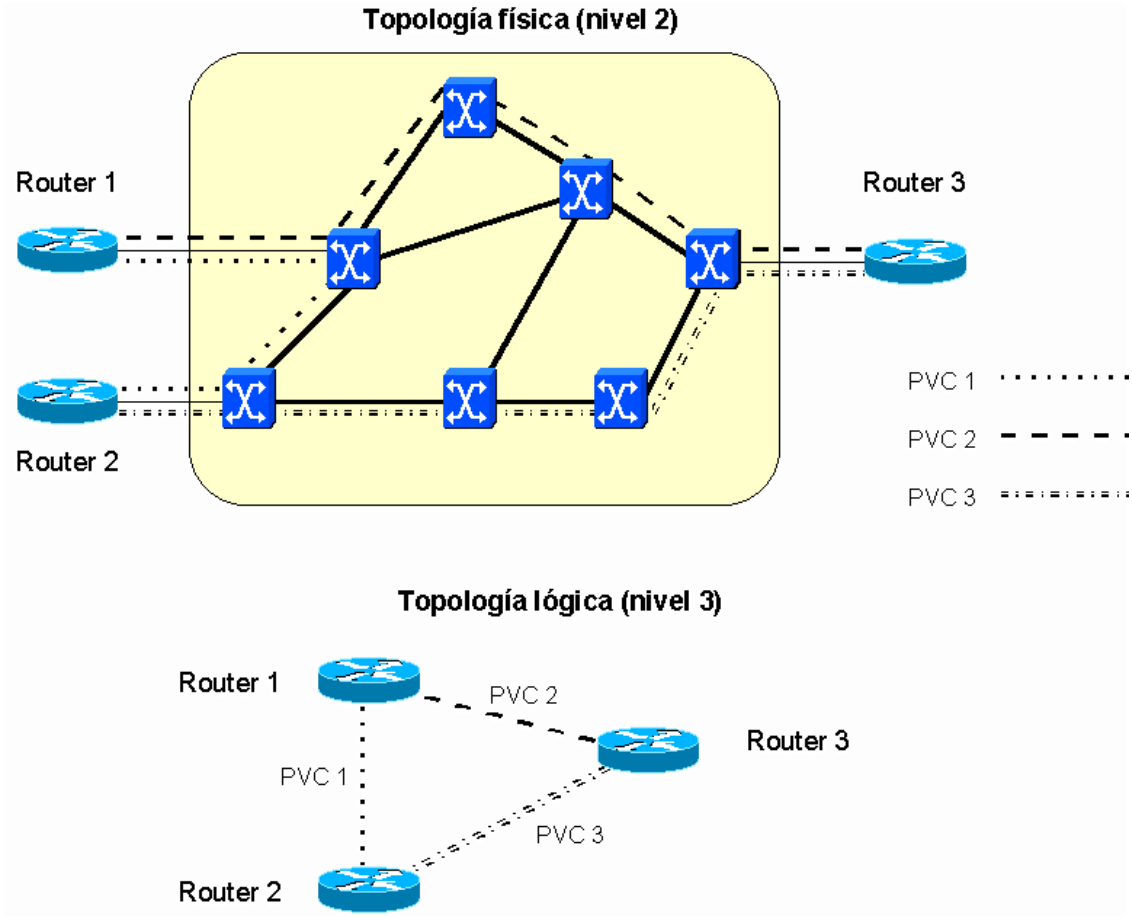


Figura 1. Topología física ATM y topología lógica IP superpuesta.

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y *routing*) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del *backbone*; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían

una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 2 se representa el modelo IP/ATM con la separación de funciones entre los que es *routing* IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

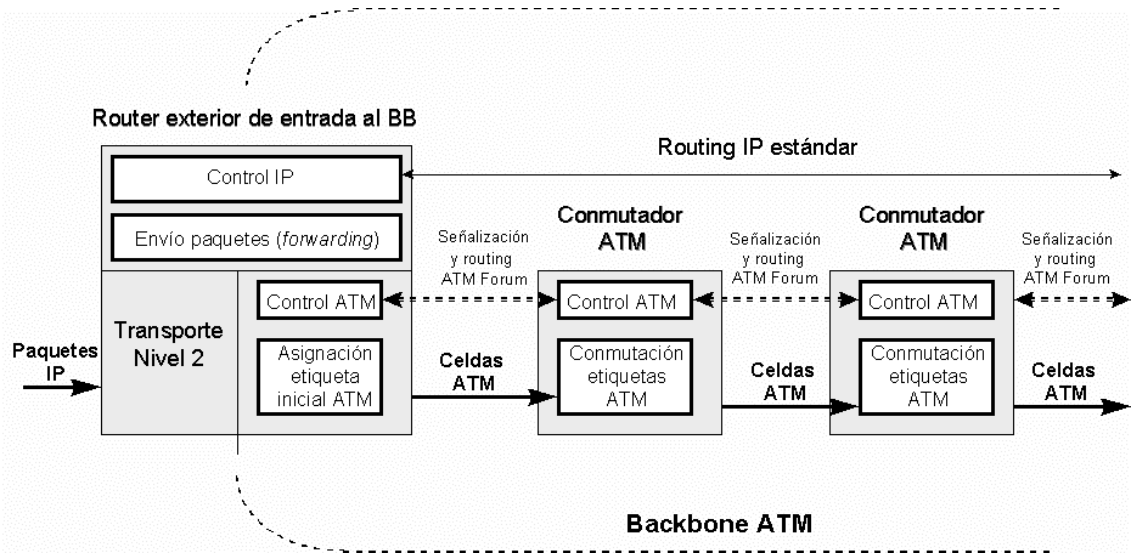


Figura 2. Modelo Funcional IP sobre ATM.

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de primer nivel (la mayor parte telcos), ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de las necesidades del tráfico IP, utilizando la clase de servicio ATM UBR6 (*Unspecified Bit Rate*), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los *routers* los PVCs necesarios, con una topología lógica entre routers totalmente mallada.

El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los *routers* con los PVCs, a través de los cuales se intercambian los *routers* la información de encaminamiento correspondiente al protocolo interno IGP7.

Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal. Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un *overhead* aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, p. ej. , en una red con 5 routers externos

con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 = 20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5 = 30). Un problema adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP. Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades.

2.3.- Conmutación IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señales anteriormente. Esas técnicas se conocieron como "conmutación IP" (multilayer switching). Una serie de tecnologías privadas —entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba— condujeron finalmente a la adopción del actual estándar MPLS del IETF.

El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.
Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

· La separación entre las funciones de control (routing) y de envío (forwarding).

· El paradigma de intercambio de etiquetas para el envío de datos.

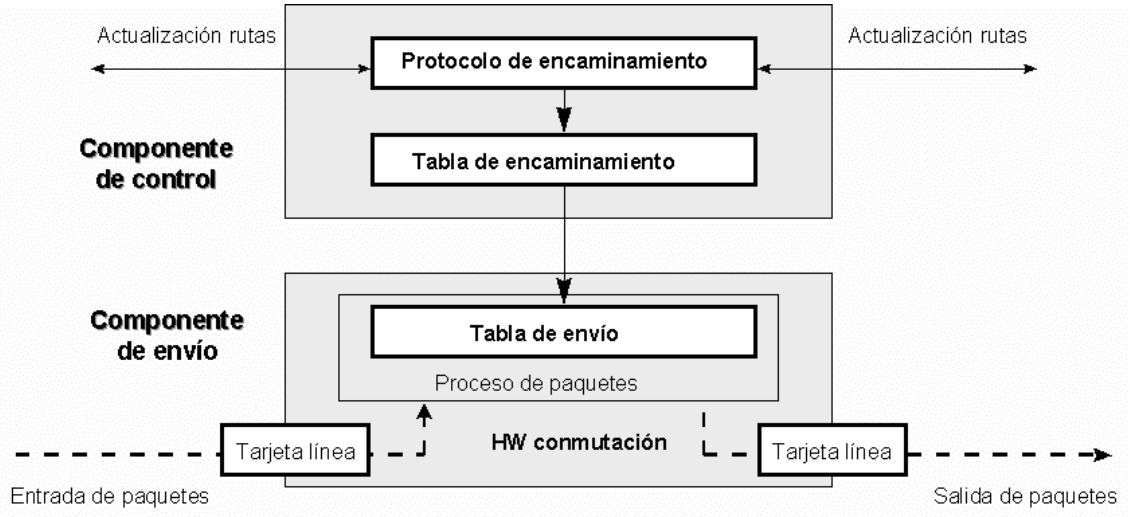


Figura 3. Separación funcional de encaminamiento y envío.

En la figura 3 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento.

Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete.
En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.
Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella se puede implementar y modificar independientemente.
El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento. En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC).
Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay.
En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

2.4.- Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

· Ingeniería de tráfico.

· Diferenciación de niveles de servicio mediante clases (CoS).

· **Servicio de redes privadas virtuales (VPN).**

Vamos a ver brevemente las de redes privadas virtuales ya que es el servicio necesario básico para que este proyecto pueda implantarse en la red de Caixa Penedès.

Redes Privadas Virtuales (VPNs)

Una red privada virtual (VPN) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales. Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR) 9. Algo similar se puede hacer con ATM, con diversas clases de garantías.

Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs. (Algo similar a lo que se vio en la solución IP sobre ATM de la sección 2).
Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.
Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

· En el nivel 3, mediante el protocolo IPSec del IETF.

· En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

En las VPNs basadas en túneles IPSec (Internet Protocol security**)**, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP.
Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS (Quality of Service) son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la Información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

· Están basadas en conexiones punto a punto (PVCs o túneles).
· La configuración es manual.
· La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
· Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
· La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN.
De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS.

Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos

sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer QoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

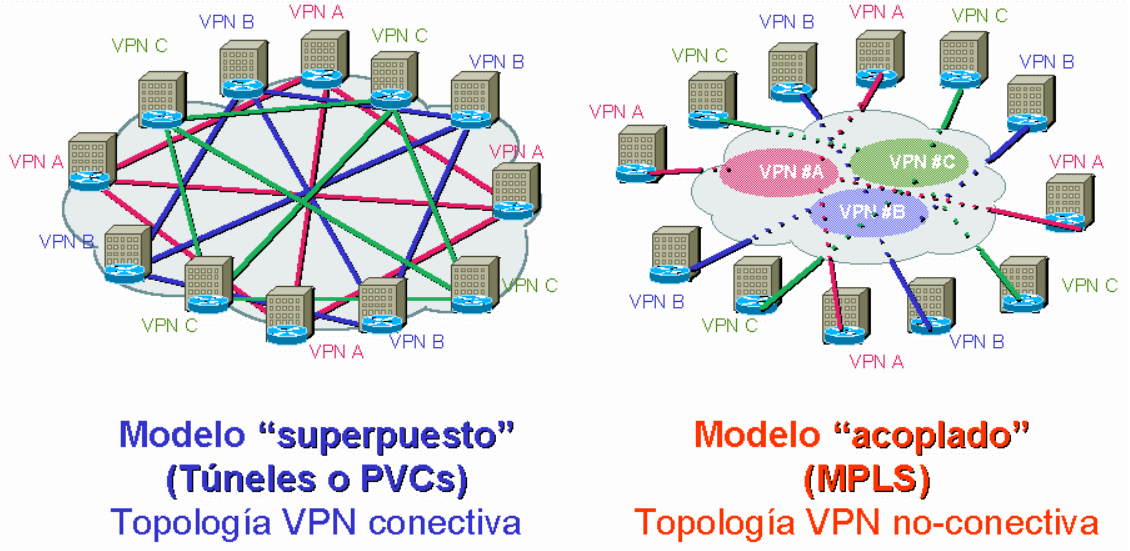


Figura 9. Modelo "superpuesto" (túneles/PVCs) vs. modelo "acoplado" (MPLS).

En la figura 9 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, basados en LSPs, y no de extremo a extremo a través de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

· Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).

· Evita la complejidad de los túneles y PVCs.

· La provisión de servicio es sencilla: una nueva conexión afecta a un solo router tiene mayores opciones de crecimiento modular.

· Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

· Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

3.- Protocolos Videoconferencia

3.1- Introducción

Hasta ahora hemos visto una introducción a las capas 2 y 3 (el protocolo MPLS relaciona las capas 2 y 3) de la pila de protocolos TCP/IP pero este proyecto se encuentra dentro de la capa de Aplicación.

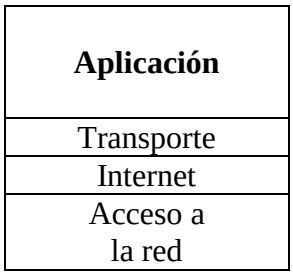


Figura 10: Modelo de internet

La capa de aplicación se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo.

3.2.- Protocolos para videoconferencia: familia de protocolos H.32x

El H.32x es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX (Internetwork Packet Exchange) sobre Ethernet o Fast Ethernet. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

Este estándar define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define los siguientes componentes más relevantes: Terminal, Gateway, Gatekeeper y MCU (Multipoint Control Unit).

El H.323 utiliza los mismos algoritmos de compresión para el vídeo y el audio que la norma H.320, aunque introduce algunos nuevos. Se utiliza T.120 para la colaboración de datos.

3.3.- El H.323 en perspectiva histórica

Anteriormente al H.323, el ITU se enfocó exclusivamente en la estandarización de las redes globales de telecomunicaciones. Por ejemplo, en 1985 se comenzó el trabajo en la especificación que define el envío de imagen y voz sobre redes de circuitos conmutados, tales como RDSI (Red Digital de Servicios Integrados). La ratificación de la norma (H.320) tuvo lugar 5 años después (fue aprobada por el CCITT, Comité Consultivo Internacional Telegráfico y Telefónico, en Diciembre de 1990). Sólo 3 años después se dispuso de equipos que cumplieran con la norma y que permitieran la interoperabilidad entre sí.

En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores propuso la creación de un nuevo estándar ITU-T (Sector de Normalización de las Telecomunicaciones) para incorporar videoconferencia en la LAN. Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo hubo de contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

El H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local, metropolitana, regional o de área extensa. Soporta así mismo Internet e intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para "los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

Nótese que H.323 también soporta videoconferencia sobre conexiones punto a punto, telefónicas y RDSI. En estos casos, se debe disponer un protocolo de transporte de paquetes tal como PPP (Point-to-point Protocol).

H.323: Una extensión del H.320

El H.323 se fundamenta en las especificaciones del H.320. Muchos de los componentes del H.320 se incluyen en el H.323. A este respecto, el H.323 se puede ver como una extensión del H.320. El nuevo estándar fue diseñado específicamente con las siguientes ideas en mente:

- Basarse en los estándares existentes, incluyendo H.320, RTP (Real Time Protocol) y Q.931
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

3.4.- Ventajas de la tecnología H.323

Reducción de los costes de operación.

H.323	H.320
Se pueden utilizar los cableados de campus, las conexiones WAN basadas en routers IP y los servicios WAN para enviar vídeo. Esto es una fuente potencial de importantes ahorros de explotación. Los costes de soporte de las infraestructuras (por ejemplo SNMP) pueden combinarse.	La tecnología H.320 requiere típicamente redes separas para el vídeo y los datos. Esto supone doble cableado e infraestructuras de red. Este modelo incrementa el coste de implantación por sistema.

Más amplia difusión y mayor portabilidad.

H.323	H.320
Con H.323, cada puerto con soporte IP puede potencialmente soportar vídeo. Esto hace la tecnología accesible a una más amplia variedad de usuarios. Además, es más fácil mover un equipo en nuestro entorno, lo que hará que un mismo equipo pueda ser usado para más aplicaciones.	Con H.320, se debe dedicar una línea por cada localización. La mayor parte de las salas o de los ordenadores personales no podrán fácilmente soportar vídeo, lo cual limita también la accesibilidad y portabilidad de los sistemas.

Un diseño Cliente / Servidor rico en prestaciones.

H.323	H.320
El diseño del H.323 descansa fuertemente en los componentes de la red. Sus capacidades están distribuidas a través de la red. Un ejemplo es el gatekeeper. Un gatekeeper puede residir en un servidor, en un Gateway o en una MCU. Se encarga de registrar los usuarios o clientes (sistemas de videoconferencia) y puede potencialmente ofrecerles un conjunto de funciones de comunicación.	Como norma, un equipo H.320 no se conecta a un servidor. Las características del sistema residen en la plataforma de videoconferencia misma. Este enfoque de comunicación orientado al terminal no soporta servicios suplementarios tales como enrutado de llamadas, transferencia o retención. Son servicios a los que estamos acostumbrados por la tecnología de las centralitas telefónicas.

¿Por qué es importante H.323?

El H.323 es la primera especificación completa bajo la cual, los productos desarrollados se pueden usar con el protocolo de transmisión más ampliamente difundido (IP). Existe tanto interés y expectación en torno al H.323 porque aparece en el momento más adecuado. Los administradores de redes tienen amplias redes ya instaladas y se sienten confortables con las aplicaciones basadas en IP, tales como el acceso a la web. Además, los ordenadores personales son cada vez más potentes y por lo tanto, capaces de manejar datos en tiempo real tales como voz y vídeo.

II – ESTADO DEL ARTE

1.- Comunicaciones Unificadas

El término Comunicaciones Unificadas se utiliza comúnmente por los proveedores de tecnologías de la información para designar la integración de "los servicios de telefonía, mensajería unificada (la misma bandeja de entrada para correo electrónico, correo de voz y fax), mensajería instantánea corporativa, conferencias web y estado de disponibilidad del usuario en una sola e innovadora experiencia para los colaboradores y para el personal que administra y da mantenimiento a la infraestructura".

Hoy en día, las empresas deben enfrentarse con entornos de comunicaciones cada vez más complejos que presentan una gran variedad de métodos de comunicación. Los empleados, los socios comerciales, los clientes y los integrantes de las empresas se comunican entre sí mediante infinitas combinaciones de teléfonos conectados, inalámbricos y móviles, mensajes de voz, correo electrónico, fax, clientes móviles y conferencias con tecnología multimedia avanzada. Sin embargo, con frecuencia, estas herramientas no se utilizan con eficacia con la que se podrían utilizar. Esto genera exceso de información, falta de agilidad y comunicaciones mal dirigidas que retrasan las decisiones, ralentizan los procesos, alejan a los clientes y reducen la productividad. Las comunicaciones ineficientes también producen pérdida de ingresos porque las empresas no están preparadas para reaccionar con rapidez a los cambios del mercado.

Las soluciones de comunicaciones unificadas han demostrado ser valiosas para ayudar a las organizaciones a solucionar estos problemas, lo que les permite optimizar los procesos comerciales y disminuir los costes. Durante años, las empresas de todos los tamaños han obtenido las ventajas que supone la transmisión de voz, datos, video y las comunicaciones móviles sobre una red IP convergente.

Hoy en día existen aplicaciones que unifican aplicaciones móviles, de voz, de vídeo y de datos en redes fijas y móviles, lo que facilita una experiencia de trabajo en equipo con tecnología multimedia avanzada, en espacios de trabajo de empresas, organismos de gobierno e instituciones. Estas aplicaciones, al utilizar la red como plataforma para mejorar la ventaja competitiva, aceleran el tiempo de decisión y reducen el tiempo de las transacciones. La seguridad, elasticidad y escalabilidad de la red permite que los usuarios de cualquier espacio de trabajo puedan conectarse fácilmente, en cualquier lugar en cualquier momento, utilizando cualquier medio dispositivo o sistema operativo.

Las empresas pueden colaborar en tiempo real utilizando aplicaciones avanzadas como videoconferencias, conferencia integrada de voz y web, correo de voz y más, desde una interfaz integrada. La solución permite ahorrar tiempo, ayuda a controlar los costes, aumenta la productividad y la competitividad. Un estudio realizado por Sage Research en el año 2009 reveló que el 86% de las empresas que utilizaban comunicaciones unificadas experimentaron un aumento de productividad. Más del 60% de las empresas informaron un ahorro de tres o más horas a la semana por trabajador itinerante. Estos estudios confirmaron que migrar aun sistema de comunicaciones unificadas proporciona un retorno considerable de la inversión (ROI, return on investment) y una reducción del coste total de propiedad (TCO, total cost of ownership).

2.- La videoconferencia

La videoconferencia no es una nueva tecnología que haya surgido de la noche a la mañana, ni mucho menos recientemente. Lo que sí es cierto es que su uso popular, al margen de las grandes corporaciones, no comenzó hasta hace muy pocos años. Han hecho falta 35 años para que las tecnologías evolucionasen lo suficiente como para proporcionar una videoconferencia de calidad y asequible para una sociedad que ha cambiado sustancialmente.

En 1968, en pleno apogeo del movimiento contracultural, Theodore Roszak expresaba sus ideas sobre el papel de la ciencia y la tecnología en el mundo contemporáneo:
«Cualesquiera que sean las demostraciones y los beneficiosos adelantos que la explosión universal de la investigación produce en nuestro tiempo, el principal interés de quienes financian pródigamente esa investigación seguirá polarizado en el armamento, las técnicas de control social, la mercancía comercial, la manipulación del mercado y la subversión del proceso democrático a través del monopolio de la información y del consenso prefabricado» .

Las palabras de Roszak, tremendas y exageradas como corresponden a un teórico de la contracultura, reflejan, no obstante, el espíritu de los tiempos que corrían: una creciente sensibilidad social y una preocupación política por las consecuencias negativas de una ciencia y una tecnología fuera de control. Es lo que se ha llamado *«síndrome de Frankenstein»*, que empezó a extenderse en la opinión pública de los años 60 y 70. Por el contrario en estos primeros años del siglo XXI el sustento tecnológico, la cultura de la sociedad global, la ciber cultura, en el escenario de la postmodernidad, ha generado profundos cambios sociales, económicos y culturales, un nuevo tipo de sociedad, una sociedad inmersa en el vertiginoso desarrollo tecnológico, en el esnobismo de la última tecnología.

Actualmente, las grandes consultoras de tecnologías de la información prevén que el incremento de la incidencia de las tecnologías de videoconferencia será de un 30% anual en los próximos 3 años. Hace relativamente poco tiempo, los desplazamientos tal y como los entendemos hoy no existían. Emprender un viaje suponía un elevado coste económico o una inversión importante de tiempo. Los medios de transporte en los últimos 50 años han sufrido una transformación incuestionable. Si a este abaratamiento de coste y tiempo en movernos, le añadimos las necesidades surgidas de un mercado globalizado, tenemos la respuesta a los flujos humanos que circulan por el mundo. En las últimas décadas muchos trabajadores han tenido que trasladarse, por motivos laborales, para reuniones de dos horas, a ciudades situadas a grandes distancias. Cierto es que hay empleos en los que estar presente es una necesidad, sin embargo otras muchas veces con nuestra presencia virtual se soluciona el problema. Los desplazamientos implican necesariamente un coste económico y temporal, pudiendo incidir negativamente en la productividad, equilibrio trabajo-vida privada e incluso en el medioambiente.

La videoconferencia ya no es una tecnología cara y exclusiva de grandes instalaciones, pero la variedad de equipos existentes y las diferencias en coste y complejidad de uso, nos obliga a saber elegir el adecuado a nuestras necesidades, tanto en cuanto a equipo, como en lo referente a la conexión. Cada día aumentan las alternativas de comunicación

Audiovisual, podemos llevar a cabo este tipo de comunicación a través de la web o incluso a través de teléfonos celulares equipados. Las ventajas de las videoconferencias de hoy en día son muchas. Para empezar, ahorramos el tiempo de viaje. En las grandes ciudades, moverse entraña dificultades. Coordinarse con los medios, encontrar aparcamiento, la lluvia, el tráfico, son circunstancias que nos hacen perder tiempo, un bien de incalculable valor en nuestras apresuradas jornadas. Por otro lado, el uso y abuso de los medios de transporte vienen provocando una alta emisión de gases contaminantes. Reducir nuestros desplazamientos a lo estrictamente necesario, ayuda en gran medida a preservar el medio ambiente. Y como tercera ventaja, con el sistema de videoconferencias no sólo reducimos tiempo y emisiones contaminantes, también reducimos los costes. Muchas empresas empiezan a plantearse la utilidad de sus encuentros físicos. Hasta el momento se habían tratado aspectos que interesan a nivel de individuo, sin embargo estos gastos en desplazamientos afectan de un modo directo a los presupuestos tanto de las grandes multinacionales como de las pequeñas o medianas empresas.

En un estudio encargado por 'Tandberg' a la firma 'Ipsos Mori' en 2003 (que podemos consultar en la página web: http://www.tandberg.com/collateral/tandberg_videoconfering_travel_survey.pdf) se pone de manifiesto que una de cada tres reuniones que se producen en los viajes de negocios podría realizarse a través de videoconferencias. Además se comenta que este tipo de soluciones pueden evitar el estrés derivado de los viajes, que afecta al 51% de los hombres y mujeres de negocio español y hasta al 81% de los italianos. El estudio afirma que incluso un 7% de los ejecutivos europeos estaría dispuesto a cambiar de trabajo por viajar con menor frecuencia, así como dice que un 15% de los directivos europeos declara ser menos productivo cuando tiene que viajar para celebrar una reunión.

Actualmente la mayoría de las grandes compañías o instituciones utilizan las videoconferencias para

- **Reuniones a distancia**: Como se ha comentado, en muchos casos ya no es necesario llevar a cabo largos viajes simplemente para asistir a una reunión.

- **Telemedicina**: En aplicaciones médicas se puede desde intercambiar opiniones con colegas hasta dirigir complejas cirugías sin necesidad de estar presente en un pabellón. Con video de alta calidad se pueden ver hasta los más mínimos detalles de una operación, y con la comunicación en tiempo real, ir siguiendo o dirigiendo cada paso. El diagnóstico clínico remoto por videoconferencia se usa más frecuentemente en áreas rurales.

- **Conferencias**: Ya no es necesario estar físicamente presente para dictar conferencias y dirigirse a un público numeroso. Se puede participar en conferencias a distancia sin necesidad de estar presente en el auditorio y disfrutando de la posibilidad de interactuar en tiempo real.

- **Educación**: La educación es una herramienta que permite el desarrollo de la sociedad, es por ello que las instituciones buscan cada vez más opciones que les permitan llegar a más gente. Actualmente se pueden realizar cursos a distancia o

hacer clases más interactivas gracias a la inclusión de la tecnología de videoconferencia.

- **Tele-justicia**: La llegada de la videoconferencia a los tribunales de justicia ayuda también a la protección de testigos o a la efectividad de las presentaciones en juicios y otros. Se puede tener a personas en salas completamente separadas y hacerlos interactuar con el resto, contar sus testimonios o presentar sus pruebas sin necesidad de que tengan que estar en la misma habitación que sus contrapartes.

- **Servicio al cliente**: Obtener soporte inmediato en productos o servicios. A las empresas les permite dar soporte y ayuda a clientes sin tener que enviarles un técnico o representante. Si vendes un producto o servicio que necesita un soporte, darle este servicio por video conferencia reducirá costes y mejorará las relaciones con el cliente al darle una asistencia rápida y efectiva.

A la videoconferencia también se le da actualmente otros muchos usos como: control de la manufactura, contratación/entrevistas, supervisión, adiestramiento/capacitación, etc..

3.- Aplicaciones de Videoconferencia y de Comunicaciones Unificadas

En este apartado vamos a mencionar algunos de los programas de videoconfencia y comunicaciones unificadas que existen en internet a nivel de usuario casero (estos acostumbran a ser gratuitos) y a nivel empresarial. Mencionaremos my brevemente sus características más relevantes y los inconvenientes que encontramos.

3.1.- Aplicaciones orientadas al uso personal

Microsoft Net Meeting

Se trata de un cliente de videoconferencia VoIP (Voice over IP) multipunto incluido en muchas versiones de "Microsoft Windows" antiguas. Desde el lanzamiento de "Windows XP", Microsoft lo abandonó en favor de "Windows MSN Messenger". Implementaba una solución de videoconferencia sobre Internet con chat, pizarra electrónica, posibilidad de compartir el escritorio o transferir archivos, aparte de la transmisión punto a punto del audio y el vídeo. No existía la posibilidad de grabar la videoconferencia.

MSN Messenger

MSN Messenger fue el relevo de Microsoft Net Meeting es un programa de mensajería instantánea creado en 1999 y actualmente sustituido por "Windows Live Messenger". La primera versión de MSN Messenger que incluyó video llamada fue la 7.0, lanzada en abril de 2005. Dicha versión cuenta con chat, video llamada, conversación de voz, etc.

Este programa fue renombrado como "Windows Live Messenger" a partir de la versión 8.0. Tampoco permitía la grabación de la video llamada.

Windows Live Messenger

Windows Live Messenger nace el 13 de diciembre del 2005. Ofrece, como sus antecesores, servicios de video llamada de ordenador a ordenador, pero ahora incluso con imágenes a pantalla completa. El principal inconveniente continúa siendo la incapacidad de grabar las video llamadas.

Skype

Skype es un exitoso programa de vídeo llamadas que proporciona a los usuarios una imagen de gran tamaño de su interlocutor y mensajería instantánea. Es muy sencillo y fácil de usar. Se puede asimismo compartir el escritorio y enviar archivos. Destaca la calidad del audio. No permite la grabación de las vídeo llamadas.

Google Talk

Google Talk es un cliente de mensajería instantánea y telefonía IP de protocolo XMPP, (parecido a Skype) desarrollado por Google. La versión beta de Google Talk fue lanzada el 24 de agosto de 2005.

3.2.- Aplicaciones/Servicios orientados a empresas

Microsoft Office Communicator

Microsoft Office Communicator es una versión de MSN Messenger orientada a empresas para aumentar su conectividad entre si o con otras empresas. Facilita el uso de la mensajería instantánea, funciona sin problemas con las aplicaciones de Office familiares que los usuarios emplean a diario. Se puede usar simultáneamente varios modos de comunicación, incluida mensajería instantánea, videoconferencia, telefonía, uso compartido de aplicaciones y transferencia de archivos.

Cisco Unified Personal Communicator

Es una aplicación de Cisco que mediante una interfaz fácil de usar proporciona a los usuarios un acceso rápido a potentes herramientas de comunicación: voz, video, mensajería instantánea, conferencia web, gestión de llamadas, información de presencia.

Webex (Cisco)

Webex es una herramienta de colaboración web que permite organizar reuniones virtuales con vídeo, audio-conferencia, el compartir aplicaciones y documentos, gestión de asistentes, cuestionarios y estadísticas, grabación de sesiones, mensajería instantánea,

etc.. Es un servicio que está en internet y que se compra a través de licencias de número de usuarios conectados de manera simultánea.

Microsoft Live Meeting

Microsoft Live Meeting es una herramienta de colaboración web competencia directa de webex que se integra con se integra los sistemas y aplicaciones de productividad de Microsoft. Es un servicio que puede ser interno, la empresa puede tener los servidores en sus instalaciones, o comprar solo licencias para poder usurarlo a través de internet.

Cisco Unified Videoconferencing

Es una herramienta de colaboración que a diferencia de las dos anteriores es únicamente interno y se integra directamente con los sistemas de comunicaciones de cisco. Ofrece la capacidad de gestionar y supervisar elementos de red de videoconferencias, además de programar, adaptar y controlar las videoconferencias con facilidad.

4.- Elección del sistema a Implantar

Tras realizar un estudio de las herramientas que existen en el mercado, se ha decidido implantar Cisco Unified Videoconferencing Manager ya que cumple los requerimientos que Caixa Penedès propone.

El sistema permite realizar reuniones en las que el usuario puede interactuar con los demás usuarios, puede compartir aplicaciones además de difundir video y audio. También permite que los usuarios se puedan conectar por internet o internamente, tiene funciones de solo streaming y los usuarios pueden entrar solo con audio si es necesario.

Pero el motivo principal sobre la decisión es la integración del sistema sobre la arquitectura de Caixa Penedès, ya que actualmente dispone de telefonía IP de Cisco con la cual el sistema se integra de manera casi inmediata y permite más funcionalidades que otros sistemas.

Otro motivo importante, es que este sistema es interno administrado totalmente por Caixa Penedès y no un servicio externo contratado por licencias que se facturan cada mes.

III – CISCO UNIFIED VIDEOCONFERENCING MANAGER (CUVM)

1.- Cisco Unified Videoconferencing Manager (CUVM)

Cisco Unified Videoconferencing Manager permite la colaboración para que las organizaciones puedan adaptarse rápidamente a los mercados aumentando la productividad, mejorando competitividad través de la velocidad y la innovación, y ofrecer una experiencia de medios enriquecidos a través de cualquier espacio de trabajo, de forma segura y con una calidad óptima.

Control de reuniones y asistencia sencilla y flexible

CUVM ayuda a las organizaciones de todos los tamaños mejorar las comunicaciones mediante el uso de sus recursos de vídeo más eficaz. Con esta aplicación, se pueden programar fácilmente conferencias de vídeo desde un navegador web y desde Microsoft Outlook o IBM Lotus Notes, donde se puede ver, comprobar la disponibilidad y reservar recursos de vídeo, tales como unidades de control multipunto (MCU) y gateways. La aplicación reduce la complejidad y facilita la utilización óptima de los recursos mediante la comunicación con múltiples MCU y dispositivos de puerta de enlace y automáticamente reserva de los recursos apropiados en los lugares más eficientes. Las características adicionales, tales como reuniones personalizadas plantillas que identifican el ancho de banda, el diseño y las preferencias de la terminal, integración de LDAP (Lightweight Directory Access Protocol), notificaciones por correo electrónico y llamadas automáticas a los terminales de vídeo.

1.1.- Características principales

- Visión global y centralizada de todos los equipos de video y elementos de videoconferencia de la red, lo que nos permite realizar un seguimiento, control y mantenimiento de cada dispositivo desde una sola interfaz.
- Programación fácil basada en web y videoconferencia improvisada, proporcionando reserva de recursos de ancho de banda y monitorización.
- Integración de Microsoft Outlook y Lotus Notes de IBM para la programación de reuniones a través del escritorio.
- Streaming de video para la asistencia a reuniones solo para la visión y la escucha.
- Permite la grabación de videoconferencias.

1.2.- Funcionalidades

Programación y asistencia	• Permite la programación de reuniones por web, vía Microsoft Outlook o Lotus Notes, • Permite configurar salas de videoconferencias personalizadas para realizar videoconferencias improvisadas. • Ofrece una agenda personal, para poder programar reuniones de forma fácil con los contactos favoritos. • Permite la reserva de recursos como MCU's (Multipoint Control Unit), gateways y anchos de banda. • Permite programar reuniones periódicas. • Ofrece notificaciones por correo electrónico a los participantes de la

	reunión con la información de marcación incluida y las direcciones URL para realizar la reunión vía web.
Videoconferencias	**Modos de conectividad:** • Participación interactiva en videoconferencias incluyendo dos sentidos de audio, video y H.239 (data sharing) • Streaming no interactivo que incluye audio, video y H.239. **NAT (Network Address Translation) y Firewall:** • Capacidad para atravesar firewalls locales y remotos. • Soporta NAT para redes privadas. **Video de Alta definición**: • CUVM permite que los clientes trabajen con video HD720p. **Opciones de Asistencia y Programación:** • Las reuniones se programan desde una misma interfaz, Microsoft Outlook o IBM Lotus Notes. • Reserva de recursos desde los clientes. • Se puede acceder a los dos tipos de reuniones con un solo click. **Controles de usuario:** • Mute y unmute. • Stop, pausa y start video • Call-back del sistema a los usuarios **Integración con Webex:** • Soporte de los estándar de video como reuniones webex • Video HD 720p **Seguridad:** • SRTP (Secure Real-Time Transport Protocol) entre el cliente y el servidor • Salas de espera, las reuniones no empiezan hasta que el moderador no entra. • Salas predefinidas, en este modo solo se pueden utilizar estas salas.
Control de reuniones	• Vistas y control de las reuniones desde una sola interfaz. • Invitar o llamar a participantes adicionales. • Cambiar las disposición del escritorio en tiempo real • Alargar el tiempo de una reunión en tiempo real.
Grabación de reuniones y reproducción.	• Iniciar la grabación desde el escritorio de cliente • Reproducir las grabaciones desde un navegador. • El administrador puede proteger con contraseñas las grabaciones guardadas.
Funcionalidades administrativas	• Se pueden realizar reportes para facturación

	• Se pueden usar distintas zonas horarias**.**
Alarmas y Monitorización	• Tiene un sistema para monitorizar los equipos de video de la red. • Permite descubrir automáticamente los equipos de video y la infraestructura de red de video con un solo click.

2.- Componentes del sistema

CUVM contiene dos componentes de software:

- **Cisco Unified Videoconferencing Manager (CUVM)**: Componente para la programación de reuniones y para la administración de recursos de videoconferencia.
- **Cisco Unified Videoconferencing Desktop (CUVM-D)**: Componente para la realización de reuniones interactivas y para streaming.

Para la implantación e integración de CUVM son necesarios los siguientes componentes. Vamos a explicar y definir los elementos que integran la solución:

MCU (Multipoint Control Unit):

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

La comunicación bajo H.323 contempla las señales de audio y vídeo. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo el estándar T.120 que permite la compartición de aplicaciones en conferencias punto a punto y multipunto.

Gateway:

Un gateway H.323 (GW) es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

Gatekeeper:

El gatekeeper (GK) es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN. El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

Esquema de los componentes para una implementación centralizada:

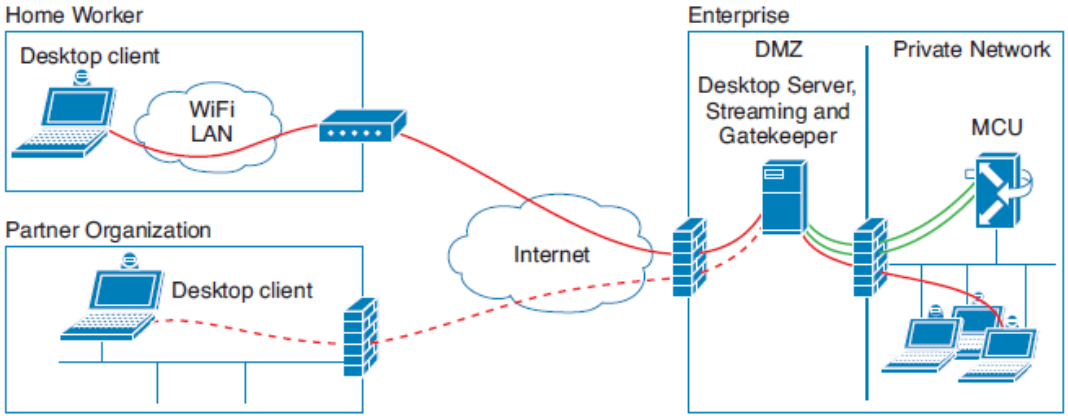


Figura 11: Implementación centralizada

Esta implementación incluye:

- Una MCU localizada en una red protegida de la organización.
- El servidor CUVM (incluye gatekeeper interno) localizado en una DMZ (demilitarized zone).
- Clientes a través de internet.
- Clientes dentro de la organización.

3.- Requerimientos del Sistema

3.1.- Servidor

Servidor CUVM
Hardware: - **Cisco Unified Videoconferencing 3500 Series MCU.** - **Cisco Media Convergence Server (MCS) 7835 o 7845 (*)** - **Cisco Unified Videoconferencing 3500 Series Gateway** **Software:** - **Cisco Unified Videoconfencing Desktop CD-ROM** - **Código de licencia** - **Cisco Unified Videoconfencing Manager CD-ROM** - **Cisco Unified Vidoeconferencing 3500 Series MCU CD-ROM** **Cisco MCS Server Sistema Operativo (CD-ROM)**

(*) Tabla de capacidades según servidor MCS

Funcionalidades	Capacidades	
	MCS 7835	MCS 7845
Resource Manager and Desktop manager	500 puertos MCU	500 puertos MCU
Desktop Interactivo	50 conexiones simultaneas	75 conexiones simultaneas
Desktop Streaming	300 conexiones de streaming	300 conexiones de streaming
Streaming, Interactivo y grabación	50 conexiones interactivas 150 streaming, y 1 grabación	75 conexiones interactivas, 225 streaming y 3 grabaciones

3.2.- Cliente

Clientes
Hardware: - **1G RAM** - **Tarjeta de red** - **SVGA (1024x768)** - **Altavoces y Micrófono compatibles.**
Software: - **Windows XP o Windows 7.** - **Modo Interactivo: Navegador Internet Explorer 6 o 7** - **Modo Streaming: Navegador Internet Explorer 6 o 7, Firefox, o Apple Safari**

3.2.- Requerimientos de red

El servidor CUVM actúa como un gateway entre los clientes y la MCU. En la siguiente tabla se muestra el ancho de banda requerido entre 50 y 100 usuarios conectados al sistema.

Se recomienda usar los siguientes valores por defecto: 384 kbps para conexiones interactivas y 256 para conexiones de streaming.

Para cada cliente, el tráfico que se genera es el siguiente:

- Cliente envía tráfico media al Servidor.
- Servidor reenvía el tráfico media a la MCU
- La MCU retorna el tráfico media al Servidor
- Servidor lo envía al cliente

Por lo tanto, la fórmula para calcular el ancho de banda requerido para sesiones interactivas es el siguiente:

Ancho de Banda = Ancho de banda requerido por una conexión x 4 x número de conexiones

Así, para una conexión de 384 Kbps, hay 1536 Kbps de trafico media a través del Servidor para cada cliente.

Para sesiones de Streaming, el servidor envía el tráfico media a los clientes. La fórmula para calcular el ancho de banda requerido es la siguiente:

Ancho de Banda = Ancho de banda requerido por una conexión x número de conexiones.

Conexiones Interactivas	Conexiones de Streaming	Ancho de banda para conexiones interactivas	Ancho de banda para conexiones de Streaming	Ancho de banda Total
		384 Kbps	**256 Kbps**	
10	30	15360	7680	23040
25	75	38400	19200	57600
50	150	76800	38400	115200
100	300	153600	76800	230400
		768 Kbps	**768 Kbps**	
10	30	30720	23040	53760
25	75	76800	57600	134400
50	150	153600	115200	268800
100	300	307200	230400	537600

3.4.- Calidad de Servicio

En un entorno de convergencia, voz, video y tráfico de datos viajan a través de una sola infraestructura de red. No todos los tráficos deben tratarse de la misma manera. El tráfico de datos es tolerante a la perdida de paquetes y no es sensible al retardo. El tráfico de video, por otro lado tiene muy poca tolerancia a la perdida de paquetes y es muy sensible al retardo. Se trata de proveer el nivel de servicio requerido para los tres tipos de tráfico.

Clasificación del Tráfico (QoS)

El primer paso es preservar la calidad del video en la red de datos, para esto hay que clasificar este tráfico como alta prioridad y permitir que viaje por la red antes que otro tráfico con menos prioridad. El trafico de datos puede ser clasificado en varias clases con colas sin que afecte a su rendimiento por sus características TCP ya se encarga de corregir errores de transmisión. Para el video, se recomienda clasificar el tráfico en la capa 2 y en la capa 3.

Capa 2: Usar los tres bits del campo CoS (Class of Service) en el protocolo 802.1Q para etiquetar el tráfico.

Capa 3: Usar los tres bits de DSCP (Differentiated Services Code Point) de la cabecera IP.

La siguiente tabla recomienda la clasificación del tráfico para varias aplicaciones

Aplicación	DSCP (Differentiated Services Code Point)	CoS (Class of Service)
Routing	**48**	**6**
Real Time Transport Protocol (RTP)	**46**	**5**
Videoconferecias	**34**	**4**
Streaming Video	**32**	**4**
Señalización de Voz	**24**	**3**
Transaccional	**18**	**2**
Gestión de red	**16**	**2**

IV – ESTUDIO DE LA INFRAESTRUCTURA E INTEGRACIÓN

1.- Arquitectura de red de Caixa Penedès

En este apartado se pretende dar una visión global de la infraestructura de red que tiene implementada Caixa Penedès para ver que tipo de implementación vamos a realizar del sistema CUVM dentro de dicha infraestructura.

1.1.- Arquitectura LAN

Caixa d'Estalvis del Penedès (CEP) tiene una arquitectura LAN que está dividida en *Building Blocks* (concepto de Cisco, donde se ordena la electrónica de red según el papel que desempeña dentro de la red teniendo en cuenta las características de los servicios a los que provee y la seguridad necesaria dentro de la red). Dichos building blocks (BBlocks) están unidos mediante una red de transporte que los une para las todas conexiones necesarias entre BBlock's. CEP dispone de dos CPD's (Centro Procesamiento de datos) unidos mediante DWDM (Dense wavelength Division Multiplexing).

Actualmente CEP dispone de los siguientes BBlocks:

Internet: Conjunto de electrónica que da servicios a nivel de internet, tanto de la web corporativa (balanceadores, firewalls, routers etc..) como de conexiones con empresas externas a través de internet vía vpn's. CEP dispone de un Sistema Autónomo en internet que explicaremos más adelante.

Datacenter: Conjunto de electrónica necesaria para interconectar todos los servidores del datacenter. (Balanceadores, swicth's, firewalls, etc..)

Voz/Video: Conjunto de electrónica necesaria para dar servicios de voz que incluye Call Managers, MCU's, Gateways y todos los servidores de comunicaciones unificadas. Este BBlock está muy relacionado con el servicio de videoconferencia CUVM ya que se integra con elementos que pertenecen a este BBlock.

WAN: Conjunto de electrónica que da conectividad a la WAN. A través de este BBlock se accede a toda la red MPLS de oficinas. Más adelante entraremos en detalle sobre la red MPLS de Caixa Penedés.

Gestión: Conjunto de electrónica y servidores que se utilizan para gestionar y monitorizar la infraestructura de red, incluye servidores de monitorización, RADIUS, equipos de seguridad etc..

Planta: Conjunto de electrónica que da acceso a la red a los pc's y teléfonos IP's de CEP. (Básicamente incluye switch's).

En la figura 12 se muestra un esquema a nivel de BBlocks:

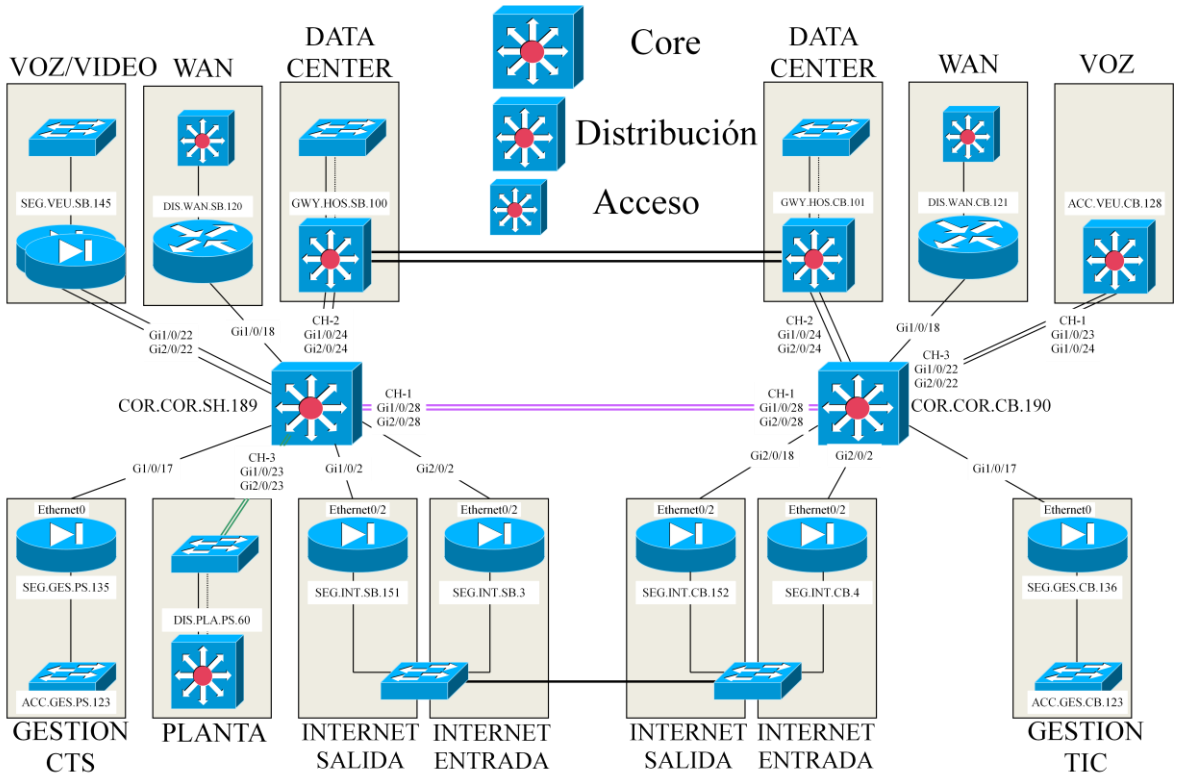


Figura 12: Esquema General BBlocks CEP

Todos los BBlocks se encuentran duplicados en un CPD extendido que se encuentra a 50 Km del CPD principal.

BBlock de Internet (Sistema Autónomo)

El BBlock de internet se puede dividir en servicios en entrada y servicios de salida. Los servicios de entrada son para las webs corporativas, correo electrónico, VPN's, SFTP (Secure FTP) etc.. y los servicios de salida son para la salida de proxy, blackberry's, NTP (Network Time Protocol) etc..

Que es un sistema autónomo?

En Internet, un sistema autónomo o AS se trata de un conjunto de redes IP y routers que se encuentran bajo el control de una misma entidad (en ocasiones varias) y que poseen una política de encaminamiento similar a Internet.

Caixa Penedès dispone de un Sistema Autónomo de manera que gestiona todo el enrutamiento hacia internet con sus propios routers frontales y su propio direccionamiento IP.

El servicio de entrada a internet está formado por varias capas:

1ª capa: Routers frontales de acceso (contienen todas las rutas de internet)
2ª capa: Firewalls (ofrecen la seguridad por los ataques desde internet)
3ª capa: Balanceadores (balancean los servicios para dar redundancia)
4ª capa: Hosts (dan servicio de Internet Explorer o de Apache)
5ª capa: Firewalls (dan la seguridad al BBlock de internet contra los demás BBlocks)

En la siguiente imagen se puede observar la infraestructura del Sistema Autónomo de Internet de Caixa Penedès:

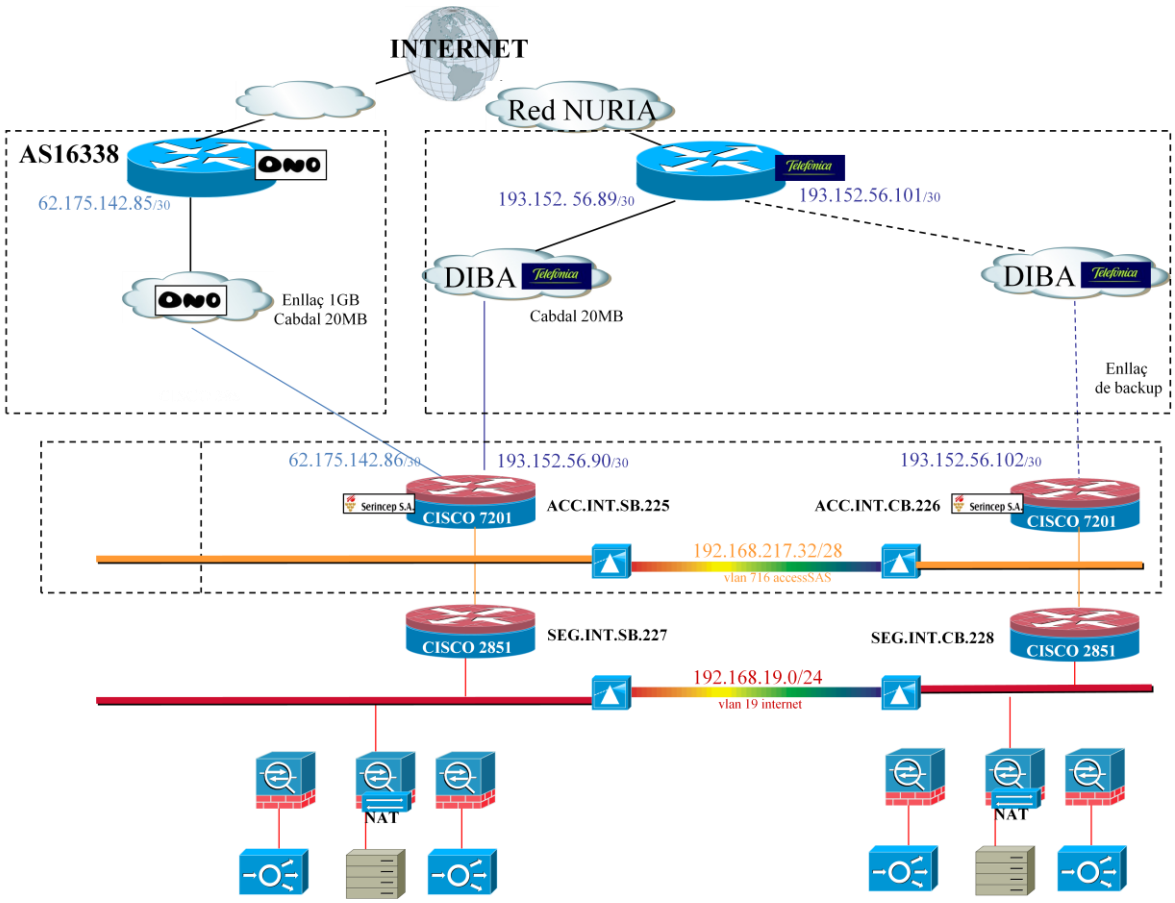


Figura 13: Esquema BBlock Internet

1.2.- Arquitectura WAN (Red MacroLan)

Caixa Penedès dispone de una red MacroLAN contratada a Telefonica. Se trata de una red MPLS, en la cual el cliente contrata vpn's para cada oficina. Las oficinas acceden a la red MPLS a través de una red ATM y una pasarela hacia un PE. Se trata de una tipología mallada en la cual todos los extremos (oficinas y servicios centrales) son visibles entre sí.

Caixa Penedès tiene actualmente unas 550 oficinas repartidas en Catalunya, Aragón, Valencia y Madrid. Todas ellas disponen de una conexión local tipo ADSL (Red ATM) desde la cual acceden a la red MPLS.

Cada oficina, en función del tamaño y por tanto del tráfico que se maneja, tiene contratado un ancho de banda diferente. La mayoría de oficinas tienen contratada ADSL *Advance o Class*

Actualmente existen estos tipos de ADSL en función del ancho de banda:

Tipo ADSL	Velocidad Bajada	Velocidad Subida	Garantía de caudal
Acceso ADSL Premium ACG	8 M	640 K	50%
Acceso ADSL Advance ACG	4 M	640 K	50%
Acceso ADSL Class ACG	2 M	640 K	50%
Acceso ADSL Básico ACG	1 M	320 K	50%
Acceso ADSL TOP	10 M	320 K	0%
Acceso ADSL Premium	8 M	640 K	10%
Acceso ADSL 6 Megas	6 M	300 K	0%
Acceso ADSL Advance	4 M	512 K	10%
Acceso ADSL Máxima	3 M	320 K	0%
Acceso ADSL Class	2M	320 K	10%
Acceso ADSL Básico	1 M	320 K	10%

En la figura 14 se puede observar un esquema de la red MPLS de CEP. En el CPD existen dos EDC's (Electronic Data Capture) uno principal y otro de backup donde se concentra todo el tráfico hacia los host y los servicios que tiene CEP. El ancho de banda contratado para absorber todo el tráfico de oficinas en servicios centrales es de 62 Mbps.

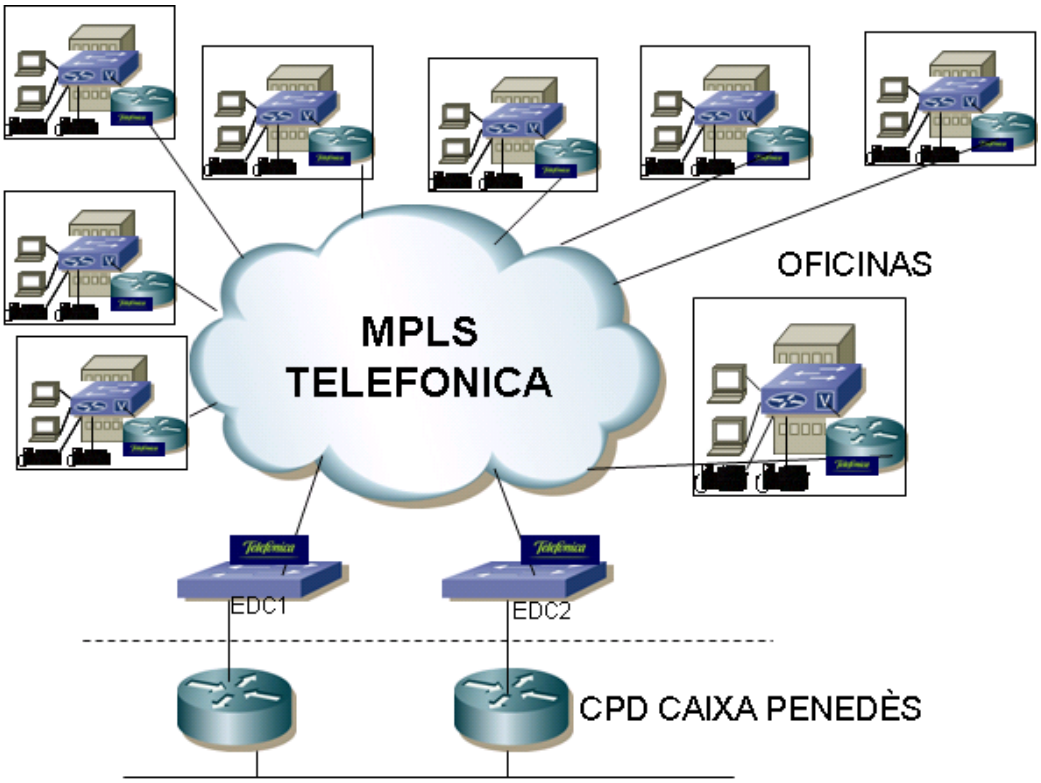


Figura 14: Esquema red MPLS CEP

Telefónica dispone de diferentes calidades de servicio, los paquetes IP se envían a la red MPLS con prioridades en función del tipo de tráfico (voz, transaccional, video etc..).

Los EDC's marcan los paquetes con la el campo DSCP (Differentiated Services Code Point) del paquete IP de manera que cuando estos llegan a la red MPLS se les añade las cabeceras MPLS correspondientes a la calidad de servicio contratada para que puedan ser priorizados y entregados hasta su destino.

MacroLan define tres clases de servicio contratables por el cliente Plata, Oro y Multimedia; más una clase interna adicional para el tráfico de gestión de los EDC's, que es transparente para el cliente.

1- Clase de Servicio PLATA:

Orientada al tráfico Intranet del cliente.
Prioridad normal.
El tratamiento que se hace del tráfico plata, en los EDC's, y PE's (Provider edge) en función del tipo de caudal contratado.
Es la clase de servicio que se asigna por defecto. Cuando un cliente no contrata calidad de servicio, todo su tráfico se cursa como Plata.

2- Clase de Servicio ORO:

Orientada al tráfico Intranet del cliente de aplicaciones críticas.
Prioridad normal.
El tratamiento que se hace del tráfico oro, en los EDC's y PE's, en función del tipo de caudal contratado.
Los SLA's (Service Level Agreement) asociados a la pérdida de paquetes y retardos son más exigentes que los de la clase Plata.

3- Clase de Servicio MULTIMEDIA:

Orientada al tráfico muy sensible al retardo y/o jitter (VoIP multimedia, etc...).
Máxima Prioridad.
Los SLA's asociados a retardos son más exigentes que los del resto de clases.
Además lleva asociado un SLO (Service level objective) de jitter.
El tratamiento que se hace del tráfico multimedia, en los EDC's y PE's, en función del tipo de caudal contratado.
El tráfico asociado a VoIP (Ibercom IP básicamente) se cursa con esta clase de servicio.

4- Clase de Servicio GESTIÓN:

Asociada al tráfico de gestión de los EDCs. No es una clase de servicio contratable por el cliente.
Caudal garantizado en cada conexión de acceso a la MAN y en la conexión con la red IP/MPLS.

Caixa Penedès tiene contratada la clase de servicio PLATA que es la que menos calidad aporta a la red. Una vez estudiada la arquitectura y las necesidades de la aplicación se recomienda contratar la clase de servicio MULTIMEDIA en la red MacroLAN y las conexiones locales en oficinas deberían ser como mínimo Advance pero con garantía de caudal del 50%.

Conceptos y compromisos de red de Telefónica

a) Perdida de paquetes

Telefónica garantiza que el valor de pérdida de paquetes en su Red IP, se encuentra por debajo de un valor máximo para cada una de las Clases de Servicio. La pérdida de paquetes es un concepto global para la red sobre la que se mide. Como depende de ésta y no del cliente, los valores medidos en la red son aplicables para todos los clientes. Hay un valor de pérdida de paquetes diferente por cada tipo de Clase de Servicio.

Condiciones:

Al ser un parámetro de red, no se incluye en el cálculo, los tiempos correspondientes a los accesos. También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN.

Cálculo Pérdida Diaria de Paquetes:

Se mide como el valor medio máximo diario de los porcentajes de paquetes perdidos entre los nodos de la Red IP. Se corresponde con el valor más alto de la pérdida de paquetes entre nodos. Se calcula como la media aritmética de todos los valores medidos (por clase de servicio) para obtener un valor único por cada CoS.

Pérdida Diaria de Paquetes	SLA
Clase Plata	< o igual 0.9 %
Clase Oro	< o igual 0.8%
Clase Multimedia	< o igual 0.7%

b) Retardo de Tránsito en red IP

El Retardo en red IP es el tiempo de transmisión medio en milisegundos entre los nodos de la red. Se considera como tiempo de transmisión, el tiempo de ida y vuelta de un paquete de prueba. El retardo de tránsito es un concepto global para la red sobre la que se mide. Como el retardo depende de la red y no del cliente existirá un valor único válido para todos los clientes de Telefónica. Hay valores diferenciados para cada Clase de Servicio.

Condiciones:

Al ser un parámetro de red, no van incluidos en el cálculo de los tiempos los correspondientes a las líneas de acceso. También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN (sólo aplica este SLA para caudales Nacionales de MacroLAN).

Cálculo Retardo de Tránsito Diario:
El sistema de Gestión de Red realizará medidas periódicas de retardo entre los distintos nodos de la Red IP, generando una tabla con las sucesivas medidas. Diariamente se calculará la media aritmética de estas medidas para obtener un valor único para cada clase de servicio.

Retardo Diario de Tránsito	SLA
Clase Plata	45msg
Clase Oro	35msg
Clase Multimedia	25msg

C) Jitter en la red IP

El Jitter en Red IP es un parámetro que se mide únicamente en la clase multimedia. Se define como la diferencia de retardo entre un paquete y el siguiente en la transmisión de la comunicación.

Condiciones:
Al ser un parámetro de red, no se incluye en el cálculo, los tiempos correspondientes a los accesos. También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN (sólo aplica este SLA para caudales Nacionales de MacroLAN).

Cálculo Jitter Diario:
Se calcula como la media aritmética de todos las medidas hechas periódicamente.

Se establece un compromiso de jitter medio diario

Jitter Diario	SLA
Clase Multimedia	2msg

1.3.- Integración de CUVM

Una vez explicados con más detalle los BBlock's implicados en el funcionamiento de CUVM, vamos a ver en que BBlock queda incluido CUVM y que conectividades necesita con los demás BBlock's.

Conectividades necesarias del servicio CUVM

- Es necesario que los usuarios puedan acceder desde internet, ha de ser un servicio público y que debe ser seguro.
- Es necesario que los usuarios que se encuentran tanto en oficinas (WAN) como en servicios centrales (LAN) tengan acceso.
- El servidor CUVM, requiere conectividad con la MCU que se encuentra en el BBlock de Voz/Video .

Teniendo en cuenta las conectividades necesarias y la seguridad que este servicio requiere, se ha decidido ubicar el servidor dentro del BBlock de internet y concretamente en una DMZ. El servidor tendrá dos tarjetas de red, una para el acceso desde internet y otra para el acceso desde redes internas. Se comunicará con los BBlock's de Voz/Video, Planta y WAN a través de la red interna.

Esquema general por capas de la conectividad del servidor CUVM dentro del BBlock de internet:

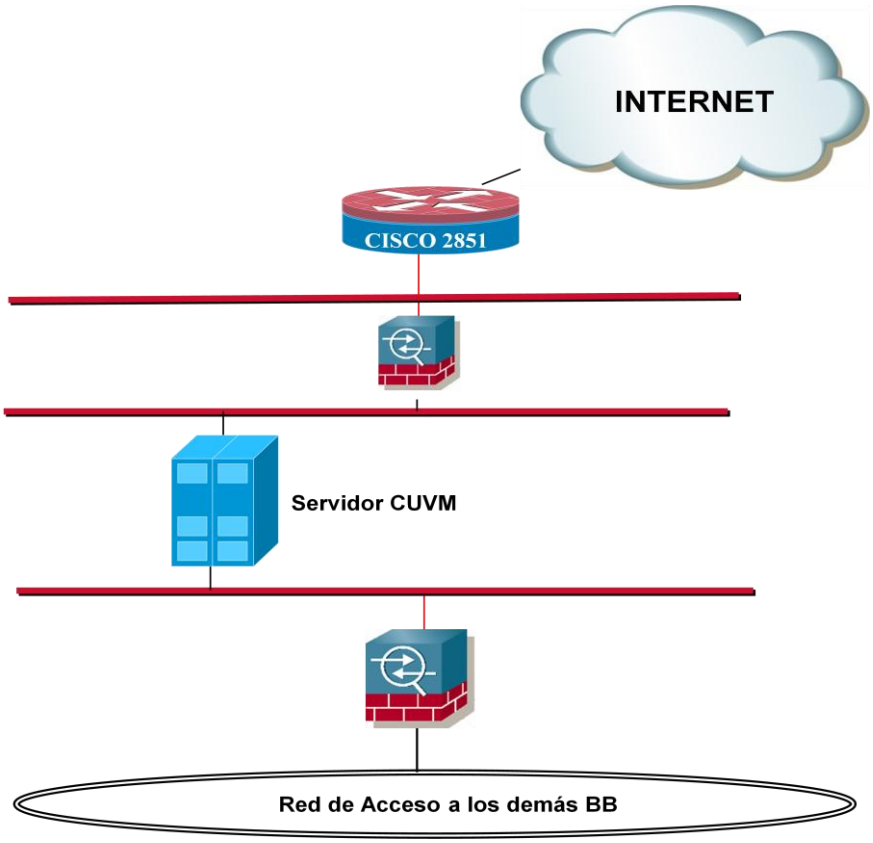


Figura 15: Esquema conectividad CUVM

V – CONFIGURACIÓN E INSTALACIÓN

1.- Instalación

1.1.- Instalación del componente Cisco Unified Videoconferencing Manager (CUVM)

A continuación se detallan los pasos a seguir para realizar la instalación del componente principal del sistema:

Pasos a seguir:

1- Ejecutar el instalador de CUVM para empezar la instalación.
2- Botón Siguiente en la ventana de Introducción.
3- Leer y aceptar la licencia del producto.
4- Dejar la opción por defecto en el tipo de instalación a realizar.
5- Seleccionar la carpeta donde se quiere realizar la instalación.
6- Introducir el nombre del equipo, en este caso ***CEPVCM.caixapenedes.com***.
7- Seleccionar el tipo de base de datos, en este caso Base de datos Interna.
8- Introducir la información del servidor de correo para que el sistema pueda enviar e-mails. En este caso es *mailcep.caixapenedes.com.*
9- Crear una cuenta de administrador para la configuración del sistema. En este caso Usuario**: *administrator Password: xxxxx***
10- Repasar el resumen de la instalación en la ventana de pre-instalación y proceder con la Instalación.
11- No interrumpir la instalación, después dejar que el sistema se inicie tras varios minutos, ya es posible hacer login en la interfaz web de configuración.

1.2.- Instalación del componente Cisco Unified Videoconferencing Desktop (CUVM-D)

A continuación se detallan los pasos a seguir para realizar la instalación del componente Desktop del sistema:

Pasos a seguir:

1- Ejecutar setup.exe del CD-ROM de instalación.
2- Seleccionar el idioma de instalación, en este caso **inglés** y seguir con la instalación.
3- Leer y aceptar la licencia del producto.
4- Introducir la el número serie para activar la licencia.
5- Especificar la carpeta destino de la instalación. Por defecto ***C:\Program Files\Darwin Streaming Server.***
6- Configurar el puerto del servidor web en la ventana de configuración de red del sistema. En este caso configuramos el ***puerto 80.***
7- Repasar la configuración y proceder con la instalación.

2.- Configuración

2.1.- Configuración de la Infraestructura de red de Caixa Penedès

Configuración del switch

El switch da conectividad a nivel 2. Se trata de un Cisco Catalyst 3750 que tiene 24 interfaces que pueden llegar a 1Gigabit de velocidad.

Figura 16: Switch Cisco Catalyst 3750

A nivel 2 el switch funciona por VLAN'S (Virtual Lans), este tiene creadas todas la vlan's para conectar cualquier equipo dentro del BBlock de internet. A nivel de nuestro sistema la configuración del swich es la siguiente:

```
vlan 692
 name transbalint1
  private-vlan primary
  private-vlan association 687-691
!
Vlan 221
name transint
!
interface GigabitEthernet1/0/14
 description .SWI.HOS.692.CEPVCM
 switchport access vlan 692
 switchport private-vlan host-association 692 687
 switchport mode private-vlan host
 spanning-tree portfast
end
¡
¡
interface GigabitEthernet1/0/24
 description .SWI.HOS.221.CEPVCM
 switchport access vlan 221
 switchport mode access
 spanning-tree portfast
end
```

La vlan 692 es la que da conectividad externa (DMZ internet), se trata de una red aislada para obtener seguridad a nivel 2.

La vlan 221 es la que da conectividad interna, se utiliza para acceder al servidor internamente.

Configuración de red del servidor CUVM

Para la infraestructura que tiene la red de Caixa Penedès es necesario que el servidor tenga configuradas dos tarjetas de red, una da la conectividad interna y la otra conectividad a través de internet.

Direcciones IP asignadas al servidor:

IP red interna: **192.168.221.19 255.255.255.0**

IP DMZ internet: **192.168.218.141 255.255.255.128** Puerta de Enlace: **192.168.218.132**

IP pública: **93.92.230.23 255.255.255.0** Nombre en internet: **vc.serincep.com**

Para acceder al servidor desde la redes internas se añaden rutas a través de la puerta de enlace **192.168.221.254**. En la siguiente figura se puede ver como queda configurado el servidor a nivel de red:

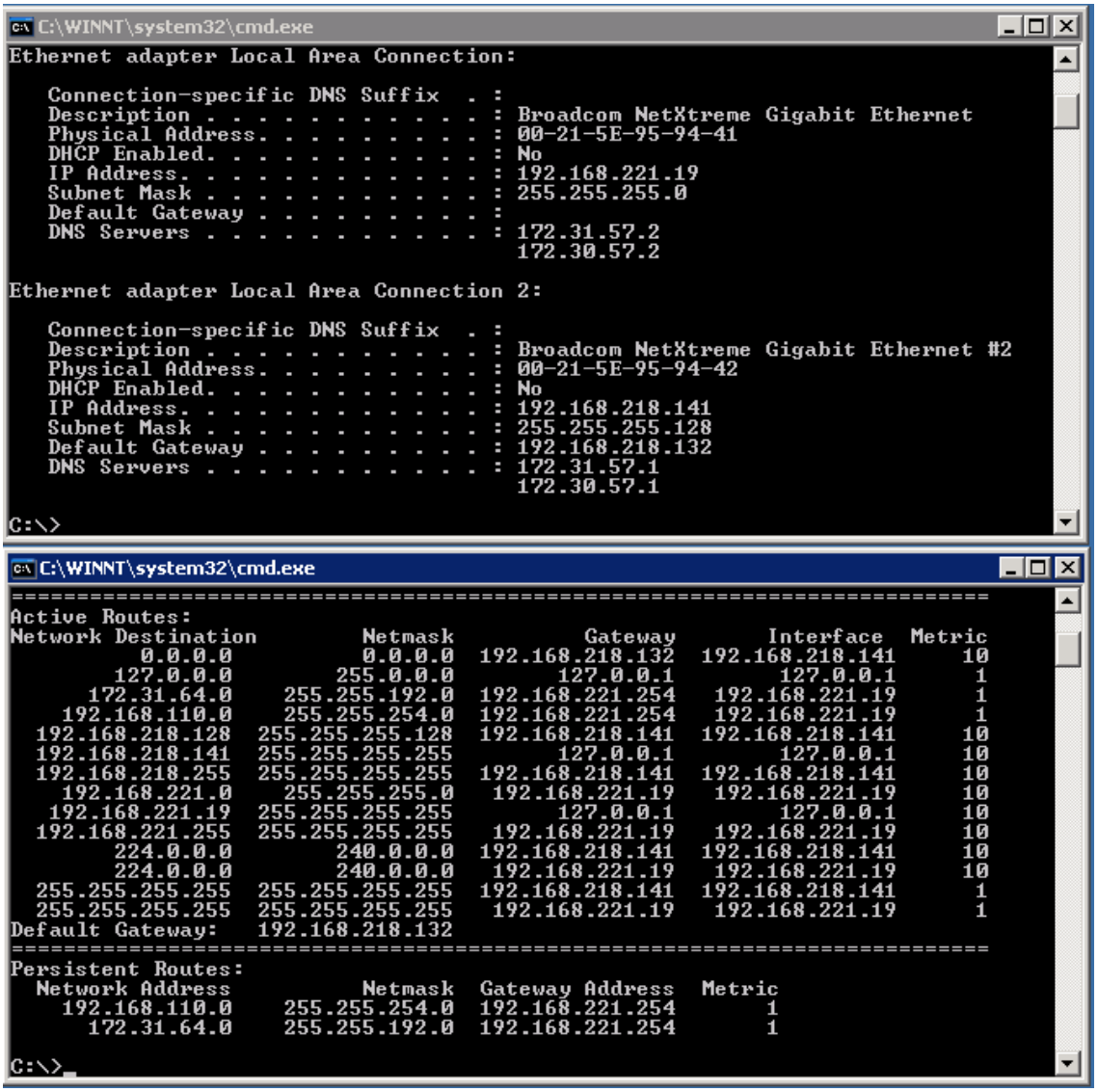


Figura 17: Configuración de red y rutas del servidor CUVM

Configuración de los firewalls y puertos internos

A continuación se muestra una tabla donde aparecen todos los puertos necesarios para el correcto funcionamiento del servidor, tanto para conexiones internas del servidor como externas.

CUVM

Protocolo	Puerto	Tipo	Propósito	Destino
HTTP	80	TCP	Servicio y acceso web.	CUVM
HTTPS	443	TCP	Servicio y acceso web seguro	CUVM
VIDEO	4684 - 4686	UDP	Servicio de Video+Audio	CUVM
XML	3386	TCP	Control de llamadas de la MCU	CUVM
SNMP	161	UDP	Configuración y estado del servicio	CUVM
FTP	21	TCP	Recuperación de logs.	CUVM
XML	3271	TCP	Conexión interna del Resource Manager con la API del gatekeeper.	CUVM
Conexión Base de datos	3306	TCP	Para la conexión con la base de datos interna.	CUVM
TCP	7070	TCP	Puerto Streaming	CUVM

MCU

Protocolo	Puerto	Tipo	Propósito	Destino
HTTP	80	TCP	Acceso web	MCU
XML	3336	TCP	Control de llamadas de la MCU	MCU
XML	3337	TCP	Control de cascada de la MCU.	MCU
SNMP	161	UDP	Configuración y estado del servicio	MCU
Telnet	23	TCP	Recuperación de Logs	MCU

A nivel de firewalls, existen dos de ellos en la infraestructura, uno que ofrece la seguridad para la conectividad con internet y el otro que ofrece la seguridad con las LAN's y con los BBlock's internos.

En el firewall externo (DMZ internet) se crean las siguientes reglas de acceso y de NAT (Network Address Translation):

! Definición de la ip interna:

name 192.168.218.141 NAT_h0000cepvideo
host 192.168.218.141
!

! Definición de la ip pública

name 93.92.230.23 h0000cepvideo
host 93.92.230.23

!

! Traducción de la ip pública a la ip interna:

object network NAT_h0000cepvideo
nat (inside,outside) static h0000cepvideo

! Grupo de puertos de acceso al servidor:

object-group service DM_INLINE_TCP_1 tcp
port-object eq 7070
port-object eq www
port-object eq https
!

! Regla de acceso desde cualquier ip origen y destino la ip del servidor y los puertos definidos anteriormente en el grupo DM_INLINE_TCP_1

access-list outside_access_in extended permit tcp any host 192.168.218.141 object-group DM_INLINE_TCP_1 tcp

En el firewall interno se crean las siguientes reglas de acceso:

! Grupo de equipos a los que se conecta el servidor: MCU, Call Manager y Gatekeeper

object-group network EQUIPS_VEU
network-object host MCU.VEU.SB.131
network-object host MCU.VEU.SB.131B
network-object host CEPCM1
network-object host CEPCM2
network-object host TRC.VEU.SB.68
network-object host CEPCM3

! Regla de acceso que permite ip contra el grupo de equipos anterior.

access-list DMZInt_access_in extended permit ip host CEPVCM object-group EQUIPS_VEU

! Regla de acceso que permite acceso al servidor de correo por smtp.

access-list DMZInt_access_in extended permit tcp host CEPVCM host mailcep eq smtp

2.2.- Configuración del componente CUVM-D

Este componente permite la realización de reuniones interactivas on-line y de streaming.

La interfaz de configuración es la siguiente:

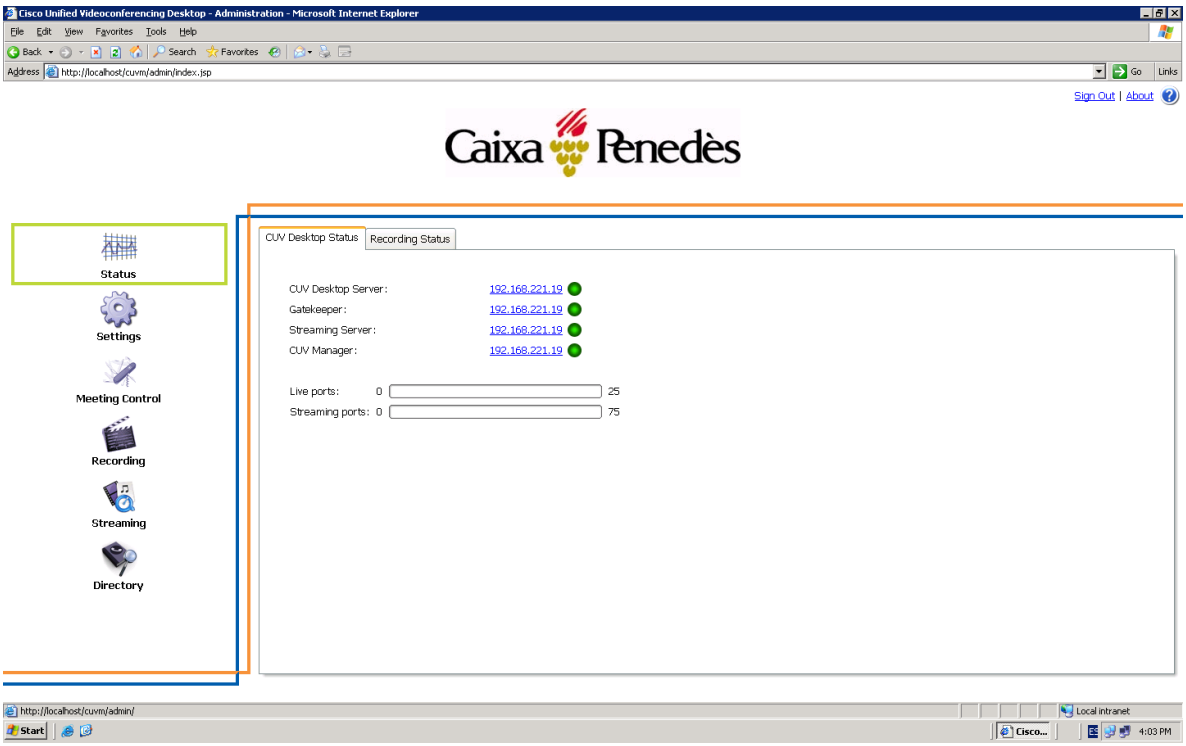


Figura 18: Pantalla configuración del componente CUVM-D

En esta pantalla se puede ver el estado del servidor y de los servicios de este componente. También podemos ver que no hay puertos de video ni puertos de streaming que se estén utilizando.

En el apartado ***Configuración*** configuramos los siguientes parámetros:

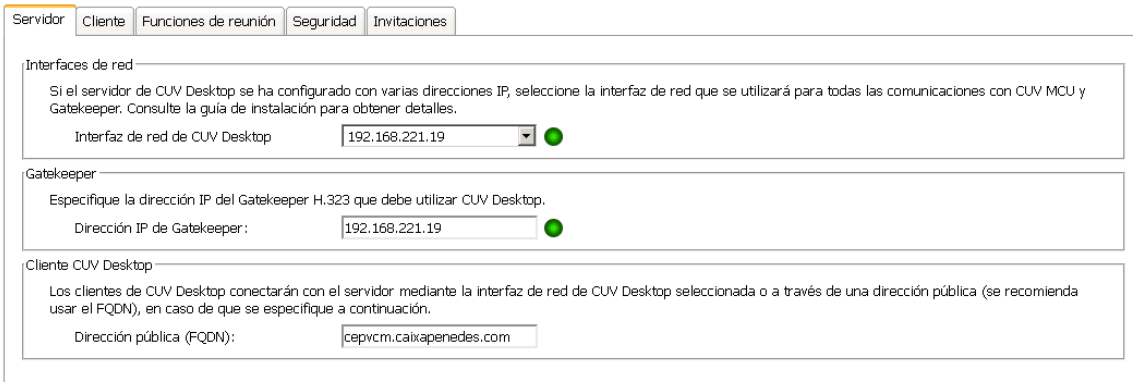


Figura 19: Configuración del servidor

El primer parámetro es la dirección ip desde la cual el servidor se comunicara con la MCU y el gatekeeper, en este caso es la ip de la red interna.

El segundo parámetro es la ip del gatekeeper, en este caso es la ip de la red interna ya que el gatekeeper esta interno en el servidor. Más adelante se explicara la configuración concreta del gatekeeper.

El tercer parámetro es el nombre DNS con el que se conectaran los clientes al servidor para realizar las reuniones.

En la pestaña de ***Meeting Features*** habilitamos el servicio de compartición de escritorio y también el de chat.

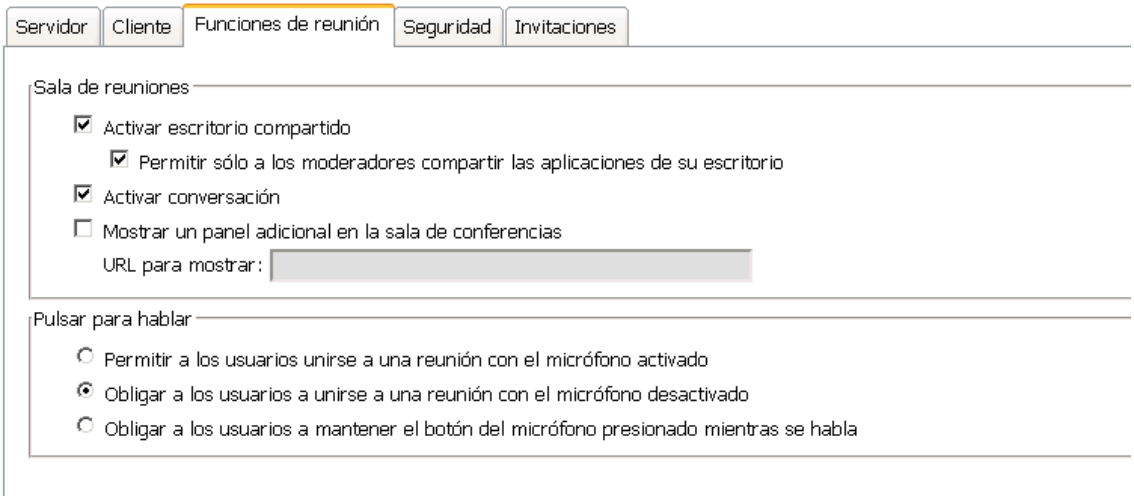


Figura 20: Configuración de las reuniones interactivas

En el apartado ***Control de reuniones*** configuramos los siguientes parámetros:

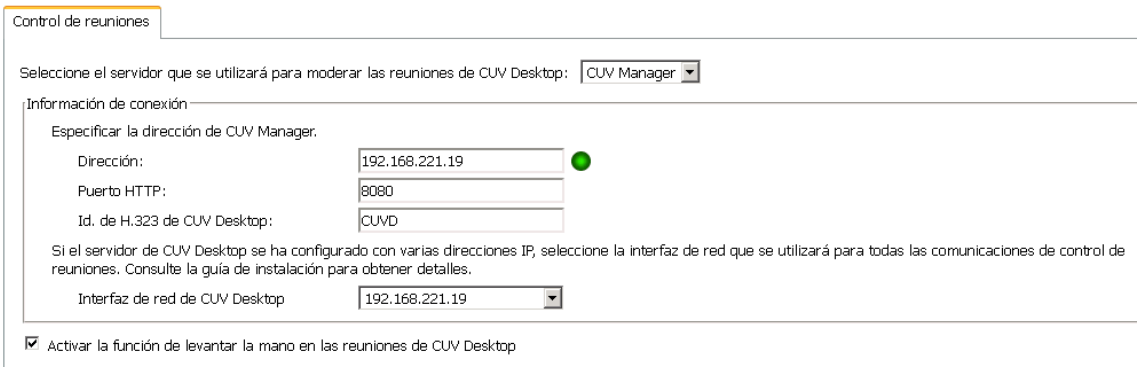


Figura 21: Configuración del control de reuniones

Para el control de las reuniones, es necesario configurar la ip del componente CUVM (Manager) el puerto que utilizaremos y el identificador H323.

En el apartado de ***Grabación*** configuramos los siguientes parámetros:

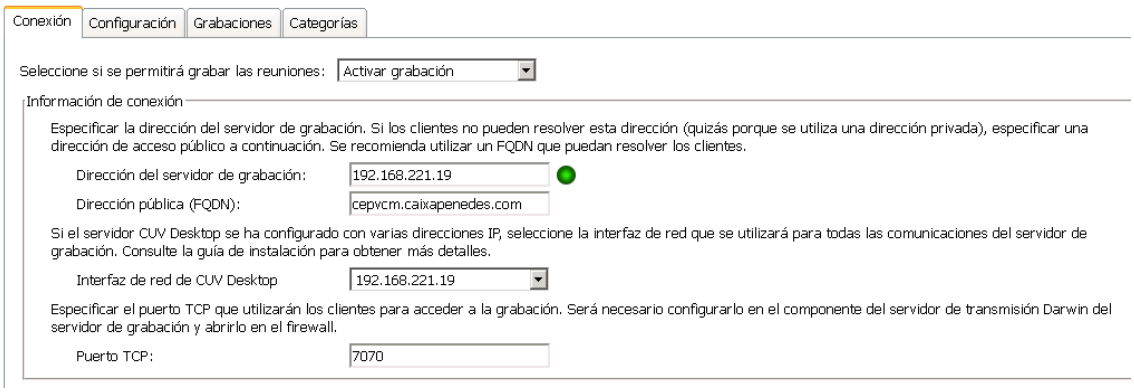


Figura 22: Configuración de las grabaciones

En este apartado configuramos todo lo referente a las grabaciones de las reuniones, se configura la ip de servidor que realiza la grabación, el nombre por el que accederán los clientes a las grabaciones y el puerto por el que accederán.

En el apartado de ***Streaming*** configuramos los siguientes parámetros:

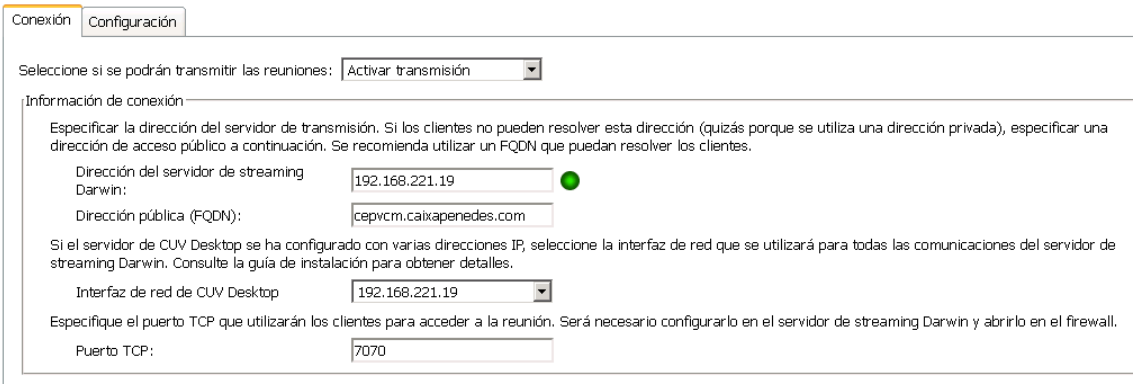


Figura 23: Configuración del apartado de streaming

En este apartado se habilita el servicio de streaming, también se configura la ip del servidor que realizará el streaming y el puerto.

2.3.- Configuración del componente CUVM

Dentro de este componente existe la parte de administración del sistema y la parte de usuario, desde la cual se programan las reuniones. En este apartado se va a explicar la configuración de la parte de administración.

Para entender el funcionamiento de este componente, es necesario explicar la integración del sistema con los diversos componentes de videoconferencia.

Con estas configuraciones en todos los dispositivos conseguimos integrar todos los componentes para poder realizar videoconferencias o audio conferencias desde un dispositivo que se encuentre en el Call Manager, un ejemplo de esto podría ser empezar una videoconferencia desde un teléfono IP registrado en el Call Manager.

Integración con Call Manager:

Que es el Call Manager?

Cisco Unified Communications Manager (CUCM), más conocido como Call Manager es un software basado en un sistema de tratamiento de llamadas y telefonía sobre IP, desarrollado por Cisco Systems.

CUCM rastrea todos los componentes telefonía IP activos en la red, esto incluye teléfonos, gateways, puentes para conferencia, recursos para transcodificación, y sistemas de mensajería de voz, entre otros. Call Manager a menudo utiliza el SCCP (Skinny Client Control Protocol) como un protocolo de comunicaciones para la señalización de parámetros de hardware del sistema, tales como teléfonos IP.

A continuación hay un esquema sobre el funcionamiento de los gatekeepers, Call Manager y MCU dentro del sistema.

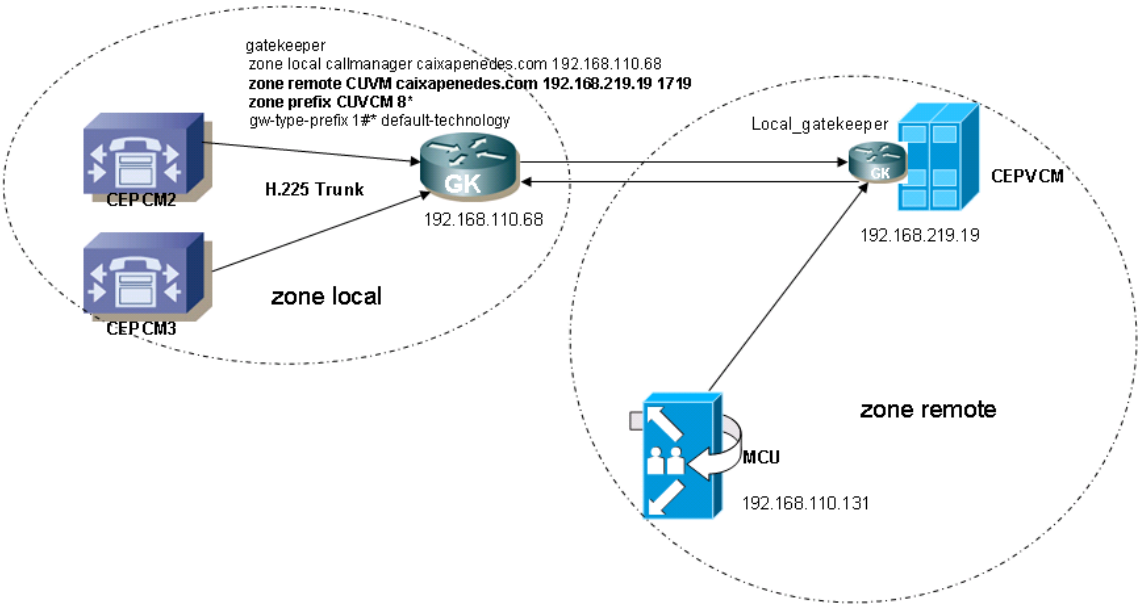


Figura 24: Esquema integración Call Managers

Los gatekeepers funcionan por zonas, existen dos gatekeepers, uno es interno del sistema CUVM (zone remote) y el otro es un IOS gatekeeper que está registrado en el Call Manager (zone local).

Estos gatekeepers se comunican entre ellos para intercambiar información sobre los dispositivos registrador y poder integrarlos de la manera más transparente posible con el plan de numeración existente.

La MCU (componente hardware principal para realizar videoconferencias) se registra en el gatekeeper interno para que el sistema CUVM para que el sistema lo utilice como recurso.

La configuración del IOS (Internetwork Operating System) gatekeeper es la siguiente:

gatekeeper
zone local callmanager caixapenedes.com 192.168.110.68
zone remote CUVCM caixapenedes.com 192.168.219.19 1719
zone prefix CUVCM 8*
gw-type-prefix 1# default-technology*

En esta configuración se puede observar que existen dos zonas, la zona local es la zona por defecto (la ip es la del mismo gatekeeper) y la zona remote es la zona donde se encuentra el sistema CUVCM donde se envía la numeración 8* para que el gatekeeper remoto resuelva la numeración h323.

El Call Manager se registra en este gatekeeper para que este pueda resolver la numeración h323 de las zonas o de los dispositivos que tenga registrados.

La configuración del Call Manager es la siguiente:

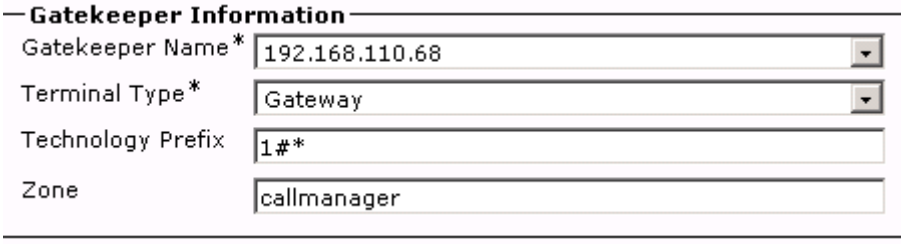


Figura 25: Configuración Gatekeeper en el Call Manager

Se configura un trunk h225 en el Call Manager para que este se pueda comunicar con el gatekeeper y resolver numeración h323. Para poder enviar la numeración hay que configurar una "ruta" en el Call Manager

ROUTE PATTERN 85XXX -> TRUNK GATEKEEPER (PARA VIDEO)
ROUTE PATTERN 80XXX -> TRUNK GATEKEEPER (PARA AUDIO)

La configuración del gatekeeper local del sistema CUVM es la siguiente:

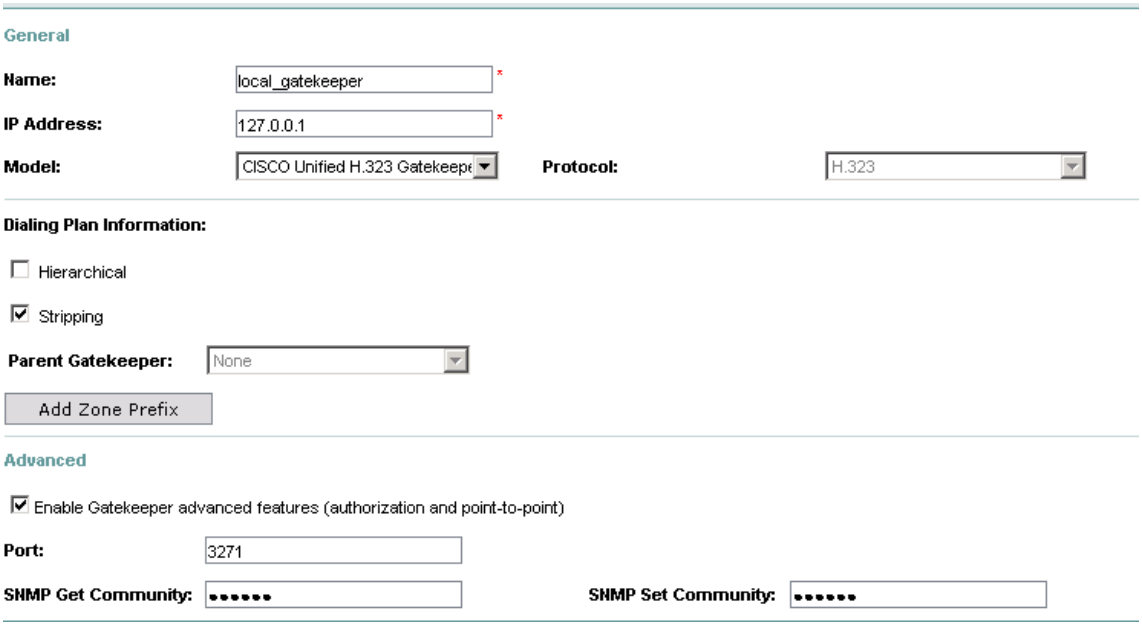


Figura 26: Configuración del gatekeeper en el CUVM

En esta configuración se puede observar que el gatekeeper es interno ya que la dirección IP es la interna del sistema y que se trata de un gatekeeper H323.

En este gatekeeper se registra la MCU para poder utilizarla como recurso. La configuración de la MCU es la siguiente:

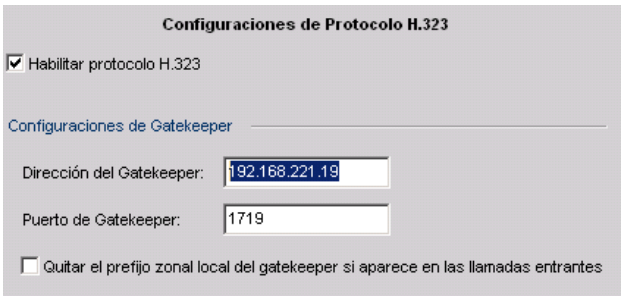


Figura 27: Configuración del gatekeeper en la MCU

El puerto que se utiliza para registrar dispositivos H323 en el gatekeeper es el 1719.

Integración con la MCU

La MCU es el recurso necesario para que el sistema pueda realizar videoconferencias, ya que es este hardware el que se encarga de "merzclar" el video y enviarlo a los clientes.

Esta es la configuración necesaria dentro del componente CUVM. Se le configura la IP de la MCU, el nombre, el modelo y se le dice en que gatekeeper está registrada. Tal y como se ha explicado en el apartado anterior, la MCU se registra en el gatekeeper interno para que este pueda gestionar las videoconferencias por h323.

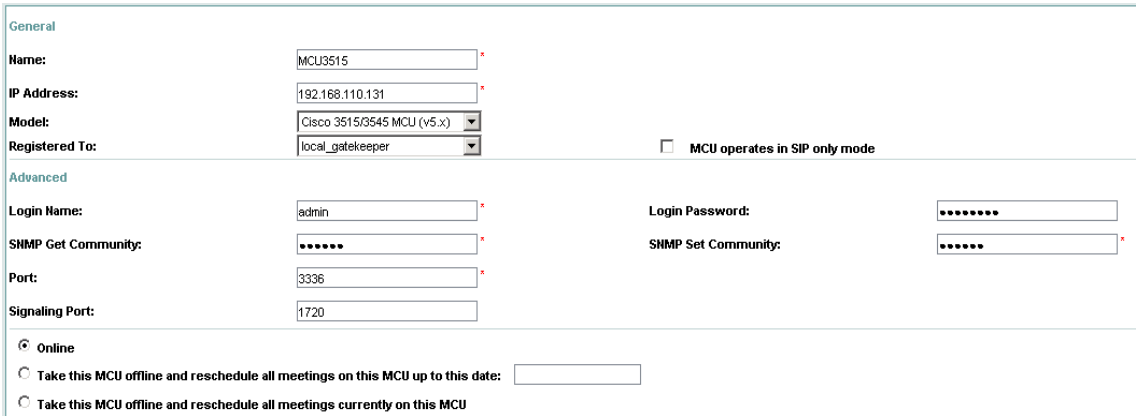
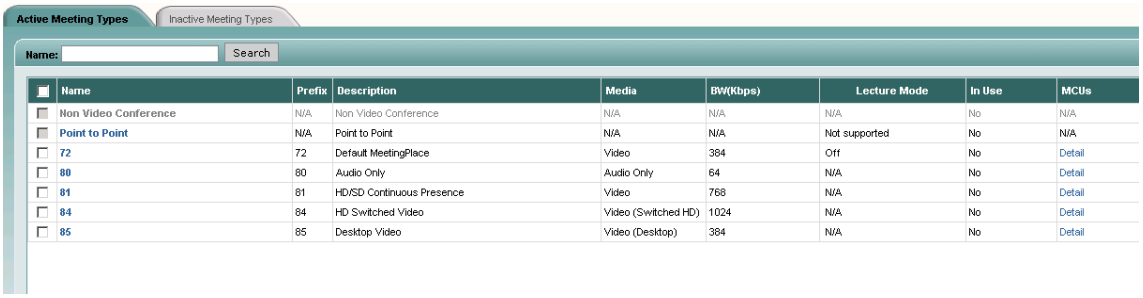


Figura 28: Configuración de la MCU en el servidor

Tipos de reuniones

En este apartado, se configuran los diversos prefijos para acceder los diversos tipos de videoconferencias, en este caso, al haber realizado la integración con la MCU, los prefijos vienen predefinidos.



Name	Prefix	Description	Media	BW(Kbps)	Lecture Mode	In Use	MCUs
Non Video Conference	N/A	Non Video Conference	N/A	N/A	N/A	No	N/A
Point to Point	N/A	Point to Point	N/A	N/A	Not supported	No	N/A
72	72	Default MeetingPlace	Video	384	Off	No	Detail
80	80	Audio Only	Audio Only	64	N/A	No	Detail
81	81	HD/SD Continuous Presence	Video	768	N/A	No	Detail
84	84	HD Switched Video	Video (Switched HD)	1024	N/A	No	Detail
85	85	Desktop Video	Video (Desktop)	384	N/A	No	Detail

Figura 29: Configuración del tipo de reuniones

La MCU permite todos estos tipos de videoconferencia:

Audio Only: para realizar solo audio conferencias entre varios participantes (hasta 70 participantes de manera simultánea)

HD/SD Continuous Presence: para realizar videoconferencias de manera continua en HD/SD.(hasta 24 usuarios de manera simultánea).

HD Switched Video: para realizar videoconferencias de manera que se enfoca a la persona que esta hablando.

Desktop Video : este es el tipo de videoconferencia que utiliza el componente CUVM-D que es accesible vía web.

Cada tipo de videoconferencia tiene un prefijo predefinido para que la MCU pueda diferenciar que tipo se requiere realizar en cada momento.

Configuración de usuarios y reuniones

Existe un apartado donde se configuran los usuarios que se pueden registrar en el sistema para programar reuniones y reservar recursos. Estos usuarios pueden tener asignadas "virtual rooms" (salas de videoconferencia con parámetros predeterminados por el administrador).

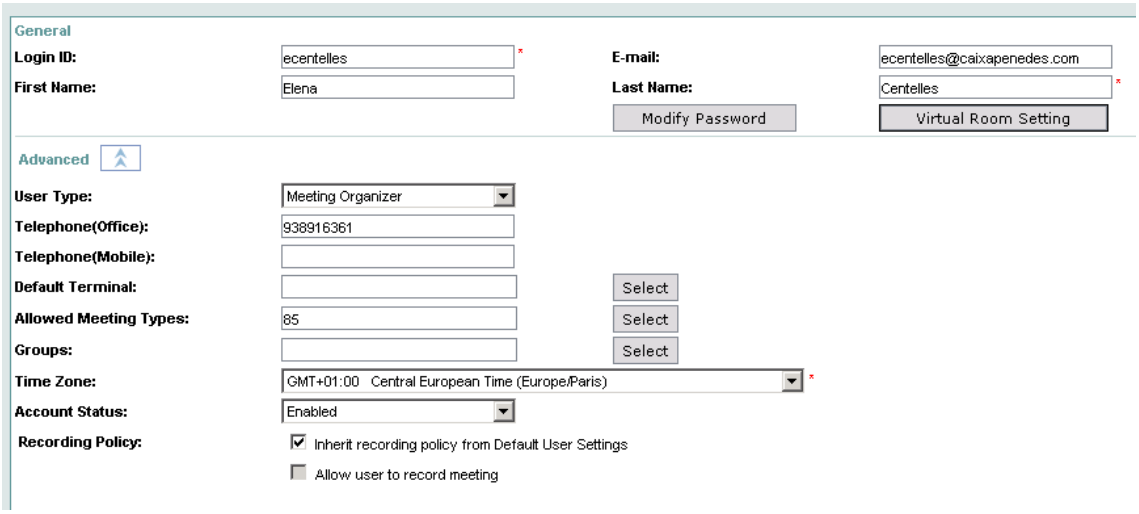


Figura 30: Configuración de usuarios

Existe otro apartado donde se configuran las características de cada tipo de reunión, en este caso, solamente vamos a configurar el tipo de reunión Desktop Video que es la que se requiere para el proyecto.

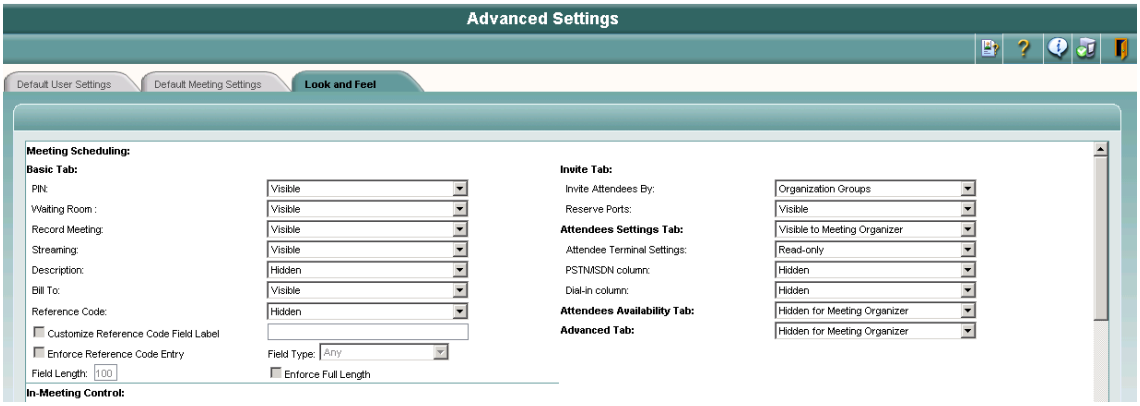


Figura 31: Configuración de una reunión tipo interactiva.

VI – PRUEBAS DEL SISTEMA

1.- Pruebas sobre funcionalidades e integración del sistema

Para probar el funcionamiento del sistema, se han realizado las siguientes pruebas internamente, es decir, con clientes en servicios centrales, se da por supuesto que no hay problemas de ancho de banda ya que se trata de una LAN. Se prueban todos los escenarios posibles dentro del sistema.

a) Se realiza una reunión entre 3 empleados + 1 profesor de manera interactiva i programada por e-mail.

En la figura 32 se puede ver como la pantalla se va partiendo en función del número de empleados conectados.

Figura 32: Imagen de la videoconferencia

En la figura 33 podemos ver que se está presentando un documento Power Point y a un lado queda la imagen.

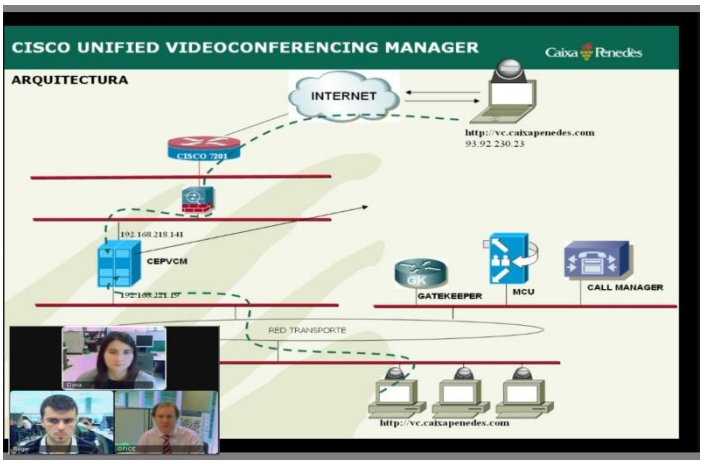


Figura 33: Imagen de la reunión con presentación

En la figura 34 se puede ver el e-mail que reciben los empleados para asistir a la reunión. Solo es necesario acceder al link que viene adjunto.

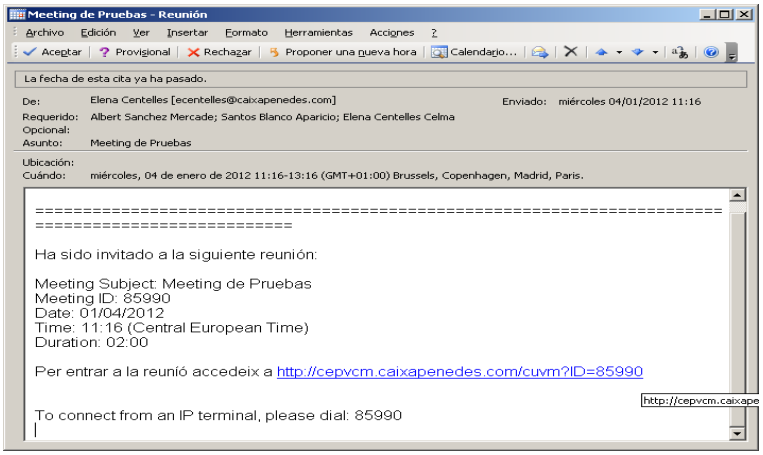


Figura 34: Email de invitación a una reunión

b) Se realiza una reunión entre empleados vía web y con empleados solo por audio.

Puede interesar que haya empleados que puedan acceder vía teléfono solamente para escuchar. Solo deben llamar al número de la videoconferencia que se haya asociado a un número externo previamente en el Call Manager.

c) Grabación de una reunión y posterior visionado vía Streaming.

En este caso se graba una reunión previamente con contenidos ya predefinidos y los empleados pueden ver la presentación en cualquier momento.

d) Empezar una reunión con videoconferencia desde un teléfono cisco.

En este caso un usuario con un teléfono IP y que tenga webcam puede empezar una videoconferencia y a través de los botones del teléfono ir agregando empleados a la misma reunión sin tener que configurar previamente nada más.

2.-Pruebas del sistema sobre Oficinas

Para poder ver el impacto que puede tener la aplicación en la red de oficinas se prueba realizar una reunión interactiva en la oficina de pruebas de Caixa Penedès y medir el ancho de banda que necesita para funcionar y poder extrapolarlo a las demás oficinas. Se entiende que el "profesor" se conecta a la reunión des de Servicios Centrales.

Disponemos de una herramienta llamada *Netflow Tracker* de Fluke Networks que a través del protocolo netflow es capaz de analizar el tráfico de routers y switch's para realizar estudios del tráfico de la red.

Descripción de la oficina de pruebas:
Se trata de una oficina que se utiliza para probar cualquier aplicación que se quiera poner en producción y que a nivel de comunicaciones tiene una ADSL tipo Advance (4 Mbps de bajada y 512 Kbps de subida) que se conecta a la red MPLS para tener conectividad con todas las oficinas y con Servicios Centrales.

Se programa una reunión interactiva de una hora de duración (7:00–8:00 p.m) entre un PC de una oficina y un PC de servicios centrales (que será el profesor y realizará una presentación). Vamos a medir el tráfico de subida y de bajada que necesita la aplicación para funcionar en una oficina.
La dirección ip del PC de la oficina es la **200.9.62.9** y el servidor es **cepvcm.caixapenedes.com.**

a) Gráfica del tráfico de subida para la oficina. Servidor -> Cliente

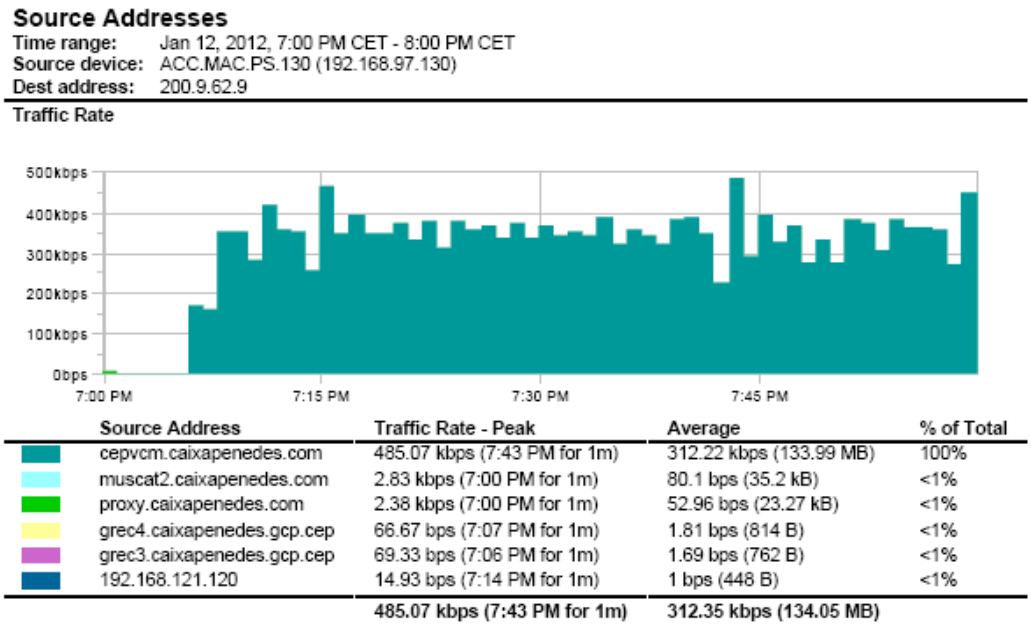


Figura 35: Tráfico origen servidor destino cliente

En la gráfica se observa que el tráfico que envía el servidor al cliente de media es de **312 kbps** . En este tráfico va incluido el video (mezclada por la MCU), el audio y la presentación que se está realizando

b) Gráfica del tráfico de bajada para la oficina. Cliente-> Servidor

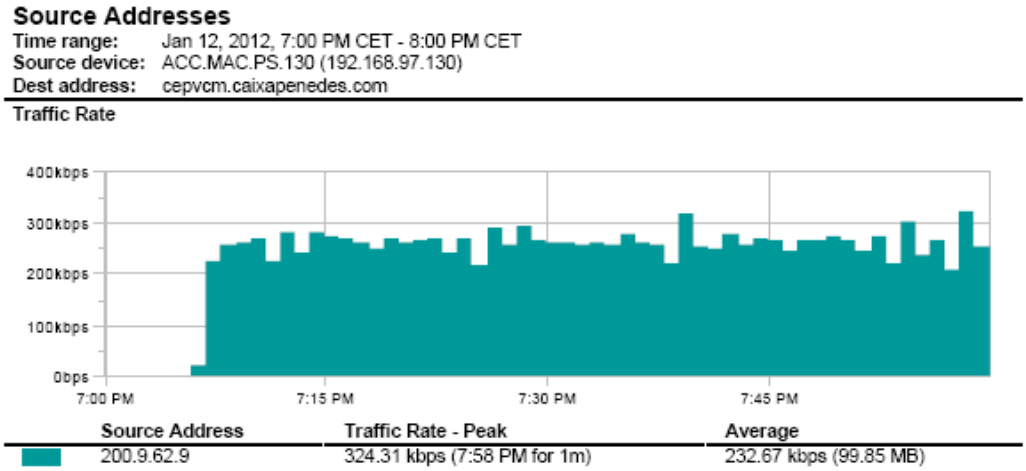


Figura 36: Tráfico origen cliente destino servidor

En la gráfica se observa que el tráfico que envía el cliente es menor que en la gráfica anterior ya que este solo envía la parte de un cliente. La media es de unos **232 kbps.**

c) Grafica de los puertos a los que se conecta el cliente contra el servidor

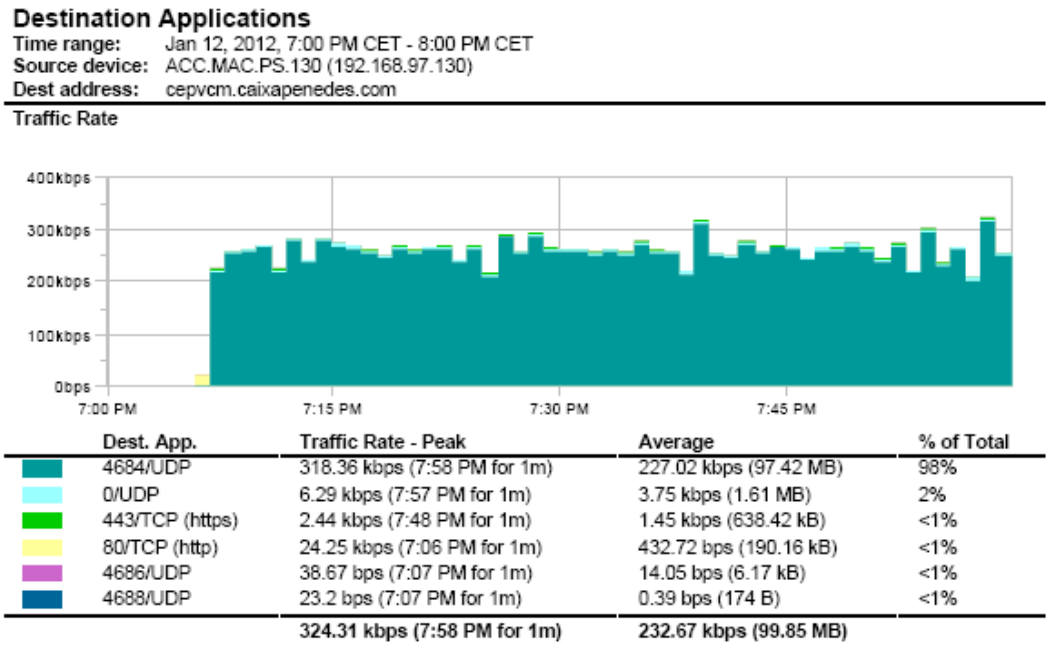


Figura 37: Puertos entre cliente y servidor

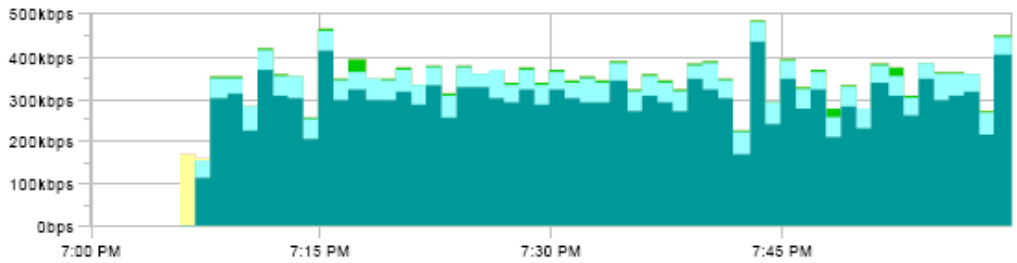
En esta gráfica se puede observar los puertos que utiliza el cliente contra el servidor para conectarse. La mayor parte del tráfico es UDP (vídeo y audio) y se conecta a través del puerto 4684.

d) Grafica de los puertos a los que envía tráfico el servidor hacia el cliente

Source Applications

Time range: Jan 12, 2012, 7:00 PM CET - 8:00 PM CET
Source device: ACC.MAC.PS.130 (192.168.97.130)
Source address: cepvcm.caixapenedes.com
Dest address: 200.9.62.9

Traffic Rate



Source App.	Traffic Rate - Peak	Average	% of Total
4684/UDP	437.73 kbps (7:43 PM for 1m)	264.33 kbps (113.44 MB)	85%
4686/UDP	64.9 kbps (7:26 PM for 1m)	40.18 kbps (17.24 MB)	13%
443/TCP (https)	26.79 kbps (7:17 PM for 1m)	4.8 kbps (2.06 MB)	2%
80/TCP (http)	169.28 kbps (7:06 PM for 1m)	2.9 kbps (1.25 MB)	<1%
4688/UDP	23.2 bps (7:07 PM for 1m)	0.39 bps (174 B)	<1%
	485.07 kbps (7:43 PM for 1m)	**312.22 kbps (133.99 MB)**	

Figura 38: Puertos entre servidor y cliente

En este gráfico vemos los puertos destino del servidor hacia el cliente.

Se realiza una segunda prueba, en la que se crea una reunión no interactiva, a la cual los clientes solo accederán vía streaming. De esta manera podremos ver las diferencias entre una reunión interactiva y una con solo streaming. La oficina donde se prueba es la misma que en la prueba anterior,
La dirección ip del PC de la oficina es la **200.9.62.9** y el servidor es **cepvcm.caixapenedes.com.**

a) Gráfica del tráfico de subida para la oficina. Servidor -> Cliente

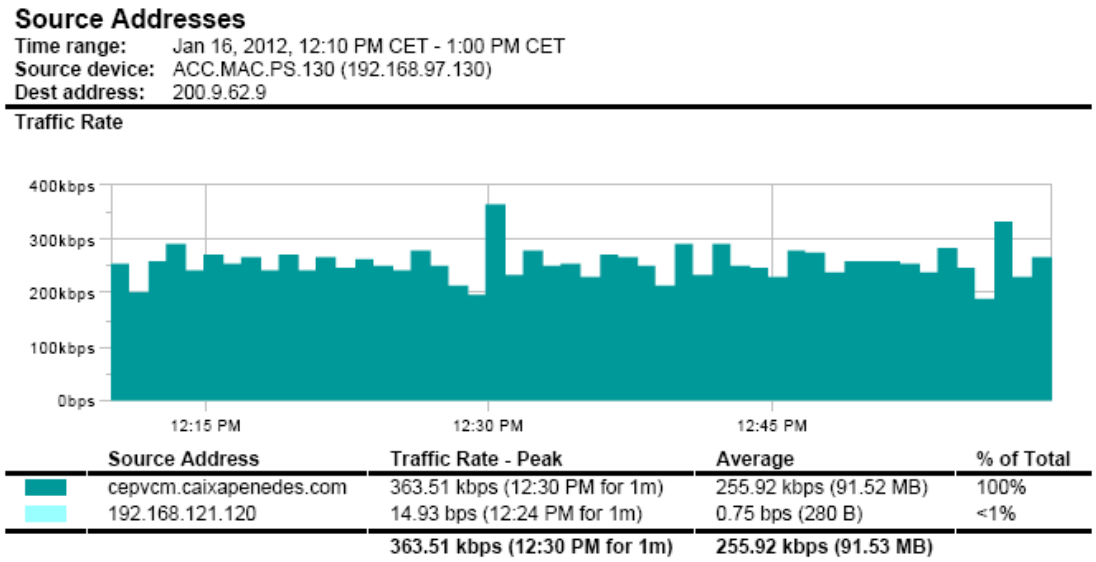


Figura 39: Tráfico origen servidor destino cliente

Se puede ver que el tráfico medio para una reunión de streaming es de **256 Kbps** tal y como recomienda el fabricante del sistema.

b) Gráfica del tráfico de bajada para la oficina. Cliente-> Servidor

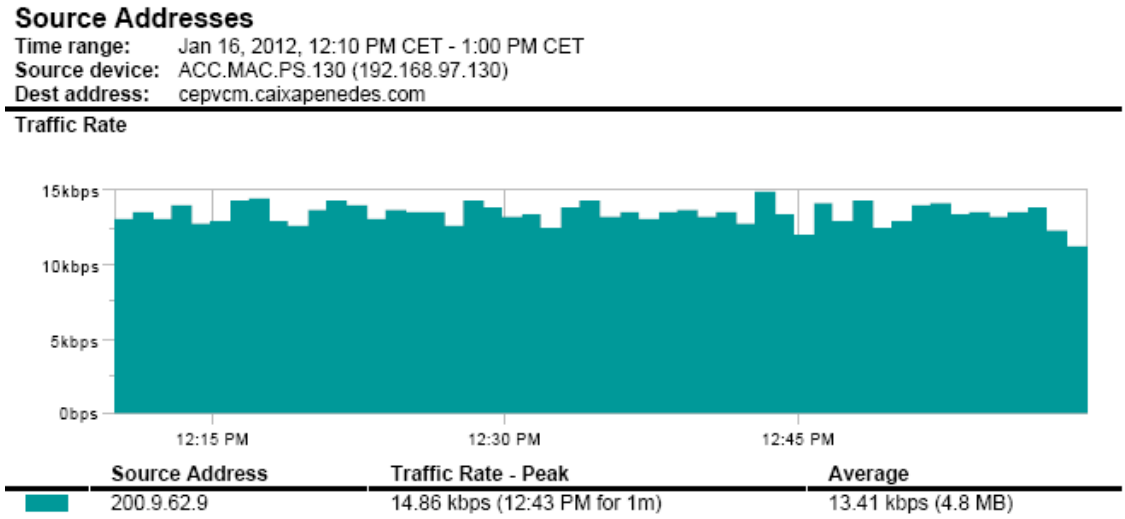


Figura 40: Tráfico origen cliente destino servidor

En esta gráfica se observa que el tráfico que envía el cliente al servidor es mínimo, se entiende que solo es para mantener la sesión TCP por el puerto 7070 que es el que se utiliza para streaming. La media es de **13 Kbps.**

c) Grafica de los puertos a los que se conecta el servidor contra el cliente

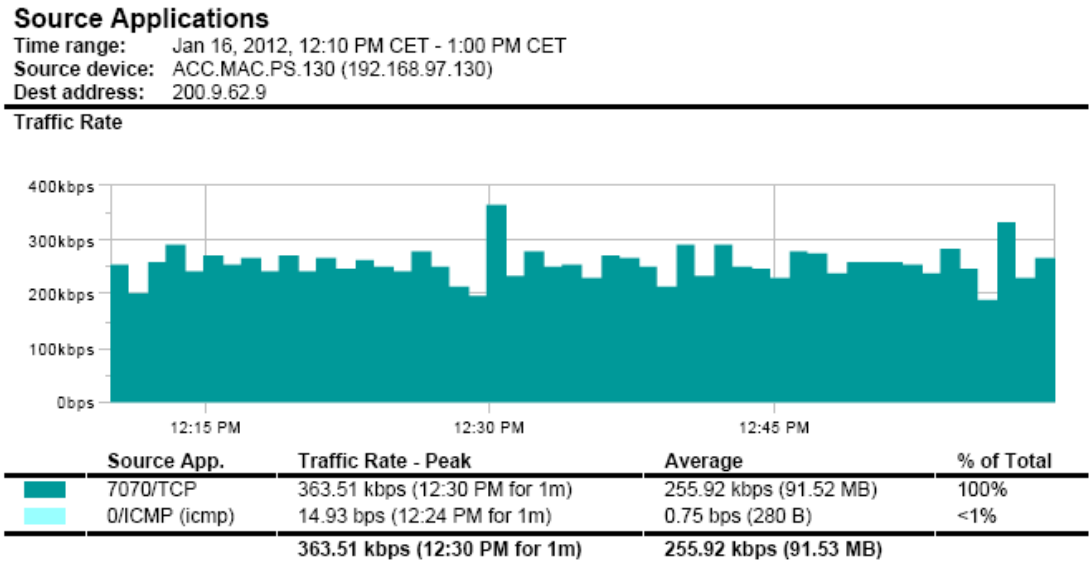


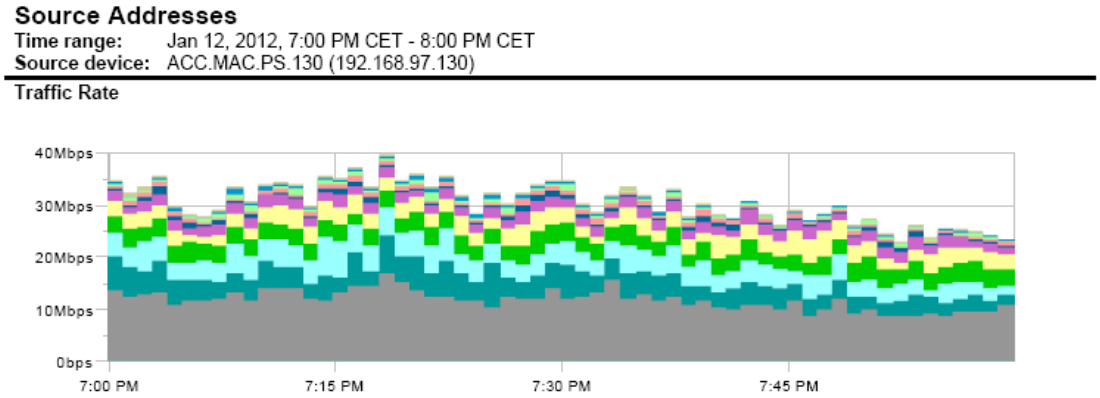
Figura 41: Tráfico origen servidor destino cliente

En esta gráfica se puede ver la conexión por el puerto 7070 (streaming) desde el servidor hacia el cliente. Todo el tráfico de streaming funciona por este puerto.

Para finalizar, en la figura 42 se adjunta una gráfica donde se puede ver todo el tráfico que colapsa en el frontal de servicios centrales. Se realiza la medida en un día de trabajo normal en oficinas durante una hora.

Sabiendo el tráfico medio que pueden tener todas las oficinas trabajando normalmente, podemos prever el impacto que puede tener la aplicación sobre la red.

a) Grafica del tráfico entre todas las oficinas de CEP y servicios centrales.



Source Address	Traffic Rate - Peak	Average	% of Total
mailcep.caixapenedes.com	8.55 Mbps (7:25 PM for 1m)	4.18 Mbps (1.75 GB)	14%
muscat2.caixapenedes.com	7.31 Mbps (7:14 PM for 1m)	4.02 Mbps (1.69 GB)	13%
staffware2081.caixapenedes.com	4.47 Mbps (7:50 PM for 1m)	3.33 Mbps (1.39 GB)	11%
NAT_muscat2	5.05 Mbps (7:47 PM for 1m)	2.87 Mbps (1.2 GB)	9%
NAT_staffware2081	2.77 Mbps (7:42 PM for 1m)	1.9 Mbps (815.17 MB)	6%
grec1.caixapenedes.gcp.cep	1.43 Mbps (7:03 PM for 1m)	624.44 kbps (267.98 MB)	2%
intranet.caixapenedes.com	1.1 Mbps (7:27 PM for 1m)	624.05 kbps (267.81 MB)	2%
fip_resd2081.caixapenedes.com	1.44 Mbps (7:30 PM for 1m)	538.16 kbps (230.95 MB)	2%
NAT_intranet	1.11 Mbps (7:08 PM for 1m)	392.04 kbps (168.24 MB)	1%
fip_retu2081.caixapenedes.com	453.47 kbps (7:01 PM for 1m)	374.7 kbps (160.8 MB)	1%
Others	17.14 Mbps (7:18 PM for 1m)	11.82 Mbps (4.96 GB)	39%
	39.99 Mbps (7:18 PM for 1m)	**30.68 Mbps (12.86 GB)**	

Figura 42: Tráfico origen todas las oficinas contra SSCC

En la gráfica se observa que el tráfico total está entre los 30 Mbps y los 40 Mbps, el ancho de banda contratado a telefónica es de 62 Mbps actualmente. La concurrencia de usuarios conectados al sistema es de una máximo de 24 con lo cual no existe el problema de saturar la red WAN en Servicios Centrales.

3.- Conclusiones

Los objetivos del proyecto que se planteaban han quedado resueltos. Se ha implementado un sistema de videoconferencia especialmente pensado para la formación sin tener un coste muy alto y con la máxima integración posible dentro de la infraestructura de Caixa Penedès.

Se ha podido ver que el sistema permite la asistencia a "clases interactivas" que permiten a los alumnos interactuar con el profesor en tiempo real pero también es interesante la opción de streaming ya que es posible grabar lecciones y visionarlas en el momento que se requiera. La opción de streaming necesita menos ancho de banda y puede ser más óptima en algunos momentos.

Tras el estudio realizado de la red MacroLAN (MPLS) de telefónica y de las conexiones de las oficinas, el resumen que se puede extraer sobre la infraestructura de red es el siguiente:

Caixa Penedès dispone de una red MacroLAN (MPLS) a la cual las oficinas se conectan mediante un ADSL local, por lo que para acceder a la red MPLS atraviesan una red ATM y una pasarela hasta el PE de entrada a la red MPLS. Todos estos saltos hacen difícil controlar la calidad de servicio por el cliente. Tal y como se explica en el apartado de la WAN, Telefónica ofrece diferentes calidades de servicio mediante los bits DSCP del paquete IP que se etiquetan en los PE's de entrada a la red MPLS.

Caixa Penedès actualmente no dispone de ninguna calidad contratada, la que ofrecen por defecto es la clase Plata, con lo que tratan el tráfico todo por igual y no se priorizan los paquetes de video y voz.

Se ha comprobado con las pruebas realizadas que la red da mejores resultados de los que Telefónica garantiza y que la aplicación funciona correctamente siempre y cuando el tráfico de la oficina no provoque que las latencias de los paquetes sean muy altas. Las oficinas utilizan normalmente un ancho de banda medio de 150 Kbps.

Para garantizar que no habrán problemas de mal funcionamiento (la voz y el video son muy sensibles a latencias altas en la red) se recomienda contratar la Clase Multimedia de manera que los paquetes de video y voz se prioricen sobre los demás. También es recomendable que las conexiones locales que tienen actualmente las oficinas en las cuales Telefónica únicamente garantiza un 10% del ancho de banda se aumenten al 50%.

VII -PRESUPUESTO

1.-Presupuesto

Para realizar el presupuesto se parte del hecho de que Caixa Penedès ya dispone de VoIP (Call Managers) y que la infraestructura de red ya esta implementada. No se tienen en cuenta los elementos hardware periféricos (webcams, micrófonos o altavoces) que se necesitan para conectarse a una reunión interactiva.

CONCEPTO	**PRECIO (€)**
Elementos Hardware:	
- Servidor Cisco MCS 7945	3.500
- MCU 3515 24 puertos	23.300
- Software CUVM	3.700
- Router Cisco 2801(Gatekeeper)	1.500
Implantación:	
- Estudio previo (15 días)	4.000
- Configuración e instalación. (1 mes)	7.000
- Pruebas (15 días)	3.500
- Puesta en producción y formación (15 días)	4.000
Mantenimiento:	
- Mantenimiento hardware (durante 1 año)	1.500
- Mantenimiento software (posibles incidencias durante 1 año)	1.000

(*)TOTAL **53.000 €**

El tiempo estimado para las tareas de implantación es aproximado

(*) IVA no incluido.

.

Bibliografía

[1] Wendell Odom. CCENT/CCNA ICND1 (Guia oficial para el examen de Certificación)

[2] María Sol Canalis. MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI

[3] TANDBERG. Discussion Document: Assessing the Real Impact on Business Travel
http://www.tandberg.com/collateral/tandberg_videoconfering_travel_survey.pdf

[4] Cisco Systems. Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component

[5] Cisco Systems. Cisco Unified Videoconferencing Solution Reference Network Design (SRND).

[6] Cisco Systems. Configuration Guide for Cisco Unified Videoconferencing Manager.

Direcciones URL

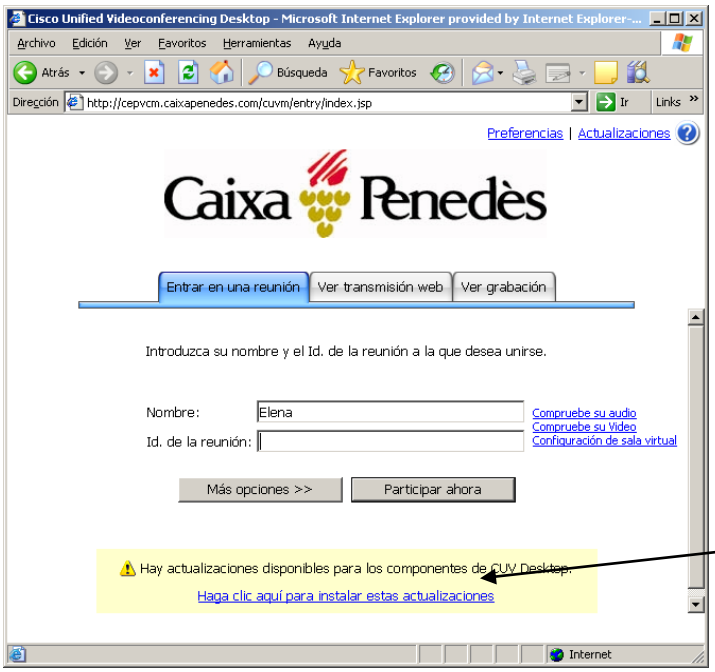
- www.cisco.com
- http://voip.bankoi.com/articulos/h323.htm

ANEXOS

Manual de instalación para cliente web.

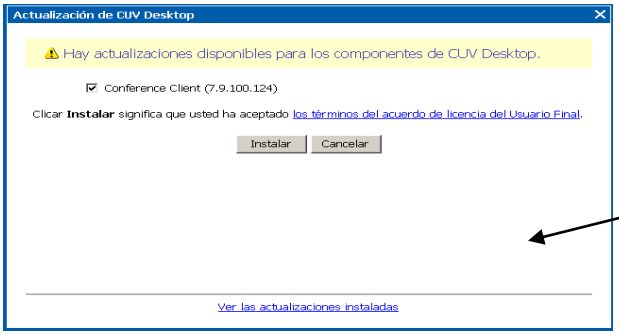
Entrar en la web http://vc.serincep.com y seguir los pasos que hay a continuación:

Paso1:



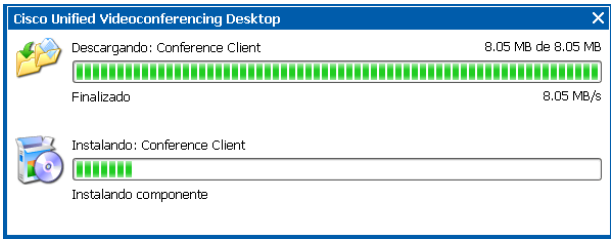
Hacer click en el link que indica

Paso 2:

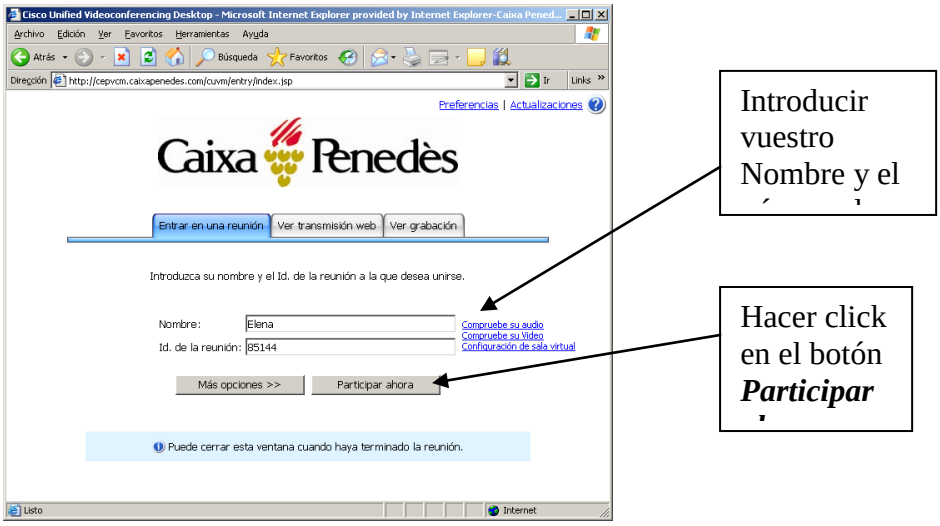


Hacer click en el botón Instalar.

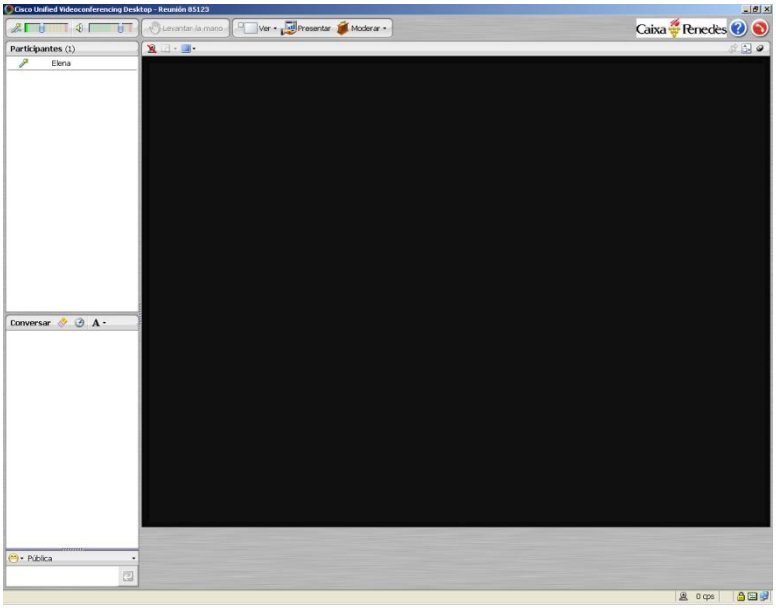
Paso 3: Ver que se instala correctamente:



Paso 4: Comprobar que funciona la aplicación. Desde la página principal Introducir los datos:



Paso 5: Comprobar que se abre la siguiente ventana. Si la cámara esta conectada en la ventana saldrá la imagen.

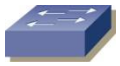
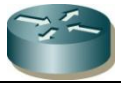


Índice de Siglas:

- ASIC: Application Specific Integrated Circuits
- ATM: Asynchronous Transfer Mode
- BBlock: Building BlocK
- CCITT: Comité Consultivo Internacional Telegráfico y Telefónico
- CEP: Caixa d'Estalvis del Penedès
- CoS: Class of Service
- CUCM: Cisco Unified Communications Manager o Call Manager
- CUVM: Cisco Unified Videoconferencing Manager
- CUVMD: Cisco Unified Videoconferencing Desktop
- DNS: Domain Name System
- DSCP: Differentiated Services Code Point
- DWDM: Dense Wavelength Division Multiplexing
- EDC: Electronic Data Capture
- FEC: Forwarding Equivalence Class
- FTP: File Transfer Protocol
- GK: Gatekeeper
- IAB: Internet Architecture Board
- IANA: Internet Assigned Numbers Authority
- IOS: Internetwork Operating System
- IPSec: Internet Protocol security
- IPX: Internetwork Packet Exchange
- LSP: LabelSwitched Paths
- MCU: Multipoint Control Unit
- MIT: Massachusetts Institute of Technology
- MPLS: MultiPrototocol Label Switching

- OSI: open system interconnection
- P2P: Peer to Peer
- PE: Provider edge
- PPP: Pointtopoint Protocol
- PVCs: Permanent virtual circuit
- QoS: Quality of Service
- RDSI: Red Digital de Servicios Integrados
- ROI: return on investment
- RTP: (Real Time Protocol)
- SCCP: Skinny Client Control Protocol
- SLA : Service Level Agreement
- SLO: Service level objective
- SMTP: Simple Mail Transfer Protocol
- TCO: Total cost of ownership.
- UBR: Unspecified Bit Rate
- VLAN: Virtual Lan
- VoIP: Voice over IP
- VPN: Virtual Private network
- WWW: World Wide Web

Descripción Iconos

DESCRIPCIÓN	ICONO
Switch	
Router	
Firewall ASA	
Balanceadores	
Switch’s nivel 3	
DWDM