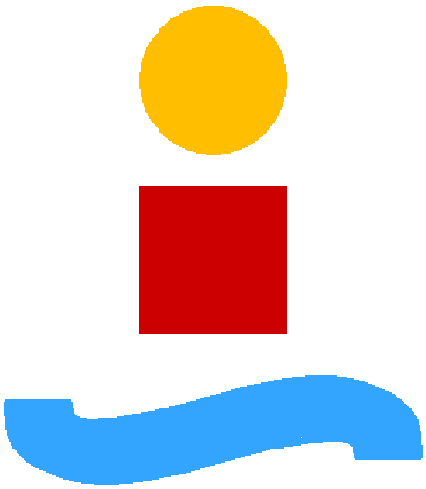
Proyecto Fin de Carrera

HispalNet



Ingeniería de Telecomunicación
Escuela Técnica Superior de Ingenieros
Universidad de Sevilla

Curso 2007-2008
Francisco Pérez Gómez

1. INTRODUCCIÓN

El presente documento trata de dar respuesta al pliego de prescripciones técnicas de la AIE DeSevilla, para la creación de una red de telecomunicaciones metropolitana con presencia en el Ayuntamiento y en las sedes de la AIE, y que soporte entre otros los servicios de voz, datos y videoconferencia.

El objetivo principal es proporcionar una estructura fiable, segura, gestionable y abierta que se ajuste al máximo a los requisitos indicados en dicha solicitud en los siguientes aspectos:

- **Arquitectura**: En cuanto al número de los equipos que proporcionan la solución, a la forma en que se interconectan los distintos equipos, las funciones que deben realizar cada uno de ellos y los niveles funcionales que conforman la solución.

- **Funcionalidades**: Los equipos se han escogido en función del grado de cumplimiento y adecuación a las diversas funcionalidades requeridas y, en su defecto, en la previsión de adecuación en el futuro próximo a dichas funcionalidades.

- **Escalabilidad**: Los equipos elegidos se ajustan en número y prestaciones a las necesidades recogidas, pero permiten el crecimiento de la red en lo relativo a recursos disponibles y, sobre todo a la escalabilidad de la propia solución.

- **Efectiva en costes**: La configuración de los equipos propuestos ofrece un equilibrio entre prestaciones, nivel de redundancia y coste de la solución. La solución puede mejorarse técnicamente en algunos aspectos a un coste algo mayor, pero para los servicios básicos ofrecemos redundancia y alta disponibilidad.

- **Inversión**: Nuestro objetivo es conseguir que aquello que supone un gasto fijo en la empresa se convierta en una inversión. Implantar una red propia supone también reducir los gastos en comunicaciones entre las distintas sedes de las empresas que forman la AIE y el Ayuntamiento. Así como, en una fase más avanzada, puede incluso llegar a producir beneficios al pasar a ser un Operador.

- **Innovación Tecnológica**: La red que en este documento se propone esta compuesta por los dispositivos de red más avanzados del mercado y soporta todas las nuevas funcionalidades existentes. La configuración que aquí presentamos es capaz de soportar todos los nuevos servicios que se implantan actualmente en el mundo empresarial y de operador. Esto no significa que la red pueda tener problemas de implementación, ya que este tipo de diseño ya ha sido probado con gran éxito en distintos proyectos.

- **Gestión**: Hemos pensado, para esta red, que la gestión se realice centralmente. Para el control de fallos, alarmas, configuraciones, etc. de la estructura de red proponemos una solución centralizada ya que los recursos son comunes, ofreciendo eficacia y facilidad de manejo. Para los servicios de voz corporativa, la gestión también se realizará desde el CASSI de manera centralizada y al tener un Cluster de Call Managers por empresa, cada una podrá gestionar sus recursos individualmente si lo desea.

El **Capitulo 2** se centra en la parte de infraestructura de troncal y en la parte de acceso a esta troncal. En el apartado 2.2, se describen los diferentes niveles lógicos de la red, la Calidad de Servicio que se propone aplicar, y finalmente el equipamiento propuesto. Para todo lo referente al despliegue de la fibra y la explicación detallada de los anillos y de la distribución de las sedes, se ha hecho un documento aparte. Este documento compone el *"ANEXO A: Solución Troncal y Conexión a sedes secundarias".*

Las sedes secundarias, por donde no pasa la troncal de fibra, serán accesibles a través de diferentes accesos (Radioenlaces, WiMAX, Fibra, xDSL,…). El apartado 2.3 describe brevemente los modos de conexión a las sedes secundarias y el equipamiento propuesto. Este apartado hace referencia al documento "*"ANEXO A: Solución Troncal y Conexión a sedes secundarias"* que describe detalladamente la conexión de las sedes secundarias.

El apartado 2.4 se centra en el cableado de los equipos de la red MAN, los racks y todo lo necesario para su instalación física. En el apartado 2.5, se comenta la redundancia en la red tanto a nivel Hardware como a nivel de enlaces. El apartado 2.6 describe el equipamiento y el cableado de las redes locales de cada sede. El apartado 2.7 describe el Plan de direccionamiento IP propuesto para todas las empresas de la AIE y el Ayuntamiento.

Finalmente, en el apartado 2.8, nos centramos en la seguridad en la red.

Para dimensionar los enlaces y, por lo tanto, el tipo de equipamiento a proponer, se ha tenido que realizar una serie de cálculos de dimensionados que se describen en el Capitulo 3.

En el Capitulo 4, se describe como se conectarán las redes externas y los otros lotes a la red metropolitana propuesta.

El Capitulo 5 se centra en el enrutamiento en la red, con los protocolos de routing propuestos para implementar la red propuesta.

En el Capitulo 6, se detallan los servicios que se darán o que se podrán dar sobre la red propuesta, explicando los elementos involucrados en el funcionamiento de cada uno de ellos así como las necesidades existentes para la puesta en marcha de los mismos.

Finalmente, el Capitulo 7 cubre la Gestión de la red y se divide en varios sub-apartados, uno para la gestión de la voz corporativa, otro para la gestión de la red de datos y otro más para la gestión de la red Wireless de las sedes con el equipamiento propuesto para cada tipo de red.

2. DESCRIPCIÓN DE LA CONFIGURACIÓN DE LA RED DE SOPORTE DEL SERVICIO

2.1 INTRODUCCIÓN

En este capítulo, se describe la solución propuesta en cuanto a la troncal de fibra que permitirá conectar las sedes principales del Ayuntamiento y de la AIE a la red metropolitana. Con el fin de aprovechar la topología de fibra en anillos y para dar redundancia de camino a todas las sedes, se ha decidido instalar en cada sede de la troncal un equipo Cisco 3750 integrado en un anillo de fibra. Los anillos de fibra se terminan en equipos Cisco 7604 que, a su vez se conectan a dos 7606 de core.

El primer apartado (Arquitectura de red) se centra en la arquitectura global de la red, empezando por los diferentes niveles lógicos en la que se puede dividir, seguido por una explicación detallada del tendido de fibra a nivel físico y terminando por una descripción del equipamiento propuesto que permita cumplir con los requerimientos del pliego.

2.2 ARQUITECTURA DE RED

2.2.1 NIVELES

La red metropolitana propuesta se ha divido en varios niveles lógicos, cada uno desempeñando una función bien específica. El primer nivel es el **nivel de acceso** formado por los equipos instalados en cada sede, que son los 3750 conectados al anillo y los Gateways de voz configurados de tal manera que permitan el backup de la telefonía en caso de fallo de conectividad con los elementos centrales (Call Manager). El segundo nivel es el **nivel de agregación** recogiendo las diferentes sedes en unos equipos Cisco 7604 con capacidad MPLS. El tercer y último nivel es el **Nivel de Core** compuesto por equipos Cisco 7606 que también disponen de funcionalidades MPLS.

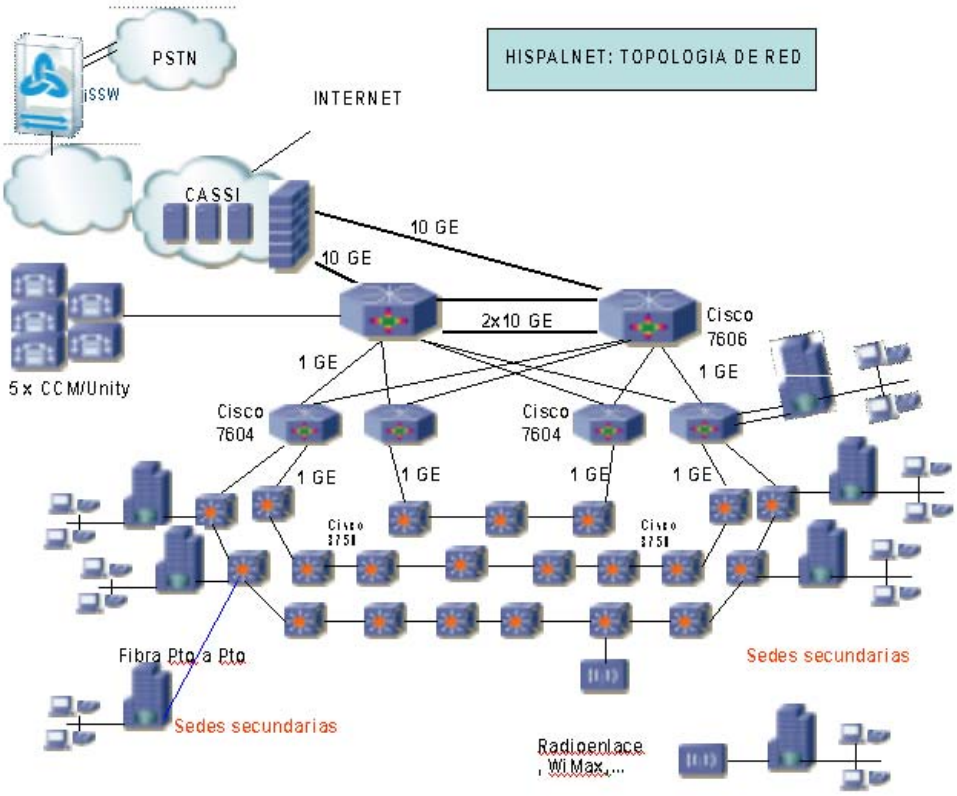


Figura 1 Arquitectura de Red Propuesta a AIE DeSevilla

A continuación, se describen los diferentes niveles lógicos de la red.

2.2.1.1 Nivel de Acceso

Para aprovechar la estructura en anillo y la redundancia de camino que permite esta topología, se ha puesto en cada sede de la troncal un equipo Cisco Catalyst 3750 conectado a ambos lados del anillo de fibra al que pertenece esta sede. Este equipo se conecta directamente a la LAN de la sede mediante un acceso Ethernet 10/100/1000 en cobre o SFP de 1 GE y enruta el tráfico a nivel 3.

Sedes Principales:

Para las sedes principales de EMASESA y del AYUNTAMIENTO, el modo de conexión difiere un poco ya que estas dos sedes disponen en sus dependencias de equipos de Agregación y Core. Por lo tanto, cada sede de esas se conectará mediante 2 enlaces a un equipo Cisco 7604 tal como lo describe el diagrama siguiente:

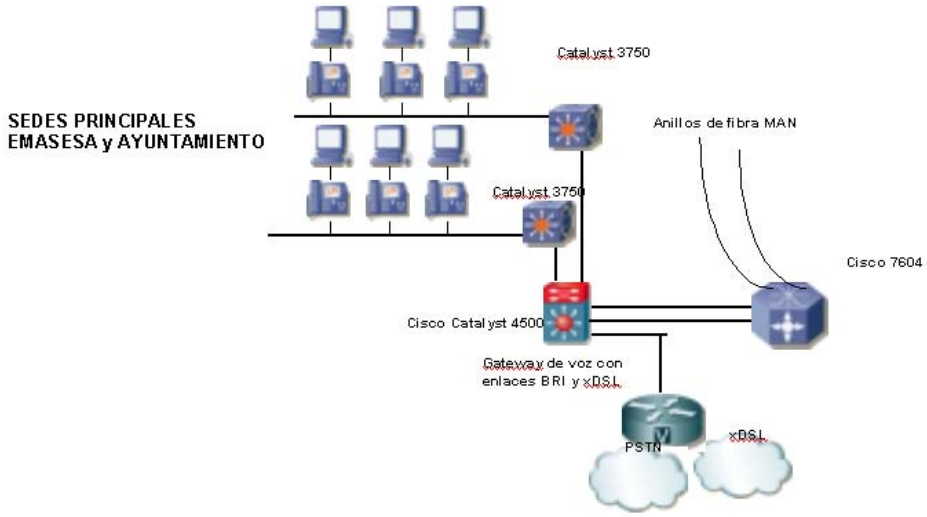


Figura 2 Acceso a Sedes Principales AYUNTAMIENTO y EMASESA

Para el resto de sedes principales (4 en total), el Switch de la LAN de la sede se conectará mediante 2 enlaces GE en cobre o en fibra a dos 3750 tal como lo describe la figura siguiente:

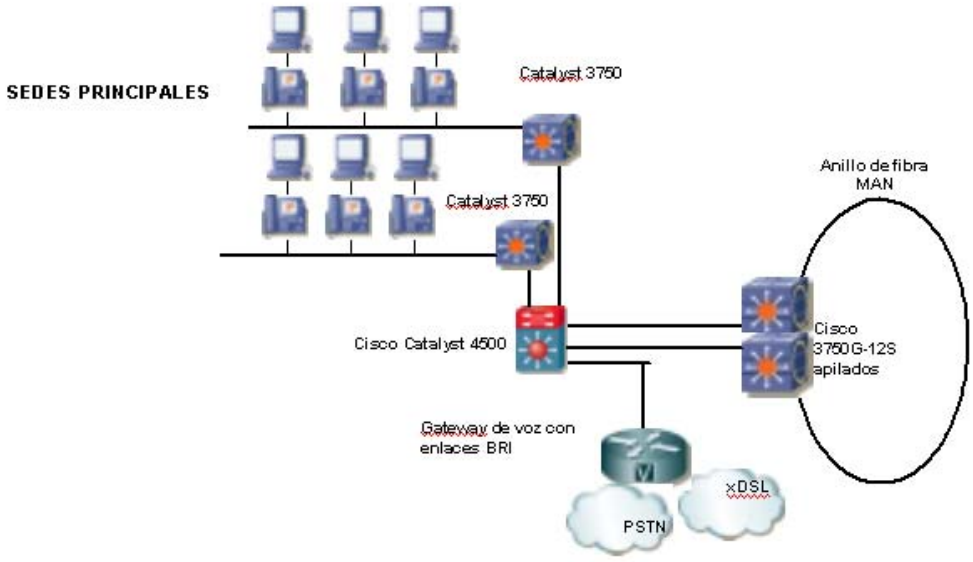


Figura 3 Solución propuesta para las Sedes principales

Por otro lado, cada sede de la troncal dispondrá de un Gateway que, básicamente se encargara de proporcionar backup de telefonía con interfaces BRI o PRI y de datos mediante interfaces xDSL. Los equipos propuestos son los routers Cisco ISR de la gama 2800 o 3800 o 877 para las sedes pequeñas. Estos routers están equipados con las interfaces (BRI, PRI, etc.) y los DSPs necesarios para el servicio de Backup de telefonía por la PSTN y, además, están preparados para implementar nuevos servicios como firewall, IPsec, etc.
Como se describe en el documento de Solución de voz, las sedes que dispongan de un cluster de Call Managers en sus dependencias no requieren la funcionalidad SRST en sus Gateways. Por lo tanto, la única sede principal que dispondrá de esta funcionalidad será la sede principal de GMU.

Otras sedes conectadas a la troncal de fibra

Para el resto de las sedes conectadas directamente a la troncal la topología de acceso consiste en un enlace desde la LAN de la sede hasta un 3750 del anillo. Todas estas sedes disponen de un Gateway con funcionalidad SRST para Backup de voz y interfaces xDSL para el Backup de datos. En las sedes de Tipo A y B, el Gateway incluye interfaces SHDSL y en las sedes de tipo C y D, las interfaces son ADSL.

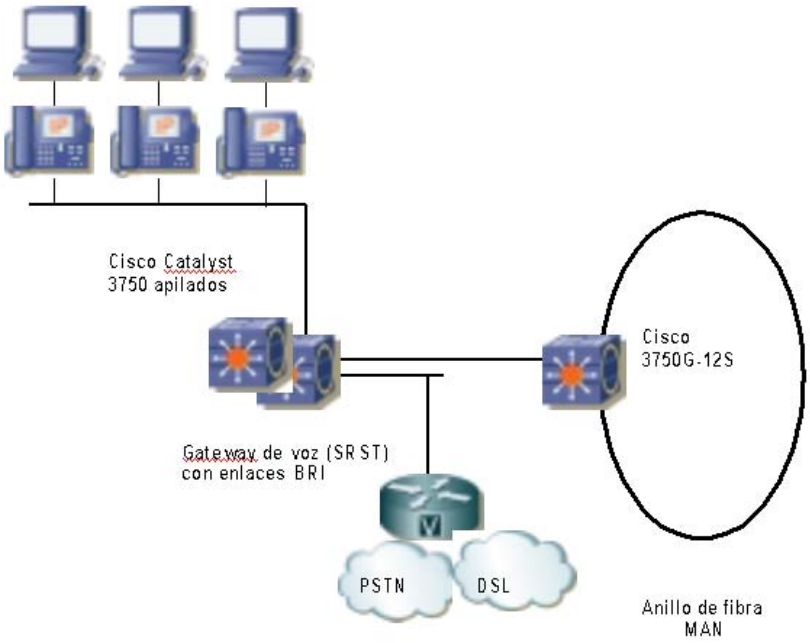


Figura 4 Solución propuesta para las Sedes de la troncal (No Ppales)

Para estas sedes de la troncal, se podría redundar el equipo 3750 pero no se ha considerado esta opción por un tema puramente económico. Si la AIE lo considera necesario, se podría tener en cuenta esta opción y solo se trataría de añadir un equipo 3750 y un cable Stackwise para apilar estos 2 equipos.

En cuanto al resto de sedes no descritas en este apartado, se conectarán o bien mediante un enlace de fibra en punta, o bien mediante Radioenlaces o WiMax. Estas sedes secundarias se describen en el apartado de “Conexión de las sedes secundarias”.

2.2.1.2 Nivel de Agregación

Este nivel de agregación se compone de routers Cisco 7604 que pueden recoger las fibras directamente de las sedes importantes o de los Catalyst 3750 instalados en las sedes. Se han analizado múltiples opciones antes de escoger las plataformas propuestas. Se ha considerado la posibilidad de utilizar plataformas diferentes a la propuesta, utilizar modelos diferentes para la topología en anillo y la topología en estrella. Su función principal es la de formar los anillos de la red metropolitana recogiendo y entregando, allí donde fuera necesario, el tráfico de las diferentes sedes.

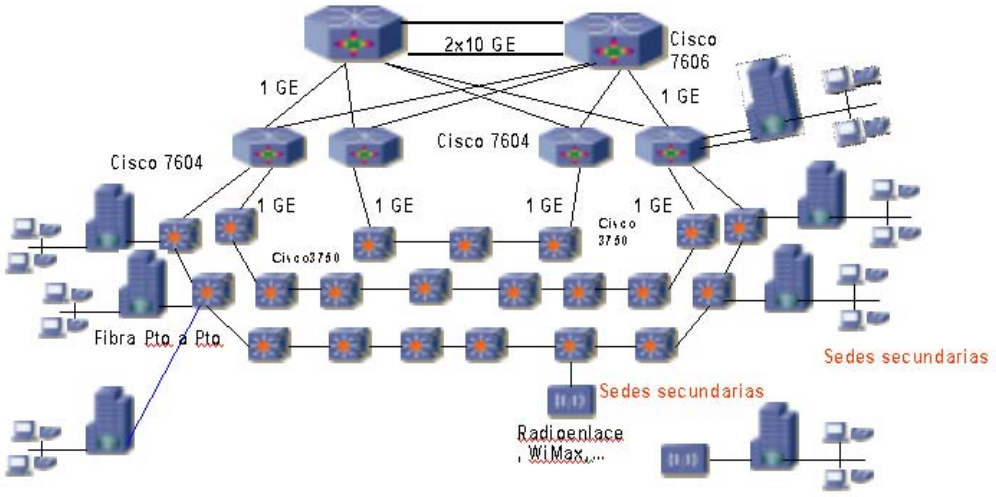


Figura 5 Solución propuesta para la agregación

2.2.1.3 Nivel de Core

Este nivel es el responsable de la agregación de los distintos anillos en un punto redundado de la red, además es el punto de unión entre la red MAN, Internet a través del CASSI y la red PSTN a través de la red IP del operador.

Estos dispositivos forman parte del mundo MPLS (funcionalidad de Provider (P)), ello implica que sean los responsables del soporte de las VPNs de MPLS para dar servicio a las VPNs de nivel 3. Todo el tratamiento de estas funcionalidades se realiza directamente en la tarjeta que recibe las conexiones provenientes del nivel inferior sin interferir con el funcionamiento del procesador central. El soporte de estos dos servicios puede ser fácilmente extendido dentro de la misma red metropolitana e incluso a otras redes. Todos los equipos presentados en la solución soportan versión de software IOS Nativo, así como la portabilidad de funcionalidades a cualquiera de los puntos de la red. Esto garantiza una homogeneidad en toda la red Metropolitana desde la agregación hasta el core.

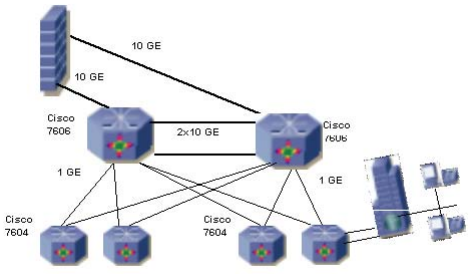


Figura 6 Solución propuesta para core

Estos equipos pueden tener funcionalidades extendidas dentro de la arquitectura de red, dada su flexibilidad a la hora de definir nuevos servicios se pueden descargar sobre ellos funcionalidades como: NAT, Caching, WCCP, Firewall.... eliminando la necesidad de nuevos equipos para dar soporte a esos servicios e incluso permitir la entrada a otros nuevos no cubiertos en las expectativas iniciales.

El balanceo de tráfico y redundancia de caminos depende de cómo se implementen cada uno de los servicios en este nivel. Si es conmutado a nivel 3 es el IGP (nuestra recomendación es usar OSPF) correspondiente el encargado de establecer el camino activo y, en su caso el balanceo de carga y el tiempo de convergencia (en este sentido un IGP de tipo link state (OSPF) suele reducir notablemente los tiempos de convergencia). Si se trata de un servicio MPLS como es el caso en la solución propuesta, depende de LDP la determinación del camino óptimo, que a su vez descansa sobre el protocolo de routing unicast, en nuestro caso OSPF.

2.2.2 CALIDAD DE SERVICIO

El equipamiento ofertado y sus diferentes interfaces están ampliamente dimensionados para soportar grandes tasas de tráfico utilizando, en algunos casos, enlaces de 10 Gigabit Ethernet. Sin embargo, siempre puede ocurrir puntualmente que algún enlace se congestione y, en estos casos, es necesario una buena política de Calidad de Servicio en la red.

Todos los equipos propuestos en la solución soportan calidad de servicio de tipo DiffServ (Differentiated Services). Los servicios diferenciados (Diffserv) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Los paquetes que pertenecen a una determinada clase se marcan con un código específico (DSCP – Diffserv CodePoint). Este código es todo lo que se necesita para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior). De esta manera a través de Diffserv planteamos asignar prioridades a los diferentes paquetes que son enviados a la red. Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades.

Una vez marcados y clasificados, los paquetes de tráfico real-time deben recibir un tratamiento especial en la red y es el papel de las colas en los equipos de la red. Para la VoIP se requiere una cola de alta prioridad y se recomienda utilizar Low Latency Queueing (LLQ) por su flexibilidad y su facilidad de configuración.
Sin embargo, se necesita un estudio más amplio de los patrones de tráfico de la red para realizar una propuesta de Calidad de Servicio completa en la red.

2.2.3 TRADUCCIÓN DE DIRECCIONES (NAT)

Las diferentes empresas que forman la AIE DeSevilla y el Ayuntamiento tienen direccionamientos IP privados para sus redes de datos y en algunos de los casos, solapados. Como se verá en el apartado de servicios sobre VPNs MPLS de este documento, cada una de las empresas tendrá su propia VPN y para el acceso a los servicios centralizados (Internet, etc.) estas direcciones se deben traducir para evitar el solapamiento y posibilitar el dialogo entre las diferentes empresas.
El acceso a Internet se realizará de manera centralizada en el CASSI y las diferentes VPNs transportando el tráfico Internet de las empresas acabarán en un único equipo situado en el CASSI que realizará la traducción de direcciones privadas internas a direcciones públicas enrutables en Internet.

En el caso del tráfico de voz corporativa, cada empresa tendrá un cluster integrado en su propia VPN. El tráfico interno a la empresa no requerirá ninguna traducción ya que estará gestionado por un único Cluster y no habrá ningún solapamiento entre las diferentes direcciones IP implicadas en una llamada.
En cuanto al tráfico entre diferentes empresas, el elemento encargado de realizar las traducciones a nivel de direccionamiento IP es el Session Border Element (Net-Net SD de Acme Packet) de la solución IN-BVS. El Net-Net SD se puede incluir en une red MPLS a través de un router PE, que mapea un label MPLS VPN a un tag 802.1q de VLAN. Cada interfaz FE o GE de un Net-Net SD puede terminar varias VLANs 802.1q en diferentes interfaces de red (Network Interface) que pueden representar diferentes VPNs de clientes, en nuestro caso, las VPNS de las empresas de la AIE y del Ayuntamiento. En la configuración de sus interfaces de red, el Net-Net SD incluye la dirección IP, la máscara y el tag 802.1q de la VLAN. Esto permite gestionar diversas VPNs con solapamiento de direccionamiento IP. Este elemento es capaz de ver las diferentes VPNs y asegura la

intercomunicación entre todas estas VPNs. Sin embargo, el plan de direccionamiento IP propuesto para esta oferta está hecho de tal manera que no hay solapamiento de direccionamiento IP entre las diferentes empresas, por lo tanto, no hay necesidad de traducir las direcciones para el tráfico entre las diferentes empresas. A pesar de esta facilidad ofrecida por el Session Border Controller, se propone un plan de direccionamiento a la AIE que evita todo tipo de solapamiento entre empresas.

De la misma manera, todo el tráfico destinado a la PSTN pasará a través del Session Border Controller para acabar en los Media Gateways que realizarán la conversión IP-PSTN. Una descripción más detallada de este equipo se encuentra en el documento de la solución de voz corporativa IN-BVS de Cisco-Italtel.

2.2.4 DESPLIEGUE DE LA RED TRONCAL DE FIBRA

Como ya se ha comentado anteriormente, la red de Telecomunicaciones Metropolitana de la AIE DeSevilla y del Ayuntamiento se basa en un tendido de fibra existente en parte y objeto de este pliego por otra parte. Uno de los requisitos imprescindible es que este tendido de fibra permita una redundancia en cualquier parte del camino. Para lograr esta redundancia, la mejor forma es de definir diferentes anillos de fibra recogiendo las sedes definidas como troncal en el pliego.

Todo el despliegue de la red de fibra, los diferentes anillos propuestos y las sedes incluidas se describen en detalle en el documento *"ANEXO A: Solución Troncal y Conexión a sedes secundarias"*.

2.2.5 DESCRIPCIÓN / DIMENSIONADO DEL EQUIPAMIENTO PARA LA SOLUCIÓN DE TRONCAL Y ACCESO

En este apartado describimos el equipamiento propuesto para el core (2 x Cisco 7606 con Supervisora 720), la agregación (4 x Cisco 7604 con Supervisora 32) y el acceso (Cisco Catalyst 3750). El equipamiento de cada sede (Gateway de voz, switching, etc.) se describe en el Capitulo de la solución propuesta para la voz corporativa.

2.2.5.1 Nivel de acceso

Como lo hemos descrito anteriormente, en cada una de las sedes de la troncal se instalará un

equipo (o 2 para las sedes principales) Cisco Catalyst 3750 de Cisco conectado con dos SFPs a ambos lados del anillo y mediante cobre o fibra a la LAN de la sede. Con la densidad de puertos de la que dispone este equipo, será capaz de agregar también las sedes secundarias que se conecten a través de tecnologías alternativas como WiMax o Radioenlaces.
Las sedes principales de EMASESA y del AYUNTAMIENTO, al disponer de equipos de agregación 7604 instalados en sus dependencias, se conectarán directamente a estos equipos mediante 2 enlaces GE en cobre. Las 4 sedes principales restantes dispondrán de 2 Catalyst 3750 cada una y se conectarán mediante 2 enlaces GE a cada uno de estos 3750. A continuación, se describe el equipo 3750 propuesto. El Cisco 7604 se describe en el apartado *"Nivel de agregación".*

El Catalyst 3750 es un equipo orientado a empresas medianas que facilita el despliegue de aplicaciones convergentes y provee una configuración flexible adaptándose a cualquier cambio de negocio

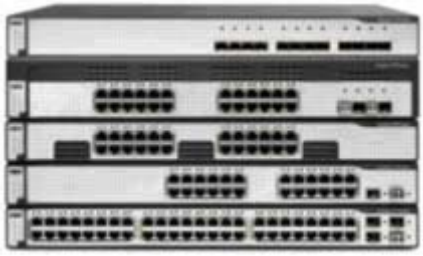


Figura 7 Cisco Catalyst 3750

Los equipos propuestos en esta oferta son los 3750-12S (1 RU) de 12 puertos basados en SFP lo que permite conectar tanto puertos de fibra como de cobre..Estos equipos existen en 2 modalidades de Software IP Base o IP Services. El Software ofertado es el IP Services (previamente llamado EMI, Enhanced Multilayer Image), el más avanzado porque necesitamos que este equipo trabaje a nivel 3 y tenga posibilidad de gestionar VRF en el caso de conectar varias sedes de diferentes empresas al mismo 3750 y así diferenciar el tráfico de una y de otra en el mismo equipo. Los puertos Gigabit ethernet basados en SFP soportan una gran variedad de transceivers SFP. Las opciones disponibles para los SFPs son 100BASE-LX, 100BASE-FX, 1000BASE-T, 1000Base-SX, 1000Base-LX y CWDM.
El Cisco catalyst 3750 tiene una gran ventaja a nivel de ocupación de espacio ya que es un

equipo muy compacto y que ofrece varias modalidades de montaje. Todos los conectores se encuentran en la parte delantera del equipo lo que facilita el troubleshooting y el acceso a los conectores para la instalación.

Tecnología Stackwise

La tecnología Stackwise de Cisco es una tecnología de Stacking optimizada para Gigabit Ethernet. Esta tecnología permite apilar hasta nueve Catalyst 3750 en una sola unidad lógica utilizando un cable y un software especial. El Stack se comporta como una única unidad lógica gestionada por un master elegido entre uno de los miembros del stack. El master crea y actualiza automáticamente el switching y todas las tablas de routing. Un stack puede aceptar nuevos miembros y borrar antiguos sin interrupción del servicio.
Se pueden apilar hasta 9 Catalyst 3750 en una sola unidad lógica llegando a un total de 468 puertos Ethernet o PoE 10/100, o 488 Ethernet 10/100/1000 o PoE 10/100/1000, o 9 puertos 10 Gigabit Ethernet. Se pueden combinar los diferentes tipos de 3750 sin ningún problema.

2.2.5.2 Nivel agregación

Para este nivel, se ha elegido un equipo (Cisco 7604) de la misma familia que el equipo de core pero con una tarjeta Supervisora 32. Este equipo realiza la función de Provider Edge (PE) dentro de la arquitectura propuesta basada en MPLS VPNs. Aparte de agregar el tráfico de los diferentes anillos de Cisco Catalyst 3750, el Cisco 7604 estará instalado en una sede Principal de la AIE y se conectará a la LAN de esta sede recogiendo el tráfico de todos los usuarios de la sede.

El Cisco 7604 es un router compacto de 4 slots diseñado para el edge de la red donde se necesita un alto rendimiento y servicios IP/MPLS para el transporte de tráfico de aplicaciones Triple Play (voz, video y datos) tanto para el mercado residencial como para la empresa. Además, gracias a su arquitectura modular, cumple con todos los requerimientos de alta disponibilidad y redundancia de una solución como la red Metropolitana de la AIE.

Con un rendimiento de hasta 144-Mbps distribuido y un throughput de 320 Gbps, el 7604 provee rendimiento y confiabilidad con las opciones de disponer de tarjeta supervisora y alimentación redundantes

.***Figura 8 Cisco 7604 para agregación***

El Cisco 7604 se puede configurar de dos formas distintas: con una única Supervisora y hasta 3 tarjetas de línea o con 2 tarjetas Supervisoras para alta disponibilidad y redundancia. Este equipo también soporta la fuente de alimentación 2700W redundante.
En la solución propuesta, los 7604 llevan todos Supervisora 32 redundante y fuente redundante.

2.2.5.3 Nivel de core

Este nivel está basado en el equipo de conmutación de la gama Cisco Catalyst 7606 con supervisora SUP720, MSFC3 y PFC3B. La familia Catalyst® 6000, que se compone de las series Catalyst 6500 y Catalyst 6000, ofrece una familia de soluciones de conmutación de alto rendimiento para redes empresariales y de proveedores de servicios. Diseñada para afrontar los crecientes requisitos de densidad gigabit, la integración de datos y voz, la convergencia LAN/WAN/MAN/IDC, la capacidad de ampliación, la alta disponibilidad y la conmutación inteligente multicapa. Concretamente, la plataforma 7606 ofrece las siguientes características principales:

- Capacidad de conmutación de 720 Gbps y puede escalar hasta más de 400Mpps.
- Separación del plano de control (MSFC3) y el de forwarding (PFC3B)
- Densidad de puertos ampliable. Es un equipo modular de 6 slots con posibilidad de contener hasta 20 puertos de 10GE, 82 interfaces GE, 480 puertos 10/100 o

240 puertos 100BaseFX. Soporta Fast Etherchannel y Gigabit Etherchannel que permite agregar ancho de banda hasta 16Gbps utilizando puertos de diversas tarjetas.

- Convergencia LAN/WAN/MAN/IDC.
- Extensas funcionalidades de QoS. Marcado de valores de QoS y limitación de la tasa de tráfico en entrada mediante verificación de listas de acceso, WRED, WRR, asignación de prioridades a RSVP, ...
- Funcionalidades de seguridad avanzadas. Aplicación de listas de acceso, envío de información de routing encriptada, posibilidad de utilizar módulos de detección de intrusiones.
- Alto nivel de redundancia. Un tiempo medio entre fallos de 7 años. Posibilidad de incorporar tarjetas supervisoras redundantes, fuentes de alimentación redundantes y con balanceo de carga, Switch Fabric, relojes del sistema redundantes, múltiples ventiladores. Todos los elementos son insertables en caliente, por lo que los tiempos de parada por avería son mínimos.
- Proporciona funcionalidades MPLS (EoMPLS, MPLS VPN, MPLS QoS, MPLS TE,...).

Soporta todas las funcionalidades necesarias para unir los dos mundos de conmutación (niveles 2 y 3) ya que se trata de un conmutador multinivel con funcionalidades de routing sin degradación en el encaminamiento de tráfico. Simultáneamente múltiples funcionalidades como listas de acceso, capacidades de calidad de servicio, funcionamiento en entornos MPLS... están soportadas sin degradación del rendimiento.

Cabe decir que este nivel se encargará de agregar los flujos de tráfico provenientes todos los anillos desplegados (GigaEthernet) y encaminarlos vía interfaces 10GE al nivel superior: Servicios, PSTN o Internet.

2.5 REDUNDANCIA EN LA RED

2.5.1 REDUNDANCIA DE ENLACES

El diseño de la red se ha hecho pensando en una redundancia total de enlaces para dar siempre dos caminos posibles o más y paliar los posibles fallos de los equipos o de los enlaces de la red.

2.5.1.1 Redundancia en el acceso

De todas las sedes principales, 2 estarán conectadas a unos 7604 con enlaces redundantes. Estas sedes son las del Ayuntamiento y EMASESA donde están instalados los equipos de Core (7606) y de agregación (7604). Para las otras 4 sedes definidas como principales en el pliego, se propone redundar el 3750 del anillo mediante tecnología Stackwise de Cisco y así dar doble enlace a estas 4 sedes principales y evitar tener un único punto de fallo.

Por otro lado, en las sedes que dispongan de un router con acceso xDSL, se configurará un proceso HSRP entre este router y el 3750 del anillo para suplir un posible fallo del Catalyst 3750.

2.5.1.2 Redundancia en el anillo

Los diferentes anillos que recogen el tráfico de todas las sedes ofrecen evidentemente 2 caminos de un 3750 hacia un 7604 de agregación. Además, se ofrece una redundancia geográfica ya que un anillo siempre empieza en una sede principal y acaba en otra sede principal, diferente de la primera.

2.5.1.3 Redundancia entre agregación y core

Como se ha descrito en el capitulo de Arquitectura de red, cada 7604 de agregación se conecta mediante un enlace GE a cada uno de los 7606 de core lo que garantiza en cada momento un camino alternativo hacia el nivel superior.

2.5.1.4 Redundancia entre core y CASSI

Cada uno de los routers Cisco 7606 se conecta mediante un enlace de 10GE al equipo que el adjudicatario del lote III (CASSI) pondrá a disposición de los otros lotes para su interconexión. Este equipo deberá disponer de interfaces 10GE para poder conectarse con la MAN del Ayuntamiento y DeSevilla.

2.5.2 REDUNDANCIA EN EL HARDWARE

En el nivel de acceso, la LAN de la sede se conecta a un switch del anillo. Como se ha descrito en capítulos anteriores, habrá 2 sedes principales (donde terminan los anillos) donde se instalarán dos 7604 y un 7606. Para estas dos sedes, se propone conectar su LAN mediante 2 enlaces agregados en Etherchannel a uno de los 7604. Este 7604 dispone de 2 tarjetas supervisoras, por lo tanto, un enlace iría a una Supervisora y el otro a la otra Supervisora. Para las otras sedes principales, se proponen dos 3750 apilados mediante la tecnología Stackwise de Cisco, en lugar de uno solo y la LAN de esta sede iría conectada mediante dos enlaces agregados en Etherchannel a cada uno de los 3750 apilados.

Aunque no se haya incluido en la oferta económica por razones de coste, creemos conveniente presentar como opción la posibilidad de redundar físicamente todos los demás Cisco 3750 de los anillos y así dotar de redundancia física a todas las sedes.

Todos los equipos de Core (7606) y de agregación (7604) disponen de alimentación redundante y los equipos Cisco 7604 propuestos llevan 2 tarjetas Supervisoras una redundante de la otra.

2.6 REDES LOCALES

2.6.1 INTRODUCCIÓN

La instalación de un sistema de telefonía IP en una sede, requiere la comprobación de que dicha sede dispone de cableado mínimo categoría 5, en buen estado, y dispone de tecnología LAN de switching.

Adicionalmente, si se requiere conectar el teléfono y el PC al mismo puerto del switch, con el objetivo de no ocupar dos puertos por usuario y tener que realizar cableado nuevo, el switch debe disponer de la funcionalidad de Auxiliary VLAN.

Por otro lado, los nuevos terminales, se pueden conectar a una toma de red eléctrica, si está disponible, o por el contrario, pueden recibir la alimentación del conmutador al que estén conectados, mediante la tecnología power over ethernet, en adelante PoE.

Todos estos requisitos, han hecho que consideremos necesario presentar a la AIE una propuesta de renovación de los equipos de LAN, por nuevos equipos de switching capaces de proveer las funcionalidades citadas en el párrafo anterior.

La propuesta realizada tiene en cuenta **un incremento del 25%** sobre el máximo entre usuarios LAN actuales y extensiones de teléfonos requeridas, para cubrir posibles nuevos puntos de red.:

Puertos requeridos = (max(usuarios lan ; extensiones totales))*(1+25%)

En base a este cálculo, se obtiene el número de **puertos requeridos** y se dimensionan los equipos para cubrir este número de puertos, teniendo en cuenta además, la distribución en plantas de dichos puntos. El diseño realizado sigue la siguientes pautas:

Sedes de menos de 48 puertos requeridos, con una única planta: se dota a la sede de un cisco catalyst 3560, no apilable.

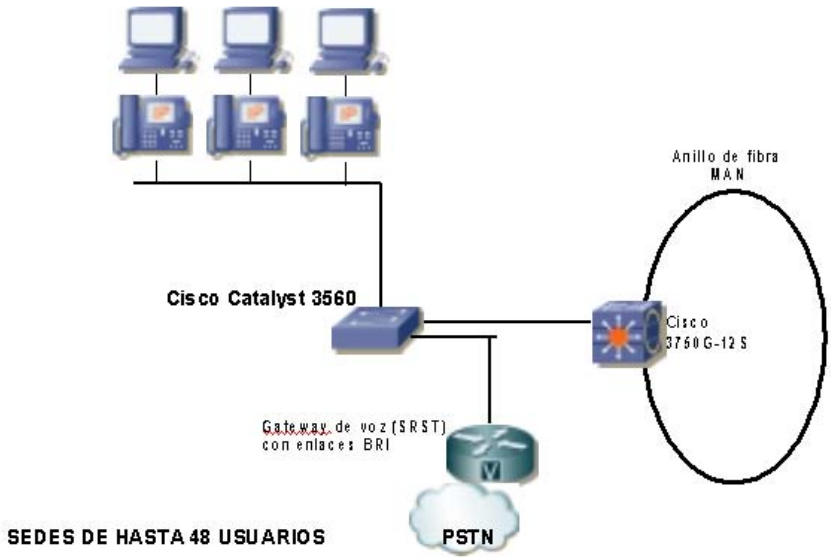


Figura 14 LAN Sedes de hasta 48 usuarios

Sedes de más de 48 puertos requeridos, con una única planta: se dota a la sede de un equipo cisco Catalyst 3750, con tecnología gigastack, que permite apilar varios equipos y poderlos gestionar como una única entidad lógica:

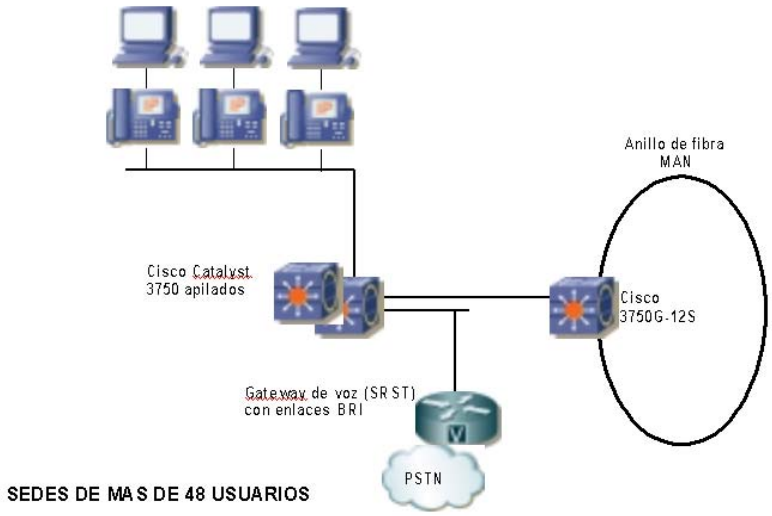


Figura 15 LAN Sedes de más de 48 usuarios

Sedes de más de una planta: para estas sedes se presenta una arquitectura de acceso y de distribución. En las distintas plantas se ubican los equipos de acceso, Cisco Catalyst 3750, con power inline, que agregarán los distintos usuarios. Estos equipos colapsarán en un equipo 4500 situado en la primera planta de cada edificio, mediante enlaces de fibra.

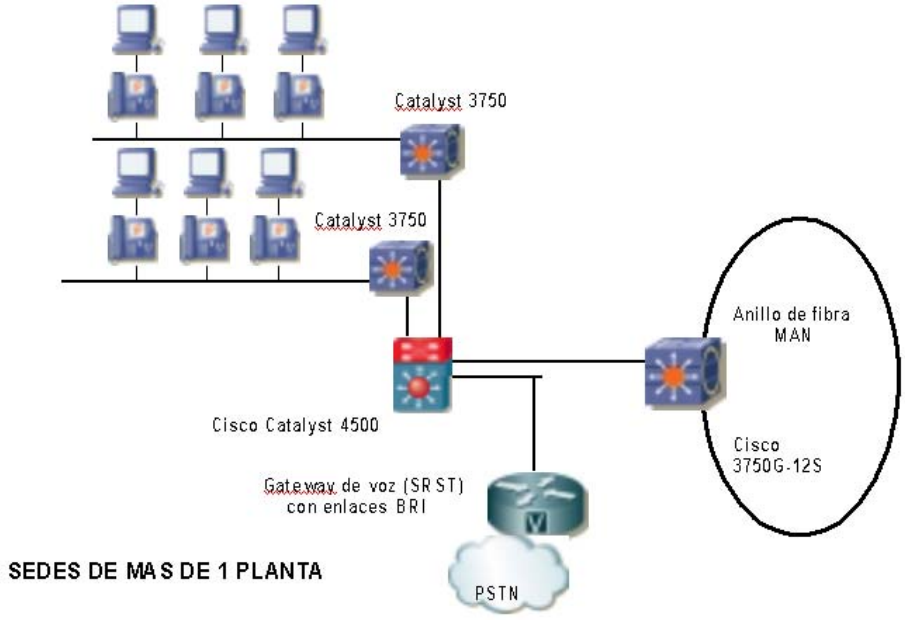


Figura 16 LAN Sedes de más de 1 planta

Todos los puertos de acceso de usuario son 10/100 BaseT y disponen de PoE para la alimentación de los teléfonos IP.
Los puertos requeridos se reparten equitativamente entre el número de plantas y se dimensionan los equipos a tal efecto. El 4500 alimenta a los usuarios de su misma planta.

A pesar de ser posible la reutilización de parte del equipamiento disponible hoy en día en algunas de las sedes de la AIE, dada la escasa información directa de que disponemos, al no haberse realizado ningún replanteo de las sedes, Italtel ha preferido presentar un diseño homogéneo para las lanes y dotarlas a todas de nueva tecnología de swithing power inline de Cisco, facilitando a su vez la gestión de toda la red.
No obstante, Italtel recomienda que una vez adjudicado el concurso, se realice un replanteo de la red actual y se realice un estudio más exhaustivo del equipamiento y cableado disponible, para ver si en algunas sedes se puede reutilizar el equipamiento existente de switching para conectar los nuevos teléfonos IP, y dotar a estos teléfonos de alimentadores locales power cube. Esta opción sería válida en las sedes, teniendo en cuenta que, si el conmutador no dispone de auxiliary vlan, necesitaremos dos puertos de red disponibles por usuario (uno para PC y otro para teléfono), que se requiere tecnología de switching y que el cableado esté en buenas condiciones.

2.7 PLAN DE DIRECCIONAMIENTO IP

Partiendo de la información proporcionada por el pliego sobre la asignación de direccionamiento IP en las distintas empresas, se propone un esquema de direccionamiento IP siguiendo las siguientes líneas:

Evitar solapamiento entre el direccionamiento de las distintas empresas. De esta forma se consigue que la comunicación entre todas ellas sea más sencilla y eficiente evitando el uso de traductores de direcciones en la red para el tráfico interno.

Separar el direccionamiento dedicado a equipos de datos del de equipos de voz. Así se refuerzan las políticas de seguridad de la red y se consigue separar ambos tipos de tráfico de forma adecuada.

Uso de direccionamiento privado para la red de voz: Al igual del que ya dispone la red de datos, la red de voz también se ha diseñado con direccionamiento privado para todo su equipamiento.

Mantenimiento dentro de lo posible del direccionamiento existente en las distintas empresas.

Como consecuencia de estas guías, se ha decidido de forma arbitraria en la propuesta de plan de direccionamiento la modificación de las subredes asignadas a algunas empresas cuando existía conflicto con el direccionamiento de otra, escogiendo un nuevo rango libre dentro de un direccionamiento privado. Por supuesto esta elección puede modificarse en función de la mayor o menor facilidad de migración de cada direccionamiento concreto.

2.8 SEGURIDAD

2.8.1 SEGURIDAD DE LA RED MAN

Los mecanismos de seguridad incluidos en la solución propuesta incluyen:

Virtual LANs:

Dentro de las diferentes sedes se propone el uso de VLANs separadas para el tráfico de datos y de voz. De esta forma se consigue el tráfico de voz no sea visible a los usuarios de datos y viceversa. Con esto se consigue:

Prevenir fraude: Con la configuración adecuada se puede conseguir que usuarios autorizados de datos consigan acceso a la red de voz, o viceversa.

Prevenir ataques DoS: Se evita que los ataques DoS –normalmente originados desde un PC- afecten a la red de voz.

Prevenir interceptación: Al encontrarse en redes separadas, se previene que un usuario de datos desde un PC pueda capturar el tráfico de voz.

VPNs:

La solución propuesta incluye un núcleo de red MPLS usando VPNs de nivel 3 diferentes para el tráfico de datos por empresa y el de voz también por empresa. Por tanto, de forma similar al caso de las VLANs para las redes de acceso, se consigue separar los distintos tipos de tráfico y por empresa.

Listas de acceso:

Estos mecanismos, presentes en todos los equipos de red presentes en la solución, permiten limitar el acceso a/desde recursos específicos. Con esto se consigue:

Prevenir fraude: Permite controlar desde qué orígenes se puede acceder a determinados recursos de la red.

Prevenir ataques DoS: Con la configuración adecuada se puede conseguir que en las zonas de la red deseadas sólo se permita pasar al tráfico conocido, evitando flujos de tráfico no deseados.

Port security:

Esta funcionalidad está presente en todos los equipos de acceso (switches) de la solución permite realizar un control de acceso de usuarios internos. De esta forma se permite limitar el acceso de usuarios a los recursos de la red y protege la red de voz consiguiendo:

Prevenir fraude: Se deniega el acceso a usuarios no autorizados.

Prevenir ataques DoS: El puerto del equipo no cursa ningún tipo de tráfico mientras que el equipo y el usuario no han sido autorizados.

Prevenir spoofing y suplantación de personalidad: Permite limitar el número de direcciones MAC conectadas a un puerto, evitando que una dirección falsa sustituya a una válida.

Servidor RADIUS:

Junto con la funcionalidad de port security anterior, este servidor da acceso a usuarios gracias a su login/password enviados durante la fase de conexión a red. Se proponen en esta oferta dos servidores Radius ACS de Cisco que almacenarán los datos de los usuarios de la red.

DHCP snooping:

Los equipos de acceso a red permiten filtrar los mensajes DHCP, permitiendo las respuestas –enviadas por servidores- sólo desde fuentes confiables. De esta forma se evitan ataques de DHCP spoofing.

Como lo hemos comentado anteriormente, el tráfico de voz y de datos está totalmente separado a nivel lógico mediante el uso de VLANs en las sedes y de VPNs MPLS en la red MAN. Sin embargo, existen algunas situaciones en las que las dos redes tienen que

intercambiar tráfico. El caso más evidente es el de los Softphones. En efecto, los Softphones son teléfonos Software instalados en los PCs de los usuarios y necesitan intercambiar tráfico de señalización con los elementos centrales de la voz corporativa (Call Managers) y tráfico RTP con los demás dispositivos de telefonía que se encuentran en la red de voz. Para solucionar este tema, se propone el uso de la autenticación y Autorización de estos dispositivos (PCs con Softphones) mediante un servidor Radius (Cisco Secure Access Control Server) situado en el CASSI que define que derechos tiene el usuario autenticado (uso de servicios de datos y voz por ejemplo). Además se puede hacer uso de listas de acceso en los equipos de red que permitirán limitar el intercambio de tráfico solamente viniendo de aquellos Softphones con los elementos de la red de voz y vice-versa.

2.8.1.1 Servidor Radius propuesto

Para cumplir con los requisitos de seguridad de la red propuesta, se propone un Cisco Secure Access Control de Cisco. De hecho, se proponen 2 máquinas por redundancia.
Cisco Secure Access Control Server (ACS) provee una solución de control de acceso basada en identidad, para las redes de información inteligentes de Cisco. Es la capa de integración y control para gestionar usuarios, administradores y recursos de infraestructura de red, en redes empresariales.
Cisco Secure ACS está disponible como un appliance dedicado montable en rack o como un software que se ejecuta sobre Windows 2000 y 2003. Ambos productos, aseguran a la AIE los servicios de autentificación, autorización y accounting (AAA).

Cisco Secure ACS es un servidor de acceso, altamente escalable, de alto rendimiento, que opera como un Server RADIUS centralizado y TACACS+. Extiende la seguridad en el acceso, combinando la autentificación de usuario, y el acceso de administrador, con control de políticas dentro de una solución de red con identidad centralizada, permitiendo una flexibilidad mayor y movilidad, incremento de la seguridad y una mayor productividad del usuario. Refuerza una política de seguridad uniforme para todos los usuarios, independientemente de la tipología de acceso a la red. Reduce el trabajo administrativo y de gestión relativo al escalado de usuarios y de administradores a la red. Utiliza una base de datos centralizada para todas la cuentas de usuario de tal forma que centraliza el control de los privilegios de todos los usuarios y los distribuye por centenares de puntos de acceso en toda la red. Como servicio de accounting, Cisco Secure ACS provee un reporte detallado y capacidades de

monitorización del comportamiento de los usuarios de la red y guarda un record de cada conexión de acceso y cambios en las configuraciones de equipos en cualquier punto de la red. ACS soporta una gran variedad de accesos, incluyendo lan o wireless lan, dialup, broadband, content, storage, VoIP, firewalls y VPNs.

La propuesta a la AIE incluye el ACS 1113, que se presenta en el formato appliance, y que incluye HW y SW.

2.8.2 SEGURIDAD DE LA RED CORE DE VOZ

Con el fin de ocultar la topología de los elementos centrales de la solución de voz y protegerlos, se propone un equipo Session Border Controller de Acme Packet descrito más en detalle en el documento descriptivo de la solución de voz. A continuación se describen las funcionalidades de seguridad que cumple este equipo.

2.8.2.1 Topology hiding

El SD oculta tanto la topología de nivel 3 (IP) como la de nivel 5 (signaling) lo que permite ocultar la topología de señalización y media a unos peers “un-trusted”. El ocultamiento de la topología de nivel 3 se hace mediante NAPT completo de la “source” y de la “destination” de todas las sesiones media. A nivel 5, el ocultamiento se realiza con un B2BUA (Back-to-Back User Agent) SIP integrado, un Proxy MGCP de señalización/media y vía un Gatekeeper Proxy y un B2BGW (Back-to-Back gateway) H323. Estas funciones aseguran que la infraestructura de señalización de red del operador no se vea comprometida, lo que puede llevar a piratería de red y/o a ataques de Denial of Service contra elementos de señalización no protegidos.

La implementación completa de NAT a nivel 3/5 es, en sí, la mejor protección contra ataques potenciales desde redes “untrusted”.

2.8.2.2 Access Control

El Net-Net SD implementa NAPT (Network Address & Port Translation) dinámico así como VLAN mapping para flujos de media y de señalización asociados a un servicio VoIP o multimedia. Para cada sesión SIP, MGCP o H323 establecida, el Net-Net SD asigna unos “bindings” NAPT para los flujos de media asociados con la sesión. Además, se usan VLANs para separar diferentes redes privadas.

La agregación de VLAN se puede extender de la red privada de la empresa hacia la frontera del operador. En algunos entornos específicos, esta solución permite ahorrar equipamiento CPE adicional y métodos de señalización no estándar. Un único Session Border Controller puede soportar muchas conexiones de clientes, y permite enrutar desde/hacia y entre las redes con solapamiento de direccionamiento IP.

2.8.2.3.1 Overload DoS Protection:

El SD define cuantas sesiones están autorizadas y cual es la tasa de iniciación de sesiones y el burst para los elementos de señalización adyacentes. Estos límites permiten al SD gestionar situaciones donde el elemento de señalización trusted ha sido atacado y genera más intentos de inicio de sesiones de lo que está autorizado.

En cuanto a la parte Media, el SD puede transmitir y filtrar los paquetes de Media hasta una tasa de 5 Gbps, ya que todo el filtrado de paquetes se hace a nivel Hardware. El packet processing plane y el signaling processing plane están separados asegurando que la demanda de recursos por parte del media nunca compite con el procesado de la llamada. El overload basado en Media no es posible con el SD.

2.8.2.3.2 Protección de Señalización contra DoS

Las partes de señalización SIP y H323 del Net-Net SD han sido testeadas y declaradas invulnerables por el SIP CERT Advisory CA-2003-06 y el NISCC Vulnerability Advisory 006489/H.323 respectivamente. Estos “advisories” identifican vulnerabilidades que pueden permitir a un “attacker” obtener acceso no autorizado con privilegios altos, provocar ataques DoS o causar un comportamiento instable del sistema.

2.8.2.4 Conexiones ICMP/TELNET/FTP restringidas

El Session Director no permite ninguna conexión entrante ICMP, TELNET o FTP por sus interfaces Media. Descartará de manera “silenciosa” cualquier request ICMP y no responderá a TCP SYNs para sesiones Telnet o FTP.

No respondiendo a ICMP en la parte “untrusted” de la red, no será posible para un usuario final, descubrir la dirección IP del Session Director mediante comando Traceroute. No responderá tampoco a paquetes HTTP, random UDP o TCP, protegiendo así la visibilidad de sus propias direcciones IP.

Se puede configurar el Session Director para aceptar ICMP/FTP/TELNET en las interfaces MEDIA si necesario. Esto podría ser un requerimiento para la parte core de la red.

2.8.2.5 Separación de interfaces para Media y Management

El Session Director recibe el tráfico de señalización y de Media en interfaces diferentes a las de Management.

Se usan las interfaces Wancom en la parte trasera del equipo para la gestión Telnet, FTP o SNMP.

Las interfaces Wancom son gestionadas por un procesador dedicado para evitar consumir recursos del procesador principal.

3. DIMENSIONADO DE LOS ENLACES

3.1 CALCULO DEL ANCHO DE BANDA DE VOZ

Con el fin de calcular el ancho de banda consumido por las llamadas de voz saliendo de cada sede, se ha considerado el codec G.711 con una paquetización de 20ms.
El ancho de banda por llamada se calcula de la siguiente forma:

Ancho de banda por llamada = (Tamaño paquete de voz) x (Nº paquetes por segundo)

Donde:
Tamaño paquete de voz = (Tamaño cabeceras) + (Tamaño payload voz)
Nº paquetes por segundo = (Codec bit rate) / (Tamaño payload voz)

Un ejemplo de una llamada G.711 con 20ms de paquetización en Ethernet: sin cRTP y sin VAD:

Tamaño payload de voz = (8kBytes/s x 20ms) / 1000 ms = 160 bytes
Tamaño cabeceras = 12 (RTP) + 8 (UDP) + 20 (IP) + 18 (Eth)= 58 Bytes
Tamaño paquete de voz = 160 bytes + 58 bytes =218 bytes
Nº paquetes por segundo = 8000 kBps / 160 Bytes = 50 pps

Ancho de banda por llamada = 218 bytes x 50 pps = 87,2 kbps

Añadiendo un 5% para la señalización, obtenemos el resultado siguiente:

Ancho de banda por llamada con señalización = 91,56 kbps

Por lo tanto, conociendo el número de líneas, se puede deducir de manera sencilla el ancho de banda consumido por todos estos usuarios si llaman simultáneamente. En el documento "*ANEXO B: Cálculos de Anchos de Banda*" se encuentra una tabla donde se ha calculado para cada sede el ancho de banda requerido para las comunicaciones de voz.
Para realizar el calculo de ancho de banda requerido, se ha considerado un tráfico de 0,1 Erlang por usuario lo que viene a significar que un 10% de los usuarios de la sede llaman simultáneamente hacia el exterior (PSTN u otra sede).

3.2 CALCULO DEL ANCHO DE BANDA DE DATOS

En cada una de las sedes, se ha tenido en cuanta el número de usuarios LAN y se ha considerado un ancho de banda de unos 200 kbit/s por usuario. De esta manera, se obtiene el ancho de banda requerido para cada una de las sedes.
Independientemente de este calculo, cualquier sede conectada a un puerto de un 3750 del anillo dispondrá de un acceso de 1 Gigabit/s lo que, considerando 200 kb/s por usuario, supera con creces el ancho de banda requerido por sede.

3.3 CAPACIDADES REQUERIDAS EN LA TRONCAL

Se muestra en la siguiente tabla el dimensionado realizado para los enlaces de acceso y anchos de banda requeridos (voz y datos) para las diferentes sedes que pertenecen a la troncal

Oficina/Institución	EMPRESA	EXT_TOT				Acceso_ Ofrecido (Mbps)	TIPO_ SEDE	ANILLOS
Gerencia Municipal de Urbanismo (S. Central)	GMU	374	460	1000	95	1000	**PPAL**	
Encarnación	AYTO	296	275	100	58	1000	TIPO A	CENTRO
Arenal	AYTO	216	300	100	62	1000	PPAL	CENTRO
Oficina Central	EMASESA	225	218	4	46	1000	**PPAL**	CENTRO
Store	EMASESA	64	66	1000	14	1000	TIPO A	ESTE
Oficina Central	LIPASAM	81	85	100	18	1000	**PPAL**	NOROESTE
Juventud	AYTO	80	40	0,5	9	1000	TIPO A	NOROESTE
Distrito Triana - Los Remedios	AYTO	88	60	0,5	13	1000	TIPO A	NOROESTE
Participación Ciudadana. Marqués del Contadero	AYTO	64	20	0,5	5	1000	TIPO A	CENTRO
Carambolo	EMASESA	42	43	18	9	200	TIPO A	RadioEnlace
Cartuja	AYTO				0	1000	TIPO D	
Gobernación	AYTO	10	120	2	24	1000	TIPO A	
Instituto Municipal de Deportes. Sede Central	IMD	88	125	10	26	1000	TIPO A	
UTS El Esqueleto	AYTO	96	10	0,5	3	1000	TIPO B	CENTRO-SUR
Bomberos - Sur	AYTO	10	35	2	7	1000	TIPO A	CENTRO-SUR
Edificio Catalana	AYTO	64			1	1000	TIPO A	CENTRO-SUR

Parques y Jardines (Pabellón Marroquí)	AYTO	48	60	0,5	12	1000	TIPO A	CENTRO-SUR
Pabellón Real	AYTO	128	25	2	6	1000	TIPO A	CENTRO-SUR
Medio Ambiente (Pabellón de la Madrina)	AYTO	120	85	2	18	1000	TIPO A	NOROESTE
Diego de Riaño	AYTO	9	60	0,5	12	1000	TIPO A	ESTE
Centro de Urgencias y Especialidades - Equipo Quirurgico	AYTO	96	45	0,5	10	1000	TIPO A	ESTE
Bomberos - Parque Central	AYTO	64	35	2	8	1000	TIPO A	ESTE
Torre de la Plata	AYTO	48	15	2	3	1000	TIPO B	NOROESTE
Real Alcázar	ALCÁZAR	44	10		2	1000	TIPO B	NOROESTE
Agencia Municipal de Recaudaciónm (SSCC)	AMR	75	59	100	12	1000	TIPO A	ESTE
Oficina Central	EMVISESA	80	67	0,75	14	1000	**PPAL**	CENTRO-SUR
Alcaldía	AYTO	232	75	2	17	1000	TIPO A	CENTRO-SUR
Pajaritos	AYTO	143	70	2	15	1000	TIPO A	CENTRO-SUR
Gabinete de prensa y otros. (Edif. Laredo)	AYTO	96	25	100	6	1000	TIPO A	CENTRO-SUR
Cultura	AYTO	48	35	0,5	7	1000	TIPO A	CENTRO
Multas	AYTO	16	30	2	6	1000	TIPO A	CENTRO
Hemeroteca Municipal	AYTO	48	25	0,5	5	1000	TIPO B	CENTRO
Educación	AYTO	48	10	0,5	2	1000	TIPO B	CENTRO-SUR
Arroyo	EMASESA	43	38	0,25	8	1000	TIPO A	ESTE
Laboratorio Municipal	AYTO	48	10	2	2	1000	TIPO A	ESTE
Bienestar Social (Palacio Marqueses de la Algaba)	AYTO	112	60	0,5	13	1000	TIPO A	NOROESTE
Hogar Virgen de los Reyes - UTS Macarena	AYTO	80	20	0,5	5	1000	TIPO B	NOROESTE
Pica	EMASESA	32	29	0,25	6	1000	TIPO A	ESTE
Oficina Central	TUSSAM	174	150	2	32	1000	**PPAL**	ESTE
Estadística	AYTO	80	80	2	17	1000	TIPO A	ESTE
Mantenimiento de Edificios	AYTO	64	20	0,5	5	1000	TIPO A	
Bomberos - Carretera Amarilla	AYTO	32	5	0,5	1	1000	TIPO C	ESTE

Tabla 15 Anchos de banda propuestos en la troncal de fibra

Los cálculos de la columna "BW_Calculado" se han realizado sumando el ancho de banda consumido por los usuarios LAN (200 kbps/usuario) y el ancho de banda consumido por las llamadas de voz (91,56 kbps /llamada considerando un tráfico de 0,1 Erlang por usuario).

A pesar de disponer de un acceso de 1 GE para todas las sedes de la troncal, es recomendable limitar el ancho de banda que se pone a disposición de una sede para evitar que, en un momento dado, la sede haga un uso abusivo del ancho de banda disponible. Los perfiles de ancho de banda pueden aplicarse sobre el tráfico cursado en cada uno de los puertos asignados a las sedes y en función del servicio (Voz o Datos) que debe controlarse. Existe la posibilidad de hacerlo tanto en entrada como en salida de cada puerto sin que su configuración reduzcan el resto de funcionalidades del equipo dentro de los límites marcados.
La forma de configurar el traffic policing (o limitación de ancho de banda) podrá depender de si los servicios están asociados a puertos físicos o conexiones lógicas.

En el documento "*ANEXO B: Cálculos de Anchos de Banda"*, se ha calculado el ancho de banda requerido para cada una de las sedes.

Conexión con redes externas y otros lotes

3.4 Intercomunicación con el CASSI

En la solución propuesta, la interconexión con el CASSI es de vital importancia ya que el CASSI alberga toda la infraestructura de conexión con redes externas como la PSTN, Internet y otras redes. Por otro lado, los servidores de gestión también se encuentran en el CASSI.
Por lo tanto, la conexión de la red Metropolitana a este centro se realiza mediante 2 enlaces fibra de 10 GE hacia el CASSI. Cada uno de estos enlaces sale de uno de los dos 7606 de Core evitando tener un único punto de fallo en la interconexión.

Para terminar los dos enlaces de 10 GE que salen del core de la MAN, se propone el equipo Cisco Catalyst 3750G-16TD. Este equipo será el Punto de Terminación del lote de datos respecto al CASSI (PdTB). Se pondrán 2 de estos equipos apilados con la tecnología Stackwise de Cisco Cada uno de los enlaces terminará en un Catalyst 3750G-16TD que se describe a continuación.

El Cisco Catalyst 3750G-16TD forma parte de la serie de los 3750 de Cisco Catalyst, un producto que representa una nueva generación de conmutadores ofreciendo la tecnología Stackwise de Cisco, un método de apilamiento con una interconexión de 32 Gbps. Esta tecnología permite apilar hasta nueve unidades de Cisco Catalyst 3750 en una sola unidad lógica mediante unos cables de interconexión específicos para adaptarse a cualquier cambio de la red manteniendo un alto rendimiento. La densidad ofrecida por el Stack es muy elevada ya que permite llegar hasta un máximo de 468 puertos 10/100, 468 puertos 10/100/1000, 108 puertos ópticos de agregación, 9 puertos 10 Gigabit Ethernet o cualquier mezcla de estos puertos.

Figura 25 Catalyst 3750G-16TD para PdTB

La pila (Stack) se comporta como una única unidad lógica gestionada por un switch master elegido dentro de los miembros de la pila.

El equipo propuesto a la AIE para realizar la función de interconexión con el CASSI se compone de una pila de 2 Catalyst 3750G-16TD con el Software mejorado, cada equipo provisto de un puerto 10 GE mediante el módulo XENPAK (10GBASE-LR) soportando fibra monomodo y distancias de hasta 10 km.

3.5 CONEXIÓN CON RED PSTN

El acceso a la PSTN está centralizado en los Media Gateways controlados con las funcionalidades de Media Gateway Controler disponibles en iSSW de Italtel, que garantizará el "interworking" necesario entre los distintos dominios de red incluidos en la solución.
La disponibilidad de una interconexión centralizada SS7 (mediante enlaces E1s) a la red PSTN, controlada por iSSW, permite eliminar los requisitos de conectividad locales interconectándose de manera eficiente a la red de Proveedor de Servicios y disfrutando de las ventajas de mecanismos de enrutamiento avanzados para la optimización de la entrega de tráfico a la PSTN.

La interconexión centralizada en SS7 permite garantizar la independencia de la numeración asignada a la empresa del acceso físico TDM, lo que permite mantener la numeración asignada en los procesos de migración de tecnología TDM a IP.

4. ENRUTAMIENTO

Como ya se ha comentado en anteriores apartados, la red propuesta se basa principalmente en el protocolo MPLS en el core y en VPNs MPLS para aislar el tráfico de las diferentes empresas de la AIE DeSevilla y del Ayuntamiento. A continuación se describen los diferentes protocolos que se proponen utilizar en la red para el routing:

Protocolos OSPF y BGP

Para poder implementar esta funcionalidad de VPN, es necesario activar en los equipos de core/agregación que realizarán la función de P y de PE el protocolo MPLS y MPLS LDP (Label Distribution Protocol).
El protocolo de routing IGP propuesto para implementar la solución es OSPF Open Shortest Path First. Este protocolo se habilita en los equipos 7606 del core, en los 7604 de agregación en los 3750 de acceso. El diseño del routing se basaría en una area de Backbone (Area 0) compuesta por los equipos 7606 de core y las interfaces de los equipos 7604 conectados a los7606. Cada anillo tendría su propia area (Area 1, Area 2, Area 3 y Area 4). De esta forma el Area 0 se encuentra en el centro de todas las otras areas. A nivel de seguridad, se configuraría una clave en cada router para establecer adyacencias seguras y garantizar la autenticidad de los paquetes OSPF recibidos.
Por otra parte, el protocolo de routing que permite el transporte de etiquetas entre los Pes (Provider Edge) para el establecimiento de VPNs MPLS es MP-BGP (Multiprotocol BGP). Por lo tanto se establecerán sesiones i-BGP (full-mesh i-BGP) entre todos los PEs (los 7604) de la red Metropolitana y se configurarán las VPNs de cada empresa en estos equipos. De esta forma, los routers P's no tienen conocimiento de las VPNs y su función es la de conmutar etiquetas dentro de la red para llevar los paquetes a su destino.

Funcionalidad multi-VRF CE

En la topología en anillo, puede darse el caso de que una conexión CE-PE no sea directa y

que el tráfico entre un CE de una sede y un PE tenga que cruzar uno o varios hops IP. En este caso, se utilizará una funcionalidad disponible en el IOS de los 3750 que se denomina multi- VRF CE y que permite crear varias tablas de routing en un mismo equipo para diferenciar el tráfico de las sedes del anillo y llevarlo hasta el router PE.

Routing en las sedes

En todas las sedes del Ayuntamiento y DeSevilla, se configurará una VLAN de voz y una VLAN de datos. En principio, los PCs de usuarios que dispongan de teléfonos IP irán conectados al puerto (switch integrado) del teléfono lo que permite conectar los 2 dispositivos
al mismo puerto del switch de la LAN y ahorrar en cableado y en puertos del switch. Esto es posible utilizando la funcionalidad de Auxiliary VLAN disponible en los switches de Cisco que separa lógicamente el tráfico de voz del de datos metiéndolos en VLANs diferentes. Se configurarán los switches para que todos los PCs estén en la VLAN de datos y los teléfonos en la VLAN de voz.
El Default Gateway de los teléfonos será el interface VLAN de voz configurado en el switch del anillo. De la misma manera, el Default Gateway de los PCs de la sede será el interface VLAN de datos configurado en el mismo switch del anillo. A partir de este punto, el tráfico de voz se transportará en la VPN de voz a nivel 3 y el tráfico de datos en su VPN correspondiente.

5. SERVICIOS

5.1 VPNS DE NIVEL 3

El servicio de MPLS VPNs permite conectar usuarios y recursos en cualquier sitio en la red sin comprometer el rendimiento o el diseño de la red. La escalabilidad de las VPNs MPLS es indudable y permite mantener los gastos de operación reducidos ya que no se requiere ninguna reconfiguración manual cuando se añaden o modifican grupos. Por otro lado es una tecnología muy recomendable delpunto de vista de la escalabilidad. A continuación se describe brevemente la nomenclatura utilizada para MPLS y el servicio propuesto a la AIE para su red MAN.

En la nomenclatura de MPLS VPNs, existen básicamente 3 tipos de funcionalidades que se describen brevemente a continuación.

Customer Edge (CE)

Un equipo CE provee acceso a la red Metropolitana, anuncia sus rutas locales al router PE y aprende rutas remotas de la VPN desde el router PE.

Provider Edge (PE)

Los PEs intercambian información de routing con los CEs utilizando RIPv2, OSPF o EBGP. Después de aprender las rutas locales de la VPN, el PE intercambia información de routing VPN con otros routers PEs mediante iBGP. Se puede utilizar Route Reflectors en el caso de tener muchos PEs para evitar el full-mesh iBGP pero, en nuestro caso, optaremos por una solución full-mesh ya que tenemos pocos PEs.

Provider Routers (P)

Un router Provider (P) realiza tareas de forwarding de tráfico VPN entre routers PE.
Dentro de los servicios que se proponen para la red Metropolitana de Telecomunicaciones de la AIE DeSevilla y del Ayuntamiento, se ofrece el servicio de Red Privada Virtual de nivel 3 basado en la tecnología MPLS (Multi Protocol Label Switching). El servicio de VPN MPLS permite crear Redes Privadas virtuales sobre una red IP ofreciendo privacidad, escalabilidad y flexibilidad a los usuarios de estas VPNs. La facilidad de provisión de estas VPNs permite en cualquier momento y con una configuración limitada, añadir una sede a la Red Privada Virtual.

La solución propuesta consta de una VPN por cada empresa lo que garantiza la independencia de cada una de las empresas de la AIE y del Ayuntamiento aún compartiendo la misma infraestructura de red. De esta manera, cada una puede gestionar su plan de direccionamiento IP como quiere sin preocuparse del posible solapamiento que pueda existir entre diferentes sedes. Por otra parte, en el momento que lo desea y sin demasiada complicación, la AIE y el Ayuntamiento pueden juntar sus redes a nivel lógico cuando se haya realizado la adecuación del plan de direccionamiento de todas las sedes y así tener una única red IP para las cinco empresas.

La red de gestión de los diferentes equipos de la solución también se basará en una única MPLS VPN tal y como lo requiere el pliego. Esta red integrará todos los elementos que se hayan instalado en las sedes y los elementos que dan conectividad entre las sedes con los servidores de gestión, permitiendo una administración global de los recursos.

5.2 ACCESO A INTERNET

Todo el tráfico de las sedes hacia y desde Internet se enrutará a través de los diferentes elementos de acceso, agregación y core pasando siempre por el CASSI que dispondrá del acceso al ISP. De esta forma, garantizamos una total seguridad a todos los usuarios porque cualquier tráfico destinado a la red pública estará analizado y filtrado por los elementos de seguridad del CASSI.

La primera consideración a tener en cuenta es decidir si se va a utilizar direccionamiento público o privado. En el entorno empresarial parece impensable que cada máquina del cliente tenga una dirección pública. Una vez tomada la decisión de utilizar un direccionamiento privado, se tiene que decidir donde realizar la traducción de direcciones privadas a direcciones públicas para la salida a Internet.

Hacerlo de forma centralizada puede plantearse en caso de que el direccionamiento de los clientes no pudieran solaparse entre sí o que se dispusiera de un dispositivo centralizado capaz de soportar NAT por contextos virtuales o por VRF. Al utilizar una solución basada en MPLS VPNs podemos manejar perfectamente direccionamiento solapado y utilizar un equipo centralizado que soporta NAT por VRF. Este equipo estaría situado en el CASSI y no forma parte de esta oferta.

5.3 SERVICIO DE VOZ CORPORATIVA Y VIDEOCONFERENCIA

La solución a estos servicio objeto del Lote 1 de Datos se describe en detalle en documentos de especificaciones técnicas propiedad de Italtel en colaboración con Cisco Systems, por lo que no ha sido considerado conveniente incluirlo en la documentación básica anexa al PFC, en caso de necesidad podrán ser consultados bajo pedido y previa autorización de Italtel.

5.5 RED INALÁMBRICA

5.5.1 SOLUCIÓN PROPUESTA

La solución de red inalámbrica se basa en los equipos AP1131 de Cisco que pueden dar cobertura tanto a los dispositivos inalámbricos de usuarios como a los teléfonos inalámbricos incluidos en esta oferta. Al no tener una distribución de los sitios donde se tienen que instalar estos equipos, se ha hecho una aproximación recogida en la oferta económica.
En la estimación hecha, cada AP1231 da cobertura a una planta y se conecta al switch de la planta recibiendo alimentación del mismo.

Para determinar el número de Access Points necesarios para la AIE, se requiere un replanteo y un estudio de cobertura previo en cada una de las sedes que tendrán cobertura inalámbrica.

5.5.2 EQUIPAMIENTO PROPUESTO

El equipamiento propuesto para dar servicio a los equipos inalámbricos de todas las sedes de la AIE es el Cisco AP1131.

Part Number	Descripción	Qty
AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	314
AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	314
AIR-PWR-CORD-CE	AIR Line Cord Central Europe	314
AIR-PWR-A	Pwr Sply In:100-240VAC Out:48VDC 380mA -1100, 1130AG	
S113RK9W-12311JX	Cisco 1130 Series IOS WIRELESS LAN LWAPP RECOVERY	314
AIRLAP-FIPSKIT	FIPS Kit for LWAPP APs	314

Tabla 16 Access Point propuesto: Cisco AP131AG

La serie Aironet 1130AG de Cisco soportando IEEE 802.11a/b/g provee un alto rendimiento, una alta seguridad ofreciendo acceso WLAN a un coste reducido.

Figura 26 Access Point AP1131AG

El soporte de encripción en hardware (Advanced Encryption Standard (AES) o Temporal Key Integrity Protocol (TKIP)) permite la interoperabilidad con la seguridad basada en IEEE 802.11i, WiFi Protected Acces 2 (WPA2) o WPA.

El Aironet 1130AG se encuentra disponible en dos versiones distintas: "unified" o "autonomous". Los Access Points "unified" utilizan el protocolo LWAPP (Lightweight Access Point Protocol) y funcionan conjuntamente con Wireless LAN controllers de Cisco y el Cisco Wireless Control System (WCS). Cuando está configurado con LWAPP, el Airones detecta automáticamente el mejor Cisco Wireless LAN Controller y baja su configuración y las políticas adecuadas sin necesidad de intervención manual. Los Access Points "autonomous" se basan en el IOS de Cisco y pueden operar opcionalmente con CiscoWorks Wireless LAN Solution Engine (WLSE). Los APs "autonomous", juntos con CWLSE ofrecen un conjunto de funcionalidades claves y se pueden actualizar en campo adaptándose a la evolución de los requerimientos de red.

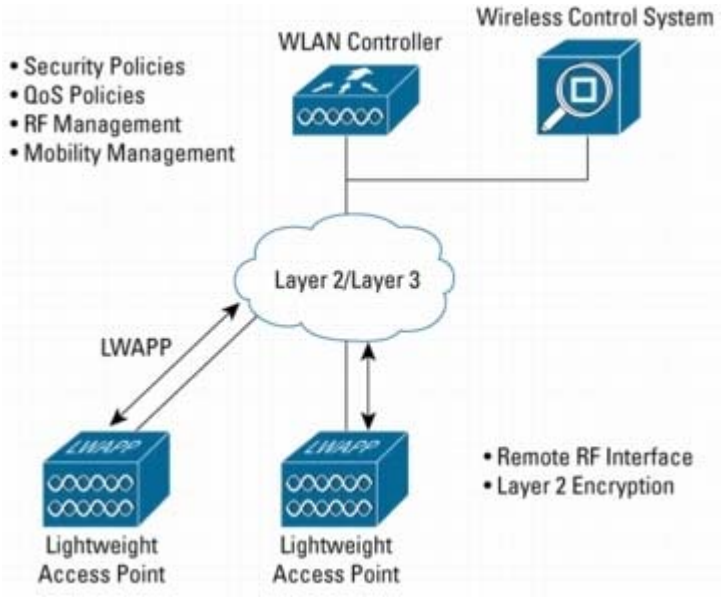
Las antenas integradas ofrecen una cobertura omnidireccional y los brackets permiten montar los Acces Points fácilmente en techos y paredes.

A nivel de seguridad, el equipo soporta 802.11i, Wi-Fi Protected Access (WPA), WPA2 y varios tipos de EAP (Extensible Authentication Protocol). WPA y WPA2 son las certificaciones de la Wi-Fi Alliance para seguridad WLAN estándar e interoperable. Estas certificaciones soportan 802.11x para la autenticación de usuarios, TKIP para la encripción WPA y AES para WPA2.

Estas certificaciones permiten asegurar la interoperabilidad entre dispositivos Wi-Fi de diferentes fabricantes también certificados. Cuando se utiliza el protocolo LWAPP, descrito anteriormente, los Access Points soportan Cisco Unified Intrusión Detection System/Intrusión Prevention System (IDS/IPS), una funcionalidad Software. Cuando un cliente asociado envia tráfico malicioso en la red Wireless, un dispositivo IDS detecta el ataque y manda peticiones shun al Cisco Wireless LAN Controller que eliminará automáticamente la asociación del cliente.

Los Access Points de la serie 1130AG en modo "autonomous" soportan el modelo de protección de Management Frame para la autenticación tramas de management 802.11 por la infraestructura de red Wireless. Esto permite a la red detectar tramas "spoofed" desde Access Points o usuarios maliciosos. Si un Access Point detecta un ataque, genera un evento (incident) y el Cisco Wireless LAN controler, el Cisco WCS o el CiscoWorks WLSE recoge los informes.

Para la gestión de los Access Points de la red y el control de la configuración y de las políticas, se propone el Wireless LAN Controller 4400 y el Wireless Control System. El dibujo siguiente describe el flujo en la red entre los Access Points y estos dos elementos.



La oferta propuesta incluye tanto el AP1131 con LWAPP como 3 Wireless LAN Controller 4404 y el sistema Wireless Control System.

6. GESTIÓN DE LA RED

6.1 GESTIÓN DE LA RED DE DATOS

En este apartado del documento se describe cual será la arquitectura de gestión para la red de datos. Como único elemento para la gestión de todos los dispositivos que componen la red de datos se propone el elemento de gestión CiscoWorks LAN Management Solution (LMS), elemento que proporciona todas las herramientas de gestión integradas necesarias para simplificar la configuración, administración, supervisión, y localización de averías de las redes Cisco. Por lo tanto el esquema de red sería el siguiente:

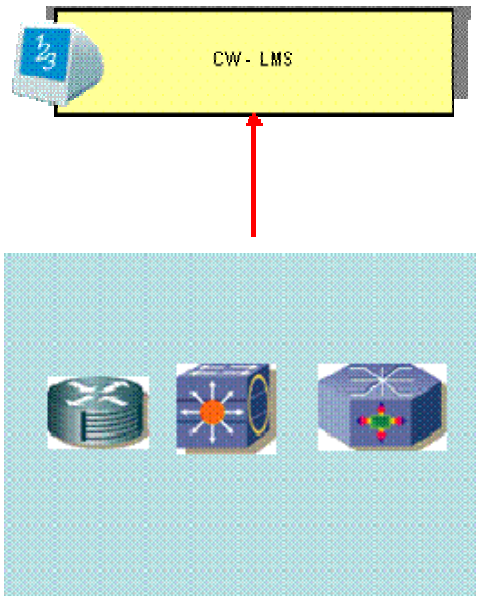


Figura 27 Arquitectura gestión red de datos

6.1.1 CISCOWORKS LAN MANAGEMENT SOLUTIONS

CiscoWorks LMS proporciona al cliente un sistema integrado para compartir la información de los dispositivos a través de las aplicaciones de gestión, automatizando las tareas de gestión de los dispositivos, visualizando el estado y la capacidad de la red e identificando y localizando eventuales fallos en la red. Mediante el conocimiento del inventario de red, CiscoWorks LMS proporciona en una plataforma única todas las capacidades funcionales de gestión y proporciona las capacidades de integración con los sistemas de la capa superior.

CiscoWorks LMS 2.6 incluye:

- CiscoWorks Common Services: un conjunto de servicios compartidos entre todas las aplicaciones de CiscoWorks LMS. Common Services incluye los componentes CiscoView, que proporciona un "front panel" grafico que muestra los elementos gestionados permitiendo a los usuarios interactuar con facilidad con los elementos para cambiar los parámetros de configuración y estadísticas de monitorización, y Integration Utility, el modulo que permite la integración con NMS (Network Management System) de otros fabricantes.
- Resource Manager Essentials (RME) que proporciona la gestión del ciclo de vida de los dispositivos de red. Diseñado para reducir el error humano y eliminar muchas de las tareas manuales asociadas a mantener una red. CicosWorks RME incluye las herramientas para configurar los dispositivos, almacena el inventario de la configuración de los dispositivos, controla cambios en la configuración de estos y gestiona las imágenes software cargadas en los dispositivos y permite la actualización de estos a las nuevas versiones disponibles.
- Campus Manager (CM): proporciona las funcionalidades de descubrimiento de conexiones, visualización de la topología de red, gestión VLANs, permite la creación, modificación y borrado de las VLAN y la asignación a estas de puertos de los equipos gestionados, así como la visualización de la configuración detallada y del estado de los puertos de una VLAN, User Tracking, permite la localización de los equipos conectados a la red. Cada usuario o equipo conectado a la LAN se puede identificar mediante nombre de usuario, dirección IP o MAC, pudiendo localizar exactamente el switch y puerto del switch al cual el equipo está conectado. Las tablas con estas informaciones se almacenan en el mismo sistema, y Path Análisis para el traceo de la conectividad entre dos equipos de la red, sea a nivel físico que lógico
- Device Fault Manager (DFM): que proporciona la capacidad de supervisar en tiempo real las averías de los dispositivos y de determinar la causa raíz correlacionando las averías del dispositivo. DFM puede publicar notificaciones de condiciones críticas la red vía email. Dispone de un histórico de fallos que permite al operador almacenar y tener acceso a la información histórica sobre alarmas y averías que han sido detectadas y procesadas por DFM
- Internetwork Performance Monitor (IPM): mide el rendimiento de la red basándose en la tecnología sintética de generación del tráfico dentro del software Cisco IOS®, que

se conoce como Cisco IOS IP SLA. Utilizando esta tecnología sintética de generación del tráfico permitimos al elemento de gestión tener un alto grado de flexibilidad en la selección de los endpoints de la red objeto del análisis del rendimiento. Esta flexibilidad hace que IPM sea una herramienta de localización de averías altamente eficaz. IPM utiliza la tecnología Cisco IOS IP SLA para configurar agentes de rendimiento en los routers, los colectores.

Estos colectores como parte de la configuración tienen al dispositivo de origen, el de destino y el tipo de operación a realizar.

6.2 GESTIÓN DE LA RED WI-FI

En este apartado del documento se describe cual será la arquitectura de gestión para la red inalámbrica. Los elementos propuestos son el **Cisco Wireless LAN Controllers** para el control de las funciones de los Access Points y **Cisco Wireless Control System (WCS)** que proporciona las herramientas para la planificación, la configuración y la gestión de una LAN inalámbrica.

6.2.1 CISCO WIRELESS LAN CONTROLLERS

El elemento Cisco Wireless LAN Controller es el ideal para la gestión de LAN inalámbricas proporcionando funcionalidades como las políticas de seguridad, la prevención de intrusión, la gestión de la RF, la calidad de servicio (QoS) y la movilidad. El Cisco Wireless LAN Controller está integrado y trabaja conjuntamente a las Cisco Access Points y al Cisco Wireless Control System (WCS) para el soporte de las aplicaciones inalámbricas.

Desde el acceso a los servicios de voz hasta la localización del equipo el WLAN controller proporciona el control, la escalabilidad y la confiabilidad necesaria para la implementación de una red inalámbrica segura.

El Cisco Wireless LAN Controller se integra suavemente en una red empresarial que ya esté en servicio y permite un facil despliegue de una nueva red inalámbrica. Comunica con los APs a través de infraestructuras de nivel 2 (ethernet) o de nivel 3 (IP) mediante el protocolo Lightweight Access Point Protocol (LWAPP). Este nuevo estándar IETF ayuda a mantener la seguridad en la comunicación entre Access Points y Wireless LAN Controller y proporciona la completa automatización de las funciones de gestión y configuración.

El Cisco Wireless LAN Controller permite la creación y el cumplimiento de políticas ent-to-end en una LAN inalambrica que soporte aplicaciones críticas. Varios WLAN Controllers se reconocen automáticamente y coordinan los servicios de WLAN de manera uniforme en la red. De este modo los sistemas trabajan en conjunto como un sistema solo para proporcionar una red WLAN escalable hasta disponer de miles de APs.

A continuación se describen las funcionalidades proporcionadas por el sistema.

Intelligent RF Management. El WLAN Controller dispone del software necesario para la gestión de la RF en "adaptive real-time", utilizando un algoritmo RRM (Radio Resource Management) que detecta y adapta en tiempo real los cambio que se produzcan en la trata de radio frecuencia. Estos ajustes permiten la creación de la topología de red óptima para la red inalámbrica en la misma manera que los protocolos de routing crean la mejor topología posible para las redes IP. Las capacidades de gestión de la RF incluyen:

- Asignación dinámica de los canales 802.11.
- Detección de interferencias y ajuste de la red para optimizar el rendimiento.
- Balanceo de carga de los usuarios entre los puntos de acceso.
- Detección de los puntos de baja cobertura y ajuste de la potencia de emisión de los puntos de acceso.
- Control dinámico de la potencia de emisión de los puntos de acceso.

Airtight Security. El WLAN Controller adhiere al nivel más estricto de los estándares de seguridad, incluyendo:

- 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, and Wired Equivalent Privacy (WEP)
- 802.1X with multiple Extensible Authentication Protocol (EAP) types—Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS), EAP-FAST, EAP-SIM and Cisco LEAP
- VPN termination and Management Frame Protection
- Federal Information Processing Standards (FIPS) 140-2 Level 2 Validation

En la arquitectura de LAN inalámbrica de Cisco los puntos de acceso actúan como monitores aéreos, comunicando la información que se refieren al dominio inalámbrico a los controladores WLAN en tiempo real. Todas las amenazas de seguridad son identificadas rápidamente y presentadas al administrador de la red vía Cisco WCS, donde se puede realizar el análisis exacto y tomar la decisión sobre la acción correctiva a realizar.

La red dispone de varios niveles de protección, que son:

- RF Security, detecta y evita interferencias 802.11 y controla la propagación de RF no deseada.
- Prevención de intrusiones en la red inalámbrica y localización de intrusos.
- Control de accesos y autenticación distintos por usuario o por grupo de usuarios.
- Network Admisión Control (NAC).
- Secure Mobility.
- Guest Tunneling, para permitir el acceso a usuarios invitados que pero no pueden tener acceso a determinados recursos de red.
- Secure backhaul que permite la encriptación del tráfico de datos sobre enlaces de backhaul inalámbricos para garantizar seguridad adicional

Real-Time Applications Support. El WLAN Controller proporciona el mejor rendimiento posible para aplicaciones en tiempo real como la voz permitiendo la conmutación rápida entre distintos puntos de acceso y múltiples controladores, proporcionando una movilidad suave sin interrupción en el servicio al cliente.

Mobility. El WLAN Controller permite que los usuarios puedan moverse en ambientes distintos (interior o exterior) conmutando el servicio entre distintos Access Points y manteniendo los niveles de seguridad y QoS establecidos para cada usuario y así asegurando que la movilidad no compromete el rendimiento, la confiabilidad o la privacidad.

La utilización de WLAN Controller no requiere ninguna modificación a las infraestructuras existentes o a dispositivos de cliente para permitir la movilidad.

6.2.2 CISCO WIRELESS CONTROL SYSTEM (WCS)

El Cisco Wireless Control System (WCS) es la plataforma que proporciona las herramientas para la planificación, la configuración, la gestión de una LAN inalámbrica.

Cisco WCS utiliza el protocolo SNMPv3 para la comunicación con los controladores de LAN inalámbrica. El sistema también soporta las versiones 1 y 2 de SNMP, que permiten que otras plataformas de gestión de la red accedan para consultar las informaciones que almacena. Los administradores de la red pueden acceder a los WCS de Cisco vía cualquier navegador HTTP o HTTP seguro (HTTPS), que permite el acceso a las funcionalidades de gestión en cualquier momento y desde cualquier lugar.

El Cisco WCS permite realizar en la red inalámbrica las siguientes funciones:

- **Planificación y diseño de la LAN inalámbrica.** Mediante la herramienta de predicción de RF integrada se puede crear un diseño de red detallado, incluyendo la colocación de los puntos de acceso y la configuración de la misma estimando el rendimiento de la red. Se puede importar los planos de los edificios en el sistema y asignar las características de RF a las distintas áreas de los edificios para aumentar la exactitud del diseño. Los mapas de calor ayudan a visualizar el comportamiento de la red previsto para una planificación más fácil y realizar cambios más rápidamente.
- **Network Monitoring and Troubleshooting.** WCS de Cisco proporciona las herramientas que permiten la visualización del diseño de la red inalámbrica y monitorizan el rendimiento de la WLAN. Esto incluye mapas de calor detallados que indican la cobertura de RF en relación con el plan importado. Además se dispone de un portal para gestionar la RF en tiempo real consultando las informaciones proporcionadas por los WLAN Controllers, incluyendo la asignación de los canales y la potencia de emisión de los Access Points. Con estas informaciones Cisco WCS permite consultar los datos de cobertura, las alarmas y las estadísticas de la WLAN de modo que se pueda actuar rapidamente en caso de fallo de la red.
- **Secure Guest Access.** Cisco WCS soporta la customización del acceso de “invitados” a la red para garantizar la seguridad de la red y proporcionar el acceso a usuarios externo a la empresa.
- **Indoor Location Tracking.** Cisco WCS puede asociar cual Access Point está asociado a un device inalámbrico y así determinar cual es la localización de cada equipo inalámbrico conectado a la red.
- **Software Update.** Cisco WCS permite la actualización del software de los equipos de la WLAN desde un punto centralizado.
- **Network Mapping.** Cisco WCS descubre automáticamente los equipos de la WLAN a gestionar, permitiendo eliminar los errores de configuración manual de la base de datos de los equipos.
- **Informes Personalizados.** Cisco WCS permite la realización de informes personalizados para documentar la actividad de la red. Esto incluye estadísticas de clientes, utilización de la RF, contadores 802.11, alarmas, etc...

6.3 GESTIÓN DE LA RED DE VOZ CORPORATIVA

En este apartado del documento se describe cual será la arquitectura de gestión para la red de voz corporativa. En este escenario se propone utilizar los elementos Cisco Unified Operations Manager (CUOM) para la supervisión en tiempo real de los dispositivos Cisco de la solución y el elemento Cisco Unified Service Monitor (CUSM) para la monitorización y evaluación de la calidad de la voz.

Los restantes elementos de la solución (iSSW y Session Border Controller) disponen tanto de funciones FCAPS embebidas como de interfaces estándar para la fácil integración con sistemas comerciales y por lo tanto no se considera necesario que dispongan de un elemento de gestión dedicado.

Sin embargo se propone la utilización de las plataformas i-A&BM (Italtel Accounting&Billing Management) y Serviber de AT4Wireless para implementar una gestión flexible del control de los costes.

La arquitectura de gestión será por la tanto la indicada en la figura siguiente:

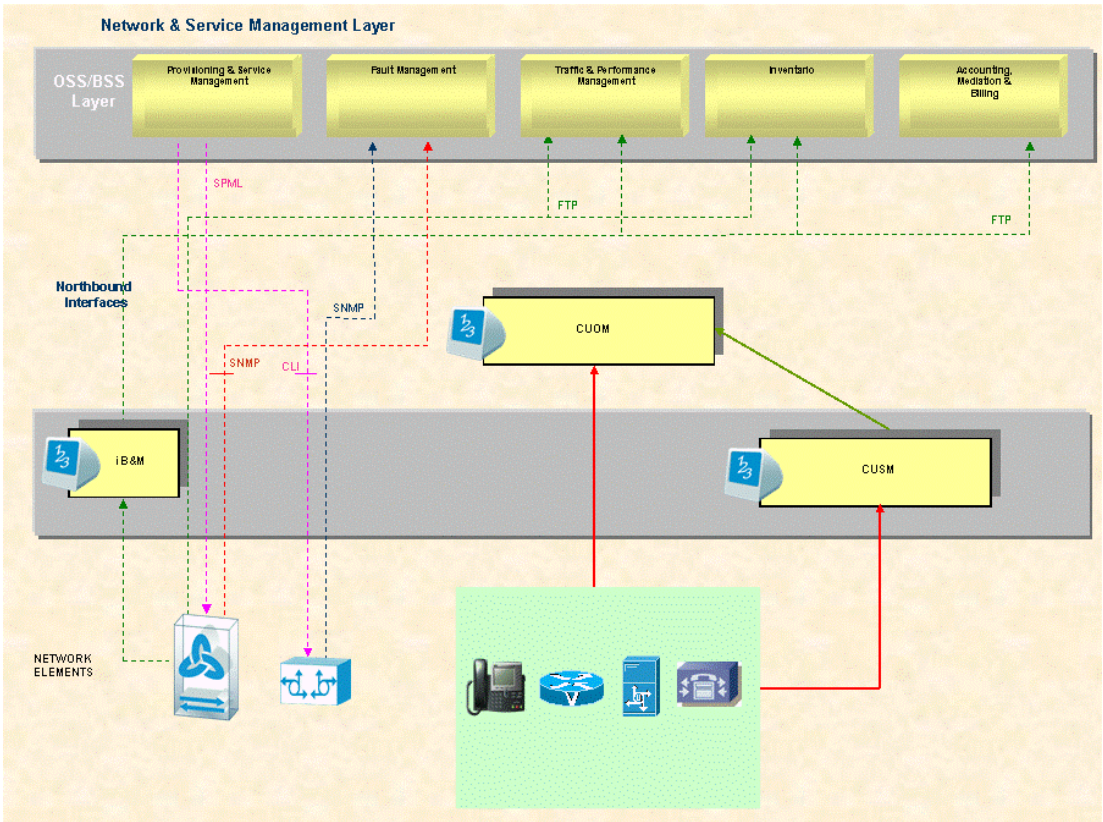


Figura 28 Arquitectura de gestión red de voz corporativa

6.3.1 CISCO UNIFIED OPERATIONS MANAGER

Cisco Unified Operations Manager; para esta propuesta con la versión 1.0 monitoriza el estado de la infraestructura de Comunicaciones IP y de la infraestructura que la soporta. Usa interfaces abiertos como Simple Network Management Protocol (SNMP) y Hyper Text Transfer Protocol (HTTP) para recoger remotamente información de los distintos elementos Cisco que formen parte del despliegue. No necesita de la implementación de ningún agente software en los dispositivos que monitoriza y por tanto es no-disruptivo para la operación de los sistemas.

Con esta herramienta se monitorizarán lo siguientes equipos:

- Cisco Unified CallManager
- Cisco Unity
- Cisco IP Phones
- Cisco Gateways
- Cisco Routers
- Cisco Switches

Las funcionalidades principales de esta herramienta que serán utilizadas son:

- Descubrimiento automático de dispositivos y teléfonos
- Vistas de nivel de servicio (estado de funcionamiento) del despliegue completo del sistema de telefonía con información en tiempo real de todos los dispositivos monitorizados.

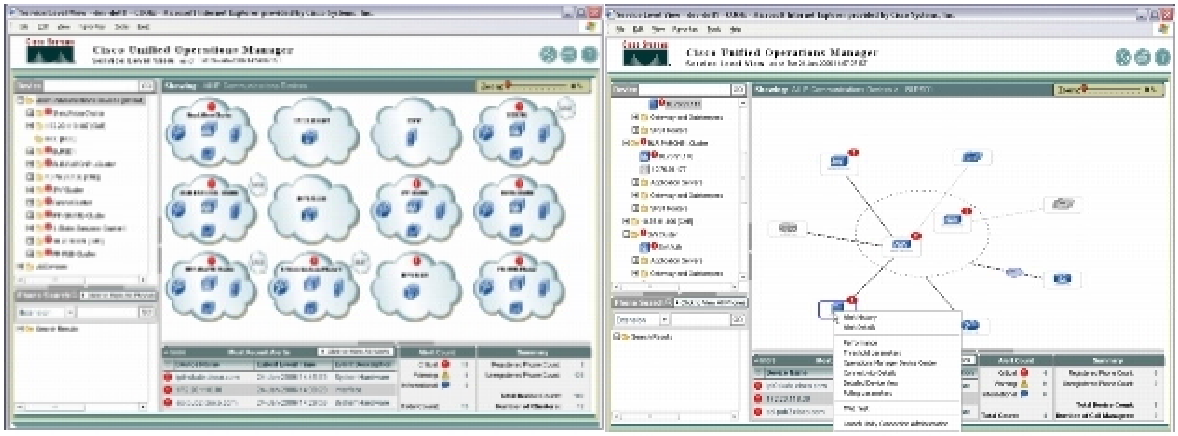


Figura 29 CUOM: Información visual a nivel de servicio

- Incrementa la productividad del gestor de la red y permite una rápida resolución de problemas ofreciendo herramientas de diagnostico para el troubleshooting.
- A través de tests de diagnóstico, rendimiento y detalles de conectividad sobre los diferentes elementos de la solución.
- Usando test sintéticos que replican la actividad del usuario final y verificando la disponibilidad del gateway y otras configuraciones y aspectos de la operación de la solución de Cisco
- A través de Service-level agreement (SLA), test que pueden medir el rendimiento de enlaces WAN y la calidad de la red entre nodos Cisco
- Ofreciendo información en los mensajes de notificación sobre la que haciendo un click nos lleva a un nivel mayor de detalle sobre los cortes en el servicio
- Presenta alertas de la calidad del servicio usando la información disponible a través del Cisco Unified Service Monitor 1.0 (presentado en esta oferta). Presenta el resultado de MOS asociado a la calidad de voz entre pares de terminales (teléfonos IP, gateways, buzón
de voz…) y el tiempo donde se produjo un posible problema. Puede también similar una conversación entre dos terminales y reportar cortes o problemas en nodos intermedios.

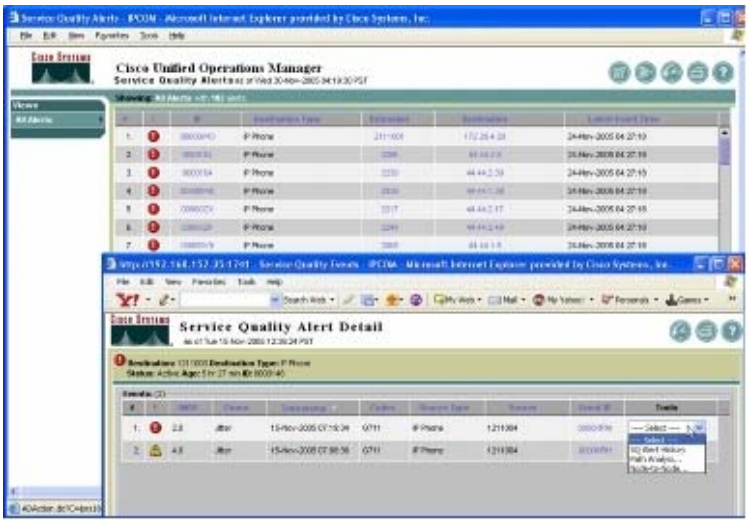


Figura 30 CUOM: Alerta de calidad de servicio

- Proporciona información actual sobre cortes en la conectividad o el registro que afecten a los teléfonos IP en la red y ofrece información para permitir la localización e identificación de los teléfonos IP.

- Permite el seguimiento de los dispositivos de Comunicaciones IP, inventario de teléfonos, hace el seguimiento de los cambios de estado en los teléfonos y crea varios tipos de informes que documentan los cambios, movimientos y añadidos de terminales en la red que gestiona.
- Ofrece la posibilidad de integración con herramientas de gestión de más alto nivel vía alarmas en tiempo real en modo de traps SNMP y notificaciones syslog. También permite enviar e-mails ante determinados problemas en la red.
- Estado de los terminales e informes de cambio en los mismos (se monitoriza a qué switch está conectado e incuso de qué router con funcionalidad srst depende cada teléfono).
- Supervisión y recolección de nivel de variables de dispositivos Cisco (CPU, memoria, utilización de DSPs, utilización de Primarios, etc.).

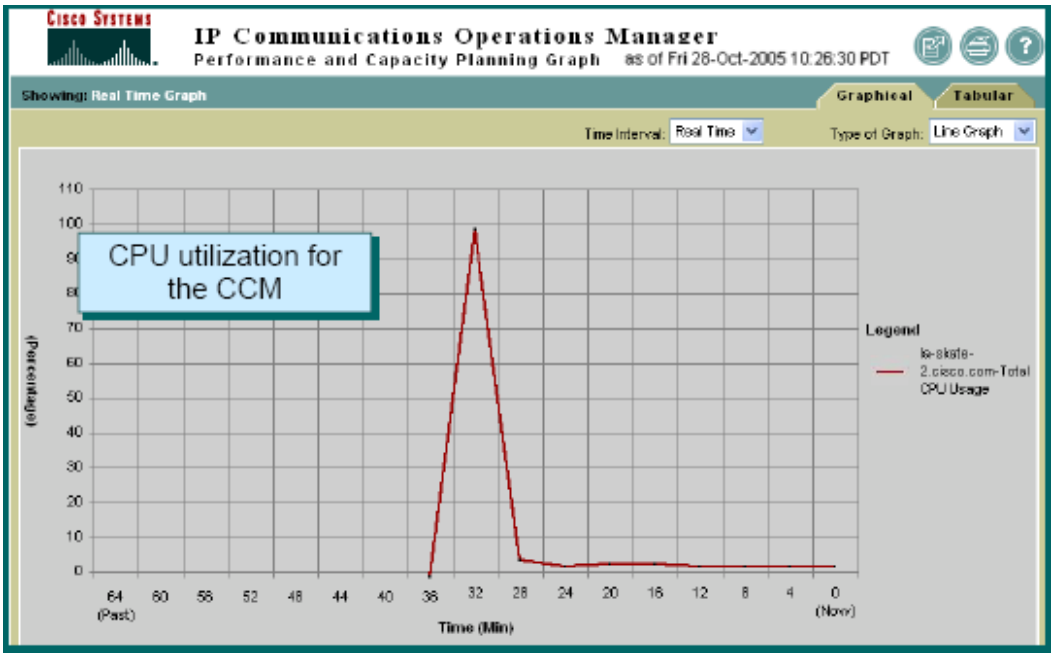


Figura 31 CUOM: Visualización estadísticas de rendimiento

Gracias a la posibilidad de definición personalizada de vistas y separación por clusters se pueden diferenciar la gestión de los distintos cluster presentes de ToIP

6.3.2 CISCO UNIFIED SERVICE MONITOR

Para una monitorización más eficiente y proactiva se propone la plataforma Cisco Unified Service Monitor (CUSM) en su versión 2.0. CUSM proporciona un eficiente método de monitorización y evaluación de la calidad de la voz en soluciones de Comunicaciones Unificadas de Cisco. CUSM monitoriza continuamente las llamadas activas y proporciona notificaciones en tiempo casi-real cuando la calidad de la voz cae por debajo de unos niveles definidos.
Para entender la experiencia del usuario en cuanto a la calidad de la voz, es necesario medir esta calidad y hacer un reporte de posibles problemas en tiempo quasi-real. Para este objetivo se implementa Cisco Unified Service Monitor.

La solución de Cisco Unified Service Monitor consiste en dos elemento: El sensor Cisco 1040 y una aplicación software centralizada. El sensor Cisco 1040 monitoriza los streams RTP y obtiene el MOS. El software centraliza toda la información, controla los sensores y provee información al Cisco Unified Operations Manager o a otros gestores vía SNMP.
Algunas de sus funciones clave son: (mirar también la siguiente figura):

- **Monitorización de la calidad de la voz en tiempo real**. Cisco Unified Service Monitor ayuda a los gestores de la red a gestionar eficientemente las soluciones basadas en los sistemas Cisco Unified Communications proporcionando información en tiempo quasi-real sobre la experiencia del usuario asociada a las llamadas activas en su red. Esta experiencia
  se expresa como Mean Opinion Score (MOS) y se calcula según el estándar ITU G.107. La experiencia del usuario es capturada, analizada y reportada con el dato MOS cada 60 segundos.
- **Alertas de Calidad de Voz en tiempo Real**. Cisco Unified Service Monitor monitoriza la calidad del servicio analizando los flujos Real-Time Transport Protocol (RTP) entre terminales IP. Si el valor del MOS, cae for debajo del humbral definido, se genera un trap SNMP (Simple Network Management Protocol) y se envía al Cisco Unified Operations Manager o a la plataforma de gestión implementada en la AIE. El Cisco Unified Operations Manager utiliza esta información para presentar alarmas de voz a nivel se servicio en su pantalla en tiempo quasi-real y asiste con otras informaciones para la resolución de los problemas que hayan podido ocasionar esa perdida de calidad.

- **Facilidad de Instalación y uso**. El despliegue de los sensores Cisco 1040 y su configuración es similar a la de un teléfono IP. Usan el estándar IEEE 802.3af Power over Ethernet (PoE), obtiene su configuración por TFTP, que puede ser el mismo que el usado para los terminales de voz, y usa Skinny Client Control Protocol (SCCP) para asegurar la continua comunicacion con el Cisco Unified Service Monitor.
- **Escalabilidad y redundancia**. Cada copia del software centralizado Cisco Unified Service Monitor soporta hasta 50 sensores. Se pueden desplegar múltiples instancias del CUSM con el fin de hacer el despliegue más distribuido y redundante. Cada sensor Cisco 1040 puede monitorizar hasta 80 streams RTP. El switch puede ser configurado para hacer span del tráfico entrante y saliente, siendo la configuración optima hacer span solo del tráfico entrante. En un despliegue típico los sensores se colocan en parejas en los puertos Switch Port Analyzer (SPAN) asociados con switches lo más cercanos a los teléfonos IP. Cada Sensor puede configurar multiples Cisco Unified Service Monitor (como primario, secundario…) para asegurar alta disponibilidad y fiabilidad en cuanto a la monitorización de la calidad de voz.
- Interfaces Northbound. Cisco Unified Service Monitor proporciona traps SNMP que pueden ser enviados al Cisco Unified Operations Manager o cualquier otra plataforma comercial. En el caso especifico se propone el envío de las traps SNMP al Cisco Unified Operations Manager.

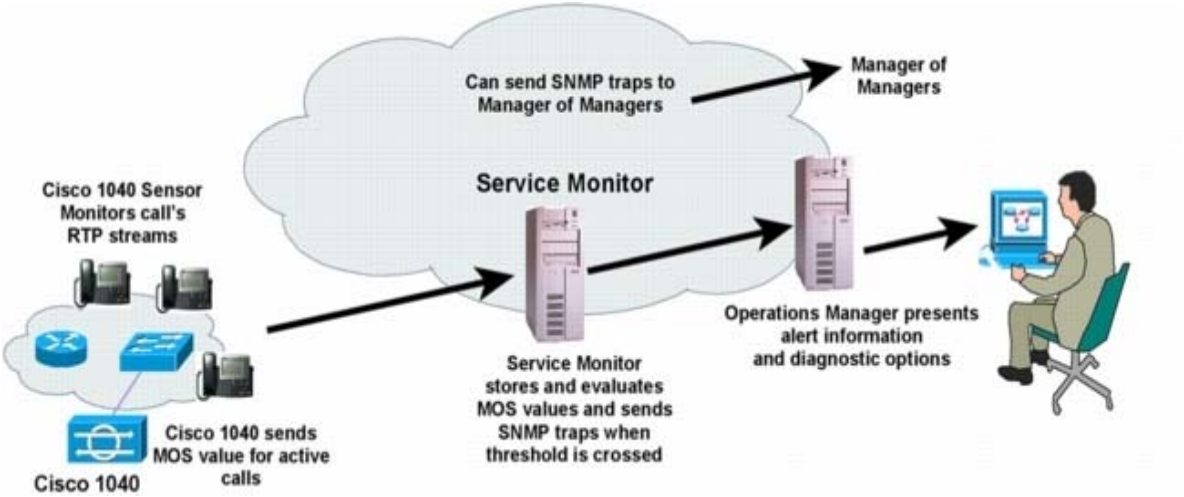


Figura 32 Cisco Unified Service Monitor

6.3.3 GESTIÓN I-SSW

Como indicado anteriormente para la gestión del i-SSW no se propone un elemento de gestión dedicado en cuanto se consideran suficientes para la gestión de los elementos las interfaces northbound Standard proporcionadas por el mismo elemento. Solo se propone un servidor externo que realice las funciones da recogida y almacenamiento de los CDRs generados por el i-SSW.

6.3.3.1 Command Line Interface (CLI)

El sistema dispone de una interfaz CLI accesible localmente mediante consola o remotamente vía telnet. Esta interfaz permite la ejecución de comandos para realizar todas las tareas de operación y mantenimiento del equipo, que son:

- Configuration
- Provisioning
- Consultas de Alarmas
- Activación y consultas de Estadisticas

Los comandos pueden ser interactivos o ejecutables en modalidad “batch”.

6.3.3.2 Estadísticas

Los datos de las medidas de tráfico generados en el i-SSW pueden ser exportados en ficheros en formato XML, que estarán disponibles en un directorio dedicado y el genérico sistema utilizador puede recogerlos mediante protocolo FTP.
La activación de las medidas de trafico puede realizarse mediante el interfaz CLI mencionado anteriormente o mediante el intercambio de traps SNMP con el sistema de análisis del trafico.

6.3.3.3 Alarmas

Las alarmas detectadas por el i-SSW y generadas por el mismo en tiempo real se pueden exportar mediante traps SNMP a sistemas de supervisión comerciales.

6.3.3.4 Accounting

Los CDRs se generan llamada por llamada. Cada registro contiene el detalle de las informaciones relevantes (para estadísticas y para facturación) de una llamada, como son:

- Información del llamante

- Información del llamado
- Información del destino de la llamada
- Resultado de la llamada
- Duración de la llamada
- Enlaces de entrada y salida
- Informaciones de QoS

Si el resultado de la llamada fuera negativo en las informaciones presentes en el CDR se indica la causa del fallo tanto si depende de la red de señalización como de anomalías internas del iSSW. En cualquier caso se indica el valor establecido en la norma ITU-T Q.850 para definir la causa del fallo de la llamada.
Los CDRs generados por el iSSW se recogen y almacenan en el iA&BM, que se ocupa de formatearlos en el formato estándar XML y los mete a disposición de los sistemas utilizadores, ejecutando los siguientes pasos:

- El modulo OMS del i-SSW recoge periódicamente todos los CDR de todos los módulos, y los prepara para su transferencia al iA&BM. El período de transferencia se puede configurar.
- El iA&BM recoge los CDR y convierte su formato a otro más adecuado para los sistemas utilizadores.
- Los CDR convertidos se almacenan en un búfer de duración configurable (típicamente, se almacenan durante 5 días).
- Los CDR que se hayan transmitido se mueven a un búfer configurable de “otra copia”, quedando disponibles para los sistemas utilizadores, por si fuese necesario volver a recuperarlos.
- Además en el iA&BM se guarda una copia de los CDRs en el formato propio del i-SSW.

El protocolo utilizado para la transferencia de los CDR es el FTP.

6.3.4 GESTIÓN SESSION BORDER CONTROLLER

Como indicado anteriormente para la gestión de los SBC’s no se propone un elemento de gestión dedicado en cuanto se consideran suficientes para la gestión de los elementos las interfaces northbound Standard proporcionadas por el mismo elemento.

6.3.4.1 Command Line Interface (CLI)

El sistema dispone de una interfaz CLI accesible localmente mediante interfaz serial o remotamente vía telnet. Esta interfaz permite la ejecución de comandos para realizar todas las tareas de operación y mantenimiento del equipo, que son:

- Configuration
- Provisioning
- Control
- Log Viewing
- Monitoring

Los comandos pueden ser interactivos o ejecutables en modalidad “batch”.

6.3.4.2 XML

La interfaz XML disponible en el SBC permite la realización de las tareas de configuración y provisión desde sistemas OSS comerciales.

Las tareas XML soportadas son:

- Create
- Get
- Read
- Save
- Delete

6.3.4.3 SNMP

El SBC soporta interfaces SNMP que permiten la integración con sistemas OSS comerciales.

La versión del protocolo soportada en SNMPv2. El elemento dispone de MIB específicas para la monitorización del sistema y MIBs adicionales como son:

- MIBII – estadísticas de red (RFC-1213)
- Syslog MIB – interfaz de trazas
- Host resources MIB – estadísticas de sistema operativo, file system, procesos, etc..

El sistema soporta múltiples SNMP communities y la generación de las TRAPs puede ser gestionada mediante filtros definidos para cada comunidad que tenga acceso al sistema. Una lista de acceso controla los accesos remotos vía SNMP.

6.3.5 CONTROL DEL COSTE

La solución propuesta para control de costes está basada en la aplicación Serviber de la compañía AT4Wireless.
La solución propuesta se basa principalmente en la implantación de dos sistemas que operan de forma integrada:

- **Serviber BS:** para la gestión y control de la tarificación de las centrales telefónicas y sistemas de telefonía IP. Incluye Módulo de Tarificación Web y Módulo de Análisis de Tráfico.

- **Serviber GF**: para la gestión y verificación de las facturas de los distintos operadores, permitiendo realizar un reparto de los costes y la generación de una factura unificada a los distintos centros de coste.

Dentro de la solución propuesta, los Call Detailed Records (CDRs) se generan en dos elementos: en el iSSW para todas las llamadas cursadas por este (en función del modelo de arquitectura seleccionado) y en los CCMs.

Los CDRs disponibles en el iA&BM y en los CCM serán recogidos por el sistema Serviber y elaborados según las necesidades del AIE siendo configurable los report a realizar. En la figura que sigue se indica come sería el esquema de conexión de los sistemas involucrados en esta tarea:

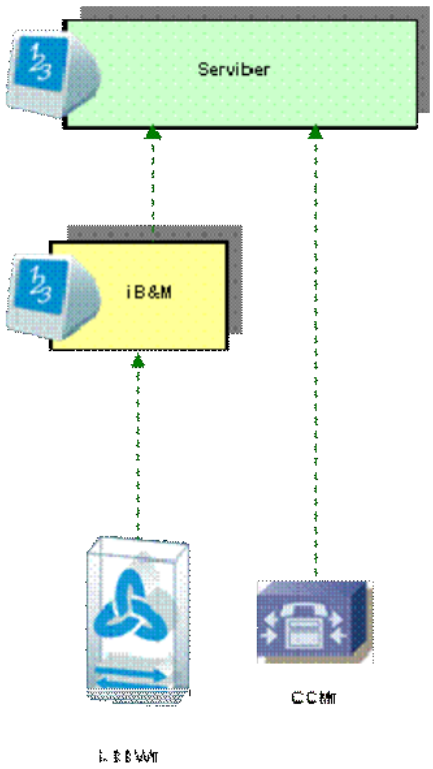


Figura 33 Arquitectura para control de costes

6.3.5.1 Serviber BS: Gestión de Tarificación

Como principales características funcionales del sistema se pueden destacar las siguientes:

- **Multioperador**: el sistema tarifica según el precio del Operador Telefónico a través del cual se efectúan las llamadas (Telefónica, ONO, Orange, BT, Jazztel, Colt Telecom, Tele2, Vodafone, etc.).
- **Tarificación de extensiones, líneas de enlace, códigos de acceso, móviles y centros de coste**: Serviber BS procesa y almacena datos de tarificación relativos al tráfico telefónico generado por llamadas entrantes, salientes, interiores y transferidas (según PABX) por cada línea de enlace, extensión y código de acceso.
- **Control de llamadas excepcionales**: El sistema permite marcar aquellas llamadas que cumplan un determinado patrón de excepciones.
- **Representación Gráfica del Organigrama**: Todos los recursos telefónicos de la empresa quedan recogidos de forma flexible, visual y sin límite de niveles en el Organigrama.

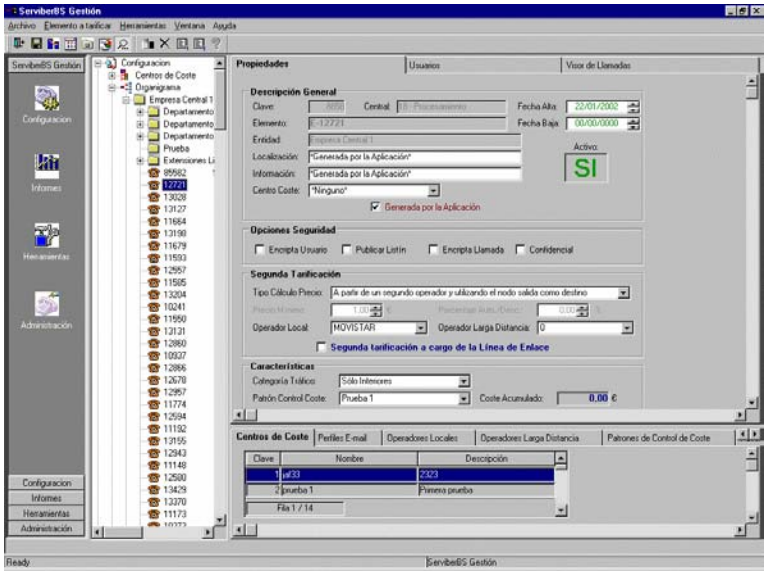


Figura 34 Servidor Serviber

- **Generación automática nuevos elementos a tarificar**: Serviber BS es capaz de detectar, generar y configurar nuevos elementos sobre en el Organigrama de forma automática.
- **Doble Tarificación**: El Sistema tiene como característica la posibilidad de tarificar aplicando los costes del Operador principal y otro secundario. Esto posibilita la comparación del tráfico cursado y del coste generado entre ambos operadores.
- **Actualización de Tarifas**: La actualización de las tarifas de los Operadores se realiza de forma sencilla; mediante un sencillo asistente que efectúa una conexión FTP con el servidor de AT4Wireless.
- **Avisos**: Serviber BS dispone de una herramienta de monitorización que informa sobre la actividad del sistema mediante la configuración y generación de avisos o alarmas.
- **Consultas e Informes**: Serviber BS dispone de un amplio abanico de informes predefinidos, así como la posibilidad de generar informes personalizados por el usuario. Estos informes pueden ser obtenidos en pantalla, impresora, en formato PSR, HTML y muchos de ellos pueden ser incluso configurados para poder ser enviados directamente por e-mail.

- **Tareas Programadas**: Serviber BS permite definir como tareas programadas los principales procesos de administración y explotación del sistema, como procesamiento de la información, emisión de informes, comunicación con las distintas centrales, etc.

6.3.5.2 Serviber BS WEB

Serviber BS WEB permite realizar consultas a través de su navegador de la información relativa al tráfico telefónico de su empresa, accediendo a la misma información que se encuentra en su Tarificador y posibilitando que la información almacenada esté disponible para todos los usuarios Web tanto en la modalidad de Intranet como de Internet. El usuario sólo requiere de un PC con un navegador Web, sin necesidad de realizar ninguna instalación adicional.

A continuación se describen los principales módulos del sistema.

Jerarquía

Es posible consultar el Organigrama de cada uno de los distintos centros.

Dispone además de un servicio de directorio (listín telefónico) vía WEB con un interfaz sencillo e intuitivo para la búsqueda por diferentes criterios, tal como se muestra en la siguiente figura:

Figura 35

Listados

Posibilidad de realizar distintos tipos de Listados sobre el consumo telefónico (globales, detalle, desglosados, listines telefónicos, etc...)

Gráficos

Posibilidad de realizar distintos Gráficos según distintos conceptos (coste, nº de llamadas y duración) en distintos formatos: barras horizontales, verticales, en tarta, etc.

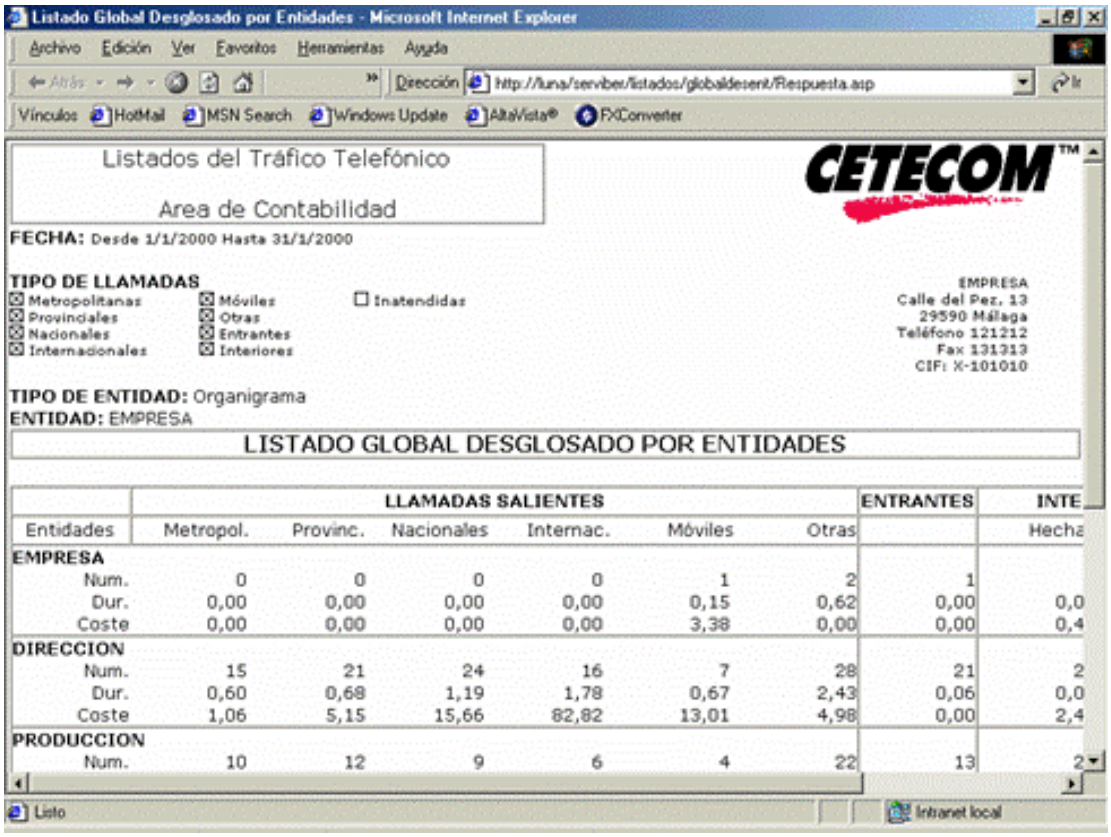


Figura 36 Serviber: Gráficos

Herramientas

Herramienta Web que permite consultar las tarifas de los distintos operadores. Además permite realizar una simulación del coste de una llamada según las tarifas de los distintos operadores, de esta forma sabremos cuál es el operador más óptimo según el tipo de llamada a realizar.

Administración

El Administrador de su sistema podrá dar de alta cada uno de los usuarios que harán uso de Serviber BS WEB y a cada uno de ellos le asignará el nivel de permisos adecuado que vendrá determinado por las distintas opciones dentro de cada módulo al que tienen acceso e, incluso, determinar qué entidades del organigrama estarán visibles para cada usuario. De esta forma,

el usuario sólo podrá realizar los informes para los que tenga permiso relativos a las entidades definidas en su perfil.

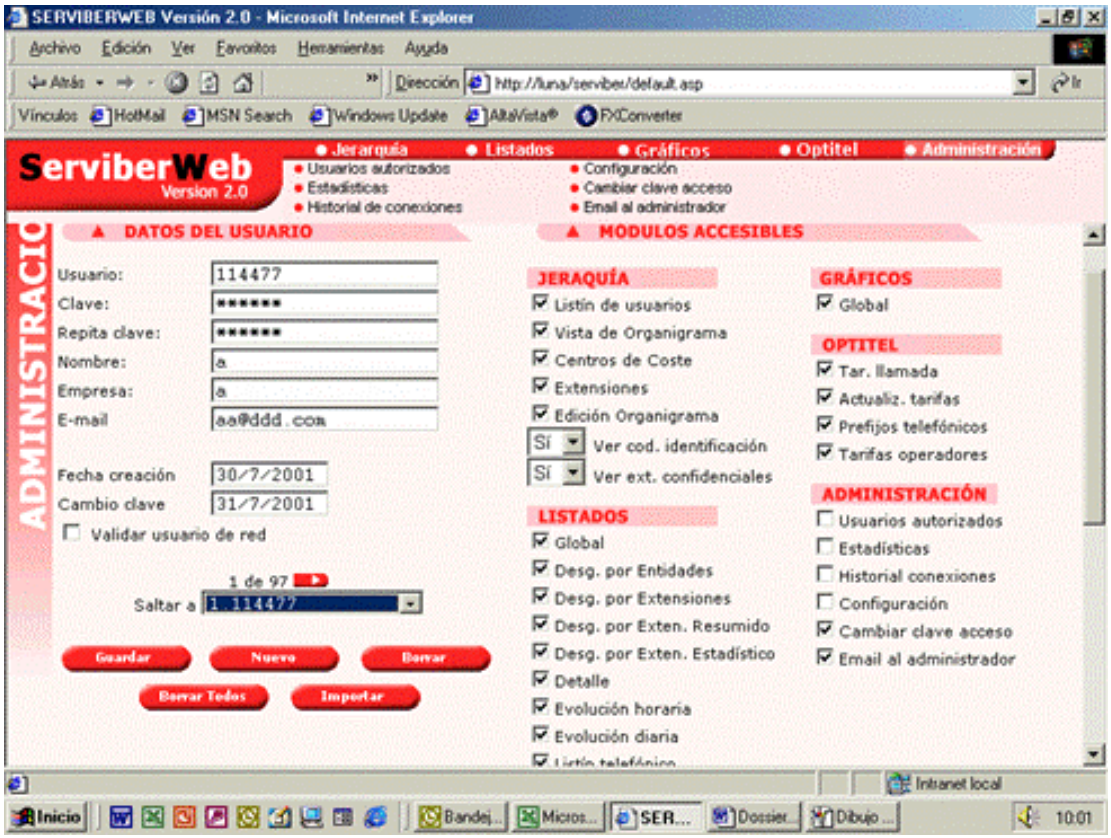


Figura 37 Serviber BS Web. Administración

Características diferenciadoras

- Flexibilidad y potencia. Con esta nueva funcionalidad se abre al mundo Internet.
- Facilidad de manejo. Interfaz Web completa tanto a nivel de usuario como administrador.
- Cliente ligero. El usuario de Serviber BS WEB sólo requiere en su PC conectividad con la Red y un navegador Web.
- Total integración. Totalmente compatible con su sistema actual de tarificación de AT4Wireless. Puede compartir la misma base de datos.
- Obtención de estadísticas e informes acerca de la actividad del sistema. Información sobre las conexiones de los distintos usuarios y qué información han consultado.

Por sus características, Serviber BS ha sido seleccionado por las principales empresas y organismos públicos de gran tamaño como el más idóneo para la gestión de la tarificación de sus redes de comunicaciones, contando en la actualidad con implantaciones de proyectos de más de 60.000 extensiones y más de un centenar de centrales.

6.3.5.3 Serviber GF: Gestión de la Facturación

Como características generales del sistema se pueden destacar las siguientes:

- Arquitectura J2EE: El sistema esta enmarcado dentro de la plataforma J2EE y utilizará una arquitectura multinivel que asegura la independencia entre los distintos niveles de la aplicación (lógica de presentación, lógica de negocio, servicios).
- Interfaz de usuario basado en Web

A continuación se describen los principales procesos que pueden realizarse con el sistema.

Gestión de Facturas

- Configuración del formato de las facturas: desde una de las opciones del interfaz se podrán configurar los distintos formatos de las facturas y las características del proceso de carga de las facturas de diferentes operadores (Telefónica, MoviStar, Vodafone, Auna, Amena, etc.), con posibilidad de determinar la información a procesar en cada una de las facturas (cabecera, servicios, totales por número, detalle por número, descuentos,...)
- Carga y procesamiento de las facturas de múltiples operadores, tanto de telefonía fija como móviles o datos.
- Consulta de las facturas cargadas: El sistema permite la presentación y consulta homogeneizada de todas las facturas procesadas, con diferentes vistas según el tipo de información y posibilidad de filtrado.
- Asignación de Costes: de los servicios, conceptos y llamadas que aparecen en las facturas a los distintos elementos del organigrama.
- Facturación unificada: una vez realizado el proceso de asignación de costes, la generación de la factura unificada supone asociar a un periodo de facturación definido por el cliente los costes de una serie de facturas de diferentes operadores, pudiendo además utilizar un coeficiente para calcular los costes que se imputarán a cada centro de coste a partir de los costes de las facturas de los operadores.

Gestión del Organigrama

- Representación gráfica del organigrama de la empresa, con varios niveles entre los que se incluyen los centros de coste y los empleados. La gestión del organigrama incluye la creación, edición y borrado de los elementos, además de mover una rama completa o imprimir el árbol.

- Además, el sistema dispone de un mecanismo de importación del organigrama y del inventario de servicios para que pueda ser cargado desde archivos de texto con un determinado formato.

Informes

- Se podrán realizar multitud de informes sobre la información procesada por el sistema, tanto de los costes de los servicios facturados como de aspectos del tráfico a partir de las llamadas contenidas en las facturas.

Administración De Usuarios

- La administración de los usuarios está basada en roles, posibilitando establecer distintas políticas de acceso a los datos de facturación telefónica de la empresa.
- Integración con un servidor LDAP para la autentificación de los usuarios, con la posibilidad también de sincronización periódica de la estructura de usuarios y roles desde el servidor LDAP hacia el sistema de gestión de facturas.

Análisis de la Facturación (Panel de Control)

El sistema incluye una potente herramienta de análisis de la facturación enfocada a los responsables de las distintas entidades que componen la estructura organizativa del cliente. Esta herramienta proporciona, de una forma gráfica y muy intuitiva, distintos niveles de desglose de la información según diferentes criterios y permite consultar la evolución temporal de los conceptos seleccionados.

6.3.5.4 Serviber BS: Módulo de Análisis de Tráfico

Permite conocer y tomar decisiones relativas al volumen de tráfico telefónico cursado, cuya medida se expresa en “erlangs” (intensidad de tráfico correspondiente a un dispositivo o grupode dispositivos o a un circuito o grupo de circuitos, que cursan un volumen de llamadas durante un periodo de tiempo determinado.
Ofrece información para tomar decisiones relativas a la dimensión óptima de la Red de Comunicaciones, evitando problemas de saturación de los recursos disponibles y favoreciendo la calidad del servicio ofrecido.

Figura 39 Serviber Análisis de Tráfico